TwinMOS Octopus

802.11 b/g
Wireless AP
(71-WGAIU-C01)

User's Manual

TwinMOS®

Contents

PACKAGE CONTENTS

Unpack your ***Octopus Wireless AP*** kit and verify that all items are present.

- ***Octopus*** Wireless AP
- User's Manual (on CD)
- Quick Installation Guide
- AC Power Adapter (5V/ 2A)
- Ethernet Cable

If any of the items described appear to be damaged or missing, please contact your reseller.

INTRODUCTION

Thank you for purchasing the Wireless AP. The Wireless AP is an ideal broadband sharing solution for SOHO and home networks, featuring a wireless LAN function that reduces the necessity of connecting stations via a wired LAN.

The Wireless AP manages all IP address assignments by DHCP, relieving users of the necessity of manually configuring clients for inter-client communication and access to the Internet.

The intuitive Web browser interface enables users to configure all aspects of the AP, including making LAN settings, making access restrictions, setting administrative and user passwords.

This ***Octopus Wireless AP*** supports following features：

- Compatible with IEEE 802.11b/g Direct Sequence high data rate specifications.
- Supports high-speed wireless connections up to 54 Mbps
- Dynamic data rate scaling at 1,2,5.5,6,9,11,12,18,22,24,36,48,and 54Mbps.
- Easy setup through a Web browser on any operating system that supports TCP/IP.
- 10/100 Mbps Ethernet port.
- DHCP client.
- Supports WPA(Wi-Fi Protected Access) security.
- 64/128-bit Wired Equivalent Privacy (WEP) data encryption.

Description of Hardware

Front Panel

The front panel provides LED's for device status. Refer to the following table for the meaning of each feature.

LED	State	Color	Meaning
Power	On	Green	The device is receiving power.
	Off	—	The device is not receiving power.
WLAN	On	Green	Indicates WLAN status.
	On	Flashing Green	Indicates WLAN traffic.
LAN	On	Red	Indicates link speed (100/10 Mbps)
	On	Flashing Red	Packet transmits or receives activity.
	Off	—	No link activity.

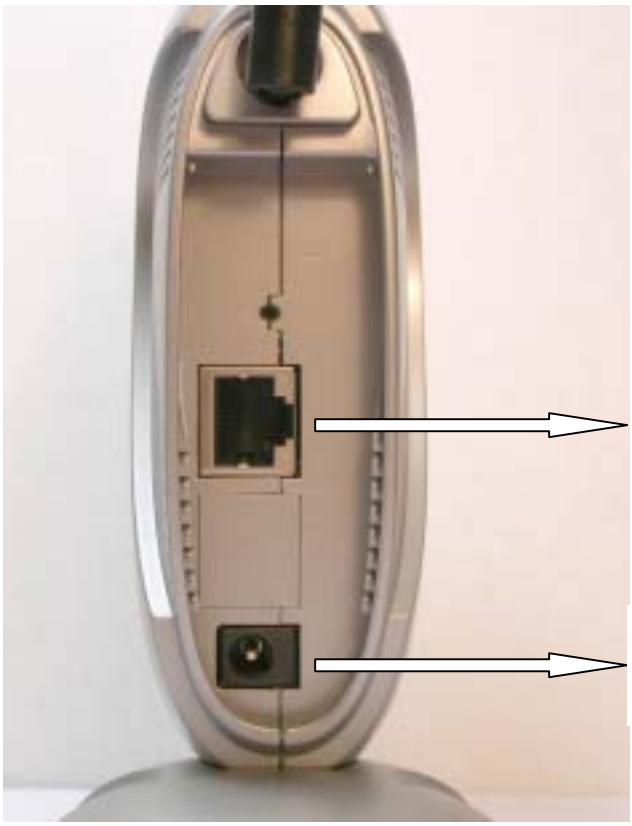
Rear Panel

Item	Description
LAN port	The four RJ-45 Ethernet ports allow you to connect client PC or LAN hubs to the Wireless AP.
Power port	Connect the included power adapter to this inlet. **Warning:** The included power adapter is DC 5V/2A. Using the wrong type of power adapter may cause damage.
Antenna	Two antennas provide wireless LAN functionality and ensure optimal signal strength.
Reset button (Side)	Use this button to reset the power and restore the default factory settings by pressing this button for five seconds.

Basic Installation Procedure

Connecting the AP to the LAN

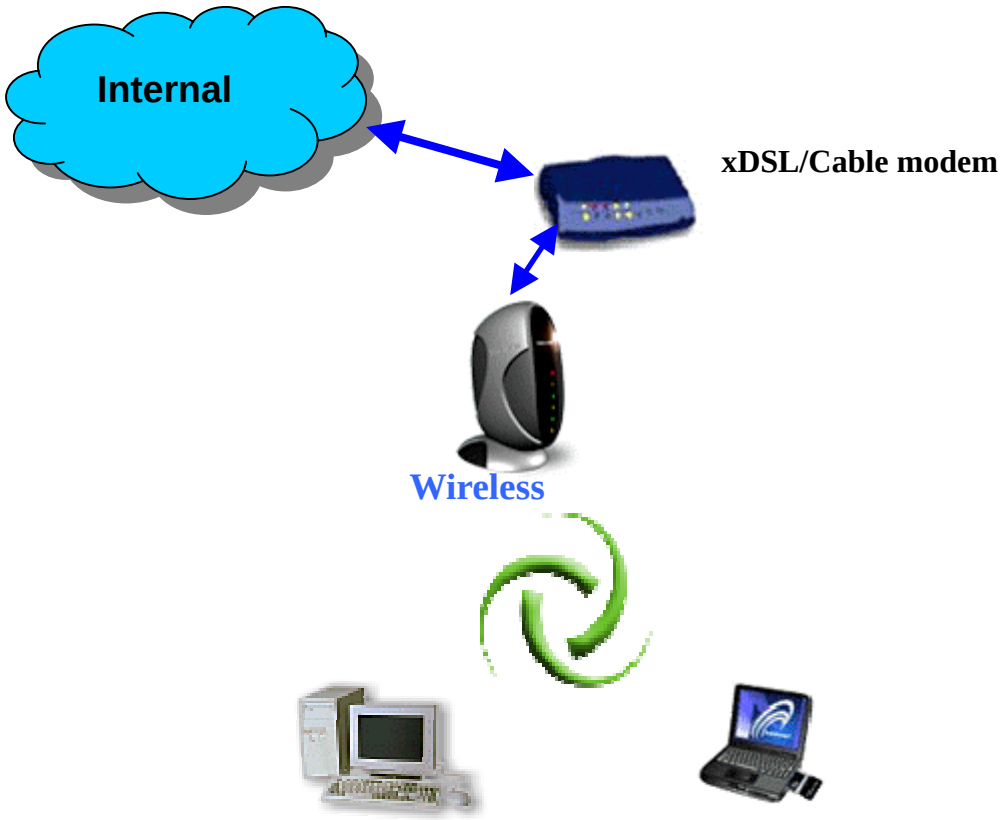
You can connect the WLAN 11b AP to your PC, a hub, or a switch. Run the Ethernet cable from one of the LAN ports on the rear of the WLAN 11b AP to your computer's network adapter or to another network device. You can also connect the WLAN 11b AP to your PC or to a client adapter via radio signals. Position one antenna on the back of the WLAN 11b AP into the desired positions.



