Air Live®
Powered by OvisLink Corp.

WH-5420CPE

Hi-Powered Wireless
Outdoor CPE

User's Manual

www.airlive.com

Declaration of Conformity

We, Manufacturer/Importer

OvisLink Corp.
5F., NO.6, Lane 130, Min-Chuan Rd.,
Hsin-Tien City, Taipei County, Taiwan

Declare that the product

Hi-Powered Wireless Outdoor CPE
AirLive WH-5420CPE

is in conformity with

In accordance with 2004/108/EC Directive and 1999/5 EC-R & TTE Directive

Clause	Description
■ **EN 300 328 v1.6.1 (2004-11)**	Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband transmission equipment operating in the 2.4GHz ISM band And using spread spectrum modulation techniques; Part 1：technical Characteristics and test conditions Part2：Harmonized EN covering Essential requirements under article 3.2 of the R&TTE Directive
■ **EN 301 489-01 V1.6.1 (2005-09)** ■ **EN 301 489-17 V1.2.1 (2002-08)**	Electromagnetic compatibility and Radio spectrum Matters (ERM); Electromagnetic compatibility(EMC) standard for radio equipment and Services; Part 17：Specific conditions for wideband data and HIPERLAN equipment
■ **EN 50383:2002**	Basic standard for the calculation and measurement of electromagnetic field strength and SAR related to human exposure from radio base stations and fixed terminal stations for wireless telecommunication systems (110 MHz – 40 GHz).
■ **EN 60950-1:2001/A11 :2004**	Safety for information technology equipment including electrical business equipment
■ **CE marking**	CE ①

Manufacturer/Importer

Signature : Albert Yeh

Name : **Albert Yeh**

Position/ Title： **Vice President** (Stamp) Date： **2008/10/1**

AirLive WH-5420CPE CE Declaration Statement

Country	Declaration	Country	Declaration
cs Česky [Czech]	OvisLink Corp. tímto prohlašuje, že tento AirLive WH-5420CPE je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.	**lt** Lietuvių [Lithuanian]	Šiuo OvisLink Corp. deklaruoja, kad šis AirLive WH-5420CPE atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
da Dansk [Danish]	Undertegnede OvisLink Corp. erklærer herved, at følgende udstyr AirLive WH-5420CPE overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.	**nl** Nederlands [Dutch	Hierbij verklaart OvisLink Corp. dat het toestel AirLive WH-5420CPE in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
de Deutsch [German]	Hiermit erklärt OvisLink Corp., dass sich das Gerät AirLive WH-5420CPE in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.	**mt** Malti [Maltese]	Hawnhekk, OvisLink Corp, jiddikjara li dan AirLive WH-5420CPE jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
et Eesti [Estonian]	Käesolevaga kinnitab OvisLink Corp. seadme AirLive WH-5420CPE vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.	**hu** Magyar [Hungarian]	Az OvisLink Corporation kijelenti, hogy az AirLive WH-5420CPE megfelel az 1999/05/CE irányelv alapvető követelményeinek és egyéb vonatkozó rendelkezéseinek.
en English	Hereby, OvisLink Corp., declares that this AirLive WH-5420CPE is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.	**pl** Polski [Polish]	Niniejszym OvisLink Corp oświadcza, że AirLive WH-5420CPE jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
es Español [Spanish]	Por medio de la presente OvisLink Corp. declara que el AirLive WH-5420CPE cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.	**pt** Português [Portuguese]	OvisLink Corp declara que este AirLive WH-5420CPE está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
el Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ OvisLink Corp. ΔΗΛΩΝΕΙ ΟΤΙ AirLive WH-5420CPE ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.	**sl** Slovensko [Slovenian]	OvisLink Corp izjavlja, da je ta AirLive WH-5420CPE v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
fr Français [French]	Par la présente OvisLink Corp. déclare que l'appareil AirLive WH-5420CPE est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE	**sk** Slovensky [Slovak]	OvisLink Corp týmto vyhlasuje, že AirLive WH-5420CPE spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
it Italiano [Italian]	Con la presente OvisLink Corp. dichiara che questo AirLive WH-5420CPE è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.	**fi** Suomi [Finnish]	OvisLink Corp vakuuttaa täten että AirLive WH-5420CPE tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen
lv Latviski [Latvian]	Ar šo OvisLink Corp. deklarē, ka AirLive WH-5420CPE atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.	Íslenska [Icelandic]	Hér með lýsir OvisLink Corp yfir því að AirLive WH-5420CPE er í samræmi við grunnkröfur og aðrar kröfur, sem gerðar eru í tilskipun 1999/5/EC.
sv Svenska [Swedish]	Härmed intygar OvisLink Corp. att denna AirLive WH-5420CPE står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.	**no** Norsk [Norwegian]	OvisLink Corp erklærer herved at utstyret AirLive WH-5420CPE er i samsvar med de grunnleggende krav og øvrige relevante krav i direktiv 1999/5/EF.

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

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

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

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.

Copyright Statement

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, whether electronic, mechanical, photocopying, recording or otherwise without the written consent of OvisLink Corp.
Windows™ 95/98 and Windows™ 2000 are trademarks of Microsoft® Corp.
Pentium is trademark of Intel.

All copyright reserved.

Table of Contents

Chapter1. Introduction 4

1.1 Overview 4

1.2 Firmware Features 5

1.3 Installing WH-5420CPE 8

1.3.1 Package Content 8

1.3.3 Mounting Configuration 11

1.3.4 Antenna polarization 12

1.3.5 Configuration steps 13

1.3.6 Set up a wireless client as a DHCP client 14

1.3.7 Configuration Setups 16

2. Operation Mode 17

2.0 Change Operation Mode 18

2.1 About the Operation Modes 18

2.1 About the Operation Modes 19

2.1.1 Access Point Mode 19

2.1.2 Client Mode 20

2.1.3 Bridge Mode 21

2.1.4 WDS Repeater 22

2.1.5 Universal Repeater 23

2.1.6 WISP (Client Router) mode 24

2.1.7 WISP + Universal Repeater mode 25

2.1.8 Gateway (AP + Router) 26

3. Wireless Settings 27

3.1 Access Point Mode Settings 27

3.2 Client Mode Settings 29

3.3 Bridge Mode Settings 31

3.4 WDS Repeater Mode Settings 33

3.5 Universal Repeater Mode Settings 37

3.6 WISP Mode Settings 39

3.7 WISP + Universal Mode Settings 43

3.8 Gateway Mode (AP + Router) Settings 48

3.9 Wireless Security 53

3.10 Advanced Wireless Settings 58

3.11 Access Control 61

3.12 QoS Traffic Control 62

4. System Management 72

4.1 LAN Interface Setup 72

4.2 Upgrade Firmware 74

4.3 Save / Reload Settings 75

4.4 Change Password 77
4.5 Enable System Log 78
4.6 NTP Settings 79
5. System Status 80
5.1 System Data 80
5.2 Statistics 80
5.3 Active Clients 81
6 System Recovery 83
7. Specification 84
Appendix Command Line Management 86

Chapter1. Introduction

1.1 Overview

The WH-5420CPE is a outdoor wireless CPE based on IEEE 802.11g 2.4-GHz radio technologies. It contains an 802.11g wireless interface and one half/full-duplex 10/100 LAN interface. Moreover, WH-5420CPE features a total of 8 wireless modes: Access Point, Universal Repeater, WDS Repeater, WDS Bridge, Wireless Client, WISP (Client Router), WISP + Universal Repeater and Gateway.
The web-based management utility is provided for easy configuration that your wireless network connection is ensured to be always solid and hassle free.

Wireless Client Isolation
The WH-5420CPE features the new Wireless Client Isolation function previous available only in more expensive APs. When you enable this function, the wireless clients will not be able to see each other. Therefore, it is an important function for office and Hotspot operator to protect the security between different wireless users.

ACK Timeout and TX Power Regulation
The WH-5420CPE features ACK timeout function to let you adjust the timeout value for long distance operation. In addition, 6-level TX power adjustment let you match different antennas for law compliance. The ability to set lower TX output power is also crucial if you want to match the AP with external power amplifier.

Extended Security Features
AirLive WH-5420CPE provides 64/128bit WEP encryption, WPA and IEEE802.1x which ensures a high level of security to protect users' data and privacy. The MAC Address filter prevents the unauthorized MAC Addresses from accessing your Wireless LAN. Your network security is therefore double assured.

Whether it's for office or home environment, the AirLive 802.11g family brings you the maximum performance and security for today's high speed wireless network.

1.2 Firmware Features

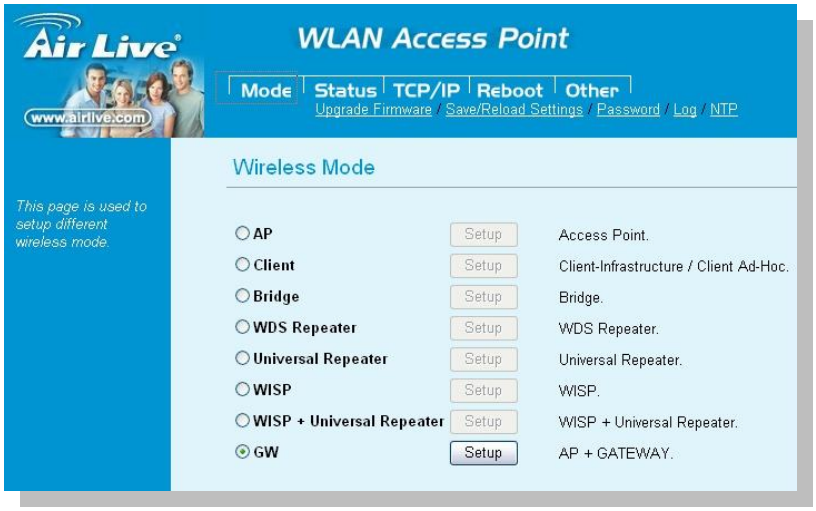
AirLive Wireless AP Firmware Features

The Most Powerful AP Firmware Ever!

WH-5420CPE

As the leading global WISP solution provider, AirLive understands the application environments of WISP operators. As a result, we are constantly upgrading our AP's firmware to meet the changing demand of WISP operators. The firmware adds high end features not commonly found in the AP of this class. The AirLive multi-function CPEs not only work for long distance application, they work much better than the competitions.

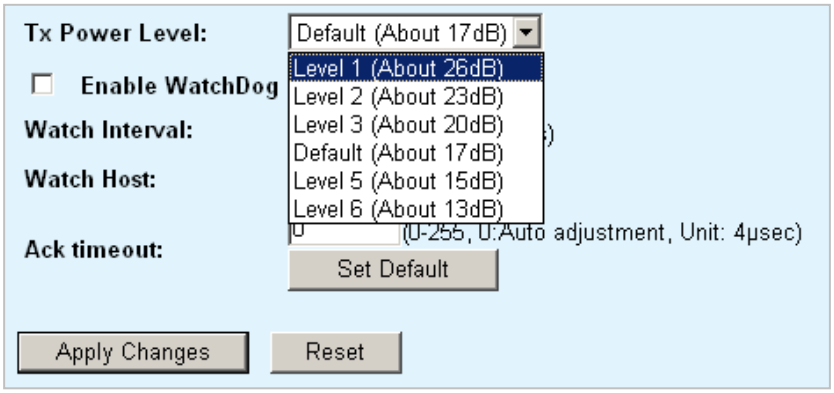
8 Wireless Operation Modes



The AirLive WH-5420CPE can operate in 8 different wireless modes. It can work as a Wireless Router, AP, Client, Repeater, Bridge, and much more. Whether it is for home, office, or WISP; the AirLive AP has a solution for you.

Up to 400mW of Output Power*

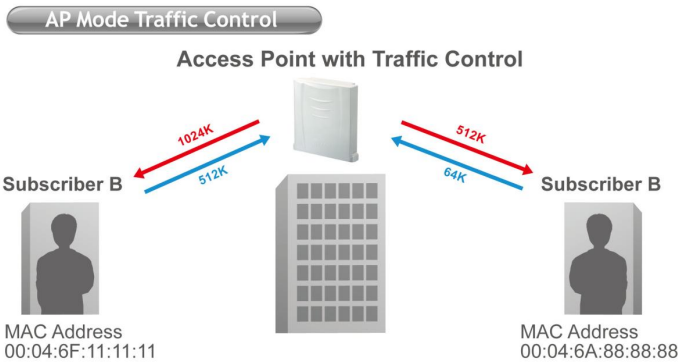
AirLive's high quality hardware let the AP expand its RF output power up to 26dBm using South American firmware. That's 4 times the output power of regular AP! It means much greater distance and coverage.



*** For South America only. Not available for other regions.**

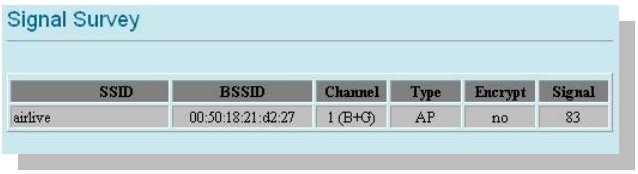
Traffic Control QoS Function

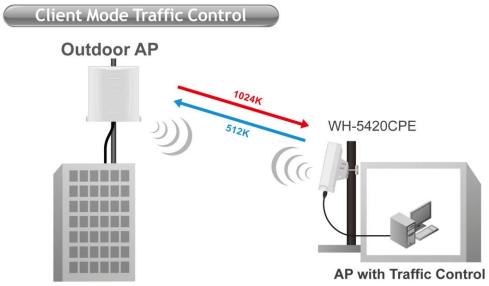
Traffic Control is a great tool to control the bandwidth of the WISP subscribers. Therefore, the WISP operators can offer different class of connection speeds for different subscription fees - just like the ADSL service! The AirLive advance Traffic Control firmware can control the bandwidth by Interface or IP/MAC.



Dynamic Signal Survey Function for Antenna Alignment

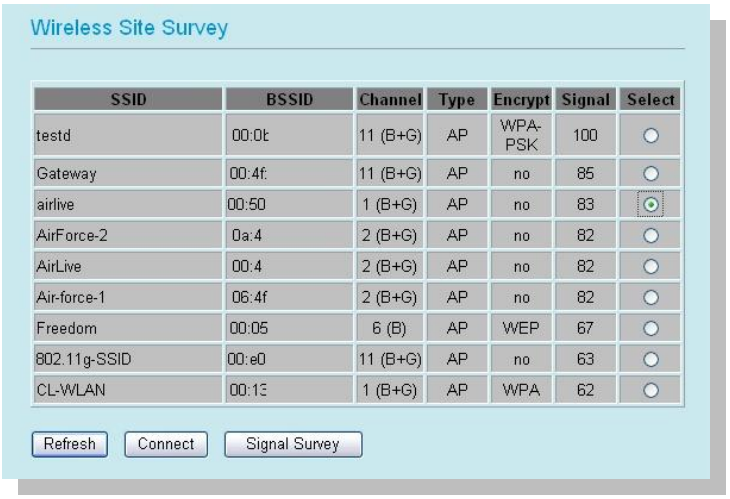
Having trouble align your antenna correctly to the other outdoor AP? The AirLive Wireless Signal Survey function tells you the receiving signal strength dynamically as your antenna turns. It automatically refreshes itself in the process, therefore, making antenna alignment much simpler than before.





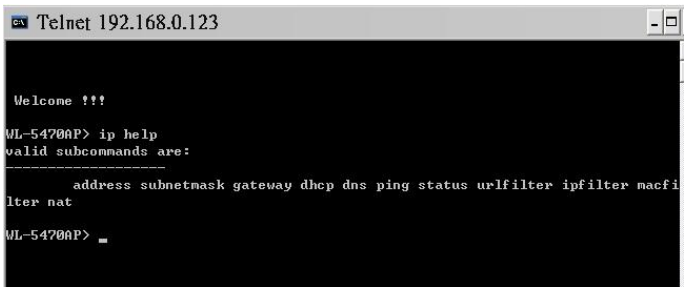
Wireless Site Survey Connection Wizard

During a new WISP service installation, the installer will need to find out which outdoor AP to provide the best signal in the area for connection. The AirLive wireless site survey function provides one step setup for this process. First, the site survey page shows which AP has the strongest the signal. Then the installer performs antenna alignment by using the signal survey function. At last, the installer simply clicks on "connect" button to establish connection. The site survey is available even in AP mode, so the installer can check the channels used by surrounding APs to avoid interferences.



Telnet Function

Some WISP operators prefer to use CLI command line for configurations. The firmware provides full command line feature via Telnet.

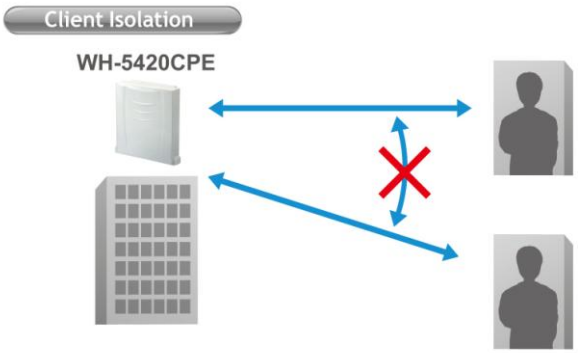


SSH login

WH-5420CPE provides SSH secure connection for remote management. The program SSH (Secure Shell) is a secure replacement for telnet. It provides an encrypted channel for logging into WL-5420POE over a network, executing commands on WH-5420CPE from your workstation. SSH provides strong host-to-host and user authentication as well as secure encrypted communications over an insecure Internet.

Wireless Client Isolation

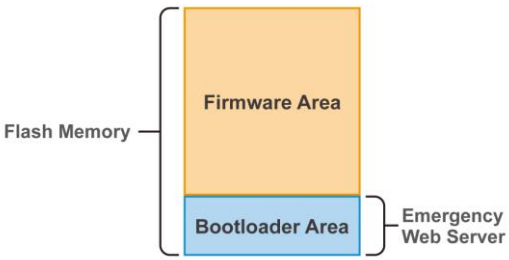
AirLive firmware's ***Client Isolation*** function protects the security and privacy of each individual subscriber. Therefore, subscriber does not need to worry about hacker attacks in the same wireless network.



Emergency Recovery

How many times your machine crashed and lost access completely?

The AirLive's Emergency web server function means you can recover your AP even during if the machine failed during a firmware upgrade. This greatly reduces the service loading for WISP operators.



1.3 Installing WH-5420CPE

This section describes the installation procedure for the WH-5420CPE. 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-5420CPE. Finally, this section explains how to configure a Windows PC to communicate with the WH-5420CPE.

1.3.1 Package Content

The WH-5420CPE package contains the following items:

- ✓ One WH-5420CPE main unit
- ✓ One 48V 0.4A DC power adapter with a splitter
- ✓ Wall Mounting kit
- ✓ One CD of the WH-5420CPE
- ✓ Quick Start Guide

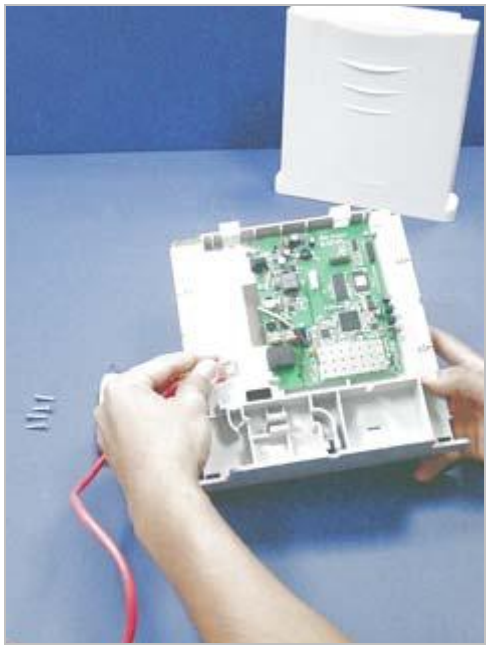
Regarding to the specification of each application, the PoE Ethernet cable is not included in the package.
You may choose outdoor specification Ethernet cable according to the length you need.

1.3.2 Hardware Presentation

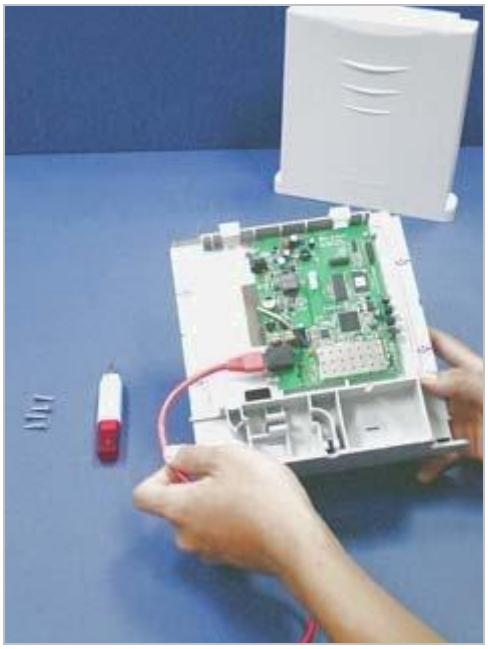
Please take the device unit from the color box, a scroll driver, an Ethernet cable with adequate length according to your application.

Step 1: A scroll driver and Ethernet Cable, four screws and WH-5420CPE main unit

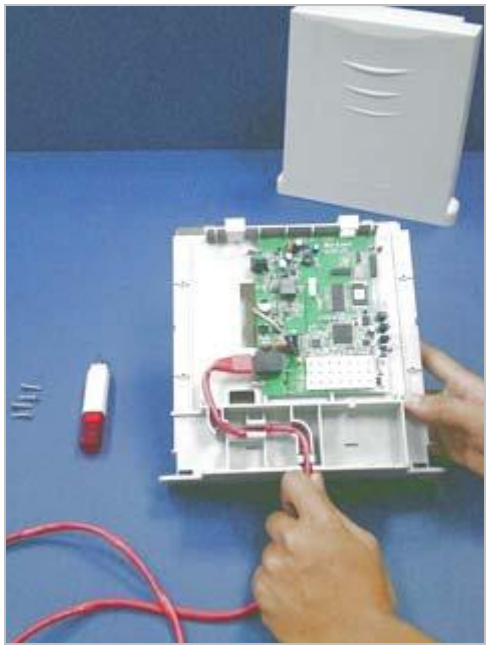
Step 2: Open the housing of WH-5420CPE



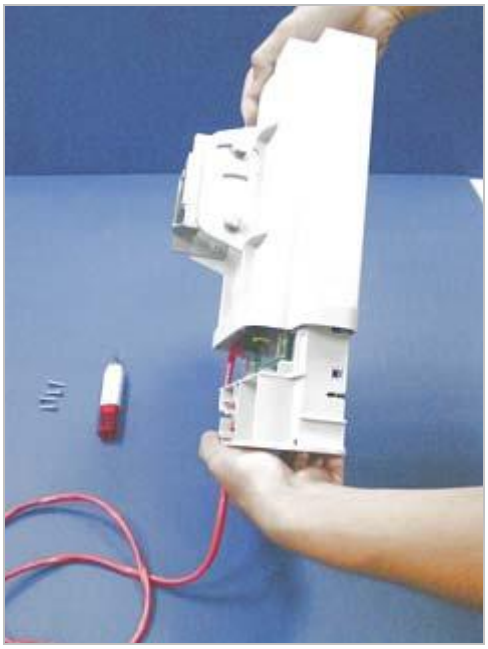
Step 3: Turn the WH-5420CPE to another side, the RJ-45 jack is at the middle of LEFT side of main board.



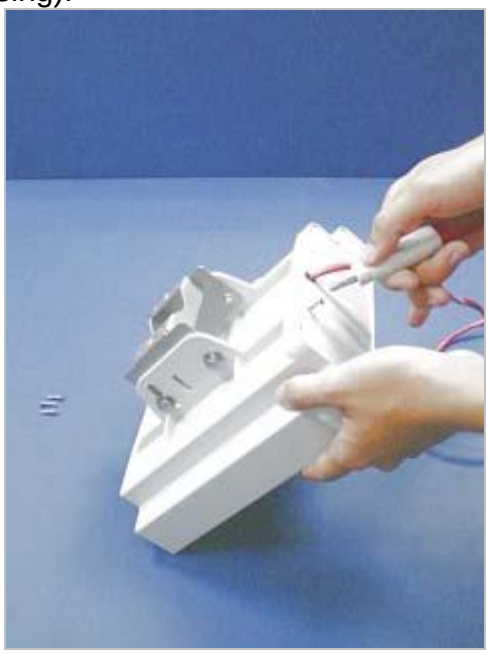
Step 4: Plug one side of RJ-45 cable into the Ethernet port.



Step 5: Put the Ethernet cable along the module, till the exit (at the bottom of Housing).

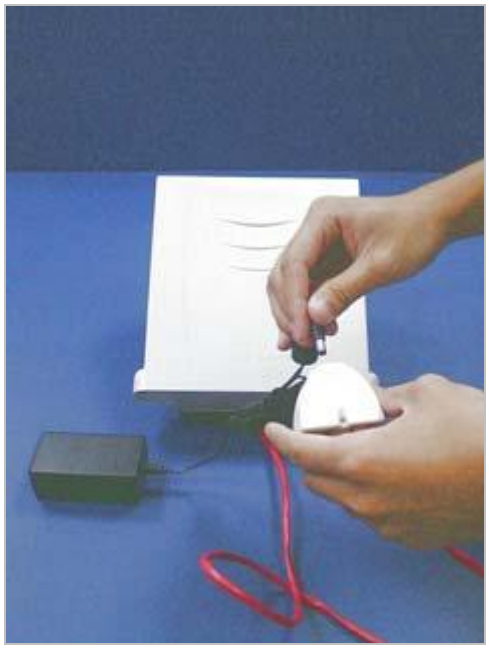


Step 6: Make sure that the other side of Ethernet cable is out of housing. Close the housing.

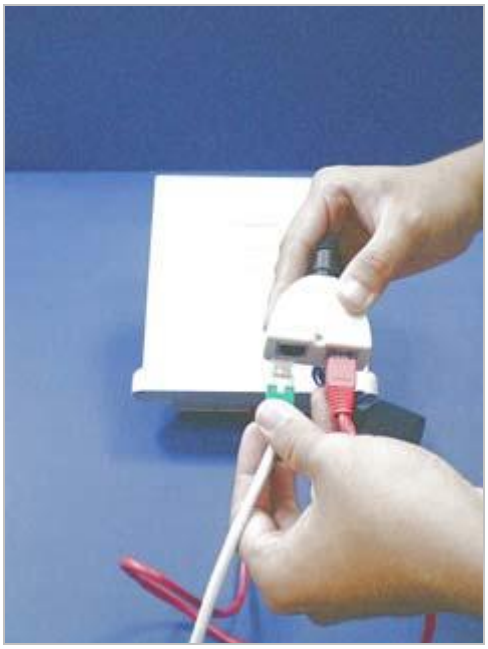


Step 7: Scroll up 4 screws well. Be careful, this is very important; it could protect your device against the water.

Step 8: Plug the Ethernet to the PoE “P + DATA OUT” jack of injector.

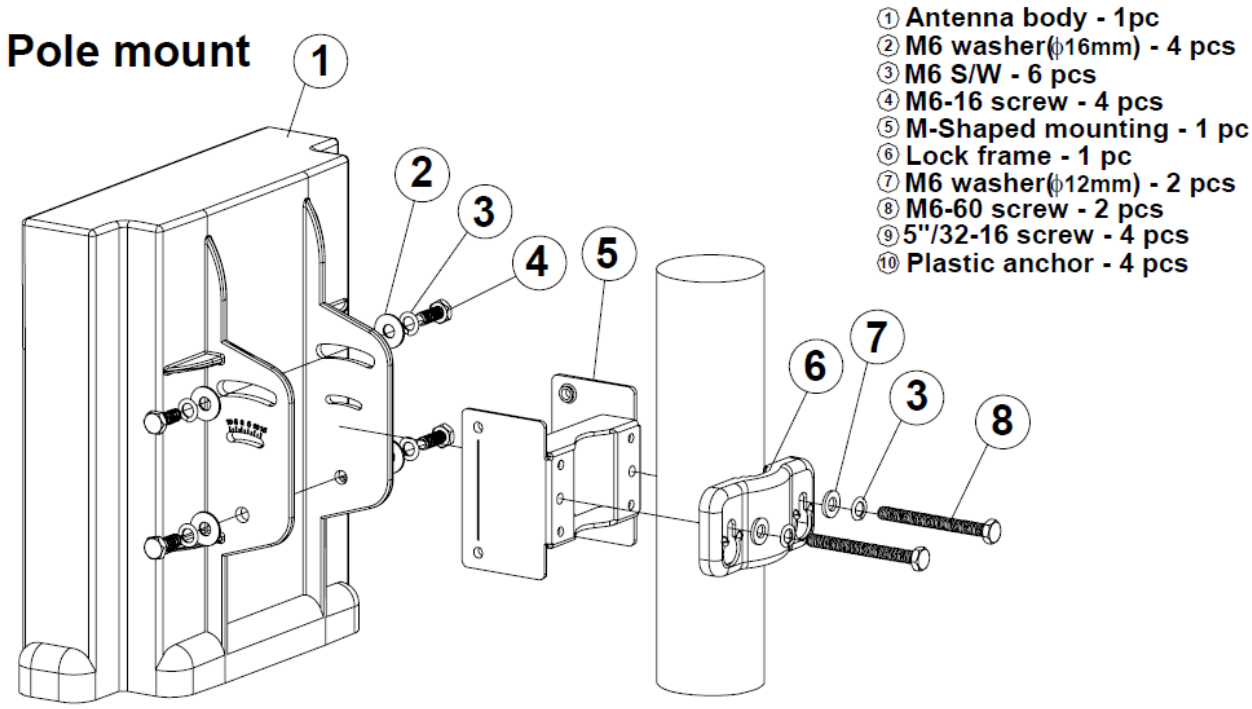


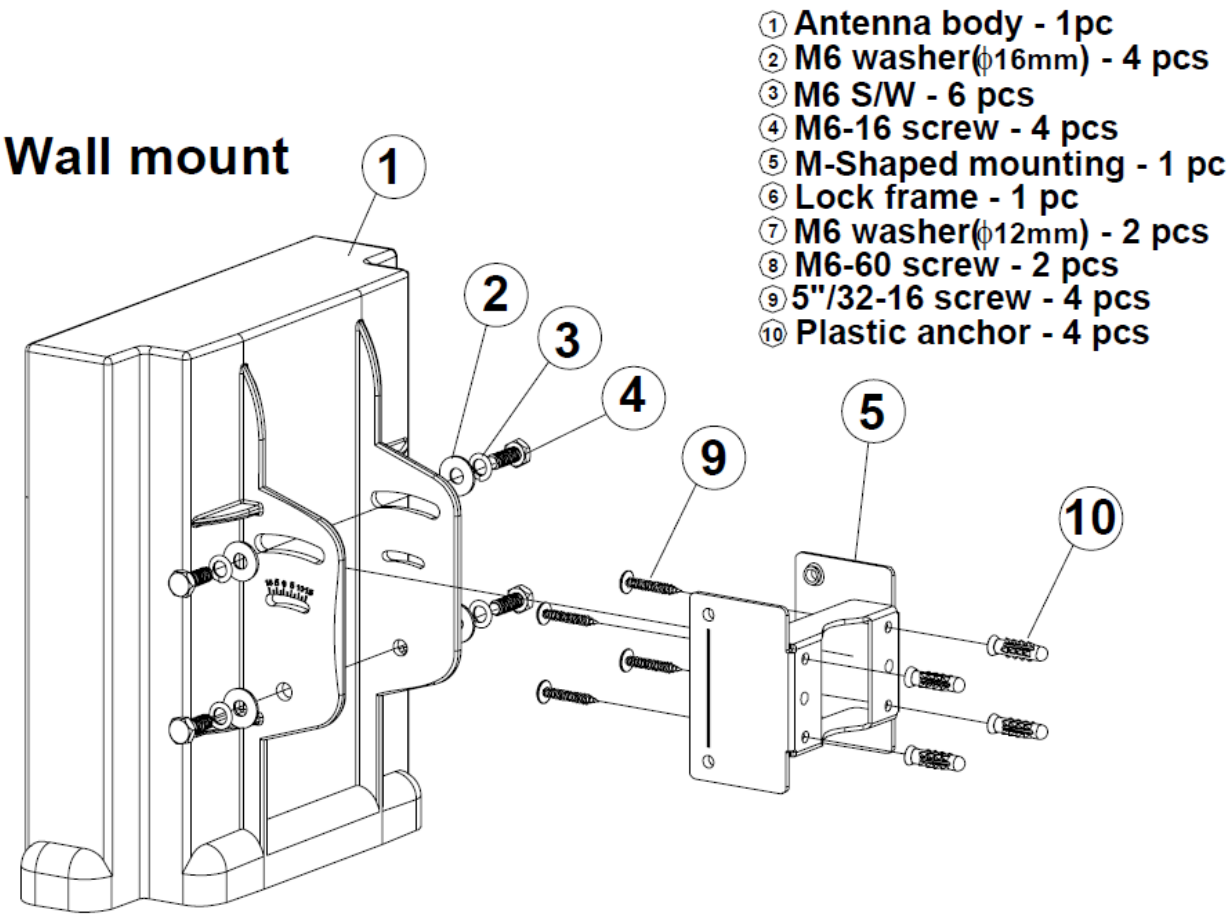
Step 9: Plug the power cord of adaptor into the injector “POWER IN” port.



