

TwinMOS Booming

802.11b Wireless AP

User's Manual

Contents

PACKAGE CONTENTS	2
INTRODUCTION	3
DESCRIPTION OF HARDWARE	4
BASIC INSTALLATION PROCEDURE	6
CONNECTING THE AP	9
WEB MANAGEMENT SETTINGS	13
TROUBLESHOOTING	21
GLOSSARY	24
TECHNICAL SPECIFICATIONS	27
FCC CAUTION	28

PACKAGE CONTENTS

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

- *Booming* 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 *Booming Wireless AP* supports following features :

- Compatible with IEEE 802.11b Direct Sequence high data rate specifications.
- Supports high-speed wireless connections up to 11 Mbps.
- Supports WDS function.
- Easy setup through a Web browser on any operating system that supports TCP/IP.
- DHCP for dynamic IP configuration, and DNS for domain name mapping.
- 64/128-bit Wired Equivalent Privacy (WEP) data encryption.
- Supports WPA(Wi-Fi Protected Access) security.
- Web-based firmware upgrade.

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 Link	On	Red	Indicates that the device is connected to WLAN.
WLAN Act	Blinking	Green	Indicates WLAN traffic.
LAN Link	On	Green	Link is established.
	Off	?	No link activity.
LAN Act	On	Flashing Red	Packet transmits or receives activity.
	Off	?	No link activity.