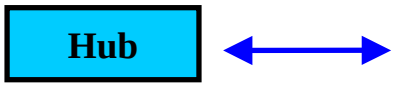
Power On

Connect the power adapter to the WLAN 11b AP.

SOHO/Home Networking



Office Networking



CONNECTING THE AP

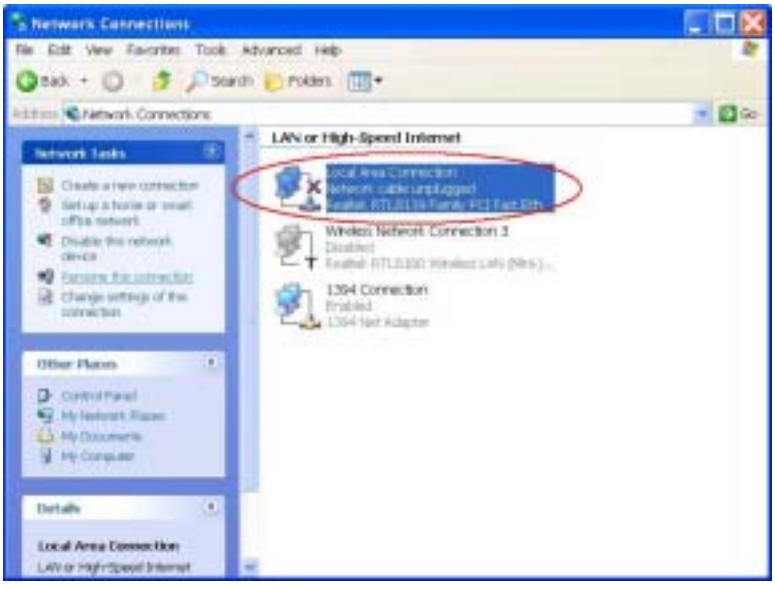
Follow the procedure below to connect the AP.

LAN connecting

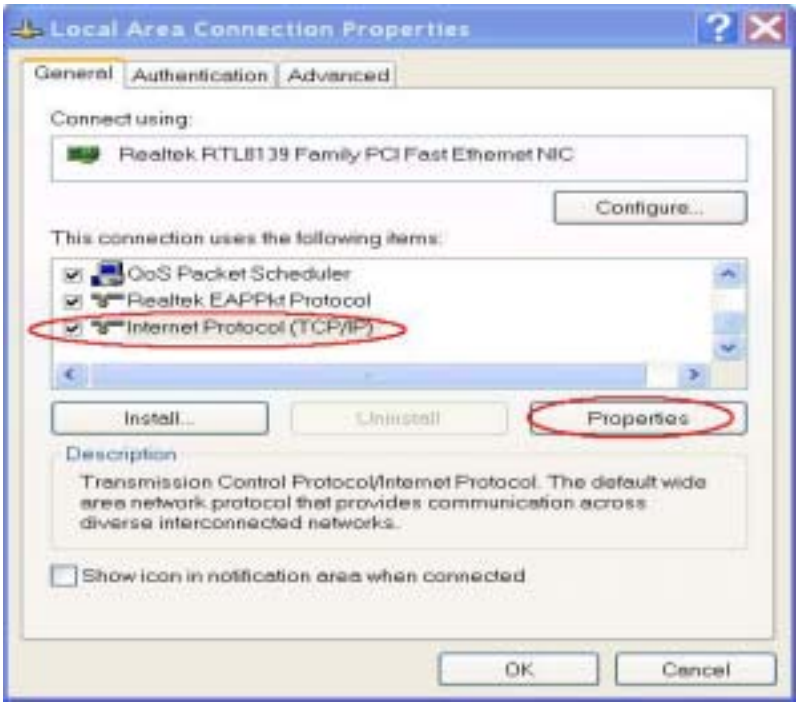
- **Plug an Ethernet cable into LAN port at the rear of the AP. Plug the other end of the cable into the RJ-45 port on your computer.**
- **Turn on power supply for AP.**
- **Setting TCP/IP to work with the AP.**
  - **Windows XP**

1. Click **Start**, **Settings**, then click **Control Panel**. The Control Panel opens:

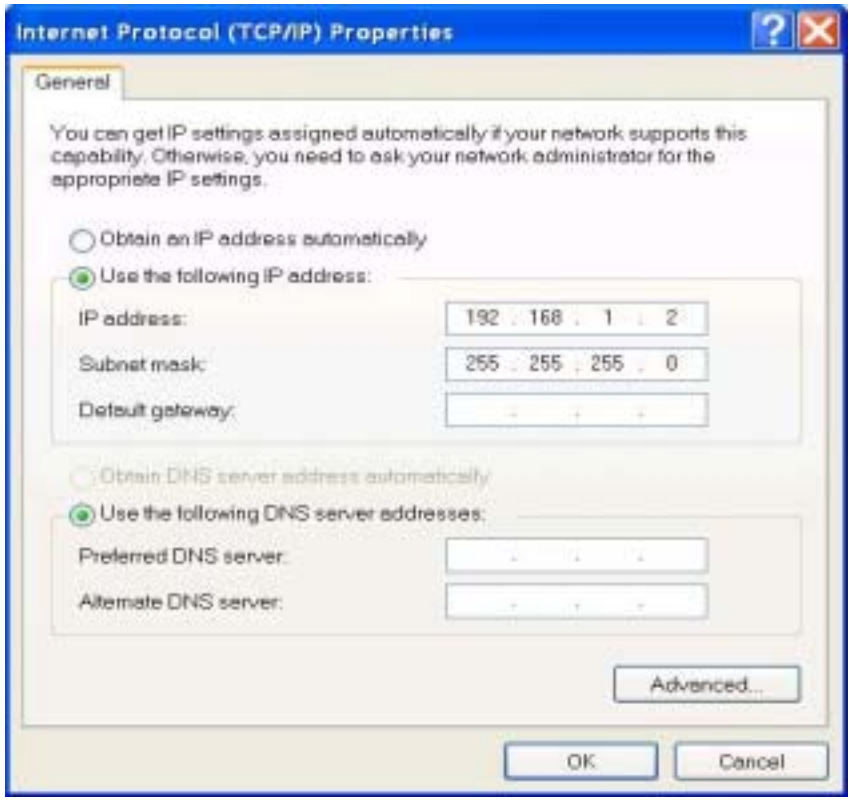
2. Right-click the **Network** icon and select ″OPEN″ to open the Network Connections dialog:



3.Right- clicks the appropriate LAN connection and click ″Properties ″ to open the properties dialog for the connection:



4. Check the box next to Internet Protocol (TCP/IP) and click Properties:



5.Assign an IP address: follow these steps:

a. In the TCP/IP Properties dialog box, click the radio button next to **Use the following IP address**:

b. Enter an IP address in the IP field. In the example shown, IP addresses is ***192.168.1.X*** (Where X means 2-239)

c. Type a Subnet Mask value is **255.255.255.0.**

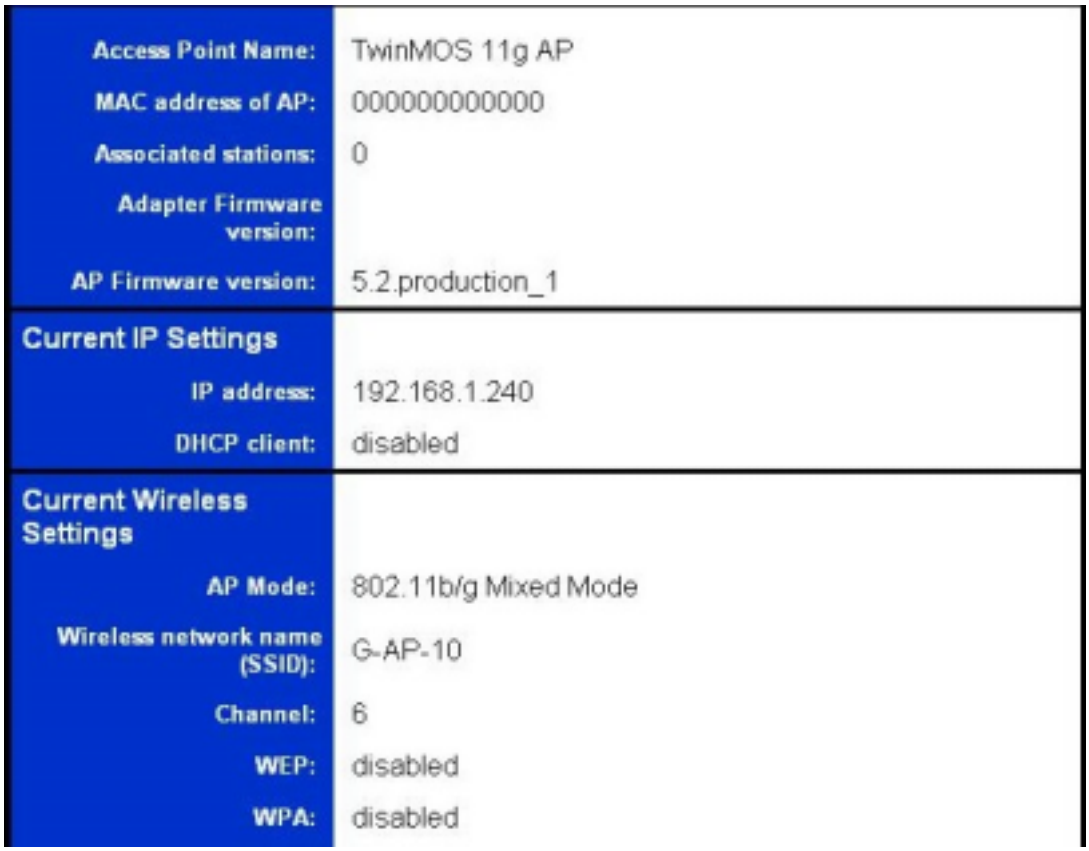
d. Check the radio button next to "Use the following DNS server addresses" and type the ISP do-main name server IP address.

e. Click **OK**. You are returned to the Network configuration dialog box.

6. Click **OK** to apply the settings and exit the Network configuration dialog box.

- **Open your Web browser and type the AP`s IP address in the address bar. The AP default IP address is *192.168.1.240* . The default user name and password is null.**

When you see the photo above then you can set the AP. The default setting below:



Wireless connecting

- **Turn on power supply for Wireless AP.**
- **Insert 802.11b/g wireless LAN card to your PC.**
- **Setting your wireless utility. The SSID is "G-AP-10", WEP off, and Infrastructure mode.**
- **Setting TCP/IP to work with the Wireless AP.**
  (Please follow LAN connecting procedure)
- **Open your Web browser and type the AP`s IP address in the address bar. The AP default IP address is *192.168.1.240*. The default user name and password is null.**

WEB MANAGEMENT SETTINGS

Before using the Web browser interface, be sure you have set up your computer's network configuration. Refer to page 9.

Login Page

Please type user name and password to the text. The default user name and password is null. Please click "OK" to open WEB.

Wireless AP Information Page

This page shows the current status and some basic settings of the device.

Access Point Name:	TwinMOS 11g AP
MAC address of AP:	000000000000
Associated stations:	0
Adapter Firmware version:	
AP Firmware version:	5.2.production_1
Current IP Settings	
IP address:	192.168.1.240
DHCP client:	disabled
Current Wireless Settings	
AP Mode:	802.11b/g Mixed Mode
Wireless network name (SSID):	G-AP-10
Channel:	6
WEP:	disabled
WPA:	disabled

Wireless Page

This page is used to configure the parameters for wireless LAN clients, which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

Wireless Configuration

On this page you can configure the basic 802.11g access point settings. Any new settings will not take effect until the access point is rebooted.

Visibility Status:	◉ Visible ○ Invisible
Performance Mode:	802.11b/g Mixed Mode
Wireless Network Name (SSID):	G-AP-10
Channel:	6
Transmission rate (Mbits/s):	Best (automatic)

Save Cancel

- **Visibility Status**

When Invisibility is selected, the AP is protected against discovery by wireless sniffers, and all wireless clients must explicitly know and use the SSID.

- **Performance Mode**

These profiles control a number of settings for overall wireless network usage. Their meanings are self-explanatory.

- **SSID**

This is the name of the access point on the wireless network. Stations that associate to this access point may have to know this name.

- **Channel**

This is the radio channel that the access point will operate on. If you experience interference (e.g. lost connections or slow data transfers) you may need to try different channels to see which is the best.