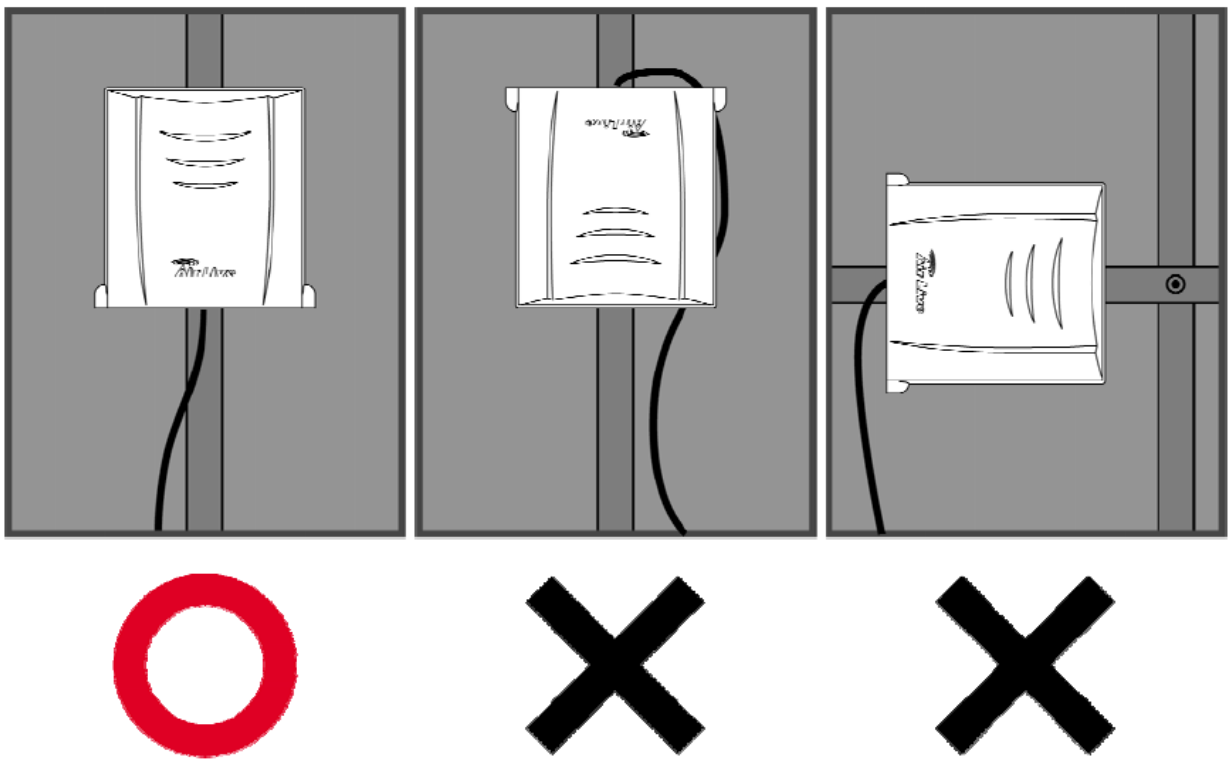
Step 10: Plug the Data Ethernet cable to the port “DATA IN” of injector.

1.3.3 Mounting Configuration

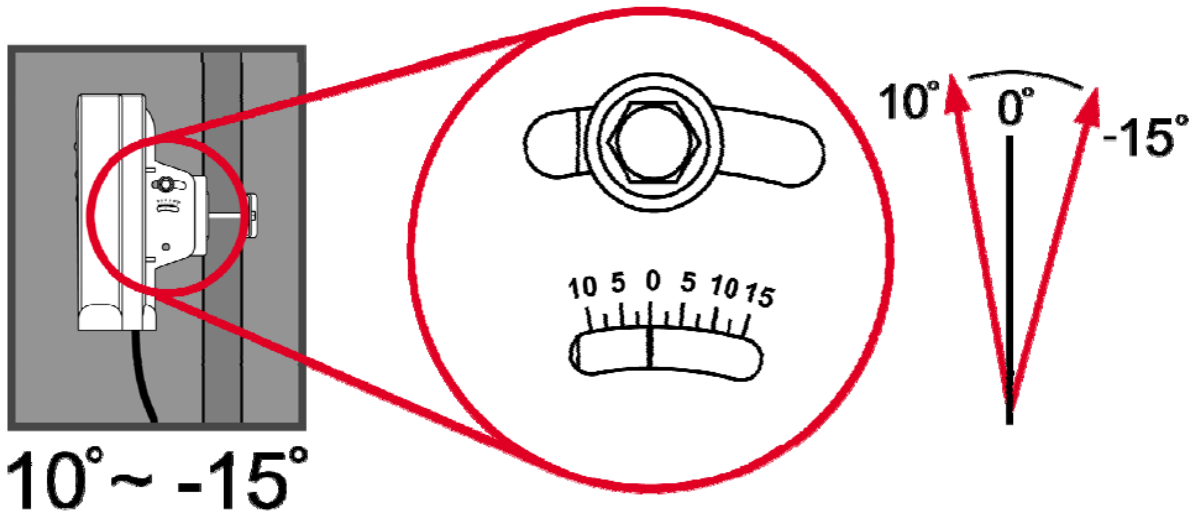




1.3.4 Antenna polarization



Pease install the CPE in the UP RIGHT position only.
Do not put the CPE into water.



Pease do not tilt the CPE more than 15 degree angle from vertical

1.3.5 Configuration steps

This section describes configuration required for the WH-5420CPE before it can work properly in your network.
First, it is assumed that in your LAN environment, a separate DHCP server will be available for assigning dynamic (and often private) IP addresses to requesting DHCP clients. Additionally, since you need to perform various configuration changes to the WH-5420CPE, including the SSID, Channel number, the WEP key, …, etc., it is necessary to associate a fixed IP address with the WH-5420CPE, which is why the WH-5420CPE will be shipped with a factory default private IP address of **192.168.100.252** (and a network mask of 255.255.255.0).
Therefore, during the system installation time, you need to build an isolated environment with the WH-5420CPE and a PC, and then perform the following steps:
Step 1. Manually change the IP address of the PC to become 192.168.100.199.
Step 2. Connect the PC to the WH-5420CPE via PoE and change its configuration to a static IP address based on your network environment. For example, if there is a DHCP server that assigns IP addresses from the range 192.168.23.10 - 192.168.23.254 to DHCP client devices, it can reserve 192.168.23.10 for the WH-5420CPE and then the address pool with the DHCP server becomes 192.168.23.11 – 192.168.23.254.

If there is no DHCP server on your network environment, you just have to make sure that there is no machine in the environment has the same IP address as another machine. Please note that after you change the IP address of the CPE, the PC client may not be able

to reach the CPE. This is because they may no longer belong to the same IP network address space.

Step 3. Change the setting of the PC back to “obtain IP addresses dynamically”. Now you can put the WH-5420CPE and the PC to your network where the DHCP server is connected. From then on, any wireless client configured to “obtain IP addresses dynamically” will work with the CPE, with each other, and with devices on the wired LAN network.

1.3.6 Set up a wireless client as a DHCP 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 LAN attached PC, the PC must have an Ethernet interface installed properly, be connected to the WH-5420CPE either directly or through an external LAN switch, and have TCP/IP installed and configured to obtain an IP address automatically from a DHCP server in the network.

In the case of using a wireless client, the client must also have an 802.11a wireless interface installed properly, be physically within the radio range of the WH-5420CPE, and have TCP/IP installed and configured to obtain an IP address automatically from a DHCP server in the network.

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

Step 1. From the Win95/98/2000/XP Start Button, select Settings, then Control Panel. The Win95/98/2000/XP 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: **Bindings Tab:** both **Client for Microsoft Networks** and **File and printer sharing for Microsoft Networks** should be selected. **Gateway Tab**: All fields should be blank. **DNS Configuration Tab: Disable DNS** should be selected. **IP Address Tab: Obtain IP address automatically** should be selected.

Step 8. With the WH-5420CPE powered on, reboot the PC/wireless client. After the PC/wireless client is re-booted, you should be ready to configure the WH-5420CPE. See Chapter 2.

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.

1.3.7 Configuration Setups

The factory default settings of WH-5420CPE are as following:

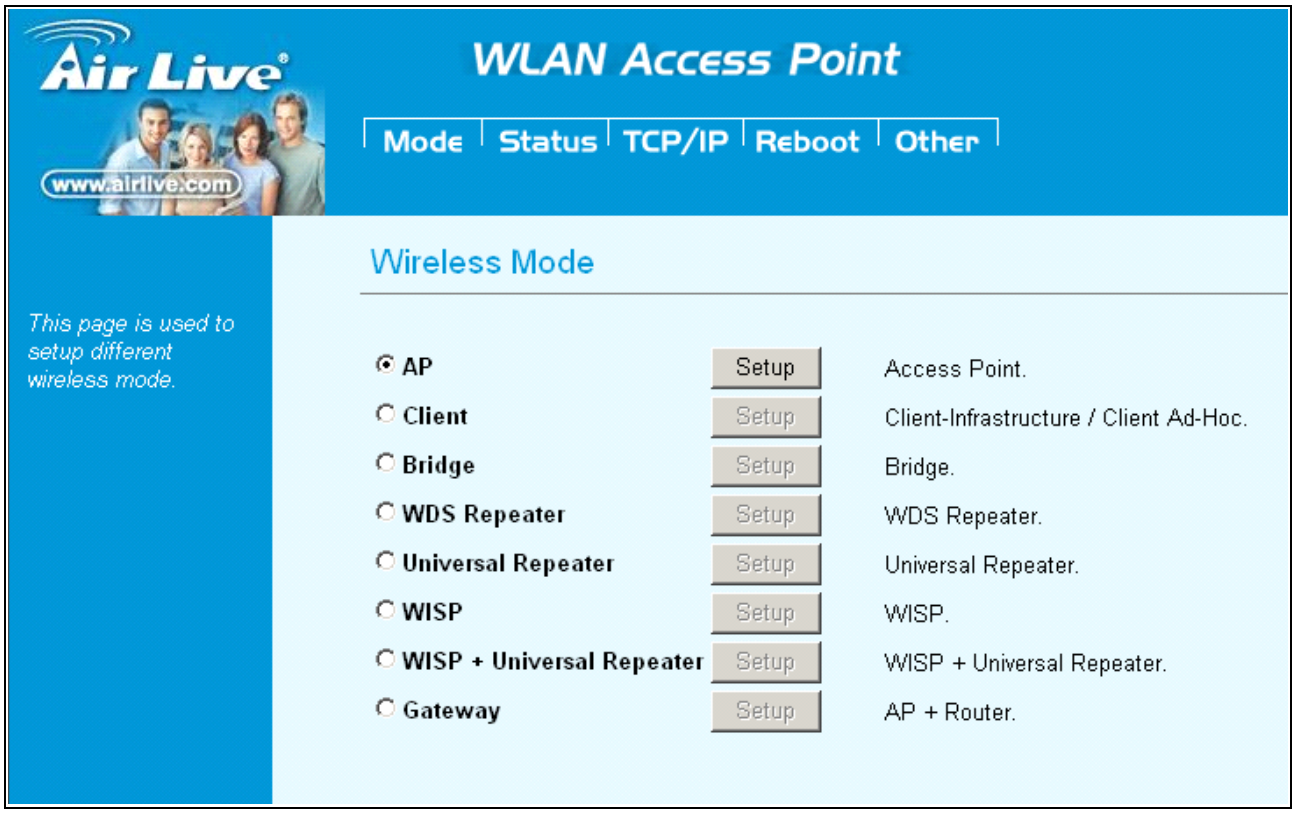
Settings	Default Value
Device Name	WH-5420CPE
Radio	802.11b/g
SSID	airlive
Channel	11
WEP	Disabled
IP Address	192.168.100.252
DHCP Server	➢ In **AP**, **Client**, **Bridge**, **WDS Repeater** and **Universal Repeater** mode, the default DHCP Server is **disabled**, please set your PC's IP to the same subnet as the AP to access the AP. ➢ In **WISP**, **WISP + Universal Repeater** and **Gateway** mode, the default DHCP server is **enabled**. Please restart your PC to renew the IP address.
DHCP IP Range	192.168.100.100 ~ 192.168.100.200

Table 3: Default Setting

2. Operation Mode

The WH-5420CPE device provides all 8 modes of wireless operational applications with:

Mode	Radio	LAN 1	LAN 2
AP	AP	LAN	LAN
Client	Client	LAN	LAN
Bridge	WDS	LAN	LAN
WDS Repeater	WDS + AP	LAN	LAN
Universal Repeater	AP + Client	LAN	LAN
WISP	Client Router	LAN	LAN
WISP + Universal Repeater	Client Router + AP	LAN	LAN
Gateway	AP+ Router	WAN	LAN

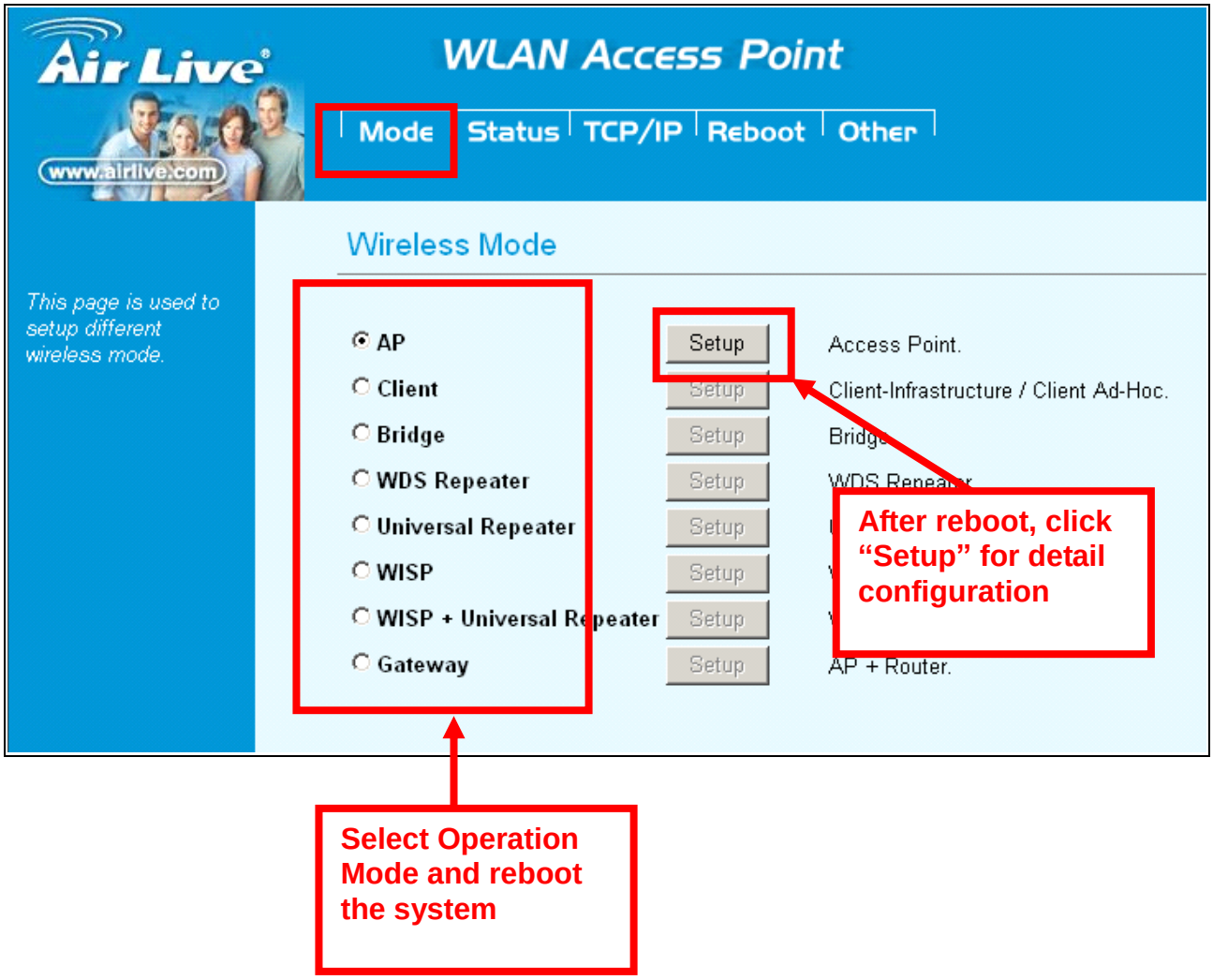


2.0 Change Operation Mode

WH-5420CPE is default in AP mode. If the mode had been changed, click the **“Mode”** button to change back.

To change operation Mode:

1. Click on **“Mode“**
2. Select Operation Mode in the main page
3. Reboot device
4. Click Setup for detail configuration



2.1 About the Operation Modes

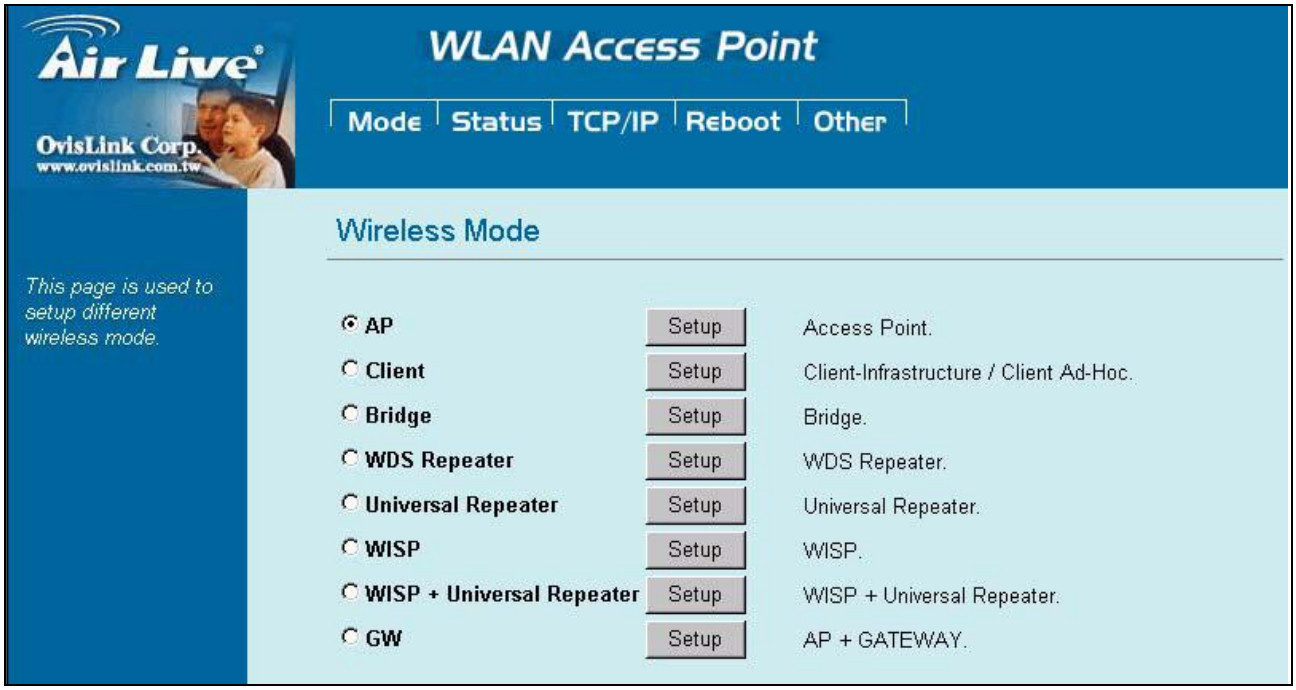
This device provides four operational applications with **Access Point, Bridge, Client (Ad-hoc) and Client (Infrastructure)** modes, which are mutually exclusive.

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

2.1.1 Access Point Mode

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

To set the operation mode to Access Point, please go to **“Mode”** field and select the **“AP”** mode.

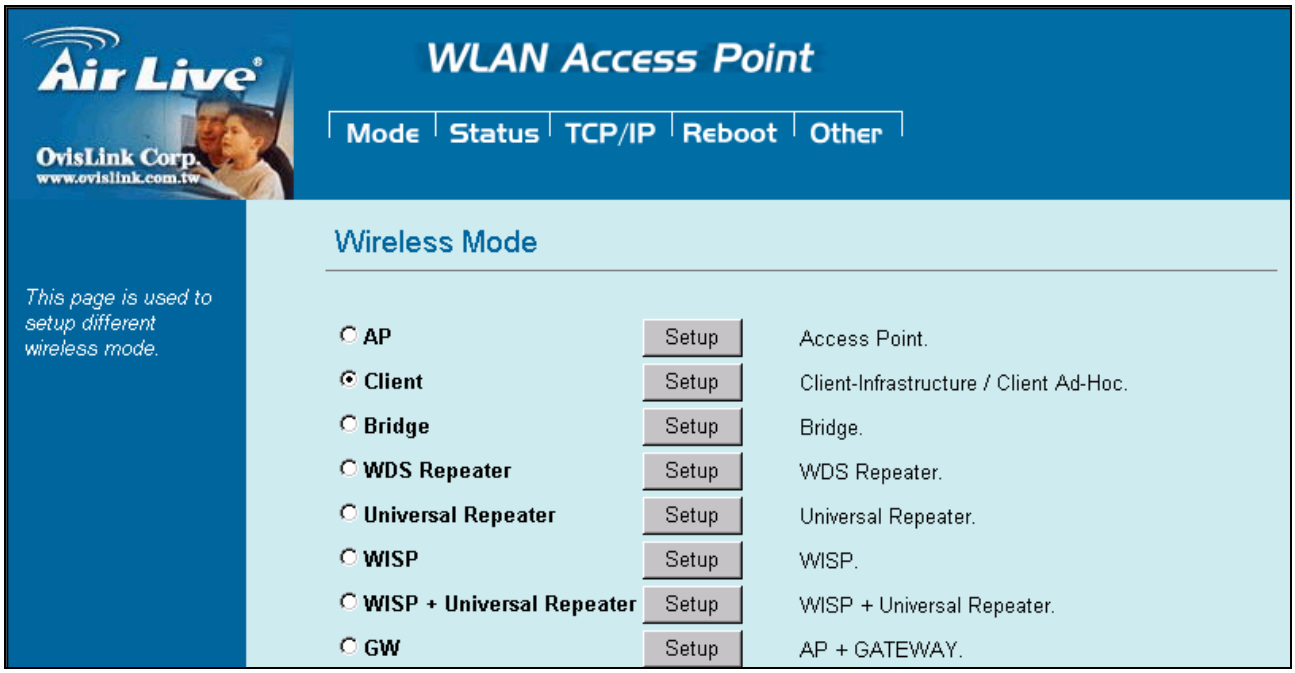


2.1.2 Client Mode

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

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

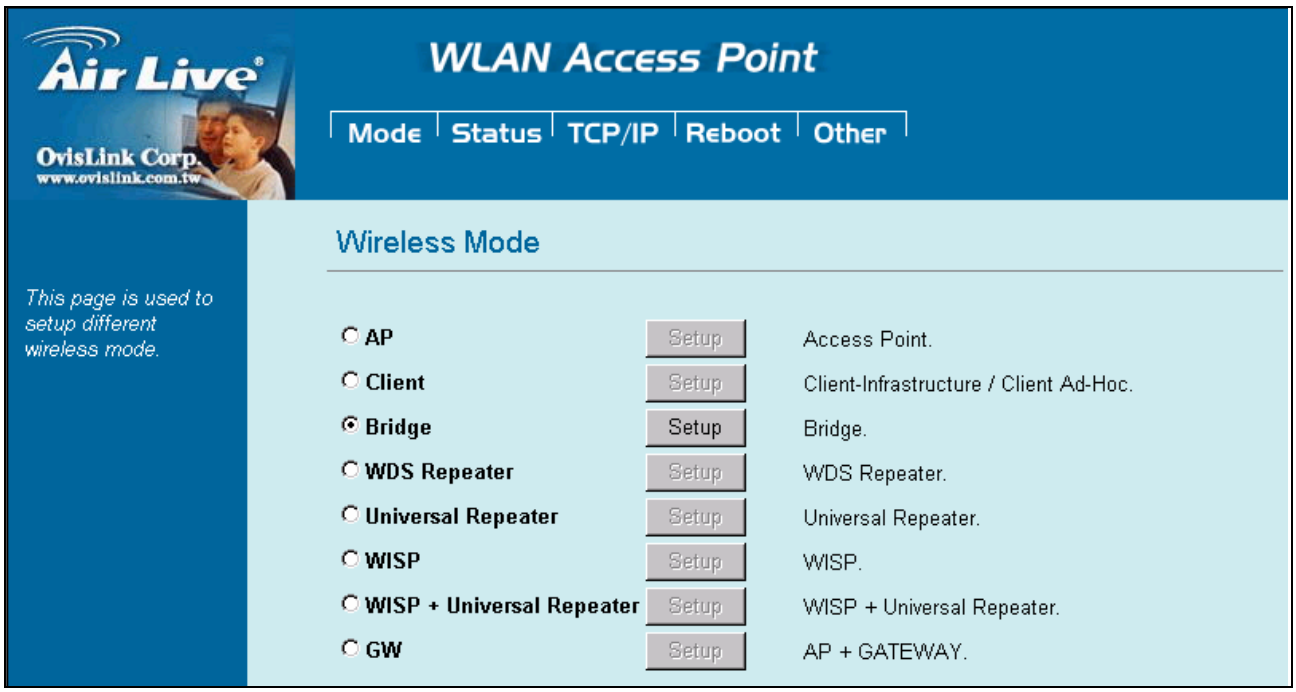
To set the operation mode to Client (Infrastructure), please go to **"Mode"** field and select the **"Client"** mode.



2.1.3 Bridge Mode

The WDS (Wireless Distributed System) function let this access point acts as a wireless LAN access point and repeater at the same time. Users can use this feature to build up a large wireless network in a large space like airports, hotels and schools …etc. This feature is also useful when users want to bridge networks between buildings where it is impossible to deploy network cable connections between these buildings.

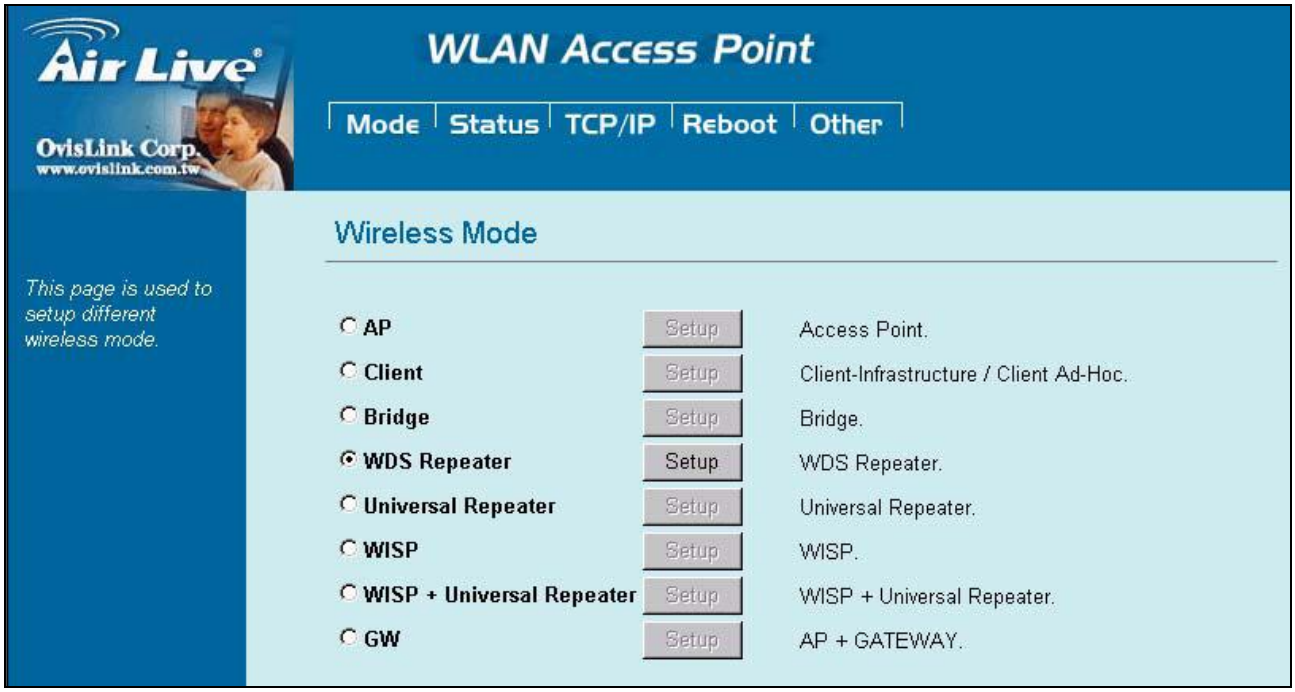
To set the operation mode to Client (Infrastructure), please go to **"Mode"** field and select the **"Bridge"** mode.



2.1.4 WDS Repeater

Refer to the illustration below. While acting as Bridges, AP1 (with Station 1 being associated to) and AP2 (with Station 2 being associated) can communicate with each other through wireless interface (with WDS). Thus Station 1 can communicate with Station 2 and both Station 1 and Station 2 are able to access the Internet if only AP1 or AP2 has the Internet connection.

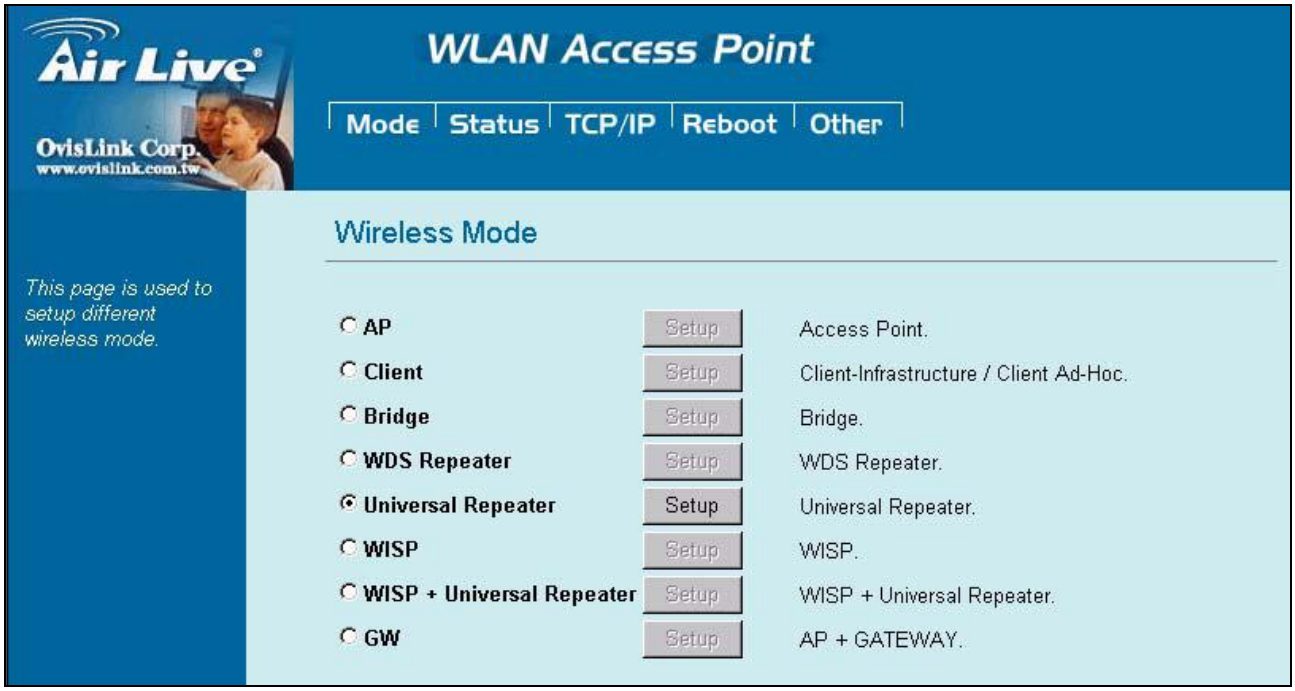
To set the operation mode to Client (Infrastructure), please go to **"Mode"** field and select the **"WDS Repeater"** mode.



2.1.5 Universal Repeater

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

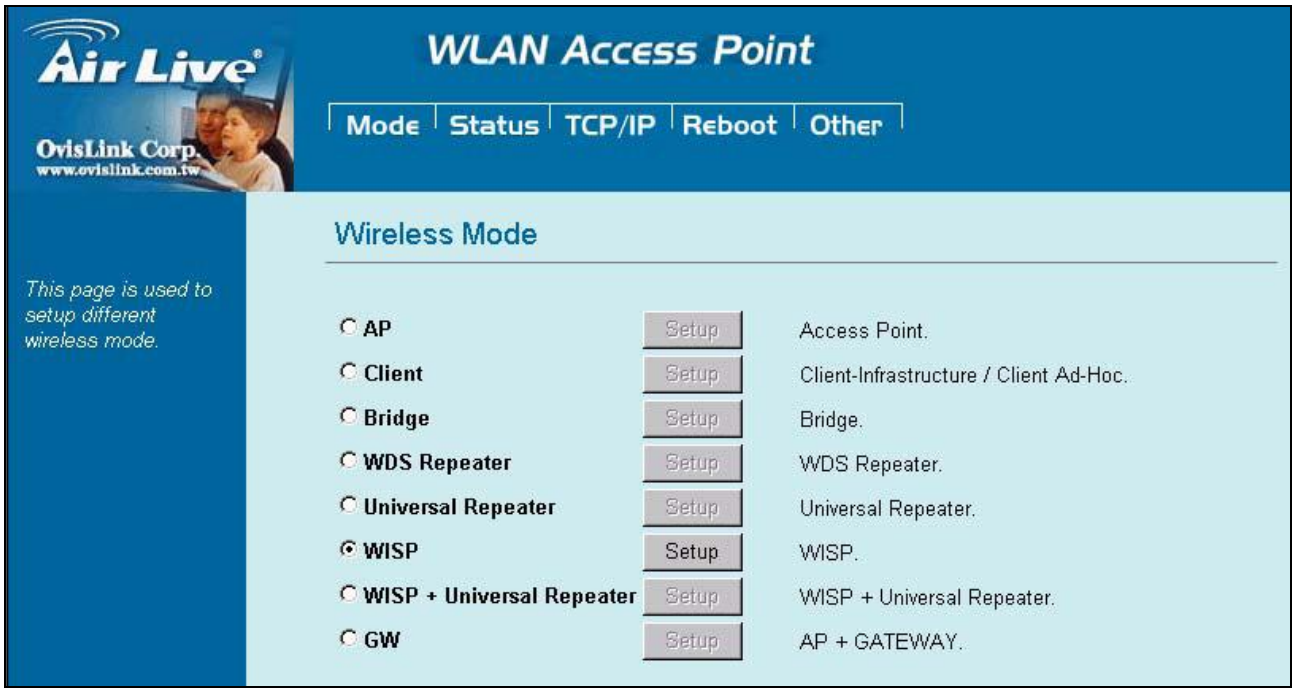
To set the operation mode to Client (Infrastructure), please go to **"Mode"** field and select the **"Universal Repeater"** mode.



