Air Live®

www.airlive.com

WLA-5200AP

802.11a/b/g 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

802.11a/b/g Multi-function Wireless Access Point
WLA-5200AP
is in conformity with

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

Clause	**Description**
■ **EN 301 893 v1.2.3 (2003-08)**	Broadband Radio Access Network(BRAN); 5GHz high performance RLAN; Harmonized EN Covering essential requirements of Article 3.2 of the R&TTE Directive.
■ **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 1technical Characteristics and test conditions Part2: Harmonized EN covering Essential requirements under article 3.2 of the R&TTE Directive
■ **EN 301 489-1 v1.5.1 (2004-11)** ■ **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 50371:2002**	Generic standard to demonstrate the compliance of low power Electronic and electrical apparatus with the basic restrictions related to human exposure to electromagnetic field (10MHz – 300GHz) -General public
■ **EN 60950-1:2001/ A11:2004**	Safety for information technology equipment including electrical Business equipment
■ **CE marking**	CE1177 (!)

Manufacturer/Importer

Signature : albert

Name : **Albert Yeh**

Position/ Title : **Vice President**

Date : **2007/5/29**

(Stamp)

WLA-5200AP CE Declaration Statement

Country	Declaration	Country	Declaration
cs Česky [Czech]	OvisLink Corp. tímto prohlašuje, že tento WLA-5200AP je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.	**lt** Lietuvių [Lithuanian]	Šiuo OvisLink Corp. deklaruoja, kad šis WLA-5200AP atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
da Dansk [Danish]	Undertegnede OvisLink Corp. erklærer herved, at følgende udstyr WLA-5200AP overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.	**nl** Nederlands [Dutch	Hierbij verklaart OvisLink Corp. dat het toestel WLA-5200AP 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 WLA-5200AP in 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 WLA-5200AP jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
et Eesti [Estonian]	Käesolevaga kinnitab OvisLink Corp. seadme WLA-5200AP vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.	**hu** Magyar [Hungarian]	Alulírott, OvisLink Corp nyilatkozom, hogy a WLA-5200AP megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.
en English	Hereby, OvisLink Corp., declares that this WLA-5200AP is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.	**pl** Polski [Polish]	Niniejszym OvisLink Corp oświadcza, że WLA-5200AP 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 WLA-5200AP cumple 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 WLA-5200AP está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
el Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ OvisLink Corp. ΔΗΛΩΝΕΙ ΟΤΙ WLA-5200AP ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.	**sl** Slovensko [Slovenian]	OvisLink Corp izjavlja, da je ta WLA-5200AP 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 WLA-5200AP est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE	**sk** Slovensky [Slovak]	OvisLink Corp týmto vyhlasuje, že WLA-5200AP spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
it Italiano [Italian]	Con la presente OvisLink Corp. dichiara che questo WLA-5200AP è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.	**fi** Suomi [Finnish]	OvisLink Corp vakuuttaa täten että WLA-5200AP 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 WLA-5200AP atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.	Íslenska [Icelandic]	Hér með lýsir OvisLink Corp yfir því að WLA-5200AP 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 WLA-5200AP 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 WLA-5200AP 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

AirLive WLA-5200AP is an IEEE802.11a/b/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.

This Access Point provides 64/128bit WEP encryption, WPA and IEEE802.1x which ensures a high level of security to protects 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

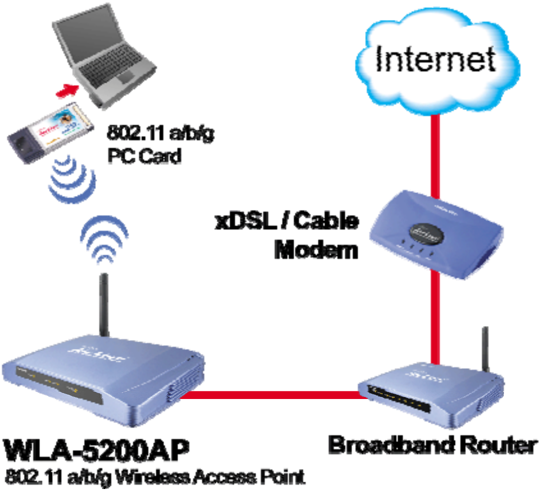
- Two LAN ports for Wireless AP cascade
- Support WPA-PSK and WPA2-PSK

  Support of 7 Wireless modes:

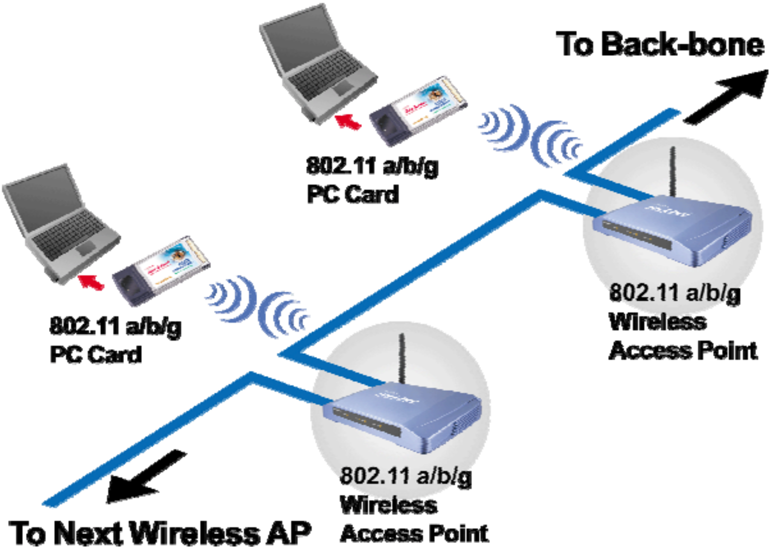
  AP, **Client, Bridge**, **WDS Repeater**, **Universal Repeater**, **WISP (Client Router)**, and **WISP + Universal Repeater** modes
- Support data rate automatic fallback
- Automatic channel selection
- Client access control
- Support 802.1x/Radius client with, TKIP, AES and TKIP_AES encryption
- Support IAPP
- Adjustable Tx power, Tx rate, and SSID broadcast
- Allow WEP 64/128 bit
- Web interface management
- Support System event log and statistics
- MAC filtering (For wireless only)
- Support wireless 802.11 SNMP management
- WatchDog timer to warm boot system

Application

Example 1

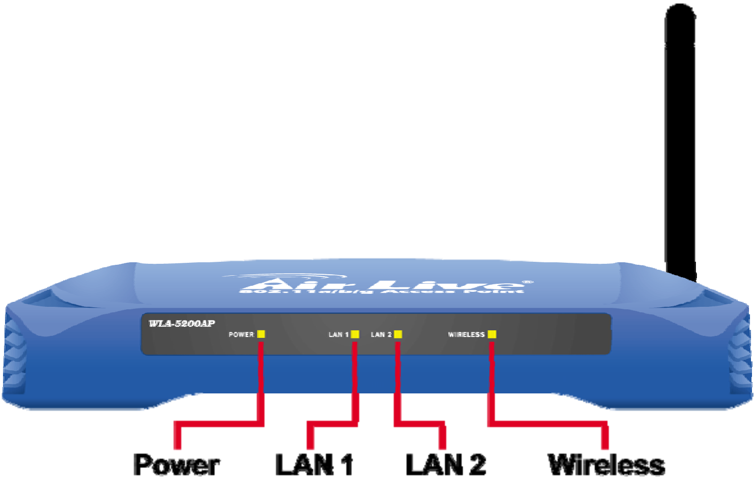


Example 2



Parts Names and Functions

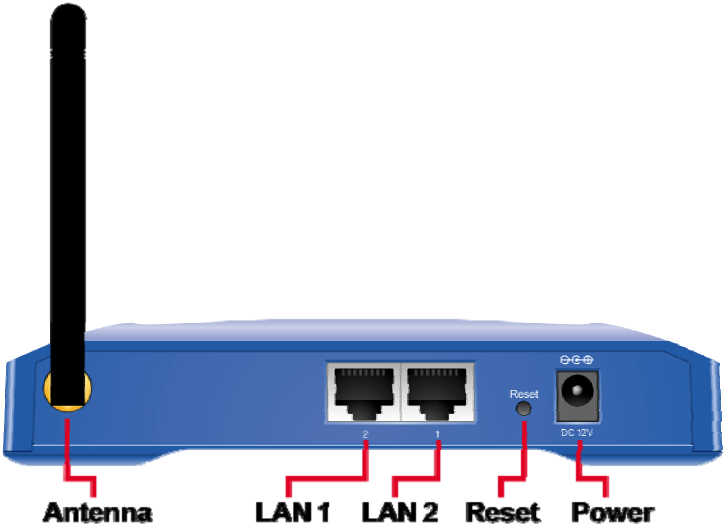
1. Front Panel: (LED Indicators)



LED Indicator	Color	Status	
		Solid	**Flashing**
Power	Yellow	Turns solid green when the power is applied to this device.	N/A.
LAN1, LAN2	Yellow	Turns solid Yellow when the Ethernet cable is connected the LAN port.	Receiving/ Sending data
Wireless	Yellow	Turns solid Yellow when the power is applied to this device.	Receiving/ Sending data

Table 1: LED Indicators

2. Rear Panel: Connection Ports

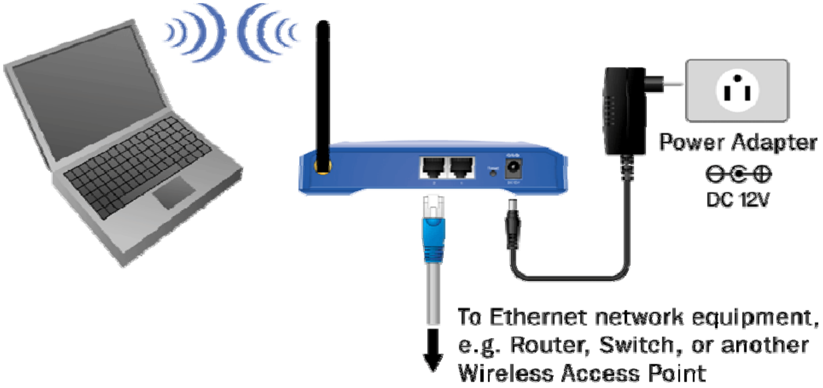


Port/button	Functions
LAN ports (LAN1,LAN2)	Use standard LAN cables (RJ45 connectors) to connect your PCs to these ports. If required, any port can be connected to another hub. Any LAN port will automatically function as an "Uplink" port when necessary.
(Factory) RESET	Press over 3 seconds to reboot this device. Press for over 10 seconds to restore factory settings. Performing the Factory Reset will erase all previously entered device settings.
12V DC	Connects the power adapter plug

Table 2: Connection Ports

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.


Power Adapter
DC 12V
To Ethernet network equipment, e.g. Router, Switch, or another Wireless Access Point

1. **Connect to your local area network:** connect a **Ethernet cable** to one of the **Ethernet** port (LAN1,or LAN2) of this Wireless Access Point, and the other end to a hub, switch, router, or another wireless access point.
2. **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.
3. **Configure your PC:** Make sure your local PC(s) has wireless network adapter(s) installed.

ABOUT THE WIRELESS OPERATION MODES

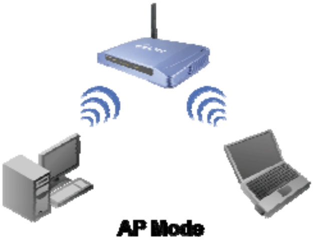
This device provides seven operational applications with **AP, Bridge, Client (Ad-hoc), Client (Infrastructure) ,WDS Repeater, Universal Repeater** , **WISP(Client Router) mode** which are mutually exclusive.

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.

AP Mode

When acting as an access point, 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.

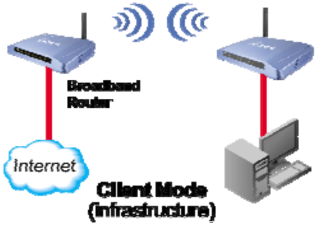
To set the operation mode to **Access Point,** please go to "**Wireless →Basic Settings"**, in the "**Mode**" field click the down arrow ▼ to select AP mode.



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.

