Air Live®
Powered by OvisLink Corp.

WH-9200AP

802.11a/b/g Dual Radio
Wireless Base Station

User's Manual

www.airlive.com

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.

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.

Copyright Statement

Table of Contents

1. Introduction

1.1 Overview

The WH-9200AP is a dream device for WISP to build their wireless networks. The AP features 2 Atheros 11a/b/g radios that run in 5GHz or 2.4GHz frequency band. Moreover, it provides hi-power at 11a mode for extra long distance application. There is an intergraded 802.3af POE port to let you run the AP at up to 100 meter distance away from the power source.

Dual Wireless + Hi Power + 2 LAN Ports

The WH-9200AP is equipped with 2 high-powered Atheros radios. The radio 1 runs in the 11a 5GHz mode only while the radio 2 runs at the 11a/b/g dual band mode. AirLive adds high power amplifier to run the AP at 23dBm in 11a mode (200mW), that's 4 times the output power of normal 11a radio (50mW). In addition, 2 programmable LAN ports are available for multi-mode AP/Gateway configuration.

Multiple Operation Modes

The WH-9200AP can operate in multiple wireless modes for different application environments such as Dual AP, Dual WDS, Duplex link aggregation, Separate Bridge, AP + Client, AP + WDS, WDS + Gateway, AP + Gateway, and AP + WISP. These modes can be changed and configured easily by the Web user interface.

802.3af PoE Port

WH-9200AP is equipped with an 802.3af Power over Ethernet port. It thus can be powered by a PoE PSE and operate at up to 100 meter away.

VLAN & QoS

WH-9200AP provides Multi-SSID to create different wireless networks using one AP. The TAG VLAN feature allows service provider to control service content of each SSID network all the way back to core router. The QoS feature allows prioritizing the different package according the 802.11e WMM protocol and triple play (Voice, Video and Data). Bandwidth control feature allow WH-9200AP to limit the bandwidth on distinct IP/MAC or on the total device.

IP67 Environmental Protection Enclosure

With IP-67 industrial standard enclosure, WH-9200AP is highly protected against dust and water. So that WH-9200AP can be used in a hardened environment.

1.2 Installing WH-9200AP

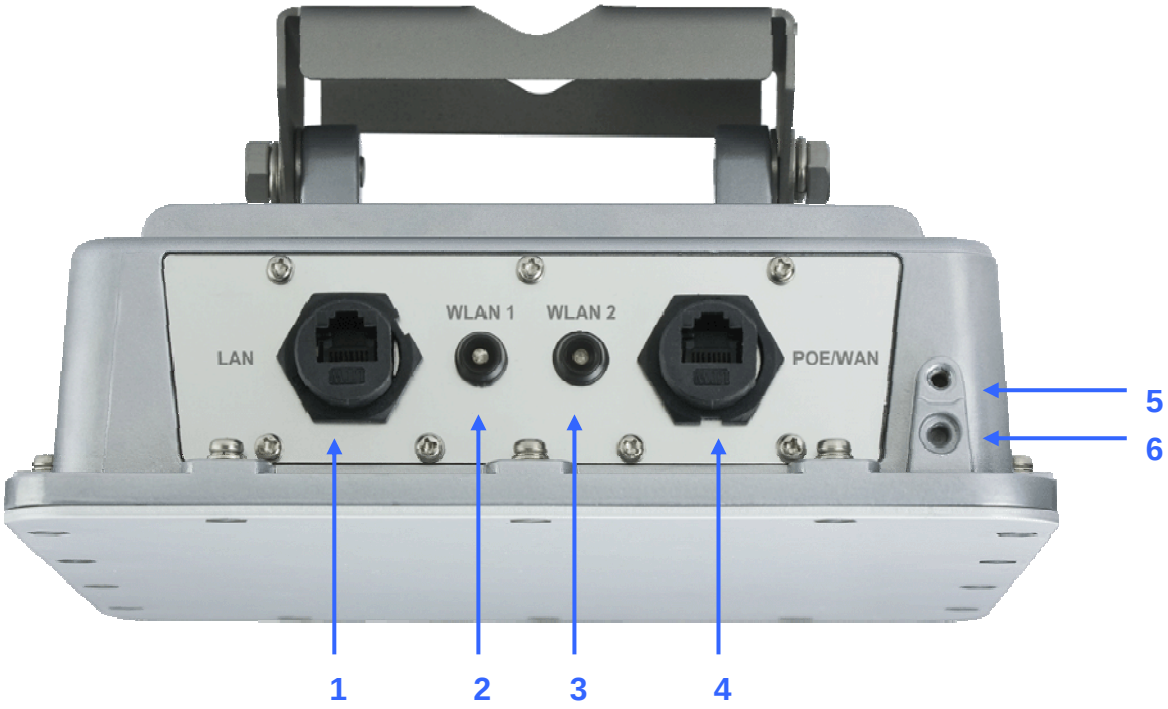
This section describes the installation procedure for the WH-9200AP. It starts with a summary of the content of the package you have purchased, followed by steps of how to power up and connect the WH-9200AP. Finally, this section explains how to configure a Windows PC to communicate with the WH-9200AP.

1.2.1 Package Content

The WH-9200AP package contains the following items:

- One WH-9200AP main unit
- 48VDC PoE injector kits
- Pole/Wall mount kit
- One CD of the WH-9200AP
- Quick Start Guide

1.2.2 Hardware Presentation



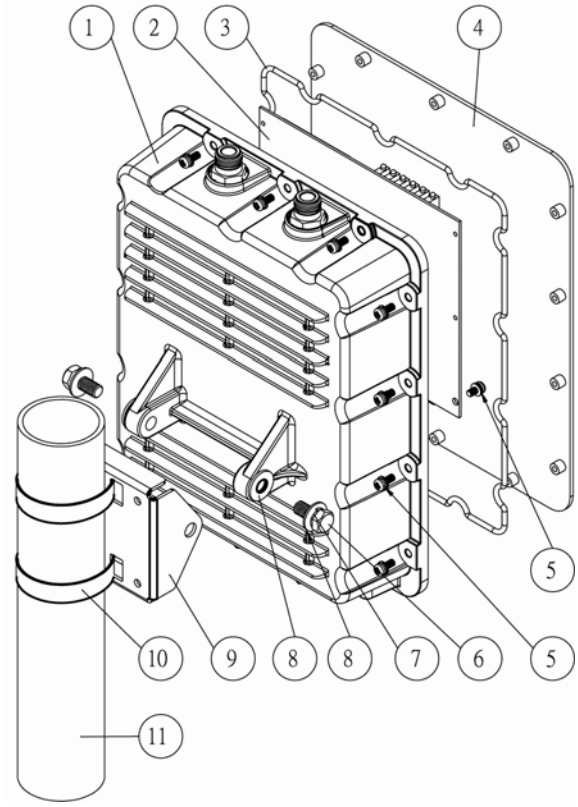
LED #	Function	Color	Description
1	LAN	-	LAN port #2
2	WLAN1 LED	Blue	No Connection: Off Low Signal: Flash per second Better Signal: Flash every 2 seconds Best Signal: Steady On
3	WLAN2 LED	Green	
4	POE/WAN	-	LAN port #1, compatible with 802.3af PoE. Become WLAN port when operate in Gateway mode
5	Ground Pin	-	Reference point for electric current
6	Sluice	-	Sluice out the water in device


N-Type connector for outdoor antenna of Radio 1
N-Type connector for outdoor antenna of Radio 2
Air Live
Antenna 1
Antenna 2

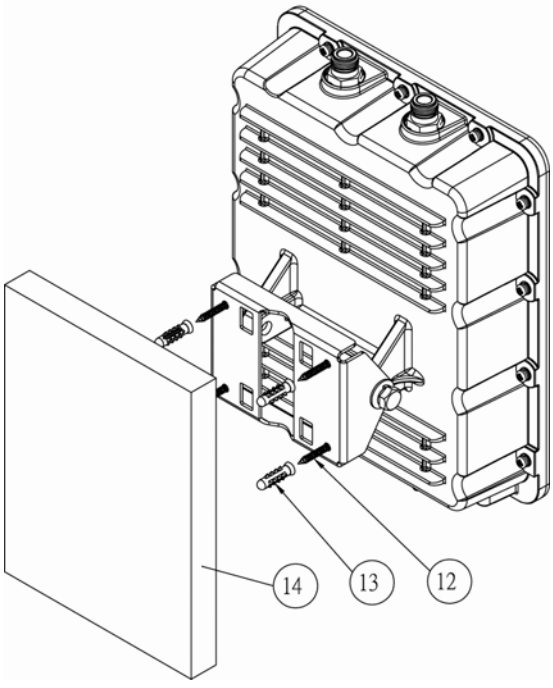
Pole Mount/Wall mount Installation

①	Enclosure assembly	- 1 set
②	PCB assembly	- 1 set
③	Gasket of front cover	- 1 pc
④	Front cover	- 1 pc
⑤	M4-10 screw	- 16 pcs
⑥	M8-20 screw	- 2 pcs
⑦	M8 spring washer	- 2 pcs
⑧	M8 washer	- 4 pcs
⑨	Mounting	- 1 pc
⑩	Pole clamp	- 2 pcs
⑪	POLE(MAX.:2 inch)	
⑫	Wall screw	- 4 pcs
⑬	Plastic anchor	- 4 pcs
⑭	Wall	

