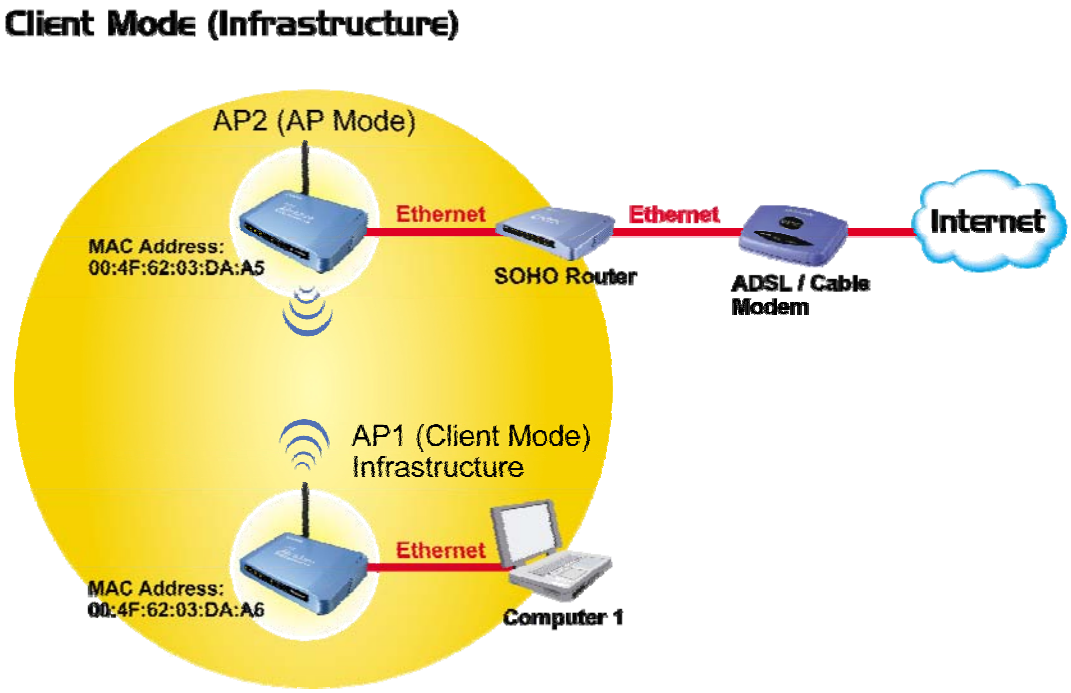
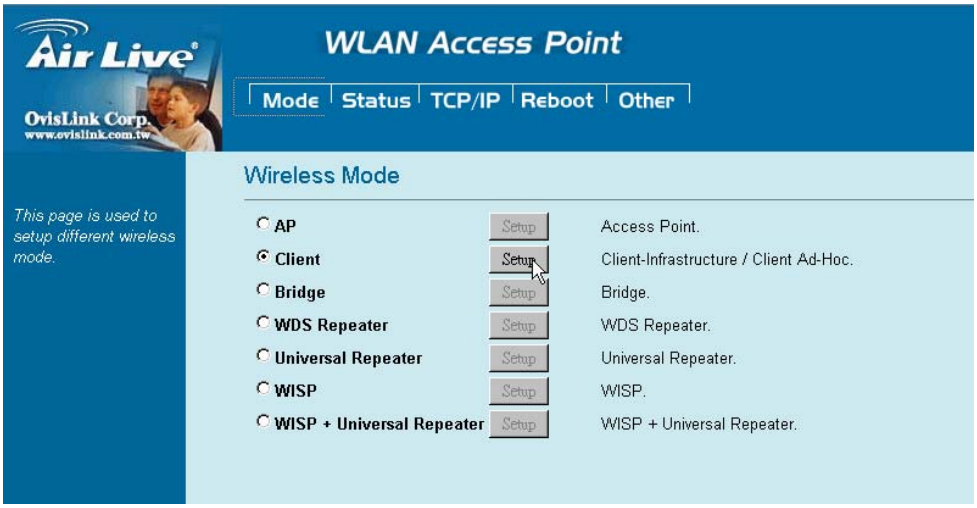
Client Mode (Infrastructure)

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.