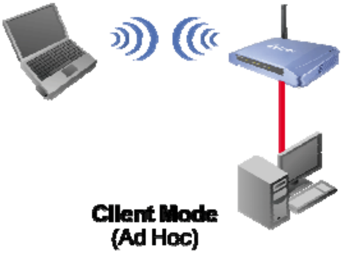
To set the operation mode to **Client (Infrastructure),** please go to "**Wireless →Basic Settings**", in the "**Mode**" field click the down arrow ▼ to select **Client** mode, and then select **"Network Type"** as "**Infrastructure**".



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).

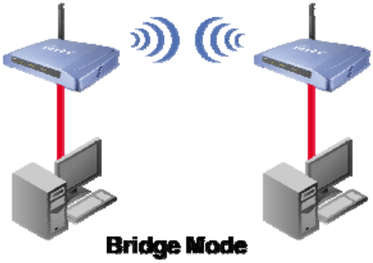
To set the operation mode to **Client (Ad-hoc),** please go to "**Wireless →Basic Settings**", in the "**Mode**" field click the down arrow ▼ to select **Client** mode, and then select Network Type as "**Ad-hoc**".



Bridge Mode

You will be able to connect two wireless LANs together under the Bridge mode. This only works with another Wireless a/b/g Access Point. If enabled you must enter the MAC address of that Wireless a/b/g Access Point.

To set the operation mode to **Bridge mode,** please go to "**Wireless →Basic Settings**", in the "**Mode**" field click the down arrow ▼ to select **Bridge** mode.

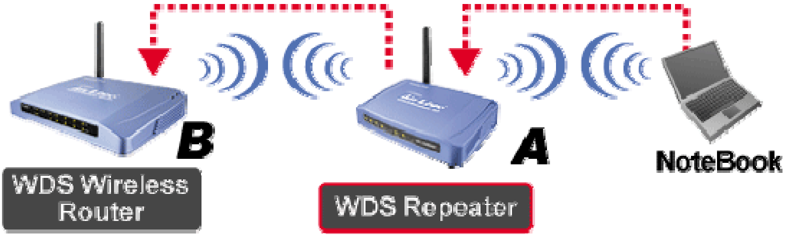


WDS Repeater Mode

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 →Repeater**”, click the **“Setup”** button

in the **“Network Type”** field, select as “**WDS Repeater ”** for configuration



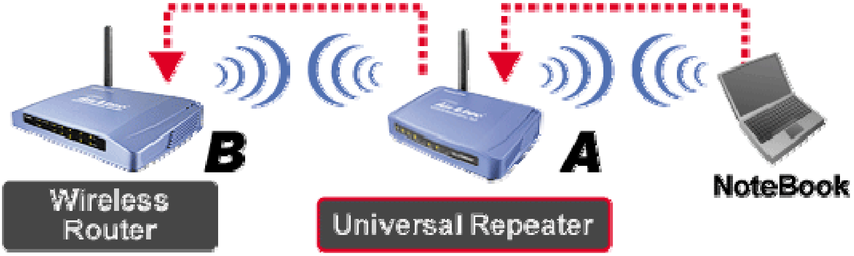
Universal Repeater Mode

A universal repeater can also extend the wireless coverage of another wireless AP or router without requiring the remote device to have WDS function. Therefore, it can work with almost any wireless device.

To set the operation mode to **Universal Repeater,** please go to “**Mode →Repeater**”, click the **“Setup”** button

in the **“Network Type”** field, select as “**Universal Repeater ”** for configuration

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



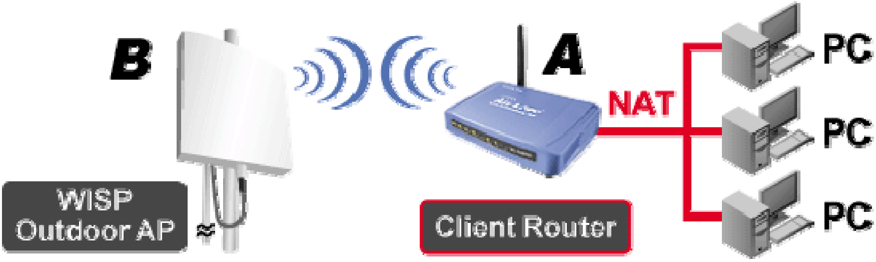
WISP (Client Router) Mode

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.

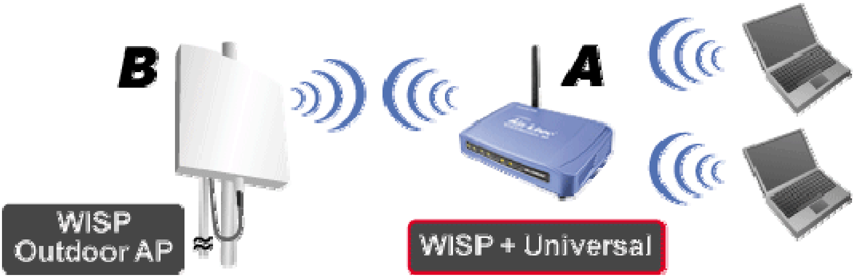
To set the operation mode to **WISP mode,** please go to "**Mode →WISP**", click the **"Setup"** button

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.

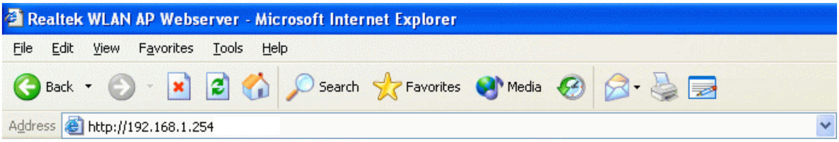


CONFIGURATION

Login

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. 192.168.1.254
3. Start your WEB browser. In the *Address* box, enter the following:

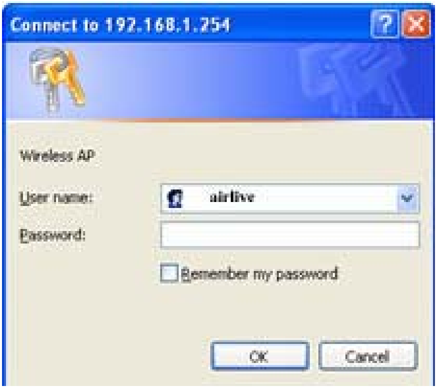
http://192.168.1.254



Realtek WLAN AP Webserver - Microsoft Internet Explorer

Address http://192.168.1.254

4. Enter **airlive** in the Username and password column when you are prompted the login screen.



Connect to 192.168.1.254

Wireless AP

User name: airlive

Password:

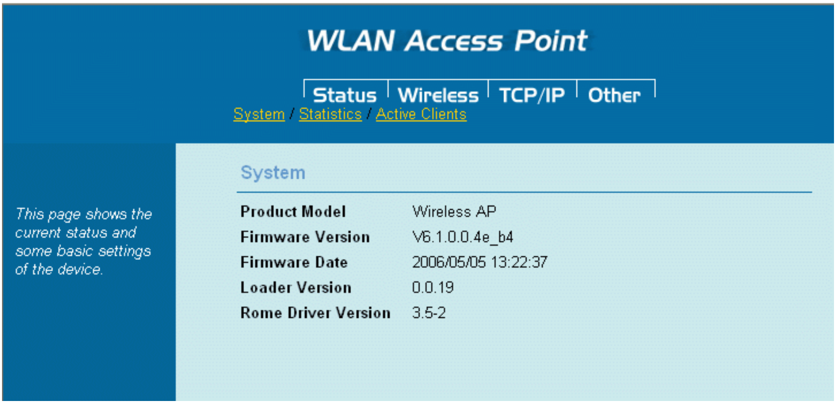
□ Remember my password

The configuration menu is divided into four categories: **Status, Wireless, TCP/IP,** and **Other settings**. 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.

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



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

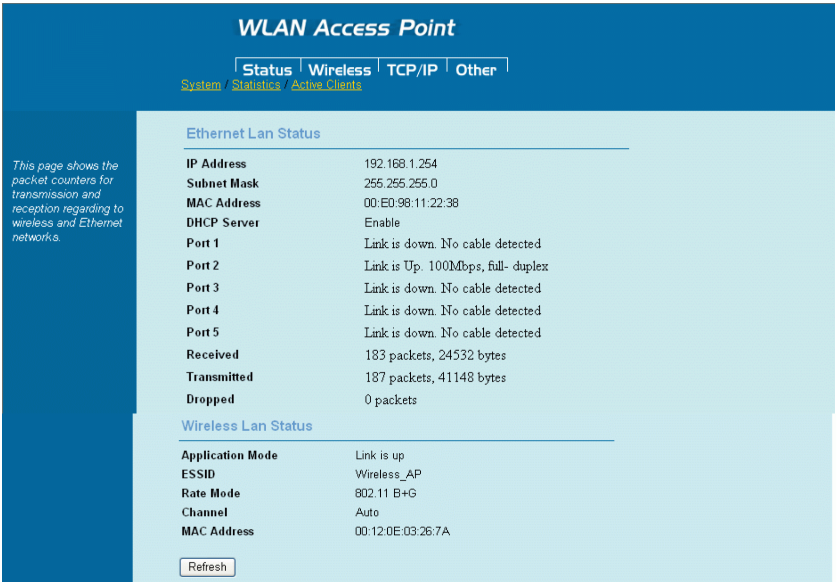
System

Product Model	Wireless AP
Firmware Version	V6.1.0.0.4e_b4
Firmware Date	2006/05/05 13:22:37
Loader Version	0.0.19
Rome Driver Version	3.5-2

System	
Product Model	Shows the product model name.
Firmware Version	The current version of the firmware installed in this device.
Firmware Date	Shows the firmware date.
Loader Version	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.
Rome Driver Version	Shows the Rome driver version.

Statistics

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



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

Ethernet Lan Status

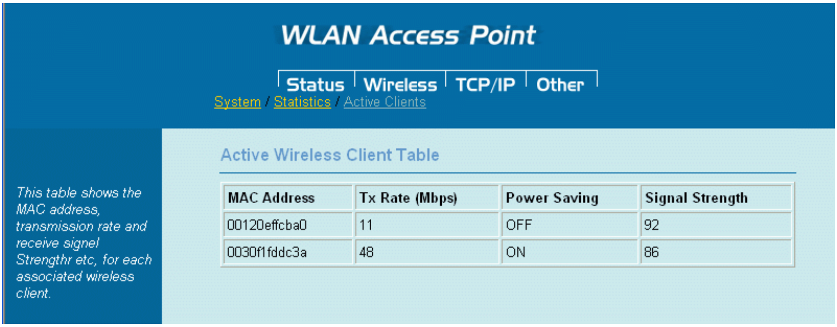
IP Address	192.168.1.254
Subnet Mask	255.255.255.0
MAC Address	00:E0:98:11:22:38
DHCP Server	Enable
Port 1	Link is down. No cable detected
Port 2	Link is Up. 100Mbps, full- duplex
Port 3	Link is down. No cable detected
Port 4	Link is down. No cable detected
Port 5	Link is down. No cable detected
Received	183 packets, 24532 bytes
Transmitted	187 packets, 41148 bytes
Dropped	0 packets

Wireless Lan Status

Application Mode	Link is up
ESSID	Wireless_AP
Rate Mode	802.11 B+G
Channel	Auto
MAC Address	00:12:0E:03:26:7A

Active Client

Shows the information of the devices that are currently associating with this Wireless Access Point.



This table shows the MAC address, transmission rate and receive signel Strengthr etc, for each associated wireless client.

