Air Live®
Powered by OvisLink Corp.

WLA-5000AP v3

802.11a/b/g
Wireless Access Point

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

802.11a/b/g Wireless Access Point
WLA-5000AP v3
is in conformity with

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

Clause	Description
■ **EN 301 893 v1.2.3 (2003-08)**	Broadband Radio Access Network(BRAN); 5GHz high performance RLAN; Harmonized EN Covering essential requirements of Article 3.2 of the R&TTE Directive.
■ **EN 300 328 V1.6.1 (2004-11)**	Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband transmission equipment operating in the 2.4GHz ISM band And using spread spectrum modulation techniques; Part 1：technical Characteristics and test conditions Part2：Harmonized EN covering Essential requirements under article 3.2 of the R&TTE Directive
■ **EN 301 489-1 V1.5.1 (2004-11)** ■ **EN 301 489-17 V1.2.1 (2002-08)**	Electromagnetic compatibility and Radio spectrum Matters (ERM); Electromagnetic compatibility(EMC) standard for radio equipment and Services; Part 17：Specific conditions for wideband data and HIPERLAN equipment
■ **EN 50371:2002**	Generic standard to demonstrate the compliance of low power Electronic and electrical apparatus with the basic restrictions related to human exposure to electromagnetic field (10MHz – 300GHz) -General public
■ **EN 60950-1:2001/ A11:2004**	Safety for information technology equipment including electrical business equipment
■ **CE marking**	CE ①

Manufacturer/Importer

Signature：
Name ： **Albert Yeh**
Position/ Title ： **Vice President**

Date： **2006/12/14**

(Stamp)

WLA-5000APV3 CE Declaration Statement

Country	Declaration	Country	Declaration
cs Česky [Czech]	OvisLink Corp. tímto prohlašuje, že tento WLA-5000APV3 je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.	lt Lietuvių [Lithuanian]	Šiuo OvisLink Corp. deklaruoja, kad šisWLA-5000APV3 atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
da Dansk [Danish]	Undertegnede OvisLink Corp. erklærer herved, at følgende udstyr WLA-5000APV3 overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.	nl Nederlands [Dutch	Hierbij verklaart OvisLink Corp. dat het toestel WLA-5000APV3 in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
de Deutsch [German]	Hiermit erklärt OvisLink Corp., dass sich das Gerät WLA-5000APV3 in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.	mt Malti [Maltese]	Hawnhekk, OvisLink Corp, jiddikjara li dan WLA-5000APV3 jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
et Eesti [Estonian]	Käesolevaga kinnitab OvisLink Corp. seadme WLA-5000APV3 vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.	hu Magyar [Hungarian]	Alulírott, OvisLink Corp nyilatkozom, hogy a WLA-5000APV3 megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.
en English	Hereby, OvisLink Corp., declares that this WLA-5000APV3 is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.	pl Polski [Polish]	Niniejszym OvisLink Corp oświadcza, że WLA-5000APV3 jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
es Español [Spanish]	Por medio de la presente OvisLink Corp. declara que el WLA-5000APV3 cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.	pt Português [Portuguese]	OvisLink Corp declara que este WLA-5000APV3 está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
el Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ OvisLink Corp. ΔΗΛΩΝΕΙ ΟΤΙWLA-5000APV3 ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.	sl Slovensko [Slovenian]	OvisLink Corp izjavlja, da je ta WLA-5000APV3 v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
fr Français [French]	Par la présente OvisLink Corp. déclare que l'appareil WLA-5000APV3 est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE	sk Slovensky [Slovak]	OvisLink Corp týmto vyhlasuje, že WLA-5000APV3 spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
it Italiano [Italian]	Con la presente OvisLink Corp. dichiara che questo WLA-5000APV3 è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.	fi Suomi [Finnish]	OvisLink Corp vakuuttaa täten että WLA-5000APV3 tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen
lv Latviski [Latvian]	Ar šo OvisLink Corp. deklarē, ka WLA-5000APV3 atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.	Íslenska [Icelandic]	Hér með lýsir OvisLink Corp yfir því að WLA-5000APV3 er í samræmi við grunnkröfur og aðrar kröfur, sem gerðar eru í tilskipun 1999/5/EC.
sv Svenska [Swedish]	Härmed intygar OvisLink Corp. att denna WLA-5000APV3 står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.	no Norsk [Norwegian]	OvisLink Corp erklærer herved at utstyret WLA-5000APV3 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

Table of Contents

1 Introduction

1.1 Overview

NOTE: For simplicity throughout this document, WLA-5000AP v3 Firmware 2.x will simply be referred to as WLA-5000AP v3.

The WLA-5000AP v3 is a wireless access-point based on IEEE 802.11a/g 5-GHz and 2.4-GHz radio technologies. It contains an 802.11a/g wireless interface and one half/full-duplex 10/100 LAN interface. WLA-5000AP v3, with the new 2.0 firmware, features a total of 6 wireless modes: Access Point, WDS Repeater, WDS Bridge, Client Infrastructure, Client Ad Hoc and WISP Router.

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

To address growing security concerns in a wireless LAN environment, different levels of security can be enabled in WLA-5000AP v3:

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

1.2 Features

- Compliant with 802.11a, 802.11b and 802.11g, Super A™ and Super G™ standards with roaming capability.
- Supports 6 wireless multi-function modes: Access Point, WDS Repeater, WDS Bridge, Client Infrastructure, Client Ad Hoc and WISP Router.
- Static assignment or DHCP client to set the device IP address.
- Multiple security measures: SSID hiding, Access Control List, WEP based encryption (64, 128, 152 bits), enhanced Security with 802.1x using a primary and a backup RADIUS Server with/without dynamic WEP keys, WPA-PSK, WPA, and WPA2.
- Extensive monitoring capability such as event logging, traffic/error statistics monitoring. Support of remote logging.
- Easy configuration and monitoring through the use of a Web-browser based GUI, SNMP commands from a remote SNMP management station, and UPnP for users to automatically discover the device.
- Setup Wizard for easy configuration/installation.
- Configuration file download and restore.
- Firmware upgradeable.

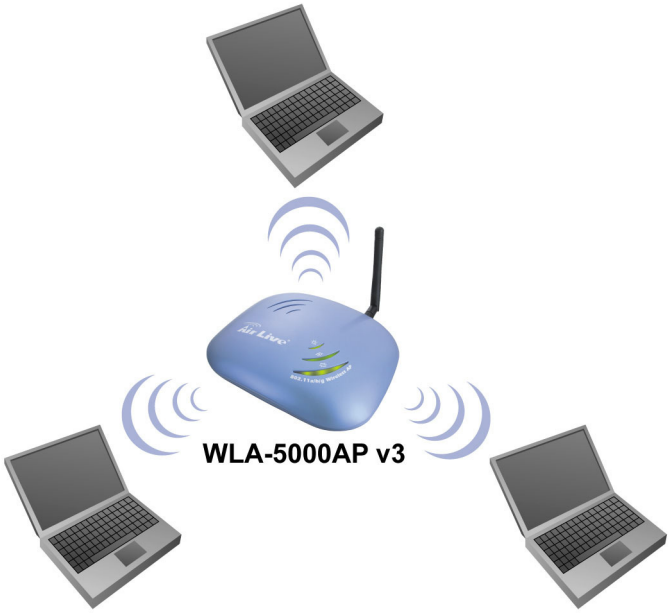
1.3 Wireless Operation Modes

A group of wireless stations communicating with each other is called a Basic Service Set (BSS) and is identified by a unique SSID.

When a WLA-5000AP v3 is used, it can be configured to operate in the following network configurations.

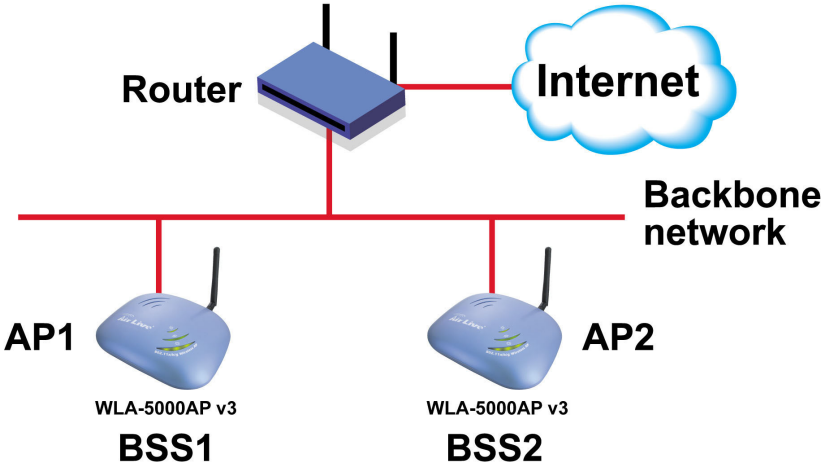
1.3.1 Access Point Mode

When configured in the Access Point mode, the WLA-5000AP v3 allows a group of wireless stations to communicate with each other through it. Such a network is called an Infrastructure BSS.



The WLA-5000AP v3 further provides bridging functions between the wireless network and the wired LAN network.

When multiple access points are connected to the same LAN segment, stations can **roam** from one WLA-5000AP v3 to another without losing their connections, as long as they are using the same SSID. See the diagram below.



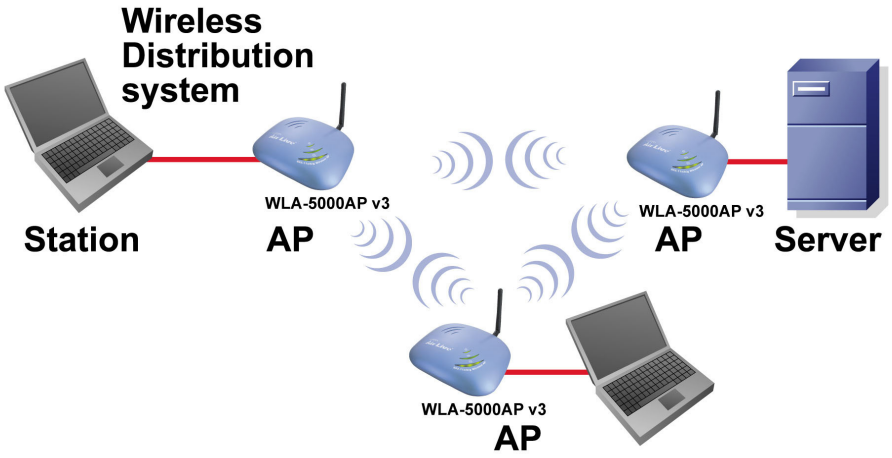
1.3.2 WDS Repeater Mode

In Repeater mode, the WLA-5000AP v3 set as a repeater extends the range of wireless LAN. The remote wireless AP/Router must also support WDS.

1.3.3 WDS Bridge Mode

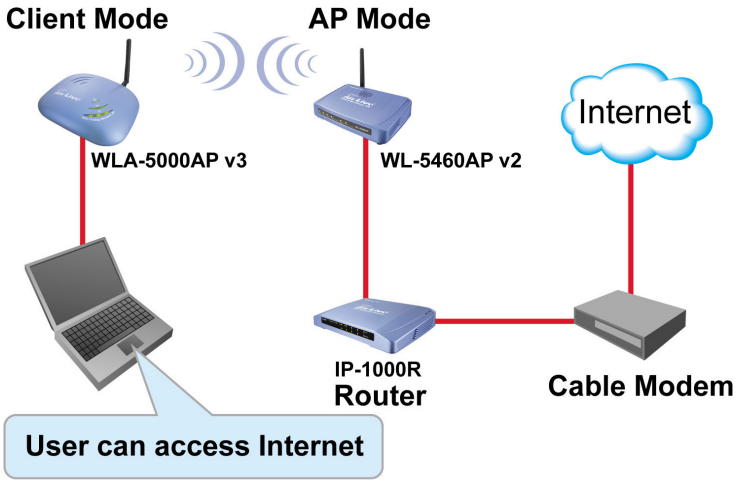
When configured to operate in the Wireless Distribution System (WDS) Mode, the WLA-5000AP v3 provides bridging functions between the LAN behind it and separates LANs behind other APs' operating in the WDS mode. The system will support up to ***eight*** APs in a WDS configuration.

Note that a WLA-5000AP v3 runs in the WDS mode can also support wireless stations simultaneously. See the diagram below:



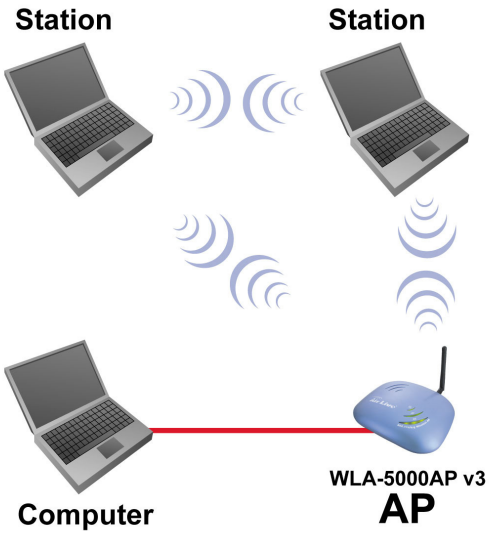
1.3.4 Client Infrastructure Mode

In Client Infrastructure mode, the WLA-5000AP v3 is connected to a computer and acts like a wireless station, so that the computer can wirelessly access the other network's services, such as Internet.



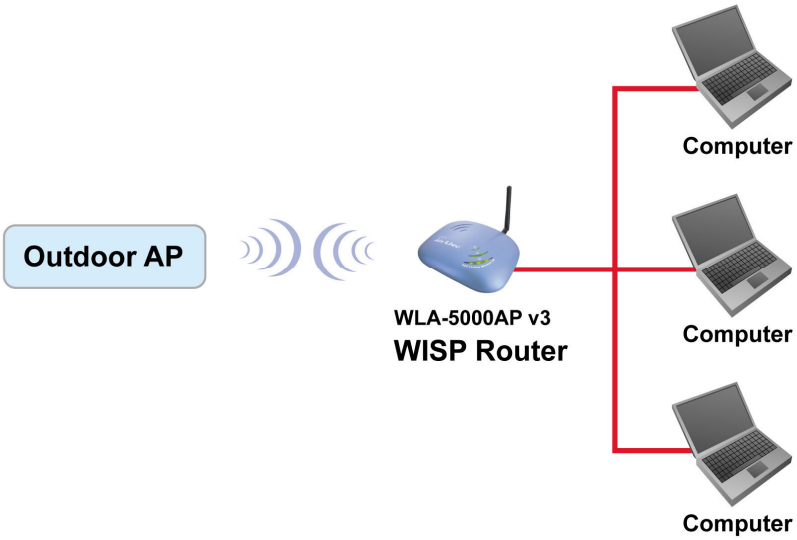
1.3.5 Client Ad Hoc Mode

In Client Ad Hoc mode, WLA-5000AP v3 is connected to a computer and acts like a wireless station, so that the computer can wirelessly share files and printers with other wireless stations.



1.3.6 WISP Router Mode

In WISP Router Mode, WLA-5000AP v3 is connected to several computers and acts like a Client mode AP. With IP sharing function, the computers can share the WISP connection via WLA-5000AP v3.



1.4 Set up the device

The WLA-5000AP v3 can be managed remotely by a PC through either the wired or wireless network. To do this, the WLA-5000AP v3 must first be assigned an IP address, which can be done using one of the following two methods.

1.4.1 STATIC IP

The default IP address of the LAN interface of an WLA-5000AP v3 is a *private IP address* of **192.168.1.1**, and a *network mask* of 255.255.255.0. This means IP addresses of other devices on the LAN should be in the range of 192.168.1.2 to 192.168.1.254.

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

1.4.2 AUTOMATIC IP

The WLA-5000AP v3 can also be configured to "obtain" an IP address automatically from a DHCP server on the network. This address is called "dynamic" because it is only *dynamically* assigned to the device, which may change depends on the IP assignment policy used by the DHCP server on the network. Since the IP address in this case may change from time to time, this method is not recommended - unless the user uses UPnP or other management tools that do not depend on a fixed IP address.

2 Install the 802.11 A/G Access Point

This section describes the installation procedure for the WLA-5000AP v3. 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 WLA-5000AP v3. Finally, this section explains how to configure a Windows PC to communicate with the WLA-5000AP v3.

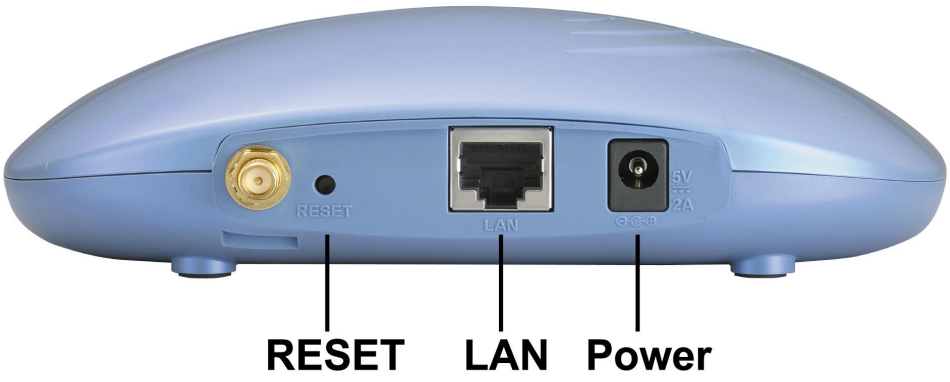
2.1 What's in the box?

The WLA-5000AP v3 package contains the following items:

- One WLA-5000AP v3
- One 5V DC power adapter with a barrel connector
- One CD of the WLA-5000AP v3 User Guide

2.2 Connect the cables

The Back Panel of the WLA-5000AP v3 appears as follows:



Follow these steps to install your WLA-5000AP v3:

Step 1. Connect a LAN hub to the LAN port on the WLA-5000AP v3 using the supplied LAN cable.

Step 2. Connect the power adapter to an electrical outlet and the WLA-5000AP v3.

You can reset the Access Point's Settings to factory defaults by pushing a paperclip in the RESET hole. Push and hold until the lights at the front of the Access Point are off.

2.3 Configuration steps

This section describes configuration required for the WLA-5000AP v3 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 WLA-5000AP v3, including the SSID, Channel number, the WEP key, …, etc., it is necessary to associate a fixed IP address with the WLA-5000AP v3, which is why the WLA-5000AP v3 will be shipped with a factory default private IP address of **192.168.1.1** (and a network mask of 255.255.255.0).

Therefore, during the system installation time, you need to build an isolated environment with the WLA-5000AP v3 and a PC, and then perform the following steps:

Step 1. Manually change the IP address of the PC to become 192.168.1.3.

Step 2. Connect the PC to the WLA-5000AP v3 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 WLA-5000AP v3 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 ACCESS POINT, the PC client may not be able to reach the ACCESS POINT. This is because they may no longer belong to the same IP network address space.

Step 3. Change the setting of the PC back to “obtain IP addresses dynamically”.

Now you can put the WLA-5000AP v3 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 AP, with each other, and with devices on the wired LAN network.

2.4 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 WLA-5000AP v3 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/b/g wireless interface installed properly, be physically within the radio range of the WLA-5000AP v3, 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, please consult the manufacturer’s documentation.

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

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

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

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

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

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

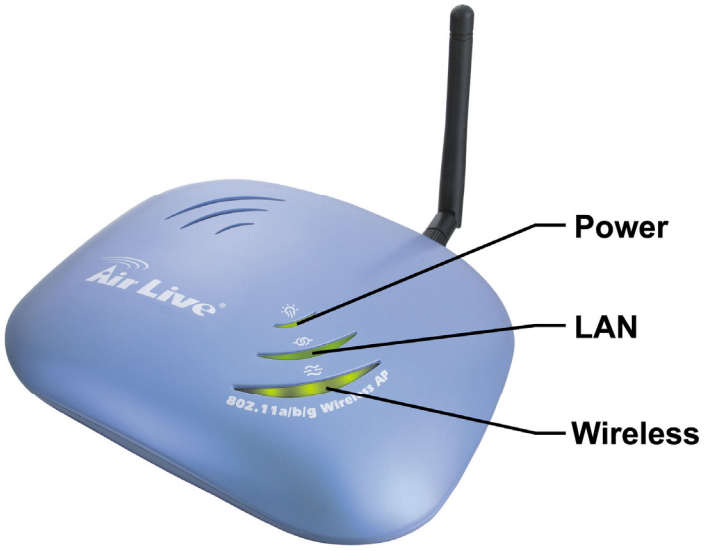
Step 7. Click **Properties,** and check the settings in each of the TCP/IP Properties window: **Bindings Tab**: both **Client for Microsoft Networks** and **File and printer sharing for Microsoft Networks** should be selected. **Gateway Tab**: All fields should be blank. **DNS Configuration Tab**: **Disable DNS** should be selected. **IP Address Tab**: **Obtain IP address automatically** should be selected.

Step 8. With the WLA-5000AP v3 powered on, reboot the PC/wireless client. After the PC/wireless client is re-booted, you should be ready to configure the WLA-5000AP v3. See Chapter 3.

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

2.5 Front panel

The LEDs on the front of the WLA-5000AP v3 reflect the operational status of the unit. The status of the LAN, the WLAN, and Power can be monitored from this display.



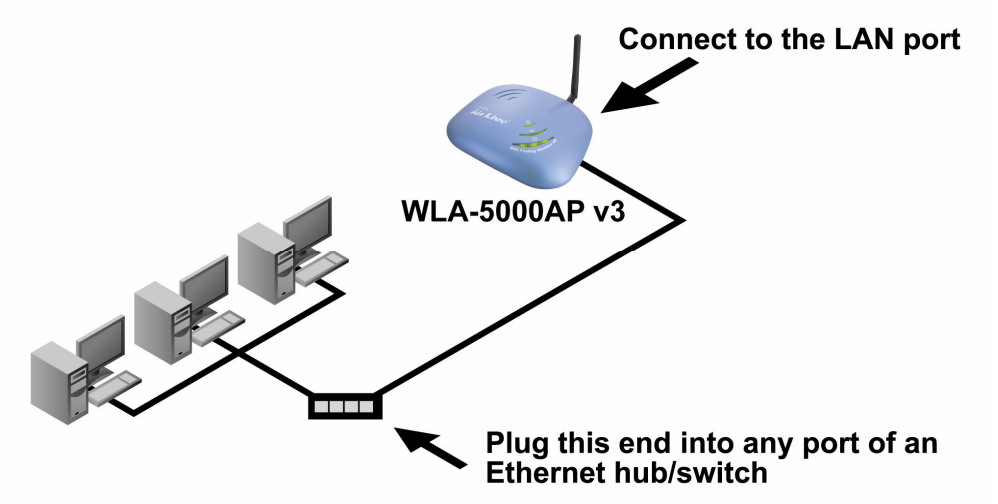
WLA-5000AP v3 LED Descriptions

Label	LAN	WLAN	POWER
SOLID	Link is active	Link is active	Power
OFF	No Wireless connection	No LAN connection	No Power
FLASH	XMT/RCV Data	XMT/RCV Data	N/A

* “Link is active” has lower FLASH frequency than “XMT/RCV Data”.

2.6 Connect more devices through a hub

The WLA-5000AP v3 provides an RJ45 LAN interface that you can use to connect to a PC or an external hub.



3 Basic Configuration

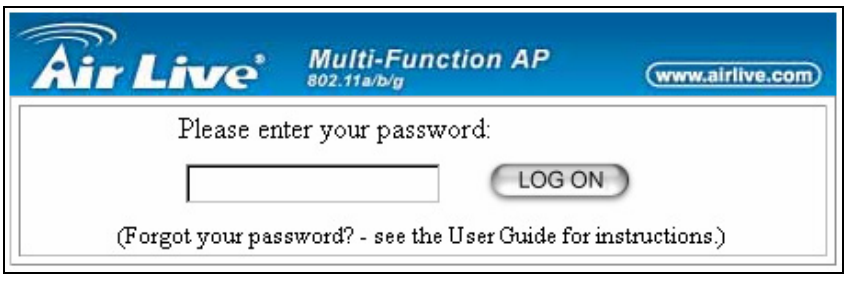
This section describes the basic configuration procedure for the WLA-5000AP v3. It describes how to set up the WLA-5000AP v3 for wireless connections, and the configuration of the local LAN environment. All basic configurations may be effected through a standard Web browser such as Microsoft Internet Explorer. From a PC that has been configured as described in Chapter 2, enter the IP address of the WLA-5000AP v3 as the URL in your browser, e.g. **http://192.168.1.1**.

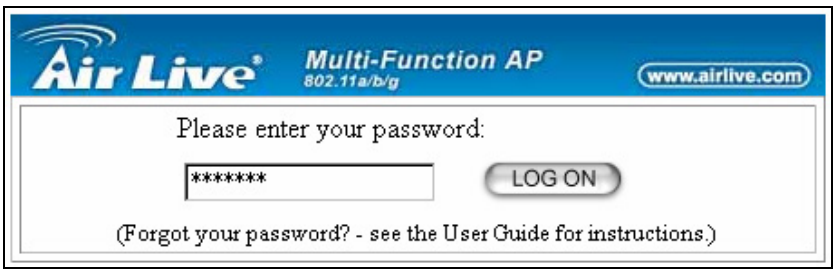
The IP address of your PC must be in the same IP subnet as the WLA-5000AP v3.

The Home Page of the WLA-5000AP v3 screen will appear. Its main menu displays on the right hand side of the window. The main menu includes the following choices: Setup Wizard, Device Status, Advanced Settings, System Tools, and Help.

Log On

If you attempt to access a configuration item from the browser menu, an administrator logon screen, shown below, will appear.





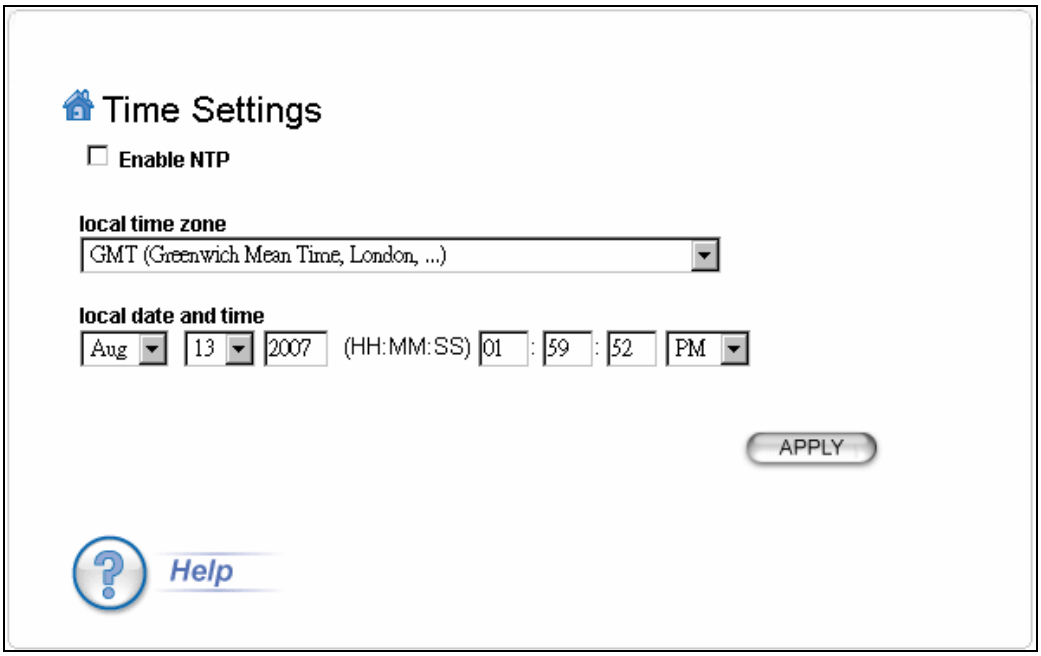
If you are logging on for the first time, you should use the factory default setting "**airlive**". The password is always displayed as a string of wildcards or dots. Click the **LOG ON** button to start the configuration session.

3.1 Setup wizard

The Setup Wizard will guide you through a series of configuration screens to set up the basic functionality of the device. Every time you modify the settings, remember to click **APPLY** button to save the changes.