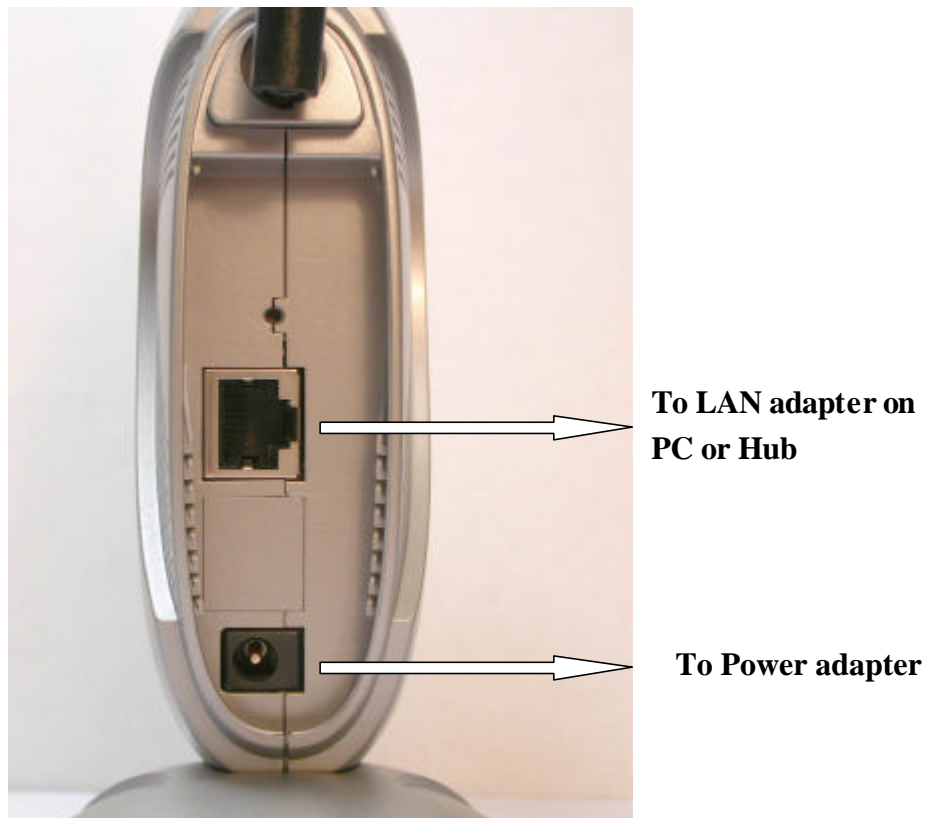
Rear Panel

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

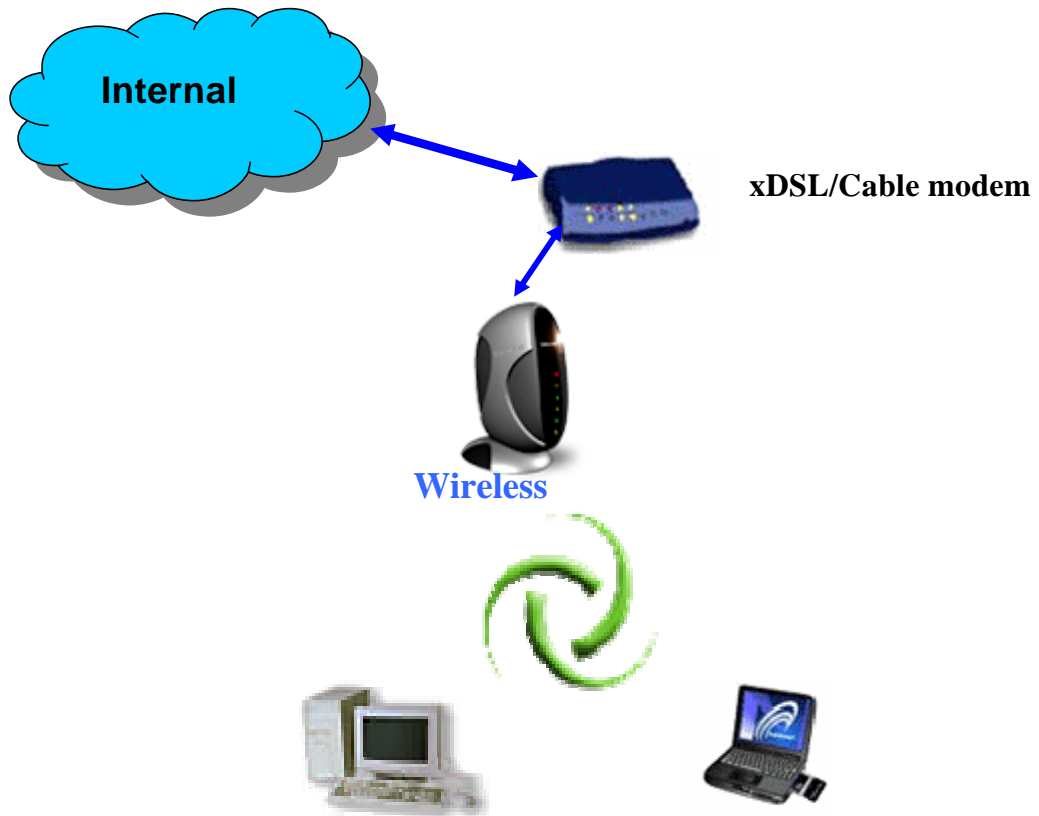
You can connect the WLAN 11b Router to your PC, a hub, or a switch. Run the Ethernet cable from one of the LAN ports on the rear of the WLAN 11b Router to your computer's network adapter or to another network device. You can also connect the WLAN 11b Router to your PC or to a client adapter via radio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



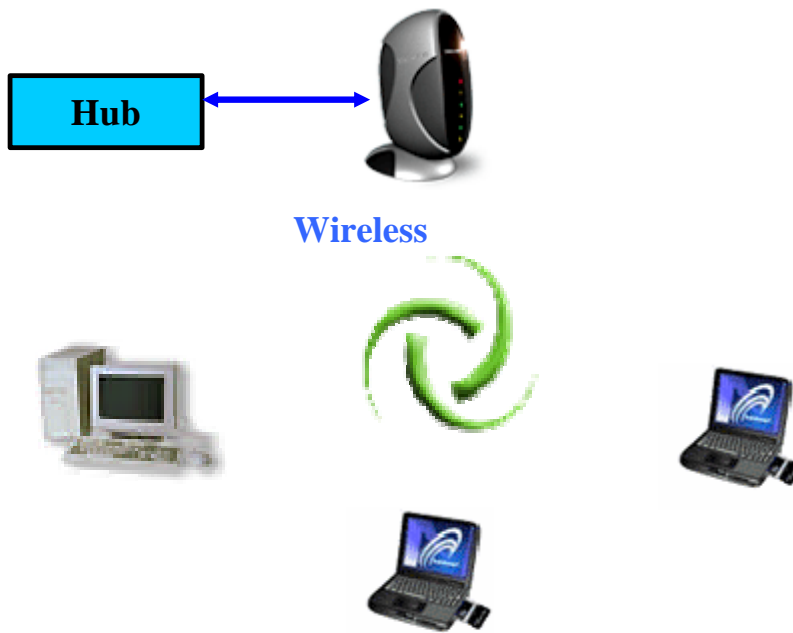
Power On

Connect the power adapter to the WLAN 11b Router.

