Air Live®
Powered by OvisLink Corp.

WLA-9000AP

108Mbps 802.11a/b/g
Dual Radio Access Point

User's Manual

Copyright & Disclaimer

OvisLink Corp. has made the best effort to ensure the accuracy of the information in this user's guide. However, we are not liable for the inaccuracies or errors in this guide. Please use with caution. All information is subject to change without notice

This product require professional installation. Please do not attemp to install the device witho the necessary knowledge in regards to your country's wireless regulations

Regulatory Information

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: To assure continued compliance, (example - use only shielded interface cables when connecting to computer or peripheral devices) any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this 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.

For product available in the USA/Canada market, only channel 1~11 can be operated.

Selection of other channels is not possible.

IMPORTANT NOTE

FCC Radiation Exposure Statement:

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

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

FCC NOTICE: To comply with FCC part 15 rules in the United States, the system must be professionally installed to ensure compliance with the Part 15 certification. It is the responsibility of the operator and professional installer to ensure that only certified systems are deployed in the United States. The use of the system in any other combination (such as co-located antennas transmitting the same information) is expressly forbidden.

Table of Contents

1 Introduction

1.1 Overview

The WLA-9000AP is a wireless access-point based on IEEE 802.11a/g 5-GHz and 2.4-GHz radio technologies. It contains an 802.11a/g wireless interface and one half/full-duplex 10/100 LAN interface WLA-9000AP, with the new 2.0 firmware, features a total of 6 wireless modes: Access Point, Repeater, WDS Bridge, Client Infrastructure, Client Ad Hoc and WISP Router.

Since the 802.11g shares the same 2.4GHz radio band with the 802.11b technology, it can interoperate with existing 802.11b (up to 11Mbps) devices. Therefore, you can reserve your existing investment in 802.11b client cards, and migrate to the high-speed 802.11g standard as your needs grow.

To address growing security concerns in a wireless LAN environment, different levels of security can be enabled in WLA-9000AP:

- To disable SSID broadcast to restrict association to only those client stations that are already pre-configured with the correct SSID
- To enable WEP (Wireless Encryption Protocol) 64, 128, or 152-bit encryption to protect the privacy of your data.
- Support of Access List Control to allow you to grant/deny access to/from specified wireless stations
- Provisioning of centralized authentication through RADIUS Server.
- WPA-PSK (Wi-Fi Protected Access, Pre-Shared Key) for home users to provide authentication, data integrity, and data privacy.

WPA (Wi-Fi Protected Access) works with a RADIUS server to provide stronger authentication as well as data integrity and privacy.

1.2 How to Use This Guide

WLA-9000AP is an advanced wireless Base Station with many functions. It is recommended that you read through the entire user's guide whenever possible. The user guide is divided into different chapters. You should read at least go through the first 3 chapters before attempting to install the device.

Recommended Reading

Chapter 1: This chapter explains the basic information for WLA-9000AP. It is a must read.

Chapter 2: This chapter is about hardware installation. You should read through the entire chapter.

Chapter 3:

- **3.1 Important Information**: This section has information of default setting such as IP, Username, and Password.
- **3.3 Management Interface**: This section introduces Web management, and Console management.
- **3.4 Introduction to Web Management**: This section tells you how to get into the WebUI using HTTP.
- **3.5 Initial Configuration**: This section guide you through the essential initial configurations such as choosing operation mode, set device IP, password, and change frequency domain.

Chapter 4: This chapter explains Wireless and WAN settings via Web management.

Chapter 5: This chapter explains System Configuration via Web management and System Status.

Chapter 6: This chapter explains all of the management functions via CLI.

If any trouble in using WLA-9000AP, you can refer to this chapter

Chapter 7~15: Each chapter explains how to configure one Wireless mode for your application.

Chapter 16: If you have a question about WLA-9000AP that is not found on other part of this manual, you might find your answer here.

Chapter 17: This chapter explains technical specification of WLA-9000AP.

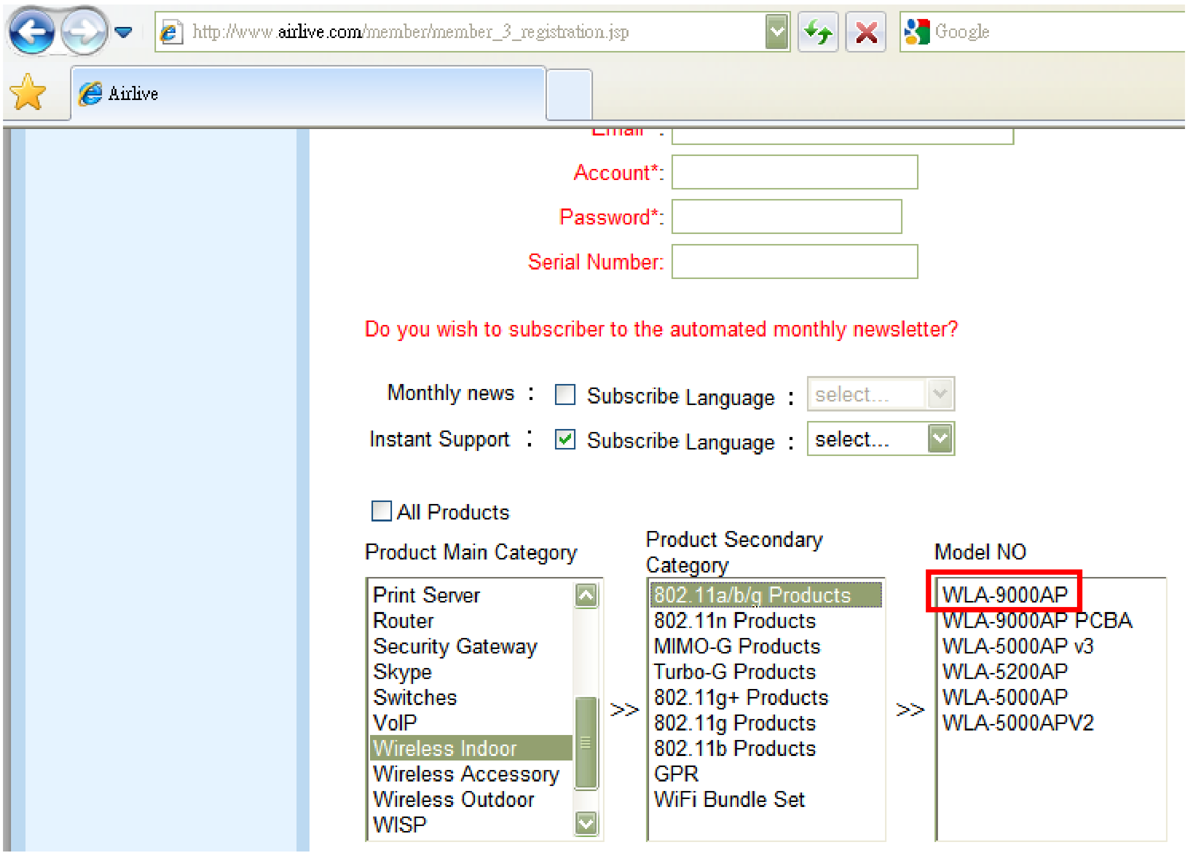
Chapter 18: Explanation on network technical terms from A to Z. Highly recommended for reference when you encounter an unfamiliar term.

1.3 Firmware Upgrade and Tech Support

If you encounter a technical issue that can not be resolved by information on this guide, we recommend that you visit our comprehensive website support at www.airlive.com. The tech support FAQ are frequently updated with latest information.

In addition, you might find new firmwares that either increase software functions or provide bug fixes for WLA-9000AP. You can reach our on-line support center at the following link: http://www.airlive.com/support/support_2.jsp

Since 2009, AirLive has added the “Newsletter Instant Support System” on our website. AirLive Newsletter subscribers receives instant email notifications when there are new download or tech support FAQ updates for their subscribed AirLive models. To become an AirLive newsletter member, please visit: http://www.airlive.com/member/member_3.jsp



http://www.airlive.com/member/member_3_registration.jsp

Airlive

Email :

Account*:

Password*:

Serial Number:

Do you wish to subscriber to the automated monthly newsletter?

Monthly news ： □ Subscribe Language ： select...

Instant Support ： ☑ Subscribe Language ： select...

□ All Products

Product Main Category >> Product Secondary Category >> Model NO

Product Main Category:
Print Server
Router
Security Gateway
Skype
Switches
VoIP
Wireless Indoor
Wireless Accessory
Wireless Outdoor
WISP

Product Secondary Category:
802.11a/b/g Products
802.11n Products
MIMO-G Products
Turbo-G Products
802.11g+ Products
802.11g Products
802.11b Products
GPR
WiFi Bundle Set

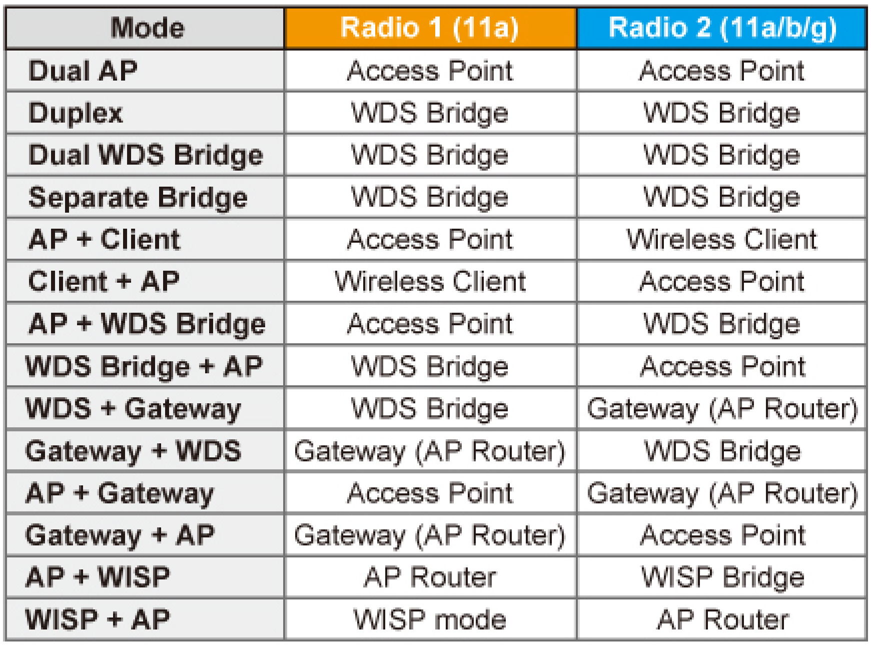
Model NO:
WLA-9000AP
WLA-9000AP PCBA
WLA-5000AP v3
WLA-5200AP
WLA-5000AP
WLA-5000APV2

1.4 Feature

- Compliant with 802.11a, 802.11b and 802.11g, Super A™ and Super G™ standards with roaming capability.
- Dual Wireless interfaces support multi-function modes: Dual Access Point, Dual WDS Bridge, AP + Client Infrastructure, AP + WDS mode.
- Static assignment or DHCP client to set the device IP address.
- Multiple security measures: SSID hiding, Access Control List, WEP based encryption (64, 128, 152 bits), enhanced Security with 802.1x using a primary and a backup RADIUS Server with/without dynamic WEP keys, WPA-PSK, WPA, and WPA2.
- Extensive monitoring capability such as event logging, traffic/error statistics monitoring.
- Easy configuration and monitoring through the use of a Web-browser based GUI with predefined operation mode. SNMP commands from a remote SNMP management station and UPnP for users to automatically discover the device.
- Setup Wizard for easy configuration/installation.
- Configuration file download and restore.
- Firmware upgradeable for flexibility to add extra features.

1.5 Wireless Operation Modes

The WLA-9000AP device provides all 14 modes of wireless operational applications with:



Mode	Radio 1 (11a)	Radio 2 (11a/b/g)
Dual AP	Access Point	Access Point
Duplex	WDS Bridge	WDS Bridge
Dual WDS Bridge	WDS Bridge	WDS Bridge
Separate Bridge	WDS Bridge	WDS Bridge
AP + Client	Access Point	Wireless Client
Client + AP	Wireless Client	Access Point
AP + WDS Bridge	Access Point	WDS Bridge
WDS Bridge + AP	WDS Bridge	Access Point
WDS + Gateway	WDS Bridge	Gateway (AP Router)
Gateway + WDS	Gateway (AP Router)	WDS Bridge
AP + Gateway	Access Point	Gateway (AP Router)
Gateway + AP	Gateway (AP Router)	Access Point
AP + WISP	AP Router	WISP Bridge
WISP + AP	WISP mode	AP Router

2 Installing the WLA-9000AP

This section describes the hardware features and the hardware installation procedure for the WLA-9000AP. For software configuration, please go to chapter 3 for more details.

2.2 Before You Start

It is important to read through this section before you install the WLA-9000AP.

- The WLA-9000AP comes with everything you need to start installation with exception of the PoE Ethernet Cable. You can use a good quality CAT-5E outdoor graded Ethernet cable (shielded with anti-UV) according to the length you need.
- The use of 5GHz spectrum, Turbo modes, and 5/10MHz channel bandwidth might be prohibited in some countries. Please consult with your country's telecom regulation first.
- You must set the distance parameter to make long distance connection work. Please refer to chapter 4 of this user's guide for details.

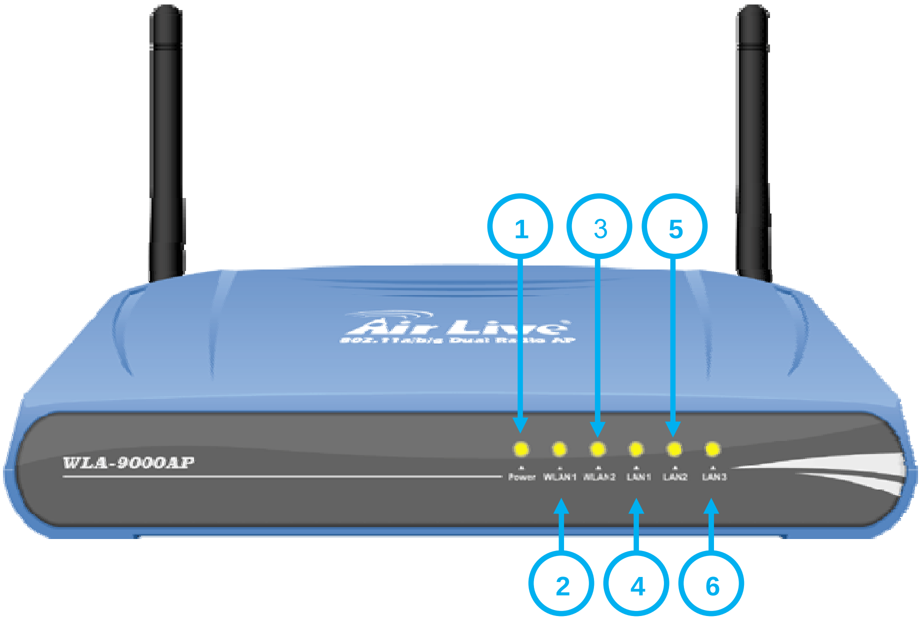
2.3 Installing WLA-9000AP

The WLA-9000AP package contains the following items:

- One WLA-9000AP main unit
- One 5.5V 2.5A DC power adapter
- Indoor detachable Omni Antenna x 2
- One CD of the WLA-9000AP Quick Start Guide

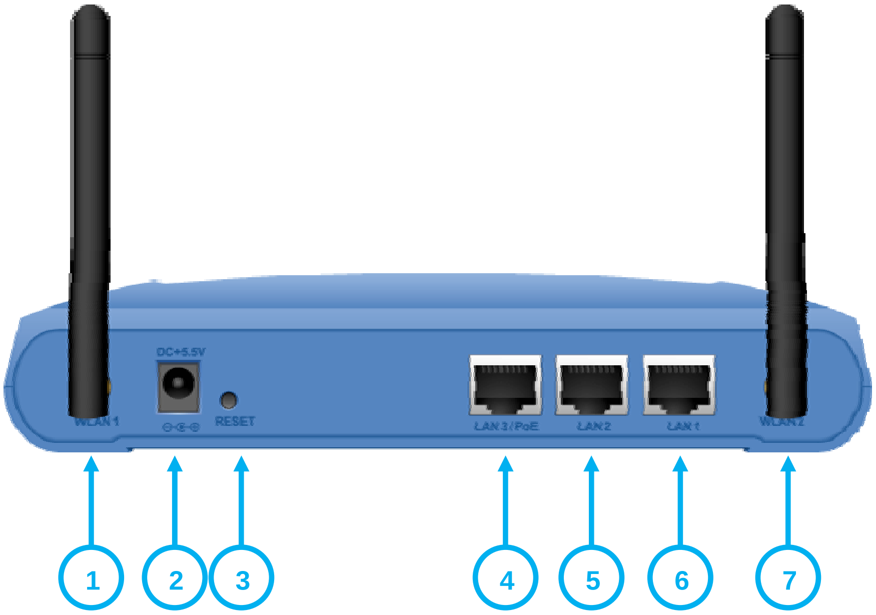
2.4 Knowing Your WLA-9000AP

2.4.1 Front side introduction



LED #	Display	Description
1	Power	Solid Green LED while the device is powered on, either by power adaptor or PoE.
2	WLAN1	Solid Green LED while the device is powered on. Blinking while there is Data transmission, dark when this interface is turn off.
3	WLAN2	
4	LAN 1	LAN ports status LED, Solid Green LED shows when a port is actively connected, blinking while there is data transmission, turns into dark when this disconnected.
5	LAN 2	
6	LAN 3	

2.4.2 Back side introduction



Port #	Display	Description
1	WLAN1	Detachable antenna with R-SMA connector. 2 indoor 2dBi antennas are delivered.
2	Power Adaptor	5.5V 2.5A power supply adaptor delivered with product.
3	RESET	Reset button for rebooting and reset device as default factory value.
4	LAN 3/PoE	LAN port 3 and PoE port. It can be plug 802.3af compliant PoE as power and data supply.
5	LAN 2	LAN port 2
6	LAN 1	LAN port 1
7	WLAN2	Detachable antenna with R-SMA connector.

2.5 Configuration steps

This section describes configuration required for the WLA-9000AP before it can work properly in your network.

Set up the device

The WLA-9000AP can be managed remotely by a PC through either the wired or wireless network. To do this, the WLA-9000AP must first be assigned an IP address, which can be done using one of the following 2 methods.

WLA-9000AP's Factory default value IP

The default IP address of the LAN interface of an WLA-9000AP is a *private IP address* of **192.168.1.1**, and a *network mask* of 255.255.255.0. This means IP addresses of other devices on the LAN should be in the range of 192.168.1.2 to 192.168.1.254.

This IP address can be modified to either a different address in this same subnet or to an address in a different subnet, depending on the existing network settings (if there is any) or user's preferences.

First, you need to perform various configuration changes to the WLA-9000AP, including the SSID, Channel number, the WEP key, …, etc., it is necessary to associate a fixed IP address with the WLA-9000AP, which is why the WLA-9000AP will be shipped with a factory default private IP address of **192.168.1.1** (and a network mask of 255.255.255.0).

Therefore, during the system installation time, you need to build an isolated environment with the WLA-9000AP and a PC, and then perform the following steps.

2.5.1 Set up a wired connection with Ethernet cable

In the case of using a LAN attached PC, the PC must have an Ethernet interface installed properly, be connected to the WLA-9000AP either directly or through an external LAN switch, and have TCP/IP installed and configured as fixed IP and same subnet mask scope as the AP.

Then perform the following steps for either of the cases above. To configure types of workstations other than Windows 95/98/NT/2000, please consult the manufacturer's documentation.

Step 1. From the Win95/98/2000 Start Button, select Settings, then Control Panel. The Win95/98/2000 Control Panel displays.

Step 2. Double-click on the *Network* icon.

Manually change the IP address of the PC to become 192.168.1.3. To do this , move your mouse and high light the node device (please go to your network device such as Ethernet card), right click on your mouse. Click **Properties,** and check the settings in each of the TCP/IP Properties window. Select fixed IP and assign the IP as 192.168.1.3 and subnet mask as 255.255.255.0.

Step 3. Once you have modified the PC's IP as same network scope as the default IP of WLA-9000AP, you can then open a browser and start to configure the AP by typing the default IP address into the URL line.

Please note that after you change the IP address of the ACCESS POINT, the PC client may not be able to reach the ACCESS POINT. This is because they may no longer belong to the same IP network address space.

2.5.2 Set up a wireless client as a fixed IP client

The following will give detailed steps of how to configure a PC or a wireless client to “obtain IP addresses automatically”.

In the case of using a wireless client, the client must also have an 802.11a/b/g wireless interface installed properly, be physically within the radio range of the WLA-9000AP, and have TCP/IP installed and configured as fixed IP and same subnet mask scope as the AP.

Then perform the following steps for either of the cases above. To configure types of workstations other than Windows 95/98/NT/2000, please consult the manufacturer’s documentation.

Step 1. From the Win95/98/2000 Start Button, select Settings, then Control Panel. The Win95/98/2000 Control Panel displays.

Step 2. Double-click on the *Network* icon.

Step 3. Check your list of Network Components in the Network window Configuration tab. If TCP/IP has already been installed, go to Step 8. Otherwise, select Add to install it now.

Step 4. In the new Network Component Type window, select Protocol. In the new Select Network Protocol window, select Microsoft in the Manufacturers area.

Step 5. In the Network Protocols area of the same window, select TCP/IP, then click OK. You may need your Win95/98 CD to complete the installation. After TCP/IP installation is complete, go back to the Network window described in Step 4.

Step 6. Select TCP/IP in the list of Network Components.

Step 7. Click **Properties,** and check the settings in each of the TCP/IP Properties window. Manually change the IP address of the PC to become 192.168.1.4 and Subnet mask as 255.255.255.0.

Step 8. With the WLA-9000AP powered on, reboot the PC/wireless client. After the PC/wireless client is re-booted, you should be ready to configure the WLA-9000AP. See Chapter 3.

The procedure required to set a static IP address is not too much different from the procedure required to set to “obtain IP addresses dynamically” - except that at the end of step 7, instead of selecting “obtain IP addresses dynamically, you should specify the IP address explicitly.

3 Configuring the WLA-9000AP

The WLA-9000AP offers many different types of management interface. You can configure through standard web browser (http), secured web (https), command line (telnet), secured command shell (SSH, SSH2), and SNMP management. In this chapter, we will explain WLA-9000AP's available management interfaces and how to get into them. Then, we will provide the introduction on Web Management and recommended initial settings.

3.1 Important Information

The following information will help you to get start quickly. However, we recommend you to read through the entire manual before you start. Please note the password and SSID are case sensitive.

Settings	**Default Value**	
	Wireless1	**Wireless2**
Device Name	WLA-9000AP	
Radio	802.11a	802.11a
SSID	airlive1	airlive2
Channel	36	36 (auto in 802.11b/g)
WEP	Disabled	
IP Address	192.168.1.1	
Subnet Mask	255.255.255.0	
DHCP Server	Disabled. Available and default enabled when each of the wireless is configured as a gateway.	
DHCP IP Range	192.168.1.2 ~ 192.168.1.254	
Access Password	airlive	

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.

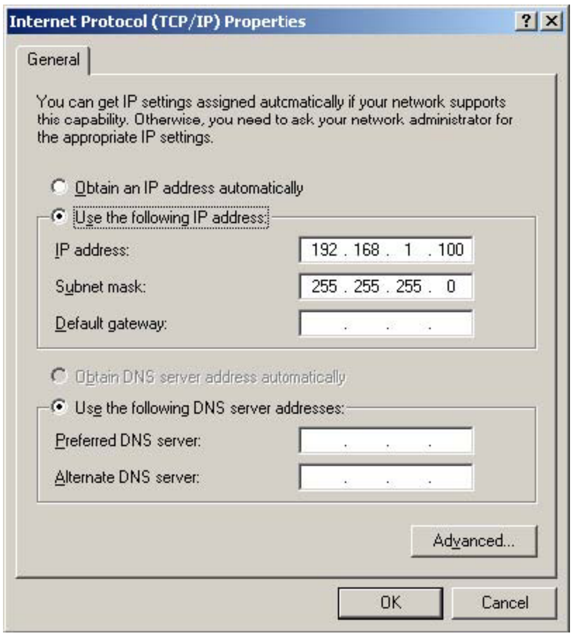
3.2 Prepare Your PC

The WLA-9000AP can be managed remotely by a PC through either the wired or wireless network. The default IP address of the WLA-9000AP is **192.168.1.1** with a *subnet mask* of 255.255.255.0. This means the IP address of the PC should be in the range of 192.168.1.2 to 192.168.1.254.

To prepare your PC for management with the WLA-9000AP, please do the following:

1. Connect your PC directly to the LAN port on the DC Injector of WLA-9000AP

2. Set your PC's IP address manually to 192.168.1.100 (or other address in the same subnet)



You can get IP settings assigned autcmatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 100

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

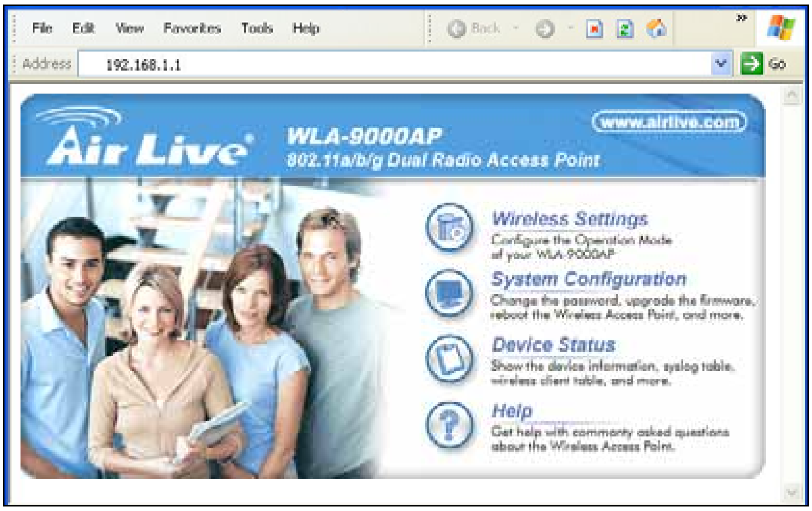
Alternate DNS server: . . .

You are ready now to configure the WLA-9000AP using your PC.

3.3 Management Interface

The WLA-9000AP can be configured using one the management interfaces below:

- **Web Management (HTTP):** You can manage your WLA-9000AP by simply typing its IP address in the web browser. Most functions of WLA-9000AP can be accessed by web management interface. We recommend using this interface for initial configurations. To begin, simply enter WLA-9000AP's IP address (default is 192.168.1.1) on the web browser. The default password is both "airlive".



WLA-9000AP
802.11a/b/g Dual Radio Access Point

Wireless Settings
Configure the Operation Mode of your WLA-9000AP

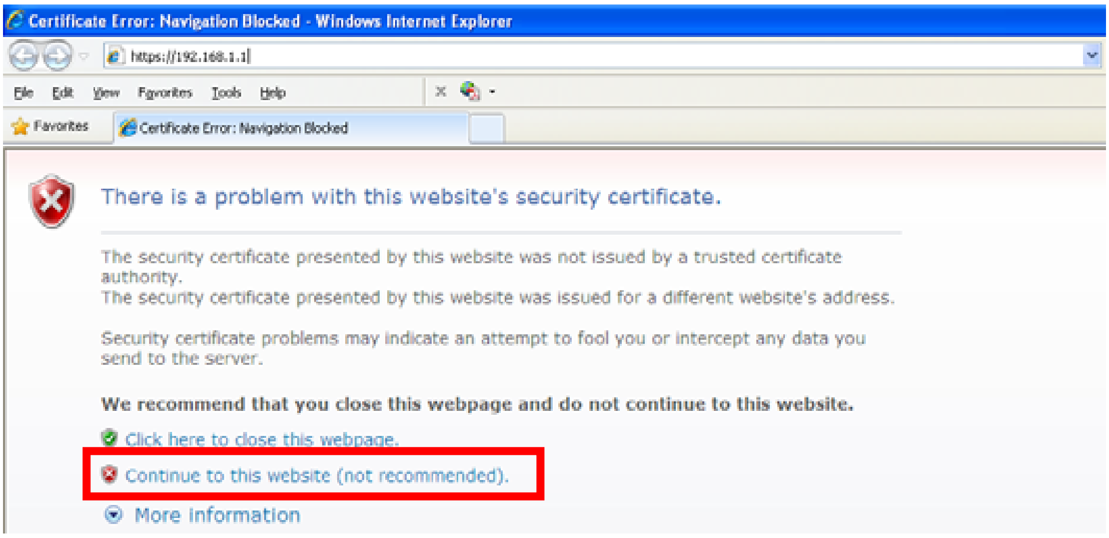
System Configuration
Change the password, upgrade the firmware, reboot the Wireless Access Point, and more.

Device Status
Show the device information, syslog table, wireless client table, and more.

Help
Get help with commonly asked questions about the Wireless Access Point.

- **Secured Web Management (HTTPS):** HTTPS is also using web browser for configuration. But all the data transactions are securely encrypted using SSL encryption. Therefore, it is a safe and easy way to manage your WLA-9000AP. We highly recommend WISP and service provider to use HTTPS for management.

  To begin, simply enter https://192.168.1.1 on your web browser. A security alert screen from your browser will pop up. Please click "Continue to this website" to login WLA-9000AP.


Certificate Error: Navigation Blocked - Windows Internet Explorer
https://192.168.1.1
File Edit View Favorites Tools Help
Favorites
Certificate Error: Navigation Blocked

There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

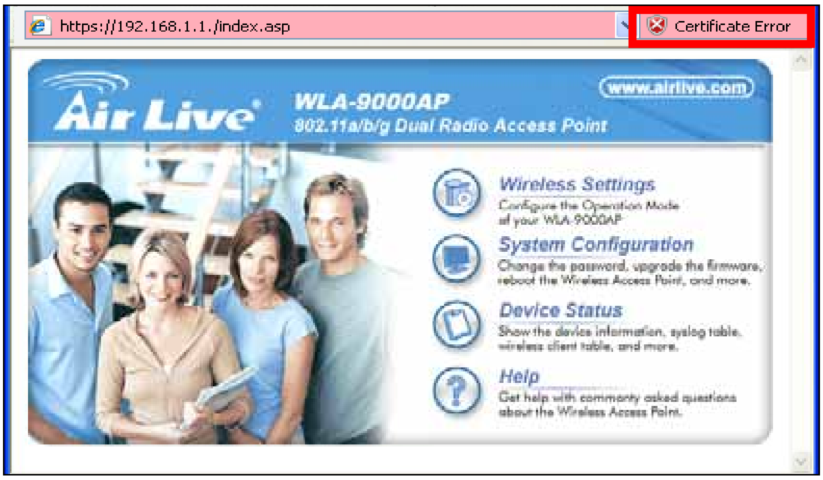
We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

More information

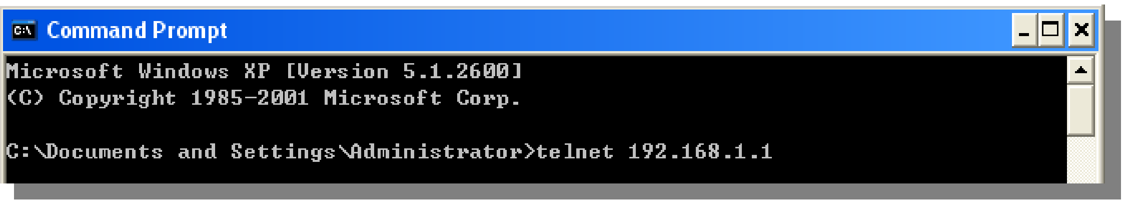
After you pass the security warning screen, you will enter the secured web management interface. The default password is "airlive". Please ignore the "Certificate Error" warning icon, it just notice you that you are in an un-certificated site, you still can configure the WLA-9000AP without limitation.


https://192.168.1.1./index.asp
Certificate Error
Air Live
WLA-9000AP
802.11a/b/g Dual Radio Access Point
www.airlive.com
Wireless Settings
Configure the Operation Mode of your WLA-9000AP
System Configuration
Change the password, upgrade the firmware, reboot the Wireless Access Point, and more.
Device Status
Show the device information, syslog table, wireless client table, and more.
Help
Get help with commonly asked questions about the Wireless Access Point.

For more information about Web Management and HTTPS, please make sure to read through "Introduction to Web Management" in this chapter, Chapter 4, and Chapter 5

- **Command Line Interface (Telnet):** WLA-9000AP can be managed through the command line interface (CLI). It is possible to write a text script file, and then paste it into the CLI to execute several commands at once. However, Telnet does not encrypt its message. Therefore, it is not secure. The default Telnet management port is TCP port 23.

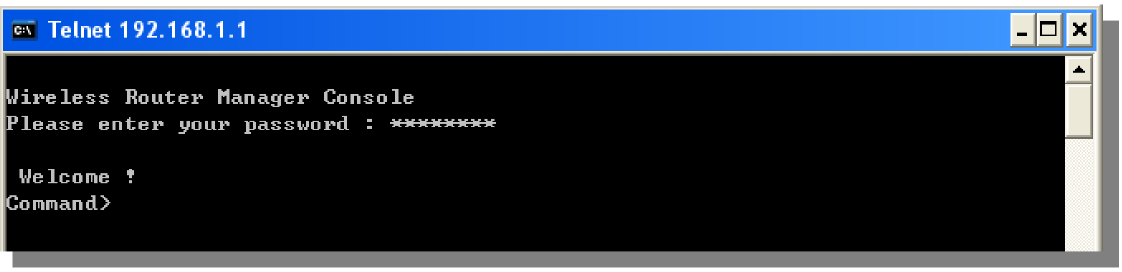
  To use the CLI, please open the command line window. Then type "telnet 192.168.1.1" to start.



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>telnet 192.168.1.1
```

  When asked for password, please enter "airlive".



```
Wireless Router Manager Console
Please enter your password : *********

 Welcome !
Command>
```

  To get a list of available command and their usage, please type "help" on the command prompt.

- **Secure Shell (SSH, SSH2)**: SSH is an encrypted Command Line Interface that allow user to send text commands through SSL encryption. Therefore, it provides the added advantage of security comparing to Telnet. As with Telnet, the SSH and

SSH2 provide the possibility to write a text script and paste into the CLI interface for multiple command execution. It also makes configuration change across many WLA-9000APs easier. The default management port for SSH/SSH2 is TCP/UDP port 22.

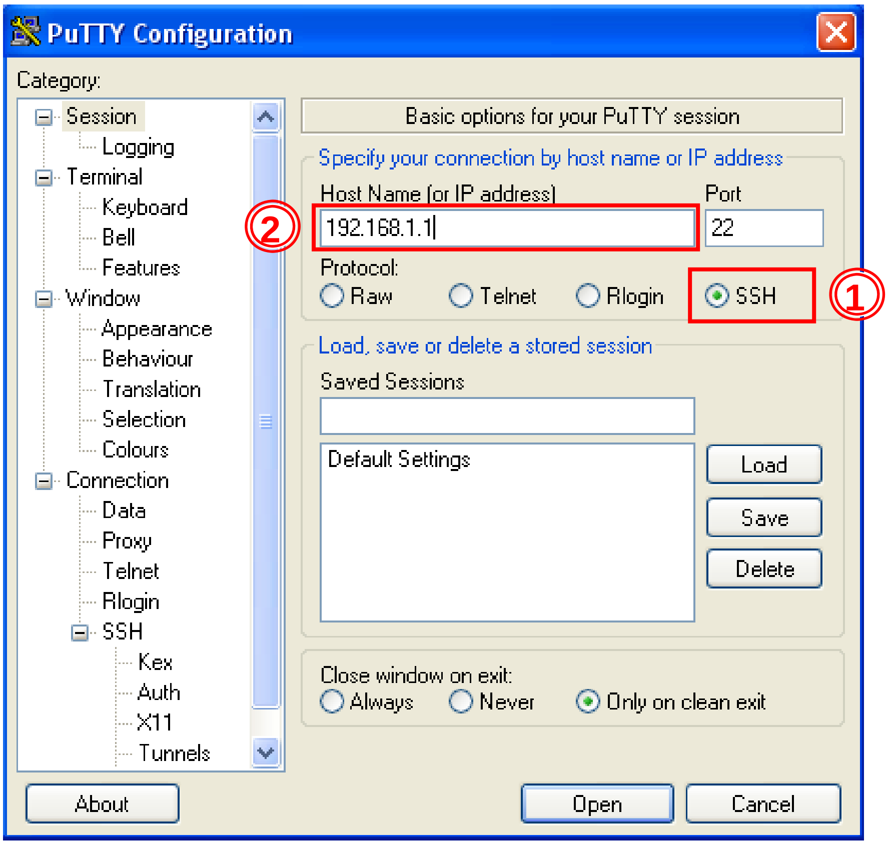
To manage via the SSH/SSH2 protocol, you would need a SSH client. Free SSH clients are widely available on the Internet. You can find where to download them by using Internet search engine such as Google. In this guide, we will use a popular SSH/Telnet utility call Putty.

Once you have download and install Putty. Please follow the figure below to make a connection with WLA-9000AP:

1. Choose "SSH" as indicated in the diagram

2. Enter the IP address of WLA-9000AP

3. Click on "Open" to start the SSH session.



Basic options for your PuTTY session

Specify your connection by host name or IP address

Host Name (or IP address): 192.168.1.1

Port: 22

Protocol: ○ Raw ○ Telnet ○ Rlogin ● SSH

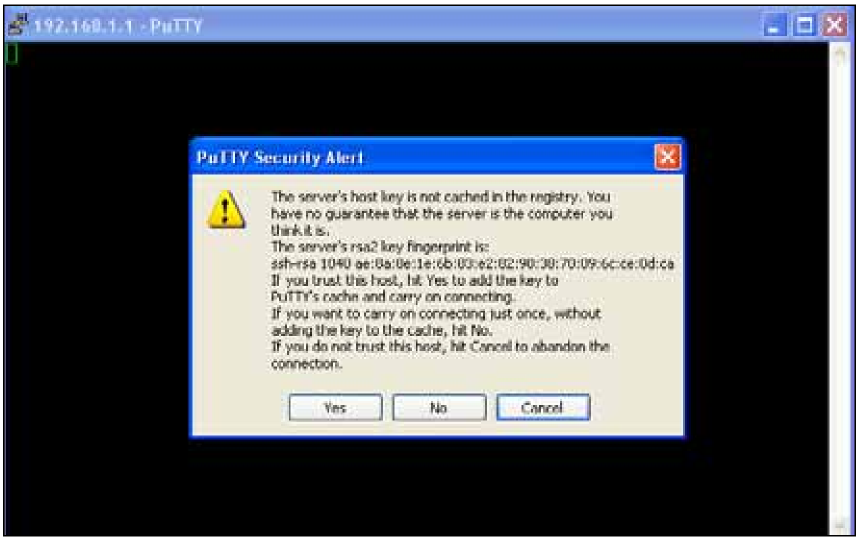
Load, save or delete a stored session

Saved Sessions

Default Settings

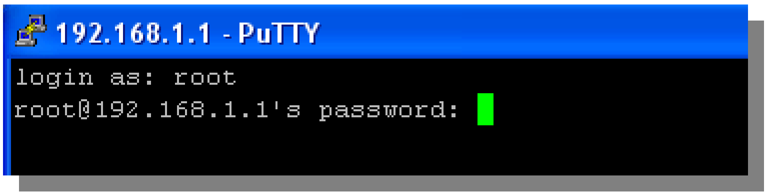
Close window on exit: ○ Always ○ Never ● Only on clean exit

When the following screen appear, click on "Yes" to continue



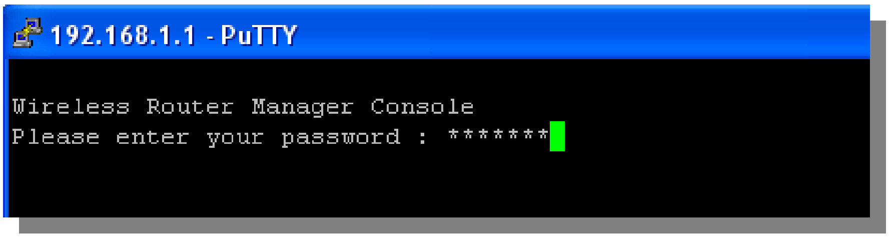
The server's host key is not cached in the registry. You have no guarantee that the server is the computer you think it is.
The server's rsa2 key fingerprint is:
ssh-rsa 1040 ae:0a:0e:1e:6b:03:e2:02:90:30:70:09:6c:ce:0d:ca
If you trust this host, hit Yes to add the key to PuTTY's cache and carry on connecting.
If you want to carry on connecting just once, without adding the key to the cache, hit No.
If you do not trust this host, hit Cancel to abandon the connection.

When the following screen appears, enter “root” for login. Then press Enter when password for root is requested, do not enter any password



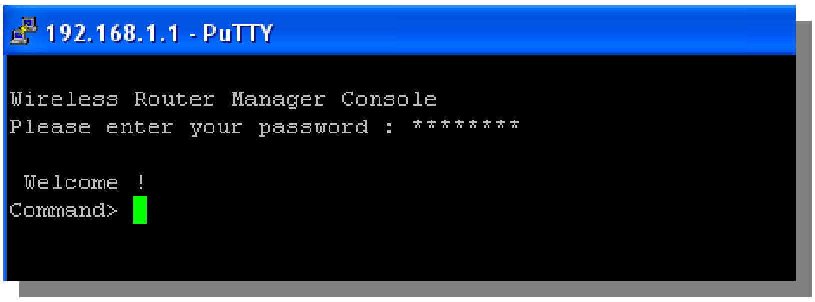
```
login as: root
root@192.168.1.1's password:
```

When the “Wireless Router Manager Console” appears, please enter “airlive” for password. This password will change when you change the password.



```
Wireless Router Manager Console
Please enter your password : *******
```

Now you are ready to enter commands