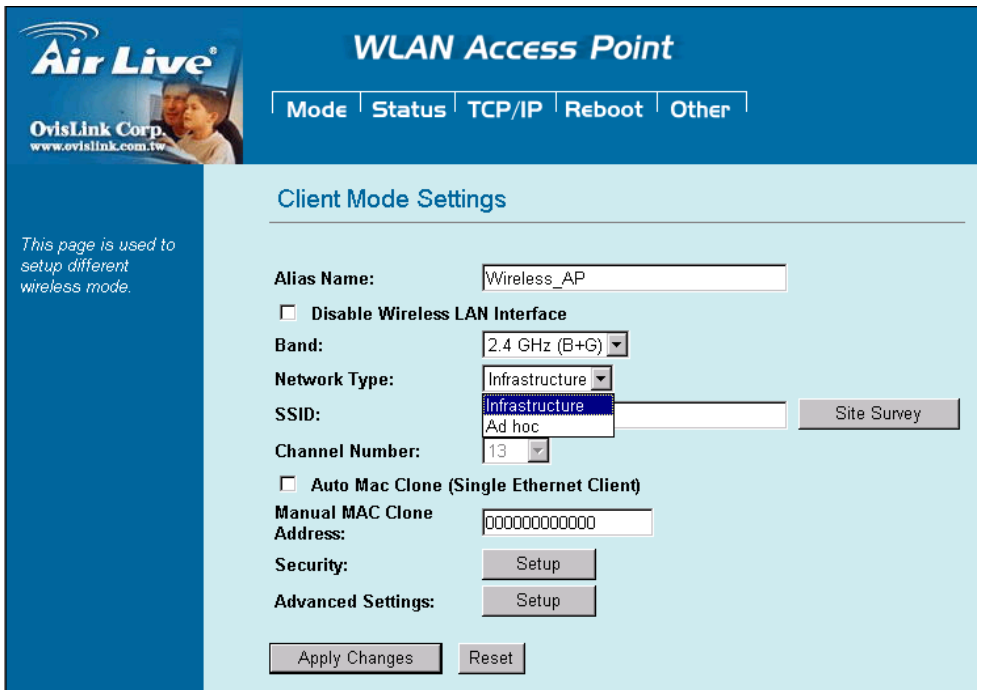
Refer to the illustration below. This station (AP1 plus the connected computer 1) can associate to another Access Point (AP2), and then can have the Internet access if the other Access Point (AP2) has the Internet connection.



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



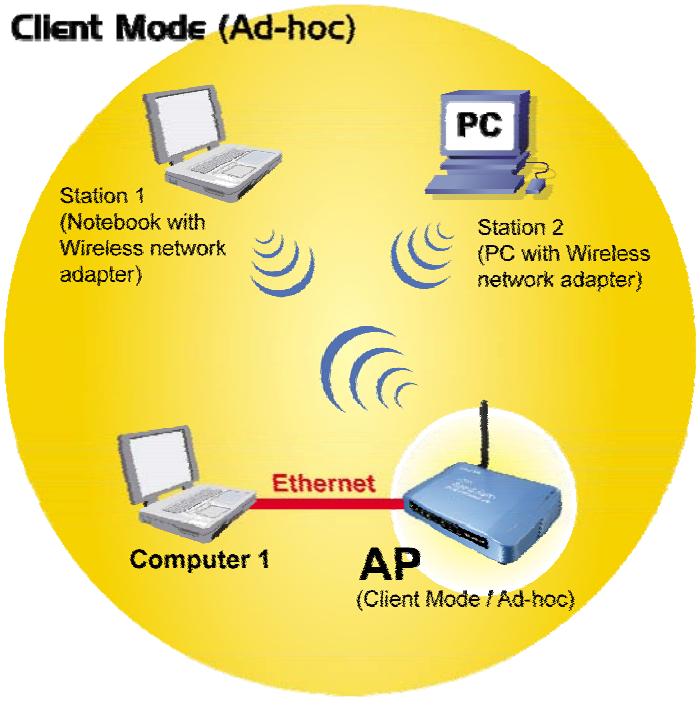
In the **"Network Type"** field, select as **"infrastructure"** for configuration.


Air Live
OvisLink Corp.
www.ovislink.com.tw
WLAN Access Point
Mode
Status
TCP/IP
Reboot
Other
This page is used to setup different wireless mode.
Client Mode Settings
Alias Name:
Wireless_AP
Disable Wireless LAN Interface
Band:
2.4 GHz (B+G)
Network Type:
Infrastructure
Infrastructure
Ad hoc
SSID:
Site Survey
Channel Number:
13
Auto Mac Clone (Single Ethernet Client)
Manual MAC Clone Address:
000000000000
Security:
Setup
Advanced Settings:
Setup
Apply Changes
Reset

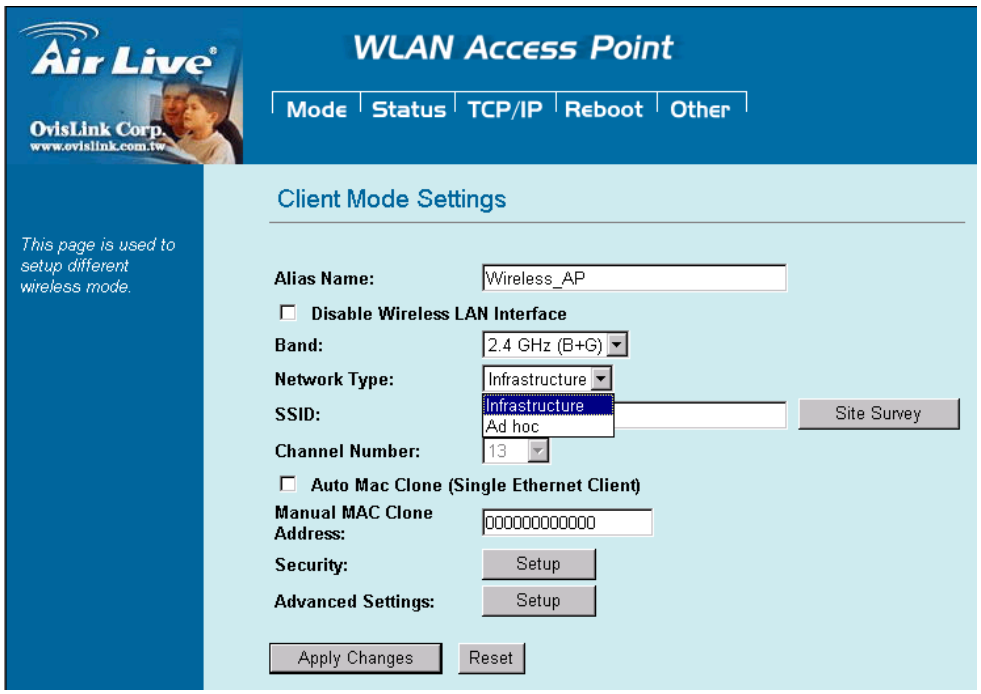
Client Mode (Ad-hoc)