- **Transmission Rate**

This is the speed at which the access point will transmit data. Normally you should select 'best' here, although if your wireless network is unusually noisy or quiet you may which to use a fixed low or high rate.

- **Save**

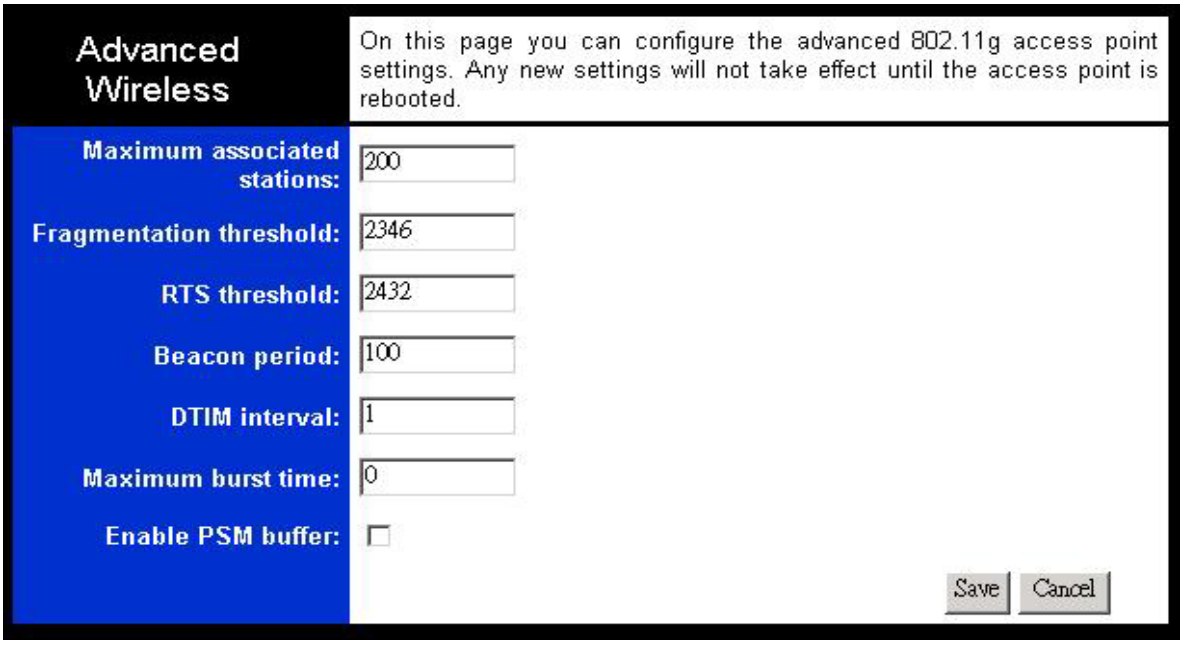
Click “Save” button to save and implement the new settings.

- **Cancel**

Click “Cancel” button to cancel the settings.

Advanced Settings Page

These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Access Point.



- **Maximum associated stations**

This the maximum number of wireless stations that can be associated at any one time.

- **Fragmentation Threshold**

The value defines the maximum size of packets: any packet size larger than the value will be fragmented. If you have decreased this value and experience high packet error rates, you can increase it again, but it will likely decrease overall network performance. Select a setting within a range of 256 to 2346 bytes. Minor change is recommended.

- **RTS Threshold**

Minimum packet size required for an RTS (Request To Send). For packets smaller than this threshold, an RTS is not sent and the packet is transmitted directly to the WLAN. Select a setting within a range of 0 to 2432 bytes. Minor change is recommended

- **DTIM Interval**

This is the number of beacons per DTIM (Delivery Traffic Indication Message),e.g. '1' means send a DTIM with each beacon, '2' means with every 2nd beacon, etc.

- **Maximum burst time**

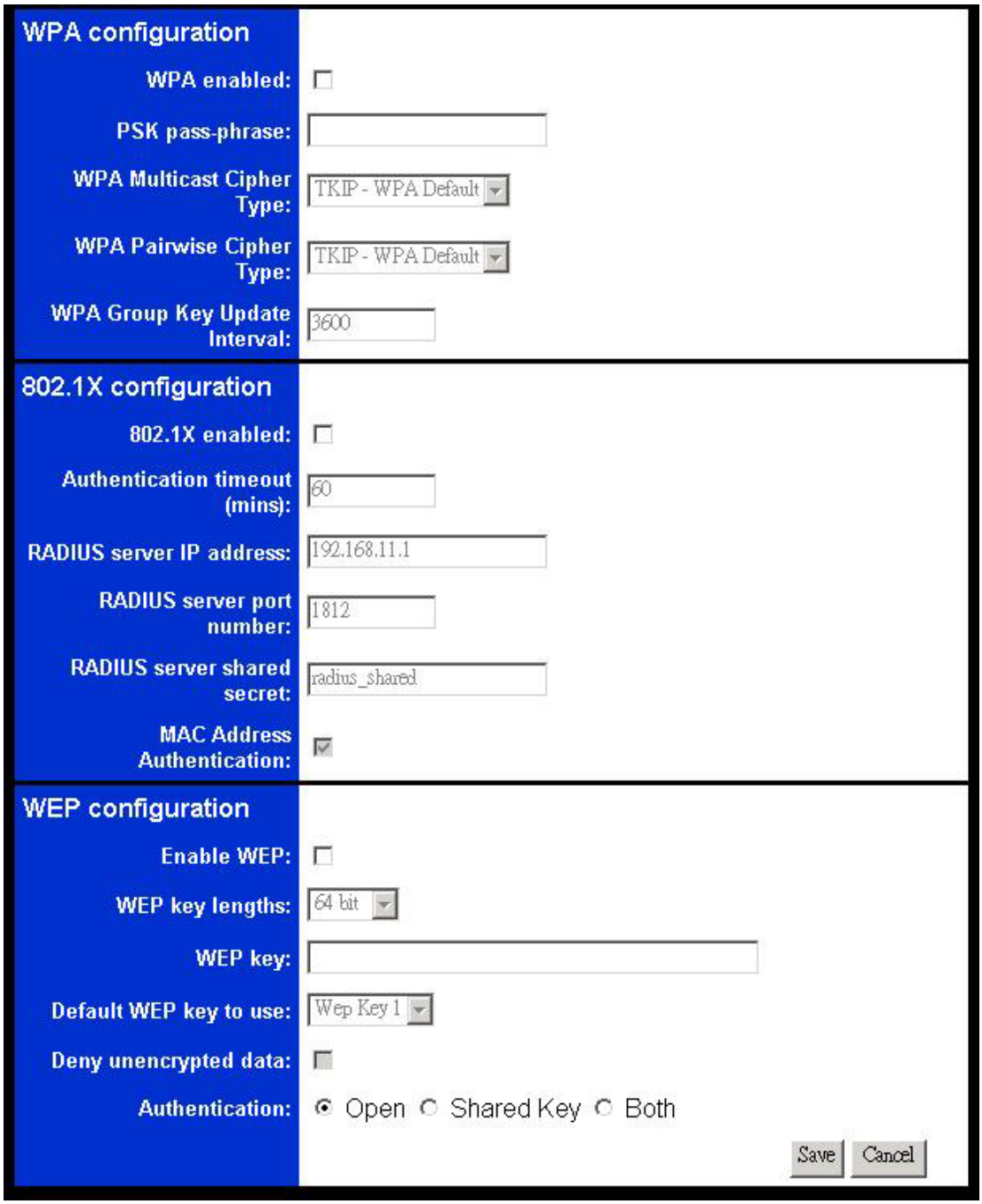
This is also known as PRISM Nitro (tm) technology. The technology uses fully standards-compliant methods that eliminate collisions in mixed-mode networks, while greatly increasing the performance of both pure 802.11g and mixed 802.11b/g networks. The setting is for the amount of time the radio will be reserved to send data without requiring an ACK. This number is in units of microseconds. A typical value would be 1000 microseconds. When this number is zero, bursting is disabled.