```
Wireless Router Manager Console
Please enter your password : ********

 Welcome !
Command>
```

To get a list of available command and their usage, please type “help” on the command prompt.

⚠ ***For more information about Telnet and SSH configuration, please go to Chapter 7 Command Line Interface*.**

- **SNMP Management**: The WLA-9000AP support SNMPv1/v2 management. If you have SNMP management software, it can manage the WLA-9000AP. The WLA-9000AP’s SNMP support is as followed:
  - ❑ SNMP v1/v2 support
  - ❑ SNMP Read/Write Community String
  - ❑ SNMP Trap support
  - ❑ MIB and MIB II Support
  - ❑ Ether-like MIB
  - ❑ IEEE802dot11 MIB
  - ❑ Private MIB

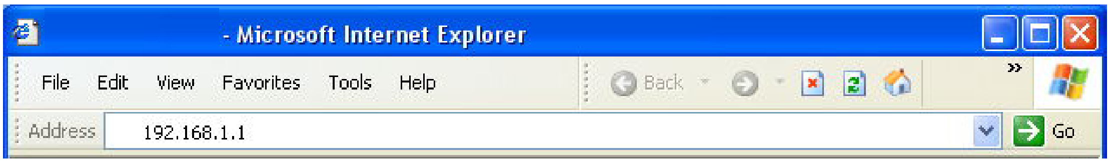
3.4 Introduction to Web Management

The WLA-9000AP offers both normal (http) and secured (https) Web Management interfaces. Their share the same interface and functions, and they can both be accessed through web browsers. The only difference is HTTPS are encrypted for extra security. Therefore, we will discuss them together as “Web Management” on this guide.

3.4.1 Getting into Web Management

Normal Web Management (HTTP)

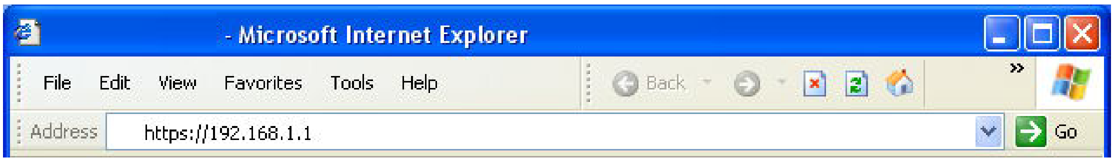
To get into the Normal Web Management, simply type in the WLA-9000AP’s IP address (default IP is 192.168.1.1) into the web browser’s address field.



Address: 192.168.1.1

Secured Web Management (HTTPS)

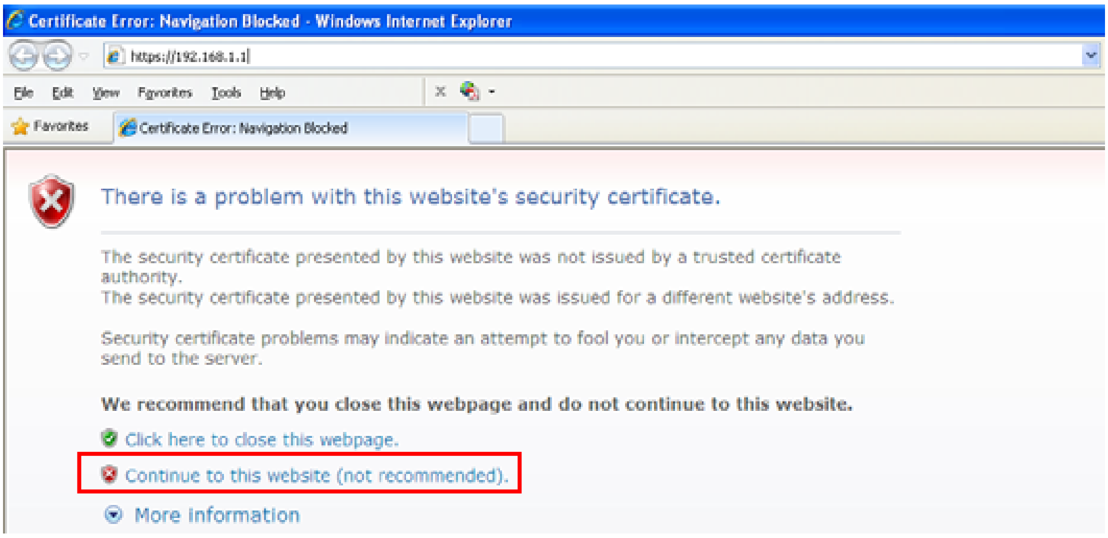
To get into the Secured Web Management, just type "https://192.168.1.1" into the web browser's address field. The "192.168.1.1" is WLA-9000AP's default IP address. If the IP address is changed, the address entered in the browser should change also.


- Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address
Go

https://192.168.1.1

A security warning screen from your browser will then pop-up depending on the browser you use. Please follow step below to clear the security screen.

❑ Internet Explorer: Click "Continue to this website" to proceed


Certificate Error: Navigation Blocked - Windows Internet Explorer
https://192.168.1.1
File Edit View Favorites Tools Help
Favorites
Certificate Error: Navigation Blocked

There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

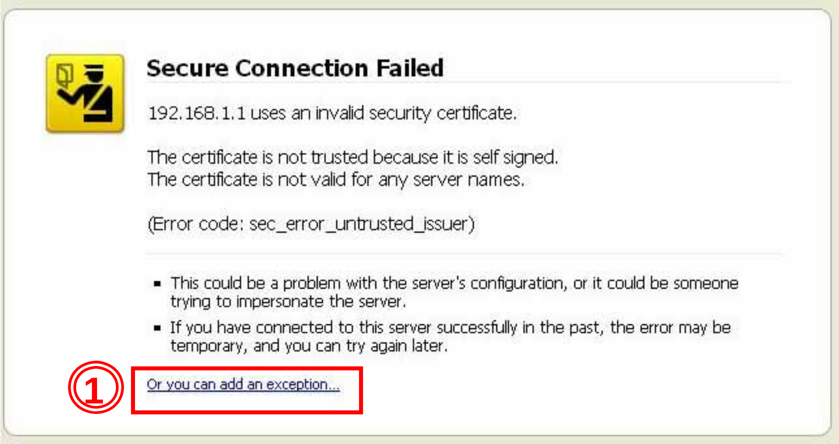
Click here to close this webpage.

Continue to this website (not recommended).

More information

❑ Firefox:

1. Select "or you can add an exception"



Secure Connection Failed

192.168.1.1 uses an invalid security certificate.

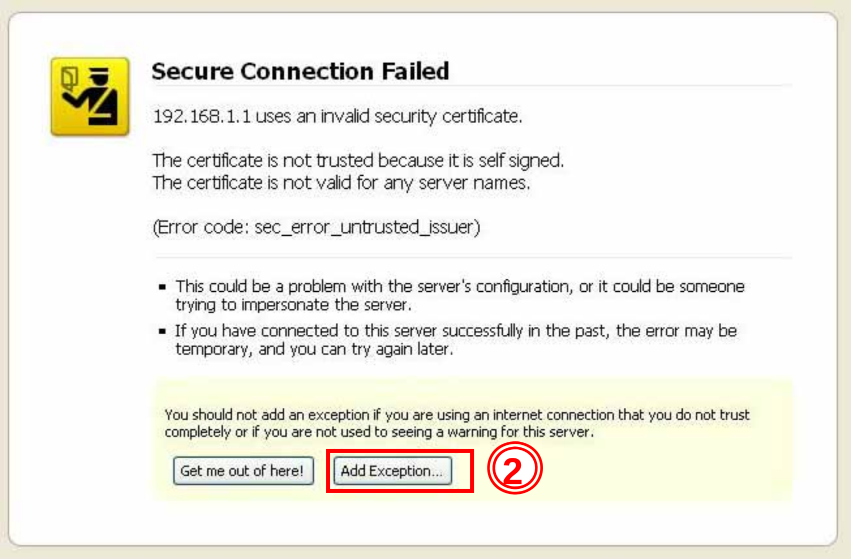
The certificate is not trusted because it is self signed.
The certificate is not valid for any server names.

(Error code: sec_error_untrusted_issuer)

- This could be a problem with the server's configuration, or it could be someone trying to impersonate the server.
- If you have connected to this server successfully in the past, the error may be temporary, and you can try again later.

Or you can add an exception...

2. Click on "Add Exception"



Secure Connection Failed

192.168.1.1 uses an invalid security certificate.

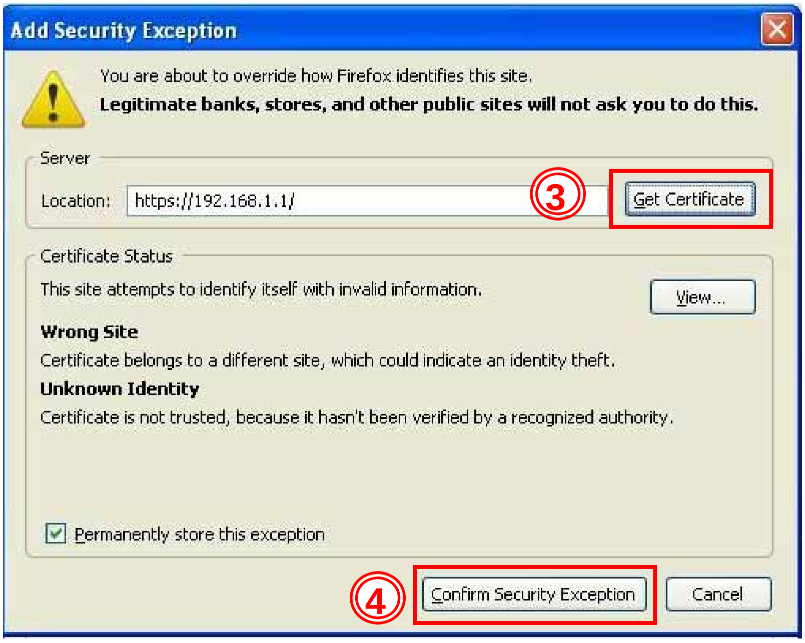
The certificate is not trusted because it is self signed.
The certificate is not valid for any server names.

(Error code: sec_error_untrusted_issuer)

- This could be a problem with the server's configuration, or it could be someone trying to impersonate the server.
- If you have connected to this server successfully in the past, the error may be temporary, and you can try again later.

You should not add an exception if you are using an internet connection that you do not trust completely or if you are not used to seeing a warning for this server.

3. Click on "Get Certificate". Then, please enter WLA-9000AP's IP address. Finally, please click on "Confirm Security Exception."



Add Security Exception

You are about to override how Firefox identifies this site.
Legitimate banks, stores, and other public sites will not ask you to do this.

Server

Location: https://192.168.1.1/

Certificate Status

This site attempts to identify itself with invalid information.

Wrong Site

Certificate belongs to a different site, which could indicate an identity theft.

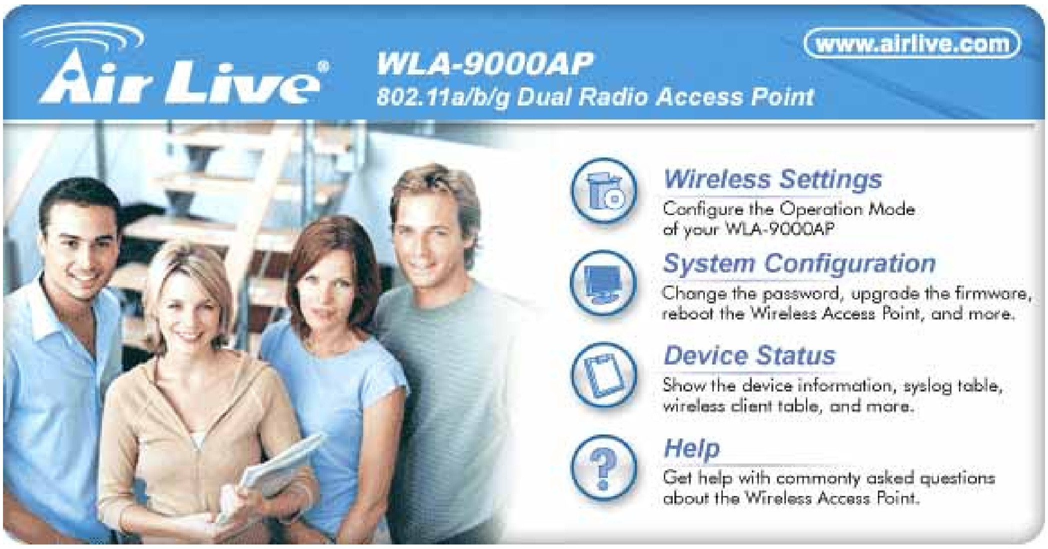
Unknown Identity

Certificate is not trusted, because it hasn't been verified by a recognized authority.

☑ Permanently store this exception

3.4.2 Welcome Screen and Login

After the procedure above, the Welcome Screen will appear. Welcome Screen gives a brief introduction of the WLA-9000AP's main function category. By clicking on the function category, it will direct you to the corresponding web management menu.



Wireless Settings
Configure the Operation Mode of your WLA-9000AP

System Configuration
Change the password, upgrade the firmware, reboot the Wireless Access Point, and more.

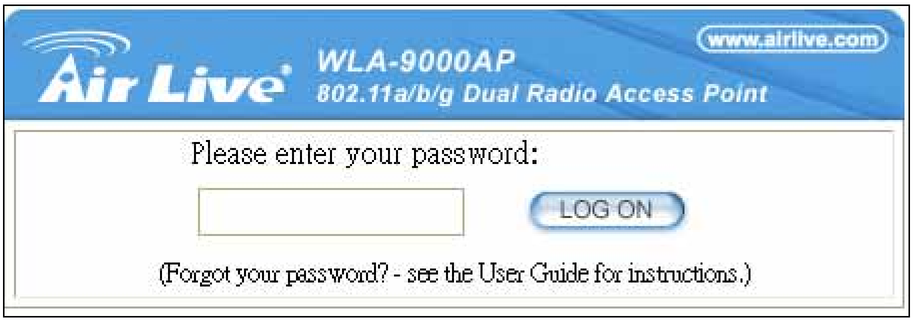
Device Status
Show the device information, syslog table, wireless client table, and more.

Help
Get help with commonly asked questions about the Wireless Access Point.

- **Wireless Settings**: Click on this part will bring you to the wireless operation mode menu. The WLA-9000AP's wireless settings are different between wireless modes. Only functions that are applicable to the wireless mode will show to simplify configuration. For example, multiple SSID option is only workable for Access Point and AP Router mode. Therefore, the function will only appear in these 2 modes. For this reason, the first step to configure the WLA-9000AP is to select the wireless mode. The router mode specific functions are also in this menu category. For explanation of different wireless modes, please refer to Chapter 1.
- **System Configuration:** All non-wireless and router mode settings are in this category. The system configurations including changing password, upload firmware, backup configuration, settings PING watchdog, and setting management interface. The default management timeout is 10 minutes; we recommend you should change password and management timeout during the first time login.
- **Device Status**: This section for monitoring the status of WLA-9000AP. It provides information on device status, Ethernet status, wireless status, wireless client table, and system log.
- **Help:** This is the online help system for quick reference. We still recommend you to read this user's guide for more information.

TIPS: *You can choose any menu categories to begin; you can switch to other menu later*

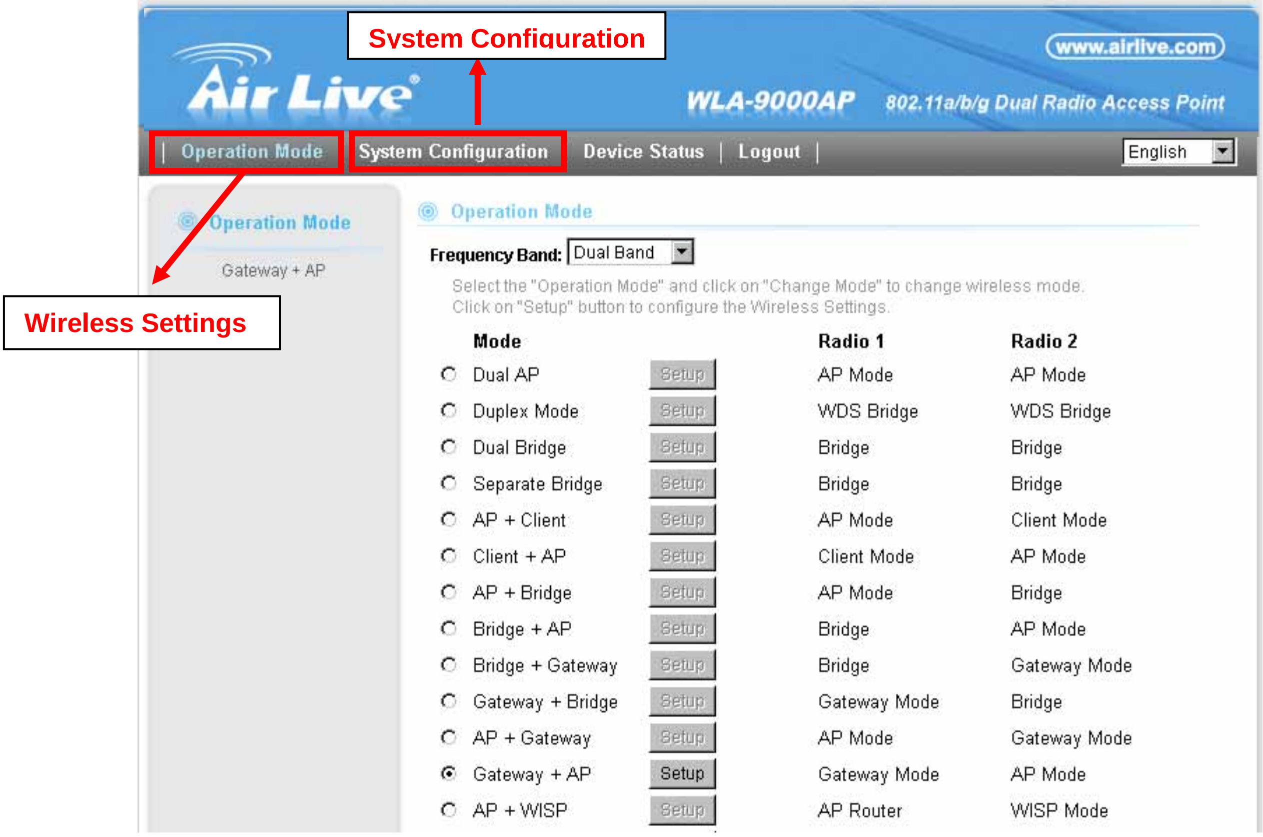
When you choose one of the menu categories, the WLA-9000AP will require you to enter the username and password. Please enter "**airlive**" (all lower cases) for both username and password.



Please enter your password:

(Forgot your password? - see the User Guide for instructions.)

After you enter the correct password, the following screen will appear corresponding to the menu category you selected.



Operation Mode

Frequency Band: Dual Band

Select the "Operation Mode" and click on "Change Mode" to change wireless mode.
Click on "Setup" button to configure the Wireless Settings.

	Mode		Radio 1	Radio 2
○	Dual AP	Setup	AP Mode	AP Mode
○	Duplex Mode	Setup	WDS Bridge	WDS Bridge
○	Dual Bridge	Setup	Bridge	Bridge
○	Separate Bridge	Setup	Bridge	Bridge
○	AP + Client	Setup	AP Mode	Client Mode
○	Client + AP	Setup	Client Mode	AP Mode
○	AP + Bridge	Setup	AP Mode	Bridge
○	Bridge + AP	Setup	Bridge	AP Mode
○	Bridge + Gateway	Setup	Bridge	Gateway Mode
○	Gateway + Bridge	Setup	Gateway Mode	Bridge
○	AP + Gateway	Setup	AP Mode	Gateway Mode
●	Gateway + AP	Setup	Gateway Mode	AP Mode
○	AP + WISP	Setup	AP Router	WISP Mode

If you are placing the WLA-9000AP behind router or firewall, you might need to open virtual server ports to WLA-9000AP on your firewall/router

- HTTP: TCP Port 80
- HTTPS: TCP/UDP Port 443

This procedure is not necessary in most cases unless there is a router/firewall between your PC and WLA-9000AP.

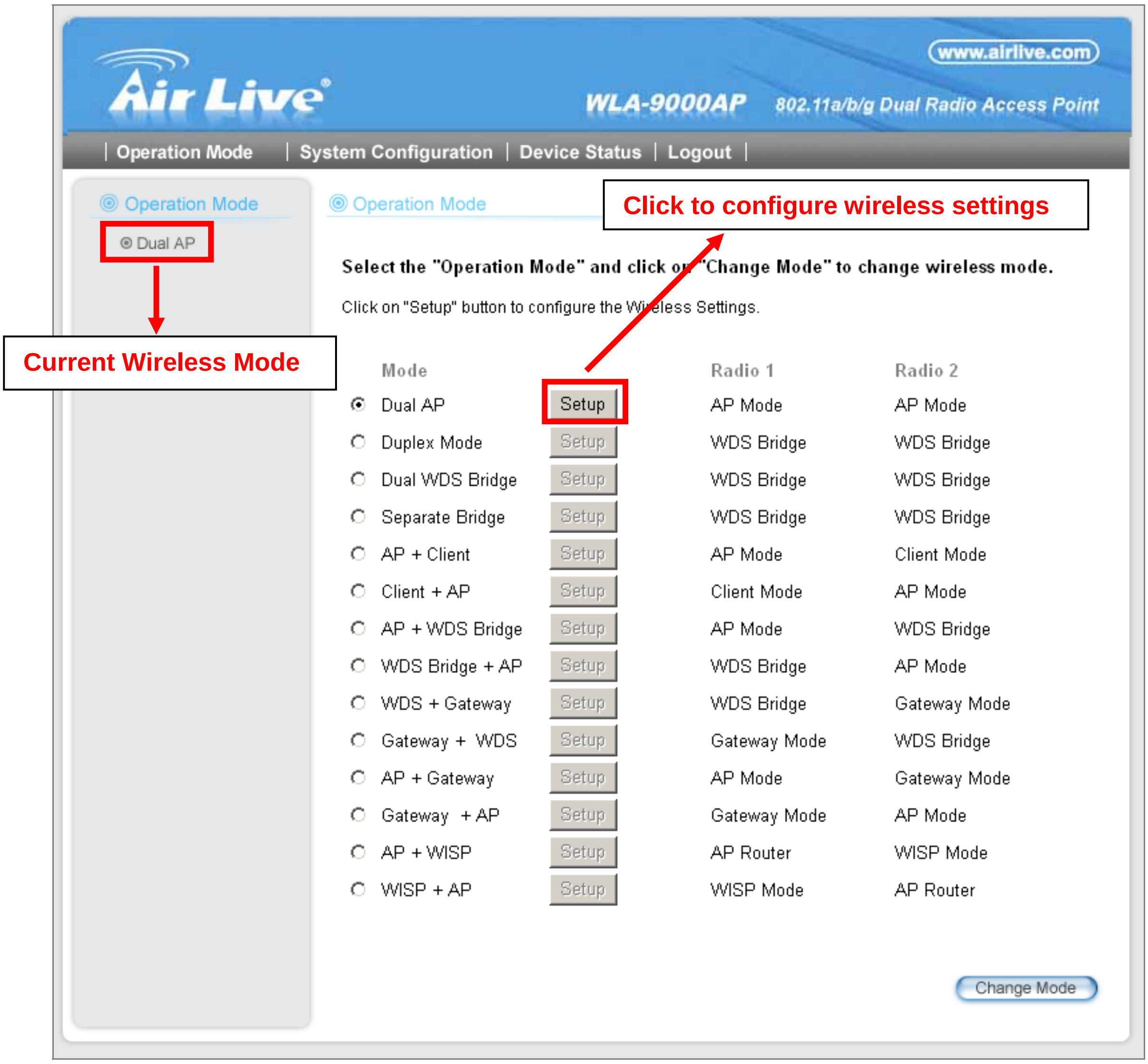
3.5 Initial Configuration

We recommend users to browse through WLA-9000AP's web management interface to get an overall picture of the functions and interface. Below are the recommended initial configurations for first time login:

3.5.1 Choose the wireless Operation Modes

The wireless settings of WLA-9000AP are dependant on the wireless operation mode you choose. Therefore, the first step is to choose the operation mode. For explanation on when to use what operation mode, please refer to Chapter 1

When you click on the "Wireless Settings" on the welcome screen or the "Operation Mode" on the top menu bar, the following screen will appear.



Click to configure wireless settings

Current Wireless Mode

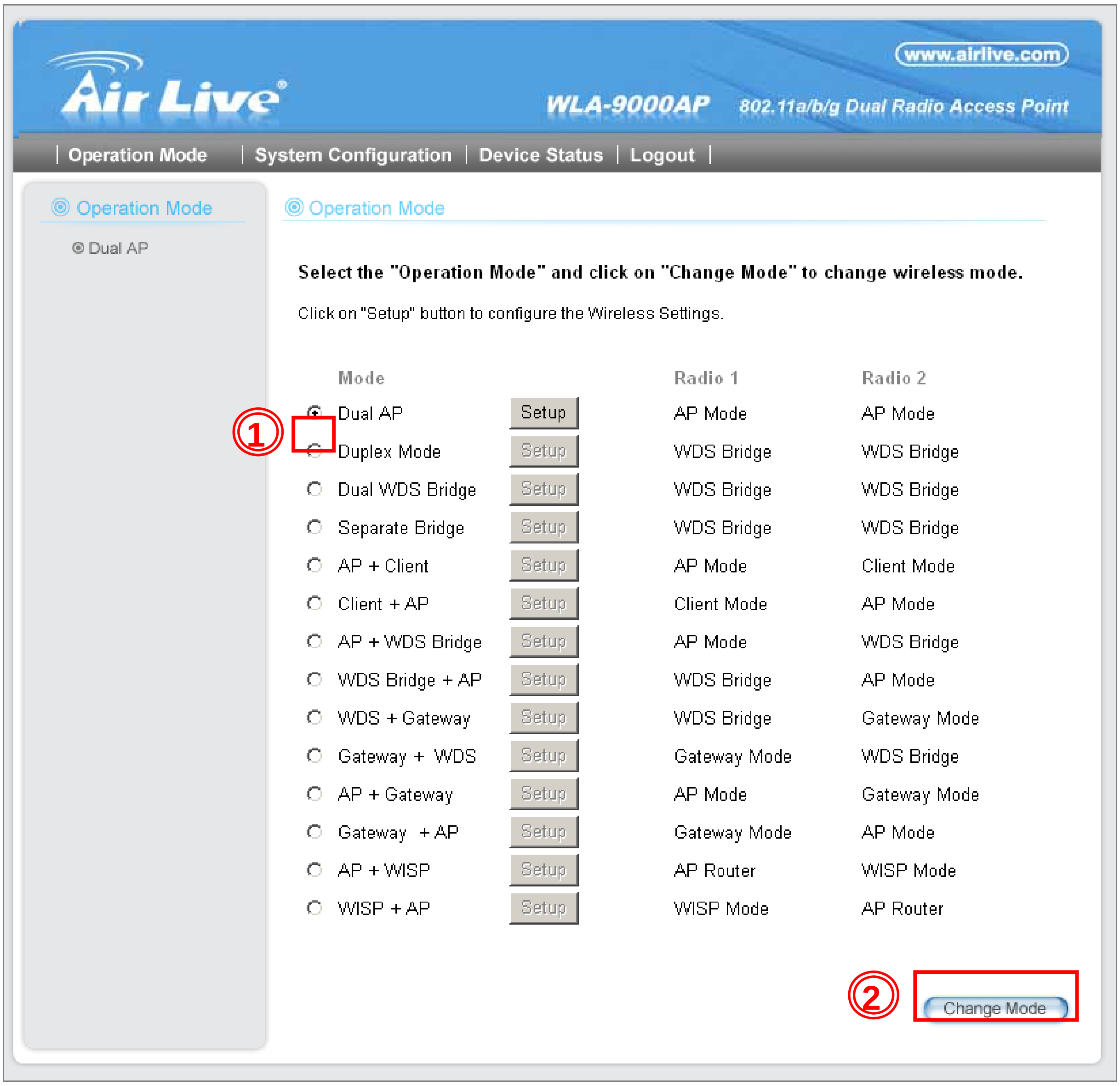
Select the "Operation Mode" and click on "Change Mode" to change wireless mode.

Click on "Setup" button to configure the Wireless Settings.

	Mode		Radio 1	Radio 2
●	Dual AP	Setup	AP Mode	AP Mode
○	Duplex Mode	Setup	WDS Bridge	WDS Bridge
○	Dual WDS Bridge	Setup	WDS Bridge	WDS Bridge
○	Separate Bridge	Setup	WDS Bridge	WDS Bridge
○	AP + Client	Setup	AP Mode	Client Mode
○	Client + AP	Setup	Client Mode	AP Mode
○	AP + WDS Bridge	Setup	AP Mode	WDS Bridge
○	WDS Bridge + AP	Setup	WDS Bridge	AP Mode
○	WDS + Gateway	Setup	WDS Bridge	Gateway Mode
○	Gateway + WDS	Setup	Gateway Mode	WDS Bridge
○	AP + Gateway	Setup	AP Mode	Gateway Mode
○	Gateway + AP	Setup	Gateway Mode	AP Mode
○	AP + WISP	Setup	AP Router	WISP Mode
○	WISP + AP	Setup	WISP Mode	AP Router

Follow the example below to change to “Client Infrastructure” mode

1. Select “Duplex” mode.
2. Click on “change mode” button
3. The AP will reboot, wait for about one minute


www.airlive.com
WLA-9000AP 802.11a/b/g Dual Radio Access Point
Operation Mode | System Configuration | Device Status | Logout
Operation Mode
Dual AP
①
②
Change Mode

Operation Mode

Select the "Operation Mode" and click on "Change Mode" to change wireless mode.

Click on "Setup" button to configure the Wireless Settings.

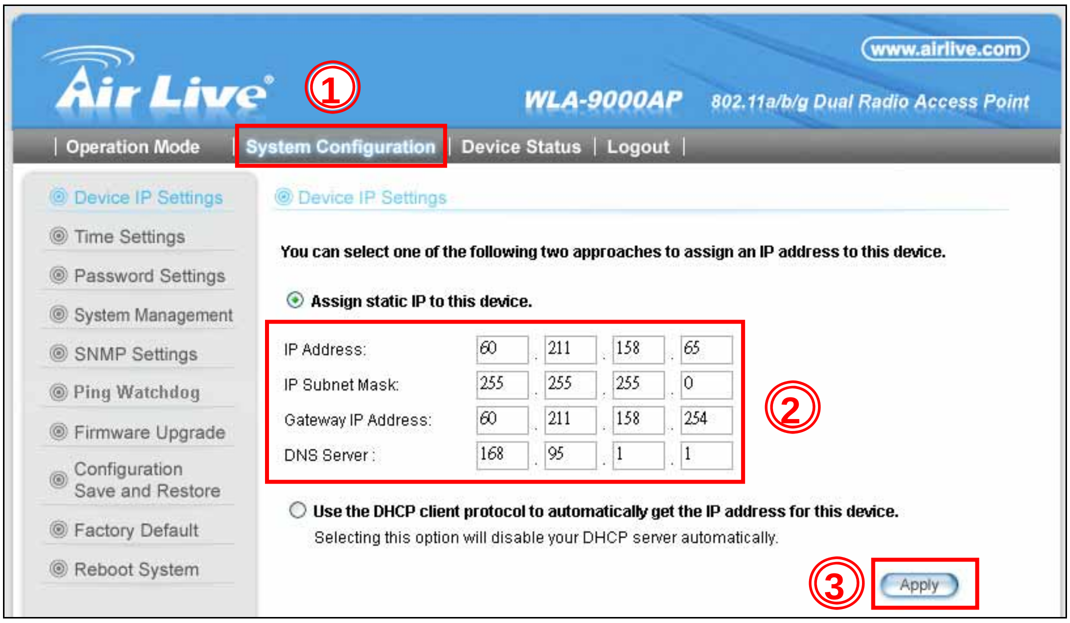
Mode		Radio 1	Radio 2
● Dual AP	Setup	AP Mode	AP Mode
○ Duplex Mode	Setup	WDS Bridge	WDS Bridge
○ Dual WDS Bridge	Setup	WDS Bridge	WDS Bridge
○ Separate Bridge	Setup	WDS Bridge	WDS Bridge
○ AP + Client	Setup	AP Mode	Client Mode
○ Client + AP	Setup	Client Mode	AP Mode
○ AP + WDS Bridge	Setup	AP Mode	WDS Bridge
○ WDS Bridge + AP	Setup	WDS Bridge	AP Mode
○ WDS + Gateway	Setup	WDS Bridge	Gateway Mode
○ Gateway + WDS	Setup	Gateway Mode	WDS Bridge
○ AP + Gateway	Setup	AP Mode	Gateway Mode
○ Gateway + AP	Setup	Gateway Mode	AP Mode
○ AP + WISP	Setup	AP Router	WISP Mode
○ WISP + AP	Setup	WISP Mode	AP Router

3.5.2 Change the Device’s IP Address

The default IP address is at 192.168.1.1. You should change it to the same subnet as your network. Also, if you want to manage WLA-9000AP remotely, you have to set the Gateway and DNS server information.

To setup the IP settings for WLA-9000AP, please select “System Configuration” -> Device

IP Settings”. After entering the IP information, click on “Apply” to finish.



Device IP Settings

You can select one of the following two approaches to assign an IP address to this device.

● Assign static IP to this device.

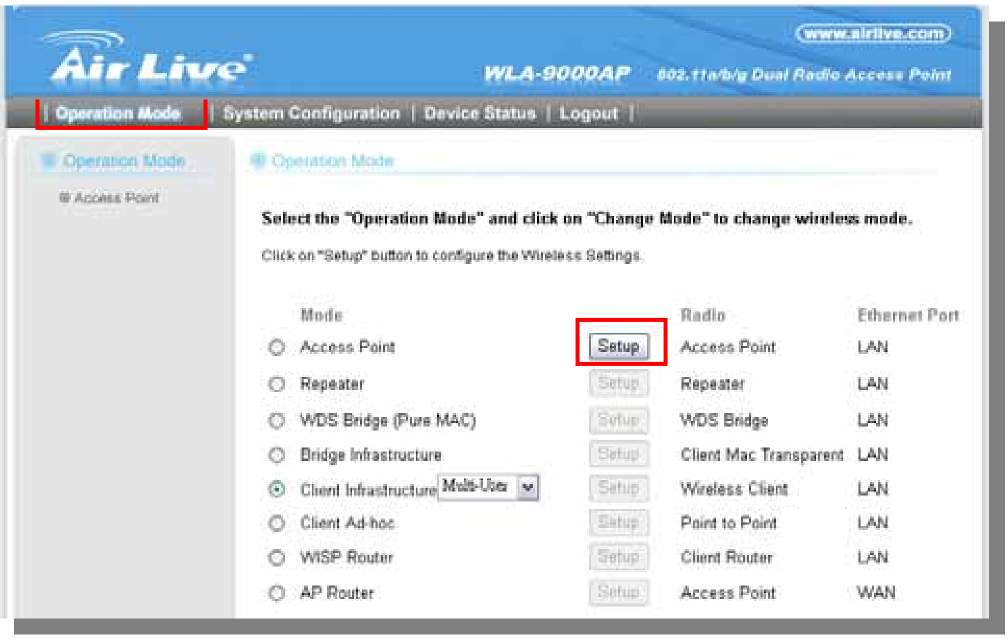
IP Address:	60	211	158	65
IP Subnet Mask:	255	255	255	0
Gateway IP Address:	60	211	158	254
DNS Server :	168	95	1	1

○ Use the DHCP client protocol to automatically get the IP address for this device.
Selecting this option will disable your DHCP server automatically.

3.5.3 Change the Country Code

The legal frequency and channels in 5GHz spectrum varies between countries. The default country code is United Kingdom which should require no changes If you are living in Europe. If you are living outside EU, you should change the country code accordingly. In the example below, we will change the country code to United States which enables the use of 5.8GHz spectrum.

Step 1. Select “Operation Mode” -> “Setup”



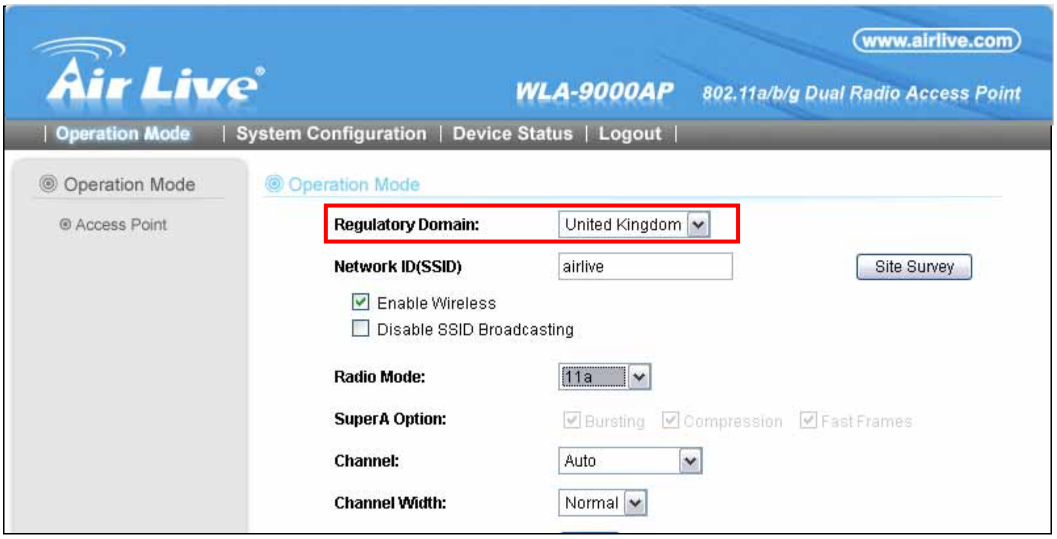
Operation Mode

Select the "Operation Mode" and click on "Change Mode" to change wireless mode.

Click on "Setup" button to configure the Wireless Settings.

	Mode		Radio	Ethernet Port
○	Access Point	Setup	Access Point	LAN
○	Repeater	Setup	Repeater	LAN
○	WDS Bridge (Pure MAC)	Setup	WDS Bridge	LAN
○	Bridge Infrastructure	Setup	Client Mac Transparent	LAN
●	Client Infrastructure Multi-User	Setup	Wireless Client	LAN
○	Client Ad-hoc	Setup	Point to Point	LAN
○	WISP Router	Setup	Client Router	LAN
○	AP Router	Setup	Access Point	WAN

Step 2. From the Regulatory Domain, please select your country


www.airlive.com
Air Live
WLA-9000AP 802.11a/b/g Dual Radio Access Point
| Operation Mode | System Configuration | Device Status | Logout |
Operation Mode
Access Point
Operation Mode

Regulatory Domain: United Kingdom

Network ID(SSID) airlive

☑ Enable Wireless

□ Disable SSID Broadcasting

Radio Mode: 11a

SuperA Option: ☑ Bursting ☑ Compression ☑ Fast Frames

Channel: Auto

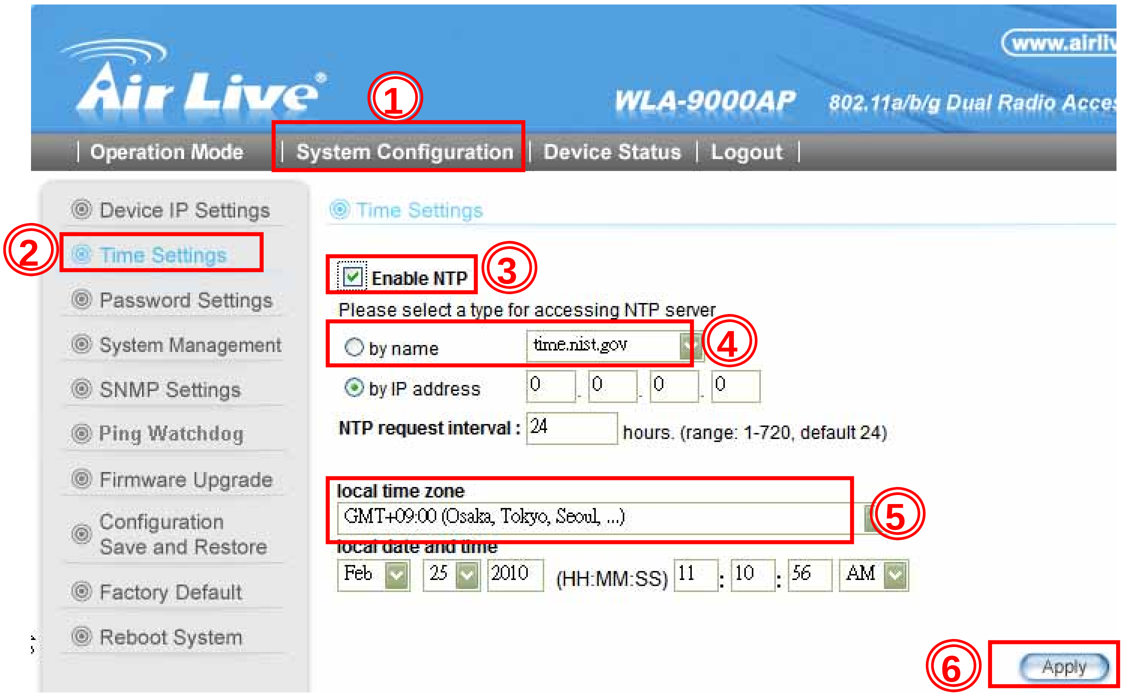
Channel Width: Normal

Step 3. Select the United States from the list.

Step 4. Click on “Apply” to finish.

3.5.4 Set the Time and Date

It is important that you set the date and time for your WLA-9000AP so that the system log will record the correct date and time information. Please go to “*System Configuration”* ->*Time Settings*. We recommend you choose “Enable NTP” so the time will be keep even after reboot. If your WLA-9000AP is not connected to Internet, please enter the time manually. Please remember to select your local time zone and click “Apply” to finish.



Time Settings

☑ Enable NTP

Please select a type for accessing NTP server

○ by name time.nist.gov

● by IP address 0 . 0 . 0 . 0

NTP request interval : 24 hours. (range: 1-720, default 24)

local time zone

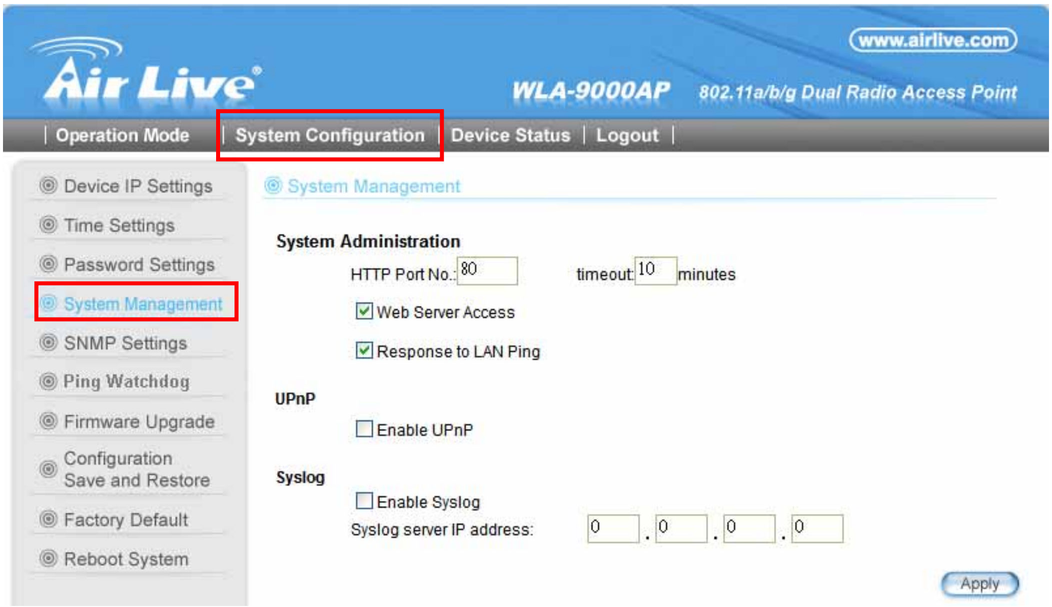
GMT+09:00 (Osaka, Tokyo, Seoul, ...)

local date and time

Feb 25 2010 (HH:MM:SS) 11 : 10 : 56 AM

3.5.5 Change System Management

It is recommended that you change the system management settings first. Please go to "*System Configuration*"-> "*System Management*". The default web management time out is 10 minutes, you can set to longer period if needed. For WISP administrators, you can consider turning off HTTP and Telnet for security purpose.



System Management

System Administration

HTTP Port No.: 80 timeout: 10 minutes

☑ Web Server Access

☑ Response to LAN Ping

UPnP

☐ Enable UPnP

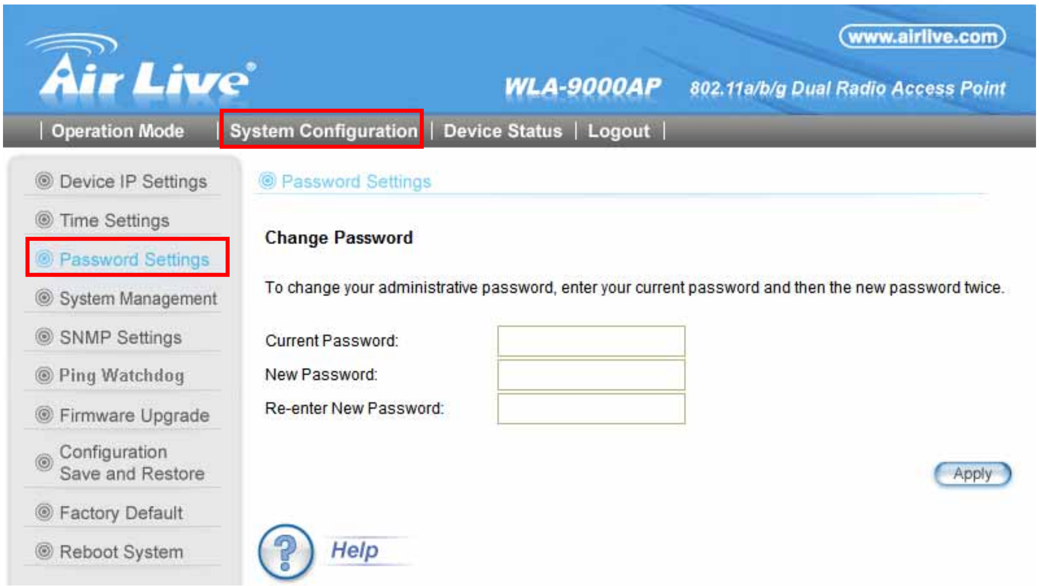
Syslog

☐ Enable Syslog

Syslog server IP address: 0 . 0 . 0 . 0

3.5.6 Change Password

You should change the password for WLA-9000AP at the first login. To change password, please go to *"System Configuration" -> "Password Settings"* menu.



Change Password

To change your administrative password, enter your current password and then the new password twice.

Current Password:

New Password:

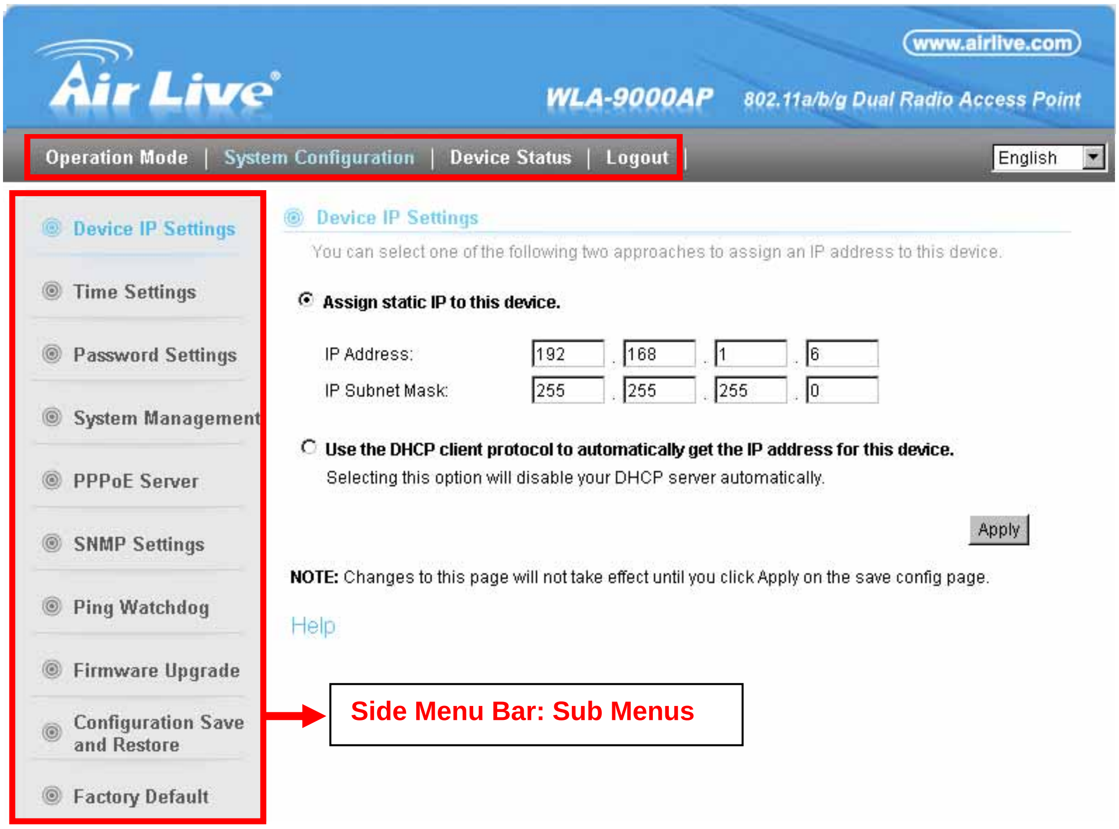
Re-enter New Password:

4 Web Management: Wireless and WAN Settings

In this chapter, we will explain about the wireless settings and router mode settings in web management interface. Please be sure to read through Chapter 3's "*Introduction to Web Management"* and *"Initial Configurations"* first. For system configurations, device status, and other non-wireless related settings; please go to Chapter 5.

4.1 About WLA-9000AP Menu Structure

The WLA-9000AP's web management menu is divided into 3 main menus: *Operation Modes, System Configurations*, and *Device Status*. The main menus are displayed in "Top Menu Bar". Within each main menu category, there are sub-menu options which are displayed on the "Side Menu Bar"



Device IP Settings

You can select one of the following two approaches to assign an IP address to this device.

● Assign static IP to this device.

IP Address: 192 . 168 . 1 . 6

IP Subnet Mask: 255 . 255 . 255 . 0

○ Use the DHCP client protocol to automatically get the IP address for this device.

Selecting this option will disable your DHCP server automatically.

NOTE: Changes to this page will not take effect until you click Apply on the save config page.

Side Menu Bar: Sub Menus

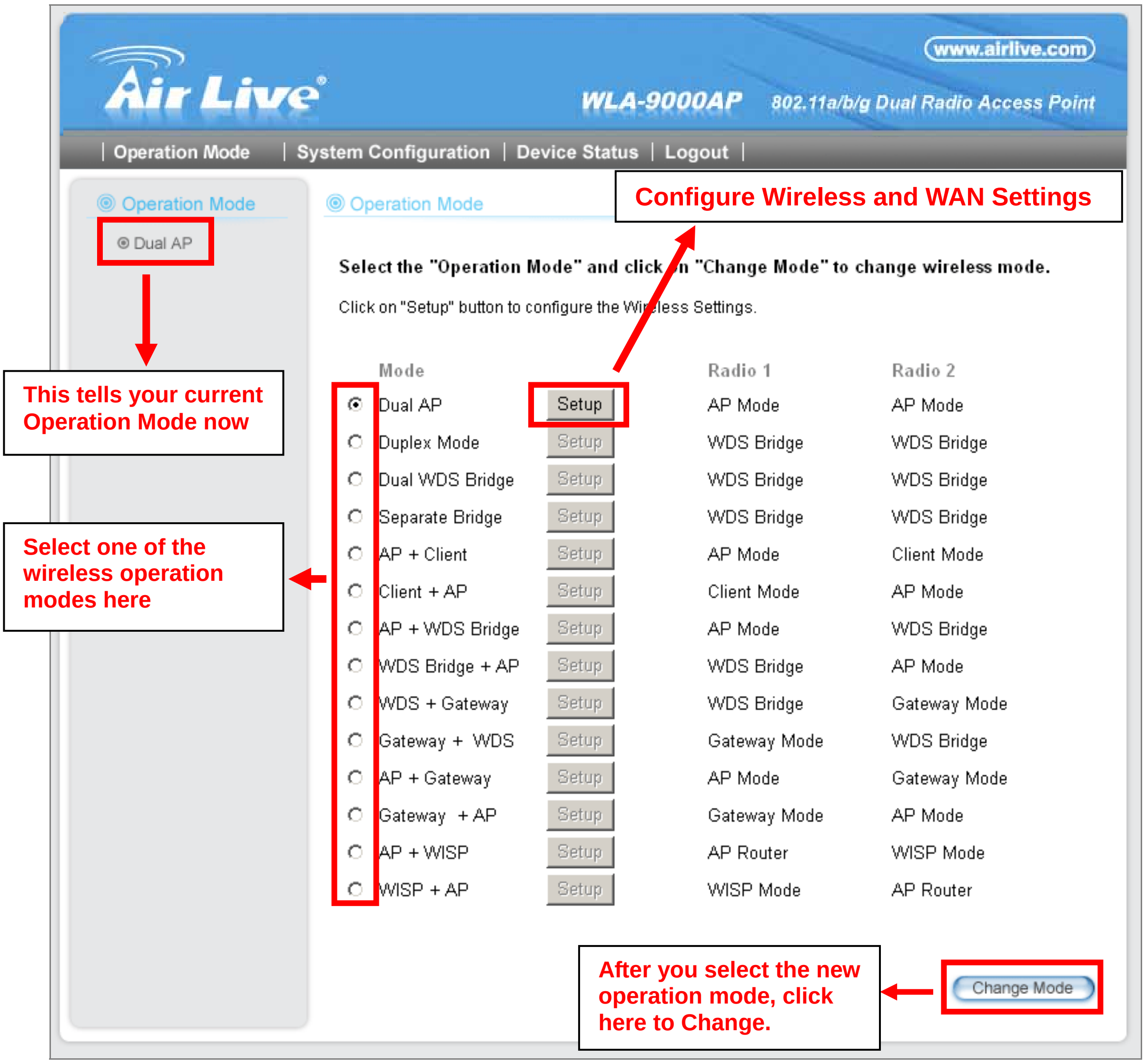
- **Operation Mode**: This menu is where you will find wireless and WAN settings. The WLA-9000AP's wireless settings are dependant on the wireless operation mode you choose; only the applicable wireless settings for selected operation mode are shown. For example; WAN port setting is available only for AP Router and WISP Router mode, it will only be shown in those modes. To access wireless settings, click on the "*Setup*" button within each operation mode. For explanation on different wireless modes, please refer to Chapter 1. We will talk about functions in this menu for this chapter.

- **System Configuration:** All settings besides Wireless and WAN functions are in this category. The system configuration including changing password, upload firmware, backup configuration, settings PING watchdog, and setting management interface. We will talk about this menu's function in Chapter 5.
- **Device Status**: This section for monitoring the status of WLA-9000AP. It provides information on device status, Ethernet status, wireless status, wireless client table, and system log.
- **Logout:** Please make sure to Logout after you finish all settings.

4.2 Operation Modes (Wireless and WAN Settings)

The wireless settings of WLA-9000AP are dependant on the wireless operation mode you choose. Therefore, the first step is to choose the operation mode. For explanation on when to use what operation mode, please refer to Chapter 1.

When you select "*Wireless Settings*" in the welcome screen, or click on the "*Operation Mode*" on the top menu; the following screen will appear:


www.airlive.com
WLA-9000AP 802.11a/b/g Dual Radio Access Point
Operation Mode | System Configuration | Device Status | Logout
Operation Mode
Dual AP
Operation Mode

Select the "Operation Mode" and click on "Change Mode" to change wireless mode.

Click on "Setup" button to configure the Wireless Settings.

	Mode		Radio 1	Radio 2
●	Dual AP	Setup	AP Mode	AP Mode
○	Duplex Mode	Setup	WDS Bridge	WDS Bridge
○	Dual WDS Bridge	Setup	WDS Bridge	WDS Bridge
○	Separate Bridge	Setup	WDS Bridge	WDS Bridge
○	AP + Client	Setup	AP Mode	Client Mode
○	Client + AP	Setup	Client Mode	AP Mode
○	AP + WDS Bridge	Setup	AP Mode	WDS Bridge
○	WDS Bridge + AP	Setup	WDS Bridge	AP Mode
○	WDS + Gateway	Setup	WDS Bridge	Gateway Mode
○	Gateway + WDS	Setup	Gateway Mode	WDS Bridge
○	AP + Gateway	Setup	AP Mode	Gateway Mode
○	Gateway + AP	Setup	Gateway Mode	AP Mode
○	AP + WISP	Setup	AP Router	WISP Mode
○	WISP + AP	Setup	WISP Mode	AP Router

Configure Wireless and WAN Settings

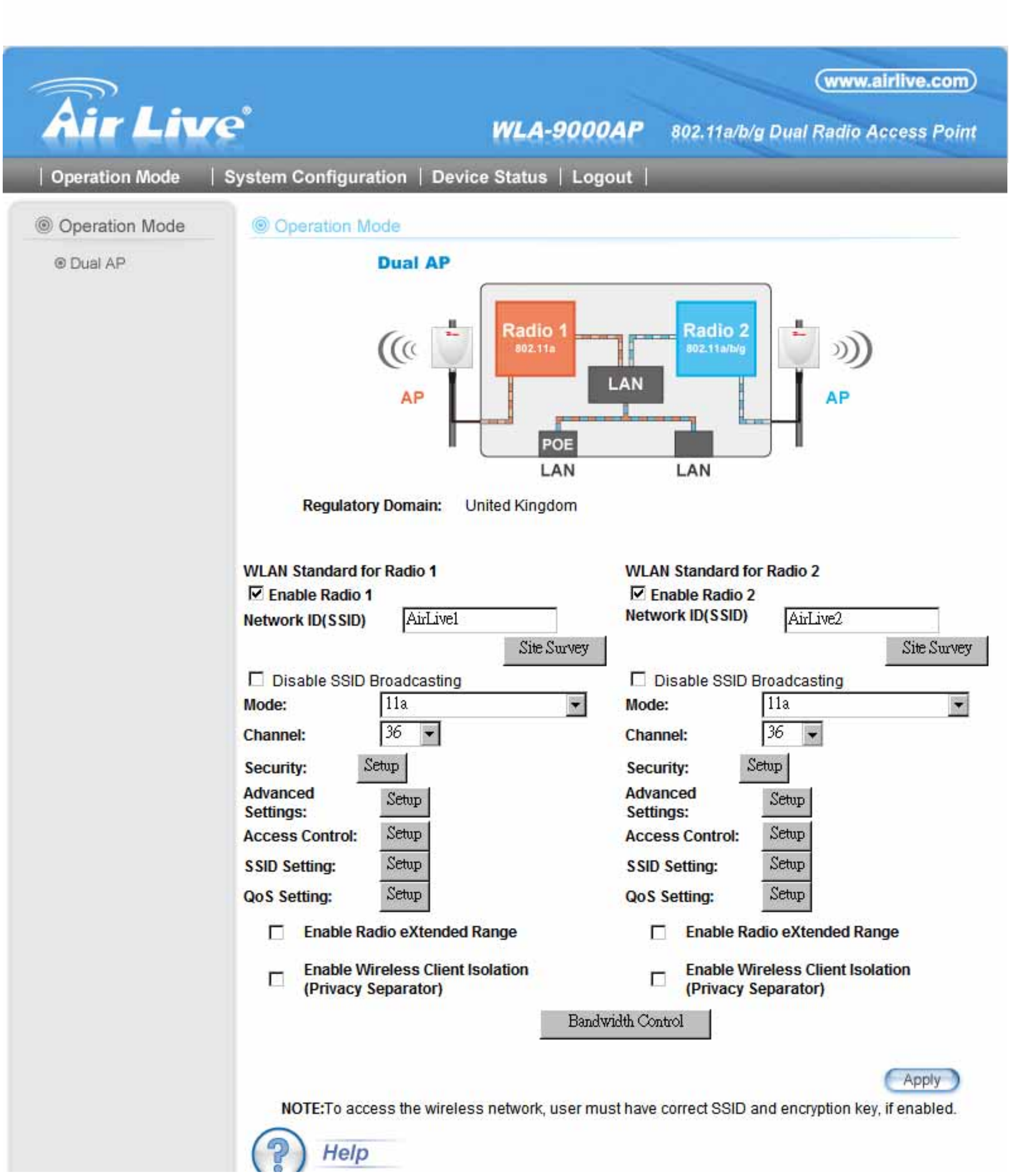
This tells your current Operation Mode now

Select one of the wireless operation modes here

After you select the new operation mode, click here to Change.

- **Mode:** The available wireless operation modes for WLA-9000AP. Select one and click on "Change Mode" button to switch between modes.
- **Setup:** Click here to configure the Wireless and WAN(in router mode) settings.

Once you click on the "Setup" page, the wireless settings will appear.


www.airlive.com
WLA-9000AP 802.11a/b/g Dual Radio Access Point
| Operation Mode | System Configuration | Device Status | Logout |
Operation Mode
Dual AP
Radio 1 802.11a
Radio 2 802.11a/b/g
LAN
POE
LAN
LAN
AP
AP
Help

Operation Mode

Dual AP

Regulatory Domain: United Kingdom

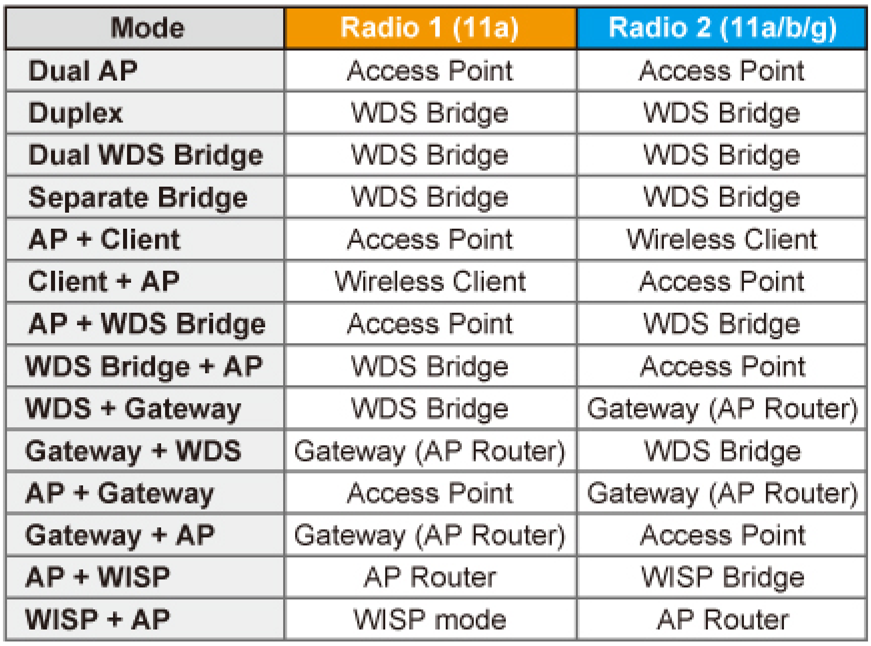
WLAN Standard for Radio 1		WLAN Standard for Radio 2	
☑ Enable Radio 1		☑ Enable Radio 2	
Network ID(SSID)	AirLive1	Network ID(SSID)	AirLive2
	Site Survey		Site Survey
☐ Disable SSID Broadcasting		☐ Disable SSID Broadcasting	
Mode:	11a	Mode:	11a
Channel:	36	Channel:	36
Security:	Setup	Security:	Setup
Advanced Settings:	Setup	Advanced Settings:	Setup
Access Control:	Setup	Access Control:	Setup
SSID Setting:	Setup	SSID Setting:	Setup
QoS Setting:	Setup	QoS Setting:	Setup
☐ Enable Radio eXtended Range		☐ Enable Radio eXtended Range	
☐ Enable Wireless Client Isolation (Privacy Separator)		☐ Enable Wireless Client Isolation (Privacy Separator)	

Bandwidth Control

Apply

NOTE:To access the wireless network, user must have correct SSID and encryption key, if enabled.

The WLA-9000AP device provides all 14 modes of wireless operational applications with:



Mode	Radio 1 (11a)	Radio 2 (11a/b/g)
Dual AP	Access Point	Access Point
Duplex	WDS Bridge	WDS Bridge
Dual WDS Bridge	WDS Bridge	WDS Bridge
Separate Bridge	WDS Bridge	WDS Bridge
AP + Client	Access Point	Wireless Client
Client + AP	Wireless Client	Access Point
AP + WDS Bridge	Access Point	WDS Bridge
WDS Bridge + AP	WDS Bridge	Access Point
WDS + Gateway	WDS Bridge	Gateway (AP Router)
Gateway + WDS	Gateway (AP Router)	WDS Bridge
AP + Gateway	Access Point	Gateway (AP Router)
Gateway + AP	Gateway (AP Router)	Access Point
AP + WISP	AP Router	WISP Bridge
WISP + AP	WISP mode	AP Router

4.2.1 Network SSID

Operation Mode -> Setup -> Network SSID

The SSID is the network name used to identify a wireless network. The SSID must be the same for all devices in the same wireless network. In WLA-9000AP; it is possible to create more than one SSID in AP and AP Router mode, please check the "Multiple SSID & VLAN" section in this chapter. Conversely, several access points on a network can have the same SSID. The SSID length is up to 32 characters. The default SSID is "**airlive**".

- **Enable Radio 1/2**: The default wireless is on. You can uncheck this box to disable wireless interface.
- **Disable SSID Broadcasting**: If you check this box, the SSID will be hidden; only users who know the SSID can associate with this network.

4.2.2 Site Survey

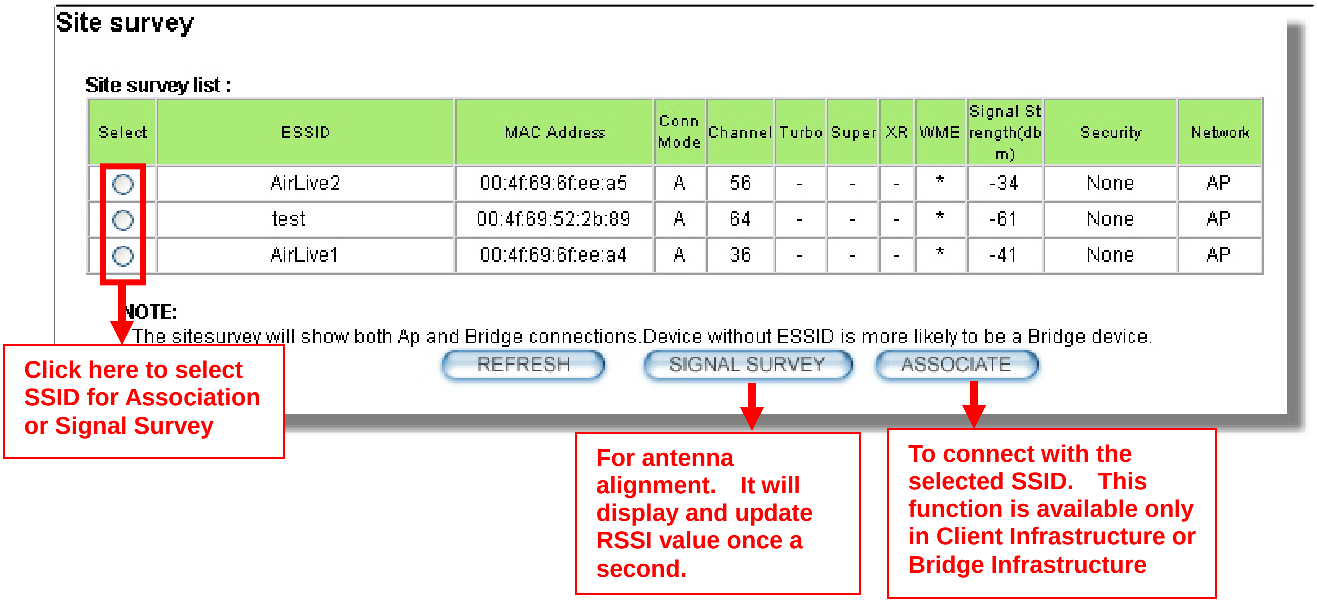
Operation Mode -> Setup -> Site Survey

The Site Survey function in WLA-9000AP provides 4 important functions

- In Client and Bridge Infrastructure mode, site survey will scan for available AP network. Then allow user to select and connect to the AP. This greatly simplify the installation
- Once Site Survey displays the available AP or Bridge networks, you can select a particular SSID to display its RSSI value continuously. This function is called "Signal Survey". Signal Survey can be used for antenna alignment. For detail explanation of about RSSI value, please visit "How to Make Antenna Alignment" Chapter.

- For WDS Bridge mode, the Site Survey will scan for available AP and Bridge networks. User can then find the MAC address (BSSID) of the remote Bridges.
- For AP and AP router mode, the Site Survey allows administrator to check what channels are already occupied for choosing a cleaner channel.

When you click on Site Survey, the following screen will appear. It might take a few minutes to scan all the channels in the 5GHz spectrum.



Site survey

Site survey list :

Select	ESSID	MAC Address	Conn Mode	Channel	Turbo	Super	XR	WME	Signal Strength(dbm)	Security	Network
○	AirLive2	00:4f:69:6f:ee:a5	A	56	-	-	-	*	-34	None	AP
○	test	00:4f:69:52:2b:89	A	64	-	-	-	*	-61	None	AP
○	AirLive1	00:4f:69:6f:ee:a4	A	36	-	-	-	*	-41	None	AP

NOTE:
The sitesurvey will show both Ap and Bridge connections.Device without ESSID is more likely to be a Bridge device.

Click here to select SSID for Association or Signal Survey

For antenna alignment. It will display and update RSSI value once a second.

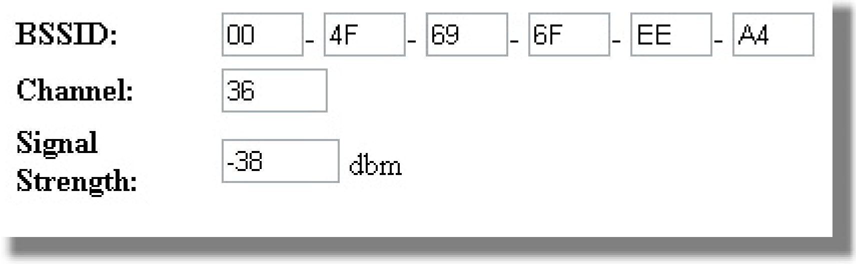
To connect with the selected SSID. This function is available only in Client Infrastructure or Bridge Infrastructure

- **Associate**: Please choose a SSID before click on this button. This button is available only in Client Infrastructure or Bridge Infrastructure modes. Once you click on this button, WLA-9000AP will attempt to make a connection with the selected ESSID. If there is encryption needed, the WLA-9000AP will prompt you to enter the encryption key. Please make sure you enter the correct encryption key, the WLA-9000AP will not check whether the encryption key is correct.
- **RSSI**: RSSI is a value to show the Receiver Sensitivity of the WLA-9000AP. In general, remote APs with stronger signal will display higher RSSI values. For RSSI value, the smaller the absolute value is, the stronger the signal. For example, “-50db” has stronger signal than “-80dB”. For outdoor connection, signal stronger than -60dB is considered as a good connection.

4.2.3 Signal Survey

Operation Mode -> Setup -> Site Survey -> Signal Survey

The Signal Survey will continuously display the RSSI value of the selected SSID for antenna alignment purpose. To use Signal Survey function, please enter the “Site Survey” function first; please refer to the instruction in the above section. Once you select the ESSID and click on the “Signal Survey” button, the following screen will appear.



BSSID: 00 - 4F - 69 - 6F - EE - A4

Channel: 36

Signal Strength: -38 dbm

- **BSSID**: This is the remote AP's MAC address.
- **Channel**: The current scanned channel
- **Signal Strength**: This is the RSSI value. It will refresh itself every second. The smaller the absolute value of the RSSI, the stronger the signal. For example -38dbm is stronger than -70dBm.

4.2.4 Radio Mode (11a, SuperA, TurboA)

Operation Mode -> Setup -> Radio Mode

WLA-9000AP has 4 different options for WLAN transmission. All devices in the same network should use the same WLAN mode.

- **11a mode** (normal-A): This is the IEEE standard for WiFi operating in 5GHz frequency band. 11a is the most stable mode. If you are getting packet loss or disconnection using Super-A or Turbo-A mode. Please use 11a mode instead.
- **SuperA:** Super-A add Bursting, Compression, and Fast Frames to increase the speed over 11a mode. If you live in countries that prohibit the channel binding technology (i.e. Europe), you should choose "Super-A" If you need more speed than 11a mode. However, this mode is not as stable as 11a mode.
- **Super-A with Static Turbo**: Turbo mode uses channel binding technology to increase the speed further over Super-A mode. This mode might not be allowed in countries that prohibit channel binding (i.e. some EU countries). This mode will always turn on the turbo mode in all conditions
- **Super-A with Dynamic Turbo**: Dynamic Turbo mode will be turn on only when adjacent channel is not used. It is also know as intelligent turbo mode. This mode might not be allowed in countries that prohibit channel binding (i.e. some EU countries). In addition, this mode does not work in WDS Bridge mode.

4.2.5 Channel

Operation Mode -> Setup -> Channel

The channel is the frequency range used by radio. In 802.11a standard, each channel occupies 20MHz width. For 2 wireless devices to connect, they must use the same channel. The number of available legal channels might be different between countries. For example, Channel 149 to 161 are available only to United States and a few other countries. If you are living outside EU, please change the country from the "*Regulatory Domain*" option in this page. Below is the table list of channels and frequency.

Frequency Domain	Channel	Frequency (MHz)
5.15 to 5.25GHz U-NII Low ETSI Band1	36	5180
	40	5200
	44	5220
	48	5240
5.25 to 5.35GHz U-NII Mid ETSI Band1	52	5260
	56	5280
	60	5300
	64	5320
5.47 to 5.725GHz U-NII World Wide ETSI Band3	100	5500
	104	5520
	108	5540
	112	5560
	116	5580
	120	5600
	124	5620
	128	5640
	132	5660
	136	5680
	140	5700

**Super Channel is NOT available in EU countries*

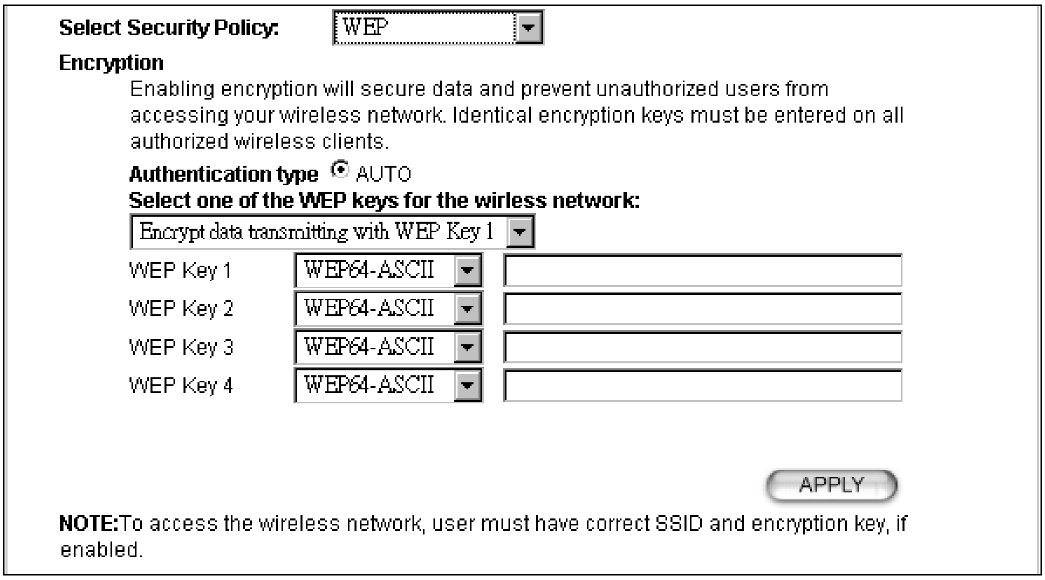
4.2.6 Security Settings

Operation Mode -> Setup -> Security Settings

Security settings allow you to use encryption to secure your data from eavesdropping. You can select different security policy to provide association authentication and/or data encryption. The WLA-9000AP features various security policies including WEP, 802.1x, WPA, WPA-PSK, WPA2, WPA2-PSK, WPA-Auto, and WPA-PSK-Auto. Please note not all security policies are available in all operation modes. For example, only WEP is available currently in WDS Bridge mode and Client Ad hoc mode. All wireless devices on the same network must use the same security policy. We recommend using WPA-PSK or WPA2-PSK whenever possible. For WDS Bridge and Client Ad hoc mode, we recommend using WEP-152 encryption.

WEP

WEP Encryption is the oldest and most available encryption method. However, it is also the least secure. Due to the limitation of the chipset, only WEP encryption is available for WDS Bridge Pure MAC mode and Client Adhoc mode.



Select Security Policy: WEP

Encryption

Enabling encryption will secure data and prevent unauthorized users from accessing your wireless network. Identical encryption keys must be entered on all authorized wireless clients.

Authentication type ● AUTO

Select one of the WEP keys for the wirless network:

Encrypt data transmitting with WEP Key 1

WEP Key 1	WEP64-ASCII	
WEP Key 2	WEP64-ASCII	
WEP Key 3	WEP64-ASCII	
WEP Key 4	WEP64-ASCII	

NOTE: To access the wireless network, user must have correct SSID and encryption key, if enabled.

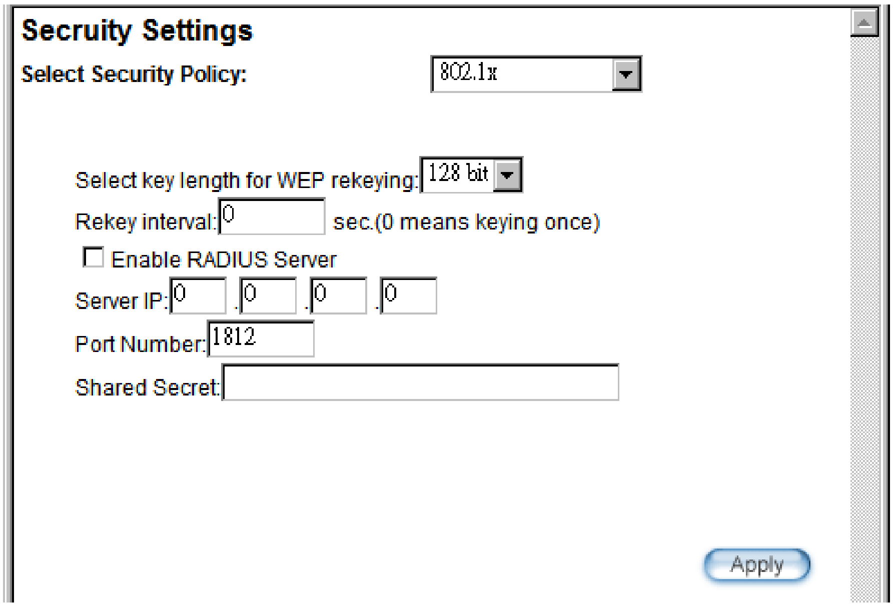
- **Select one of the WEP key for wireless network:** There are total of 4 possible keys for WEP encryption. You need to choose which key will be used for encryption. All wireless devices on the same network have to use the same settings. We recommend using WEP Key 1 as in default setting.

- **WEP Keys:** Please enter the WEP keys used for encryption. You need to fill at least the "Select WEP Key". For example; if you choose "Encrypt Data with WEP Key 1" in the previous field, then it is necessary to fill WEP Key 1. The length of key is dependant on the Key Length and Key type you choose.
  - **Key Length:** The WLA-9000AP offers 64bit, 128 bit, and 152 bit for WEP key length. The longer the Key Length, the more secure the encryption is.
  - **Key Type:** 2 types are available: ASCII and HEX. ASCII is a string of ASCII code including alphabetical characters, space, signs and numbers (i.e. "airlivepass12"). HEX is a string of 16-bit hexadecimal digits (0..9, a, b, c, d, e, f). All wireless devices on the network must match the exact key length and Key type. Some Wireless clients only allow HEX type for WEP.
  - **ASCII-64:** This is a key with 64-bit key length of ASCII type. Please enter **5** ASCII Characters if you choose this option. For example, "passw"
  - **HEX-64:** This is a key with 64-bit key length of HEX type. Please enter **10** Hexadecimal digits if you choose this option. For example, "12345abcdef"
  - **ASCII-128:** This is a key with 64-bit key length of ASCII type. Please enter **13** ASCII Characters if you choose this option. For example, "airlivewepkey"
  - **HEX-128:** This is a key with 128-bit key length of HEX type. Please enter **26** Hexadecimal digits if you choose this option. For example,

"1234567890abcdef1234567890"

- **ASCII-152:** This is a key with 64-bit key length of ASCII type. Please enter **16** ASCII Characters if you choose this option. For example, "airlivewepkey123"
- **HEX-152:** This is a key with 128-bit key length of HEX type. Please enter **32** Hexadecimal digits if you choose this option. For example, "1234567890abcdef1234567890abcdef"

802.1x



Secruity Settings

Select Security Policy: 802.1x

Select key length for WEP rekeying: 128 bit

Rekey interval: 0 sec.(0 means keying once)

□ Enable RADIUS Server

Server IP: 0 . 0 . 0 . 0

Port Number: 1812

Shared Secret:

802.1x allows users to leverage a RADIUS server to do association authentications. You can also enable dynamic WEP key (128 bit) to have data encryption. You do not have to enter the WEP key manually because it will be generated automatically and dynamically.

- **Rekey interval** is time period that the system will change the key periodically. The shorter the interval is, the better the security is.

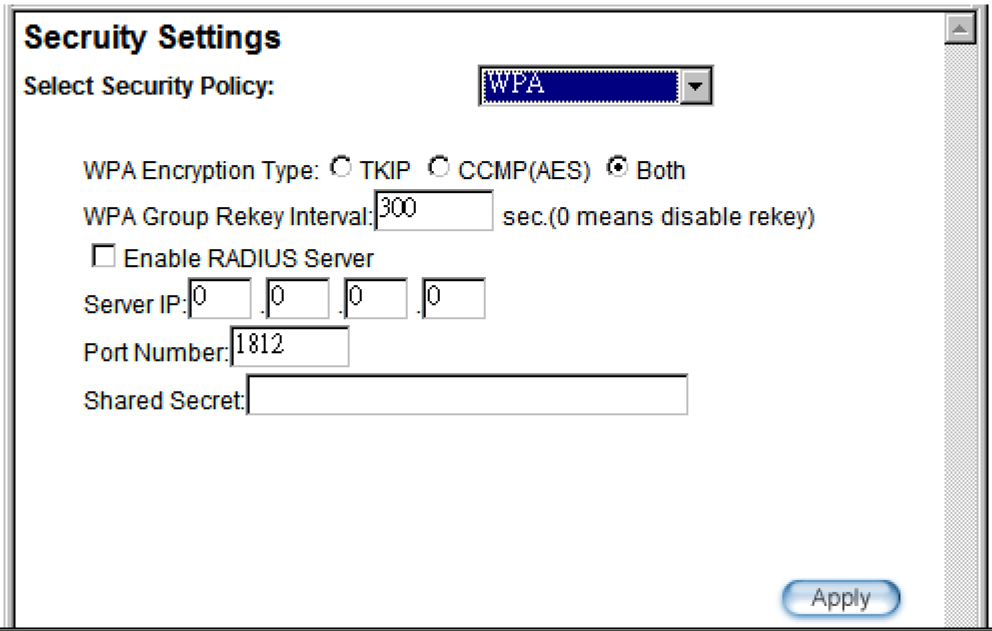
To Enable RADIUS Server:

- **Server IP:** The IP address of the RADIUS server.
- **Port Number:** The port number that your RADIUS server uses for authentication. The default setting is 1812.
- **Shared Secret:** This is used by your RADIUS server in the Shared Secret field in

RADIUS protocol messages. The shared secret configured in the WLA-9000AP must match the shared secret configured in the RADIUS server. The shared secret can contain up to 64 alphanumeric characters.

WPA, WPA2, WPA-AUTO

Wi-Fi Protected Access (WPA) introduces the Temporal Key Integrity Protocol (TKIP) that provides added security. WPA2 adds full support for 802.11i standard and the CCMP (AES Encryption). The WPA-AUTO tries to authenticate wireless clients using WPA or WPA2. All 3 requires a RADIUS server available in order to do authentication (same as 802.1x), thus there is no shared key required.



Secruity Settings

