Air Live®

www.airlive.com

WL-5460AP v2

802.11g Multi-function Wireless Access Point

User's Manual

Declaration of Conformity

We, Manufacturer/Importer

OvisLink Corp.

5F., NO.6, Lane 130, Min-Chuan Rd.,

Hsin-Tien City, Taipei County, Taiwan

Declare that the product

802.11g Multi-function Wireless Access Point

WL-5460AP , WL-5450AP

is in conformity with

In accordance with 89/336 EEC-EMC Directive and 1999/5 EC-R & TTE Directive

Clause	Description
■ **EN 300 328 V1.6.1 (2004-11)**	Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband transmission equipment operating in the 2.4GHz ISM band And using spread spectrum modulation techniques; Part 1：technical Characteristics and test conditions Part2：Harmonized EN covering Essential requirements under article 3.2 of the R&TTE Directive
■ **EN 301 489-1 V1.4.1 (2002-08)** ■ **EN 301 489-17 V1.2.1 (2002-08)**	Electromagnetic compatibility and Radio spectrum Matters (ERM); Electromagnetic compatibility(EMC) standard for radio equipment and Services; Part 17：Specific conditions for wideband data and HIPERLAN equipment
■ **EN 55022: 1998/A1 :2000/A2:2003**	Limits and methods of measurement of radio disturbance characteristics of information technology equipment
■ **EN 55024:1998/A1 :2001/A2:2003**	Information Technology equipment-Immunity characteristics-Limits and Methods of measurement
■ **EN 50385**	Product standard to demonstrate the Compliance of radio base stations and Fixed terminal stations for wireless Telecommunication System with the Basic restrictions or the reference levels related to human exposure to radio Frequency electromagnetic fields (110 MHz － 40 GHz) - General public
■ **EN 60950-1:2001/ A11:2004**	Safety for information technology equipment including electrical business equipment
■ **CE marking**	CE0560

Manufacturer/Importer

Signature：

Name ： **Albert Yeh**

Position/ Title ： **Vice President**

Date： **2007/4/18**

(Stamp)

WL-5450(5460)AP CE Declaration Statement

Country	Declaration	Country	Declaration
cs Česky [Czech]	OvisLink Corp. tímto prohlašuje, že tento WL-5450(5460)AP je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.	lt Lietuvių [Lithuanian]	Šiuo OvisLink Corp. deklaruoja, kad šisWL-5450(5460)AP atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
da Dansk [Danish]	Undertegnede OvisLink Corp. erklærer herved, at følgende udstyr WL-5450(5460)APoverholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.	nl Nederlands [Dutch	Hierbij verklaart OvisLink Corp. dat het toestel WL-5450(5460)AP in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
de Deutsch [German]	Hiermit erklärt OvisLink Corp., dass sich das Gerät WL-5450(5460)APin Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.	mt Malti [Maltese]	Hawnhekk, OvisLink Corp, jiddikjara li dan WL-5450(5460)AP jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
et Eesti [Estonian]	Käesolevaga kinnitab OvisLink Corp. seadme WL-5450(5460)AP vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.	hu Magyar [Hungarian]	Alulírott, OvisLink Corp nyilatkozom, hogy a WL-5450(5460)AP megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.
en English	Hereby, OvisLink Corp., declares that this WL-5450(5460)AP is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.	pl Polski [Polish]	Niniejszym OvisLink Corp oświadcza, że WL-5450(5460)AP jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
es Español [Spanish]	Por medio de la presente OvisLink Corp. declara que el WL-5450(5460)APcumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.	pt Português [Portuguese]	OvisLink Corp declara que este WL-5450(5460)APestá conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
el Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ OvisLink Corp. ΔΗΛΩΝΕΙ ΟΤΙWL-5450(5460)AP ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.	sl Slovensko [Slovenian]	OvisLink Corp izjavlja, da je ta WL-5450(5460)AP v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
fr Français [French]	Par la présente OvisLink Corp. déclare que l'appareil WL-5450(5460)AP est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE	sk Slovensky [Slovak]	OvisLink Corp týmto vyhlasuje, že WL-5450(5460)AP spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
it Italiano [Italian]	Con la presente OvisLink Corp. dichiara che questo WL-5450(5460)AP è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.	fi Suomi [Finnish]	OvisLink Corp vakuuttaa täten että WL-5450(5460)AP tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen
lv Latviski [Latvian]	Ar šo OvisLink Corp. deklarē, ka WL-5450(5460)AP atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.	Íslenska [Icelandic]	Hér með lýsir OvisLink Corp yfir því að WL-5450(5460)AP er í samræmi við grunnkröfur og aðrar kröfur, sem gerðar eru í tilskipun 1999/5/EC.
sv Svenska [Swedish]	Härmed intygar OvisLink Corp. att denna WL-5450(5460)AP står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.	no Norsk [Norwegian]	OvisLink Corp erklærer herved at utstyret WL-5450(5460)AP er i samsvar med de grunnleggende krav og øvrige relevante krav i direktiv 1999/5/EF.

A copy of the full CE report can be obtained from the following address:

OvisLink Corp.
5F, No.6 Lane 130,
Min-Chuan Rd, Hsin-Tien City,
Taipei, Taiwan, R.O.C.

This equipment may be used in AT, BE, CY, CZ, DK, EE, FI, FR, DE, GR, HU, IE, IT, LV, LT, LU, MT, NL, PL, PT, SK, SI, ES, SE, GB, IS, LI, NO, CH, BG, RO, TR

FCC Certifications

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 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.

CAUTION:

Any changes or modifications not expressly approved by the grantee of this device could void the user's authority to operate the equipment.

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 RF Radiation Exposure Statement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20cm between the radiator and your body.

CE Mark Warning

This is a Class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

All trademarks and brand names are the property of their respective proprietors.

Specifications are subject to change without prior notification.

Table of Contents

Introduction

・ **WL-5460APv2** is world's most popular multi-function access point. It features an impressive total of 7 wireless multi-function modes that are not available in normal access point. In addition, the ACK timeout and RSSI feature makes it suitable for long distance application. From ordinary AP application to Hotspot and WISP usage, you will find the WL-5460AP is the device you want.

・ **WL-5460APv2** is an IEEE802.11b/g compliant 11 Mbps & 54 Mbps Ethernet Wireless Access Point. The Wireless Access Point is equipped with two 10/100 M Auto-sensing Ethernet ports for connecting to LAN and also for cascading to next Wireless Access Point.

・ **WL-5460APv2** provides 64/128bit WEP encryption, WPA-PSK, WPA2-PSK and IEEE802.1x which ensures a high level of security to protect users' data and privacy. The MAC Address filter prevents the unauthorized MAC Addresses from accessing your Wireless LAN. Your network security is therefore double assured.

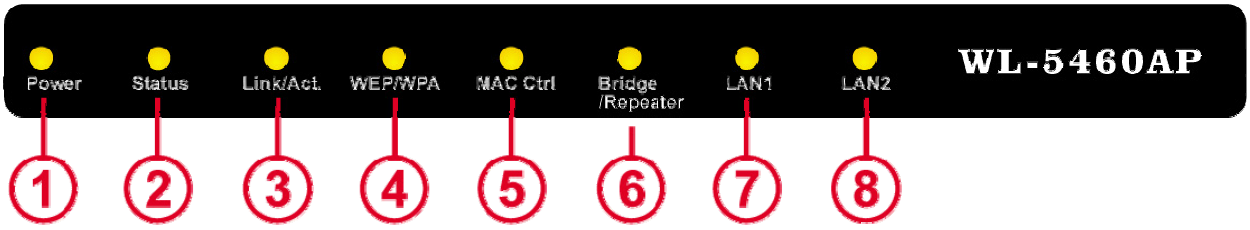
The web-based management utility is provided for easy configuration that your wireless network connection is ensured to be always solid and hassle free.

Features

1. 2x100Mbps LAN ports for Wireless AP cascade.,2MB flash,16MB SDRAM.
2. 18dBm output Power.
3. **AP** , **Client**, **Bridge** ,**WDS Repeater**, **Universal Repeater** mode.
4. **WISP Client Router**, **WISP+ Universal Repeater** mode.
5. Allows WEP 64/128 bit.
6. Support WPA-PSK, WPA2-PSK encryption.
7. Support data rate automatic fallback.
8. Automatic channel selection.
9. Allowable channels: 1~11 (USA [FCC]), 1~13 (Europe [ETSI])
10. Client access control.
11. Supports 802.1x/Radius client with EAP-TLS, TKIP, AES encryption.
12. Supports IAPP.
13. Adjustable Tx power, Tx rate, and SSID broadcast.
14. ACK Timeout , Watch dog function.
15. Web interface management.
16. Support System event log and statistics.
17. MAC filtering (For wireless only).

Parts, Names, and Functions

1. Front Panel: (LED Indicators) (5460AP / 5460AP v2)



	LED Indicator	Color	Status	
			Solid	**Flashing**
1	**Power**	Green	Turns solid green when power is applied to this device.	N/A.
2	**Status**	Red	Turns solid red when the device is booting, after boot successfully, the light turn off.	
3~6 Wireless	**Link/Act.**	Green	Turns solid green when connected and associated to at least a client station.	Receiving/ Sending data
	WEP/WPA	Orange	Turns solid orange when wireless security is enabled.	N/A
	MAC Ctrl	Orange	Turns solid orange when MAC Control is enabled.	N/A
	Bridge / Repeater	Orange	Turn solid **orange** when Bridge or Repeater is enabled.	N/A
7~8 Wired	**LAN 1**	Green	Turns solid green when linked to a local network.	Receiving/ Sending data
	LAN 2			

Table 1: LED Indicators

2. Rear Panel: Connection Ports (5460AP / 5460AP v2)

	Port/button	Functions
A	**12V DC**	Connects the power adapter plug
B	**LAN1**	Connects to Ethernet
C	**LAN2**	Connects to Ethernet
D	**(Factory) RESET**	Press over 3 seconds to reboot this device. Press for over 10 seconds to restore factory settings. Performing the Factory Reset will erase all previously entered device settings.

Table 2: Connection Ports

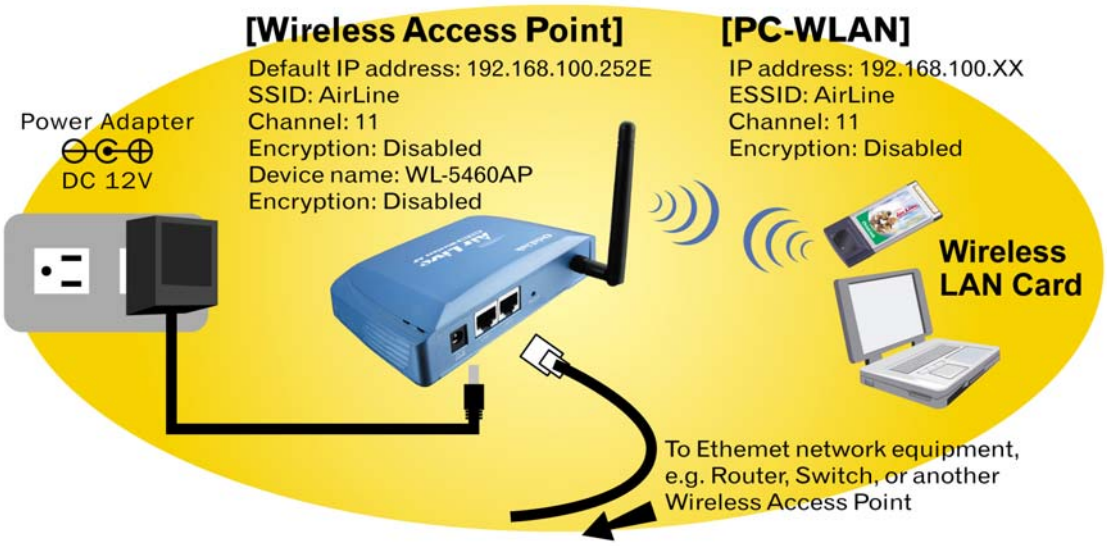
Factory Default Settings

Setting	Wireless Access Point
Device Name	**WL-5460AP v2**
SSID	Default value: **airlive**
Channel	Default value: **13**
WEP	Default value: **Disabled**
IP Address	Default value: **192.168.100. 252**
DHCP Server	• In **AP**, **Client**, and **Repeater** mode, the default DHCP Server is **disabled**, Please set your PC's IP to the same subnet as the AP to access the AP. • In **WISP** mode, the default DHCP server is **enabled**. Please restart your PC to renew the IP address.
DHCP Server IP Range	192.168.100.100~192.168.100.200

Table 3: Default Setting

Hardware Connection

Note: Before you starting hardware connection, you are advised to find an appropriate location to place the Access Point. Usually, the best place for the Access Point is at the center of your wireless network, with line of straight to all your wireless stations. Also, remember to adjust the antenna; usually the higher the antenna is placed; the better will be the performance.



1. Connect to your local area network: connect an Ethernet cable to one of the Ethernet port.
2. (LAN1 or LAN2) of this Wireless Access Point, and the other end to a hub, switch, router, or another wireless access point.
3. Power on the device: connect the included AC power adapter to the Wireless Access Point's power port and the other end to a wall outlet.

· **Check the LED:**

The Power and LAN # LED should be ON. LAN# LED will even blink if there is traffic.

The Link/Act LED will be on in static when associated with a station and blink whenever this AP receives data packets in the air.

If the Status LED glows after self-test, it means the Wireless Access Point fails on self test. Please ask your dealer for technical support.

4. Please make sure your computer IP is in the same subnet as the AP (i.e. 192.168.100.x).
5. please make sure your computer has wireless network adapter installed.
6. Open the web browser and enter http://192.168.100.252/.

About the Wireless Operation Modes

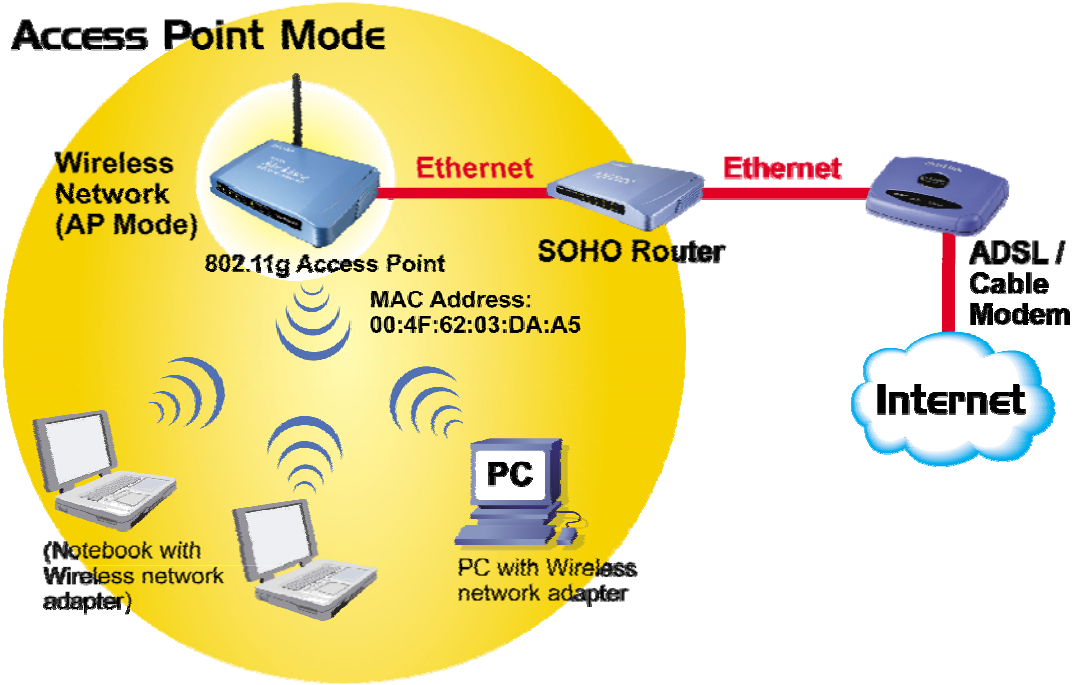
The WL-5460AP v2 device provides all 7 modes of wireless operational applications with:

1. **Access Point Mode.**
2. **Client Mode.**
3. **Bridge Mode.**
4. **WDS Repeater Mode.**
5. **Universal Repeater Mode.**
6. **WISP (Client Router) Mode.**
7. **WISP + Universal Repeater Mode.**

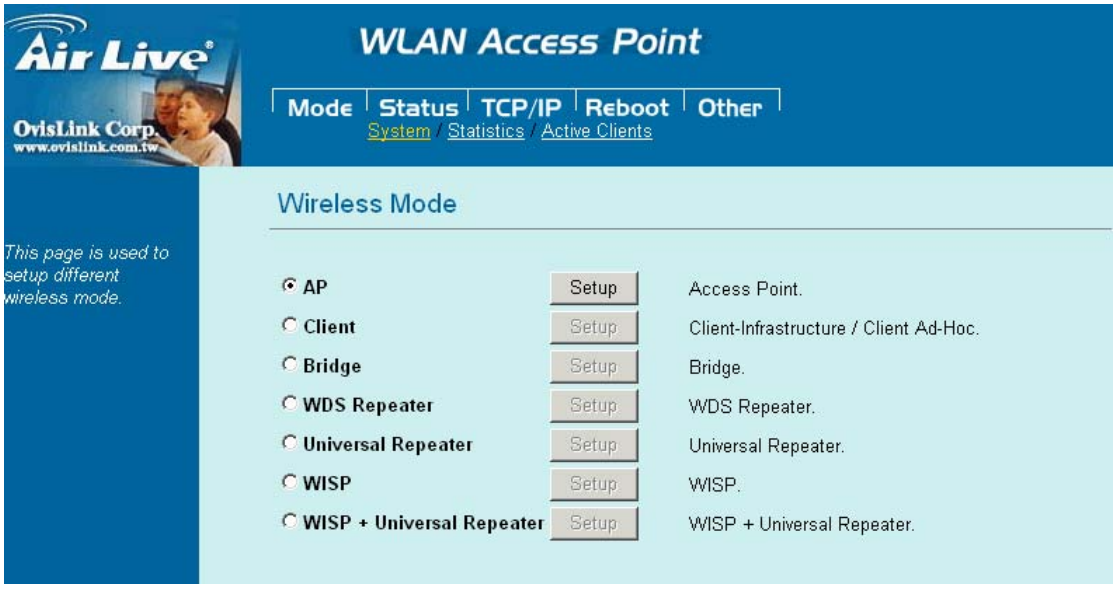
This device is shipped with configuration that is functional right out of the box. If you want to change the settings in order to perform more advanced configuration or even change the mode of operation, you can use the web-based utility provided by the manufacturer as described in the following sections.

