Air Live®
Powered by OvisLink Corp.

AP60

Wireless-N POE Access Point

User's Manual

Copyright & Disclaimer

This product contains some codes from GPL. In compliance with GPL agreement, AirLive will publish the GPL codes on our website. Please go to www.airlive.com and go to the "Support → GPL" menu to download source code.

FCC Statement

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

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation. For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.

This device and its antenna(s) must not be co-located or operation in conjunction with any other antenna or transmitter.

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.

Table of Contents

1 Introduction

1.1 Overview

The AP60 is a wireless multi-function router based on 150Mbps wireless-b/g/n 2.4GHz radio technologies. The Wireless Access Point is equipped with four 10/100 Mbps Auto-sensing Ethernet ports for connecting to LAN and also for cascading to next Wireless Access Point.

Passive PoE Port

You can supply power through Ethernet cable to AP60 using the passive PoE port. The AP60's passive PoE port can accept 12V to 24V power from a passive PoE switch (such as AirLive POE-FSH8PW) or a passive PoE DC Injector (AirLive POE-1P).

9 Wireless Modes

The AP60 has 9 different wireless operation modes. Therefore, it can perform different functions such as AP, Bridge, Client, Repeater, Router and more.

Long Distance Radio

The AP60 features a long distance and wide coverage radio. It has potential to provide greater coverage than ordinary AP/Router. However, the output power is set to comply with your country regulation. Please do not use more power than allowed in your country.

Versatile Management

The AP60 comes with a user friendly interface that can access through web browser. There is a setup wizard to help you setup quickly. The IP finder utility can help you to find your AP.

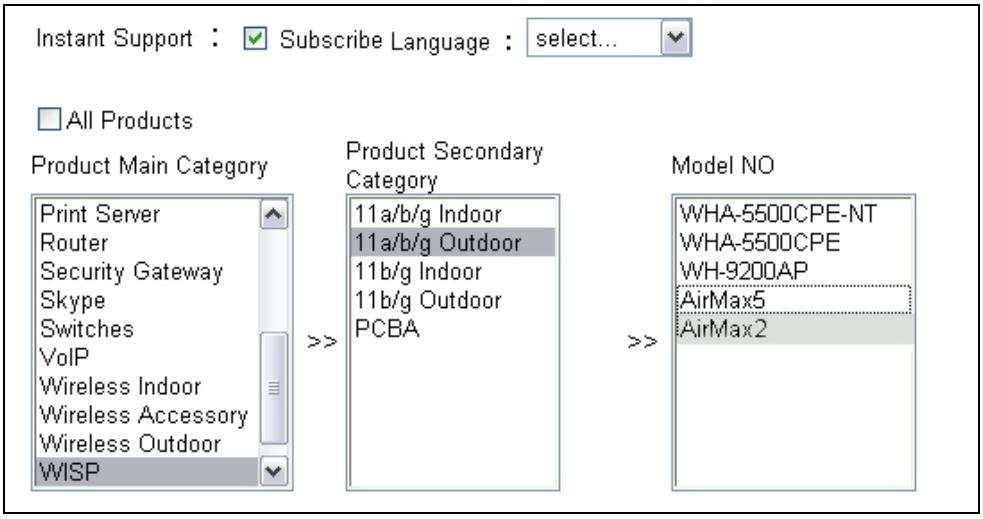
Whether it's for own, office, hotspot, or WISP environments, the AirLive Wireless-B/G/N AP Router family brings you the maximum performance and security for today's high speed wireless network.