Select Security Policy: WPA

WPA Encryption Type: ○ TKIP ○ CCMP(AES) ● Both

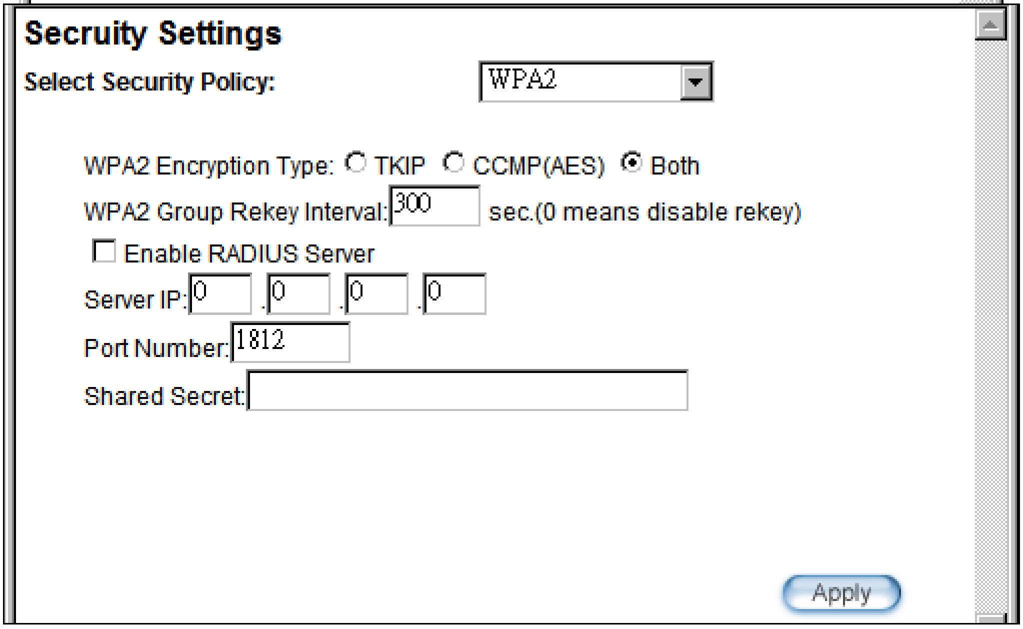
WPA Group Rekey Interval: 300 sec.(0 means disable rekey)

□ Enable RADIUS Server

Server IP: 0 . 0 . 0 . 0

Port Number: 1812

Shared Secret:



Secruity Settings

Select Security Policy: WPA2

WPA2 Encryption Type: ○ TKIP ○ CCMP(AES) ● Both

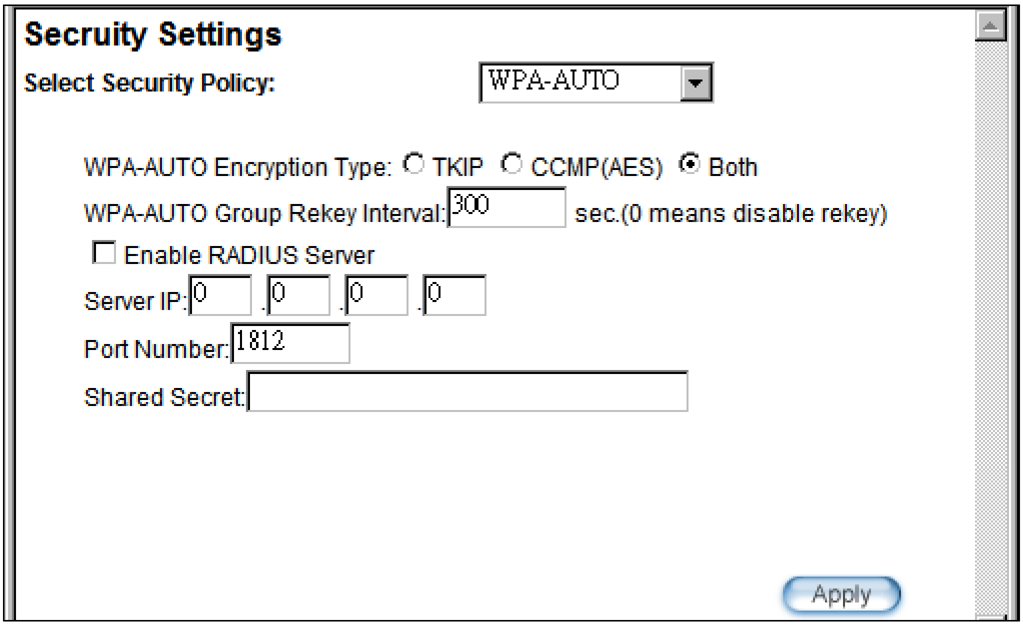
WPA2 Group Rekey Interval: 300 sec.(0 means disable rekey)

□ Enable RADIUS Server

Server IP: 0 . 0 . 0 . 0

Port Number: 1812

Shared Secret:



Secruity Settings

Select Security Policy: WPA-AUTO

WPA-AUTO Encryption Type: ○ TKIP ○ CCMP(AES) ● Both

WPA-AUTO Group Rekey Interval: 300 sec.(0 means disable rekey)

□ Enable RADIUS Server

Server IP: 0 . 0 . 0 . 0

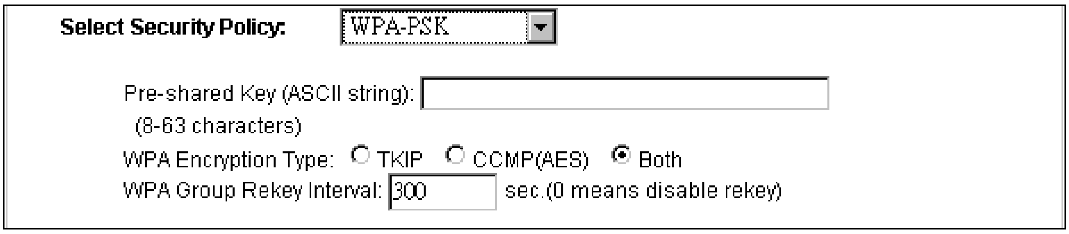
Port Number: 1812

Shared Secret:

- **Encryption Type**: There are two encryption types **TKIP** and **CCMP (AES)**. While CCMP provides better security than TKIP, some wireless client stations may not be equipped with the hardware to support it. You can select **Both** to allow TKIP clients and CCMP clients to connect to the Access Point at the same time.
- **Group Rekey Interval**: A group key is used for multicast/broadcast data, and the re-key interval is time period that the system will change the group key periodically. The shorter the interval is, the better the security is. The default is 300 sec.

WPA-PSK, WPA2-PSK, WPA-PSK-Auto

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. WPA2-PSK adds CCMP and AES encryption for even better security. WPA-PSK-AUTO tries to authenticate wireless clients using WPA-PSK or WPA2-PSK.

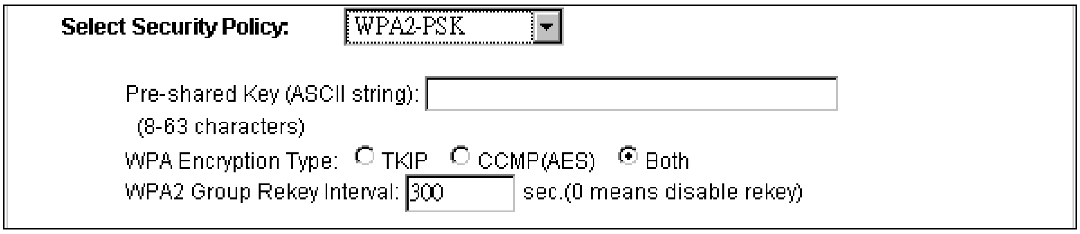


Select Security Policy: WPA-PSK

Pre-shared Key (ASCII string):
(8-63 characters)

WPA Encryption Type: ○ TKIP ○ CCMP(AES) ● Both

WPA Group Rekey Interval: 300 sec.(0 means disable rekey)

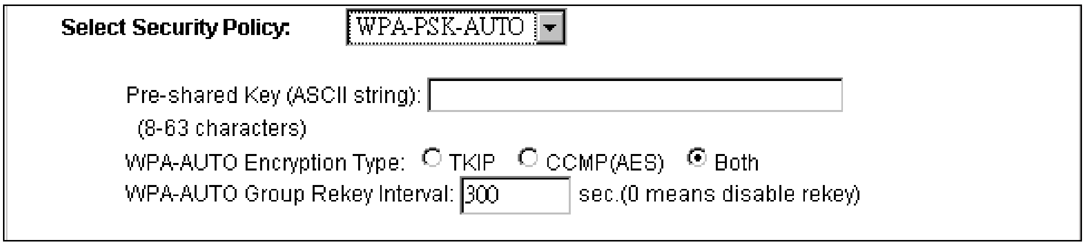


Select Security Policy: WPA2-PSK

Pre-shared Key (ASCII string):
(8-63 characters)

WPA Encryption Type: ○ TKIP ○ CCMP(AES) ● Both

WPA2 Group Rekey Interval: 300 sec.(0 means disable rekey)



Select Security Policy: WPA-PSK-AUTO

Pre-shared Key (ASCII string):
(8-63 characters)

WPA-AUTO Encryption Type: ○ TKIP ○ CCMP(AES) ● Both

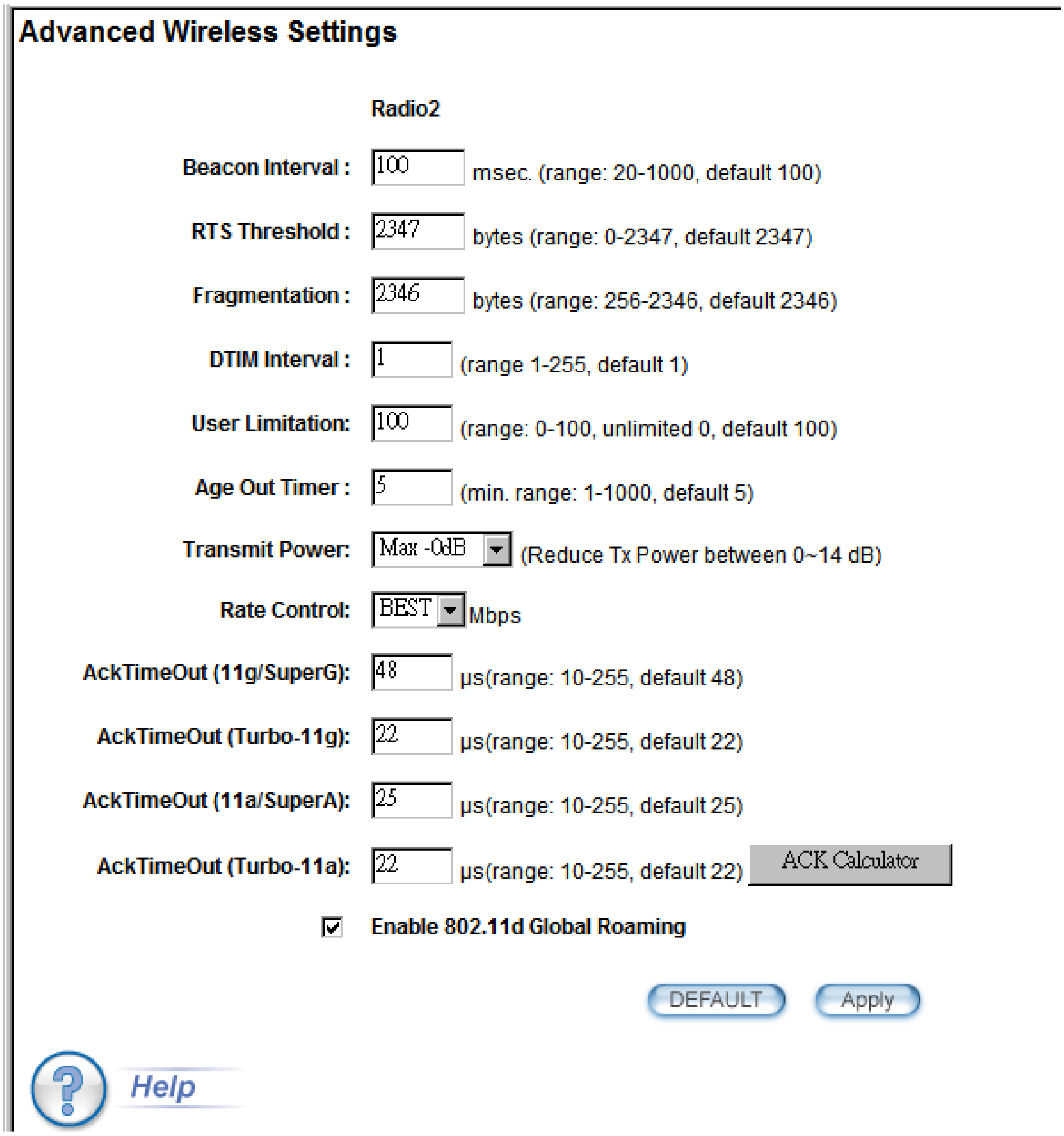
WPA-AUTO Group Rekey Interval: 300 sec.(0 means disable rekey)

- **Pre-shared Key**: This is an ASCII string with 8 to 63 characters. Please make sure that both the WLA-9000AP and the wireless client stations use the same key.
- **Encryption Type**: There are two encryption types **TKIP** and **CCMP (AES)**. While CCMP provides better security than TKIP, some wireless client stations may not be equipped with the hardware to support it. You can select **Both** to allow TKIP clients and CCMP clients to connect to the Access Point at the same time.
- **Group Rekey Interval**: A group key is used for multicast/broadcast data, and the re-key interval is time period that the system will change the group key periodically. The shorter the interval is, the better the security is. The default is 300 sec.

4.2.7 Advance Settings

Operation Mode -> Setup -> Advance Settings

This page includes all the wireless settings that change the RF behaviors of WLA-9000AP. It is important to read through this section before attempting to make changes.



Advanced Wireless Settings

	Radio2
Beacon Interval :	100 msec. (range: 20-1000, default 100)
RTS Threshold :	2347 bytes (range: 0-2347, default 2347)
Fragmentation :	2346 bytes (range: 256-2346, default 2346)
DTIM Interval :	1 (range 1-255, default 1)
User Limitation:	100 (range: 0-100, unlimited 0, default 100)
Age Out Timer :	5 (min. range: 1-1000, default 5)
Transmit Power:	Max -0dB (Reduce Tx Power between 0~14 dB)
Rate Control:	BEST Mbps
AckTimeOut (11g/SuperG):	48 µs(range: 10-255, default 48)
AckTimeOut (Turbo-11g):	22 µs(range: 10-255, default 22)
AckTimeOut (11a/SuperA):	25 µs(range: 10-255, default 25)
AckTimeOut (Turbo-11a):	22 µs(range: 10-255, default 22) ACK Calculator

☑ Enable 802.11d Global Roaming

4.2.7.1 Beacon Interval

The device broadcasts beacon frames regularly to announce its existence. The beacon Interval specifies how often beacon frames are transmitted in time unit of milliseconds. The default value is **100**, and a valid value should be between 1 and 65,535.

4.2.7.2 RTS Threshold

RTS/CTS frames are used to gain control of the medium for transmission. Any unicast (data or control) frames larger than specified RTS threshold must be transmitted following the RTS/CTS handshake exchange mechanism. The RTS threshold should have a value between 256-2347 bytes, with a default of **2347**. It is recommended that this value does not deviate from the default too much.

4.2.7.3 Fragmentation

When the size of a unicast frame exceeds the fragmentation threshold, it will be fragmented before the transmission. It should have a value of 256-2346 bytes, with a default of 2346. If you experience a high packet error rate, you should slightly decrease the Fragmentation Threshold.

4.2.7.4 DTIM Interval

The WLA-9000AP buffers packets for stations that operate in the power-saving mode. The Delivery Traffic Indication Message (DTIM) informs such power-conserving stations that there are packets waiting to be received by them. The DTIM interval specifies how often the beacon frame should contain DTIMs. It should have a value between 1 to 255. Default value is 1.

4.2.7.5 User Limitation

This limitation applies to number of wireless clients the device can associate. If you need serving wireless connection to large number of users in one location. You can deploy many APs and limit the number of wireless clients, so any additional wireless connection attempt will be rejected (therefore, redirect to other AP). The range of user limitation is from 1 to 100.

4.2.7.6 Age Out Timer

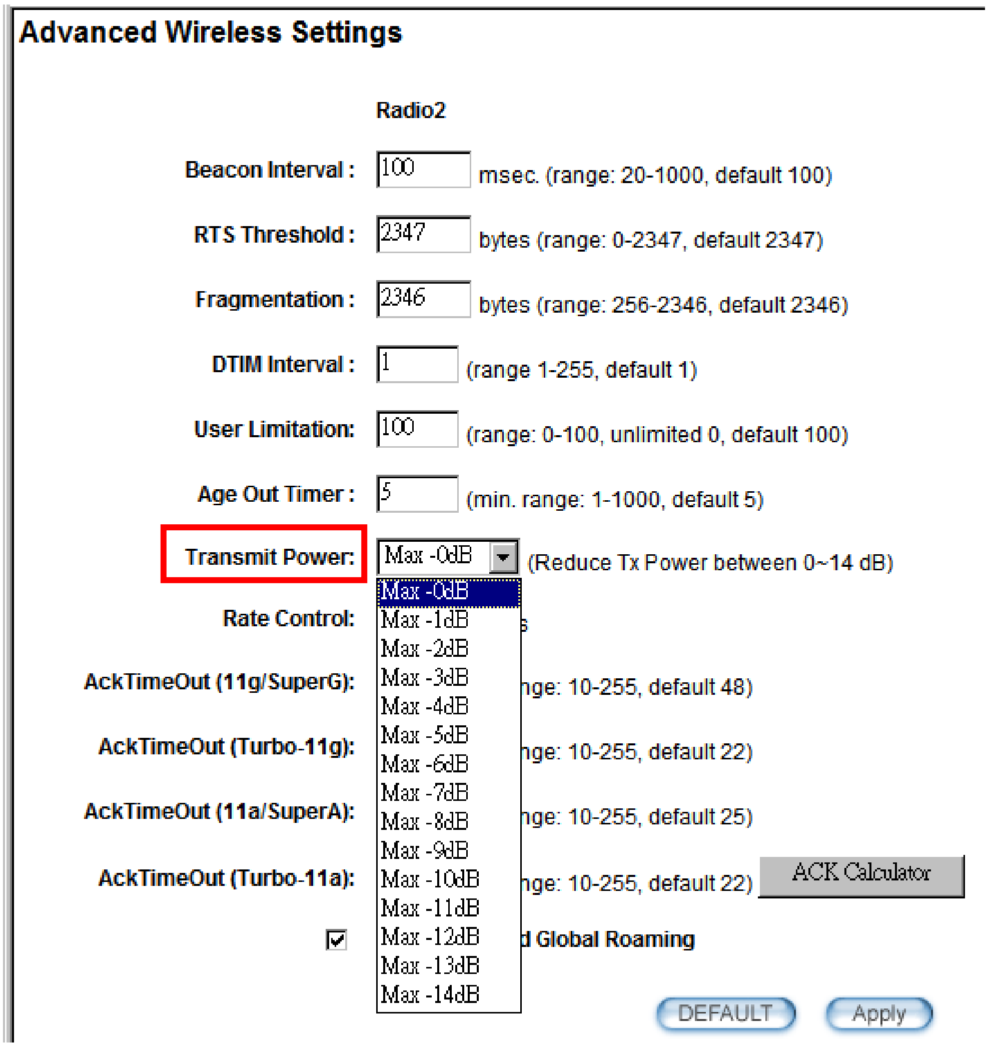
Set the age out timer for the wireless client. If there is no traffic from client for more than the timer, the wireless client will be dropped. The default is 300 sec. This function is available only for the Access Point and AP router mode.

4.2.7.7 Transmit Power

You can adjust the transmit output power of the WLA-9000AP’s radio from 10dBm to 24dBm. The higher the output power, the more distance WLA-9000AP can deliver. However, it is advised that you use just enough output power so it will not create excessive interference for the environment. Also, using too much power at close distance can create serious performance drop due to signal distortion.

At less than 200meter distance, the best output power is about 14dBm. At 2km distance;

the best output power setting is 18dBm for “11a” and “Super-A without Turbo”, 24dBm for “Super-A with Static/Dynamic Turbo”.



Advanced Wireless Settings

Radio2

Beacon Interval : 100 msec. (range: 20-1000, default 100)

RTS Threshold : 2347 bytes (range: 0-2347, default 2347)

Fragmentation : 2346 bytes (range: 256-2346, default 2346)

DTIM Interval : 1 (range 1-255, default 1)

User Limitation: 100 (range: 0-100, unlimited 0, default 100)

Age Out Timer : 5 (min. range: 1-1000, default 5)

Transmit Power: Max -0dB (Reduce Tx Power between 0~14 dB)

Rate Control: s

AckTimeOut (11g/SuperG): nge: 10-255, default 48)

AckTimeOut (Turbo-11g): nge: 10-255, default 22)

AckTimeOut (11a/SuperA): nge: 10-255, default 25)

AckTimeOut (Turbo-11a): nge: 10-255, default 22)

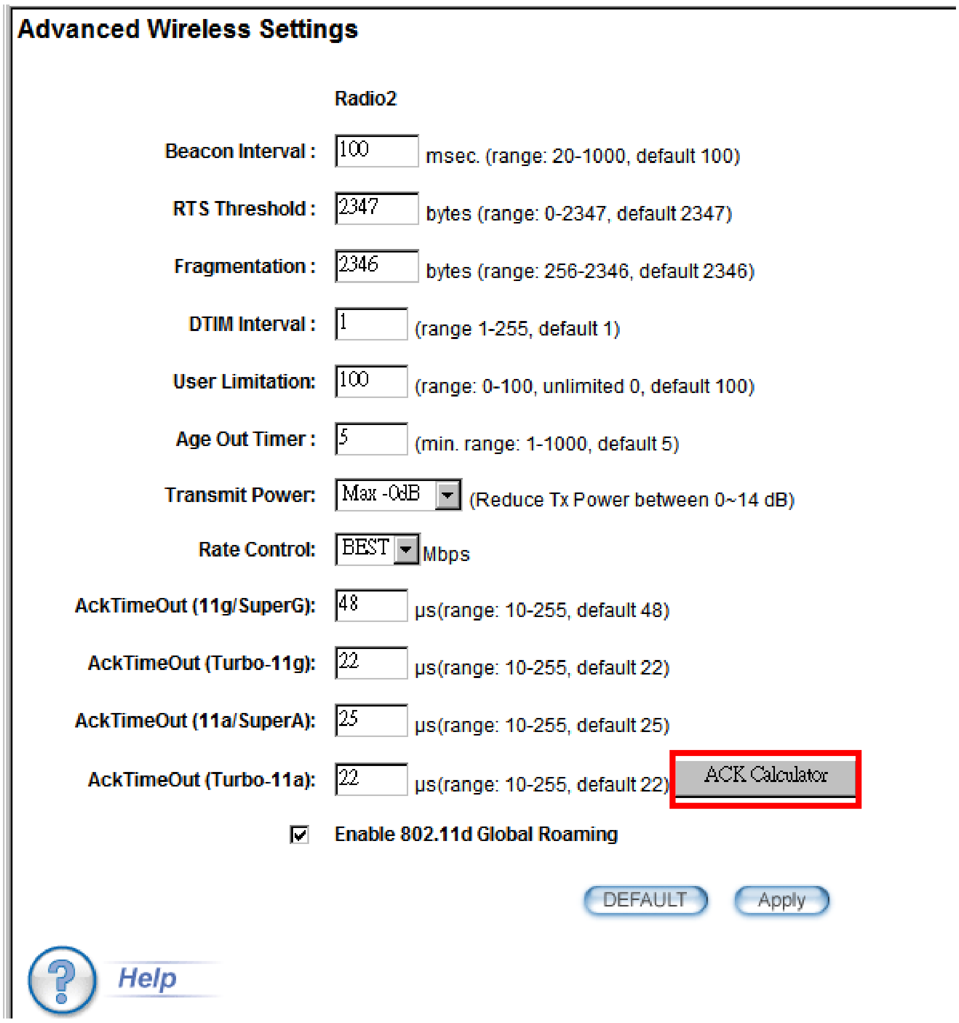
☑ d Global Roaming

4.2.7.8 Rate Control

Select here to change the Data Rate for the radio. Lower data rate sometimes provide longer distance. In most cases, however, we recommend to keep the setting at “Best”.

4.2.7.9 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. The station will only wait for a certain amount of time, this time is called the ACK timeout. 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. If the ACK setting is too low then the ACK window will have expired and the returning packet will be dropped, greatly lowering throughput. By having the ability to adjust the ACK setting we can effectively optimize the throughput over long distance links.



Advanced Wireless Settings

Radio2

Beacon Interval : 100 msec. (range: 20-1000, default 100)

RTS Threshold : 2347 bytes (range: 0-2347, default 2347)

Fragmentation : 2346 bytes (range: 256-2346, default 2346)

DTIM Interval : 1 (range 1-255, default 1)

User Limitation: 100 (range: 0-100, unlimited 0, default 100)

Age Out Timer : 5 (min. range: 1-1000, default 5)

Transmit Power: Max -0dB (Reduce Tx Power between 0~14 dB)

Rate Control: BEST Mbps

AckTimeOut (11g/SuperG): 48 μs(range: 10-255, default 48)

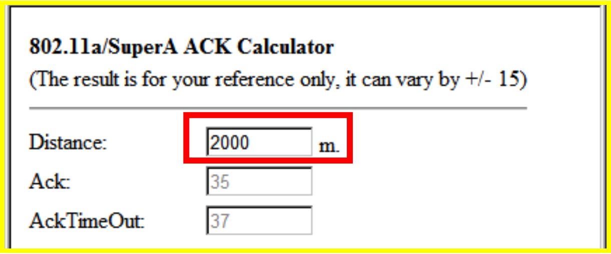
AckTimeOut (Turbo-11g): 22 μs(range: 10-255, default 22)

AckTimeOut (11a/SuperA): 25 μs(range: 10-255, default 25)

AckTimeOut (Turbo-11a): 22 μs(range: 10-255, default 22)

☑ Enable 802.11d Global Roaming

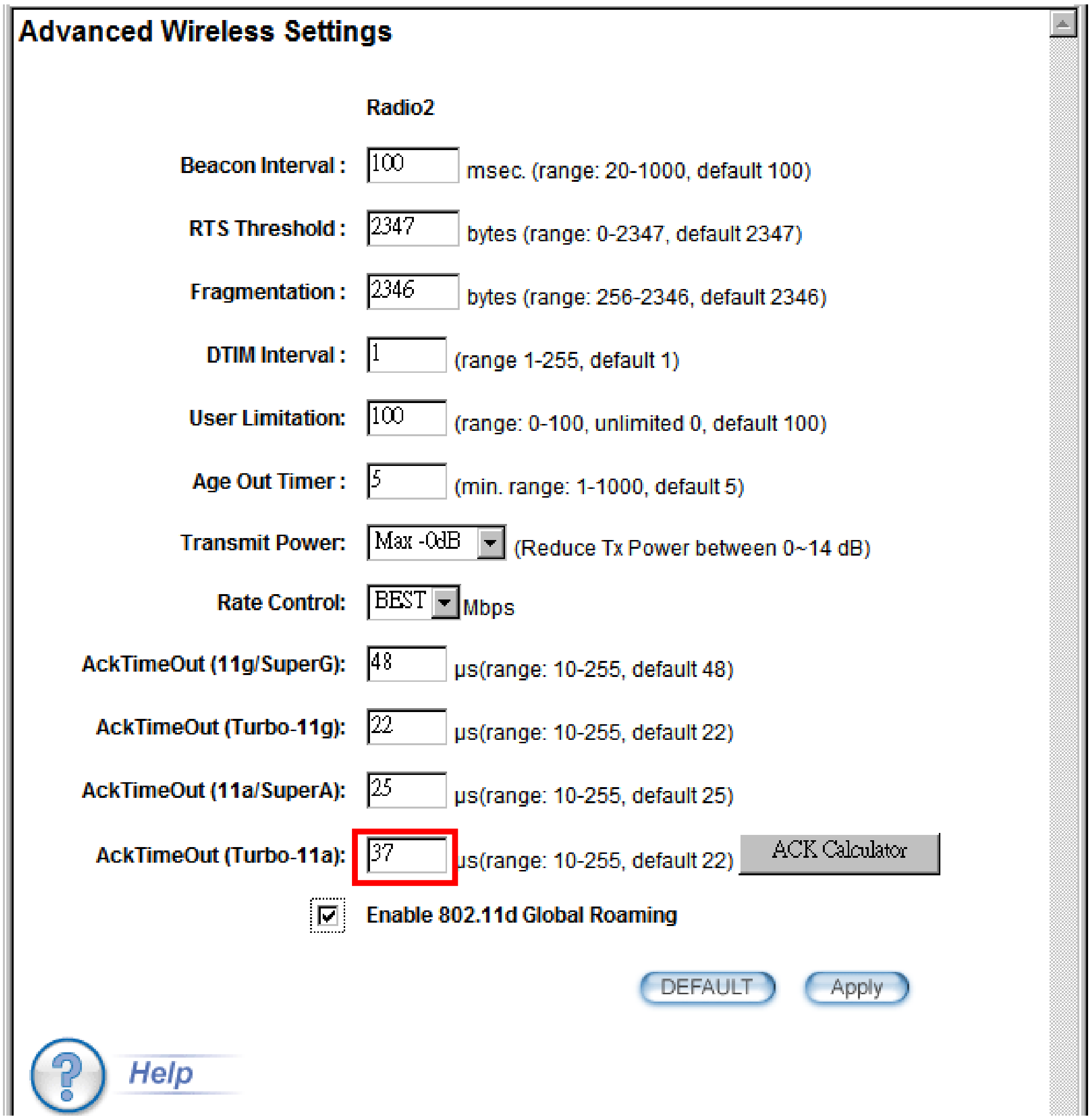
1. Click “**ACK calculator**” and it will pop up
2. Enter the distance to the remote wireless device here. The WLA-9000AP will then calculate the appropriate ACK Timeout value automatically



802.11a/SuperA ACK Calculator
(The result is for your reference only, it can vary by +/- 15)

Distance: 2000 m.
Ack: 35
AckTimeOut: 37

3. Please type ACK Timeout value into column. It is very important that you enter the correct distance for long distance connection. Failure to do so will result in poor performance.



Advanced Wireless Settings

Radio2

Beacon Interval : 100 msec. (range: 20-1000, default 100)

RTS Threshold : 2347 bytes (range: 0-2347, default 2347)

Fragmentation : 2346 bytes (range: 256-2346, default 2346)

DTIM Interval : 1 (range 1-255, default 1)

User Limitation: 100 (range: 0-100, unlimited 0, default 100)

Age Out Timer : 5 (min. range: 1-1000, default 5)

Transmit Power: Max -0dB (Reduce Tx Power between 0~14 dB)

Rate Control: BEST Mbps

AckTimeOut (11g/SuperG): 48 µs(range: 10-255, default 48)

AckTimeOut (Turbo-11g): 22 µs(range: 10-255, default 22)

AckTimeOut (11a/SuperA): 25 µs(range: 10-255, default 25)

AckTimeOut (Turbo-11a): 37 µs(range: 10-255, default 22)

☑ Enable 802.11d Global Roaming

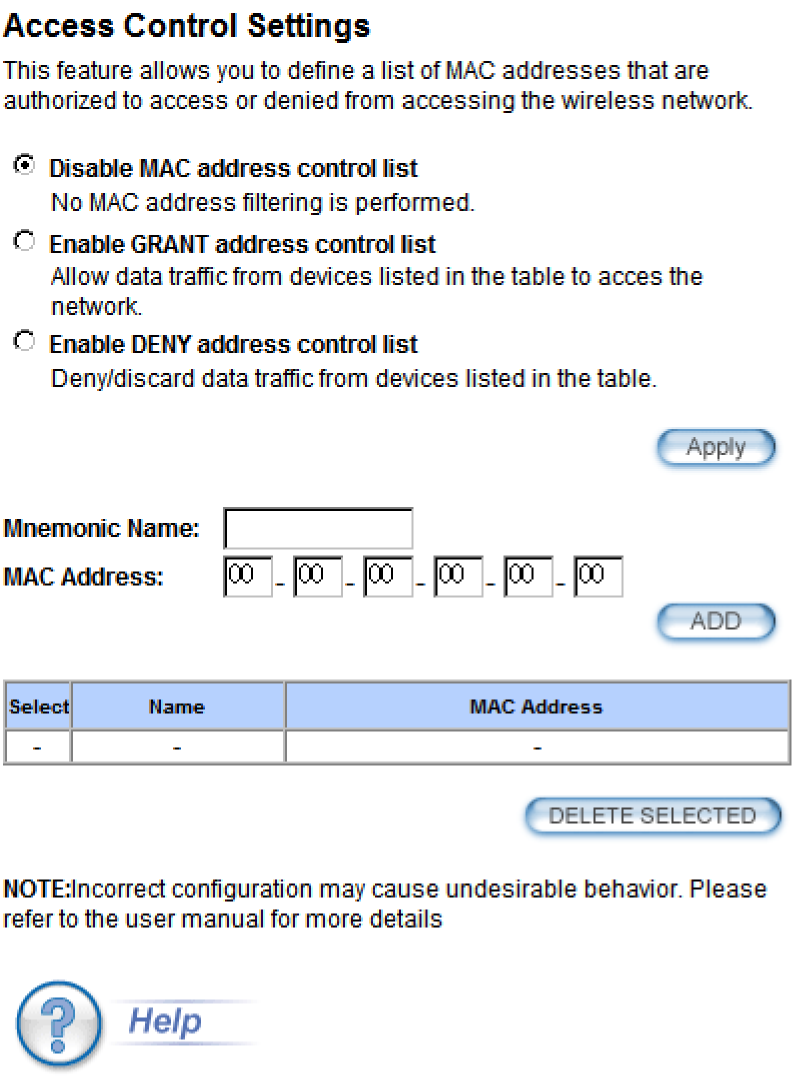
4.2.7.10 Enable 802.11d Global Roaming

It is a standard for use in countries where systems using other standards in the 802.11 family are not allowed to operate.

4.2.8 Access Control (ACL)

Operation Mode -> Setup -> Access Control

The WLA-9000AP allows you to define a list of MAC addresses that are allowed or denied to access the wireless network. This function is available only for Access Point and AP Router modes.



Access Control Settings

This feature allows you to define a list of MAC addresses that are authorized to access or denied from accessing the wireless network.

● **Disable MAC address control list**
No MAC address filtering is performed.

○ **Enable GRANT address control list**
Allow data traffic from devices listed in the table to acces the network.

○ **Enable DENY address control list**
Deny/discard data traffic from devices listed in the table.

Mnemonic Name:

MAC Address: 00 - 00 - 00 - 00 - 00 - 00

Select	Name	MAC Address
-	-	-

NOTE: Incorrect configuration may cause undesirable behavior. Please refer to the user manual for more details

- **Disable MAC address control list:** When selected, no MAC address filtering will be performed.

- **Enable GRANT address control list:** When selected, data traffic from only the specified devices in the table will be allowed in the network.

- **Enable DENY address control list:** When selected, data traffic from the devices specified in the table will be denied/discarded by the network.

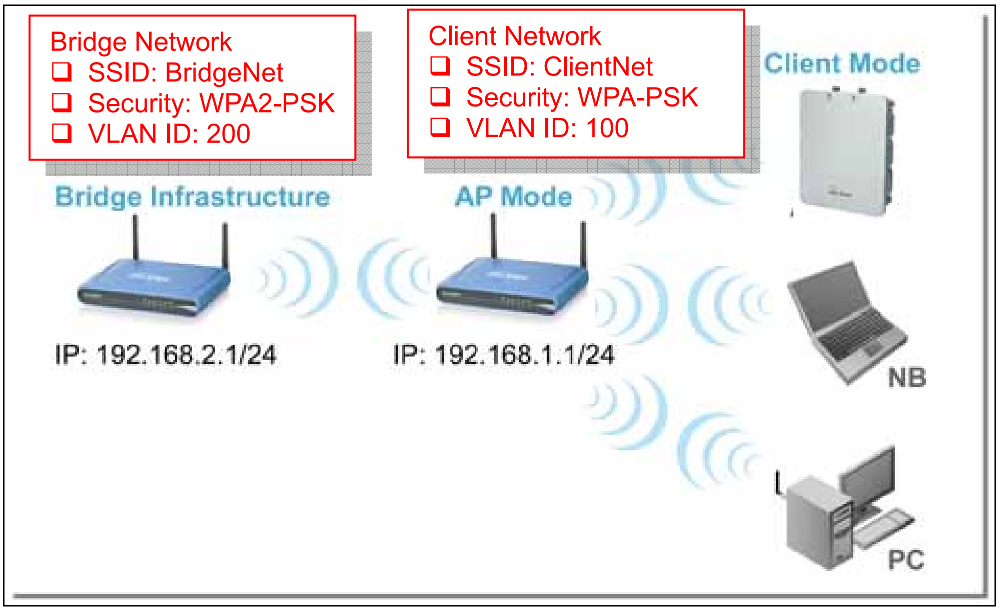
To add a MAC address into the table, enter a *Mnemonic Name* and the *MAC Address*, and then click *Add*. The table lists all configured MAC Filter entries.

To delete entries, check the corresponding *Select* boxes and then press *Delete Selected*.

4.2.9 Multiple SSID

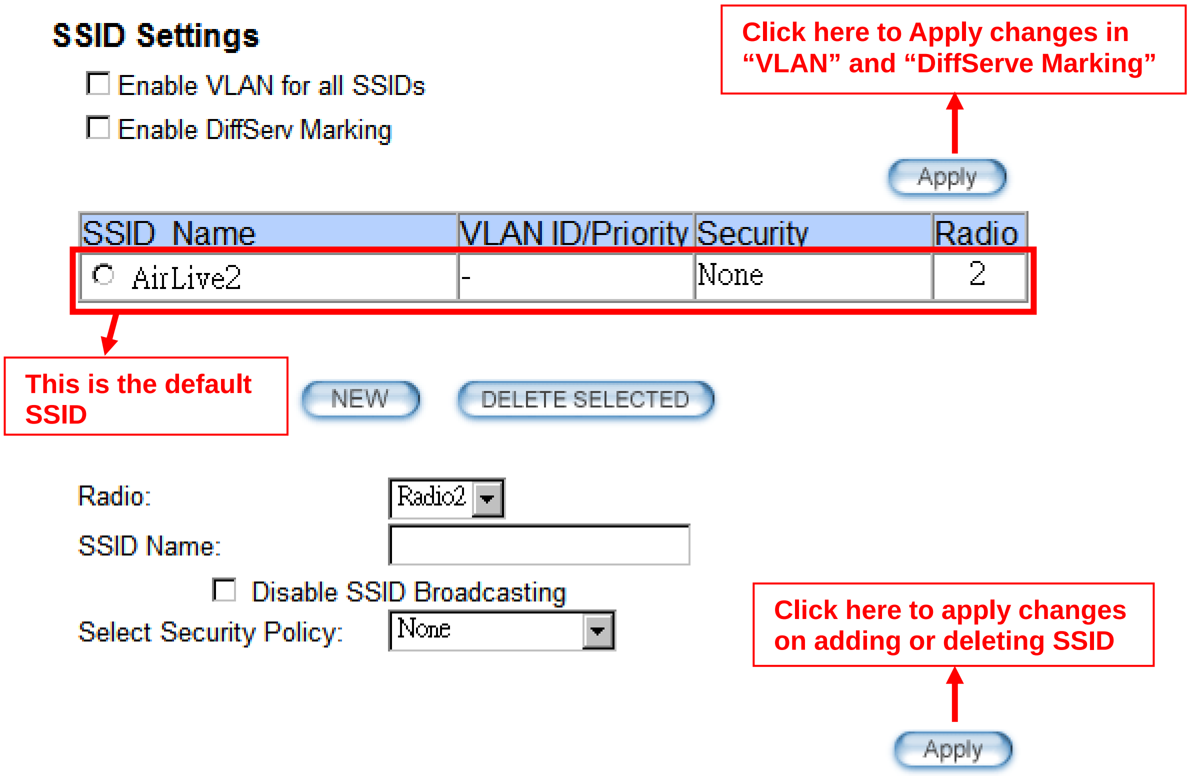
Operation Mode -> Setup -> Multiple SSID

This function is available only for Access Point and AP Router modes. Multiple SSID allows WLA-9000AP to create up to **4** different wireless networks (SSID). It is also known as "Virtual AP" function. Each SSID can have its Encryption type, VLAN Tag, and TOS settings. In the following diagram, the WLA-9000AP uses Multiple SSID function to create separate Bridge and Client network. Each has its own encryption policies.



Configuring the Multiple SSID

When you click on the "Multiple SSID" button, the following screen will appear



SSID Settings

□ Enable VLAN for all SSIDs

□ Enable DiffServ Marking

Click here to Apply changes in “VLAN” and “DiffServe Marking”

SSID Name	VLAN ID/Priority	Security	Radio
○ AirLive2	-	None	2

This is the default SSID

Radio: Radio2

SSID Name:

□ Disable SSID Broadcasting

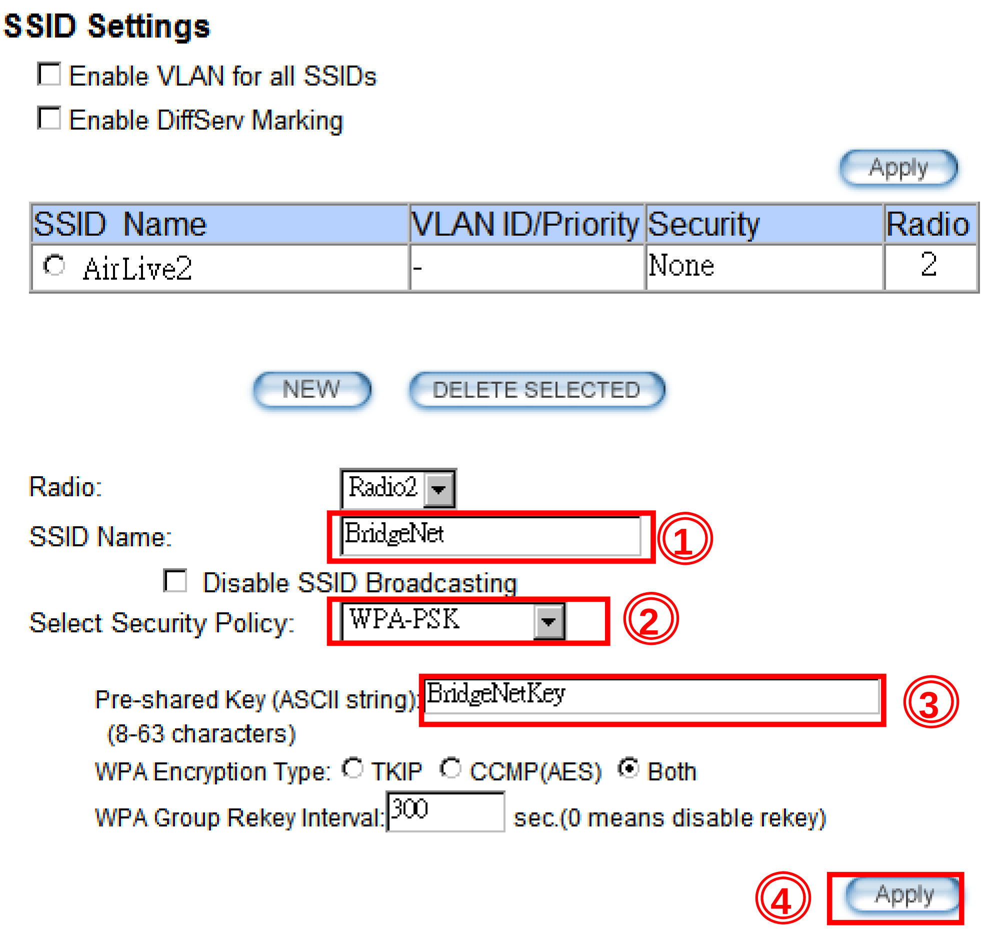
Select Security Policy: None

Click here to apply changes on adding or deleting SSID

How to add a SSID

You can add up to 4 SSID in WLA-9000AP. Please follow the procedure below:

1. Enter the SSID name (i.e. BridgeNet)
2. Select the Security Policy (i.e. WPA2-PSK)
3. Enter the Security Key (i.e. BridgeNetKey).
4. Click on “Apply” to add SSID



SSID Settings

□ Enable VLAN for all SSIDs

□ Enable DiffServ Marking

Apply

SSID Name	VLAN ID/Priority	Security	Radio
○ AirLive2	-	None	2

NEW DELETE SELECTED

Radio: Radio2

SSID Name: BridgeNet

□ Disable SSID Broadcasting

Select Security Policy: WPA-PSK

Pre-shared Key (ASCII string): BridgeNetKey
(8-63 characters)

WPA Encryption Type: ○ TKIP ○ CCMP(AES) ● Both

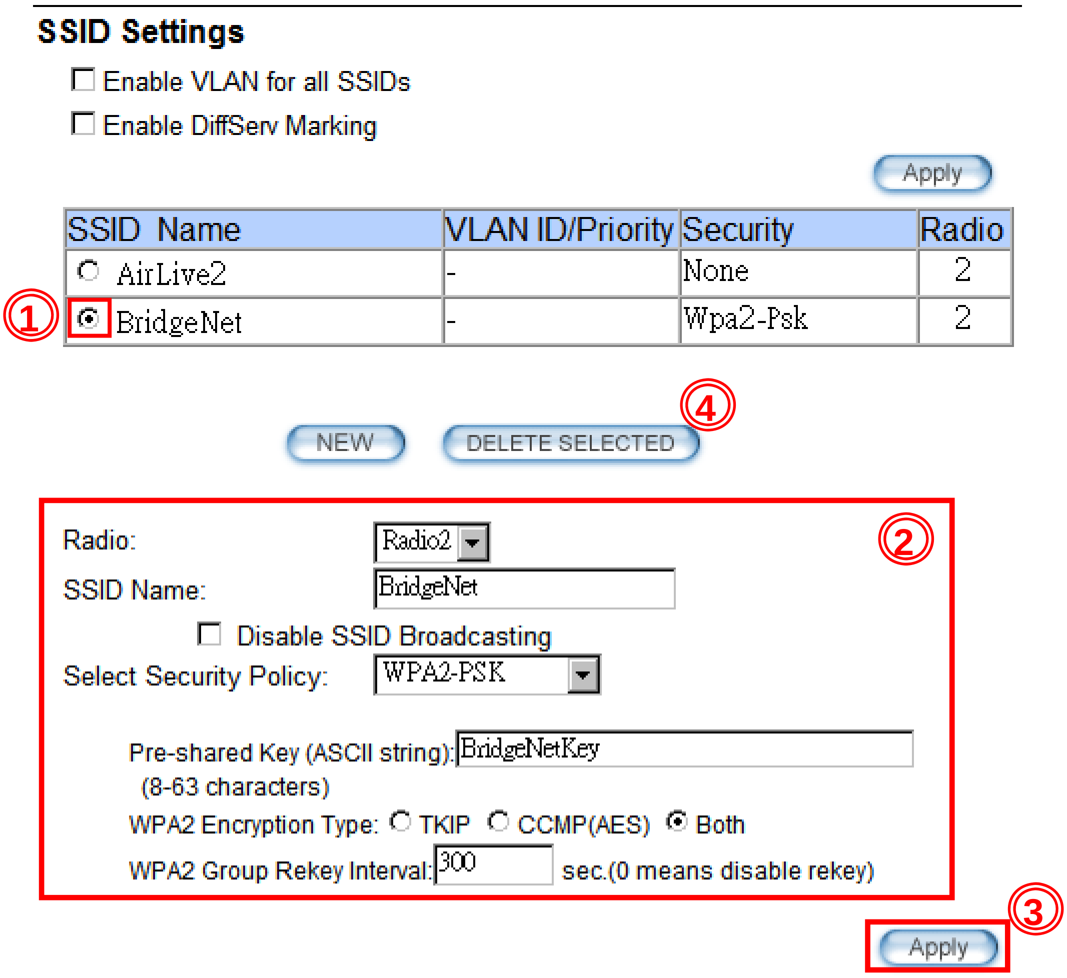
WPA Group Rekey Interval: 300 sec.(0 means disable rekey)

Apply

How to Modify or Delete a SSID

Please follow the procedure below:

1. Select the SSID you want to modify or delete
2. The SSID’s settings will be displayed in the box area. Modify any settings.
3. Click on “Apply” to complete the modification
4. Or click on “Delete Selected” to delete the SSID



SSID Settings

☐ Enable VLAN for all SSIDs

☐ Enable DiffServ Marking

Apply

SSID Name	VLAN ID/Priority	Security	Radio
○ AirLive2	-	None	2
● BridgeNet	-	Wpa2-Psk	2

NEW DELETE SELECTED

Radio: Radio2

SSID Name: BridgeNet

☐ Disable SSID Broadcasting

Select Security Policy: WPA2-PSK

Pre-shared Key (ASCII string): BridgeNetKey
(8-63 characters)

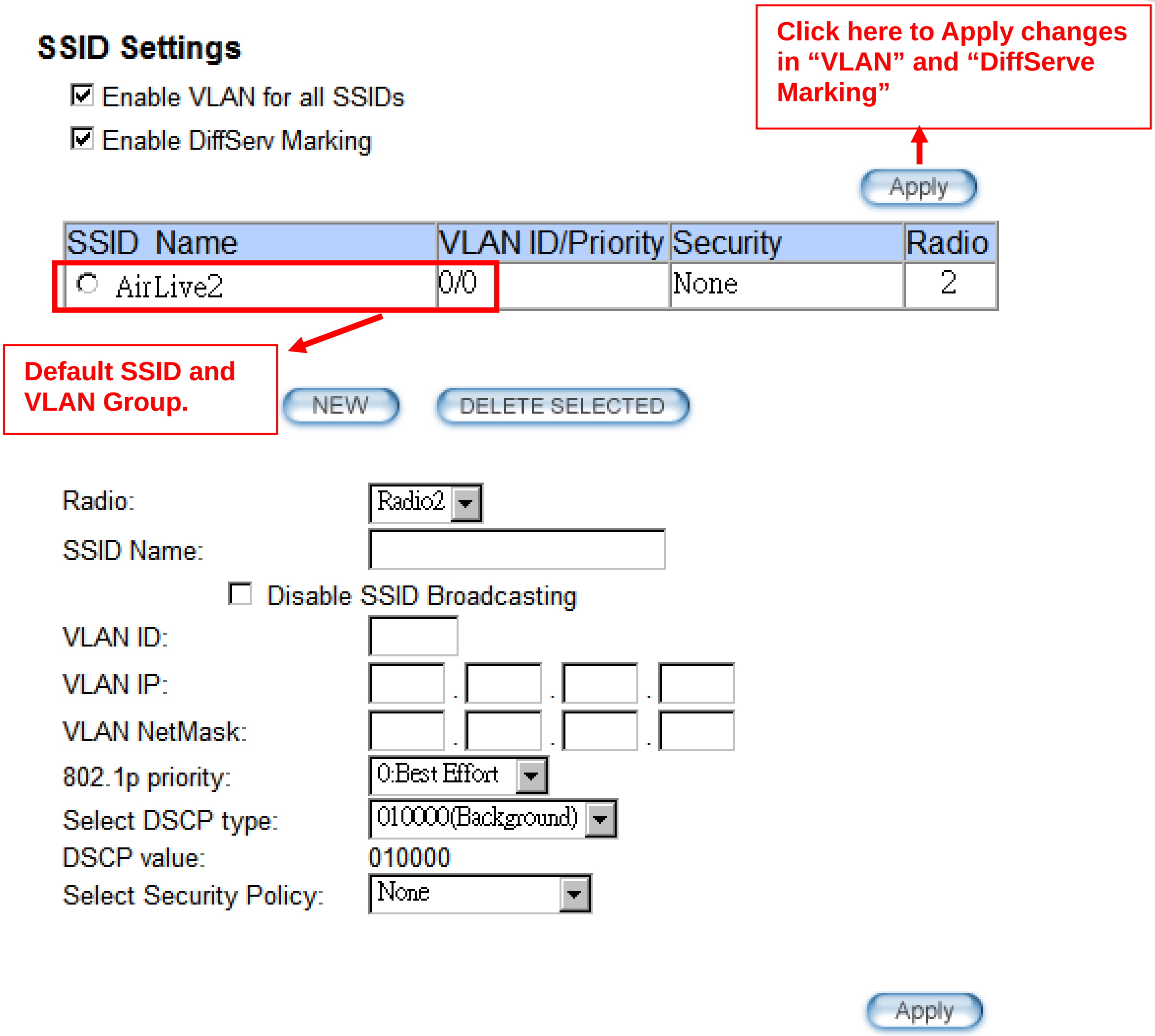
WPA2 Encryption Type: ○ TKIP ○ CCMP(AES) ● Both

WPA2 Group Rekey Interval: 300 sec.(0 means disable rekey)

Apply

Configure the VLAN and DiffServ Markings

When you check the *Enable VLAN for All SSIDs* and/or *Enable DiffServ Marking*, the following screen will appear:



Click here to Apply changes in “VLAN” and “DiffServe Marking”

Default SSID and VLAN Group.

SSID Settings

☑ Enable VLAN for all SSIDs

☑ Enable DiffServ Marking

SSID Name	VLAN ID/Priority	Security	Radio
○ AirLive2	0/0	None	2

Radio:	Radio2
SSID Name:	
	□ Disable SSID Broadcasting
VLAN ID:	
VLAN IP:	. . .
VLAN NetMask:	. . .
802.1p priority:	0:Best Effort
Select DSCP type:	010000(Background)
DSCP value:	010000
Select Security Policy:	None

- **Enable VLAN for All SSIDs:** Once this function is enabled, you can specify an individual VLAN ID and priority tag for each SSID. The packets from a SSID will be forwarded to the Ethernet with the corresponding configured VLAN ID written. *You need to click on the top “APPLY” button after making changes.*
- **Enable DiffServ Marking:** When this function is enabled, you can configure a DSCP value for each SSID. Then a packet from a station using this SSID will be forwarded with the DSCP value labeled. *You need to click on the top “APPLY” button after making changes.*
- **VLAN ID:** Packets going out of this VLAN will be tagged with the VLAN ID. Packets coming into the AP will be dropped if the VLAN Tag does not match. The valid range is between 0 to 4095. The VLAN ID “0” is the default VLAN group.
- **VLAN IP:** Each SSID can be given with different VLAN IP group. Please notice that the management IP in the VLAN will also be changed. For example, if you define the VLAN IP to be 192.168.2.X subnet, then the WLA-9000AP’s management IP in the group will change to 192.168.2.1.
- **VLAN IP NetMask:** Define your VLAN IP scope here

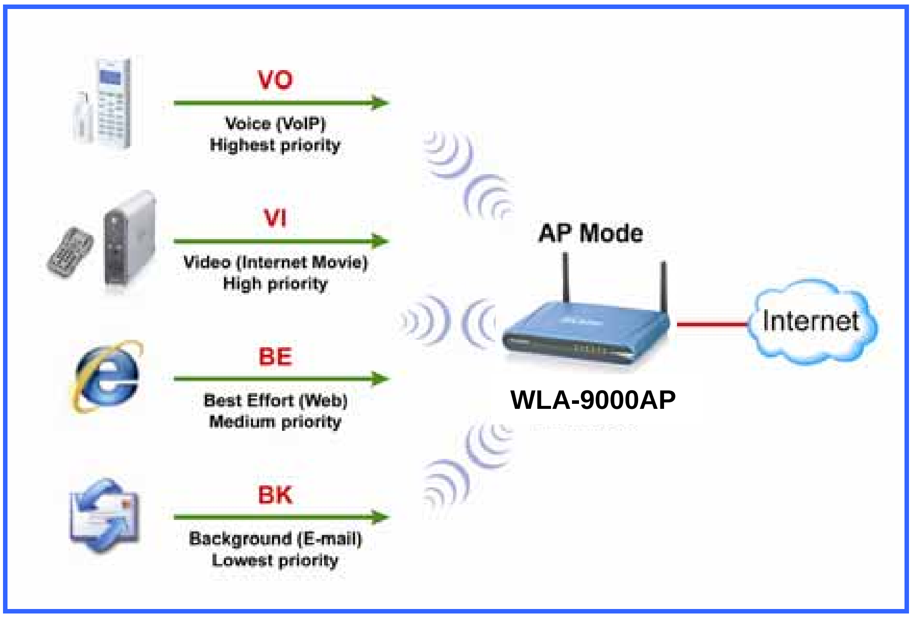
- **802.1p Priority:** Define your 802.1p priority Tag here. Value from 0 to 7
- **Select DSCP TYPE:** Assign the 6-digit DifferServ Code(DSCP) for the packets in the SSID network for QoS purpose. There are 8 preset values. To assign your own value, please select "Best Effort"
- **DSCP Value:** When you select "Best Effort" DSCP Type, you can enter the 6-dgit DSCP Value here.
- **Select Security Policy:** Select the encryption used for this SSID VLAN group. This policy can be different in each SSID VLAN group. For example, one SSID can be using WEP, the other policy can use WPA-PSK.

> ⚠ Once you enable the VLAN ID. The incoming packet from Ethernet port to your VLAN group must carry the same VLAN ID tag or the packet will be dropped.

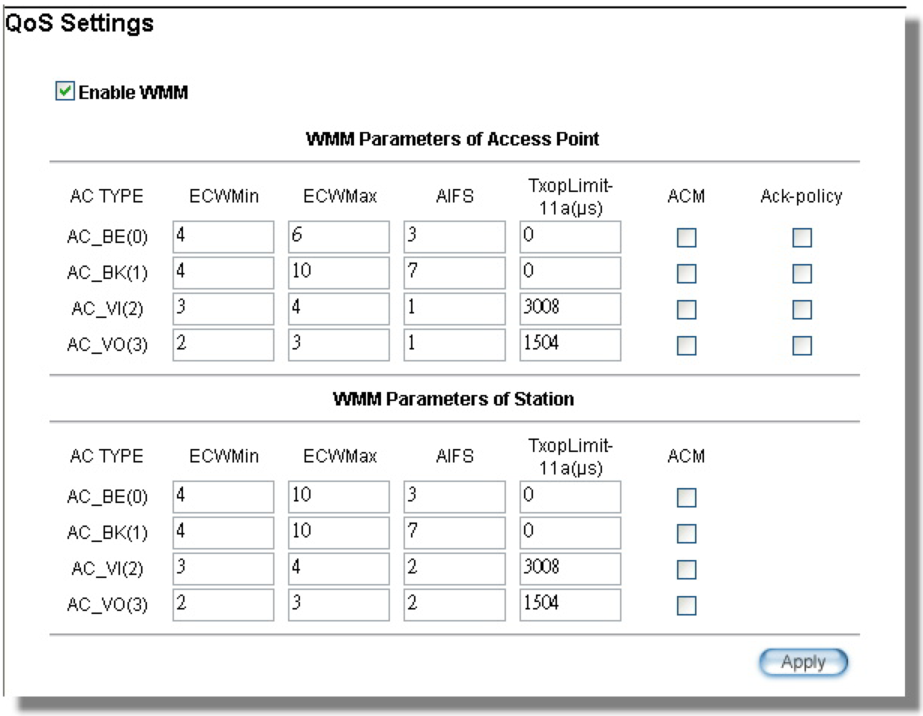
4.2.10 QoS Setting

Operation Mode -> Setup -> QoS Setting

Wi-Fi Multimedia (WMM) is a standard to prioritize traffic for multimedia applications. The WMM Settings is to specify parameters on multiple data queue for better performance of differentiated wireless traffic like Voice-over-IP (VoIP), other types of audio, video, and streaming media as well as traditional IP data over the AP.



Configure the WMM QoS Parameters



QoS Settings

☑ Enable WMM

WMM Parameters of Access Point

AC TYPE	ECWMin	ECWMax	AIFS	TxopLimit-11a(µs)	ACM	Ack-policy
AC_BE(0)	4	6	3	0	□	□
AC_BK(1)	4	10	7	0	□	□
AC_VI(2)	3	4	1	3008	□	□
AC_VO(3)	2	3	1	1504	□	□

WMM Parameters of Station

AC TYPE	ECWMin	ECWMax	AIFS	TxopLimit-11a(µs)	ACM
AC_BE(0)	4	10	3	0	□
AC_BK(1)	4	10	7	0	□
AC_VI(2)	3	4	2	3008	□
AC_VO(3)	2	3	2	1504	□

- **AC Type**

  The queue and associated priorities and parameters for transmission are as follows:

  - ❑ **Data 0 (Best Effort, BE):** Medium priority queue, medium throughput anddel ay. Most traditional IP data is sent to this queue.
  - ❑ **Data 1 (Background, BK):** Lowest priority queue, high throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example):
  - ❑ **Data 2 (Video, VI):** High priority queue, minimum delay. Time-sensitive data such as Video and other streaming media are automatically sent to this queue.
  - ❑ **Data 3 (Voice, VO):** Highest priority queue, minimum delay. Time-sensitive data such as Voice over IP (VoIP) is automatically sent to this queue.

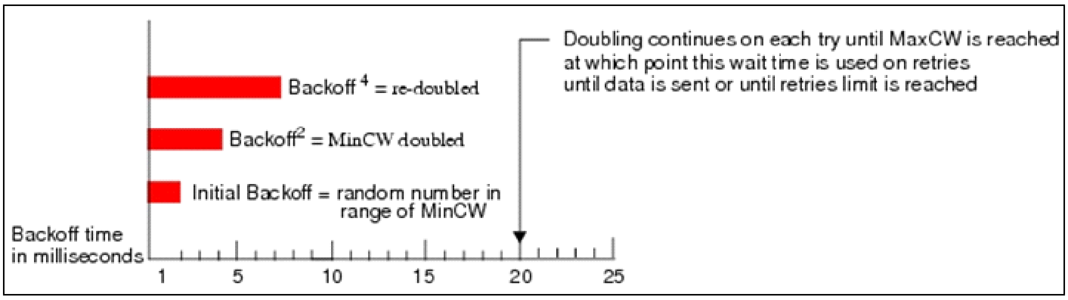
  Packets in a higher priority queue will be transmitted before packets in a lower priority queue.

- **ECWmin and ECWmax**

  If an access point detects that the medium is in use, it uses the DCF random backoff timer to determine the amount of time to wait before attempting to access a given channel again. Each access point waits some random period of time between retries. The wait time (initially a random value within a range specified as the *Minimum*

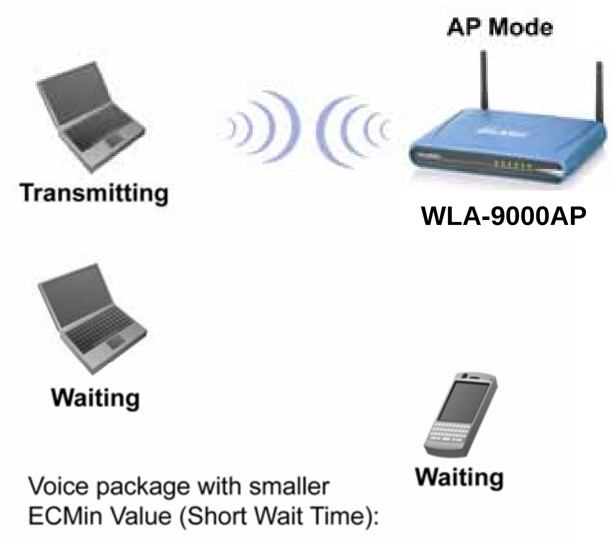
Contention Window increases exponentially up to a specified limit *Maximum Contention Window.*

The random delay avoids most of the collisions that would occur if multiple APs got access to the medium at the same time and tried to transmit data simultaneously. The more active users you have on a network, the more significant the performance gains of the backoff timer will be in reducing the number of collisions and retransmissions.


Doubling continues on each try until MaxCW is reached at which point this wait time is used on retries until data is sent or until retries limit is reached
Backoff 4 = re-doubled
Backoff2 = MinCW doubled
Initial Backoff = random number in range of MinCW
Backoff time in milliseconds
1
5
10
15
20
25

The random backoff used by the access point is a configurable parameter. To describe the random delay, a "*Minimum Contention Window" (ECWMin*) and a "*Maximum Contention Window" (ECWMax)* is defined.

- ❑ **ECWmin**: The value specified for the Minimum Contention Window is the upper limit of a range for the initial random backoff wait time. The number used in the random backoff is initially a random number between 0 and the number defined for the Minimum Contention Window.
- ❑ **ECWmax**: If the first random backoff time ends before successful transmission of the data frame, the access point increases a retry counter, and doubles the value of the random backoff window. The value specified in the Maximum Contention Window is the upper limit for this doubling of the random backoff. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached.



- **AIFS**

  The Arbitration Inter-Frame Spacing (AIFs) specifies a wait time (in milliseconds) for data frames. 802.11e uses interframe spaces to regulate which frames get access to available channels and to coordinate wait times for transmission of different types of data. The AIFs ensures that multiple access points do not try sending data at the same time but instead wait until a channel is free. Valid values for AIFs are 1 through 255.

- **Transmission Opportunity**

  The Transmission Opportunity (TXOP) is an interval of time when a WMM client station has the right to initiate transmissions onto the wireless medium. This value specifies (in milliseconds) the Transmission Opportunity (TXOP) for client stations; that is, the interval of time when a WMM client station has the right to initiate transmissions on the wireless network.

⚠ We recommend that you use the default settings on the WMM QoS page. Changing these values can lead to unexpected blockages of traffic on your wireless LAN, and the blockages might be difficult to diagnose.

4.2.11 Enable Radio eXtended Range

XR is Atheros eXtended technology to increase range. When XR is turned on, the radio can increase the receiver sensitivity greatly. However, performance may be reduced significantly also. Use this mode only if you can trade more distance for lower performance.

4.2.12 Enable Wireless Client Isolation

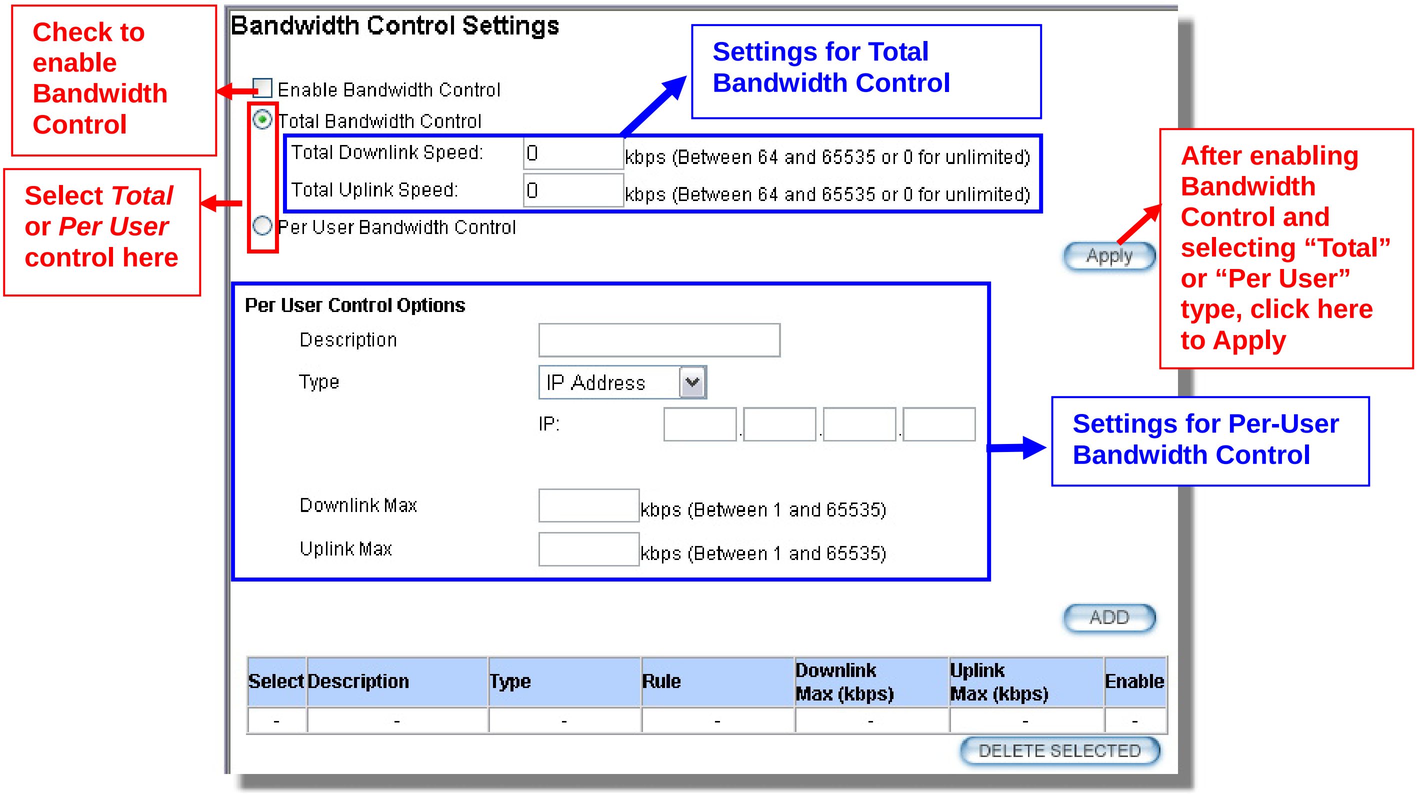
Select the check box to prohibit data transmission between client stations. This function is also known as “**Privacy Separator**”.

4.2.13 Bandwidth Control

Operation Mode -> Setup -> Bandwidth Control

Bandwidth Control can limit the maximum speed of entire wireless interface or individual device. It is also known as Traffic Shaping. The WLA-9000AP provides both Total Bandwidth and Per-User Bandwidth Control for both uplink and downlink speed. It controls the speed of both wireless and wired interface.

To configure, please click on the “Bandwidth Control” button under wireless settings. The following screen will appear:



Bandwidth Control Settings

☐ Enable Bandwidth Control

● Total Bandwidth Control

Total Downlink Speed: 0 kbps (Between 64 and 65535 or 0 for unlimited)

Total Uplink Speed: 0 kbps (Between 64 and 65535 or 0 for unlimited)

○ Per User Bandwidth Control

Per User Control Options

Description:

Type: IP Address

IP: . . .

Downlink Max: kbps (Between 1 and 65535)

Uplink Max: kbps (Between 1 and 65535)

Select	Description	Type	Rule	Downlink Max (kbps)	Uplink Max (kbps)	Enable
-	-	-	-	-	-	-

Check to enable Bandwidth Control

Select *Total* or *Per User* control here

Settings for Total Bandwidth Control

After enabling Bandwidth Control and selecting “Total” or “Per User” type, click here to Apply

Settings for Per-User Bandwidth Control

- **Enable Bandwidth**: Check to enable Bandwidth Control. Uncheck to disable it. The default value is disabled.

You must select between Total Bandwidth and Per-User Bandwidth. They can not be enabled at the same time.

- **Total Bandwidth**: Total Bandwidth control limit the bandwidth between Wireless and Ethernet interface. Therefore, it is most suitable for *Client Infrastructure Mode*, *Bridge Mode*, and *WISP Router Mode*. For WISP operator who use WLA-9000AP as the client side device; setting the Total Bandwidth control on the WLA-9000AP will easy the loading on the AP for bandwidth management. To begin, please enable the Bandwidth Management first. Then enter the downlink and uplink speed; click on Apply to finish.
  - ❑ Total Downlink Speed: Enter speed you wish to limit the download traffic in Kbps units.
  - ❑ Total Uplink Speed: Enter the speed you wish to limit the upload traffic in Kbps units.

- **Per User Bandwidth Control**: Per user Bandwidth Control can limit speed of individual PC and network device. The WLA-9000AP allows multiple Per-User bandwidth rules and can limit the bandwidth by IP address, MAC address, or IP segment. Please first enable the Bandwidth Control, then select "*Per User Bandwidth Control*" to begin. It is recommended to use this type of bandwidth control for Access Point and AP Router mode.

Per User Control Options

- ❑ **Description:** Enter a description for the bandwidth policy. For example, "VIP" subscriber
- ❑ **Type:** WLA-9000AP offers 3 types of Per-User Control
  - **IP Address:** To limit the bandwidth of one single IP address.
  - **IP Segment:** To limit the bandwidth the entire IP segment.

    For example; if you enter the address of 192.168.1.20 with subnet mask of 255.255.255.248, the WLA-9000AP will limit bandwidth of IP addresses from 192.168.1.17 to 192.168.1.22. Please use an online IP calculate if you are not familiar with IP segment calculation. Below is an example link: http://www.subnet-calculator.com/

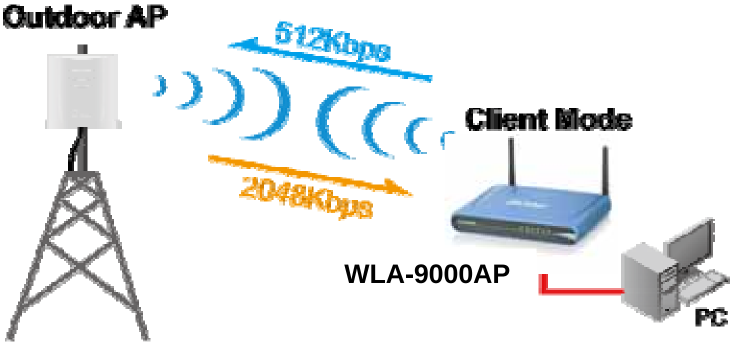
    Because the Ethernet interface is also controlled by the Bandwidth Manager, it is recommended that devices on the Ethernet side to use a wider IP subnet mask that will cover the IP range of the controlled IP segment. Therefore, the devices on Ethernet interface will not be limited by bandwidth control and still can communicate with the IP segment. For example, if your IP segment is set to 192.168.1.20 / 255.255.255.248, then the devices on the Ethernet side should be 192.168.1.X / 255.255.255.0.
  - **MAC address:** To limit the bandwidth of one single MAC address.
  - **Port Range:** This is available only in WISP router and AP Router mode. It can limit the bandwidth by application ports.

- **Application:** This option is available only in WISP router and AP Router mode. It can limit the bandwidth of HTTP, FTP, BitTorrent, and eDonkey traffic.

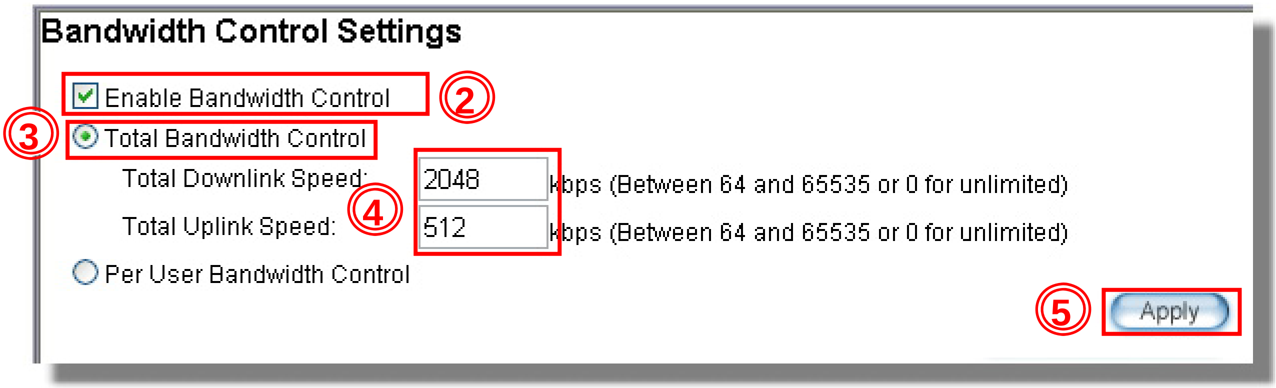
- ❑ **Downlink Max:** Enter the speed you wish to limit the download traffic in kbps units.
- ❑ **Uplink Max:** Enter the speed you wish to limit the upload traffic in kbps units

- **Example 1: Total Bandwidth Control**

In this example, the WLA-9000AP is in Client Infrastructure mode connecting to a remote AP. We want to limit the Bandwidth of the link to 2048Kbps download and 512kbps Upload.



- ❑ ***Step 1:*** From *Operation Mode* menu, select *"Setup"* -> *"Bandwidth Control"*
- ❑ ***Step 2 to 5:*** Enable the Bandwidth Control and select the "Total Bandwidth Control". Then enter the "2048" for *Total Downlink Speed* and "512"kbps for *Total Uplink Speed*. Click "Apply" to finish



Bandwidth Control Settings

② ☑ Enable Bandwidth Control

③ ● Total Bandwidth Control

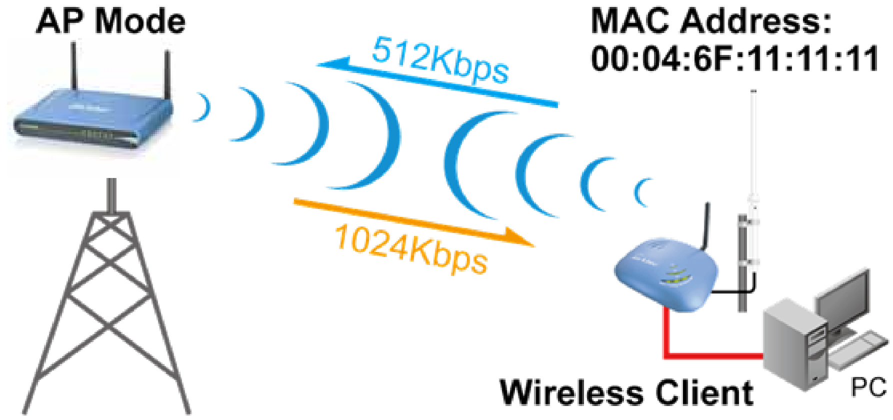
④ Total Downlink Speed: 2048 kbps (Between 64 and 65535 or 0 for unlimited)

Total Uplink Speed: 512 kbps (Between 64 and 65535 or 0 for unlimited)

○ Per User Bandwidth Control

- **Example 2: Per User Bandwidth Control**

In this example, the WLA-9000AP is Access Point mode. There is a wireless client connecting to WLA-9000AP with MAC address of 00:04:6F:11:11:11. We want to limit the bandwidth of the wireless client to 1024 downstream and 512K upstream using WLA-9000AP's Per-User Bandwidth Control.



Step 1. Enable Bandwidth Control and select "Per User Bandwidth Control"

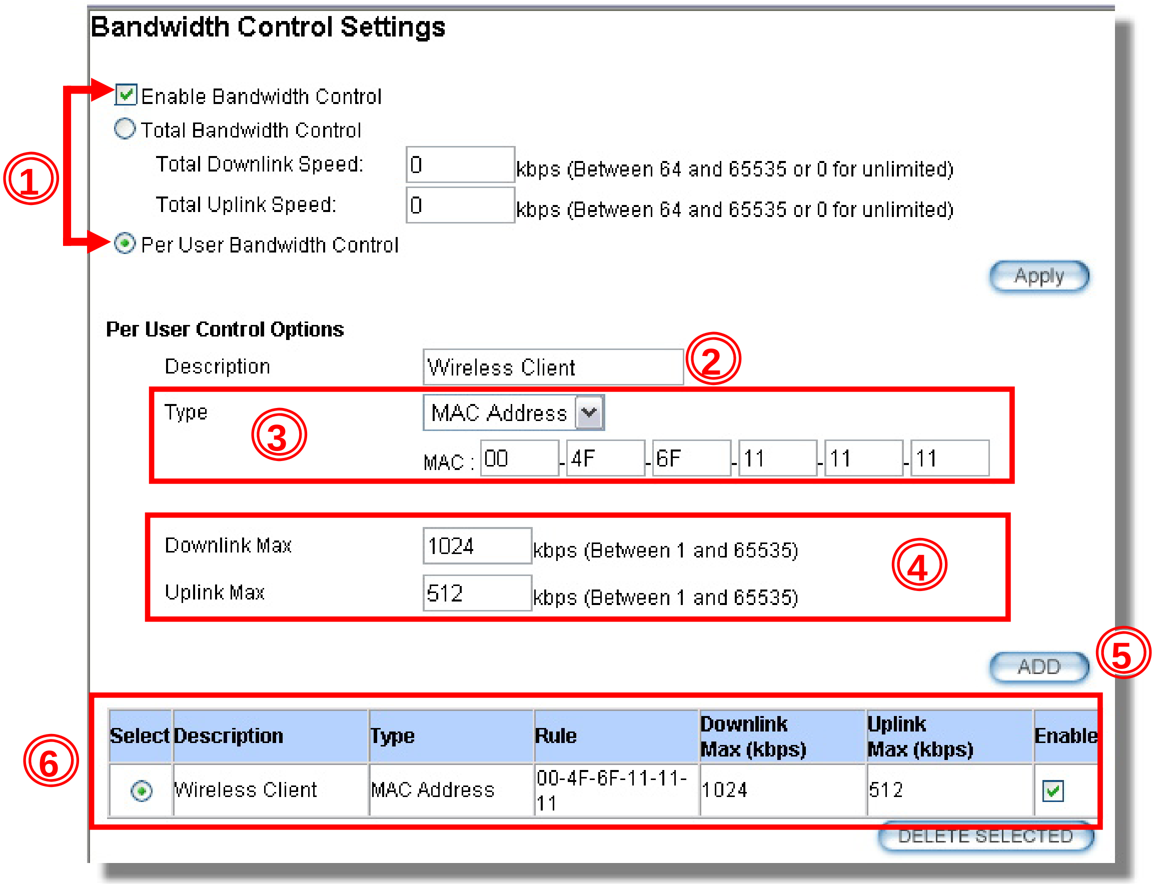
Step 2. Enter Description for this policy (Wireless Client)

Step 3. Select "MAC Address", then enter the MAC address of the wireless client.

Step 4. Enter the downlink speed as "1024" and uplink speed as "512".

Step 5. Click on "Add" button to add the bandwidth policy

Step 6. This new policy should appear on the button. You can enable/disable it.



Bandwidth Control Settings

☑ Enable Bandwidth Control

○ Total Bandwidth Control

Total Downlink Speed: 0 kbps (Between 64 and 65535 or 0 for unlimited)

Total Uplink Speed: 0 kbps (Between 64 and 65535 or 0 for unlimited)

● Per User Bandwidth Control

Apply

Per User Control Options

Description: Wireless Client

Type: MAC Address

MAC : 00 - 4F - 6F - 11 - 11 - 11

Downlink Max: 1024 kbps (Between 1 and 65535)

Uplink Max: 512 kbps (Between 1 and 65535)

ADD

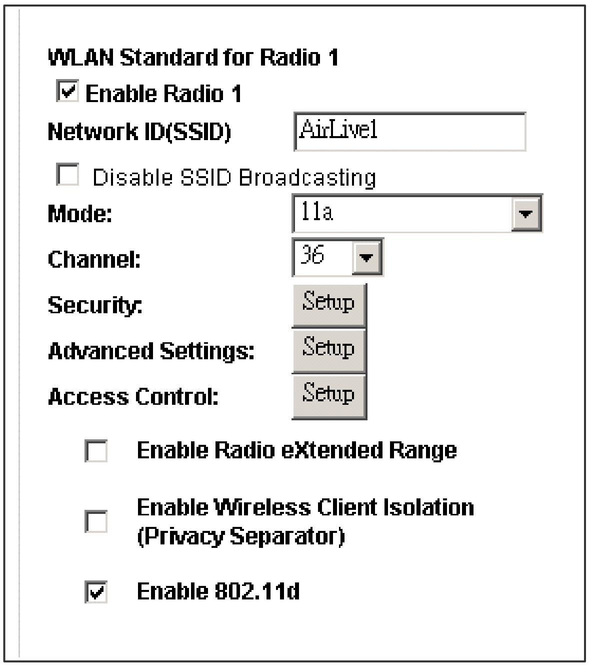
Select	Description	Type	Rule	Downlink Max (kbps)	Uplink Max (kbps)	Enable
●	Wireless Client	MAC Address	00-4F-6F-11-11-11	1024	512	☑

DELETE SELECTED

4.3 Access Point Settings

The Access Point mode is the most basic mode of multi-function Access Point. In this mode, the AP will act as a central hub for different Wireless LAN clients. Some hotspot Access Points requires 802.1x authenticator function to authenticate a user before providing internet service.

Access Point mode included in these operation modes: Dual AP, AP + Client, Client + AP, AP + WDS Bridge, WDS Bridge + AP, AP + Gateway, Gateway + AP, AP + WISP and WISP + AP modes.



WLAN Standard for Radio 1

☑ Enable Radio 1

Network ID(SSID): AirLive1

□ Disable SSID Broadcasting

Mode: 11a

Channel: 36

Security: Setup

Advanced Settings: Setup

Access Control: Setup

□ Enable Radio eXtended Range

□ Enable Wireless Client Isolation (Privacy Separator)

☑ Enable 802.11d

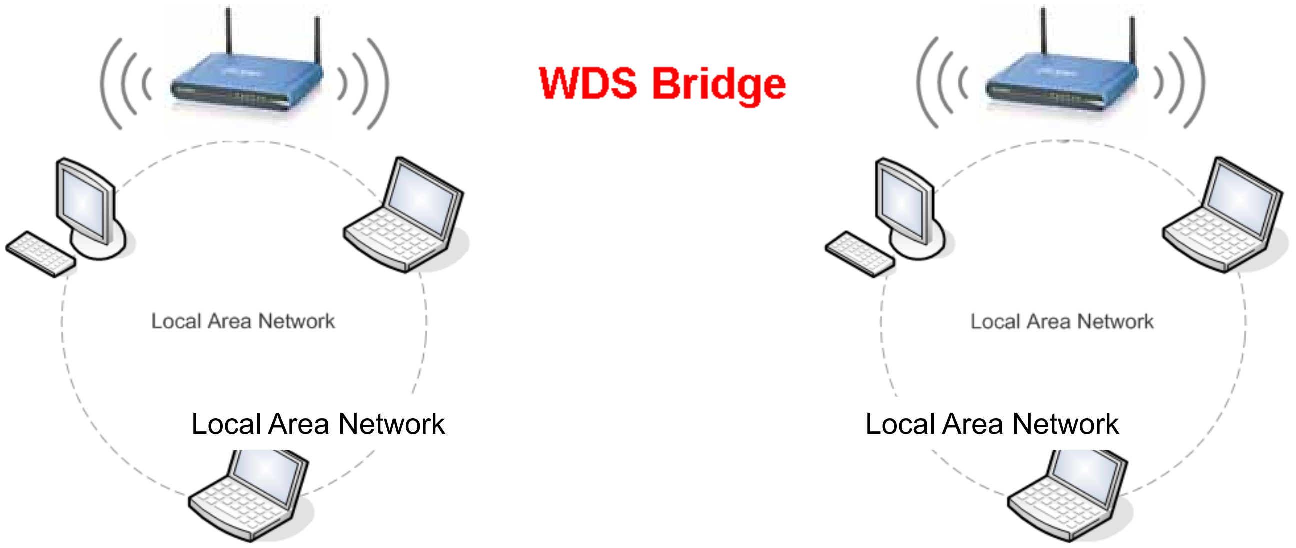
Enable Radio: Use this check box to turn on or turn off the radio.

- **Network ID (SSID):** This is to change your SSID.
- **Disable SSID Broadcasting:** Enable the check box if you want to hide your SSID in the network. This prevent an un-welcomed client survey your radio.
- **Mode:** Connection modes on WLA-9000AP and its wireless client. Note that the client must support the same mode as WLA-9000AP to connect.
- **Channel:** 11a supports channel 36 to 64 and channel 100 to 140. 11g depends on the country, USA/Canada supports channel 1 to 11, Europe supports channel 1 to 13, Japan supports channel 1 to 13, France supports channel 10 to 13, and Span supports channel 10 to 11.
- **Enable Radio eXtended Range:** Check this box to extend the wireless coverage range, this is provided by Atheros's eXtended Range (XR) technology.
- **Enable Client Isolation (Privacy Separator):** This is to prohibit data transmission between each wireless client stations.
- **Enable 802.11d:** This is to prevent network loop applying to the spanning tree standard.

4.4 WDS Settings

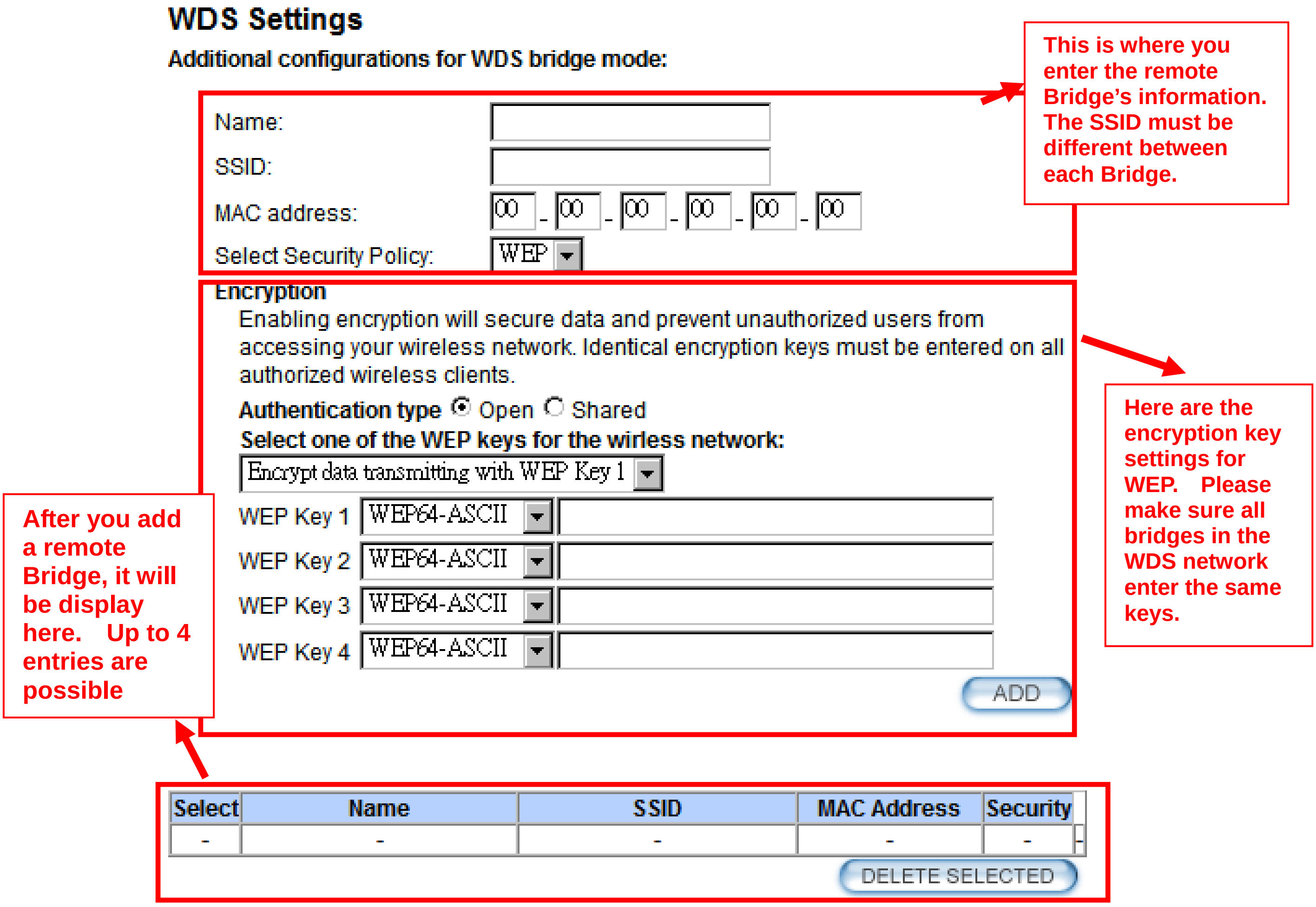
Operation Mode -> Setup -> WDS Settings

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 the WDS (Wireless Distribution System) technology.



In this section, we will talk about the WDS Settings which is available only in WDS Bridge (Pure MAC) mode. WDS Bridges are using BSSID (AP's Wireless MAC address) to authenticate each other. Therefore, it is necessary to know the remote Bridge's wireless MAC addresses. You can always do a "Site Survey" to find out the MAC Addresses.

When you click on WDS settings, the following screen will appear:



WDS Settings

Additional configurations for WDS bridge mode:

Name:	
SSID:	
MAC address:	00 - 00 - 00 - 00 - 00 - 00
Select Security Policy:	WEP

Encryption

Enabling encryption will secure data and prevent unauthorized users from accessing your wireless network. Identical encryption keys must be entered on all authorized wireless clients.

Authentication type ● Open ○ Shared

Select one of the WEP keys for the wirless network:

Encrypt data transmitting with WEP Key 1

WEP Key 1	WEP64-ASCII	
WEP Key 2	WEP64-ASCII	
WEP Key 3	WEP64-ASCII	
WEP Key 4	WEP64-ASCII	

Select	Name	SSID	MAC Address	Security
-	-	-	-	-

This is where you enter the remote Bridge's information. The SSID must be different between each Bridge.

Here are the encryption key settings for WEP. Please make sure all bridges in the WDS network enter the same keys.

After you add a remote Bridge, it will be display here. Up to 4 entries are possible

- **WEP Key**: You can set up to 4 keys; each key can have different Key Length and Key type. When you add an entry to the WDS setting and select WEP encryption, the system will ask you which key to use. All devices on the network must have the same sets of keys, but each link can have use different key. We recommend using WEP-152 whenever possible for better security.