- **Enable PSM buffer**

Turn this on to enable support for stations in power save mode.

Security Page

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.



- **WPA Configuration**

Enable WPA Authenticator to require stations to use high grade encryption and authentication.

- **PSK pass-phrase**

Leave blank if stations will be supplied a key by the 1X Authentication Server. Choose a pass-phrase between 8 and 63 characters.

- **WPA Multicast Cipher Type**

Currently TKIP is the only permitted setting.

- **WPA Pairwise Cipher Type**

Currently TKIP is the only permitted setting.

- **WPA Group Key Update Interval**

Unit: seconds.

- **802.1x Configuration**

When 802.1X authentication is enabled then the AP will authenticate clients via a remote RADIUS server.

- **WEP Configuration**

WEP is the wireless encryption standard. To use it you must enter the same key(s) into the access point and the wireless stations. For 64 bit keys you must enter 10 hex digits into each key box. For 128 bit keys you must enter 26 hex digits into each key box. A hex digit is either a number from 0 to 9 or a letter from A to F. If you leave a key box blank then this means a key of all zeros.

- **Enable WEP**

Check this box to enable WEP. For the most secure use of WEP, also select "Deny Unencrypted Data" and set Authentication to "Shared Key" when WEP is enabled.

- **WEP Key lengths**

You may select the 64-bit or 128-bit to encrypt transmitted data. Larger key length will provide higher level of security, but the throughput will be lower.

- **Default WEP key to use**

Select the key to be used as the default key. Data transmissions are always encrypted using the default key. The other keys can only be used to decrypt received data.

- **Deny unencrypted data**

Select this to require peers to use encryption.This is only effective when WEP is enabled.

- **Authentication**

This setting has to be consistent with the wireless devices, which the adapter intends to connect.

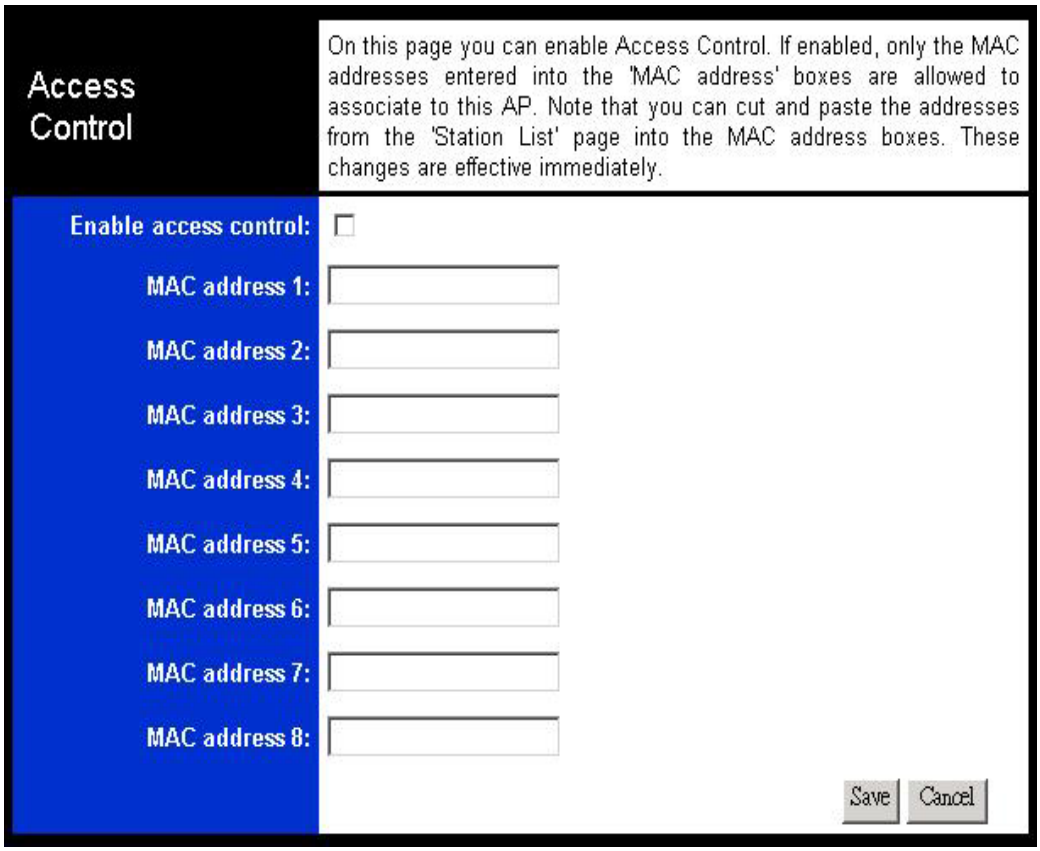
· **Open System –** No authentication is needed among the wireless devices.

· **Shared Key –** Only wireless devices using a shared key (WEP Key) are allowed to connecting each other. Setup the same key as the wireless devices, which the adapter intends to connect.

· **Both –**allows a station to use either mode.