Access Point Mode

When acting as an access point (default setting), this device connects all the stations (PC/notebook with wireless network adapter) to a wired network. All stations can have the Internet access if only the Access Point has the Internet connection. See the sample application below.



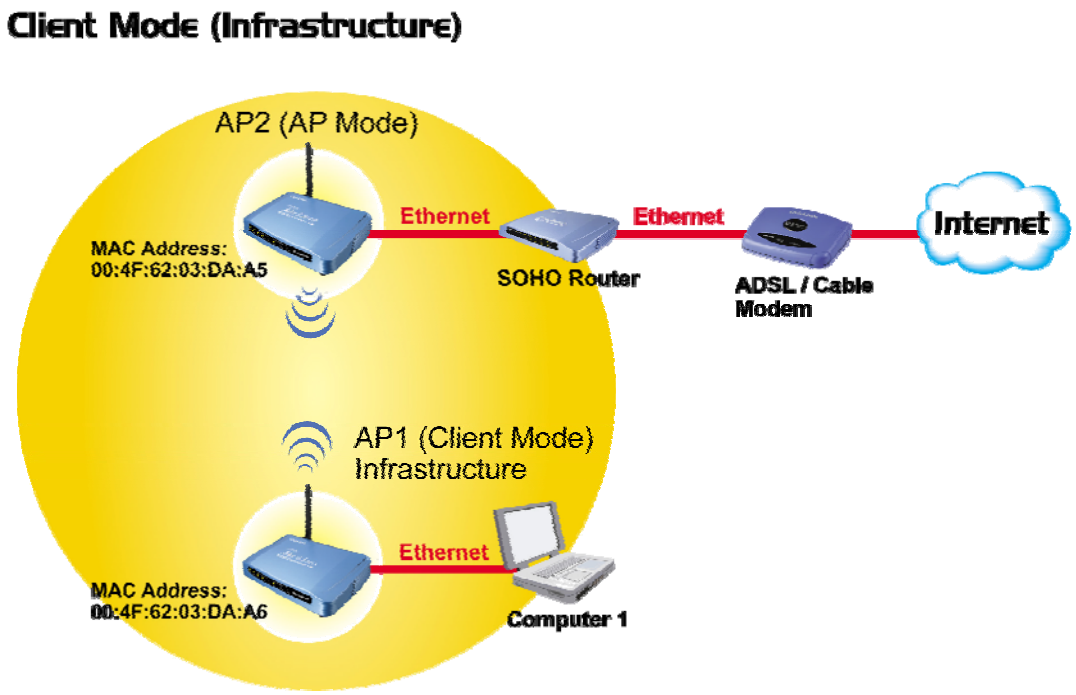
To set the operation mode to **"Access Point"**, please go to **"Mode →AP"** and click the **Setup** button.



Client Mode (Infrastructure)

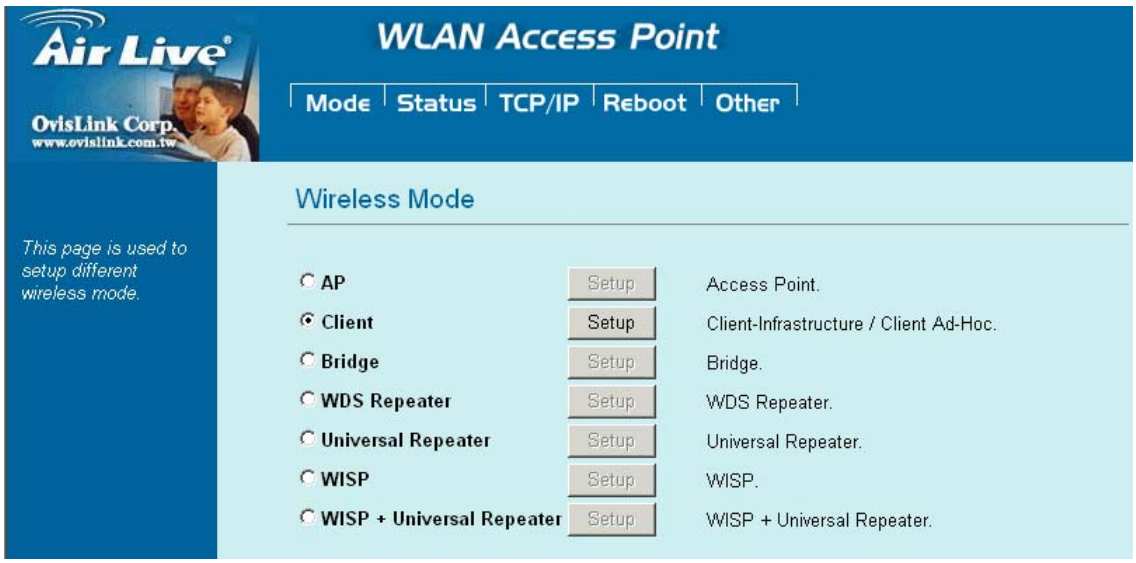
If set to Client (Infrastructure) mode, this device can work like a wireless station when it's connected to a computer so that the computer can send packets from wired end to wireless interface.

Refer to the illustration below. This station (AP1 plus the connected computer 1) can associate to another Access Point (AP2), and then can have the Internet access if the other Access Point (AP2) has the Internet connection.



To set the operation mode to **"Client (Infrastructure)"**, Please go to **"Mode →Client"** and click the **Setup** button.

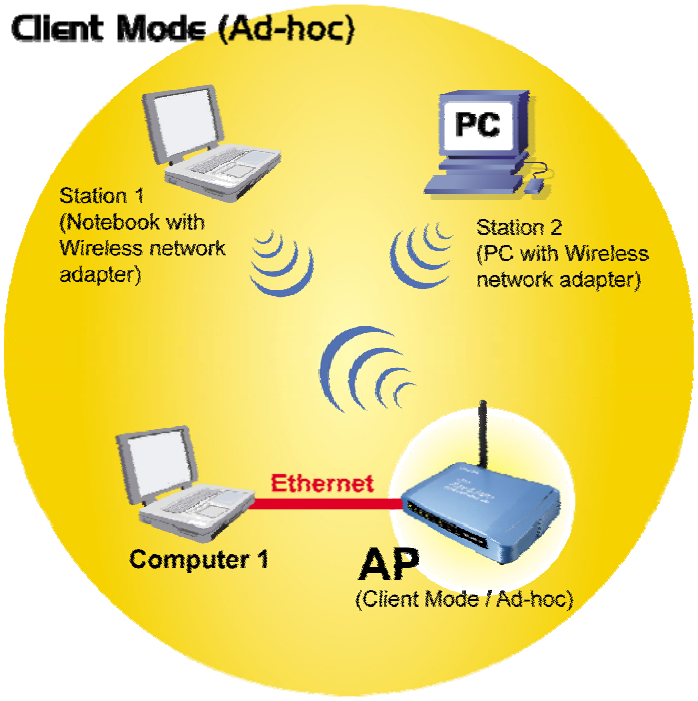
In the **"Network Type"** field, select as **"infrastructure"** for configuration.



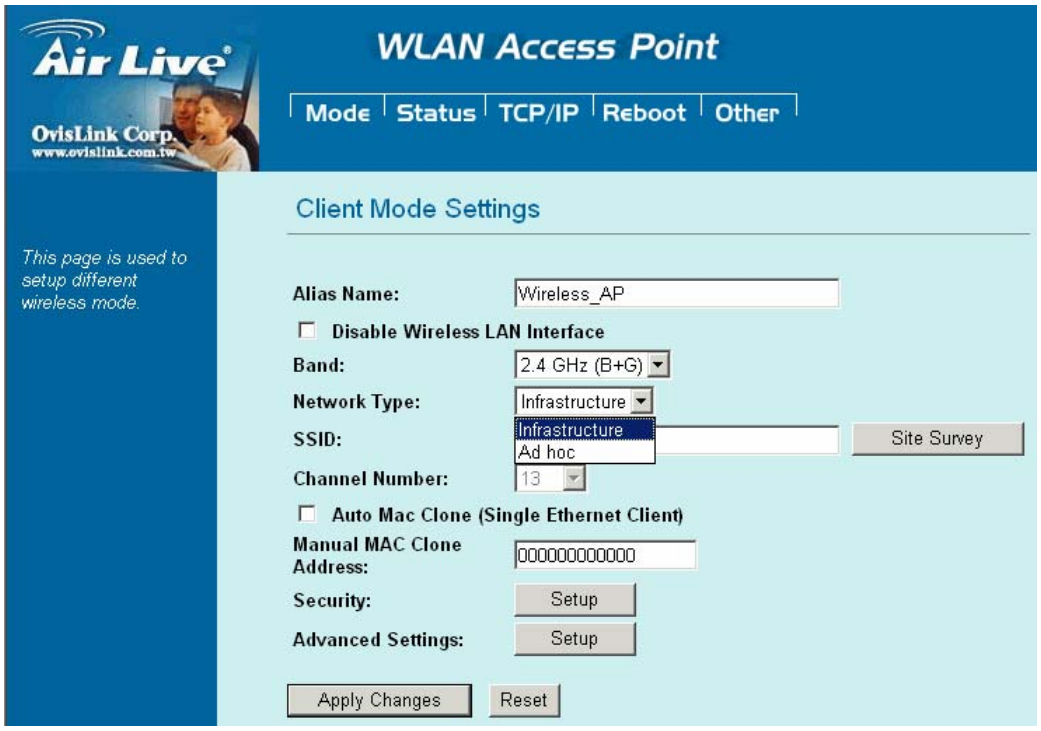
Client Mode (Ad-hoc)

If set to the Client (Ad-hoc) mode, this device can work like a wireless station when it is connected to a computer so that the computer can send packets from wired end to wireless interface. You can share files and printers between wireless stations (PC and laptop with wireless network adapter installed).

See the sample application below.



To set the operation mode to **"Client (Ad-Hoc)"**, Please go to **"Mode →Client"** and click the **Setup** button. In the **"Network Type"** field, select as **"infrastructure"** for configuration.

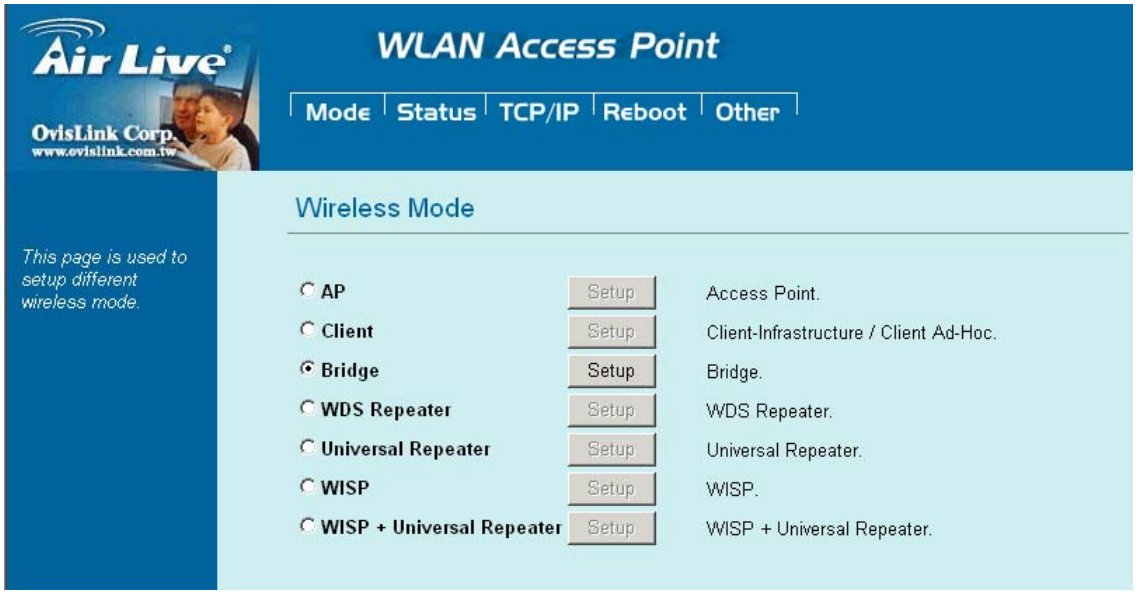


Bridge Mode

In this mode, 2 access points in two remote locations connect to each other to provide a wireless bridge between 2 remote LANs. It is mostly used by enterprise to connect 2 remote office's network together. The bridge modes are connected by using either the WDS (Wireless Distribution System) or Ad-Hoc topology.

This feature is also useful when users want to bridge networks between buildings where it is impossible to deploy network cable connections between these buildings.

To set the operation mode to **"Bridge"**, Please go to **"Mode →Bridge"** and click the **Setup** button for configuration.

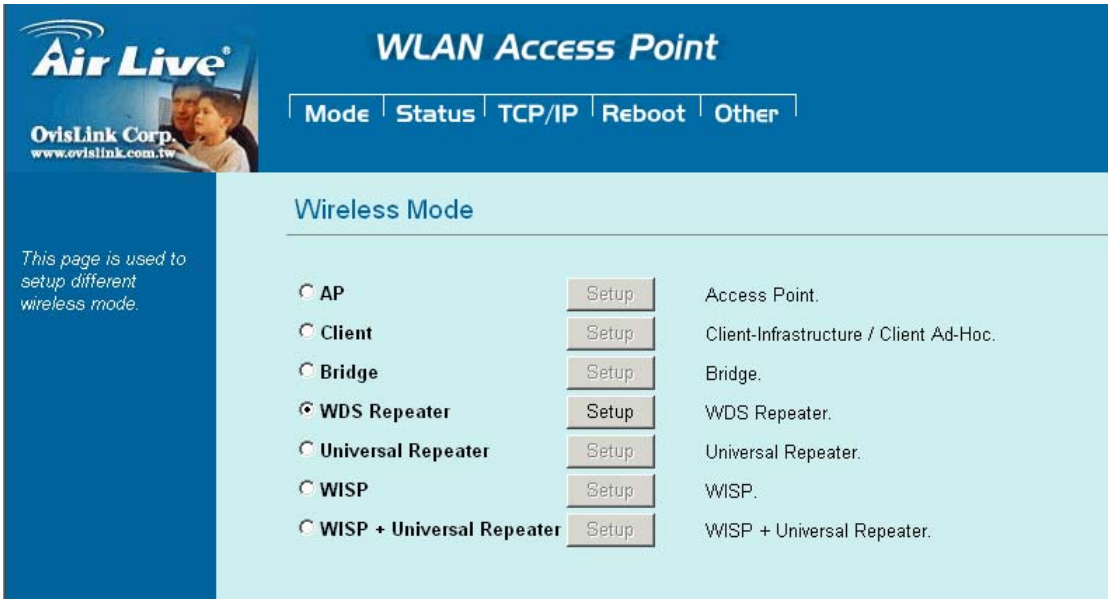


WDS Repeater Mode

A repeater's function is to extend the wireless coverage of another wireless AP or router.

For WDS repeater to work, the remote wireless AP/Router must also support WDS function.

To set the operation mode to **"WDS Repeater"**, Please go to **"Mode →WDS Repeater"** and click the **Setup** button for configuration.

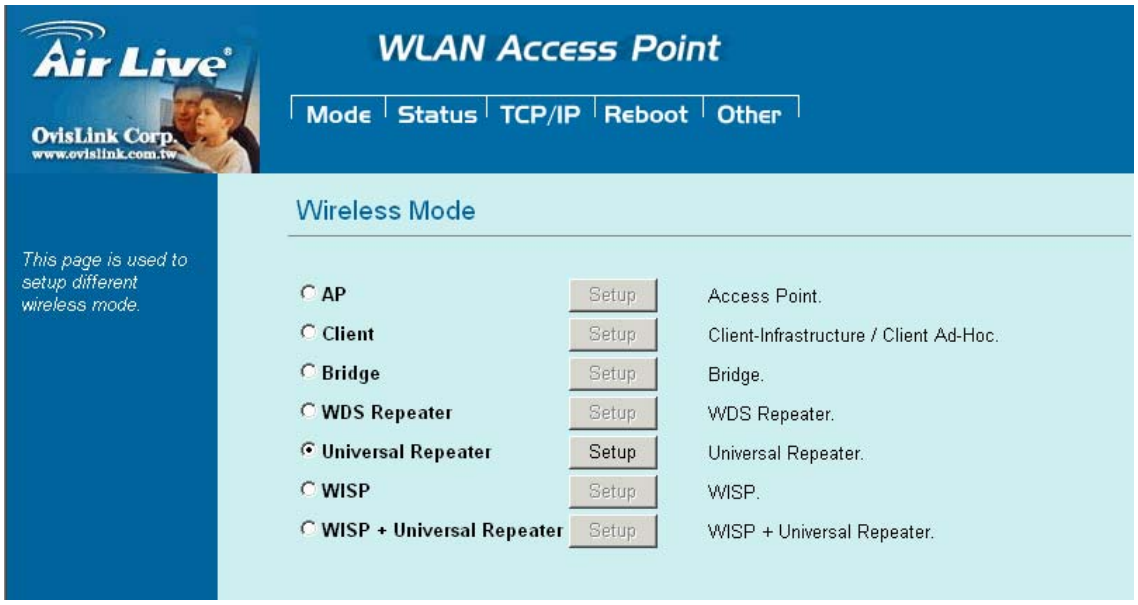


Universal Repeater Mode

A universal repeater can also extend the wireless coverage of another wireless AP or router. But the universal repeater does not require the remote device to have WDS function. Therefore, it can work with almost any wireless device.

Note: When you are using the universal repeater mode, please make sure the remote AP/Router‘s WDS function is turned off.

To set the operation mode to **“Universal Repeater”**, Please go to **“Mode →Universal Repeater”** and click the **Setup** button for configuration.