Pole Mount

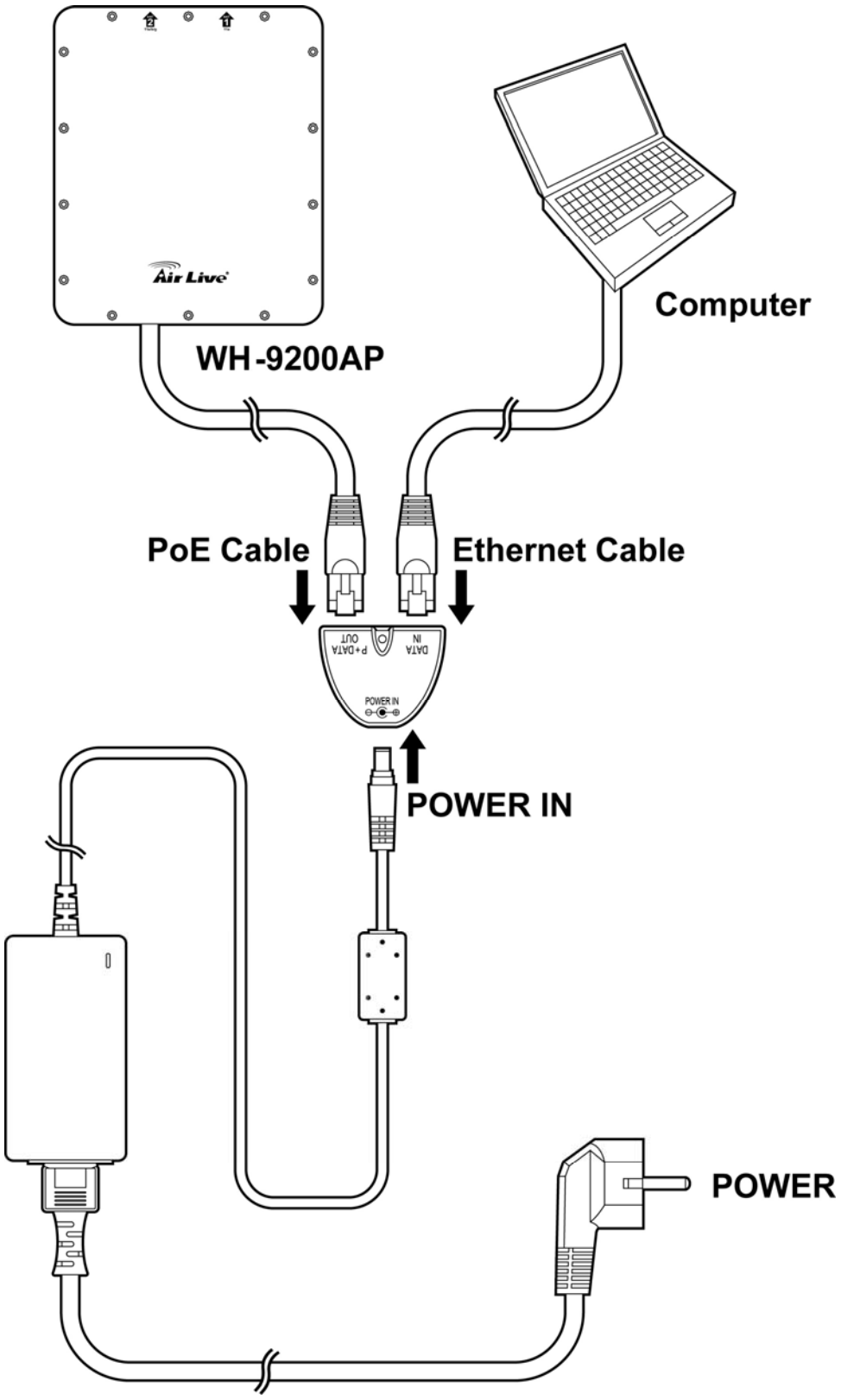


Wall Mount



Power Installation

The following image shows the power installation of WH-9200AP. Note that WH-9200AP is IEEE802.3af compatible, you should use the packed POE kit or POE switch for power injection.



1.2.3 Configuration Setups

The factory default settings of WH-9200AP are as following:

Settings	Default Value	
	Wireless1	**Wireless2**
Device Name	WH-9200AP	
Radio	802.11a	802.11a
SSID	airlive1	airlive2
Channel	36	36 (auto in 802.11b/g)
WEP	Disabled	
IP Address	192.168.1.1	
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.

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

Access to management interface

1 Please make sure your computer IP is in the same subnet as the AP (i.e. 192.168.1.x).

2 Please make sure your computer has wireless network adapter installed.

3 Open the web browser and enter http://192.168.1.1/.

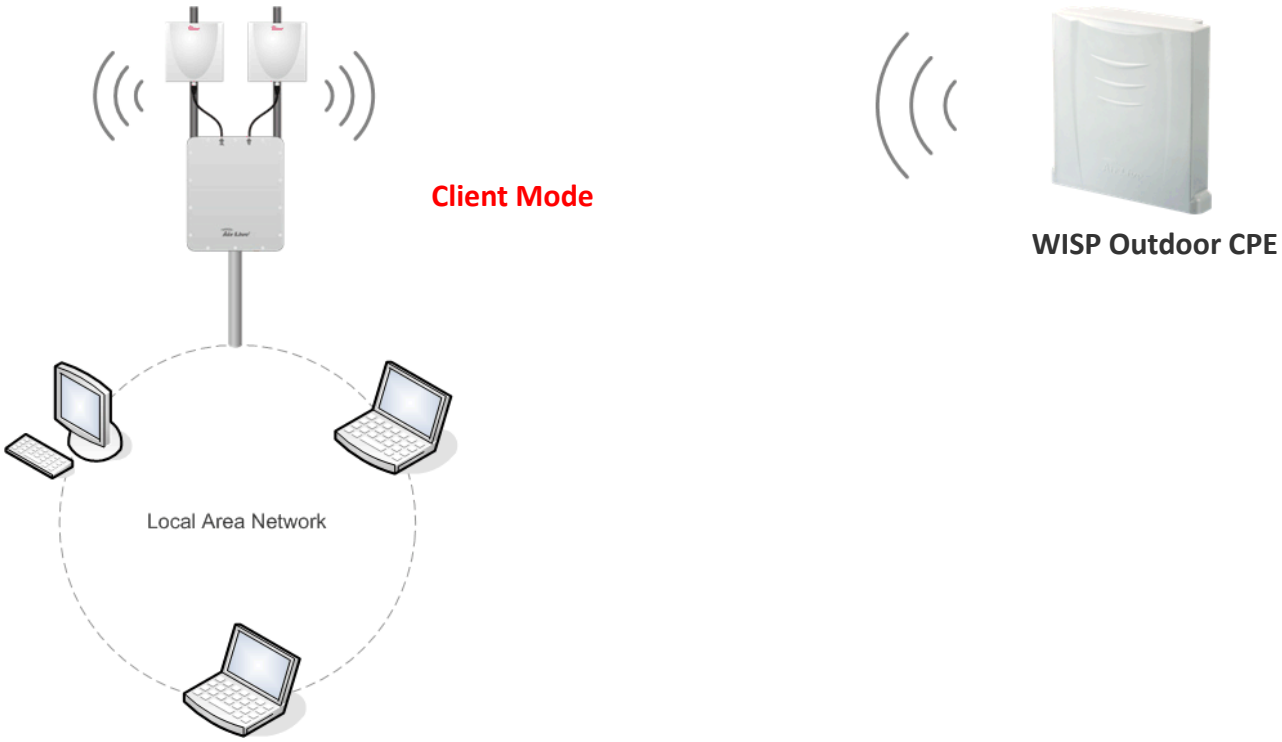
4. Connect Wireless Settings to start.

2. Wireless Settings

This section guides you to configure the mode of the Radio interface. Note that the radio can select either 11a or 11b/g mode.

2.1 Client Mode

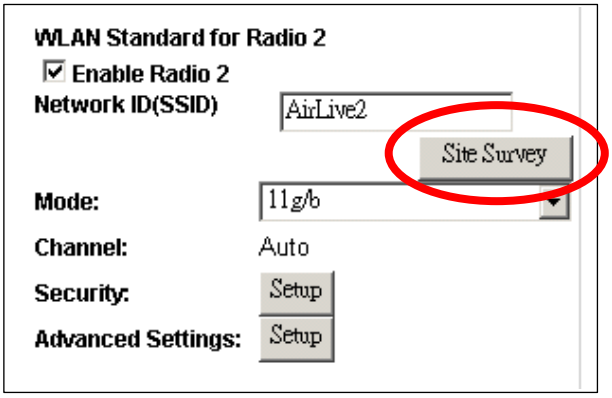
Also known as Ethernet Client. In this mode, the AP will act as a WLAN card to connect with the remote AP. Users can connect PC or local LAN to the Ethernet port of local LAN to the Ethernet port of the client mode AP. This mode is mostly used as a CPE device for WISP subscriber.