SOHO/Home Networking



Office Networking



CONNECTING THE AP

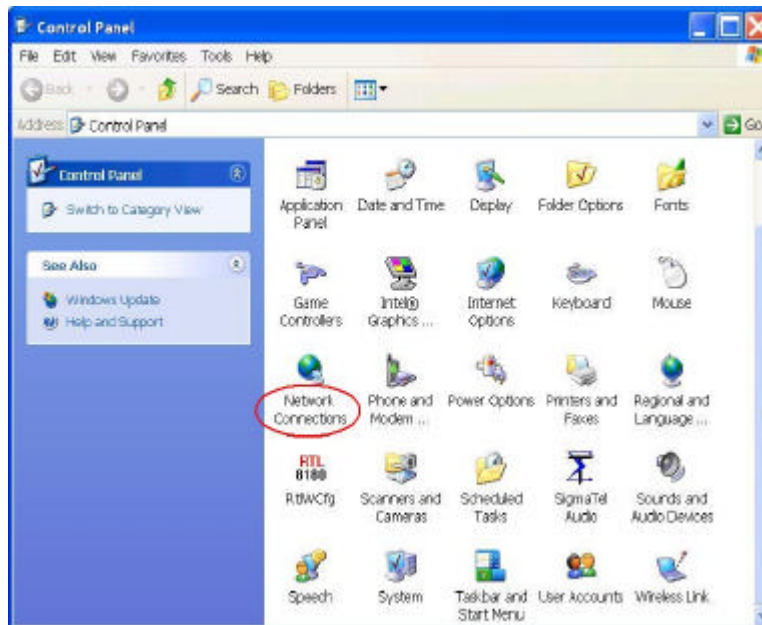
Follow the procedure below to connect the AP.

LAN connecting

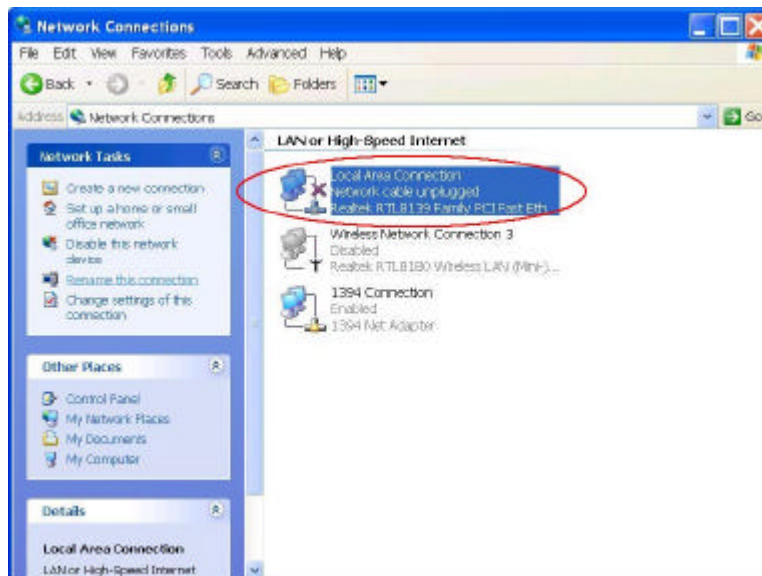
- Plug an Ethernet cable into a free LAN port at the rear of the AP. Plug the other end of the cable into the RJ-45 port on your computer.
- Turn on power supply for AP .
- Setting TCP/IP to work with the AP.

