

802.11g Wireless LAN Access Point

USER MANUAL

Contents

1. Overview.....	1
1.1 Product Feature	1
1.2 System Requirements	1
2. Getting Start with Access Point	2
2.1 Know the 54Mbps Wireless Network Access Point	2
2.2 Connect to the 54Mbps Wireless Network Access Point	2
2.3 Quick Setup with Wizard	3
2.3.1 Access the Setting Menu.....	3
2.3.2 Setup with Wizard.....	5
3. Configuration Access Point through WEB Browser	8
3.1 Status.....	8
3.2 Basic Setting	10
3.3 IP Setting	12
3.5 Security.....	15
3.6 Tools	16
4. Configuration through AP Utility.....	18
4.1 Link Information	18
4.2 AP Setting	19
4.3 IP Setting	21
4.4 WEP Setting	22
5. Glossary	24

1. Overview

1.1 Product Feature

- ? Compliance with IEEE **802.11g** and **802.11b** standards
- ? Highly efficient design mechanism to provide unbeatable performance
- ? Achieving data rate up to 54Mbps for 802.11g and 11Mbps for 802.11b with wide range coverage
- ? Strong network security with **WEP** encryption and **WPA-PSK**.
- ? Quick and easy setup with **Web-based management** utility.

1.2 System Requirements

- ? Windows 98SE, Millennium Edition (ME), 2000 and XP operating systems
- ? Microsoft Internet Explorer 5.5 or higher
- ? One CD-ROM drive
- ? At least one RJ-45 Ethernet network adapter installed.

2. Getting Start with Access Point

2.1 Know the 54Mbps Wireless Network Access Point

Ports:

- ? Power Receptor
- ? Reset Button
- ? RJ-45 Ethernet Port

Straight through cable is required to connect with router or switch

Cross-over cable is required to connect to computer directly

LEDs:

- ? Power LED: ON when the unit is powered up
- ? LAN LED: ON indicates LAN connection; BLINK indicates LAN activity
- ? WLAN LED: ON indicates WLAN is working; BLINK indicates wireless activity.

2.2 Connect to the 54Mbps Wireless Network Access Point

Build the Infrastructure Mode



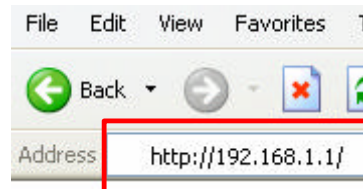
In order to setup an Infrastructure of a wireless network such as the example shown above, user will need the following:

1. A broadband Internet connection.
2. ADSL or Cable modem provided by ISP as part of the broadband connection installation.
3. A Router that connects to the ADSL/Cable modem for Internet connection sharing.
4. An Access Point to connect with the Router to form a wireless infrastructure network.
5. Wireless clients equipped with wireless networking devices such as wireless PC Card for wireless connection.

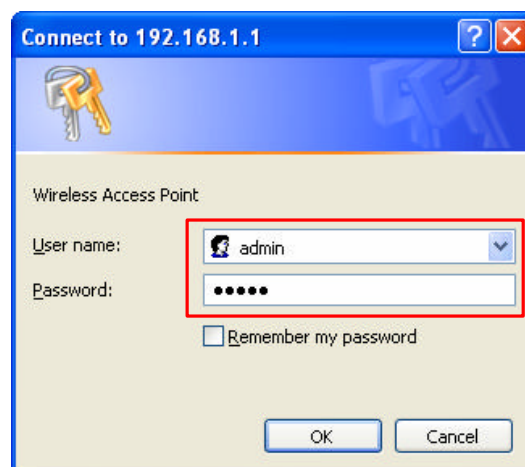
2.3 Quick Setup with Wizard

2.3.1 Access the Setting Menu

User could start to access the configuration menu anytime by opening a web browser window and typing the IP address of this access point. The default IP is 192.168.1.1.



The below window will popup. Please enter the user name and password. Both of the default is “admin”.



Now, the main menu screen is popup.



802.11g
Wireless LAN Access Point

| Wizard | **Status** | Basic Setting | IP Setting | Advanced Setting | Security | Tools |