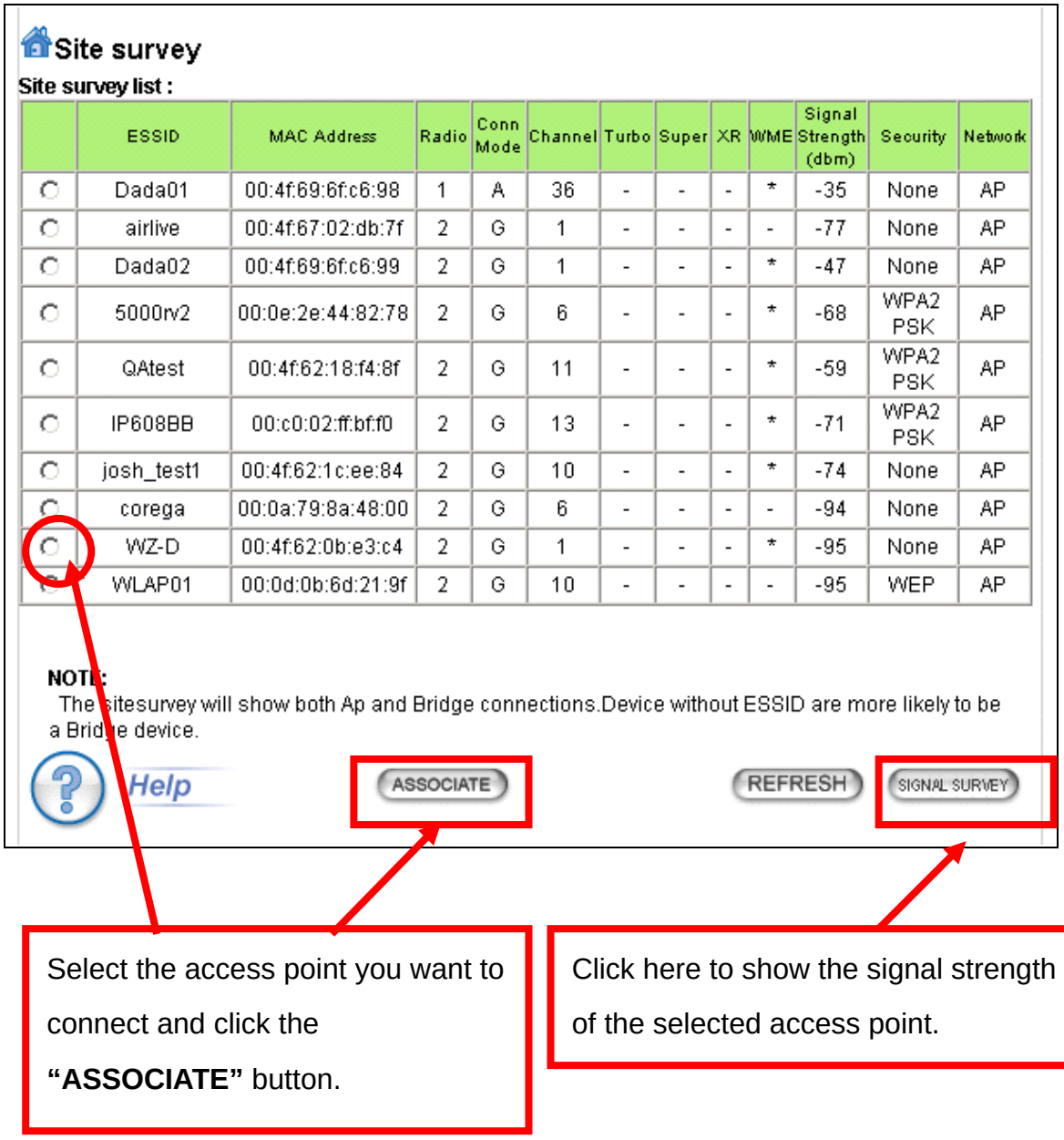


Client mode included in these operation modes: AP + Client, Client + AP, AP + WISP, and WISP + AP.

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

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

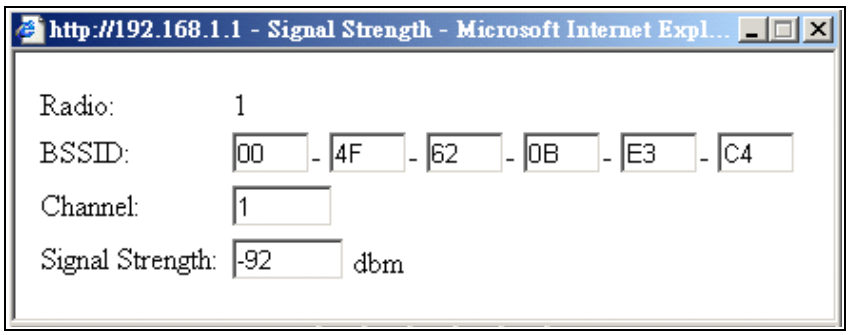




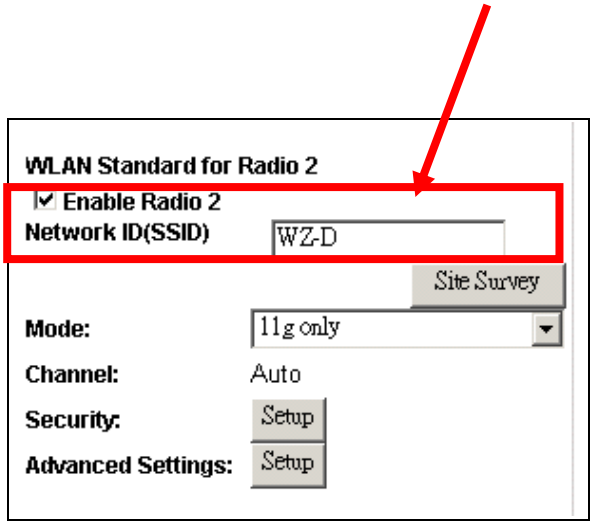
Select the access point you want to connect and click the **"ASSOCIATE"** button.

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

The Signal Survey pop up windows shows as following:



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



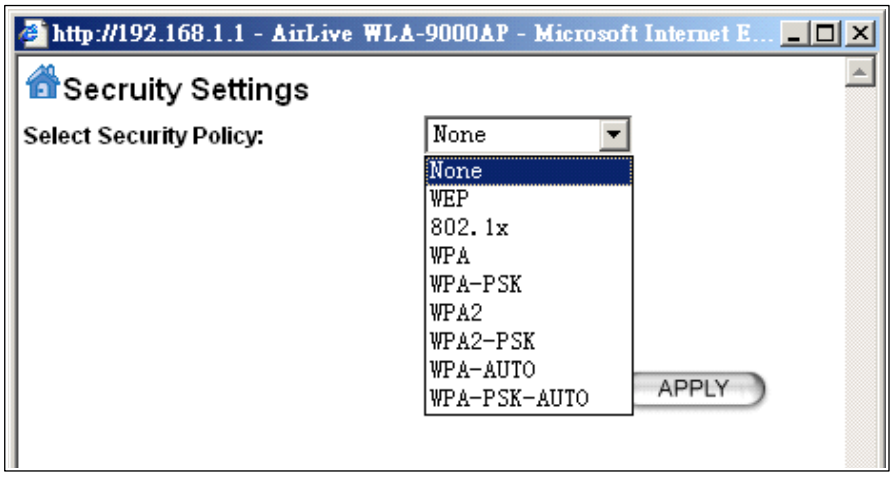
To configure the Security, please refer to Section 3.6 ……

To configure the Advanced Settings, please refer to Section 3.8……

2.2 Wireless Security

The wireless security is to configure a secure connection between two wireless devices.

WH-9200AP provides WEP, 802.1x, WPA, WPA-PSK, WPA2, WPA2-PSK, WPA-AUTO and WPA-PSK-AUTO security policy.



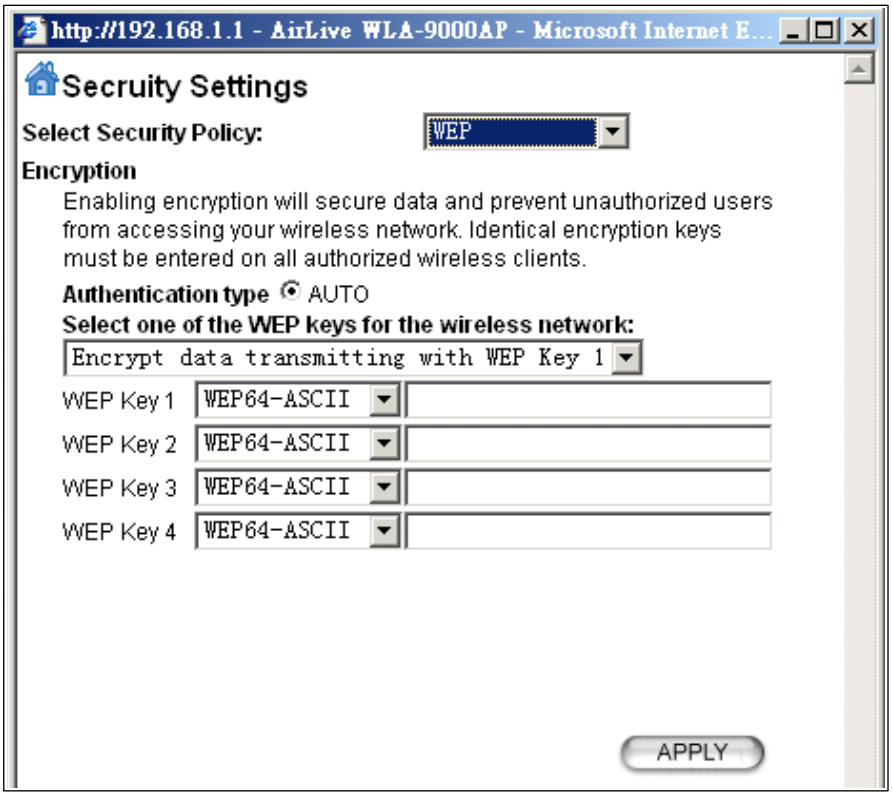
WEP

WEP allows you to use data encryption to secure your data from being eavesdropped by malicious people. It allows 3 types of key: 64 (WEP64), 128 (WEP128), and 152 (WEP152) bits. You can configure up to 4 keys using either ASCII or Hexadecimal format.

Key Settings: The length of a WEP64 key must be equal to 5 bytes, a WEP128 key is 13 bytes, and a WEP152 key is 16 bytes.

Key Index: You have to specify which of the four keys will be active.

Once you enable the WEP function, please make sure that both the WH-9200AP and the wireless client stations use the same key.



Some wireless client cards only allow Hexadecimal digits for WEP keys.