➤ Windows XP

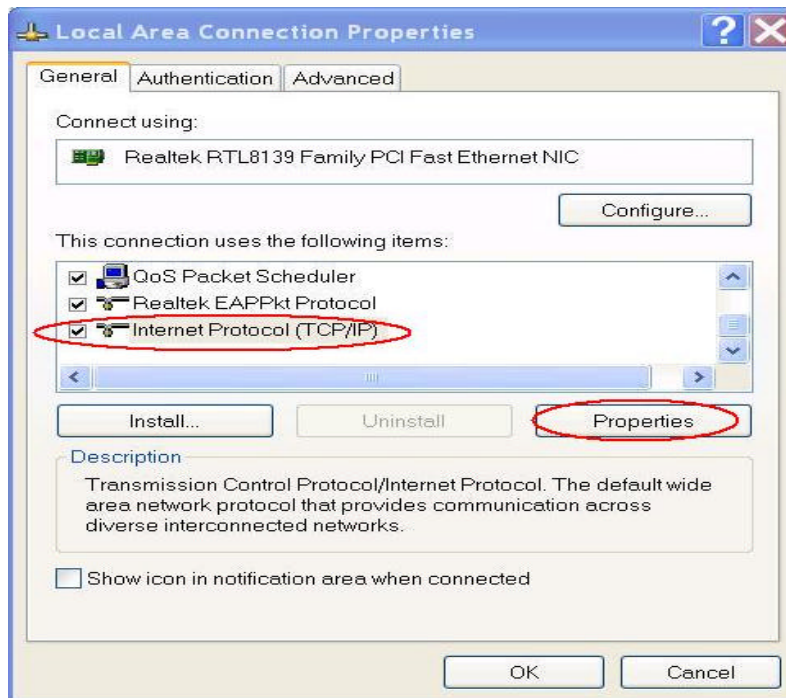
1. Click **Start**, **Settings**, then click **Control Panel**. The Control Panel opens:



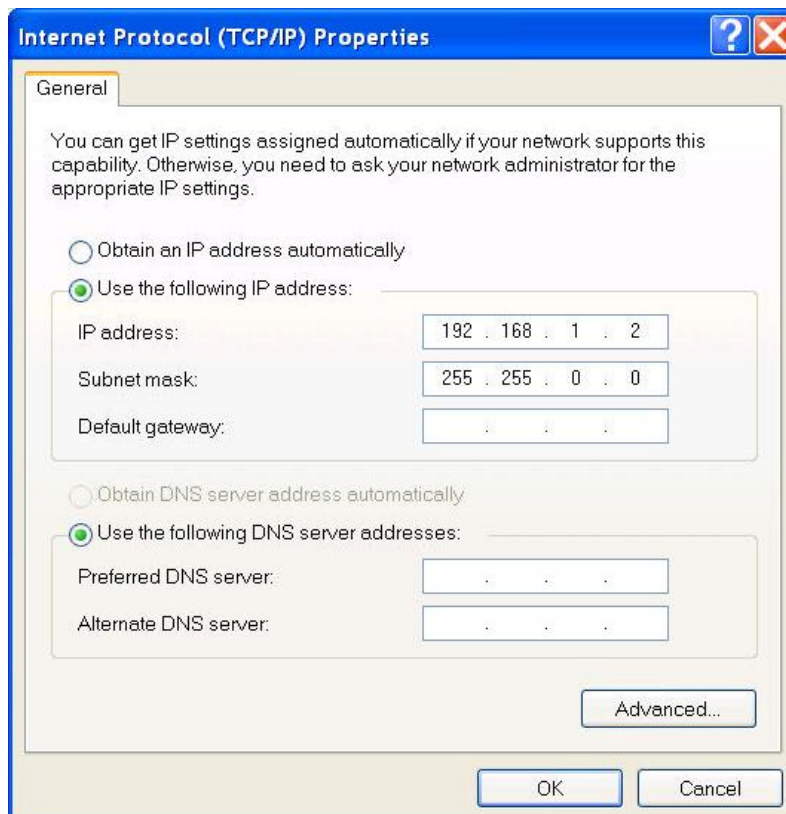
2. Right-click the **Network** icon and select "OPEN" to open the Network Connections dialog:



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:

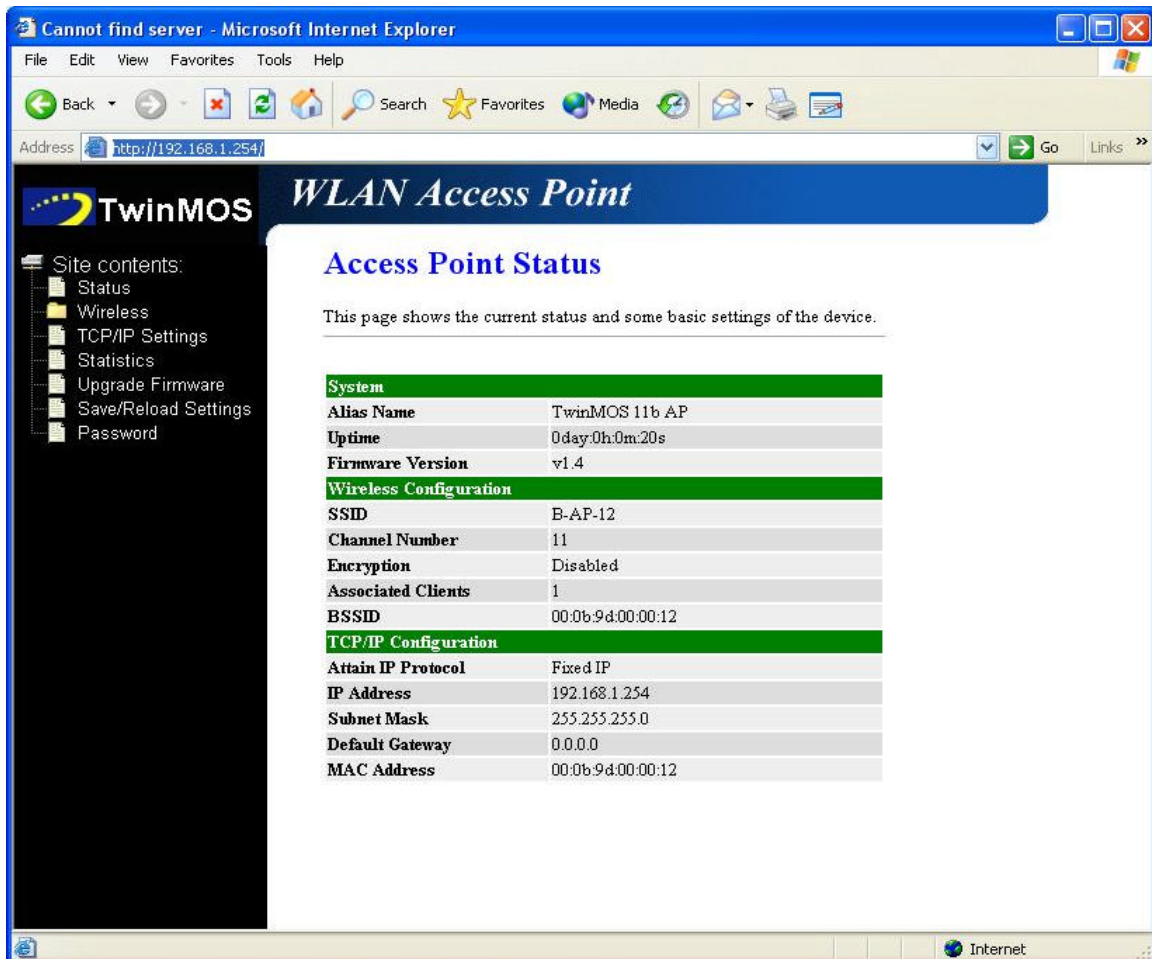


5. Assign an IP address: follow these steps:

- 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 2-253)
- 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 192.168.1.254. The default user name and password is “admin”.**



Cannot find server - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address <http://192.168.1.254/> Go Links >>

TwinMOS *WLAN Access Point*

Site contents:

- Status
- Wireless
- TCP/IP Settings
- Statistics
- Upgrade Firmware
- Save/Reload Settings
- Password

Access Point Status

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

System	
Alias Name	TwinMOS 11b AP
Uptime	0day:0h:0m:20s
Firmware Version	v1.4

Wireless Configuration	
SSID	B-AP-12
Channel Number	11
Encryption	Disabled
Associated Clients	1
BSSID	00:0b:9d:00:00:12

TCP/IP Configuration	
Attain IP Protocol	Fixed IP
IP Address	192.168.1.254
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
MAC Address	00:0b:9d:00:00:12