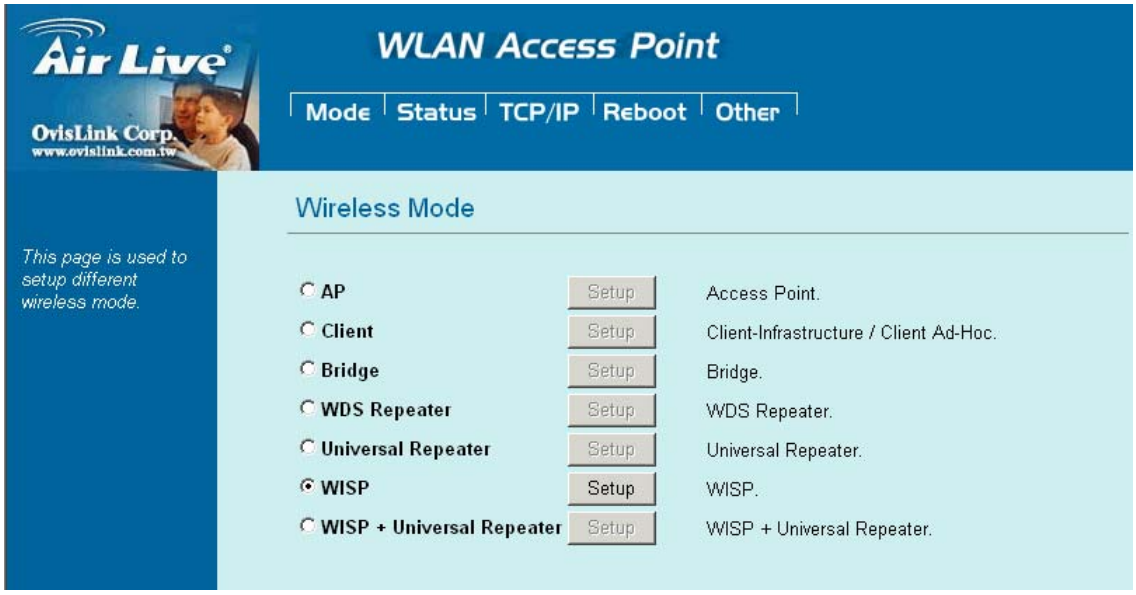


WISP (Client Router) Mode

WISP (Client Router) mode

In WISP mode, the AP will behave just the same as the Client mode for wireless function. However, Router functions are added between the wireless WAN side and the Ethernet LAN side. Therefore, The WISP subscriber can share the WISP connection without the need for extra router.

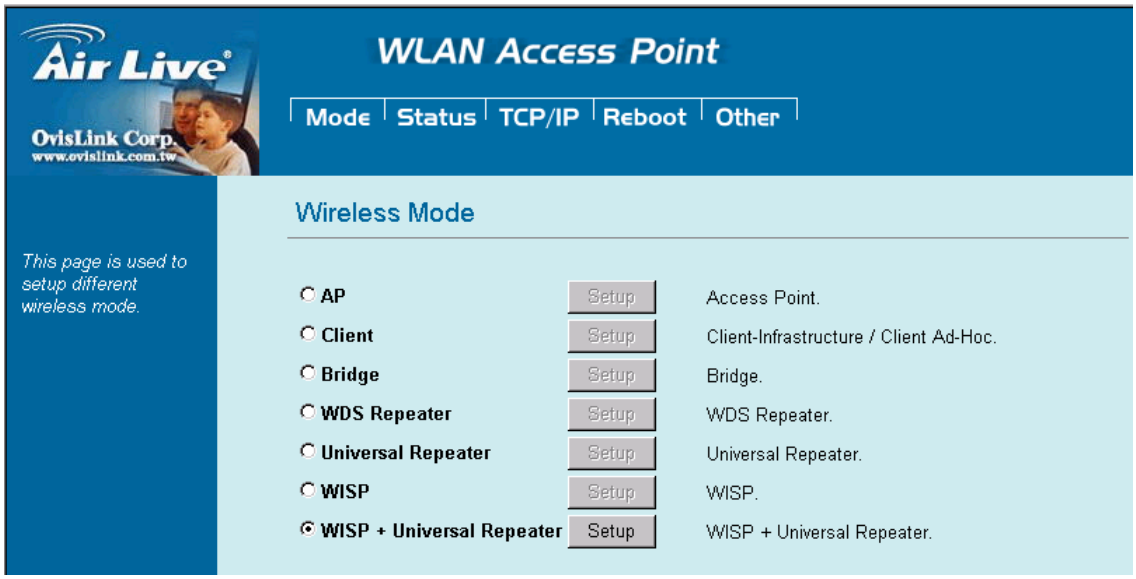
To set the operation mode to **"WISP"**, Please go to **"Mode →WISP"** and click the **Setup** button for configuration.



WISP + Universal Repeater Mode

In this mode, the AP behaves virtually the same as the WISP mode, except one thing: the AP can also send wireless signal to the LAN side. That means the AP can connect with the remote WISP AP and the indoor wireless card, and then provide IP sharing capability all at the same time! However, the output power is divided between 2 wireless sides and proper antenna installation can influence the performance greatly.

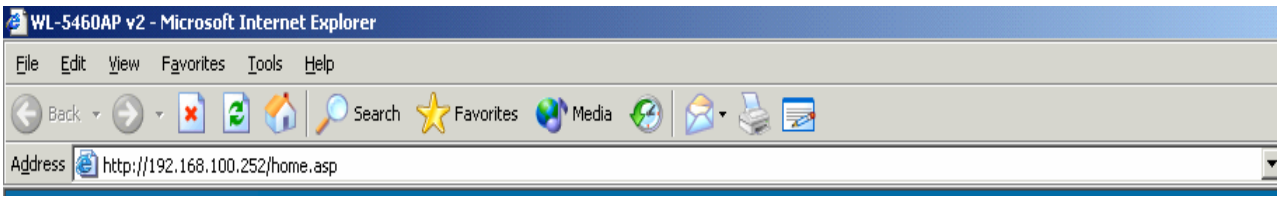
To set the operation mode to **"WISP + Universal Repeater"**, Please go to **"Mode →WISP + Universal Repeater"** and click the **Setup** button for configuration.



Configuration

1. Start your computer. Connect an Ethernet cable between your computer and the Wireless Access Point.
2. Make sure your wired station is set to the same subnet as the Wireless Access Point, i.e. 192.168.100.X
3. Start your WEB browser. In the *Address* box, enter the following:

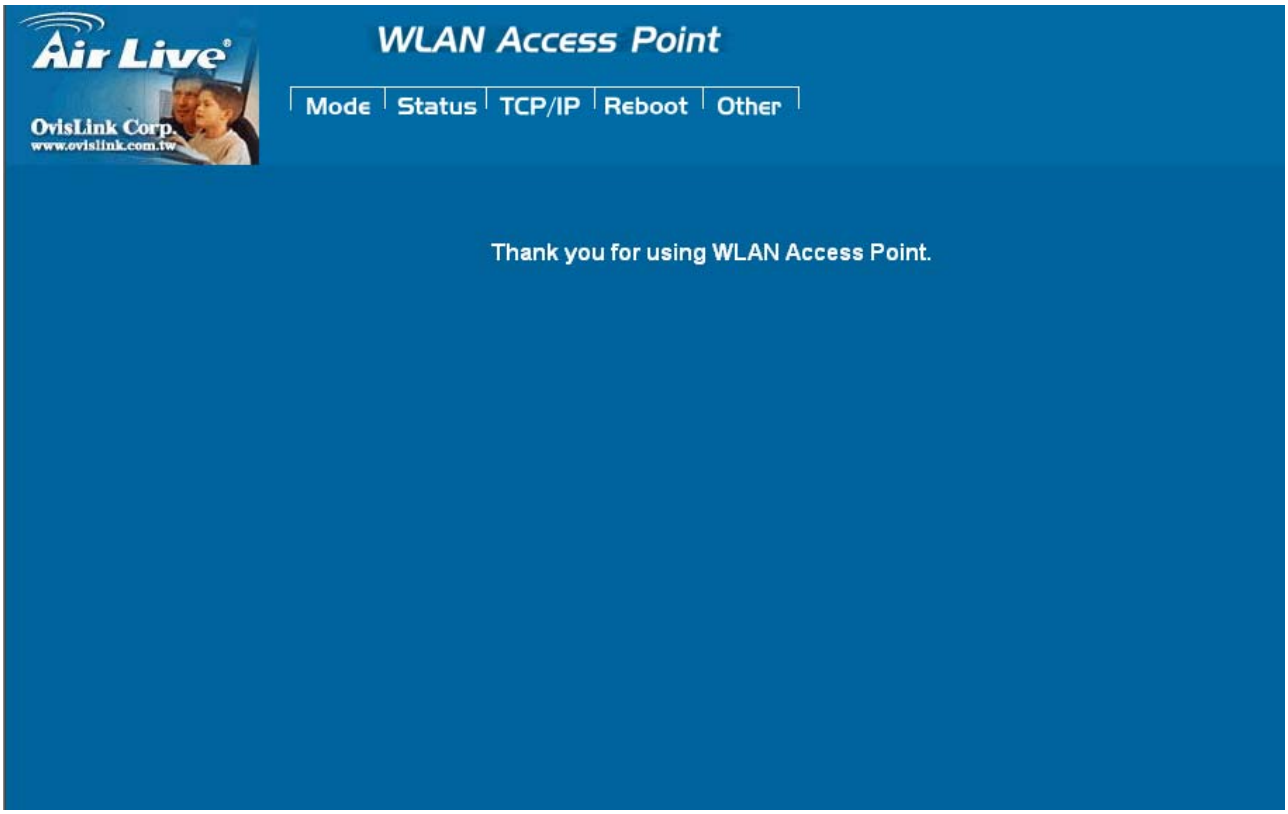
http://192.168.100.252/



The configuration menu is divided into five categories:

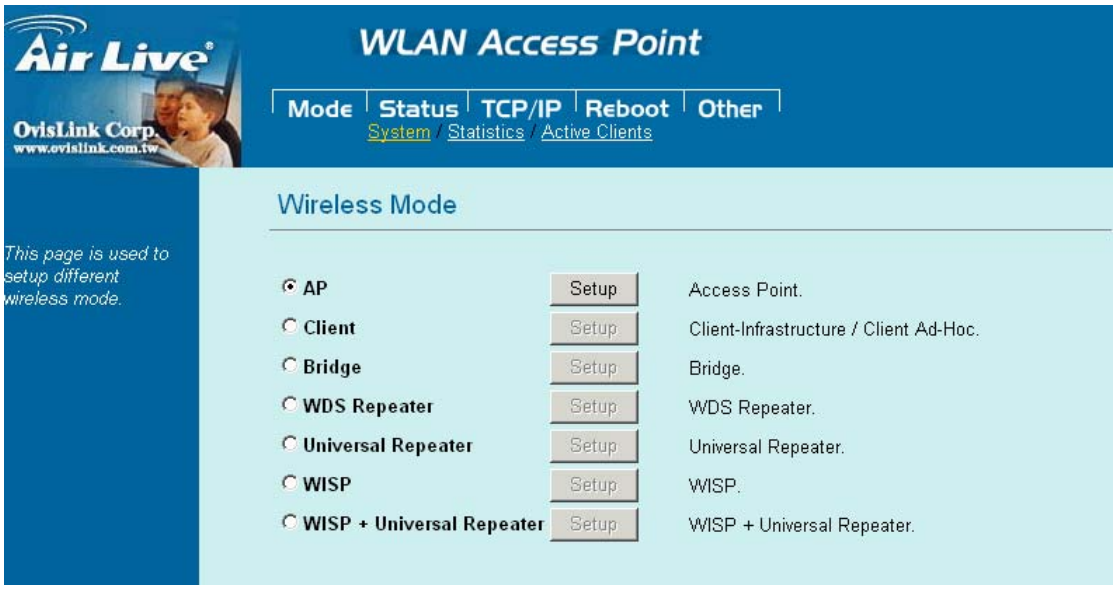
Mode, Status, TCP/IP, Reboot and **Other.**

Click on the desired setup item to expand the page in the main navigation page. The setup pages covered in this utility are described below.



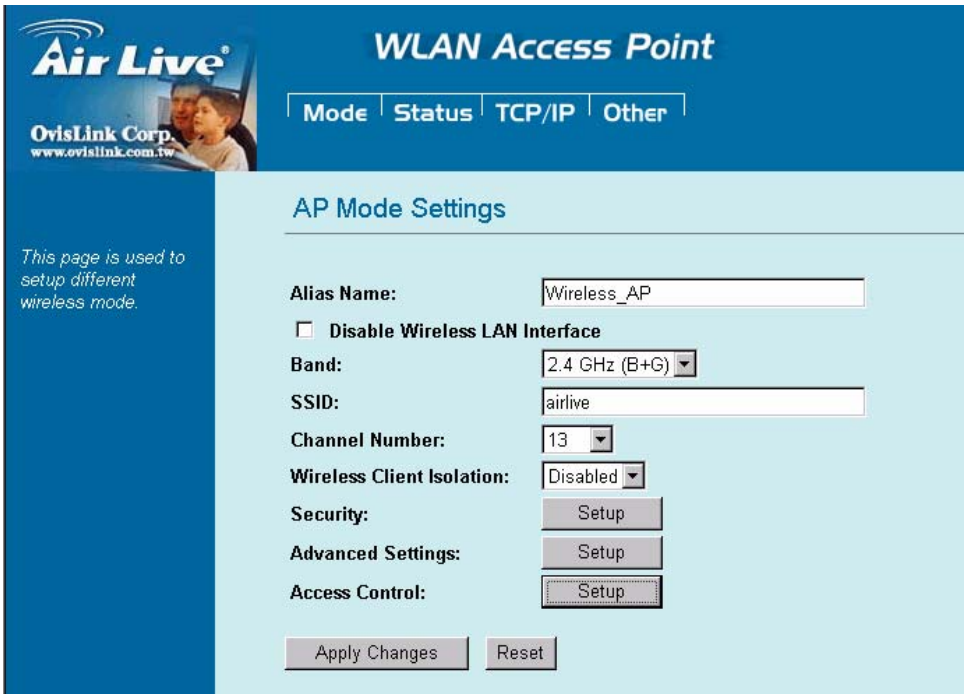
Mode

You can choose and setup different wireless mode for detail configurations



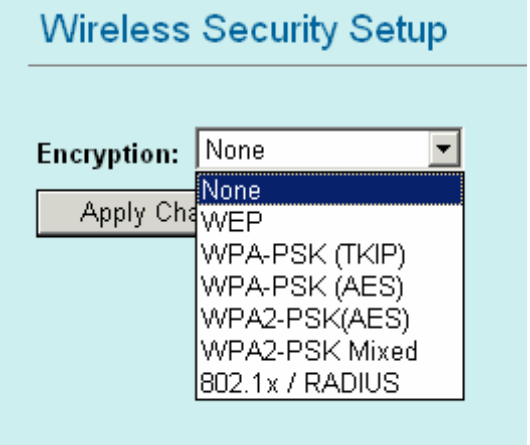
Wireless Mode	
AP	Select the AP and press Setup button for Wireless AP mode configuration.
Client	Select the Client and press Setup button for Wireless Client mode configuration.
Bridge	Select the Bridge and press Setup button for Wireless Bridge mode configuration.
WDS Repeater	Select the WDS Repeater and press Setup button for Wireless WDS Repeater mode configuration.
Universal Repeater	Select the Universal Repeater and press Setup button for Wireless Universal repeater mode configuration.
WISP	Select the WISP and press Setup button for WISP (Client Router) mode configuration.
WISP + Universal Repeater	Select the WISP + Universal Repeater and press Setup button for WISP + Universal Repeater mode configuration.

AP Mode Setting



Alias Name	You can set the alias name for this device. Limited not exceed 32 characters.
☐ **Disable Wireless LAN Interface**	Check the box to disable the Wireless LAN Interface, by so doing; you won't be able to make wireless connection with this Access Point in your located network. In other words, this device will not be visible by any wireless station.
Band	You can choose one mode of the following you need. ⊙ 2.4GHz **(B):** 802.11b supported rate only. ⊙ 2.4GHz **(G):** 802.11g supported rate only. ⊙ 2.4GHz **(B+G):** 802.11b supported rate and 802.11g supported rate. The default is 2.4GHz **(B+G)** mode.
SSID	The SSID differentiates one WLAN from another; therefore, all access points and all devices attempting to connect to a specific WLAN must use the same SSID. It is case-sensitive and must not exceed 32 characters. A device will not be permitted to join the BSS unless it can provide the unique SSID. An SSID is also referred to as a network name because essentially it is a name that identifies a wireless network. The default SSID is **airlive**.
Channel Number	Allow user to set the channel **manually** or **automatically**. If set channel manually, just select the channel you want to specify. If "Auto" is selected, user can set the channel range to have Wireless Access Point automatically survey and choose the channel with best situation for communication. The number of channels supported depends on the region of this Access Point. All stations communicating with the Access Point must use the same channel. The default channel is **13**.

Wireless Client Isolation	Allow user to set the function **Enabled** or **Disabled**. By the function, all wireless clients can't mutual link, but wireless client still link with LAN port adapter. The default value is **Disabled**.
Security	Press the setup button for detail configurations



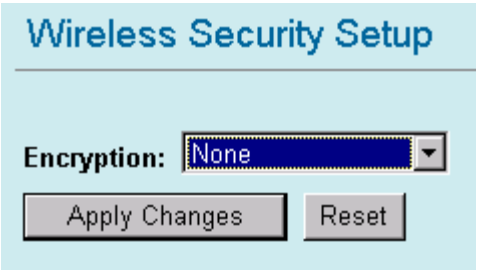
To provide a certain level of security, the IEEE 802.11 standard has defined two types of authentication methods: **Open System** or **Shared Key**. And WL-5460APv2 also support other wireless authentication and encryption methods for enhance your wireless network.

With Open System authentication, a wireless PC can join any network and receive any messages that are not encrypted. With Shared Key authentication, only those PCs that possess the correct authentication key can join the network. By default, IEEE 802.11 wireless devices operate in an Open System network and None data encryption. If you want secure your wireless network, you need to setup wireless security related function to enable security network.