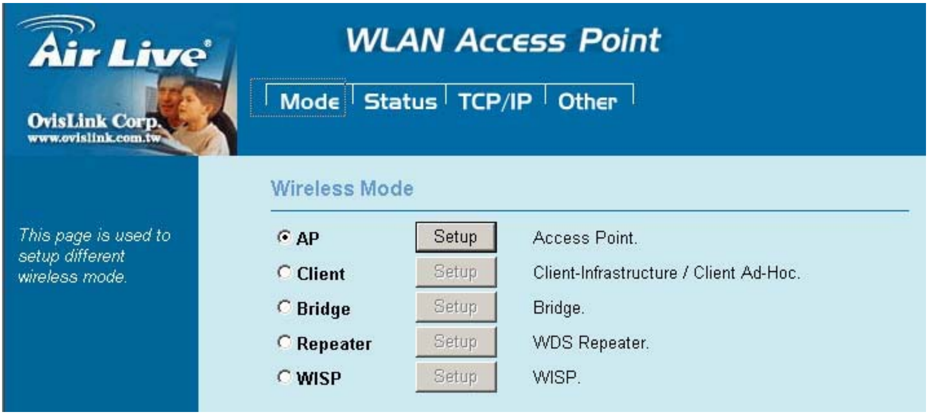
Active Wireless Client Table

MAC Address	Tx Rate (Mbps)	Power Saving	Signal Strength
00120effcba0	11	OFF	92
0030f1fddc3a	48	ON	86

Wireless Mode

Wireless mode

This page includes all wireless mode settings and major parameters. When you choose each wireless mode that will cause the device to reboot for the new wireless mode take effect.

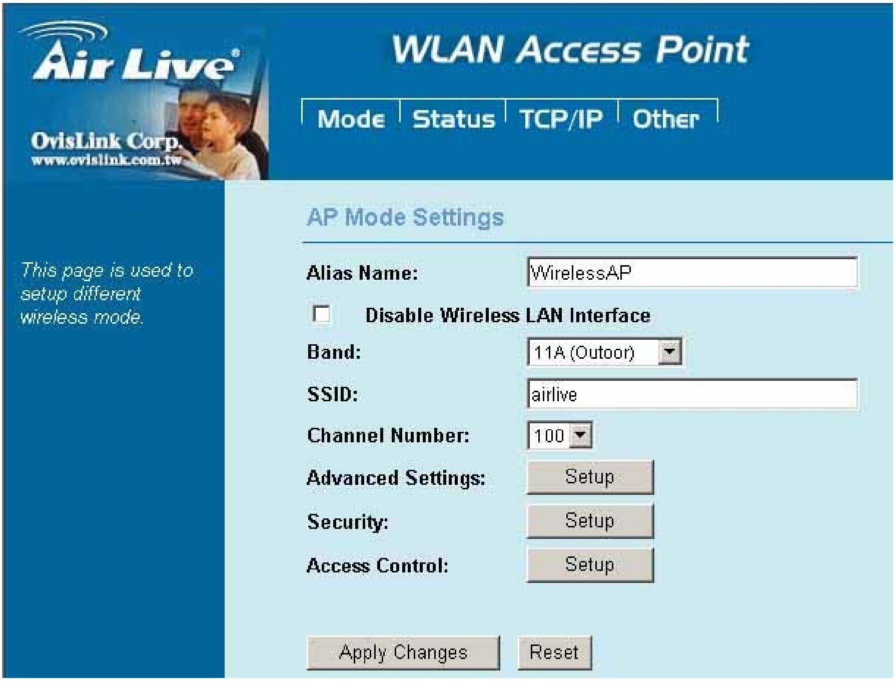


This page is used to setup different wireless mode.

Wireless Mode

● AP	Setup	Access Point.
○ Client	Setup	Client-Infrastructure / Client Ad-Hoc.
○ Bridge	Setup	Bridge.
○ Repeater	Setup	WDS Repeater.
○ WISP	Setup	WISP.

AP modes



This page is used to setup different wireless mode.

AP Mode Settings

Alias Name: WirelessAP

□ Disable Wireless LAN Interface

Band: 11A (Outoor)

SSID: airlive

Channel Number: 100

Advanced Settings: Setup

Security: Setup

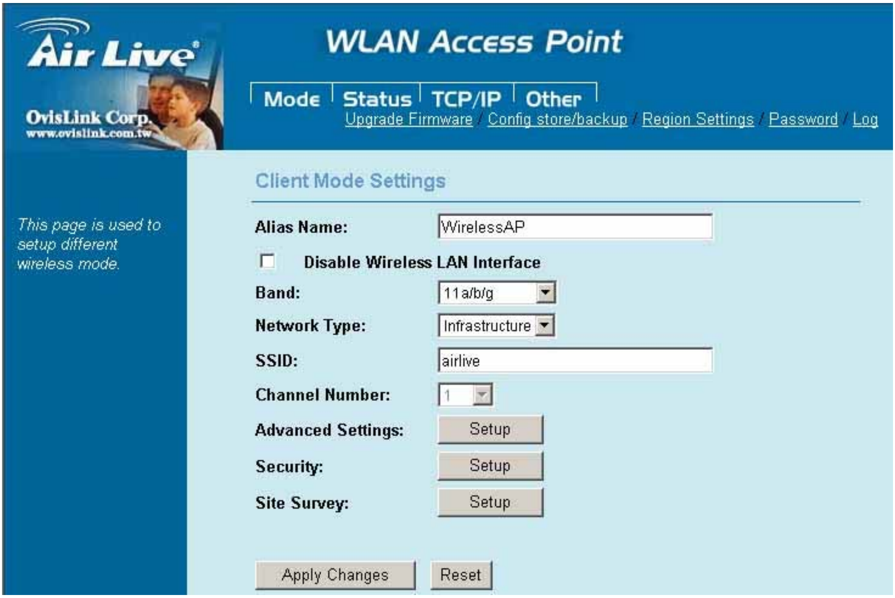
Access Control: Setup

Alias Name	The distinguishing name of this device, you may change the default alias name by entering a new one in this column.
□ 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	Choose a mode from the pull-down list. • 11b/g mixed: Select to allow both wireless-b and wireless-g devices on the network. • 11B only: Select to allow only wireless-B devices on the network. • 11G only: Select to allow only wireless-G devices on the network. • 11A (indoor): Select to allow only wireless-A devices on the indoor network. • 11A (outdoor): Select to allow only wireless-G devices on the network. • 11A (indoor): Select to allow only wireless-A devices on the outdoor network.
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	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.

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.

Client Mode Settings



Client Mode Settings

This page is used to setup different wireless mode.

Alias Name: WirelessAP

□ Disable Wireless LAN Interface

Band: 11a/b/g

Network Type: Infrastructure

SSID: airlive

Channel Number: 1

Advanced Settings: Setup

Security: Setup

Site Survey: Setup

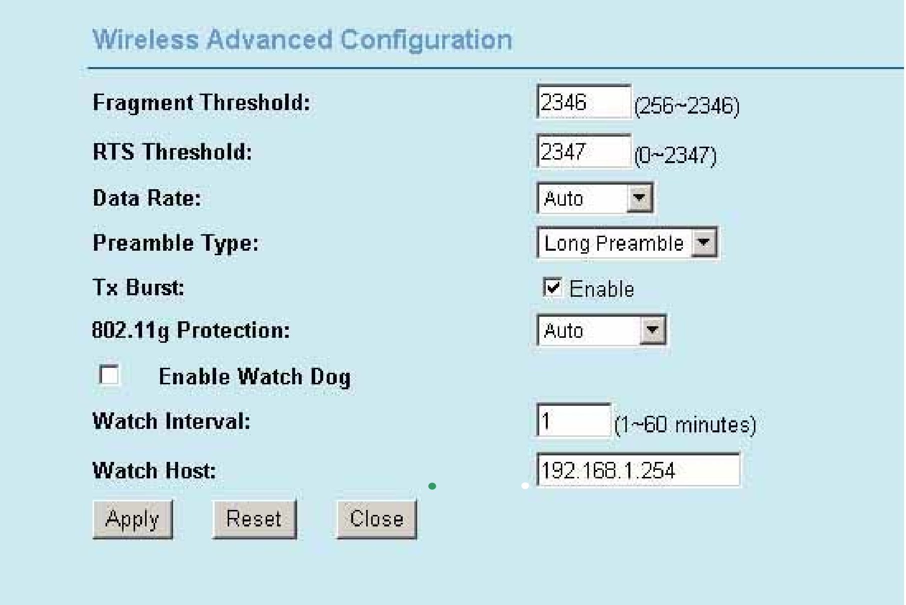
Apply Changes | Reset

Alias Name	The distinguishing name of this device, you may change the default alias name by entering a new one in this column.
□ 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	Choose a mode from the pull-down list. • 11b/g mixed: Select to allow both wireless-b and wireless-g devices on the network. • 11B only: Select to allow only wireless-B devices on the network. • 11G only: Select to allow only wireless-G devices on the network. • 11A (indoor): Select to allow only wireless-A devices on the indoor network. • 11A (outdoor): Select to allow only wireless-G devices on the network. • 11A (indoor): Select to allow only wireless-A devices on the outdoor

	network.
Network Type	You can choose the Ad-Hoc mode and Infrastructure 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	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.

Advanced Settings (AP/ Client/WISP Mode)

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



Wireless Advanced Configuration

Fragment Threshold: 2346 (256~2346)

RTS Threshold: 2347 (0~2347)

Data Rate: Auto

Preamble Type: Long Preamble

Tx Burst: ☑ Enable

802.11g Protection: Auto

□ Enable Watch Dog

Watch Interval: 1 (1~60 minutes)

Watch Host: 192.168.1.254

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

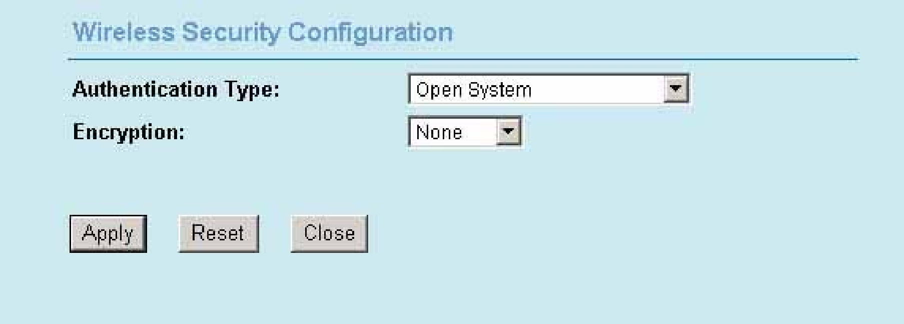
	Point, informing that it is going to transmit the data. Upon receipt, the Access Point will respond with a CTS message to all station within its range to notify all other stations to defer transmission. It will also confirm the requestor station that the Access Point has reserved it for the time-frame 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.
Tx Burst	Select the check box to enable the Tx Burst function.
802.11g Protection	The 802.11g standard includes a protection mechanism to ensure mixed 802.11b and 802.11g operations. If there is no such kind of mechanism exists, the two kinds of standards may mutually interfere and decrease network's performance.

Enable Watch Dog **Watch Interval** **Watch Host**	Check the box to enable this watch dog function and set the Watch dog time Interval (1~60 mins) and type the ip address of the host ip

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.

Security (AP/Client/WISP Mode)

Here you can configure the security of your wireless network. Selecting different method will enable you to have different level of security. Please note that by using any encryption, by which data packet is encrypted before transmission to prevent data packets from being eavesdropped by unrelated people, there may be a significant degradation of the data throughput on the wireless link.



Wireless Security Configuration

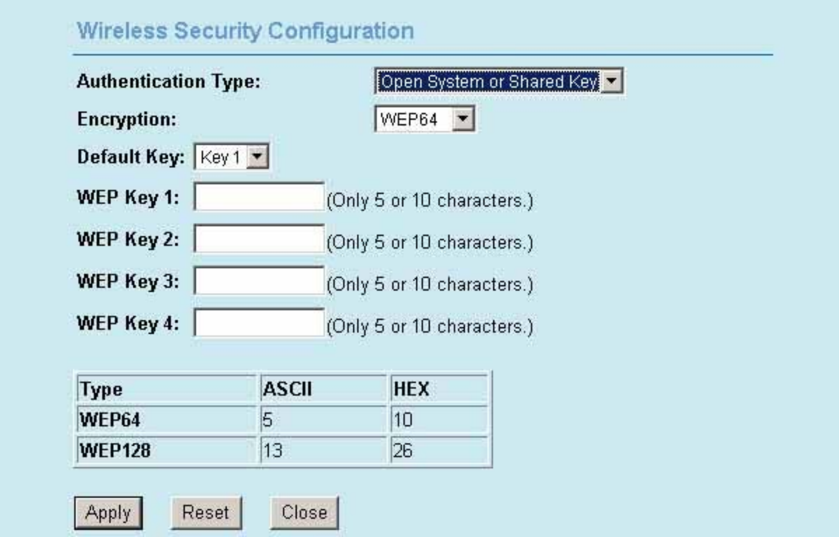
Authentication Type: Open System

Encryption: None

Authentication Type: Open System or Shared Key/Shared Key/Open System

If Open System or Shared Key/Shared Key/Open System is selected, users will have to Set WEP keys with an encryption either **WEP64** or **WEP128**. Only the **Open System** can set the encryption to **None** (Without any WEP Key protection mechanism)

- **HEX:** If you are using hexadecimal numbers (**0-9, or A-F**).
- **ASCII:** If you are using ASCII characters (**case-sensitive**).
- **Ten hexadecimal digits** or **five 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



Wireless Security Configuration

Authentication Type: Open System or Shared Key

Encryption: WEP64

Default Key: Key 1

WEP Key 1: (Only 5 or 10 characters.)