1.2 Firmware Upgrade and Tech Support

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

In addition, you might find new firmware that either increase software functions or provide bug fixes for AP60. You can reach our on-line support center at the following link: http://www.airlive.com/support/support_2.jsp

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



AirLive Newsletter Suppport System

1.3 Features

- 150Mbps 802.11b/g/n Standard
- 4MB Flash and 32MB SDRAM
- 9 wireless multi-function modes: Access Point, Client Mode, WDS Repeater, WDS Bridge, Universal Repeater, WISP Router, AP Router, WISP+ Universal Repeater, WDS Station
- R-SMA connector antenna.
- Passive PoE Port for 12V~24V Passive POE System. Passive DC Injector not included.
- Site Survey, Signal Survey
- Emergency firmware recovery mode
- Web management
- Easy Setup Wizard
- Bandwidth Control, Access Control
- Multiple SSID and Virtual AP
- Client Isolation, Watchdog
- TX Output Power Adjustment
- Wireless Scheduling
- All LED Off function

- NAT, Static Router, RIP1, RIP2
- IP Finder Management Utility

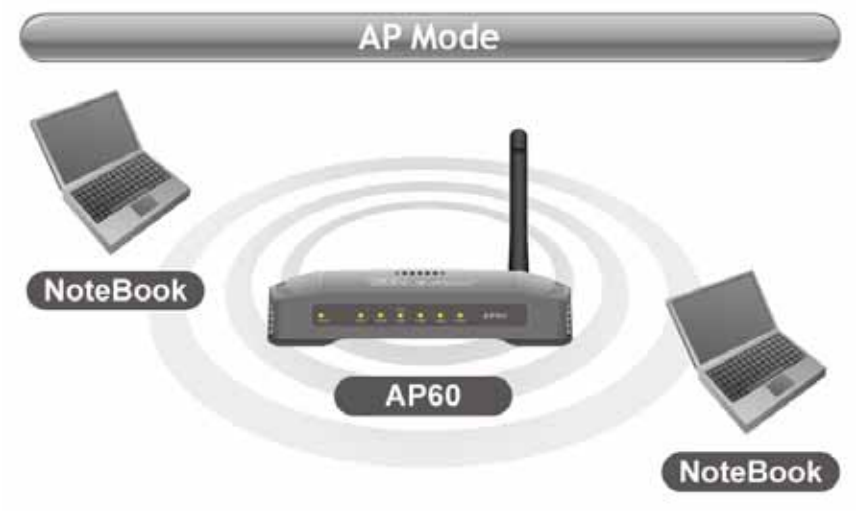
1.4 Wireless Operation Modes

The AP60 can perform as a Multi-Function wireless device. Through the AirLogic web interface, users can easily select which wireless mode they wish the AP60 to perform.

AP60 Wireless Operation Mode			
Wireless Mode	**Radio**	**WAN**	**Application**
Access Point	AP	None	Hotspot (Indoor and Outdoor)
Client	Client	None	WISP Client
Bridge	Bridge	None	Building to Building network
WDS Repeater	AP + Client	None	Extend distance of another WDS AP/Router
Universal Repeater	AP + Client	None	Extend distance of any AP Router
WISP Router	Client	Wireless	WISP Client Router
WISP + Repeater	AP + Client	Wireless	WISP 2-Way CPE (One radio only)
AP Router	AP	LAN Port	Broadband Sharing
WDS Station	Bridge	None	Bridge with SSID