None

Encryption: None (Encryption is set to **None** by default.**)**

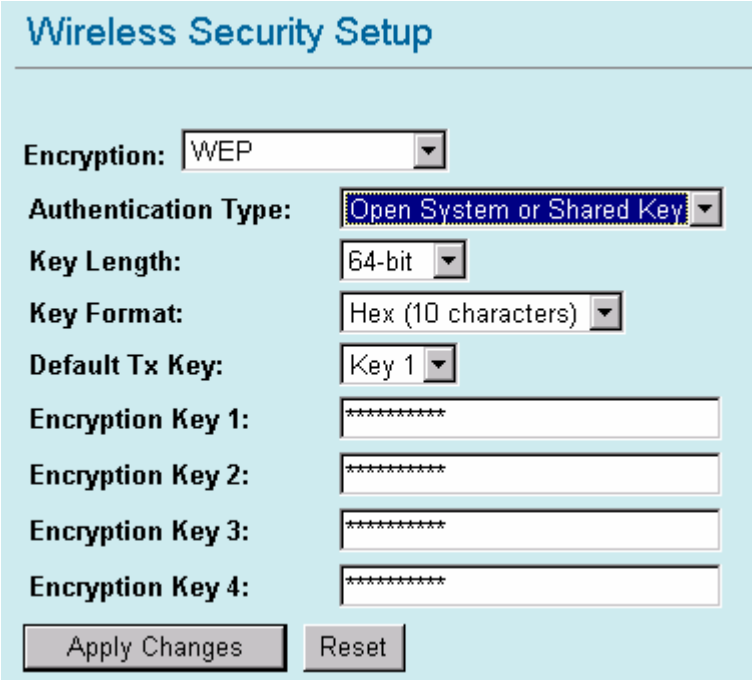
If the Access Point is using **Encryption None**, then the wireless adapter will need to be set to the same authentication mode.



WEP

Encryption: WEP

If selected WEP encryption, you must set WEP key value:



Encryption	WEP
Authentication Type	You can select **Open System** or **Shared Key** type for authentication.
Key Length	You can set **64bit** or **128bit** Encryption.
Key Format	Select **ASCII** if you are using ASCII characters (**case-sensitive**). Select **HEX** if you are using hexadecimal numbers (**0-9, or A-F**).
Default TX Key	You can enter 4 different Encryption Key and select one key to use as default.

10 hexadecimal digits or **5 ASCII characters** are needed if **64-bit WEP** is used;

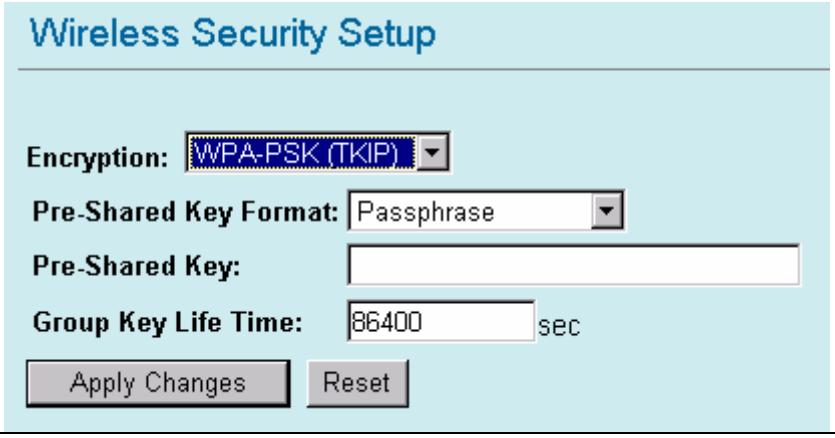
26 hexadecimal digits or **13 ASCII characters** are needed if **128-bit WEP** is used.

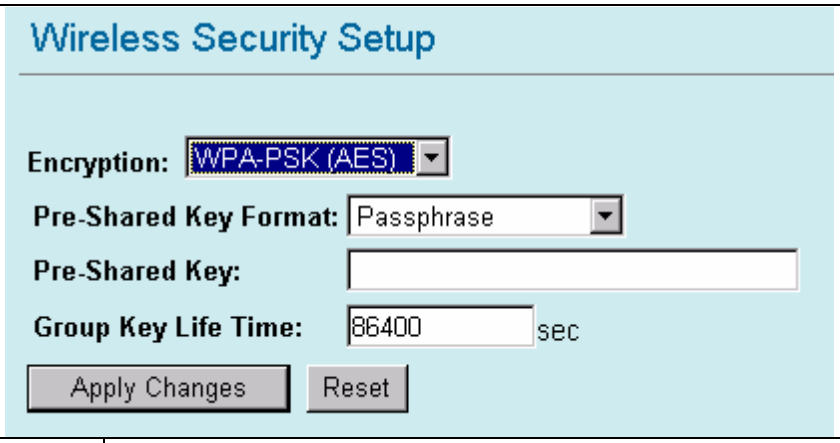
Shared Key is used when both the sender and the recipient share a secret key. So you can choose Open system, or one Shared Key authentication method.

WPA-PSK

Encryption: WPA-PSK (TKIP) or WPA-PSK (AES)

Wi-Fi Protected Access (WPA) with Pre-Shared Key (PSK) provides better security than WEP keys. It does not require a RADIUS server in order to provide association authentication, but you do have to enter a shared key for the authentication purpose. The encryption key is generated automatically and dynamically.



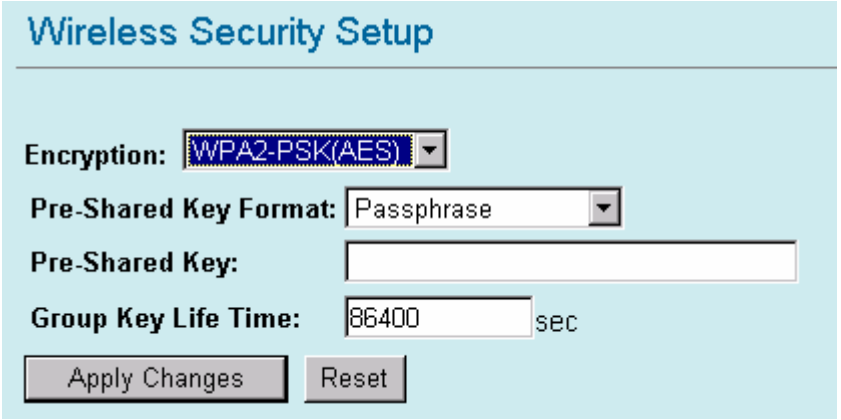


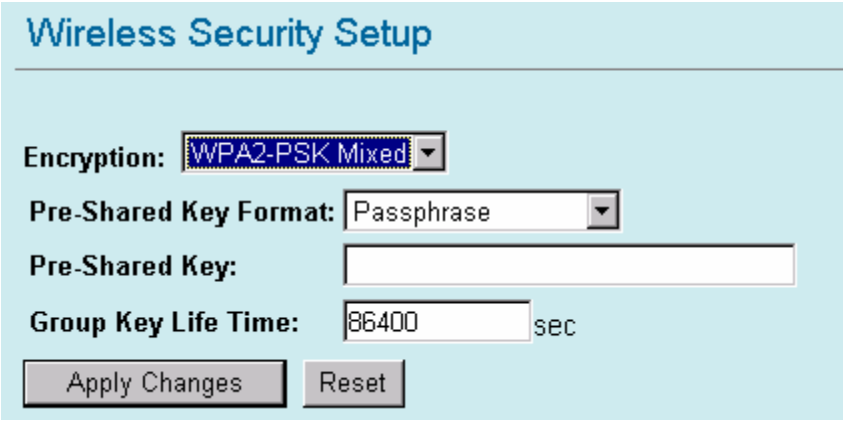
Encryption	You can select WPA-PSK (TKIP) or WPA-PSK (AES) method for data encryption.
Pre-shared Key	There are two formats for choice to set the Pre-shared key, i.e. **Passphrase** and **Hex**. If **Hex** is selected, users will have to enter a 64 characters string. For easier configuration, the **Passphrase** (at least 8 characters) format is recommended.
Group Key Life Time	Enter the number of seconds that will elapse before the group key change automatically. The default is 86400 seconds.

WPA2-PSK

Encryption: WPA2-PSK (AES) or WPA-PSK Mixed

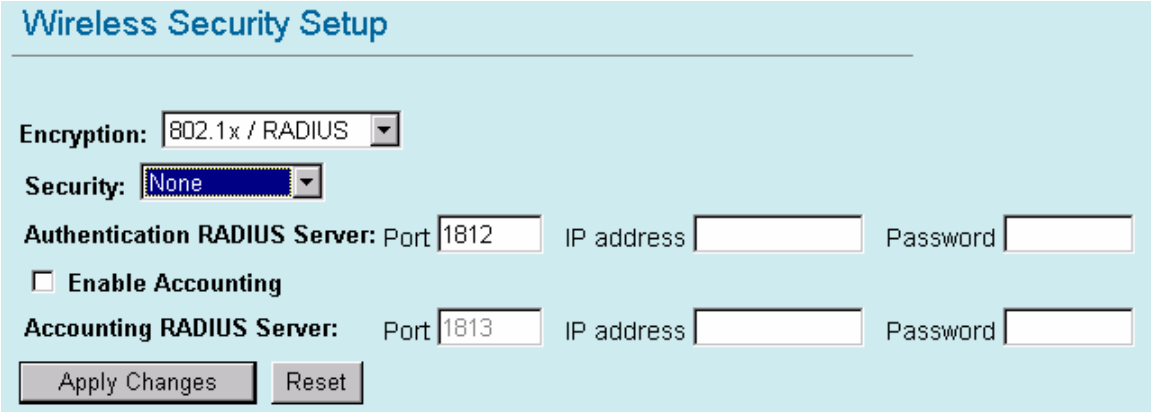
WPA2-PSK authentication method is almost like WPA-PSK, You can choose the Pre-Shared Key format and enter the Pre-shared key,

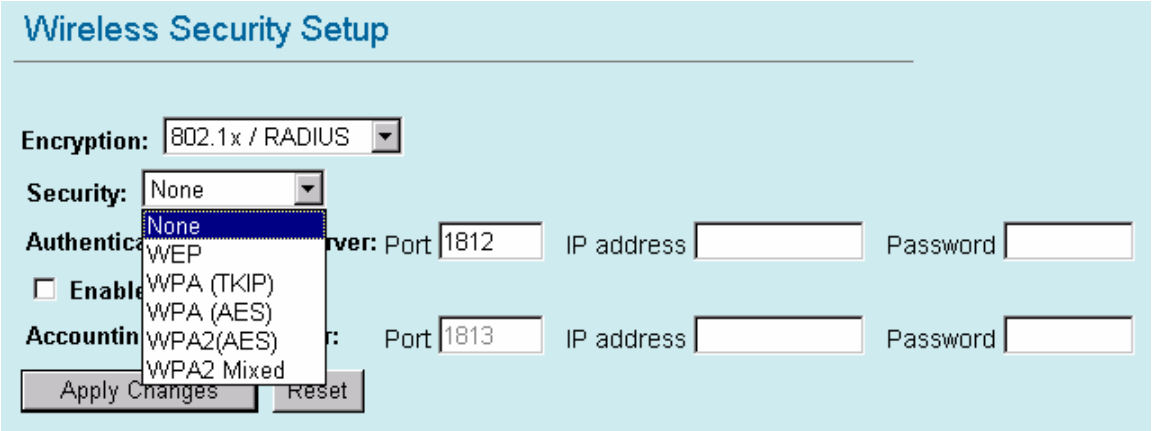




Encryption	You can select WPA2-PSK (AES) or WPA2-PSK Mixed method for data encryption
Pre-shared Key	There are two formats for choice to set the Pre-shared key, i.e. **Passphrase** and **Hex**. If **Hex** is selected, users will have to enter a 64 characters string. For easier configuration, the **Passphrase** (at least 8 characters) format is recommended.
Group Key Life Time	Enter the number of seconds that will elapse before the group key change automatically. The default is 86400 seconds.

802.1x / RADIUS





Encryption: 802.1x / RADIUS

security	You can select None, WEP, WPA (TKIP), WPA (AES), WPA2 (AES), WPA2 Mixed method for data encryption.

Encryption: **None**

No data encryption and Use 802.1x Authentication is disable.

Encryption: **WEP**

802.1x Authentication is enabled and the RADIUS Server will proceed to check the 802.1x Authentication, and make the RADIUS server to issue the WEP key dynamically.

You can select WEP 64bits or WEP 128bits for data encryption.

Encryption: **WPA (TKIP) / WPA (AES)**

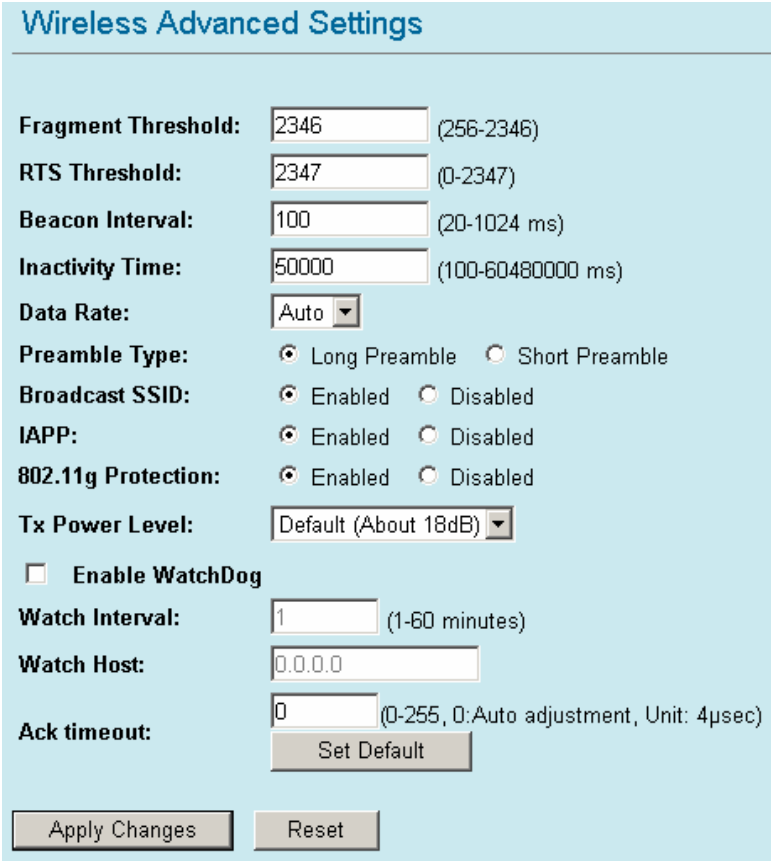
WPA-RADIUS authentication use WPA (Wi-Fi Protect Access) data encryption for 802.1x authentication.

WPA is an encryption standard proposed by WiFi for advance protection by utilizing a password key (TKIP) or certificate. It is more secure than WEP encryption.

Encryption: **WPA2-AES / WPA2-Mixed**

The two most important features beyond WPA to become standardized through 802.11i/WPA2 are: pre-authentication, which enables secure fast roaming without noticeable signal latency. Pre-authentication provides a way to establish a PMK security association before a client associates. The advantage is that the client reduces the time that it's disconnected to the network.

Authentication RADIUS Server	Enter the RADIUS Server IP address and Password provided by your ISP. **Port**: Enter the RADIUS Server's port number provided by your ISP. The default is 1812. **IP Address**: Enter the RADIUS Server's IP Address provided by your ISP. **Password**: Enter the password that the AP shares with the RADIUS Server.
Accounting RADIUS Server	Enter the Accounting RADIUS Server IP address and Password provided by your ISP
Advanced Settings	Press the setup button for detail configurations

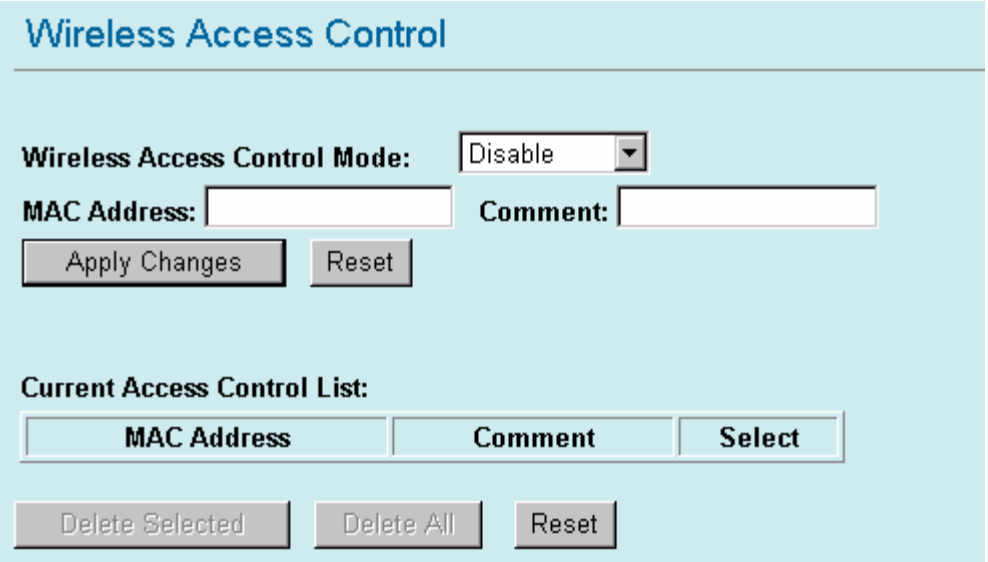


It is not recommended that settings in this page to be changed unless advanced users want to change to meet their wireless environment for optimal performance.