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 **"Ad hoc"** for configuration.

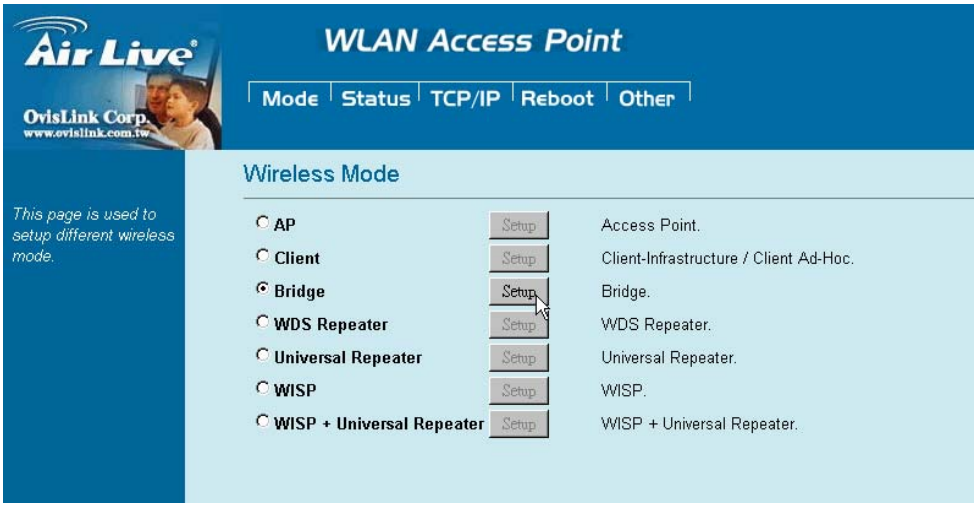


Bridge Mode

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.

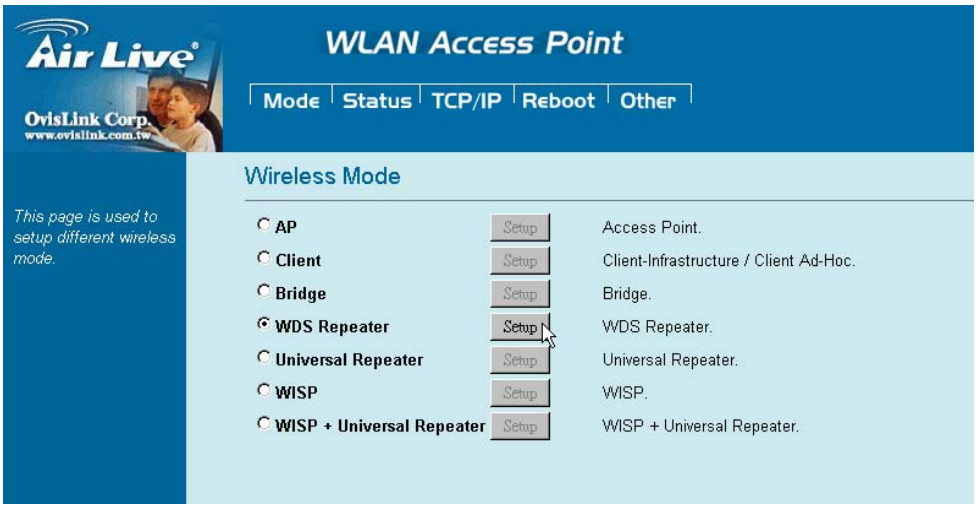


WDS Repeater Mode

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.