Status

Firmware Version 1.02

LAN MAC:00-03-2F-24-F7-C2

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

Gateway: 0.0.0.0

Send: 97

Receive: 343

Wireless

SSID: default

Encryption Function : Disabled

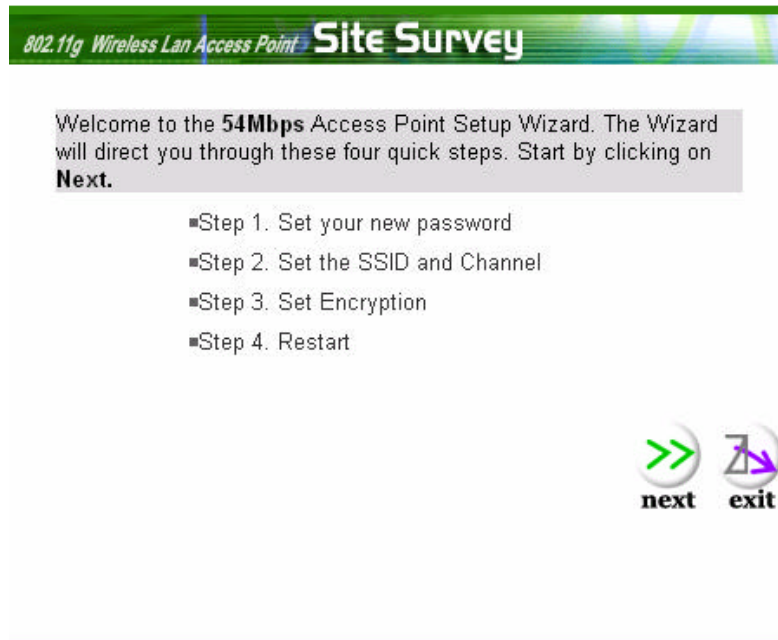
Channel: 6

Send: 1

Receive: 19

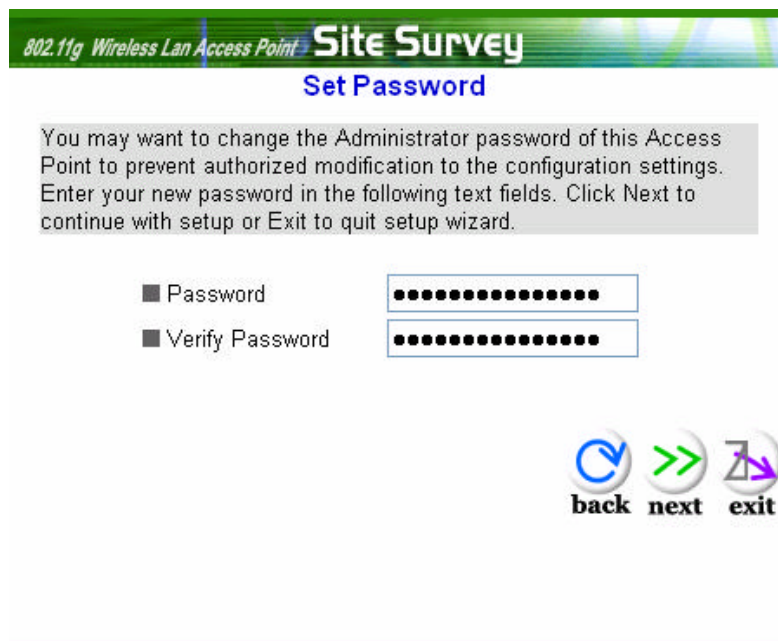
2.3.2 Setup with Wizard

Setup wizard is provided as the part of the web configuration utility. User can simply follow the step-by-step process to get Access Point configuration ready to run in 4 easy steps by clicking on the “**Wizard**” button on the function menu. The following screen will appear. Please click “**Next**” to continue.



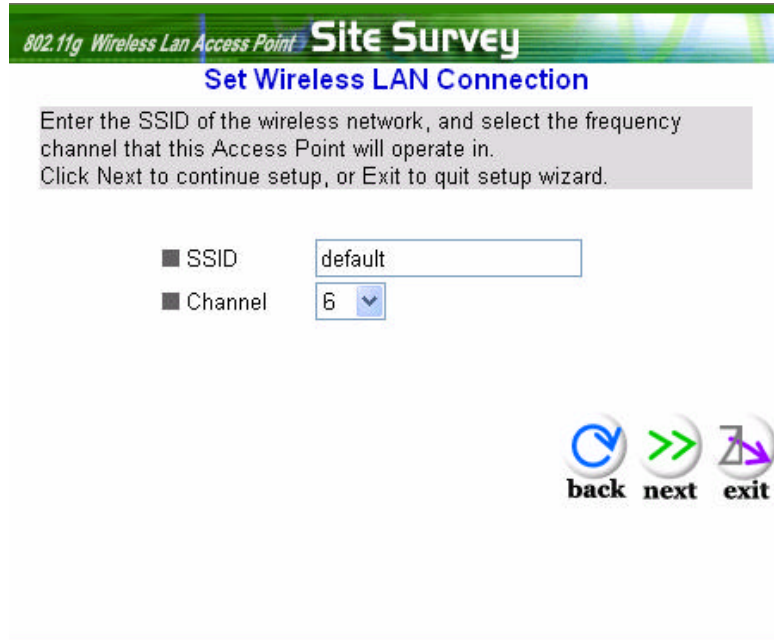
Step 1: Set Password

User can change the password and then click “**Next**” to continue.



Step2: Set WLAN Connection

Please type the name of SSID and select the channel. Then, click **'Next'** to continue.






802.11g Wireless Lan Access Point **Site Survey**

Set Wireless LAN Connection

Enter the SSID of the wireless network, and select the frequency channel that this Access Point will operate in.
Click Next to continue setup, or Exit to quit setup wizard.

■ SSID


■ Channel

back next exit

Step 3: Set WEP Encryption

If user wants to enable WEP, please click **"Enabled"**. Then, select the key size of WEP encryption and enter the key value in the key text box. Please click **"Next"** to continue.





802.11g Wireless Lan Access Point **Site Survey**

You may enable WEP security for data encryption by selecting Enabled. Select one of the WEP encryption key size and enter the value of the key in the text fields below.
Click Next to continue with setup, or Exit to quit setup wizard.

■ WEP Key Disabled 64bits 128bits

■ Mode

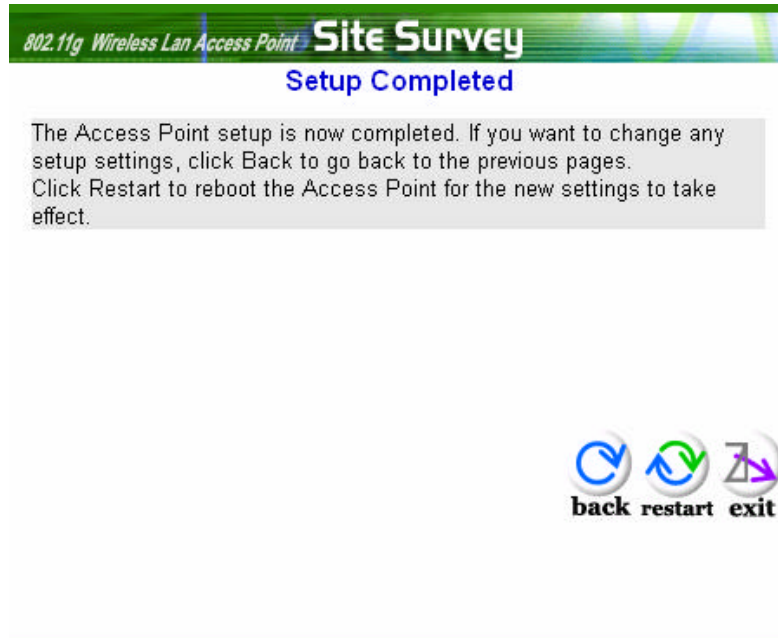
■ Key

back next exit

Step 4: Restart

The Setup wizard is now completed. The new settings will be effective after the Access Point restarted. Please click “**Restart**” to reboot the Access Point. If user does not want to make any changes, please click “**exit**” to quit without any changes. User also can go back to modify the setting by clicking “**back**”.



3. Configuration Access Point through WEB Browser

3.1 Status

This page as below shows the following information.




Firmware Version: Shows the current firmware version.

LAN: Shows the Mac address, IP address (default: 192.168.1.1), Subnet Mask, Gateway Address. The current LAN traffic calculated in terms of number of packets sent and received by AP through wired connection is also displayed.

Wireless: Shows the Mac address, current ESSID, the status of Encryption Function (Enable or Disable), the current using channel. The current wireless traffic calculated in terms of number of packets sent and received by AP through wireless communication is also displayed.

View Log: Once clicked, the page will change to login page. The login page records every event and the time that it happens.