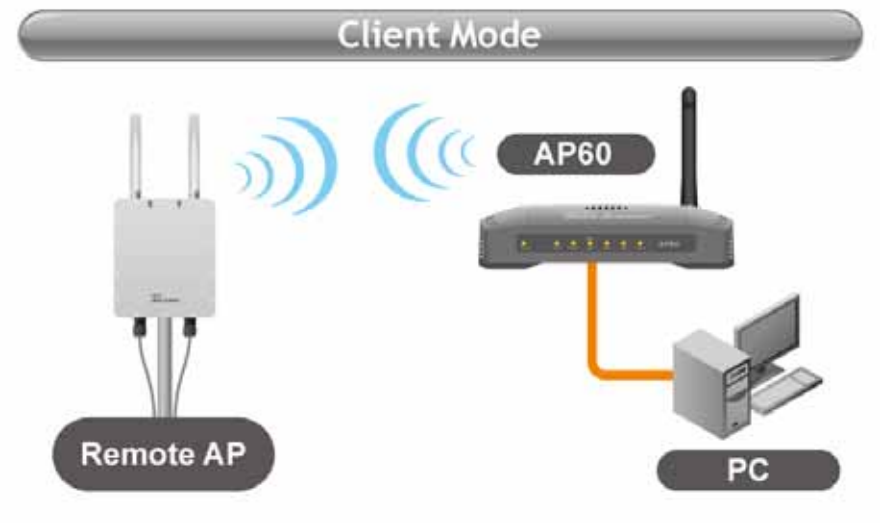
1.4.1 Access Point Mode

When operating in the Access Point mode, the AP60 becomes the center hub of the wireless network. All wireless cards and clients connect and communicate through AP60. This type of network is known as "**Infrastructure Network**". Other AP60 or 802.11b/g/n device can connect to AP mode through "**Client Mode**".



1.4.2 Client Mode

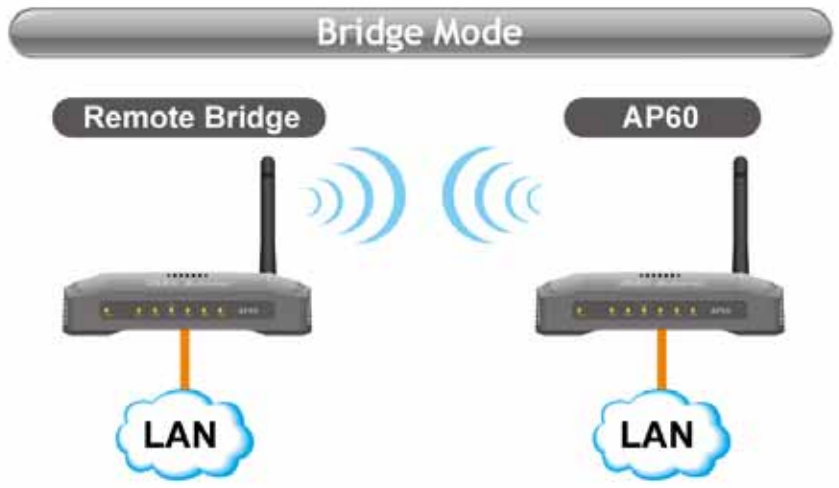
This mode is also known as "**Client**" mode. For AP60, there are 2 types of Client modes: Infrastructure and Adhoc mode. In Infrastructure mode, the AP60 acts as if it is a wireless adapter to connect with a remote Access Point. Users can attach a computer or a router to the LAN port of AP60 to get network access. This mode is often used by WISP on the subscriber's side.



In Client Ad Hoc mode, AP60 can connect to other wireless adapters without access point. Users can attach a computer or a router to the LAN port of AP60 to get network access.