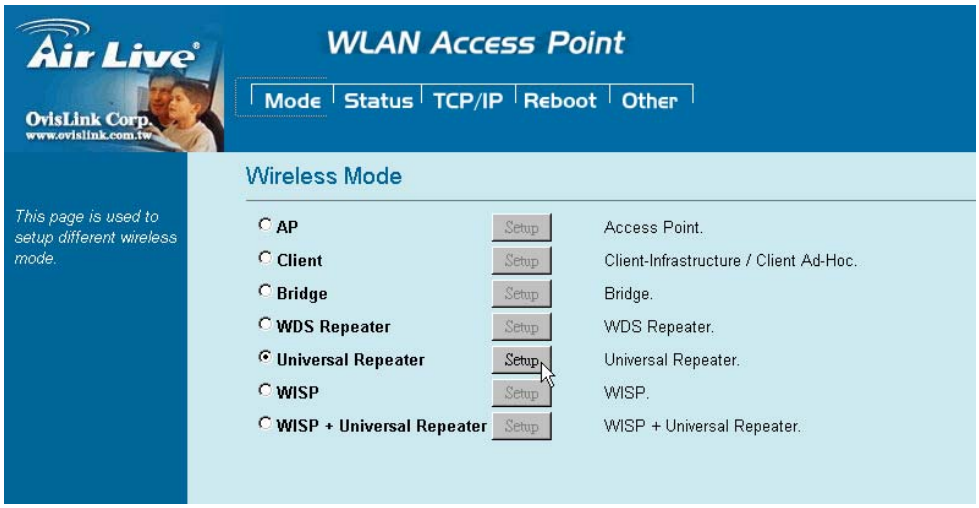


Universal Repeater Mode

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.

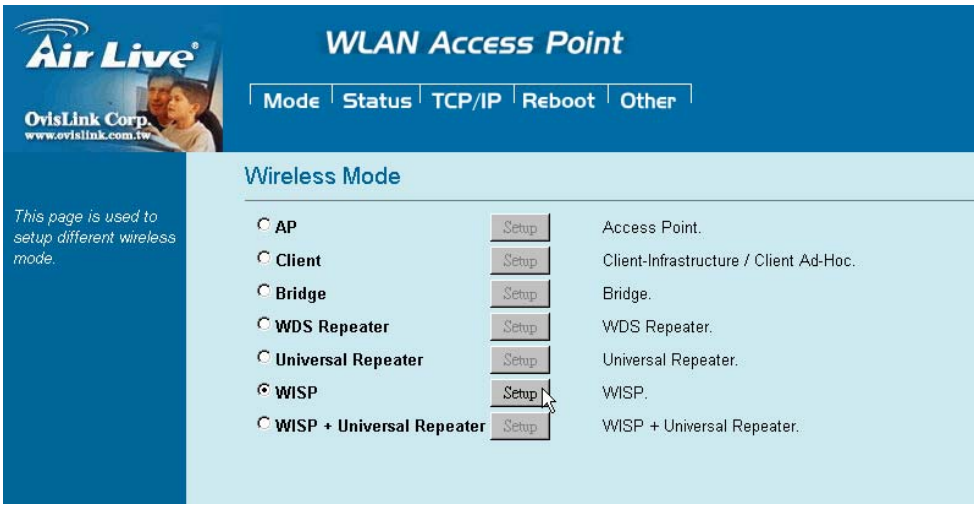


WISP (Client Router) Mode

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.

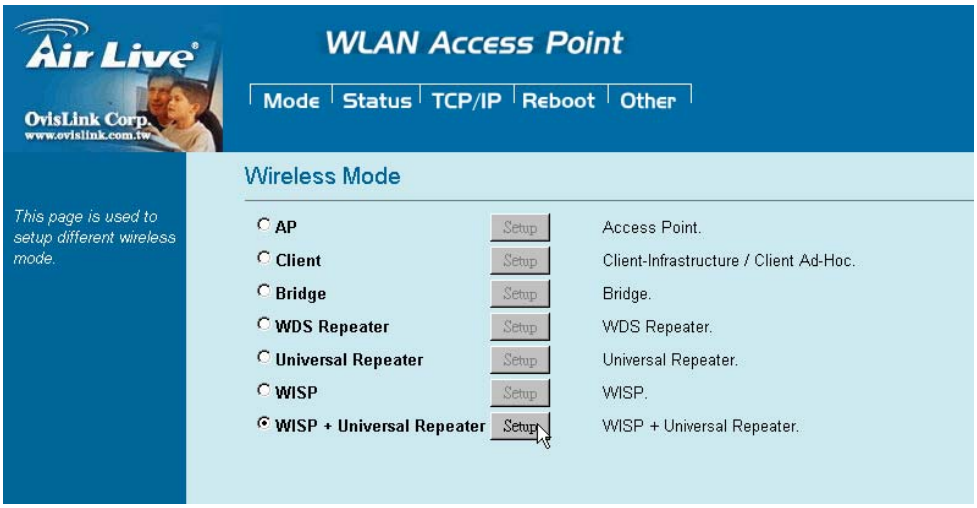
To set the operation mode to **"WISP"**, Please go to **"Mode →WISP"** and click the **Setup** button for configuration.