2.1.6 WISP (Client Router) mode

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

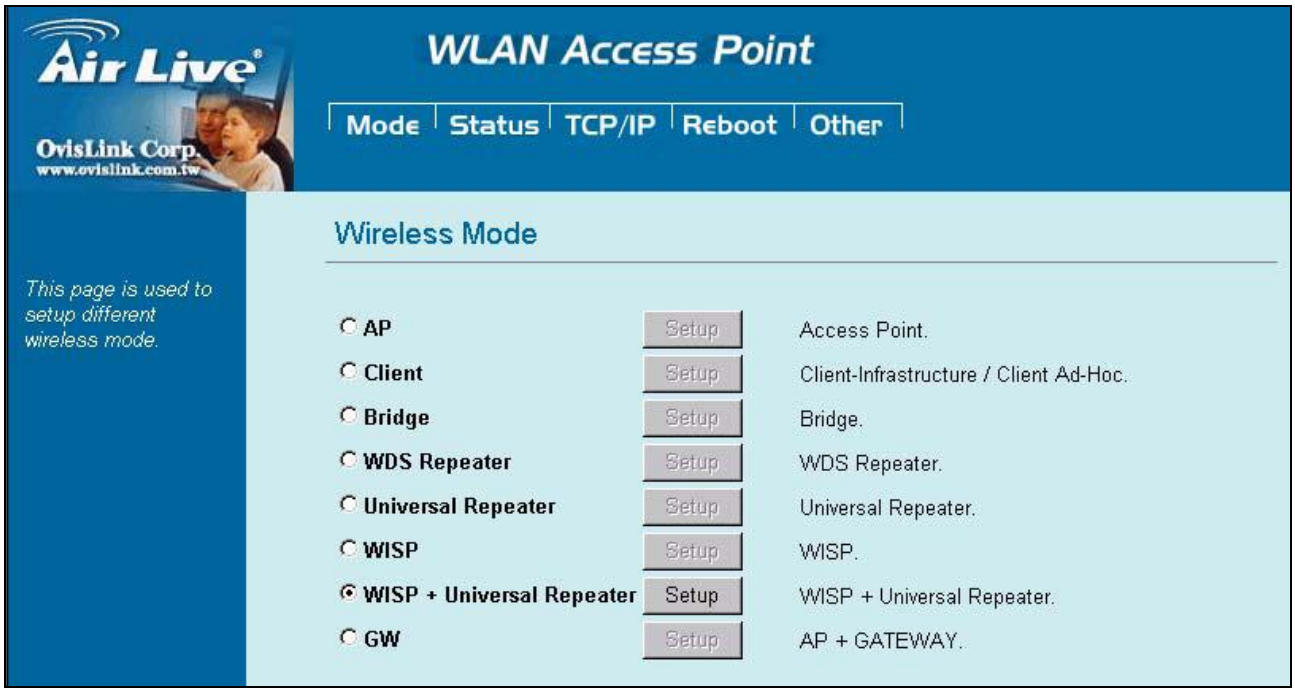
To set the operation mode to Client (Infrastructure), please go to **"Mode"** field and select the **"WISP"** mode.



2.1.7 WISP + Universal Repeater mode

In this mode, the AP behaves virtually the same as the WISP mode, except one thing: the AP can also send wireless signal to the LAN side. That means the AP can connect with the remote WISP AP and the indoor wireless card, and then provide IP sharing capability all at the same time!

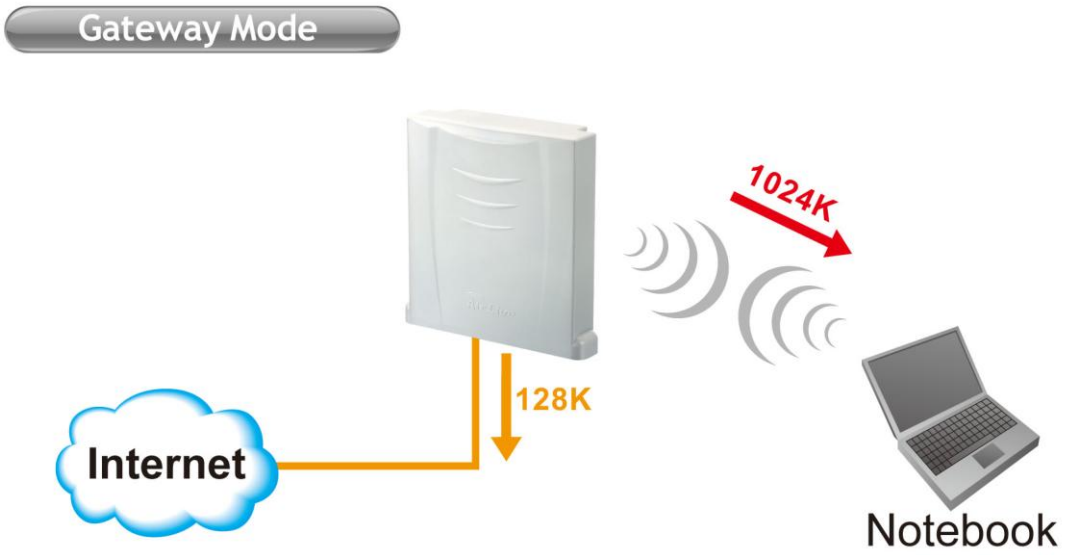
To set the operation mode to Client (Infrastructure), please go to **"Mode"** field and select the **"WISP + Universal Repeater"** mode.



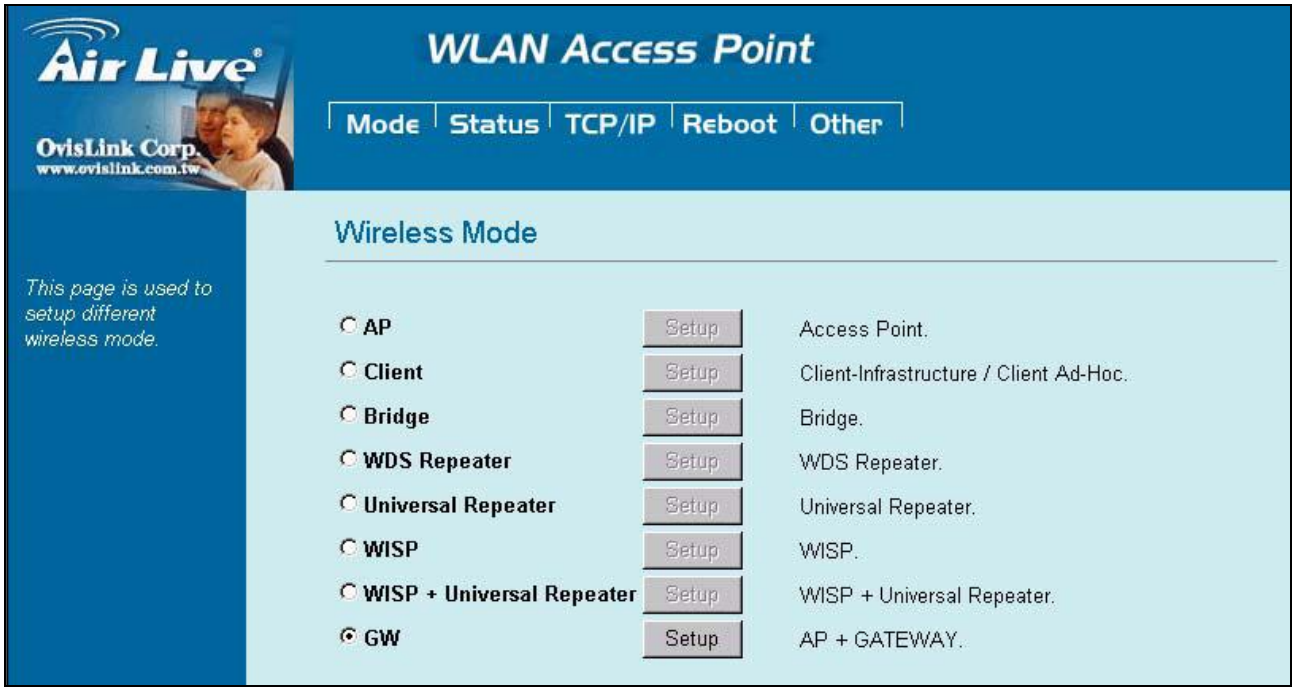
2.1.8 Gateway (AP + Router)

In this mode, router functions are added between one Ethernet port and the other network interface. The radio is an AP mode which allow wireless client to share the internet connection.

To set the operation mode to Client (Infrastructure), please go to **"Mode"** field and select the **"Gateway"** mode.



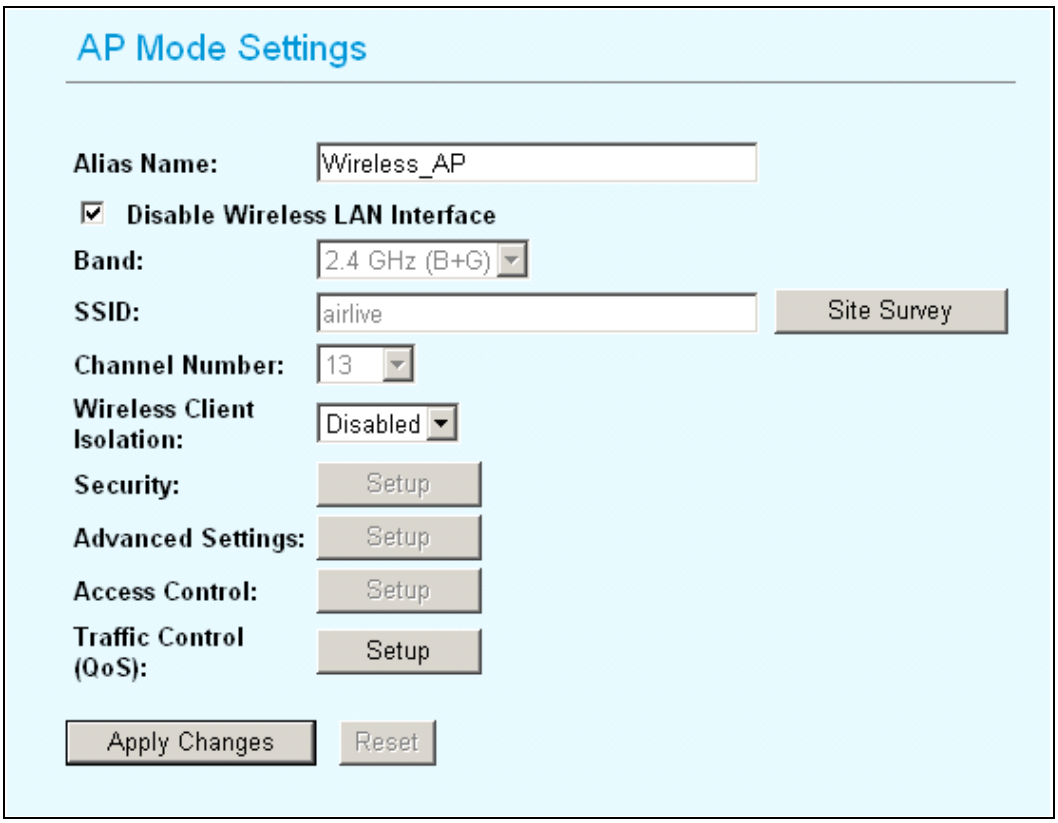
To set the operation mode to "GW Mode", Please go to "Mode → GW" and click the Setup button for configuration.



3. Wireless Settings

This section guides you to configure the mode of the Radio interface.

3.1 Access Point Mode Settings



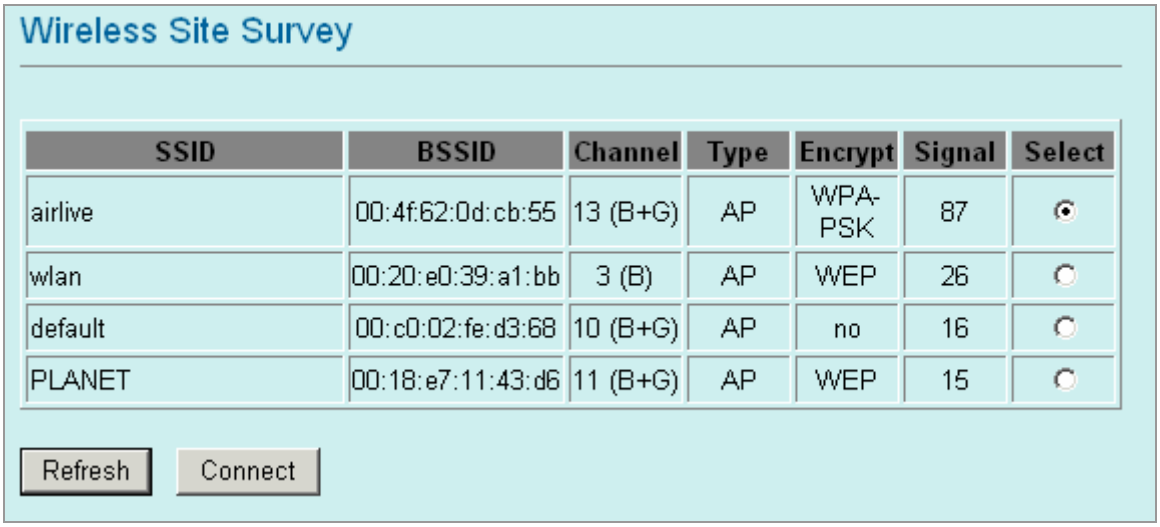
- **Alias Name**: Another name for WH-5420CPE.
- **Disable Wireless LAN Interface:** Check the box to disable the Wireless LAN Interface, by so doing, you won't be able to make wireless connection with this Access Point in the network you are located. In other words, this device will not be visible by any wireless station.
- **Band:** You can choose one mode of the following you need.
    - 2.4GHz (B): 802.11b supported rate only.
    - 2.4GHz (G): 802.11g supported rate only.
    - 2.4GHz (B+G): 802.11b supported rate and 802.11g supported rate.

  The default is 2.4GHz (B+G) mode.
- **SSID (Network ID):** The SSID differentiates one WLAN from another; therefore, all access points and all devices attempting to connect to a specific WLAN must use the same SSID. It is case-sensitive and must not exceed 32 characters. A device will not be permitted to join the BSS unless it can provide the unique SSID. An SSID is also

referred to as a network name because essentially it is a name that identifies a wireless network.

In this mode, the SSID is provided for client connection.

- **Channel Number:** Allow user to set the channel manually or automatically. If set channel manually, just select the channel you want to specify. If **"Auto"** is selected, user can set the channel range to have Wireless Access Point automatically survey and choose the channel with best situation for communication. The number of channels supported depends on the region of this Access Point. All stations communicating with the Access Point must use the same channel.
- **Wireless Client Isolation:** This is to separate wireless client if needed. Wireless clients can not communicate to each other if the field is enabled.
- **Site Survey:** Site survey helps to find out available access point around. You can also check to prevent using same SSID or channel with other AP.



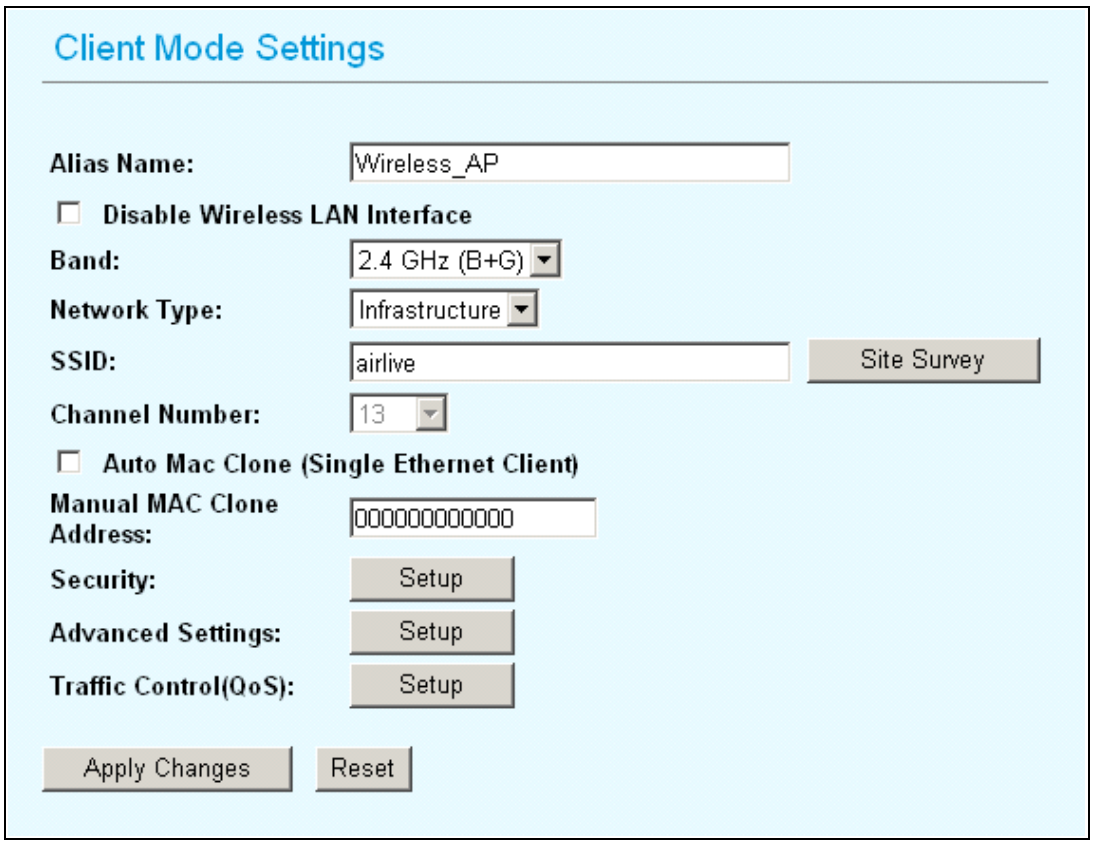
To configure the security connection, please refer to Section 3.9 Wireless Security Settings ……

To configure the Advanced Settings, please refer to Section 3.10 Advanced Wireless Settings ……

To configure the access control, please refer to Section 3.11 Access Control Settings ……

To configure the Traffic Control, please refer to Section 3.12 Access Control Settings ……

3.2 Client Mode Settings

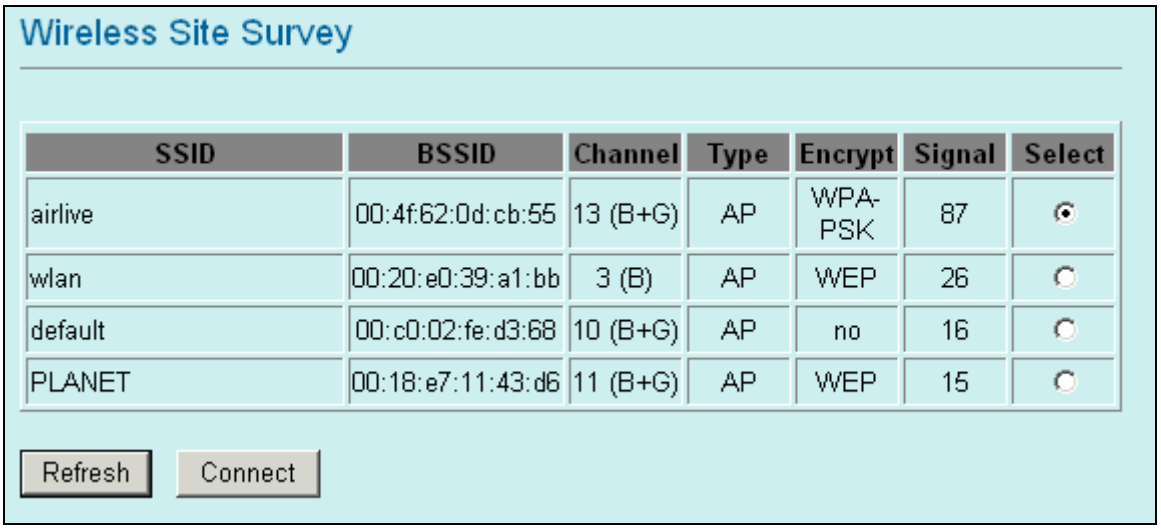


- **Alias Name**: Another name for WH-5420CPE.
- **Disable Wireless LAN Interface:** Check the box to disable the Wireless LAN Interface, by so doing, you won't be able to make wireless connection with this Access Point in the network you are located. In other words, this device will not be visible by any wireless station.
- **Band:** You can choose one mode of the following you need.
    - 2.4GHz (B): 802.11b supported rate only.
    - 2.4GHz (G): 802.11g supported rate only.
    - 2.4GHz (B+G): 802.11b supported rate and 802.11g supported rate.

  The default is 2.4GHz (B+G) mode.
- **SSID (Network ID):** The SSID differentiates one WLAN from another; therefore, all access points and all devices attempting to connect to a specific WLAN must use the same SSID. It is case-sensitive and must not exceed 32 characters. A device will not be permitted to join the BSS unless it can provide the unique SSID. An SSID is also referred to as a network name because essentially it is a name that identifies a wireless network.

  In this mode, the SSID is the available remote Access Point to connect to.

- **Channel Number:** Allow user to set the channel manually or automatically. If set channel manually, just select the channel you want to specify. If **"Auto"** is selected, user can set the channel range to have Wireless Access Point automatically survey and choose the channel with best situation for communication. The number of channels supported depends on the region of this Access Point. All stations communicating with the Access Point must use the same channel.
- **Auto Mac Clone (Single Ethernet Client):** If your ISP restricts service to PCs only, use the MAC Clone feature to copy a PC Media Access Control (MAC) address to your router. This procedure will cause the router to appear as a single PC, while allowing online access to multiple computers on your network.
- **Manual MAC Clone Address:** You can also manually provide MAC address to the router. This solves the problem if you have more than one PC which need to access the internet..
- **Site Survey:** Site survey helps to find out available access point around. You can also check to prevent using same SSID or channel with other AP.



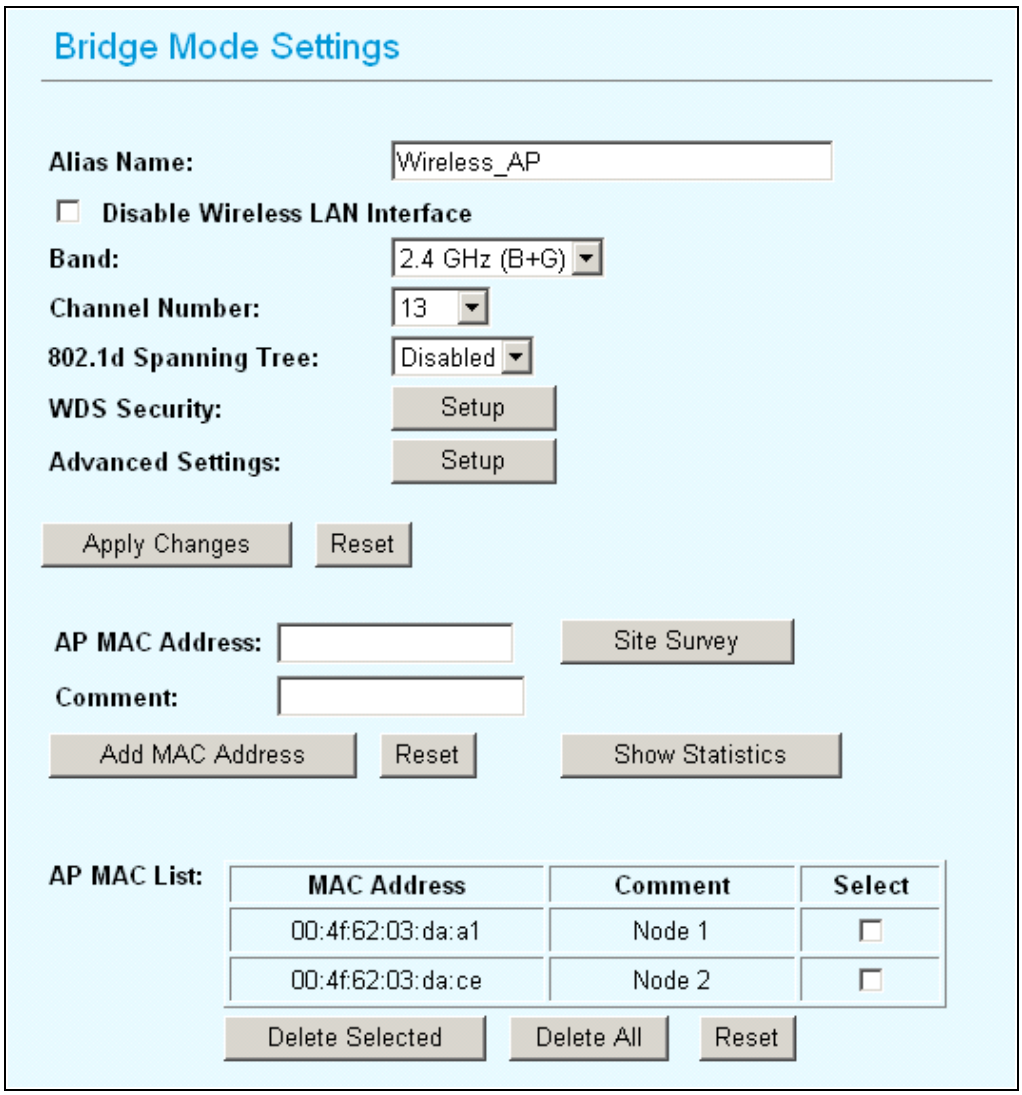
To configure the security connection, please refer to Section 3.9 Wireless Security Settings ……

To configure the Advanced Settings, please refer to Section 3.10 Advanced Wireless Settings ……

To configure the access control, please refer to Section 3.11 Access Control Settings ……

To configure the Traffic Control, please refer to Section 3.12 Access Control Settings ……

3.3 Bridge Mode Settings

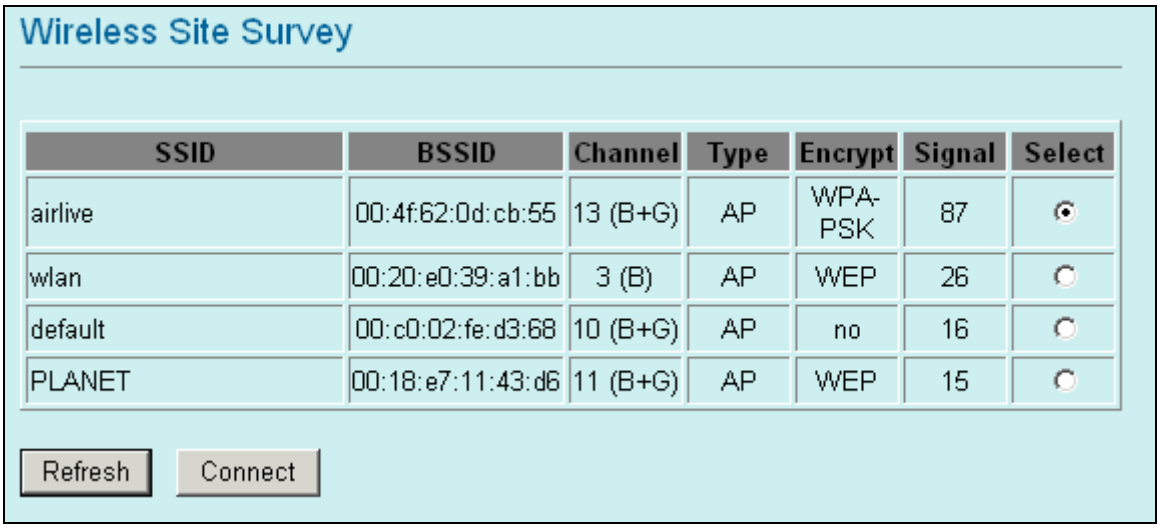


- **Alias Name**: Another name for WH-5420CPE.
- **Disable Wireless LAN Interface:** Check the box to disable the Wireless LAN Interface, by so doing, you won't be able to make wireless connection with this Access Point in the network you are located. In other words, this device will not be visible by any wireless station.
- **Band:** You can choose one mode of the following you need.
    - 2.4GHz (B): 802.11b supported rate only.
    - 2.4GHz (G): 802.11g supported rate only.
    - 2.4GHz (B+G): 802.11b supported rate and 802.11g supported rate.

  The default is 2.4GHz (B+G) mode.
- **Channel Number:** Allow user to set the channel manually or automatically. If set channel manually, just select the channel you want to specify. If **"Auto"** is selected, user can set the channel range to have Wireless Access Point automatically survey

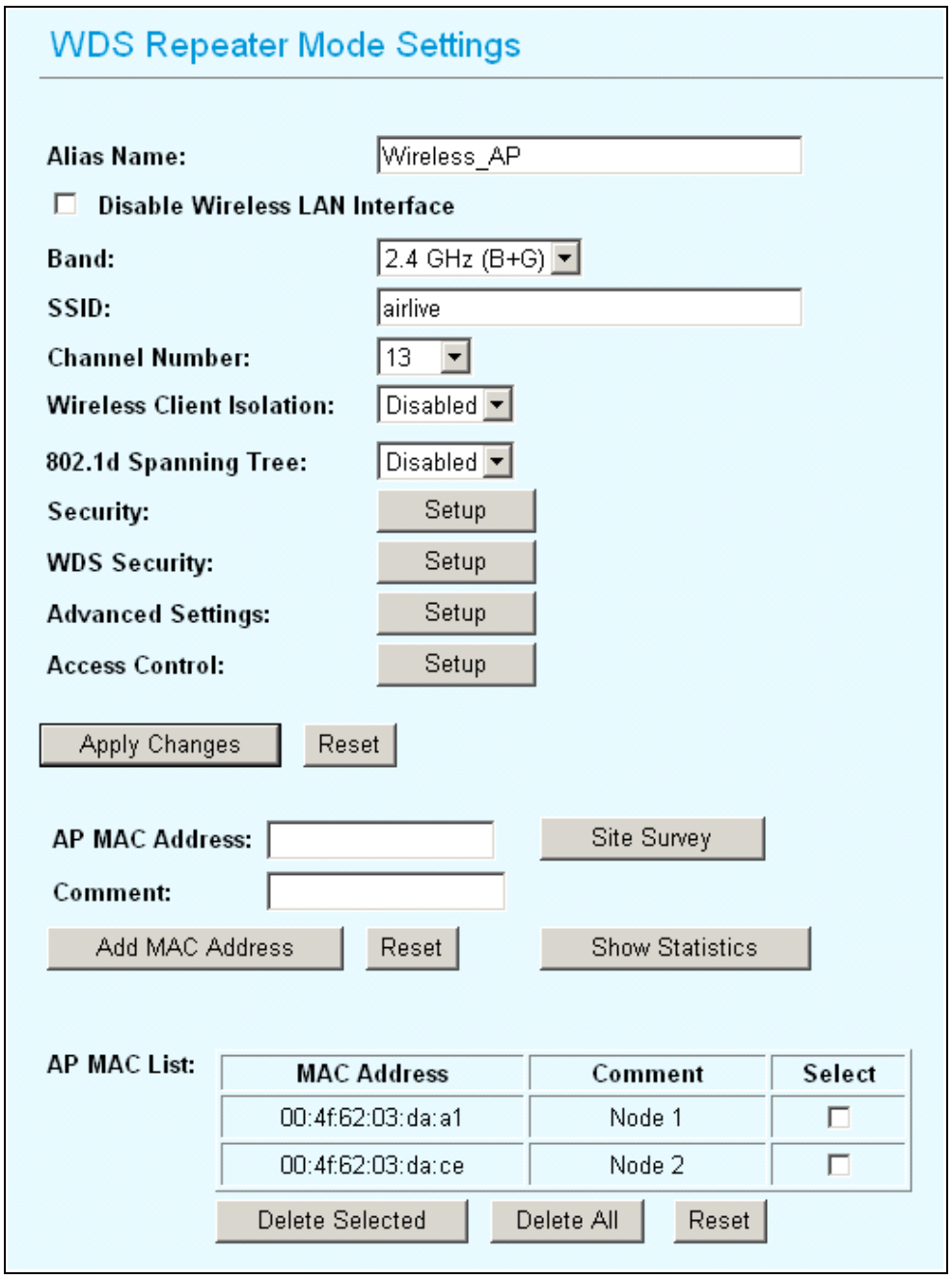
and choose the channel with best situation for communication. The number of channels supported depends on the region of this Access Point. All stations communicating with the Access Point must use the same channel.

- **802.1d Spanning Tree:** Spanning tree is to prevent bridge loop when there are multiple active paths between network nodes. Bridge loop could cause connection fail or broadcast storm. Spanning tree allows a network design to include spare (redundant) links to provide automatic backup paths if an active link fails, without the danger of bridge loops, or the need for manual enabling/disabling of these backup links.
- **AP MAC Address:** Fill the MAC address of the remote WDS node which you want to connect to.
- **Site Survey:** Use this button to find out the remote WDS node and check the signal strength. It helps to build up you WDS network correctly.



To configure the security connection, please refer to Section 3.9 Wireless Security Settings ……
To configure the Advanced Settings, please refer to Section 3.10 Advanced Wireless Settings ……
To configure the access control, please refer to Section 3.11 Access Control Settings ……
To configure the Traffic Control, please refer to Section 3.12 Access Control Settings ……

3.4 WDS Repeater Mode Settings



- **Alias Name**: Another name for WH-5420CPE.
- **Disable Wireless LAN Interface:** Check the box to disable the Wireless LAN Interface, by so doing, you won't be able to make wireless connection with this Access Point in the network you are located. In other words, this device will not be visible by any wireless station.
- **Band:** You can choose one mode of the following you need.
    - 2.4GHz (B): 802.11b supported rate only.
    - 2.4GHz (G): 802.11g supported rate only.
    - 2.4GHz (B+G): 802.11b supported rate and 802.11g supported rate.

The default is 2.4GHz (B+G) mode.

- **SSID (Network ID):** Provide SSID for wireless client survey and connection. The SSID differentiates one WLAN from another; therefore, all access points and all devices attempting to connect to a specific WLAN must use the same SSID. It is case-sensitive and must not exceed 32 characters. A device will not be permitted to join the BSS unless it can provide the unique SSID. An SSID is also referred to as a network name because essentially it is a name that identifies a wireless network.