- **Adding a new WDS link**

  The WDS link are created by entering the remote Bridge's information. This process must be repeated on both side of the bridge.

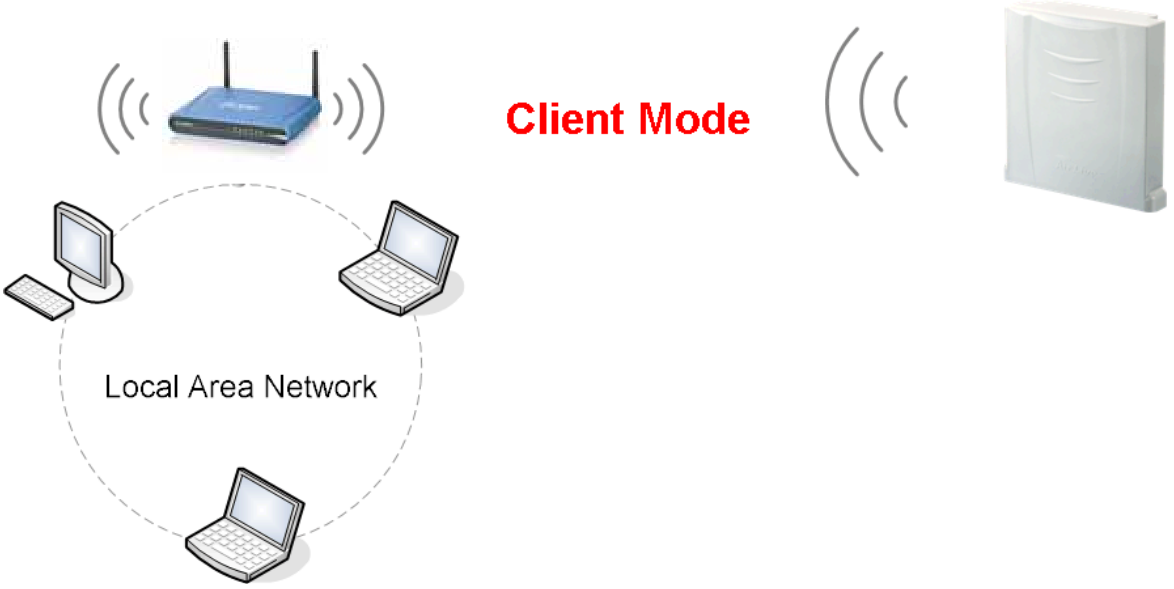
  - **Name**: This is the name for the WDS Link. You can enter any name for your own reference (i.e. WarehouseLink).
  - **SSID**: SSID is the network ID for the wireless link. If you have more than one WDS link or if you want to make WDS connection with Mikrotik devices, this field is required. Each WDS Link must have a different SSID name. If you only have one WDS link, you can leave this field empty.
  - **MAC Address**: Please enter the remote bridge's wireless MAC address in this field. This wireless SSID can be found on the device label. You can also use Site Survey function to assist you.
  - **Select Security Settings**: You can choose to use WEP encryption for better security. It is necessary to enter the same set of keys in the same WDS

network. When you select WEP, the WLA-9000AP will ask you to select from one of the 4 keys. Please be sure to select the same key on both side of the link.

- Press **Add** to finish

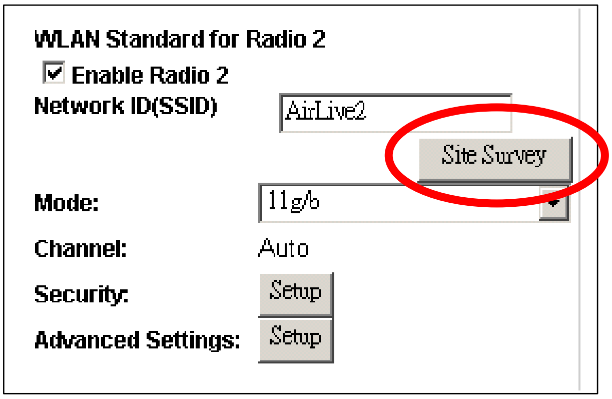
4.5 Client Settings

Also known as Ethernet Client. In this mode, the AP will act as a WLAN card to connect with the remote AP. Users can connect PC or local LAN to the Ethernet port of local LAN to the Ethernet port of the client mode AP. This mode is mostly used as a CPE device for WISP subscriber.



Client mode included in these operation modes: AP + Client, Client + AP, AP + WISP, and WISP + AP.

1. To connect to an access point, use the **"Site Survey"** button to find the Access Point.


WLAN Standard for Radio 2

☑ Enable Radio 2

Network ID(SSID) AirLive2

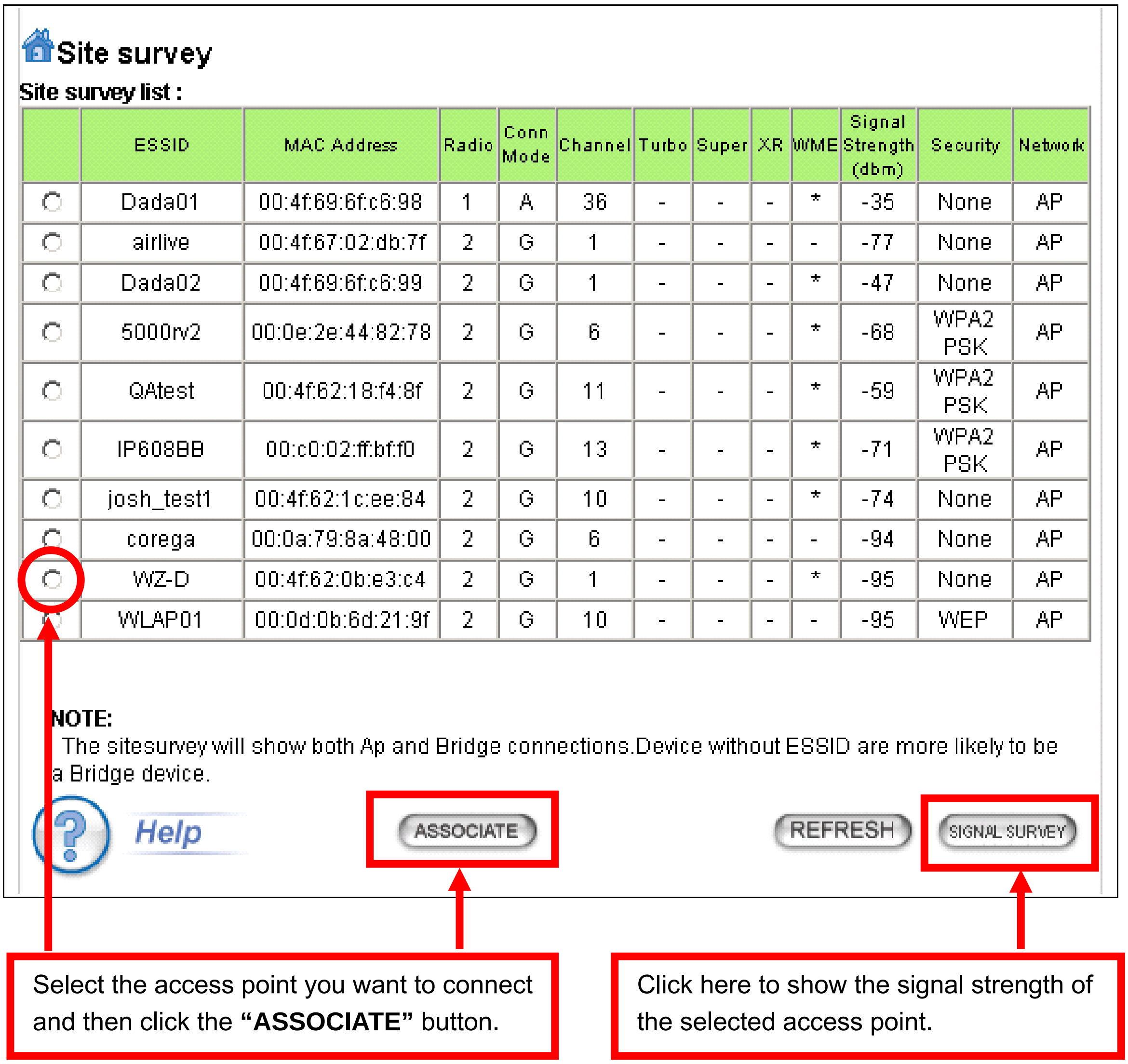
Mode: 11g/b

Channel: Auto

Security:

Advanced Settings:

2. The Site Survey pop up window then shows up and lists available access point with relative information.



Site survey

Site survey list :

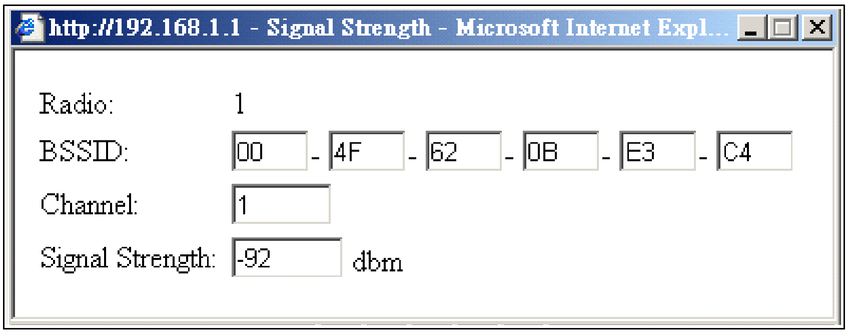
	ESSID	MAC Address	Radio	Conn Mode	Channel	Turbo	Super	XR	WME	Signal Strength (dbm)	Security	Network
○	Dada01	00:4f:69:6f:c6:98	1	A	36	-	-	-	*	-35	None	AP
○	airlive	00:4f:67:02:db:7f	2	G	1	-	-	-	-	-77	None	AP
○	Dada02	00:4f:69:6f:c6:99	2	G	1	-	-	-	*	-47	None	AP
○	5000rv2	00:0e:2e:44:82:78	2	G	6	-	-	-	*	-68	WPA2 PSK	AP
○	QAtest	00:4f:62:18:f4:8f	2	G	11	-	-	-	*	-59	WPA2 PSK	AP
○	IP608BB	00:c0:02:ff:bf:f0	2	G	13	-	-	-	*	-71	WPA2 PSK	AP
○	josh_test1	00:4f:62:1c:ee:84	2	G	10	-	-	-	*	-74	None	AP
○	corega	00:0a:79:8a:48:00	2	G	6	-	-	-	-	-94	None	AP
○	WZ-D	00:4f:62:0b:e3:c4	2	G	1	-	-	-	*	-95	None	AP
○	WLAP01	00:0d:0b:6d:21:9f	2	G	10	-	-	-	-	-95	WEP	AP

NOTE:
The sitesurvey will show both Ap and Bridge connections.Device without ESSID are more likely to be a Bridge device.

Select the access point you want to connect and then click the **"ASSOCIATE"** button.

Click here to show the signal strength of the selected access point.

3. The Signal Survey pop up windows shows as following:



http://192.168.1.1 - Signal Strength - Microsoft Internet Expl...

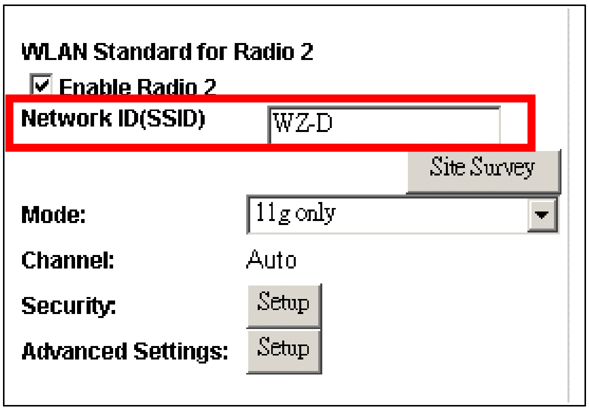
Radio: 1

BSSID: 00 - 4F - 62 - 0B - E3 - C4

Channel: 1

Signal Strength: -92 dbm

4. After the access point is selected, its SSID shows automatically in the Network ID (SSID) field.



WLAN Standard for Radio 2

☑ Enable Radio 2

Network ID(SSID) WZ-D

Mode: 11g only

Channel: Auto

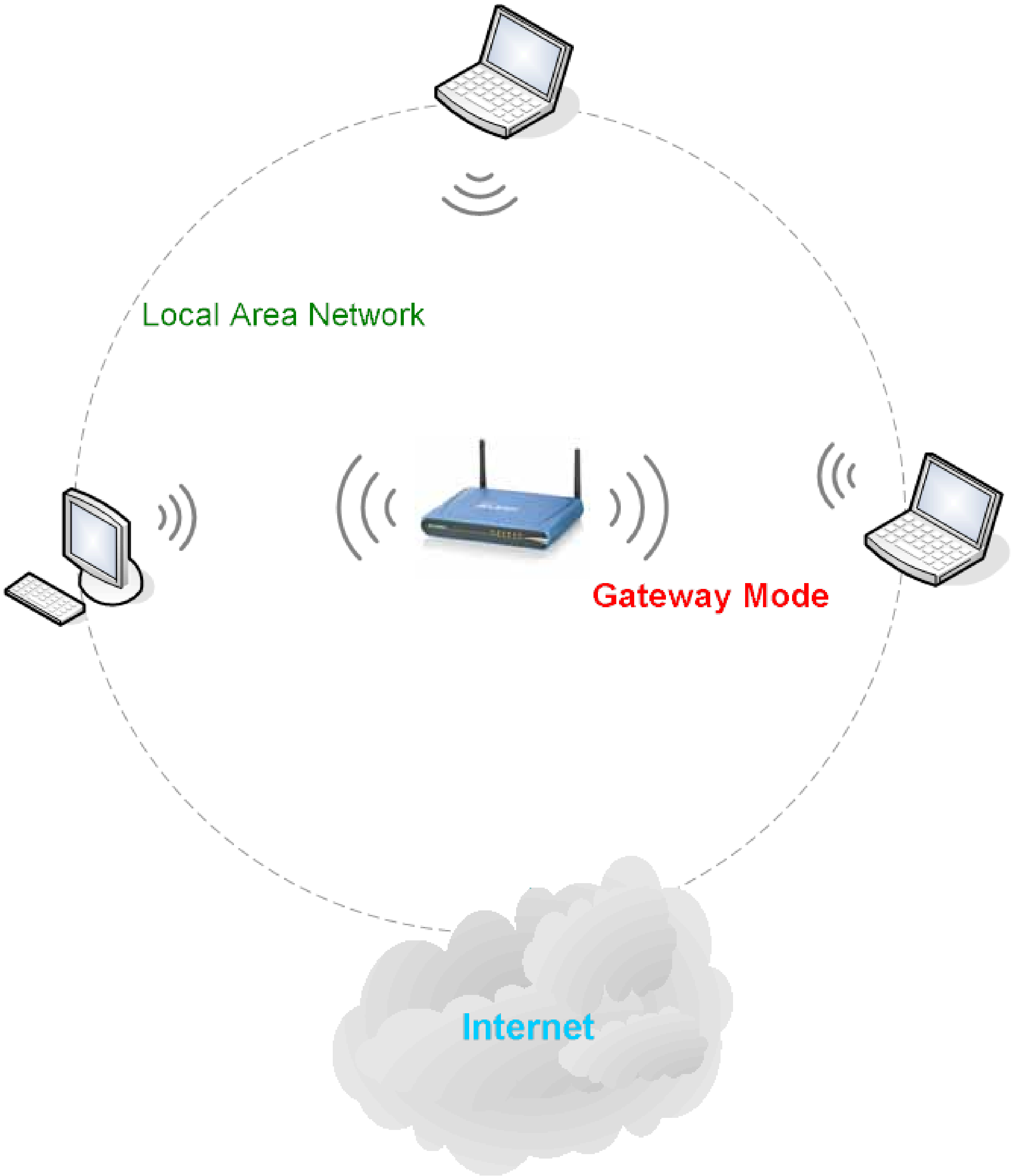
Security: Setup

Advanced Settings: Setup

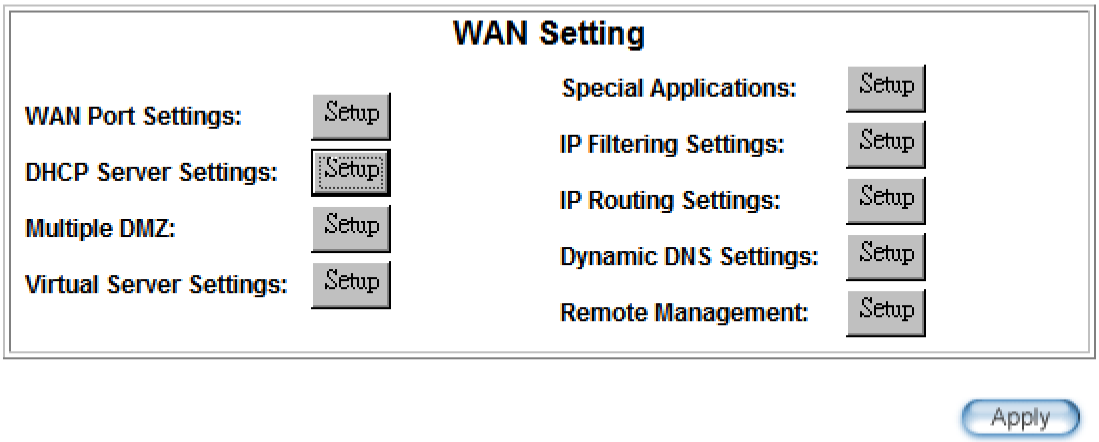
4.6 Gateway (AP Router) Settings

Operation Mode -> Setup

In Gateway mode, router functions are added between one Ethernet port and other network interfaces. Therefore, the ISP subscriber can share the ISP connection without need for extra router.



Gateway mode acts both in AP and Router which included in these operation modes: AP + Gateway and Gateway + AP.



WAN Setting

WAN Port Settings: Setup

DHCP Server Settings: Setup

Multiple DMZ: Setup

Virtual Server Settings: Setup

Special Applications: Setup

IP Filtering Settings: Setup

IP Routing Settings: Setup

Dynamic DNS Settings: Setup

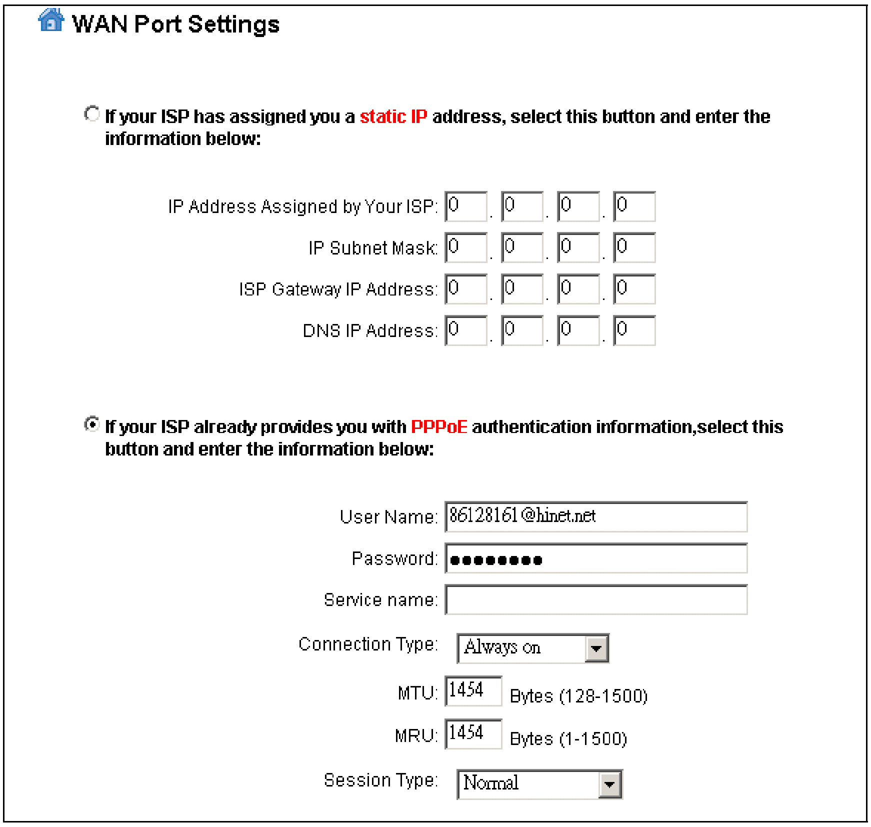
Remote Management: Setup

WAN Port Select: Either the Ethernet port 1 or port 2 can be set to be the WAN port.

4.6.1 WAN Port Settings

Operation Mode -> Setup -> WAN Port Settings

The WLA-9000AP support different authentication and IP assignment standards for the WAN port. It includes fixed IP, DHCP, PPPoE and PPTP protocols. Please consult with your ISP about what authentication type is used for the WAN port conection.



WAN Port Settings

○ If your ISP has assigned you a static IP address, select this button and enter the information below:

IP Address Assigned by Your ISP: 0 . 0 . 0 . 0

IP Subnet Mask: 0 . 0 . 0 . 0

ISP Gateway IP Address: 0 . 0 . 0 . 0

DNS IP Address: 0 . 0 . 0 . 0

● If your ISP already provides you with PPPoE authentication information,select this button and enter the information below:

User Name: 86128161@hinet.net

Password: ●●●●●●●●●

Service name:

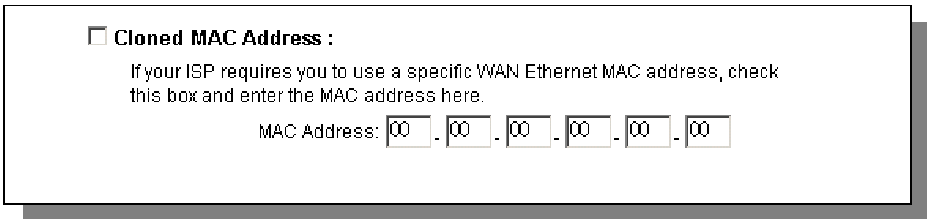
Connection Type: Always on

MTU: 1454 Bytes (128-1500)

MRU: 1454 Bytes (1-1500)

Session Type: Normal

- **Clone MAC Address:** Some service provider (Cable Modem provider) lock to certain MAC address. In this situation, the WAN port of WLA-9000AP needs to clone the MAC address. Please check the “Clone MAC address” box and enter the address that need to be cloned.



□ Cloned MAC Address :

If your ISP requires you to use a specific WAN Ethernet MAC address, check this box and enter the MAC address here.

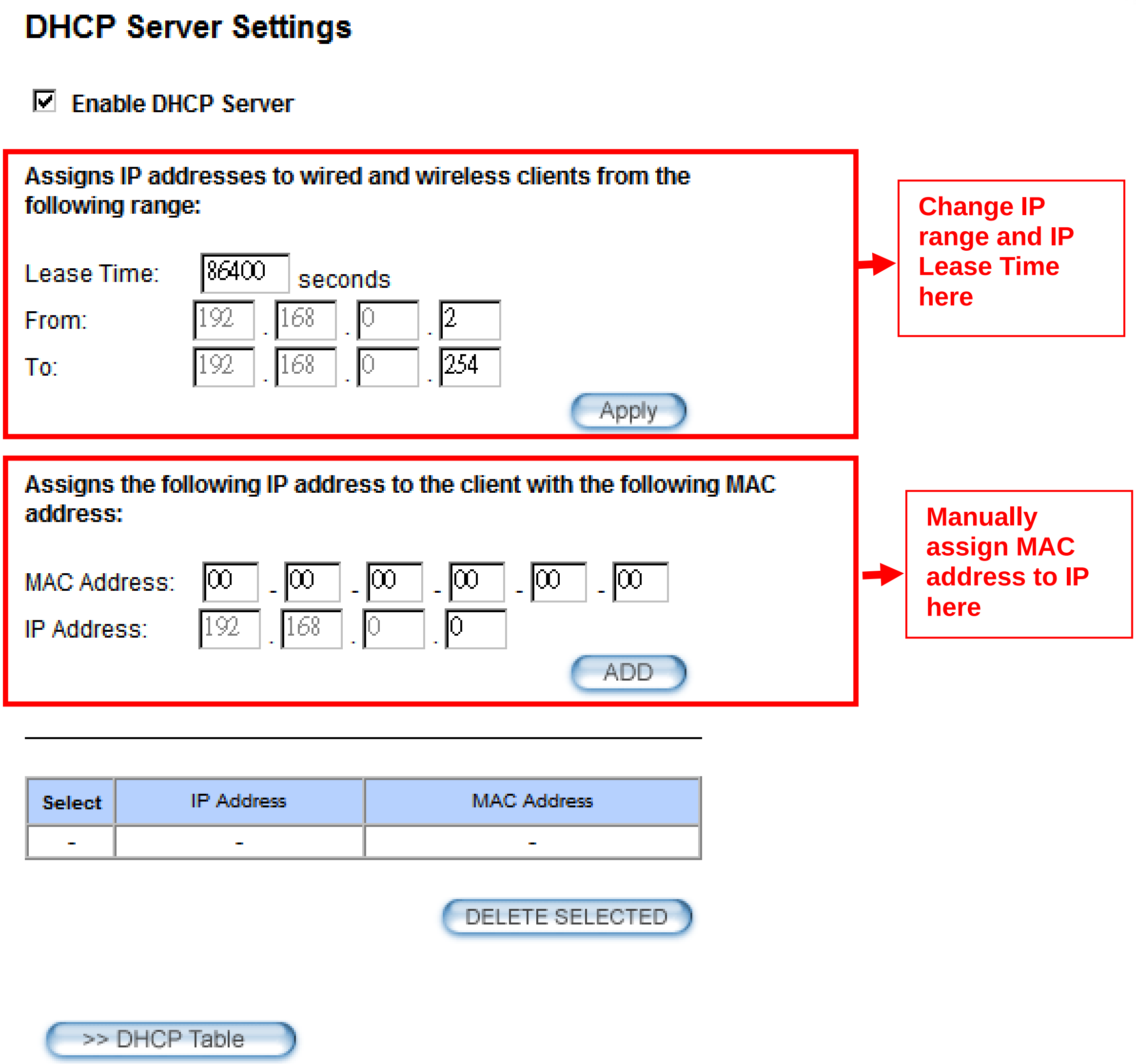
MAC Address: 00 - 00 - 00 - 00 - 00 - 00

4.6.2 DHCP Server Settings

Operation Mode -> Setup -> DHCP Server Settings

DHCP Server Settings is to assign private IP address to the devices in your local area network (LAN). Note that WLA-9000AP keeps the IP address of 192.168.1.1 and act as the default gateway of the LAN.

You can assign IP address to MAC address; the DHCP server will keep the IP for the MAC address.



DHCP Server Settings

☑ Enable DHCP Server

Assigns IP addresses to wired and wireless clients from the following range:

Lease Time: 86400 seconds

From: 192 . 168 . 0 . 2

To: 192 . 168 . 0 . 254

Change IP range and IP Lease Time here

Assigns the following IP address to the client with the following MAC address:

MAC Address: 00 - 00 - 00 - 00 - 00 - 00

IP Address: 192 . 168 . 0 . 0

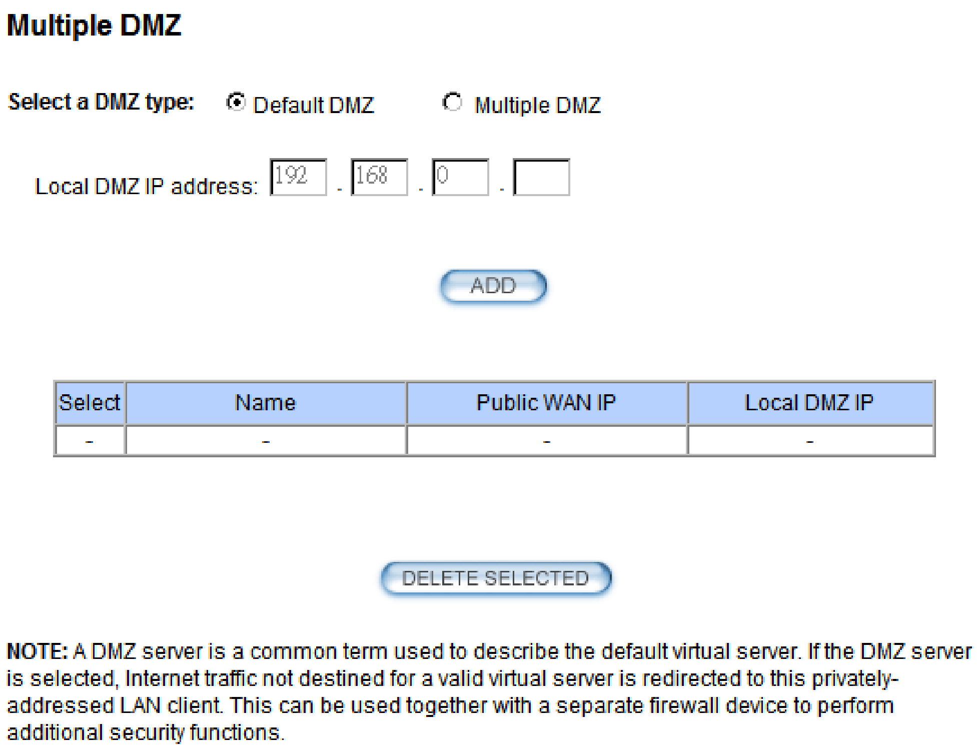
Manually assign MAC address to IP here

Select	IP Address	MAC Address
-	-	-

4.6.3 Multiple DMZ

Operation Mode -> Setup -> Multiple DMZ

Multiple DMZ opens all TCP/UDP ports to particular IP address on the LAN side.   It allows setting up servers behind the WLA-9000AP.



Multiple DMZ

Select a DMZ type: ● Default DMZ ○ Multiple DMZ

Local DMZ IP address: 192 . 168 . 0 .

Select	Name	Public WAN IP	Local DMZ IP
-	-	-	-

NOTE: A DMZ server is a common term used to describe the default virtual server. If the DMZ server is selected, Internet traffic not destined for a valid virtual server is redirected to this privately-addressed LAN client. This can be used together with a separate firewall device to perform additional security functions.

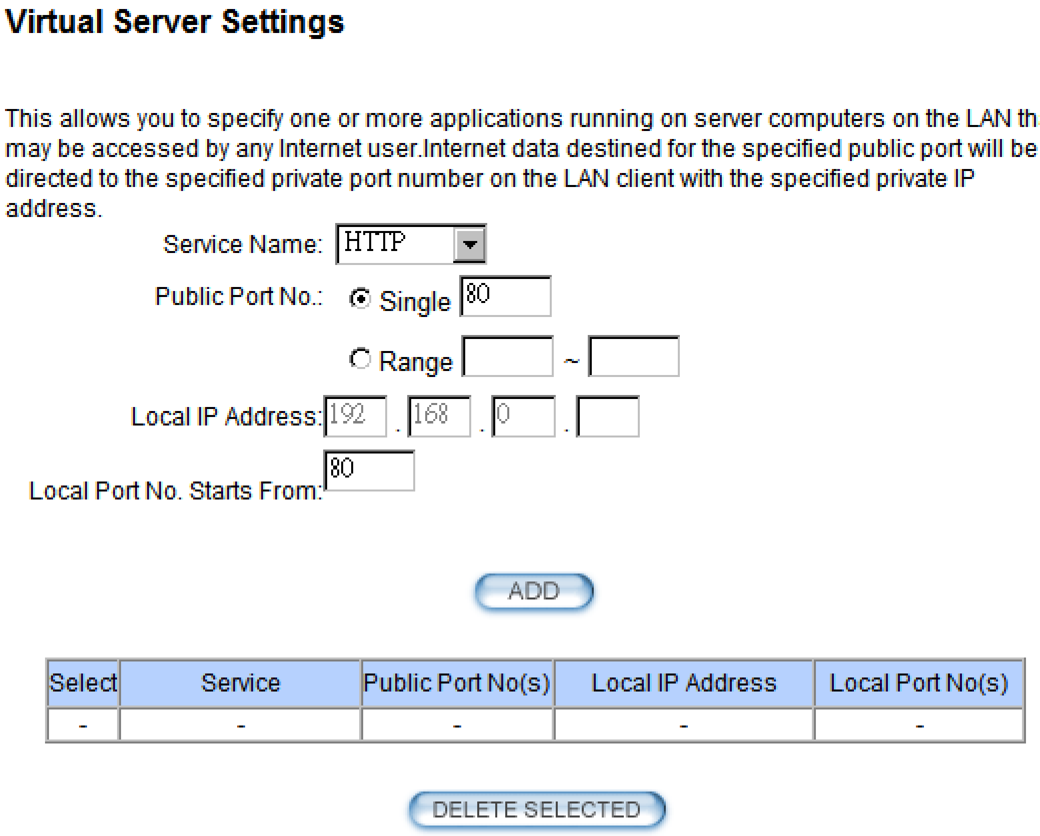
Select a DMZ type and then enter the local DMZ IP address.

A DMZ server is a common term used to describe the default virtual server. If the DMZ server is selected, Internet traffic not destined for a valid virtual server is redirected to this privately addressed LAN client. This can be used together with a separate firewall device to perform additional security functions.

4.6.4 Virtual Server Settings

Operation Mode -> Setup -> Virtual Setting

This allows you to specify one or more applications running on server computers on the LAN that may be accessed by any Internet user. Internet data destined for the specified public port will be directed to the specified private port number on the LAN client with the specified private IP address.



Virtual Server Settings

This allows you to specify one or more applications running on server computers on the LAN that may be accessed by any Internet user.Internet data destined for the specified public port will be directed to the specified private port number on the LAN client with the specified private IP address.

Service Name: HTTP

Public Port No.: ● Single 80

○ Range ~

Local IP Address: 192 . 168 . 0 .

Local Port No. Starts From: 80

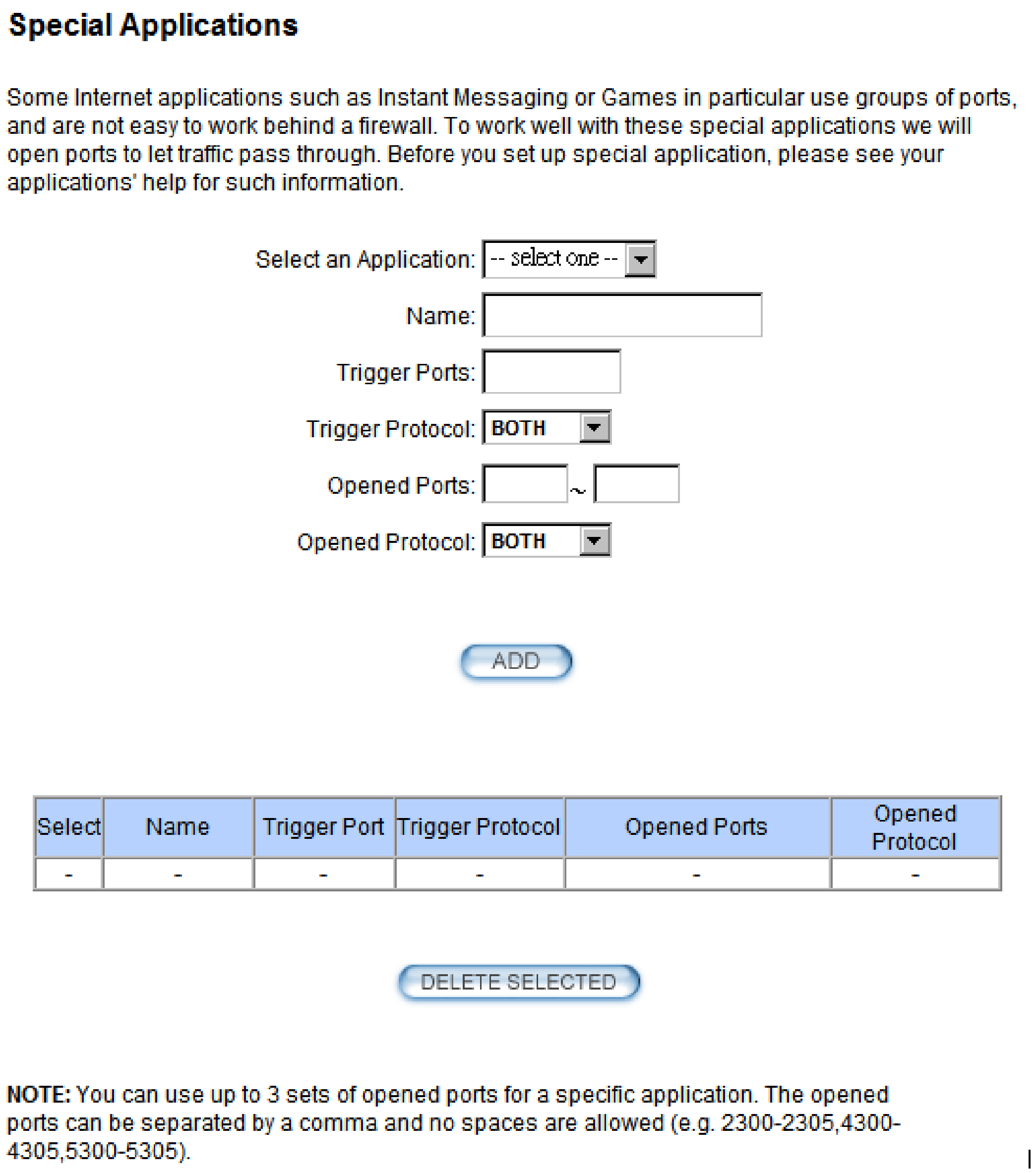
Select	Service	Public Port No(s)	Local IP Address	Local Port No(s)
-	-	-	-	-

4.6.5 Special Applications

Operation Mode -> Setup -> Special Applications

Some Internet application such as Instant Messaging or games use groups of ports, and are not easy to work behind a firewall. To work well with these special applications we will open ports to let traffic pass through.

Note: You can use up to 3 sets of opened ports for a specific application. The opened ports can be separated by a comma and no spaces are allowed (e.g. 2300-2305, 4300-4305, 5300-5305).



Special Applications

Some Internet applications such as Instant Messaging or Games in particular use groups of ports, and are not easy to work behind a firewall. To work well with these special applications we will open ports to let traffic pass through. Before you set up special application, please see your applications' help for such information.

Select an Application: -- select one --

Name:

Trigger Ports:

Trigger Protocol: BOTH

Opened Ports: ~

Opened Protocol: BOTH

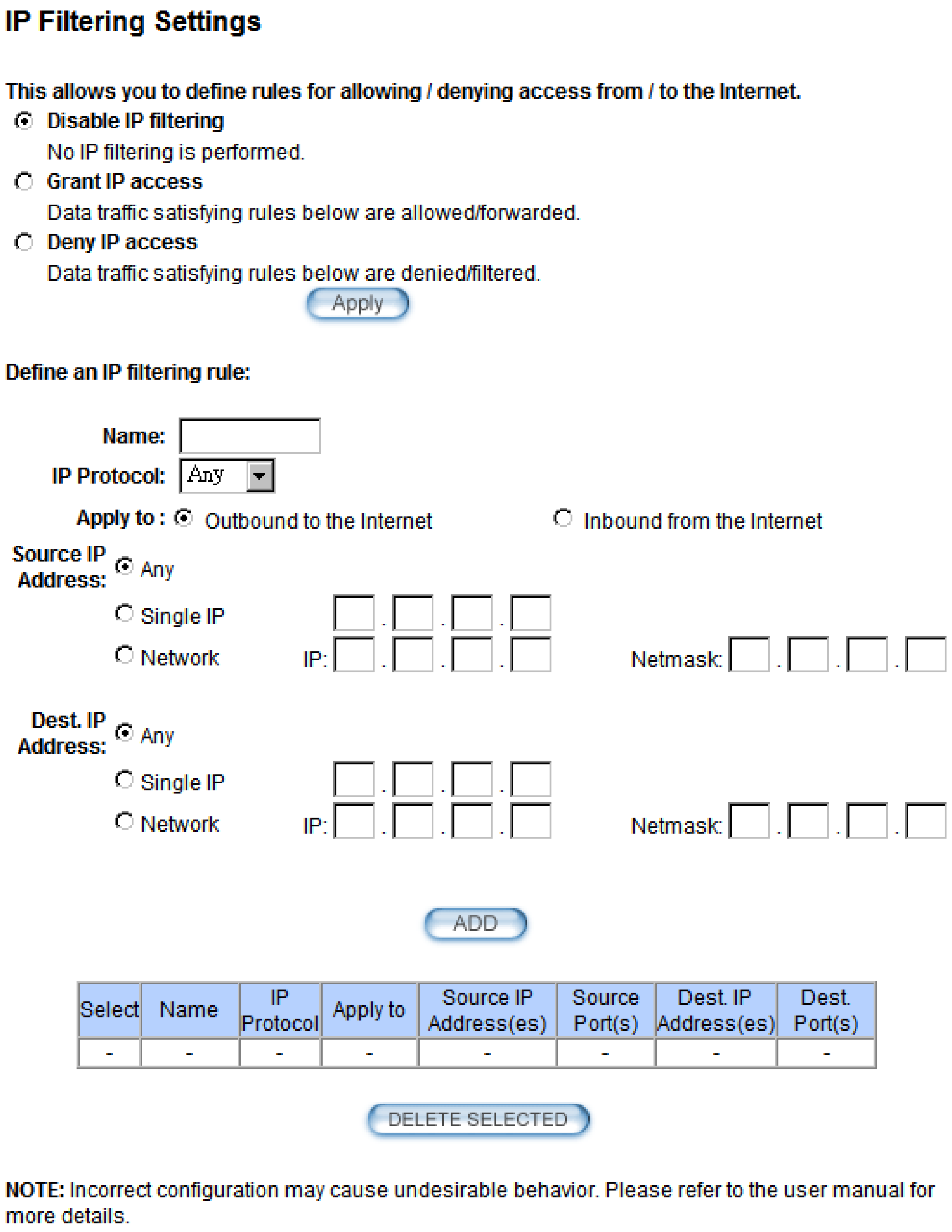
Select	Name	Trigger Port	Trigger Protocol	Opened Ports	Opened Protocol
-	-	-	-	-	-

NOTE: You can use up to 3 sets of opened ports for a specific application. The opened ports can be separated by a comma and no spaces are allowed (e.g. 2300-2305,4300-4305,5300-5305).

4.6.6 IP Filtering Settings

Operation Mode -> Setup ->IP Filtering Settings

IP filtering is simply a mechanism that decides which types of IP datagram will be processed normally and which will be discarded.



IP Filtering Settings

This allows you to define rules for allowing / denying access from / to the Internet.

● Disable IP filtering
No IP filtering is performed.

○ Grant IP access
Data traffic satisfying rules below are allowed/forwarded.

○ Deny IP access
Data traffic satisfying rules below are denied/filtered.

Define an IP filtering rule:

Name: □

IP Protocol: Any

Apply to : ● Outbound to the Internet ○ Inbound from the Internet

Source IP Address: ● Any
○ Single IP □ . □ . □ . □
○ Network IP: □ . □ . □ . □ Netmask: □ . □ . □ . □

Dest. IP Address: ● Any
○ Single IP □ . □ . □ . □
○ Network IP: □ . □ . □ . □ Netmask: □ . □ . □ . □

Select	Name	IP Protocol	Apply to	Source IP Address(es)	Source Port(s)	Dest. IP Address(es)	Dest. Port(s)
-	-	-	-	-	-	-	-

NOTE: Incorrect configuration may cause undesirable behavior. Please refer to the user manual for more details.

This allows you to define rules for allowing / denying access from / to the Internet.

Please do set both inbound/outbound in order to get complete connection. Only inbound or outbound will not allow to get response from the destination IP.

Disable IP filtering: No IP filtering is performed.

Grant IP access: Data traffic satisfying rules below are allowed/forwarded.

Deny IP access: Data traffic satisfying rules below are denied/filtered.

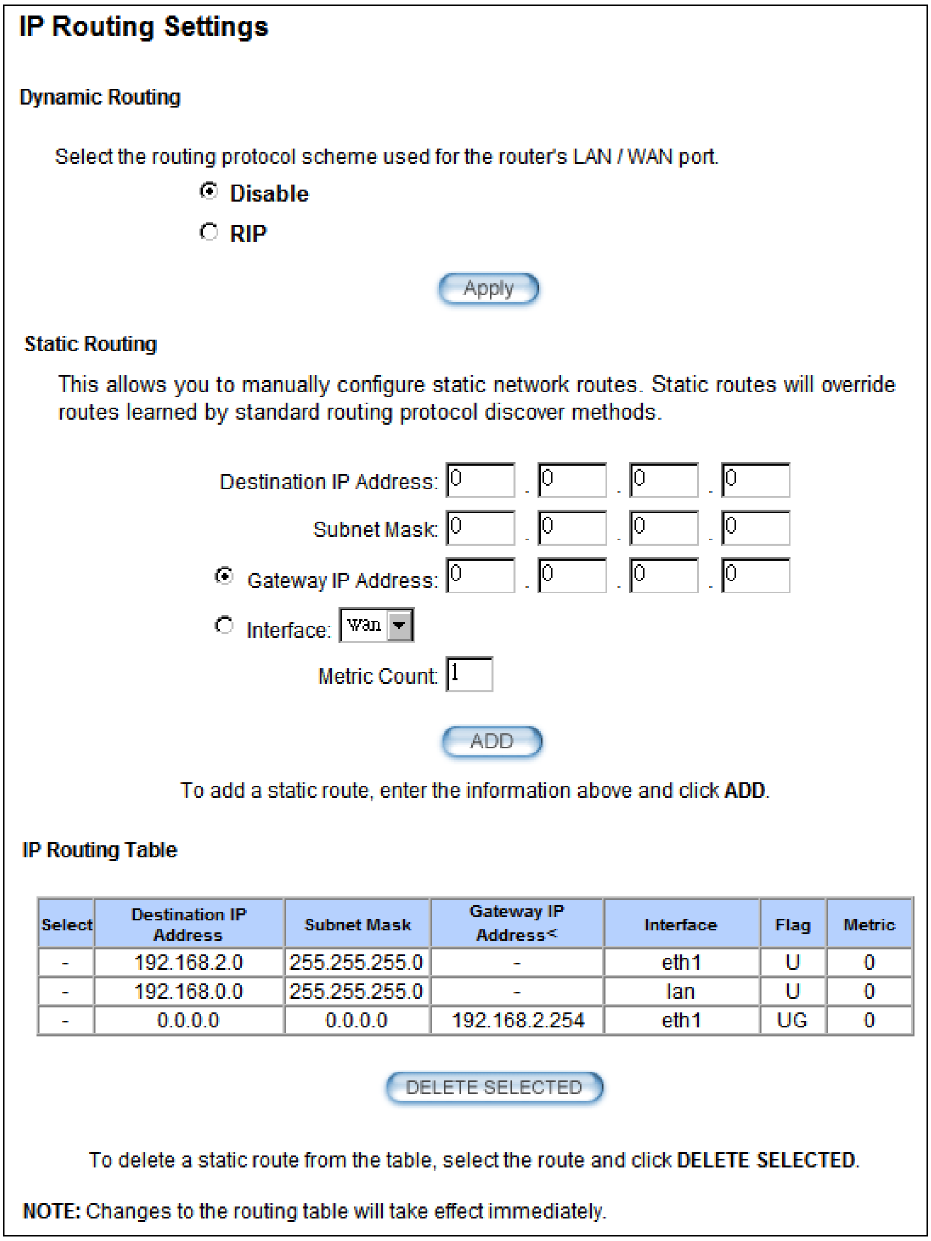
You can also define IP filtering rule, such as:
Name; IP Protocol; Apply to either Outbound to the Internet or Inbound from the Internet; Source IP Address and Dest. (Destination) IP Address.

To grant or deny IP address, select **ADD** or **Delete Selected**.

4.6.7 IP Routing Settings

Operation Mode -> Setup -> IP Routing Settings

The IP Routing Settings allows you to configure routing feature in the gateway



IP Routing Settings

Dynamic Routing

Select the routing protocol scheme used for the router's LAN / WAN port.

● Disable
○ RIP

Static Routing

This allows you to manually configure static network routes. Static routes will override routes learned by standard routing protocol discover methods.

Destination IP Address: 0 . 0 . 0 . 0
Subnet Mask: 0 . 0 . 0 . 0
● Gateway IP Address: 0 . 0 . 0 . 0
○ Interface: Wan
Metric Count: 1

To add a static route, enter the information above and click **ADD**.

IP Routing Table

Select	Destination IP Address	Subnet Mask	Gateway IP Address<	Interface	Flag	Metric
-	192.168.2.0	255.255.255.0	-	eth1	U	0
-	192.168.0.0	255.255.255.0	-	lan	U	0
-	0.0.0.0	0.0.0.0	192.168.2.254	eth1	UG	0

To delete a static route from the table, select the route and click **DELETE SELECTED**.

NOTE: Changes to the routing table will take effect immediately.

- **Dynamic Routing:**

  Select the routing protocol scheme used for the router's LAN / WAN port.

- **Static Routing:**

  This allows you to manually configure static network routes. Static routes will override routes learned by standard routing protocol discover methods.

- **IP Routing Table:**

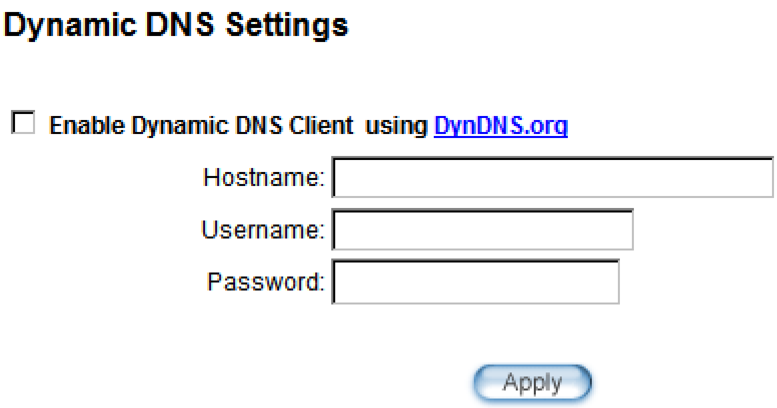
  To delete a static route from the table, select the route and click DELETE SELECTED.

Note: Changes to the routing table will take effect immediately.

4.6.8 Dynamic DNS Settings

Operation Mode -> Setup -> Dynamic DNS Settings

Dynamic DNS (DDNS) allows you to create a hostname that points to your dynamic IP or static IP address or URL. WLA-9000AP provide Dynamic DNS client using DynDNS, please visit http://www.dyndns.org for detail.



Dynamic DNS Settings

□ Enable Dynamic DNS Client using DynDNS.org

Hostname:

Username:

Password:

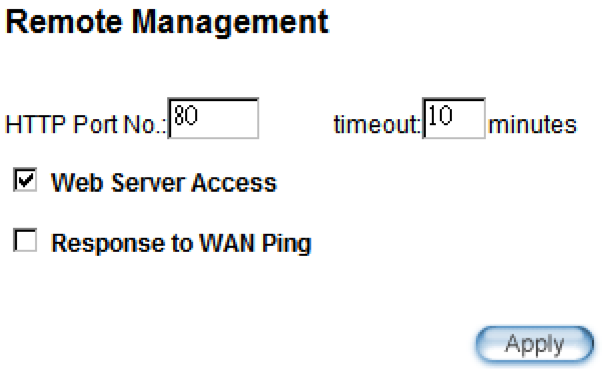
4.6.9 Remote Management Settings

Operation Mode -> Setup -> Remote Management

Remote Management allows administrator to manage the WLA-9000AP from WAN side. You can also change the management port and other settings here.

- **HTTP Port No**: The default port for HTTP is Port 80, you can change the value here
- **Timeout**: The default management timeout is 10 minutes. After timeout, the WLA-9000AP will ask you to login again. You can change the timeout value here.

- **HTTP Web Server Access**: You can enable or disable HTTP service from WAN side
- **HTTPS Web server Access**: You can enable or disable HTTPS Web Server Access from WAN side
- **Response to WAN ping**: You can disable or enable whether WLA-9000AP will response to PING command.



Remote Management

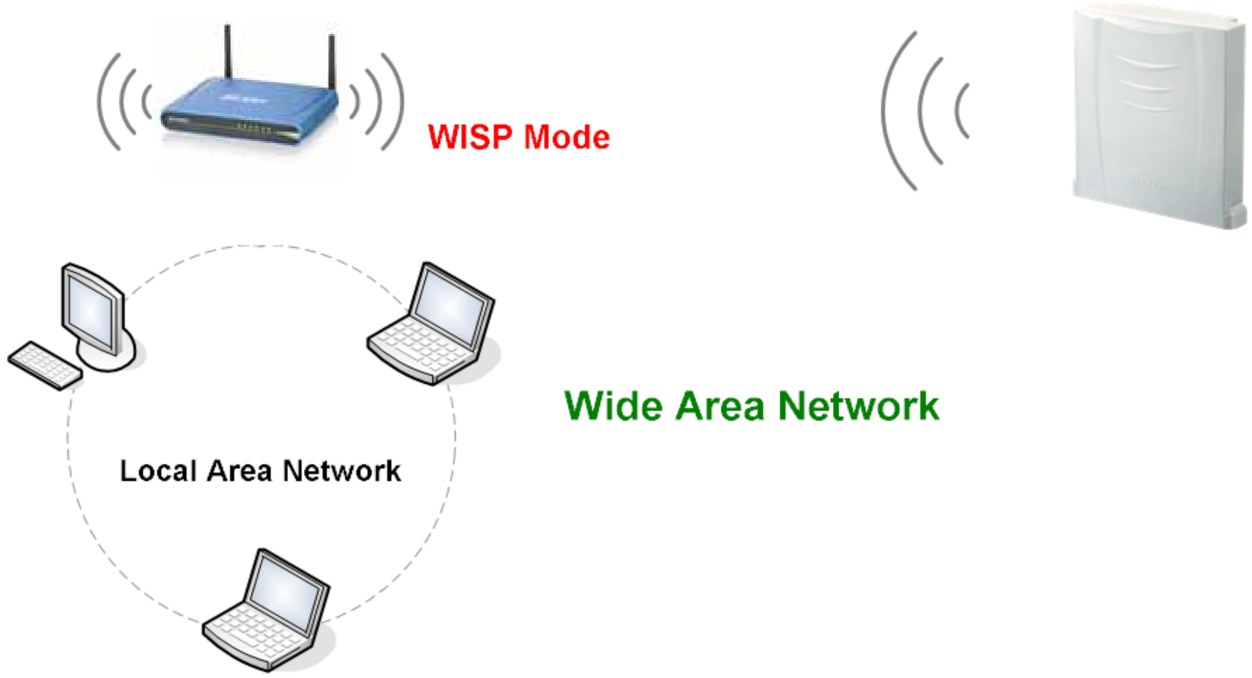
HTTP Port No.: 80 timeout: 10 minutes

☑ Web Server Access

☐ Response to WAN Ping

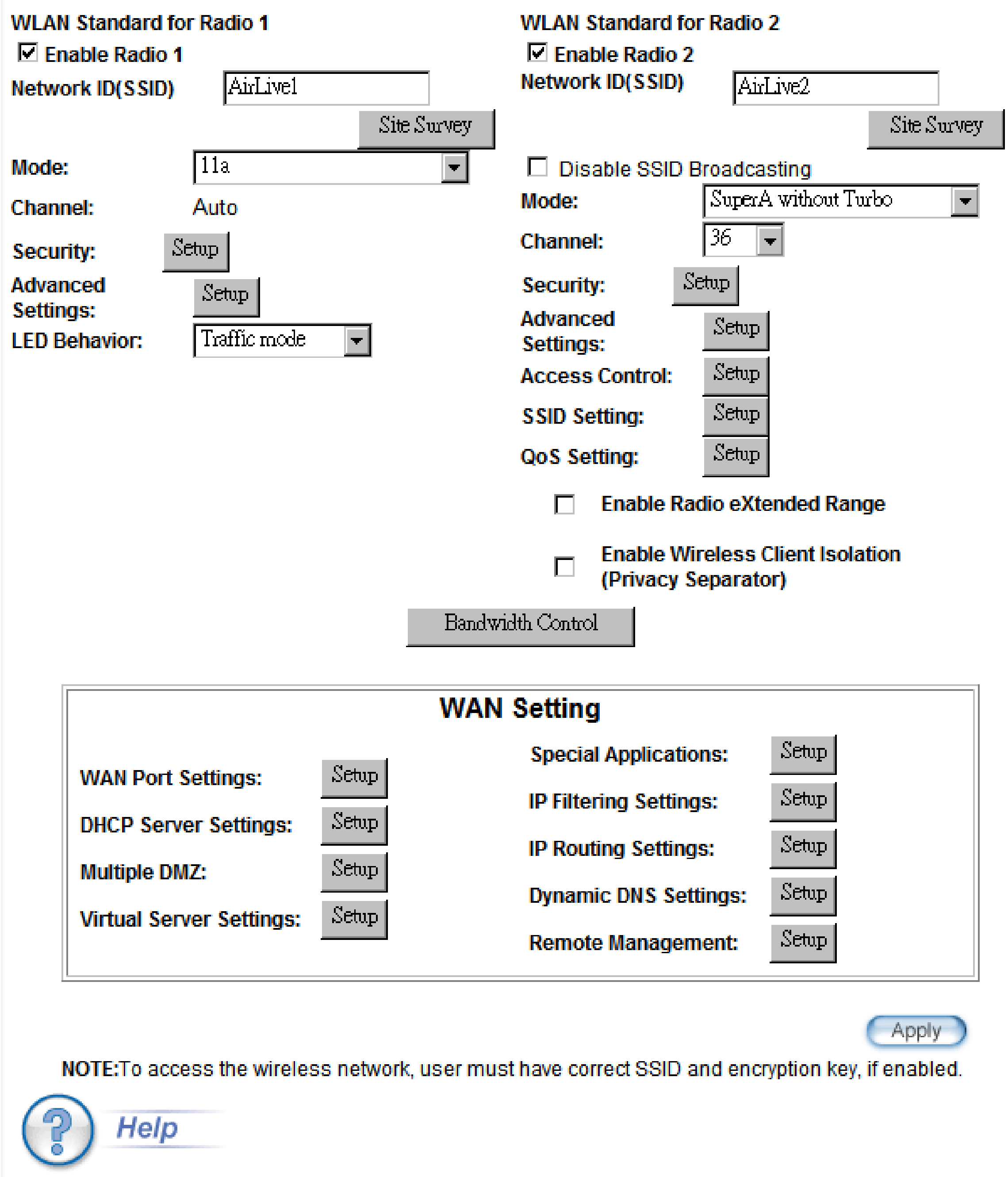
4.7 WISP Settings

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 need for extra router.



WISP mode acts both in AP and Router which included in these operation modes: AP + WISP and WISP + AP.

In WISP + AP mode, the Radio 1 is actually a wireless client of the WISP wireless node and also the gateway of the local area network.



WLAN Standard for Radio 1

☑ Enable Radio 1

Network ID(SSID): AirLive1

Mode: 11a

Channel: Auto

LED Behavior: Traffic mode

WLAN Standard for Radio 2

☑ Enable Radio 2

Network ID(SSID): AirLive2

☐ Disable SSID Broadcasting

Mode: SuperA without Turbo

Channel: 36

☐ Enable Radio eXtended Range

☐ Enable Wireless Client Isolation (Privacy Separator)

WAN Setting

NOTE:To access the wireless network, user must have correct SSID and encryption key, if enabled.

Please refer to **Section 4.6** for gateway settings.

To configure the AP mode, Please refer to Section 4.3 Access Point Setting.

To configure the WDS mode, Please refer to Section 4.5 Client Setting.

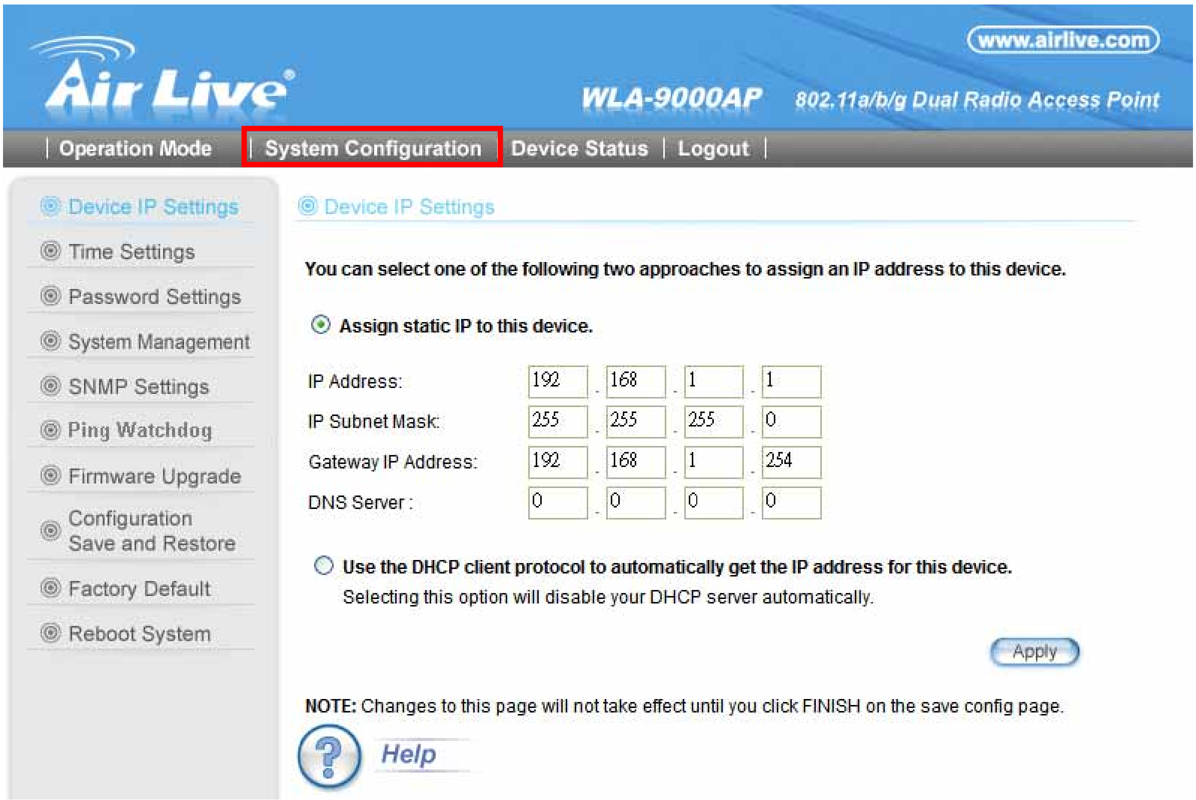
To configure the Gateway (Router) mode, Please refer to Section 4.6 Gateway (AP router) Setting.

5 Web Management 2: System Configuration and Status

In this chapter, we will explain about *System Configurations* in web management interface. Please be sure to read through Chapter 3's "*Introduction to Web Management"* and *"Initial Configurations"* first. .

5.1 System Configuration

When you click on the "System Configuration" menu on the top menu bar, the following screen will appear. The system configuration includes all non-wireless settings. We will explain their functions here.



Device IP Settings

You can select one of the following two approaches to assign an IP address to this device.

● Assign static IP to this device.

IP Address:	192	168	1	1
IP Subnet Mask:	255	255	255	0
Gateway IP Address:	192	168	1	254
DNS Server :	0	0	0	0

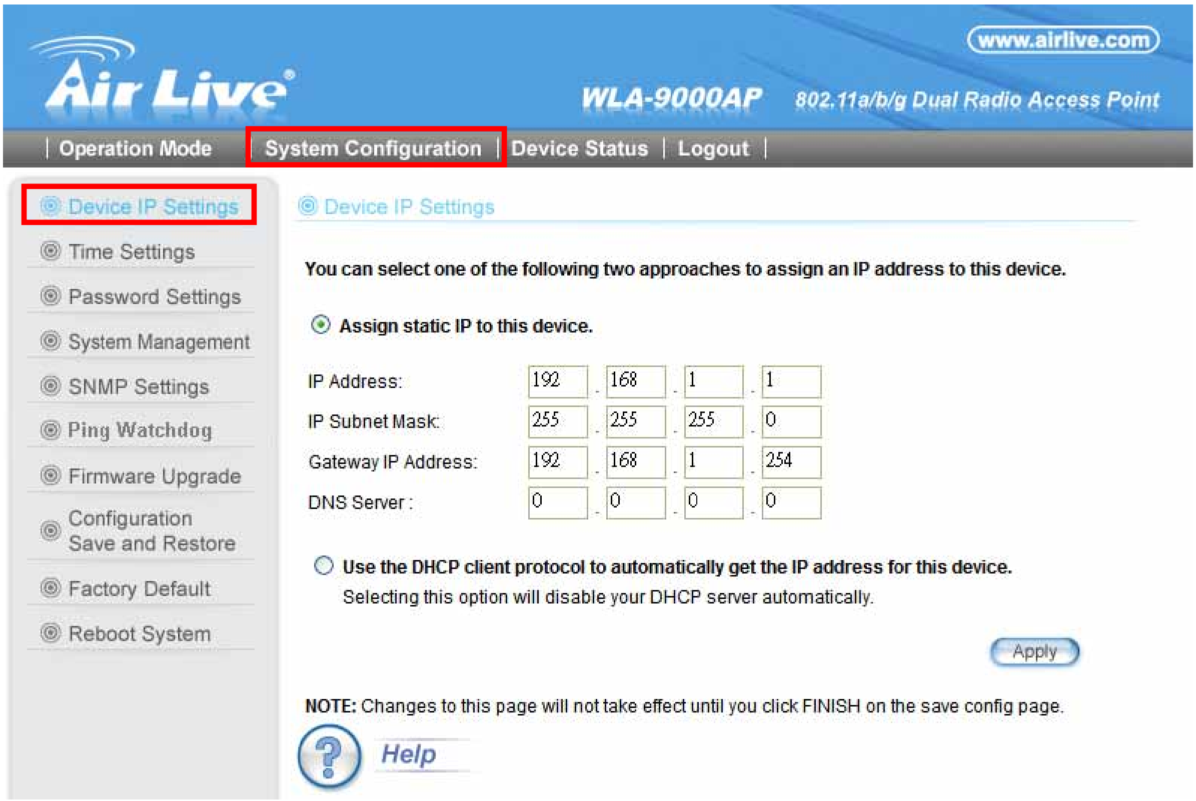
○ Use the DHCP client protocol to automatically get the IP address for this device.
Selecting this option will disable your DHCP server automatically.

NOTE: Changes to this page will not take effect until you click FINISH on the save config page.

5.1.1 Device IP Settings

System Configurations>> Device IP Settings

The Device IP Settings screen allows you to configure the IP address and subnet of the device. Although you can rely on a DHCP server to assign an IP address to the WLA-9000AP automatically, it is recommended that you configure a static IP address manually in most applications.



Device IP Settings

You can select one of the following two approaches to assign an IP address to this device.

● Assign static IP to this device.

IP Address:	192	168	1	1
IP Subnet Mask:	255	255	255	0
Gateway IP Address:	192	168	1	254
DNS Server :	0	0	0	0

○ Use the DHCP client protocol to automatically get the IP address for this device.
Selecting this option will disable your DHCP server automatically.

NOTE: Changes to this page will not take effect until you click FINISH on the save config page.

Assign Static IP to the Device

If you choose to assign the IP address manually, enable the checkbox of “Assign static IP to this device” and then fill in the following fields

- **IP Address** and **IP Subnet Mask**: Default values are 192.168.1.1 and 255.255.255.0 respectively. It is important to note that there are similar addresses falling in the standard private IP address range and it is an essential security feature of the device. Because of this private IP address, the device can no longer be accessed (seen) from the Internet.

- **Gateway IP Address**: Enter the IP address of your default gateway.

- **DNS Server**: The Domain Name System (DNS) is a server on the Internet that translates logical names such as “www.yahoo.com” to IP addresses like 66.218.71.80. In order to do this, a query is made by the requesting device to a DNS server to provide the necessary information. If your system administrator requires you to manually enter the DNS Server addresses, you should enter them here.

- Click **APPLY** to go to the next screen.

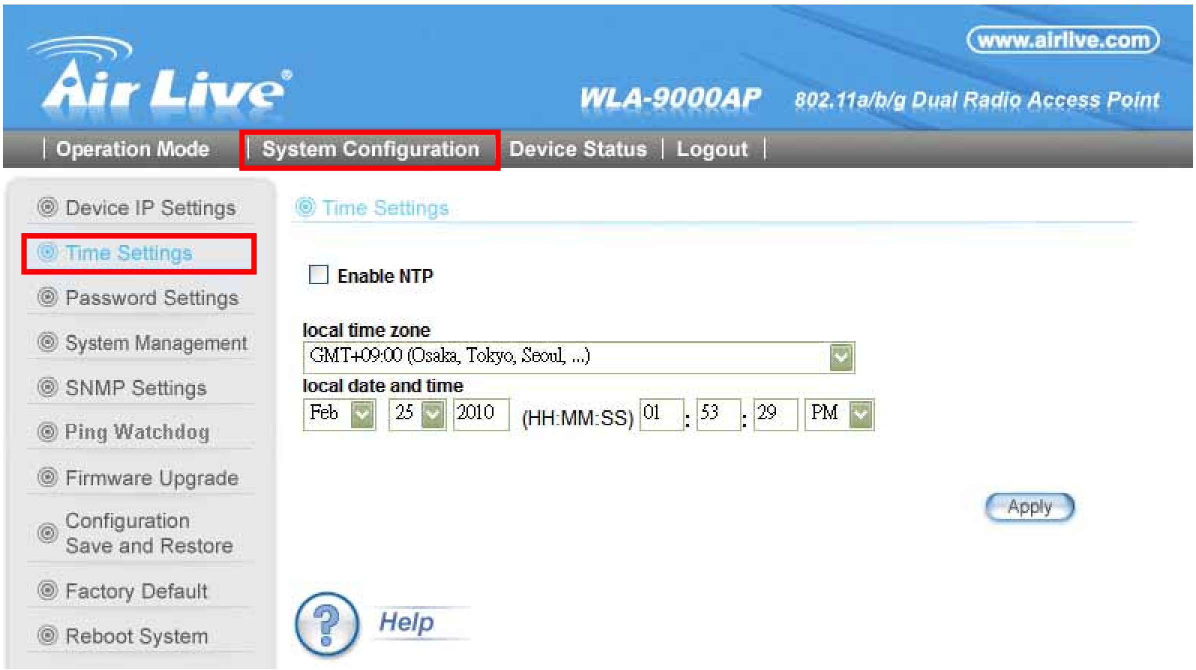
Use DHCP Client Protocol to Get IP automatically

If you choose to use a DHCP Server to acquire an IP address for the WLA-9000AP automatically, enable the check box “Use the DHCP client protocol to automatically get the IP address for this device”. Then click “Next” to go to the next screen. As a reminder, you might loss the IP address of WLA-9000AP when IP is assigned dynamically.

5.1.2 Time Settings

System Configuration ->Time Settings

It is important that you set the date and time for your WLA-9000AP so that the system log will record the correct date and time information. We recommend you choose “Enable NTP” so the time will be keep even after reboot. If your WLA-9000AP is not connected to Internet, please enter the time manually. Please remember to select your local time zone and click “Apply” to finish.



Time Settings

□ Enable NTP

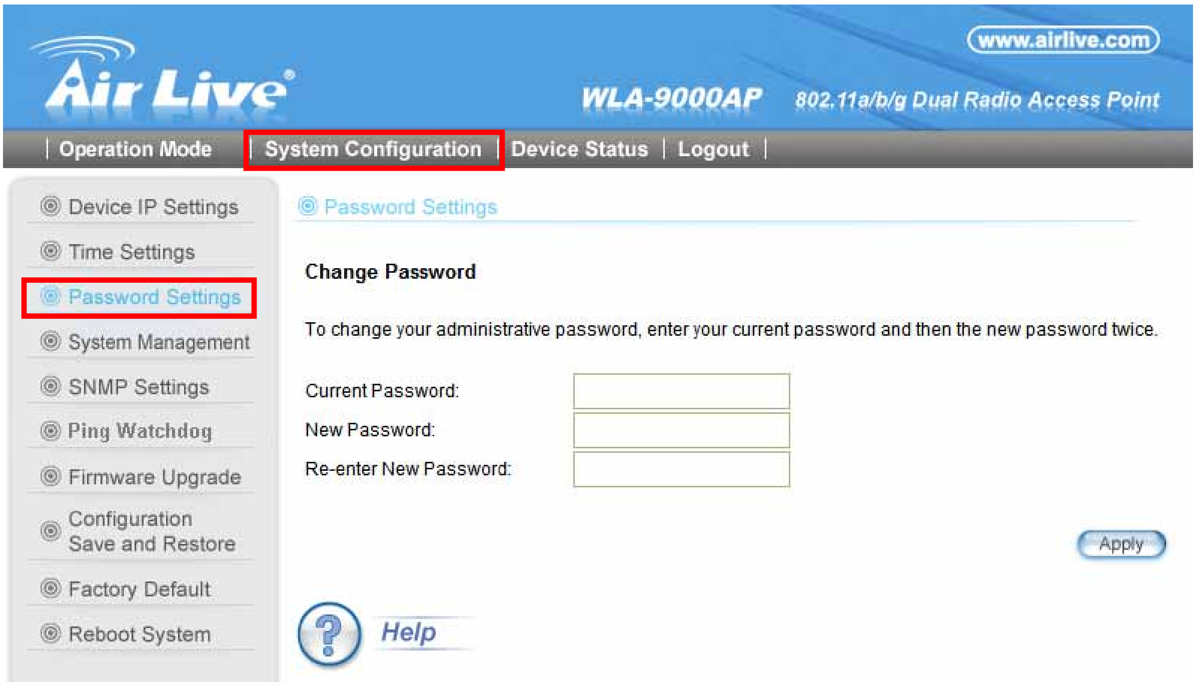
local time zone
GMT+09:00 (Osaka, Tokyo, Seoul, ...)

local date and time
Feb 25 2010 (HH:MM:SS) 01 : 53 : 29 PM

5.1.3 Password Settings

System Configuration ->Password Settings

To change password, please go to *“System Configuration”* -> *“Password Settings”* menu.



Change Password

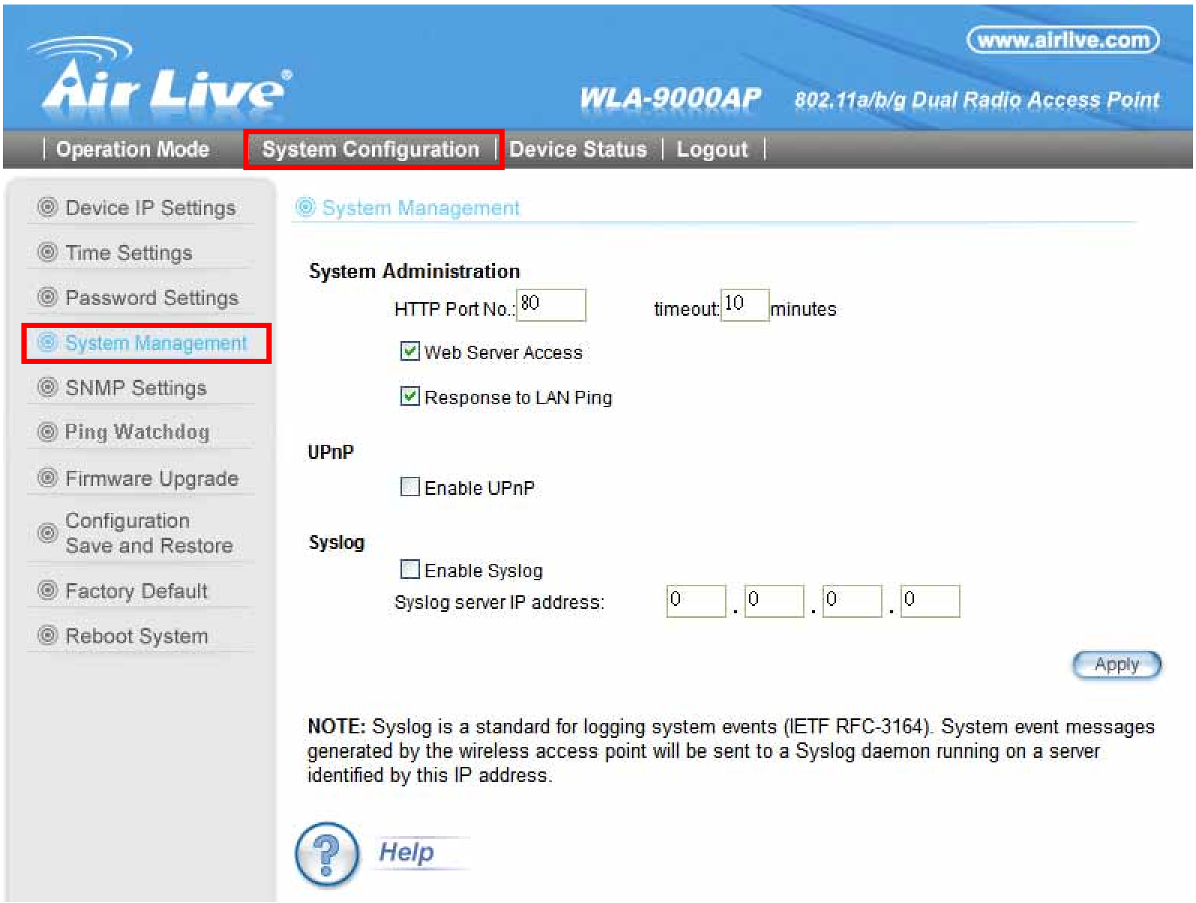
To change your administrative password, enter your current password and then the new password twice.

Current Password:	
New Password:	
Re-enter New Password:	

5.1.4 System Management

System Configuration -> System Management

In this page, administrator can change the management parameters and disable/enable management interface.



System Management

System Administration

HTTP Port No.: 80 timeout: 10 minutes

☑ Web Server Access

☑ Response to LAN Ping

UPnP

□ Enable UPnP

Syslog

□ Enable Syslog

Syslog server IP address: 0 . 0 . 0 . 0

NOTE: Syslog is a standard for logging system events (IETF RFC-3164). System event messages generated by the wireless access point will be sent to a Syslog daemon running on a server identified by this IP address.

System Administration

- **HTTP Port No**: The default port for HTTP is Port 80, you can change the value here
- **Timeout**: The default management timeout is 10 minutes. After timeout, the WLA-9000AP will ask you to login again. You can change the timeout value here.
- **Web Server Access**: You can enable or disable HTTP service from WAN side
- **Response to WAN ping**: You can disable or enable whether WLA-9000AP will response to PING command.

UPnP: Click here to enable UPnP. It is recommended not to open UPnP for security reason.

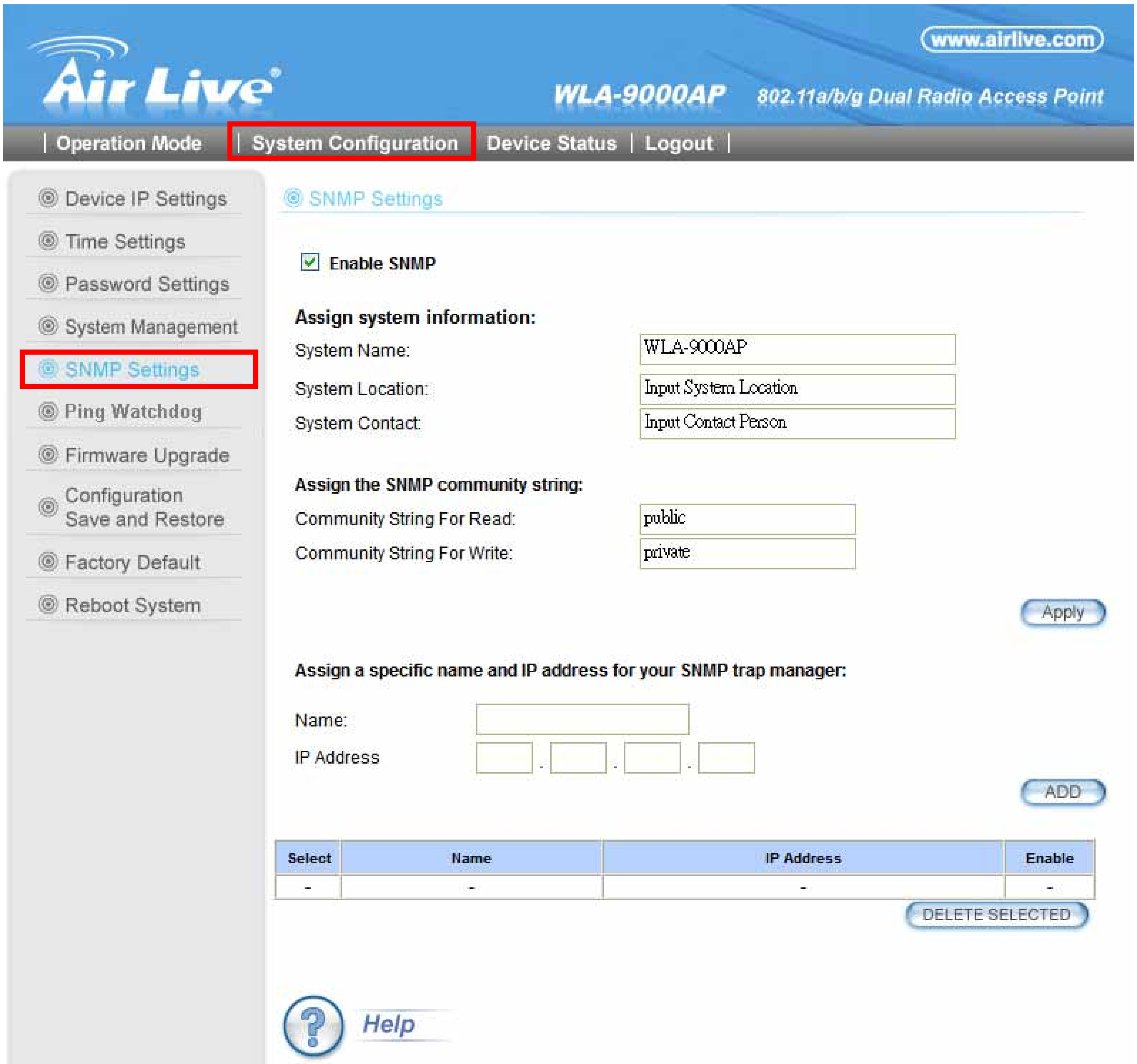
Syslog: Syslog is an IETF (Internet Engineering Task Force - the Internet standards body)-conformant standard for logging system events (RFC-3164). When the WLA-9000AP encounters an error or warning condition (ie., a log-in attempt with an invalid password), it will create a log in the system log table. To be able to remotely view such system log events, you need to check the *Enable Syslog* box and configure the IP address of a Syslog daemon. When doing so, the WLA-9000AP will send logged events over network to the daemon for future reviewing.

Syslog server IP address: System event messages generated by the wireless access point will be sent to a Syslog daemon running on a server identified by this IP address.

5.1.5 SNMP Settings

System Configuration -> SNMP Settings

This screen allows you to configure SNMP parameters including the system name, the location and contact information.



SNMP Settings

☑ Enable SNMP

Assign system information:

System Name: WLA-9000AP

System Location: Input System Location

System Contact: Input Contact Person

Assign the SNMP community string:

Community String For Read: public

Community String For Write: private

Assign a specific name and IP address for your SNMP trap manager:

Name:

IP Address . . .

Select	Name	IP Address	Enable
-	-	-	-

- **System Name:** A name that you assign to your WLA-9000AP. It is an alphanumeric string of up to 30 characters.

- **System Location:** Enter a system location.

- **System Contact:** Contact information for the system administrator responsible for managing the WLA-9000AP. It is an alphanumeric string of up to 60 characters.

- **Community String For Read:** If you intend the router to be managed from a remote SNMP management station, you need to configure a read-only “community string” for read-only operation. The community string is an alphanumeric string of up to 15 characters.

- **Community String For Write:** For read-write operation, you need to configure a write “community string”.

- **Assign a specific name and IP address for your SNMP trap manager:**

  A trap manager is a remote SNMP management station where special SNMP trap messages are generated (by the router) and sent to in the network.

  You can define trap managers in the system.

  You can add a trap manager by entering a *name*, an *IP address*, followed by pressing the *ADD* button.

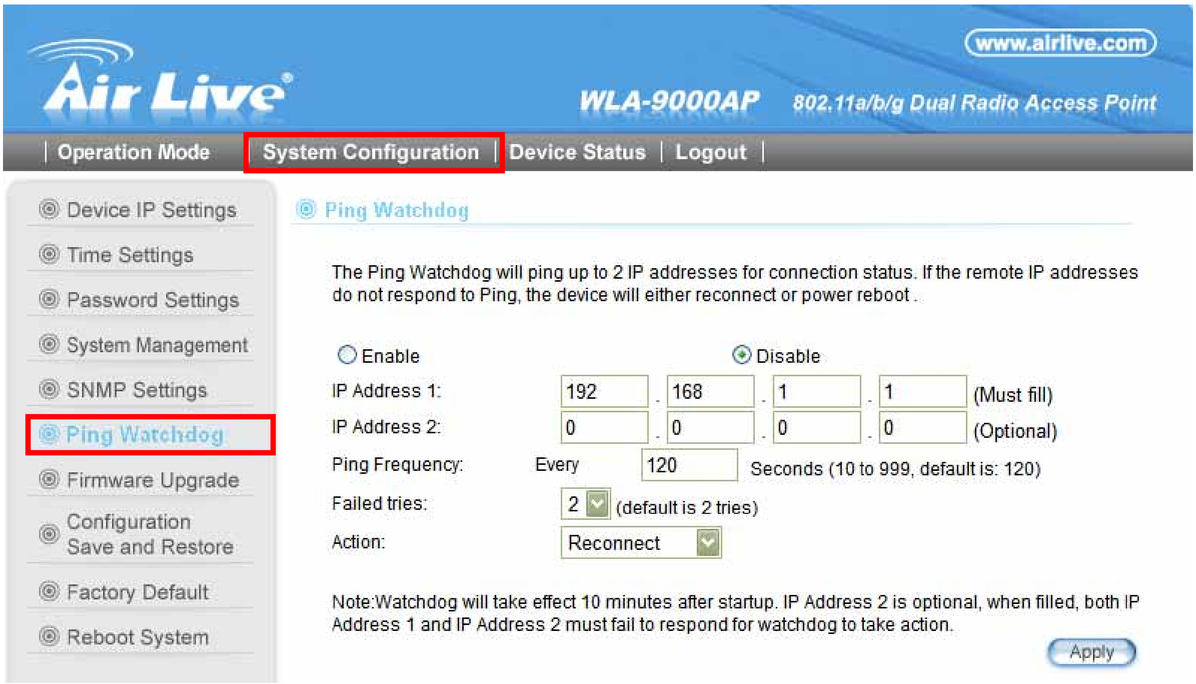
  You can delete a trap manager by selecting the corresponding entry and press the *DELETE SELECTED* button.

  To enable a trap manager, check the *Enable* box in the corresponding entry; to disable it, un-check the *Enable* box.

5.1.6 Ping Watchdog

System Configuration -> Ping Watchdog

The Ping Watchdog will ping remote IP addresses to make sure the wireless connection is active, if not, it can either reconnect or reboot. To prevent the AP from power recycling, the PING watchdog will start 10 minutes after power up to prevent power recycle problem.



Ping Watchdog

The Ping Watchdog will ping up to 2 IP addresses for connection status. If the remote IP addresses do not respond to Ping, the device will either reconnect or power reboot .

○ Enable ● Disable

IP Address 1: 192 . 168 . 1 . 1 (Must fill)

IP Address 2: 0 . 0 . 0 . 0 (Optional)

Ping Frequency: Every 120 Seconds (10 to 999, default is: 120)

Failed tries: 2 (default is 2 tries)

Action: Reconnect

Note:Watchdog will take effect 10 minutes after startup. IP Address 2 is optional, when filled, both IP Address 1 and IP Address 2 must fail to respond for watchdog to take action.

- **PING Frequency** means: "How often the CPE will PING". For example, it will PING once every "1" minute.

- **Fail Tries** means "How many times fails before the CPE will judge the PING failed". For example "2" means the CPE will reconnect if the PING doesn't respond for 2 times.

When you set the Ping Frequency to every "2" minutes and Fail Tries to "2". It means the CPE will ping every 2 minutes, after the second failure, it will reconnect.

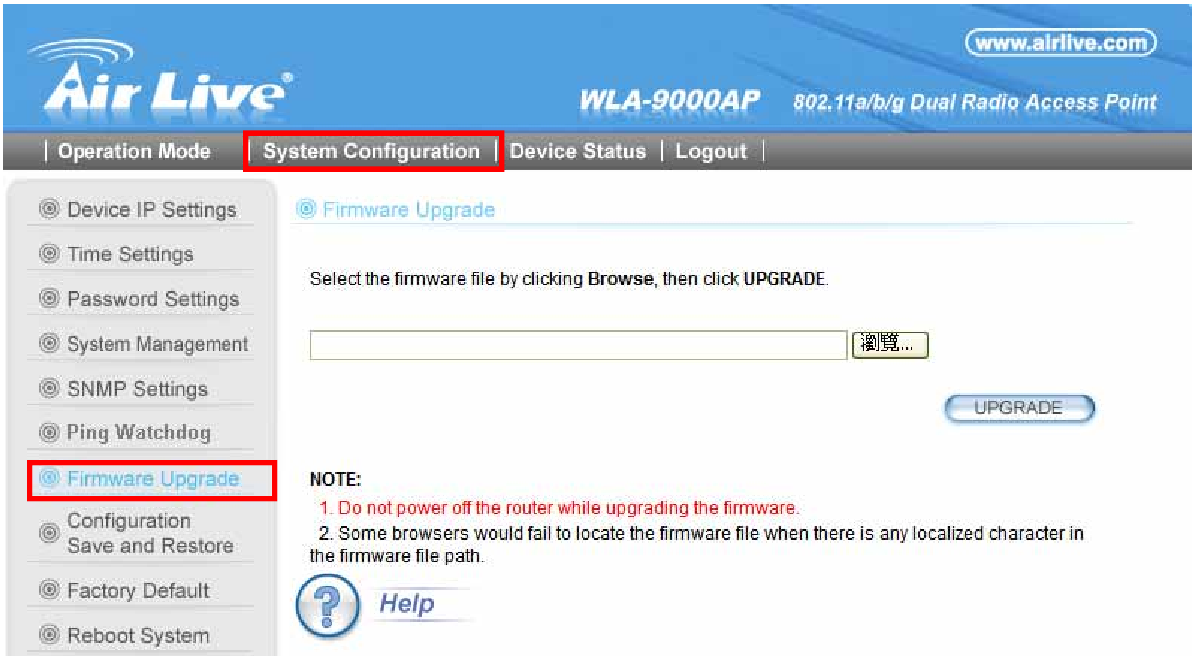
Actions:

- Reconnect: the WLA-9000AP will attempt to re-establish the connection. It is recommend to use this option for WDS Bridge connection.
- Reboot: the WLA-9000AP will do a power recycle.

5.1.7 Firmware Upgrade

System Configuration -> Firmware Upgrade

You can upgrade the firmware of your WLA-9000AP (the software that controls your WLA-9000AP's operation). Normally, this is done when a new version of firmware offers new features that you want, or solves problems that you have encountered with the current version.



Select the firmware file by clicking **Browse**, then click **UPGRADE**.

NOTE:

1. Do not power off the router while upgrading the firmware.
2. Some browsers would fail to locate the firmware file when there is any localized character in the firmware file path.

- **Upgrade Firmware:**

  To update the WLA-9000AP firmware, first download the firmware from AirLive web site to your local disk, and then from the above screen enter the path and filename of the firmware file (or click **Browse** to locate the firmware file). Next, Click the **Upgrade** button to start.

  The new firmware will be loaded to your WLA-9000AP. After a message appears telling you that the operation is completed, you need to reset the system to have the new firmware take effect.

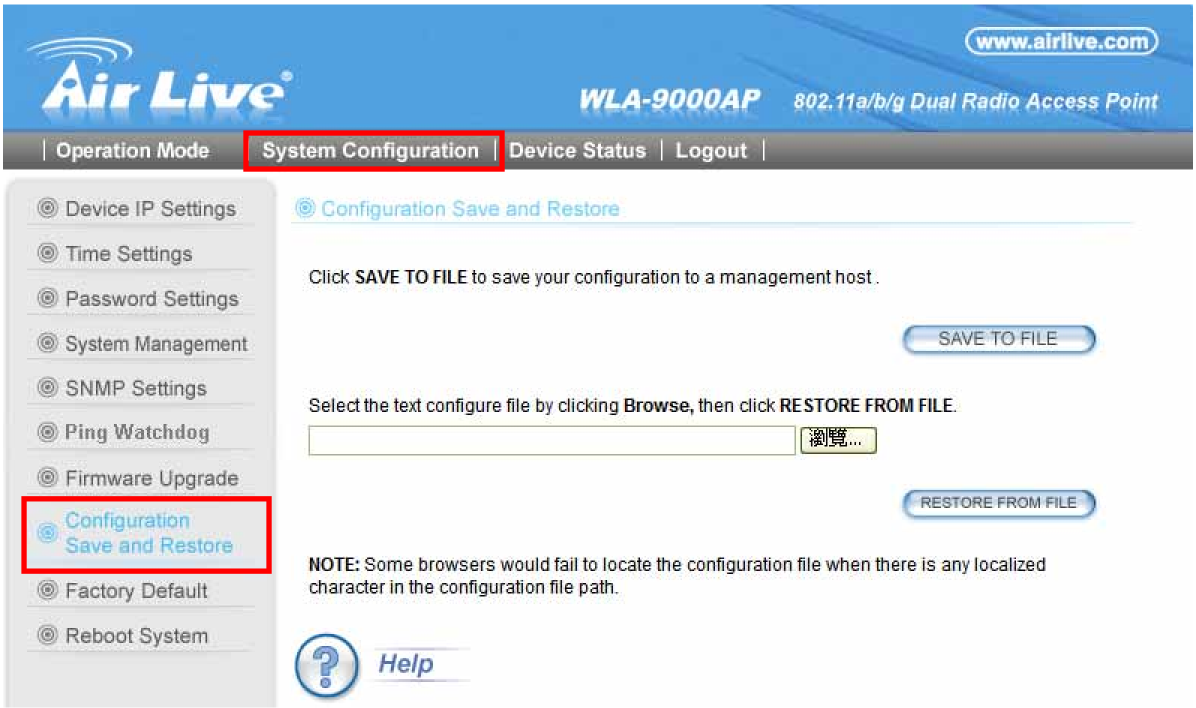
⚠ Do not power off the device while upgrading the firmware.
It is recommended that you do not upgrade your WLA-9000AP unless the new firmware has new features you need or if it has a fix to a problem that you've encountered.

5.1.8 Configuration Save and Restore

System Configuration -> Configuration Save and Restore

You can save system configuration settings to a file, and later download it back to the WLA-9000AP by following the steps.

Step 1 Select *Configuration Save and Restore* from the *System Configurations* menu.



Click **SAVE TO FILE** to save your configuration to a management host .

Select the text configure file by clicking **Browse**, then click **RESTORE FROM FILE**.

NOTE: Some browsers would fail to locate the configuration file when there is any localized character in the configuration file path.

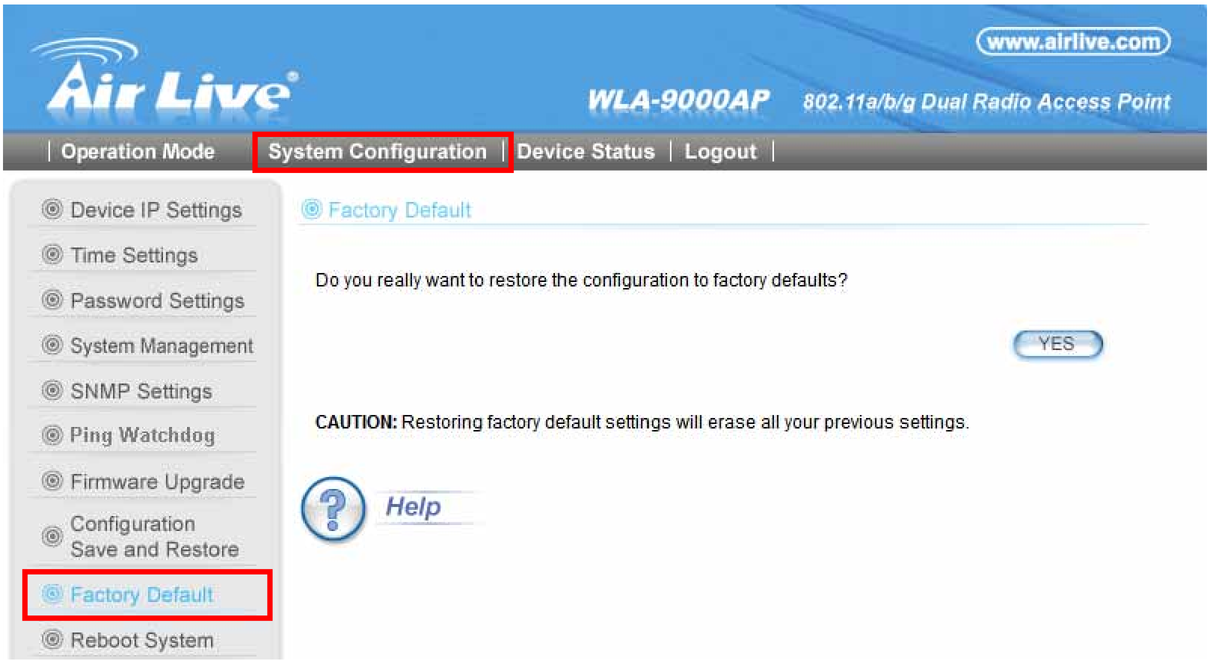
Step 2 Enter the path of the configuration file to save-to/restore-from (or click the *Browse* button to locate the configuration file). Then click the *SAVE TO FILE* button to save the current configuration into the specified file, or click the *RESTORE FROM FILE* button to restore the system configuration from the specified file.

5.1.9 Factory Default

System Configuration -> Factory Default

You can reset the configuration of your WLA-9000AP to the factory default settings.

Step 1 Select *Factory Default* from the *System Configuration* menu.



Factory Default

Do you really want to restore the configuration to factory defaults?

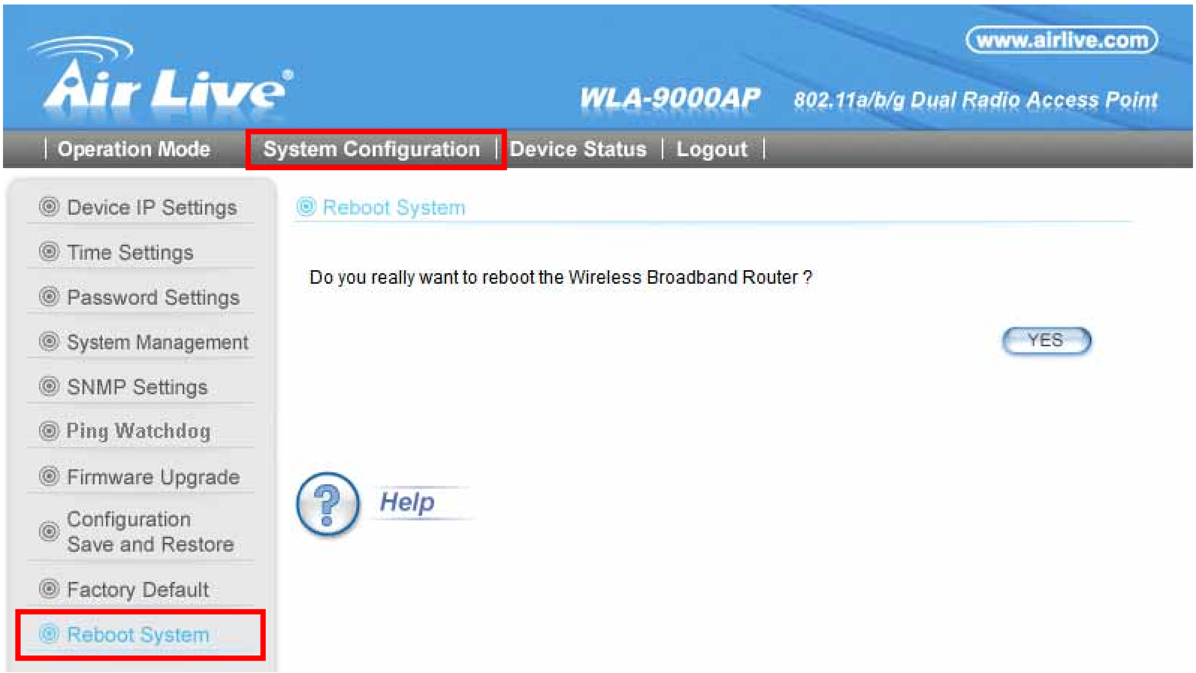
CAUTION: Restoring factory default settings will erase all your previous settings.

Step 2 Click *YES* to go ahead and restore the configuration to the factory default.

5.1.10 Reboot System

System Configuration -> Reboot System

You can reboot WLA-9000AP in this page.



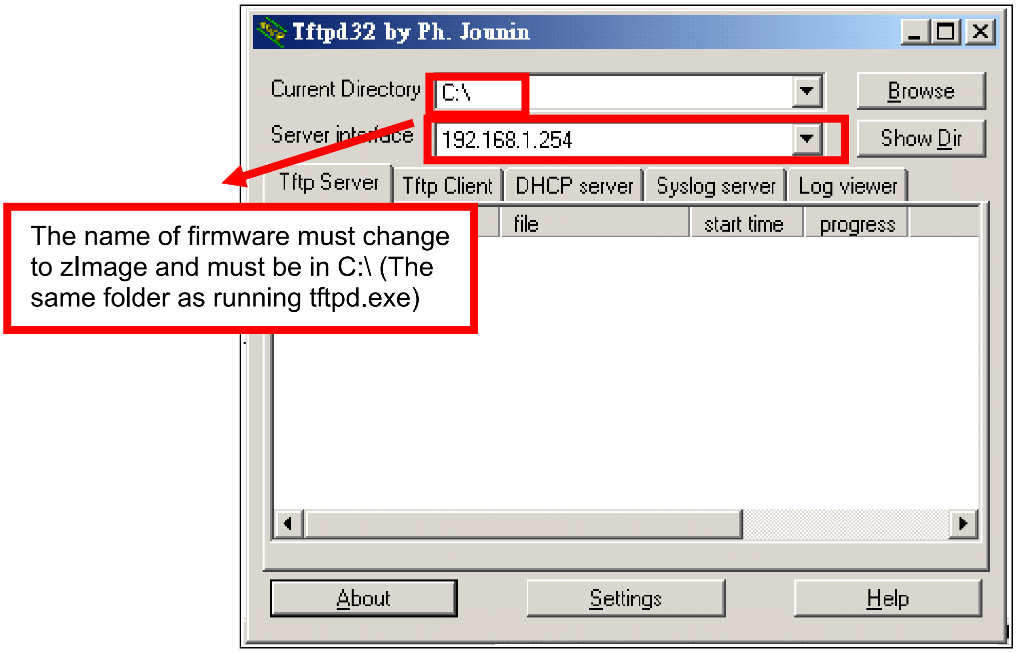
Reboot System

Do you really want to reboot the Wireless Broadband Router ?

5.1.1 WLA-9000AP Emergency Recovery

This section guides to recover your WLA-9000AP system if the firmware crashed.

1. Download the tftp server to your PC. In the following example, we use tftpd32: http://tftpd32.jounin.net/tftpd32_download.html.
2. Copy the tftpd32.exe of the downloaded file to C:\.
3. Change the IP address of your PC to 192.168.1.254 / 255.255.255.0
4. Copy the WLA-9000AP firmware to C:\ and rename the firmware to **"zImage"**. Note that the name must be zImage and no extension.
5. Connect WLA-9000AP and PC with an Ethernet cable.
6. Run the tftpd32.exe. Note that the IP address must be 192.168.1.254.



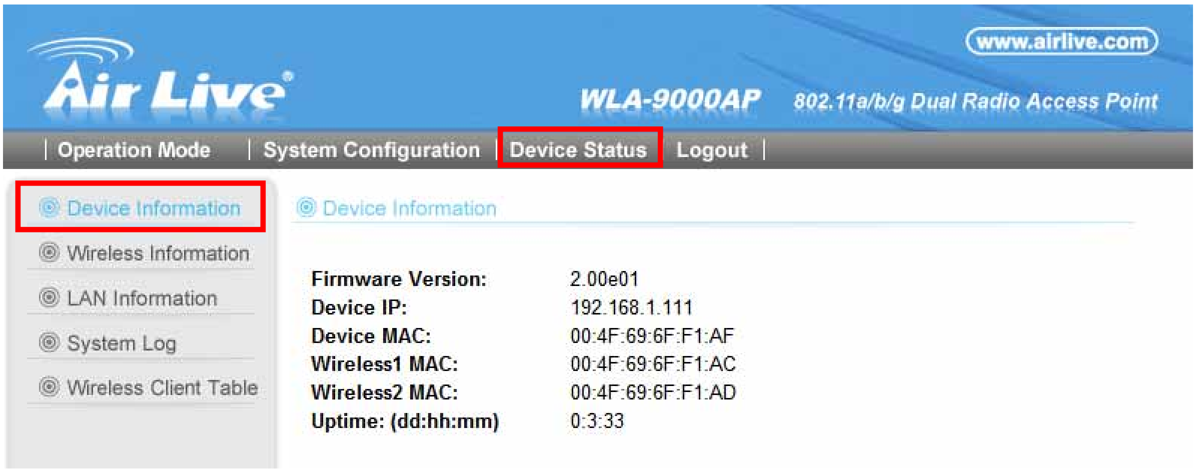
The name of firmware must change to zImage and must be in C:\ (The same folder as running tftpd.exe)

7. Power on WLA-9000AP, the **"Status"** LED will light on after 3 seconds.
8. Push the **"Reset"** button until the **"Status"** LED off and on again and release the **"Reset"** button.
9. If the above process success, the WLA-9000AP LAN LED keep flashing and the tftp serve shows file download information.
10. It takes around 5 minutes to download firmware and around 5 minutes to update the firmware.
11. After a successful recovery, the WLA-9000AP boots up automatically.
12. Try access 192.168.1.1, or the IP address you had changed before.

Repeat the processes again if failed.

5.2 Device Status

When you click on the "Device Status" on the top menu bar, the sub menu for device status will appear.



Firmware Version:	2.00e01
Device IP:	192.168.1.111
Device MAC:	00:4F:69:6F:F1:AF
Wireless1 MAC:	00:4F:69:6F:F1:AC
Wireless2 MAC:	00:4F:69:6F:F1:AD
Uptime: (dd:hh:mm)	0:3:33

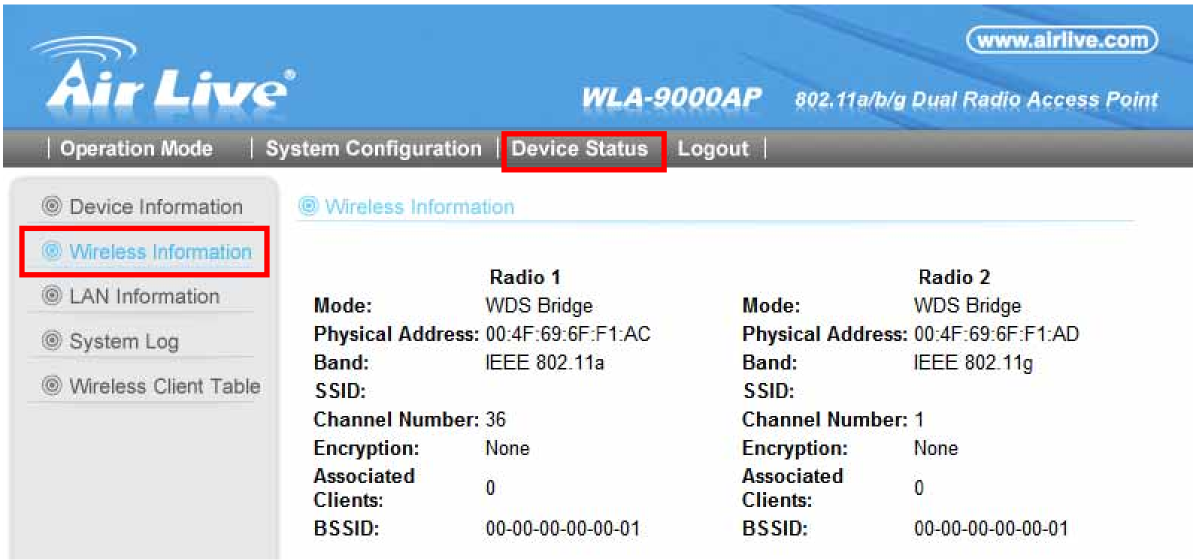
5.2.1 Device Information

This page shows the general information about WLA-9000AP such as firmware version, device IP/MAC, WAN IP/MAC(in router modes), Gateway IP(in router modes), DNS IP…etc. Below are some additional explanations on some status information of this page:

- **Firmware version**:   In general, AirLive will refer to its firmware as exx (such as e2) version on the release note
- **Device IP**:   It shows LAN IP.
- **Device MAC**:   It shows MAC address of LAN.
- **Wan IP**:   It shows WAN IP.
- **Wan MAC**:   It shows MAC address of WAN.
- **Gateway IP**: It shows IP address of Gateway.
- **DNS IP**:   It shows IP address of DNS.
- **Wireless MAC**: This is the wireless MAC address (BSSID) of this WLA-9000AP.   This is the address to enter on the remote WDS Bridge for the WDS link.
- **Uptime**:   This is the time that the WLA-9000AP has been running since last power up.

5.2.2 Wireless Information

This page shows the information about wireless status such as current operation mode, wireless traffic, error packets, RSSI, Remote device's BSSD, connecting State, channel, and encryption used.

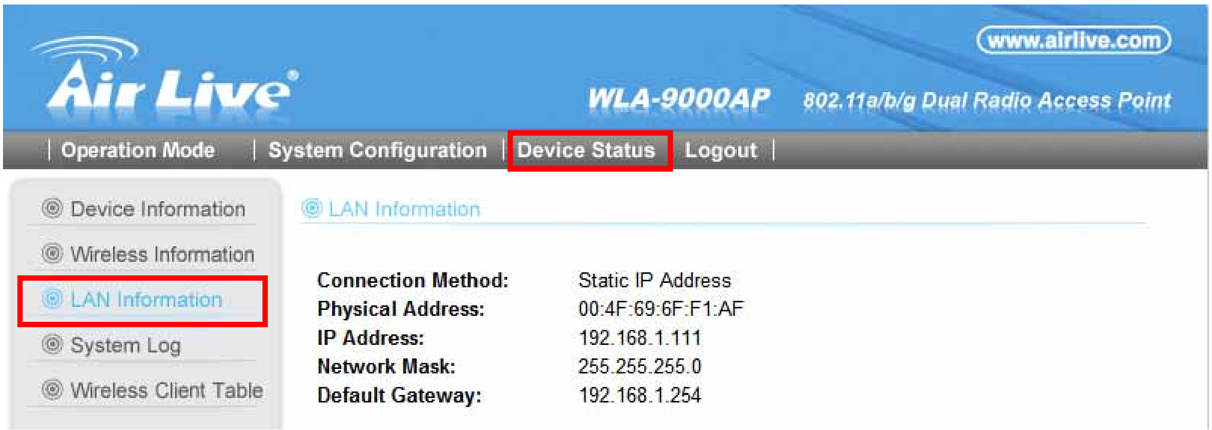


Wireless Information

	Radio 1		Radio 2
Mode:	WDS Bridge	Mode:	WDS Bridge
Physical Address:	00:4F:69:6F:F1:AC	Physical Address:	00:4F:69:6F:F1:AD
Band:	IEEE 802.11a	Band:	IEEE 802.11g
SSID:		SSID:	
Channel Number:	36	Channel Number:	1
Encryption:	None	Encryption:	None
Associated Clients:	0	Associated Clients:	0
BSSID:	00-00-00-00-00-01	BSSID:	00-00-00-00-00-01

5.2.3 LAN Information

This page shows the information about LAN port of the WLA-9000AP. It includes the type of LAN port authentication used and the IP address information about the LAN port.

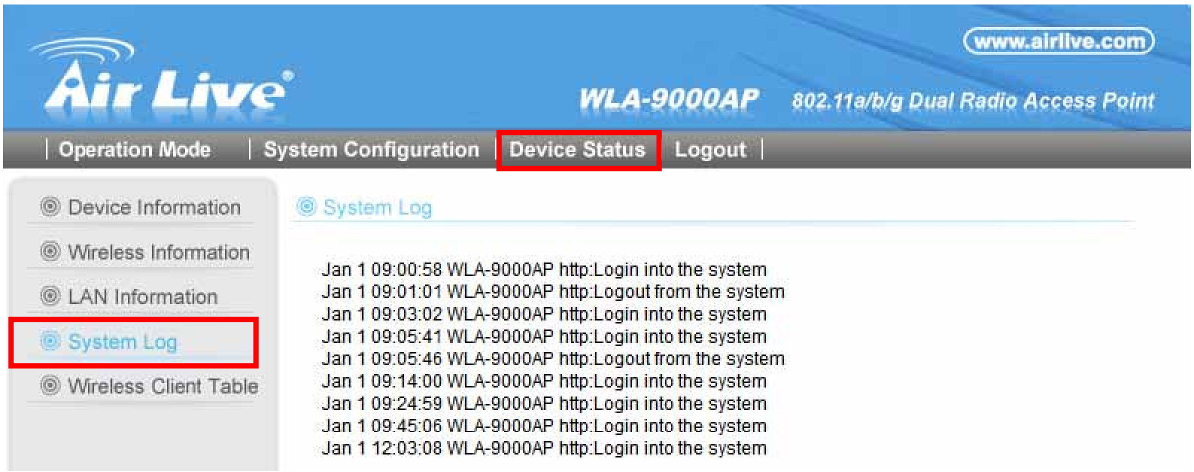


LAN Information

Connection Method:	Static IP Address
Physical Address:	00:4F:69:6F:F1:AF
IP Address:	192.168.1.111
Network Mask:	255.255.255.0
Default Gateway:	192.168.1.254

5.2.4 System Log

The System Log displays the system activities, login, and system error report. If you need to report a problem to Air Live, please be sure to send us the System Log information also.

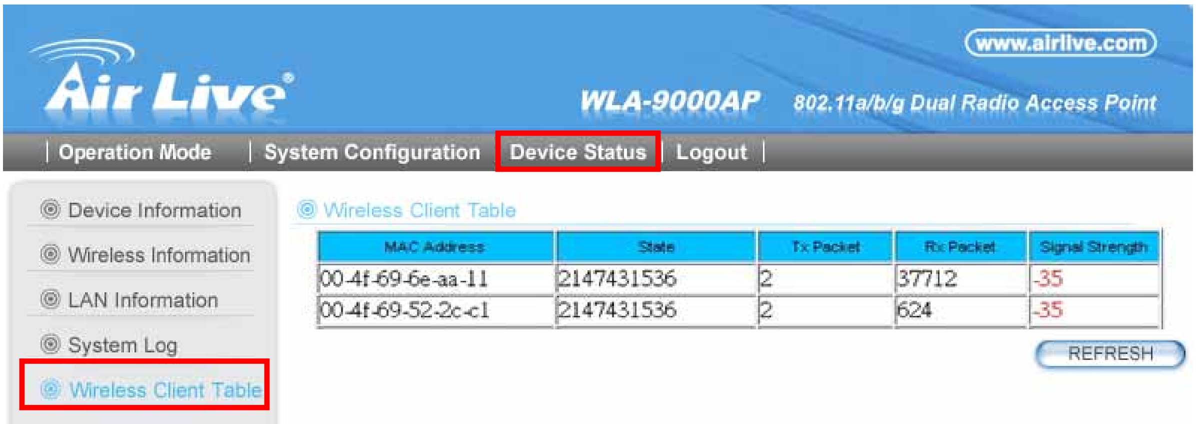


System Log