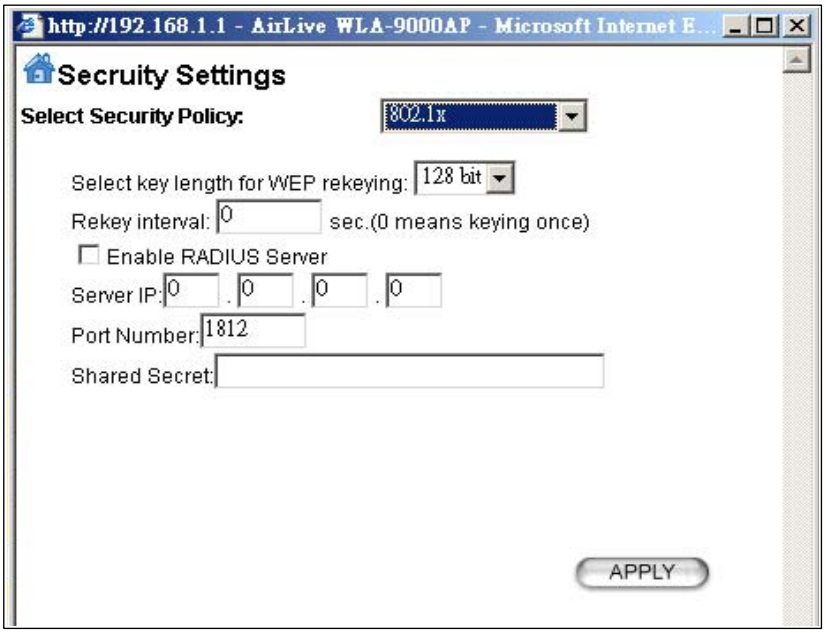
Please note that when configuring WEP keys, a WEP128 ASCII key looks like

"**This is a key**"(13 characters), while a WEP128 Hex key looks like "**54686973206973206120b6579**"(26 HEX)

(hexadecimal notation are 0-9 and A-F).

802.1X

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. Here 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.

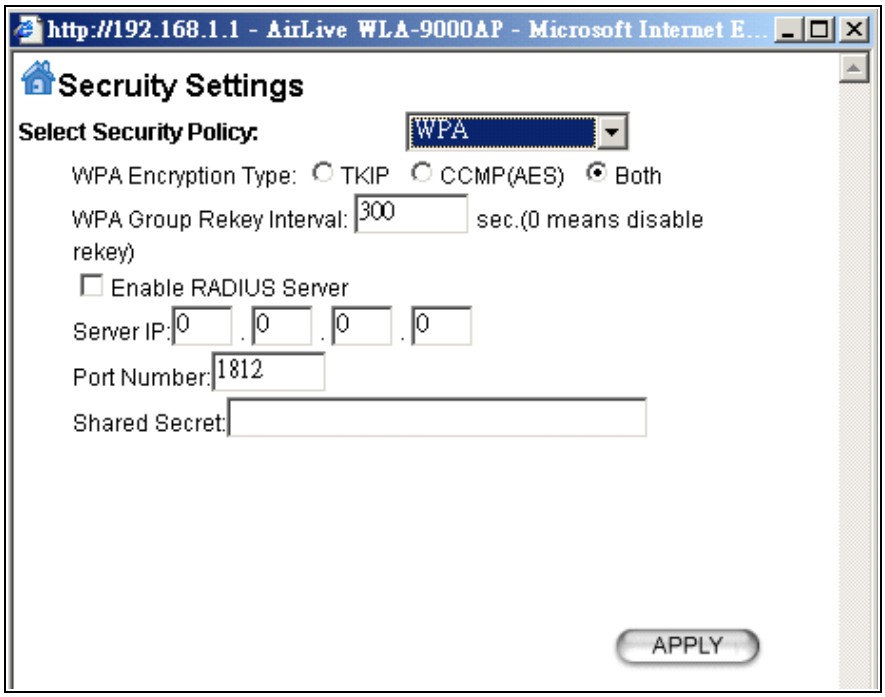
Server IP and Shared Secret: If you have connect AP to a RADIUS server behind, key in the Server IP and share secret, it will redirect incoming connection request first to this RADIUS for Authentication. In general you don't have to change Port Number, which is 1812 by default and used by most RADIUS server.

After you have finished the configuration wizard, you have to configure the RADIUS Settings in Advanced Settings in order to make the 802.1x function work.

Share secret is the key for AP to communicate with RADIUS server, check with your Authentication provider for more details.

WPA

Wi-Fi Protected Access (WPA) requires a RADIUS server available in order to do authentication (same as 802.1x), thus there is no shared key required.

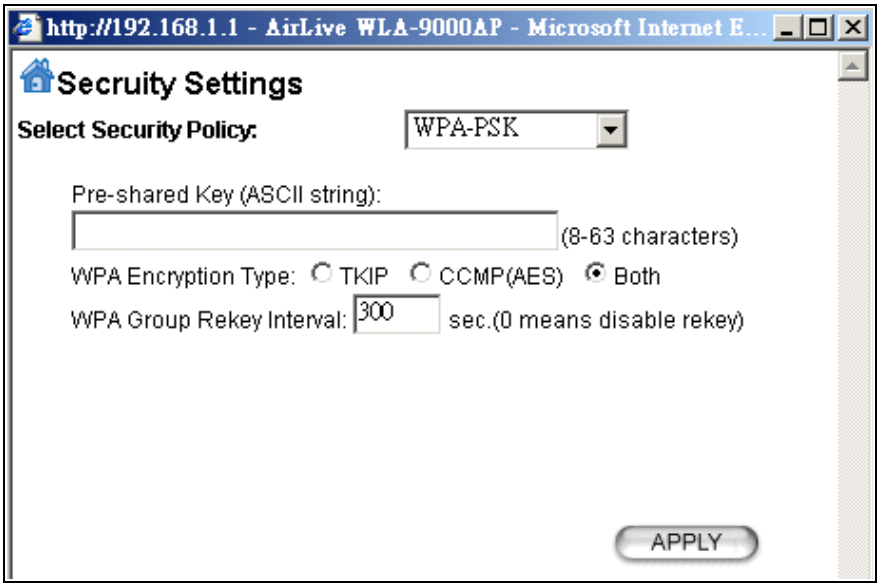


Encryption Type: There are two encryption types **TKIP** and **CCMP (AES)**. While CCMP provides better security than TKIP, some wireless client stations may not be equipped with the hardware to support it. You can select **Both** to allow TKIP clients and CCMP clients to connect to the Access Point 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

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.



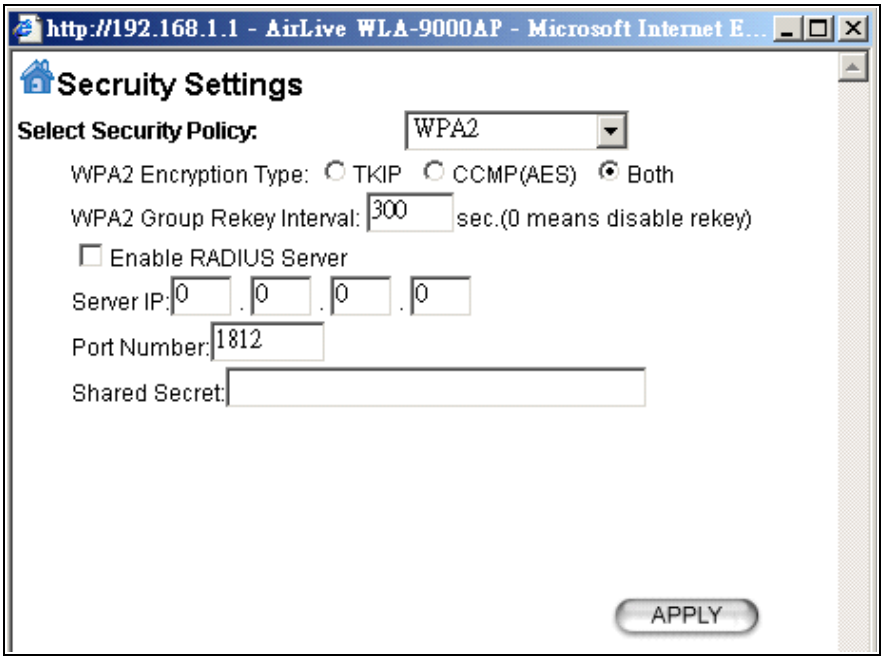
Pre-shared Key: This is an ASCII string with 8 to 63 characters. Please make sure that both the WH-9200AP and the wireless client stations use the same key.

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.

WPA2

WPA2 stands for Wi-Fi Protected Access 2. It provides stronger data protection and network access control then WPA. Only authorized users can access the wireless networks.

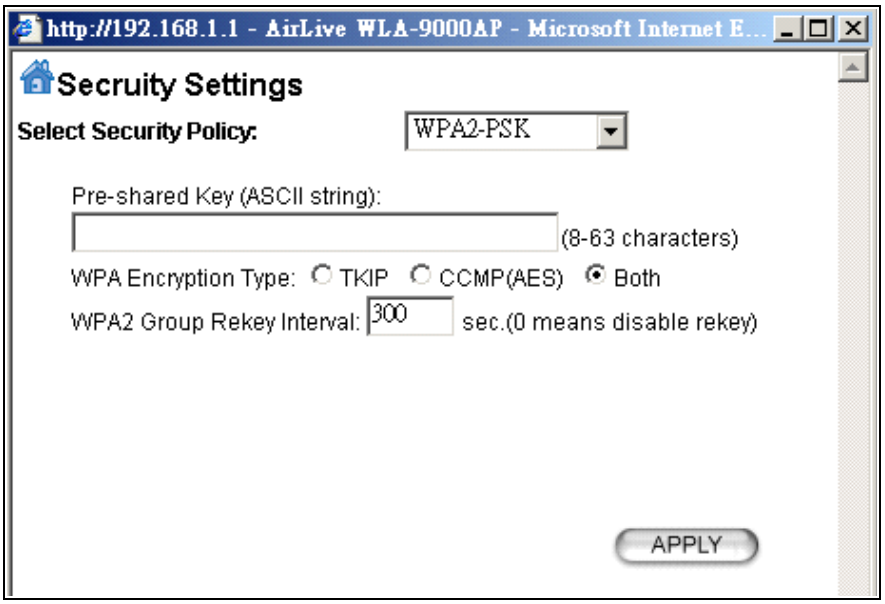


Encryption Type: There are two encryption types **TKIP** and **CCMP (AES)**. While CCMP provides better security than TKIP, some wireless client stations may not be equipped with the hardware to support it. You can select **Both** to allow TKIP clients and CCMP clients to connect to the Access Point 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.