WEP Key 2: (Only 5 or 10 characters.)

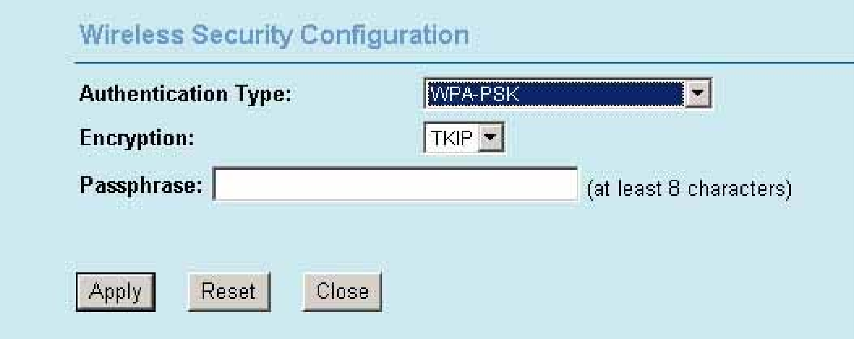
WEP Key 3: (Only 5 or 10 characters.)

WEP Key 4: (Only 5 or 10 characters.)

Type	ASCII	HEX
WEP64	5	10
WEP128	13	26

Authentication Type: WPA-PSK/WPA2-PSK

If **WPA-PSK/WPA2-PSK** is selected, users will have to select the Encryption from the pull-down list, **TKIP**, **AES** or **TKIP_AES** and then enter a passphrase.



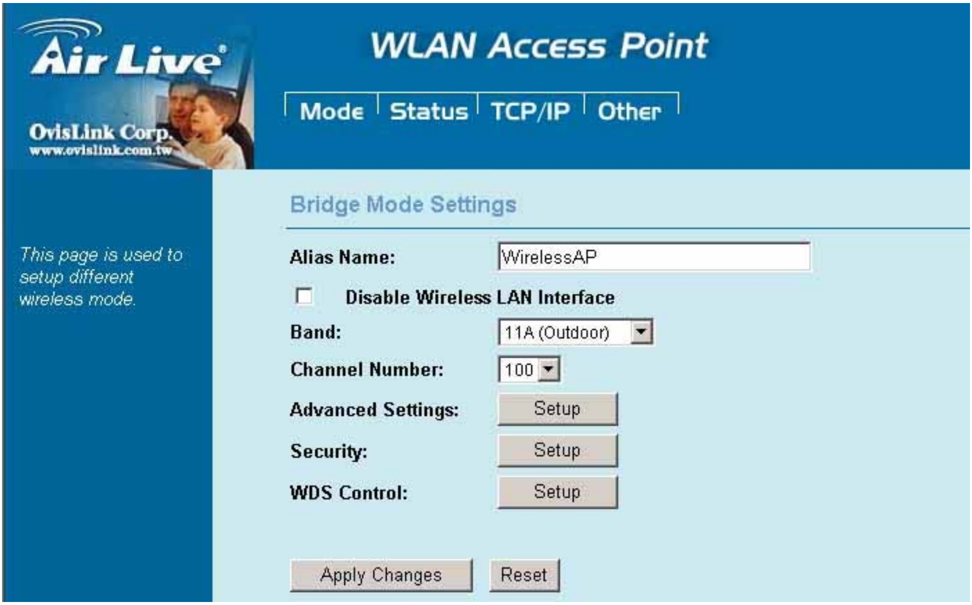
Wireless Security Configuration

Authentication Type: WPA-PSK

Encryption: TKIP

Passphrase: (at least 8 characters)

Bridge Mode Setting



Bridge Mode Settings

Alias Name: WirelessAP

□ Disable Wireless LAN Interface

Band: 11A (Outdoor)

Channel Number: 100

Advanced Settings: Setup

Security: Setup

WDS Control: Setup

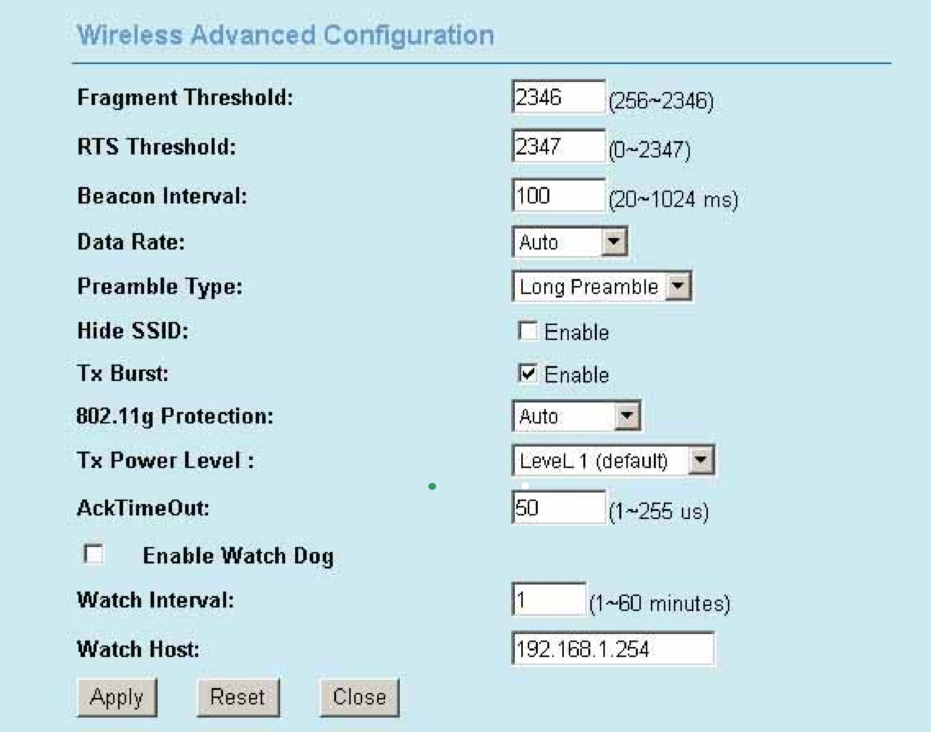
Apply Changes   Reset

Alias Name	The distinguishing name of this device, you may change the default alias name by entering a new one in this column.
□ 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	Choose a mode from the pull-down list. • 11b/g mixed: Select to allow both wireless-b and wireless-g devices on the network. • 11B only: Select to allow only wireless-B devices on the network. • 11G only: Select to allow only wireless-G devices on the network. • 11A (indoor): Select to allow only wireless-A devices on the indoor network. • 11A (outdoor): Select to allow only wireless-G devices on the network. • 11A (indoor): Select to allow only wireless-A devices on the outdoor network.

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.
Advanced Setting	

Advanced Settings (Bridge/Repeater Mode)

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



Wireless Advanced Configuration

Fragment Threshold: 2346 (256~2346)

RTS Threshold: 2347 (0~2347)

Beacon Interval: 100 (20~1024 ms)

Data Rate: Auto

Preamble Type: Long Preamble

Hide SSID: □ Enable

Tx Burst: ☑ Enable

802.11g Protection: Auto

Tx Power Level : LeveL 1 (default)

AckTimeOut: 50 (1~255 us)

□ Enable Watch Dog

Watch Interval: 1 (1~60 minutes)

Watch Host: 192.168.1.254

Fragment Threshold	Fragmentation mechanism is used for improving the efficiency when high traffic flows along in the

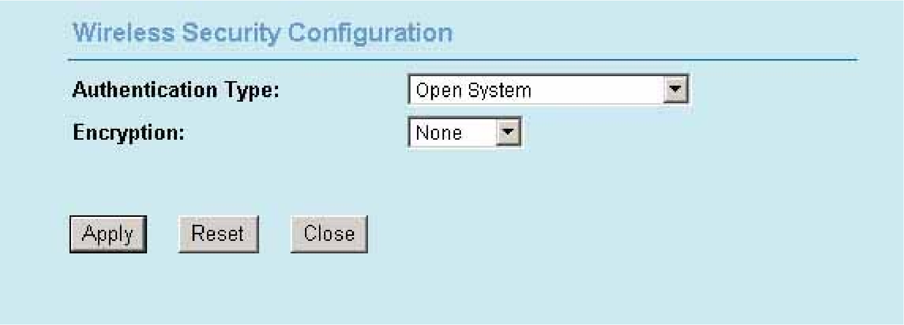
	wireless network. If your 802.11g Wireless LAN PC Card often transmit large files in wireless network, you can enter new Fragment Threshold value to split the packet. The value can be set from 256 to 2346. The default value is **2346**.
RTS Threshold	RTS Threshold is a mechanism implemented to prevent 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.
Hide SSID	Select **enabled** to allow all the wireless stations to hide the SSID of this router.
Tx Burst	Select the check box to enable the Tx Burst function.
802.11g Protection	The 802.11g standard includes a protection mechanism to ensure mixed 802.11b and 802.11g operations. 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	Totally have 6 Tx Power Level, default is Level one you can select Level2~Level6 to reduce the Tx Power
AckTimeOut	Maximum time, in microseconds, that the failover daemon will wait for an ACK or NOACK message to be received from the peer failover daemon. For each message the failover daemon sends, the peer failover daemon sends an ACK or NOACK message to indicate that the peer is still functioning. Default: **50** microseconds
Enable Watch Dog **Watch Interval** **Watch Host**	Check the box to enable this watch dog function and set the Watch dog time Interval (1~60 mins) and type the ip address of the host ip

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.

Security (Bridge/Repeater Mode)

Here you can configure the security of your wireless network. Selecting different method will enable you to have different level of security. Please note that by using any encryption, by which data packet is encrypted before transmission to prevent data packets from being eavesdropped by unrelated people, there may be a significant degradation of the data throughput on the wireless link.



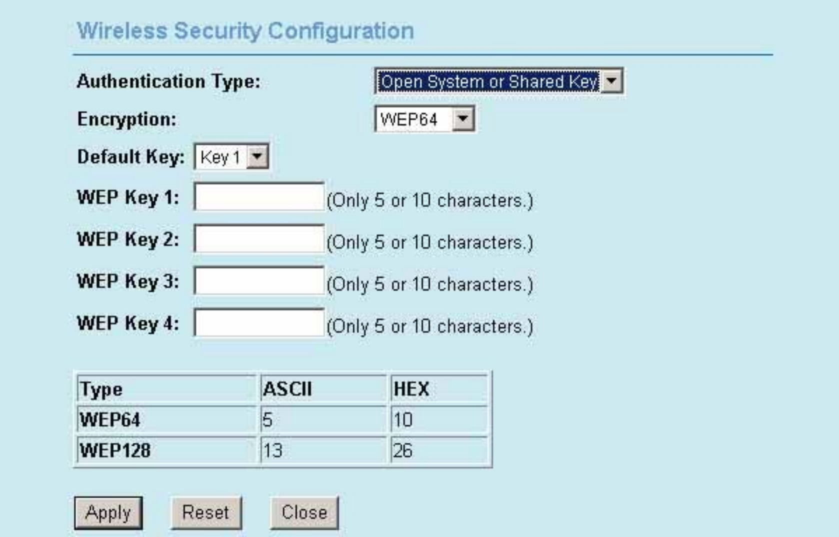
Wireless Security Configuration

Authentication Type: Open System

Encryption: None

Authentication Type: Open System or Shared Key/Shared Key/Open System
If Open System or Shared Key/Shared Key/Open System is selected, users will have to Set WEP keys with an encryption either **WEP64** or **WEP128**. Only the **Open System** can set the encryption to **None** (Without any WEP Key protection mechanism)

- **HEX:** If you are using hexadecimal numbers (**0-9, or A-F**).
- **ASCII:** If you are using ASCII characters (**case-sensitive**).
- **Ten hexadecimal digits** or **five 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



Wireless Security Configuration

Authentication Type: Open System or Shared Key

Encryption: WEP64

Default Key: Key 1

WEP Key 1: (Only 5 or 10 characters.)