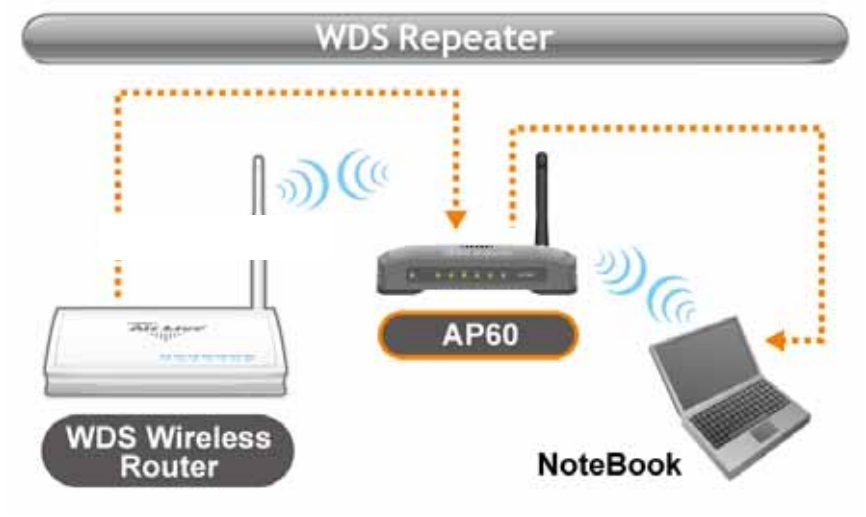
1.4.3 Bridge Mode

This mode is also known as “WDS Pure MAC Bridge mode”. When configured to operate in the Wireless Distribution System (WDS) Mode, the AP60 provides bridging functions with remote LAN networks in the WDS system. The system will support up to total of 8 bridges in a WDS network (by daisy chain). However, each bridge can only associate with maximum of 4 other bridges in the WDS configuration. This mode is best used when you want to connect LAN networks together wirelessly (for example, between office and warehouse). If you have more than 2 AP in WDS Bridges mode, please remember to turn on the “802.1d Spanning Tree” or “STP” option on to avoid network loop. This mode usually delivers faster performance than infrastructure mode.



1.4.4 WDS Repeater Mode

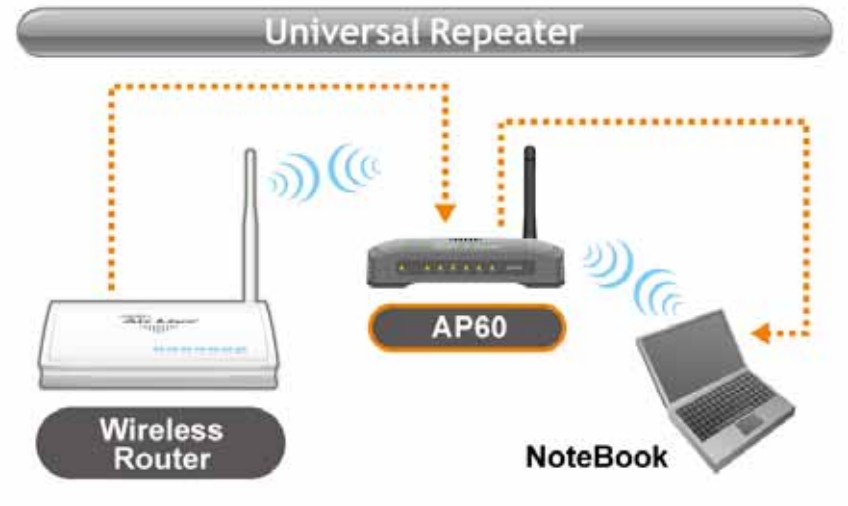
In WDS Repeater mode, the AP60 functions as a repeater that extends the range of remote wireless LAN. In this mode, the remote Access Point must have WDS (Wireless Distribution System) capability. If you require the PC's MAC addresses to be preserved when the data pass through the Repeater, it is necessary to use the WDS Repeater mode. Because the radio is divided into WDS + AP mode, the Repeater mode will have less performance and distance.



1.4.5 Universal Repeater Mode

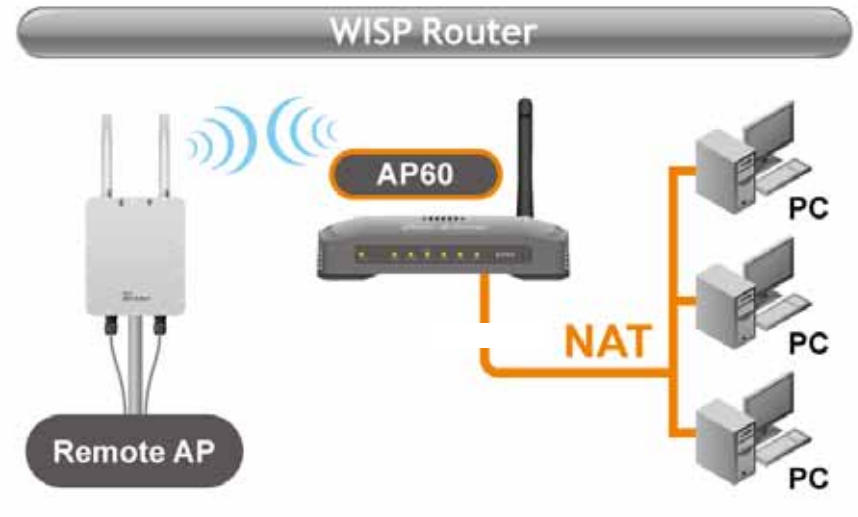
In Universal Repeater mode, the AP60 functions as a repeater that extends the range of remote wireless LAN. This mode can repeat the signal of any remote AP/Router, even if they do not have WDS capability. However, the MAC addresses of any wireless traffic going through Universal Repeater are "translated" into the Repeater's MAC address. As a result, any applications that require identification by MAC address (such as hotspot or firewall) can not use this mode. It is also recommended to use "DHCP" Relay function to get IP address from remote DHCP server.