The image shows a web interface for an 802.11g Wireless LAN Access Point. At the top, there is a banner with the text "802.11g Wireless LAN Access Point" and images of people using wireless devices. Below the banner, there is a navigation bar with buttons for "First Page", "Last Page", "Previous Page", "Next Page", "Clear Log", and "Refresh". A "View Log" link is also present. The log table has two columns: "Time" and "Message".

Time	Message
Jul/27/2004 11:14:20	System started
Jul/27/2004 11:14:20	SSID = default CHANNEL = 06

User may clear the entries recorded in the log by clicking the “**Clear Log**” button, and refresh the screen to show the latest log entries by clicking the “**Refresh**” button.

3.2 Basic Setting

This is the page allow user to change the access point settings.

The screenshot shows the 'Basic Setting' page for an 802.11g Wireless LAN Access Point. The page features a green header with the product name and a navigation menu. The main content area is white with a green sidebar on the left labeled 'Basic Setting'. The settings include: AP Name (Wireless Access Point), SSID (default), Channel (6), Authentication (Open System selected), WEP Key (Disable selected), Mode (ASCII), and four radio buttons for key lengths (1, 2, 3, 4). Buttons for Apply, Cancel, and Help are at the bottom.

AP Name: The name of the AP, which can be used to identify the Access Point among the all the Access Points in the wireless network.

SSID: Service Set Identifier, which is a unique name shared among all clients and nodes in a wireless network. The SSID must be identical for each clients and nodes in the wireless network.

Channel: The channel that AP will operate in. User can select the channel range from 1 to 11 for North America (FCC) domain, 1 to 13 for European (ETSI) domain and 1 to 14 for Japanese domain.

Authentication Type: The authentication type default is set to open system. There are four options: open system; shared key; WPA and WPA-PKS. User may want to set to Shared Key when the clients and AP in the same wireless network enable the WEP encryption. All the nodes and hosts on the network must use the same authentication type.

WEP Key: To disable WEP security, click on the “Disable” option. To enable WEP security, there are 2 types to select – 64bits and 128 bits. When it is selected, the key value must be entered in ASCII or HEX format.

Note: When WEP security is enabled, all the wireless clients that wish to connect to the Access Point must also have WEP enabled with the identical WEP Key value entered.

Apply: For the changes made to any of the items above to be effective, click “Apply”. The new settings are now been saved to Access Point and will be effective once the Access Point restarts.

If **WPA-PSK** is enabled, user needs to set the key in the passphrase field as the below screen. The key length should be 8 characters at least.



The screenshot shows the configuration interface for an 802.11g Wireless LAN Access Point. The page title is "802.11g Wireless LAN Access Point". The navigation menu includes "Wizard", "Status", "Basic Setting" (highlighted), "IP Setting", "Advanced Setting", "Security", and "Tools". The "Basic Setting" section is active, showing the following fields and options:

- AP Name:** Wireless Access Point
- SSID:** default
- Channel:** 6
- Authentication:** Open System Shared Key WPA-PSK
- Passphrase:** [Empty text box]
- Confirmed Passphrase:** [Empty text box]

At the bottom of the form, there are three buttons: "Apply", "Cancel", and "Help".

3.3 IP Setting

This page allows user to configure the IP and DHCP settings of the Access Point.

The screenshot shows the configuration interface for the 802.11g Wireless LAN Access Point. The page title is "802.11g Wireless LAN Access Point". The navigation bar includes "Wizard", "Status", "Basic Setting", "IP Setting", "Advanced Setting", "Security", and "Tools". The "IP Setting" section is highlighted in the sidebar. The main content area has a light blue background. The "LAN IP" section has two radio buttons: "Obtain IP Automatically" (unselected) and "Fixed IP" (selected). Below this are three rows of input fields: "Address" (192, 168, 1, 1), "Subnet Mask" (255, 255, 255, 0), and "Gateway" (0, 0, 0, 0). The "DHCP Server" section has two radio buttons: "On" (unselected) and "Off" (selected). Below this are two rows of input fields for "IP Range": "From" (192, 168, 1, 100) and "to" (192, 168, 1, 199). The "DNS Server" section has one row of input fields (0, 0, 0, 0). At the bottom are three buttons: "Apply", "Cancel", and "Help".

The default IP address of this access point is 192.168.1.1 with the subnet mask of 255.255.255.0. User can type in other values for IP Address, Subnet Mask and Gateway and click “**Apply**” button for the changes to be effective.

User can also set the Access Point to obtain the IP from a DHCP server, but it is not recommended. Select the option “Obtain IP Automatically” and click “**Apply**” button for the changes to be effective.

DHCP Server: It is not recommended to enable the DHCP Server if user has a DHCP server running in LAN network because it probably will cause possible the conflict of IP assignment. Enable the DHCP server function by selecting the option “**On**”, and enter the IP range.

Click “**Apply**” for the changes to be effective.

3.4 Advanced Setting

This page contains configurations for advanced users, which the change reflects the wireless performance and operating modes.



802.11g
Wireless LAN Access Point

| Wizard | Status | Basic Setting | IP Setting | **Advanced Setting** | Security | Tools |

Advanced Setting

Beacon Interval (msec, range: 1~1000, default: 100)

RTS Threshold (range: 256~2432, default: 2432)

Fragmentation Threshold (range: 256~2346, default: 2346, even number only)

DTIM Interval (range: 1~255, default: 3)

SSID broadcast Enable Disable

Mode Setting G Mode Mix Mode

TX Rates (Mbps)

AP Mode: Select one of the AP operating modes for different application of Access Point.

AP – The normal Access Point operating mode which forms a wireless ESS network with its wireless clients.

Note: All APs have to use the same **Channel** and **SSID** in order to set a Multiple Bridge network.

Beacon Interval: To set the period of time in milliseconds that AP sends out a beacon. Default is 100 milliseconds.

RTS Threshold: To set the size of RTS/CTS packet size. Default is 2432 bytes.

Fragmentation Threshold: To set the number of bytes used for the fragmentation boundary for directed messages. Default is 2436 bytes.

DTIM Interval: This value indicates the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the access point has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM interval value. Access point clients hear the beacons and awaken to receive the broadcast and multicast messages.

SSID Broadcast: While SSID Broadcast is enabled, all wireless clients will be able to communicate with the access point. For secure purpose, user may want to disable SSID broadcast to allow only those wireless clients with the AP SSID to communicate with the access point.

3.5 Security

This page is where user configures the security features supported by this Access Point.

The screenshot shows the configuration interface for the 802.11g Wireless LAN Access Point. The page has a green header with the product name and a navigation bar with tabs: Wizard, Status, Basic Setting, IP Setting, Advanced Setting, Security (selected), and Tools. A green sidebar on the left contains the word "Security".