WEP Key 2: (Only 5 or 10 characters.)

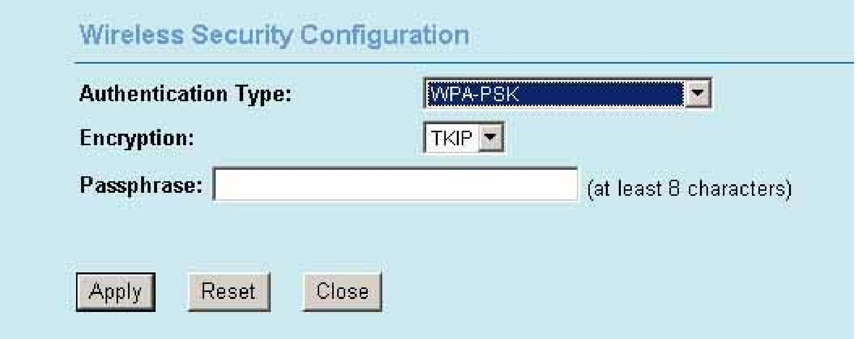
WEP Key 3: (Only 5 or 10 characters.)

WEP Key 4: (Only 5 or 10 characters.)

Type	ASCII	HEX
WEP64	5	10
WEP128	13	26

Authentication Type: WPA-PSK/WPA2-PSK

If **WPA-PSK/WPA2-PSK** is selected, users will have to select the Encryption from the pull-down list, **TKIP**, **AES** or **TKIP_AES** and then enter a passphrase.



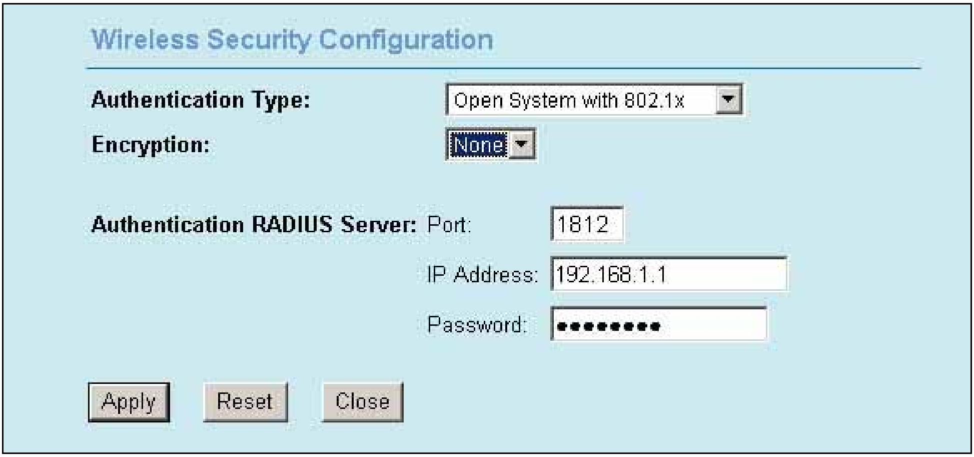
Wireless Security Configuration

Authentication Type: WPA-PSK

Encryption: TKIP

Passphrase: (at least 8 characters)

Authentication Type: Open System with 802.1x/WPA-RADIUS/WPA2-RADIUS



Wireless Security Configuration

Authentication Type: Open System with 802.1x

Encryption: None

Authentication RADIUS Server: Port: 1812

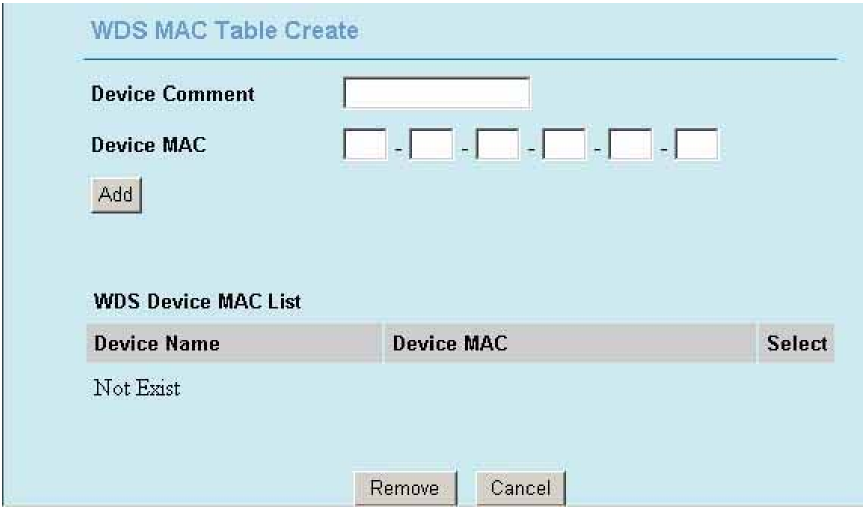
IP Address: 192.168.1.1

Password: ●●●●●●●●●

If the **Open System with 802.1x/WPA-RADIUS/WPA2-RADIUS** is selected, users will have to select the Encryption from the pull-down list, **TKIP**, **AES** or **TKIP_AES** and configure a RADIUS server, the RADIUS Server will proceed to check the 802.1x Authentication. Only the **Open System with 802.1x** can set the encryption to **None** (Without any WEP Key protection mechanism)

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

WDS Control



WDS MAC Table Create

Device Comment

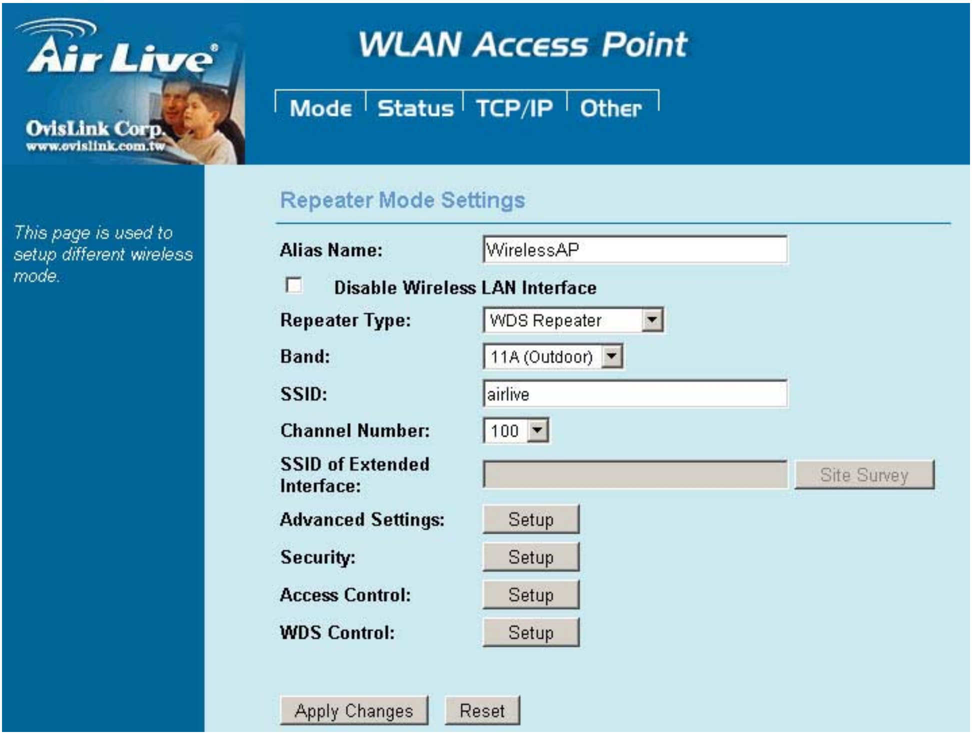
Device MAC

WDS Device MAC List

Device Name	Device MAC	Select
Not Exist		

WDS MAC Table Create	
Device Comment	You may enter up to 20 characters as a remark to the previous MAC Address.
Device MAC	Enter the MAC Address of a station that is allowed to access this Access Point.
Remove	To remove clients from access to this Access Point, you may firstly check the **Select** checkbox next to the MAC address and Comments, and press **Remove button**

Repeater Mode Settings



This page is used to setup different wireless mode.

Repeater Mode Settings

Alias Name: WirelessAP

□ Disable Wireless LAN Interface

Repeater Type: WDS Repeater

Band: 11A (Outdoor)

SSID: airlive

Channel Number: 100

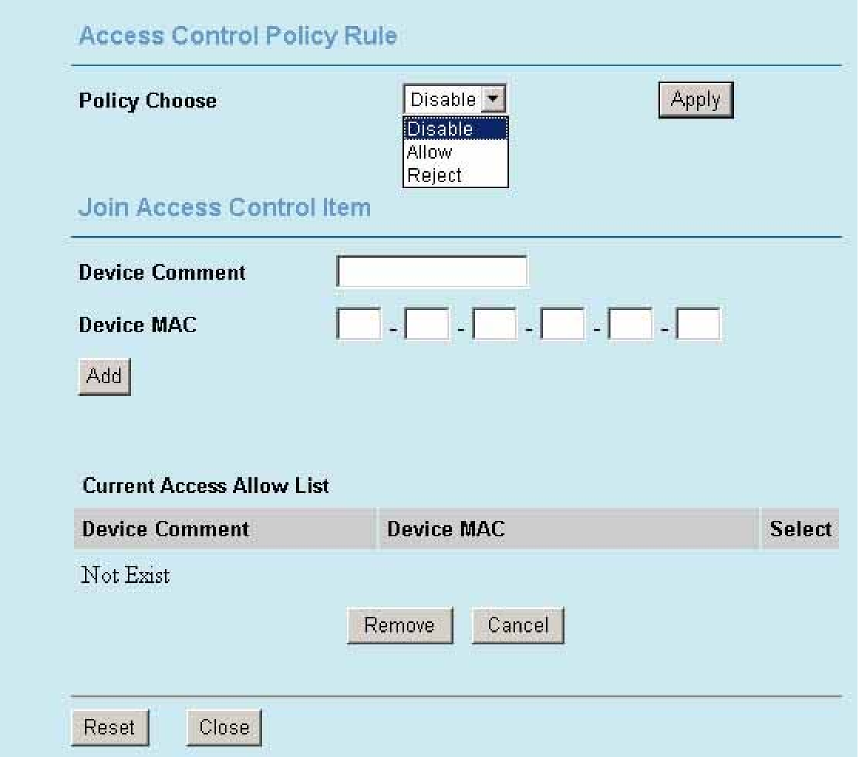
SSID of Extended Interface:

Alias Name	The distinguishing name of this device, you may change the default alias name by entering a new one in this column.
□ 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.
Repeater Type	You can choose WDS Repeater or Universal Repeater mode
Band	Choose a mode from the pull-down list. • 11b/g mixed: Select to allow both wireless-b and wireless-g devices on the network. • 11B only: Select to allow only wireless-B devices on the network. • 11G only: Select to allow only wireless-G devices on the network. • 11A (indoor): Select to allow only wireless-A devices on the indoor

	network. • 11A (outdoor): Select to allow only wireless-G devices on the network. • 11A (indoor): Select to allow only wireless-A devices on the outdoor network.
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	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.
SSID of extended interface	If you choose the Universal Repeater mode This filed just can let you fill in the SSID of extended interface, the SSID can be the same with this device or not; **please make sure the remote AP/Router WDS function is turned off.**
Advanced Settings	Same as the Bridge mode.
Security	Same as the Bridge mode
Access Control	Please see details as below :
WDS Control	Same as the Bridge mode

Access Control (Repeater mode)

You can define the Access Control Policy Rule , to allow or reject those clients whose wireless MAC addresses listed in the access control list can /or can’t access this Access Point.