Internet

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

System	
Alias Name	TwinMOS 11b AP
Uptime	0day:1h:22m:16s
Firmware Version	v1.4
Wireless Configuration	
SSID	B-AP-12
Channel Number	11
Encryption	Disabled
Associated Clients	0
BSSID	00:0b:9d:00:00:12
TCP/IP Configuration	
Attain IP Protocol	Fixed IP
IP Address	192.168.1.254
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
MAC Address	00:0b:9d:00:00:12

Wireless connecting

- Turn on power supply for AP .
- Insert 802.11b wireless LAN card to your PC.
- Setting your wireless utility. The SSID is “B-AP-12”, WEP off, and Infrastructure mode.
- Setting TCP/IP to work with the AP.
(Please follow LAN connecting procedure)
- Open your Web browser and type the router IP address in the address bar. The AP default IP address is *192.168.1.254*.

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 “**admin**”.



Access Point Status Page

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

System	
Alias Name	TwinMOS 11b AP
Uptime	0day:1h:22m:16s
Firmware Version	v1.4
Wireless Configuration	
SSID	B-AP-12
Channel Number	11
Encryption	Disabled
Associated Clients	0
BSSID	00:0b:9d:00:00:12
TCP/IP Configuration	
Attain IP Protocol	Fixed IP
IP Address	192.168.1.254
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
MAC Address	00:0b:9d:00:00:12

Wireless--Basic Settings 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.

Alias Name:	<input type="text" value="TwinMOS 11b AP"/>
<input type="checkbox"/> Disable Wireless LAN Interface	
SSID:	<input type="text" value="B-AP-12"/>
Channel Number:	<input type="text" value="11"/>
Associated Clients:	<input type="button" value="Show Active Clients"/>
<input type="button" value="Apply Changes"/>	<input type="button" value="Reset"/>

- **Disable Wireless LAN Interface**

When the setting is checked, the RF signal of the device will be disabled.

- **SSID**

The name of the wireless network: This name cannot be longer than 32 characters. The default value is "B-AP-12."

- **Channel Number**

A transmission channel for wireless communications: The channel of any wireless device must match the channel selected here in order for the wireless device to access the LAN via the AP.

- **Associated Clients**

Click "Show Active Clients" button to launch the Active Wireless Client Table. This table shows the MAC address, transmission, receipt packet counters and encrypted status for each associated wireless client.

- **Apply Changes**

Click "Apply" button to save and implement the new settings.

- **Reset**

Click "Reset" button to reload default settings.

Wireless—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.

Authentication Type:	<input type="radio"/> Open System	<input type="radio"/> Shared Key	<input checked="" type="radio"/> Auto
Fragment Threshold:	<input type="text" value="2346"/>	(256-2346)	
RTS Threshold:	<input type="text" value="2347"/>	(0-2347)	
Beacon Interval:	<input type="text" value="100"/>	(20-1024 ms)	
Data Rate:	<input type="text" value="Auto"/>		
Preamble Type:	<input checked="" type="radio"/> Long Preamble	<input type="radio"/> Short Preamble	
Broadcast SSID:	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled	
IAPP:	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled	

• Authentication Type

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.

Auto – Auto switch the authentication algorithm depending on the wireless devices which the adapter is connecting to.

• Fragment 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 2347 bytes. Minor change is recommended

- **Beacon Interval**

This value specifies the duration between beacon packets (milliseconds). The beacon packets include the AP's information and are broadcasted to the WLAN network period.

- **Data Rate**

Auto - When it is enabled, the device will choose the most suitable transmission rate automatically.

- **Preamble Type**

Select either a short preamble or long preamble. Select a short preamble for WLANs with high network traffic; select a long preamble when the network traffic is low.

- **Broadcast SSID**

Enables and disables a Service Set Identifier broadcast. When enabled, the SSID of the AP is sent to wireless enabled devices on the LAN. Set the AP's SSID in the Basic screen.

- **IAPP:**

Inter Access Point Protocol

Wireless—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.