The main content area is divided into two sections:

- Password:** This section contains three input fields: "Administrator id:" with the value "admin", "AP Password New:" with masked characters, and "Confirm:" with masked characters. Below these fields are three buttons: "Apply", "Cancel", and "Help".
- MAC Filter:** This section has two radio buttons: "Enabled" (unselected) and "Disabled" (selected). Below the radio buttons are two options:
 - Only **deny** PCs with MAC listed below to access device
 - Only **allow** PCs with MAC listed below to access deviceA dropdown menu shows "1~10". Below this are seven rows of input fields for MAC addresses, labeled "MAC 1" through "MAC 7". Each row consists of six individual input boxes separated by hyphens.

Password: Allow user to change the new login password. Here are the necessary steps:

1. Enter the new password in the “**AP Password New:**” field.
2. Enter the new password again in the “**Confirm**” field.
3. Click “**Apply**”

MAC Filter: MAC Filter function controls the MAC of the network devices that are listed in this table for access authorization or denial. When MAC Filter is enabled, by selecting the “**Enabled**” radio box, select one of two choices:

?Only deny PCs with MAC listed below to access device

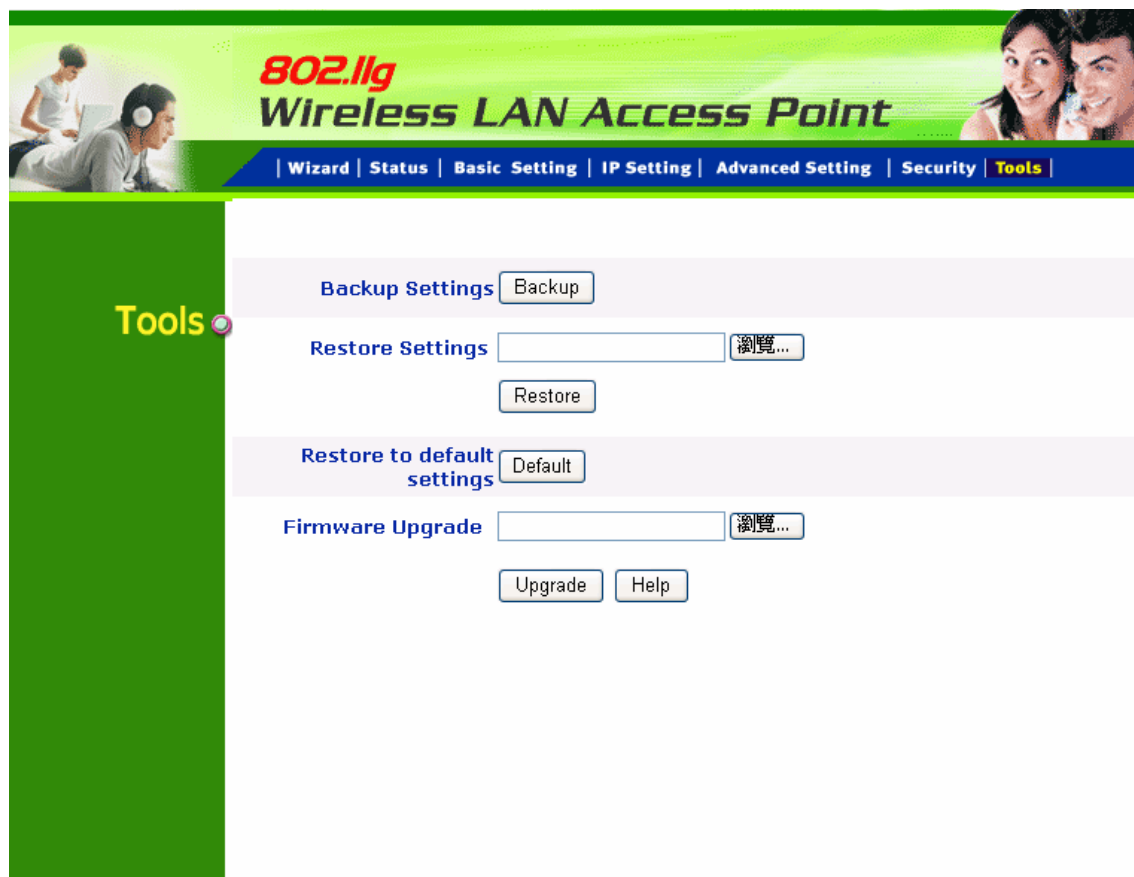
?Only allow PCs with MAC listed below to access device

The maximum number of MAC addresses that can be stored is 50. User can browse through the MAC address saved by selecting the drop-down box.

For any changes made in the security page, click “**Apply**” for the changes to be effective.

3.6 Tools

Four functions are provided in this page, Backup, Restore Settings, Restore default settings and Firmware Upgrade.



Backup Settings: Click on “**Backup**” button, which will open a FileSave Dialog box, where user gets to save all the current settings and configurations to a file.

Restore Settings: Click on the “**Browse**” button to open a FileOpen Dialog box, where user gets to select the file, which saves previous settings and configurations. Upon selecting the saved file, click “**Restore**” and complete the restore process when the access point re-operates after it restarts.