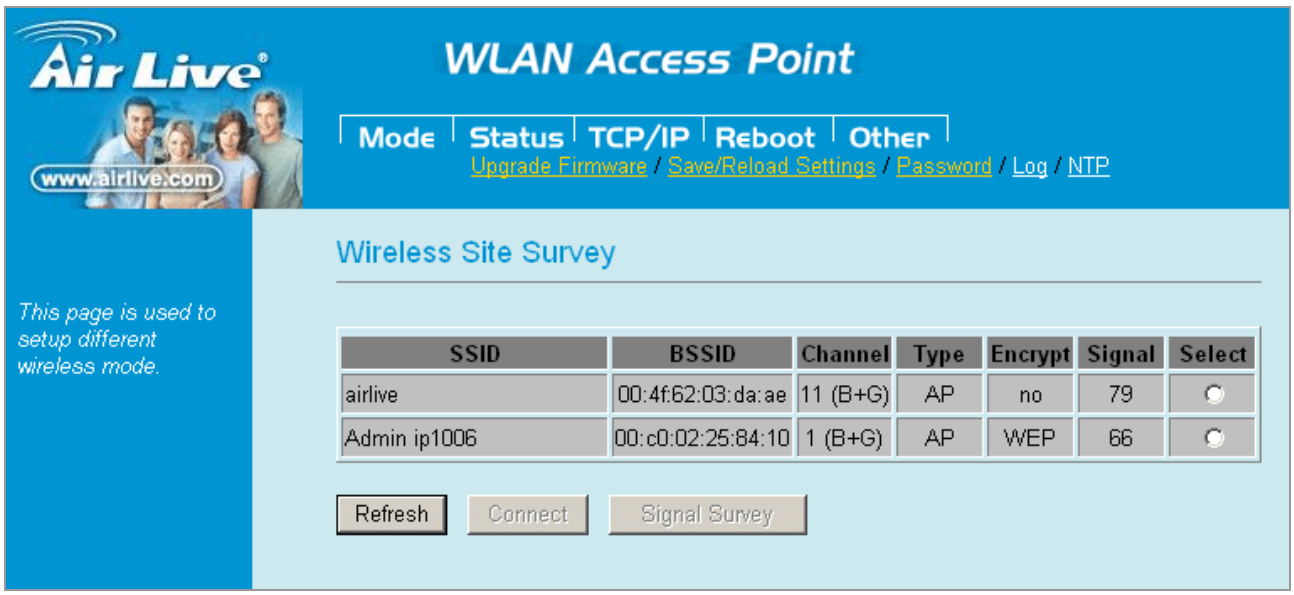
  In this mode, the SSID is provided for wireless client connection.

- **Channel Number:** Allow user to set the channel manually or automatically. If set channel manually, just select the channel you want to specify. If **"Auto"** is selected, user can set the channel range to have Wireless Access Point automatically survey and choose the channel with best situation for communication. The number of channels supported depends on the region of this Access Point. All stations communicating with the Access Point must use the same channel.

- **802.1d Spanning Tree:** Spanning tree is to prevent bridge loop when there are multiple active paths between network nodes. Bridge loop could cause connection fail or broadcast storm. Spanning tree allows a network design to include spare (redundant) links to provide automatic backup paths if an active link fails, without the danger of bridge loops, or the need for manual enabling/disabling of these backup links.

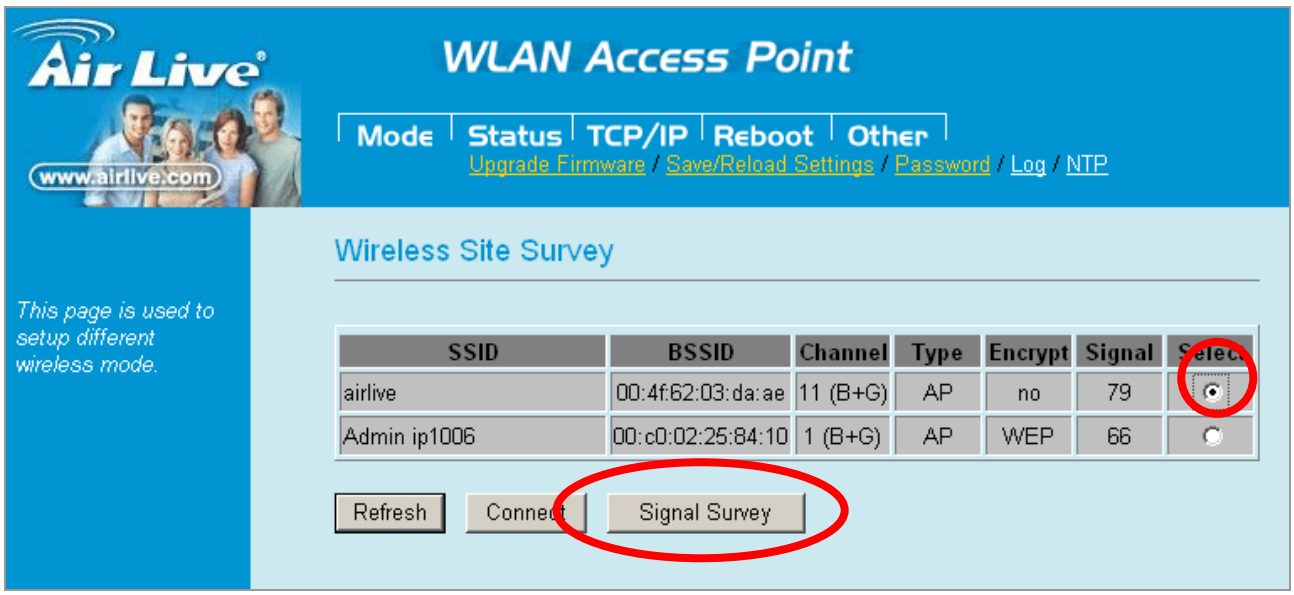
- **AP MAC Address:** Fill the MAC address of the remote WDS node which you want to connect to.

- **Site Survey:** Use this button to find out the remote WDS node and check the signal strength. It helps to build up you WDS network correctly.

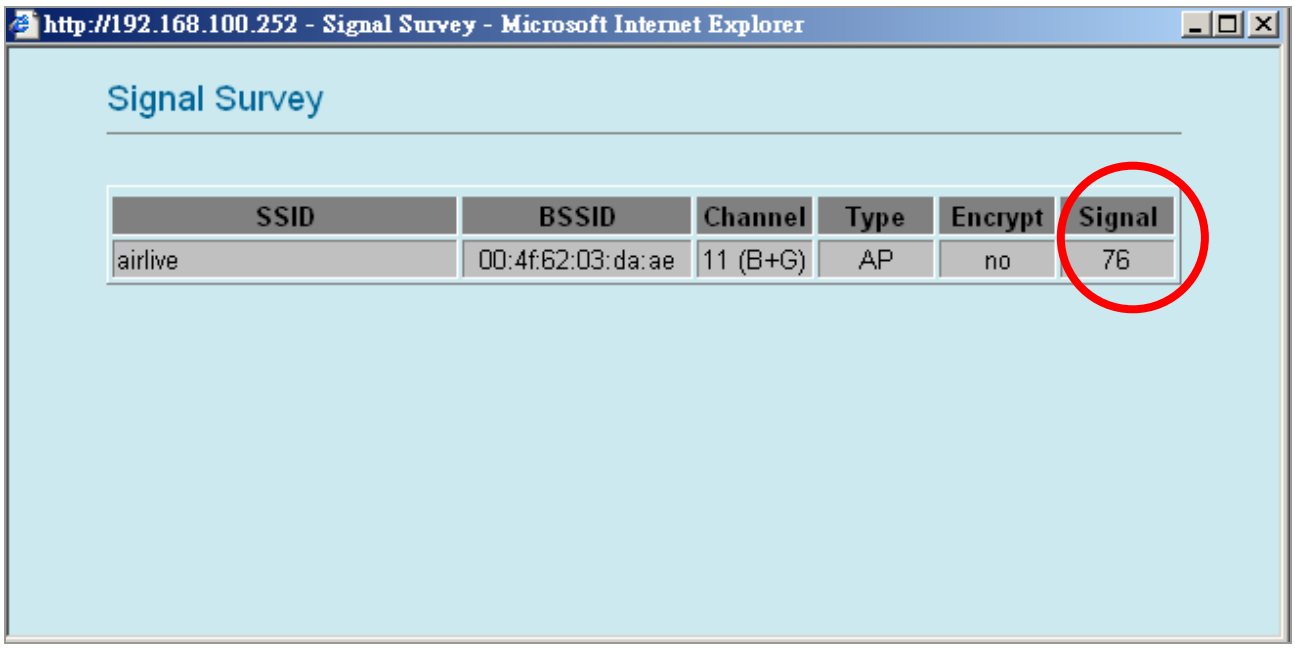


You can also use the Signal survey for alignment.
To do this,

1. Select the surveyed device in the list.
2. The "Signal Survey" button then enabled.



3. Click on **"Signal Survey"** button.
4. A pop up page shows the signal strength.



5. The signal strength refresh every 3 seconds, you can then change your antenna for a better signal.

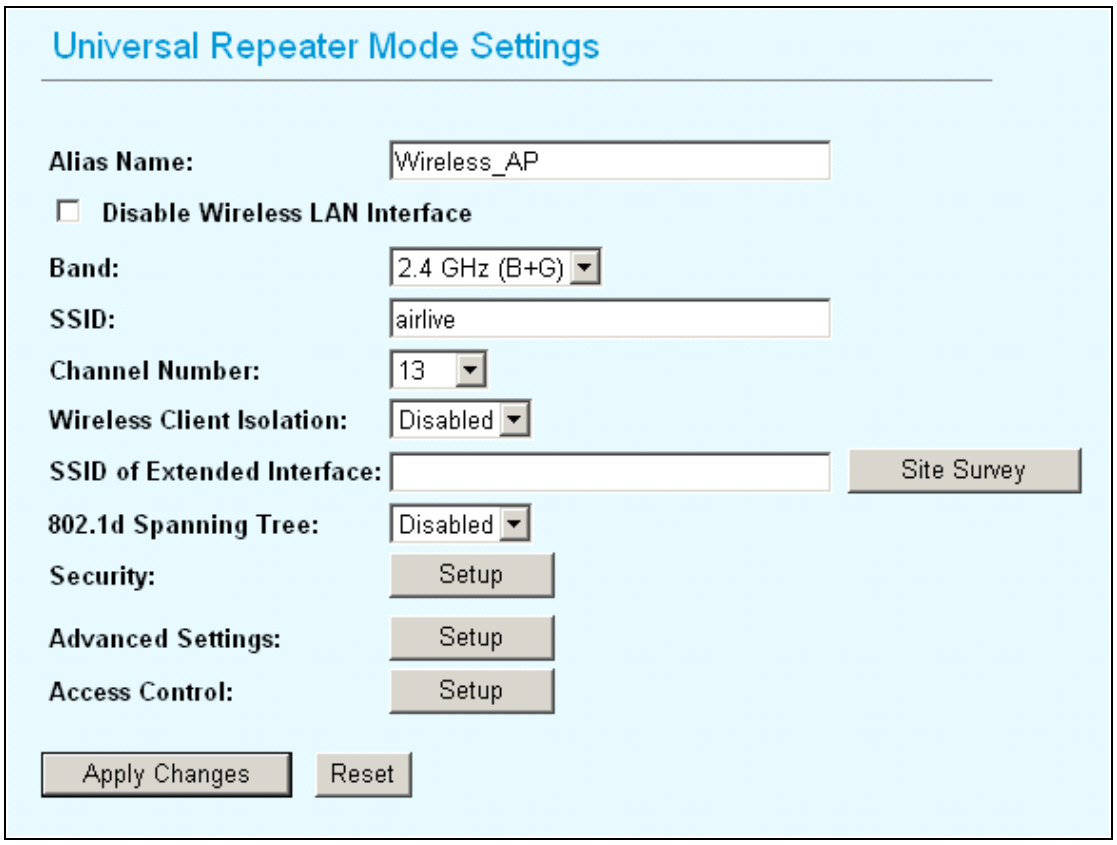
To configure the security connection, please refer to Section 3.9 Wireless Security Settings ……

To configure the Advanced Settings, please refer to Section 3.10 Advanced Wireless Settings ……

To configure the access control, please refer to Section 3.11 Access Control Settings ……

To configure the Traffic Control, please refer to Section 3.12 Access Control Settings ……

3.5 Universal Repeater Mode Settings

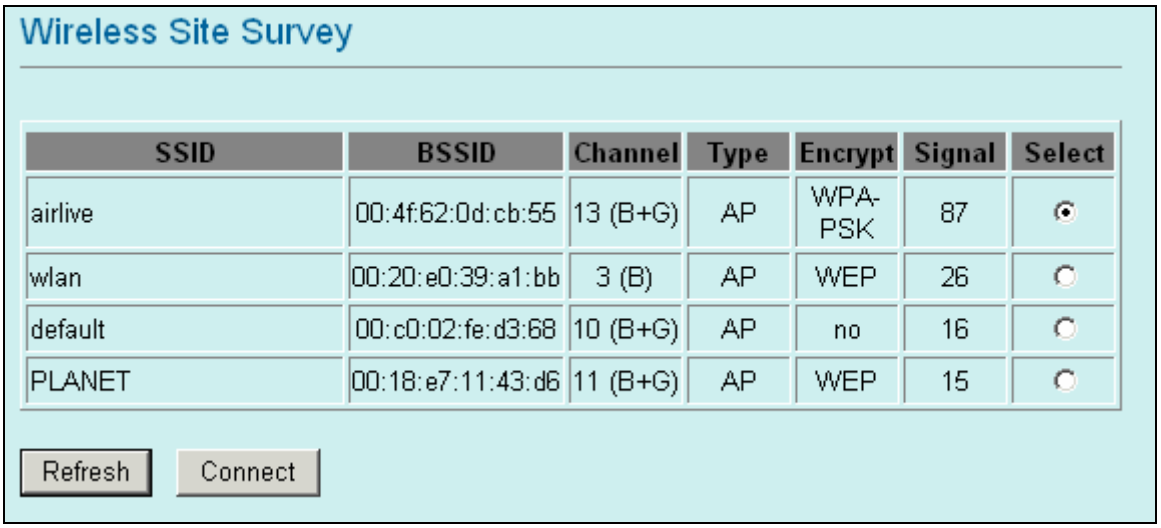


- **Alias Name**: Another name for WH-5420CPE.
- **Disable Wireless LAN Interface:** Check the box to disable the Wireless LAN Interface, by so doing, you won't be able to make wireless connection with this Access Point in the network you are located. In other words, this device will not be visible by any wireless station.
- **Band:** You can choose one mode of the following you need.
    - 2.4GHz (B): 802.11b supported rate only.
    - 2.4GHz (G): 802.11g supported rate only.
    - 2.4GHz (B+G): 802.11b supported rate and 802.11g supported rate.

  The default is 2.4GHz (B+G) mode.
- **SSID (Network ID):** Provide SSID for wireless client survey and connection. The SSID differentiates one WLAN from another; therefore, all access points and all devices attempting to connect to a specific WLAN must use the same SSID. It is case-sensitive and must not exceed 32 characters. A device will not be permitted to join the BSS unless it can provide the unique SSID. An SSID is also referred to as a network name because essentially it is a name that identifies a wireless network.

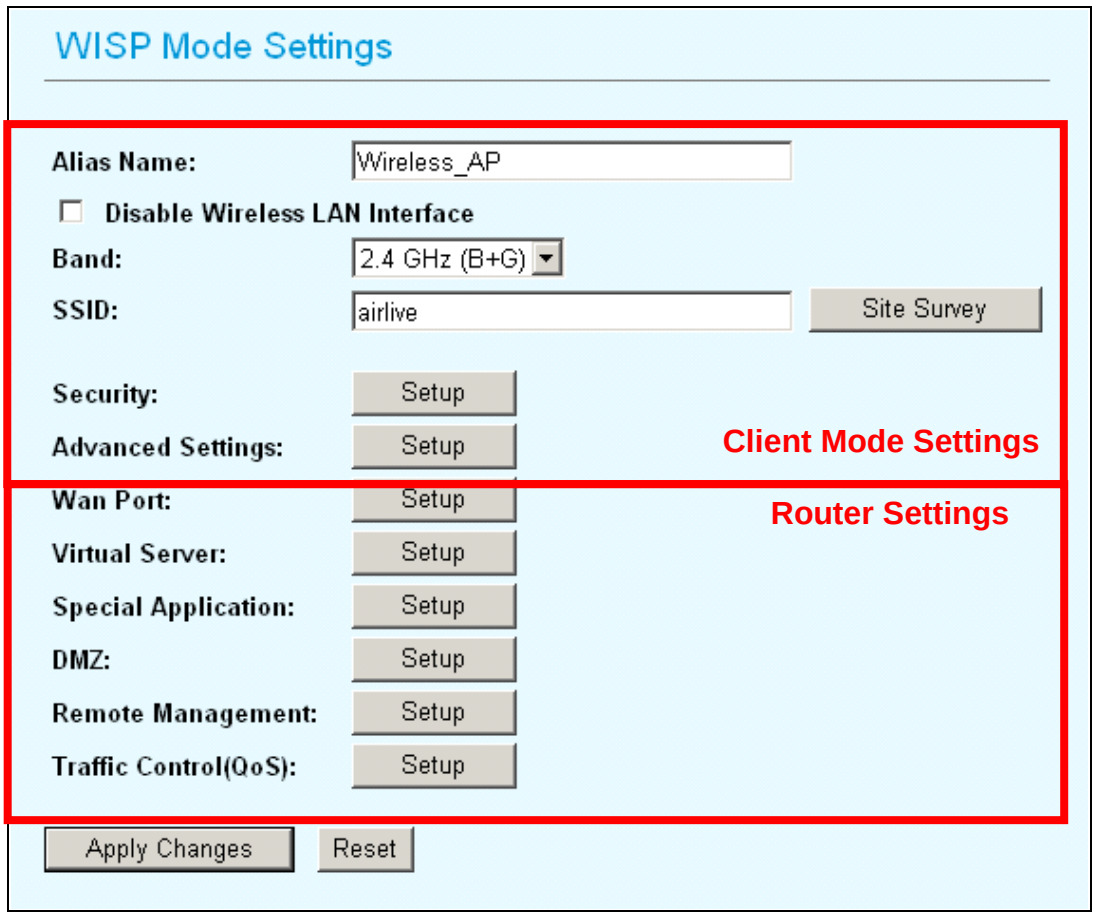
  This field is to provide for wireless client connection.

- **Channel Number:** Allow user to set the channel manually or automatically. If set channel manually, just select the channel you want to specify. If **"Auto"** is selected, user can set the channel range to have Wireless Access Point automatically survey and choose the channel with best situation for communication. The number of channels supported depends on the region of this Access Point. All stations communicating with the Access Point must use the same channel.
- **SSID of Extended Interface:** This field is the SSID of remote Access Point to connect to.
- **802.1d Spanning Tree:** Spanning tree is to prevent bridge loop when there are multiple active paths between network nodes. Bridge loop could cause connection fail or broadcast storm. Spanning tree allows a network design to include spare (redundant) links to provide automatic backup paths if an active link fails, without the danger of bridge loops, or the need for manual enabling/disabling of these backup links.
- **Site Survey:** Use this button to find out the remote Access Point and check the signal strength.



To configure the security connection, please refer to Section 3.9 Wireless Security Settings ……
To configure the Advanced Settings, please refer to Section 3.10 Advanced Wireless Settings ……
To configure the access control, please refer to Section 3.11 Access Control Settings ……
To configure the Traffic Control, please refer to Section 3.12 Access Control Settings ……

3.6 WISP Mode Settings

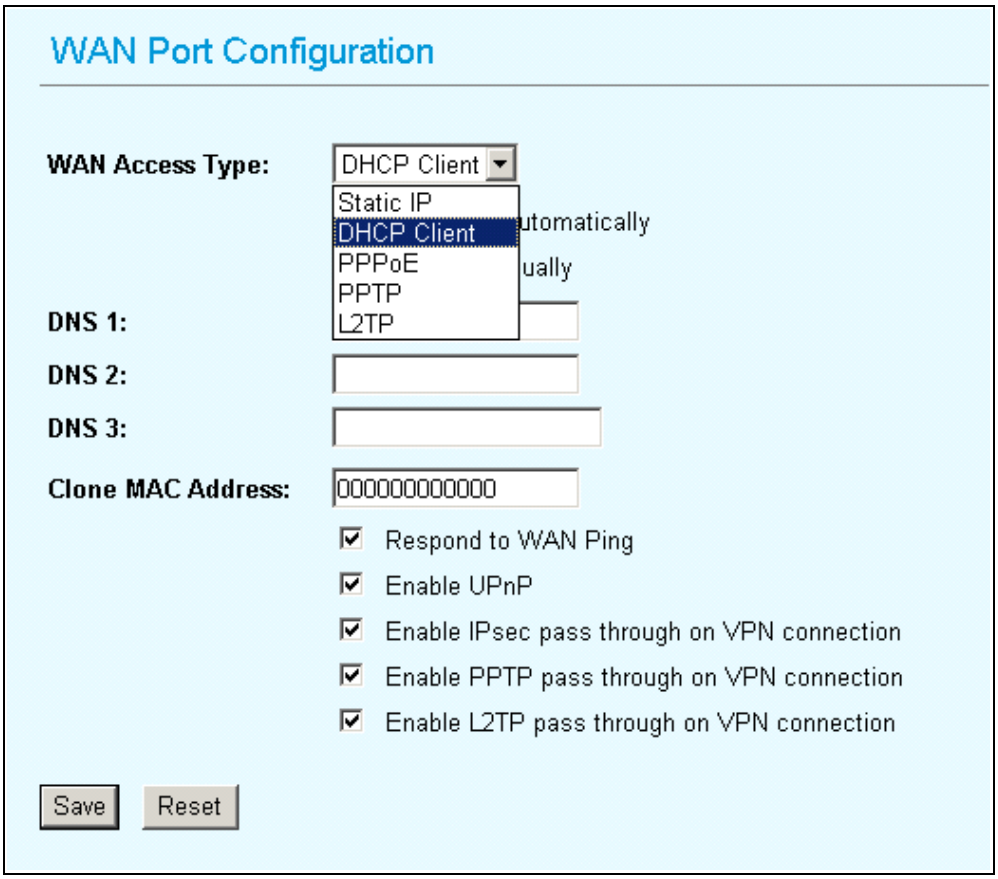


- **Alias Name**: Another name for WH-5420CPE.
- **Disable Wireless LAN Interface:** Check the box to disable the Wireless LAN Interface, by so doing, you won't be able to make wireless connection with this Access Point in the network you are located. In other words, this device will not be visible by any wireless station.
- **Band:** You can choose one mode of the following you need.
    - 2.4GHz (B): 802.11b supported rate only.
    - 2.4GHz (G): 802.11g supported rate only.
    - 2.4GHz (B+G): 802.11b supported rate and 802.11g supported rate.

  The default is 2.4GHz (B+G) mode.
- **SSID (Network ID):** The SSID differentiates one WLAN from another; therefore, all access points and all devices attempting to connect to a specific WLAN must use the same SSID. It is case-sensitive and must not exceed 32 characters. A device will not be permitted to join the BSS unless it can provide the unique SSID. An SSID is also referred to as a network name because essentially it is a name that identifies a wireless network.

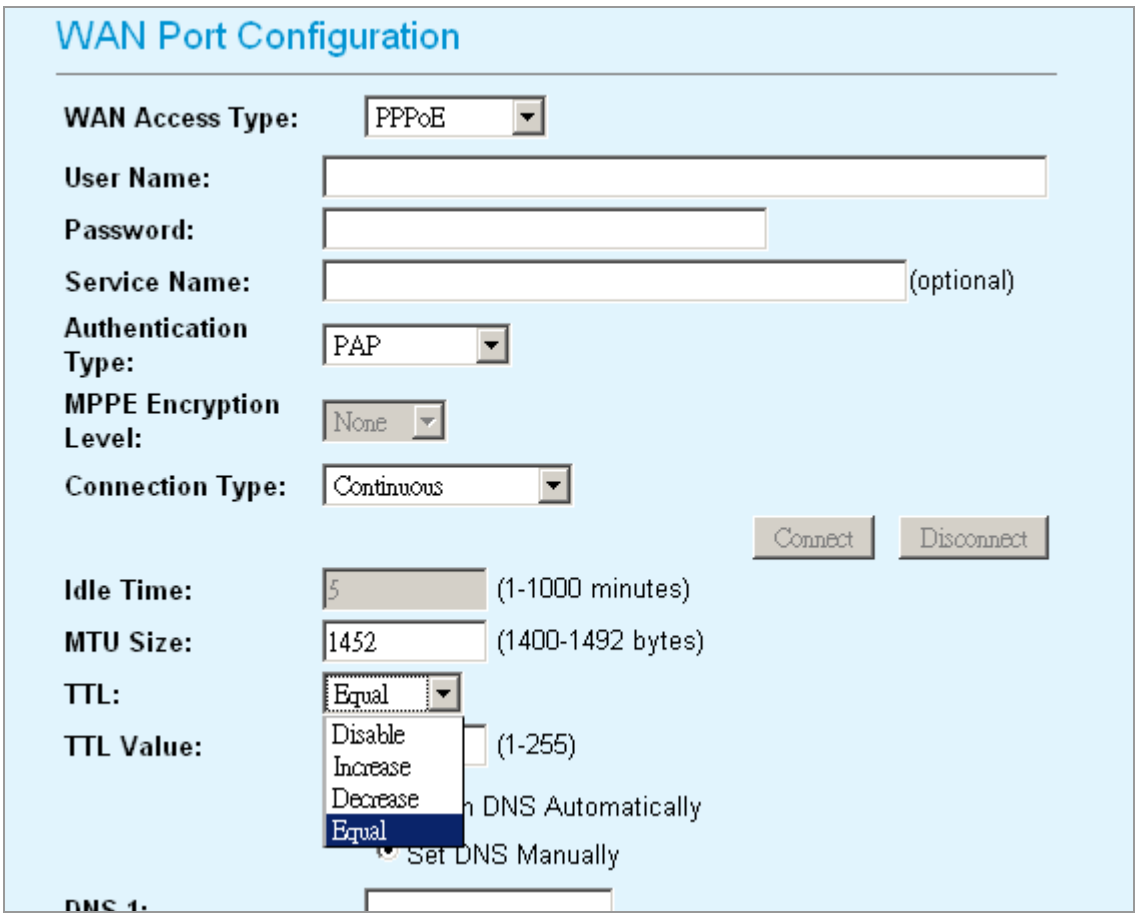
  In this mode, the SSID is the remote WISP CPE to connect to.

- **WAN Port:** WH-5420CPE provides 4 methods for client to access the internet. This depends on the location and the service which the ISP provides. You need to contact the ISP for detail information.

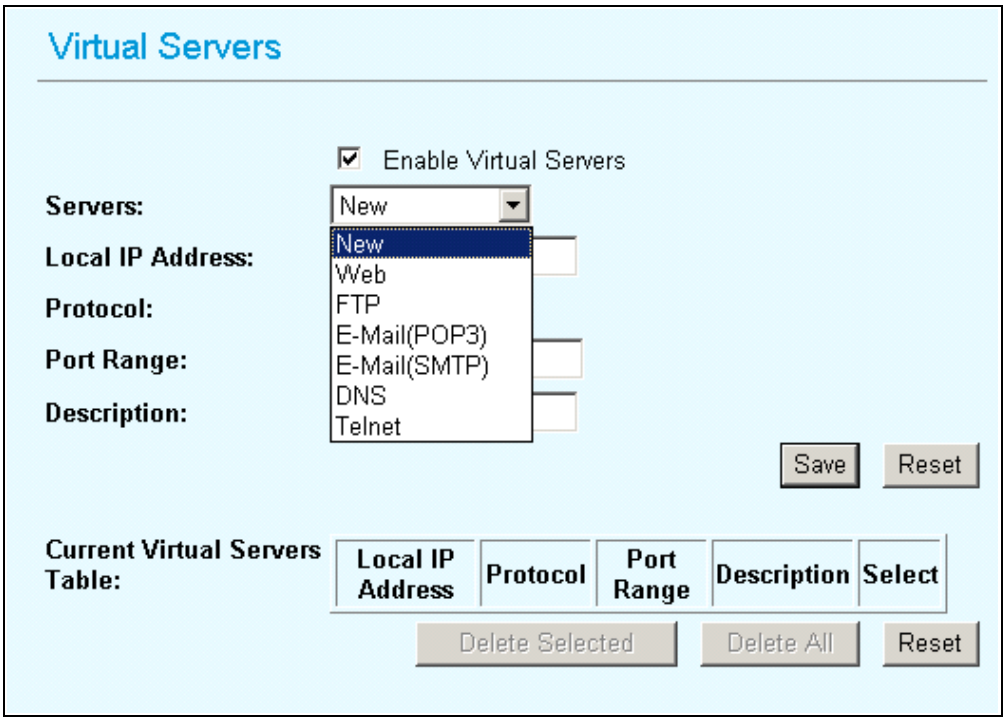


Some ISP/WISP has special inquire for TTL feature that did not decrease the TTL value when pass the first router of ISP/WISP.

When using PPPoE for WAN access, WH-5420CPE provides flexible configuration for TTL value. The default value is 255 and does not have to change in a normal situation. You can check with your ISP/WISP if TTL value causes connection problem.

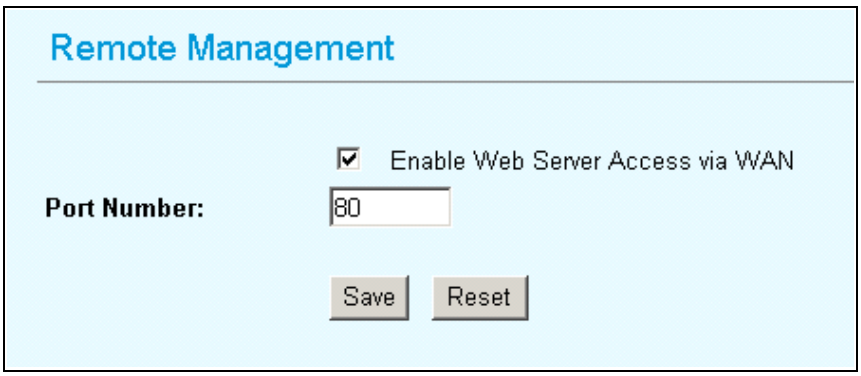


- **Virtual Server:** You can use Virtual Server Settings to provide connection on internet. For example, you can have your own web server at home and provide access on internet. This will need port 80 by default for Virtual Server Settings.

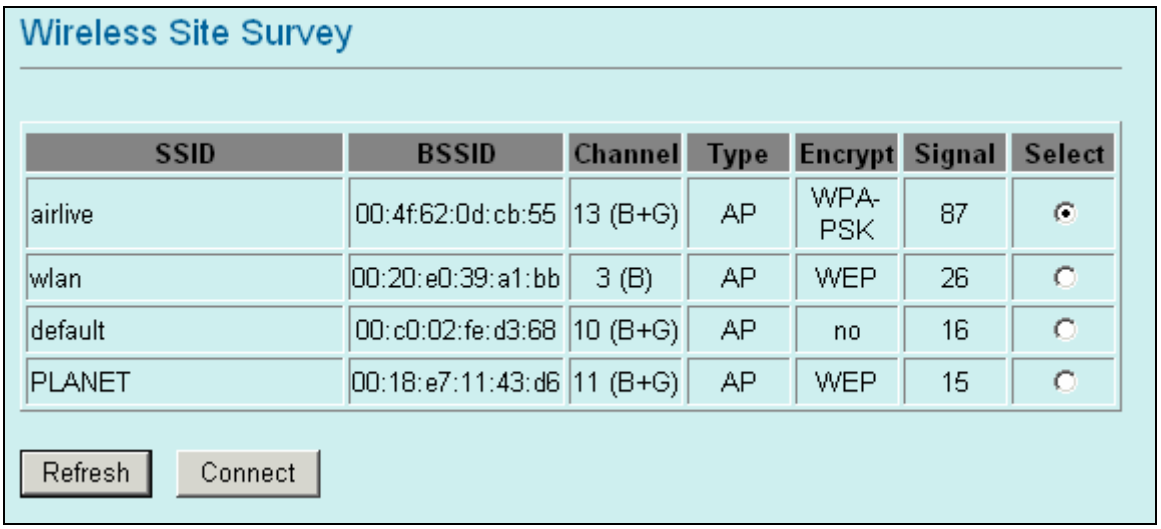


- **Special Application:** This is to enable internet service such as sound, video and so on. The routing firewall often stops these services for security reason.

- **DMZ:** You can use DMZ Settings to provide connection on internet. For example, you can have your own web server at home and provide access on internet. This will need port 80 by default for Virtual Server Settings.
- **Remote Management:** This is to configure WH-5420CPE be managed from internet. Note that port 80 is always used by web service. You can change the port to prevent conflict.