```
Jan 1 09:00:58 WLA-9000AP http:Login into the system
Jan 1 09:01:01 WLA-9000AP http:Logout from the system
Jan 1 09:03:02 WLA-9000AP http:Login into the system
Jan 1 09:05:41 WLA-9000AP http:Login into the system
Jan 1 09:05:46 WLA-9000AP http:Logout from the system
Jan 1 09:14:00 WLA-9000AP http:Login into the system
Jan 1 09:24:59 WLA-9000AP http:Login into the system
Jan 1 09:45:06 WLA-9000AP http:Login into the system
Jan 1 12:03:08 WLA-9000AP http:Login into the system
```

5.2.5 Wireless Client Table

This function is available in AP mode and AP Router mode only. It displays the information about wireless clients that are associated with WLA-9000AP. It includes signal strength, TX and RX data rate, MAC address, and the state.



Wireless Client Table

MAC Address	State	Tx Packet	Rx Packet	Signal Strength
00-4f-69-6e-aa-11	2147431536	2	37712	-35
00-4f-69-52-2c-c1	2147431536	2	624	-35

6 Command Line Interface

In this chapter, we will explain commands that are available through Telnet or SSH interface. We will provide descriptions for the commands, example settings and the WLA-9000AP's response. The purpose for this chapter is to introduce available CLI commands only. For detail descriptions on the concept and application of the settings, please refer to chapter 4 and chapter 5.

Before reading this chapter, please go through Section 3.3 of Chapter 3. It contains information on how to login Telnet or SSH/SSH2 interface. For quick reference, the login and password is as bellowed:

- **Telnet**
  - ❑ Password: airlive

- **SSH/SSH2**
  - ❑ First login
    - Login: root
    - Password: <nothing, just press enter>
  - ❑ Second login:
    - Password: airlive

  When you change WLA-9000AP's password, it will change the second login's password only.

You can get a list of available commands by typing "help" at the command prompt.

> ⚠ You must remember to save the configurations by typing "***save config***" at the command prompt after making changes, otherwise, the configuration will be lost after reboot.

6.1 System Commands

■ **ping <IP address>**

This is the command

❑ *Purpose*: to ping a remote IP address

Here explains the usage of the command

❑ *Example*:

```
Command> ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: icmp_seq=0 ttl=64 time=1.8 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=1.0 ms
```

Example command and response

■ **change password**

❑ *Purpose:* Change login password

❑ *Example:*

```
Command> change password 123
password is set to: 123
```

■ **ftptest <ssid> 11a <channel>**

❑ *Purpose:* Test if a SSID's connection is okay

❑ *Example:*

```
Command> ftptest   airlive 11a 40
Set SSID : airlive , mode = 11a , channel = 40 ok !
```

■ **save config**

❑ *Purpose:* save configuration file. Please remember to "save config" after making changes

❑ *Example:*

```
Command> save config
None
```

■ **clear config**

❑ *Purpose:* Clear configuration to default

❑ *Example:*

```
Command> clear config
```

```
Are you sure ? ( y/n ) : y
Write flash block [/dev/mtd3]
Write file is [/etc/defsysconfig.conf]
Rebooting...
```

- **webservice <lan | wan> <enable | disable>**
- ❑ *Purpose:* Enable or Disable Web management interface on LAN or WAN
- ❑ *Example:*

```
Command> webservice lan enable
webservice from lan enable
```

- **site survey**
- ❑ *Purpose:* Site Survey display
- ❑ *Example:*

```
Command> site survey
Please wait a moment for site survey...

ESSID        MAC Address     Conn Mode Channel Turbo Super XR WME Signal Strength(dbm) Security    Network
=====================================================================================================
airlive       00:4f:79:90:00:27      A          36        -        --    *          -49                None              AP
airlive       00:4f:69:52:a1:ca      A          36        -        --    *          -61                None              AP
airmax-ap   00:4f:69:90:00:01      A          36        -        --    *          -56                None              AP
```

- **signal survey <bssid> <channel>**
- ❑ *Purpose:* Display continuous RSSI for the remote AP/Bridge
- ❑ *Example:*

```
Command> signal survey 00-4f-69-52-a1-ed 36

BSSID                        Channel     Signal Strength(dbm)
==================================================
00-4F-69-52-A1-ED          36                -40
```

```
BSSID                    Channel     Signal Strength(dbm)
===================================================
00-4F-69-52-A1-ED           36              -40
...
.
```

6.2 Debugging Commands

Those debugging commands are commands used for manufacturing testing process. If a z_debug command looks similar to a Set command, please use the Set command instead.

- ■ **z_debug http logout**
- ❑ *Purpose:* log out HTTP
- ❑ *Example:*

```
Command> z_debug http logout
```

- ■ **z_debug signature <enable/disable>**
- ❑ *Purpose:* Enable or disable signature check on firmware
- ❑ *Example:*

```
Command> z_debug signature disable

Are you sure ? ( y/n ) : y
Signature check is now DISABLED!!!
```

- ■ **z_debug add ssid <ssid>**
- ❑ *Purpose:* This command will replace the default ssid with the new one. It will not add an additional SSID. We recommend to use the following commands instead:
  - ■ **add ssid <ssidname> broadcast (enable/disable)** to add a new SSID
  - ■ **set ssid <ssidname>** to replace the current ssid name with a new one
- ❑ *Example:*

```
Command> z_debug add ssid air1
```

- **z_debug reboot**
- ❑ *Purpose:* reboot your WLA-9000AP
- ❑ *Example:*

```
Command> z_debug reboot
Rebooting...
```

- **z_debug set port radio1 11a <ssid> <channel>**
- ❑ *Purpose:* Set SSID and Channel. We recommend using set commands instead;
  - **set ssid <ssid>** : to set the ssid name
  - **set rate mode <mode value>**: set radio mode to *11a* | *supera_no_turbo* | *supera_static_turbo*.| *supera_dynamic_turbo*
- ❑ *Example:*

```
Command> z_debug set port radio1 11a air2 64
```

6.3 Show Commands

Show Commands are command that show the settings and status of WLA-9000AP

- **show arp table**
- ❑ *Purpose:* Show ARP Table
- ❑ *Example:*

```
Command> show arp table
IP address          Flags   HWaddress            Device
-----------------------------------------------------------------------------------------
192.168.1.100        C       00:1D:60:5E:AE:A0    lan
```

- **show http**
- ❑ *Purpose:* Show HTTP service settings
- ❑ *Example:*

```
Command> show http
```

```
HTTP service port: 80
HTTP session timeout: 10 minutes
```

■ **show upnp**

❑ *Purpose:* Show UPnP information

❑ *Example:*

```
Command> show upnp
UPnP is disabled
```

■ **show mac**

❑ *Purpose:* show the MAC address table in MAC filter mode. *This might change to show the wireless MAC address of WLA-9000AP in future firmware release*

❑ *Example:*

```
Command> show mac
Filter Name          MAC address
-----------------------------------------------------
ailrive            00-4f-62-24-12-34
```

■ **show mac filter**

❑ *Purpose:* show mac address table in the Access Control List

❑ *Example:*

```
Command> show mac filter
Filter Name          MAC address
------------------------------------------------
hello            00-4f-62-24-12-34
airlive            00-4f-62-24-11-11
```

■ **show mac filter mode**

❑ *Purpose:* Show whether the current MAC address is enable or not

❑ *Example:*

```
Command> show mac filter mode
MAC filter mode: disable
```

■ **show mac filter <string up to 16 characters>**

❑ *Purpose:* show mac filter status with the filter name

❑ *Example:*

```
Command> show mac filter hello
Filter Name          MAC address
--------------------------------------------------
hello              00-4f-62-24-12-34
```

■ **show community string read**

❑ *Purpose:* Show SNMP community string

❑ *Example:*

```
Command> show community string read
SNMP Community String (read-only):   public
```

■ **show snmp**

❑ *Purpose:* Show whether SNMP is enable or disabled

❑ *Example:*

```
Command> show snmp
SNMP is enabled
```

■ **show trap manager**

❑ *Purpose:* Show SNMP Trap manager status

❑ *Example:*

```
Command> show trap manager
Trap Manager     IP Address            Status
------------------------------------------------------------------
```

```
ailrive           192.168.1.123          enabled
```

■ **show trap manager <string up to 16 characters>**

❑ *Purpose:* Show SNMP Trap manager status with the assigned name

❑ *Example:*

```
Command> show trap manager airlive
Trap Manager     IP Address             Status
-----------------------------------------------------------------
ailrive           192.168.1.123          enabled
```

■ **show radius server**

❑ *Purpose:* Show radius server settings

❑ *Example:*

```
Command> show radius server

RADIUS Server                  State                       IP/Port
-----------------------------------------------------------------------------------
Primary                        Disabled                     0.0.0.0/1812
Secondary                       Disabled                    0.0.0.0/1812

RADIUS Server reattempt: 60 seconds
```

■ **show radius server <primary | secondary>**

❑ *Purpose:* Show settings of primary or secondary radius server

❑ *Example:*

```
Command> show radius server primary
RADIUS Server: primary
State: Disabled
Server IP: 0.0.0.0
Port Number: 1812
Shared Secret:
```

■ **show log level**

❑ *Purpose:* show log level

❑ *Example:*

```
Command> show log level
Log level is 8
```

■ **show telnet / system**

❑ *Purpose:* show telnet management information and system status

❑ *Example:*

```
Command> show telnet
Telnet session timeout: 0 minutes
Telnet port number: 23
Telnet state: enable

Command> show system
System Name: WLA-9000AP
----------------------------------------------------------------------------
S/W Version:                1.00e09a
H/W Version:                S0A
System LAN MAC:               00-4F-79-90-00-16
Wireless MAC:                 00-4F-79-90-00-15

WMAC-0:            00-4F-79-90-00-15
```

■ **show snmp statistics**

❑ *Purpose:* Show SNMP satistics

❑ *Example:*

```
Command> show snmp statistics

Timeout: No Response from 192.168.1.1
```

```
                              Received      Transmitted
------------------------------------------------------------------------
Total Packets                       1             1
Request Variables                  11
SET Variables                       0
GET Requests                        0
GETNEXT Requests                   15
GET-RESPONSEs                       0            25
SET Requests                        0

Errors:
Bad Versions                        0
Bad Community Uses:                 0
ASN1 Parse Errors                   0
Packet Too Long                     0
NO-SUCH-NAME Errors                 0
BAD-VALUE Errors                    0
READ-ONLY Errors                    0
GENERAL-ERR Errors                  0
```

- **show rssi**

❑ *Purpose:* Show RSSI signal strength

❑ *Example:*

```
Command> show rssi
Please wait a moment for site survey...


ESSID                     MAC Address           Signal Strength(dbm)
=====================================================================
airlive                    0:4f:69:52:a1:ca              -59
airmax-ap                 00:4f:69:90:00:01             -47
```

■ **show mode**

❑ *Purpose:* Show what operation is WLA-9000AP currently set to

❑ *Example:*

```
Command> show mode
operation mode: access point
```

■ **show wireless setting**

❑ *Purpose:* Show wireless settings

❑ *Example:*

```
Command> show wireless setting
Radio[1] operation mode:   access point
ssid name                :   air2
wireless state         :   enable
ssid broadcast          :   enable
radio[1] mode            :   11a
radio[1] channel       :   64
```

■ **show wireless security**

❑ *Purpose:* Show current wireless security policy

❑ *Example:*

```
Command> show wireless security
Radio1 security policy: none
```

■ **show <wan | lan> settings**

❑ *Purpose:* Show LAN or WAN port IP settings

❑ *Example:*

```
Command> show lan settings
Lan ip type       :          static
Lan ip address :   192.168.1.1
Lan ip netmask :   255.255.255.0
Lan ip gateway :   192.168.1.254
Lan ip dnsserv :    0.0.0.0

show firmware version
show vlan ssid list
show wds settings
show advanced wireless
show syslogd
```

- **show antenna**
- ❑ *Purpose:* Check antenna polarization
- ❑ *Example:*

```
Command> show antenna
Antenna setting is Vertical;
```

- **show ratemode**
- ❑ *Purpose:* Show whether the AirMax is using 5*MHz, 10MHz, or 20MHz* channel width
- ❑ *Example:*

```
Command> show ratemode
Ratemode is Full(20Mhz);
```

- **show noise immunity**
- ❑ *Purpose:* Show the noise immunity setting
- ❑ *Example:*

```
Command> show noise immunity
Noise immunity is enable
```

6.4 Set Commands

The Set Commands are to make changes to the WLA-9000AP's settings

■ **set http timeout <timeout value in minutes, 1-999>**

❑ *Purpose:* Set the timeout value for HTTP management

❑ *Example:*

```
Command> set http timeout 10
HTTP timeout: 10 minutes
```

■ **set system <contact |location> <string up to 60 characters>**

❑ *Purpose:* Set the system's location and contact info

❑ *Example:*

```
Command> set system location 60
System Location: 60
```

■ **set system name <string up to 32 characters>**

❑ *Purpose:* Set system's name

❑ *Example:*

```
Command> set system name airlive
System Name: airlive
```

■ **set mac filter mode <MAC filter mode, disabled/grant/deny>**

❑ *Purpose:* Set MAC filter mode or disable MAC filtering.

❑ *Example:*

```
Command> set mac filter mode disabled
mac filter mode is set to disabled
```

■ **set community string <read |write> <string up to 32 characters>**

❑ *Purpose:* Set SNMP community string

❑ *Example:*

```
Command> set community string write test
community string for write: test
```

```
Command> set community string read test
community string for read: test
```

■ **set radius server reattempt <reattempt interval in minutes, now no limit in seconds>**

❑ *Purpose:* set radius server reattempt interval in minutes

❑ *Example:*

```
Command> set radius server reattempt 20
/etc/wlan/ap_service: 17: uname: not found
killall: wpa_supplicant: no process killed
/etc/wlan/ap_service: 17: uname: not found
Using /lib/modules/2.4.25-LSDK-5.1.0.42/wlan/ath_hal.o
Using /lib/modules/2.4.25-LSDK-5.1.0.42/wlan/ath_rate_atheros.o
Using /lib/modules/2.4.25-LSDK-5.1.0.42/wlan/ath_dfs.o
Using /lib/modules/2.4.25-LSDK-5.1.0.42/wlan/ath_ahb.o
<mapping sub-ioctl turbo to cmd 0x8BE0-1>
<mapping sub-ioctl set_installmode to cmd 0x8BE0-75>
<mapping sub-ioctl set_threslower to cmd 0x8BE0-76>
<mapping sub-ioctl set_threslow to cmd 0x8BE0-77>
<mapping sub-ioctl set_thresbetter to cmd 0x8BE0-78>
<mapping sub-ioctl set_thresbest to cmd 0x8BE0-79>
<mapping sub-ioctl maccmd to cmd 0x8BE0-17>
RTNETLINK answers: No such file or directory
RADIUS Server Reattempt Period: 20 Seconds
```

■ **set telnet port <port number, 1-65535>**

❑ *Purpose:* change the telnet port numer

❑ *Example:*

```
Command> set telnet port 23

Changing telnet port may cause current telnet connections to be lost.
Are you sure ? ( y/n ) : y
```

```
Telnet port number: 23
```

- ■ **set telnet timeout <timeout value in minutes, 0-999, 0 for no limit>**
- ❑ *Purpose:* Set Telnet management timeout
- ❑ *Example:*

```
Command> set telnet timeout 10

Changing telnet timeout may cause current telnet connections to be lost.
Are you sure ? ( y/n ) : y
Telnet session timeout: 10 minutes
```

- ■ **set wmm qos <enable | disable>**
- ❑ *Purpose:* Enable or Disable WMM QoS
- ❑ *Example:*

```
Command> set wmm qos disable
set wmm qos disable successful!
```

- ■ **set log level <1-7>**
- ❑ *Purpose:* Set the log level
- ❑ *Example:*

```
Command> set log level 7
set log level 7 successful
```

- ■ **set client isolation <enable | disable>**
- ❑ *Purpose:* Enable or Disable client isolation / privacy seperator
- ❑ *Example:*

```
Command> set client isolation disable
Set client isolation disable successful!
```

■ **set operation mode <AP |repeater| client | ad-hoc |bridge_infra| wds_bridge | wisp | router>**

❑ *Purpose:* set or change operation mode

❑ *Example:*

```
Command> set operation mode AP
Operation mode is already setting!


Command> set operation mode wds_bridge
System should be reboot...