Access Control Policy Rule

Policy Choose: Disable

Join Access Control Item

Device Comment

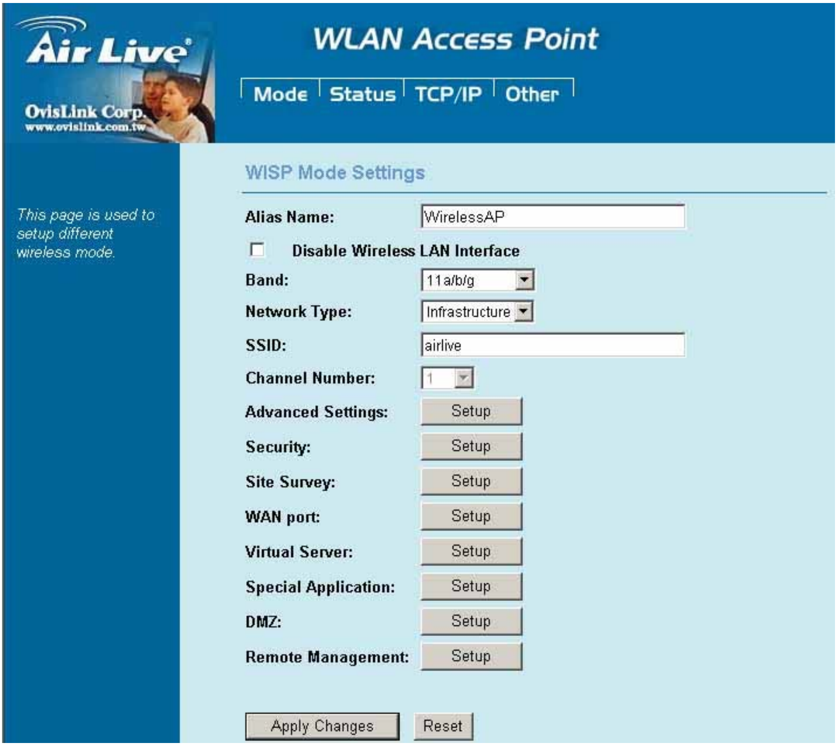
Device MAC - - - - -

Current Access Allow List

Device Comment	Device MAC	Select
Not Exist		

Policy Choose	Select the Access Control Mode from the pull-down menu. **Disable**: Select to disable Wireless Access Control Mode. **Allow**: Only the stations shown in the table can associate with the AP. **Reject**: Stations shown in the table won't be able to associate with the AP.
Device Comment	You may enter up to 20 characters as a remark to the previous MAC Address.
Device MAC	Enter the MAC Address of a station that is allowed to access this Access Point.
Add	Press add the Device to the Access Allow list
Remove	To Remove clients from access to this Access Point, you may firstly check the **Select** checkbox next to the MAC address and Comments, and press **Remove**
Reset	Press to discard the data you have entered since last time you press Apply Change.
Close	Close this window .

WISP mode Settings



This page is used to setup different wireless mode.

WISP Mode Settings

Alias Name: WirelessAP

□ Disable Wireless LAN Interface

Band: 11a/b/g

Network Type: Infrastructure

SSID: airlive

Channel Number: 1

Advanced Settings: Setup

Security: Setup

Site Survey: Setup

WAN port: Setup

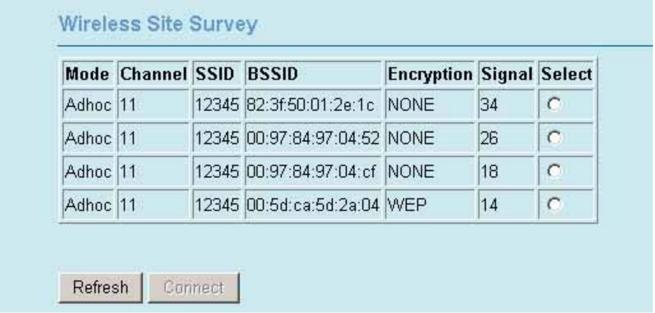
Virtual Server: Setup

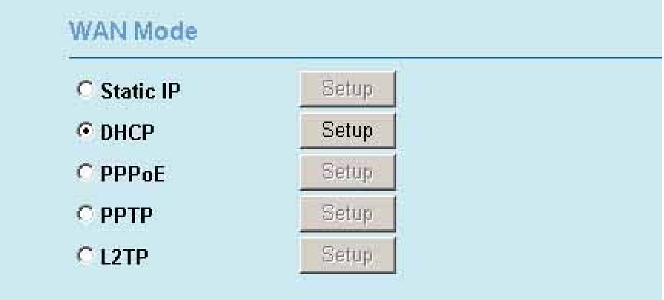
Special Application: Setup

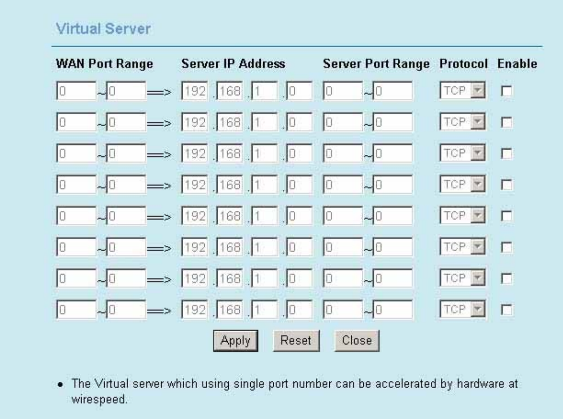
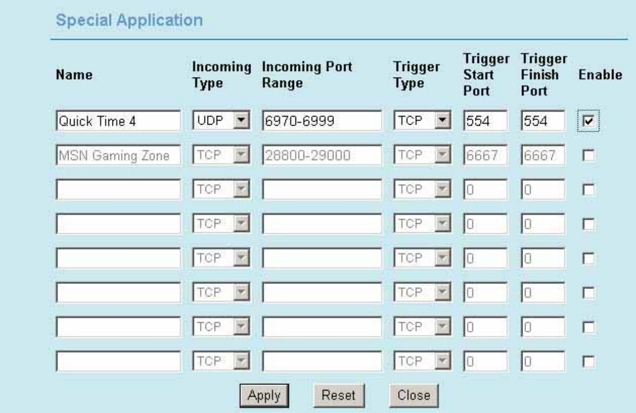
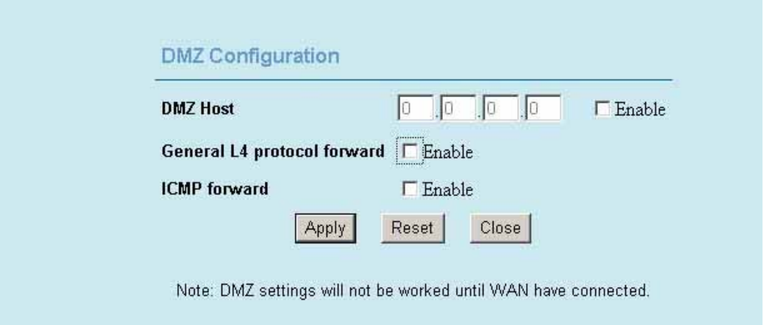
DMZ: Setup

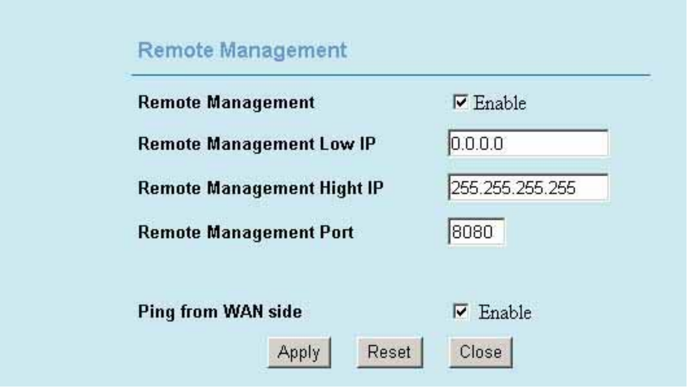
Remote Management: Setup

Alias Name	The distinguishing name of this device, you may change the default alias name by entering a new one in this column.
□ 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	Choose a mode from the pull-down list. • 11b/g mixed: Select to allow both wireless-b and wireless-g devices on the network. • 11B only: Select to allow only wireless-B devices on the network. • 11G only: Select to allow only wireless-G devices on the network. • 11A (indoor): Select to allow only wireless-A devices on the indoor network. • 11A (outdoor): Select to allow only wireless-G devices on the network. • 11A (indoor): Select to allow only wireless-A devices on the outdoor network.

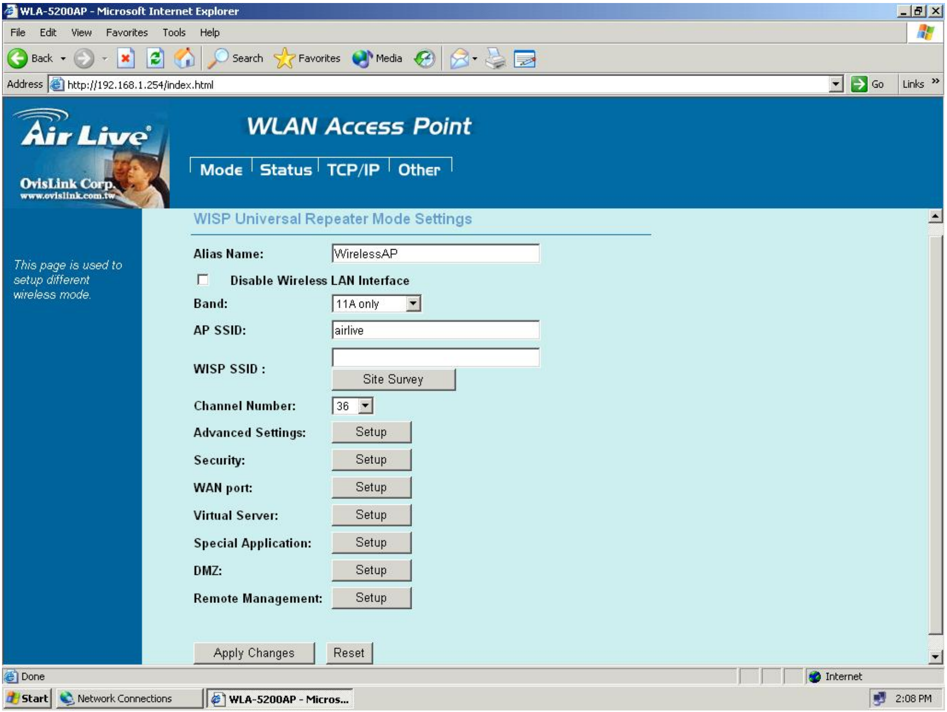
<table>
<tr><td><b>Network Type</b></td><td>You can choose the Ad-Hoc mode and Infrastructure mode</td></tr>
<tr><td><b>SSID</b></td><td>The SSID differentiates one WLAN from another; therefore, all access points and all devices attempting to connect to a specific WLAN must use the same SSID. It is case-sensitive 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.</td></tr>
<tr><td><b>Channel Number</b></td><td>Allow user to set the channel <b>manually</b> or <b>automatically</b>.
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.</td></tr>
<tr><td><b>Advance Settings</b></td><td>Same as the AP/Client mode</td></tr>
<tr><td><b>Security</b></td><td>Same as the AP/Client mode’s Security settings</td></tr>
<tr><td><b>Site Survey</b></td><td>
Wireless Site Survey
<table>
<tr><th>Mode</th><th>Channel</th><th>SSID</th><th>BSSID</th><th>Encryption</th><th>Signal</th><th>Select</th></tr>
<tr><td>Adhoc</td><td>11</td><td>12345</td><td>82:3f:50:01:2e:1c</td><td>NONE</td><td>34</td><td>○</td></tr>
<tr><td>Adhoc</td><td>11</td><td>12345</td><td>00:97:84:97:04:52</td><td>NONE</td><td>26</td><td>○</td></tr>
<tr><td>Adhoc</td><td>11</td><td>12345</td><td>00:97:84:97:04:cf</td><td>NONE</td><td>18</td><td>○</td></tr>
<tr><td>Adhoc</td><td>11</td><td>12345</td><td>00:5d:ca:5d:2a:04</td><td>WEP</td><td>14</td><td>○</td></tr>
</table>