Fragment Threshold	Fragmentation mechanism is used for improving the efficiency when high traffic flows along in the wireless network. If your 802.11g Wireless LAN PC Card often transmit large files in wireless

	network, you can enter new Fragment Threshold value to split the packet. The value can be set from 256 to 2346. The default value is **2346**.
RTS Threshold	RTS Threshold is a mechanism implemented to prevent the "**Hidden Node**" problem. "Hidden Node" is a situation in which two stations are within range of the same Access Point, but are not within range of each other. Therefore, they are hidden nodes for each other. When a station starts data transmission with the Access Point, it might not notice that the other station is already using the wireless medium. When these two stations send data at the same time, they might collide when arriving simultaneously at the Access Point. The collision will most certainly result in a loss of messages for both stations. Thus, the RTS Threshold mechanism provides a solution to prevent data collisions. When you enable RTS Threshold on a suspect "hidden station", this station and its Access Point will use a Request to Send (RTS). The station will send an RTS to the Access Point, informing that it is going to transmit the data. Upon receipt, the Access Point will respond with a CTS message to all station within its range to notify all other stations to defer transmission. It will also confirm the requestor station that the Access Point has reserved it for the time-frame of the requested transmission. If the "Hidden Node" problem is an issue, please specify the packet size. *The RTS mechanism will be activated if the data size exceeds the value you set.*. The default value is **2347**. **Warning:** Enabling RTS Threshold will cause redundant network overhead that could negatively affect the throughput performance instead of providing a remedy. This value should remain at its default setting of **2347**. Should you encounter inconsistent data flow, only minor modifications of this value are recommended.
Beacon Interval	Beacon Interval is the amount of time between beacon transmissions. Before a station enters power save mode, the station needs the beacon interval to know when to wake up to receive the beacon (and learn whether there are buffered frames at the access point).
Data Rate	By default, the unit adaptively selects the highest possible rate for transmission. Select the basic rates to be used among the following options: Auto, 1, 2, 5.5, 11or 54 Mbps. For most networks the default setting is **Auto** which is the best choice. When **Auto** is enabled the transmission rate will

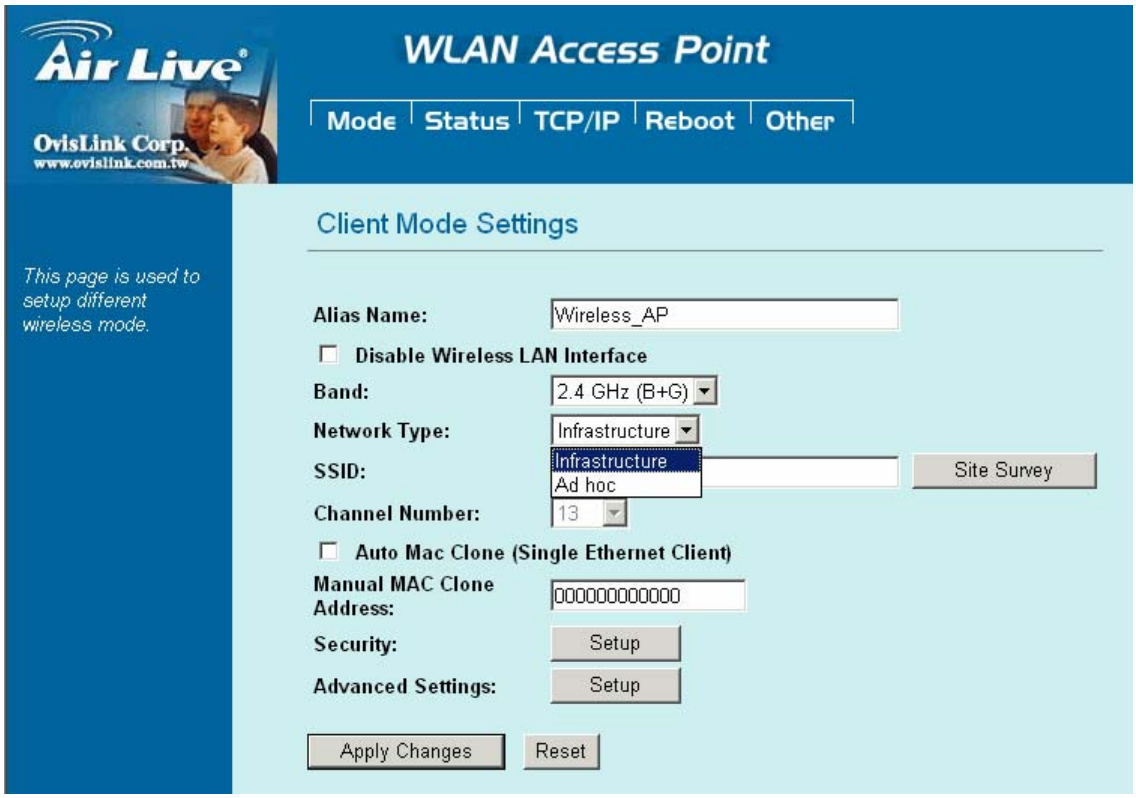
	select the optimal rate. If obstacles or interference are present, the system will automatically fall back to a lower rate.
Preamble Type	A preamble is a signal used in wireless environment to synchronize the transmitting timing including Synchronization and Start frame delimiter. In a "noisy" network environment, the Preamble Type should be set to **Long Preamble**. The **Short Preamble** is intended for applications where minimum overhead and maximum performance is desired. If in a "noisy" network environment, the performance will be decreased.
Broadcast SSID	Select **enabled** to allow all the wireless stations to detect the SSID of this Access Point.
IAPP	IAPP (Inter Access Point Protocol) is designed for the enforcement of unique association throughout a ESS (Extended Service Set) and a secure exchange of station's security context between current access point (AP) and new AP during handoff period.
802.11g Protection	The 802.11g standard includes a protection mechanism to ensure mixed 802.11b and 802.11g operation. If there is no such kind of mechanism exists, the two kinds of standards may mutually interfere and decrease network's performance.
TX Power Level	For countries that impose limit on WLAN output power, it might be necessary to reduce TX (transmit) power. There are 7 TX Power Levels to choose from — select a level to make sure that the output power measured at the antenna end will not exceed the legal limit in your country.
Enable Watch dog	Check and enable this watch dog function
Watch Interval	Setup the interval time for watch dog function between 1 to 60 mins
Watch Host	Enter the watch dog host ip address .
ACK Timeout	When a packet is sent out from one wireless station to the other, it will waits for an Acknowledgement frame from the remote station. If the ACK is NOT received within that timeout period then the packet will be re-transmitted resulting in reduced throughput. If the ACK setting is too high then throughput will be lost due to waiting for the ACK Window to timeout on lost packets. By having the ability to adjust the ACK setting we can effectively optimize the throughput over long distance links. This is especially true for 802.11a and 802.11g networks You can set as default for auto adjustment.
Apply Change	Press to save the new settings on the screen.
Reset	Press to discard the data you have entered since last time you press Apply Change.
Access Control	Press the setup button for detail configurations



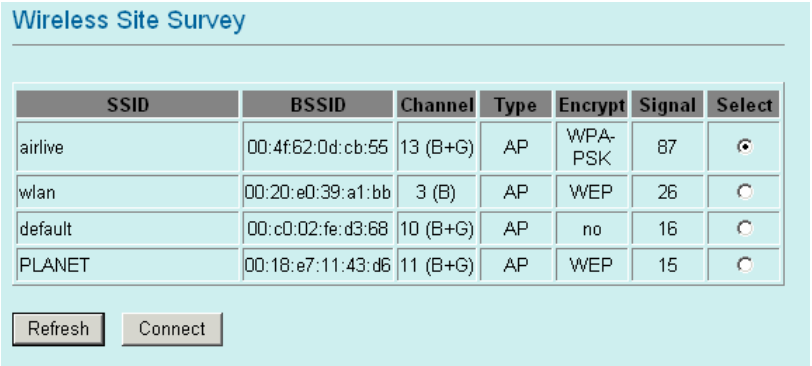
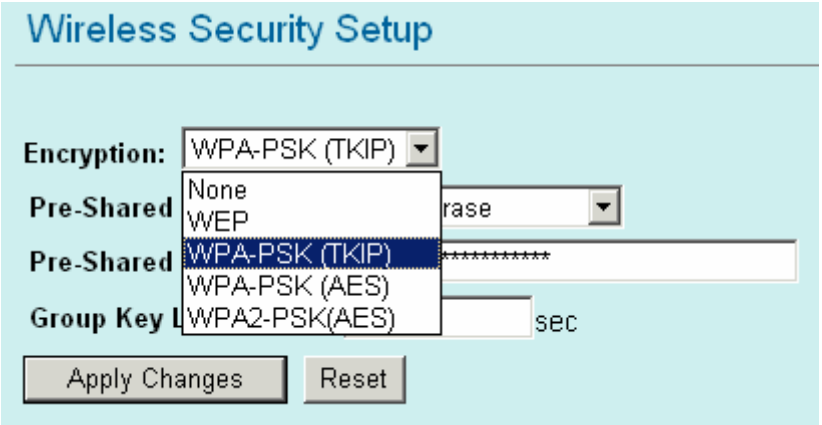
When **Enable Wireless Access Control** is checked, only those clients whose wireless MAC addresses listed in the access control list can access this Access Point. If the list contains no entries with this function being enabled, then no clients will be able to access this Access Point.

Wireless Access Control Mode	Select the Access Control Mode from the pull-down menu. **Disable**: Select to disable Wireless Access Control Mode. **Allow Listed**: Only the stations shown in the table can associate with the AP. **Deny Listed**: Stations shown in the table won't be able to associate with the AP.
MAC Address	Enter the MAC Address of a station that is allowed to access this Access Point.
Comment	You may enter up to 20 characters as a remark to the previous MAC Address.
Apply Changes	Press to save the new settings on the screen.
Reset	Press to discard the data you have entered since last time you press Apply Change.
Delete Selected	To delete clients from access to this Access Point, you may firstly check the **Select** checkbox next to the MAC address and Comments, and press **Delete Selected**.
Delete All	To delete all the clients from access to this Access Point, just press **Delete All** without selecting the checkbox.
Reset	If you have made any selection, press **Reset** will clear all the select mark.

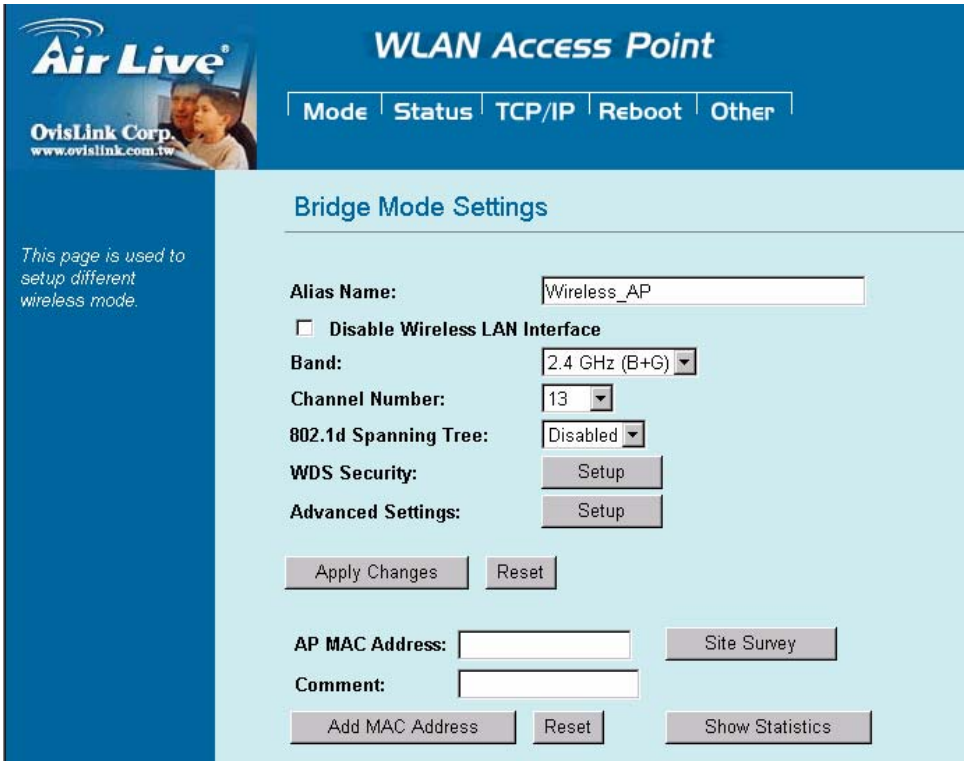
Client Mode Setting



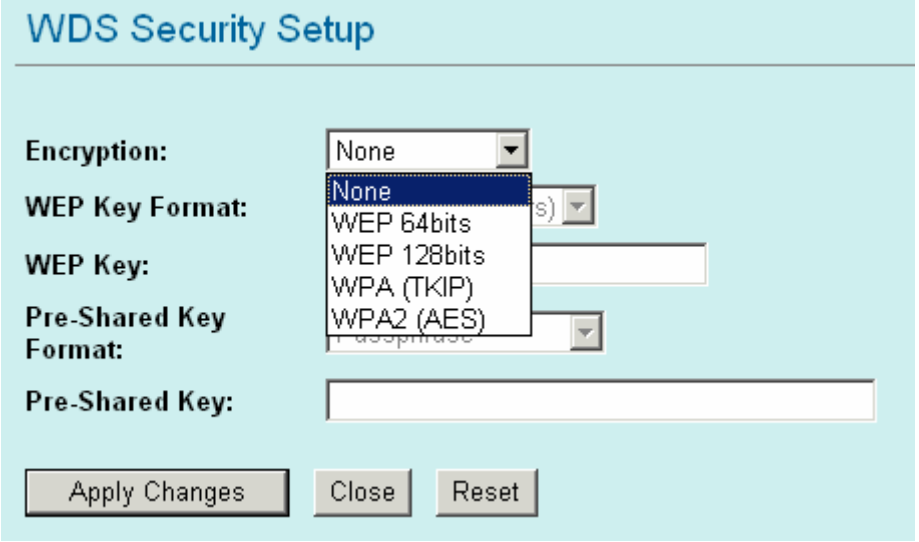
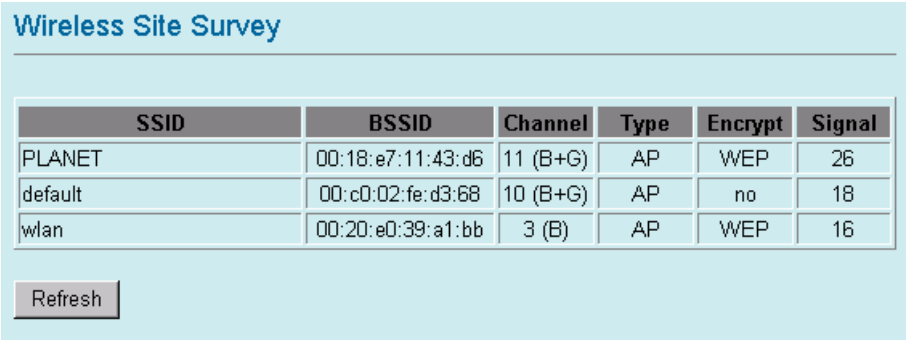
Alias Name	You can set the alias name for this device. limited not exceed 32 characters.
☐ **Disable Wireless LAN Interface**	Check the box to disable the Wireless LAN Interface, by so doing, you won't be able to make wireless connection with this Access Point in the network you are located. In other words, this device will not be visible by any wireless station.
Band	You can choose one mode of the following you need. ⊙ 2.4GHz **(B):** 802.11b supported rate only. ⊙ 2.4GHz **(G):** 802.11g supported rate only. ⊙ 2.4GHz **(B+G):** 802.11b supported rate and 802.11g supported rate. The default is 2.4GHz **(B+G)** mode.
Network Type	Client mode have two Network type : **Infrastructure** A wireless network that is built around one or more access points, providing wireless clients access to wired LAN or Internet service. It is the most popular WLAN network structure today. **AdHoc** wireless network do not use wireless AP orrouter as the central hub of the network. Instead, wireless client are connected directly to each other.
SSID	The SSID differentiates one WLAN from another; therefore, all access points and all devices attempting to connect to a specific WLAN must use the same SSID. It is case-sensitive and must not exceed 32 characters. A device will not be permitted to join the BSS unless it can provide the unique SSID. An SSID is also referred to

	as a network name because essentially it is a name that identifies a wireless network.
Site Survey	 Wireless Site Survey SSID / BSSID / Channel / Type / Encrypt / Signal / Select airlive / 00:4f:62:0d:cb:55 / 13 (B+G) / AP / WPA-PSK / 87 wlan / 00:20:e0:39:a1:bb / 3 (B) / AP / WEP / 26 default / 00:c0:02:fe:d3:68 / 10 (B+G) / AP / no / 16 PLANET / 00:18:e7:11:43:d6 / 11 (B+G) / AP / WEP / 15 Refresh Connect Site survey displays all the active Access Points and IBSS in the neighborhood. You can select one AP to associate. Press Site Survey button to search the wireless device that this client want to connect.
Channel Number	Allow user to set the channel **manually** or **automatically**. If set channel manually, just select the channel you want to specify. If "Auto" is selected, user can set the channel range to have Wireless Access Point automatically survey and choose the channel with best situation for communication. All stations communicating with the Access Point must use the same channel. when setup infrastructure of Client mode, the channel number can not Be changed. You have to go to AP mode to change the channel number
Auto MAC Clone	Check the box to enable MAC Clone for Single Ethernet Client.
Manual MAC Clone Address	Enter the MAC Address of Single Ethernet Client.
Security	Please refer the AP mode settings→ Security for details. In client mode are not supported with RADIUS 802.1x authentication.  Wireless Security Setup Encryption: WPA-PSK (TKIP) None WEP WPA-PSK (TKIP) WPA-PSK (AES) WPA2-PSK(AES) Pre-Shared rase Pre-Shared ********** Group Key L sec Apply Changes Reset
Advance Setting	Please refer the AP mode settings→ Advance Setting for details.