3.1.1 TIME SETTINGS

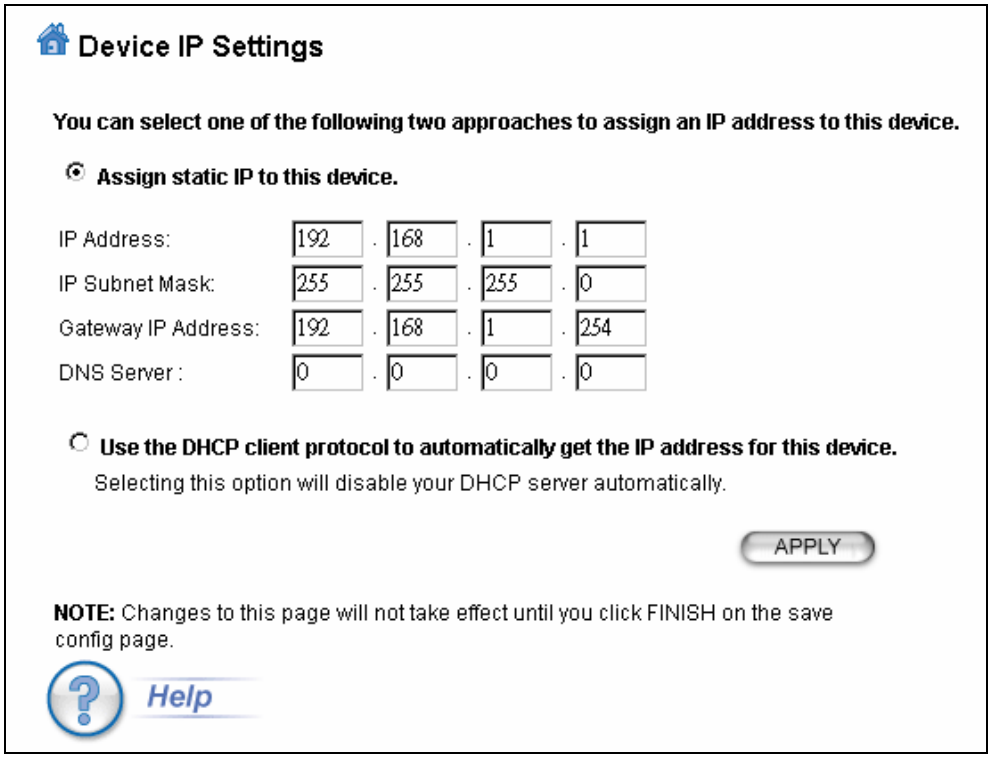
Setup Wizard>>Time Settings



After logging on, the **Time Settings** page appears. The device time is automatically set to the local time of the management PC at the first time a connection is made. To modify the device's time, modify the appropriate fields, then click **APPLY**.

3.1.2 DEVICE IP SETTINGS

Setup Wizard>> Device IP Settings



The **Device IP Settings** screen allows you to configure the IP address and subnet of the device. Although you can rely on a DHCP server to assign an IP address to the WLA-5000AP v3 automatically, it is recommended that you configure a static IP address manually in most applications.

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

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

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

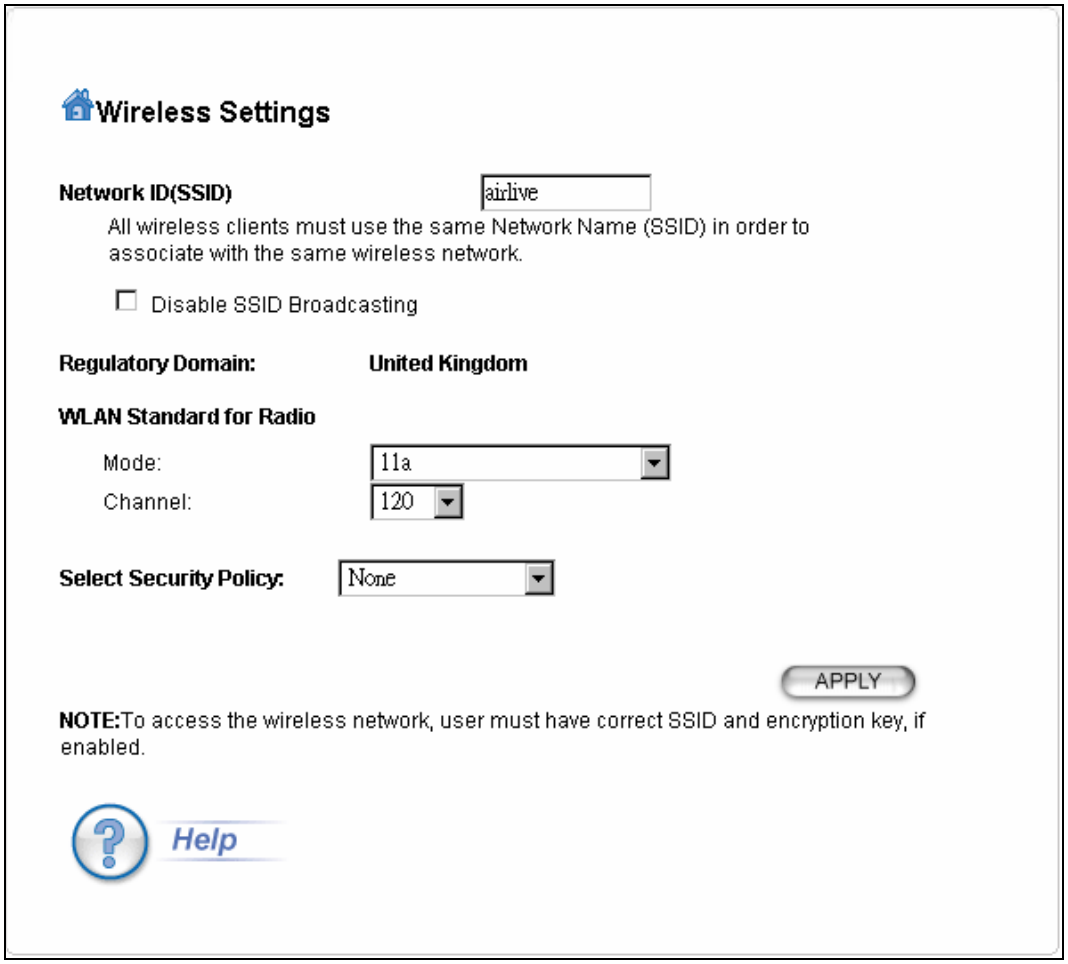
DNS Server: The Domain Name System (DNS) is a server on the Internet that translates logical names such as “www.yahoo.com” to IP addresses like 66.218.71.80. In order to do this, a query is made by the requesting device to a DNS server to provide the necessary information. If your system administrator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

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

If you choose to use a DHCP Server to acquire an IP address for the WLA-5000AP v3 automatically, enable the checkbox that says, “Use the DHCP client protocol to automatically get the IP address for this device”. Then click Next to go to the next screen. Again, as a reminder, it is recommended that your WLA-5000AP v3 should be assigned a static IP address in order to make it easy for you to manage the device later on.

3.1.3 WIRELESS SETTINGS

Setup Wizard>>Wireless Settings



Network ID (SSID): The SSID is the network name used to identify a wireless network. The SSID must be the same for all devices in the wireless network (i.e. in the same BSS). Several access points on a network can have the same SSID. The SSID length is up to 32 characters. The default SSID is "**airlive**".

Disable SSID Broadcasting: An access point periodically broadcasts its SSID along with other information, which allows client stations to learn its existence while searching for access points in a wireless network. Check **Disable SSID Broadcasting** if you do not want the device to broadcast the SSID.

Regulatory Domain: Please make sure that your regulatory domain matches your region. The default value is "**United Kingdom"**.

WLAN Mode: Select "11g/b", "11g only", "11b", "11a", "SuperG" or "SuperA". The wireless module is IEEE 802.11g and 802.11b compliant, and choosing "**11g/b**" allows both 802.11b and 802.11g client stations to get associated. However, choosing "**11g**" allows only 802.11g client stations to get associated and get better overall performance. 802.11a is not compliant with either 802.11b or 802.11g; choosing **"11a"** only allows 802.11a client stations to get associated.

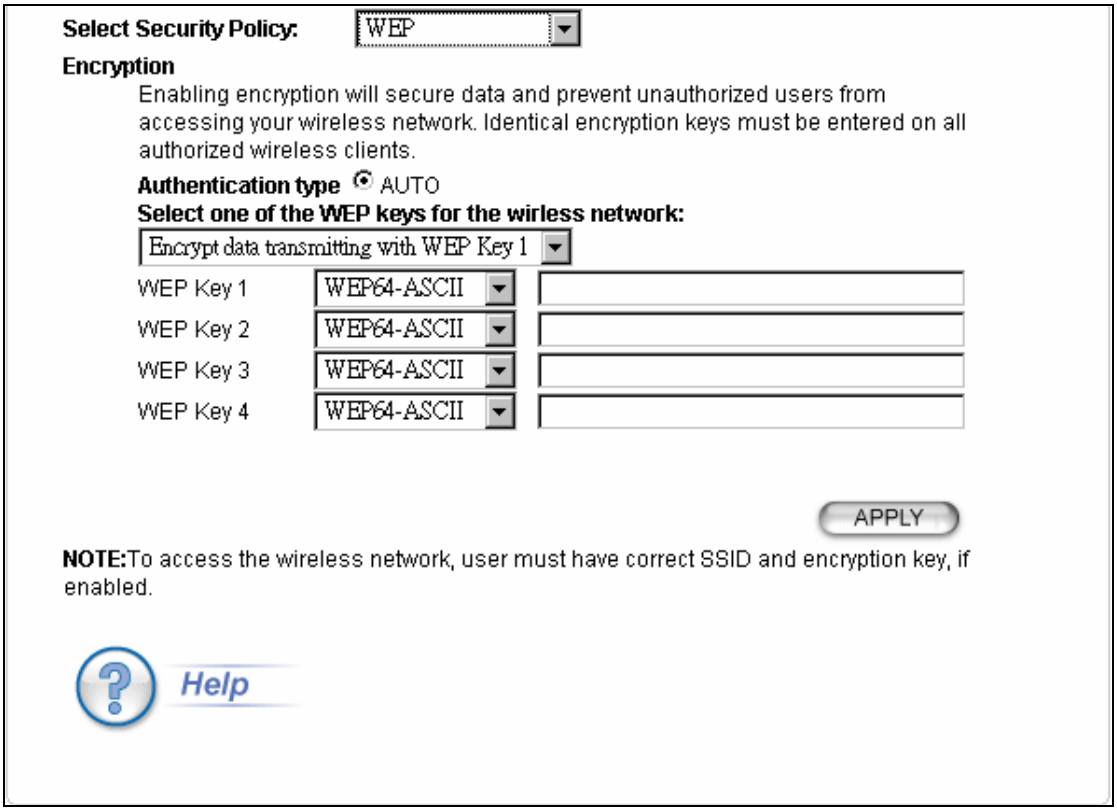
Channel: Select a channel from the drop down menu. All devices in a BSS must use the same channel. You can select **Auto** to let the system pick up the best channel for you.

The available channels are different from country to country and for different WLAN mode.

Security Policy: You can select different security policy to provide association authentication and/or data encryption.

WEP

Setup Wizard>>Wireless Settings >>Select Security Policy>>WEP



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

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

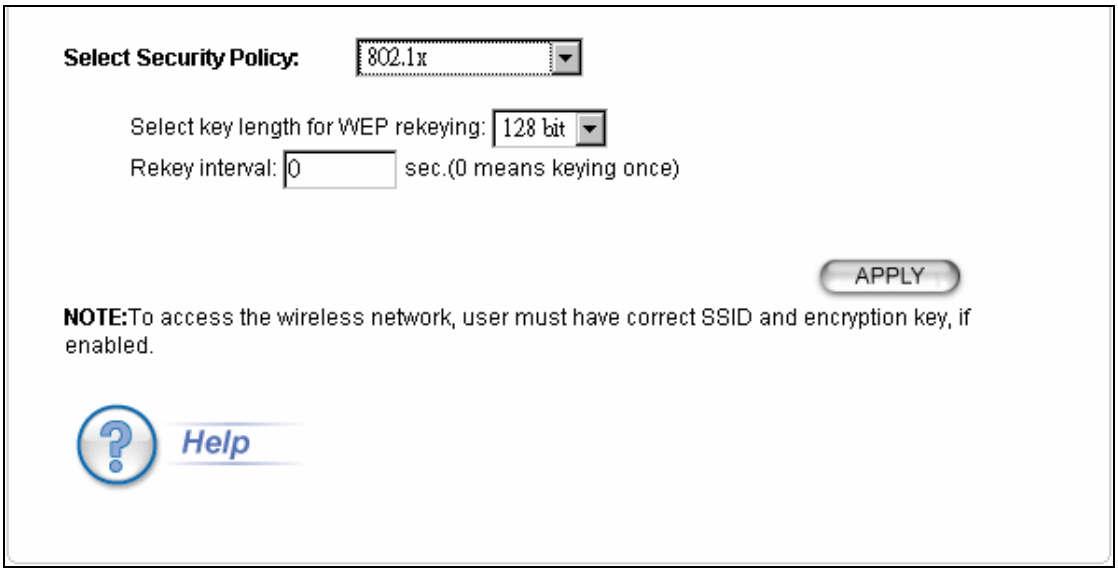
Key Index: You have to specify which of the four keys will be active.

Once you enable the WEP function, please make sure that both the WLA-5000AP v3 and the wireless client stations use the same key.

Some wireless client cards only allow Hexadecimal digits for WEP keys. Please note that when configuring WEP keys, a WEP128 ASCII key looks like "**This is a key**"(13 characters), while a WEP128 Hex key looks like "**54686973206973206120b6579**"(26 HEX) (hexadecimal notation are 0-9 and A-F).

802.1x

Setup Wizard>>Wireless Settings >>Select Security Policy>>802.1x



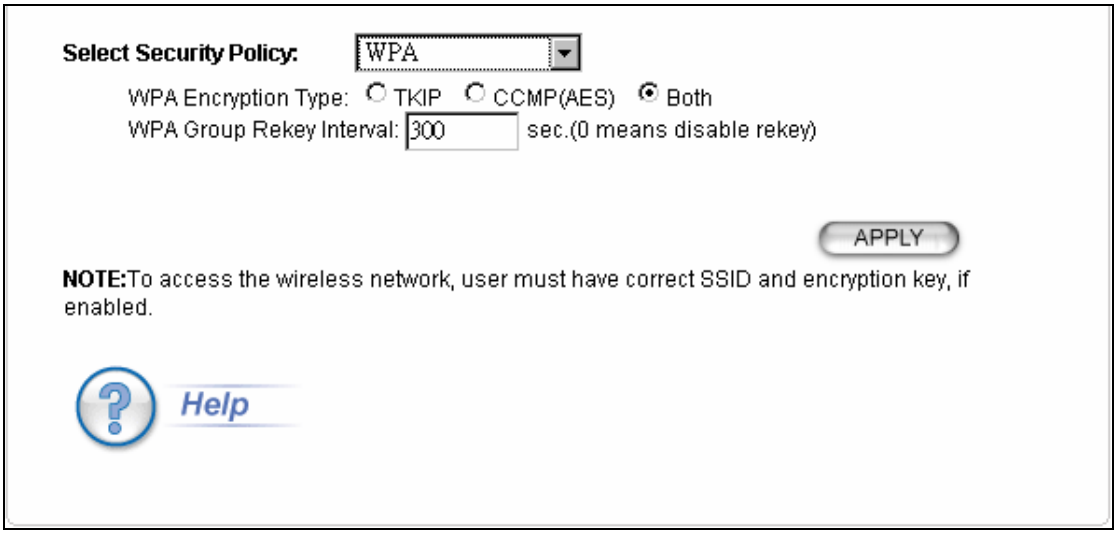
802.1x allows users to leverage a RADIUS server to do association authentications. You can also enable dynamic WEP key (128 bit) to have data encryption. Here you do not have to enter the WEP key manually because it will be generated automatically and dynamically.

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

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

WPA

Setup Wizard>>Wireless Settings >>Select Security Policy>>WPA



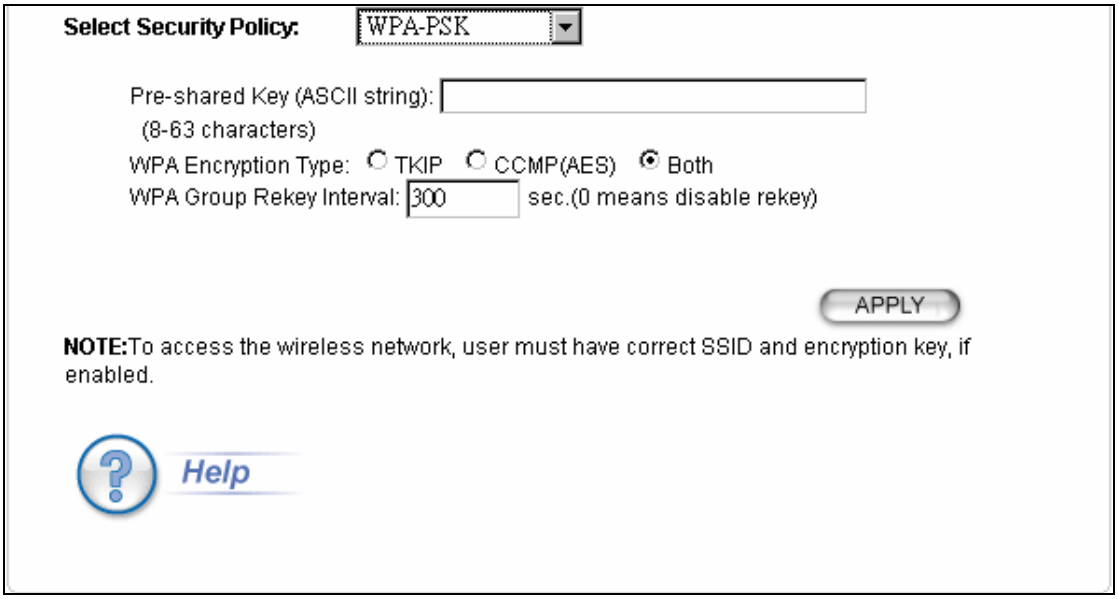
Wi-Fi Protected Access (WPA) requires a RADIUS server available in order to do authentication (same as 802.1x), thus there is no shared key required.

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

Group Rekey Interval: A group key is used for multicast/broadcast data, and the re-key interval is time period that the system will change the group key periodically. The shorter the interval is, the better the security is. The default is 300 sec.

WPA-PSK

Setup Wizard>>Wireless Settings >>Select Security Policy>>WPA-PSK



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

Pre-shared Key: This is an ASCII string with 8 to 63 characters. Please make sure that both the WLA-5000AP v3 and the wireless client stations use the same key.

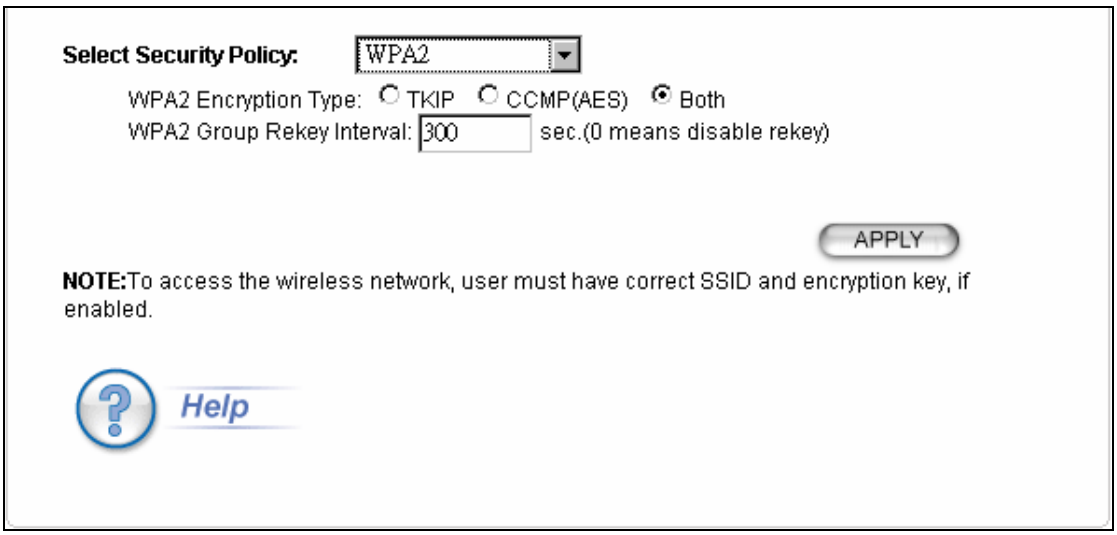
Encryption Type: There are two encryption types **TKIP** and **CCMP (AES)**. While CCMP provides better security than TKIP, some wireless client stations may not be equipped with the hardware to support it. You

can select **Both** to allow TKIP clients and CCMP clients to connect to the Access Point at the same time.

Group Rekey Interval: A group key is used for multicast/broadcast data, and the re-key interval is time period that the system will change the group key periodically. The shorter the interval is, the better the security is. The default is 300 sec.

WPA2

Setup Wizard>>Wireless Settings >>Select Security Policy>>WPA2



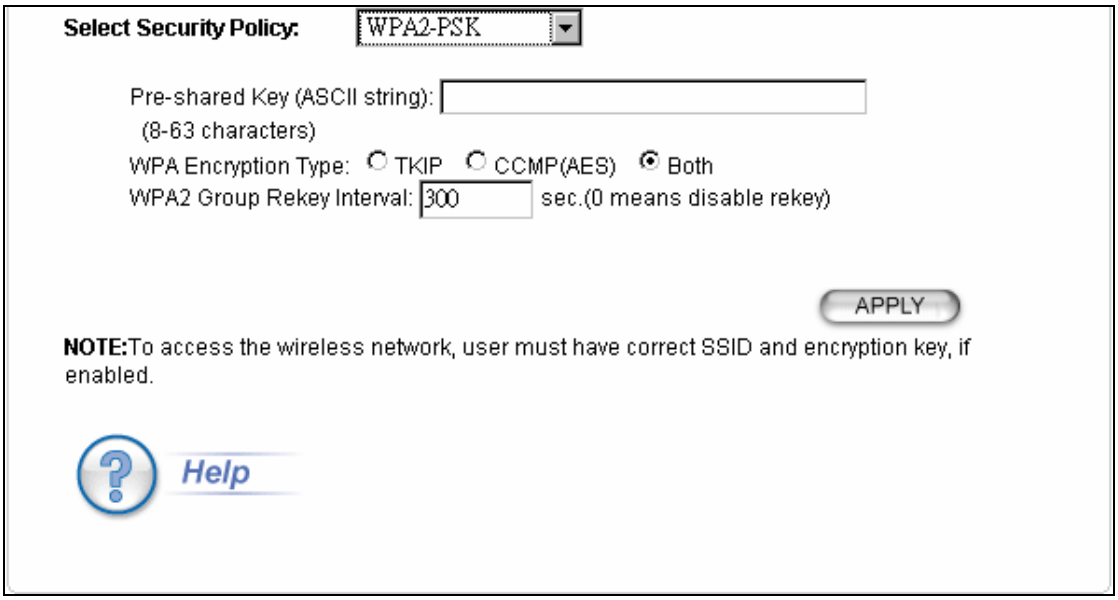
WPA2 stands for Wi-Fi Protected Access 2. It provides stronger data protection and network access control then WPA. Only authorized users can access the wireless networks.

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

Group Rekey Interval: A group key is used for multicast/broadcast data, and the re-key interval is time period that the system will change the group key periodically. The shorter the interval is, the better the security is. The default is 300 sec.

WPA2-PSK

Setup Wizard>>Wireless Settings >>Select Security Policy>>WPA2-PSK



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

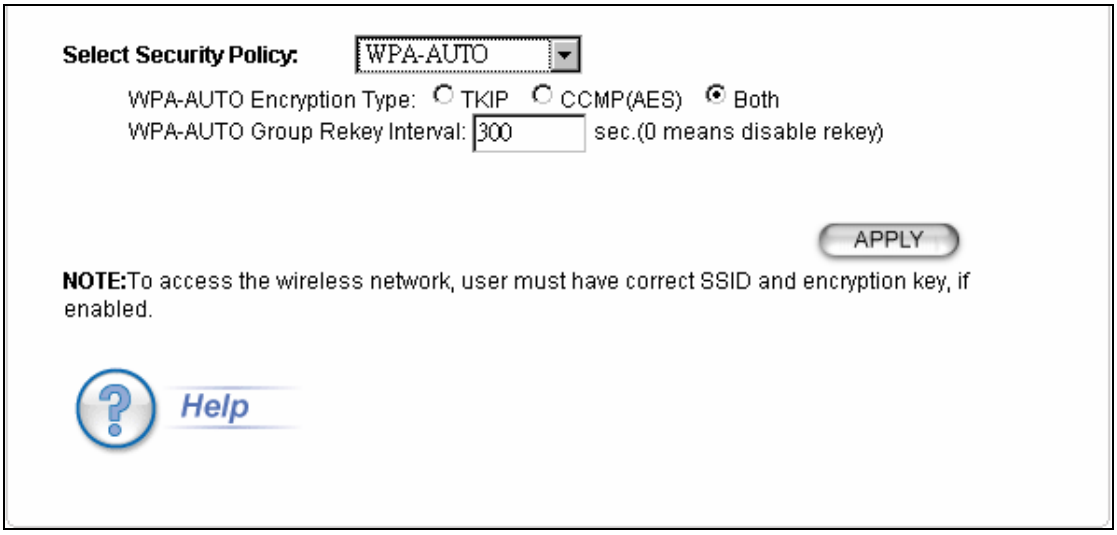
Pre-shared Key: This is an ASCII string with 8 to 63 characters. Please make sure that both the WLA-5000AP v3 and the wireless client stations use the same key.

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

Group Rekey Interval: A group key is used for multicast/broadcast data, and the re-key interval is time period that the system will change the group key periodically. The shorter the interval is, the better the security is. The default is 300 sec.

WPA-AUTO

Setup Wizard>>Wireless Settings >>Select Security Policy>>WPA-AUTO

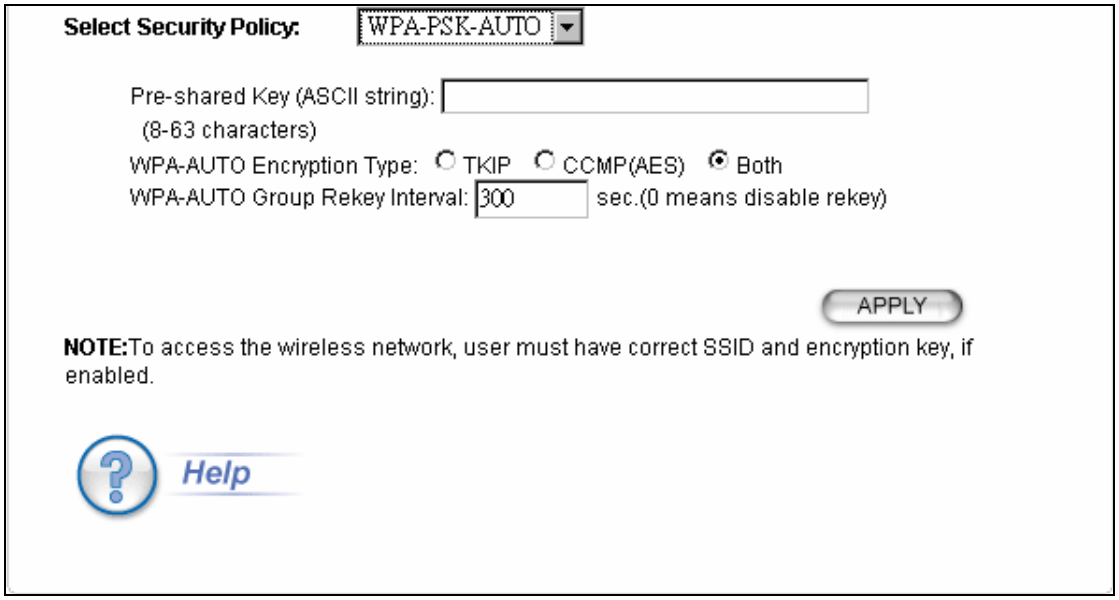


Encryption Type: There are two encryption types **TKIP** and **CCMP (AES)**. While CCMP provides better security than TKIP, some wireless client stations may not be equipped with the hardware to support it. You can select **Both** to allow TKIP clients and CCMP clients to connect to the Access Point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

Group Rekey Interval: A group key is used for multicast/broadcast data, and the re-key interval is time period that the system will change the group key periodically. The shorter the interval is, the better the security is. The default is 300 sec.

WPA-PSK-AUTO

Setup Wizard>>Wireless Settings >>Select Security Policy>>WPA-PSK-AUTO



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

Pre-shared Key: This is an ASCII string with 8 to 63 characters. Please make sure that both the WLA-5000AP v3 and the wireless client stations use the same key.

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

Group Rekey Interval: A group key is used for multicast/broadcast data, and the re-key interval is time period that the system will change the group key periodically. The shorter the interval is, the better the security is. The default is 300 sec.