Encryption:	<input type="text" value="None"/>	<input type="button" value="Set WEP Key"/>
<input type="checkbox"/> Use 802.1x Authentication	<input checked="" type="radio"/> WEP 64bits	<input type="radio"/> WEP 128bits
WPA Authentication Mode:	<input type="radio"/> WPA-RADIUS	<input checked="" type="radio"/> Pre-Shared Key
WPA Unicast Cipher Suite:	<input checked="" type="checkbox"/> TKIP	<input type="checkbox"/> AES
Pre-Shared Key Format:	<input type="text" value="Passphrase"/>	
Pre-Shared Key:	<input type="text"/>	
Authentication RADIUS Server:	Port <input type="text" value="1812"/>	IP address <input type="text"/>
		Password <input type="text"/>
<i>Note: When encryption WEP is selected, you must set WEP key value.</i>		
<input type="button" value="Apply Changes"/> <input type="button" value="Reset"/>		

- **802.1x**

As the IEEE standard for access control for wireless and wired LANs, 802.1x provides a means of authenticating and authorizing devices to attach to a LAN port. This standard defines the Extensible Authentication Protocol (EAP), which uses a central authentication server to authenticate each user on the network.

- **AES(Advanced Encryption Standard)**

Security issues are a major concern for wireless LANs. AES is the U.S. government's next-generation cryptography algorithm, which will replace DES and 3DES.

- **TKIP**

The Temporal Key Integrity Protocol, pronounced tee-kip, is part of the IEEE 802.11i encryption standard for wireless LANs. TKIP is the next generation of WEP, the Wired Equivalency Protocol, which is used to secure 802.11 wireless LANs. TKIP provides per-packet key mixing, a message integrity check and a re-keying mechanism, thus fixing the flaws of WEP.

Wireless—Security Page(Set WEP key)

This page allows you setup the WEP key value. You could choose use 64-bit or 128-bit as the encryption key, and select ASCII or Hex as the format of input value.

Key Length:	<input type="text" value="64-bit"/>
Key Format:	<input type="text" value="Hex (10 characters)"/>
Default Tx Key:	<input type="text" value="Key 1"/>
Encryption Key 1:	<input type="text" value="*****"/>
Encryption Key 2:	<input type="text" value="*****"/>
Encryption Key 3:	<input type="text" value="*****"/>
Encryption Key 4:	<input type="text" value="*****"/>

- **Key Length**

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 Tx Key**

Select one of the keys (1~4) as the encryption key.

- **Encryption Key1~Key4**

The keys are used to encrypt data transmitted in the wireless network. Fill the text box by following the rules below.

64-bit – Input 10 digit Hex values (in the “A-F”, “a-f” and “0-9” range) as the encryption keys. For example: “0123456aef”.

128-bit – Input 26 digits Hex values (in the “A-F”, “a-f” and “0-9” range) as the encryption keys. For example: “01234567890123456789abcdef”.

Wireless—Access Control Page

If you enable wireless 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

Enable Wireless Access Control

MAC Address: Comment:

Apply Changes

Reset

Current Access Control List:

MAC Address	Comment	Select
-------------	---------	--------

Delete Selected

Delete All

Reset

Wireless—WDS Setting

Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC address of other APs which you want to communicate with in the table and then enable the WDS.

Enable WDS

Add WDS AP: MAC Address Comment

Apply Changes

Reset

Show Statistics

Current WDS AP List:

MAC Address	Comment	Select
-------------	---------	--------

Delete Selected

Delete All

Reset

TCP/IP Settings—LAN Interface 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:

Subnet Mask:

Default Gateway:

DHCP:

DHCP Client Range: -

DNS Server:

802.1d Spanning Tree:

Apply Changes Reset

- **IP Address**

This is the IP address of the AP. The default IP address is 192.168.1.254.

- **Subnet Mask**

Type the subnet mask for the AP in the text box. The default subnet mask is 255.255.0.0

- **Default Gateway**

Allows administrator to use the Default Gateway address, assign a specific Gateway address, or block clients from Gateway notification.

- **DHCP Server**

Enables the DHCP server to allow the AP to automatically assign IP addresses to devices connecting to the LAN. DHCP is enabled by default. All DHCP client computers are listed in the table at the bottom of the screen, providing the host name, IP address, and MAC address of the client.

- **DHCP Client Range**

Sets the beginning address and range of addresses to be assigned by the AP's DHCP server function. Select up to 253 consecutive addresses (nodes). The IPs to be excluded from the range specification should be entered in the specified field.

Statistics Page

This page shows the packet counters for transmission and reception regarding to wireless and Ethernet networks.