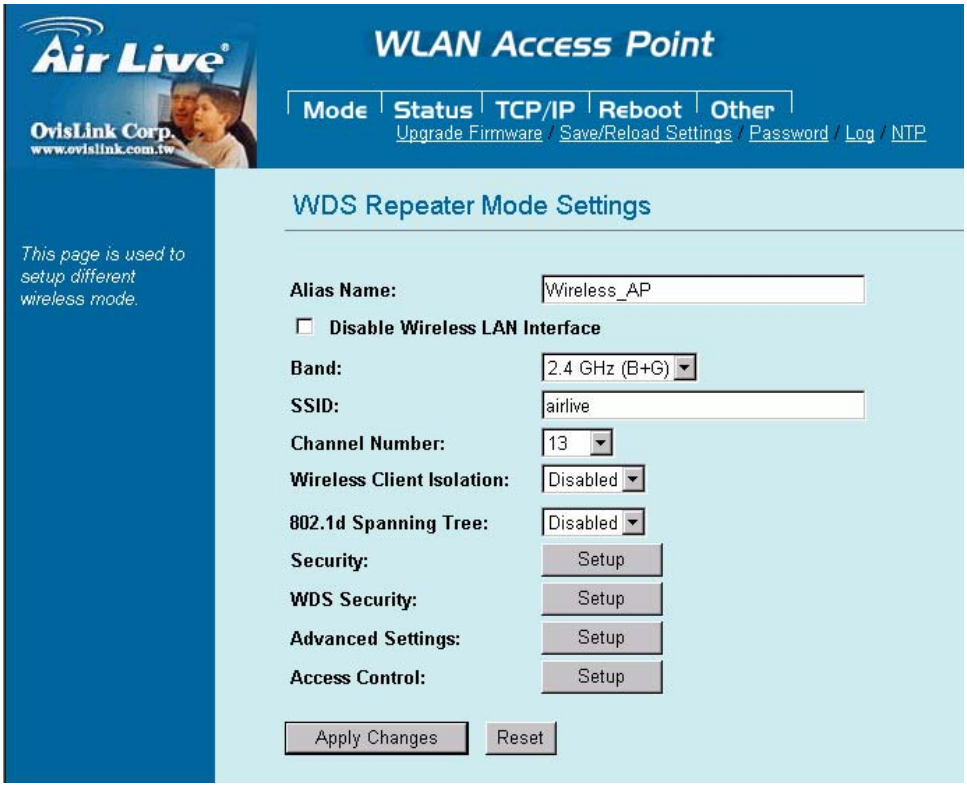
Bridge Mode Setting



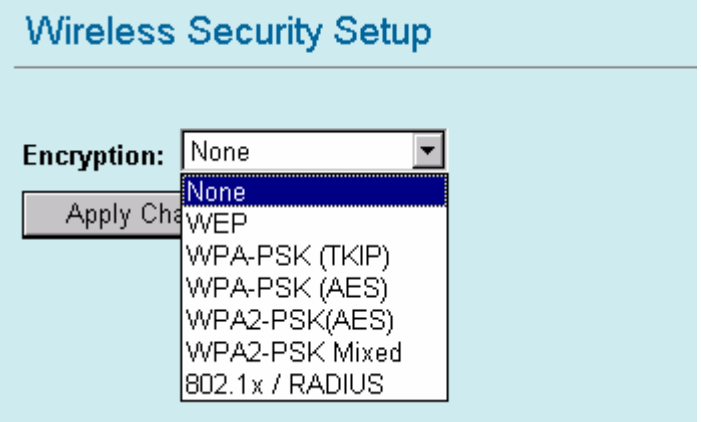
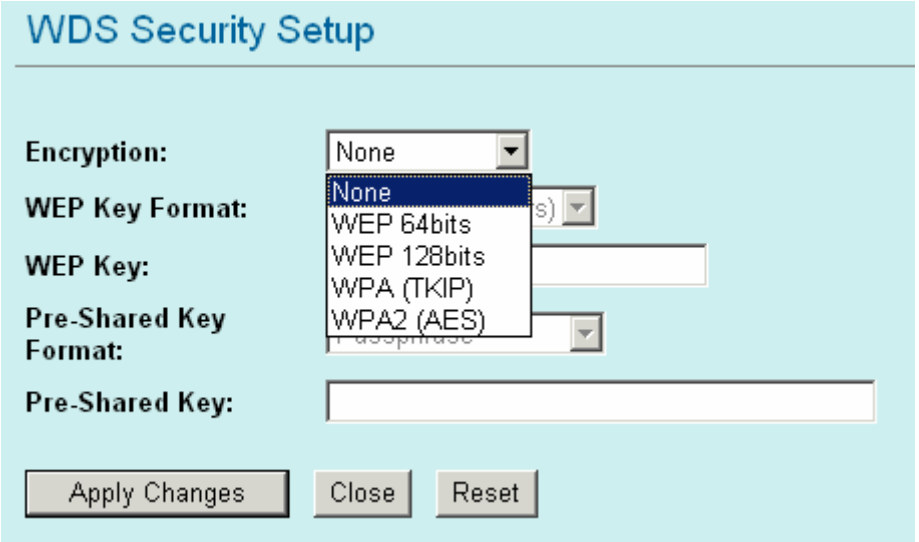
Alias Name	You can set the alias name for this device. limited not exceed 32 characters.
☐ **Disable Wireless LAN Interface**	Check the box to disable the Wireless LAN Interface, by so doing, you won't be able to make wireless connection with this Access Point in the network you are located. In other words, this device will not be visible by any wireless station.
Band	You can choose one mode of the following you need. ⊙ 2.4GHz **(B):** 802.11b supported rate only. ⊙ 2.4GHz **(G):** 802.11g supported rate only. ⊙ 2.4GHz **(B+G):** 802.11b supported rate and 802.11g supported rate. The default is 2.4GHz **(B+G)** mode.
Channel Number	In Bridge mode, both wireless AP/Router device need set to the same Channel number.
Security	Please refer the AP mode settings→ Security for details. But bridge mode are not supported with RADIUS 802.1x authentication.
WDS Security	To enable security between wireless AP/Router , you can select WEP 64bits, WEP 128bits, WPA (TKIP), WPA2(AES) for data encryption. For WEP encryption, Select **ASCII** if you are using ASCII characters. Select **HEX** if you are using hexadecimal numbers (**0-9, or A-F**). For WPA/WPA2 encryption, you need enter the Pre-Shared Key Information for the authentication purpose.

	
Advance Setting	Please refer the AP mode settings→ Advance Setting for details.
AP MAC address	Enter 12 digits in hex numbers in the AP MAC address (**BSSID**) field and press the Add MAC Address Button to associate with other's Wireless access point. Before you want to use bridge mode to connect each other to provide A wireless bridge between 2 remote LANs, you need add the BSSID of other's wireless AP first.
Site Survey	Site survey displays all the active Access Points and IBSS in the neighborhood. Press Site Survey button to search the wireless device. 
Add MAC Address	Enter MAC address of remote access point.
Reset	Press to discard the data you have entered since last time you press Apply Change.
Show Statistics	List all packets information of traffic.
Delete Selected	To delete bridge from access to this Access Point, you may firstly check the **Select** checkbox next to the MAC address and Comments, and press **Delete Selected**.
Delete All	To delete all the clients from access to this Access Point, just press **Delete All** without selecting the checkbox.

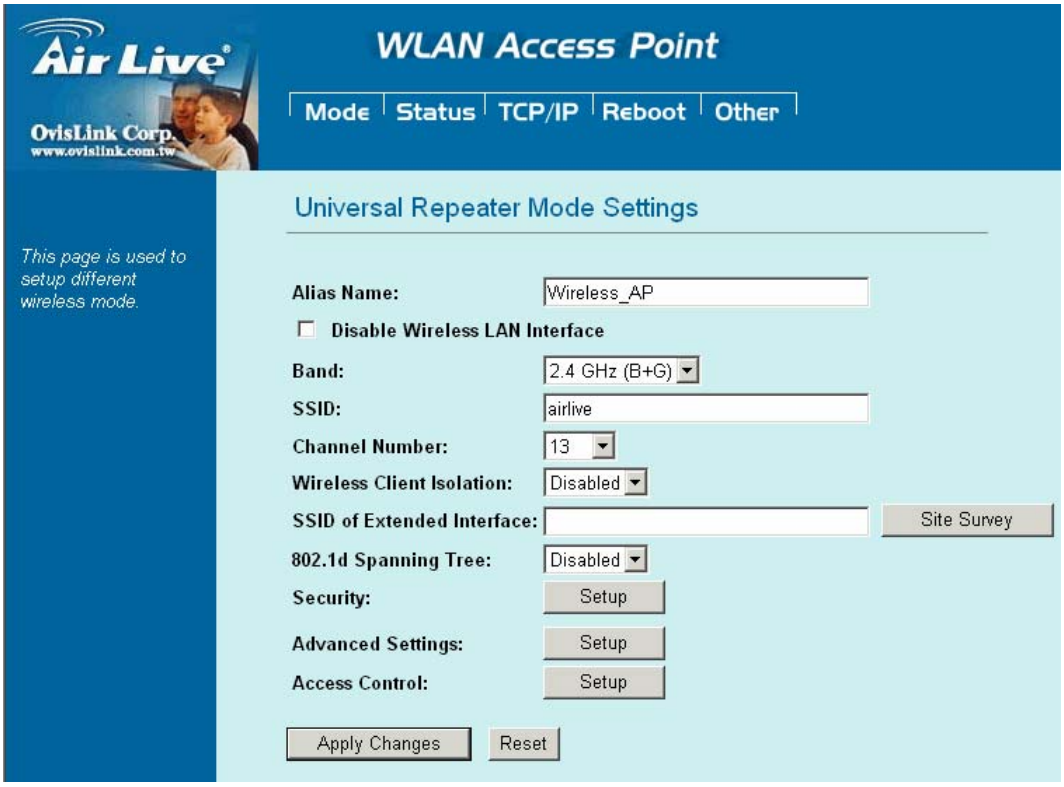
WDS Repeater Mode Setting



Alias Name	You can set the alias name for this device. limited not exceed 32 characters.
☐ **Disable Wireless LAN Interface**	Check the box to disable the Wireless LAN Interface, by so doing, you won't be able to make wireless connection with this Access Point in the network you are located. In other words, this device will not be visible by any wireless station.
Band	You can choose one mode of the following you need. ⊙ 2.4GHz **(B):** 802.11b supported rate only. ⊙ 2.4GHz **(G):** 802.11g supported rate only. ⊙ 2.4GHz **(B+G):** 802.11b supported rate and 802.11g supported rate. The default is 2.4GHz **(B+G)** mode.
SSID	The SSID differentiates one WLAN from another; therefore, all access points and all devices attempting to connect to a specific WLAN must use the same SSID. It is case-sensitive and must not exceed 32 characters. A device will not be permitted to join the BSS unless it can provide the unique SSID. An SSID is also referred to as a network name because essentially it is a name that identifies a wireless network
Channel Number	The number of channels supported depends on the region of this Access Point. All stations communicating with the Access Point must use the same channel.
Wireless Client Isolation	When enabled, the wireless clients are separated from each other. Please refer the AP mode settings→ Wireless Client Isolation for details.

Security	Please refer the AP mode settings→ Security for details, This setting is use between Wireless client and this device. 
WDS Security	Please refer to the Bridge mode settings → WDS Security for details This setting is use between both wireless AP/Router devices. 
Advance Setting	Please refer the AP mode settings→ Advance Setting for details.
Access Control	Please refer the AP mode setting → Access Control for details.
AP MAC Address	Enter 12 digits in hex numbers in the AP MAC address (**BSSID**) field and press the Add MAC Address Button to associate with other's Wireless access point. Before you want to use bridge mode to connect each other to provide A wireless bridge between 2 remote LANs, you need add the BSSID of other's wireless AP first.
Delete Selected	To delete bridge from access to this Access Point, you may firstly check the **Select** checkbox next to the MAC address and Comments, and press **Delete Selected**.
Delete All	To delete all the clients from access to this Access Point, just press **Delete All** without selecting the checkbox.

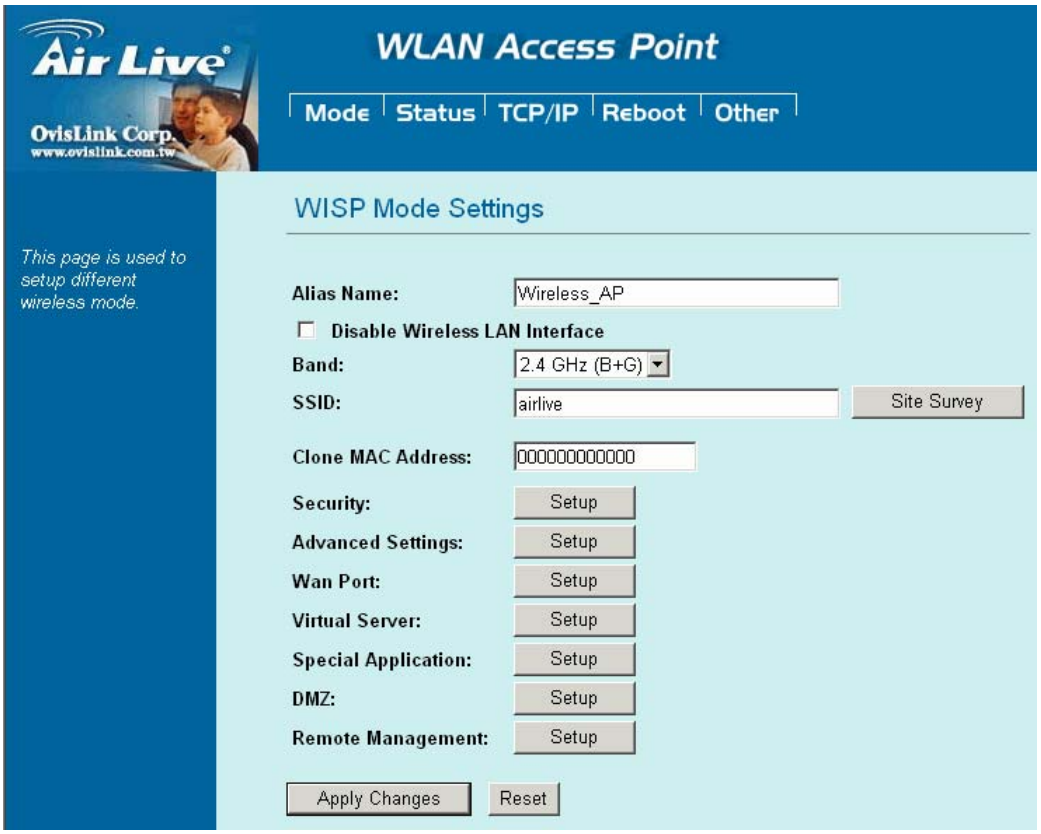
Universal Repeater Mode Setting



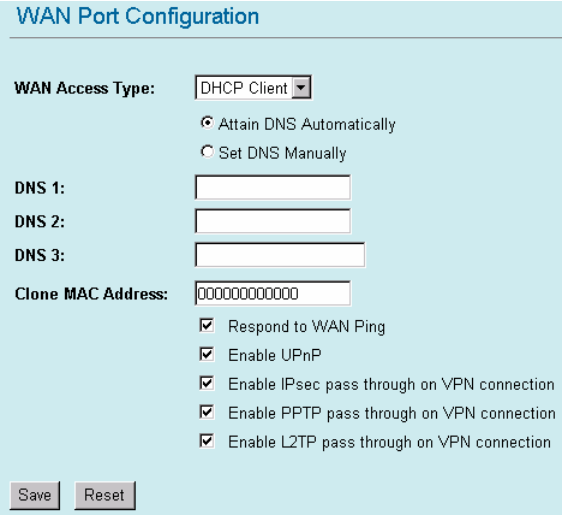
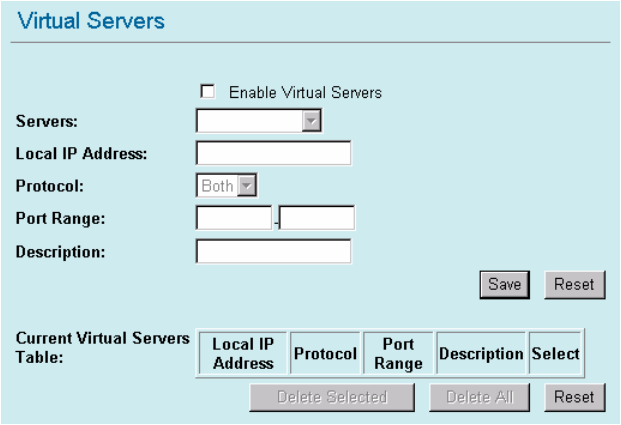
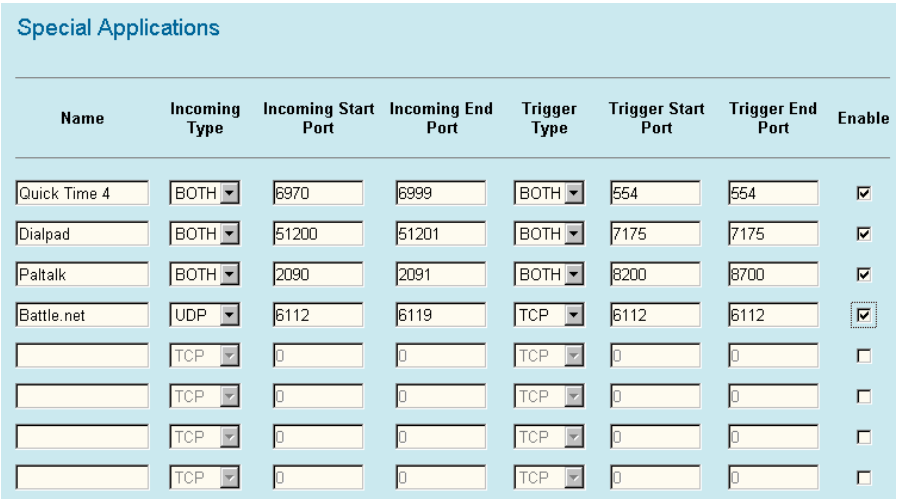
Alias Name	You can set the alias name for this device. limited not exceed 32 characters.
☐ **Disable Wireless LAN Interface**	Check the box to disable the Wireless LAN Interface, by so doing, you won't be able to make wireless connection with this Access Point in the network you are located. In other words, this device will not be visible by any wireless station.
Band	You can choose one mode of the following you need. ⦿ 2.4GHz (B): 802.11b supported rate only. ⦿ 2.4GHz (G): 802.11g supported rate only. ⦿ 2.4GHz (B+G): 802.11b supported rate and 802.11g supported rate. The default is 2.4GHz (B+G) mode.
SSID	The SSID differentiates one WLAN from another; therefore, all access points and all devices attempting to connect to a specific WLAN must use the same SSID. It is case-sensitive and must not exceed 32 characters. A device will not be permitted to join the BSS unless it can provide the unique SSID. An SSID is also referred to as a network name because essentially it is a name that identifies a wireless network
Channel Number	The number of channels supported depends on the region of this Access Point. All stations communicating with the Access Point must use the same channel.
SSID of extended Interface	When in Universal Repeater mode, you have to enter the ESSID of other's AP/Router that device want to connect. The device SSID and the SSID of extended interface can be the same or different.