3.1.4 FINISH SETUP WIZARD AND SAVE YOUR SETTINGS

After stepping through the Wizard's pages, you can click the **APPLY** button for your modification to take effect. This also makes your new settings saved into the permanent memory on your system.

Congratulations! You are now ready to use the WLA-5000AP v3.

If you change the device's IP address, as soon as you click on FINISH you will no longer be able to communicate with your WLA-5000AP v3. You need to change your IP address and then re-boot your computer in order to resume the communication.

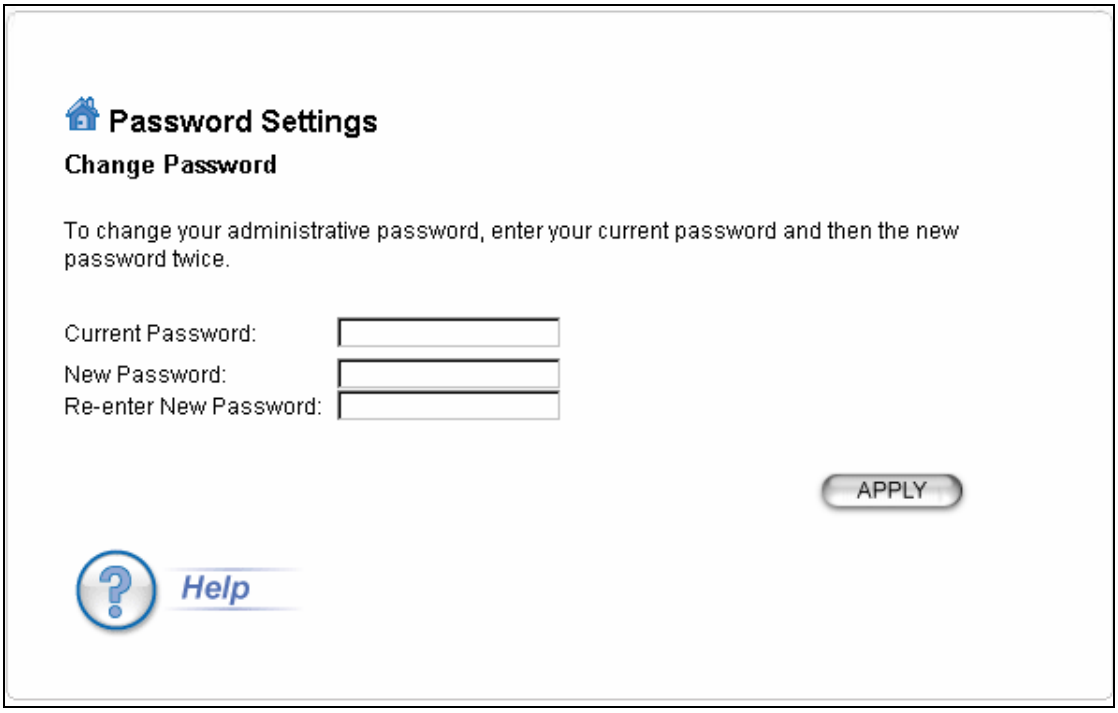
3.2 Advanced settings

The advanced settings tab on the top row of the window allows you to perform modifications that normally you may not need to do for general operations except changing your password from the default factory setting (this is highly recommended for security purposes).

3.2.1 PASSWORD SETTINGS

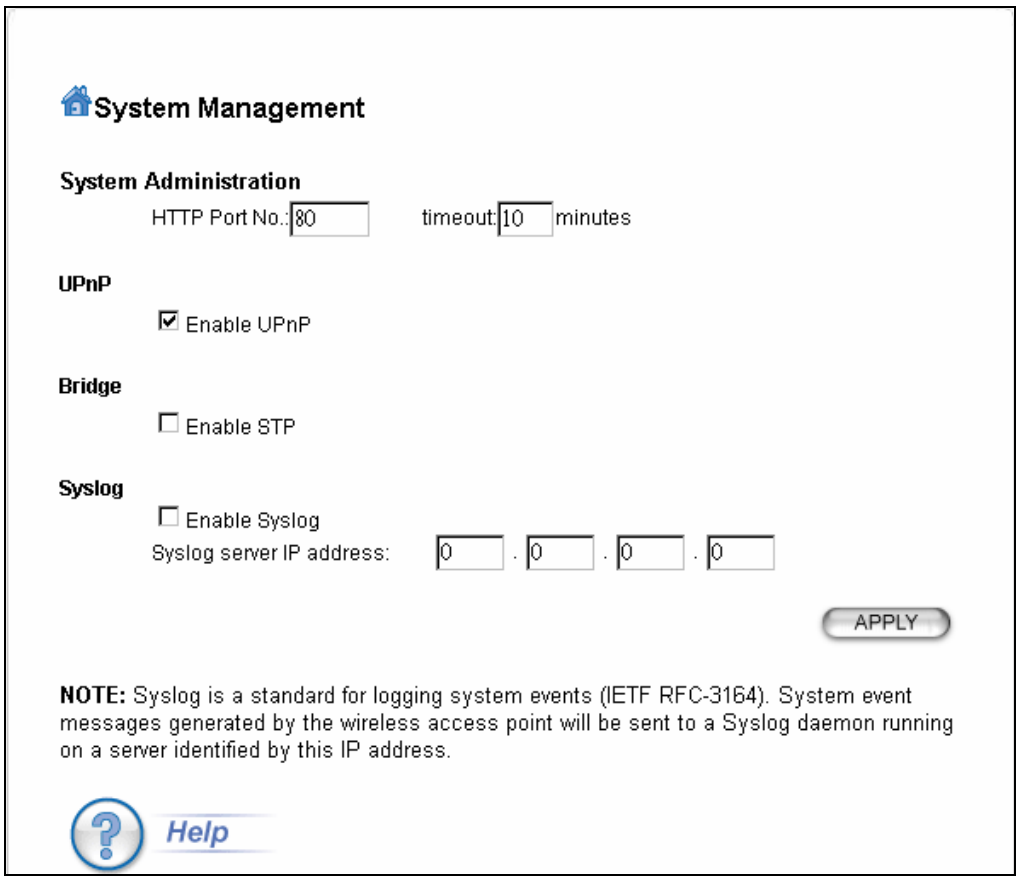
Advanced Settings>> Password Settings

The default factory password is "**password**". To change the password, press the **Password Settings** button to enter the **Password Settings** screen; then enter the Current Password followed by the New Password twice. The entered characters will appear as asterisks.



3.2.2 SYSTEM MANAGEMENT

Advanced Settings>> System Management
Clicking the **System Management** button to configure system related parameters to for the WLA-5000AP v3.



HTTP Port No.: HTTP stands for Hyper Text Transfer Protocol. The default port for the HTTP Web server is 80.

Time-out: This setting specifies the duration of idle time (inactivity) before a web browser or telnet management session times out. The default is 10 minutes.

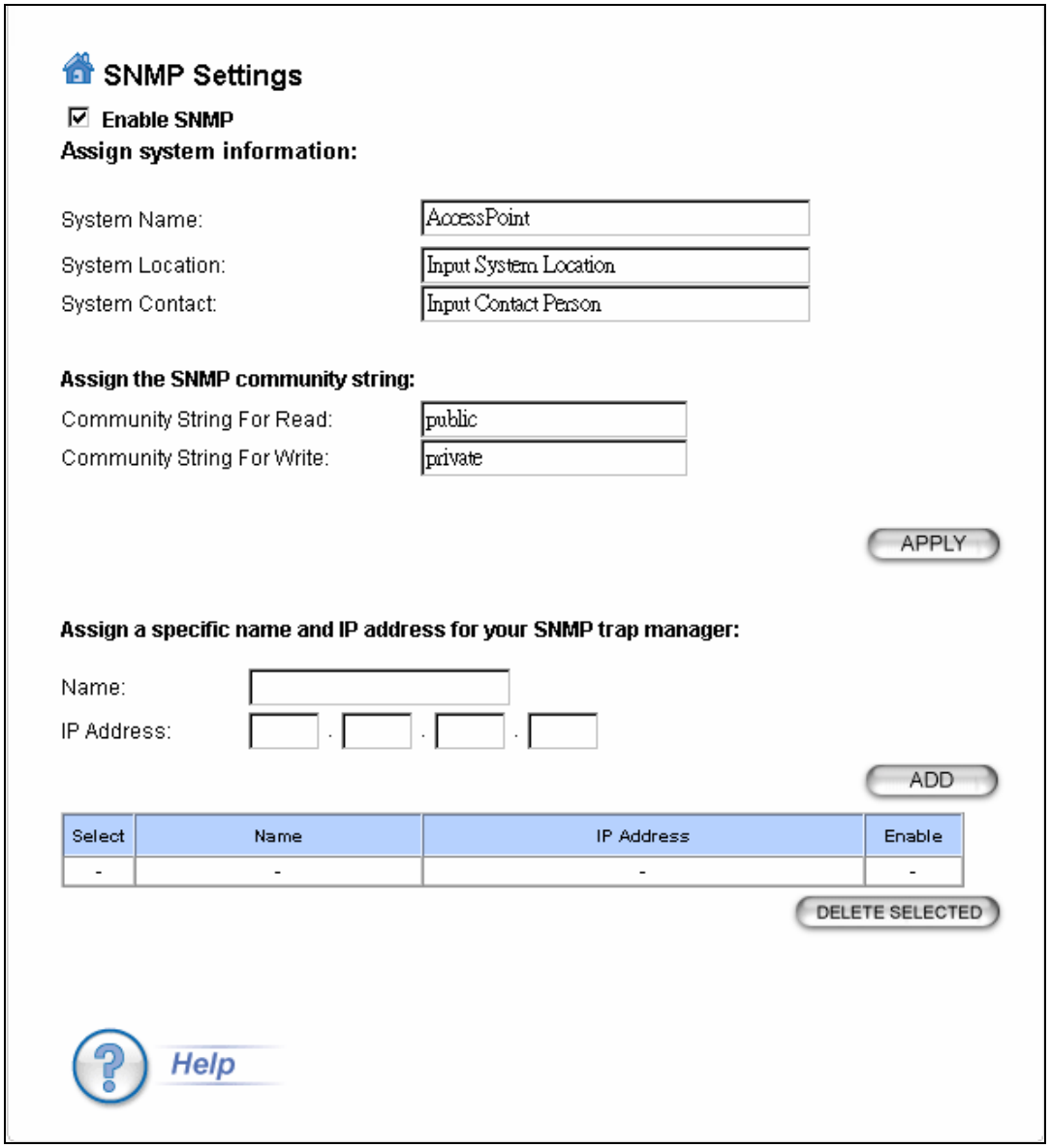
UPnP: The Universal Plug and Play (UPnP) feature allows a Windows XP/ME PC to discover this WLA-5000AP v3 and automatically show an icon on the screen. Then a user can double-click the icon to access this device directly (without having to find out its IP address).

Syslog: Syslog is an IETF (Internet Engineering Task Force - the Internet standards body)-conformant standard for logging system events (RFC-3164). When the WLA-5000AP v3 encounters an error or warning condition (e.g., a log-in attempt with an invalid password), it will create a log in the system log table. To be able to remotely view such system log events, you need to check the **Enable Syslog** box and configure the IP address of a Syslog daemon. When doing so, the WLA-5000AP v3 will send logged events over network to the daemon for future reviewing.

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

3.2.3 SNMP Settings

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



System Name: A name that you assign to your 802.11a+g Router. It is an alphanumeric string of up to 30 characters.

System Location: Enter a system location.

System Contact: Contact information for the system administrator responsible for managing your 802.11a+g Router. It is an alphanumeric string of up to 60 characters.

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

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

Assign a specific name and IP address for your SNMP trap manager:
A trap manager is a remote SNMP management station where special SNMP trap messages are generated (by the router) and sent to in the network.

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

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

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

3.2.4 MAC FILTERING SETTINGS

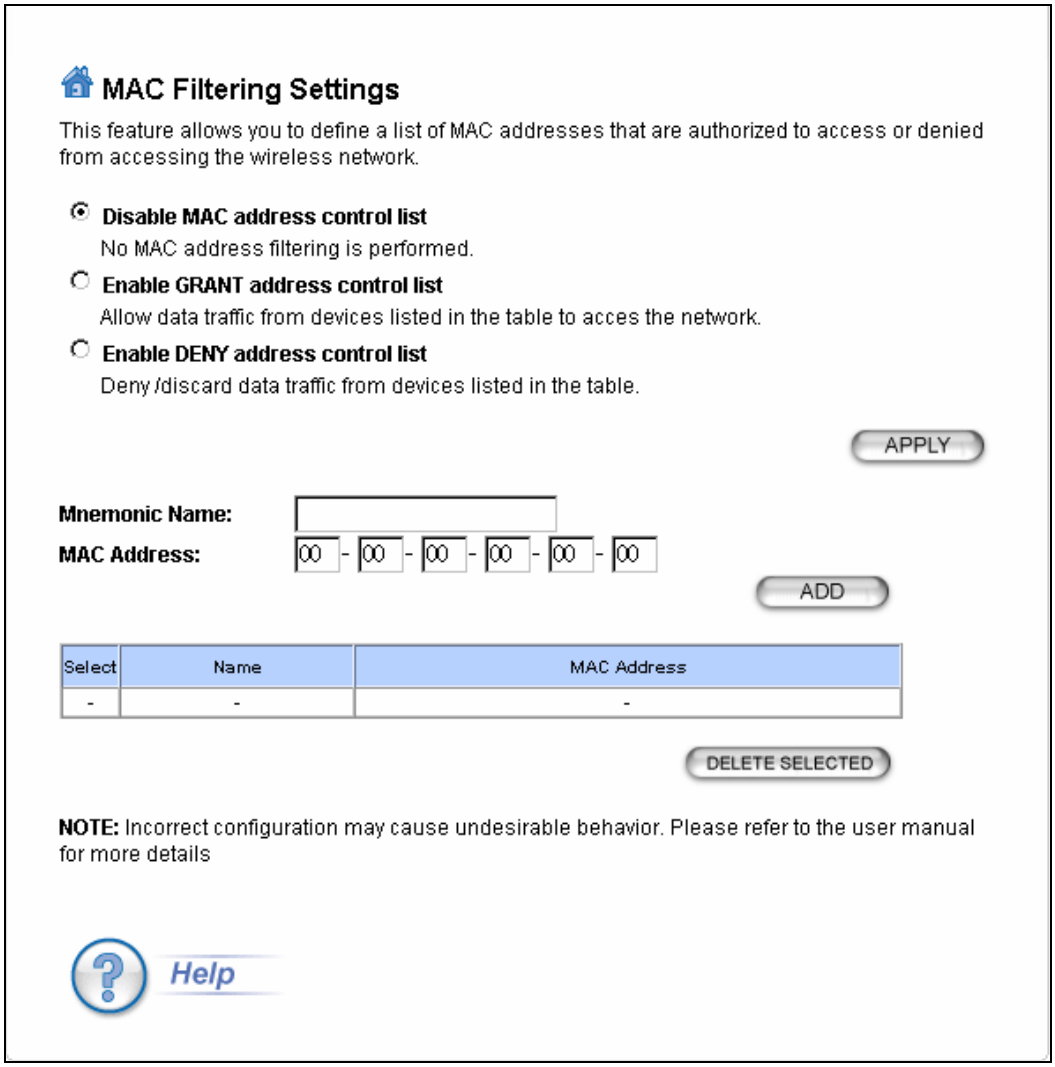
Advanced Settings>>Mac Filtering Settings

The WLA-5000AP v3 allows you to define a list of MAC addresses that are allowed or denied to access the wireless network.

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

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

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



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

To delete entries, check the corresponding **Select** boxes and then press **DELETE SELECTED.**

3.2.5 OPERATIONAL MODE

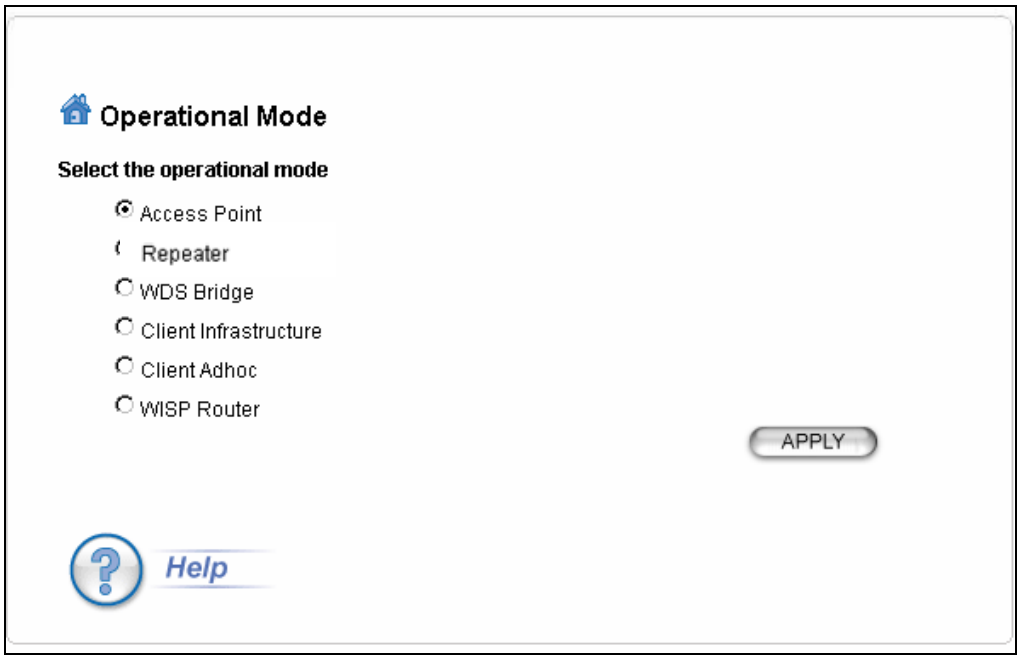
The WLA-5000AP v3 can be configured to operate in one of the following modes as mentioned previously in Chapter 1:

(1) Access Point (2) WDS Repeater (3) WDS Bridge (4) Client Infrastructure

(5) Client Adhoc (6) WISP Router

3.3 Access Point Mode Settings

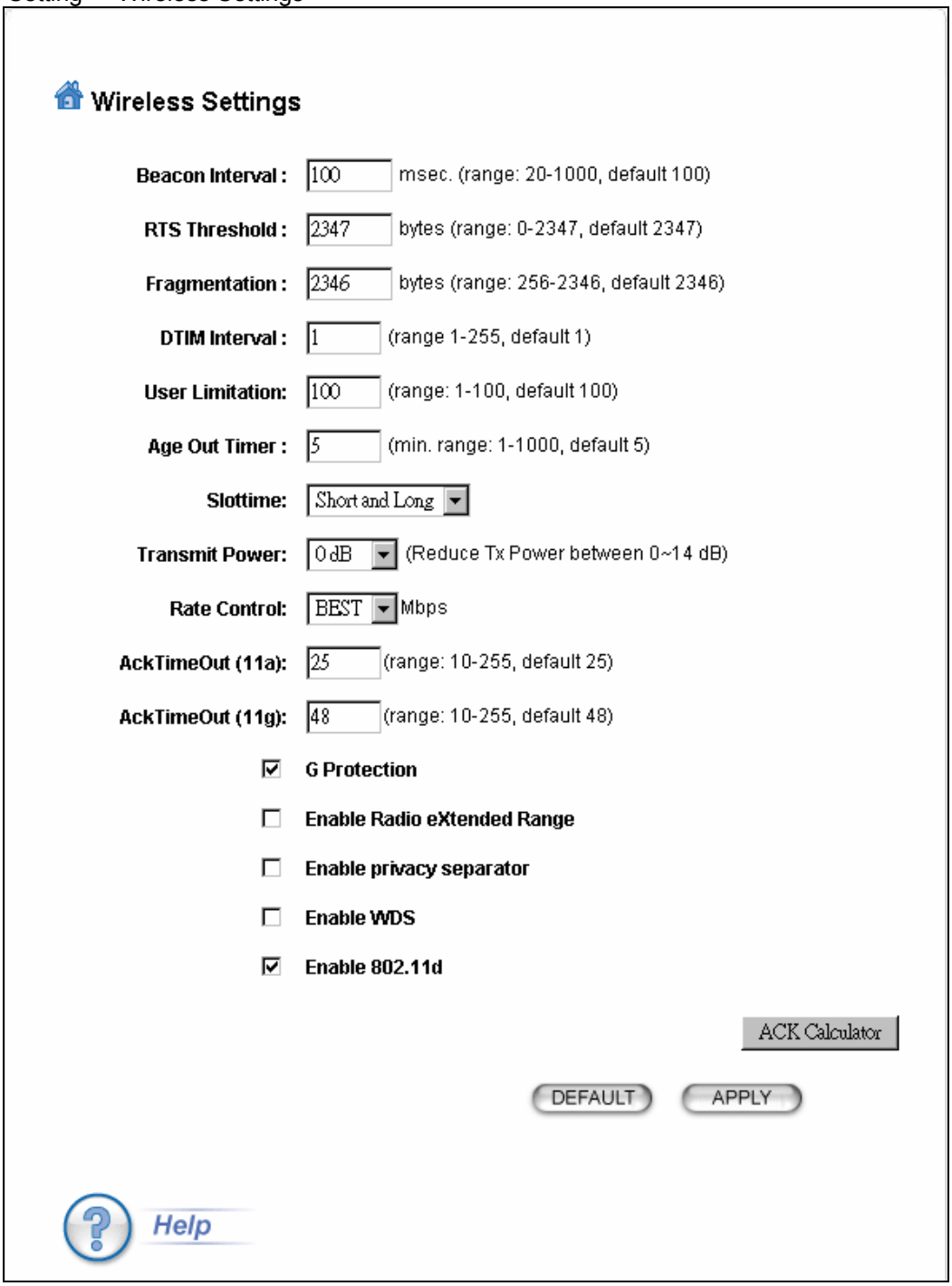
Advanced Settings>> Operation Mode>> Access Point



Select “Access Point” mode and then press **APPLY** button.

3.3.1 Wireless Settings

Advanced Setting>> Wireless Settings



Beacon Interval: The WLA-5000AP v3 broadcasts beacon frames regularly to announce its existence. The beacon Interval specifies how often beacon frames are transmitted in time unit of milliseconds. The default value is **100**, and a valid value should be between 1 and 65,535.

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

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

DTIM Interval: The WLA-5000AP v3 buffers packets for stations that operate in the power-saving mode. The Delivery Traffic Indication Message (DTIM) informs such power-conserving stations that there are packets

waiting to be received by them. The DTIM interval specifies how often the beacon frame should contain DTIMs. It should have a value between 1 to 255, with a default value of **3**.

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

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

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

Ack TimeOut (11a)/ (11g)/: The "ACK time-out" determines how long the program waits after receiving a packet from a file stream to determine that stream to be a complete file. For details, please go to Section 3.9.

Enable Radio eXtended Range: Select the check box to enable the Atheros's eXtended Range(XR) technology to extend the wireless coverage range.

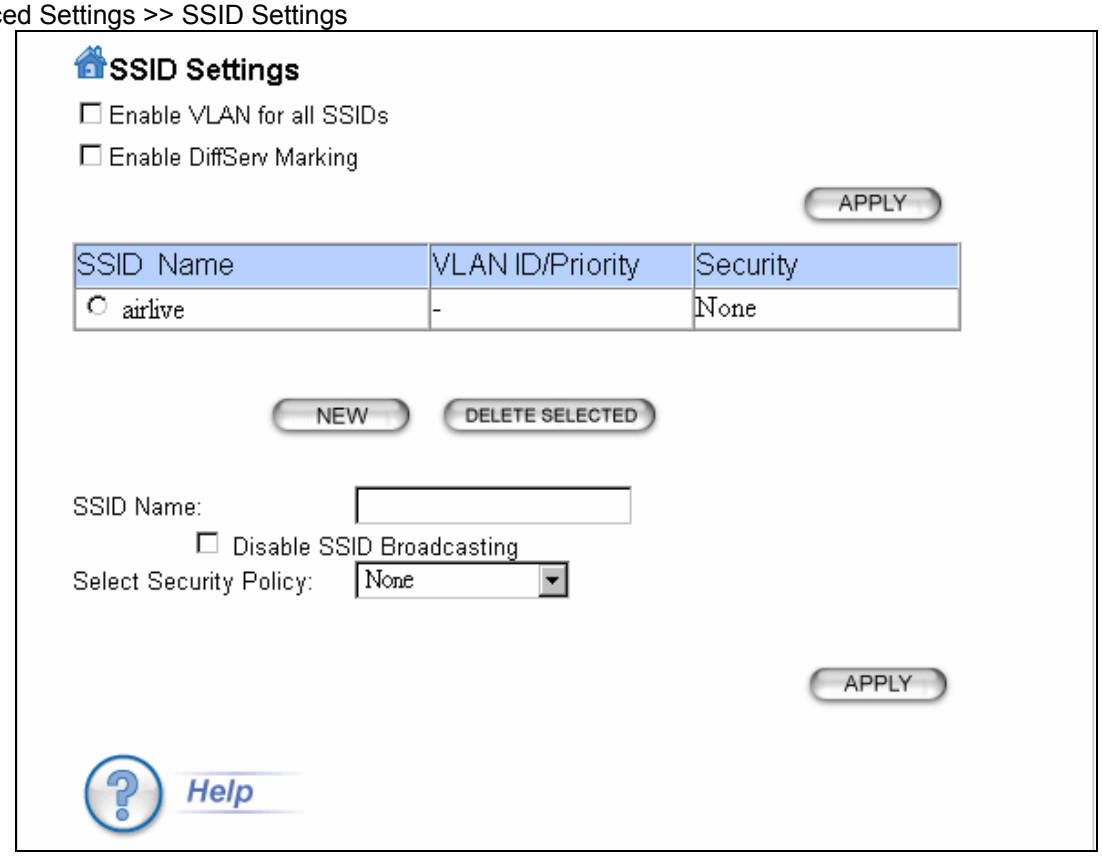
Enable privacy separator: Select the check box to prohibit data transmission between client stations.

Enable WDS: Select the check box to enable WDS (Wireless Distribution System).

Enable 802.11d: Select the check box to enable 802.11d. 802.11d is a standard for use in countries where systems using other standards in the 802.11 family are not allowed to operate.

3.3.2 SSID Settings

Advanced Settings >> SSID Settings



SSID, a name for an access point (or a network), differentiates one WLAN from another. All devices in a same

specific WLAN must use the same SSID.

VLAN: VLAN stands for Virtual Local Area Network. It is a technique allows one or more physical LAN routers or APs to deliver packets as if they were a single physical router or AP.

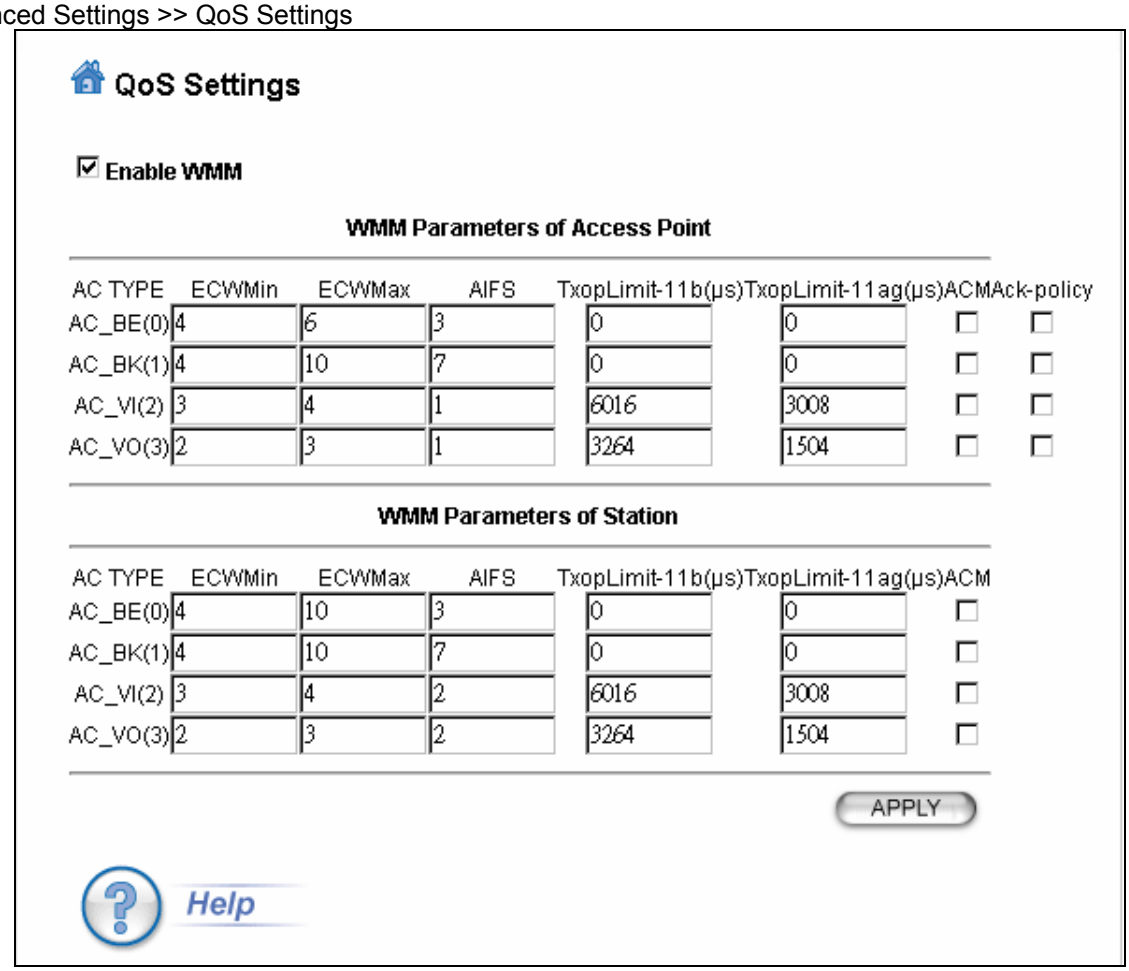
DiffServ Marking: Enable DiffServ Marking to have better traffic prioritization and bandwidth management.