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

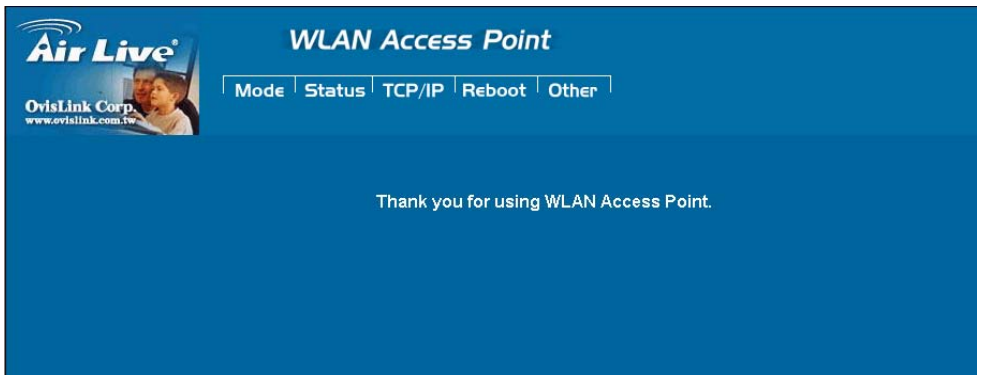
1. Start your computer. Connect an Ethernet cable between your computer and the Wireless Access Point.
2. Make sure your wired station is set to the same subnet as the Wireless Access Point, i.e. 192.168.100.X
3. Start your WEB browser. In the *Address* box, enter the following:

http://192.168.100.252/

The configuration menu is divided into five categories:

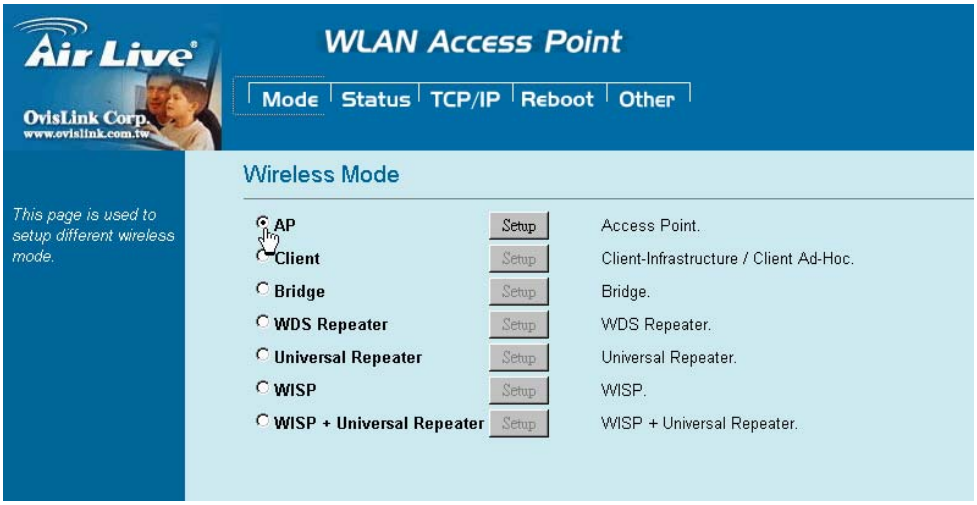
Mode, Status, TCP/IP, Reboot and **Other.**

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.