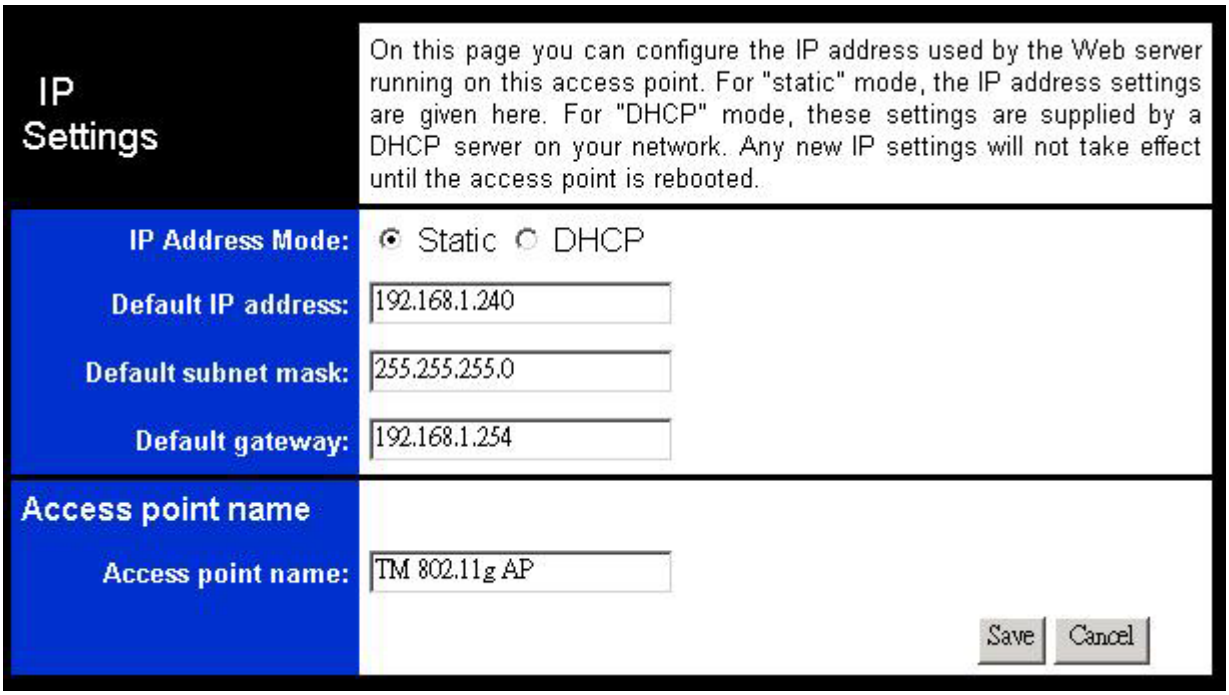
Access Control Page

If you enable access control, only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When this option is enabled, no wireless clients will be able to connect if the list contains no entries



IP Address Page

This page is used to configure the parameters for local area network, which connects to the LAN port of your Access Point. Here you may change the setting for IP address, subnet mask, DHCP, etc.



- **IP Address Mode**

Select 'DHCP' to get the IP settings from a DHCP server on your network. Select 'Static' to use the IP settings specified on this page.

- **Default IP Address**

This is the IP address of the AP. The default IP address is 192.168.1.240.

- **Subnet Mask**

Type the subnet mask for the AP in the text box. The default subnet mask is 255.255.255.0

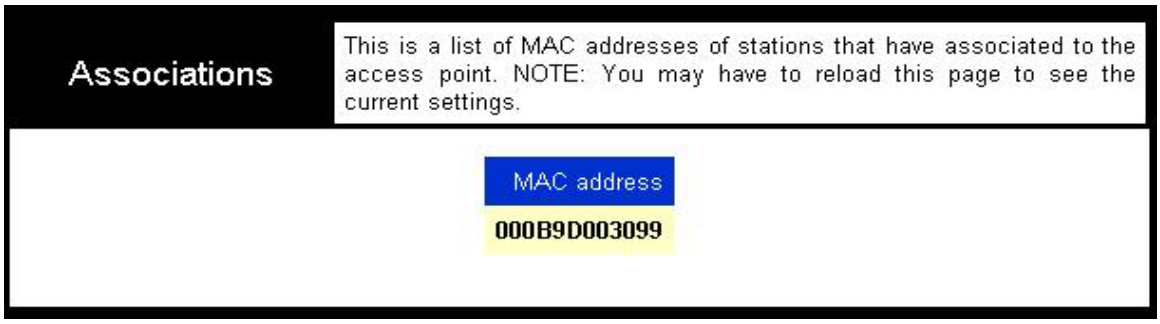
- **Default Gateway**

This is the IP address of the gateway that connects you to the internet.

- **Access point name**

This is the name that the access point will use to identify itself to external configuration and IP-address-finding programs. This is not the same as the SSID. It is okay to leave this blank if you are not using these programs.

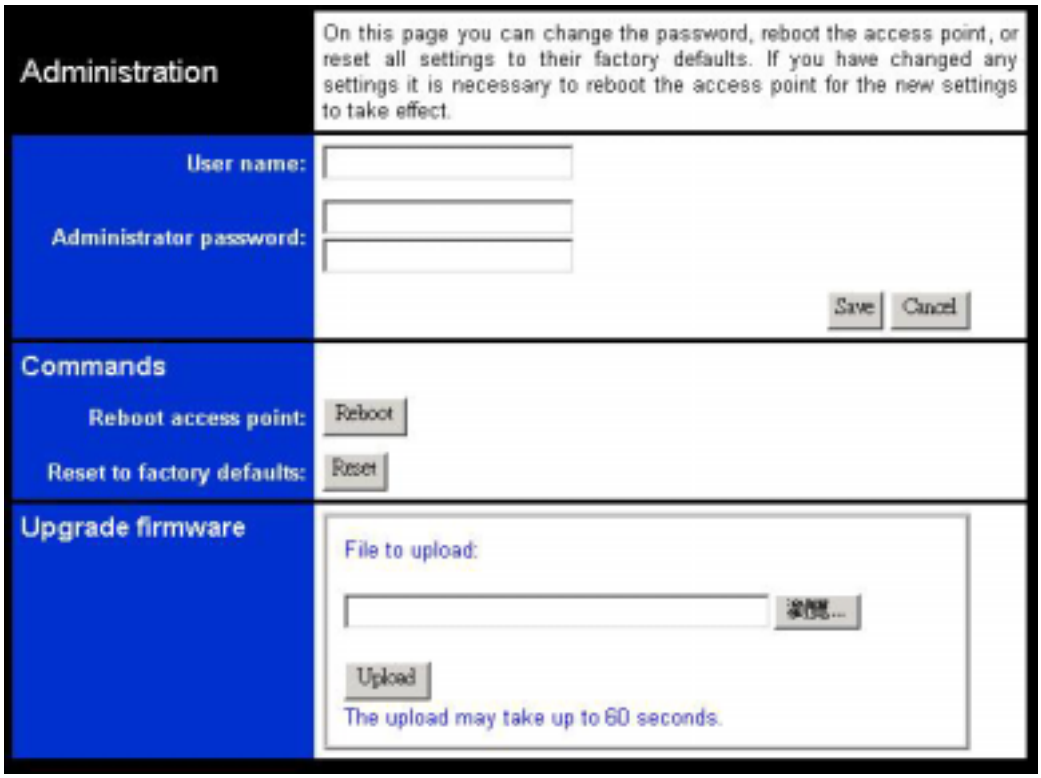
Associations Page



- **MAC Address**

A list of MAC addresses of stations that have associated to the access point.