Disable SSID Broadcasting: Select this check box to hide the SSID.

Security Policy: Select security policy. “None”, “WEP”, “802.1x”, “WPA”, “WPA-PSK”, “WPA2”, “WPA2-PSK”, “WPA-AUTO” or “WPA-PSK-AUTO”.

3.3.3 QoS Settings

Advanced Settings >> QoS Settings



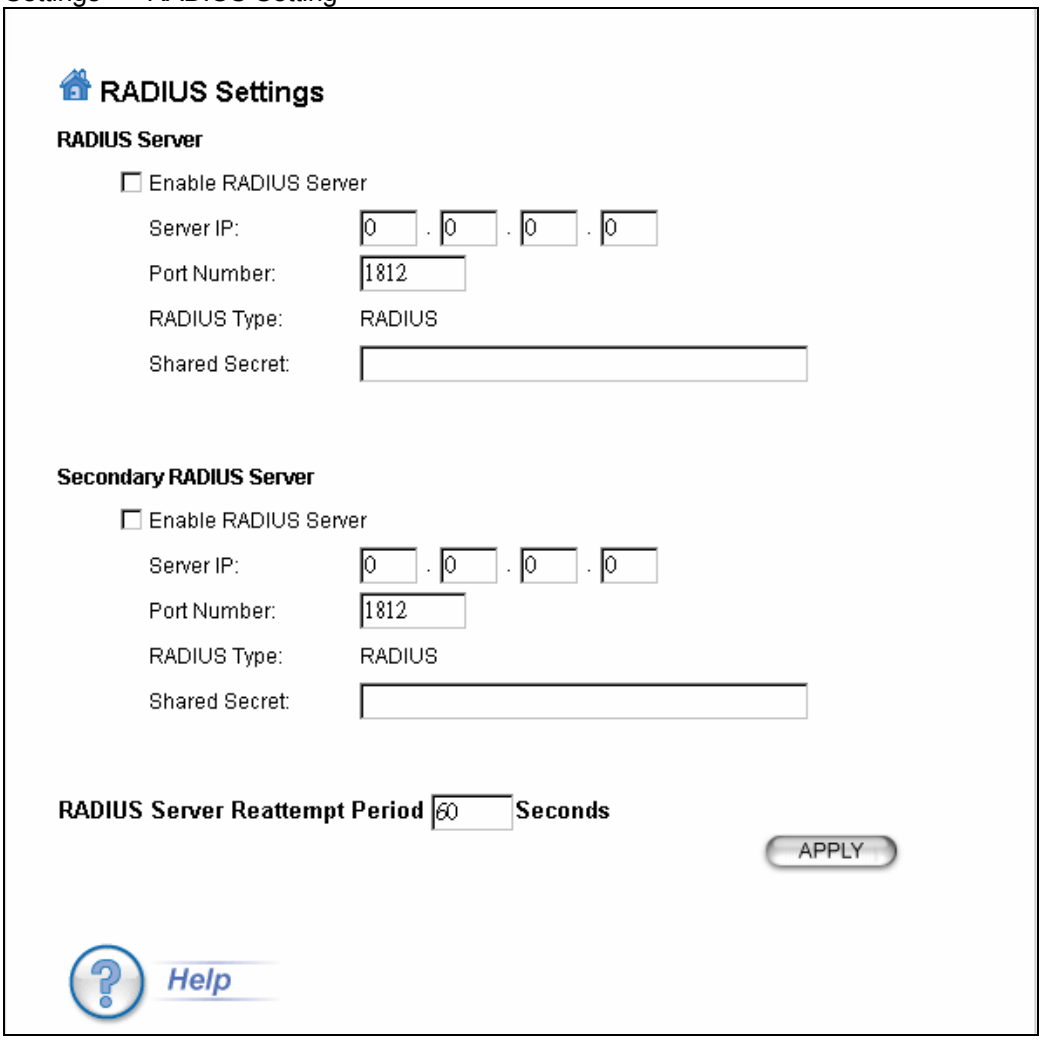
QoS stands for Quality of Service which attempts to provide different levels of quality to different types of network traffic.

WMM stands for Wi-Fi Multimedia. WMM defines quality of service (QoS) in wireless networks. WMM improves audio, video and voice applications transmitted over wireless networks. WMM adds prioritized capabilities to wireless networks and optimizes the performance when multiple concurring applications.

To **Enable WMM**, WMM Parameters of Access Point and Station are indicated. The following information is listed: AC TYPE (AC_BE; Best Effort) (AC_BK; Background)(AC_VI; Video)(AC_VO;Voice)/ ECWMIn/ ECWMax/ AIFS/ TxopLimit (11b)/ TxopLimit (11ag)ACM and Ack-policy.

3.3.4 RADIUS Settings

Advanced Settings >> RADIUS Setting



RADIUS servers provide centralized authentication services to wireless clients. Two RADIUS servers can be defined: one acts as a primary, and the other acts as a backup.

MAC address filtering based authentication requires a MAC address filter table to be created in either the WLA-5000AP v3 (as described in Chapter 3.2.3 MAC Filtering Settings) and/or the RADIUS server. During the authentication phase of a wireless station, the MAC address filter table is searched for a match against the wireless client's MAC address to determine whether the station is to be allowed or denied to access the network.

To Enable RADIUS Server:

Server IP: The IP address of the RADIUS server.

Port Number: The port number that your RADIUS server uses for authentication. The default setting is 1812.

RADIUS Type: RADIUS

Shared Secret: This is used by your RADIUS server in the Shared Secret field in RADIUS protocol messages. The shared secret configured in the WLA-5000AP v3 must match the shared secret configured in the RADIUS server. The shared secret can contain up to 64 alphanumeric characters.

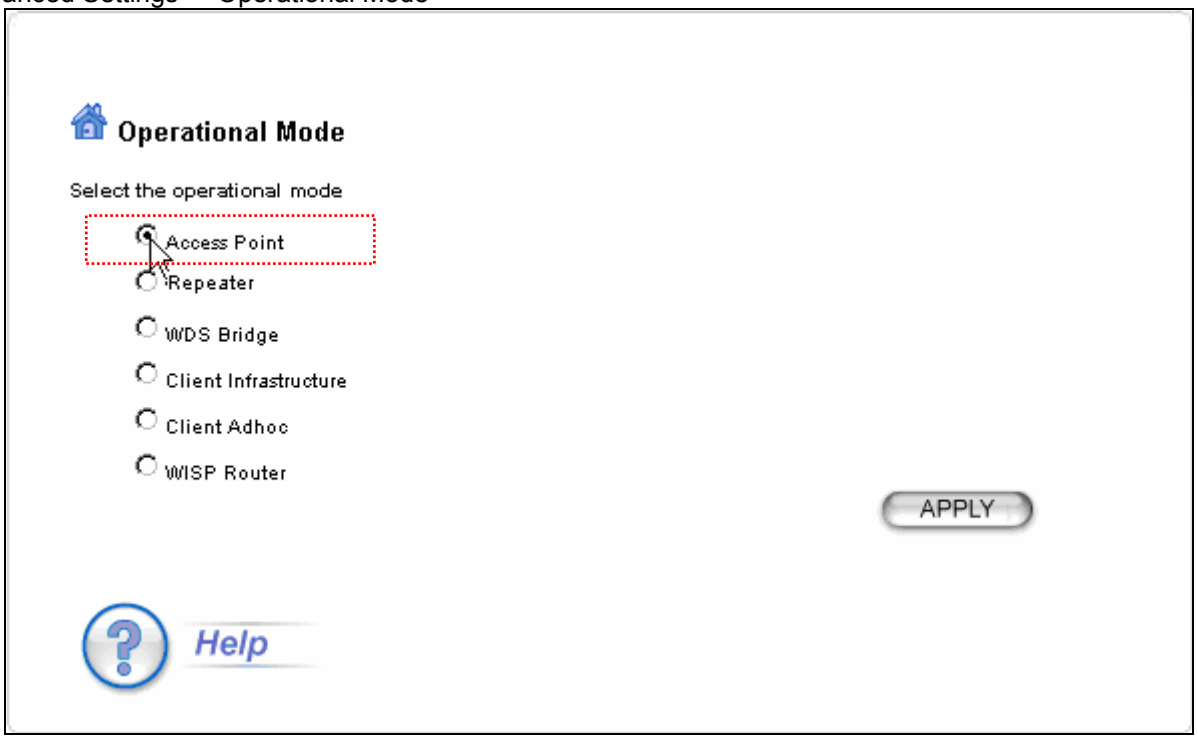
RADIUS Server Reattempt Period: The number of times the WLA-5000AP v3 should attempt to contact the primary server before giving up
Enter the information for a second RADIUS server in case that there are 2 on your network which you are using authenticate wireless clients.

3.4 Repeater Mode Settings

For the Repeater node, please be aware that current Repeater mode ONLY works with WLA-5000AP v3 firmware 2.x device as AP node.

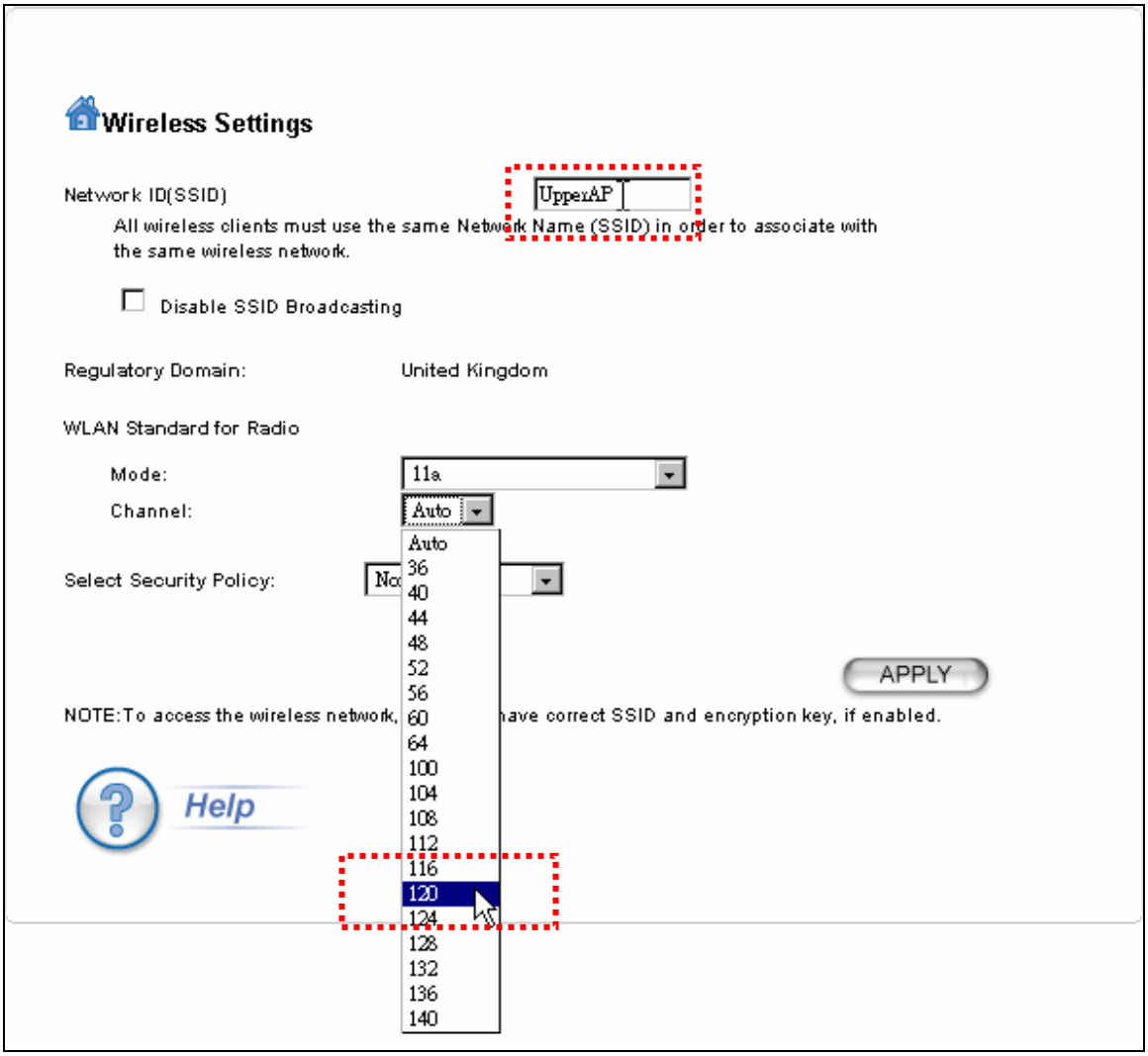
3.4.1 AP Node Settings

Advanced Settings>> Operational Mode



Set up first the device as an AP mode, click on “APPLY”,
Next Step, choose Wireless Mode and channel in the “Wireless Settings” under Setup Wizard.

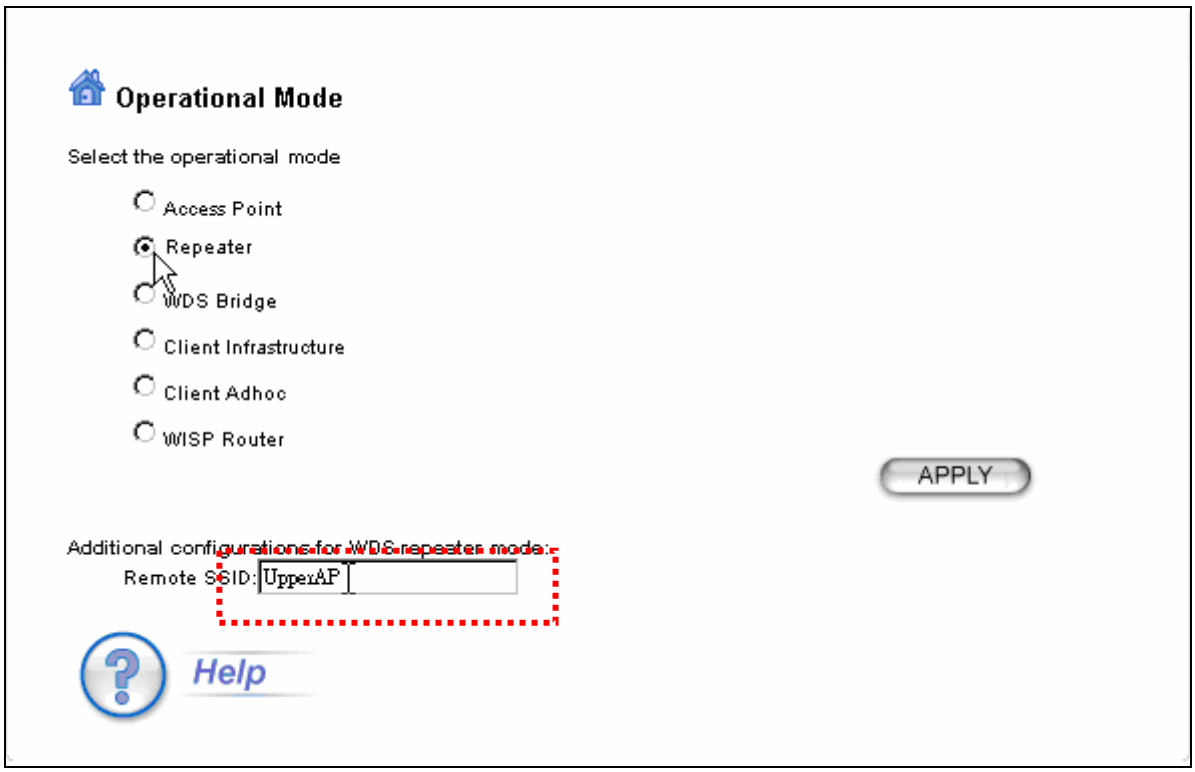
Setup Wizard>>Wireless settings



Select the WLAN mode and channel of your choice
Click on “APPLY” to finish setup.

3.4.2 Repeater Node Settings

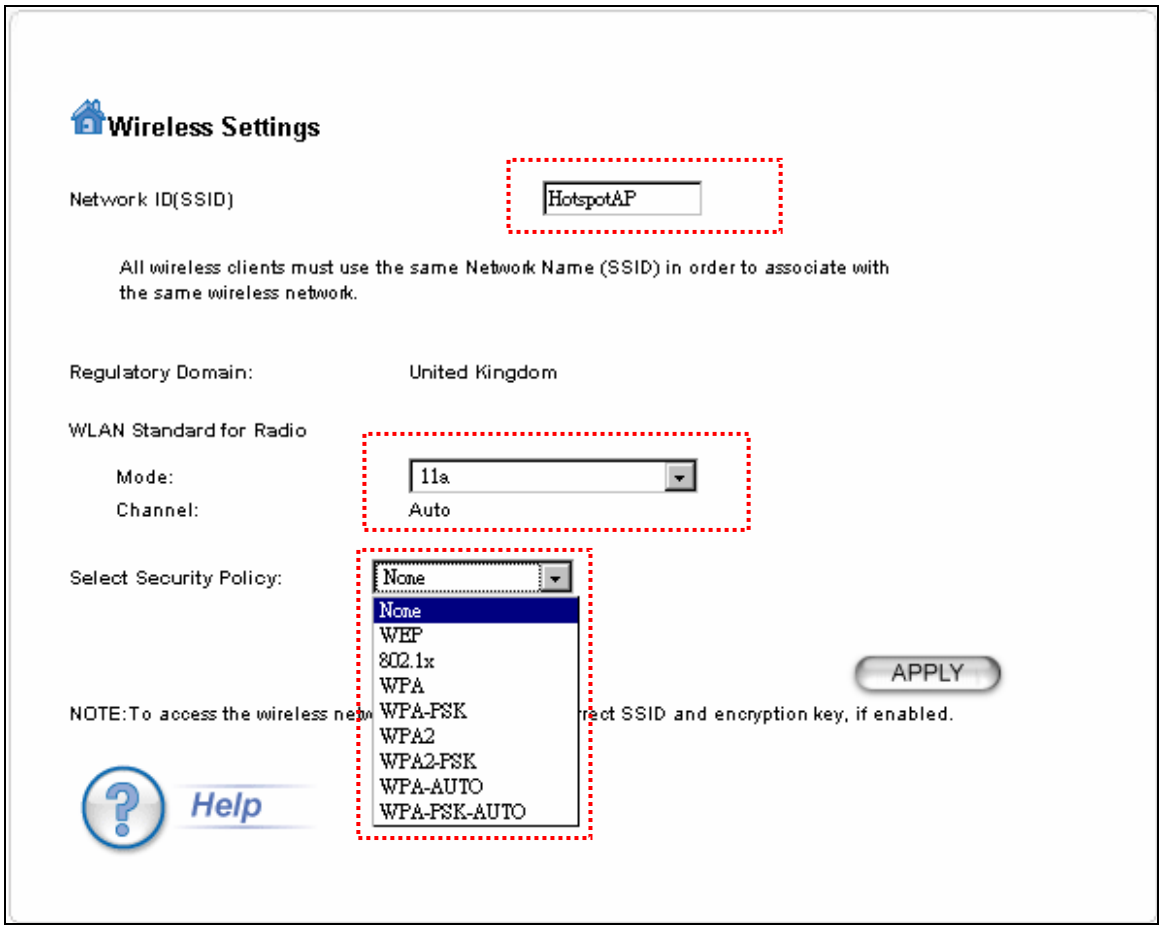
Advanced Settings>>Operation Mode
To set a device as Repeater, the device has to be first defined as repeater operation mode.



Select “Repeater” mode and then enter the “Remote SSID”, this is the SSID of AP node’s SSID.
Click on the “Repeater” radio button
Key-in the SSID of upper node’s SSID.
Click **APPLY** button.
Next step is to set the AP configuration for client device for Repeater node.

3.4.3 Repeater Node Local service Settings

Setup Wizard>>Wireless Settings
In the Setup Wizard, select the WLAN mode, in this case, only the WLAN mode and SSID can be modified, the channel will automatically readjusted as the upper node.



Set the SSID for the Hotspot service. This SSID can be different from upper node's SSID.
Its Channel will be display as "Auto" it will be same as the AP node's channel. It's necessary to set the Wireless mode as the same spectrum as AP's node.
You can set encryption for the security between hotspot services with client device.

3.4.4 Repeater Advance Wireless Setting

Advanced Settings>>Wireless setting

Beacon Interval: The WLA-5000AP V3 broadcasts beacon frames regularly to announce its existence. The beacon Interval specifies how often beacon frames are transmitted in time unit of milliseconds. The default value is **100**, and a valid value should be between 1 and 65,535.

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

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

DTIM Interval: The WLA-5000AP V3 buffers packets for stations that operate in the power-saving mode. The Delivery Traffic Indication Message (DTIM) informs such power-conserving stations that there are packets waiting to be received by them. The DTIM interval specifies how often the beacon frame should contain DTIMs. It should have a value between 1 to 255, with a default value of **3**.

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

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

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

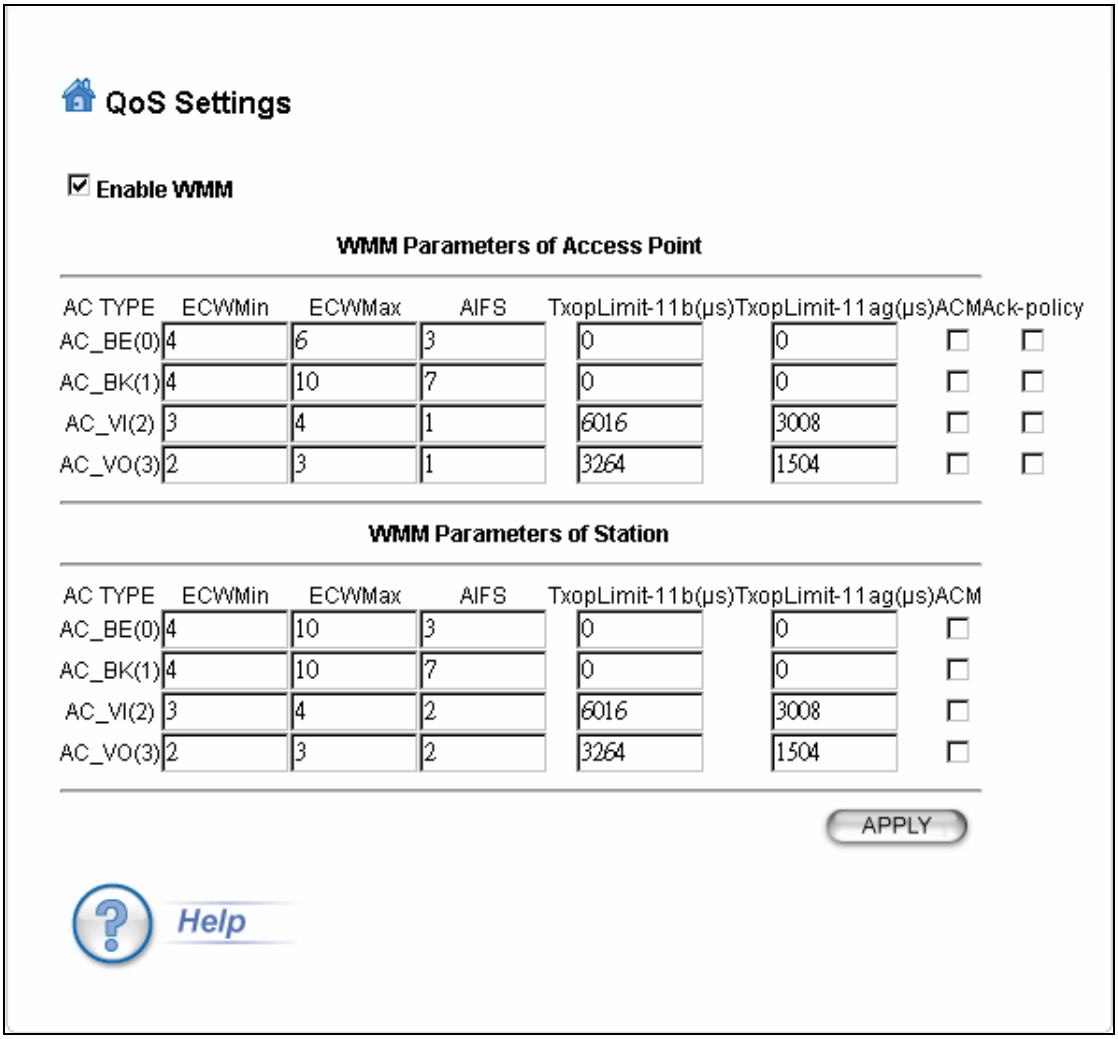
Ack TimeOut (11a)/ (11g)/: The "ACK time-out" determines how long the program waits after receiving a packet from a file stream to determine that stream to be a complete file. For details, please go to Section 3.9.

Enable Radio eXtended Range: Select the check box to enable the Atheros's eXtended Range(XR) technology to extend the wireless coverage range.

Enable privacy separator: Select the check box to prohibit data transmission between client stations.

3.4.5 QoS Settings

Advanced Setting >> QoS Settings



QoS stands for Quality of Service which attempts to provide different levels of quality to different types of network traffic.

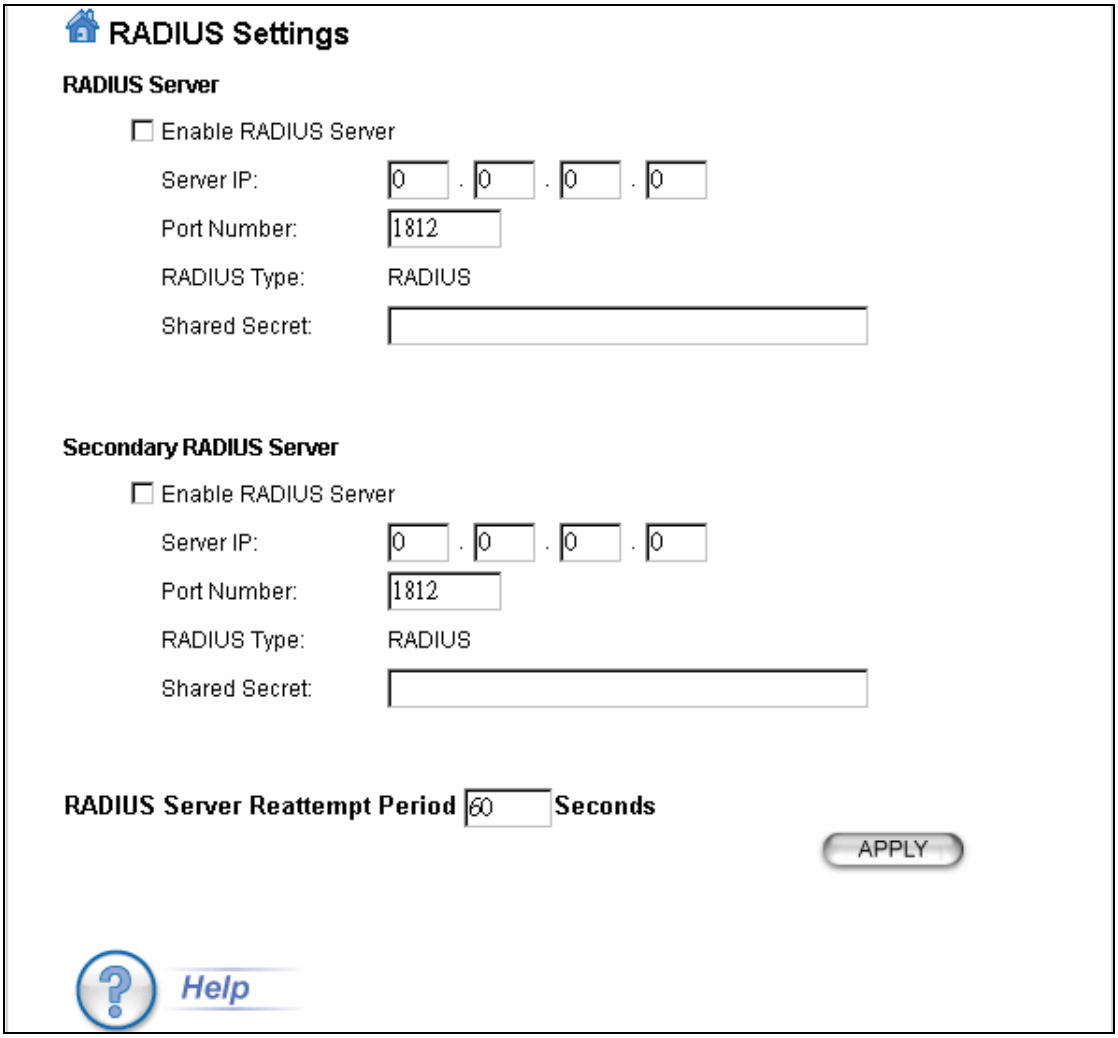
QoS stands for Quality of Service which attempts to provide different levels of quality to different types of network traffic.