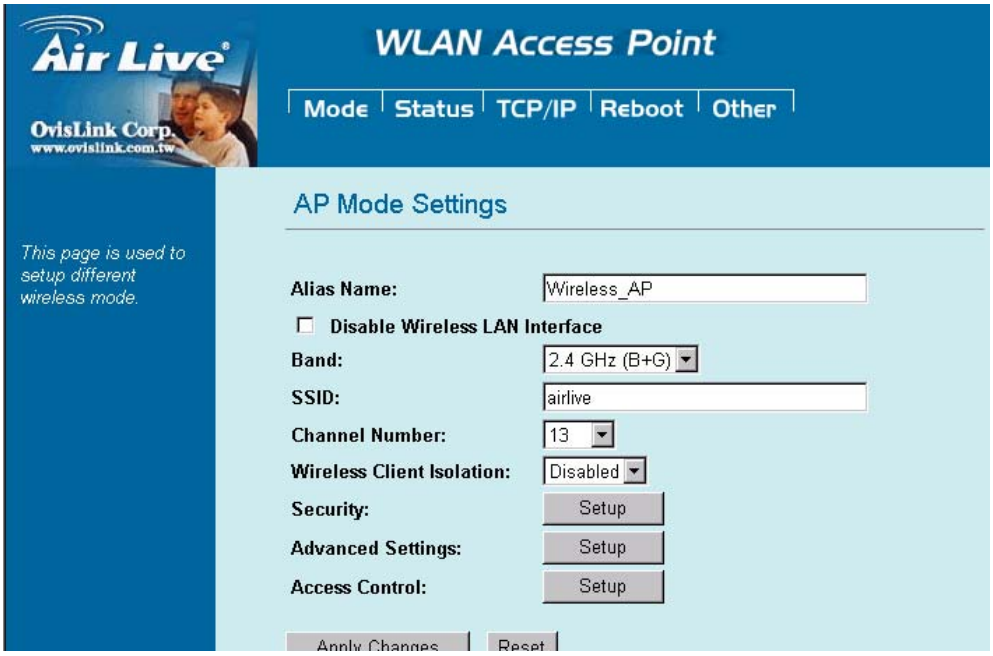
Mode

You can choose and setup different wireless mode for detail configurations



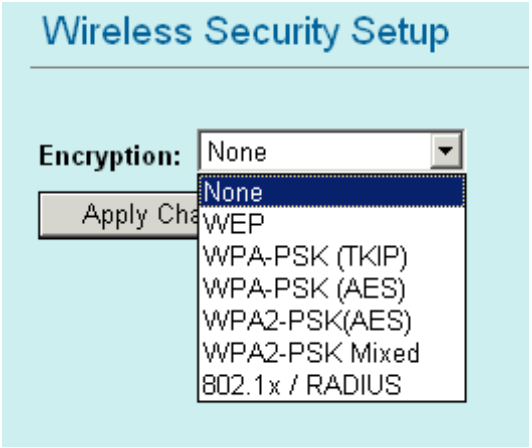
Wireless Mode	
AP	Select the AP and press Setup button for Wireless AP mode configuration.
Client	Select the Client and press Setup button for Wireless Client mode configuration.
Bridge	Select the Bridge and press Setup button for Wireless Bridge mode configuration.
WDS Repeater	Select the WDS Repeater 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	Allow user to set the function **Enabled** or **Disabled**.

Isolation	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



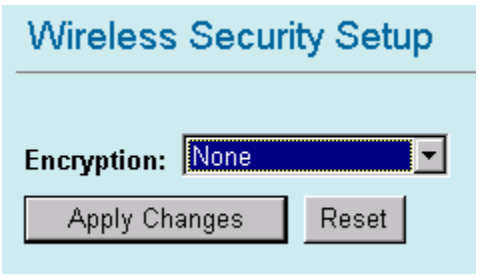
To provide a certain level of security, the IEEE 802.11 standard has defined two types of authentication methods: **Open System** or **Shared Key**. And WL-5470POE also support other wireless authentication and encryption methods for enhance your wireless network.

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.**)**

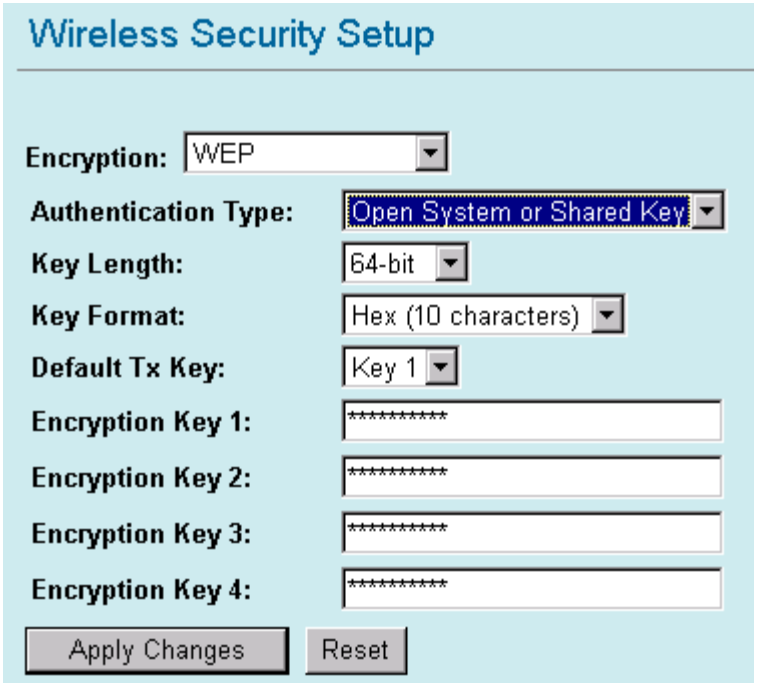
If the Access Point is using **Encryption None**, then the wireless adapter will need to be set to the same authentication mode.



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;

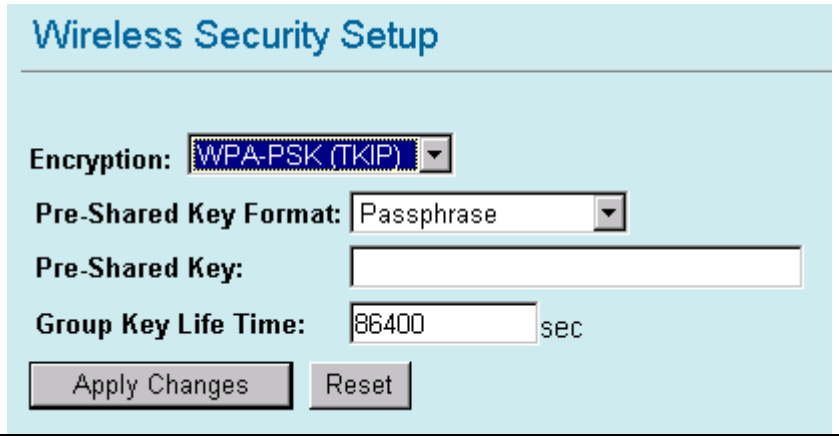
26 hexadecimal digits or **13 ASCII characters** are needed if **128-bit WEP** is used.