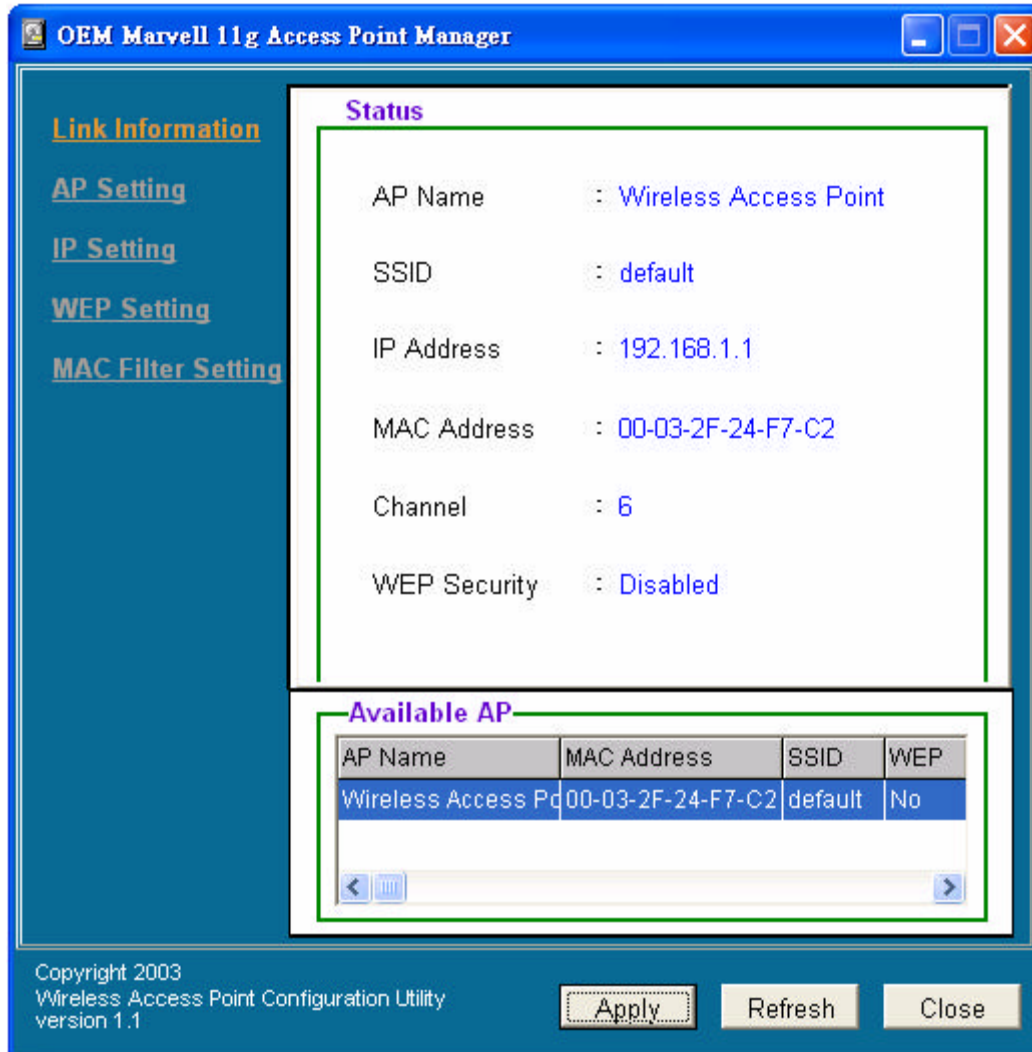
Restore to default settings: Click on “**Default**” button to restore the access point back to its manufacture default settings.

Firmware Upgrade: Click on the “**Browse**” button to open a FileOpen Dialog box, where gets to select the firmware file, which download from the web for the latest version. Upon selecting the firmware file, click “**Upgrade**” and complete the firmware upgrade process when the Access Point re-operates after it restarts.

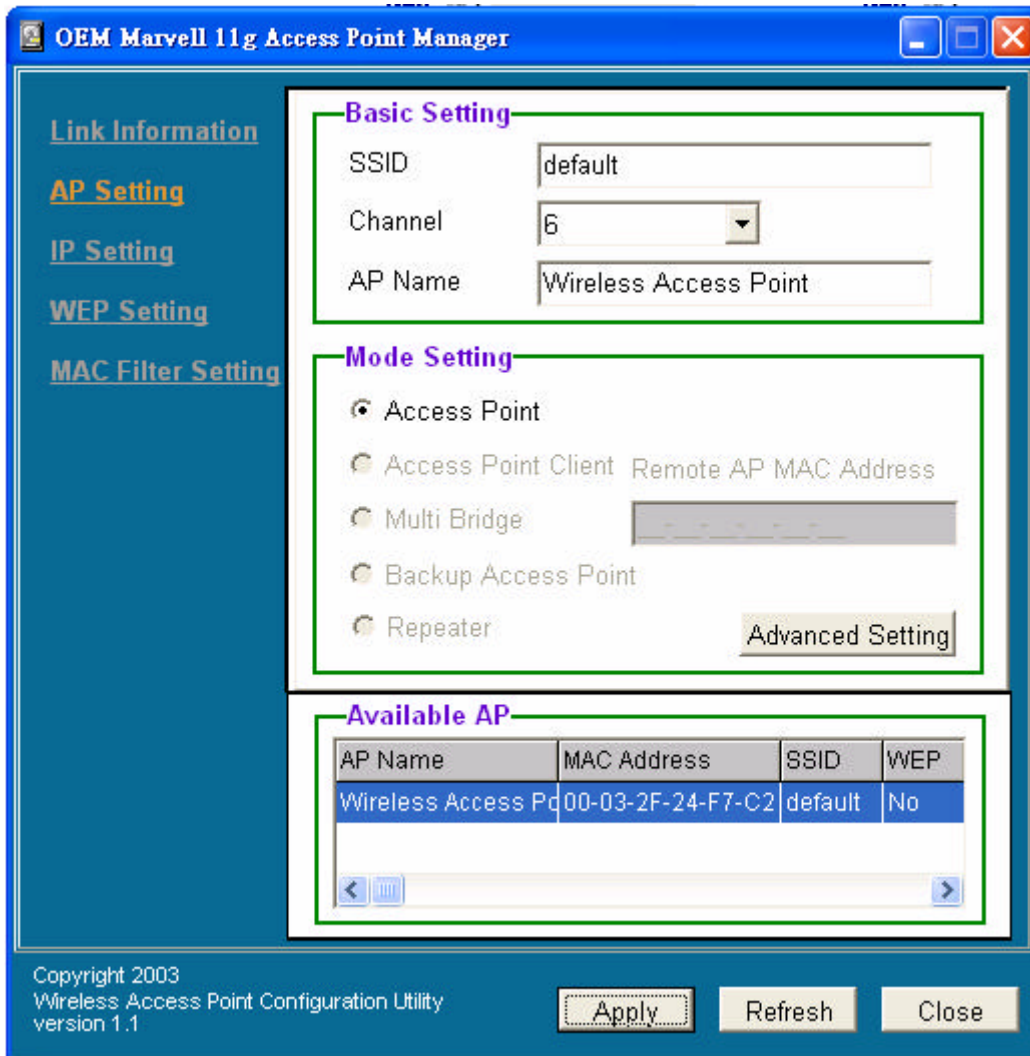
4. Configuration through AP Utility

4.1 Link Information

Link information is showing the related current setting of the first AP.



4.2 AP Setting



Basic Setting:

ESSID: All wireless devices within the wireless network use it.