WMM stands for Wi-Fi Multimedia. WMM defines quality of service (QoS) in wireless networks. WMM improves audio, video and voice applications transmitted over wireless networks. WMM adds prioritized capabilities to wireless networks and optimizes the performance when multiple concurring applications.

To **Enable WMM**, WMM Parameters of Access Point and Station are indicated. The following information is listed: AC TYPE (AC_BE; Best Effort) (AC_BK; Background)(AC_VI; Video)(AC_VO;Voice)/ ECWMIn/ ECWMax/ AIFS/ TxopLimit (11b)/ TxopLimit (11ag)ACM and Ack-policy.

3.4.6 RADIUS Settings

Advanced Setting >> RADIUS Settings



RADIUS servers provide centralized authentication services to wireless clients. Two RADIUS servers can be defined: one acts as a primary, and the other acts as a backup.

MAC address filtering based authentication requires a MAC address filter table to be created in either the WLA-5000AP V3 (as described in Chapter 3.2.3 MAC Filtering Settings) and/or the RADIUS server. During the authentication phase of a wireless station, the MAC address filter table is searched for a match against the wireless client's MAC address to determine whether the station is to be allowed or denied to access the network.

To Enable RADIUS Server:

Server IP: The IP address of the RADIUS server.

Port Number: The port number that your RADIUS server uses for authentication. The default setting is 1812.

RADIUS Type: RADIUS

Shared Secret: This is used by your RADIUS server in the Shared Secret field in RADIUS protocol messages. The shared secret configured in the WLA-5000AP V3 must match the shared secret configured in the RADIUS server. The shared secret can contain up to 64 alphanumeric characters.

RADIUS Server Reattempt Period: The number of times the WLA-5000AP V3 should attempt to contact the primary server before giving up

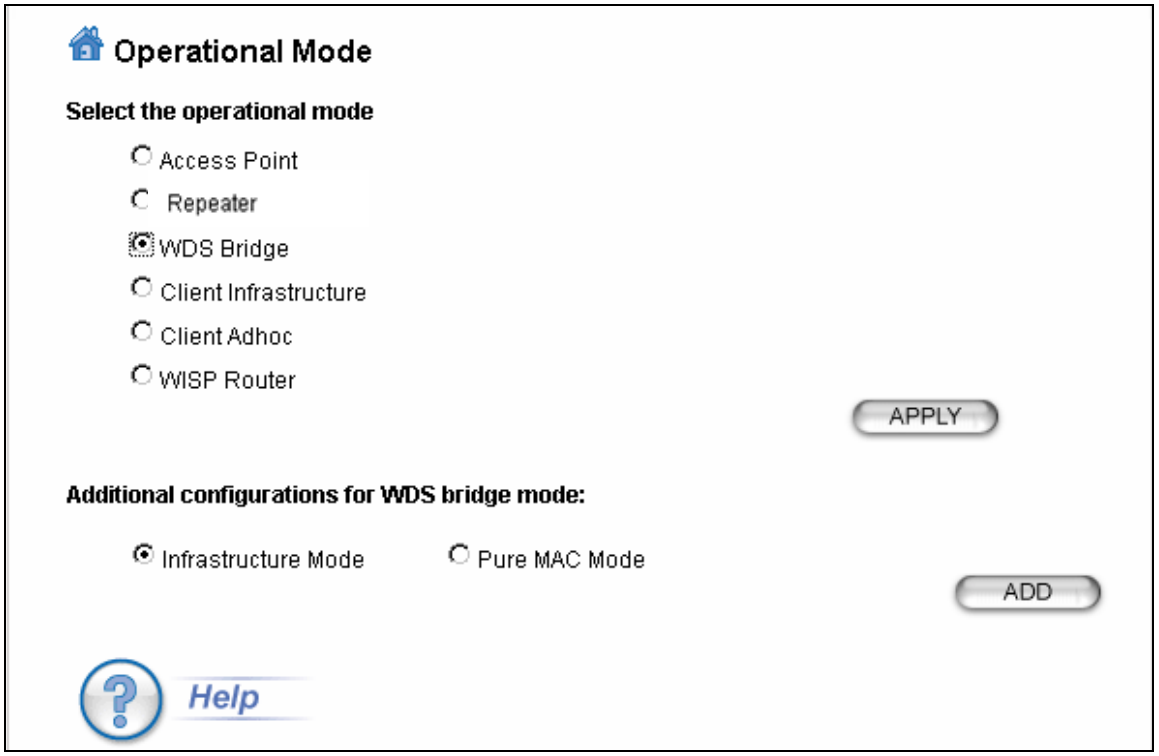
Enter the information for a second RADIUS server in case that there are 2 on your network which you are using authenticate wireless clients.

`

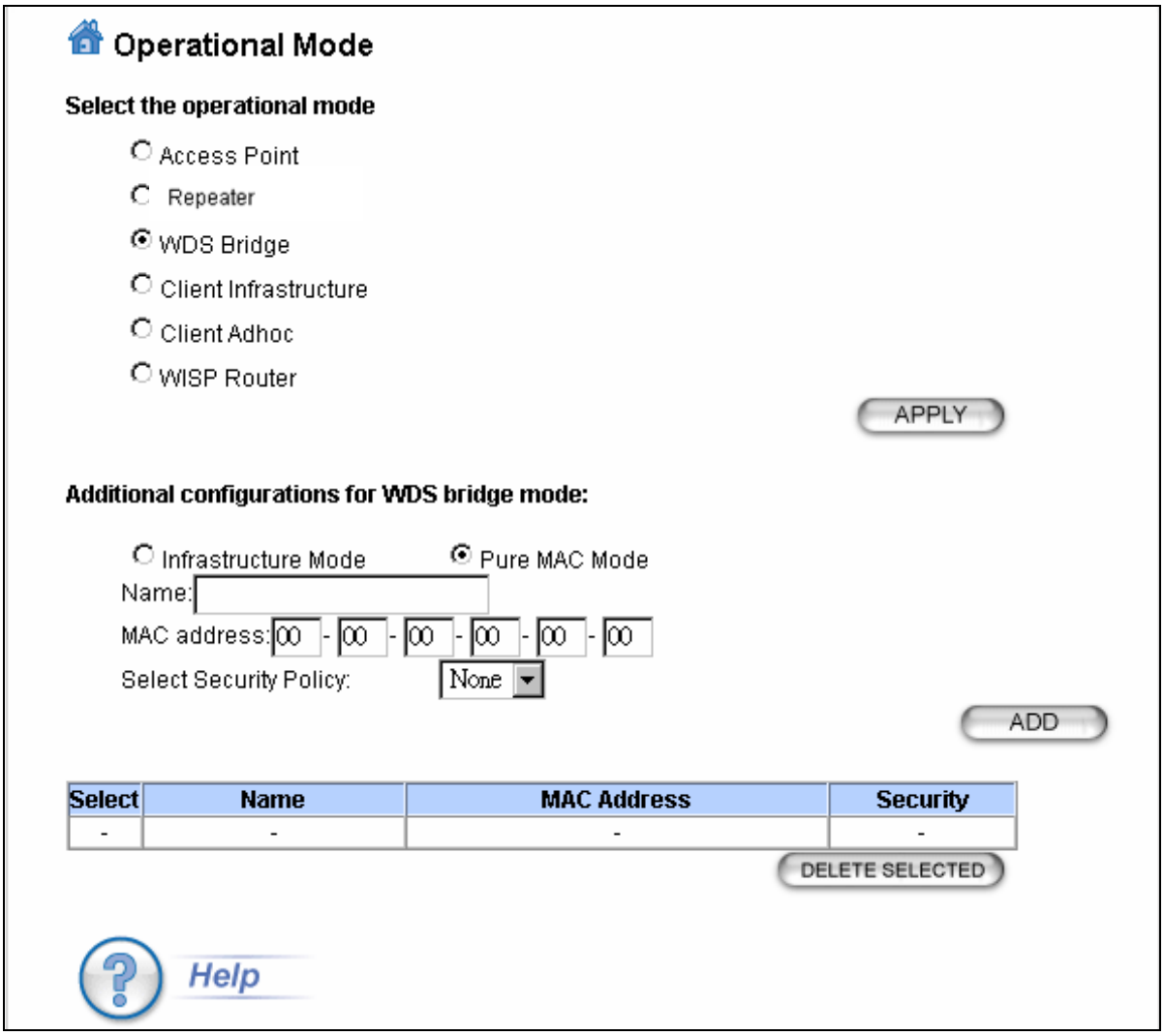
3.5 WDS Bridge Mode Settings

Advanced Setting >> Operation Mode>> WDS Bridge

Select “WDS Bridge” mode and then press the ‘APPLY‘ button. Additionally, to use the WDS as AP-client mode with SSID, please choose “Infrastructure Mode” radio button.

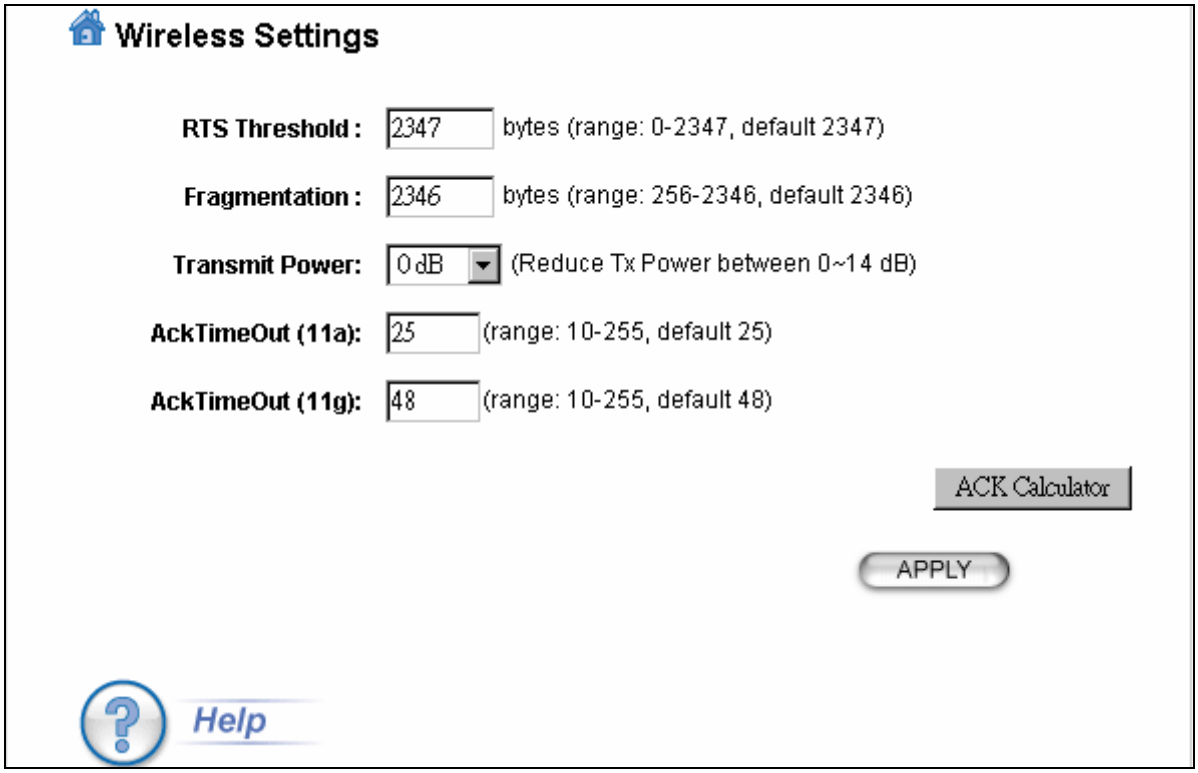


To use MAC registration mode WDS, please select the “Pure MAC Mode” radial button. When configured as a WDS Bridge Pure MAC mode, you need to further configure the name and MAC address of its peer WDS devices.



3.5.1 Wireless Settings

Advanced Setting >> Wireless Setting



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

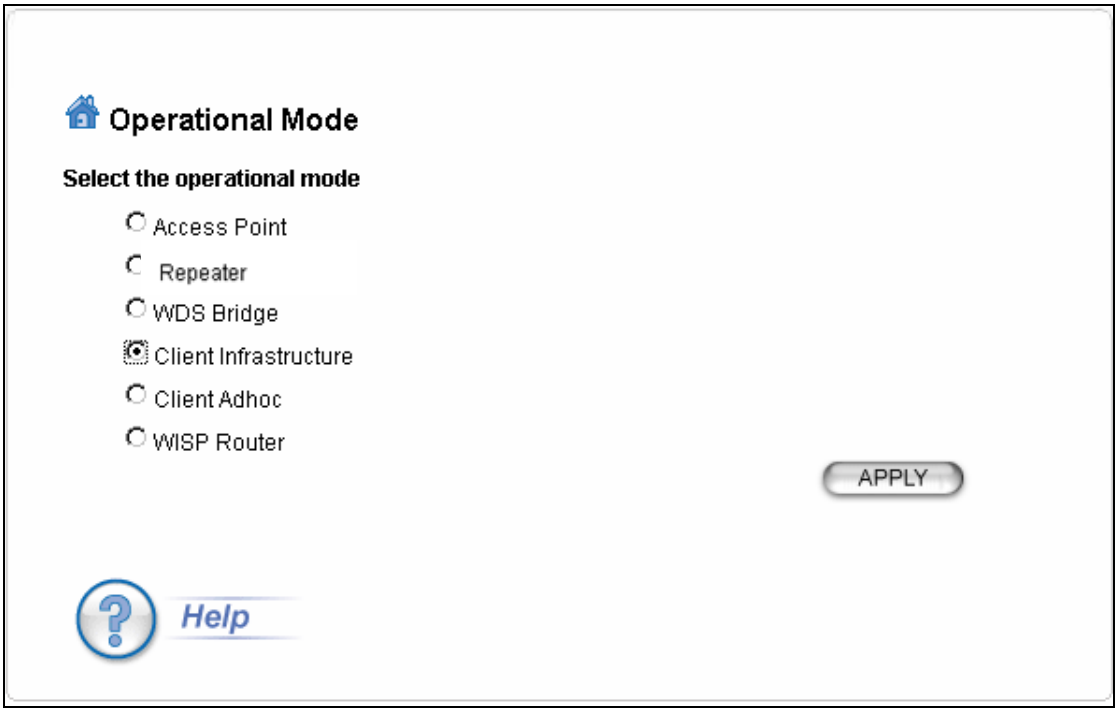
Fragmentation: When the size of a unicast frame exceeds the fragmentation threshold, it will be fragmented before the transmission. It should have a value of 256-2346 bytes, with a default of **2346**. If you experience a high packet error rate, you should slightly decrease the Fragmentation Threshold.

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

Ack TimeOut (11a)/ (11g)/: The "ACK time-out" determines how long the program waits after receiving a packet from a file stream to determine that stream to be a complete file. For details, please go to Section 3.9.

3.6 Client Infrastructure Mode Settings

Advanced Setting>>Operation Mode>> Client Infrastructure

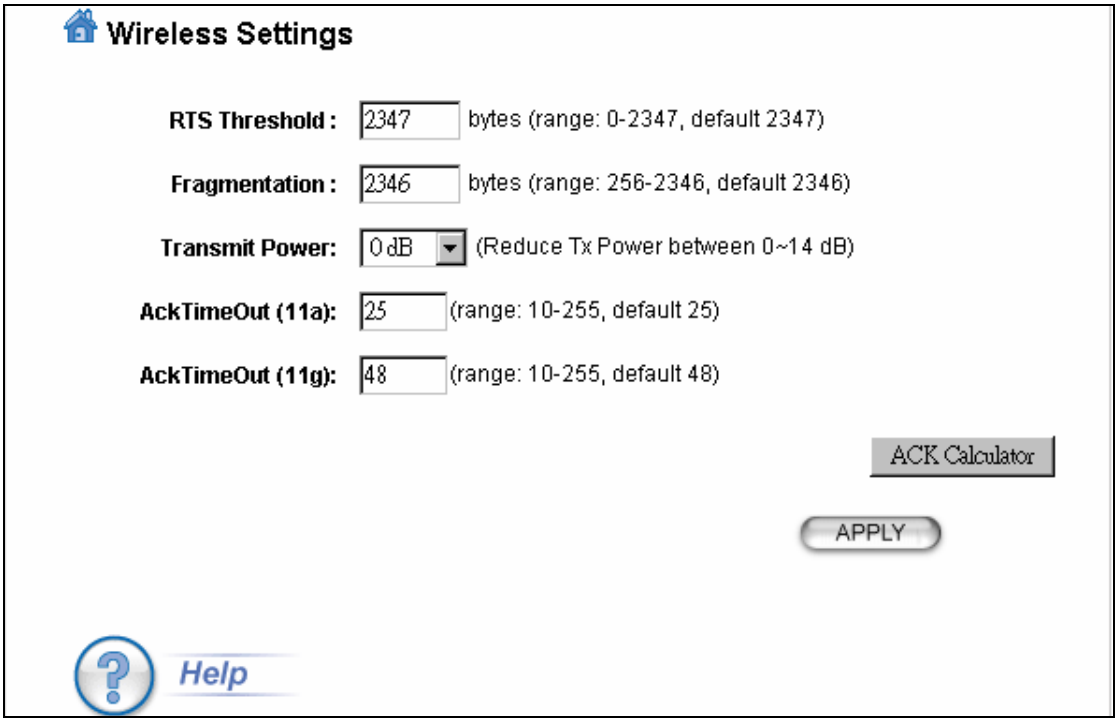


Select “Client Infrastructure” mode and then click APPLY button.

The client can search for the SSIDs of APs in the environment, in order to select the AP that he wants to make connection with. For details, please go to Section 4.5: Device Status>>Site Survey

3.6.1 Wireless Settings

Advanced Setting >> Wireless Setting



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

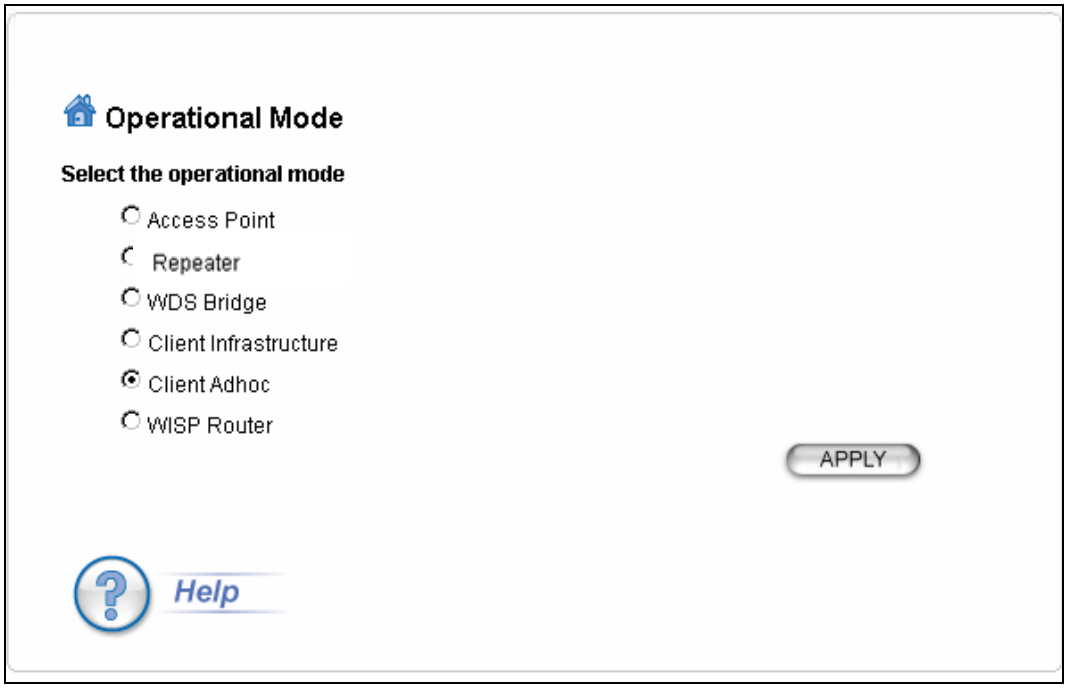
Fragmentation: When the size of a unicast frame exceeds the fragmentation threshold, it will be fragmented before the transmission. It should have a value of 256-2346 bytes, with a default of **2346**. If you experience a high packet error rate, you should slightly decrease the Fragmentation Threshold.

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

Ack TimeOut (11a)/ (11g)/: The "ACK time-out" determines how long the program waits after receiving a packet from a file stream to determine that stream to be a complete file. For details, please go to Section 3.9.

3.7 Client Adhoc Mode Settings

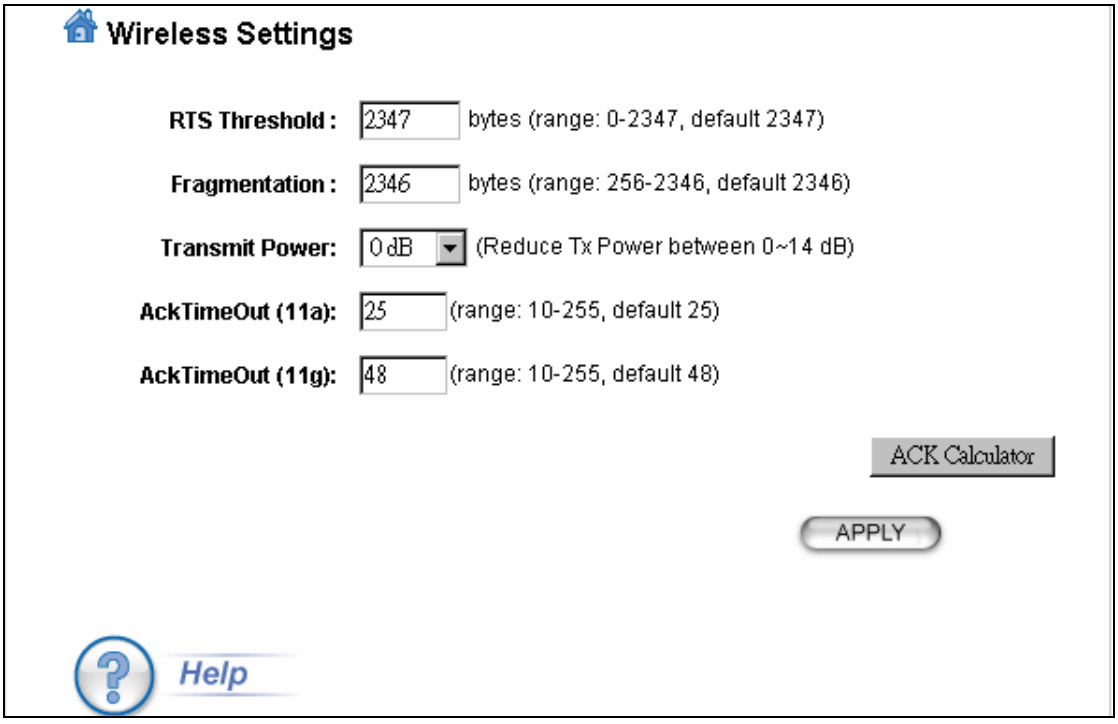
Advanced Setting >> Operation Mode >> Client Adhoc



Select “Client Adhoc” mode and then click APPLY button.

3.7.1 Wireless Settings

Advanced Setting >> Wireless Settings



RTS Threshold: RTS/CTS frames are used to gain control of the medium for transmission. Any unicast (data or control) frames larger than specified RTS threshold must be transmitted following the RTS/CTS handshake

exchange mechanism. The RTS threshold should have a value between 256-2347 bytes, with a default of **2347**. It is recommended that this value does not deviate from the default too much.

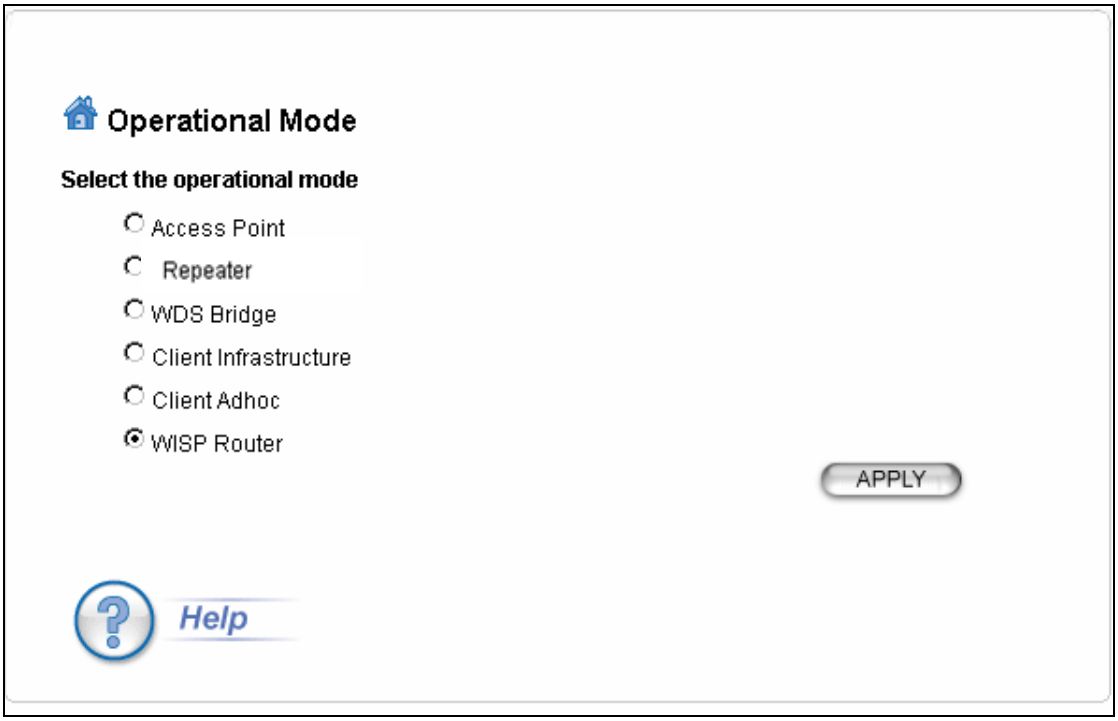
Fragmentation: When the size of a unicast frame exceeds the fragmentation threshold, it will be fragmented before the transmission. It should have a value of 256-2346 bytes, with a default of **2346**. If you experience a high packet error rate, you should slightly decrease the Fragmentation Threshold.

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

Ack TimeOut (11a)/ (11g)/: The "ACK time-out" determines how long the program waits after receiving a packet from a file stream to determine that stream to be a complete file. For details, please go to Section 3.9.