Are you sure ? ( y/n ) : y
```

■ **set <wan | lan> <webservice | ping> <enable |disable>**

❑ *Purpose:* enable/disable ping response or web server on the lan/wan side

❑ *Example:*

```
Command> set lan ping enable
set lan ping already enable
```

■ **set lan ip <ipaddress> sm <netmask> gw <gateway> dns <dns server>**

❑ *Purpose:* set LAN IP address such as IP, Subnet mask, gateway, and DNS server

❑ *Example:*

```
Command> set lan ip 192.168.1.1 sm 255.255.255.0 gw 192.168.1.254 dns
168.95.1.1
killall: dnsmasq: no process killed
LAN IP address :         192.168.1.1
Netmask          :         255.255.255.0
Gateway          :         192.168.1.254
DNS server       :          168.95.1.1
```

■ **set <enable | disable>**

❑ *Purpose:* Enable or Disable the wireless interface

❑ *Example:*

```
Command> set enable
Radio1 enabled
```

■ **set ssid <ssidname>**

❑ *Purpose:* Replace current main SSID name with a new one

❑ *Example:*

```
Command> set ssid WLA-9000AP
```

■ **set ssid remotessid <remote ssidname> Repeater Mode Only**

❑ *Purpose: Set the remote SSID name for repeater mode*

❑ *Example:*

```
Command> set ssid remotessid airlive2
```

■ **set broadcast <enable | disable>**

❑ *Purpose:* Enable or disable SSID broadcast

❑ *Example:*

```
Command> set broadcast enable
Radio1 broadcast enabled
```

■ **set radio mode <radio mode value>**

❑ *Purpose:* set radio mode to ***11a*** | ***supera_no_turbo*** | ***supera_static_turbo***.| ***supera_dynamic_turbo***

❑ *Example:*

```
Command> set radio mode supera_no_turbo
Radio1 radio mode: supera_no_turbo
```

■ **set channel <channel value>**

❑ *Purpose:* set wireless channel

❑ *Example:*

```
Command> set channel 36
Radio1 channel: 36
```

■ **set beacon interval <range:20-100>**

❑ *Purpose:* set beacon interval for wireless interface. For explanation on advance wireless parameters, please refer to section 4.2.14

❑ *Example:*

```
Command> set beacon interval 100
Radio1 beacon internal: 100
```

■ **set rts threshold <range:0-2347>**

❑ *Purpose: set rts threshold. For explanation on advance wireless parameters, please refer to section 4.2.14*

❑ *Example:*

```
Command> set rts threshold 2347
Radio1 RTS threshold: 2347
```

■ **set fragmentation <range:256-2346>**

❑ *Purpose*: set fragmentation value. For explanation on advance wireless parameters, please refer to section 4.2.14

❑ *Example:*

```
Command> set fragmentation 2346
Radio1 fragmentation: 2346
```

■ **set dtim interval <range:1-255>**

❑ *Purpose:* To set dtim interval value. For explanation on advance wireless parameters, please refer to section 4.2.14

❑ *Example:*

```
Command> set dtim interval 1
Radio1 DTIM interval: 1
```

■ **set user limitation <range:1-100>**

❑ *Purpose:* To set the user limit for wireless interface

❑ *Example:*

```
Command> set user limitation 100
Radio1 user limitation: 100
```

■ **set age out time <range:1-1000>**

❑ *Purpose:* To set the age timeout for wireless clients.

❑ *Example:*

```
Command> set age out time 5
Radio1 age out time: 5
```

■ **set transmit power <range: 0-24>**

❑ *Purpose:* To set the TX output power value of the radio

❑ *Example:*

```
Command> set transmit power 20
Radio1 transmit power: 20
```

■ **set data rate <best | 6~54>**

❑ *Purpose:* To set the date rate. For example, 54mbps, 36mbps….etc

❑ *Example:*

```
Command> set data rate 54
Radio1 data rate: 54
```

■ **set acktimeout <11A>**

❑ *Purpose:* To set the ACK timeout value

❑ *Example:*

```
Command> set acktimeout 25
AckTimeOut for radio1: 11A=25
```

■ **set vlan for ssid <enable | disable>**

❑ *Purpose:* Enable VLAN function

❑ *Example:*

```
Command> set vlan for ssid enable
```

■ **set diffserv marking <enable | disable>**

❑ *Purpose:* To enable diffserv marking function in multiple SSID & VLAN configuration.

❑ *Example:*

```
Command> set diffserv marking enable
```

■ **set security <ssid> none**

❑ *Purpose:* To remove security policy from a SSID

❑ *Example:*

```
Command> set security airlive none
Set Radio1 no security !
```

■ **set security <ssid> wep <key number> <64|128|152> <ascii | hex> <key string> <defaultkey>**

❑ *Purpose:* To set the WEP security policy

❑ *Example:*

```
Command> set security WLA-9000AP wep 1 64 hex 1234567890
Radio1 authentication type : wep !
```

- **set security <ssid> <wpa|wpa2> <tkip|aes|both> interval <0~300>**
- □ *Purpose: to set the WPA or WPA2 security policy*
- □ *Example:*

```
Command> set security WLA-9000AP wpa2 tkip interval 300
Radio1 authentication type : wpa2 !
```

- **set security <ssid> <wpa-psk|wpa2-psk> <tkip|aes|both> interval <0~300> <key string>**
- □ *Purpose: to set the WPA-PSK or WPA2-PSK security policy*
- □ *Example:*

```
Command> set security WLA-9000AP wpa2-psk aes interval 300 12345678
Radio1 authentication type : wpa2-psk !
```

- **set antenna <diversity | vertical | horizontal >**
- □ *Purpose:* To set the antenna to use horizontal, vertical, diversity polarizations.
- □ *Example:*

```
Command> set antenna horizontal
Antenna setting is Horizontal
```

- **set ratemode <full | half | quarter>**
- □ *Purpose:*
- □ *Example:*

```
Command> set ratemode full
Rate mode is Full(20Mhz)
```

- **set noise immunity <on | off>**
- □ *Purpose:* To enable/disable the noise immunity level
- □ *Example:*

```
Command> set noise immunity on
Noise immunity is enable
```

6.5 Enable/Disable Commands

Commands to enable or disable settings

■ **(enable/disable): <enable | disable> upnp**

❑ *Purpose:* To enable or disable UPnP

❑ *Example:*

```
Command>enable upnp
(Upnp)descDocName: BD.xml
UPnP Daemon: Intializing UPnP with descDocUrl=http://192.168.1.1:80/BD.xml
UPnP Daemon: ipaddress=192.168.1.1 port=80
UPnP Daemon: conf_dir_path=/var/upnp
Initializing UPnP SDK ...
UPnP SDK Successfully Initialized.
Setting the Web Server Root Directory to /var/upnp
Succesfully set the Web Server Root Directory.

UpnpGetServerPort(): 49152
Registering the root device with descDocUrl http://192.168.1.1:49152/BD.xml
IGD root device successfully registered.
Advertisements Sent.   Listening for requests ...

Command> disable upnp
Shutting down on signal 15...
UPnP is disabled
```

■ **<enable | disable> snmp**

❑ *Purpose:* To enable/disable SNMP

❑ *Example:*

```
Command> enable snmp
SNMP is enabled

Command> disable snmp
SNMP is disabled
```

- ■ **<enable | disable> syslogd**
- ❑ *Purpose:* To enable or disable syslog
- ❑ *Example:*

```
Command> enable syslogd
Invalid configuration specified.

Command> disable syslogd
Syslogd is disabled
```

- ■ **<enable | disable> radius server <primary | secondary>**
- ❑ *Purpose:* To enable or disable primary/secondary radius server
- ❑ *Example:*

```
Command> enable radius server primary
Invalid configuration specified.

Command> enable radius server secondary
Invalid configuration specified.
```

6.6 Add/Delete Commands

Commands to add or delete settings

- ■ **(add/delete): add mac filter < Mnemonics Name> <MAC address, XX-XX-XX-XX-X-XX>**
- ❑ *Purpose:* to add an entry to the MAC address filter

- ❑ *Example:*

```
Command> add mac filter aaa 00-4f-62-24-12-34
/etc/wlan/ap_service: 17: uname: not found
killall: wpa_supplicant: no process killed
/etc/wlan/ap_service: 17: uname: not found
Using /lib/modules/2.4.25-LSDK-5.1.0.42/wlan/ath_hal.o
Using /lib/modules/2.4.25-LSDK-5.1.0.42/wlan/ath_rate_atheros.o
Using /lib/modules/2.4.25-LSDK-5.1.0.42/wlan/ath_dfs.o
Using /lib/modules/2.4.25-LSDK-5.1.0.42/wlan/ath_ahb.o
<mapping sub-ioctl turbo to cmd 0x8BE0-1>
<mapping sub-ioctl set_installmode to cmd 0x8BE0-75>
<mapping sub-ioctl set_threslower to cmd 0x8BE0-76>
<mapping sub-ioctl set_threslow to cmd 0x8BE0-77>
<mapping sub-ioctl set_thresbetter to cmd 0x8BE0-78>
<mapping sub-ioctl set_thresbest to cmd 0x8BE0-79>
<mapping sub-ioctl maccmd to cmd 0x8BE0-17>
<mapping sub-ioctl authmode to cmd 0x8BE0-3>
<mapping sub-ioctl cwmin to cmd 0x8BE3-1>
<mapping sub-ioctl cwmax to cmd 0x8BE3-2>
RTNETLINK answers: No such file or directory
RTNETLINK answers: No such file or directory
mac filter aaa(00-4F-62-24-12-34) is added
```

- ■ **delete mac filter < Mnemonics Name>**
- ❑ *Purpose:* to delete a mac filter entry
- ❑ *Example:*

```
Command> delete mac filter aaa
/etc/wlan/ap_service: 17: uname: not found
killall: wpa_supplicant: no process killed
/etc/wlan/ap_service: 17: uname: not found
Using /lib/modules/2.4.25-LSDK-5.1.0.42/wlan/ath_hal.o
Using /lib/modules/2.4.25-LSDK-5.1.0.42/wlan/ath_rate_atheros.o
Using /lib/modules/2.4.25-LSDK-5.1.0.42/wlan/ath_dfs.o
Using /lib/modules/2.4.25-LSDK-5.1.0.42/wlan/ath_ahb.o
<mapping sub-ioctl turbo to cmd 0x8BE0-1>
<mapping sub-ioctl set_installmode to cmd 0x8BE0-75>
<mapping sub-ioctl set_threslower to cmd 0x8BE0-76>
<mapping sub-ioctl set_threslow to cmd 0x8BE0-77>
<mapping sub-ioctl set_thresbetter to cmd 0x8BE0-78>
<mapping sub-ioctl set_thresbest to cmd 0x8BE0-79>
<mapping sub-ioctl maccmd to cmd 0x8BE0-17>
<mapping sub-ioctl authmode to cmd 0x8BE0-3>
<mapping sub-ioctl cwmin to cmd 0x8BE3-1>
<mapping sub-ioctl cwmax to cmd 0x8BE3-2>
RTNETLINK answers: No such file or directory
RTNETLINK answers: No such file or directory
mac filter aaa is deleted
```

■ **delete wds <comment>**

❑ *Purpose:* To delete a WDS link

❑ *Example:*

```
Command> delete wds bridge
delete wds <comment> successful!
```

■ **add radius server primary**

❑ *Purpose:* to add a primary radius server

❑ *Example:*

```
Command> add radius server primary
enter server IP:
192.168.1.100
enter port number (1~65535):
655
enter shared secret:
123
enable server (yes/no):
```

```
yes
/etc/wlan/ap_service: 17: uname: not found
killall: wpa_supplicant: no process killed
/etc/wlan/ap_service: 17: uname: not found
Using /lib/modules/2.4.25-LSDK-5.1.0.42/wlan/ath_hal.o
Using /lib/modules/2.4.25-LSDK-5.1.0.42/wlan/ath_rate_atheros.o
Using /lib/modules/2.4.25-LSDK-5.1.0.42/wlan/ath_dfs.o
Using /lib/modules/2.4.25-LSDK-5.1.0.42/wlan/ath_ahb.o
<mapping sub-ioctl turbo to cmd 0x8BE0-1>
<mapping sub-ioctl set_installmode to cmd 0x8BE0-75>
<mapping sub-ioctl set_threslower to cmd 0x8BE0-76>
<mapping sub-ioctl set_threslow to cmd 0x8BE0-77>
<mapping sub-ioctl set_thresbetter to cmd 0x8BE0-78>
<mapping sub-ioctl set_thresbest to cmd 0x8BE0-79>
<mapping sub-ioctl maccmd to cmd 0x8BE0-17>
<mapping sub-ioctl authmode to cmd 0x8BE0-3>
<mapping sub-ioctl cwmin to cmd 0x8BE3-1>
<mapping sub-ioctl cwmax to cmd 0x8BE3-2>
RTNETLINK answers: No such file or directory
RTNETLINK answers: No such file or directory
add radius server primary successfully
```

■ **add radius server <primary | secondary>**

❑ *Purpose:* to add a primary or secondary radius server

❑ *Example:*

```
Command> add radius server secondary
enter server IP:
192.168.1.200
enter port number (1~65535):
766
enter shared secret:
234
enable server (yes/no):
```

```
yes
/etc/wlan/ap_service: 17: uname: not found
killall: wpa_supplicant: no process killed
/etc/wlan/ap_service: 17: uname: not found
Using /lib/modules/2.4.25-LSDK-5.1.0.42/wlan/ath_hal.o
Using /lib/modules/2.4.25-LSDK-5.1.0.42/wlan/ath_rate_atheros.o
Using /lib/modules/2.4.25-LSDK-5.1.0.42/wlan/ath_dfs.o
Using /lib/modules/2.4.25-LSDK-5.1.0.42/wlan/ath_ahb.o
<mapping sub-ioctl turbo to cmd 0x8BE0-1>
<mapping sub-ioctl set_installmode to cmd 0x8BE0-75>
<mapping sub-ioctl set_threslower to cmd 0x8BE0-76>
<mapping sub-ioctl set_threslow to cmd 0x8BE0-77>
<mapping sub-ioctl set_thresbetter to cmd 0x8BE0-78>
<mapping sub-ioctl set_thresbest to cmd 0x8BE0-79>
<mapping sub-ioctl maccmd to cmd 0x8BE0-17>
<mapping sub-ioctl authmode to cmd 0x8BE0-3>
<mapping sub-ioctl cwmin to cmd 0x8BE3-1>
<mapping sub-ioctl cwmax to cmd 0x8BE3-2>
RTNETLINK answers: No such file or directory
RTNETLINK answers: No such file or directory
add radius server secondary successfully
```

■ **add wds <comment> <mac>**

❑ *Purpose:* to add a WDS Link

❑ *Example:*