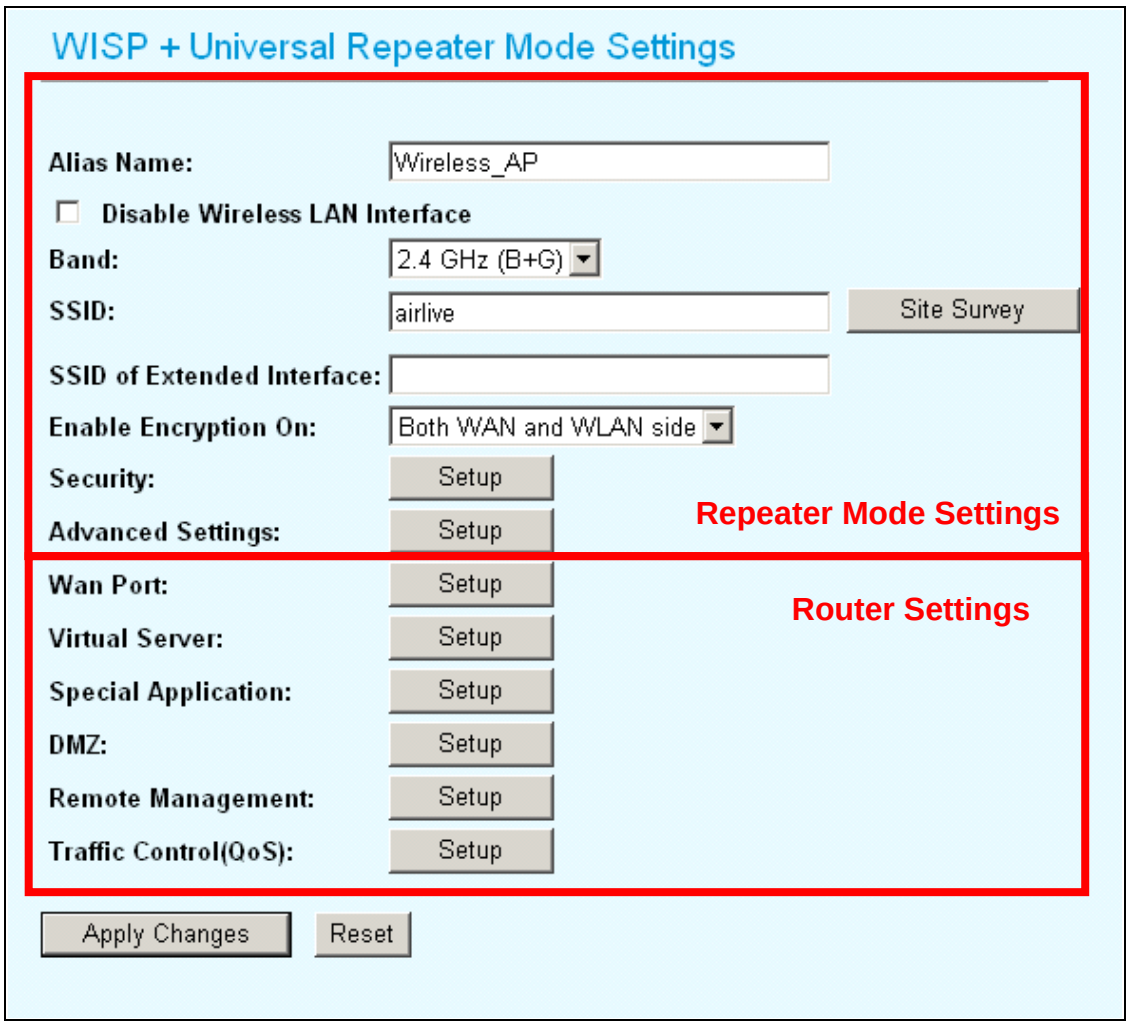


- **Site Survey:** Site survey helps to find out available access point around. You can also check to prevent using same SSID or channel with other AP.



To configure the security connection, please refer to Section 3.9 Wireless Security Settings ……
To configure the Advanced Settings, please refer to Section 3.10 Advanced Wireless Settings ……
To configure the access control, please refer to Section 3.11 Access Control Settings ……
To configure the Traffic Control, please refer to Section 3.12 Access Control Settings ……

3.7 WISP + Universal Mode Settings



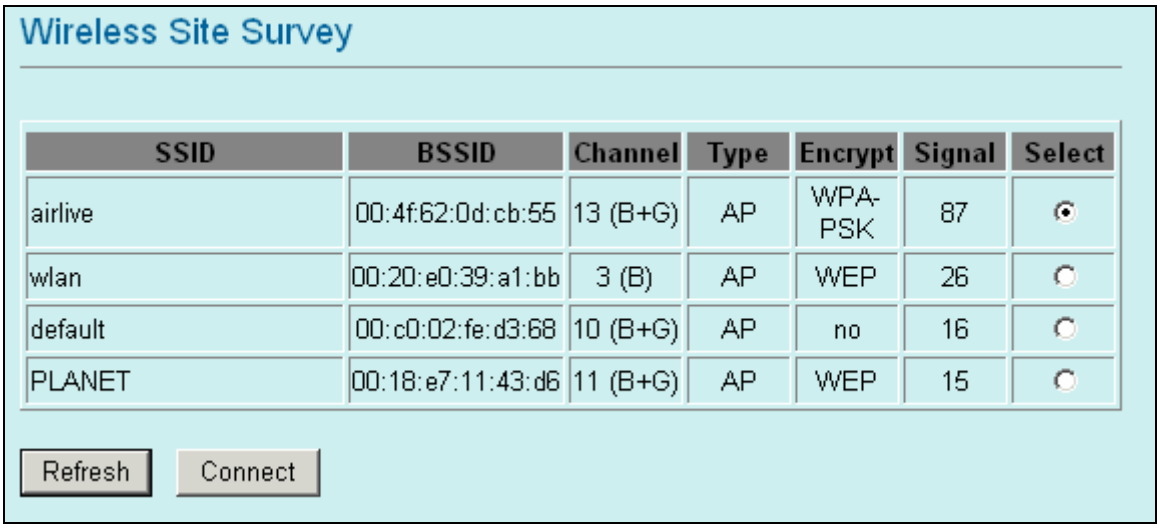
- **Alias Name**: Another name for WH-5420CPE.
- **Disable Wireless LAN Interface:** Check the box to disable the Wireless LAN Interface, by so doing, you won't be able to make wireless connection with this Access Point in the network you are located. In other words, this device will not be visible by any wireless station.
- **Band:** You can choose one mode of the following you need.
    - 2.4GHz (B): 802.11b supported rate only.
    - 2.4GHz (G): 802.11g supported rate only.
    - 2.4GHz (B+G): 802.11b supported rate and 802.11g supported rate.

  The default is 2.4GHz (B+G) mode.
- **SSID (Network ID):** The SSID differentiates one WLAN from another; therefore, all access points and all devices attempting to connect to a specific WLAN must use the same SSID. It is case-sensitive and must not exceed 32 characters. A device will not be permitted to join the BSS unless it can provide the unique SSID. An SSID is also

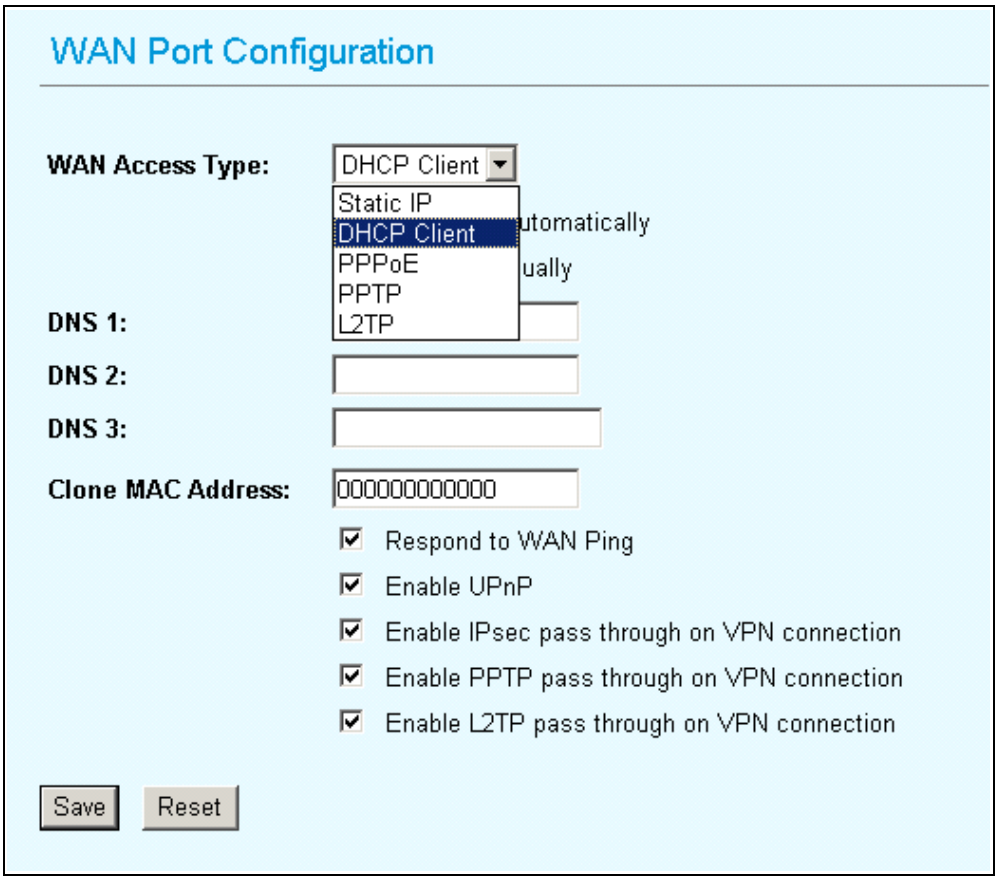
referred to as a network name because essentially it is a name that identifies a wireless network.

In this mode, the SSID is the remote WISP CPE to connect to.

- **Site Survey:** Site survey helps to find out available access point around. You can also check to prevent using same SSID or channel with other AP.

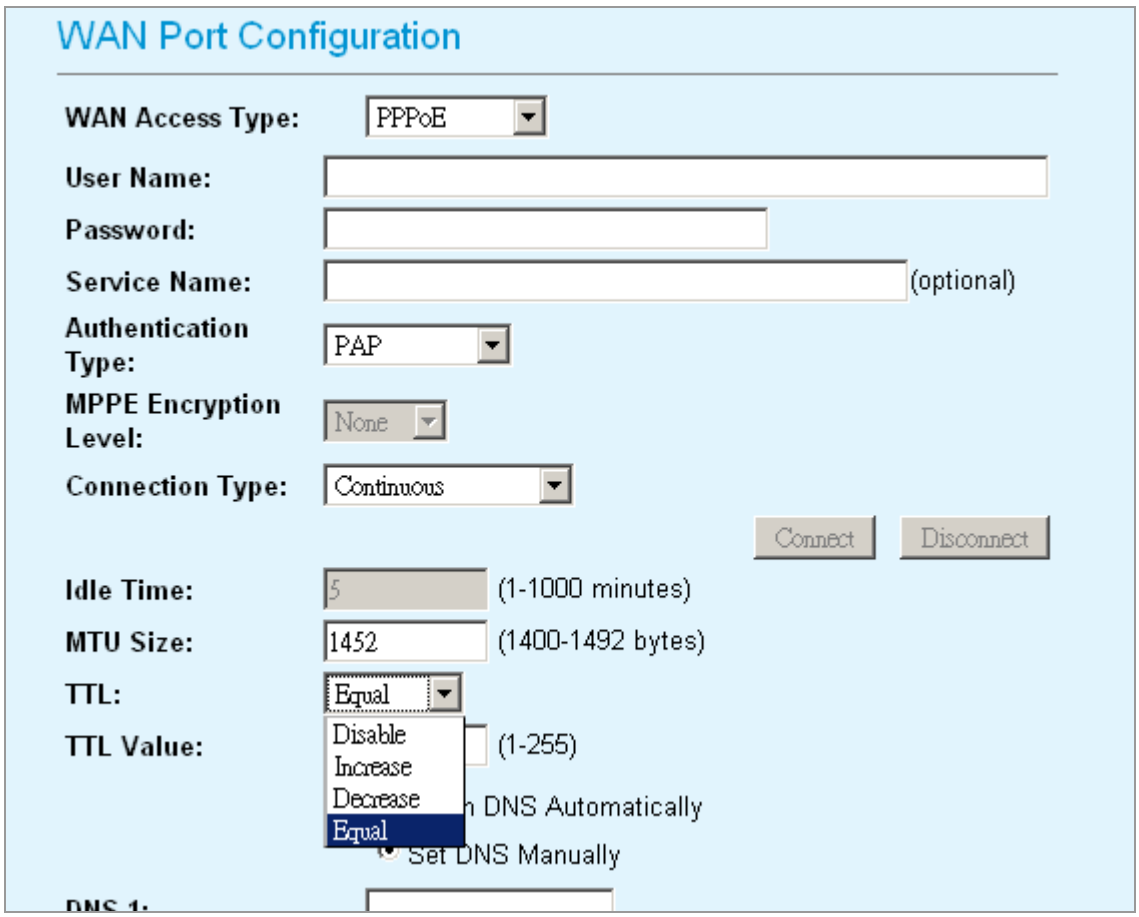


- **SSID of Extended Interface:** This field is the SSID of remote Access Point to connect to.
- **WAN Port:** Allow user to set the channel manually or automatically. If set channel manually, just select the channel you want to specify. If **"Auto"** is selected, user can set the channel range to have Wireless Access Point automatically survey and choose the channel with best situation for communication. The number of channels supported depends on the region of this Access Point. All stations communicating with the Access Point must use the same channel.
- **WAN Port:** WH-5420CPE provides 4 methods for client to access the internet. This depends on the location and the service which the ISP provides. You need to contact the ISP for detail information.

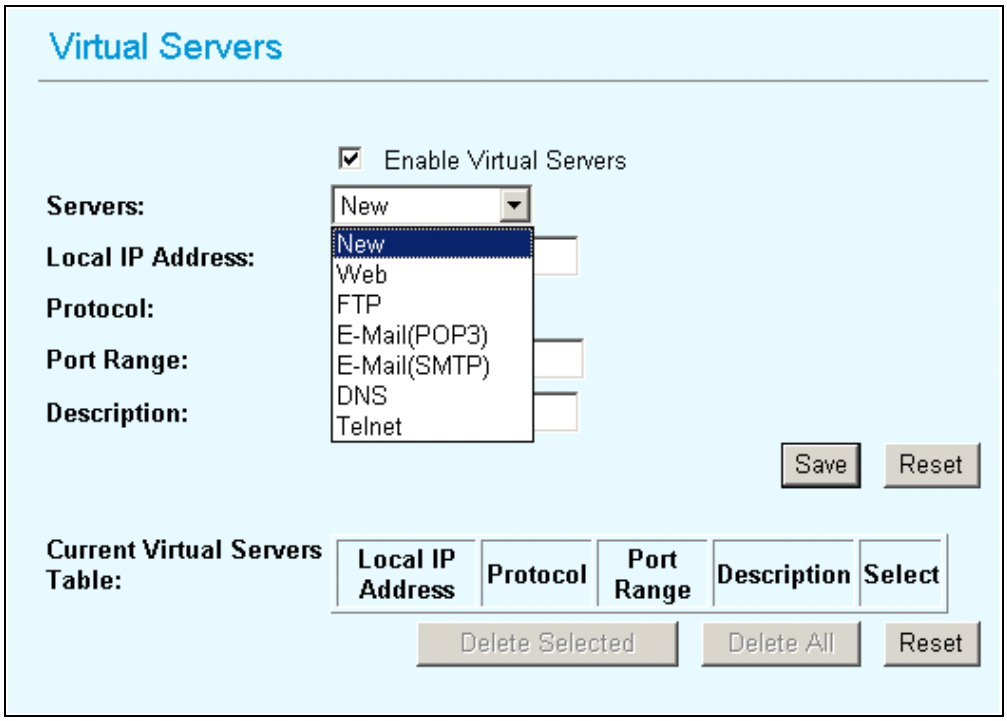


Some ISP/WISP has special inquire for TTL feature that did not decrease the TTL value when pass the first router of ISP/WISP.

When using PPPoE for WAN access, WH-5420CPE provides flexible configuration for TTL value. The default value is 255 and does not have to change in a normal situation. You can check with your ISP/WISP if TTL value causes connection problem.

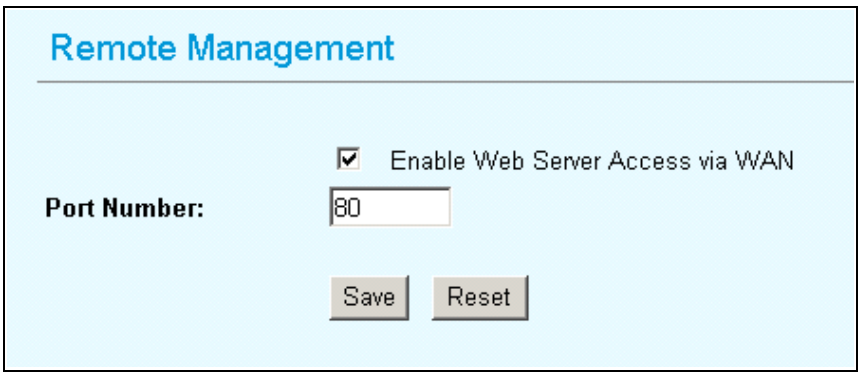


- **Virtual Server:** You can use Virtual Server Settings to provide connection on internet. For example, you can have your own web server at home and provide access on internet. This will need port 80 by default for Virtual Server Settings.



- **Special Application:** This is to enable internet service such as sound, video and so on. The routing firewall often stops these services for security reason.

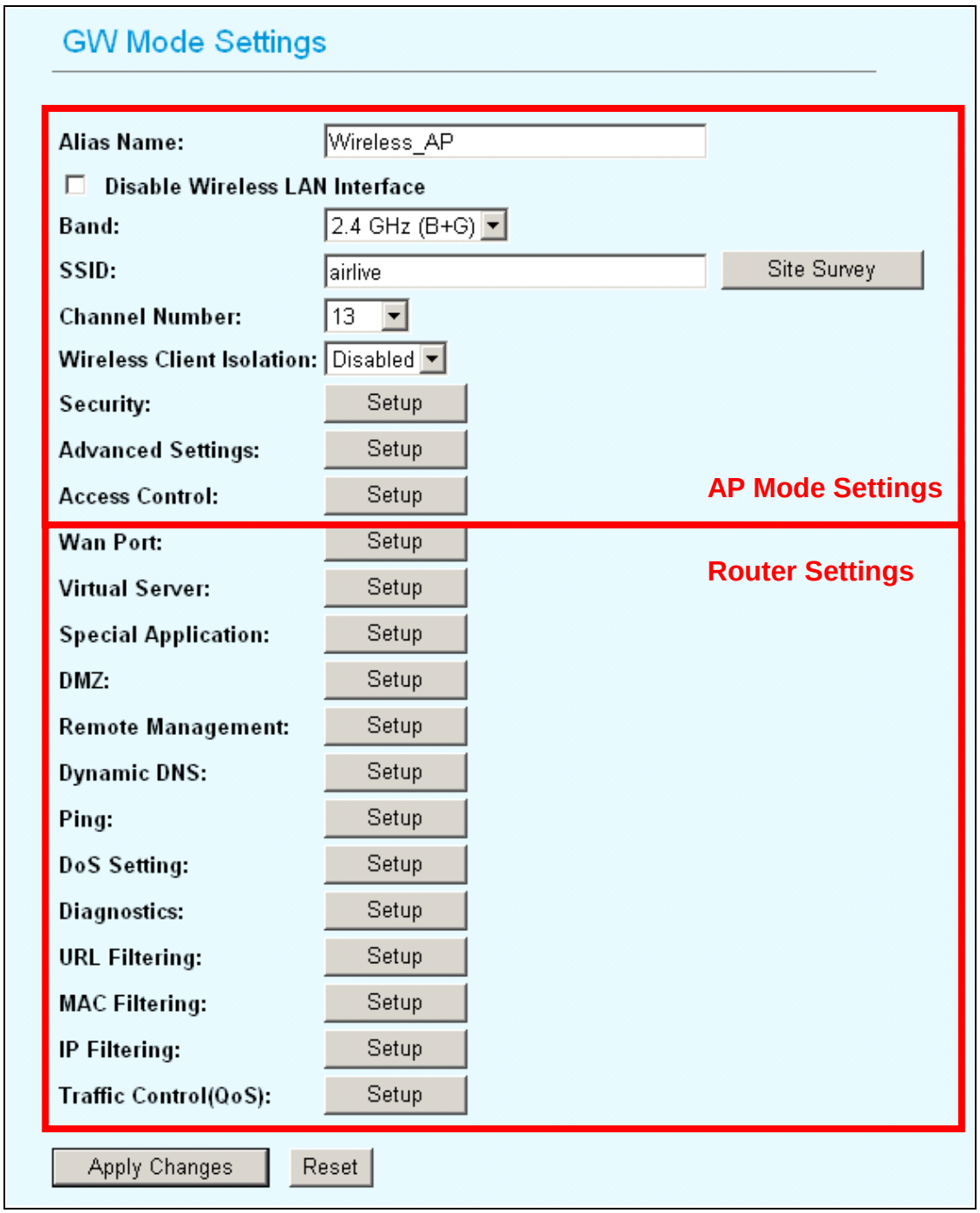
- **DMZ:** You can use DMZ Settings to provide connection on internet. For example, you can have your own web server at home and provide access on internet. This will need port 80 by default for Virtual Server Settings.
- **Remote Management:** This is to configure WH-5420CPE be managed from internet. Note that port 80 is always used by web service. You can change the port to prevent conflict.



To configure the security connection, please refer to Section 3.9 Wireless Security Settings ……
To configure the Advanced Settings, please refer to Section 3.10 Advanced Wireless Settings ……
To configure the access control, please refer to Section 3.11 Access Control Settings ……
To configure the Traffic Control, please refer to Section 3.12 Access Control Settings ……

3.8 Gateway Mode (AP + Router) Settings

Important Notice: When change to Gateway mode, the LAN 2 becomes to WAN port.

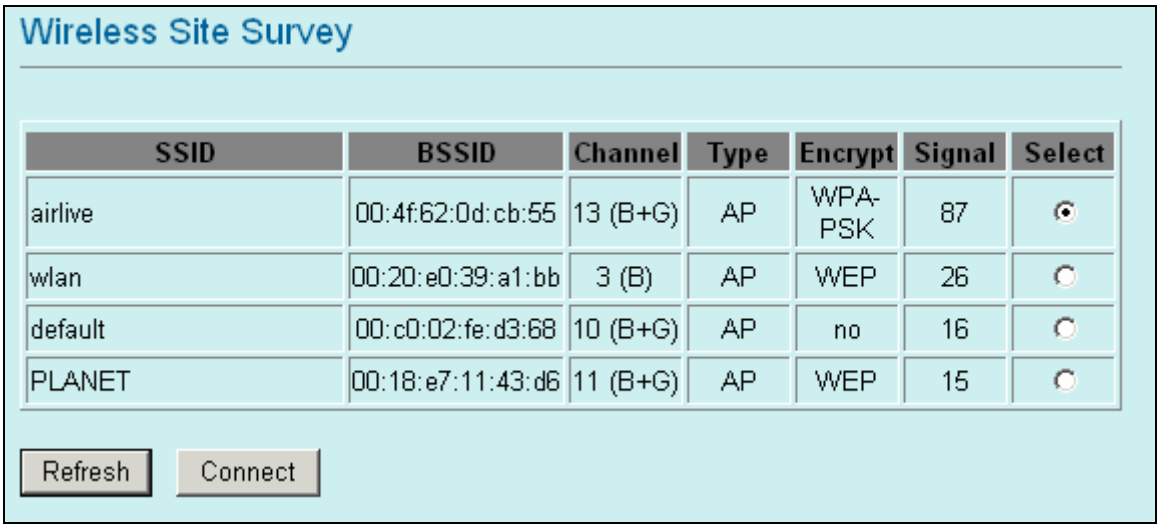


- **Alias Name**: Another name for WH-5420CPE.
- **Disable Wireless LAN Interface:** Check the box to disable the Wireless LAN Interface, by so doing, you won't be able to make wireless connection with this Access Point in the network you are located. In other words, this device will not be visible by any wireless station.

- **Band:** You can choose one mode of the following you need.
  - 2.4GHz (B): 802.11b supported rate only.
  - 2.4GHz (G): 802.11g supported rate only.
  - 2.4GHz (B+G): 802.11b supported rate and 802.11g supported rate.

  The default is 2.4GHz (B+G) mode.

- **Site Survey:** Site survey helps to find out available access point around. You can also check to prevent using same SSID or channel with other AP.



- **SSID (Network ID):** The SSID differentiates one WLAN from another; therefore, all access points and all devices attempting to connect to a specific WLAN must use the same SSID. It is case-sensitive and must not exceed 32 characters. A device will not be permitted to join the BSS unless it can provide the unique SSID. An SSID is also referred to as a network name because essentially it is a name that identifies a wireless network.

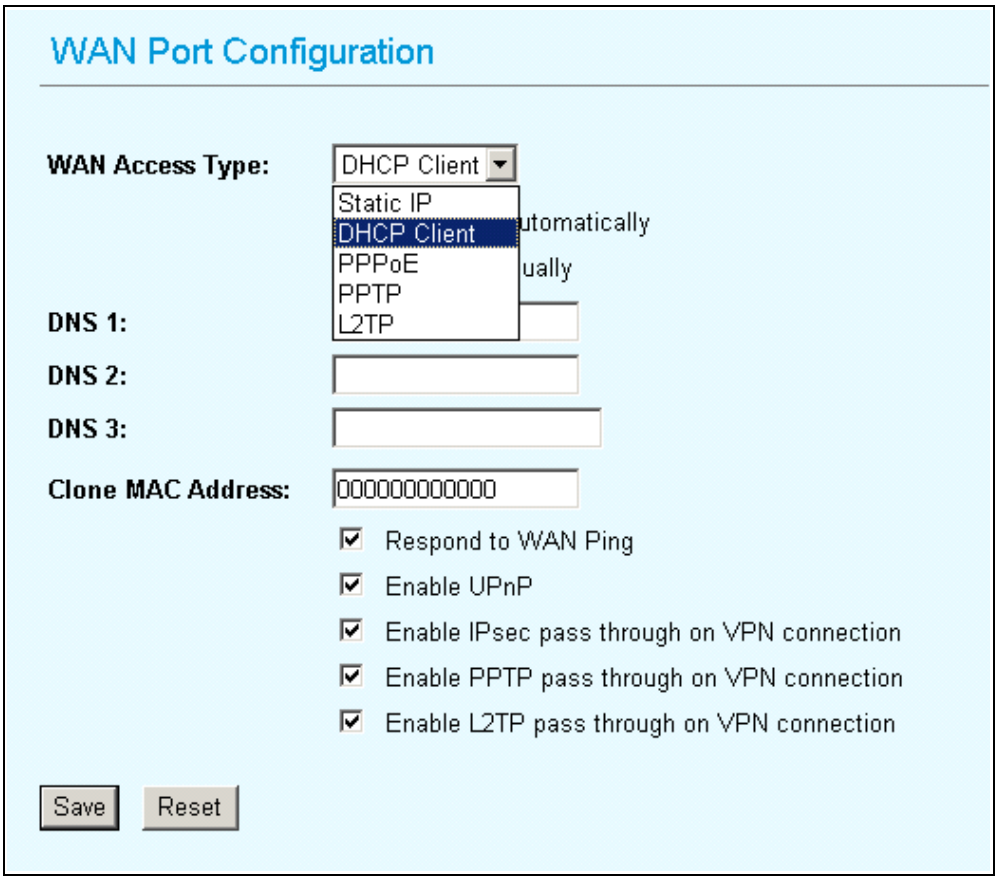
  In this mode, the SSID is provided for client connection.

- **Channel Number:** Allow user to set the channel manually or automatically. If set channel manually, just select the channel you want to specify. If **"Auto"** is selected, user can set the channel range to have Wireless Access Point automatically survey and choose the channel with best situation for communication. The number of channels supported depends on the region of this Access Point. All stations communicating with the Access Point must use the same channel.

- **Wireless Client Isolation:** This is to separate wireless client if needed. Wireless clients can not communicate to each other if the field is enabled.

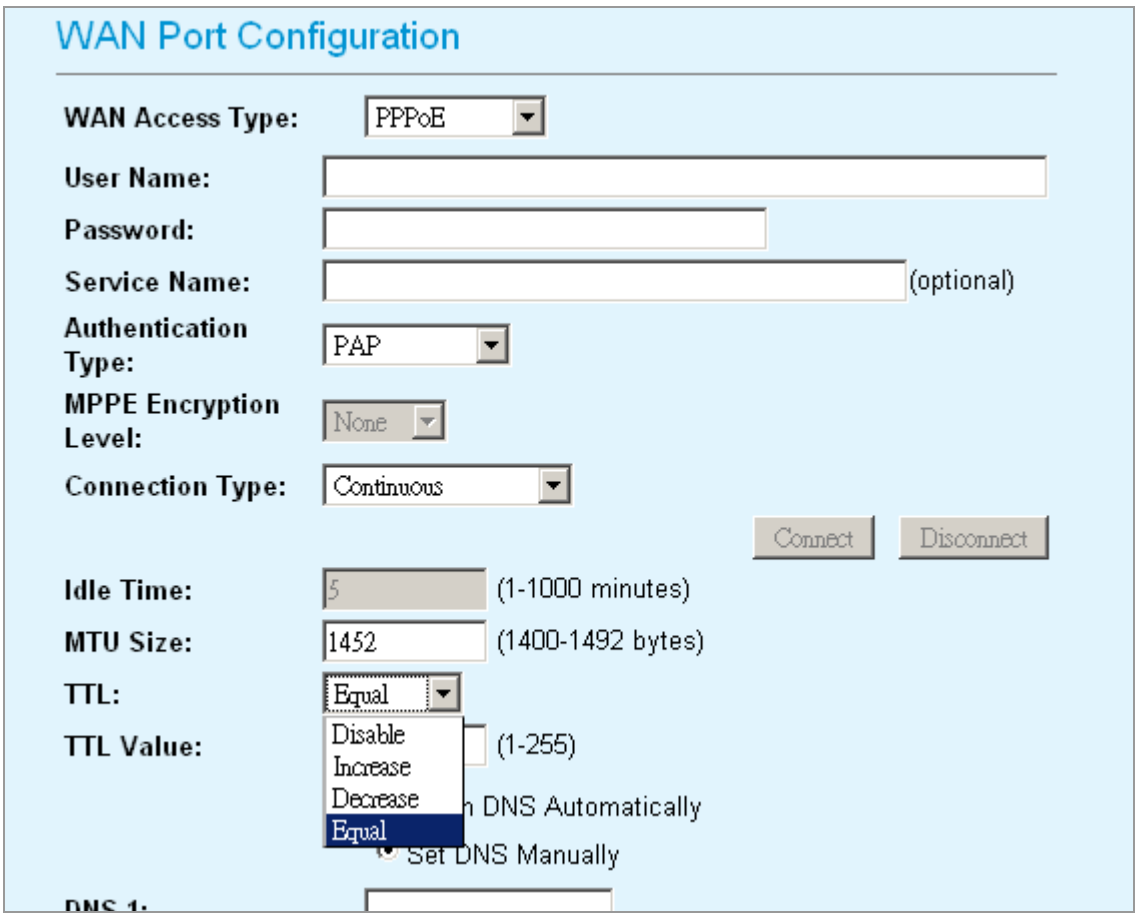
- **Site Survey:** Site survey helps to find out available access point around. You can also check to prevent using same SSID or channel with other AP.

- **WAN Port (LAN1):** WH-5420CPE provides 4 methods for client to access the internet. This depends on the location and the service which the ISP provides. You need to contact the ISP for detail information.

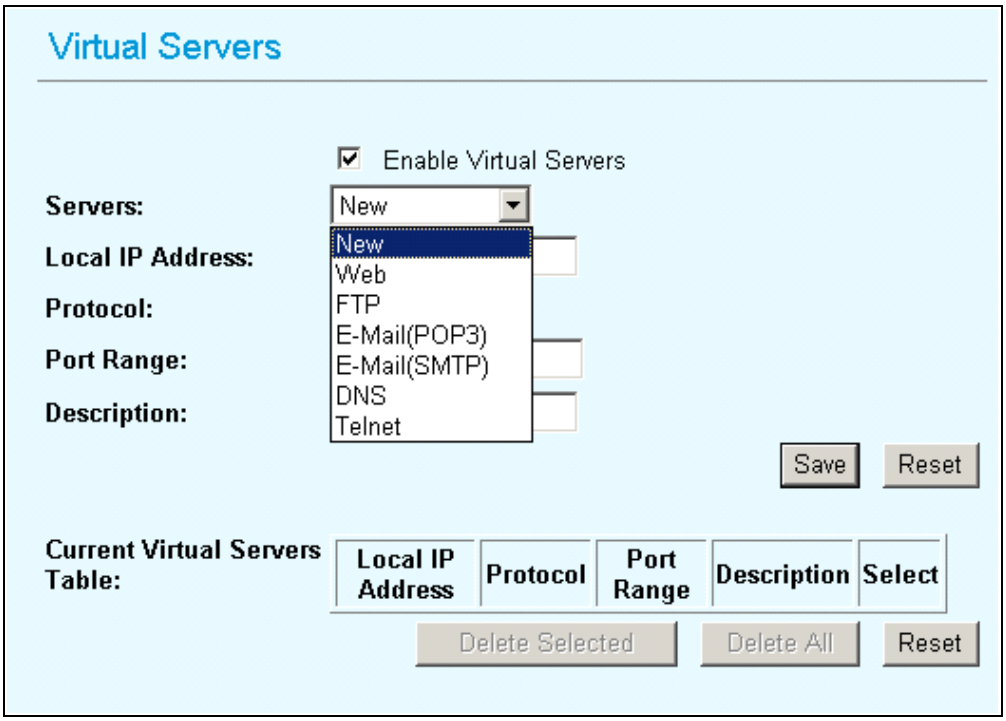


Some ISP/WISP has special inquire for TTL feature that did not decrease the TTL value when pass the first router of ISP/WISP.

When using PPPoE for WAN access, WH-5420CPE provides flexible configuration for TTL value. The default value is 255 and does not have to change in a normal situation. You can check with your ISP/WISP if TTL value causes connection problem.



- **Virtual Server:** You can use Virtual Server Settings to provide connection on internet. For example, you can have your own web server at home and provide access on internet. This will need port 80 by default for Virtual Server Settings.



- **Special Application:** This is to enable internet service such as sound, video and so on. The routing firewall often stops these services for security reason.