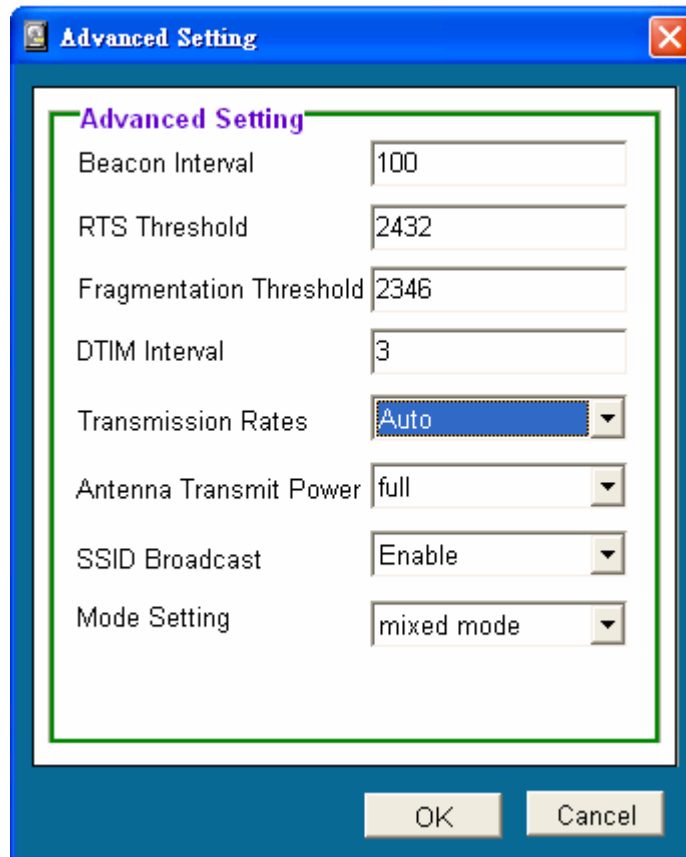
Channel: Select the appropriate channel from the dropping list. All wireless devices with the same ESSID will automatically use this channel to communicate with this access point.

AP Name: users can set the name for access point so as to easily manage the access points while there are several access points in the network.

Mode Setting:

Access Point: This is the default for this access point. It connects the wireless PCs to wired network.

Advanced Setting:



Beacon Interval: To set the period of time in milliseconds that AP sends out a beacon. Default is 100 milliseconds.

RTS Threshold: To set the size of RTS/CTS packet size. Default is 2432 bytes.

Fragmentation Threshold: To set the number of bytes used for the fragmentation boundary for directed messages. Default is 2436 bytes.

DTIM Interval: This value indicates the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the access point has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM interval value. Access point clients hear the beacons and awaken to receive the broadcast and multicast messages.

TX Rates (Mbps): Select one of the wireless communications transfer rates, measured in megabytes per second, based upon the speed of wireless adapters connected to the WLAN.

SSID Broadcast: While SSID Broadcast is enabled, all wireless clients will be able to communicate with the access point. For secure purpose, user may want to disable SSID broadcast to allow only those wireless clients with the AP SSID to communicate with the access point

Mode Setting: There are 2 modes, mixed mode and g mode, for user to decide which environment is suitable. Mixed mode means 802.11b plus 802.11g. When g mode is selected, user can run 54Mbps while all users are in the 802.11g environments. Once one of the users in the same environment using 802.11b, then all the other users can only run 11Mbps as 802.11b.

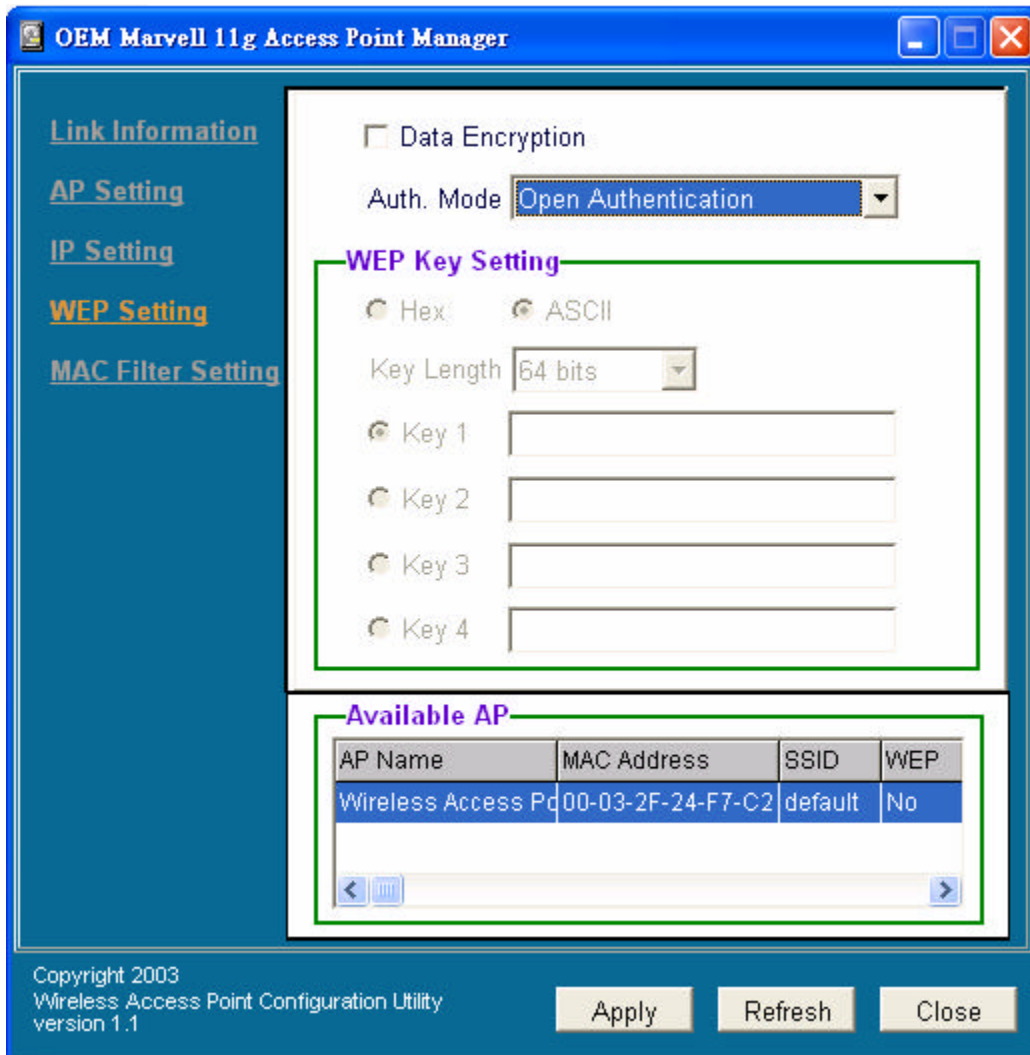
4.3 IP Setting



Fixed IP Address: Users can assign a fixed IP address to this AP manually.