```
Command> add wds bridge 00-4f-60-52-12-34
add wds <comment> <mac> successful!
```

■ **add ssid <ssid name> broadcast <enable | disable>**

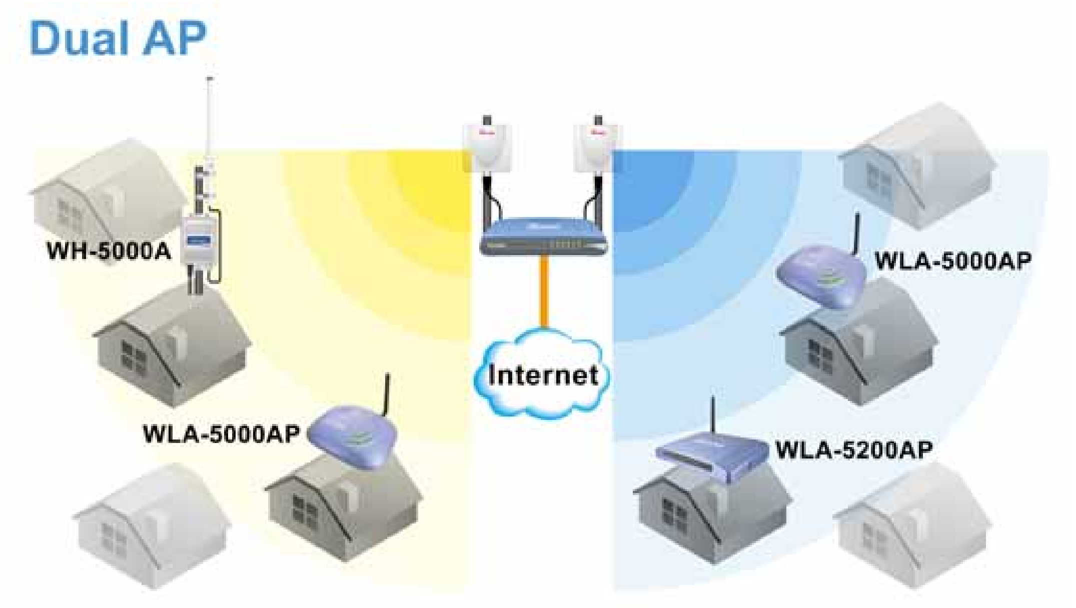
❑ *Purpose:* to add a new ssid (AP and AP Router mode) to the multiple SSID list.

❑ *Example:*

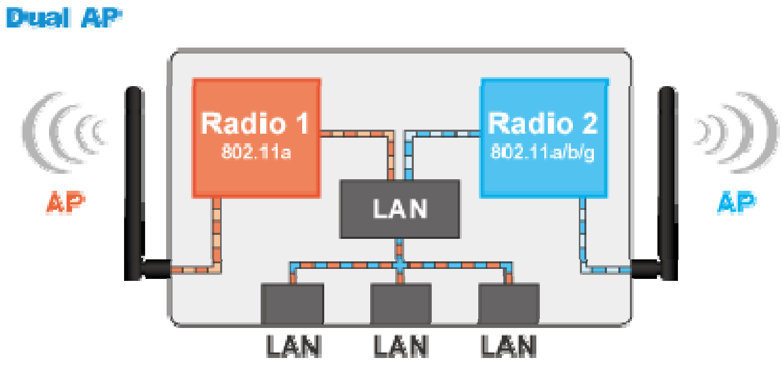
```
Command> add ssid air03 broadcast enable
Add R1 ssid <air03> broadcast enable successful!
```

7 Application Example: Dual AP Mode

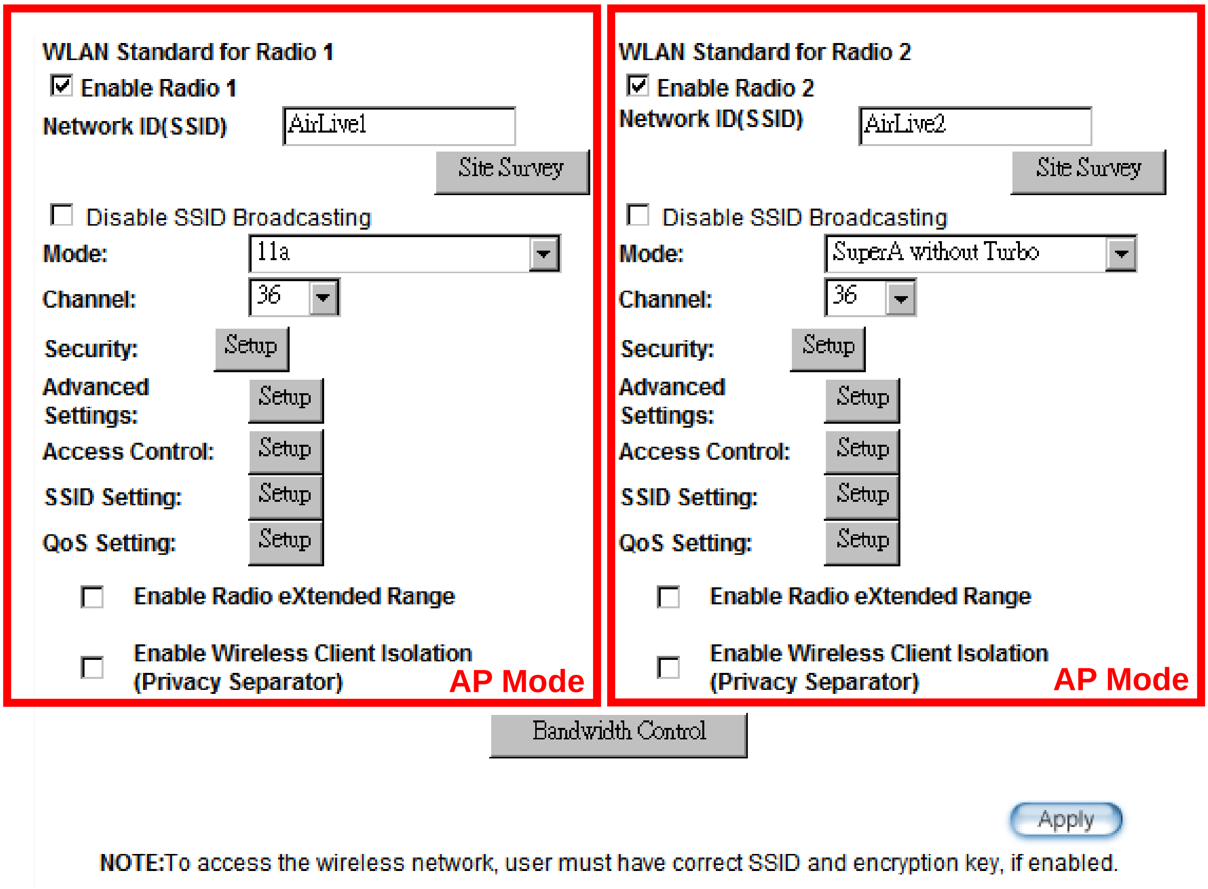
In Dual AP mode, both wireless interface of WLA-9000AP are set as AP and provide hotspot service on each interface.



- This Application provides wider coverage that difficult to be reached with a unique Omni antenna by using another adequate antenna such as sector antenna. It's particularly suitable for WISP to provide stable and high performance link.
- The image in Dual AP mode UI helps to indicate data flow related to the Wireless and the Ethernet ports.



Both Radios has its own setting interface.



WLAN Standard for Radio 1

☑ Enable Radio 1

Network ID(SSID) AirLive1

Site Survey

☐ Disable SSID Broadcasting

Mode: 11a

Channel: 36

Security: Setup

Advanced Settings: Setup

Access Control: Setup

SSID Setting: Setup

QoS Setting: Setup

☐ Enable Radio eXtended Range

☐ Enable Wireless Client Isolation (Privacy Separator)

AP Mode

WLAN Standard for Radio 2

☑ Enable Radio 2

Network ID(SSID) AirLive2

Site Survey

☐ Disable SSID Broadcasting

Mode: SuperA without Turbo

Channel: 36

Security: Setup

Advanced Settings: Setup

Access Control: Setup

SSID Setting: Setup

QoS Setting: Setup

☐ Enable Radio eXtended Range

☐ Enable Wireless Client Isolation (Privacy Separator)

AP Mode

Bandwidth Control

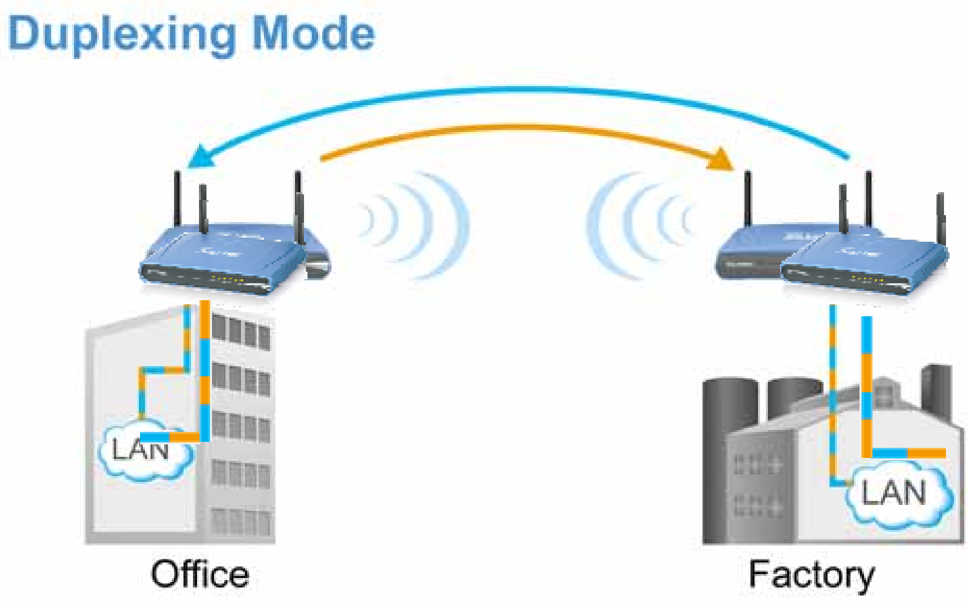
Apply

NOTE:To access the wireless network, user must have correct SSID and encryption key, if enabled.

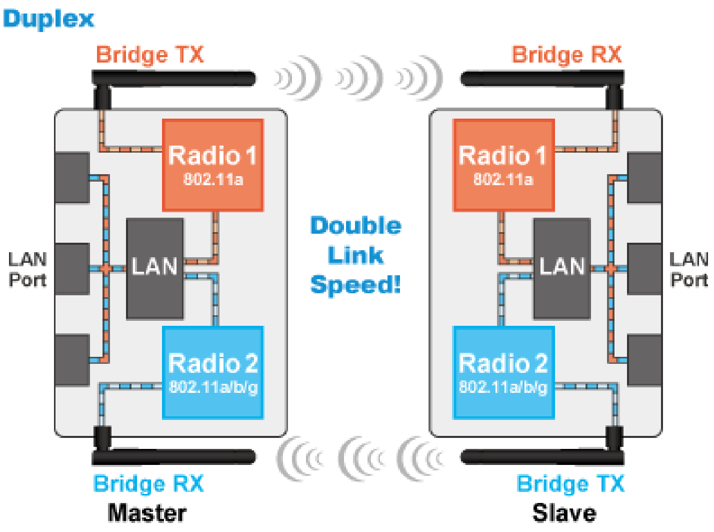
To configure the AP mode, please refer to Section 4.3 Access Point Settings.

8 Application Example: Duplex Mode

The duplex mode groups the two radios to double the bandwidth between two WLA-9000APs.



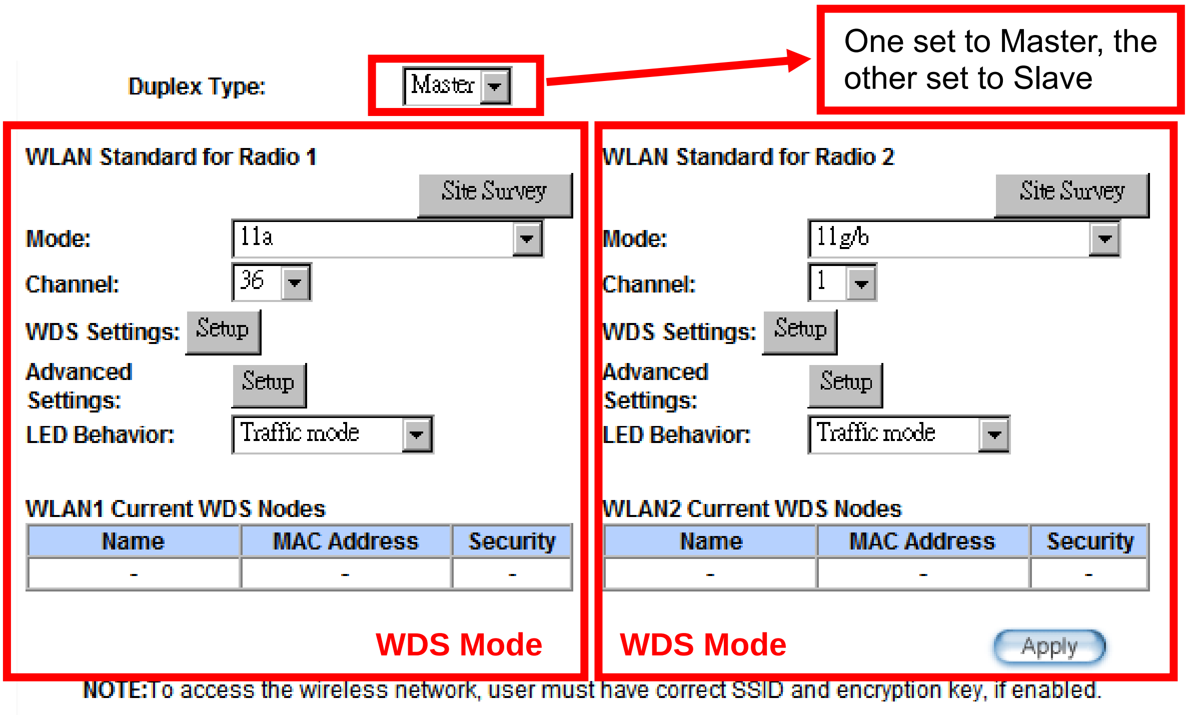
- This Application provides higher bandwidth between two locations than single radio does. When clients transmitting data which over the loading of single radio, the other radio shares the loading and make it able to transmit more data between the two WLA-9000AP.



- The image in Duplex mode UI helps to indicate data flow related to the Wireless and the Ethernet ports.

Both radios are using WDS mode for communication.

One WLA-9000AP is configured as a Master where as the other WLA-9000AP is configure to be a Slave.



One set to Master, the other set to Slave

Duplex Type: Master

WLAN Standard for Radio 1

Mode: 11a

Channel: 36

WDS Settings: Setup

Advanced Settings: Setup

LED Behavior: Traffic mode

WLAN1 Current WDS Nodes

Name	MAC Address	Security
-	-	-

WDS Mode

WLAN Standard for Radio 2

Mode: 11g/b

Channel: 1

WDS Settings: Setup

Advanced Settings: Setup

LED Behavior: Traffic mode

WLAN2 Current WDS Nodes

Name	MAC Address	Security
-	-	-

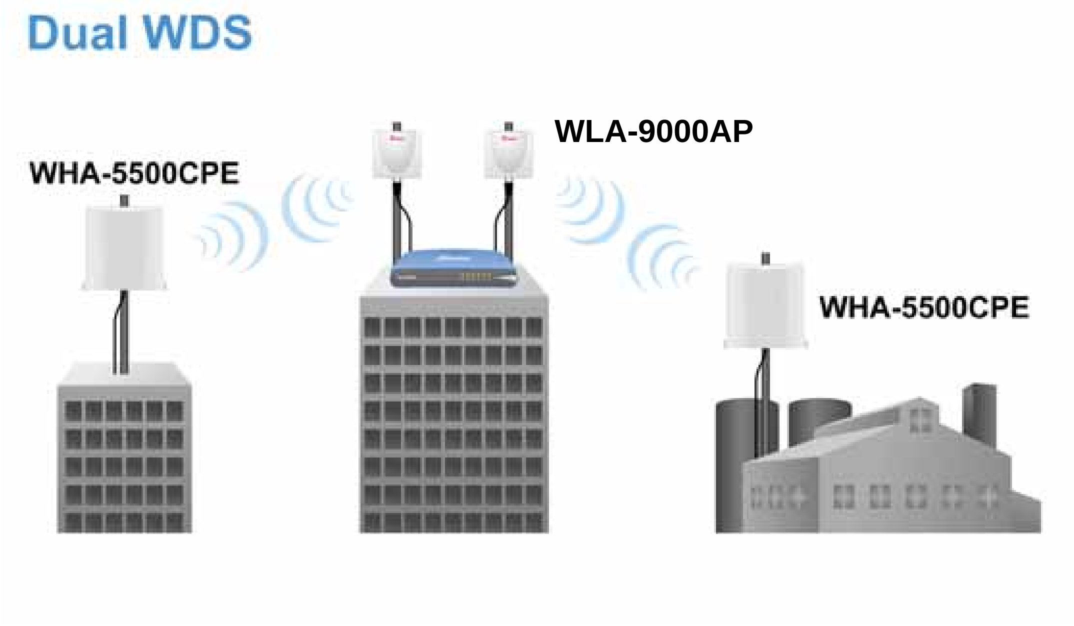
WDS Mode

NOTE:To access the wireless network, user must have correct SSID and encryption key, if enabled.

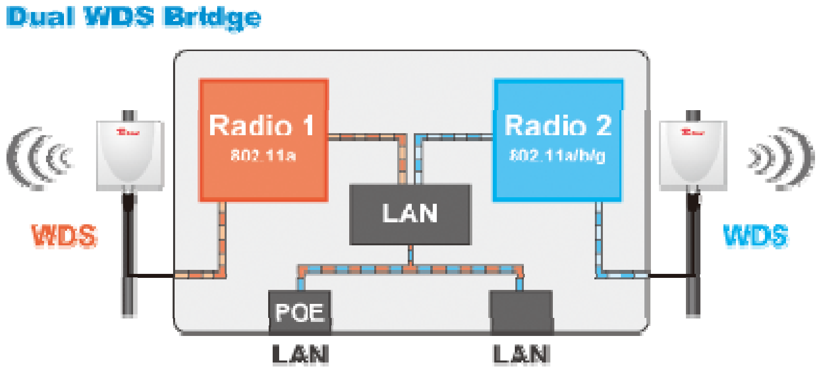
To configure the WDS mode, please refer to section 4.4 WDS Bridge Settings.

9 Application Example: Dual WDS Bridge Mode

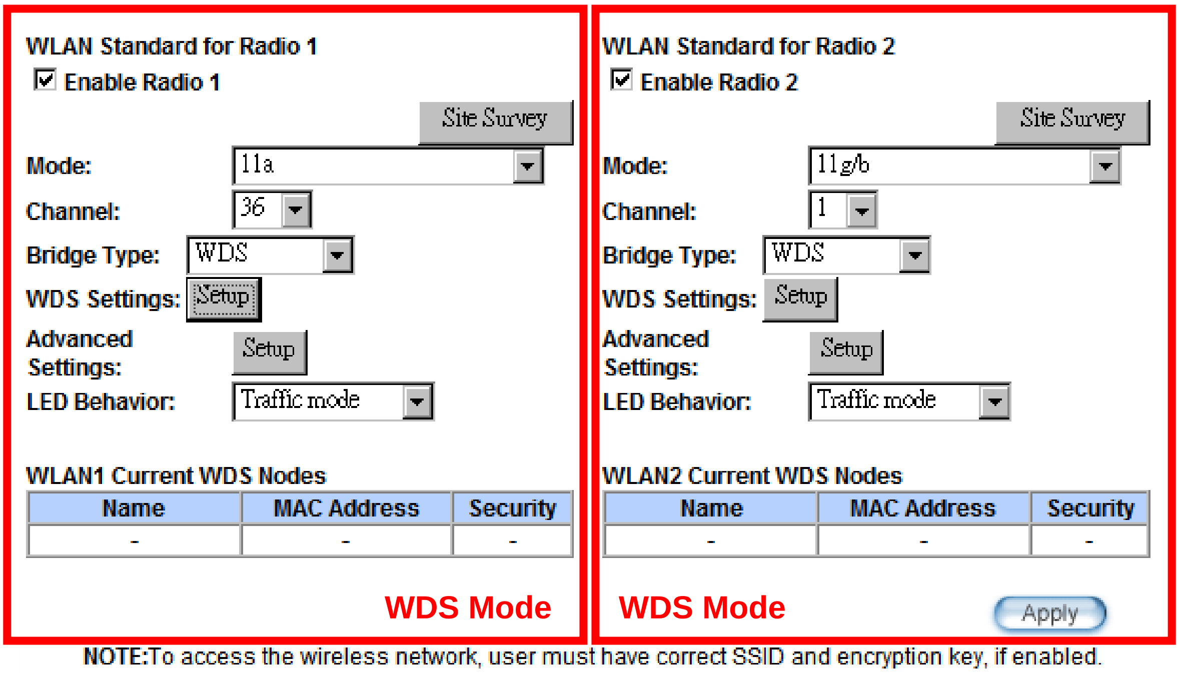
In Dual WDS Bridge mode, both wireless interface of WLA-9000AP are set as WDS Bridge and connect to remote network. When configured in the Dual WDS Bridge mode, WLA-9000AP allows solving discontinuous link due to geographical obstacles, shown as below and extension of distance between two WDS bridge nodes separated by a building.



- In this mode, the AP can act as a signal repeating station in a wireless backbone network. In addition, it can also function as directing station for NLOS application.
- The image in Duplex WDS Bridge mode UI helps to indicate data flow related to the Wireless and the Ethernet ports.



Both radios are using WDS mode for communication.



WLAN Standard for Radio 1

☑ Enable Radio 1

Mode: 11a

Channel: 36

Bridge Type: WDS

WDS Settings: Setup

Advanced Settings: Setup

LED Behavior: Traffic mode

WLAN1 Current WDS Nodes

Name	MAC Address	Security
-	-	-

WLAN Standard for Radio 2

☑ Enable Radio 2

Mode: 11g/b

Channel: 1

Bridge Type: WDS

WDS Settings: Setup

Advanced Settings: Setup

LED Behavior: Traffic mode

WLAN2 Current WDS Nodes

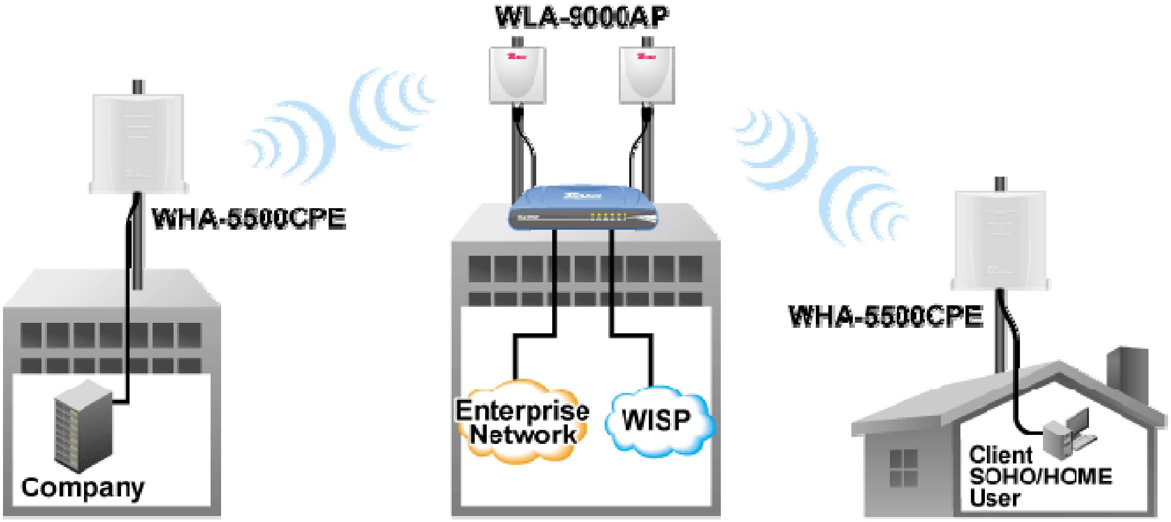
Name	MAC Address	Security
-	-	-

NOTE:To access the wireless network, user must have correct SSID and encryption key, if enabled.

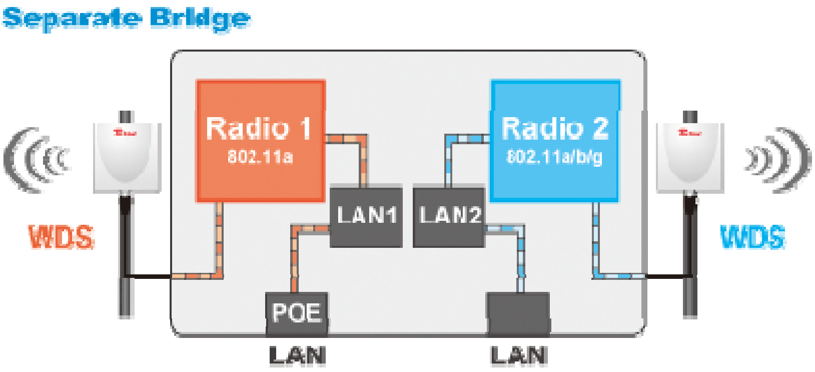
To configure the WDS mode, please refer to section 4.4 WDS Settings.

10 Application Example: Separate Bridge Mode

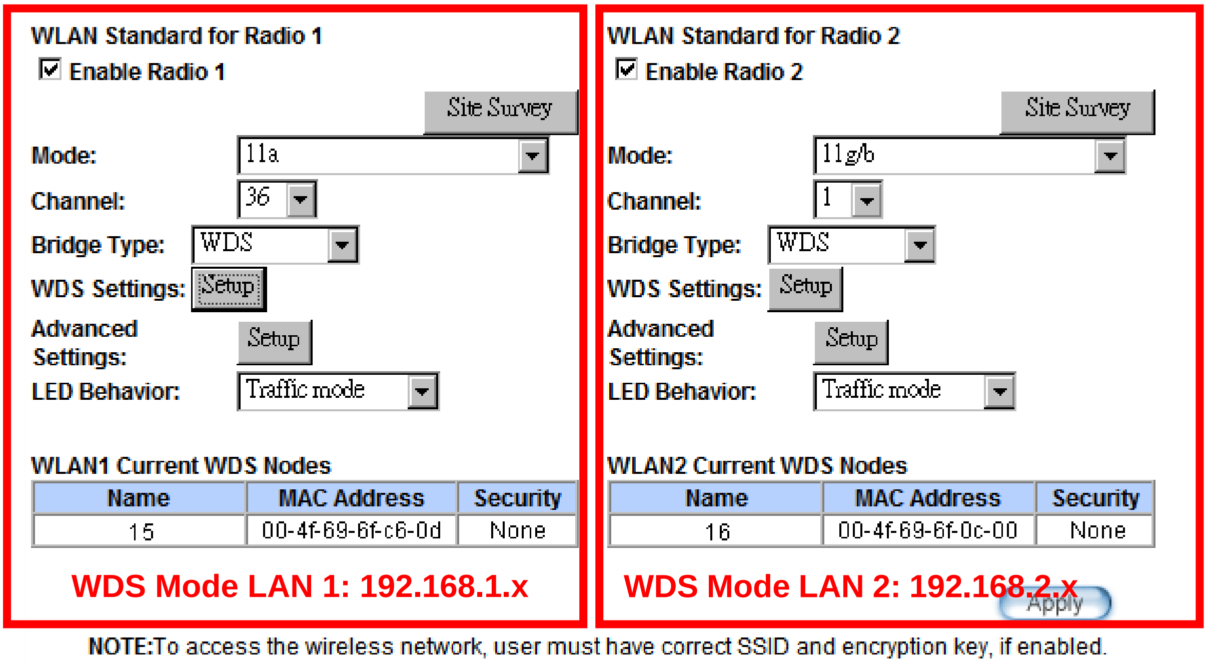
The Separate Bridge separates the device into 2 IP segments. Radio 1 and LAN 3 are in IP segment of 192.168.1.x/24 and Radio 2 and LAN1, LAN2 are in IP segment of 192.168.2.x. Devices in one IP segment can not communicate to devices in the other IP segment.



- In this application, both Radio 1 and Radio 2 are in WDS Bridge Mode.
- The image in Separate WDS Bridge mode UI helps to indicate data flow related to the Wireless and the Ethernet ports.



Both radios are using WDS mode for communication.



WLAN Standard for Radio 1

☑ Enable Radio 1

Site Survey

Mode: 11a

Channel: 36

Bridge Type: WDS

WDS Settings: Setup

Advanced Settings: Setup

LED Behavior: Traffic mode

WLAN1 Current WDS Nodes

Name	MAC Address	Security
15	00-4f-69-6f-c6-0d	None

WDS Mode LAN 1: 192.168.1.x

WLAN Standard for Radio 2

☑ Enable Radio 2

Site Survey

Mode: 11g/b

Channel: 1

Bridge Type: WDS

WDS Settings: Setup

Advanced Settings: Setup

LED Behavior: Traffic mode

WLAN2 Current WDS Nodes

Name	MAC Address	Security
16	00-4f-69-6f-0c-00	None

WDS Mode LAN 2: 192.168.2.x

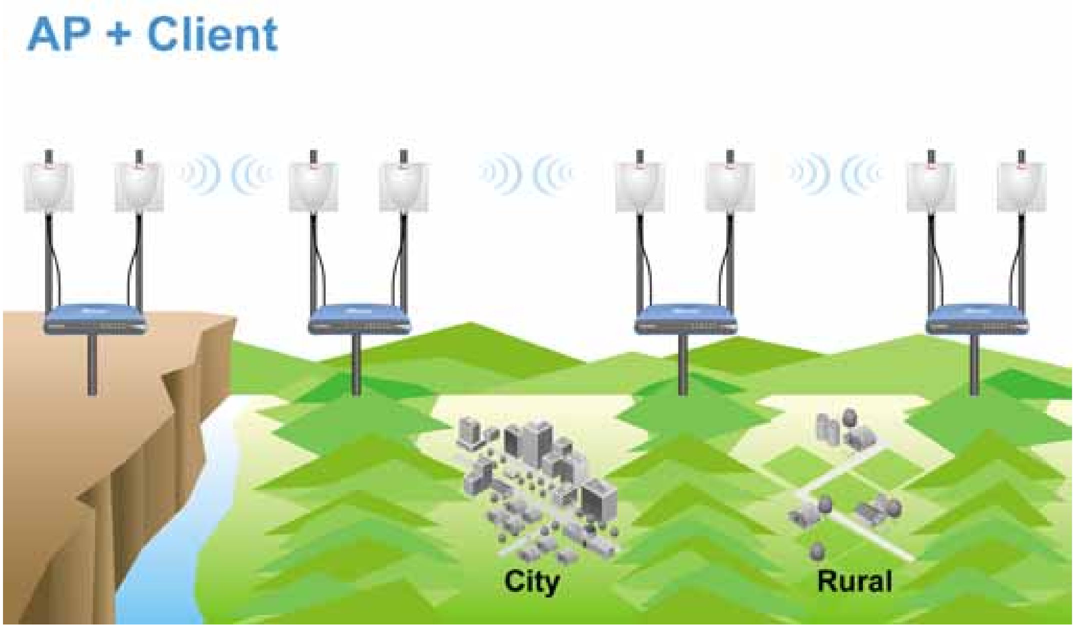
Apply

NOTE: To access the wireless network, user must have correct SSID and encryption key, if enabled.

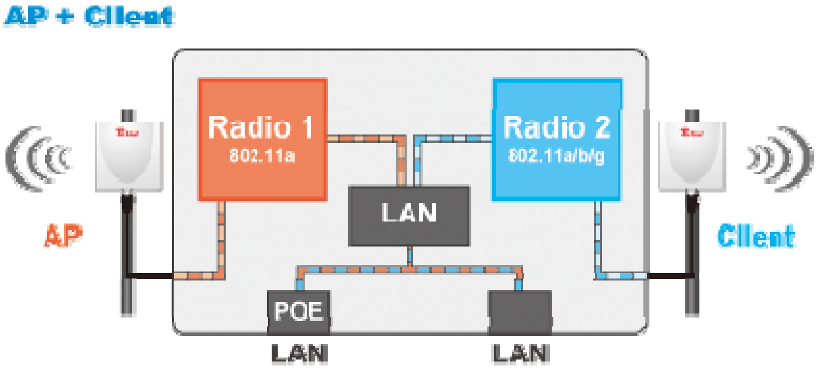
To configure the WDS mode, please refer to Section 4.4 WDS Settings.

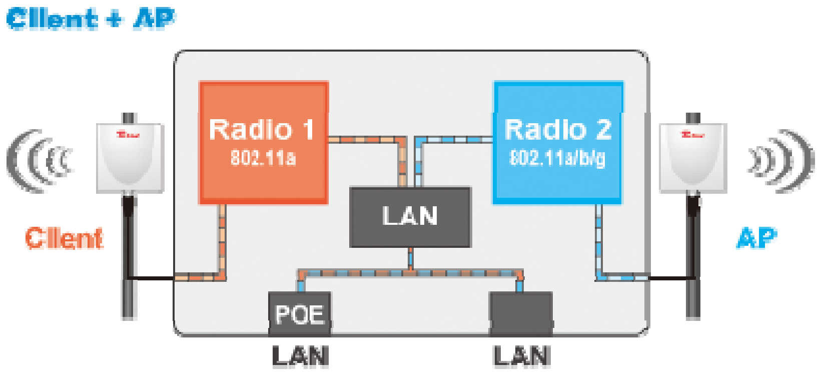
11 Application Example: AP + Client / Client + AP Mode

In this mode, one station works as an intermediate station. This enable the AP to link with remote stations using client mode, then distribute the signal to other clients using AP mode.

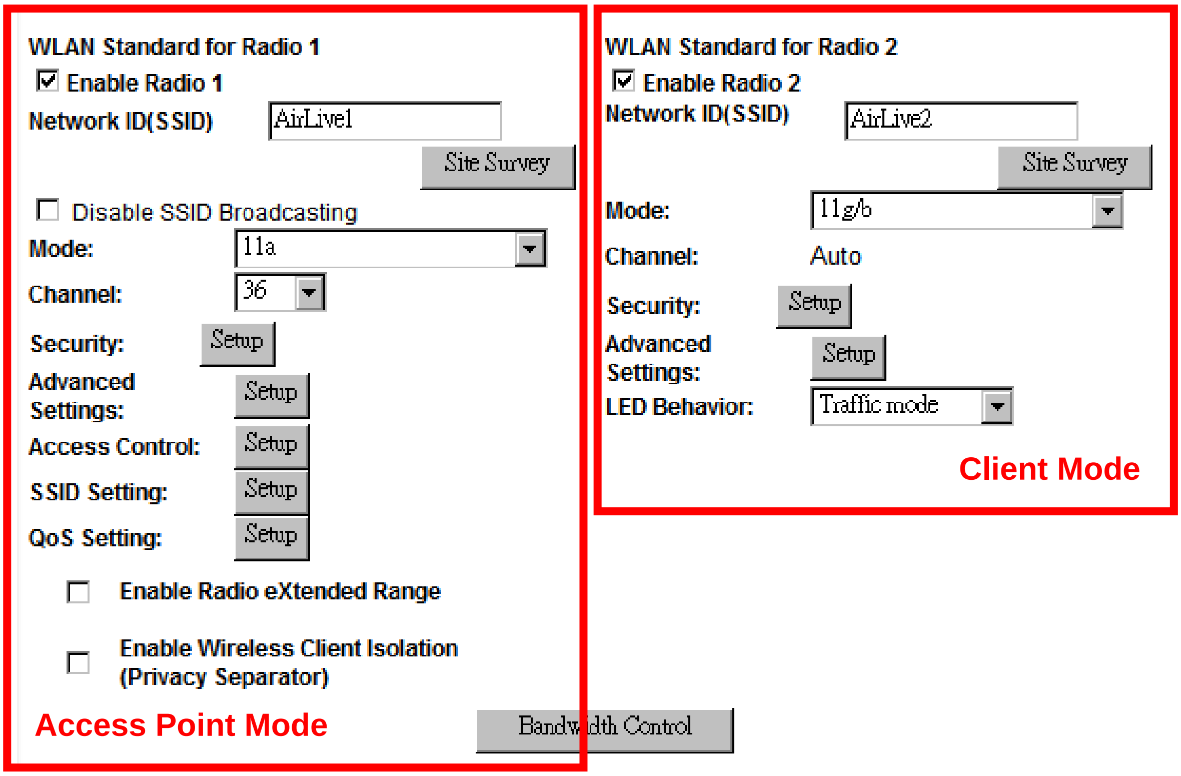


- In this application, Either Radio 1 or Radio 2 is in AP Mode, the other Radio is in Client mode.
- The image in AP + Client / Client + AP mode UI helps to indicate data flow related to the Wireless and the Ethernet ports.





The UI example of AP + Client is as following:



WLAN Standard for Radio 1

☑ Enable Radio 1

Network ID(SSID) AirLive1

Site Survey

☐ Disable SSID Broadcasting

Mode: 11a

Channel: 36

Security: Setup

Advanced Settings: Setup

Access Control: Setup

SSID Setting: Setup

QoS Setting: Setup

☐ Enable Radio eXtended Range

☐ Enable Wireless Client Isolation (Privacy Separator)

Access Point Mode

Bandwidth Control

WLAN Standard for Radio 2

☑ Enable Radio 2

Network ID(SSID) AirLive2

Site Survey

Mode: 11g/b

Channel: Auto

Security: Setup

Advanced Settings: Setup

LED Behavior: Traffic mode

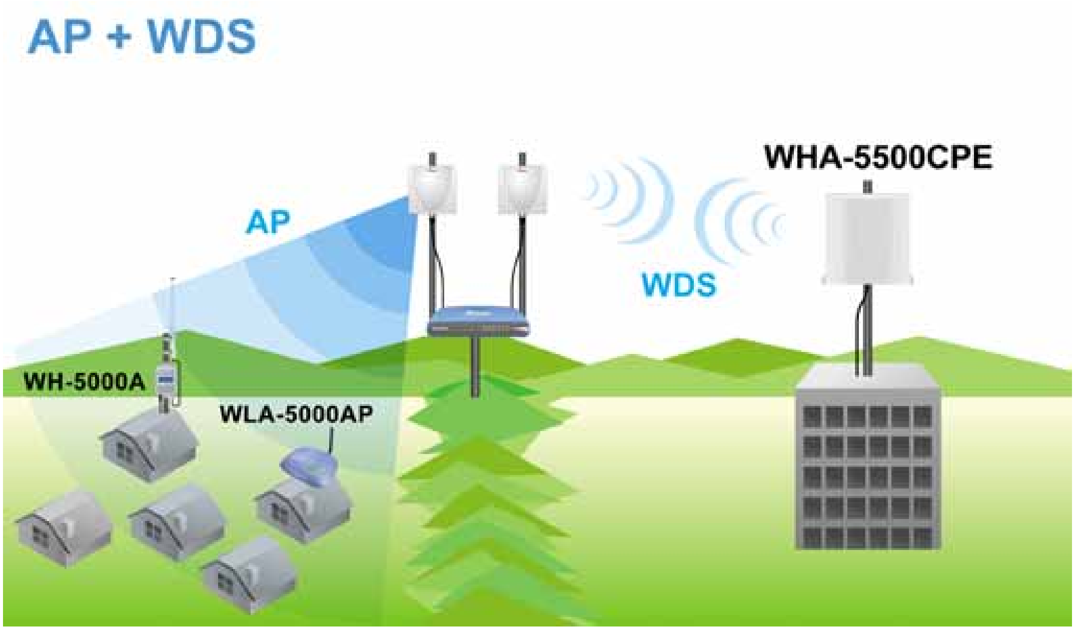
Client Mode

To configure the AP mode, please refer to Section 4.3 Access Point Settings.

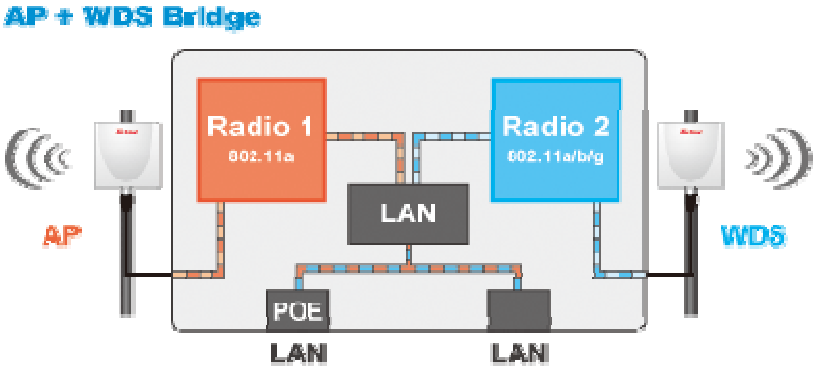
To configure the Client mode, please refer to Section 4.5 Client Settings.

12 Application Example: AP + WDS Bridge / WDS Bridge + AP Mode

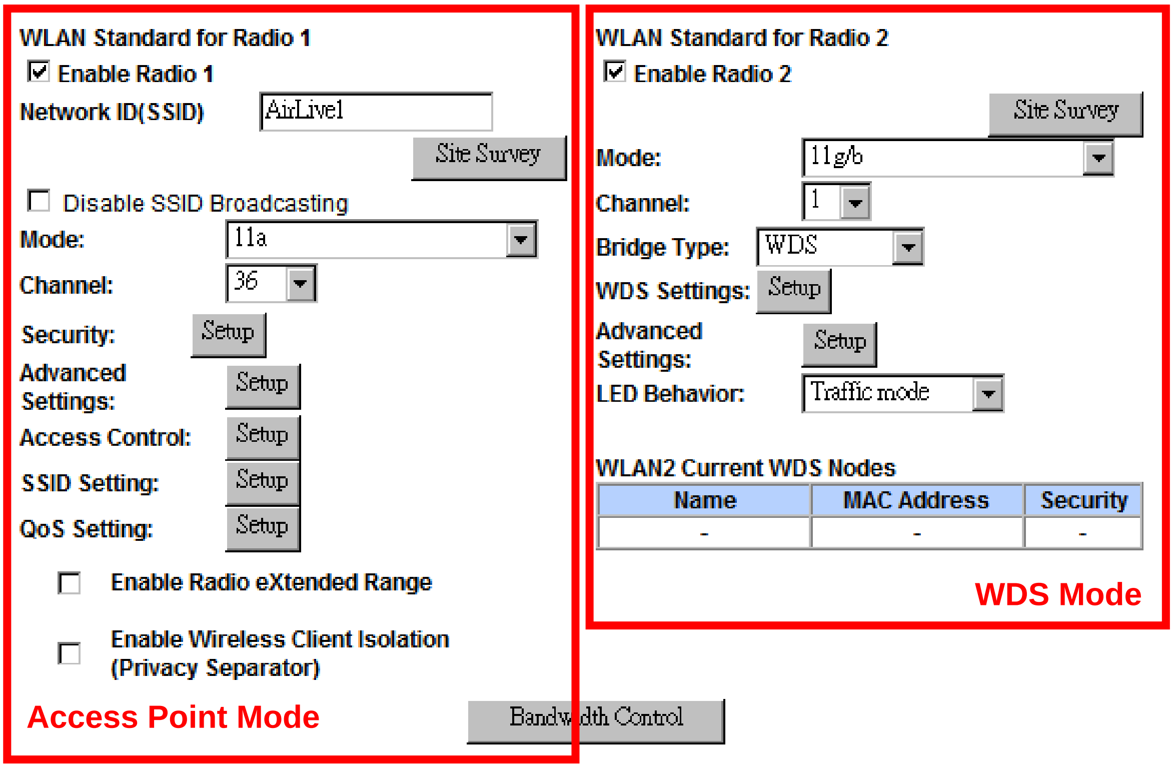
In this mode, one Radio is in Access Point mode and the other in WDS Bridge Mode.



- In this mode, the AP can act as a signal repeating station in a wireless backbone network. In addition, it can also function as directing station for NLOS application.
- The image in AP + WDS Bridge / WDS Bridge + AP mode UI helps to indicate data flow related to the Wireless and the Ethernet ports.



The UI example of AP + WDS Bridge is as following:



WLAN Standard for Radio 1

☑ Enable Radio 1

Network ID(SSID): AirLive1

Site Survey

☐ Disable SSID Broadcasting

Mode: 11a

Channel: 36

Security: Setup

Advanced Settings: Setup

Access Control: Setup

SSID Setting: Setup

QoS Setting: Setup

☐ Enable Radio eXtended Range

☐ Enable Wireless Client Isolation (Privacy Separator)

Access Point Mode

Bandwidth Control

WLAN Standard for Radio 2

☑ Enable Radio 2

Site Survey

Mode: 11g/b

Channel: 1

Bridge Type: WDS

WDS Settings: Setup

Advanced Settings: Setup

LED Behavior: Traffic mode

WLAN2 Current WDS Nodes

Name	MAC Address	Security
-	-	-

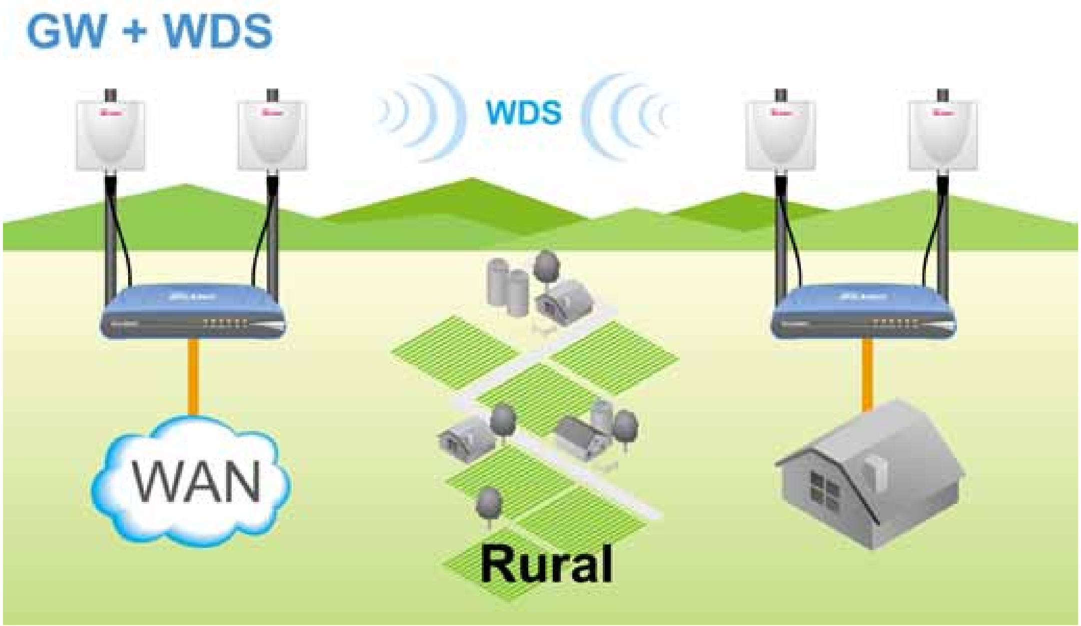
WDS Mode

To configure the AP mode, please refer to Section 4.3 Access Point Settings.

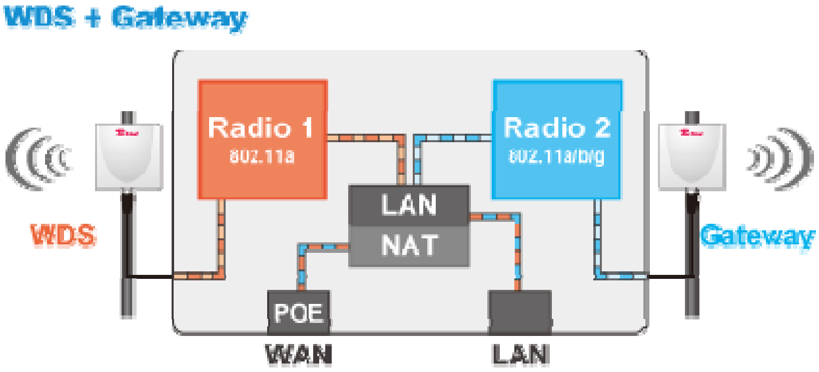
To configure the Client mode, please refer to Section 4.4 WDS Settings.

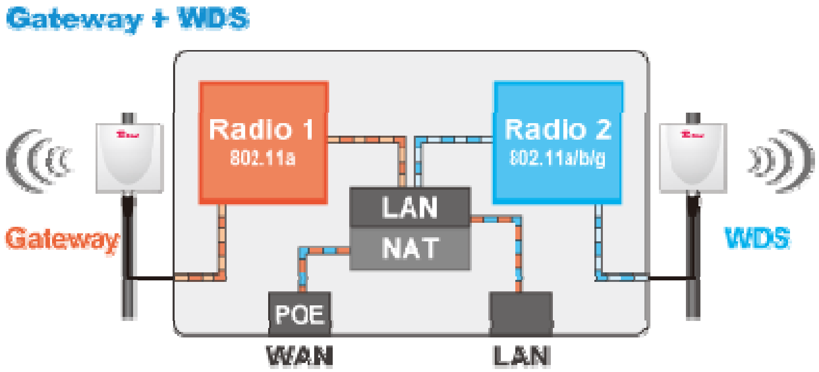
13 Application Example: WDS + Gateway / Gateway + WDS

In this mode, one radio acts as an AP router and the other a WDS bridge. One of the RJ-45 ports as the WAN interface to the internet.

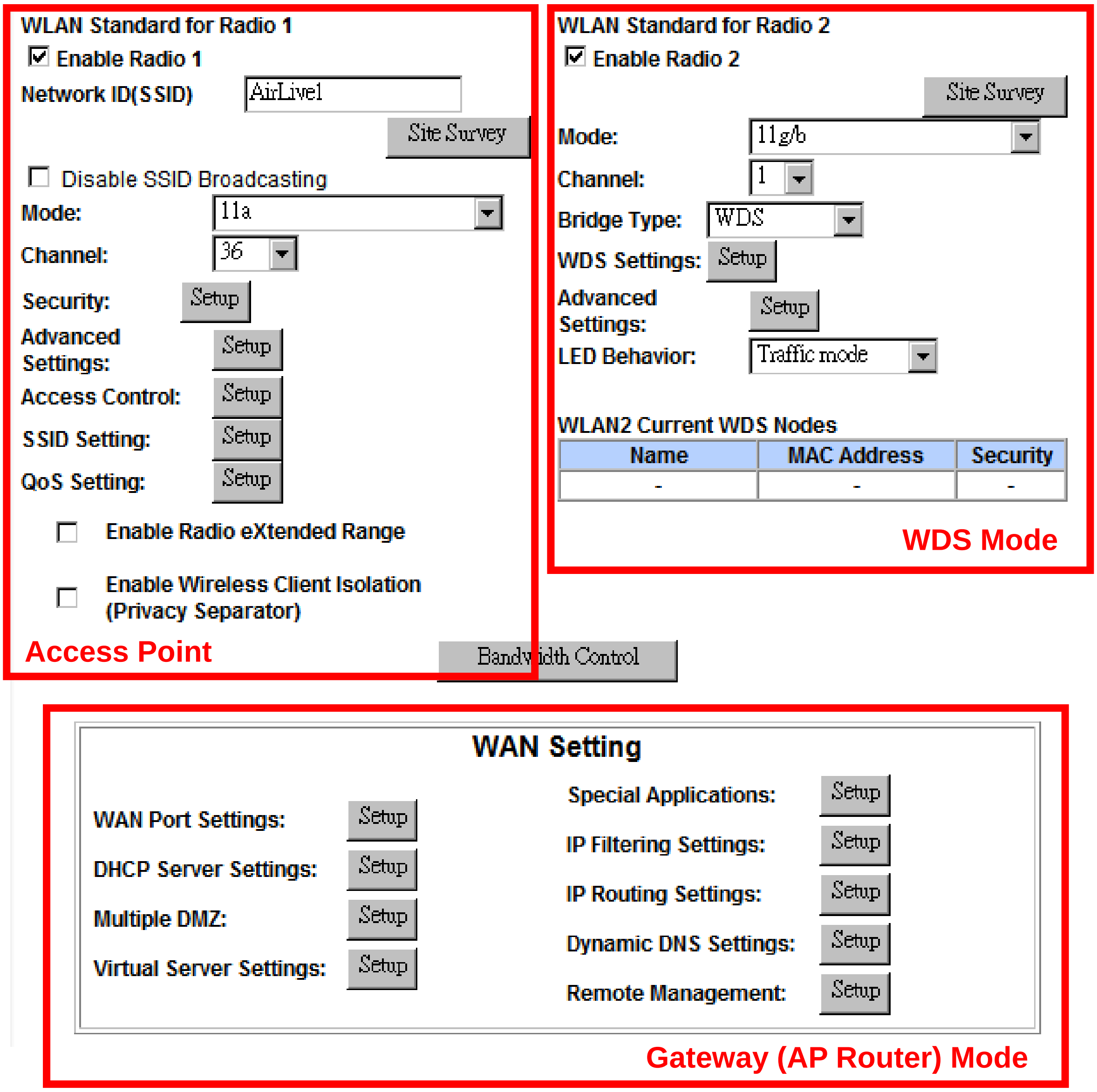


- The remote location can access the internet by way of this Access Point which acts as a gateway device of the network.
- The image in WDS + Gateway / Gateway + WDS mode UI helps to indicate data flow related to the Wireless and the Ethernet ports.





The UI example of Gateway + WDS is as following:



WLAN Standard for Radio 1

☑ Enable Radio 1

Network ID(SSID) AirLive1

Site Survey

☐ Disable SSID Broadcasting

Mode: 11a

Channel: 36

Security: Setup

Advanced Settings: Setup

Access Control: Setup

SSID Setting: Setup

QoS Setting: Setup

☐ Enable Radio eXtended Range

☐ Enable Wireless Client Isolation (Privacy Separator)

Access Point

Bandwidth Control

WLAN Standard for Radio 2

☑ Enable Radio 2

Site Survey

Mode: 11g/b

Channel: 1

Bridge Type: WDS

WDS Settings: Setup

Advanced Settings: Setup

LED Behavior: Traffic mode

WLAN2 Current WDS Nodes

Name	MAC Address	Security
-	-	-

WDS Mode

WAN Setting

WAN Port Settings: Setup

DHCP Server Settings: Setup

Multiple DMZ: Setup

Virtual Server Settings: Setup

Special Applications: Setup

IP Filtering Settings: Setup

IP Routing Settings: Setup

Dynamic DNS Settings: Setup

Remote Management: Setup

Gateway (AP Router) Mode

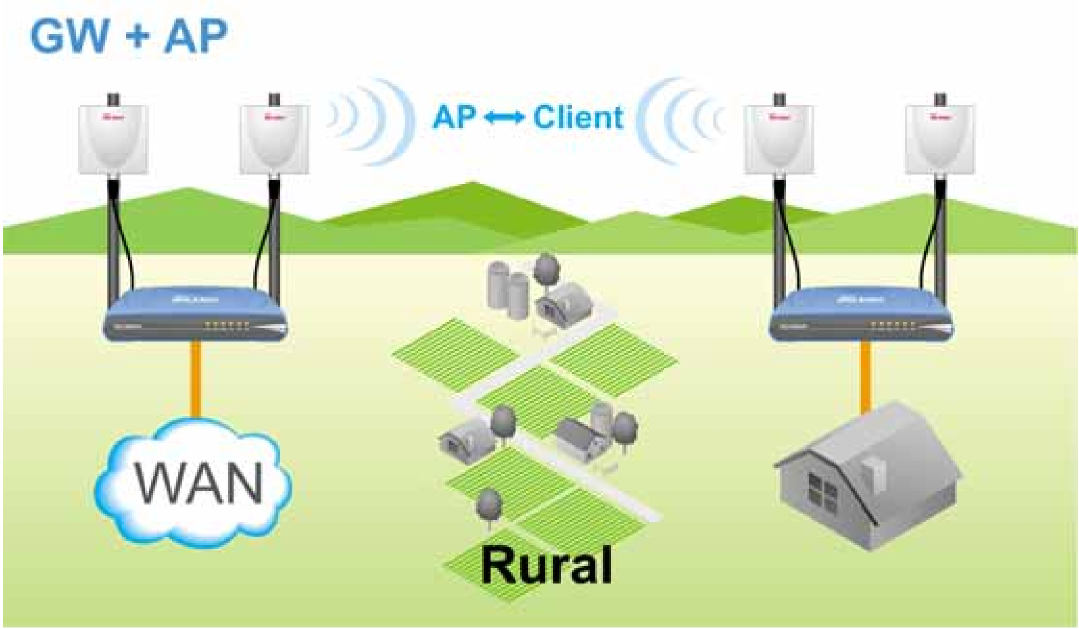
To configure the AP mode, please refer to Section 4.3 Access Point Settings.

To configure the WDS mode, please refer to Section 4.4 WDS Settings.

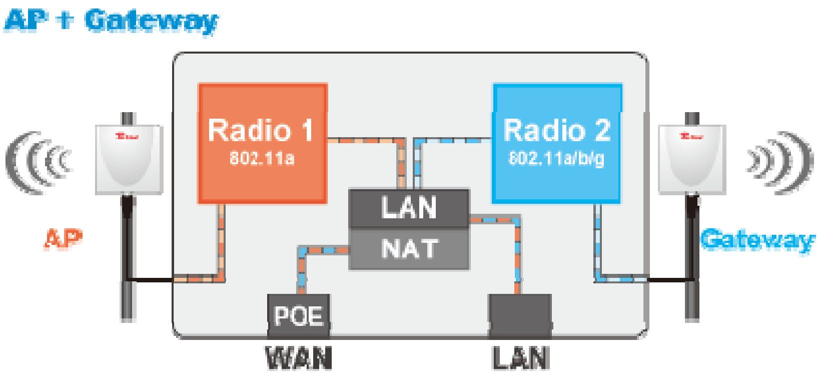
To configure the Gateway (Router) mode, please refer to Section 4.6 Gateway (AP Router) Settings.

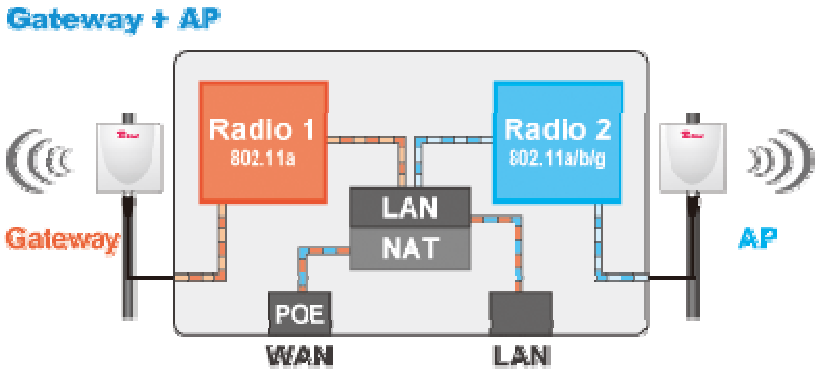
14 Application Example: AP + Gateway / Gateway + AP

In this mode, one radio acts as an AP router and the other an Access Point. One of the RJ-45 ports as the WAN interface to the internet.

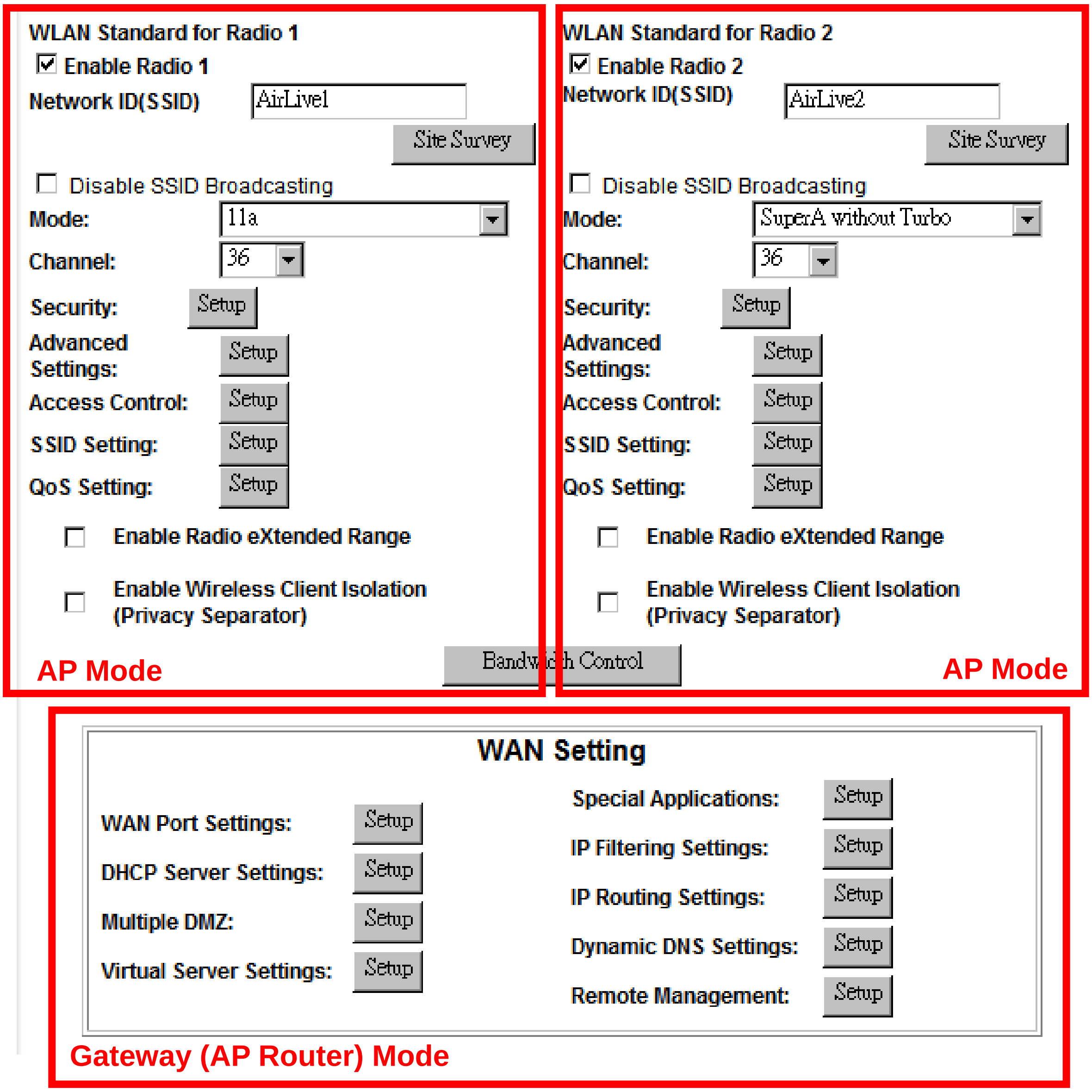


- The remote location can access the internet by way of this Access Point which acts as a gateway device of the network.
- The image in AP + Gateway / Gateway + AP mode UI helps to indicate data flow related to the Wireless and the Ethernet ports.





The UI example of Gateway + AP is as following:



WLAN Standard for Radio 1

☑ Enable Radio 1

Network ID(SSID): AirLive1 [Site Survey]

☐ Disable SSID Broadcasting

Mode: 11a

Channel: 36

Security: [Setup]

Advanced Settings: [Setup]

Access Control: [Setup]

SSID Setting: [Setup]

QoS Setting: [Setup]

☐ Enable Radio eXtended Range

☐ Enable Wireless Client Isolation (Privacy Separator)

AP Mode

WLAN Standard for Radio 2

☑ Enable Radio 2

Network ID(SSID): AirLive2 [Site Survey]

☐ Disable SSID Broadcasting

Mode: SuperA without Turbo

Channel: 36

Security: [Setup]

Advanced Settings: [Setup]

Access Control: [Setup]

SSID Setting: [Setup]

QoS Setting: [Setup]

☐ Enable Radio eXtended Range

☐ Enable Wireless Client Isolation (Privacy Separator)

AP Mode

[Bandwidth Control]

WAN Setting

WAN Port Settings: [Setup]

DHCP Server Settings: [Setup]

Multiple DMZ: [Setup]

Virtual Server Settings: [Setup]

Special Applications: [Setup]

IP Filtering Settings: [Setup]

IP Routing Settings: [Setup]

Dynamic DNS Settings: [Setup]

Remote Management: [Setup]

Gateway (AP Router) Mode

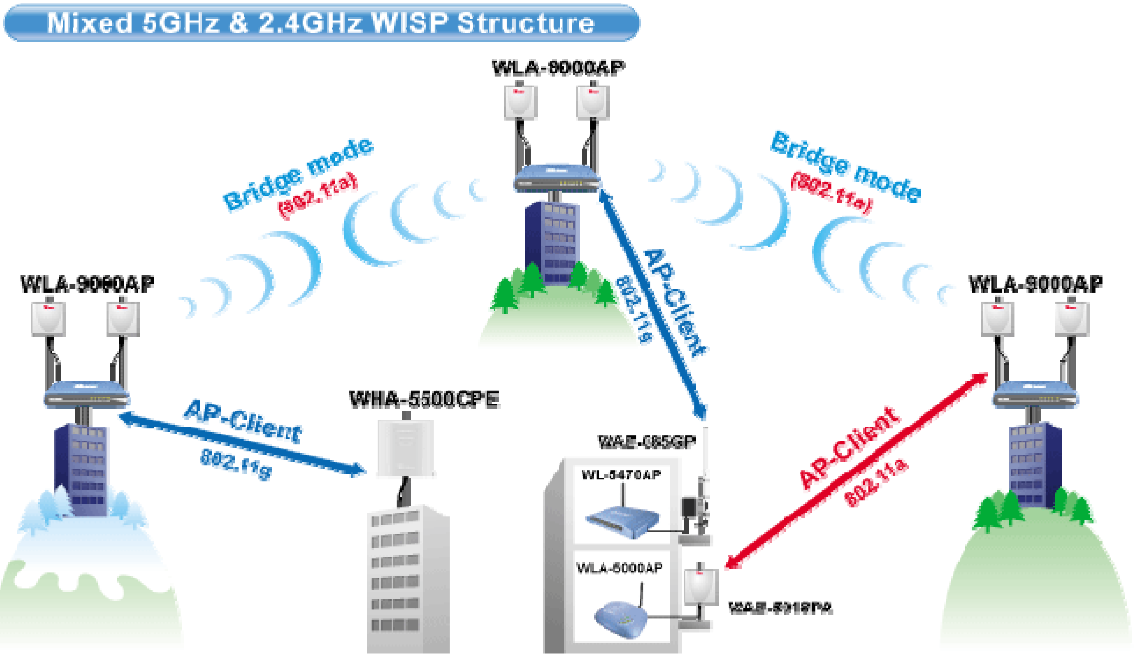
To configure the AP mode, Please refer to Section 4.3 Access Point Setting.

To configure the WDS mode, Please refer to Section 4.4 WDS Setting.

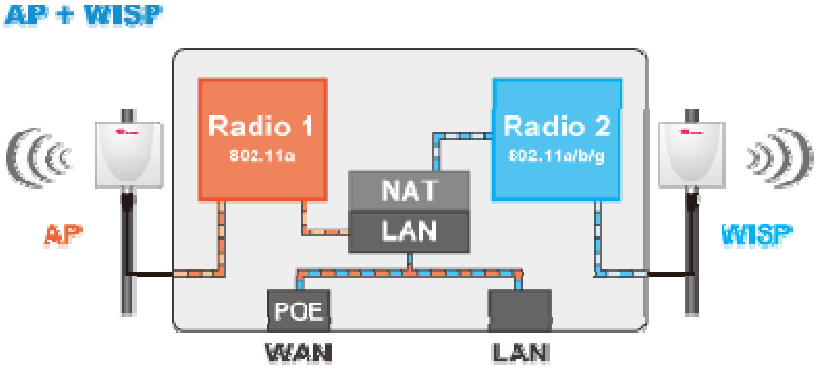
To configure the Gateway (AP Router) mode, Please refer to Section 4.6 Gateway (AP Router) Settings.

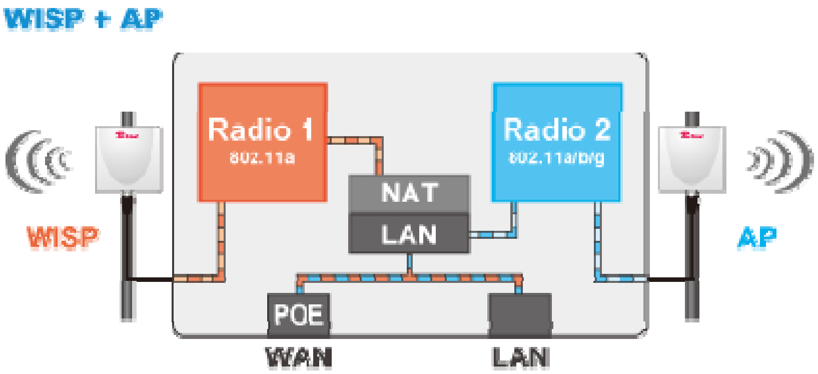
15 Application Example: AP + WISP / WISP + AP

In this mode, one radio acts as an AP and the other acts as a client router. One of the RJ-45 ports as the WAN interface to the internet.

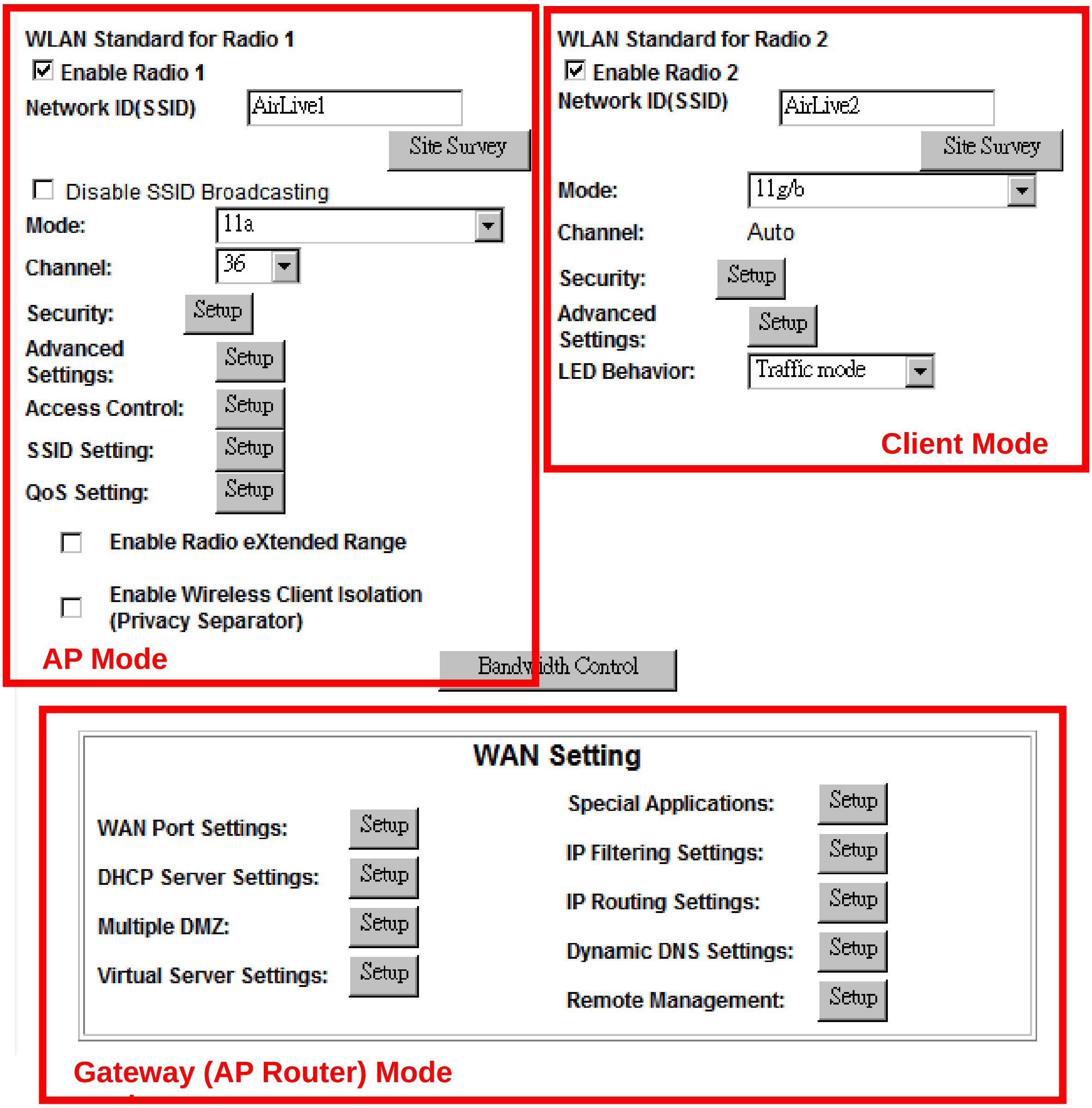


- The remote location can access the internet by way of this Access Point which acts as a gateway device of the network.
- The image in AP + WISP / WISP + AP mode UI helps to indicate data flow related to the Wireless and the Ethernet ports.





The UI example of AP + WISP is as following:



WLAN Standard for Radio 1

☑ Enable Radio 1

Network ID(SSID) AirLive1

[Site Survey]

☐ Disable SSID Broadcasting

Mode: 11a

Channel: 36

Security: [Setup]

Advanced Settings: [Setup]

Access Control: [Setup]

SSID Setting: [Setup]

QoS Setting: [Setup]

☐ Enable Radio eXtended Range

☐ Enable Wireless Client Isolation (Privacy Separator)

AP Mode

[Bandwidth Control]

WLAN Standard for Radio 2

☑ Enable Radio 2

Network ID(SSID) AirLive2

[Site Survey]

Mode: 11g/b

Channel: Auto

Security: [Setup]

Advanced Settings: [Setup]

LED Behavior: Traffic mode

Client Mode

WAN Setting

WAN Port Settings: [Setup]

DHCP Server Settings: [Setup]

Multiple DMZ: [Setup]

Virtual Server Settings: [Setup]

Special Applications: [Setup]

IP Filtering Settings: [Setup]

IP Routing Settings: [Setup]

Dynamic DNS Settings: [Setup]

Remote Management: [Setup]

Gateway (AP Router) Mode

To configure the AP mode, Please refer to Section 4.3 Access Point Settings.

To configure the WDS mode, Please refer to Section 4.5 Client Settings.

To configure the Gateway (Router) mode, Please refer to Section 4.6 Gateway (AP Router) Settings.

16 Frequent Asked Questions

In this chapter, we will address some frequent asked questions about WLA-9000AP

Question: I forgot my password or the IP address of WLA-9000AP.

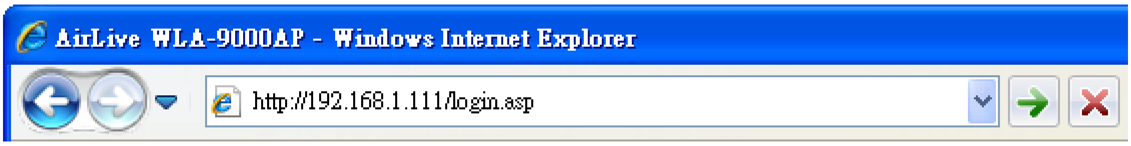
Answer: Please restore your settings to default by press the reset button for more than 5 seconds. You should be able to find your WLA-9000AP at 192.168.1.1 with password "airlive".

==

Question: When I try to configure WLA-9000AP, the following message pop-up saying there is already someone login in to the WLA-9000AP

> Another user is already logged on (IP address: 192.168.1.50,
> Try logging on later.

Answer: You can force another administrator to logout by typing "login.asp" on your browser. Then key-in the password again to enter the management interface.



http://192.168.1.111/login.asp

==

Question: I heard WLA-9000AP can limit the bandwidth of BitTorrent and eDonkey traffic. But I don't see the option on the Bandwidth Control.

Answer: The option to limit bandwidth by application or port is available only on WISP router and AP Router modes.

==

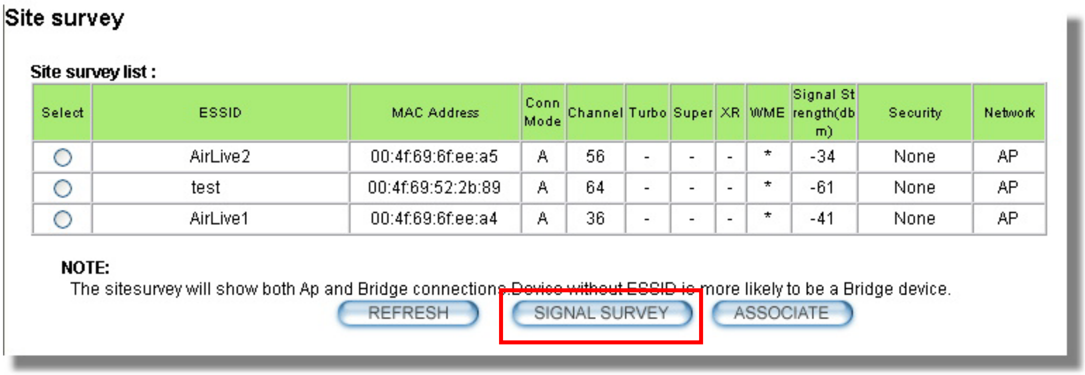
Question: When I plug in the POE cable and 48V power adapter, the WLA-9000AP's power LED is not on?

Answer: Please make sure you have connected the PoE cable to the correct port on the WLA-9000AP. Moreover, you should use an Ethernet cable with 4 twisted pairs (CAT5 or better) for POE cable.

==

Question: Where is the signal survey function that displays the RSSI value continuously?

Answer: The "Signal Survey" function is inside the Site Survey function. You can access from "*Operation Mode -> Setup -> Site Survey*" menu.



Site survey

Site survey list :

Select	ESSID	MAC Address	Conn Mode	Channel	Turbo	Super	XR	WME	Signal Strength(dbm)	Security	Network
○	AirLive2	00:4f:69:6f:ee:a5	A	56	-	-	-	*	-34	None	AP
○	test	00:4f:69:52:2b:89	A	64	-	-	-	*	-61	None	AP
○	AirLive1	00:4f:69:6f:ee:a4	A	36	-	-	-	*	-41	None	AP

NOTE:
The sitesurvey will show both Ap and Bridge connections.Device without ESSID is more likely to be a Bridge device.

==

Question: When do I use Per-User Bandwidth Control by IP, MAC, or IP segment?

Answer: In general, IP address control limits the devices on the end node (i.e. PC and WISP router). MAC address control can limit the traffic of a AP/CPE in wireless client mode.

- ❑ **IP address**: When you want to limit the bandwidth of a single notebook computer, PC, or WISP router.
- ❑ **MAC address**: When you want to limit the bandwidth of a remote AP/CPE in Client mode. For example, another WLA-9000AP in client mode
- ❑ **IP Segment**:: When you want to limit the bandwidth of an entire IP range. For example, all the PCs using the DHCP server to get IP addresses.

==

Question: When I use "Site Survey", why does the RSSI LED goes off?

Answer: When you click on the Site Survey, the WLA-9000AP thinks you are trying to choose a new network to associate. Therefore, it will disconnect from current connection and wait until you establish a new connection. ***If you require seeing the wireless link quality after connection is established, please go to "Device Status->Wireless" menu to see the "RSSI" value.***

===

17 Specifications

The specification of WLA-9000AP is subject to change without notice. Please use the information with caution.

Hardware

- 220MHz Atheros CPU
- High power design , 23dBm average power, to extend the wireless range
- Dual wireless interface 11a, 11a/b/g + 11a, operation simultaneously.
- Super A/G mode support (Atheros Proprietary)
- RoHS compliant
- IEEE 802.3af (PoE) compliance
- 8MB Flash, 32MB SDRAM
- 3 x RJ45 port (PoE support by one LANport)

Antenna

- 2 x R-SMA connector detachable omni Antenna

Frequency Range

- WLAN1(Radio 1)
  - 802.11a : 5.47 to 5.725 GHz
- WLAN2 (Radio 2)
  - 802.11b/g : 2.412 to 2.472 GHz
  - 802.11a : 5.47 to 5.725 GHz

Frequency Channel

- WLAN1(Radio 1)
  - 802.11a
    - USA (FCC) : 12
    - Europe (ETSI) : 19
- - WLAN2(Radio 2)
  - 802.11b/g

    - ◆ USA (FCC) : 11
    - ◆ Europe (ETSI) : 13
  - 802.11a
    - ◆ USA (FCC) : 12
    - ◆ Europe (ETSI) : 19

Power Supply

- External DC Power Adapter (Standard)
  - input 100~240Vac/50~60Hz , output 5.5V/2.5A
- 802.3af Power over Ethernet with DC48V/0.4A (optional)

Modulation Technology

- IEEE802.11a 5GHz OFDM
- IEEE802.11b 2.4GHz CCK
- IEEE802.11g 2.4GHz OFDM
- Atheros Proprietary Super A/G mode 802.11a Orthogonal

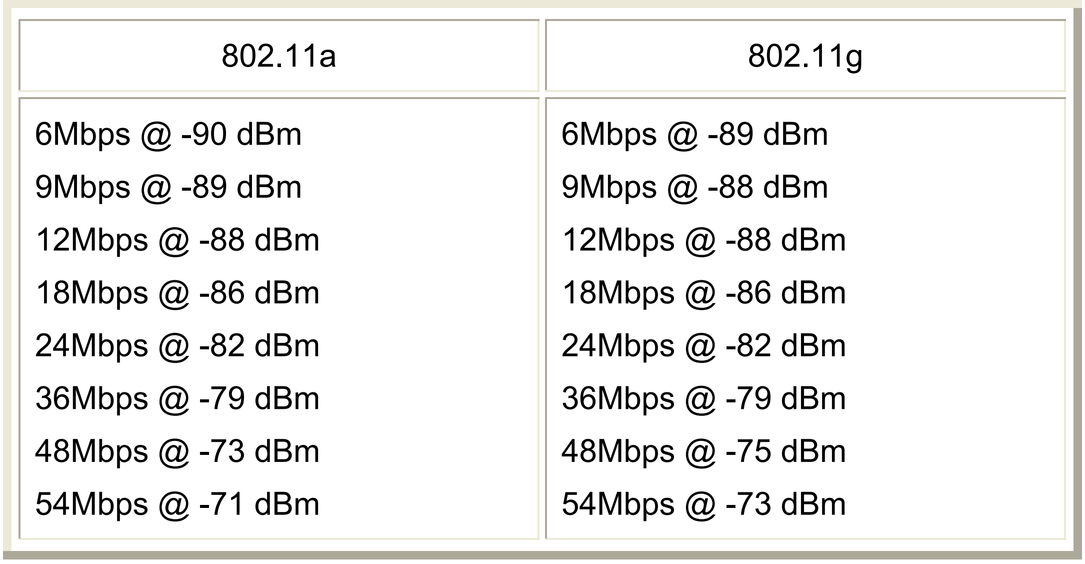
Wireless transfer Data Rate with Automatic Fallback

- 802.11b: 1, 2, 5.5, 11Mbps
- 802.11g: 1, 2, 5.5, 11, 6, 9, 12, 18, 24, 36, 48, 54Mbps
- 802.11a: 6, 9, 12, 18, 24, 36, 48, 54Mbps

Output Power

802.11a	802.11g
54 Mbps @ 17dBm 48 Mbps @ 18dBm 36 Mbps @ 19 dBm 6, 9, 12, 18, 24 Mbps @ 23 dBm	54 Mbps @ 19dBm 48 Mbps @ 20dBm 36 Mbps @ 21 dBm 6, 9, 12, 18, 24 Mbps @ 23 dBm

RSSI



802.11a	802.11g
6Mbps @ -90 dBm	6Mbps @ -89 dBm
9Mbps @ -89 dBm	9Mbps @ -88 dBm
12Mbps @ -88 dBm	12Mbps @ -88 dBm
18Mbps @ -86 dBm	18Mbps @ -86 dBm
24Mbps @ -82 dBm	24Mbps @ -82 dBm
36Mbps @ -79 dBm	36Mbps @ -79 dBm
48Mbps @ -73 dBm	48Mbps @ -75 dBm
54Mbps @ -71 dBm	54Mbps @ -73 dBm

Software

- Wi-Fi, WPA compatible interoperability
- Support WDS Bridge Mode, Client Mode, AP Mode on interface under each predefined operational mode
- Client Isolation supported
- SNMP v1/v2 support
- Support adjustable output power
- ACK Timeout setting
- User Limitation (Static Load Balancing)
- Multiple SSID, VLAN, QoSWPA with PSK/TKIP/AES support ,WPA2 support
- 152-bit WEP support (Atheros Proprietary)
- Super A/G mode support (Atheros Proprietary)
- Bootloader Protection and Emergency Firmware Upload Code in bootloader
- Radius Support
- HTB QoS
- P2P Bandwidth Control

Product Weight (g)

- 341 g (without antennas)

Product Size (L x W x H mm)

- 191 x 145.5 x 29 mm

18 Wireless Network Glossary

The wireless network glossary contains explanation or information about common terms used in wireless networking products. Some of information in this glossary might be outdated, please use with caution.

802.11a

An IEEE specification for wireless networking that operates in the 5 GHz frequency range (5.15 GHz to 5.850 GHz) with a maximum of 54 Mbps data transfer rate. The 5 GHz frequency band is not as crowded as the 2.4 GHz band. In addition, the 802.11a have 12 non-overlapping channels, comparing to 802.11b/g's 3 non-overlapping channels. This means the possibility to build larger non-interfering networks. However, the 802.11a deliver shorter distance at the same output power when comparing to 802.11g.

802.3ad

802.3ad is an IEEE standard for bonding or aggregating multiple Ethernet ports into one virtual port (also known as trunking) to increase the bandwidth.

802.3af

This is the PoE (Power over Ethernet) standard by IEEE committee. 803.af uses 48V POE standard that can deliver up to 100 meter distance over Ethernet cable.

802.11b

International standard for wireless networking that operates in the 2.4 GHz frequency band (2.4 GHz to 2.4835 GHz) and provides a throughput up to 11 Mbps.

802.1d STP

Spanning Tree Protocol. It is an algorithm to prevent network from forming. The STP protocol allows net work to provide a redundant link in the event of a link failure. It is advise to turn on this option for multi-link bridge network.

802.11d

Also known as “Global Roaming”. 802.11d is a standard for use in countries where systems using other standards in the 802.11 family are not allowed to operate.

802.11e

The IEEE QoS standard for prioritizing traffic of the VoIP and multimedia applications. The WMM is based on a subset of the 802.11e.

802.11g

A standard provides a throughput up to 54 Mbps using OFDM technology. It also operates in the 2.4 GHz frequency band as 802.11b. 802.11g devices are backward compatible with 802.11b devices.

802.11h

This IEEE standard define the TPC (transmission power control) and DFS(dynamic frequency selection) required to operate WiFi devices in 5GHz for EU.

802.11i

The IEEE standard for wireless security. 802.11i standard includes TKIP, CCMP, and AES encryption to improve wireless security. It is also know as WPA2.

802.1Q Tag VLAN

In 802.1Q VLAN, the VLAN information is written into the Ethernet packet itself. Each packet carries a VLAN ID(called Tag) as it traveled across the network. Therefore, the VLAN configuration can be configured across multiple switches. In 802.1Q spec, possible 4096 VLAN ID can be created. Although for some devices, they can only view in frames of 256 ID at a time.

802.1x

802.1x is a security standard for wired and wireless LANs. In the 802.1x parlance, there are usually supplicants (client), authenticator (switch or AP), and authentication server (radius server) in the network. When a supplicants request a service, the authenticator will pass the request and wait for the authentication server to grant access and register accounting. The 802.1x is the most widely used method of authentication by WISP.

Adhoc

A Peer-to-Peer wireless network. An Adhoc wireless network do not use wireless AP or router as the central hub of the network. Instead, wireless client are connected directly to each other. The disadvantage of Adhoc network is the lack of wired interface to Internet connections. It is not recommended for network more than 2 nodes.

Access Point (AP)

The central hub of a wireless LAN network. Access Points have one or more Ethernet ports that can connect devices (such as Internet connection) for sharing. Multi-function Access Point can also function as an Ethernet client, wireless bridge, or repeat signals from other AP. Access Points typically have more wireless functions comparing to wireless routers.

ACK Timeout

Acknowledgement Timeout Windows. When a packet is sent out from one wireless station to the other, it will waits for an Acknowledgement frame from the remote station. The station will only wait for a certain amount of time, this time is called the ACK timeout. 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. If the ACK setting is too low then the ACK window will have expired and the returning packet will be dropped, greatly lowering throughput. 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. Setting the correct ACK timeout value needs to consider 3 factors: distance, AP response time, and interference. The WLA-9000AP provides ACK adjustment capability in form of either distance or direct input. When you enter the distance parameter, the WLA-9000AP will automatically calculate the correct ACK timeout value.

Bandwidth Management

Bandwidth Management controls the transmission speed of a port, user, IP address, and application. Router can use bandwidth control to limit the Internet connection speed of individual IP or Application. It can also guarantee the speed of certain special application or privileged IP address - a crucial feature of QoS (Quality of Service) function. The WLA-9000AP's features both “Per-user Bandwidth Control” and “Total Bandwidth Control”. “Per-user Bandwidth Control” allow administrator to define the maximum bandwidth of each user by IP, IP Group, or MAC address. Total Bandwidth defines the maximum bandwidth of wireless or Ethernet interface.

Bootloader

Bootloader is the under layering program that will start at the power-up before the device loads firmware. It is similar to BIOS on a personal computer. When a firmware crashed, you might be able to recover your device from bootloader.

Bridge

A product that connects 2 different networks that uses the same protocol. Wireless bridges are commonly used to link network across remote buildings. For wireless application, there are 2 types of Bridges. WDS Bridge can be used in Point-to-Point or Point-to-Multipoint topology. Bridge Infrastructure works with AP mode to form a star topology.

Cable and Connector Loss: During wireless design and deployment, it is important to factor in the cable and connector loss. Cable and connector loss will reduce the output power and receiver sensitivity of the radio at connector end. The longer the cable length is, the more the cable loss. Cable loss should be subtracted from the total output power during distance calculation. For example, if the cable and connector loss is 3dBm and the output power is 20dBm; the output power at the cable end is only 17dBm.

Client

Client means a network device or utility that receives service from host or server. A client device means end user device such as wireless cards or wireless CPE.

CPE Devices

CPE stands for Customer Premises Equipment. A CPE is a device installed on the end user's side to receive network services. For example, on an ADSL network, the ADSL modem/router on the subscriber's home is the CPE device. Wireless CPE means a complete Wireless (usually an AP with built-in Antenna) that receive wireless broadband access from the WISP. The opposite of CPE is CO.

CTS

Clear To Send. A signal sent by a device to indicate that it is ready to receive data.

DDNS

Dynamic Domain Name System. An algorithm that allows the use of dynamic IP address for hosting Internet Server. A DDNS service provides each user account with a domain name. A router with DDNS capability has a built-in DDNS client that updates the IP address information to DDNS service provider whenever there is a change. Therefore, users can build website or other Internet servers even if they don't have fixed IP connection.

DHCP

Dynamic Hosting Configuration Protocol. A protocol that enables a server to dynamically assign IP addresses. When DHCP is used, whenever a computer logs onto the network, it automatically gets an IP address assigned to it by DHCP server. A DHCP server can either be a designated PC on the network or another network device, such as a router.

DMZ

Demilitarized Zone. When a router opens a DMZ port to an internal network device, it opens all the TCP/UDP service ports to this particular device. The feature is used commonly for setting up H.323 VoIP or Multi-Media servers.

DNS

A program that translates URLs to IP addresses by accessing a database maintained on a collection of Internet servers.

Domain Name

The unique name that identifies an Internet site. Domain Names always have 2 or more parts, separated by dots. In www.airlive.com, the "airlive.com" is the doman name.

DoS Attack

Denial of Service. A type of network attack that floods the network with useless traffic. Many DoS attacks, such as the Ping of Death and Teardrop attacks, exploit limitations in the TCP/IP protocols.

Encryption

Encoding data to prevent it from being read by unauthorized people. The common wireless encryption schemes are WEP, WPA, and WPA2.

ESSID (SSID)

The identification name of an 802.11 wireless network. Since wireless network has no physical boundary liked wired Ethernet network, wireless LAN needs an identifier to distinguish one network from the other. Wireless clients must know the SSID in order to associate with a WLAN network. Hide SSID feature disable SSID broadcast,
so users must know the correct SSID in order to join a wireless network.

Firewall

A system that secures a network and prevents access by unauthorized users. Firewalls can be software, router, or gateway. Firewalls can prevent unrestricted access into a network, as well as restricting data from flowing out of a network.

Firmware

The program that runs inside embedded device such as router or AP. Many network devices are firmware upgradeable through web interface or utility program.

FTP

File Transfer Protocol. A standard protocol for sending files between computers over a TCP/IP network and the Internet.

Fragment Threshold

Frame Size larger than this will be divided into smaller fragment. If there are interferences in your area, lower this value can improve the performance. If there are not, keep this parameter at higher value. The default size is 2346. You can try 1500, 1000, or 500 when there are interference around your network.

Full Duplex

The ability of a networking device to receive and transmit data simultaneously. In wireless environment, this is usually done with 2 or more radios doing load balancing.

Gateway

In the global Internet network, the gateways are core routers that connect networks in different IP subnet together. In a LAN environment with an IP sharing router, the gateway is the router. In an office environment, gateway typically is a multi-function device that integrates NAT, firewall, bandwidth management, and other security functions.

Hotspot

A place where you can access Wi-Fi service. The term hotspot has two meanings in wireless deployment. One is the wireless infrastructure deployment, the other is the Internet access billing system. In a hotspot system, a service provider typically need an authentication and account system for billing purposes, and a wireless AP network to provide access for customers.

IGMP Snooping

Internet Group Management Protocol (IGMP) is a Layer 3 protocol to report IP multicast memberships to neighboring multicast switches and routers. IGMP snooping is a feature that allows an Ethernet switch to "listen in" on the IGMP conversation between hosts and routers. A switch support IGMP snooping has the possibility to avoid multicast traffic being treated as broadcast traffic; therefore, reducing the overall traffic on the network.

Infrastructure Mode

A wireless network that is built around one or more access points to provide wireless clients access to wired LAN / Internet service. The opposite of Infrastructure mode is Adhoc mode.

IP address

IP (Internet Protocol) is a layer-3 network protocol that is the basis of all Internet communication. An IP address is 32-bit number that identifies each sender or receiver of information that is sent across the Internet. An IP address has two parts: an identifier of a particular network on the Internet and an identifier of the particular device (which can be a server or a workstation) within that network. The new IPv6 specification supports 128-bit IP address format.

IPsec

IP Security. A set of protocols developed by the IETF to support secure exchange of packets at the IP layer. IPsec has been deployed widely to implement Virtual Private Networks (VPNs). IPsec supports two encryption modes: Transport and Tunnel. Transport mode encrypts only the data of each packet, but leaves the header untouched. The more secure Tunnel mode encrypts both the header and the payload. On the receiving side, an IPSec-compliant device decrypts each packet.

LACP (802.3ad) Trunking

The 802.3ad Link Aggregation standard defines how to combine the several Ethernet ports into one high-bandwidth port to increase the transmission speed. It is also known as port trunking. Both device must set the trunking feature to work.

MAC

Media Access Control. MAC address provides layer-2 identification for Networking Devices. Each Ethernet device has its own unique address. The first 6 digits are unique for each manufacturer. When a network device have MAC access control feature, only the devices with the approved MAC address can connect with the network.

Mbps

Megabits Per Second. One million bits per second; a unit of measurement for data transmission

MESH

Mesh is an outdoor wireless technology that uses Spanning Tree Protocol (STP) and Wireless Distribution system to achieve self-forming, self-healing, and self-configuring outdoor network. MESH network are able to take the shortest path to a destination that does not have to be in the line of site.

MIMO

Multi In Multi Out. A Smart Antenna technology designed to increase the coverage and performance of a WLAN network. In a MIMO device, 2 or more antennas are used to increase the receiver sensitivity and to focus available power at intended Rx.

NAT

Network Address Translation. A network algorithm used by Routers to enables several PCs to share single IP address provided by the ISP. The IP that a router gets from the ISP side is called Real IP, the IP assigned to PC under the NAT environment is called Private IP.

Node

A network connection end point, typically a computer.

Packet

A unit of data sent over a network.

Passphrase

Used much like a password, a passphrase simplifies the WEP encryption process by automatically generating the WEP encryption keys for the company products.

POE

Power over Ethernet. A standard to deliver both power and data through one single Ethernet cable (UTP/STP). It allows network device to be installed far away from power ource. A POE system typically compose of 2 main component: DC Injector (Base Unit) and Splitter(Terminal Unit). The DC injector combines the power and data, and the splitter separates the data and power back. A PoE Access Point or CPE has the splitter built-in to the device. The IEEE 802.3af is a POE spec that uses 48 volt to deliver power up to 100 meter distance.

Port

This word has 2 different meaning for networking.

- The hardware connection point on a computer or networking device used for plugging in a cable or an adapter.
- The virtual connection point through which a computer uses a specific application on a server.

PPPoE

Point-to- Point Protocol over Ethernet. PPPoE relies on two widely accepted standards: PPP and Ethernet. PPPoE is a specification for connecting the users on an Ethernet to the Internet through a common broadband medium, such as a single DSL line, wireless device or cable modem.

PPTP

Point-to-Point Tunneling Protocol: A VPN protocol developed by PPTP Forum. With PPTP, users can dial in to their corporate network via the Internet. If users require data encryption when using the Windows PPTP client, the remote VPN server must support MPPE (Microsoft Point-To-Point Encryption Protocol) encryption. PPTP is also used by some ISP for user authentication, particularly when pairing with legacy Alcatel / Thomson

ADSL modem.

Preamble Type

Preamble are sent with each wireless packet transmit for transmission status. Use the long preamble type for better compatibility. Use the short preamble type for better performance

Rate Control

Ethernet switches' function to control the upstream and downstream speed of an individual port. Rate Control management uses "Flow Control" to limit the speed of a port. Therefore, the Ethernet adapter must also have the flow control enabled. One way to force the adapter's flow control on is to set a port to half-duplex mode.

RADIUS

Remote Authentication Dial-In User Service. An authentication and accounting system used by many Internet Service Providers (ISPs). When you dial in to the ISP, you must enter your username and password. This information is passed to a RADIUS server, which checks that the information is correct, and then authorizes access to the ISP system. Radius typically uses port 1812 and port 1813 for authentication and accounting port. Though not an official standard, the RADIUS specification is maintained by a working group of the IETF.

Receiver Sensitivity

Receiver sensitivity means how sensitive is the radio for receiving signal. In general; the slower the transmission speed, the more sensitive the radio is. The unit for Receiver Sensitivity is in dB; the lower the absolute value is, the higher the signal strength. For example, -50dB is higher than -80dB.

RJ-45

Standard connectors for Twisted Pair copper cable used in Ethernet networks. Although they look similar to standard RJ-11 telephone connectors, RJ-45 connectors can have up to eight wires, whereas telephone connectors have only four.

Router

An IP sharing router is a device that allows multiple PCs to share one single broadband connection using NAT technology. A wireless router is a device that combines the functions of wireless Access Point and the IP sharing router.

RSSI

Receiver Sensitivity Index. RSSI is a value to show the Receiver Sensitivity of the remote wireless device. In general, remote APs with stronger signal will display higher RSSI values. For RSSI value, the smaller the absolute value is, the stronger the signal. For example, "-50db" has stronger signal than "-80dB". For outdoor connection, signal stronger than -60dB is considered as a good connection.

RTS

Request To Send. A packet sent when a computer has data to transmit. The computer will wait for a CTS (Clear To Send) message before sending data.

RTS Threshold

RTS (Request to Send). The RTS/CTS(clear to send) packet will be send before a frame if the packet frame is larger than this value. Lower this value can improve the performance if there are many clients in your network. You can try 1500, 1000 or 500 when there are many clients in your AP's network.

SNMP

Simple Network Management Protocol. A set of protocols for managing complex networks. The SNMP network contains 3 key elements: managed devices, agents, and network-management systems (NMSs). Managed devices are network devices that content SNMP agents. SNMP agents are programs that reside SNMP capable device's firmware to provide SNMP configuration service. The NMS typically is a PC based software such as HP Openview that can view and manage SNMP network device remotely.

SSH

Developed by SSH Communications Security Ltd., Secure Shell is a program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. It provides strong authentication and secure communications over insecure channels. It is a replacement for rlogin, rsh, rcp, and rdist.

SSL

Secure Sockets Layer. It is a popular encryption scheme used by many online retail and banking sites to protect the financial integrity of transactions. When an SSL session begins, the server sends its public key to the browser. The browser then sends a randomly generated secret key back to the server in order to have a secret key exchange for that session. SSL VPN is also known as Web VPN. The HTTPS and SSH management interface use SSL for data encryption.

Subnet Mask
An address code mask that determines the size of the network. An IP subnet are determined by performing a BIT-wise AND operation between the IP address and the subnet mask. By changing the subnet mask, you can change the scope and size of a network.

Subnetwork or Subnet
Found in larger networks, these smaller networks are used to simplify addressing between numerous computers. Subnets connect to the central network through a router, hub or gateway. Each individual wireless LAN will probably use the same subnet for all the local computers it talks to.

Super A
Super A is an Atheros proprietary turbo mode to increase speed over standard 802.11a mode. It adds Bursting and Compression to increase the speed. If you live in countries that prohibit the channel binding technology (i.e. Europe), you should choose “Super-A without Turbo) if you need more speed than 11a mode

TCP
A layer-4 protocol used along with the IP to send data between computers over the Internet. While IP takes care of handling the actual delivery of the data, TCP takes care of keeping track of the packets that a message is divided into for efficient routing through the Internet.

Turbo A
Turbo A is an Atheros proprietary turbo mode to increase speed over standard 802.11a mode. It uses channel binding technology to increase speed. There are 2 types of Turbo A modes: Dynamic Turbo and Static Turbo. In Dynamic Turbo, the channel binding will be used only if necessary. In Static Turbo, the channel binding is always on. This protocol may be combined with Super-A model to increase the performance even more. The used

of channel binding might be prohibited in EU countries.

TX Output Power

Transmit Output Power. The TX output power means the transmission output power of the radio. Normally, the TX output power level limit for 2.4GHz 11g/b is 20dBm at the antenna end. The output power limit for 5GHz 802.11a is 30dBm at the antenna end..

UDP

User Datagram Protocol. A layer-4 network protocol for transmitting data that does not require acknowledgement from the recipient of the data.

Upgrade

To replace existing software or firmware with a newer version.

Upload

To send a file to the Internet or network device.

URL

Uniform Resource Locator. The address of a file located on the Internet.

VPN

Virtual Private Network. A type of technology designed to increase the security of information transferred over the Internet. VPN creates a private encrypted tunnel from the end user's computer, through the local wireless network, through the Internet, all the way to the corporate network.

Walled Garden

On the Internet, a walled garden refers to a browsing environment that controls the information and Web sites the user is able to access. This is a popular method used by ISPs in order to keep the user navigating only specific areas of the Web

WAN

Wide Area Network. A communication system of connecting PCs and other computing devices across a large local, regional, national or international geographic area. A WAN port on the network device means the port (or wireless connection) that is connected to the Internet side of the network topology.

WEP

Wired Equivalent Privacy. A wireless encryption protocol. WEP is available in 40-bit (64-bit), 108-bit (128-bit) or 152-bit (Atheros proprietary) encryption modes.

Wi-Fi

Wireless Fidelity. An interoperability certification for wireless local area network (LAN) products based on the IEEE 802.11 standards. The governing body for Wi-Fi is called Wi-Fi Alliance (also known as WECA).

WiMAX

Worldwide Interoperability for Microwave Access. A Wireless Metropolitan Network technology that complies with IEEE 802.16 and ETSI Hiperman standards. The orginal 802.16 standard call for operating frequency of 10 to 66Ghz spectrum. The 802.16a amendment extends the original standard into spectrum between 2 and 11 Ghz. 802.16d increase data rates to between 40 and 70 Mbps/s and add support for MIMO antennas, QoS, and multiple polling technologies. 802.16e adds mobility features, narrower bandwidth (a max of 5 mhz), slower speed and smaller antennas. Mobility is allowed up to 40 mph.

WDS

Wireless Distribution System. WDS defines how multiple wireless Access Point or Wireless Router can connect together to form one single wireless network without using wired uplinks. WDS associate each other by MAC address, each device

WLAN

Wireless Local Area Network. A type of local-area network that uses high-frequency radio waves rather than wires to communicate between nodes. The most popular standard for WLAN is the 802.11 standards.

WMM

Wi-Fi Multimedia (WMM) is a standard to prioritize traffic for multimedia applications. The

WMM prioritize traffic\ on Voice-over-IP (VoIP), audio, video, and streaming media as well as traditional IP data over the AP.

WMS
Wireless Management System. An utility program to manage multiple wireless AP/Bridges.

WPA
Wi-Fi Protected Access. It 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. The WPA-PSK utilizes pre-share key for encryption/authentication.

WPA2
Wi-Fi Protected Access 2. WPA2 is also known as 802.11i. It improves on the WPA security with CCMP and AES encryption. The WPA2 is backward compatible with WPA. WPA2-PSK utilizes pre-share key for encryption/authentication.