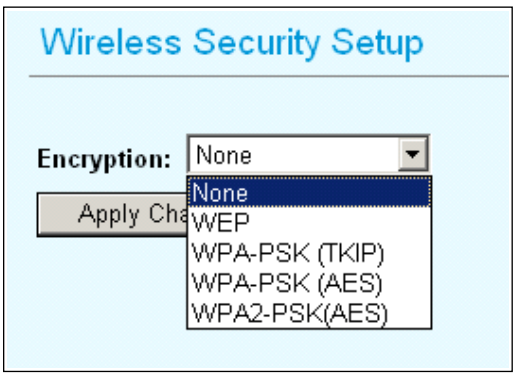
- **DMZ:** You can use DMZ Settings to provide connection on internet. For example, you can have your own web server at home and provide access on internet. This will need port 80 by default for Virtual Server Settings.
- **Remote Management:** This is to configure WH-5420CPE be managed from internet. Note that port 80 is always used by web service. You can change the port to prevent conflict.
- **Dynamic DNS:** Dynamic DNS (DDNS) allows you to create a hostname that points to your dynamic IP or static IP address or URL. WH-5420CPE provide Dynamic DNS client using DynDNS, please visit http://www.dyndns.org for detail.
- **Ping:** You can enable to the “Response to WAN Ping” to allow remotely ping your WH-5420CPE.
- **DoS Setting:** In WH-5420CPE, a denial-of-service attack (DoS attack) can block or limit the system sending network flood to your local computer.
- **Diagnostics:** The nslookup command can be used in diagnostics to find the IP addresses of a particular computer, using DNS lookup. The name means "name server lookup". The most common version of the program is included as part of the BIND package.
- **URL Filtering:** The URL filter database is used for internet filtering that blocks access to unwanted web content by URLs.
- **MAC Filtering:** Enables you to allow or deny Internet access to users within the LAN based upon the MAC address of their network interface.
- **IP Filtering:** The IP filter function enables you to define a minimum and maximum IP address range filter; all IP addresses falling within the range are not allowed Internet access

To configure the security connection, please refer to Section 3.9 Wireless Security Settings ……
To configure the Advanced Settings, please refer to Section 3.10 Advanced Wireless Settings ……
To configure the access control, please refer to Section 3.11 Access Control Settings ……
To configure the Traffic Control, please refer to Section 3.12 Access Control Settings ……

3.9 Wireless Security

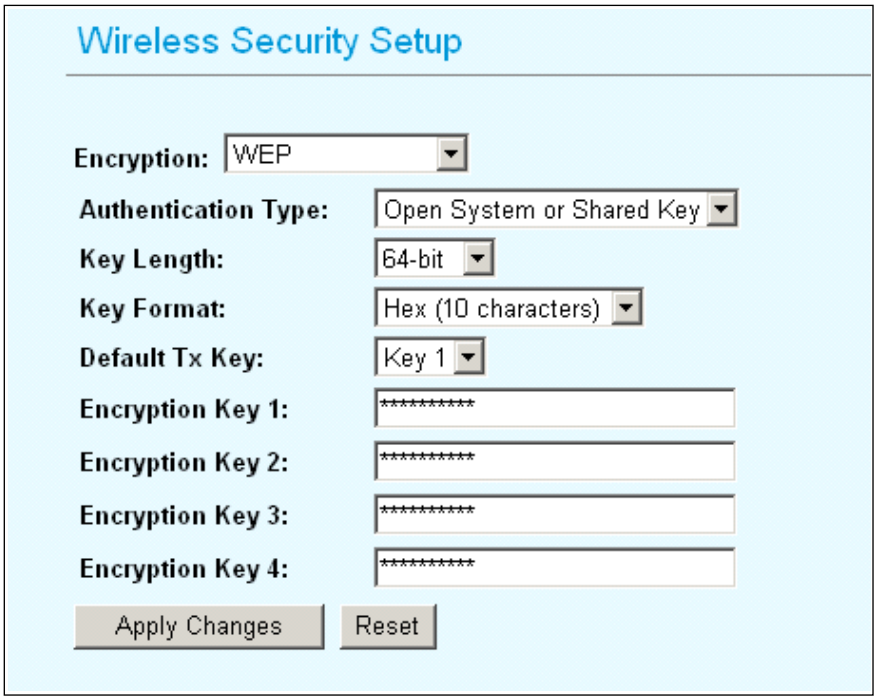
Here you can configure the security of your wireless network. Selecting different method will enable you to have different level of security. Please note that by using any encryption, by which data packet is encrypted before transmission to prevent data packets from being eavesdropped by unrelated people,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

WH-5420CPE provides WEP, WPA-PSK (TKIP), WPA2-PSK (AES) and WPA2-PSK (AES) security policy.



WEP

WEP allows you to use data encryption to secure your data from being eavesdropped by malicious people. It allows 2 types of key: 64 (WEP64) and 128 (WEP128). 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 and a WEP128 key is 13 bytes

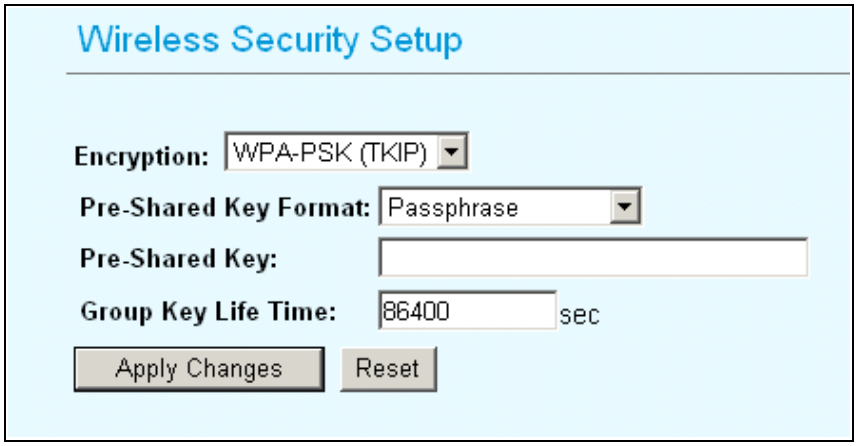
Default Tx Key: You have to specify which of the four keys will be active.
Once you enable the WEP function, please make sure that both the WH-5420CPE and the wireless client stations use the same key.

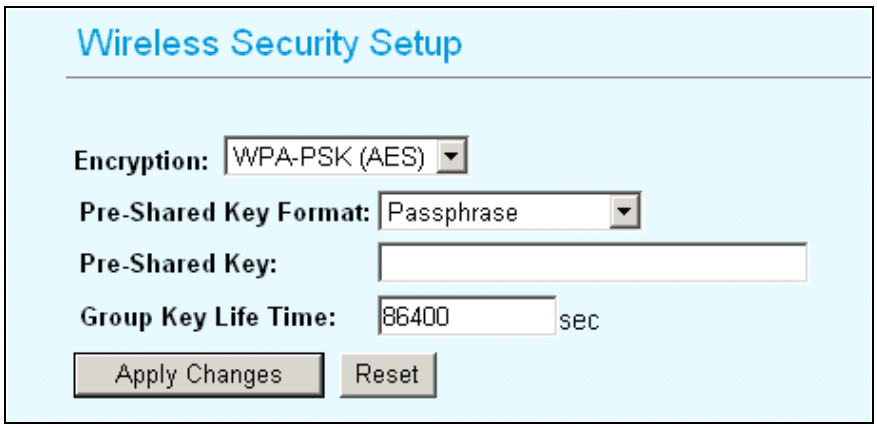
Some wireless client cards only allow Hexadecimal digits for WEP keys. Please note that when configuring WEP keys, a WEP128 ASCII key looks like "**This is a key**"(13 characters), while a WEP128 Hex key looks like "**546869732069732061206b6579**"(26 HEX) (hexadecimal notation are 0-9 and A-F).

WPA-PSK (TKIP) / WPA-PSK (AES)

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

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.



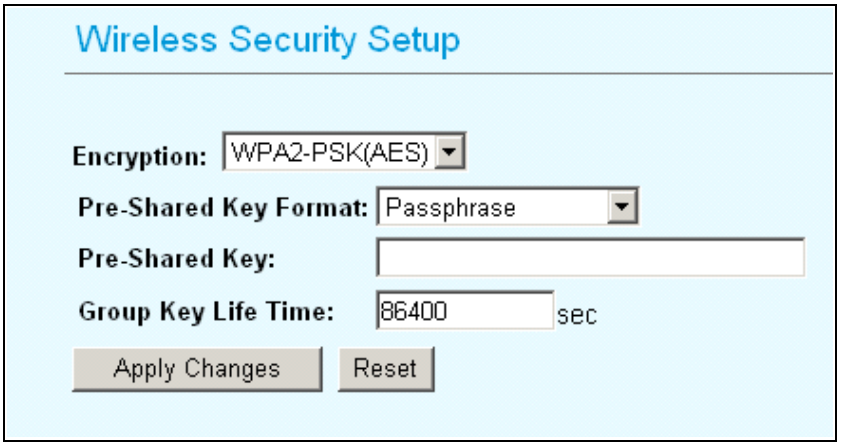


Pre-shared Key: This is an ASCII string with 8 to 63 characters. Please make sure that both the WH-5420CPE and the wireless client stations use the same key.

Group Key Life Time: 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 (AES)

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



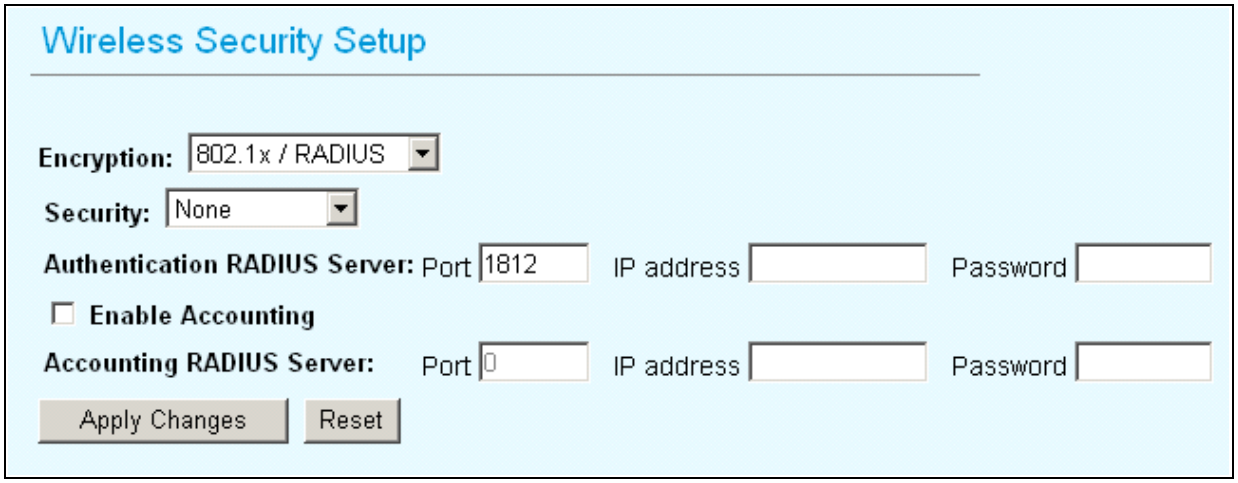
Pre-shared Key: This is an ASCII string with 8 to 63 characters. Please make sure that both the WH-5420CPE and the wireless client stations use the same key.

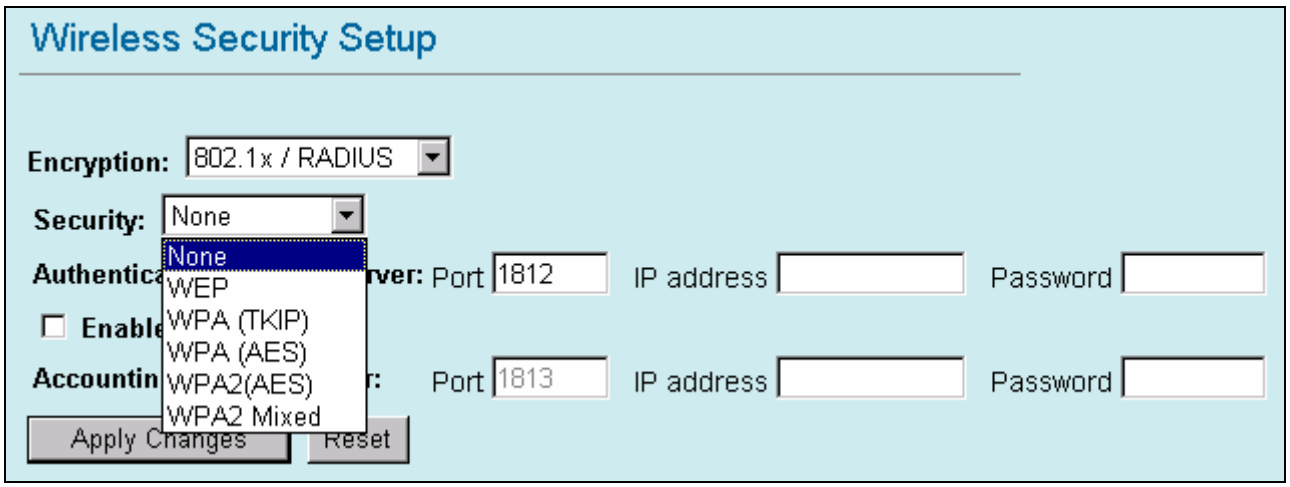
Encryption Type: There are two encryption types **TKIP** and **CCMP (AES)**. While CCMP provides better security than TKIP, some wireless client stations may not be equipped with the hardware to support it.

Group key Life Time: 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.

802.1X (Radius)

Authentication by the remote server (RADIUS Server).





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

- **WEP:** 802.1x Authentication is enabled and the RADIUS Server will proceed to check the 802.1x Authentication, and make the RADIUS server to issue the WEP key dynamically. You can select WEP 64bits or WEP 128bits for data encryption.
- **WPA (TKIP) / WPA (AES):** WPA-RADIUS authentication use WPA (Wi-Fi Protect Access) data encryption for 802.1x authentication. WPA is an encryption standard proposed by WiFi for advance protection by utilizing a password key (TKIP) or certificate. It is more secure than WEP encryption.
- **WPA2-AES / WPA2-Mixed:** The two most important features beyond WPA to become standardized through 802.11i/WPA2 are: pre-authentication, which enables secure fast roaming without noticeable signal latency. Pre-authentication provides a way to establish a PMK security association before a client associates. The advantage is that the client reduces the time that it's disconnected to the network.

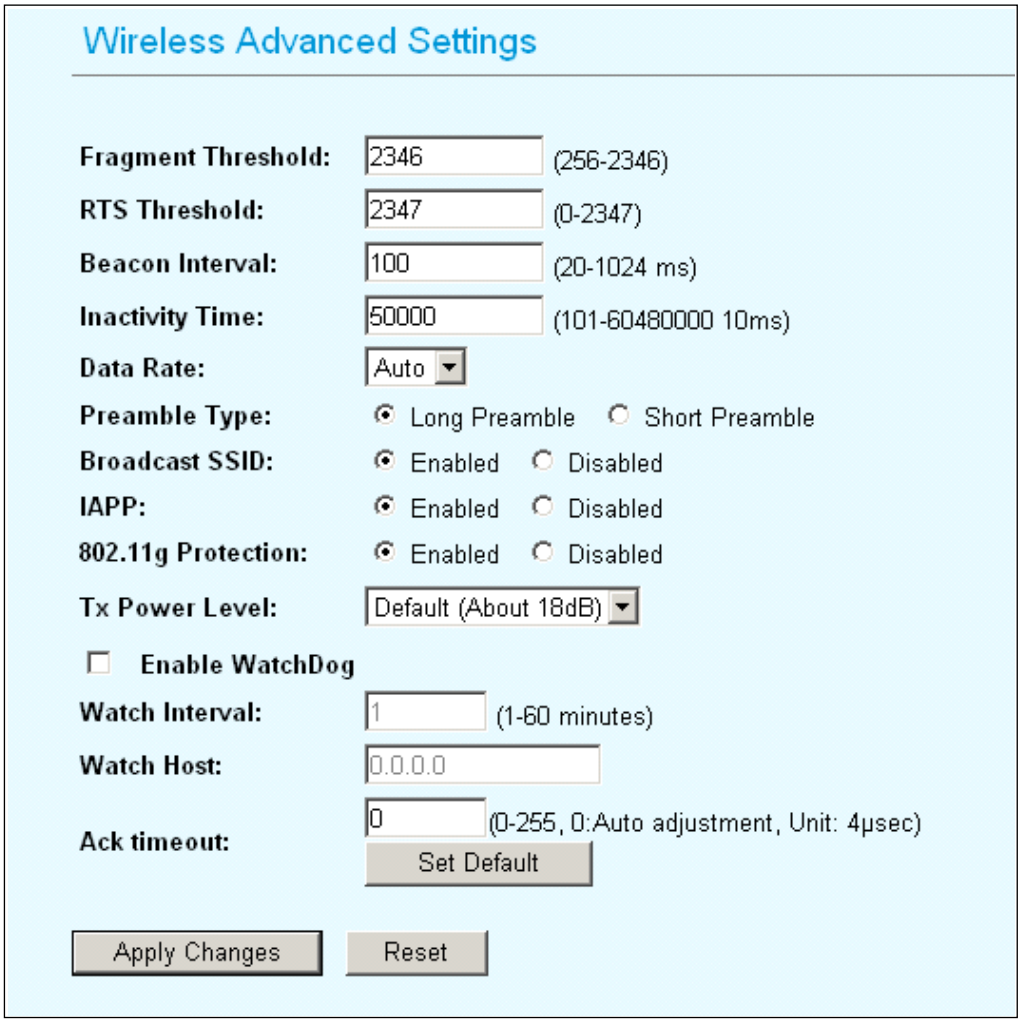
Authentication RADIUS Server: Enter the RADIUS Server IP address and Password provided by your ISP.

- **Port:** Enter the RADIUS Server’s port number provided by your ISP. The default is 1812.
- **IP Address:** Enter the RADIUS Server’s IP Address provided by your ISP.
- **Password:** Enter the password that the AP shares with the RADIUS Server.

Accounting RADIUS Server: Enter the Accounting RADIUS Server IP address and Password provided by your ISP.

3.10 Advanced Wireless Settings

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



Fragmentation: Fragmentation mechanism is used for improving the efficiency when high traffic flows along in the wireless network. If your 802.11g Wireless LAN PC Card often transmit large files in wireless network, you can enter new Fragment Threshold value to split the packet. The value can be set from 256 to 2346. The default value is 2346.

RTS Threshold: RTS Threshold is a mechanism implemented to prevent the **"Hidden Node"** problem. "Hidden Node" is a situation in which two stations are within range of the same Access Point, but are not within range of each other. Therefore, they are hidden nodes for each other. When a station starts data transmission with the Access Point, it might not notice that the other station is already using the wireless medium. When these two stations send data at the same time, they might collide when arriving simultaneously at the Access Point. The collision will most certainly result in a loss of messages for both stations.

Thus, the RTS Threshold mechanism provides a solution to prevent data collisions. When you enable RTS Threshold on a suspect "hidden station", this station and its Access Point will use a Request to Send (RTS). The station will send an RTS to the Access Point, informing that it is going to transmit the data. Upon receipt, the Access Point will respond with a CTS message to all station within its range to notify all other stations to defer

transmission. It will also confirm the requestor station that the Access Point has reserved it for the time-frame of the requested transmission.
If the “Hidden Node” problem is an issue, please specify the packet size. The RTS mechanism will be activated if the data size exceeds the value you set..
The default value is 2347.

Warning: Enabling RTS Threshold will cause redundant network overhead that could negatively affect the throughput performance instead of providing a remedy.

This value should remain at its default setting of 2347. Should you encounter inconsistent data flow, only minor modifications of this value are recommended.

Beacon Interval: Beacon Interval is the amount of time between beacon transmissions. Before a station enters power save mode, the station needs the beacon interval to know when to wake up to receive the beacon (and learn whether there are buffered frames at the access point).

Data Rate: By default, the unit adaptively selects the highest possible rate for transmission. Select the basic rates to be used among the following options: Auto, 1, 2, 5.5, 11or 54 Mbps. For most networks the default setting is Auto which is the best choice. When Auto is enabled the transmission rate will select the optimal rate. If obstacles or interference are present, the system will automatically fall back to a lower rate.

Preamble Type: A preamble is a signal used in wireless environment to synchronize the transmitting timing including Synchronization and Start frame delimiter. In a "noisy" network environment, the Preamble Type should be set to Long Preamble. The Short Preamble is intended for applications where minimum overhead and maximum performance is desired. If in a "noisy" network environment, the performance will be decreased.

Broadcast SSID: Select enabled to allow all the wireless stations to detect the SSID of this Access Point.

IAPP: IAPP (Inter Access Point Protocol) is designed for the enforcement of unique association throughout a ESS (Extended Service Set) and a secure exchange of station’s security context between current access point (AP) and new AP during handoff period.

802.11g Protection: The 802.11g standard includes a protection mechanism to ensure mixed 802.11b and 802.11g operation. If there is no such kind of mechanism exists, the two kinds of standards may mutually interfere and decrease network’s performance.

Tx Power Level: For countries that impose limit on WLAN output power, it might be necessary to reduce TX (transmit) power. There are 7 TX Power Levels to choose from —

select a level to make sure that the output power measured at the antenna end will not exceed the legal limit in your country.

Enable WatchDog: Check and enable this watch dog function.

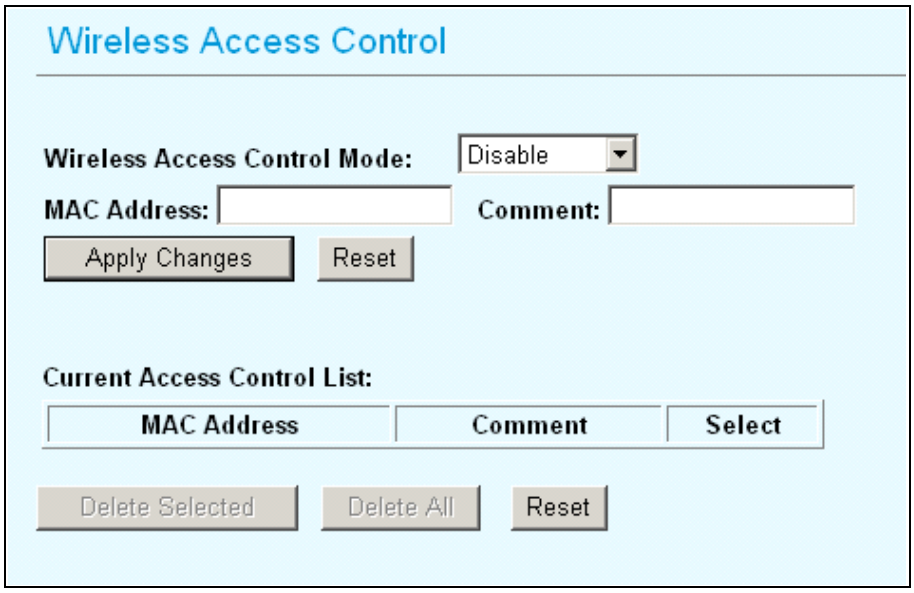
Watch Interval: Setup the interval time for watch dog function between 1 to 60 mins.

Watch Host: Enter the watch dog host ip address.

Ack timeout: When a packet is sent out from one wireless station to the other, it will waits for an Acknowledgement frame from the remote station. If the ACK is NOT received within that timeout period then the packet will be re-transmitted resulting in reduced throughput. If the ACK setting is too high then throughput will be lost due to waiting for the ACK Window to timeout on lost packets. By having the ability to adjust the ACK setting we can effectively optimize the throughput over long distance links. This is especially true for 802.11a and 802.11g networks
You can set as default for auto adjustment.

3.11 Access Control

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



Wireless Access Control Mode: Select the Access Control Mode from the pull-down menu.

- **Disable:** Select to disable Wireless Access Control Mode.
- **Allow Listed:** Only the stations shown in the table can associate with the AP.
- **Deny Listed:** Stations shown in the table won't be able to associate with the AP.

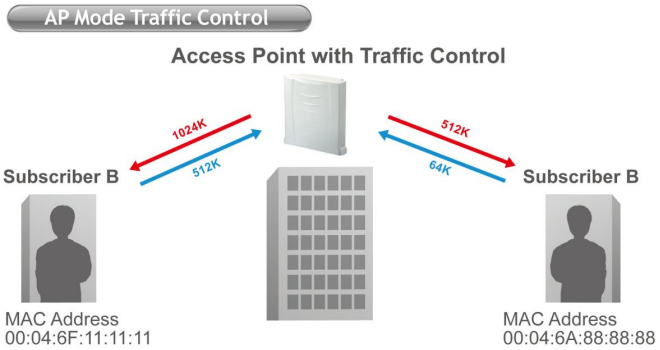
MAC Address: Enter the MAC Address of a station that is allowed to access this Access Point.

Comment: You may enter up to 20 characters as a remark to the previous MAC Address.

3.12 QoS Traffic Control

What is Traffic Control QoS?

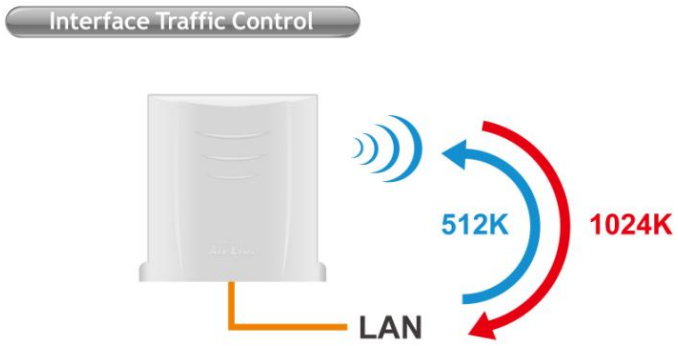
Traffic Control is a great tool to control the bandwidth of the WISP subscribers. Therefore, the WISP operators can offer different class of connection speeds for different subscription fees - just like the ADSL service! The AirLive advance firmware can control the bandwidth by Interface or IP/MAC.



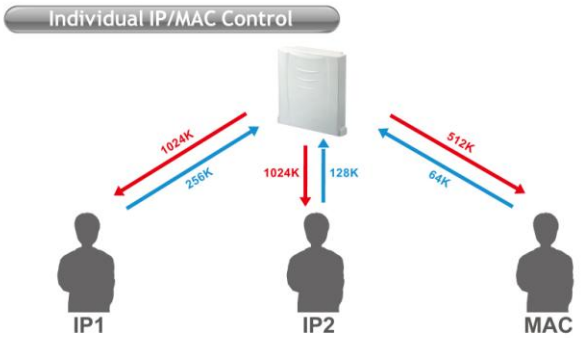
What type of Traffic Bandwidth Control does the firmware offer?

The Traffic Bandwidth limits the “Maximum Data Rate”. There are 2 types of Traffic Control it offers.

Interface Control



The interface QoS controls the data rate at the WLAN and LAN interfaces. Therefore, all traffics are controlled the same way. This type of traffic control is suitable when AP is used as a Client AP in “Client Mode” and WISP mode. So WISP can control the maximum data rate



Individual IP/MAC Control

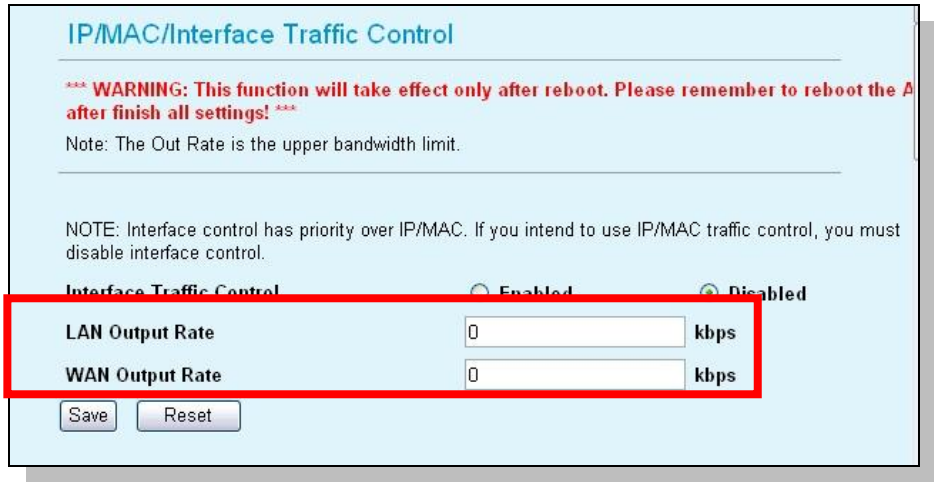
The AP can set the maximum data rate for each IP or MAC addresses. This type of traffic control is most suitable for outdoor AP in “AP” or “Gateway” mode.

What is the Output Rate?

The “Output Rate” is the data speed out of an interface. There are 3 types Output Rate supported by the AP

1. **LAN Output Rate**: This is the speed of the traffic out of the LAN port. In gateway mode, the LAN Output Rate includes both the wired LAN and WLAN interface.
2. **WLAN Output Rate**: This is the speed of the traffic out of the Wireless LAN
3. **WAN Output Rate**: This is the speed of the traffic out of the WAN port. In WISP mode, the WAN Output Rate also includes the WLAN interface.

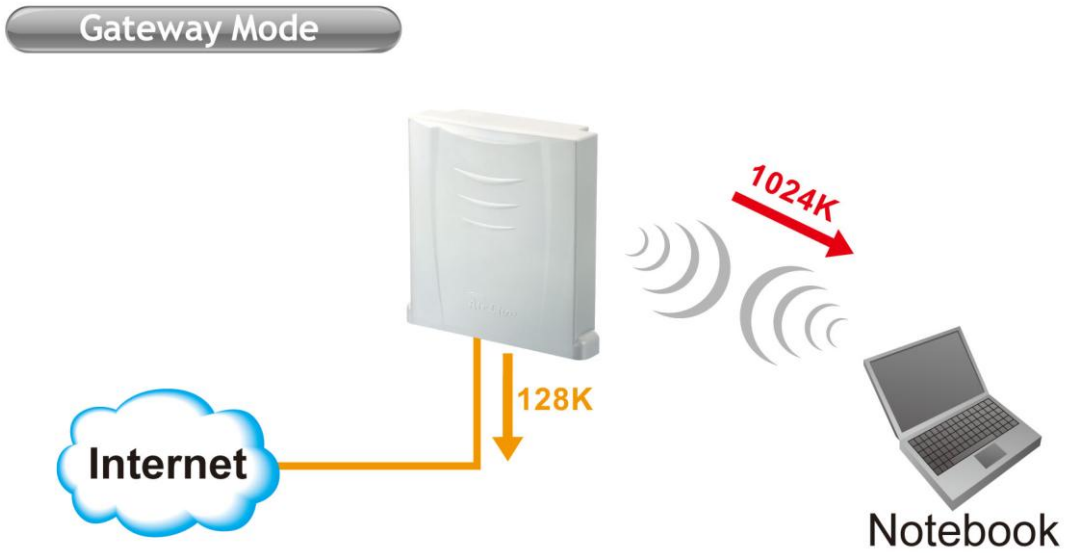
The AP's Web UI will tell you which types of output rate it supports, it differs in each wireless mode.



In the following example:

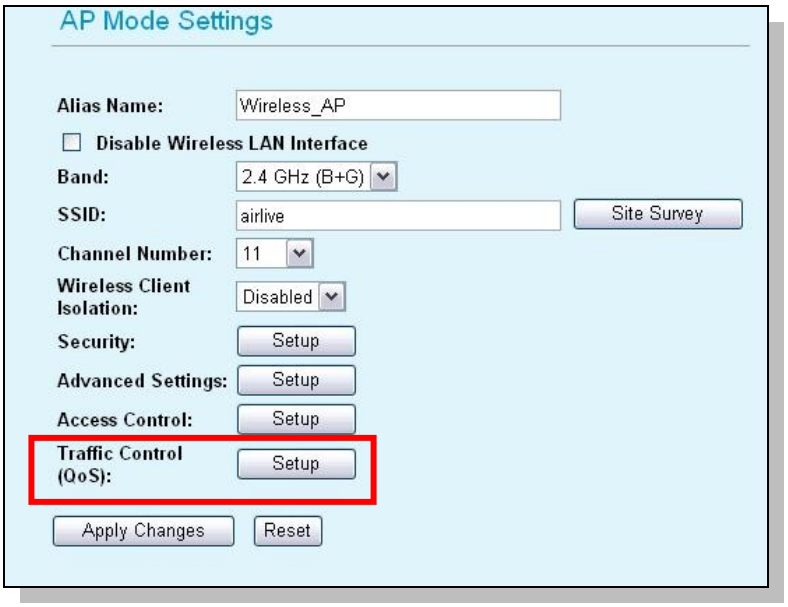
- The AP is in Gateway Mode
- The WAN Output Rate is 128K
- The LAN/WLAN Output Rate is 1024K

In this setup, the notebook users get an upstream bandwidth of 128K and downstream bandwidth of 1024K.

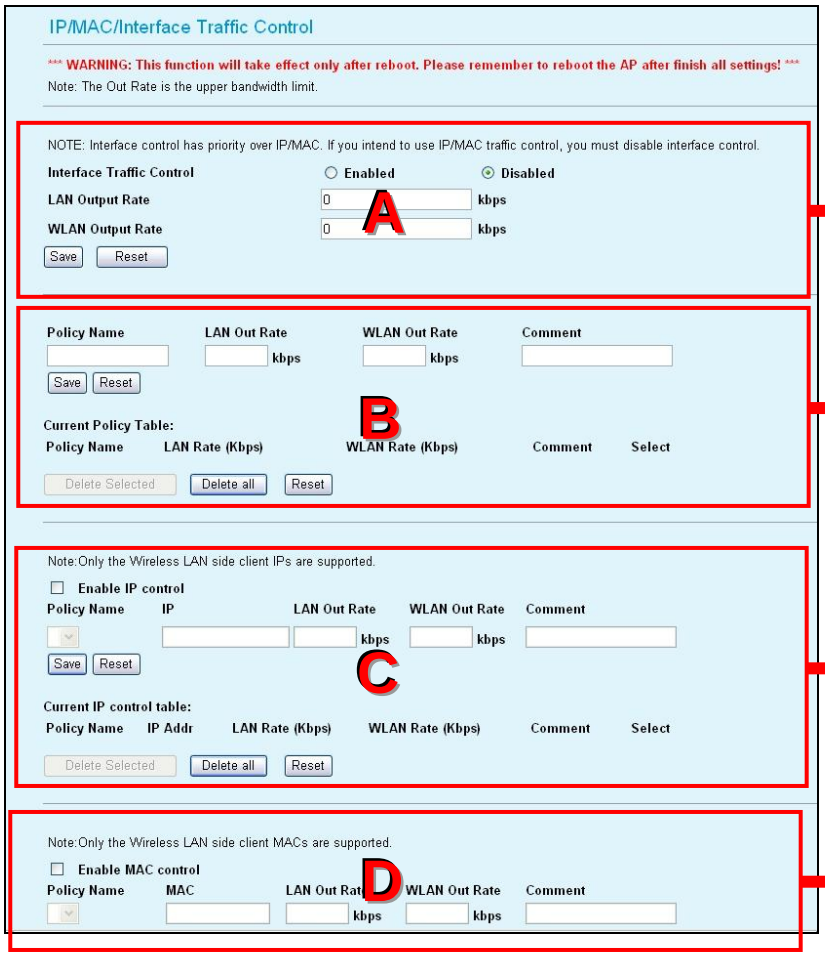


Configure the Traffic Control QoS

From the Mode Setting page, please choose the “Traffic Control(QoS)” on the bottom of the list.