Administration Page



- **User name**

This is the user name that you must type when logging in to these web pages

- .**Administrator password**

This is the password that you must type when logging in to these web pages. You must enter the same password into both boxes, for confirmation.

- **Reboot access point**

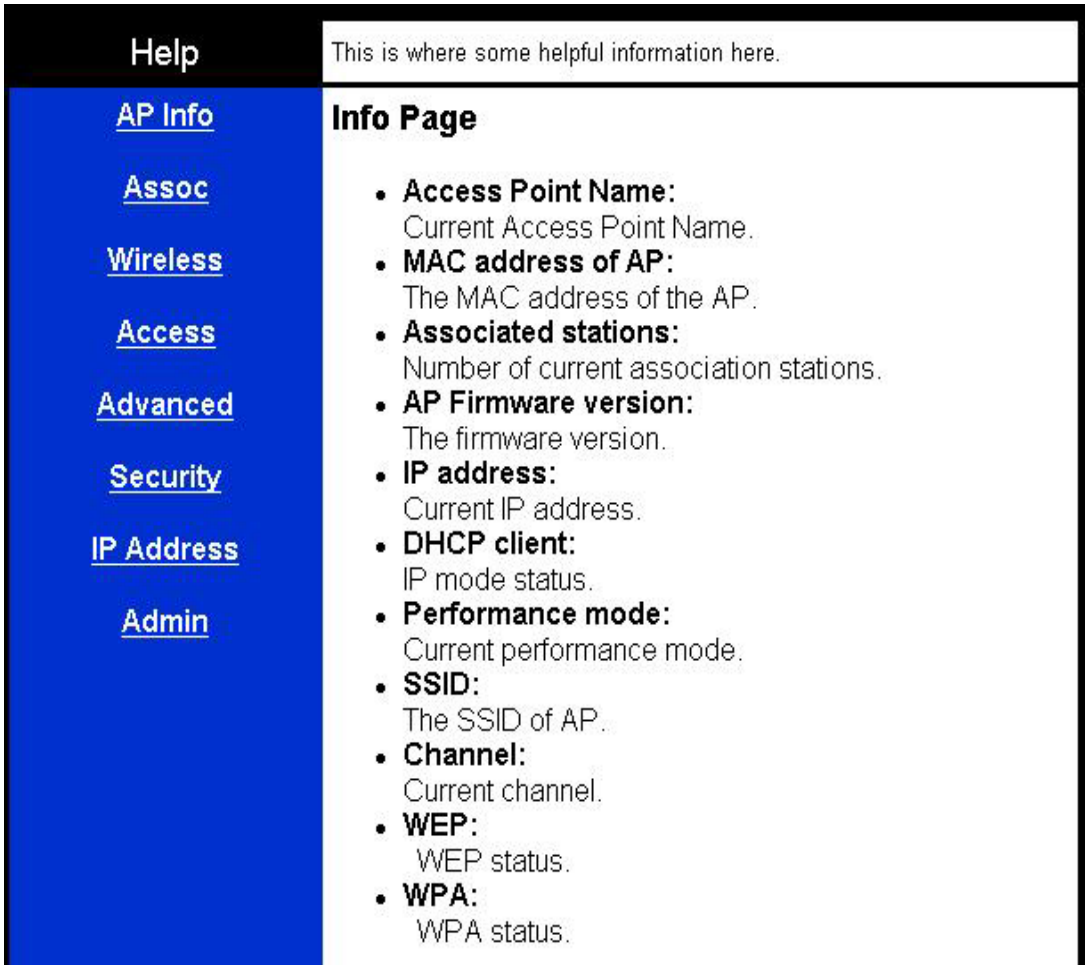
You need to reboot the AP whenever you make any configuration change.

- **Reset to factory defaults**

Reset all configuration settings to factory defaults.

Help Page

This page is online help.



TROUBLESHOOTING

Symptom: Power LED off

Resolution:

Connect the power adapter to your AP and plug it into the power outlet.

Note: Only use the power adapter provided with your AP. Using any other adapter may damage your AP .

Symptom: Can not setting AP through web browser

Resolution:

- The Ethernet cable (RJ45-crossover) must plug to LAN port of Wireless AP.
- Check that the IP address in the URL field is correct.
- Check your host PC IP address. If the IP address of AP is 192.168.1.240 then your IP of host PC must set 192.168.1.1~239.

Symptom: Forgot IP address

Resolution:

If you forgot the IP address of Wireless AP you can press reset button to restore the default factory settings by pressing this button for five seconds. The default IP is 192.168.1.240.

Symptom: Can not setting Wireless AP from a wireless card

Resolution:

- Make sure that the Mode、 SSID、Channel and encryption settings are set the same on each wireless adapter.
- Make sure that your computer is within range and free from any strong electrical devices that may cause interference.
- Check your IP Address to make sure that it is compatible with the Wireless AP.

Glossary

802.1x: The standard for wireless LAN authentication used between an AP and a client. 802.1x with EAP will initiate key handling.

Ad-Hoc Network: The wireless network based on a peer-to-peer communications session. Also referred to as AdHoc.

Access Point: Access points are way stations in a wireless LAN that are connected to an Ethernet hub or server. Users can roam within the range of access points and their wireless device connections are passed from one access point to the next.

Authentication: Authentication refers to the verification of a transmitted message's integrity.

DHCP: DHCP (Dynamic Host Configuration Protocol) software automatically assigns IP addresses to client stations logging onto a TCP/IP network, which eliminates the need to manually assign permanent IP addresses.

DSSS (Direct Sequence Spread Spectrum): Method of spreading a wireless signal into wide frequency bandwidth.

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

DNS (Domain Name System): System used to map readable machine names into IP addresses

DTIM: DTIM (Delivery Traffic Indication Message) provides client stations with information on the next opportunity to monitor for broadcast or multicast messages.

Filter: Filters are schemes, which only allow specified data to be transmitted. For example, the router can filter specific IP addresses so that users cannot connect to those addresses.

Firmware: Programming inserted into programmable read-only memory, thus becoming a permanent part of a computing device.

Fragmentation: Refers to the breaking up of data packets during transmis-sion.