3.8 WISP Router Mode Settings

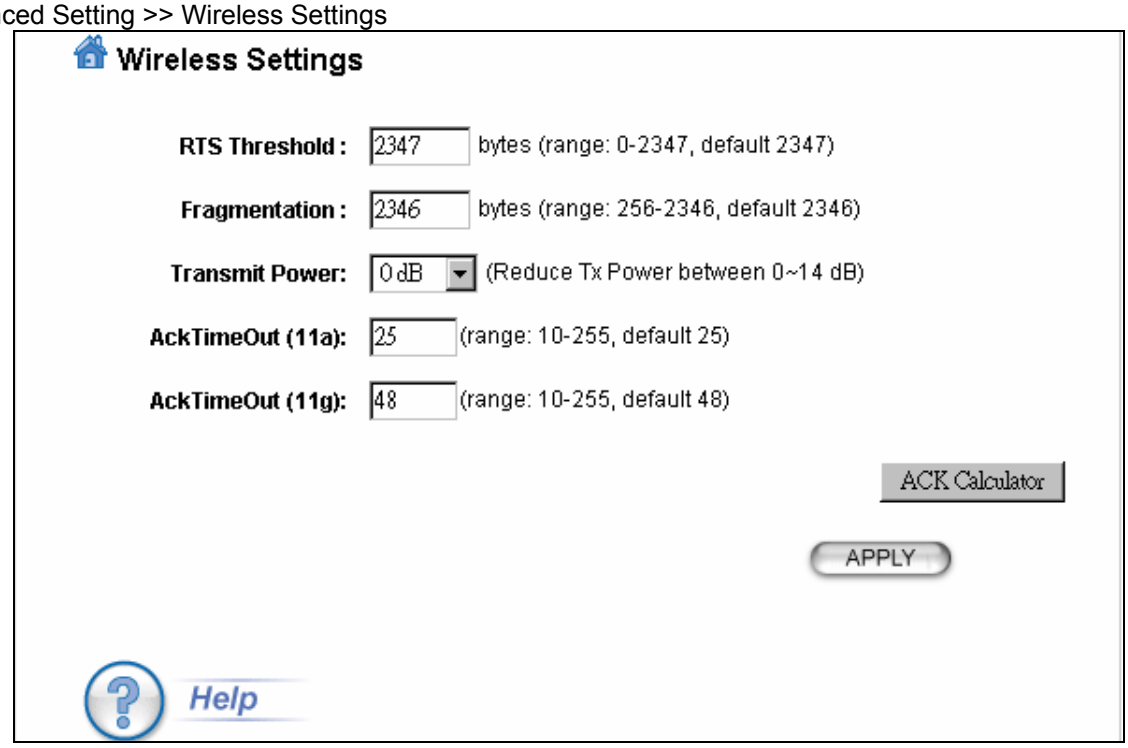
Advanced Setting >> Operation Mode >> WISP Router



Select “WISP Router” mode and then click APPLY button.

3.8.1 Wireless Settings

Advanced Setting >> Wireless Settings



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

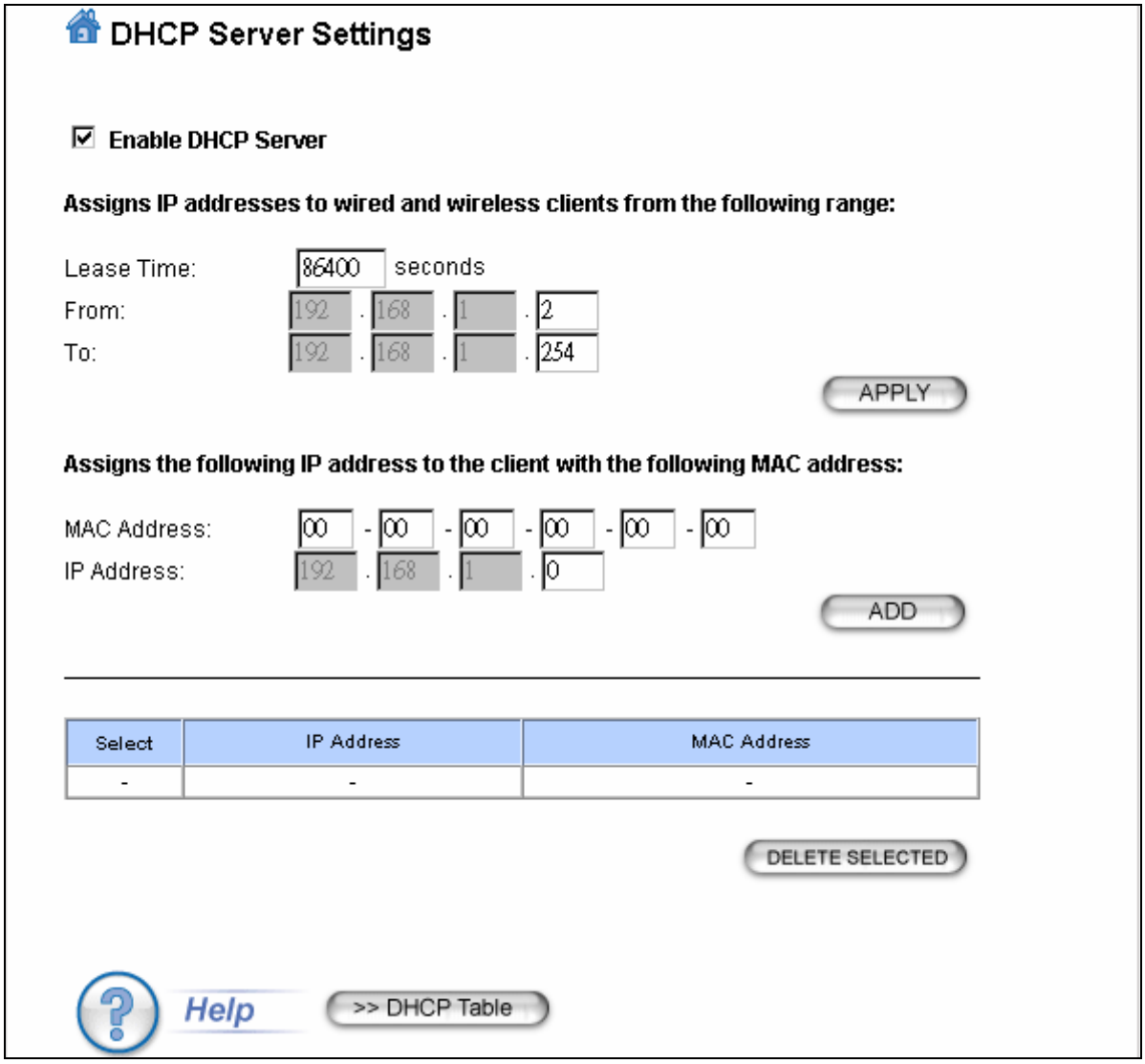
Fragmentation: When the size of a unicast frame exceeds the fragmentation threshold, it will be fragmented before the transmission. It should have a value of 256-2346 bytes, with a default of **2346**. If you experience a high packet error rate, you should slightly decrease the Fragmentation Threshold.

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

Ack TimeOut (11a)/ (11g)/: The "ACK time-out" determines how long the program waits after receiving a packet from a file stream to determine that stream to be a complete file. For details, please go to Section 3.9.

3.8.2 WISP Router DHCP Server Settings

Advanced Setting >> DHCP server Setting



DHCP stands for Dynamic Host Configuration Protocol. The DHCP server dynamically assigns IP addresses (from a pre-defined list) to clients when they log on. The client will request a new IP when the specific period of time is about to run out. If it expires, the address is returned to the pool of IP addresses.

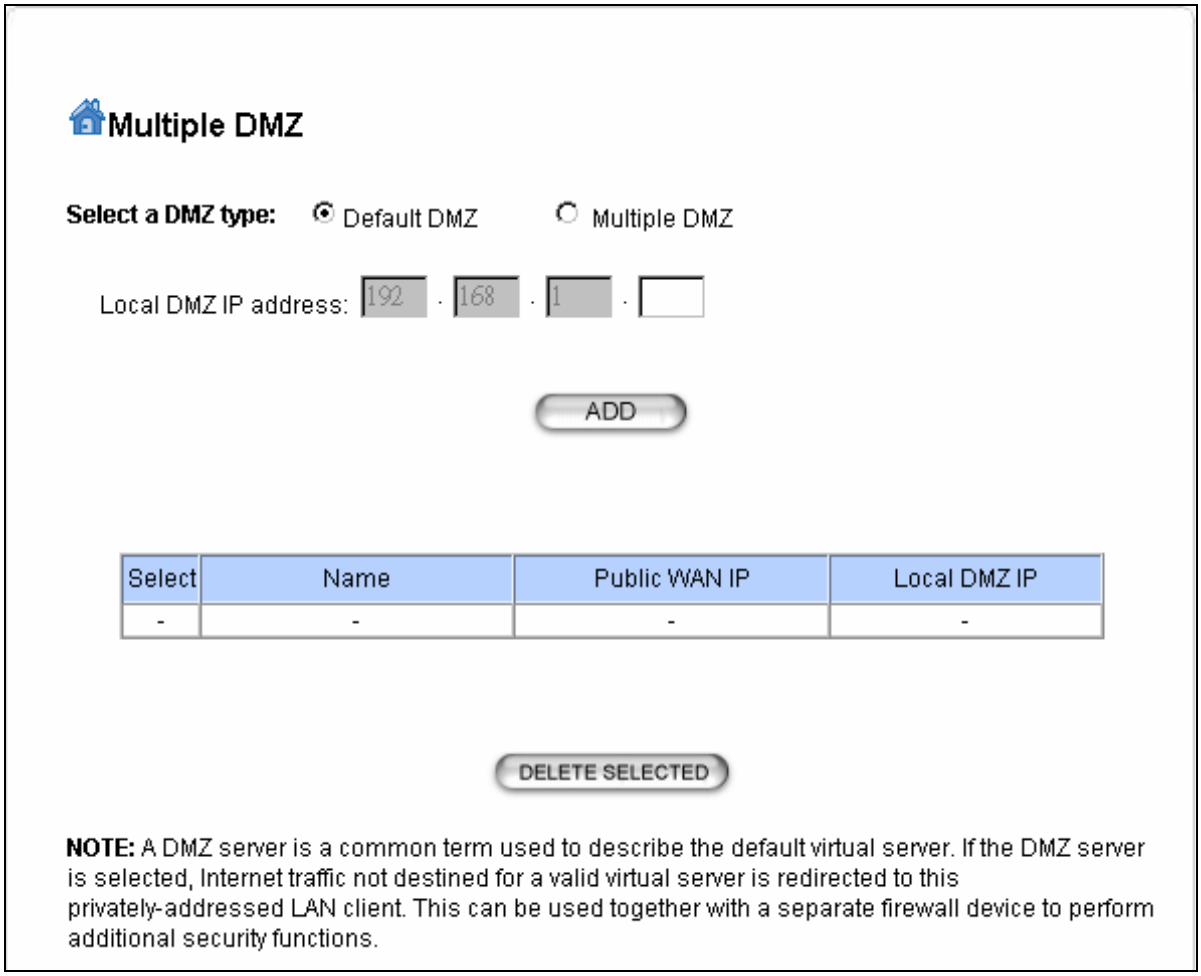
Under WISP mode, select the check box of “Enable DHCP Server” to enable DHCP server function.

The range of Clients’ IP addresses is from 192.168.1.2 to 192.168.1.254.

You can assign an IP address to a specified MAC address.

3.8.3 Multiple DMZ

Advanced Settings >> Multiple DMZ

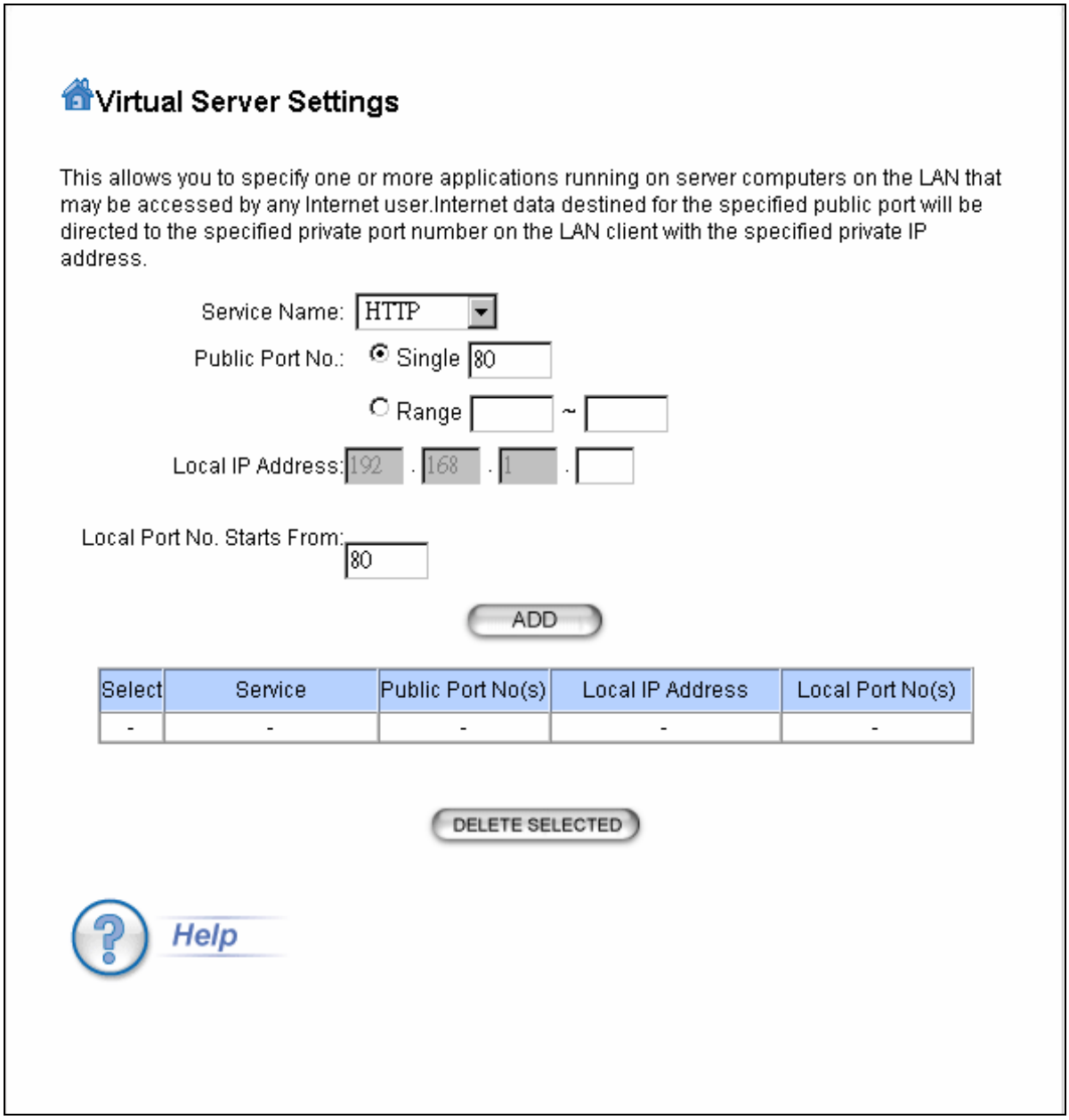


Select a DMZ type and then enter the local DMZ IP address.

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

3.8.4 Virtual Server Settings

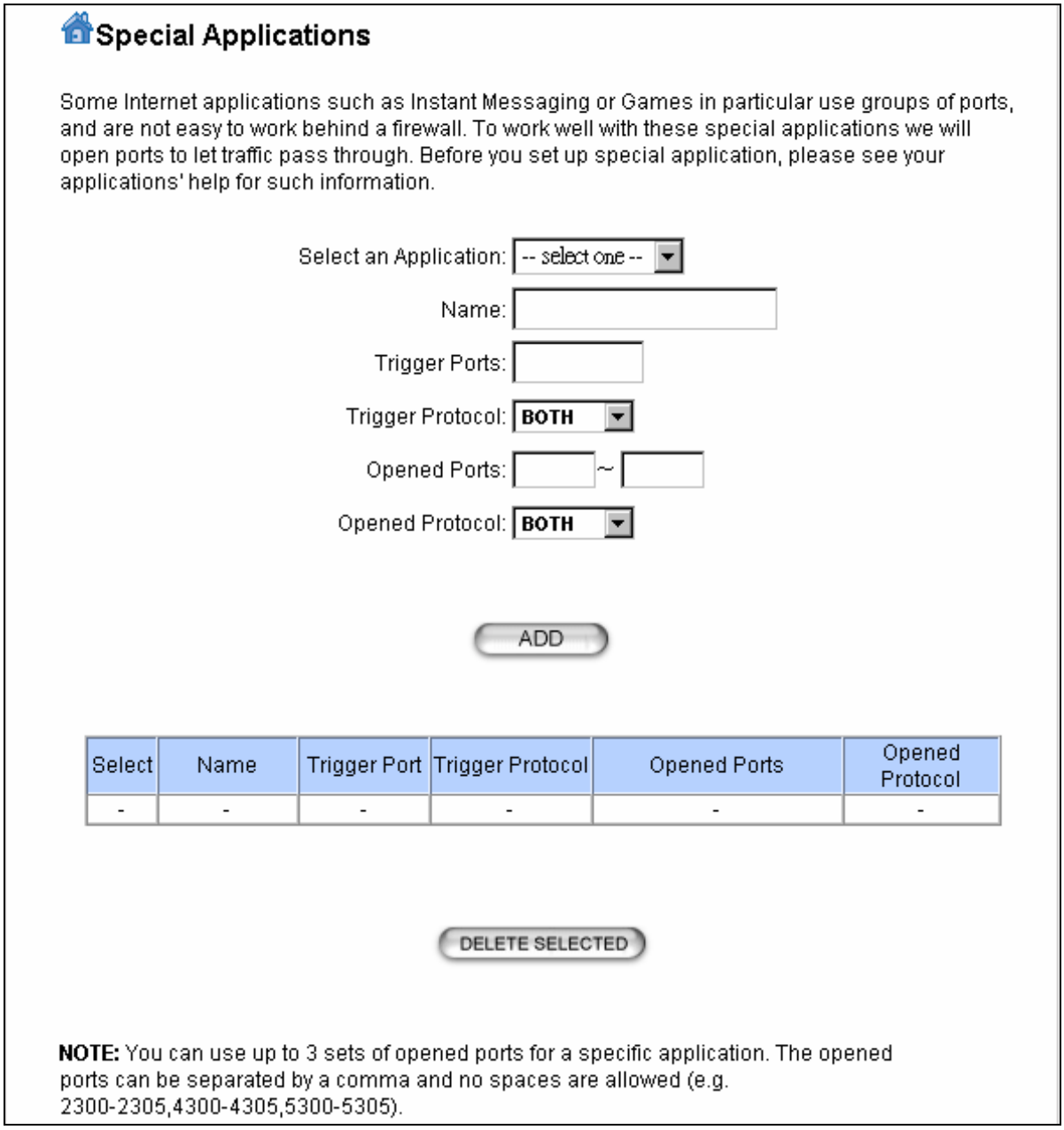
Advanced Settings >> Virtual Setting



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

3.8.5 Special Applications

Advanced Setting >> Special Applications

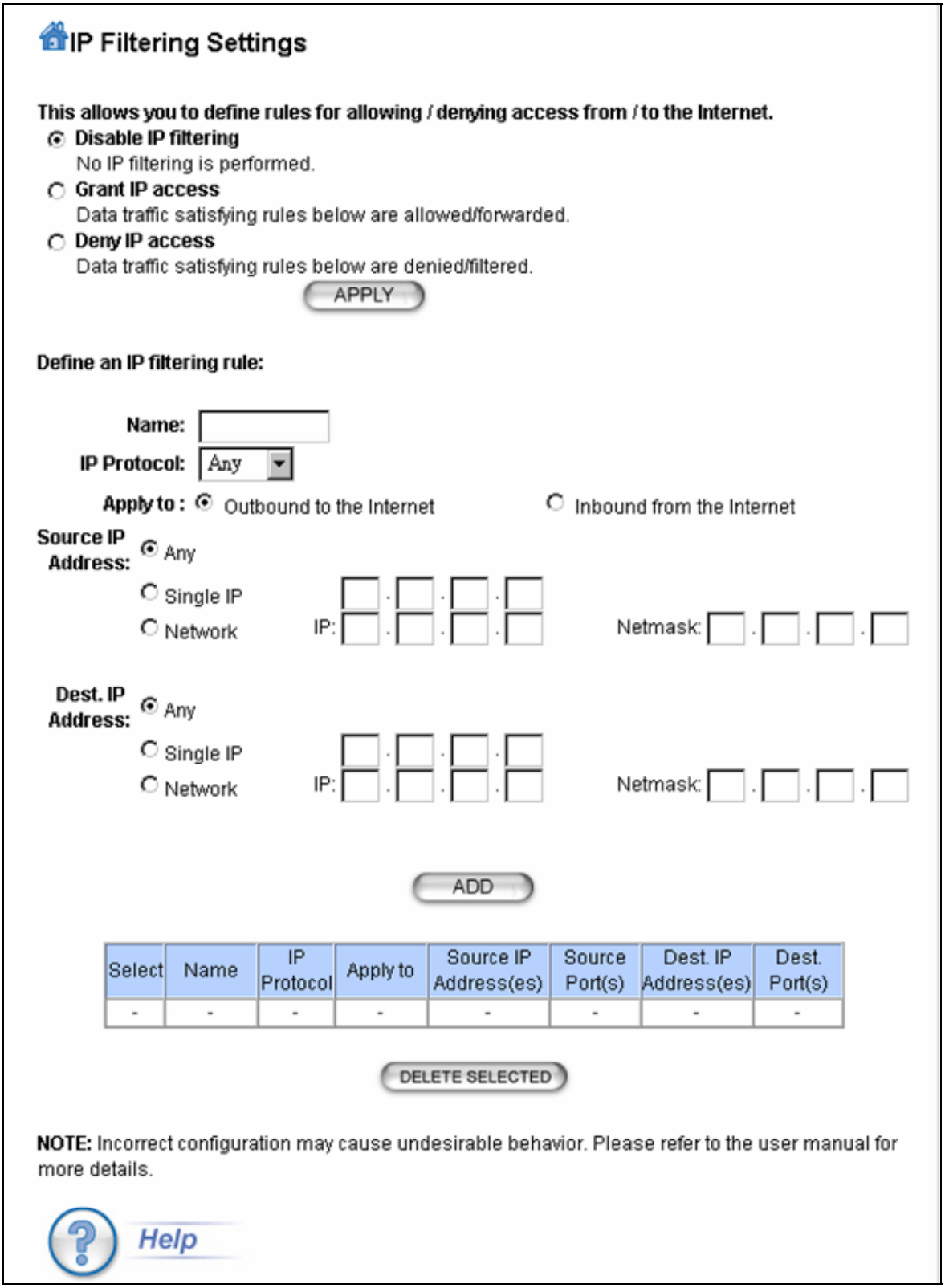


Some Internet application such as Instant Messaging or Games in particular use groups of ports, and are not easy to work behind a firewall. To work well with these special applications we will open ports to let traffic pass through.

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

3.8.6 IP Filtering Settings

Advanced Setting>>IP Filtering Settings
IP filtering is simply a mechanism that decides which types of IP datagrams will be processed normally and which will be discarded.



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

Disable IP filtering: No IP filtering is performed.

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

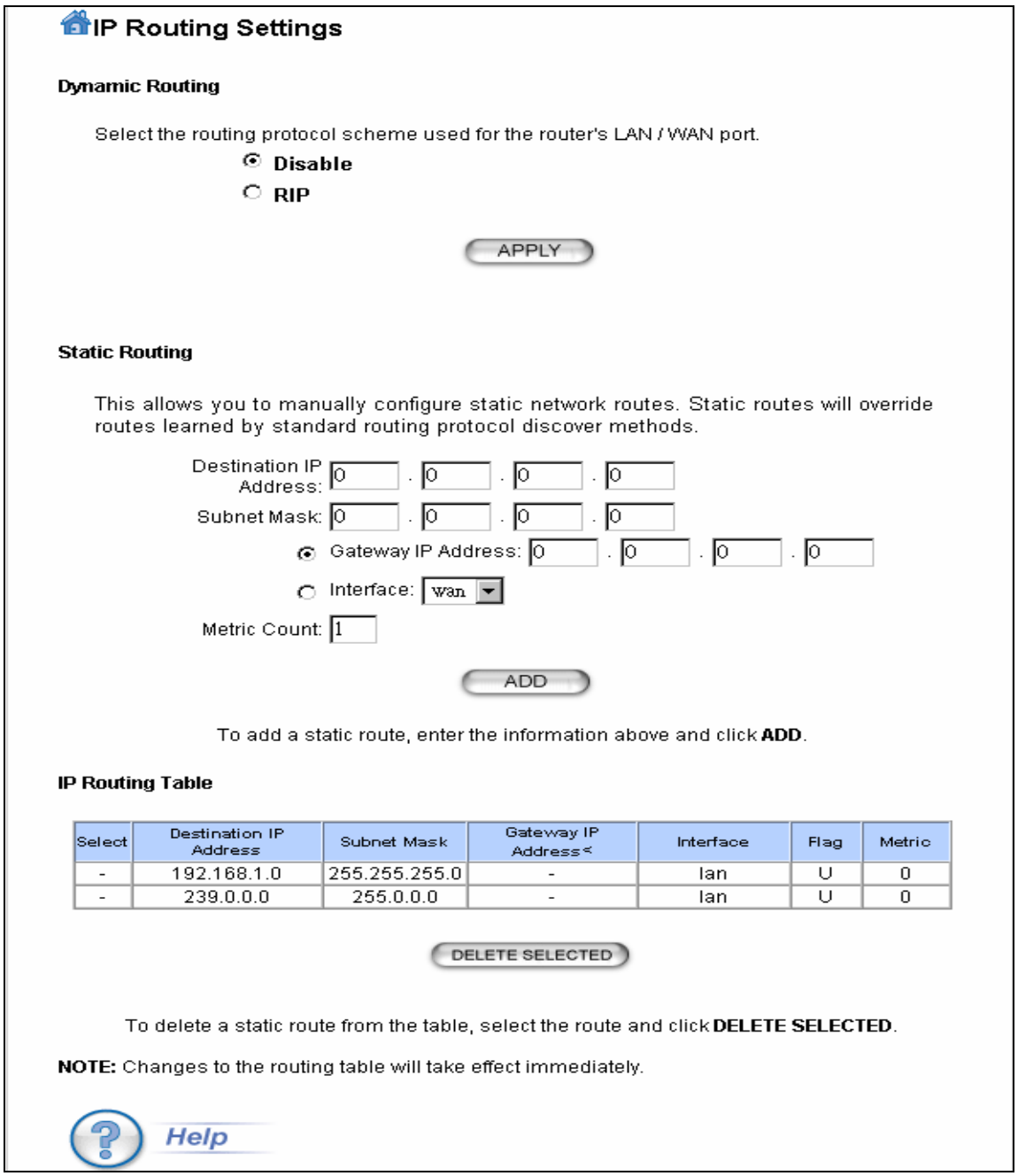
Deny IP access: Data traffic satisfying rules below are denied/filtered.

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

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

3.8.7 IP Routing Settings

Advanced Setting >> IP Routing Settings



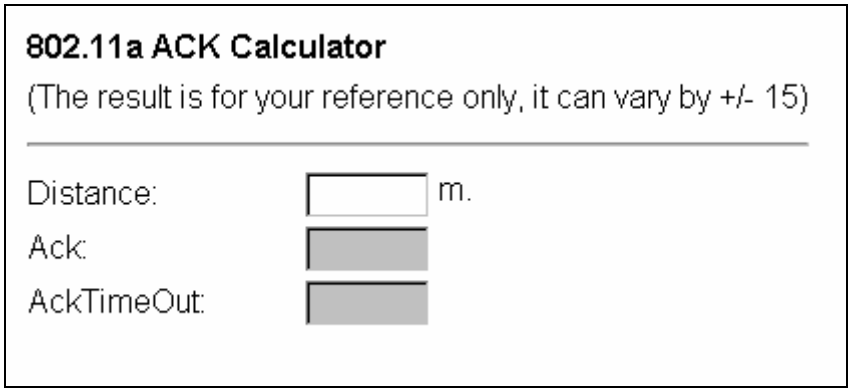
Dynamic Routing:
Select the routing protocol scheme used for the router's LAN / WAN port.
Static Routing:
This allows you to manually configure static network routes. Static routes will override routes learned by standard routing protocol discover methods.

IP Routing Table:
To delete a static route from the table, select the route and click DELETE SELECTED.