WPA2-PSK

Enter the Pre-shared Key to initiate WPA2 security. All devices try to access the network should have the matching encryption key.

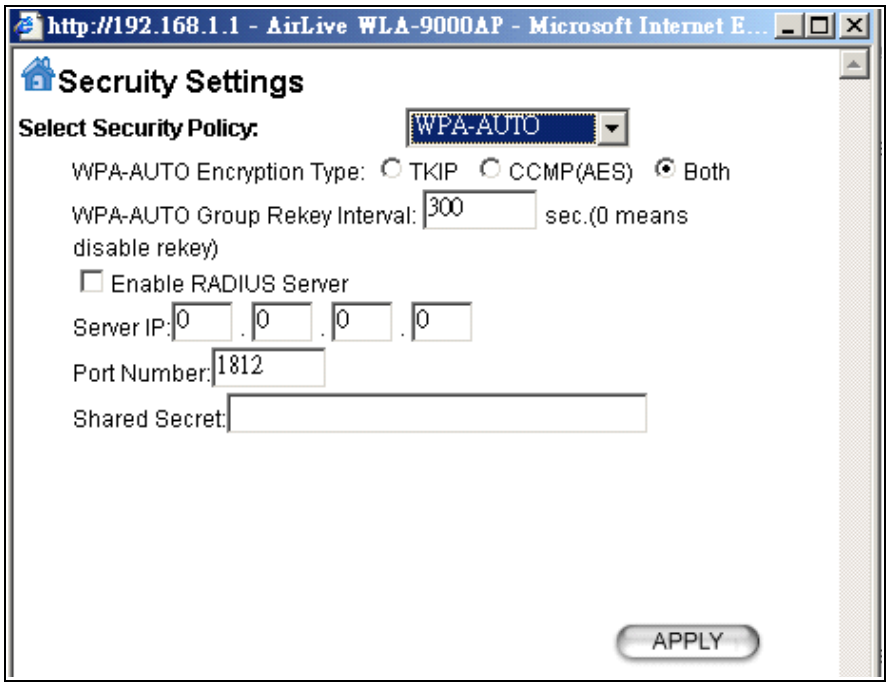


Pre-shared Key: This is an ASCII string with 8 to 63 characters. Please make sure that both the WH-9200AP and the wireless client stations use the same key.

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.

WPA-AUTO

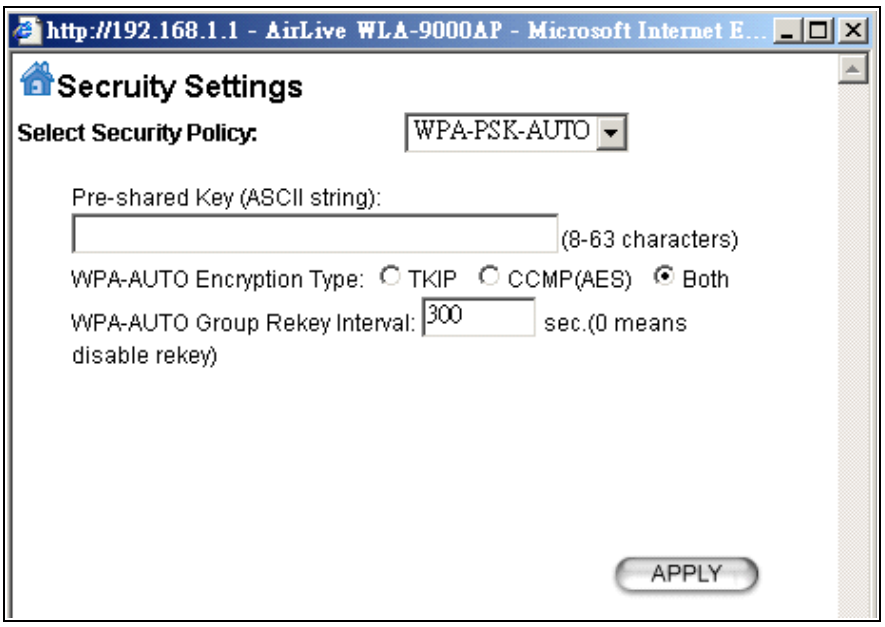


Encryption Type: There are two encryption types **TKIP** and **CCMP (AES)**. While CCMP provides better security than TKIP, some wireless client stations may not be equipped with the hardware to support it. You can select **Both** to allow TKIP clients and CCMP clients to connect to the Access Point 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-AUTO

WPA-PSK-AUTO tries to authenticate wireless clients using WPA-PSK or WPA2-PSK.



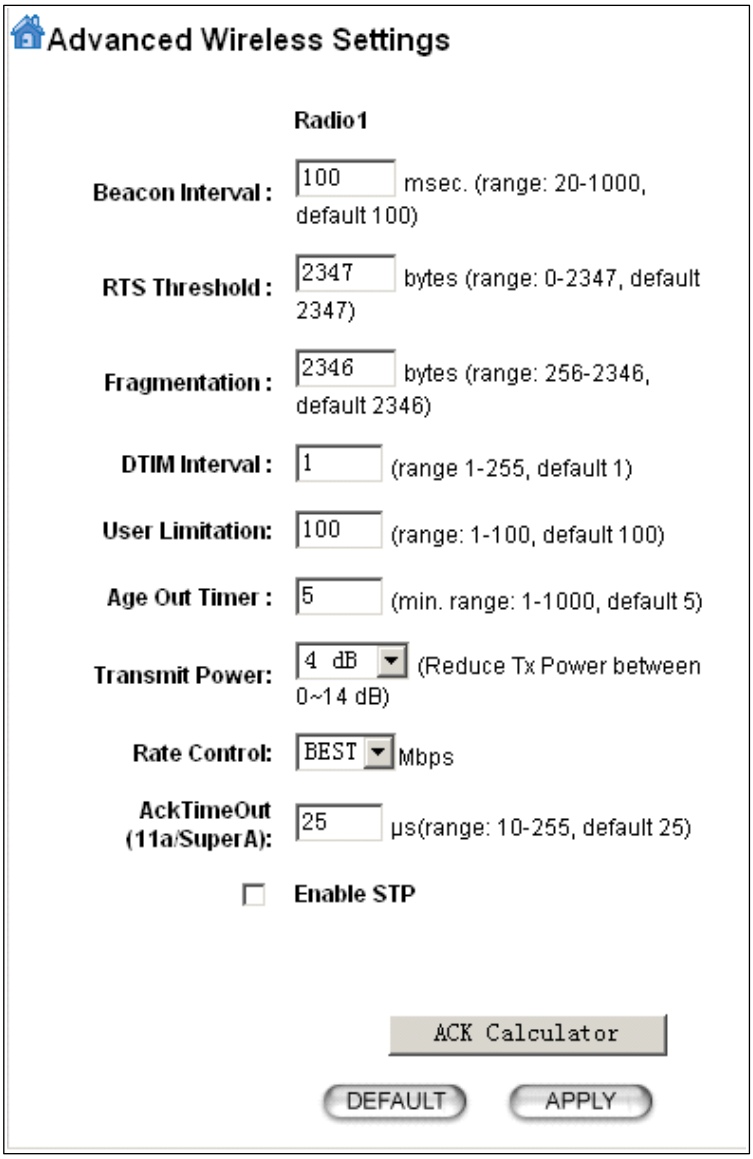
Pre-shared Key: This is an ASCII string with 8 to 63 characters. Please make sure that both the WH-9200AP and the wireless client stations use the same key.

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.

2.3 Advanced Wireless Settings

When click on Advanced Setup button under client mode, a pop-up window appears and show parameter as follow:



Beacon Interval: The WH-9200AP broadcasts beacon frames regularly to announce its existence. The beacon Interval specifies how often beacon frames are transmitted in time unit of milliseconds.

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.

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.

DTIM Interval: The WH-9200AP 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.

User Limitation: The range of user limitation is from 1 to 100.

Age Out Timer: Set the age out time. The default is 300 sec.

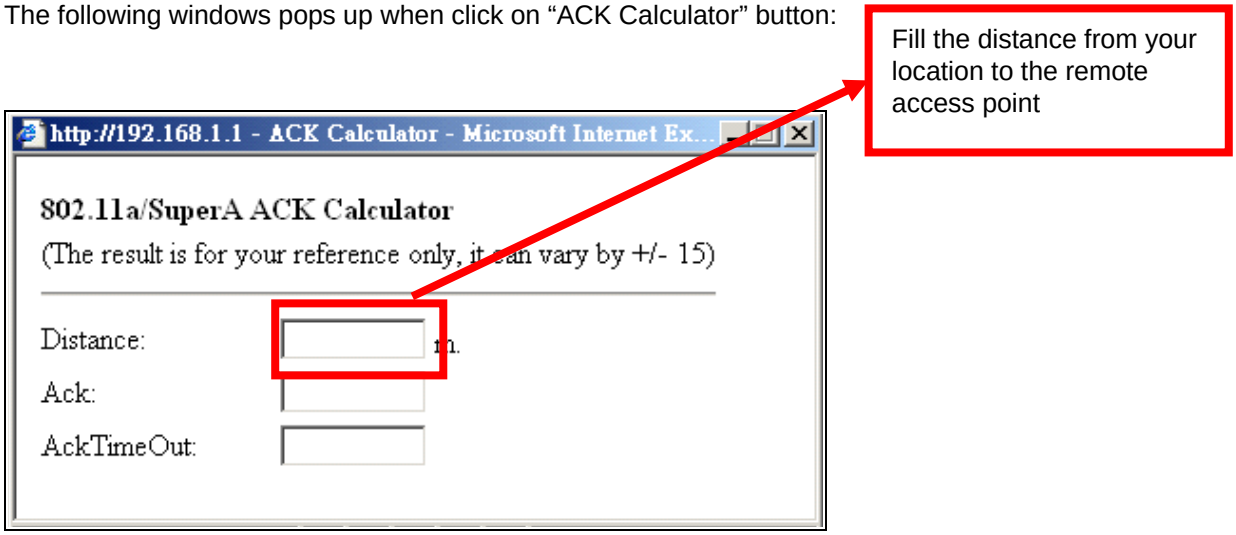
Transmit Power: Transmit power output depends upon the size and RF characteristics because that will determine the number of APs, channels, and need for antennas.