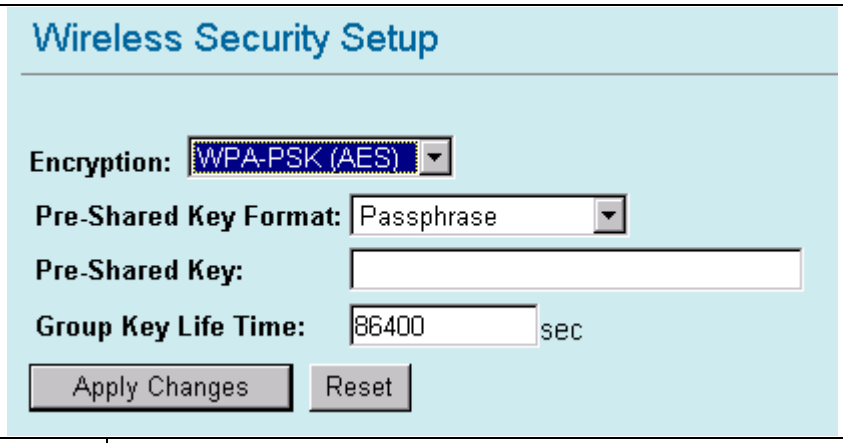
Shared Key is used when both the sender and the recipient share a secret key. So you can choose Open system, or one Shared Key authentication method.

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.



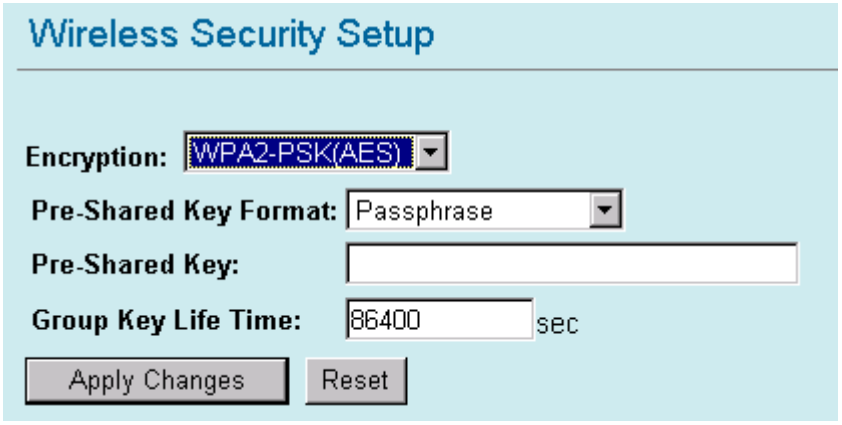


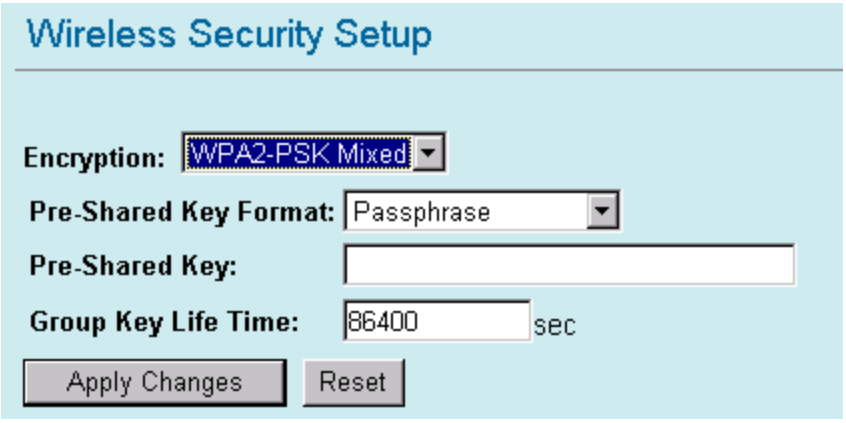
Encryption	You can select WPA-PSK (TKIP) or WPA-PSK (AES) method for data encryption.
Pre-shared Key	There are two formats for choice to set the Pre-shared key, i.e. **Passphrase** and **Hex**. If **Hex** is selected, users will have to enter a 64 characters string. For easier configuration, the **Passphrase** (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