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

3.9 ACK Timeout Setup

Ack TimeOut (11a)/ (11g)/: The "ACK time-out" determines how long the program waits after receiving a packet from a file stream to determine that stream to be a complete file. WLA-5000AP v3 provides a calculator on UI that helps you to obtain this value only by giving the distance. Click the “ACK Timeout” button, and the following dialog box will appear:



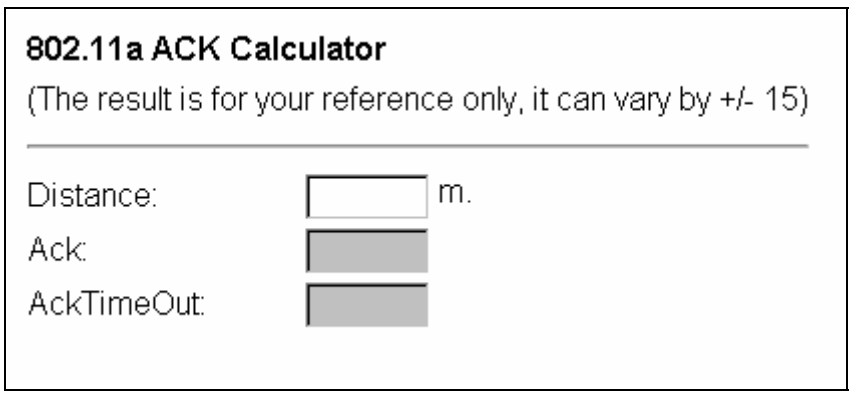
Input distance value in meters. The ACK Timeout value will be automatically calculated accordingly. This is the value to be entered into the “ACK Timeout (11a)” or “ACK Timeout (11g)” field according to the spectrum

.

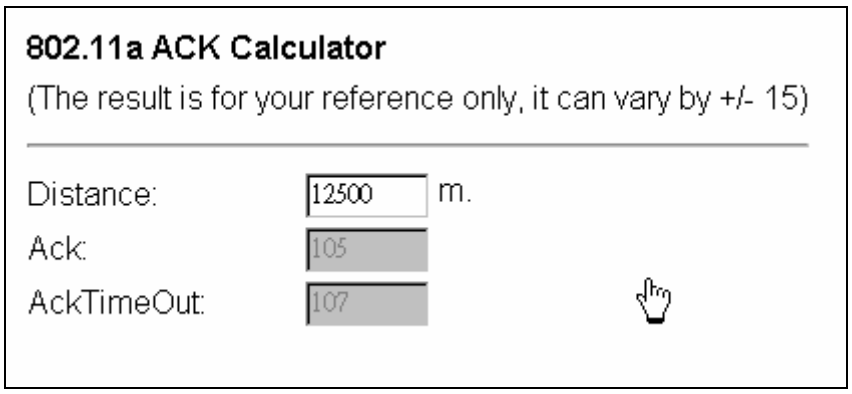
ACK Calculator

Advanced setting >> wireless settings

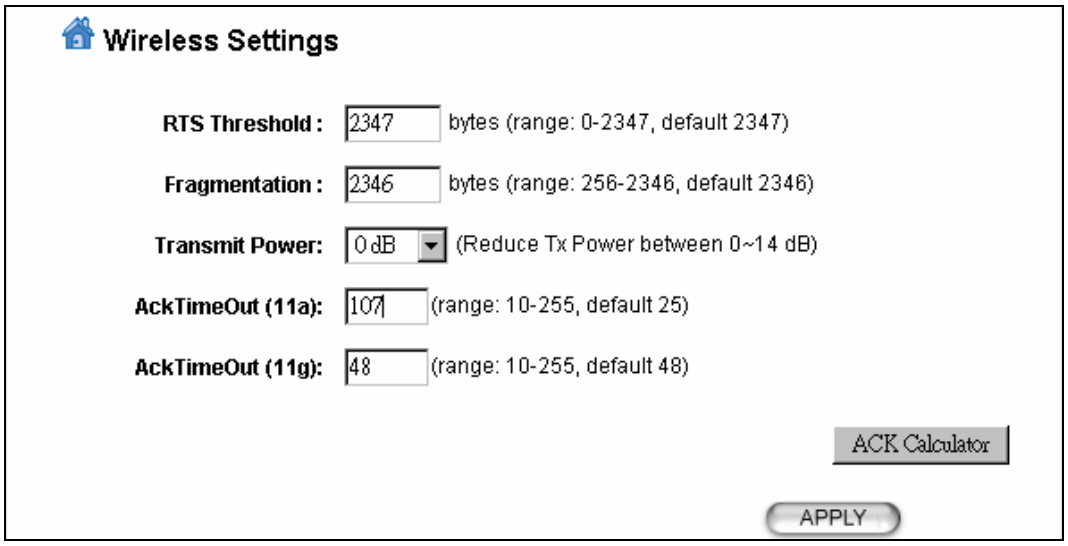
Click on the “ACK Calculator”  at the right down side of this page.



In the field of “Distance”, input the distance in “meters”.
After input the distance value, move the cursor to any place on the pop-up window out of three fields. The calculated value will display.



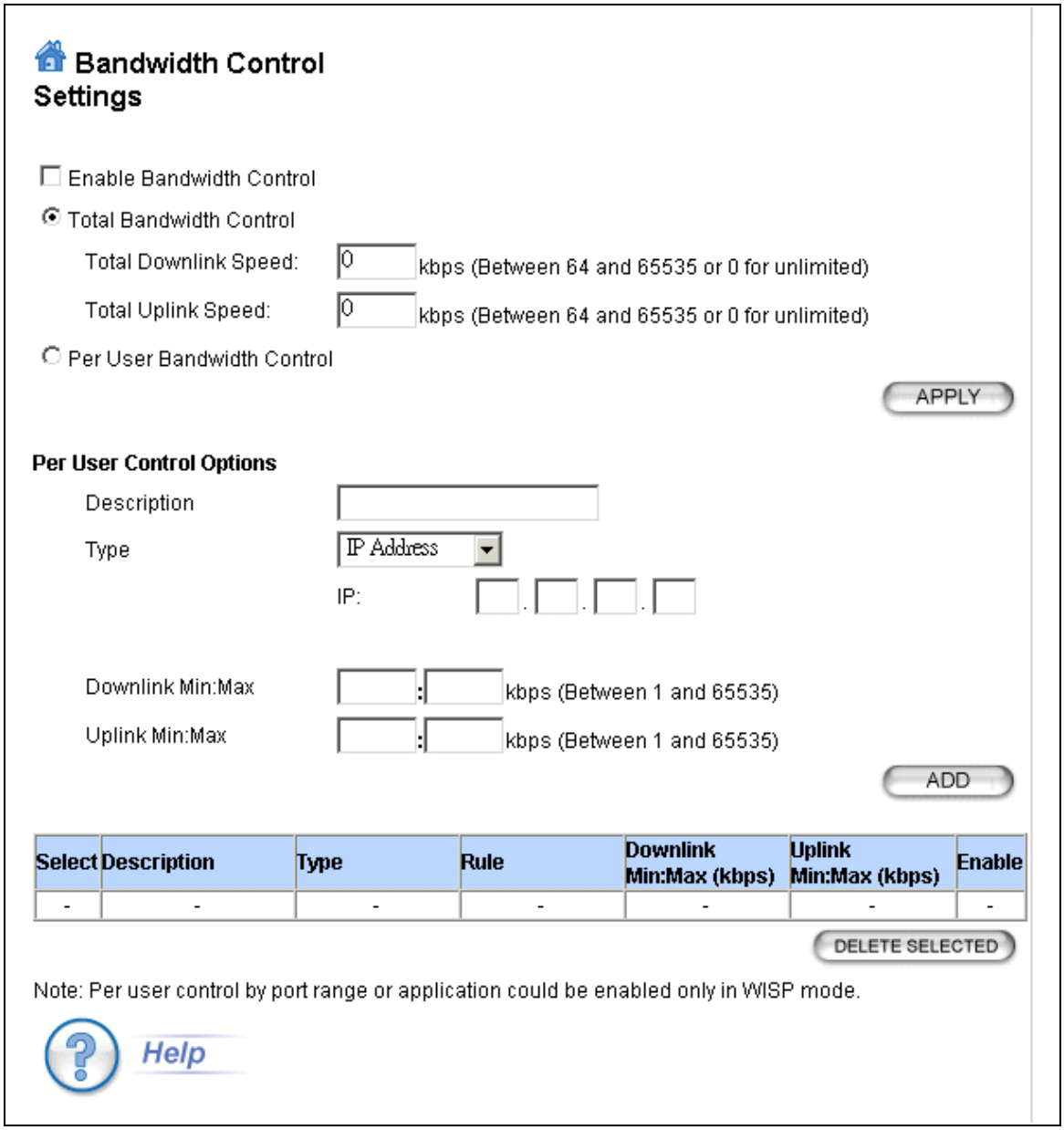
Enter the calculated value of “AckTimeOut” into the appropriate “Ack TimeOut” field (11a or 11g) in the “Wireless Settings” window.



3.10 Bandwidth Control

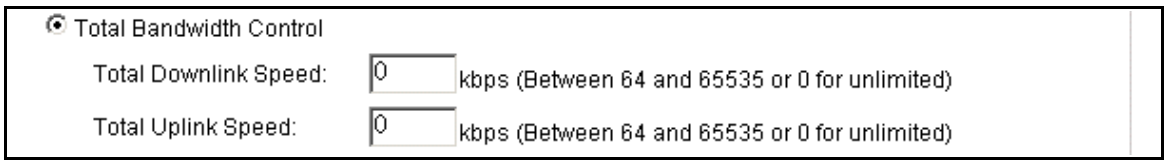
Bandwidth Control is a great tool to control the bandwidth of the WISP subscribers. Therefore, the WISP operators can offer different class of connection speeds for different subscription fees - just like the ADSL service! The AirLive advance firmware can control the bandwidth by Interface or IP/MAC.

There are 2 types of Traffic Control it offers: Total bandwidth control and Per-use bandwidth control.



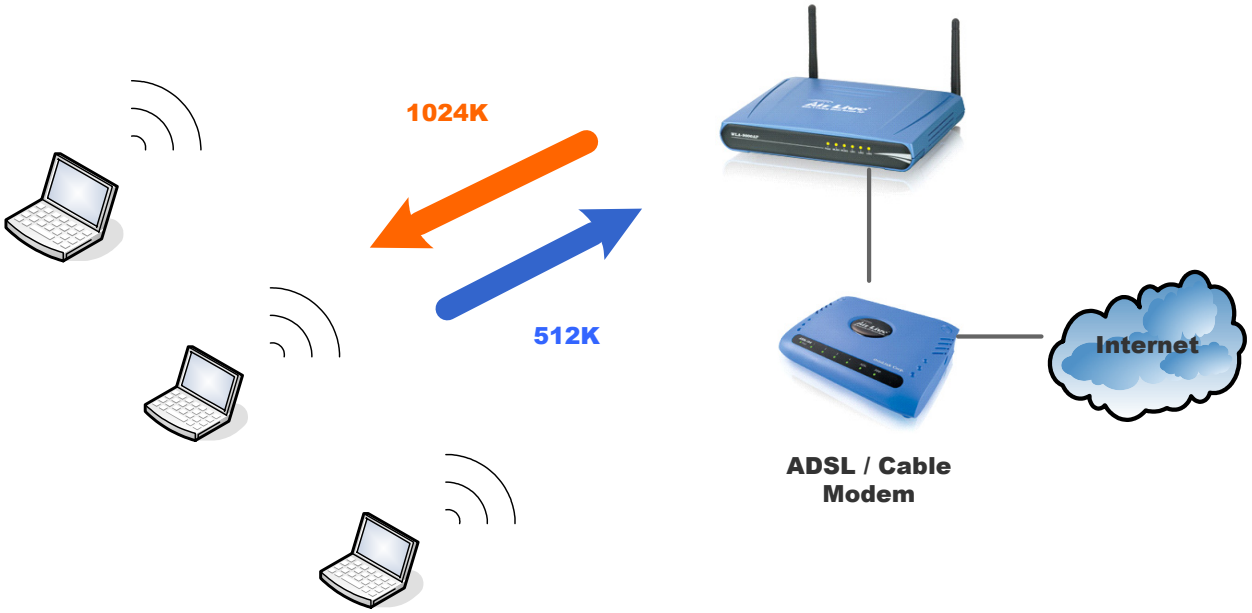
3.10.1 Total Bandwidth Control

The total bandwidth controls the data rate at either Wired or Wireless interface.



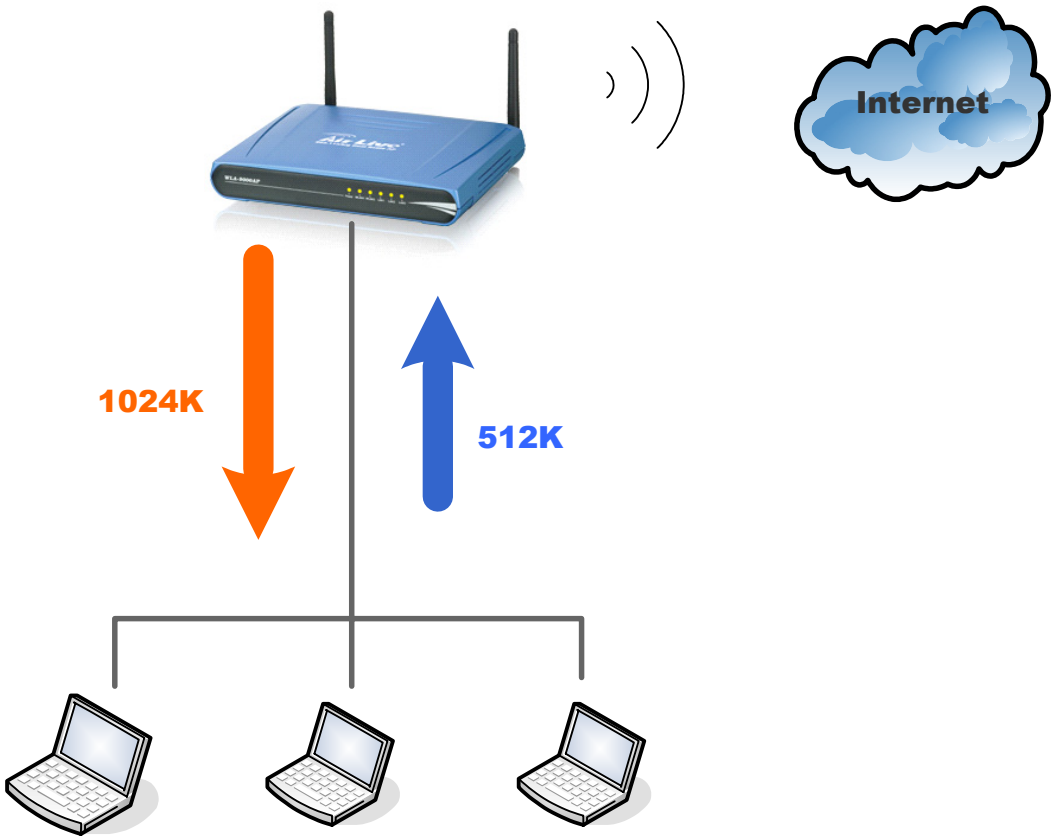
The following example limit the download bandwidth to **1024kbps** and uplink to **512kbps**

Example1: 3 wireless clients share downlink and uplink bandwidth.



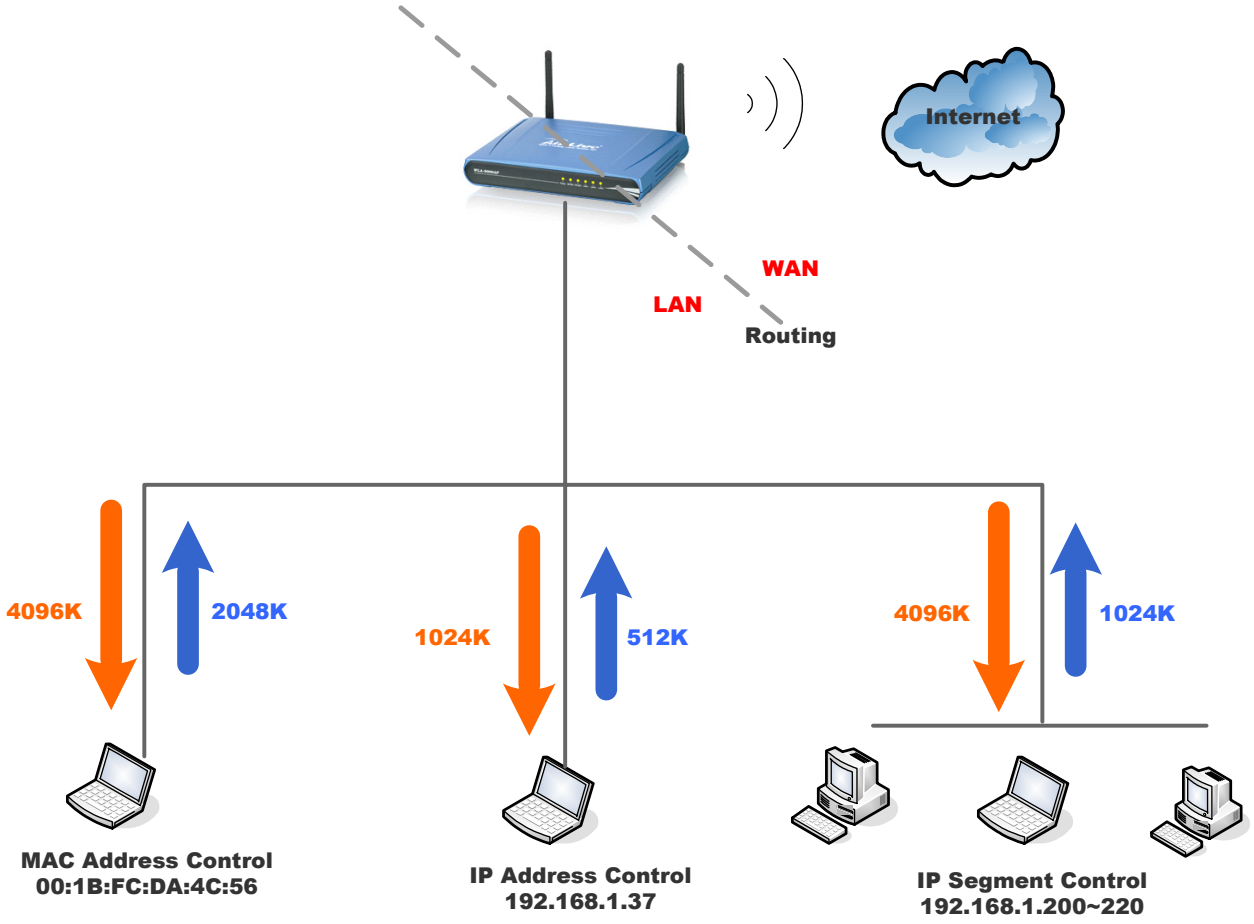
In this example, total uplink bandwidth of the 3 clients is limited to 512kbps and the total download bandwidth of the 3 clients is limited to 1024kbps.

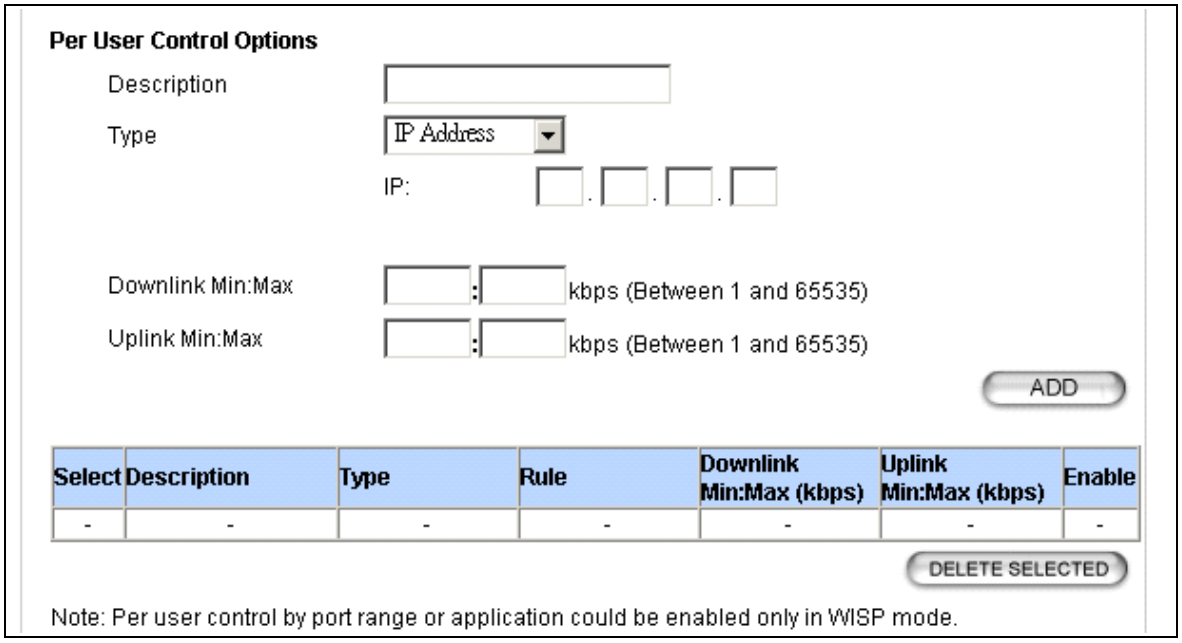
Example2:
3 wired clients share downlink and uplink bandwidth.



In this example, total uplink bandwidth of the 3 clients is limited to 512kbps and the total download bandwidth of the 3 clients is limited to 1024kbps.

3.10.2 Per user Bandwidth Control

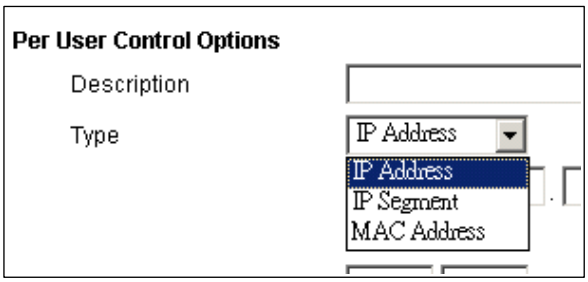




Note that this option could be enabled in WISP mode.

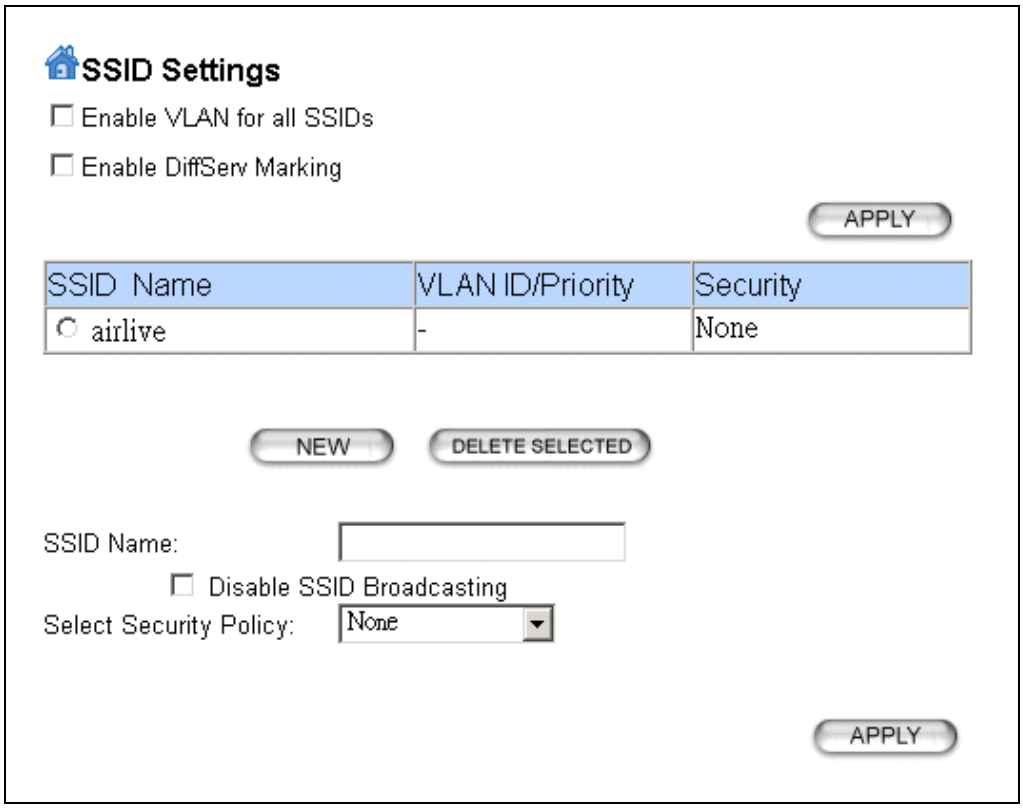
Description: You can preset your control type and named on the type.

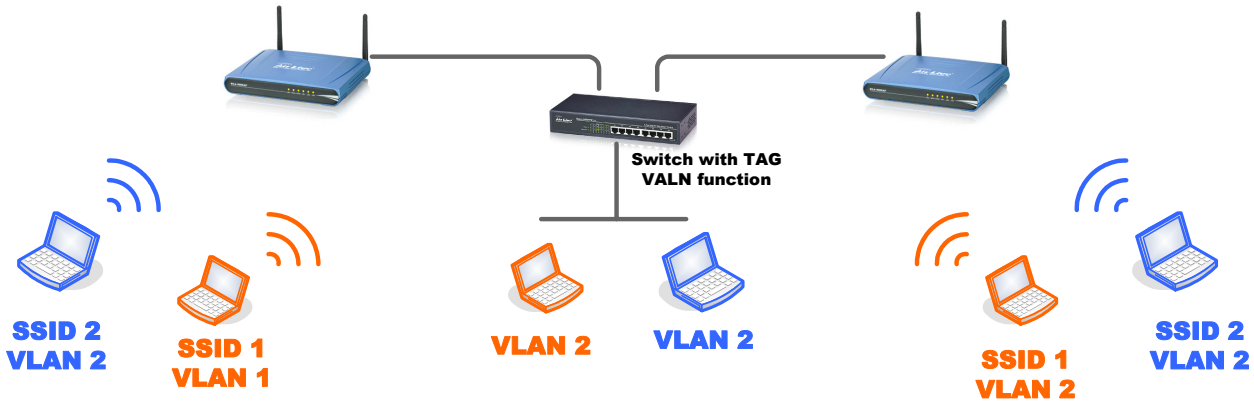
Type: Three types to be selected: IP Address, IP Segment and MAC Address. IP Segment allows you to set bandwidth limitation on an IP range.



3.11 Multiple SSID + VLAN

You can configure up to 4 SSIDs on your access point and assign different configuration settings to each SSID. All the SSIDs are active at the same time; that is, client devices can associate to the access point using any of the SSIDs. You can also assign VALN on each SSID to separate clients.
Note that the VLAN accept only tagged packet only.





In the above example, laptops in VALN 1 can only communicate with those in VLAN 1 and laptops in VALN 2 can only communicate with those in VLAN 2.

4 Manage the WLA-5000AP v3

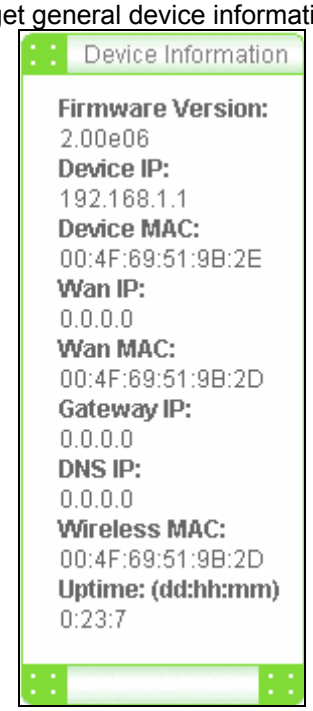
This Chapter covers other management aspects of your WLA-5000AP v3:

- Check Device Information
- View System Log
- Wireless Client Table
- Radio Table
- Site Survey
- Upgrade Firmware
- Save or Restore Configuration Changes
- Reset to Factory Default
- Reboot AP
- What if you forgot the password?

4.1 Device Status

Device status >> Device Information

You can monitor the system status and get general device information from the **Device Information** screen:



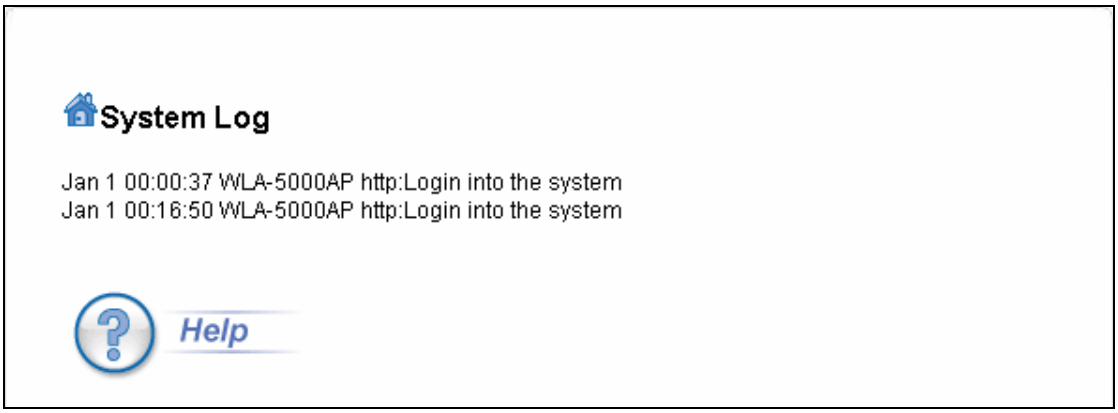
This is at the left-bottom corner of the **Device Status** window.