Because the radio is divided into Client + AP mode, the Repeater mode will have less performance and distance.



1.4.6 WISP Router Mode

In WISP Router Mode, AP60 connects to the remote Access Point as in Client Infrastructure Mode. On the LAN side, it acts like a wired router for IP sharing function. This mode is best used for IP sharing application for WISP subscribers. In this mode, the WAN is the wireless client side; the LAN is the wired side.

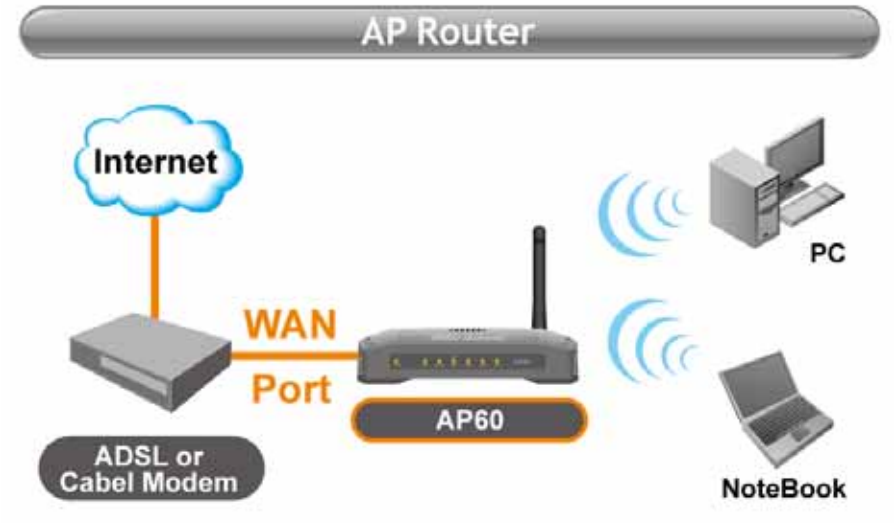


1.4.7 WISP + Repeater Mode

This mode is the combination of WISP Router mode and AP mode. The radio is divided into 2-way. One way is the client mode to connect with the remote AP, the other is the AP mode to serve the local wireless network. There is a NAT router function to share the Internet connection. Since the radio is divided by half, it is not recommended for long distance application.

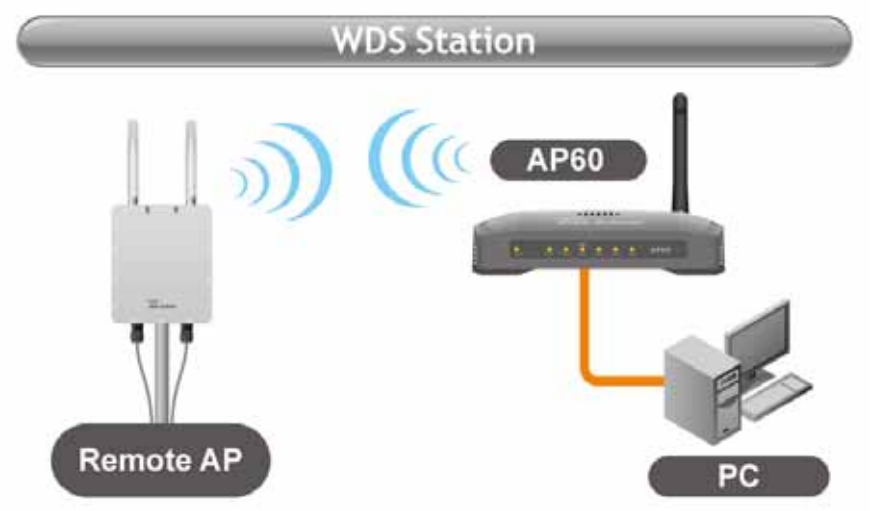
1.4.8 AP Router Mode

In AP Router Mode, the AP60 behaves like a wireless router. The LAN1 port of the AP60 will become WAN port. The wireless network of AP60 becomes the LAN side.