Once you click on the “setup” button, a new window will pop-up with the Traffic Control settings. They are divided into “A”, “B”, “C”, “D” section for further explanations.



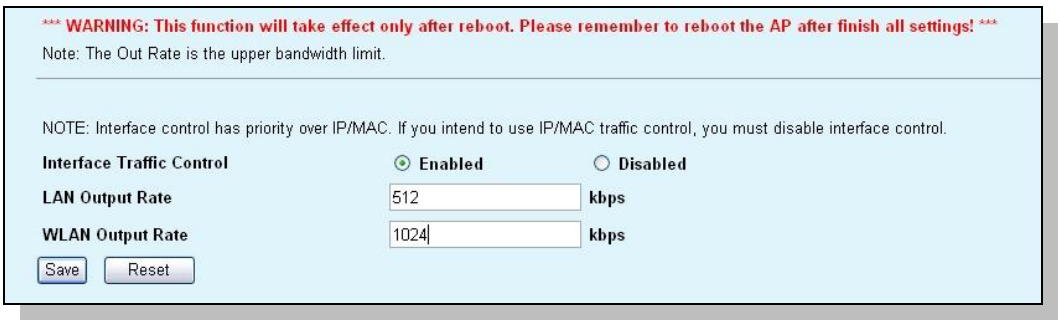
This section is the “Interface Control” session. You must disable the “interface Traffic Control” if you want to use the “IP/MAC Traffic Control”

This section is for defining the “Policy” of “Individual IP/MAC Traffic Control”. Once a policy is defined, it can be chosen as template in IP/MAC Traffic Control Settings

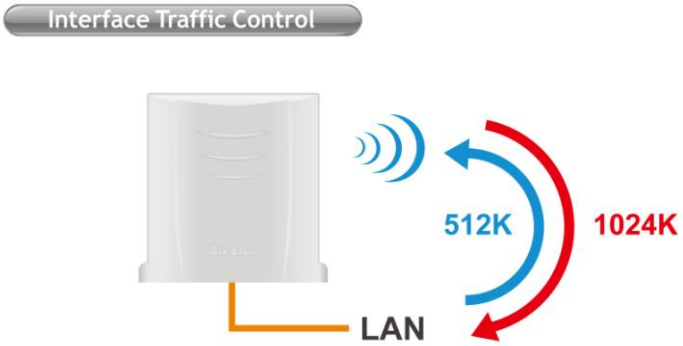
This section is to configure the bandwidth by IP address. You can control more than one IP address.

This section is to configure the bandwidth by MAC address. You can control more than one MAC address.

A. Interface Control Settings:



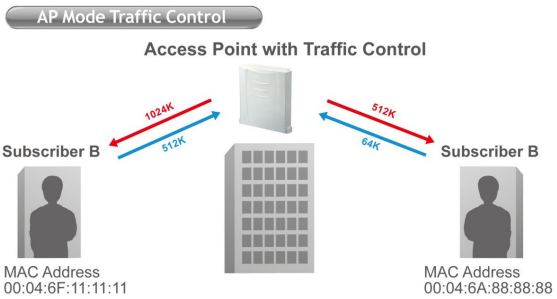
In the Interface Control Settings, the AP only controls the total bandwidth limit of an interface. For example, if you want to limit the output data rate of the LAN to 512K and the output data rate of WLAN to 1024K. You should perform the following steps:



1. Enable the “Interface Traffic Control
2. Enter “512” in the “LAN Output Rate”
3. Enter “1024” in the “WLAN Output Rate”
4. Click on “Save”
5. Reboot the AP.

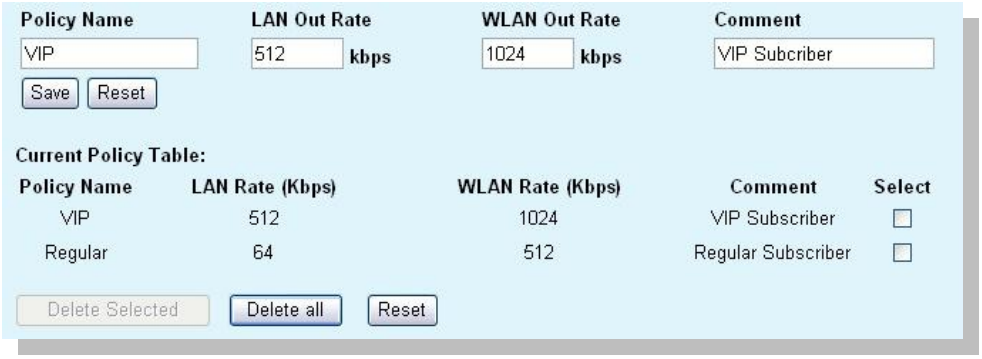
B. Define Policy

A policy is a set of bandwidth rules that can be used as a template. For example, if you want to provide 2 kinds of bandwidth speed to the users:



- VIP Subscriber:
  - LAN Out Rate: 512 Kbps
  - WLAN Out Rate: 1024 Kbps
- Regular Subscriber:
  - LAN Out Rate: 64 Kbps
  - WLAN Out Rate: 512 Kbps

You can configure the bandwidth rule as policies “VIP” and “Regular”.



Please follow the step below to create a new policy “VIP”

1. Enter “VIP” for the “PolicyName”
2. Enter “512” for the “LAN Out Rate”
3. Enter “1024” for the “WLAN Out Rate”
4. Enter “VIP Subscriber” for the “Comment”
5. Click on “Save” button
6. Now the “VIP” policy will show up in the “Current Policy Table”

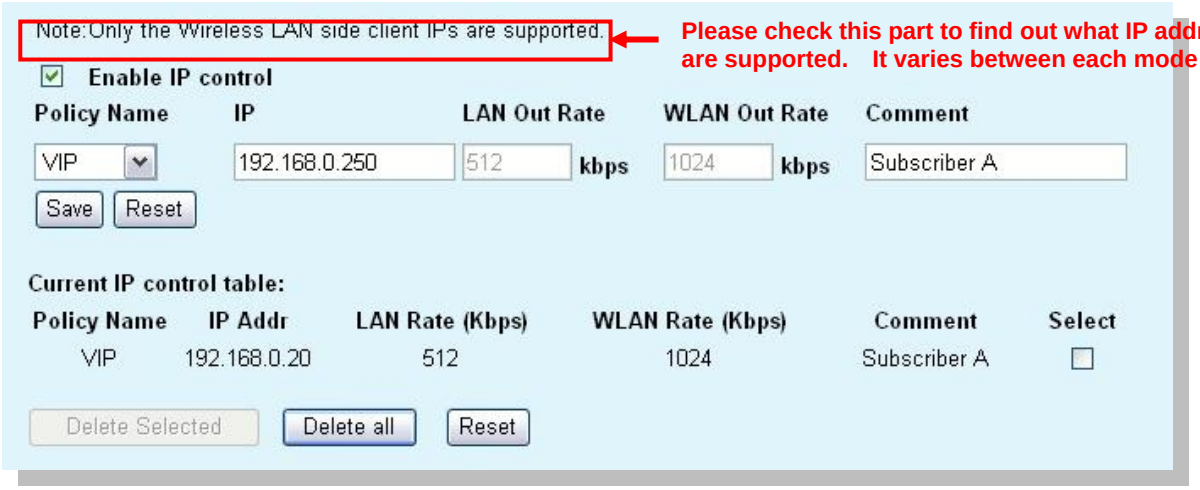
Once finished, the administrator will be able to choose the policy “VIP” for their IP/MAC Traffic Control.

C. Bandwidth Control by IP address

You can set the maximum bandwidth of a PC or a subscriber by using the IP Control.

Please follow the procedure below to setup IP Traffic Control

1. Please make sure the “Interface Traffic Control” is disabled
2. Before you start, please check the following area to see which client IPs are supported. It differs between each mode.



3. Enable the IP Control
4. If you have defined a Policy already, please choose a Policy name. The “Out Rates” will be automatically pasted from the Policy template. You cannot change the Out Rates if you have chosen a Policy

5. If you want to define new Data Rate, please do not choose any policies. Then you can enter the values in the “LAN”, “WLAN”, or “WAN” Out Rates.
6. Press “Save” to save settings
7. Reboot your AP.

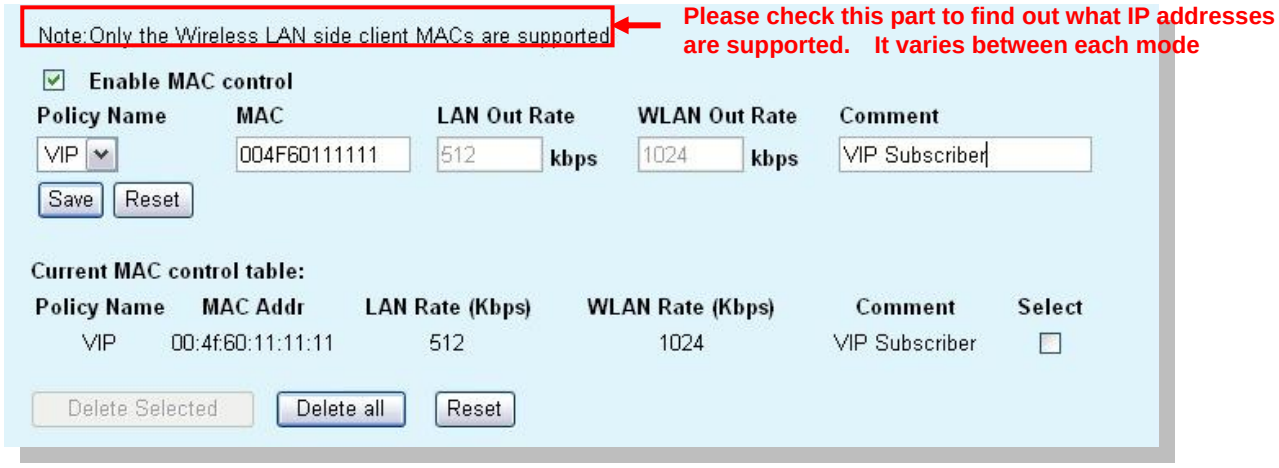
** If you want to control the traffic flow between the IPs in the same interface, please make sure both IPs are configured for the IP Traffic Control.*

D. Bandwidth Control by MAC address

You can set the maximum bandwidth of a PC or a subscriber by using the MAC Control.

Please follow the procedure below to setup MAC Traffic Control

1. Please make sure the “Interface Traffic Control” is disabled
2. Before you start, please check the following area to see which client MACs are supported. It differs between each mode.
3. Enable the MAC Control

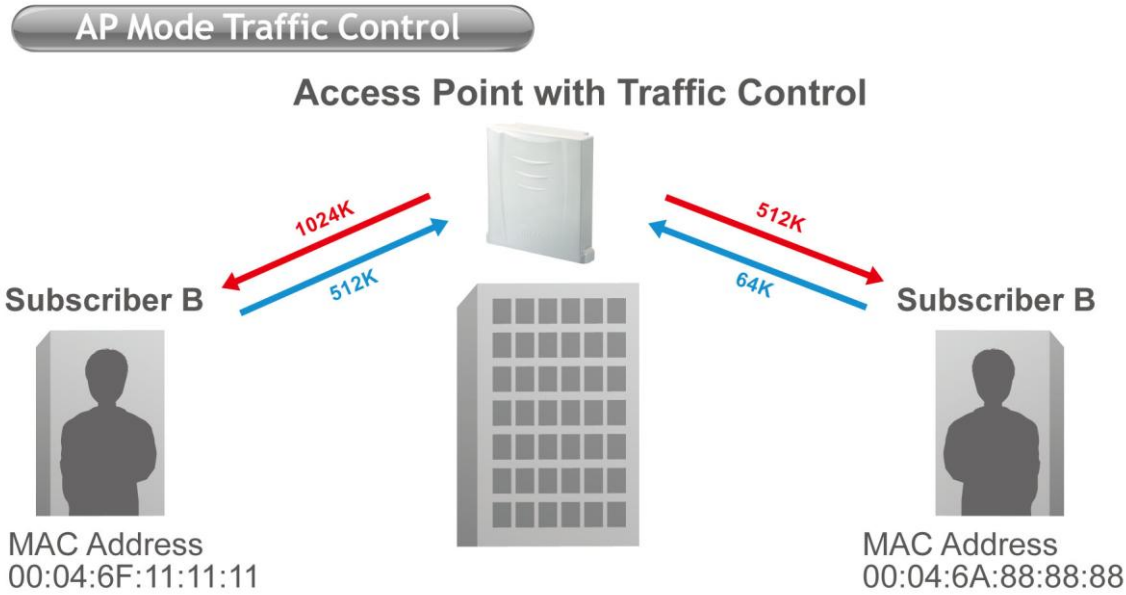


4. If you have defined a Policy already, please choose a Policy name. The “Out Rates” will be automatically pasted from the Policy template. You cannot change the Out Rates if you have chosen a Policy
5. If you want to define new Data Rate, please do not choose any policies. Then you can enter the values in the “LAN”, “WLAN”, or “WAN” Out Rates.
6. Press “Save” to save settings
7. Reboot your AP.

** If you want to control the traffic flow between MAC addresses in the same interface, please make sure both MAC addresses are configured for the MAC Traffic Control.*

Application Example

Example1: AP Mode Traffic Control



In this example, the AP is installed outdoor to provide Internet service. There are 2 different type of Internet service offered by the WISP:

- **VIP Service:**
  - Upstream Data Rate: 512 Kbps
  - Downstream Data Rate: 1024 Kbps
- **Regular Service**:
  - Upstream Data Rate: 64 Kbps
  - Downstream Data Rate: 512 Kbp

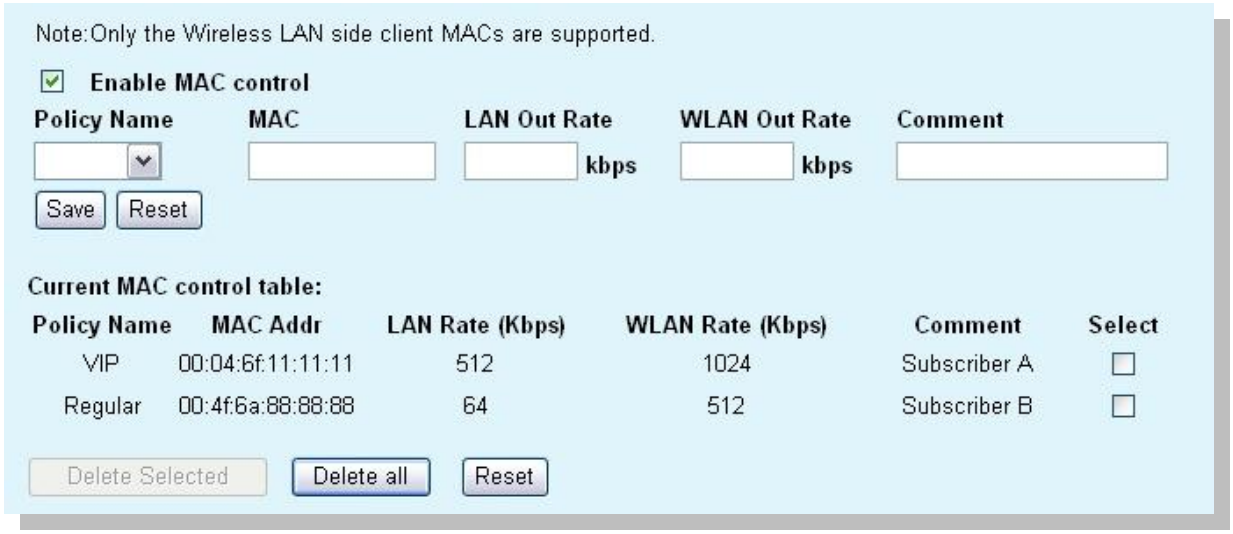
The Subscriber's information is as followed:

- Subscriber A
  - VIP Service
  - MAC Address of the PC or Wireless Client: 00:04:6F:11:11:11
- Subscriber B
  - Regular Service
  - MAC Address of the PC or Wireless Client: 00:04:6A:88:88:88

Step-by-Step Configuration

1. Please disable the "Interface Traffic Control"
2. On the Policy, please add the "VIP" and "Regular" policies as shown on the graph below

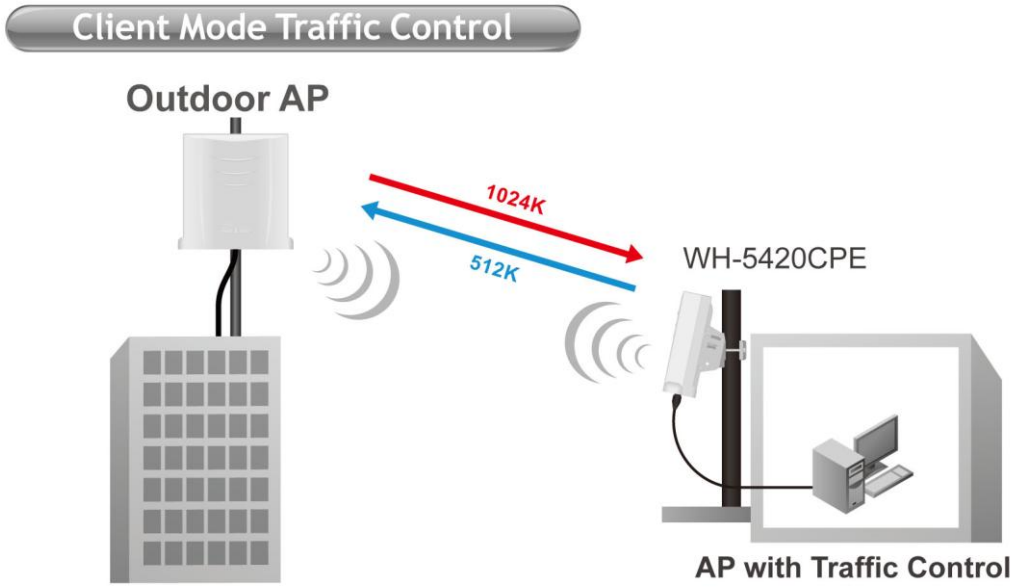
3. Please enable the “MAC Control”
4. Please fill in the 2 entries as shown on the graphic below



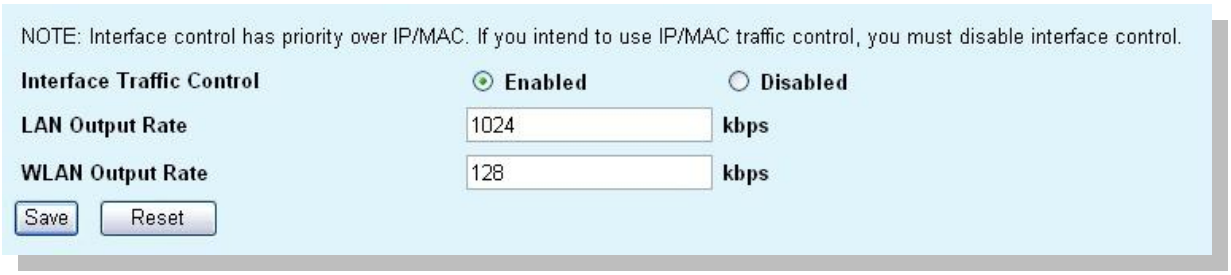
5. Reboot the AP

Example2: Client Mode Traffic Control

In the following example, the AP is used as the wireless client to the WISP Service. The Service provider need to restrict the bandwidth of the AP to 1024K Downstream and 128K Upstream.



Step-by-Step Configuration

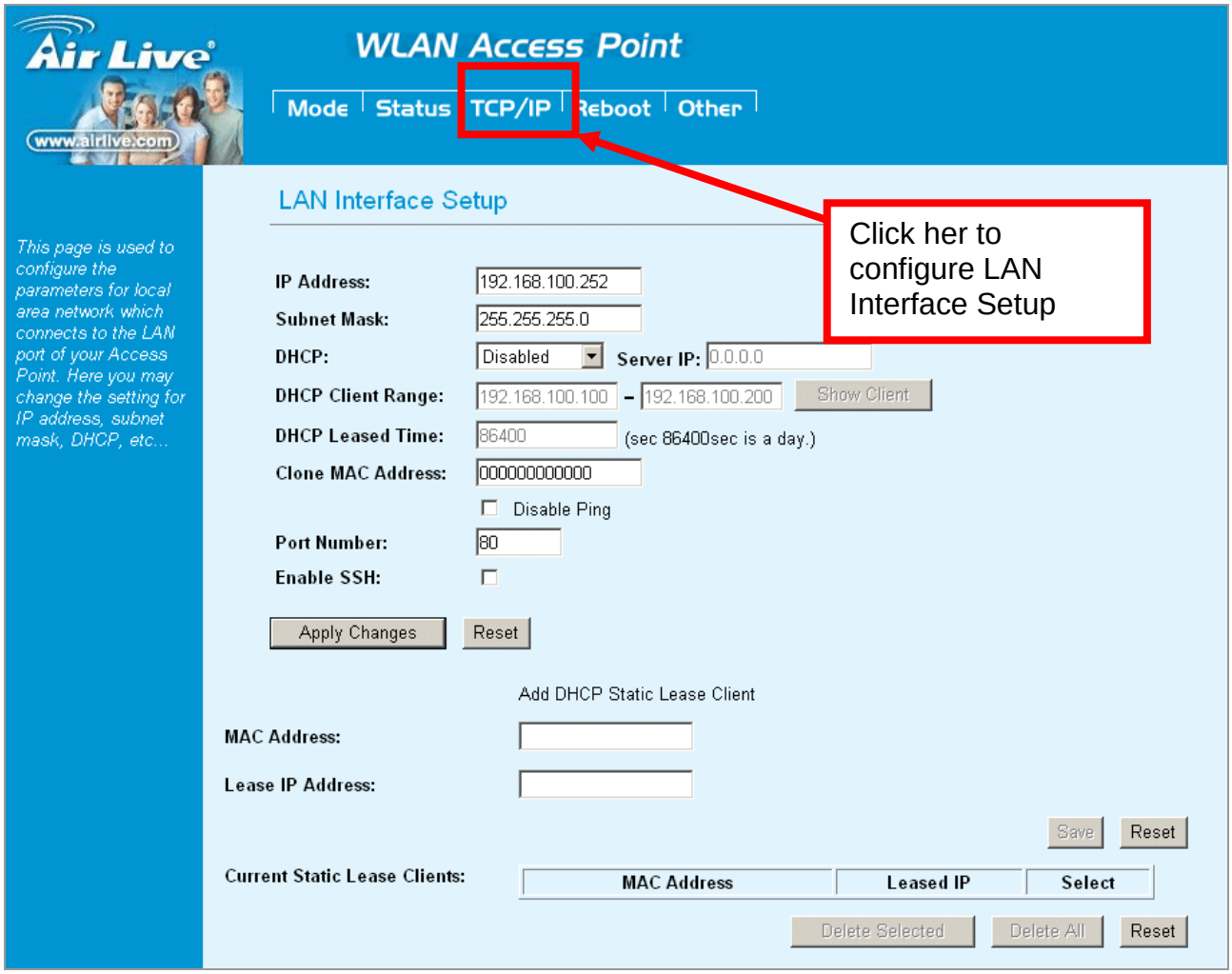


1. Please enable the “Interface Traffic Control”
2. Enter “1024” in the “LAN Output Rate” field
3. Enter “128” in the “WLAN Output Rate” field
4. Press “Save”
5. Reboot the AP

4. System Management

4.1 LAN Interface Setup

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



IP Address: This field can be modified only when DHCP Client is disabled. If your system manager assigned you static IP settings, then you will have to enter the information provided.

Subnet Mask: Enter the information provided by your system manager.

Default Gateway: Enter the information provided by your system manager.

DHCP: Select Disable, Client or Server from the pull-down menu.

- **Disable:** Select to disable DHCP server function.
- **Client:** Select to automatically get the LAN port IP address from ISP (For ADSL/Cable Modem).

- **Server:** Select to enable DHCP server function.

DHCP Client Range: WL-5060AP IP addresses continuing from 192.168.100.1 to 192.168.100.253

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

Disable Ping: WH-5420CPE did not response LAN ping if this function is checked.

Port Number: The default http port of the web management interface. You can change the port number to prevent unexpected access.

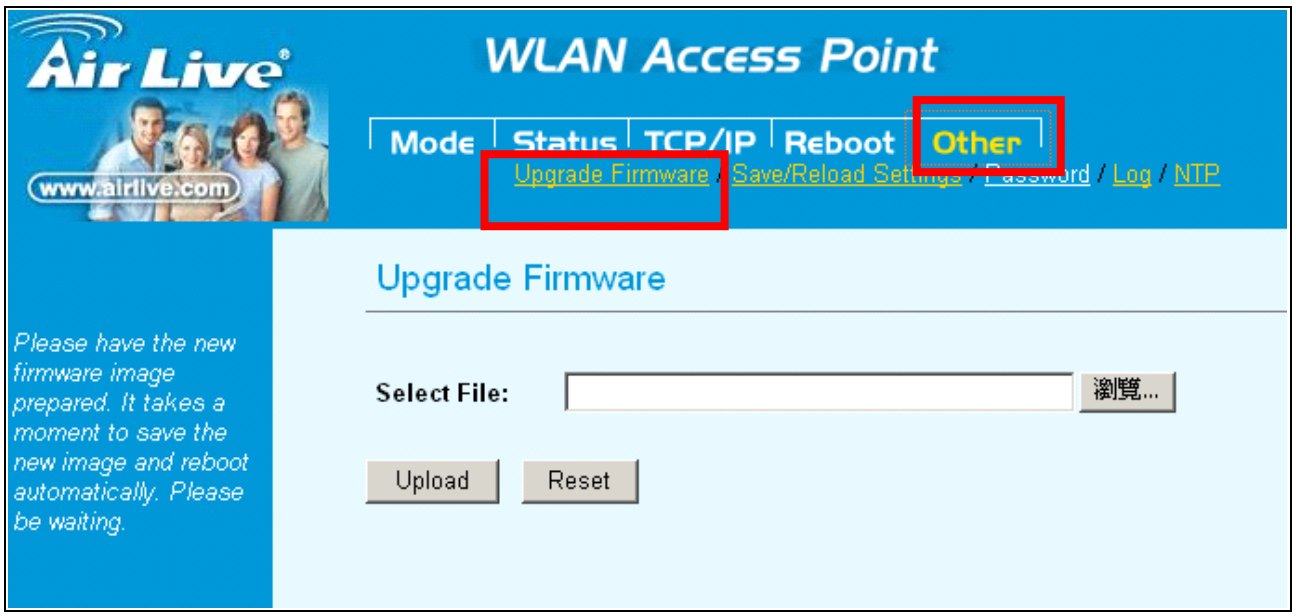
Enable SSH: Except telnet, WH-5420CPE provides SSH for secure command line management. You can enable the feature here. This device supports SSH2 for advanced security.

Some of your devices could need to fix its IP address for convenience; you can record these IP to prevent conflict. This can be done by **Add DHCP Static Lease Client.**

MAC Address: You have to fill the MAC address of the device which you want to record in WH-5420CPE.

Lease IP Address: And assign IP address to the MAC address.

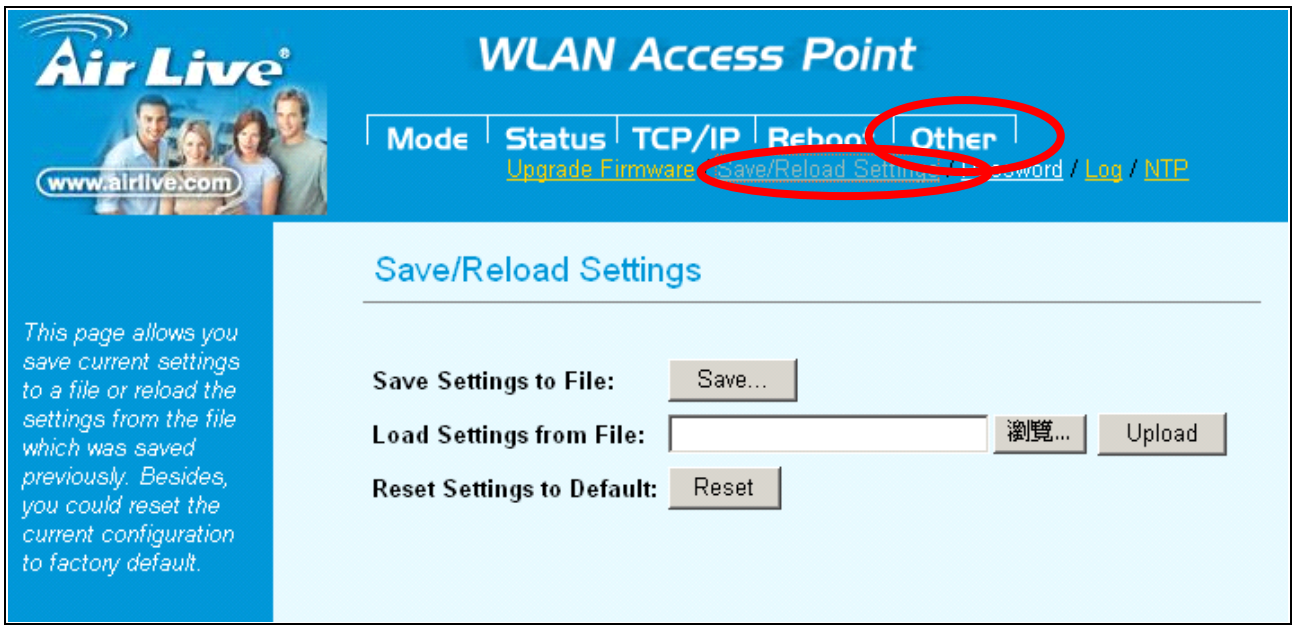
4.2 Upgrade Firmware



To Upgrade Firmware:

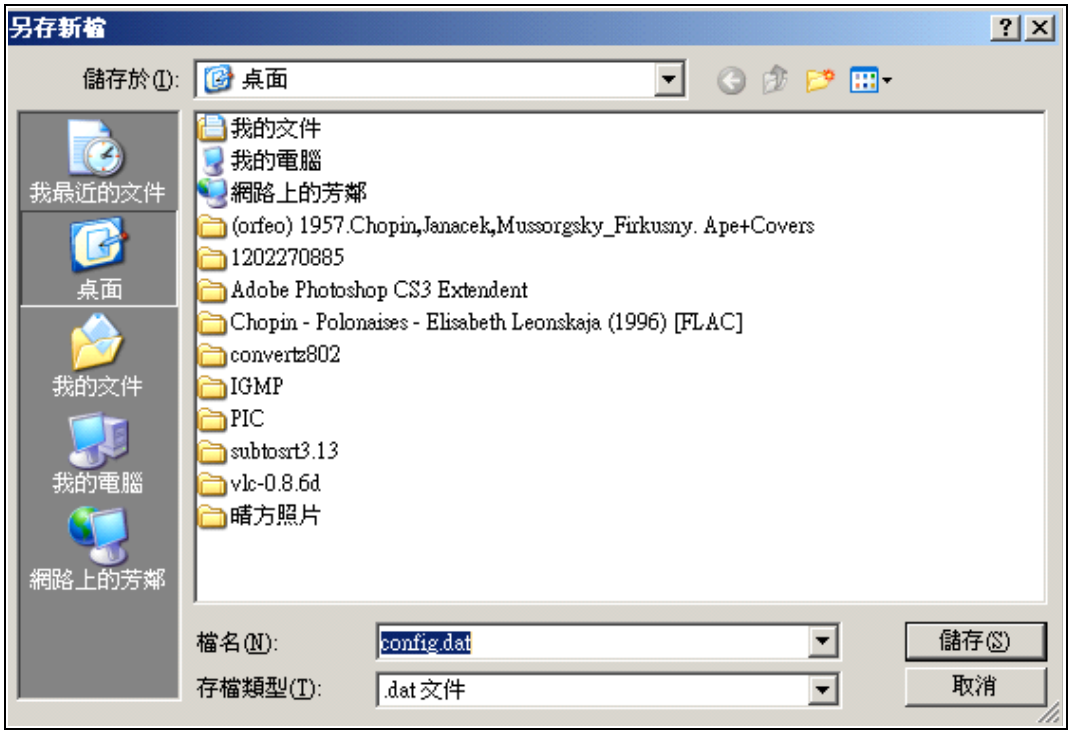
1. Download the latest firmware from your distributor and save the file on the hard drive.
2. Start the browser, open the configuration page, click on **Other,** and click **"Upgrade Firmware"** to enter the Upgrade Firmware window. Enter the new firmware's path and file name (i.e. C:\FIRMWARE\firmware.bin).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

4.3 Save / Reload Settings



This function enables users to save the current configurations as a file (i.e. config.dat) To load configuration from a file, enter the file name or click Browse… to find the file from your computer.