Click site survey setup button that will shows the WISP Outdoor AP list and you can select which WISP AP you want to connect .</td></tr>
<tr><td><b>WAN Port</b></td><td>
WAN Mode
○ Static IP Setup
● DHCP Setup
○ PPPoE Setup
○ PPTP Setup
○ L2TP Setup
You can choose the different WAN mode , like Static IP, DHCP,PPPOE,PPTP or L2TP method.</td></tr>
</table>

Virtual Server	 Virtual Server WAN Port Range / Server IP Address / Server Port Range / Protocol / Enable 0 ~0 ==> 192 .168 .1 .0 0 ~0 TCP □ 0 ~0 ==> 192 .168 .1 .0 0 ~0 TCP □ 0 ~0 ==> 192 .168 .1 .0 0 ~0 TCP □ 0 ~0 ==> 192 .168 .1 .0 0 ~0 TCP □ 0 ~0 ==> 192 .168 .1 .0 0 ~0 TCP □ 0 ~0 ==> 192 .168 .1 .0 0 ~0 TCP □ 0 ~0 ==> 192 .168 .1 .0 0 ~0 TCP □ 0 ~0 ==> 192 .168 .1 .0 0 ~0 TCP □ Apply Reset Close • The Virtual server which using single port number can be accelerated by hardware at wirespeed. Define virtual server ip address and port range, Protocol and check the box to enable virtual server, The Virtual server which using single port number can be accelerated by hardware at wirespeed
Special Application	 Special Application Name / Incoming Type / Incoming Port Range / Trigger Type / Trigger Start Port / Trigger Finish Port / Enable Quick Time 4 / UDP / 6970-6999 / TCP / 554 / 554 / ☑ MSN Gaming Zone / TCP / 28800-29000 / TCP / 6667 / 6667 / □ / TCP / / TCP / 0 / 0 / □ / TCP / / TCP / 0 / 0 / □ / TCP / / TCP / 0 / 0 / □ / TCP / / TCP / 0 / 0 / □ / TCP / / TCP / 0 / 0 / □ / TCP / / TCP / 0 / 0 / □ Apply Reset Close You can define special application that can allow outside users to access your internal application behind this AP, like QuickTime ,MSN gaming zone…
DMZ	 DMZ Configuration DMZ Host 0 .0 .0 .0 □ Enable General L4 protocol forward □ Enable ICMP forward □ Enable Apply Reset Close Note: DMZ settings will not be worked until WAN have connected. DMZ settings will not be worked until WAN have connected

Remote Mangement	 Remote Management Remote Management ☑ Enable Remote Management Low IP 0.0.0.0 Remote Management Hight IP 255.255.255.255 Remote Management Port 8080 Ping from WAN side ☑ Enable Apply Reset Close You can enable the Remote management function and define the port number let can be managed from internet .

WISP + Universal Repeater Mode Setting



WLA-5200AP - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.1.254/index.html
Go Links
Air Live
OvisLink Corp.
www.ovislink.com.tw
WLAN Access Point
Mode Status TCP/IP Other
This page is used to setup different wireless mode.
Done
Internet
Start Network Connections WLA-5200AP - Micros...
2:08 PM

WISP Universal Repeater Mode Settings

Alias Name: WirelessAP

☐ Disable Wireless LAN Interface

Band: 11A only

AP SSID: airlive

WISP SSID :

Site Survey

Channel Number: 36

Advanced Settings: Setup

Security: Setup

WAN port: Setup

Virtual Server: Setup

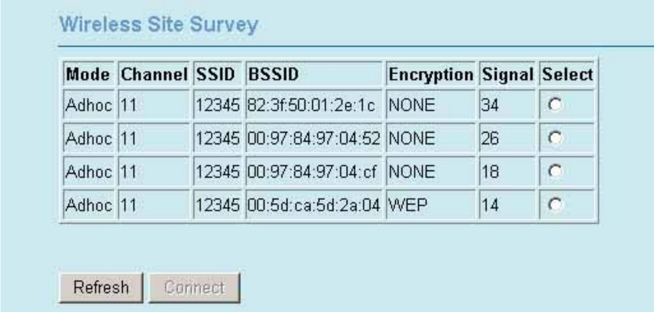
Special Application: Setup

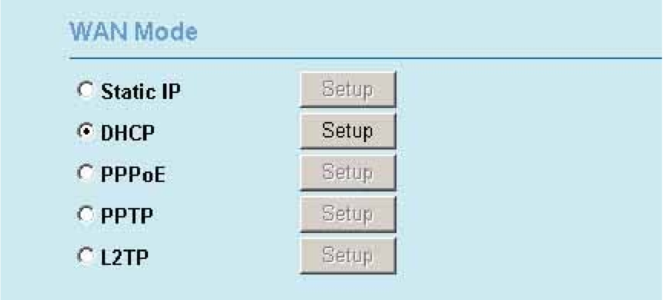
DMZ: Setup

Remote Management: Setup

Apply Changes Reset

Alias Name	You can set the alias name for this device (not exceeding 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. • 11b/g mixed: Select to allow both wireless-b and wireless-g devices on the network. • 11B only: Select to allow only wireless-B devices on the network. • 11G only: Select to allow only wireless-G devices on the network. • 11A (indoor): Select to allow only wireless-A devices on the indoor network. • 11A (outdoor): Select to allow only wireless-G devices on the network. • 11A (indoor): Select to allow only wireless-A devices on the outdoor network.
AP 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
WISP 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.

<table>
<tr><td><b>Site Survey</b></td><td>
Wireless Site Survey
<table>
<tr><th>Mode</th><th>Channel</th><th>SSID</th><th>BSSID</th><th>Encryption</th><th>Signal</th><th>Select</th></tr>
<tr><td>Adhoc</td><td>11</td><td>12345</td><td>82:3f:50:01:2e:1c</td><td>NONE</td><td>34</td><td>○</td></tr>
<tr><td>Adhoc</td><td>11</td><td>12345</td><td>00:97:84:97:04:52</td><td>NONE</td><td>26</td><td>○</td></tr>
<tr><td>Adhoc</td><td>11</td><td>12345</td><td>00:97:84:97:04:cf</td><td>NONE</td><td>18</td><td>○</td></tr>
<tr><td>Adhoc</td><td>11</td><td>12345</td><td>00:5d:ca:5d:2a:04</td><td>WEP</td><td>14</td><td>○</td></tr>
</table>

Click site survey setup button that will shows the WISP Outdoor AP list and you can select which WISP AP you want to connect .</td></tr>
<tr><td><b>Security</b></td><td>Please refer the AP mode settings→ Security for details,
This setting used Wireless client or remote AP to link this device.</td></tr>
<tr><td><b>Advance Setting</b></td><td>Please refer the AP mode settings→ Advance Setting for details.</td></tr>
<tr><td><b>Access Control</b></td><td>Please refer the AP mode setting → Access Control for details.</td></tr>
<tr><td><b>WAN Port</b></td><td>
WAN Mode

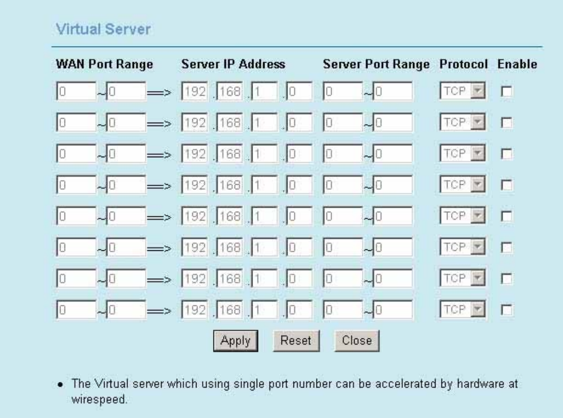
○ Static IP

● DHCP

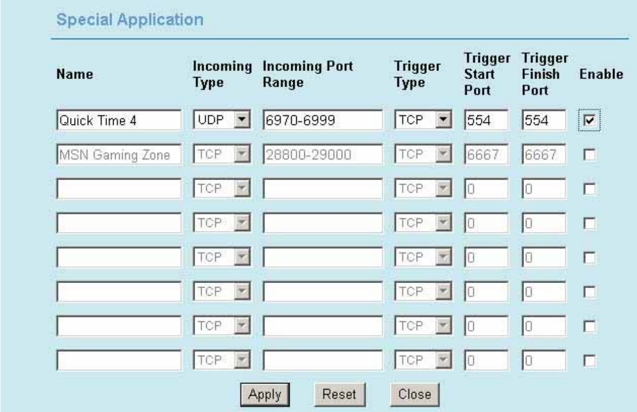
○ PPPoE

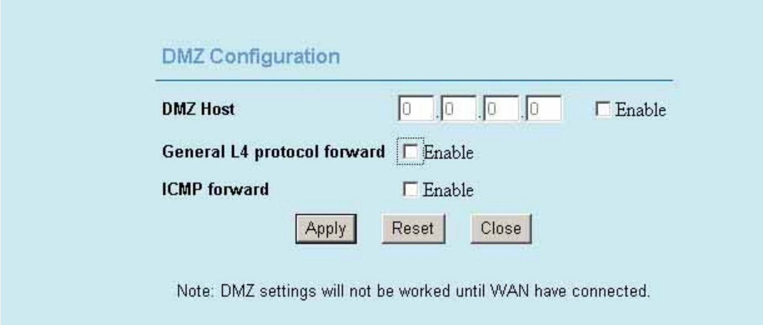
○ PPTP

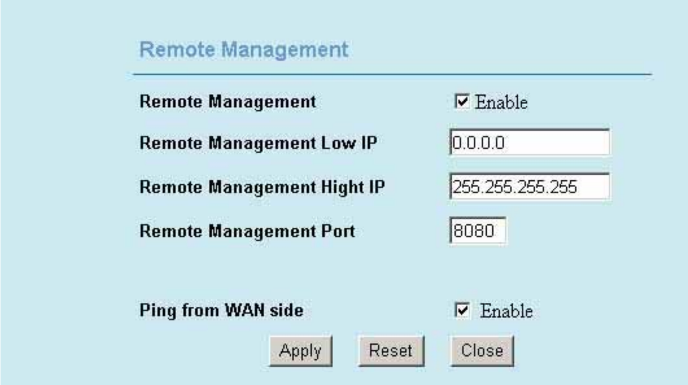
○ L2TP

You can choose the different WAN mode , like Static IP, DHCP,PPPOE,PPTP or L2TP method.</td></tr>
<tr><td><b>Virtual Server</b></td><td>
Virtual Server
<table>
<tr><th>WAN Port Range</th><th></th><th>Server IP Address</th><th>Server Port Range</th><th>Protocol</th><th>Enable</th></tr>
<tr><td>0 ~ 0</td><td>==&gt;</td><td>192 .168 .1 .0</td><td>0 ~ 0</td><td>TCP</td><td>☐</td></tr>
<tr><td>0 ~ 0</td><td>==&gt;</td><td>192 .168 .1 .0</td><td>0 ~ 0</td><td>TCP</td><td>☐</td></tr>
<tr><td>0 ~ 0</td><td>==&gt;</td><td>192 .168 .1 .0</td><td>0 ~ 0</td><td>TCP</td><td>☐</td></tr>
<tr><td>0 ~ 0</td><td>==&gt;</td><td>192 .168 .1 .0</td><td>0 ~ 0</td><td>TCP</td><td>☐</td></tr>
<tr><td>0 ~ 0</td><td>==&gt;</td><td>192 .168 .1 .0</td><td>0 ~ 0</td><td>TCP</td><td>☐</td></tr>
<tr><td>0 ~ 0</td><td>==&gt;</td><td>192 .168 .1 .0</td><td>0 ~ 0</td><td>TCP</td><td>☐</td></tr>
<tr><td>0 ~ 0</td><td>==&gt;</td><td>192 .168 .1 .0</td><td>0 ~ 0</td><td>TCP</td><td>☐</td></tr>
<tr><td>0 ~ 0</td><td>==&gt;</td><td>192 .168 .1 .0</td><td>0 ~ 0</td><td>TCP</td><td>☐</td></tr>
</table>