Gateway: Gateways are computers that convert protocols enabling different networks, applications, and operating systems to exchange information.

ISP: An ISP is an organization providing Internet access service via modems, ISDN (Integrated Services Digital Network), and private lines.

LAN(Local Area Network): A group of computers and peripheral devices connected to share resources.

MAC (Medium Access Control) Address: A unique number that distinguishes network cards.

MTU: MTU (Maximum Transmission/Transfer Unit) is the largest packet size that can be sent over a network. Messages larger than the MTU are divided into smaller packets.

NAT: NAT (Network Address Translation - also known as IP masquerading) enables an organization to present itself to the Internet with one address. NAT converts the address of each LAN node into one IP address for the Internet (and vice versa). NAT also provides a certain amount of security by acting as a firewall by keeping individual IP addresses hidden from the WAN.

Preamble: Preamble refers to the length of a CRC (Cyclic Redundancy Check) block that monitors' communications between roaming wireless enabled devices and access points.

Protocol: A standard way of exchanging information between computers.

RADIUS (Remote Authentication Dial In User Service): A server that issues authentication key to clients.

RAM (Random Access Memory): Non-permanent memory.

RIP: RIP (Routing Information Protocol) is a routing protocol that is integrated in the TCP/IP protocol. RIP finds a route that is based on the smallest number of hops between the source of a packet and its destination.

Router: Device that can connect individual LANs and remote sites to a server.

Roaming: The ability to use a wireless device while moving from one access point to another without losing the connection.

RTS: RTS (Request To Send) is a signal sent from the transmitting station to the receiving station requesting permission to transmit data.

Server: Servers are typically powerful and fast machines that store programs and data. The programs and data are shared by client machines (workstations) on the network.

Static IP Address: A permanent IP address is assigned to a node in a TCP/IP network. Also known as global IP.

Subnet Mask: Subnet Masks (SUBNET work masks) are used by IP protocol to direct messages into a specified network segment (i.e., subnet). A subnet mask is stored in the client machine, server or router and is compared with an incoming IP ad-dress to determine whether to accept or reject the packet.

SSID: SSID (Service Set Identifier) is a security measure used in WLANs. The SSID is a unique identifier attached to packets sent over WLANs. This identifier emulates a password when a wireless device attempts communication on the WLAN. Because an SSID distinguishes WLANS from each other,

access points and wireless devices trying to connect to a WLAN must use the same SSID.

TCP/IP: TCP/IP (Transmission Control Protocol/Internet Protocol) is the main Internet communications protocol. The TCP part ensures that data is completely sent and received at the other end. Another part of the TCP/IP protocol set is UDP, which is used to send data when accuracy and guaranteed packet delivery are not as important (for example, in real-time video and audio transmission).

TFTP (Trivial File Transfer Protocol): Simple form of FTP (File Transfer Protocol), which Uses UDP (User Datagram Protocol), rather than TCP/IP for data transport and provides no security features.

TKIP (Temporal Key Integrity Protocol): An encryption method replacing WEP.TKIP uses random IV and frequent key exchanges.
UDP (User Datagram Protocol): A communication method (protocol) that offers a limited amount of service when messages are exchanged between computers in a network. UDP is used as an alternative to TCP/IP.

Uplink: Link to the next level up in a communication hierarchy.

UTP (Unshielded Twisted Pair) cable: Two or more unshielded wires twisted together to form a cable.

Virtual Servers: Virtual servers are client servers (such as Web servers) that share resources with other virtual servers (i.e., it is not a dedicated server).

WEP (Wired Equivalent Privacy): An encryption method based on 64 or 128bit algorithm.

Web Browser: A software program that allows viewing of web pages.

WLAN: WLANs (Wireless LANs) are local area networks that use wireless communications for transmitting data. Transmissions are usually in the 2.4 GHz band. WLAN devices do not need to be lined up for communications like infrared devices. WLAN devices use access points, which are connected to the wired LAN and provide connectivity to the LAN. The radio frequency of WLAN devices is strong enough to be transmitted through non-metal walls and objests, and can cover an area up to a thousand feet. Laptops and notebooks use wireless LAN PCMCIA cards while PCs use plug-in cards to access the WLAN.

TECHNICAL SPECIFICATIONS

Physical Specification

Dimensions	142x102.5x76.16 mm
Weight	240g
Host Interface	RJ45 1X LAN port
Temperature & Humidity	
Operation	0℃ to 55℃ maximum humidity 95%
Transit	-20℃ to 65℃ humidity 15% to 95%
Storage	-20℃ to 65℃ humidity 10% to 95%

Power Characteristics

Power Supply	110/220V to 5V(1.5A)
Operating Voltage	3.3V±5%
Current Consumption	Nominal 500mA, Max. 750mA

Networking Characteristics

Compatibility	● IEEE 802.11b/g Standard for WLAN (DSSS/OFDM) ● Internal Wi-Fi certified by TwinMOS ● IEEE 802.3 10/100Base-T Ethernet
Host OS	● Ubicom ipOS
Media Access Protocol	● CSMA/CA ● TCP/IP ● IPX/SPX ● NetBEUI ● ARP
Management	● Set IP Session (ARP/PING) ● Web-base management ● DHCP ● HTTP
Ethernet Interface	● 10 /100Mbps RJ-45 Auto-negotiation network interface for LAN
Active Users	30

RF Characteristics

Frequency Range	2.400-2.484 GHz
Operating Channels	● 1-11 United States (FCC) ● 1-11 Canada (DOC) ● 1-14 Japan (MKK) ● 1-13 Europe (Except Spain and France) (ETSI)
Modulation Technique	● BPSK(1Mbps) ● QPSK(2 Mbps) ● CCK(5.5,11Mbps) ● OFDM WITH BPSK(6,9Mbps) ● OFDM WITH QPSK(12,18Mbps) ● OFDM WITH 16QAM(24,36Mbps) ● OFDM WITH 64QAM(48Mbps, 54Mbps)
Spreading	11-chip Barker Sequence
Transmit Power	15 dBm @ Nominal Temp Range
Receive Sensitivity	Nominal Temp Range: -82 dBm @ 11Mbps -68 dBm @ 54 Mbps
Security	● 64/128-bit WEP Encryption ● 64/128-bit WPA Encryption
Antenna	Built-in Diversity Antenna
Operating Range	Open Space: 100 ~ 300m; Indoor: 30m ~ 100m The transmission speed varies in the surrounding environment.
EMC Certification	FCC part 15B, 15C; R&TTE

FCC CAUTION

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 radiated 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 or more 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.

Changes or modifications not expressly approved by the party responsible for compliance could void the user‘s authority to operate the equipment.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20cm (8 inches) during normal operation.