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



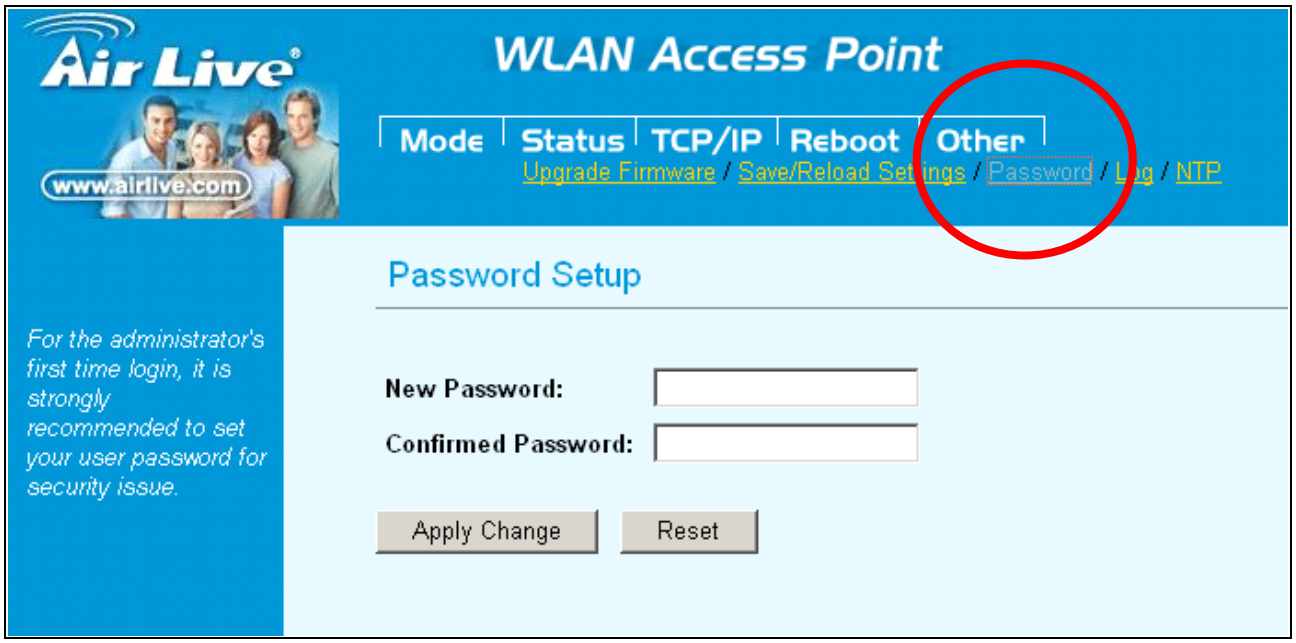
When prompted the upper left screen, select **"Save this file to disk"**, and the upper right screen will prompt you a dialog box to enter the file name and the file location.

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

Reset: Click to restore the default configuration.

4.4 Change Password

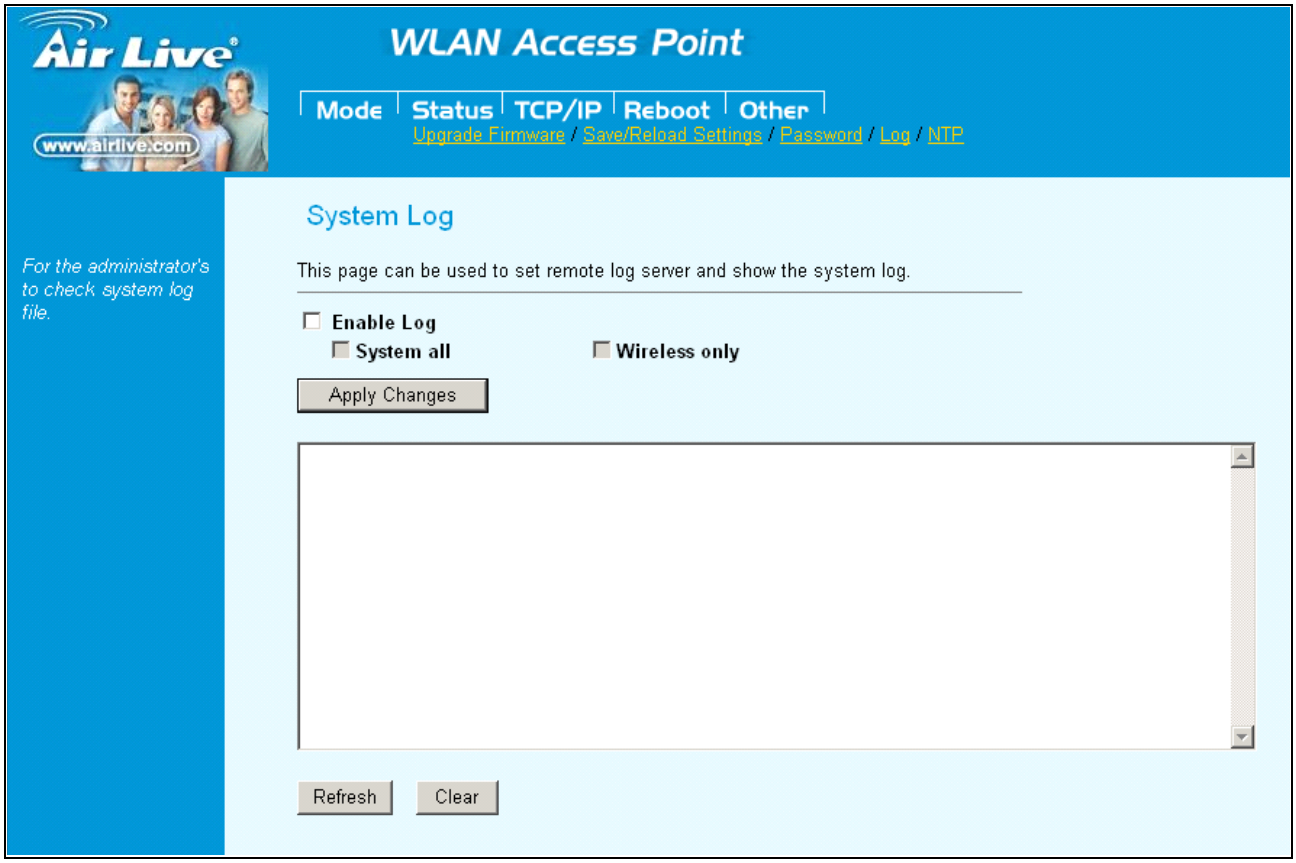
For secure reason, it is recommended that you set the account to access the web server of this Access Point. Leaving the user name and password blank will disable the protection. The login screen prompts immediately once you finish setting the account and password. Remember your user name and password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



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

4.5 Enable System Log

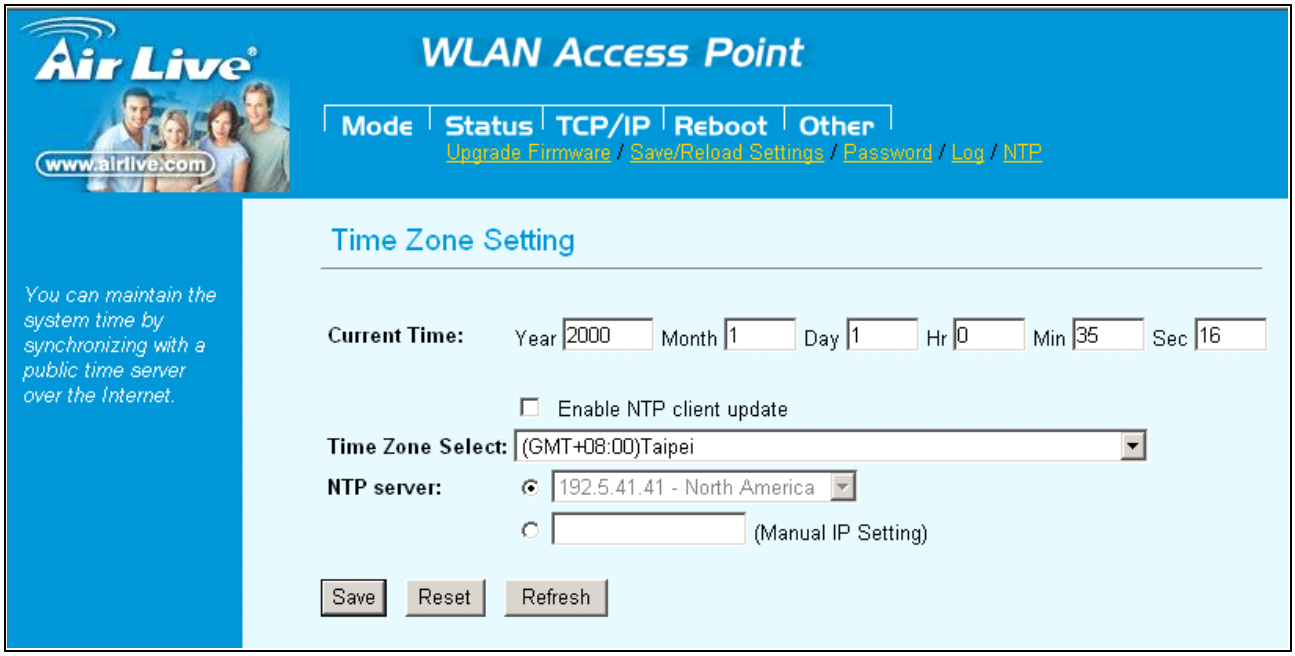
This function can list all log information about device.



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

4.6 NTP Settings

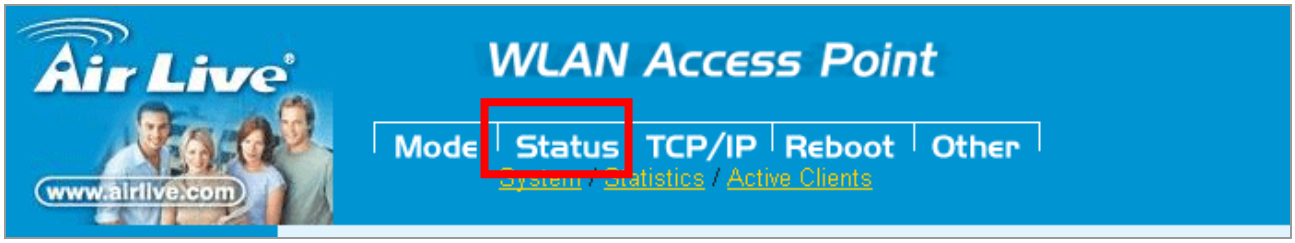
This function can set system time from local computer or Internet.



Current Time: Setting system time
Enable NTP client update: Enable or Disable setting system from Internet NTP Server.
Time Zone Select: Select system time zone.
NTP Server: Select NTP Server by Server List or Manual Input.

5. System Status

System status shows device's current configuration and operation status. To check the status, click the **"Status"** bottom on the title bar.



5.1 System Data

System data highlights the current configuration of the device.

System

System shows the alive time when device boots up and the current firmware version installed in the device.

Wireless

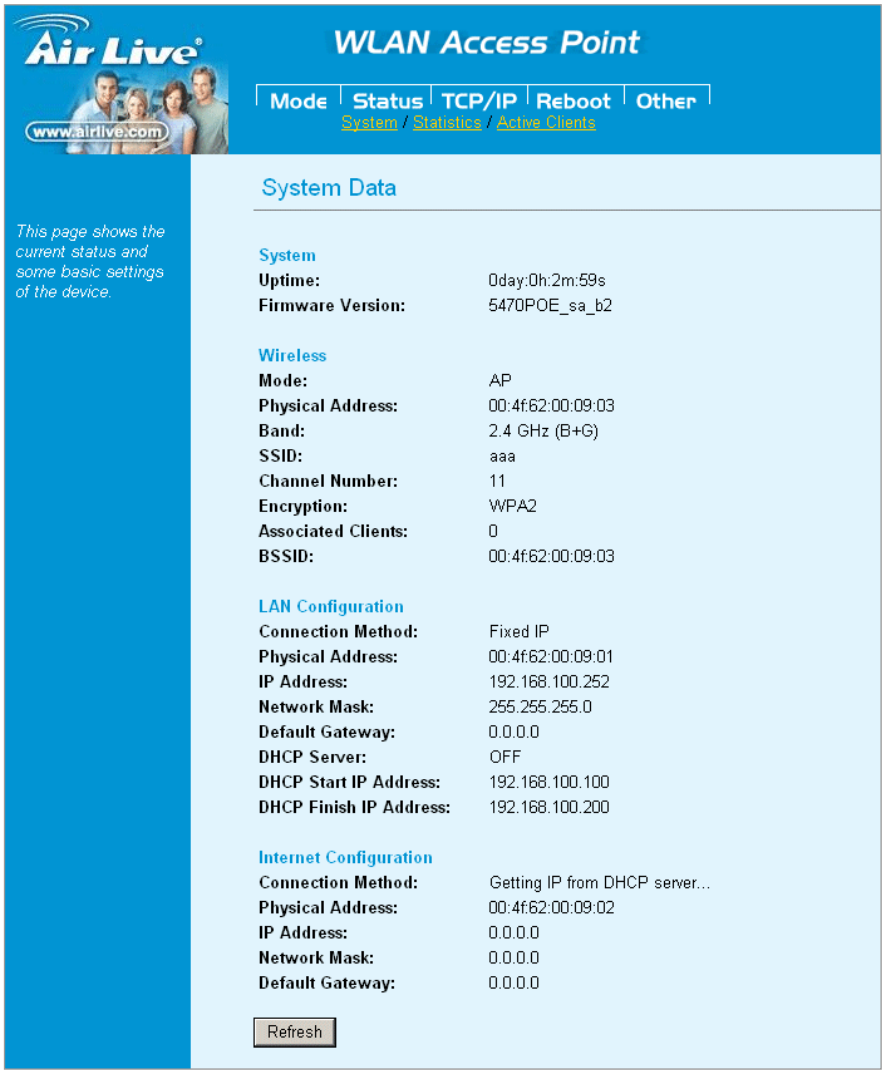
Wireless shows the current wireless operation mode, MAC address (Physical Address), wireless band, SSID, channel number, encryption method and associated clients of wireless interface.

LAN Configuration

LAN configuration shows the configuration of the Local Area Network interface.

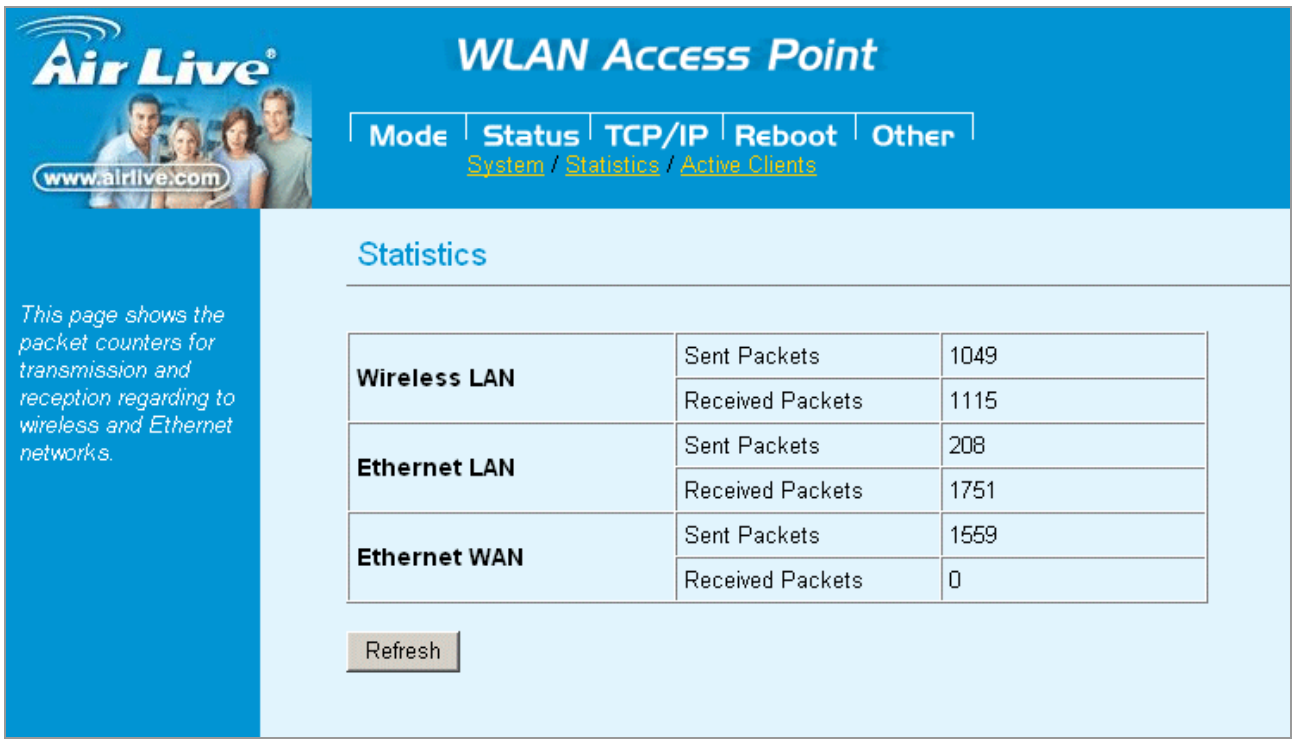
Internet Configuration

Internet Configuration shows the current situation of internet connection.



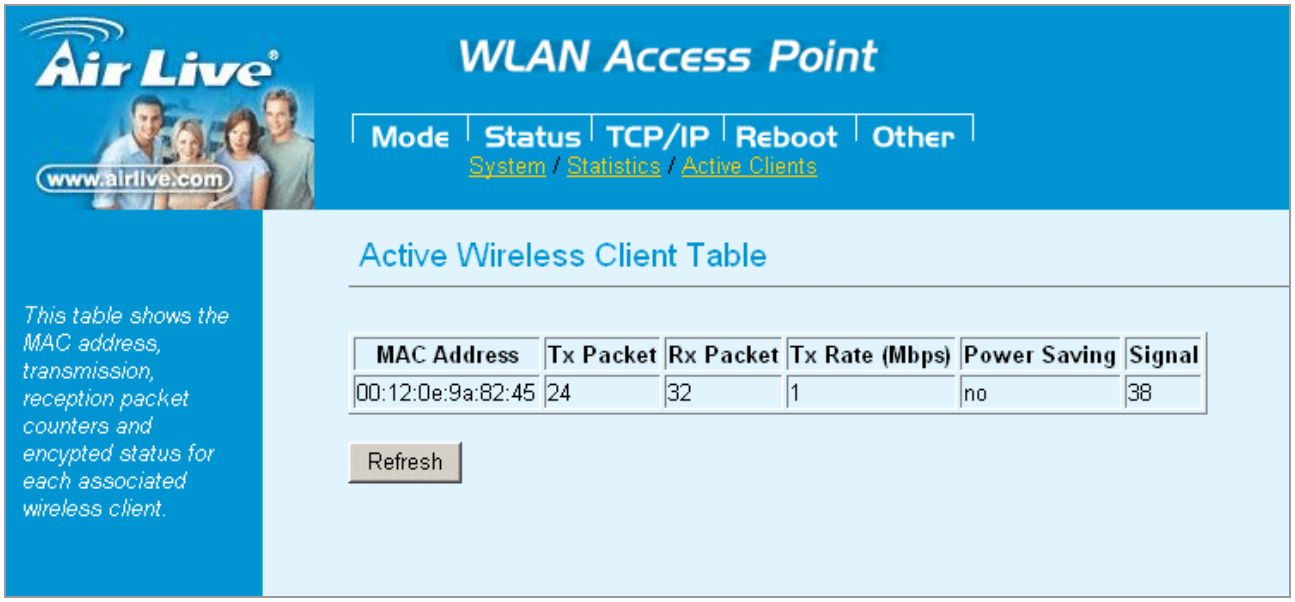
5.2 Statistics

Statistics shows the total packets pass through the interface.



Active Clients

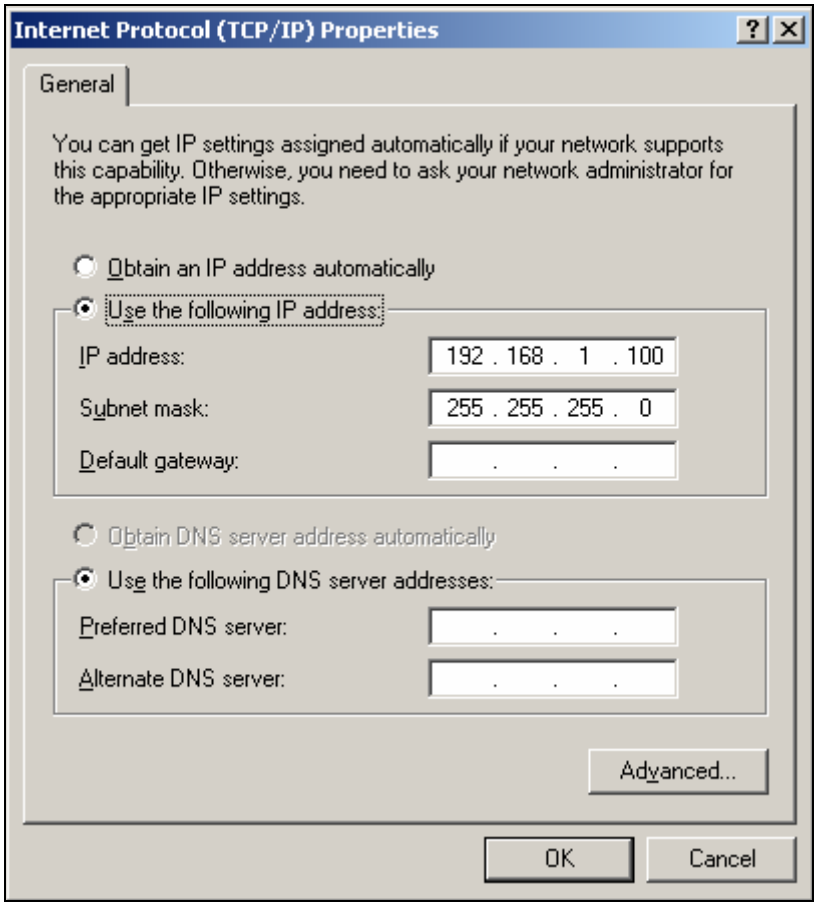
This feature shows the information of wired and wireless client connects to the device.



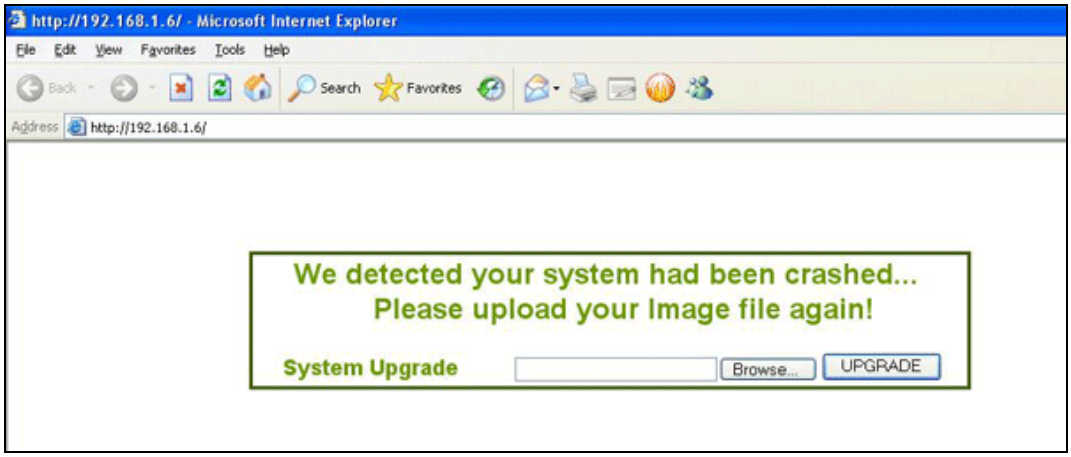
6 System Recovery

WH-5420CPE provides the system **recovery emergency code** function that can restore the machine after firmware crashed. Please follow the steps below:

1. Unplug the power of WH-5420CPE.
2. Hold the reset button while plugging the power. Do not release the reset button until the **"Status"** LED goes off.
3. Set your PC's IP address to 192.168.1.100. Connect your PC to the WH-5420CPE.



4. Open your web browser, then type **"192.168.1.6"**. You should see the emergency code page where you can upload your AirLive firmware again.



7. Specification

Feature	54Mbps Multi-function POE AP 2 x 10/100Mbps ports, 4MB Flash, 16MB SDRAM 20dBm(EU) or 26dBm(South America) Output Power R-SMA antenna connector IEEE802.3af PoE standard compliance* 8 Wireless Operation Modes Bandwidth Control and Signal Survey Client Isolation, Watchdog, and TX Power Regulation SSH2/HTTP/Telnet managements DHCP Relay Agent Supported Up to 40 Access Control List ACK Timeout Adjustment Watchdog, and TX Power Regulation
Hardware	2 x 10/100Mbps LAN Port, LAN1 1 with 802.3af PoE 4MB Flash, 16MB SDRAM Reversed SMA Antenna Port Power, LAN, WLAN LED indicators
Antenna	2 dBi detachable Dipole Antenna Reversed SMA Connector
Frequency Range	USA (FCC) 11 Channels: 2.412GHz~2.462GHz Europe (ETSI) 13 Channels : 2.412GHz~2.472GHz Japan (TELEC) 14 Channels :2.412GHz~2.483GHz
Modulation Technique	11g Orthogonal Frequency Division Multiplexing (64QAM, 16QAM, QPSK, BPSK) 11b Direct Sequence Spread Spectrum (CCK, DQPSK, DBPSK) Data Rate: 54, 48, 36, 24, 18,11, 5.5, 2, 1 Mbps
Output Power	18dBm Adjustable in 4 levels
WISP Mode	DHCP, PPTP, L2TP, PPPoE ISP Authentication Support Wireless Client function as WAN WISP mode is not the same router mode To configure the WISP mode, you PC must be connected to the LAN port

Security	64/128-bit WEP WPA/WPA2-PSK support 802.1x Radius Support WPA Enterprise support in AP/WDS mode
Configuration	Web/telnet/SSH2 Management WDS (Bridge, Client, Repeater) mode Hide ESSID 802.1x MAC Access Control MAC Access Table Wireless Client Isolation SSID, Channel, RTS Threshold, Frag Threshold
Environmental	Operating temperature: 0~60℃ Operating humidity (non-condensing): 20~80% Storage temperature: -20~65℃ Storage humidity: 95% Max
Power Supply	DC12V / 48VDC(802.3af, LAN 1)
EMI	FCC, CE
Product Weight (g)	180 g
Product Size (L x W x H (mm))	135 x 100 x 26mm

Appendix Command Line Management

WH-5420CPE provides telnet and Secure Shell (SSH) for remote management. You can use telnet or some free software such as putty (http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html) as telnet/SSH client. Refer to the following table for detail.

All commands will tack effect only after reboot

[Mode] Wireless Mode			
sys			
	operation	<0:AP|1:Client|2:Bridge|3:WDS Repeater|4:Universal Repeater|5:WISP|6:WISP+Universal Repeater|7:Gateway>	
[Mode] Basic Settings			
wlan			
	alias	[string]	
	active	[on|off]	
	chid	[channel_id|auto]	
	essid	[essid]	
	rssid	[rssid]	
	band	[b|g|bg]	
	mode	[client <infrastructure|adhoc>]	
	clone	[mac_addr|auto|manual]	
	encrypt	[both|wlan|wan]	
	wds		
		peer	
			disp
			add [mac]
			delete [id]
			clearall
		encrypt	[off]
			wep [64|128] <ascii|hex> <key>
			wpa [tkip|aes] <pass|hex> <key> [gklt]
			wpa2 [mixed|aes] <pass|hex> <key> [gklt]
	stp	[on|off]	

	isolation	[on|off]	
wlan			
	alias	[string]	
[Mode] Site Survey			
wlan			
	survey		
		connect	[id]
			(only support in Client, WISP, Universal Repeater Mode, WISP + Universal Repeater Mode)
[Mode] Security			
wlan			
	auth	[open|share|auto]	
	security		
		encrypt	[off]
			wep [64|128] <ascii|hex> <1:key1|2:key2|3:key3|4:key4> <key>
			wpa [tkip|aes] <pass|hex> <key> [gklt]
			wpa2 [mixed|aes] <pass|hex> <key> [gklt]
		1x	[off|on <port> <ip_addr> <password> <wep [64|128]|wpa [tkip|aes]|wpa2 [mixed|aes]>]
		preauth	[on|off]
		account	[off|on <port> <ip_addr> <password>]
[Mode] Advanced Settings			
wlan			wlan
	preamble	[long|short]	
	bssid	[on|off]	
	iapp	[on|off]	
	protect11g	[on|off]	
	fragment	<256~2346>	
	rts	<0~2347>	
	beacon	<20~1024>	
	inactivity	<100~60480000>	
	datarate	<0~12>	

	txpower	<1~10>	
	watchdog	[off|on <interval:1~60> <host>]	
[Mode] Access Control			
wlan			
	acl		
		disp	
		off	
		allow	
		deny	
		add [mac]	
		delete [id]	
		clearall	
[Mode] Wan Port			
wan			
	clone	[mac_addr]	
	dns	[auto|manual]	
	static	[ip_addr <netmask> <gateway>]	
	dhcp	[on|release|renew]	
	pppoe	<username> <password> [svname 0|1 <service_name>] <auth_type> <mppe> <mtu_value> dynwan dynpppoe [connect 0|1 <timeout>|2]	
	pptp	<ip [server_ip]|url [server_url]> <username> <password> <auth_type> <mppe> <mtu_value> [static <ip_addr> <netmask> <gateway>|dynamic]	
	l2tp	<ip [server_ip]|url [server_url]> <username> <password> <auth_type> <mppe> <mtu_value> [static <ip_addr> <netmask> <gateway>|dynamic] <timeout>	
		auth_type: 0. PAP 1. CHAP 2. MSCHAP 3. MSCHAP2	
		mppe: 0. none 1. 40bits	

		2. 56bits 3. 128bits	
	link	[status|set <mode>]	
	protocol	status	
sys	server	access	icmp <0:disabled|1:enabled>
	passthruvpn	ipsec <0:disabled|1:enabled>	
	passthruvpn	pptp <0:disabled|1:enabled>	
	passthruvpn	l2tp <0:disabled|1:enabled>	
[Mode] Virtual Servers			
ip			
	nat		
		server	
			disp
			delete [id]
			clearall
			add <ser_ip> <server> [proto <from_port [to_port]>]
			server: 0. Customize 1. Web, 2. FTP, 3. POP3, 4. SMTP, 5. DNS, 6. Telnet
			proto: 1. TCP+UDP, 2. TCP, 3. UDP
[Mode] Special Applications			
ip			
	nat		
		service	
			disp
			sap1 [on|off|clear|edit <name> <in_proto> <in_from_port> <in_to_port> <trig_proto> <trig_from_port> <trig_to_port>]
			sap2 [on|off|clear|edit <name> <in_proto> <in_from_port>

			<in_to_port> <trig_proto> <trig_from_port> <trig_to_port>]
			sap3 [on|off|clear|edit <name> <in_proto> <in_from_port> <in_to_port> <trig_proto> <trig_from_port> <trig_to_port>]
			sap4 [on|off|clear|edit <name> <in_proto> <in_from_port> <in_to_port> <trig_proto> <trig_from_port> <trig_to_port>]
			sap5 [on|off|clear|edit <name> <in_proto> <in_from_port> <in_to_port> <trig_proto> <trig_from_port> <trig_to_port>]
			sap6 [on|off|clear|edit <name> <in_proto> <in_from_port> <in_to_port> <trig_proto> <trig_from_port> <trig_to_port>]
			sap7 [on|off|clear|edit <name> <in_proto> <in_from_port> <in_to_port> <trig_proto> <trig_from_port> <trig_to_port>]
			sap8 [on|off|clear|edit <name> <in_proto> <in_from_port> <in_to_port>

			<trig_proto> <trig_from_port> <trig_to_port>]
			proto: 1. TCP+UDP, 2. TCP, 3. UDP
[Mode] Remote Management			
sys			
	server	access	web <0:disabled|1:enabled>
		port	web <portnum>
		access	telnet <0:disabled|1:enabled>
[Mode] URL Filtering			
ip			
	urlfilter		
		customize	
			disp
			add [string]
			delete [id]
			clearall
[Mode] MAC Filtering			
ip			
	macfilter		
		customize	
			disp
			add [mac_addr]
			delete [id]
			clearall
[Mode] IP Filtering			
ip			
	ipfilter		
		customize	
			disp
			add [ip_addr] <1:tcp+udp|2:tcp|3:udp>
			delete [id]
			clearall
[Mode] Traffic Control(Qos)			
qos			
	disableif		
	enableif	lanoutput [output rate]	
		wanoutput [output rate]	
	addpolicytab	[Policy Name][LAN Out Rate][WAN Out Rate][[Comment]]	

	disableip		
	enableip		
	addiptab	[PolicyName][IP][[Comment]]	
	disablemac		
	enablemac		
	addmactab	[PolicyName][MAC][[Comment]]	
	show	policytab	
		iptab	
		mactab	
	delallpolicy		
	delallip		
	delallmac		
	delpolicy	[Policy]	
	delip	[IP]	
	delmac	[MAC]	
[Mode] DoS Setting			
dos			
	disabledos		
	enabledos		
	enable	<clearall>[Packets/Second]<selectall>[Packets/Second]<sysfloodsyn>[Packets/Second]<sysfloodfin>[Packets/Second]<sysfloodudp>[Packets/Second]<sysfloodicmp>[Packets/Second]<persrcipfloodsyn>[Packets/Second]<persrcipfloodfin>[Packets/Second]<persrcipfloodudp>[Packets/Second]<persrcipfloodicmp><tcpudpportscan><icmpsmurf><ipland><ipspoof><ipteardrop><pingofdeath><tcpscan><tcpsynwithdata><udpbomb><udpechochargen><srcipblocktime>[sec]	
	disable	<sysfloodsyn><sysfloodfin><sysfloodudp><sysfloodicmp><persrcipfl	

		oodsyn><persrcipfloodfin><persrcipfloodudp><persrcipfloodicmp><tcpudpportscan><icmpsmurf><ipland><ipspoof><ipteardrop><pingofdeath><tcpscan><tcpsynwithdata><udpbomb><udpechochargen><srcipblocktime>	
[Mode] Dynamic DNS			
ddns			
	enabledyndns	<Domain Name><User Name/Email><Password/Key>	
	enabletzo	<Domain Name><User Name/Email><Password/Key>	
	disableddns		
	result		
[Status] Statistics			
ip			
	status		
[Status] Active Wireless Client Table			
wlan			
	association		
[TCP/IP] LAN Interface Setup			
ip	address	[addr]	
	subnetmask	[netmask]	
	gateway	[addr]	
	dhcp	on	[client|server|relay <server_ip>]
		off	
		client	
			[start_ip <end_ip>]
		status	
	dns		
		server	
			[ip1 <ip2> <ip3>]
		status	
[Reboot] Reboot System			
reboot			
[Other] Password			
sys			
	password	[pw]	(if [pw] is empty, then clear the password)
[Other] Save / Reload Setting			

save			
factorydefault			
[Other] NTP			
sys			
	ntp		
		showcurrenttime	
		setcurrenttime	<yyyy/mm/dd/hh/MM/ss>
		enablentp	
		timezoneselect	<zone num>
		ntpserver	<servernum>
			manualipsetting <ip>
		disablentp	
[Other] System Log			
sys			
	log		
		disable	
		enablesysall	[showsysall]
		enablewlanonly	[showwlanonly]
		clear	