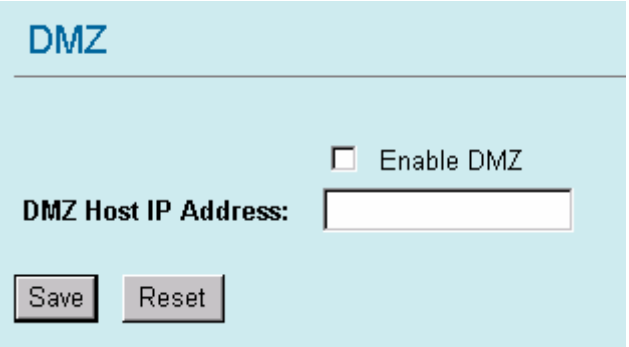
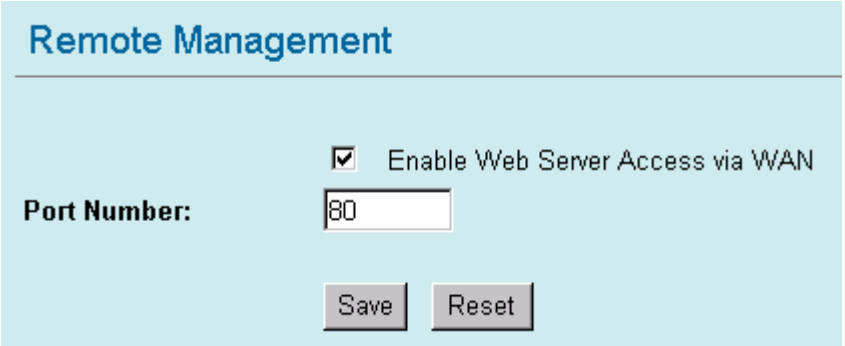
	When you are using the universal repeater mode, please make sure the remote AP/Router WDS function is turned off.
Site Survey	Please refer the Bridge mode settings→ Site Survey for details.
Security	Please refer the AP mode settings→ Security for details, This setting used Wireless client or remote AP to link this device.
Advance Setting	Please refer the AP mode settings→ Advance Setting for details.
Access Control	Please refer the AP mode setting → Access Control for details.

WISP (Client Router) Mode Setting

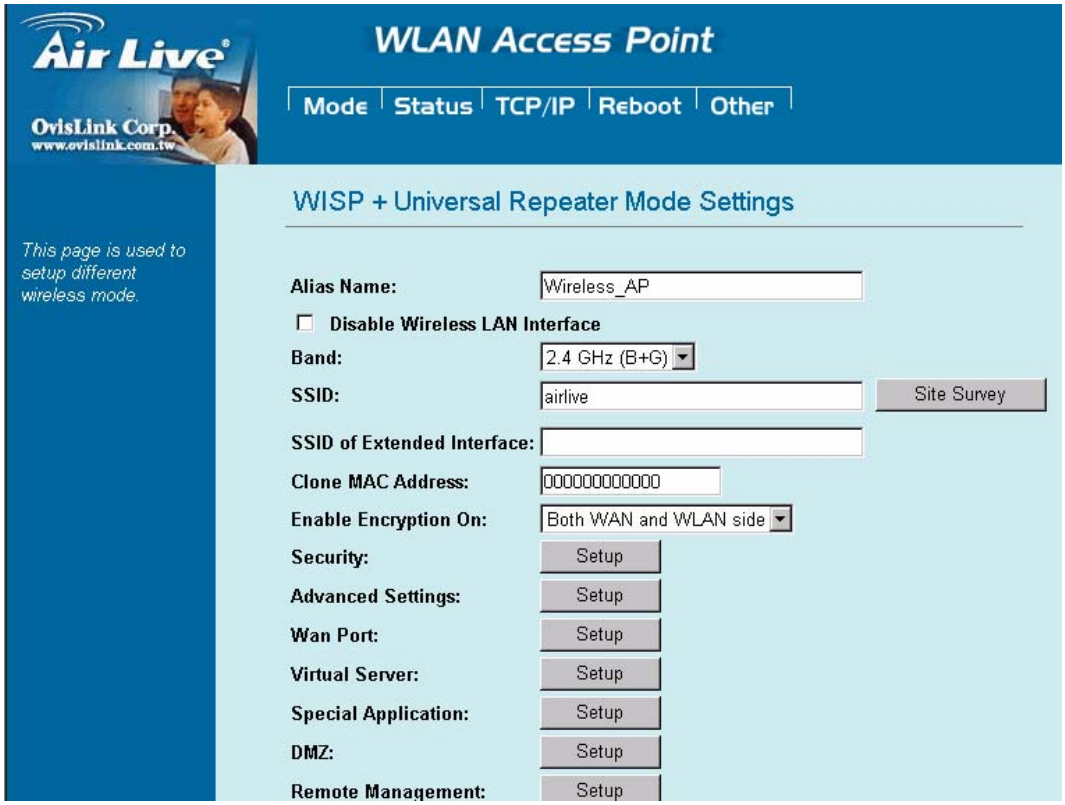


Alias Name	You can set the alias name for this device. limited not exceed 32 characters
☐ **Disable Wireless LAN Interface**	Check the box to disable the Wireless LAN Interface, by so doing, you won't be able to make wireless connection with this Access Point in the network you are located. In other words, this device will not be visible by any wireless station.
Band	You can choose one mode of the following you need. ⊙ 2.4GHz **(B):** 802.11b supported rate only. ⊙ 2.4GHz **(G):** 802.11g supported rate only. ⊙ 2.4GHz **(B+G):** 802.11b supported rate and 802.11g supported rate. The default is 2.4GHz **(B+G)** mode.
SSID	The SSID differentiates one WLAN from another; therefore, all access points and all devices attempting to connect to a specific WLAN must use the same SSID. In WISP mode, you have to enter the WISP Outdoor AP SSID manually or click the "site survey" button to connect and get SSID automatically.
Site Survey	Please refer the Client mode settings→ Site Survey for details.
MAC Clone Address	Enter the MAC Address of Single Ethernet Client.
Security	Please refer the AP mode settings→ Security Survey for details. Not supported with RADIUS 802.1x authentication.

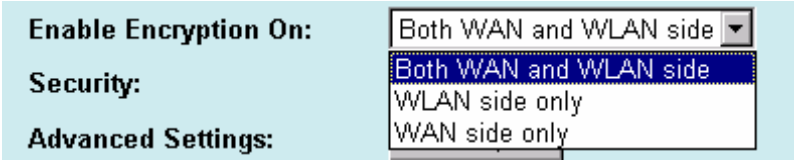
Advance Setting	Please refer the AP mode settings→ Advance Setting for details.
WAN port	 You can select many WAN Access Type : Static IP , DHCP Client, PPPOE, PPTP, and L2TP for WAN connection depend on you WISP provided.
Virtual Server	 In WISP mode, you can setup and enable Virtual server function. Like Web, FTP, Email, DNS, Telnet server. Select one virtual server type and enter the Local IP address, Local Port Range and click the save button.
Special Application	 You can enable some system default special application, like Qucktime 4

	Audio/Video application, Dialpad internet phone service. or define the special application manually, select the incoming type (TCP/UDP) Incoming start ~ End port ,Trigger Start ~ End port. Select the Trigger Type.
DMZ	 Enable DMZ and enter the DMZ Host IP address.
Remote Management	 Enable the function that setting configuration from Internet.

WISP + Universal Repeater Mode Setting

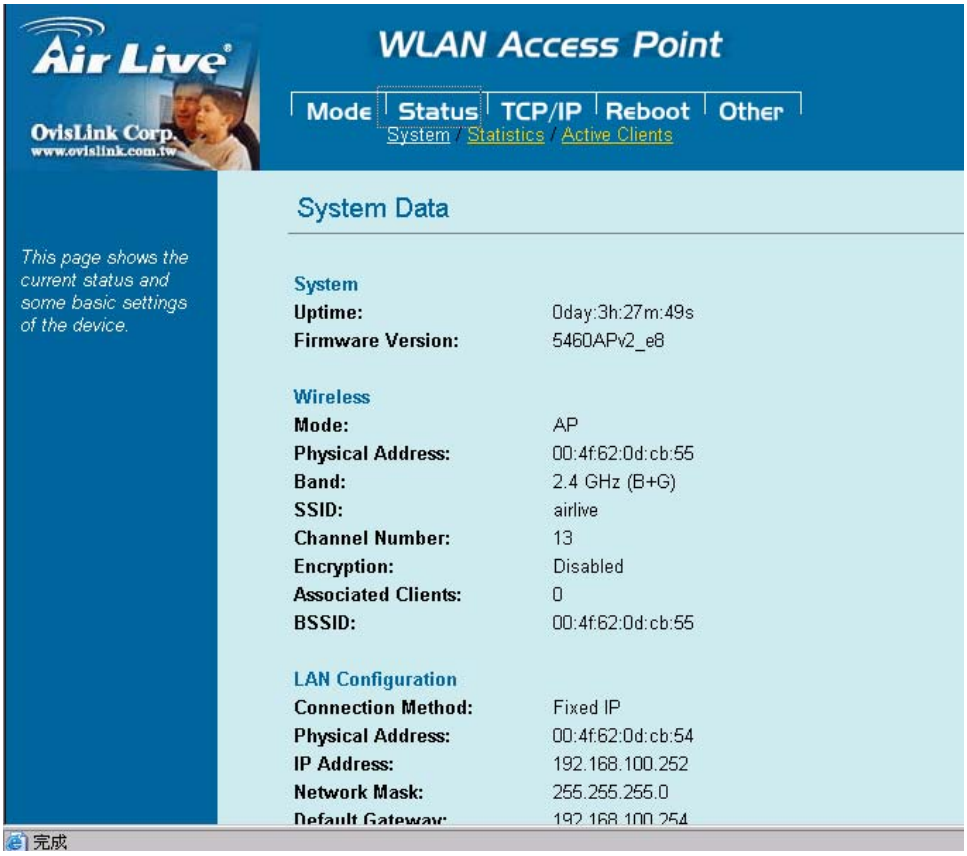


Alias Name	You can set the alias name for this device. limited not exceed 32 characters
☐ **Disable Wireless LAN Interface**	Check the box to disable the Wireless LAN Interface, by so doing, you won't be able to make wireless connection with this Access Point in the network you are located. In other words, this device will not be visible by any wireless station.
Band	You can choose one mode of the following you need. ⊙ 2.4GHz **(B):** 802.11b supported rate only. ⊙ 2.4GHz **(G):** 802.11g supported rate only. ⊙ 2.4GHz **(B+G):** 802.11b supported rate and 802.11g supported rate. The default is 2.4GHz **(B+G)** mode.
SSID	The SSID differentiates one WLAN from another; therefore, all access points and all devices attempting to connect to a specific WLAN must use the same SSID. In WISP mode, you have to enter the WISP Outdoor AP SSID manually or click the "site survey" button to connect and get SSID automatically.
Site Survey	Please refer the Client mode settings→ Site Survey for details.
SSID of extended Interface	Please refer the Universal repeater mode settings→ SSID of extended Interface for details.
MAC Clone Address	Enter the MAC Address of Single Ethernet Client.

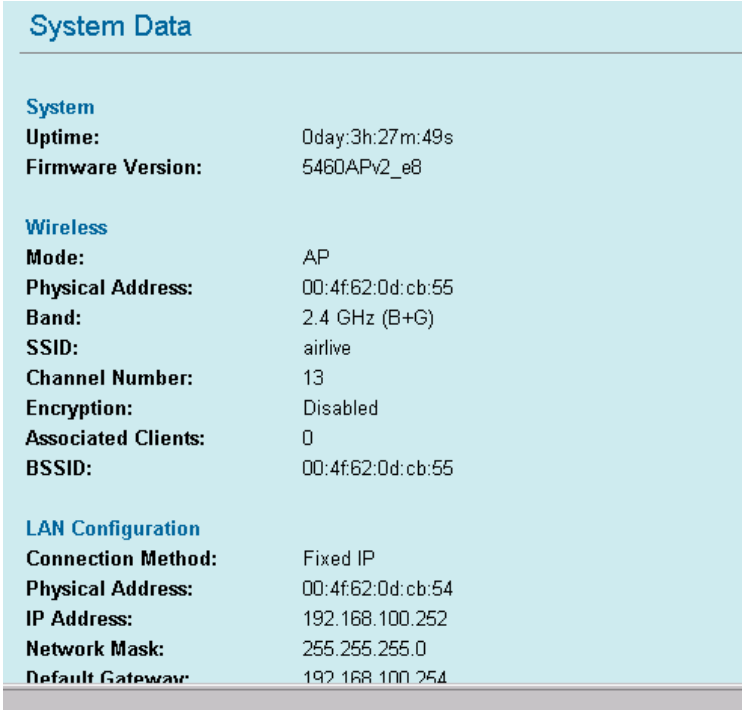
Enable Encryption On	 You can designate security to use for WLAN side, WAN side or both sides. **Both WAN and WLAN side:** The security is used on both the WISP and the Wireless Client(PC side) connection.. **WLAN side only:** The security used on wireless client connection only. The WISP side is not encrypted. **WAN side only:** The security used on WISP connection only. The WLAN side is not encrypted..
Security	Please refer the AP mode settings→ Security Survey for details. Not supported with RADIUS 802.1x authentication.
Advance Setting	Please refer the AP mode settings→ Advance Setting for details.
WAN port	Please refer the WISP mode settings→ WAN port Setting for details.
Virtual Server	Please refer the WISP mode settings→ Virtual Server Setting for details.
Special Application	Please refer the WISP mode settings→ Special Application Setting for details.
DMZ	Please refer the WISP mode settings→ DMZ Setting for details.
Remote Management	Please refer the WISP mode settings→ Remote Management Setting for details.

Status

In this screen, you can see the current settings and status of this Access Point. You can change settings by selecting specific tab described in below.



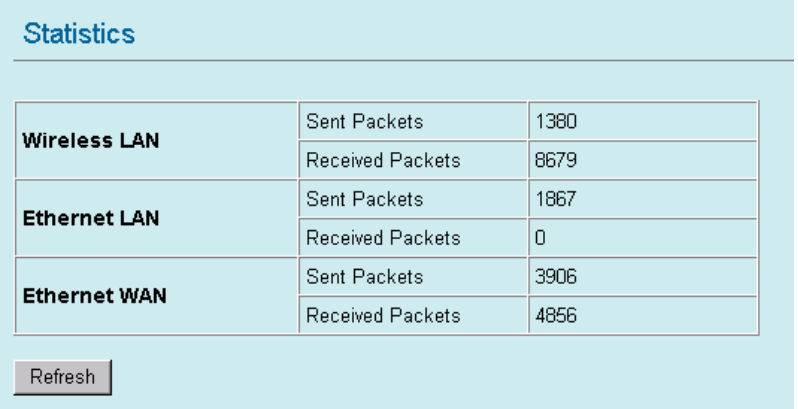
- **System**



System

Uptime	The time period since the device was up.
Firmware Version	The current version of the firmware installed in this device.
Wireless	
Mode	There are 7 modes supported, The default mode is Access Point. If you want to change to other mode, please click the Mode and select the wireless mode you want.
Physical Address	Display wireless MAC address information.
Band	Display wireless band type information.
SSID	Display the SSID of this device.
Channel Number	The number of channels supported depends on the region of this Access Point. All stations communicating with the Access Point must use the same channel.
Encryption	Display encryption setting information.
Associated Clients	Displays the total number of clients associated to this AP. You can have up to 64 clients to associate to this Access Point.
BSSID	BSSID displays the ID of current BSS, which uniquely identifies each BSS. In AP mode, this value is the MAC address of this Access Point.
LAN Configuration (TCP/IP)	
Connection Method:	Display the connection method, you can setup in TCP/IP section
Physical Address:	Display the LAN MAC address
IP Address:	Display the LAN IP address, you can setup in TCP/IP section
Network Mask:	Display the network mask, you can setup in TCP/IP section
Default Gateway:	Display the default gateway ip , you can setup in TCP/IP section
DHCP Server:	Default the DHCP Server is enabled(ON)
DHCP Start IP Address:	Display the DHCP server start IP address.
DHCP Finish IP Address:	Display the DHCP server finish IP address.
Internet Configuration	
Connection Method:	Display the internet connection method, you can setup in WISP mode→WAN Port configuration
Physical Address:	Display the AP MAC address information
IP Address:	Display the internet IP Address, you can setup in WISP mode→WAN Port configuration
Network Mask:	Display the network mask, you can setup in WISP mode→WAN Port configuration
Default Gateway:	Display the default gateway , you can setup in WISP mode→WAN Port configuration

- **Statistics**



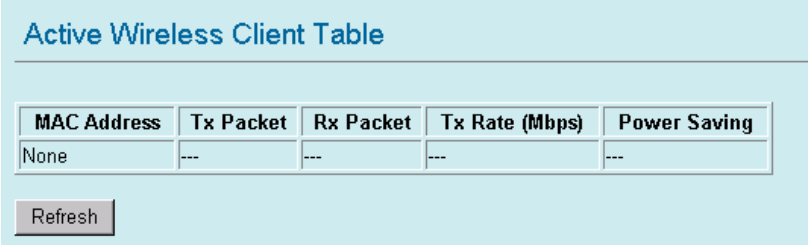
Statistics

Wireless LAN	Sent Packets	1380
	Received Packets	8679
Ethernet LAN	Sent Packets	1867
	Received Packets	0
Ethernet WAN	Sent Packets	3906
	Received Packets	4856

Refresh

The Statistics table shows the packets sent/received over wireless and ethernet LAN respectively.