Rate Control: Limit the wireless data rate to the selected number.

Enable STP: Spanning Tree Protocol prevents the condition known as a bridge loop.

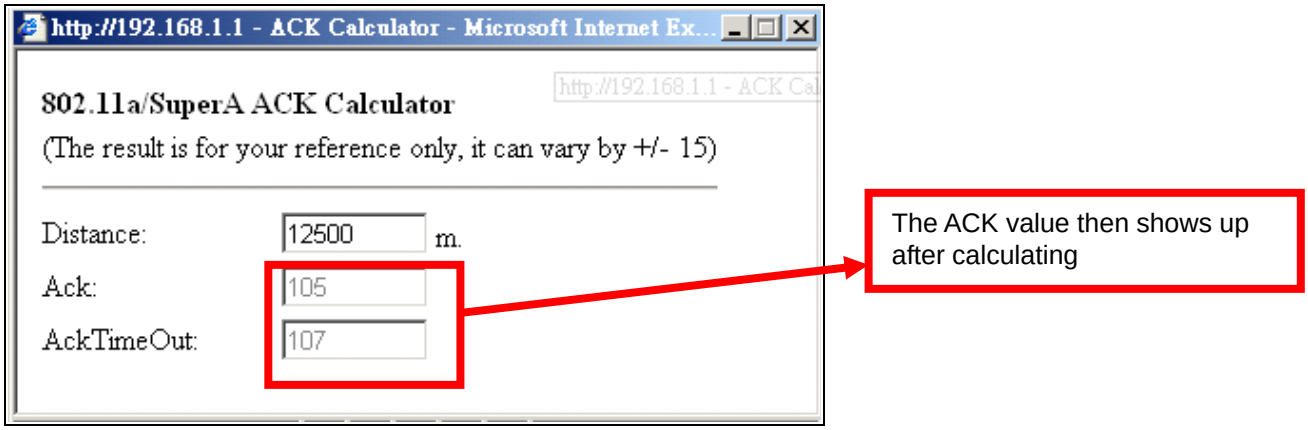
Ack TimeOut: The **"ACK time-out"** determines how long the program waits after receiving a packet from a file stream to determine that stream to be a complete file.

The following windows pops up when click on “ACK Calculator” button:

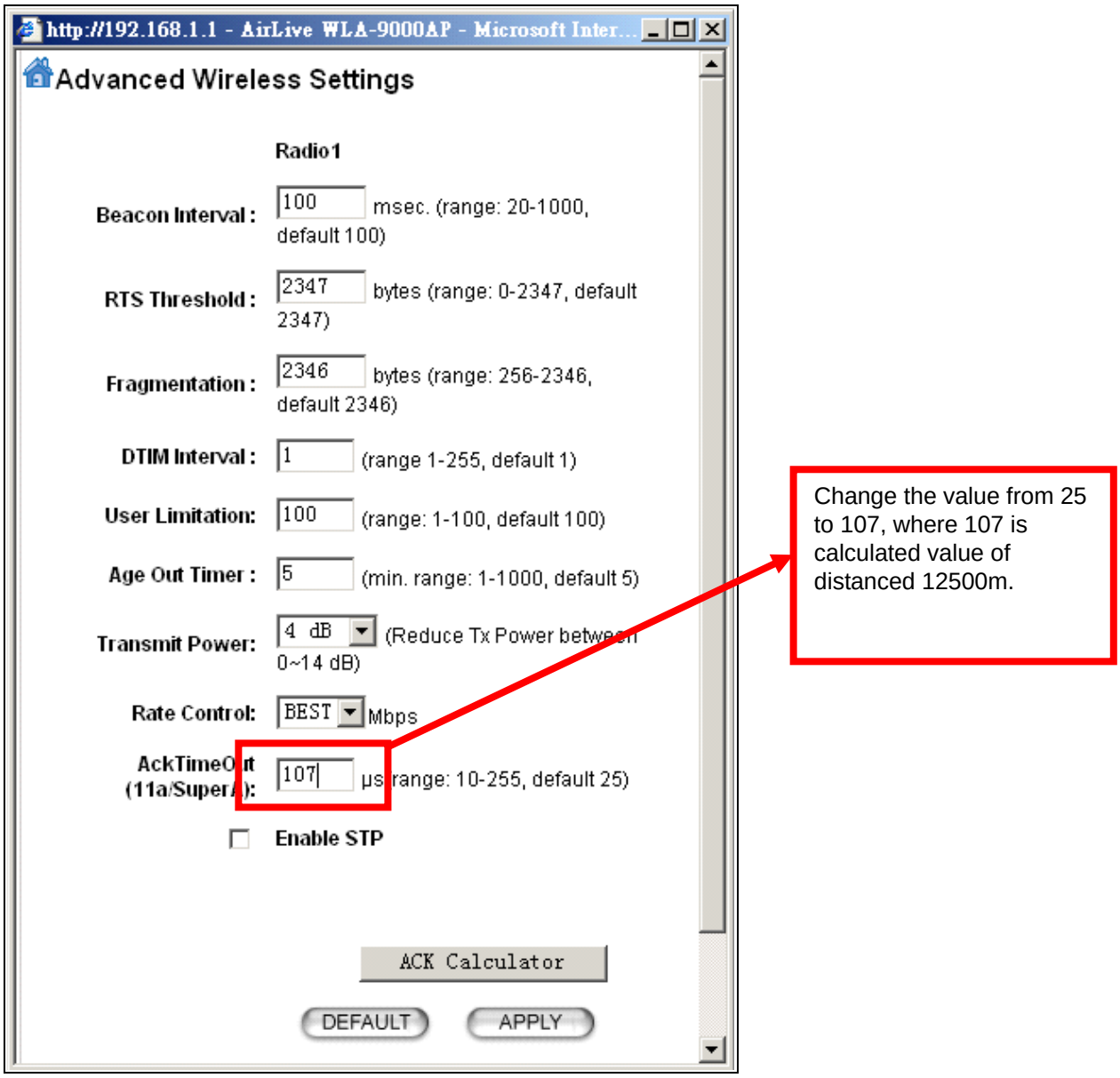


In the field of **“Distance”**, input the distance in **“meters”**.

After input the distance value, move the cursor to any place on the pop-up window out of three fields. The calculated value will display.



Enter the calculated value of **"AckTimeOut"** into the appropriate **"Ack TimeOut"** field (11a or 11g) in the **"Advanced Wireless Settings"** window.



3. System Management

You can review the Device information of your WH-9200AP by the interface. The information shows the current firmware version, IP address of your WH-9200AP.

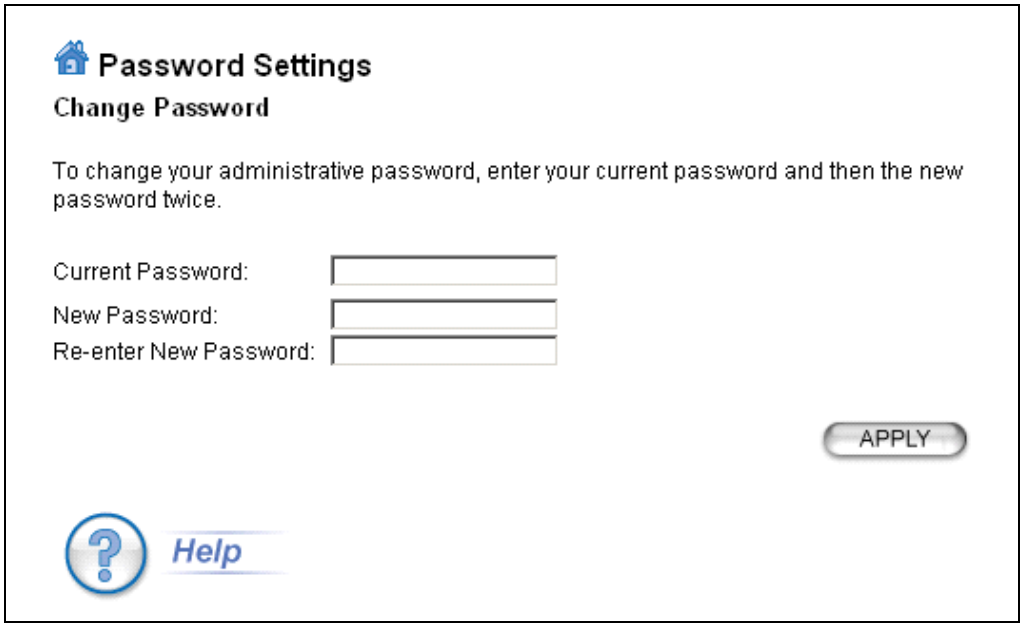
Wireless1 MAC and **Wireless2 MAC** show the MAC address of the two radios, the information helps to setup WDS connection by remote access point.