DHCP Client: Enable the DHCP server function by clicking the radio button if user has the DHCP server running in your LAN network. It is not recommended because it probably will cause possible the conflict of IP assignment.

4.4 WEP Setting

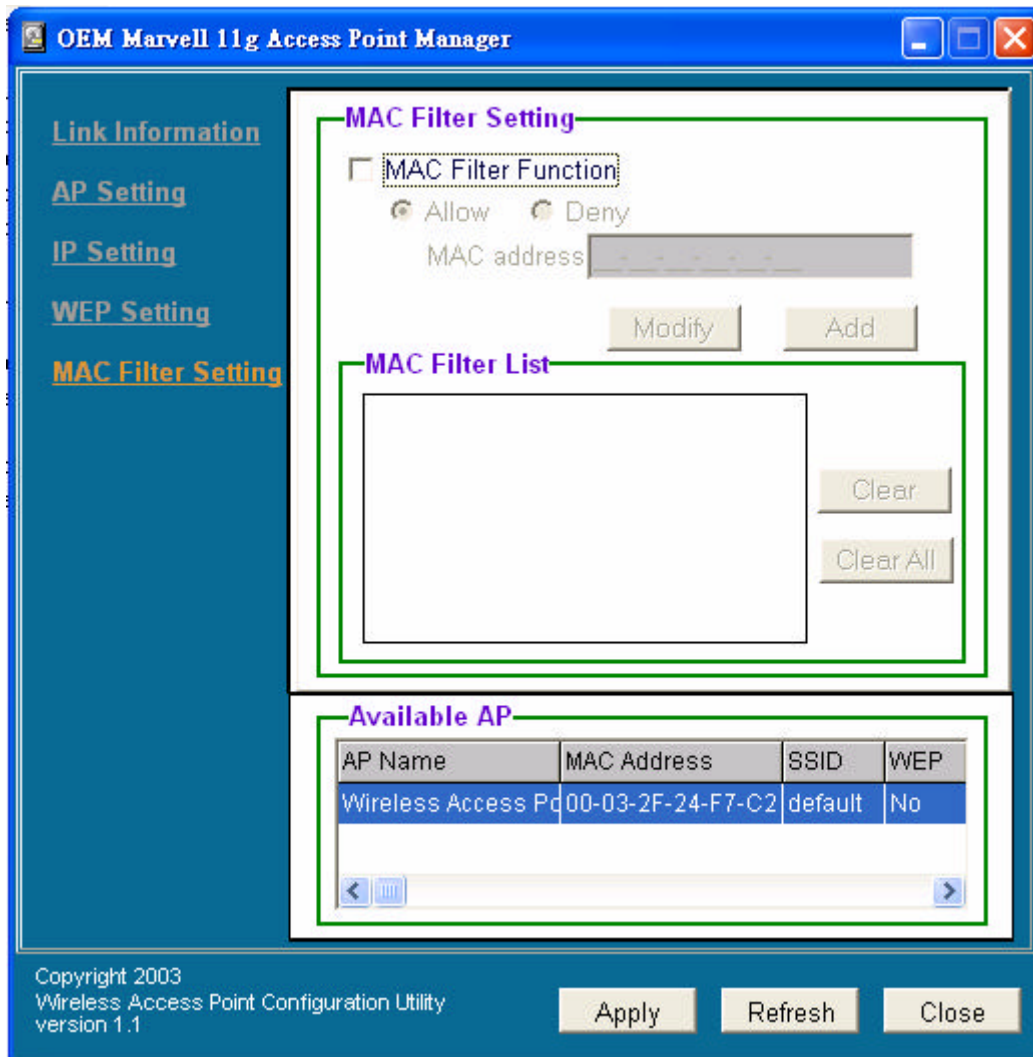


Data Encryption: Please tick it if user likes to have WEP key as the encryption mechanism.

Authentication Type: There are four options: Open System; Shared Key; WPA-PKS. User may want to set to Shared Key when the clients and AP in the same wireless network enable the WEP encryption. All the nodes and hosts on the network must use the same authentication type.

WEP Key: This will be enabled only while data encryption is selected. The key value must be entered in ASCII or HEX format by clicking the radio button. Besides, there are two options for the key length: 64bits or 128bits. There are four key sets are available to assign.

4.5 MAC Filter Setting



MAC Filter: MAC Filter function controls the MAC of the network devices that are listed in this table for access authorization or denial. When MAC Filter is enabled, by selecting the “**Enabled**” radio box, select one of two choices:
 ?Deny (PCs with MAC listed below to access device)
 ?Allow (PCs with MAC listed below to access device)
 The maximum number of MAC addresses that can be stored is 50. User can browse through the MAC address saved by selecting the drop-down box.

5. Glossary

Access Point: An internetworking device that seamlessly connects wired and wireless networks.

Ad-Hoc: An independent wireless LAN network formed by a group of computers, each with a network adapter.

ASCII: American Standard Code for Information Interchange, ASCII, is one of the two formats that you can use for entering the values for WEP key. It represents English letters as numbers from 0 to 127.

Authentication Type: Indication of an authentication algorithm which can be supported by the Access Point:

1. Open System: Open System authentication is the simplest of the available authentication algorithms. Essentially it is a null authentication algorithm. Any station that requests authentication with this algorithm may become authenticated if 802.11 Authentication Type at the recipient station is set to Open System authentication.

2. Shared Key: Shared Key authentication supports authentication of stations as either a member of those who knows a shared secret key or a member of those who does not.

Backbone: The core infrastructure of a network, which transports information from one central location to another where the information is unloaded into a local system.

Bandwidth: The transmission capacity of a device, which is calculated by how much data the device can transmit in a fixed amount of time expressed in bits per second (bps).

Beacon: A beacon is a packet broadcast by the Access Point to keep the network synchronized. Included in a beacon are information such as wireless LAN service area, the AP address, the Broadcast destination addresses, time stamp, Delivery Traffic Indicator Maps, and the Traffic Indicator Message (TIM).

Bit: A binary digit, which is either 0 or 1 for value, is the smallest unit for data.

Bridge: An internetworking function that incorporates the lowest 2 layers of the OSI network protocol model.

Browser: An application program that enables one to read the content and interact in the World Wide Web or Intranet.

BSS: BSS stands for "Basic Service Set". It is an Access Point and all the LAN PCs that associated with it.