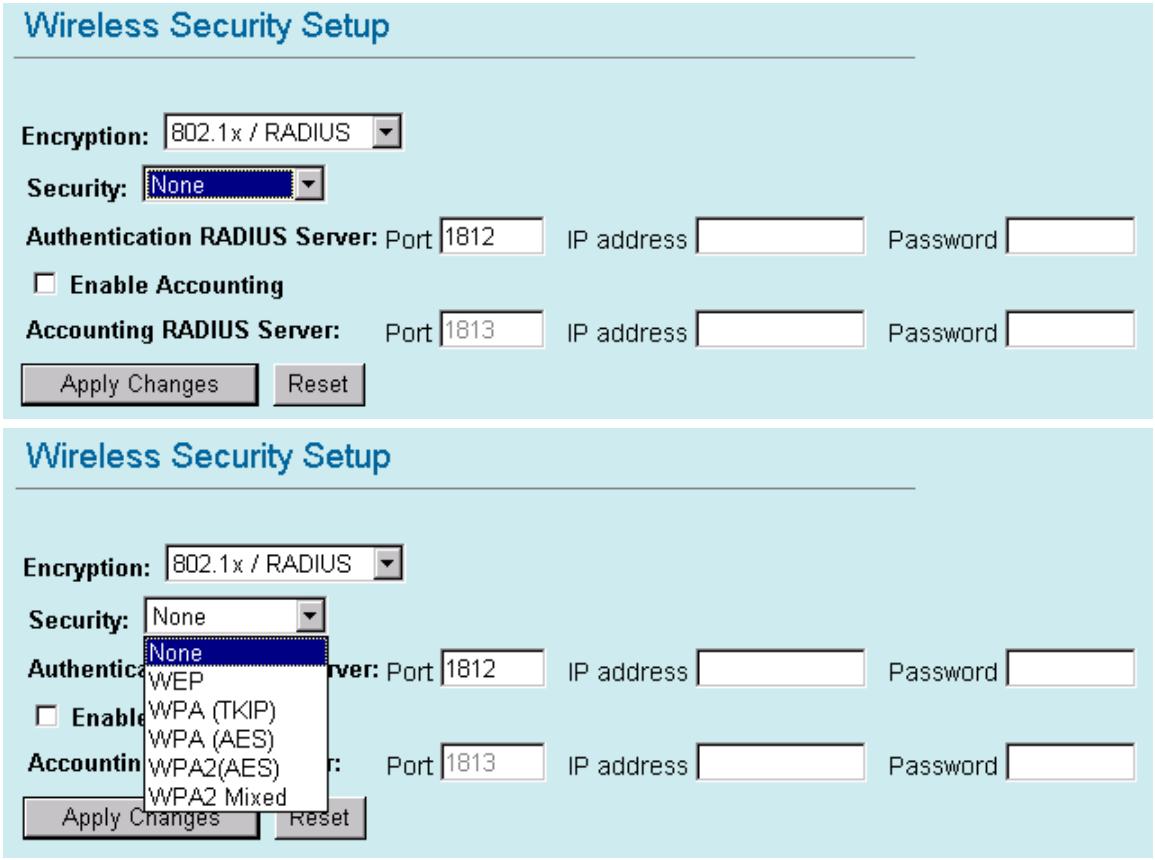
WPA2-PSK authentication method is almost like WPA-PSK, You can choose the Pre-Shared Key format and enter the Pre-shared key,





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)**

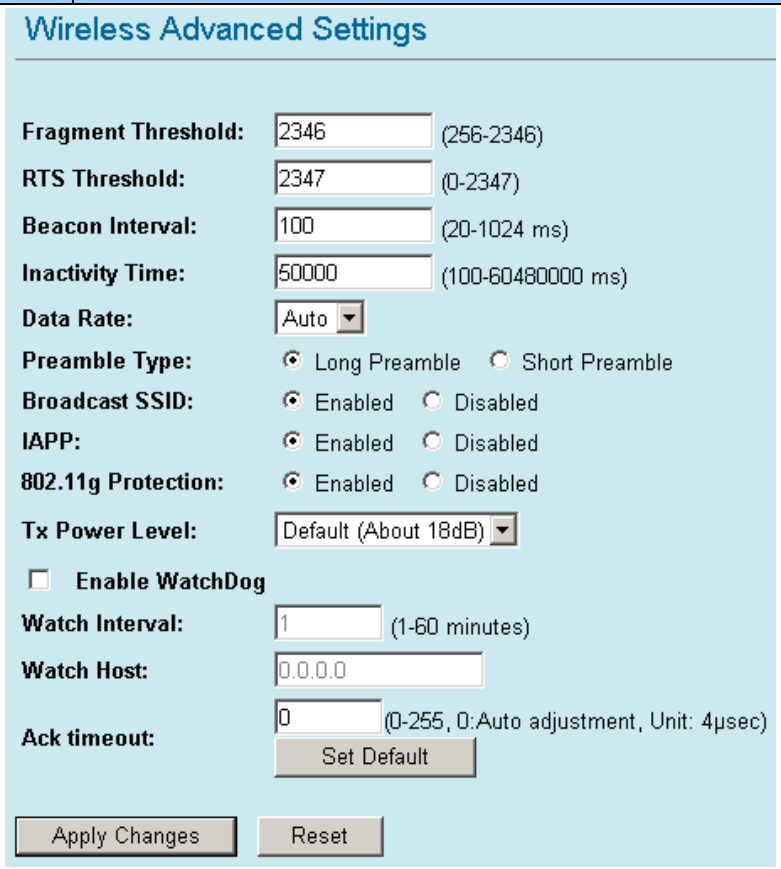
WPA-RADIUS authentication use WPA (Wi-Fi Protect Access) data encryption for 802.1x authentication.

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