The **Uptime** records the live time of WH-9200AP after boot.

dd: day; **hh:** hour; **mm:** minute

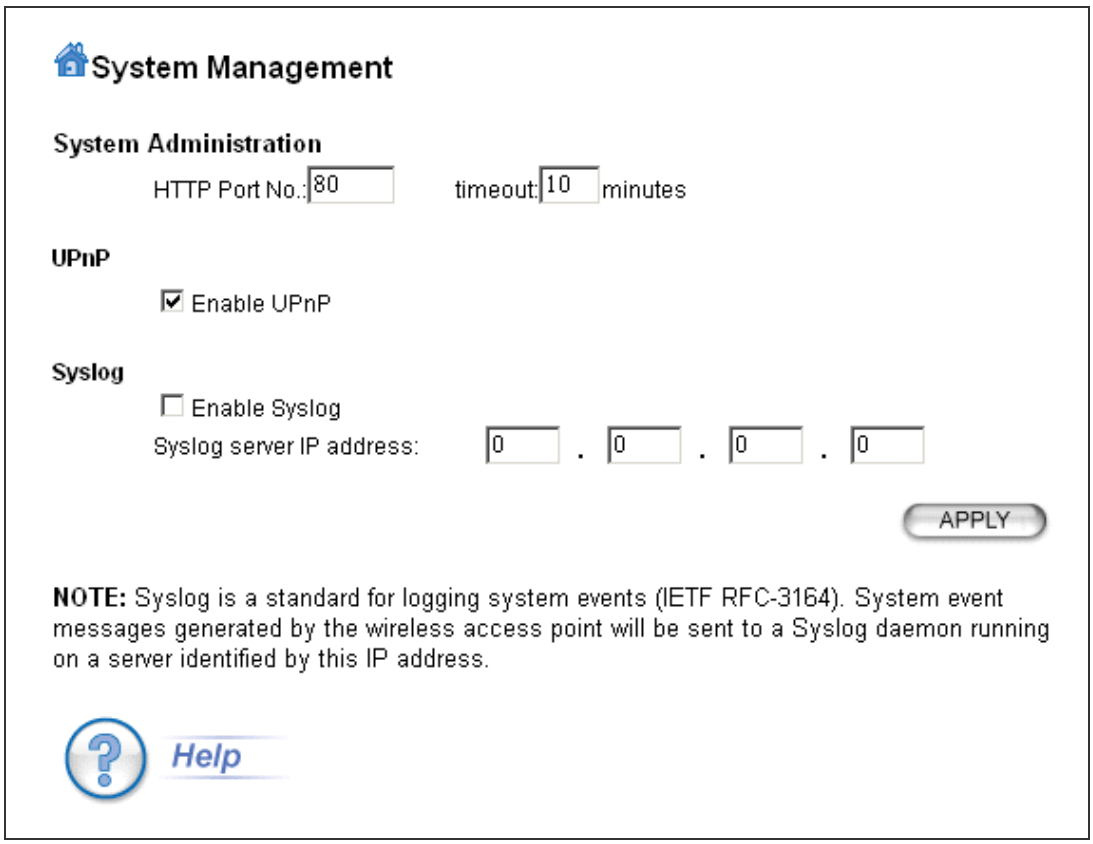
3.1 Change Password

It's recommended to set your own password instead of using default factory password. The default factory password is "**airlive**" all letters are in lower case. To change the password, press the **Password Settings** button to enter the **Password Settings** screen; then enter the Current Password followed by the New Password twice. The entered characters will appear as asterisks



3.2 System Management Settings

The WH-9200AP allow you to change the parameter of manage the system.



HTTP Port No.: This is to change the management web port of WH-9200AP. By default, the port number is 80 and we type http://192.168.1.1 in the browser to access the management web page. If we change the port to another, say, 90, then we need to type http://192.168.1.1:90 instead. This prevents unwelcome access to the management interface.

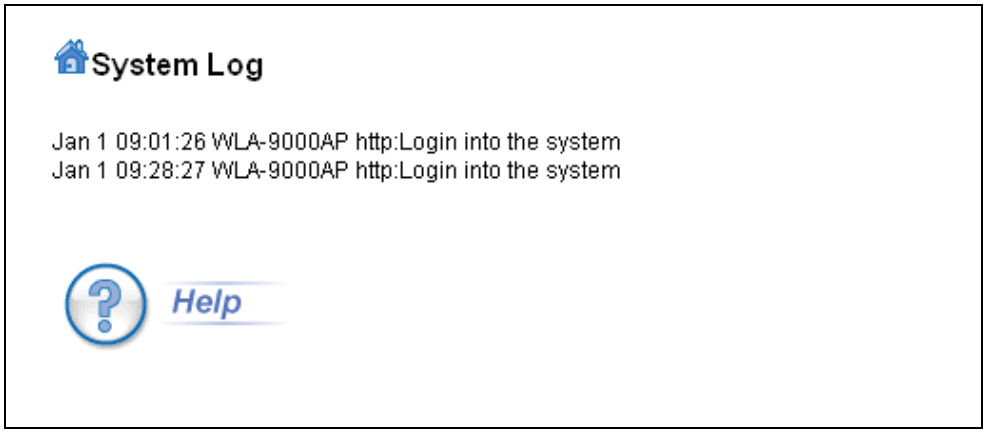
Time-out: The default is 10 minutes. If you idle on the web management interface more than 10 minutes, the system log you out and you need to login again.

UPnP: The Universal Plug and Play (UPnP) feature allows a Windows XP/ME PC to discover this WH-9200AP and automatically show an icon on the screen. Then a user can double-click the icon to access this device directly (without having to find out its IP address).

Syslog: If the Syslog is Enabled, WH-9200AP create a log in the system log table when encounters an error or warning condition. This apply to IETF (Internet Engineering Task Force - the Internet standards body)-conformant standard for logging system events (RFC-3164)

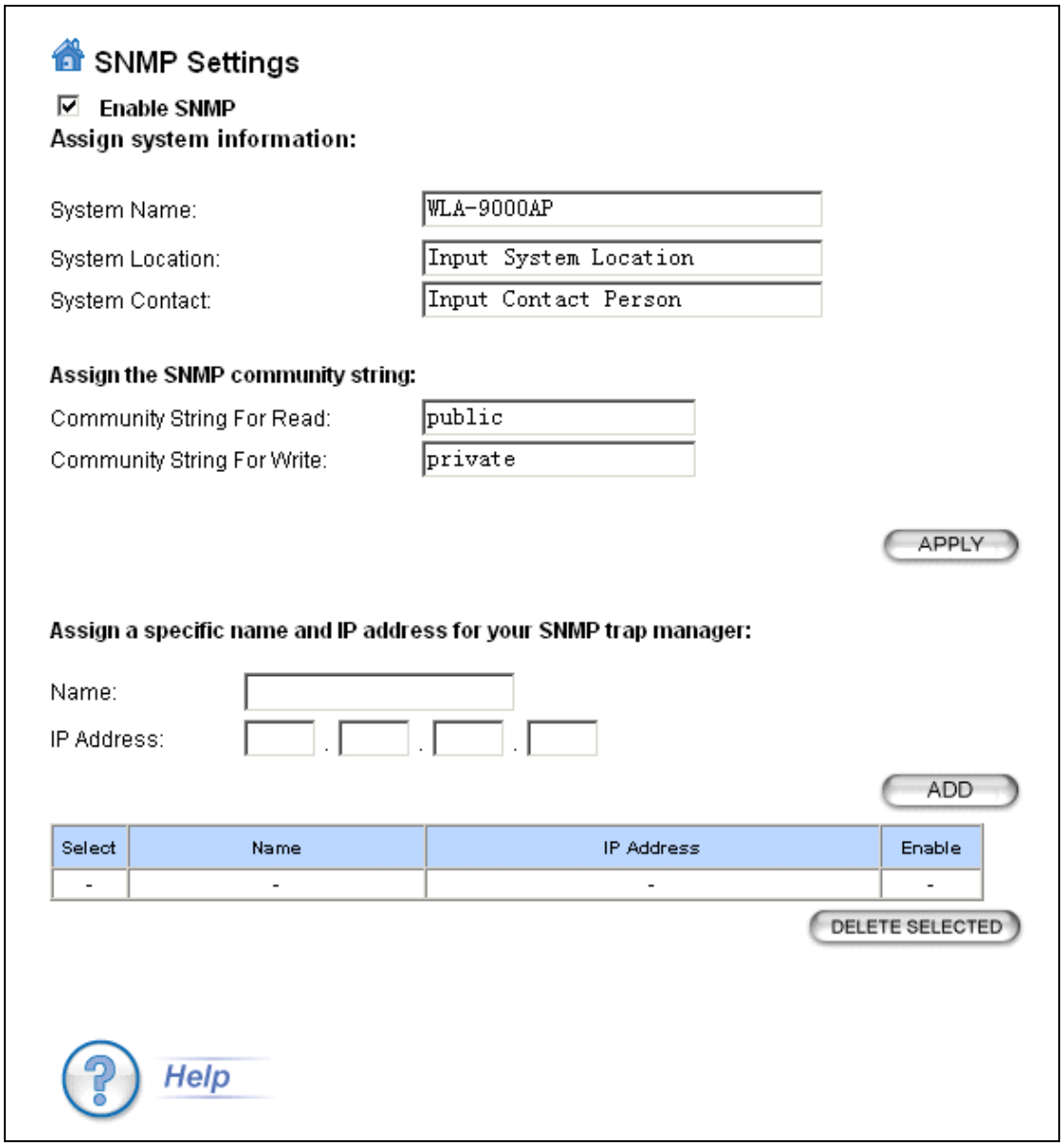
Syslog server IP address: The Syslog can also send to the identified IP address.

The system log shows in WH-9200AP:



3.3 SNMP Settings

WH-9200AP can also be managed by remote software with SNMP (simple network management protocol) protocol.



System Name: A name that you assign to your WH-9200AP for SNMP software. It is an alphanumeric string of up to 30 characters.

System Location: Enter a system location. Information for SNMP software.

System Contact: Contact information for the system administrator responsible for managing your WH-9200AP. 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”.