Channel: The bandwidth which wireless Radio operates is divided into several segments, which call them “Channels”. AP and the client stations that it associated work in one of the channels.

CSMA/CA: In local area networking, this is the CSMA technique that combines slotted time -division multiplexing with carrier sense multiple access/collision detection (CSMA/CD) to avoid having collisions occur a second time. This works best if the time allocated is short compared to packet length and if the number of situations is small.

CSMA/CD: Carrier Sense Multiple Access/Collision Detection, which is a LAN access method used in Ethernet. When a device wants to gain access to the network, it checks to see if the network is quiet (senses the carrier). If it is not, it waits a random amount of time before retrying. If the network is quiet and two devices access the line at exactly the same time, their signals collide. When the collision is detected, they both back off and wait a random amount of time before retrying.

DHCP: Dynamic Host Configuration Protocol, which is a protocol that lets network administrators manage and allocate Internet Protocol (IP) addresses in a network. Every computer has to have an IP address in order to communicate with each other in a TCP/IP based infrastructure network. Without DHCP, each computer must be entered in manually the IP address. DHCP enables the network administrators to assign the IP from a central location and each computer receives an IP address upon plugged with the Ethernet cable everywhere on the network.

DSSS: Direct Sequence Spread Spectrum. DSSS generates a redundant bit pattern for each bit to be transmitted. This bit pattern is called a chip (or chipping code). The longer the chip, the greater the probability that the original data can be recovered. Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the radio can recover the original data without the need for retransmission. To an unintended receiver, DSSS appears as low power wideband noise and is rejected (ignored) by most narrowband receivers.

Dynamic IP Address: An IP address that is assigned automatically to a client station in a TCP/IP network by a DHCP server.

Encryption: A security method that uses a specific algorithm to alter the data transmitted, thus prevent others from knowing the information transmitted.

ESS: ESS stands for “Extended Service Set”. More than one BSS is configured to become Extended Service Set. LAN mobile users can roam between different BSSs in an ESS.

ESSID: The unique identifier that identifies the ESS. In infrastructure association, the stations use the same ESSID as AP's to get connected.

Ethernet: A popular local area data communications network, originally developed by Xerox Corp. that accepts transmission from computers and terminals. Ethernet operates on a 10/100 Mbps base transmission rate, using a shielded coaxial cable or over shielded twisted pair telephone wire.

Fragmentation: When transmitting a packet over a network medium, sometimes the packet is broken into several segments, if the size of packet exceeds that allowed by the network medium.

Fragmentation Threshold: The Fragmentation Threshold defines the number of bytes used for the fragmentation boundary for directed messages. The purpose of "Fragmentation Threshold" is to increase the transfer reliability thru cutting a MAC Service Data Unit (MSDU) into several MAC Protocol Data Units (MPDU) in smaller size. The RF transmission can not allow to transmit too big frame size due to the heavy interference caused by the big size of transmission frame. But if the frame size is too small, it will create the overhead during the transmission.

Gateway: a device that interconnects networks with different, incompatible communication protocols.

HEX: Hexadecimal, HEX, consists of numbers from 0 – 9 and letters from A – F.

IEEE: The Institute of Electrical and Electronics Engineers, which is the largest technical professional society that promotes the development and application of electro technology and allied sciences for the benefit of humanity, the advancement of the profession. The IEEE fosters the development of standards that often become national and international standards.

Infrastructure: An infrastructure network is a wireless network or other small network in which the wireless network devices are made a part of the network through the Access Point that connects them to the rest of the network.

ISM Band: The FCC and their counterparts outside of the U.S. have set aside bandwidth for unlicensed use in the ISM (Industrial, Scientific and Medical) band. Spectrum in the vicinity of 2.4GHz, in particular, is being made available worldwide.

MAC Address: Media Access Control Address is a unique hex number assigned by the manufacturer to any Ethernet networking device, such as a network adapter, that allows the network to identify it at the hardware level.

Multicasting: Sending data to a group of nodes instead of a single destination.

Node: A network junction or connection point, typically a computer or workstation.

Packet: A unit of data routed between an origin and a destination in a network.

PLCP: Physical layer convergence protocol

PPDU: PLCP protocol data unit

Preamble Type: During transmission, the PSDU shall be appended to a PLCP preamble and header to create the PPDU. Two different preambles and headers are defined as the mandatory supported long preamble and header which interoperates with the current 1 and 2 Mbit/s DSSS specification as described in IEEE Std 802.11-1999, and an optional short preamble and header. At the receiver, the PLCP preamble and header are processed to aid in demodulation and delivery of the PSDU. The optional short preamble and header is intended for application where maximum throughput is desired and interoperability with legacy and non-short-preamble capable equipment is not consideration. That is, it is expected to be used only in networks of like equipment that can all handle the optional mode. (IEEE 802.11b standard)

PSDU: PLCP service data unit

Roaming: A LAN mobile user moves around an ESS and enjoys a continuous connection to an Infrastructure network.

RTS: Request To Send. An RS-232 signal sent from the transmitting station to the receiving station requesting permission to transmit.

RTS Threshold: Transmitters contending for the medium may not be aware of each other. RTS/CTS mechanism can solve this "Hidden Node Problem". If the packet size is smaller than the preset RTS Threshold size, the RTS/CTS mechanism will NOT be enabled.

SSID: Service Set Identifier, which is a unique name shared among all clients and nodes in a wireless network. The SSID must be identical for each clients and nodes in the wireless network.

Subnet Mask: The method used for splitting IP networks into a series of sub-groups, or subnets. The mask is a binary pattern that is matched up with the IP address to turn part of the host ID address field into a field for subnets.

TCP/IP: Transmission Control Protocol/ Internet Protocol. The basic communication language or protocol of the Internet, it can also be used as a communications protocol in a private network, i.e. intranet or Internet. When you are set up with direct access to the Internet, your computer is provided with a copy of the TCP/IP program just as every other computer that you may send messages to or get information from also has a copy of TCP/IP.

Throughput: The amount of data transferred successfully from one point to another in a given period of time.

WEP: Wired Equivalent Privacy (WEP) is an encryption scheme used to protect wireless data communication. To enable the icon will prevent other stations without the same WEP key from linking with the AP.

Federal Communication Commission Interference Statement

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 installation. 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.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

IMPORTANT NOTE: FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body. To maintain compliance with FCC RF exposure compliance requirements, please avoid direct contact to the transmitting antenna during transmitting.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

We declare that the product is limited in CH1~CH11 by specified firmware controlled in the USA.