- **Active Clients**



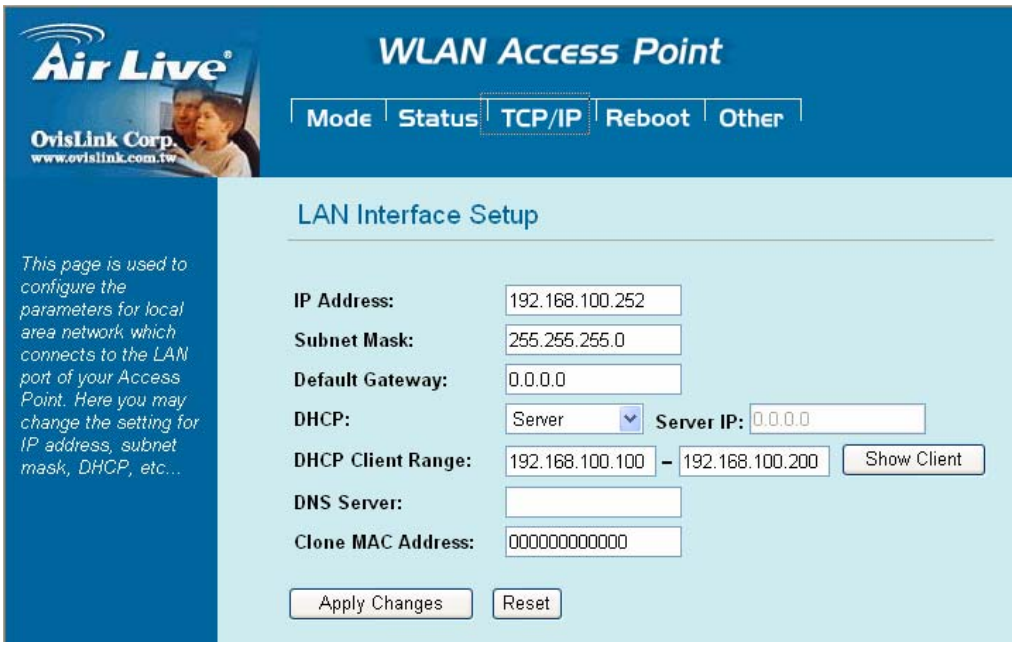
Active Wireless Client Table

MAC Address	Tx Packet	Rx Packet	Tx Rate (Mbps)	Power Saving
None	---	---	---	---

Refresh

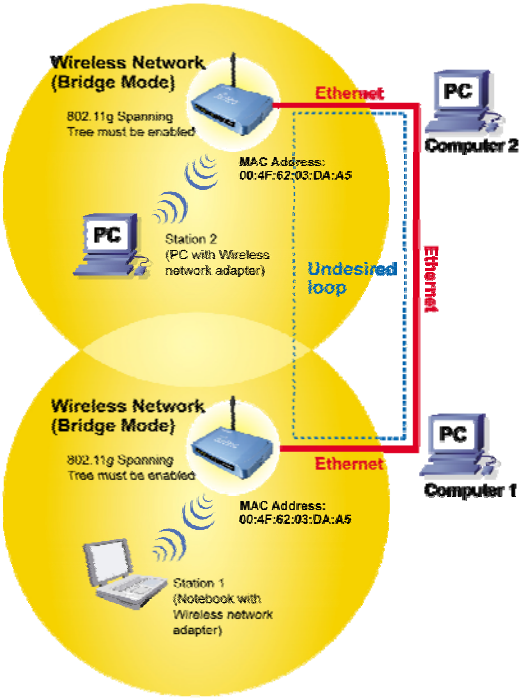
Display the active Wireless Clients information, include wireless MAC address, TX/Rx Packet, TX Rate, and Power Saving information.

TCP/IP



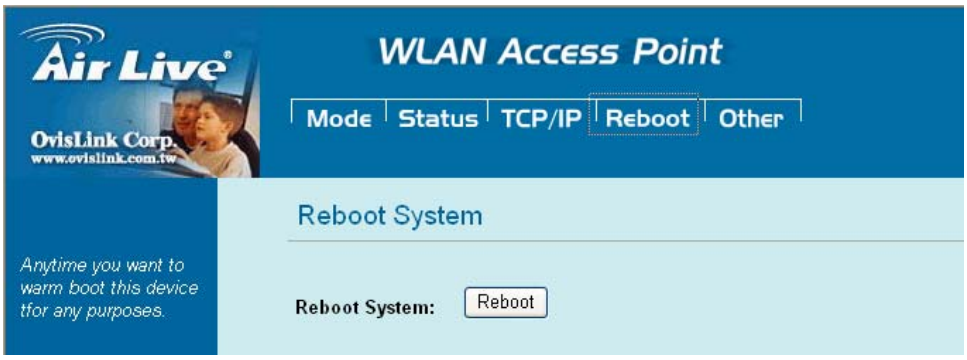
In this page, you can change the TCP/IP settings of this Access Point, select to enable/disable the DHCP Client, 802.1d Spanning Tree, and Clone MAC Address.

IP Address	This field can be modified only when DHCP Client is disabled. If your system manager assigned you static IP settings, then you will have to enter the information provided.
Subnet Mask	Enter the information provided by your system manager.
Default Gateway	Enter the information provided by your system manager.
DHCP	Select Disable, Client or Server from the pull-down menu. Disable: Select to disable DHCP server function. Client: Select to automatically get the LAN port IP address from ISP (For ADSL/Cable Modem). Server: Select to enable DHCP server function.
DHCP Client Range	WL-5060AP IP addresses continuing from 192.168.100.1 to 192.168.100.253
Show Client	Click to show Active DHCP Client table.
DNS Server	Enter the Domain Name Service IP address.
802.1d Spanning Tree	To enable 802.1d Spanning Tree will prevent the network from infinite loops. Infinite loop will happen in the network when WDS is enabled and there are multiple active paths between stations.

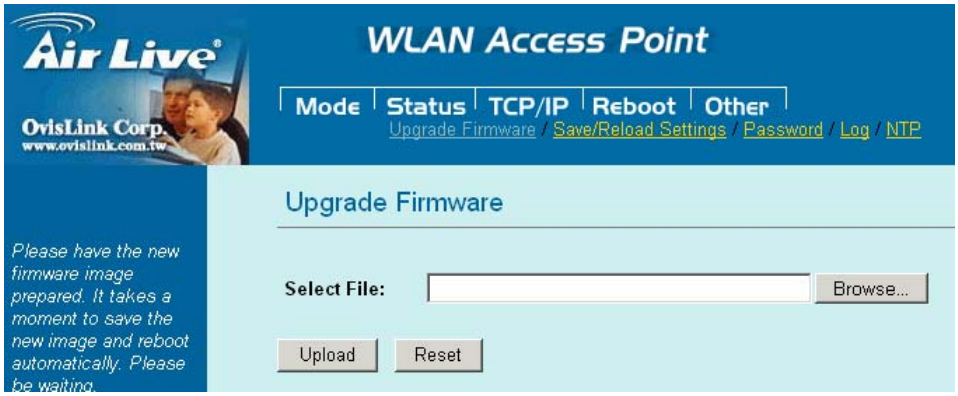
	
Clone MAC Address	You can specify the MAC address of your Access Point to replace the factory setting.

Reboot

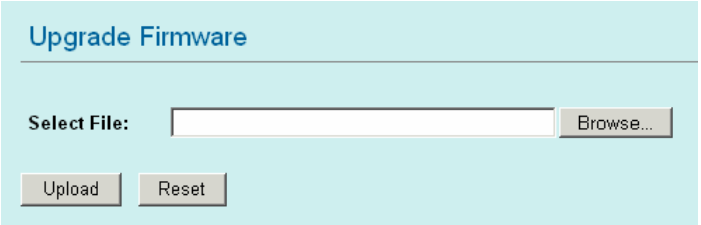
Click the **Reboot** button to restart device.



Other



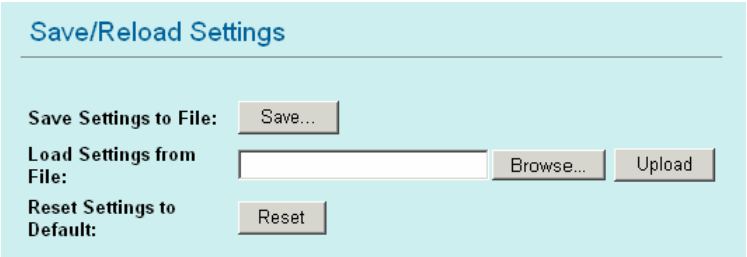
- **Upgrade Firmware**



1. Download the latest firmware from your distributor and save the file on the hard drive.
2. Start the browser, open the configuration page, click on **Other**, and click **Upgrade Firmware** to enter the **Upgrade Firmware** window.
3. Enter the new firmware's path and file name (i.e. C:\FIRMWARE\firmware.bin) or click the **Browse** button to find and open the firmware file (the browser will display to correct file path).
4. Click **Upload** button to start the upgrade function or **Reset** button to clear all the settings on this page.

   If firmware upgrade fail, please see Appendix A.

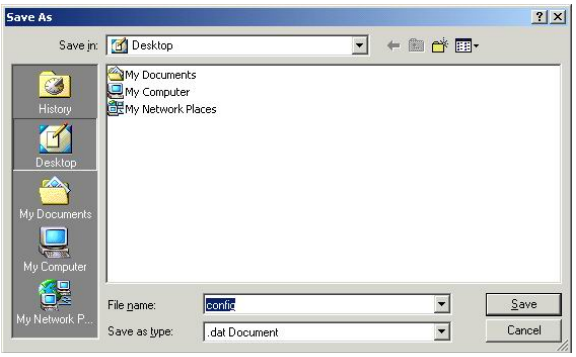
- **Save / Reload Settings**

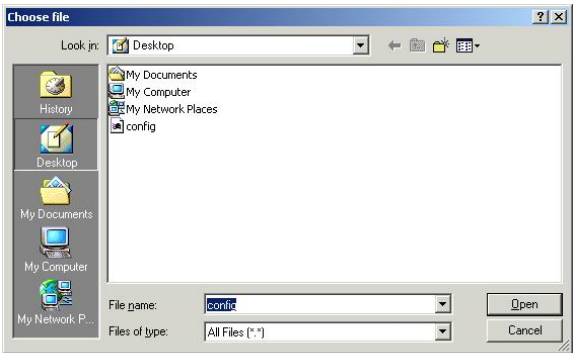


This function enables users to save the current configuration as a file (i.e. **config.dat**) or loades configuration from a file. Enter the file name or click **Browse…** to find the file from your computer.

Save Settings to File: Click **SAVE..** to save the current configuration to file.

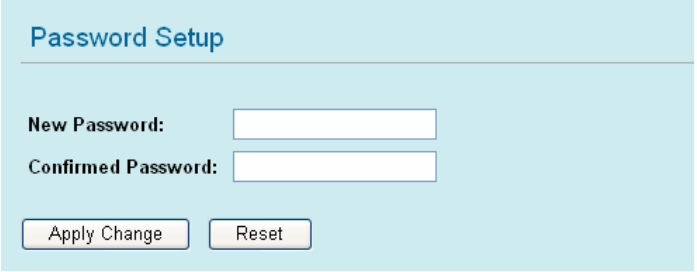
Load Settings From File: Click **Browse…** if you want to load a pre-saved file, enter the file name with the correct path and then click on **Upload** or click **Browse…** to select the file.





Reset Settings to Default: Click **Reset** button to restore the default configuration.

- ## Password

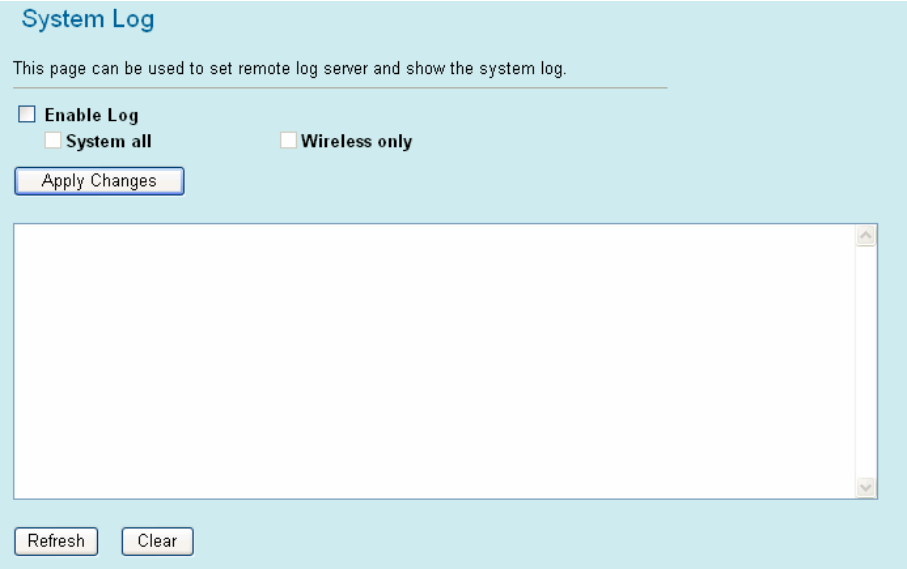


For secure reason, It is recommended that you set the account to access the web server of this Access Point. Leaving the password blank will disable the protection. The login screen prompts immediately once you finish setting password. Remember your password for you will be asked to enter them every time you access the web server of this Access Point.

New Password	Set your new password. Password can be up to 30 characters long. Password can contain letter, number and space. It is case sensitive.
Confirm Password	Re-enter the new password for confirmation.

Note: when you setup the password and click the apply change button, system will pop-up Window and ask the username and password, Please enter system default username "**admin**" (**not changeable**) and your password for entering the configuration WEB UI.

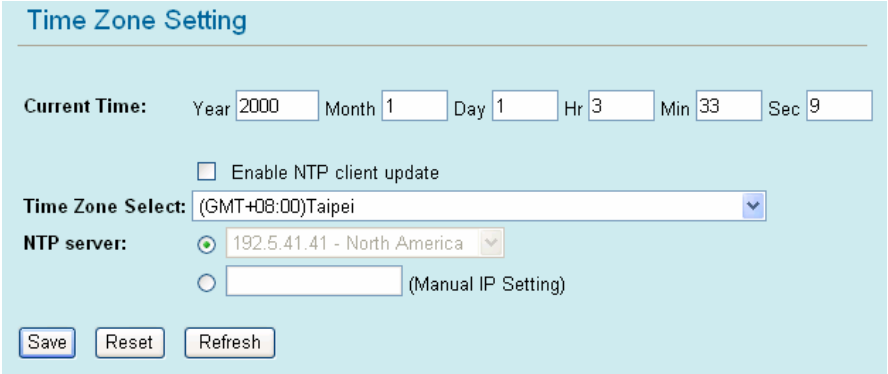
- ## Log



This function can list all log information about device.

Enable Log	Enabled or Disabled display system log information.
System All	List system all log information.
Wireless Only	List wireless log information only.
Refresh	Refresh log information.
Clear	Clear all information in window.

- **NTP**



This function can setting system time from local computer or Internet.

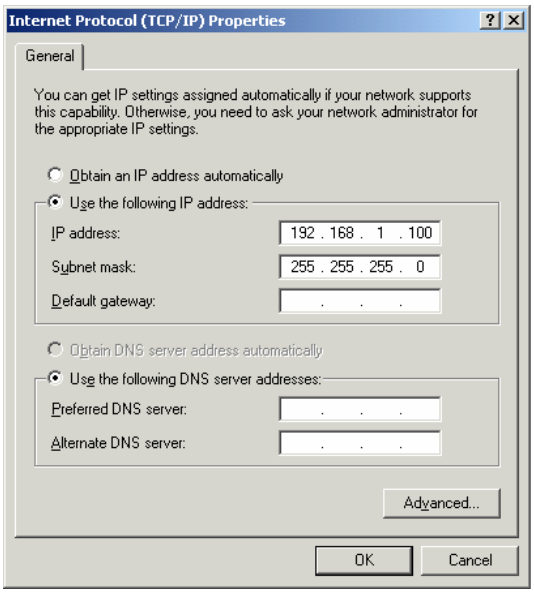
Current Time	Setting system time
Enable NTP client update	Enable or Disable setting system from Internet NTP Server.
Time Zone Select	Select system time zone.
NTP Server	Select NTP Server by Server list or manual inputing.
Save	Save configurayion to flsh.
Reset	Reset system time configurayion.
Refresh	Refresh system time information.

Appendix A

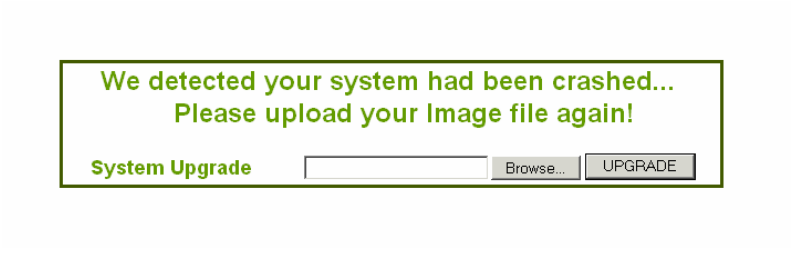
- **Emergency Code**

Should firmware upgrade fail, WL-5460AP will enter Emergency Mode. Please do the following instructions for firmware recovery:

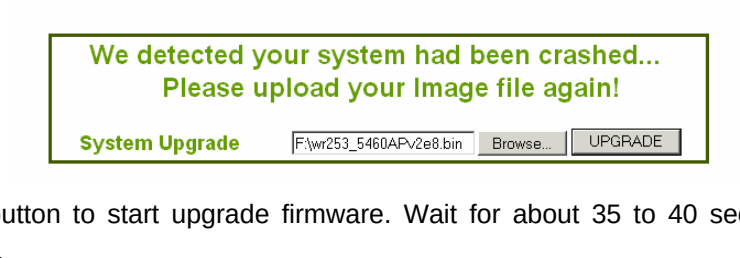
1. Open the internet protocol dialogue and set IP address at http://192.168.1.X/.



2. Open WEB broswer and enter the IP address http://192.168.1.6/ to enter Emergency Mode setup page.

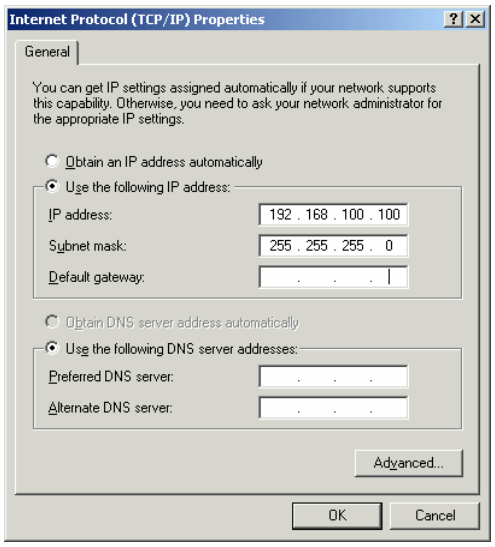


3. Click the Browser button to find and open the firmware file.



4. Click UPGRADE button to start upgrade firmware. Wait for about 35 to 40 seconds for the firmware upgrade to complete.

5. Reopen the internet protocol dialogue. Set IP address at http://192.168.100.X/.



6. Open WEB browser. Enter the IP address http://192.168.100.252/ to login to the configuration menu.