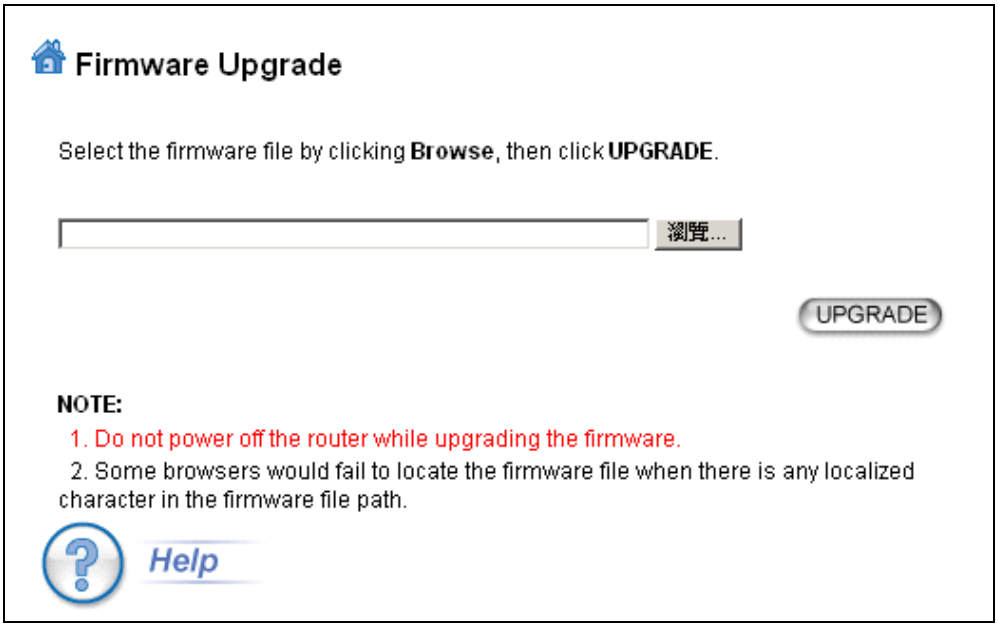
Assign a specific name and IP address for your SNMP trap manager:
A trap manager is a remote SNMP management station where special SNMP trap messages are generated (by the router) and sent to in the network.
You can define trap managers in the system.
You can add a trap manager by entering a **name**, 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.

Some extra feature of WH-9200AP does not show in the wizard because some higher knowledge of parameters of them is required. They are classified in the tab of “Advances Setting”, such as the Multi SSID for VLAN setting and 802.11e QoS configuration.

3.4 Firmware Upgrade

You can upgrade the firmware of your WH-9200AP (the software that controls your WH-9200AP'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. System upgrade can be performed through the System Upgrade window as follows:



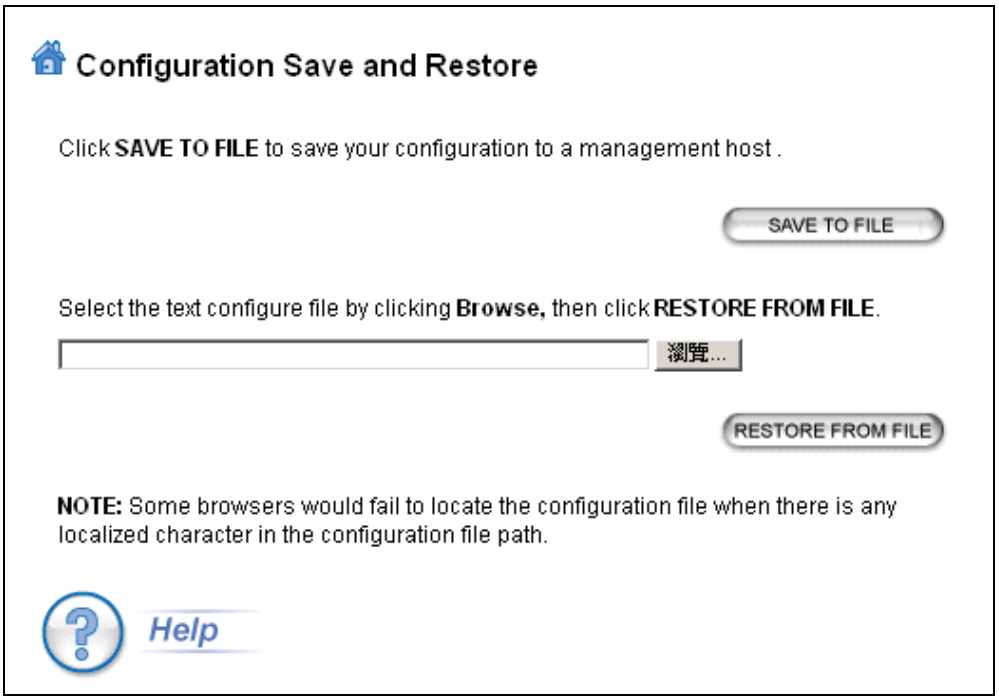
To update the WH-9200AP firmware, first download the firmware from the distributor's web site to your local disk, and then from the above screen enter the path and filename of the firmware file (or click **Browse** to locate the firmware file). Next, Click the **Upgrade** button to start.

The new firmware will be loaded to your WH-9200AP. 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 WH-9200AP unless the new firmware has new features you need or if it has a fix to a problem that you've encountered.

3.5 Configuration Save and Restore

In this interface, you can backup your system configuration to PC and restore your saved configuration file to the WH-9200AP.

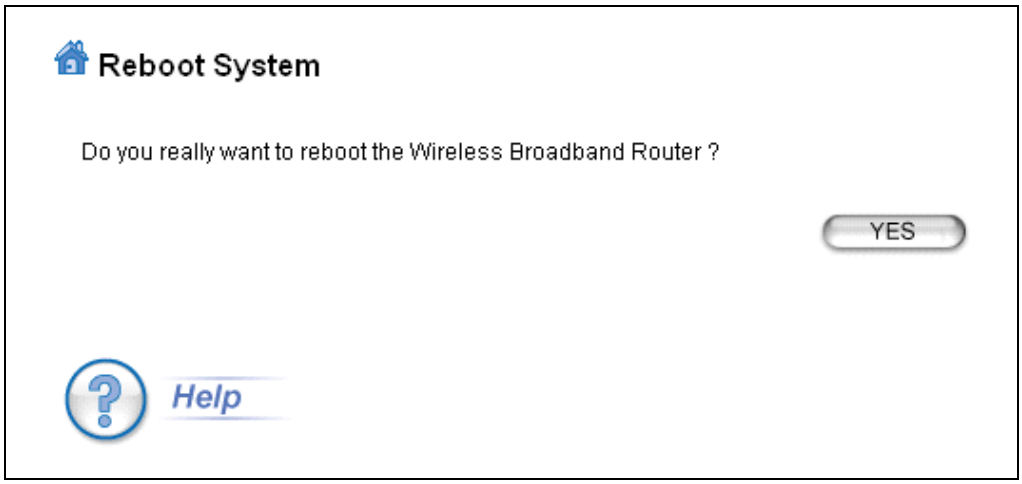


To save the configuration to your PC, click the **"SAVE TO FILE"** button and the system will lead you to save the configuration file to your PC.

To restore configure file to WH-9200AP, click the **"Browse"** button, find the saved configuration fire, then click **"RESTORE FROM FILE"** button to restore.

3.6 Reboot System

The following interface allows you to reboot your WH-9200AP. Click **"Yes"** button to reboot.

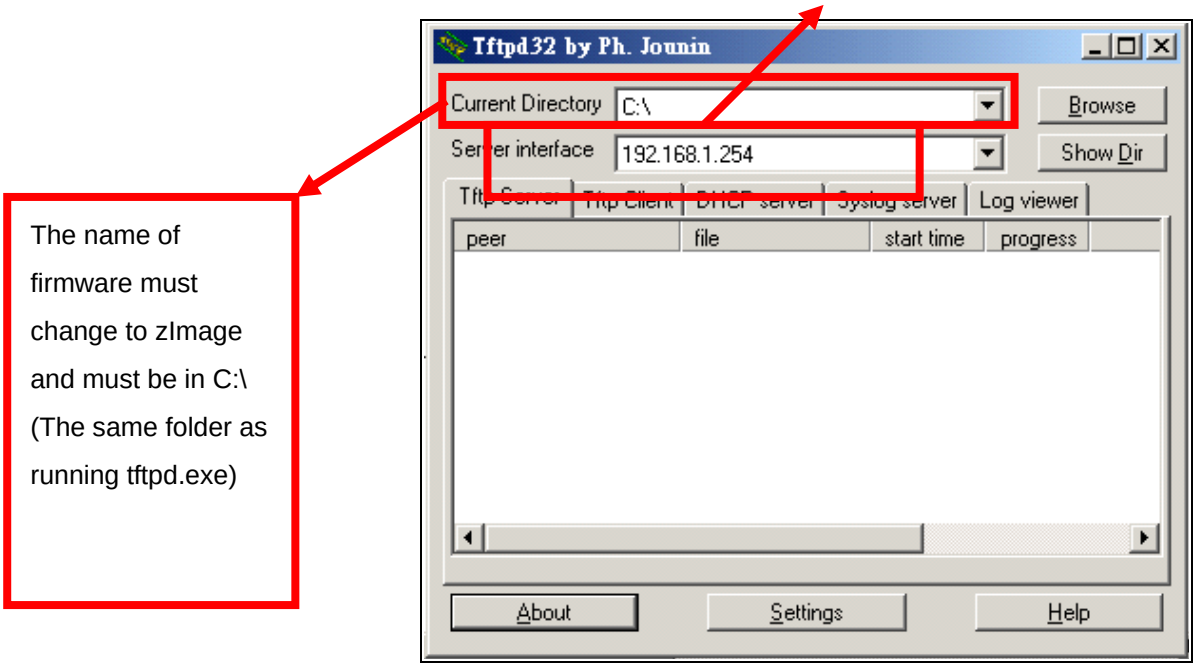


You can also reboot WH-9200AP by power off and power on it.

3.7 WH-9200AP Emergency Recovery

This document guides to recover your WH-9200AP 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 WH-9200AP firmware to C:\ and rename the firmware to **"zImage"**. Note that the name must be zImage and no extension.
5. Connect WH-9200AP and PC with an Ethernet cable.
6. Run the tftpd32.exe. Note that the IP address must be 192.168.1.254.



7. Power on WH-9200AP, 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 WH-9200AP 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 WH-9200AP boots up automatically.
12. Try access 192.168.1.1, or the IP address you had changed before.
13. Repeat the processes again if failed.