4.2 System Log

Device Status >> System Log

The WLA-5000AP v3 maintains a system log that you can use to track events that have occurred in the system. Such event messages can sometimes be helpful in determining the cause of a problem that you may have encountered.

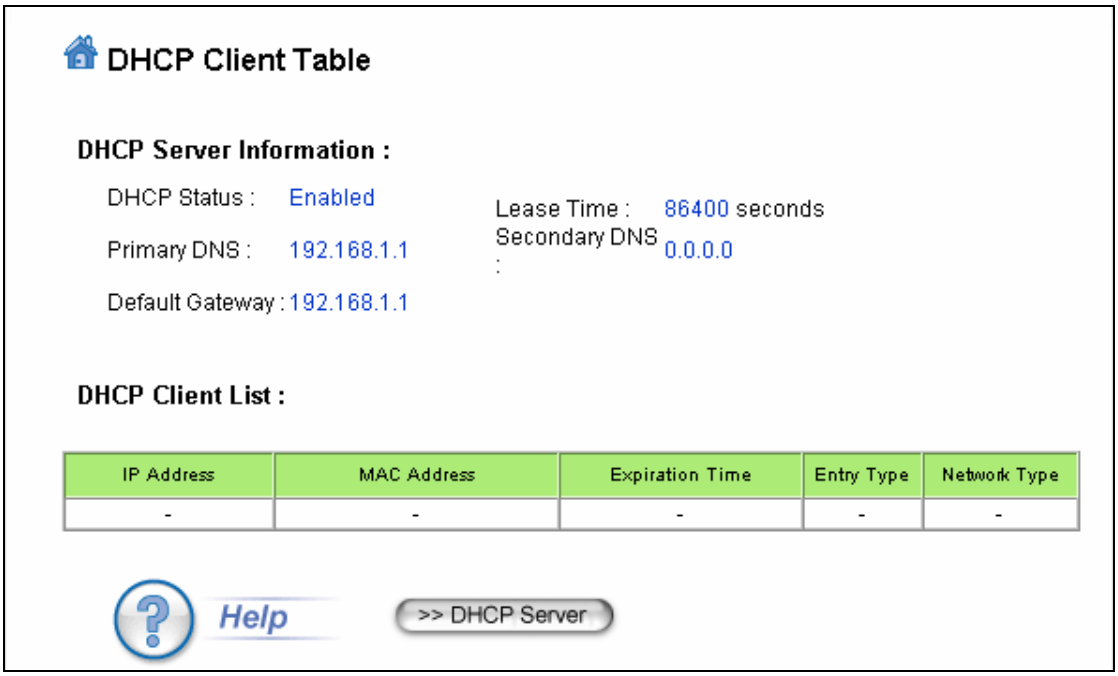
You can select **System Log** on the left side of the **Device Status** window to view log events recorded in the system. The System Log entries are shown in the main screen along with the log level, the severity level of messages that are being displayed (lower is severer), and the uptime, which is the amount of time since the WLA-5000AP v3 was boot-up.



4.3 Wireless Client Table

Device Status >> Wireless Client Table

The wireless client table lists the current wireless clients and its MAC address, state, and traffic statistics. You can check this table by clicking **Wireless Client Table** at the left side of the **Device Status** window.

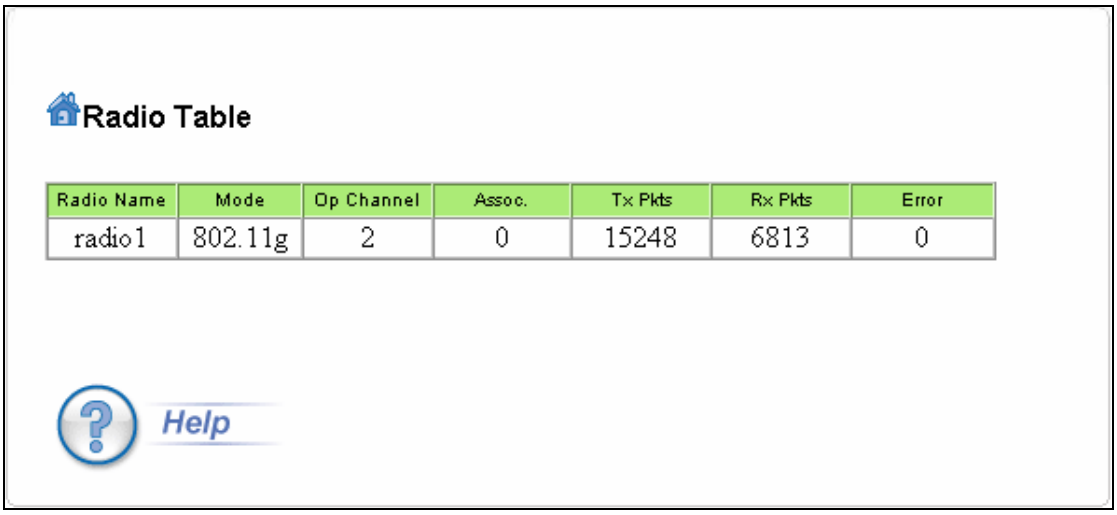


4.4 Radio Table

Device Status >> Radio Table

The Radio Table indicates wireless radio counters' data under one of the six operational modes: Access Point; WDS Repeater; WDS Bridge; Client Infrastructure, Client Adhoc and WISP Router.

Radio Table will indicate the following information: Radio Name, Mode, Op Channel, Assoc. Tx Pkts, Rx Pkts and Error.



4.5 Site Survey

Device Status >> Site Survey

The Site Survey table shows the wireless Access Point and Ad Hoc stations in your environment detected by the 802.11 A/G Access Point. You can click the **REFRESH** button to get latest environment information.

Site Survey list will indicate the following information:
ESSID, MAC Address, Conn Mode, Channel, Turbo, Super, XR, WME, Signal strength (%), Security and Network

The Site Survey table is available for only the following operation modes:

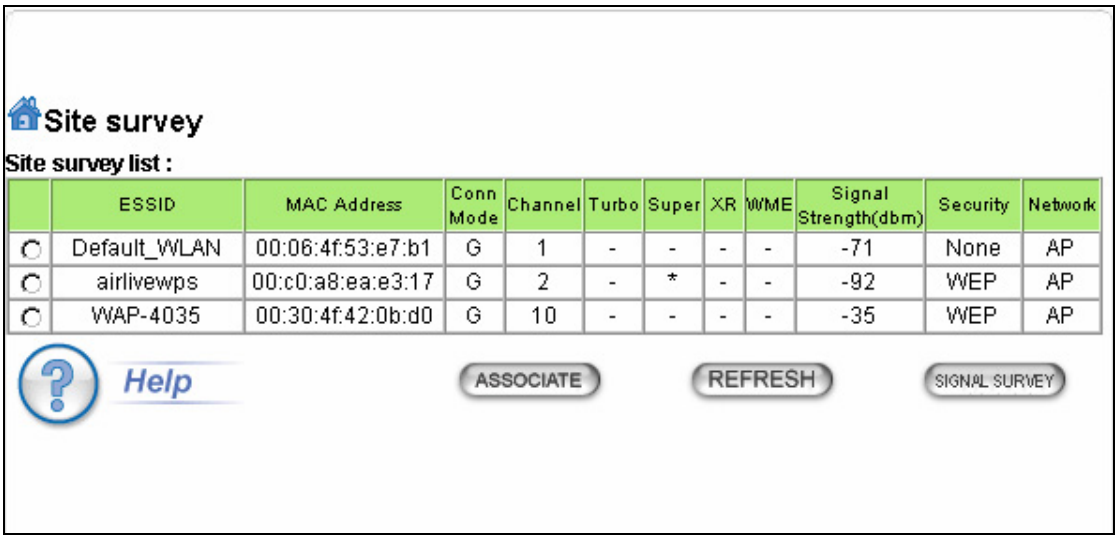
(1) Access Point

(2) WDS Repeater

(3) Client Infrastructure

(4) Client Adhoc

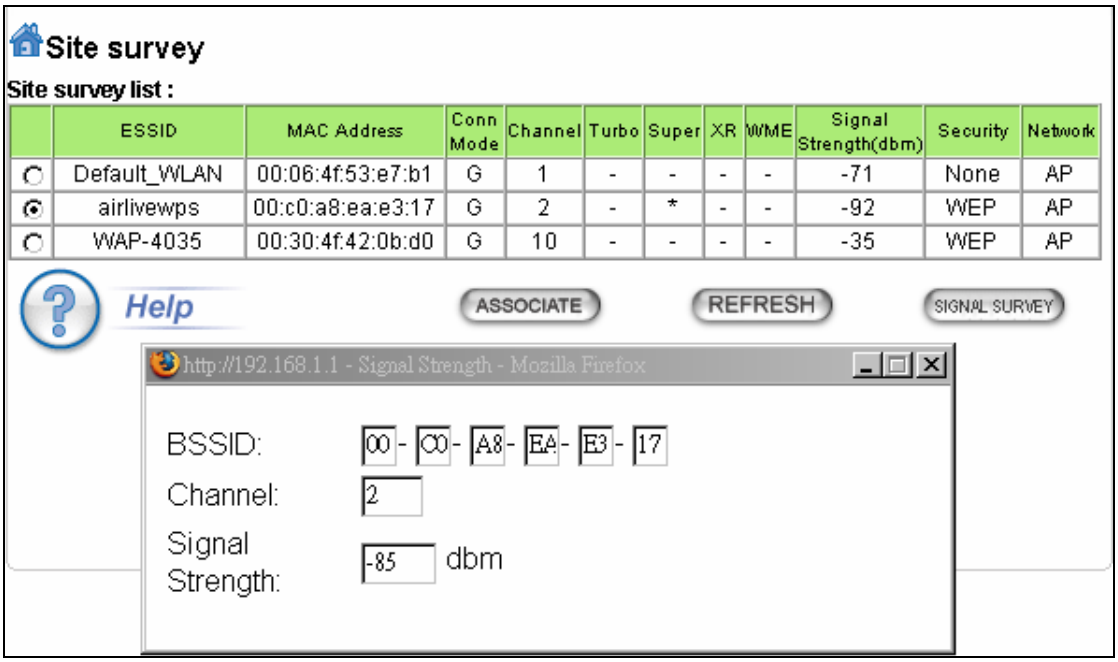
(5) WISP Router



4.5.1 Signal survey

Device Status >> Site Survey >> Signal Survey

This is a unique feature from AirLive. It provides real-time signal strength between two nodes. Better signal strength means better alignment results, which aims to improve link quality.
Click the “SIGNAL SURVEY” button. A pop-up window will continuously display signal strength in real time. The user can readjust the antenna position in order to achieve maximum signal strength.

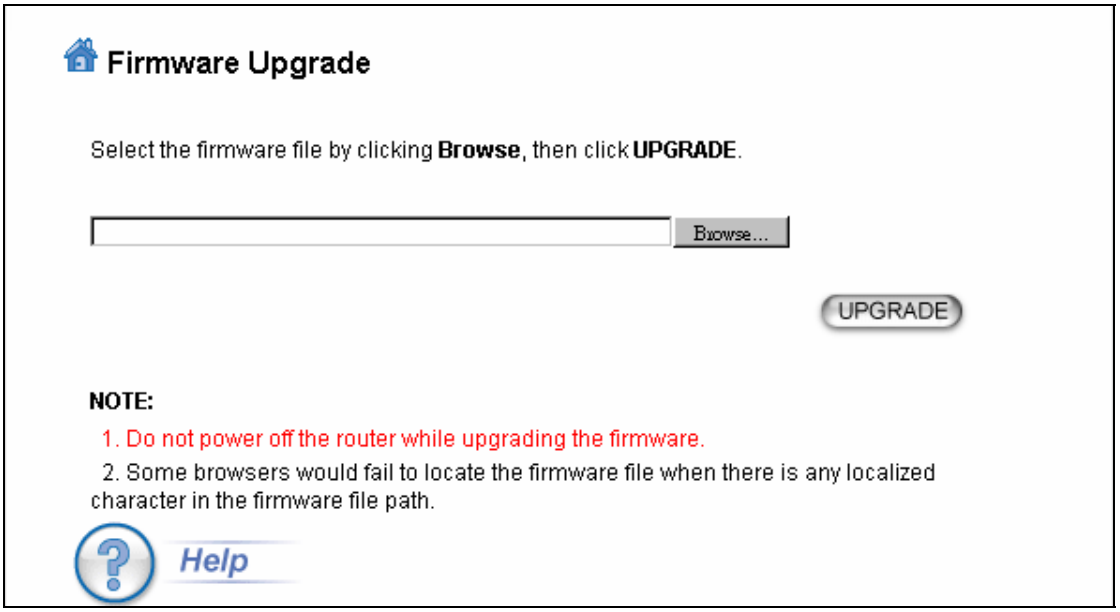


4.6 Firmware Upgrade

System tools >> Firmware Upgrade

You can upgrade the firmware of your WLA-5000AP v3 (the software that controls your WLA-5000AP v3's operation). Normally, this is done when a new version of firmware offers new features that you want, or solves problems that you have encountered with the current version. System upgrade can be performed through the System Upgrade window as follows:

Step 1 Select **System Tools,** then **Firmware Upgrade** from the menu.



Step 2 To update the WLA-5000AP v3 firmware, first download the firmware from the distributor's web site to your local disk, and then from the above screen enter the path and filename of the firmware file (or click **Browse** to locate the firmware file). Next, Click the **Upgrade** button to start.

The new firmware will be loaded to your WLA-5000AP v3. After a message appears telling you that the operation is completed, you need to reset the system to have the new firmware take effect.

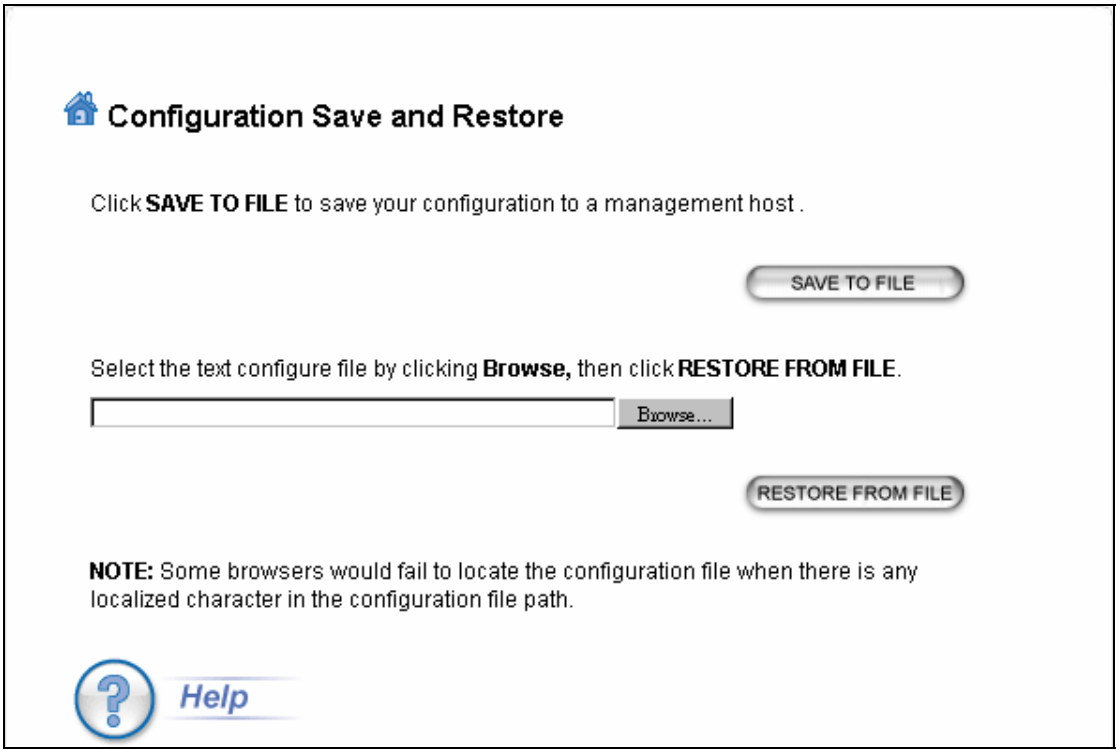
Do not power off the device while upgrading the firmware.
It is recommended that you do not upgrade your WLA-5000AP v3 unless the new firmware has new features you need or if it has a fix to a problem that you've encountered.

4.7 Configuration Save and Restore

System Tools >> Configuration Save and Restore

You can save system configuration settings to a file, and later download it back to the WLA-5000AP v3 by following the steps.

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



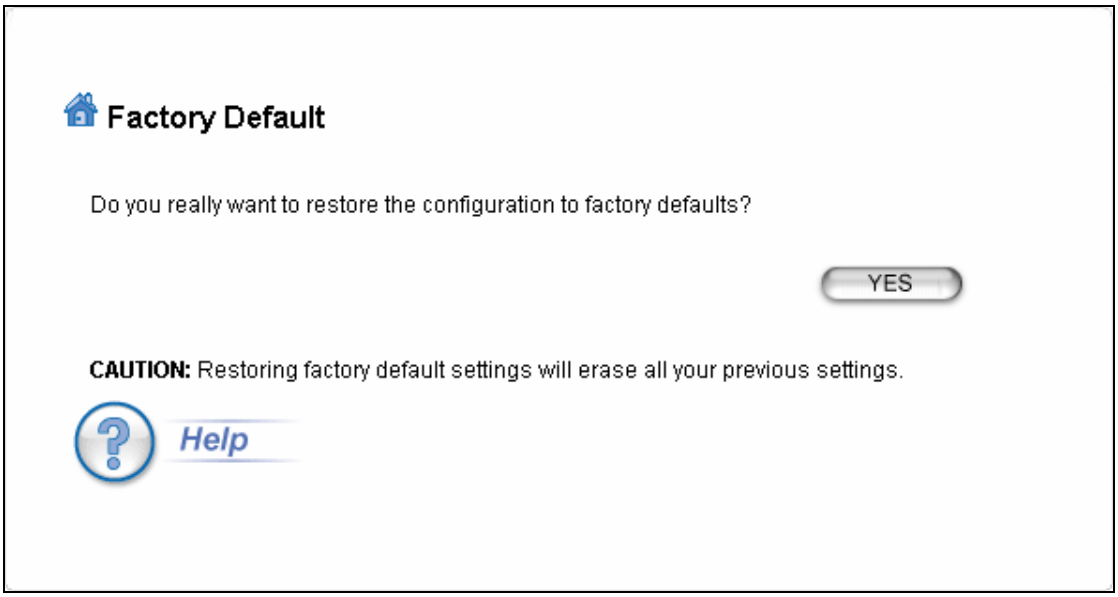
Step 2 Enter the path of the configuration file to save-to/restore-from (or click the **Browse** button to locate the configuration file). Then click the **SAVE TO FILE** button to save the current configuration into the specified file, or click the **RESTORE FROM FILE** button to restore the system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

4.8 Factory Default

System Tools >> Factory Default

You can reset the configuration of your WLA-5000AP v3 to the factory default settings. To do it:

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



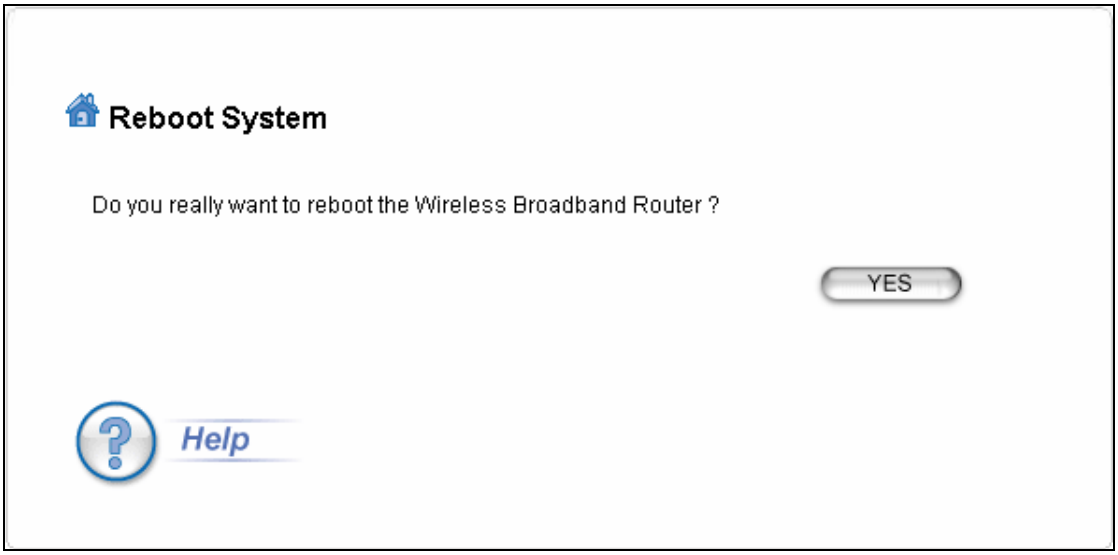
Step 2 Click **YES** to go ahead and restore the configuration to the factory default.

4.9 Reboot System

System tools>>Reboot System

You can reset your WLA-5000AP v3 from the Browser. To reset it:

Step 1 Select **Reboot System** from the **System Tools** menu.



Step 2 Click **YES** to reboot the WLA-5000AP v3.

Rebooting the WLA-5000AP v3 would disconnect any active clients and therefore will disrupt any current data traffic.

4.10 What if you forgot the password?

Hardware Reset To Factory Defaults
If you forgot the password, the only way to recover is to clear the device configuration and return the unit to its original state as shipped from the factory.

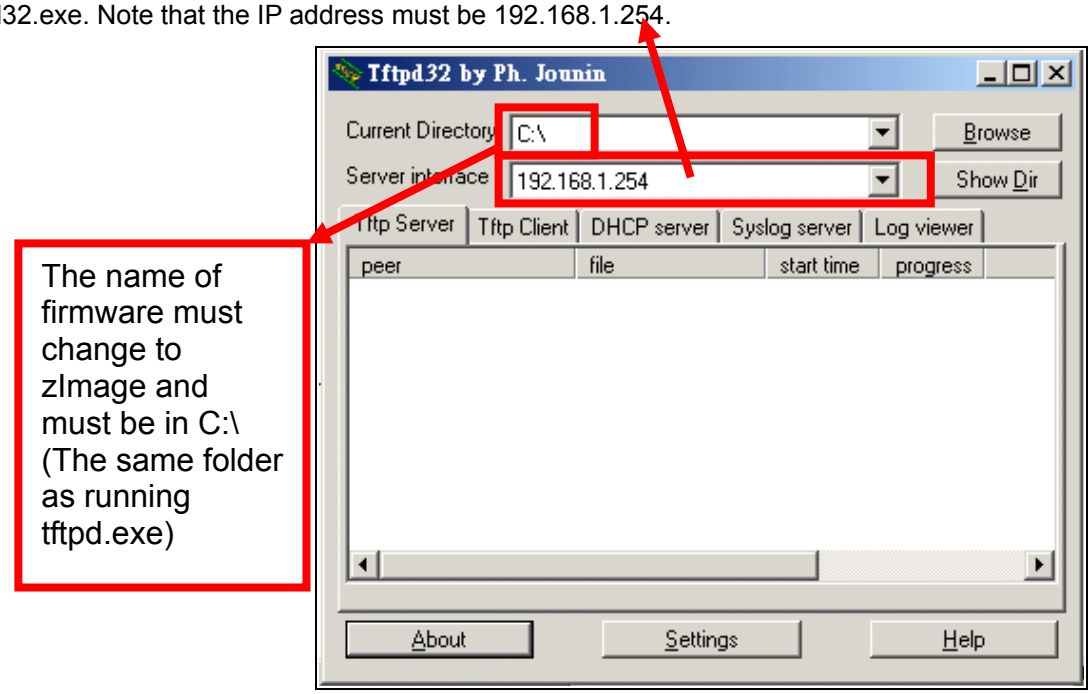
You can reset the Access Point's Settings to factory defaults by pushing a paperclip in the RESET hole on the back panel. Push and hold for around 2 seconds until the lights at the front of the Access Point are off. Doing so will clear your current configuration.

4.11 Emergency Recovery

This section guides to recover your WLA-5000AP system if the firmware crashed.

1. Download the tftp server to your PC. In the following example, we use tftpd32: http://tftpd32.jounin.net/tftpd32_download.html.
2. Copy the tftpd32.exe of the downloaded file to C:\.
3. Change the IP address of your PC to 192.168.1.254 / 255.255.255.0
4. Copy the WLA-5000AP firmware to C:\ and rename the firmware to **"zImage"**. Note that the name must be zImage and no extension.
5. Connect WLA-5000AP and PC with an Ethernet cable.
6.

7. Run the tftpd32.exe. Note that the IP address must be 192.168.1.254.



8. Power on WLA-5000AP, the **"Status"** LED will light on after 3 seconds.
9. Push the **"Reset"** button until the **"Status"** LED off and on again and release the **"Reset"** button.
10. If the above process success, the WLA-5000AP LAN LED keep flashing and the tftp serve shows file download information.
11. It takes around 5 minutes to download firmware and around 5 minutes to update the firmware.
12. After a successful recovery, the WLA-5000AP boots up automatically.
13. Try access 192.168.1.1, or the IP address you had changed before.
14. Repeat the processes again if failed.

Specifications

Recommended Outdoor Antennas	WAE-5014PA : 5GHz 14dBi Antenna WAE-5018PA : 5GHz 18dBi Antenna WAE-5023PA : 5GHz 23dBi Antenna
Feature	Atheros SuperG and SuperA mode support for 108Mbps* AP, WDS Bridge, WDS Repeater, Client Mode, WISP mode Client mode firmware Primary and secondary RADIUS server support Web-based management tool WPA with Pre-Shared Key Support, TKIP, and AES Support 152-bit WEP support (Atheros Proprietary) 802.1d Spanning Tree Protocol SNMP v1, v2, v2c support Watchdog timer
Hardware	180Mhz R4000 CPU Wireless Chipset: Atheros AR2312+AR5112 1 x 10/100Mbps LAN Port 4MB Flash, 32MB SDRAM Reversed SMA Antenna Port Power, LAN, WLAN LED indicators
Antenna	2 dBi detachable Dipole Antenna Reversed SMA Connector
Frequency Range	802.11b/g - USA (FCC) 11 Channels - Europe (ETSI) 13 Channels - Japan (TELEC) 14 Channels 802.11a - USA: 12 Channels - Europe (ETSI) 19 Channels - Japan (TELEC) 4 Channels
Frequency Channel	802.11b/g - USA (FCC): 2.412GHz~2.462GHz - Europe (ETSI): 2.412GHz~2.472GHz - Japan (TELEC):2.412GHz~2.483GHz 802.11a - U-NII - 5.15 - 5.35 GHz - 5.725 - 5.825 GHz - ISM - 5.725 - 5.850 GHz - DSRC: 5.850 - 5.925GHz - Europe (ETSI) - 5.15 - 5.35 GHz - 5.47 - 5.725 GHz - Japan (TELEC) - 4.90 - 5.00 GHz - 5.03 - 5.091 GHz - 5.15 - 5.25 GHz

Modulation Technique	11a Orthogonal Frequency Division Multiplexing 11g Orthogonal Frequency Division Multiplexing (64QAM, 6QAM, 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	802.11b: 20dBm 802.11a: 17dBm 802.11g: 17dBm
Security	64/128/152-bit WEP management WPA Support MAC address Access Control
Management	Web Management UPnP (Basic Device) SNMP: v1, v2, v2c, Ether Like MIB, MIB II, 802.11MIB Watchdog Timer to WARM boot system
Configuration	Web Management AP/WDS firmware and client firmware. Firmware upgradable Hide ESSID 802.1x Primary and Secondary Radius MAC Access Control Syslog support 802.11d STP protocol Privacy Separator
Environmental	Operating temperature: 0~60℃ Operating humidity (non-condensing): 20~80% Storage temperature: -20~65℃ Storage humidity: 95% Max
Power Supply	DC5V / 2A
EMI	FCC, CE
Product Weight (g)	210 g
Product Size (L x W x H (mm))	160 x 115 x 30 mm