- The Virtual server which using single port number can be accelerated by hardware at wirespeed.
</td><td>Define virtual server ip address and port range, Protocol
and check the box to enable virtual server,
The Virtual server which using single port number can be accelerated by hardware at wire-speed.</td></tr>
</table>

<table>
<tr>
<td><b>Special Application</b></td>
<td>

Special Application
<table>
<tr><th>Name</th><th>Incoming Type</th><th>Incoming Port Range</th><th>Trigger Type</th><th>Trigger Start Port</th><th>Trigger Finish Port</th><th>Enable</th></tr>
<tr><td>Quick Time 4</td><td>UDP</td><td>6970-6999</td><td>TCP</td><td>554</td><td>554</td><td>☑</td></tr>
<tr><td>MSN Gaming Zone</td><td>TCP</td><td>28800-29000</td><td>TCP</td><td>6667</td><td>6667</td><td>□</td></tr>
<tr><td></td><td>TCP</td><td></td><td>TCP</td><td>0</td><td>0</td><td>□</td></tr>
<tr><td></td><td>TCP</td><td></td><td>TCP</td><td>0</td><td>0</td><td>□</td></tr>
<tr><td></td><td>TCP</td><td></td><td>TCP</td><td>0</td><td>0</td><td>□</td></tr>
<tr><td></td><td>TCP</td><td></td><td>TCP</td><td>0</td><td>0</td><td>□</td></tr>
<tr><td></td><td>TCP</td><td></td><td>TCP</td><td>0</td><td>0</td><td>□</td></tr>
<tr><td></td><td>TCP</td><td></td><td>TCP</td><td>0</td><td>0</td><td>□</td></tr>
</table>

You can define special application that can allow outside users to access your internal application behind this AP, like QuickTime ,MSN gaming zone…
</td>
</tr>
<tr>
<td><b>DMZ</b></td>
<td>

DMZ Configuration
DMZ Host 0 . 0 . 0 . 0 □ Enable
General L4 protocol forward □ Enable
ICMP forward □ Enable

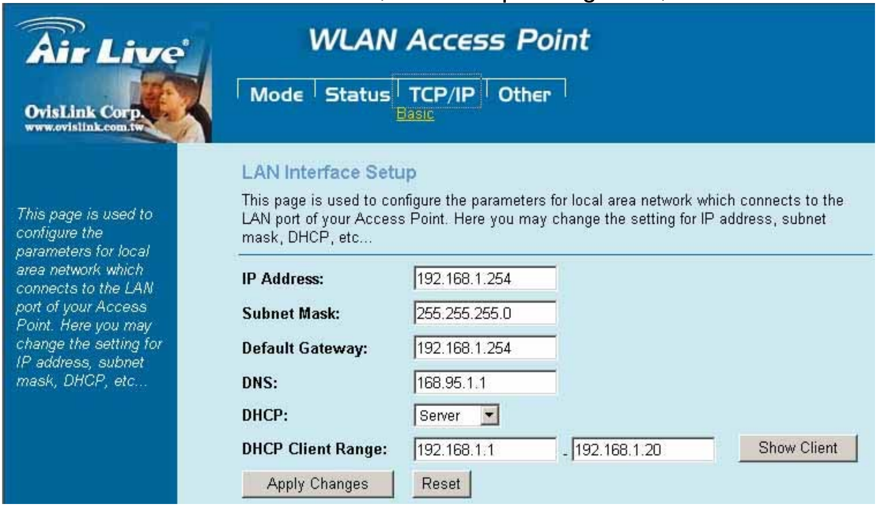
Note: DMZ settings will not be worked until WAN have connected.
DMZ settings will not be worked until WAN have connected
</td>
</tr>
<tr>
<td><b>Remote Mangement</b></td>
<td>

Remote Management
Remote Management ☑ Enable
Remote Management Low IP 0.0.0.0
Remote Management Hight IP 255.255.255.255
Remote Management Port 8080
Ping from WAN side ☑ Enable

You can enable the Remote management function and define the port
number let can be managed from internet
</td>
</tr>
</table>

TCP/IP

Basic

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.



LAN Interface Setup

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...

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: 192.168.1.254

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.254

DNS: 168.95.1.1

DHCP: Server

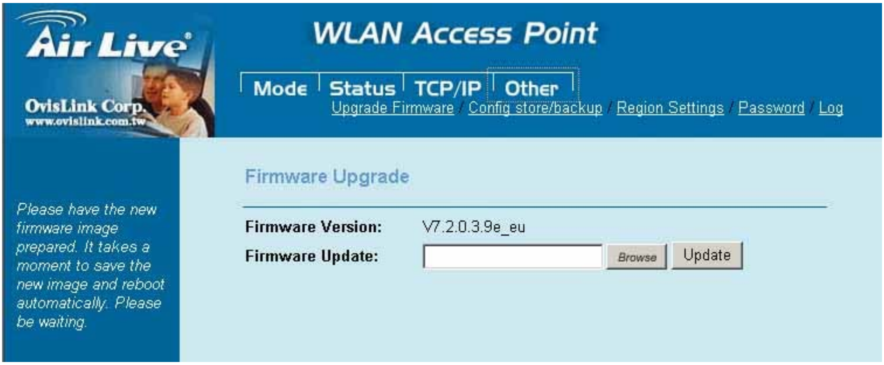
DHCP Client Range: 192.168.1.1 - 192.168.1.20

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.
DNS	Enter the Domain Name Service IP address.
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	253 IP addresses continuing from 192.168.1.1 to 192.168.1.253
Show Client	Click to show Active DHCP Client table.
Clone MAC Address	You can specify the MAC address of your Access Point to replace the factory setting.

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.

Other

Upgrade Firmware


WLAN Access Point
Mode
Status
TCP/IP
Other
Upgrade Firmware / Config store/backup / Region Settings / Password / Log
Browse
Update

Please have the new firmware image prepared. It takes a moment to save the new image and reboot automatically. Please be waiting.

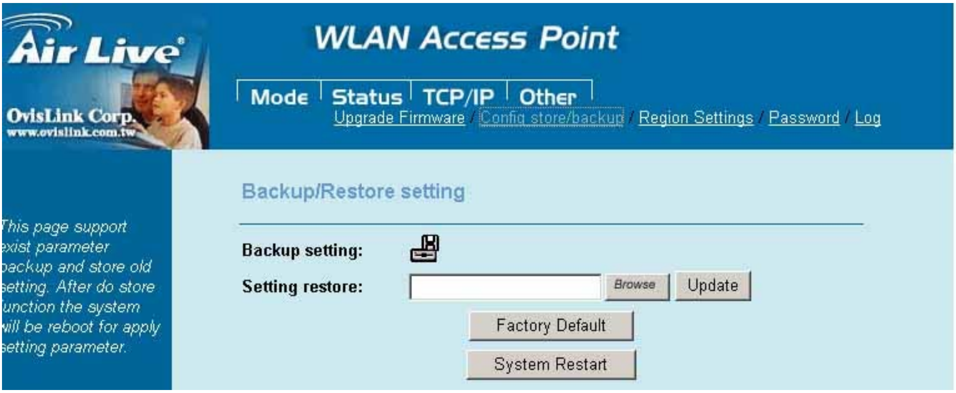
Firmware Upgrade

Firmware Version: V7.2.0.3.9e_eu

Firmware Update:

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. Enter the new firmware's path and file name (i.e. C:\FIRMWARE\firmware.bin). Or, click the **Browse** button, find and open the firmware file (the browser will display to correct file path).
3. Click **Update** to start the upgrade.

Backup/Restore Settings



This page support exist parameter backup and store old setting. After do store unction the system will be reboot for apply setting parameter.

Backup/Restore setting

Backup setting:

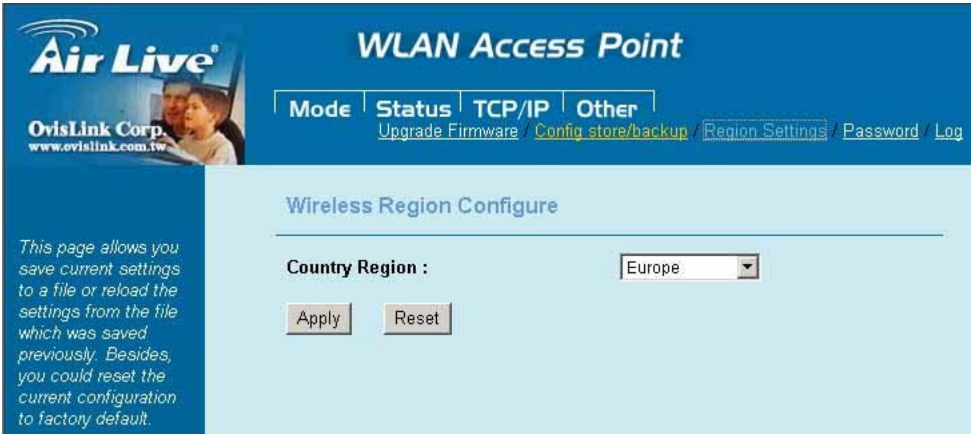
Setting restore:

This function enables users to save the current configuration~~s~~ as a file (i.e. **config.bin**) To load configuration from a file, enter the file name or click **Browse…** to find the file from your computer.anc click update button .

Factory Default: Click to restore the default configuration.

System Restart Click to restart the device.

Region Settings



Wireless Region Configure

Country Region : Europe

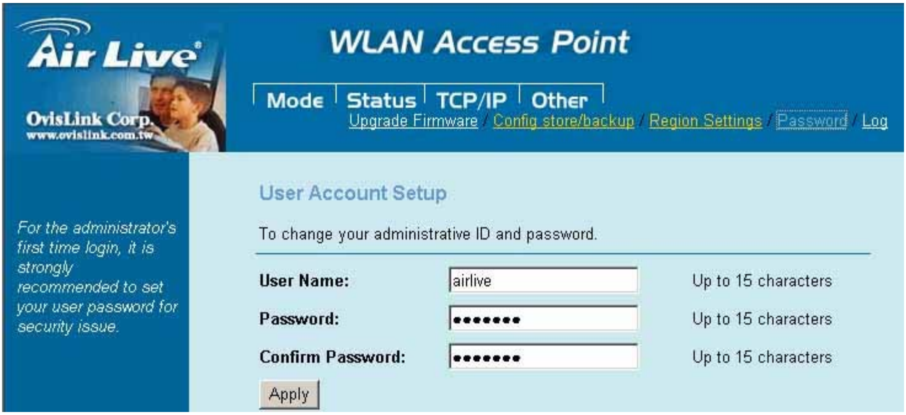
This page allows you save current settings to a file or reload the settings from the file which was saved previously. Besides, you could reset the current configuration to factory default.

You can select your country region : Europe, America, South America

Note !! Select the Country Region will affect the each Channel number of each Wireless mode.

Password

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



For the administrator's first time login, it is strongly recommended to set your user password for security issue.

User Account Setup

To change your administrative ID and password.

User Name:	airlive	Up to 15 characters
Password:	•••••••	Up to 15 characters
Confirm Password:	•••••••	Up to 15 characters

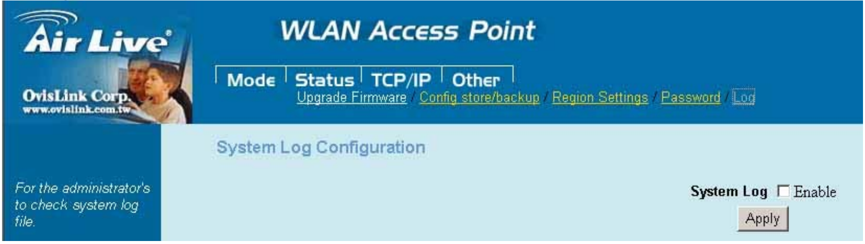
Apply

User Name	Set your new User name. User name can be up to 15 characters long. User name can contain letter, number and space. It is case sensitive.
Password	Set your new password. Password can be up to 15 characters long. Password can contain letter, number and space. It is case sensitive.
Confirm Password	Re-enter the new password for confirmation.
Apply	Press to save the new settings on the screen.

System Log

This page display log events with time when events happened, log events' types, log sources and the description for events themselves. System manager can use the system log to trace when problems occur.

Check to enable the system log function and then click **Apply** to save your configuration.



For the administrator's to check system log file.

System Log Configuration

System Log □ Enable

Apply