Wireless LAN	<i>Sent Packets</i>	375892
	<i>Received Packets</i>	79
Ethernet LAN	<i>Sent Packets</i>	2562
	<i>Received Packets</i>	3732695
Ethernet WAN	<i>Sent Packets</i>	465
	<i>Received Packets</i>	0

Refresh

Upgrade Firmware Page

This page allows you upgrade the Access Point firmware to new version. Please note, do not power off the device during the upload because it may crash the system.

Select File: 瀏覽...

Upload Reset

Follow these instructions:

1. Download the latest firmware from the manufacturer's Web site, and save it to your disk.
2. Click *Browse* and go to the location of the downloaded firmware file.
3. Select the file and click Upload to update the firmware to the latest release.

Save/Reload Setting Page

This page allows you save current settings to a file or reload the settings from the file which was saved previously. Besides, you could reset the current configuration to factory default.

Save Settings to File: Save...

Load Settings from File: 瀏覽... Upload

Reset Settings to Default: Reset

Password Page

This page is used to set the account to access the web server of Access Point. Empty user name and password will disable the protection.

User Name:	<input type="text"/>
New Password:	<input type="text"/>
Confirmed Password:	<input type="text"/>

- **User name** –Type your name to the text
- **New Password** - Type new password.
- **Confirmed Password** - Reenter the new password for confirmation.

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) must plug to LAN port of 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 192.168.1.254 then your IP of host PC must set 192.168.1.1~253.

Symptom: Forgot IP address

Resolution:

If you forgot the IP address of AP you can press reset button to restore the default factory settings by pressing this button for five seconds. The default IP is 192.168.1.254.

Symptom: Can not setting 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

10BaseT or 100BaseTx: 802.3 based Ethernet network that uses UTP (Unshielded twisted pair) cable and a star topology. 10 are 10 Mbps and 100 are 100 Mbps.

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

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 transmission.

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

Half-duplex: To transmit on the same channel in both directions, one direction at a time.

Host Name: The name given to a computer or client station that acts as a source for information on the

network.

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.

PoE (Power over Ethernet): A mechanism to send DC power to a device using a CAT5 Ethernet cable.

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.

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.

SMTP: SMTP (Simple Mail Transfer Protocol) is the standard Inter-net e-mail protocol. SMTP is a TCP/IP protocol defining message format and includes a message transfer agent that stores and forwards mail.

SNMP: SNMP (Simple Network Management Protocol) is a widely used network monitoring and control protocol. SNMP hardware or software components transmit network device activity data to the workstation used to oversee the network.

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

STP (Shielded Twisted Pair): Twisted Pair cable wrapped in a metal sheath to provide extra protection from external interfering signals.

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 address 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.

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.

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

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 objects, 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	140g
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 \pm 5%
Current Consumption	Min. 480mA(Standby) Max. 750mA

Networking Characteristics

Compatibility	<ul style="list-style-type: none"> ● IEEE 802.11b Standard for WLAN (DSSS) ● Internal Wi-Fi certified by TwinMOS ● IEEE 802.3 10/100Base-T Ethernet
Media Access Protocol	<ul style="list-style-type: none"> ● CSMA/CA ● TCP/IP ● IPX/SPX ● NetBEUI ● ARP
Management	<ul style="list-style-type: none"> ● Set IP Session (ARP/PING) ● Web-base management ● DHCP(Client & Server) ● WDS
Ethernet Interface	<ul style="list-style-type: none"> ● 10 /100Mbps RJ-45 Auto-negotiation network interface for LAN
Active Users	30

RF Characteristics

Frequency Range	2.400-2.484 GHz
Operating Channels	<ul style="list-style-type: none"> ● 1-11 United States (FCC) ● 1-11 Canada (DOC) ● 1-14 Japan (MKK) ● 1-13 Europe (Except Spain and France) (ETSI)
Modulation Technique	<ul style="list-style-type: none"> ● BPSK(1Mbps) ● QPSK(2 Mbps) ● CCK(5.5,11Mbps)
Spreading	11-chip Barker Sequence
Transmit Power	15 dBm @ Nominal Temp Range
Receive Sensitivity	Nominal Temp Range: -82 dBm @ 11Mbps
Security	<ul style="list-style-type: none"> ● 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

The equipment version marketed in US is restricted to usage of the channels 1-11 only.

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.

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