1.4.9 WDS Station (Bridge Send Beacon)

The WDS Station mode is similar to Bridge mode with the exception that the link has added "SSID" as basis for the bridge link. This mode is for added bridge mode compatibility with Atheros base wireless device.



2 Installing the AP60

This section describes the installation procedure for the AP60. 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 AP60. Finally, this section explains how to configure a Windows PC to communicate with the AP60.

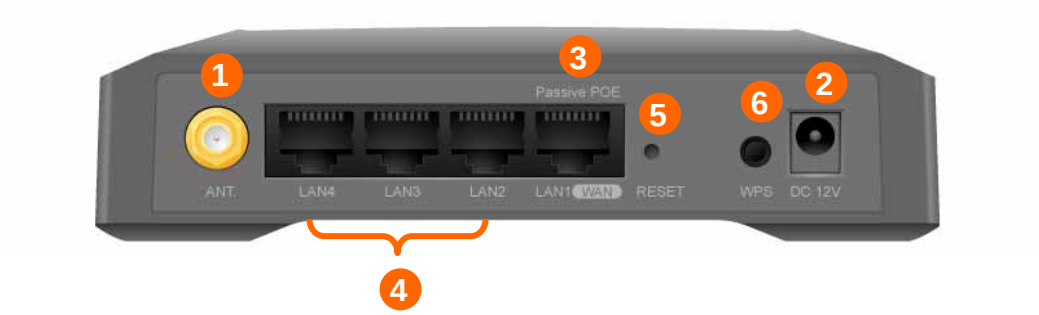
2.1 Package Content

The AP60 package contains the following items:

- One AP60 main unit
- One 12V DC power adapter
- One antenna
- One CD of the AP60
- Quick Start Guide

2.2 Knowing your AP60

Below are descriptions and diagrams of the product:



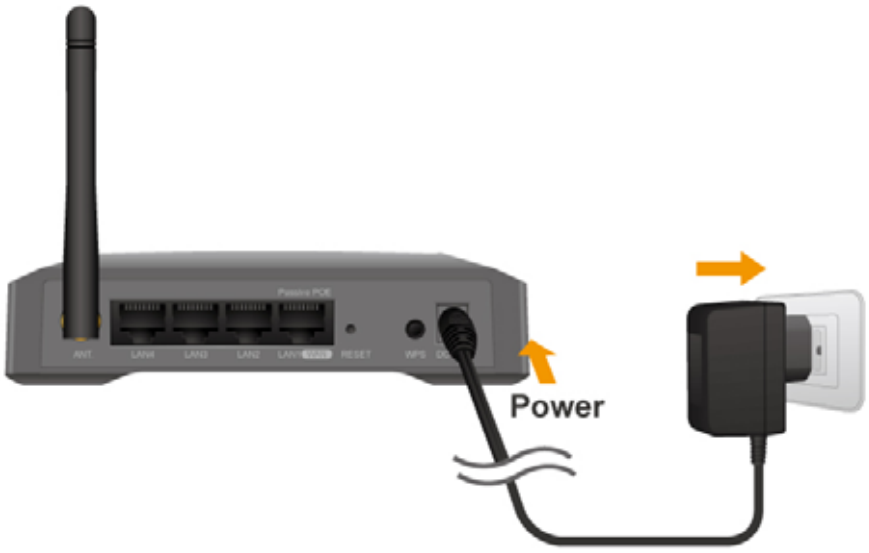
1. Antenna Connector
2. Power Adapter Connector
3. LAN Port 1, Passive PoE, or WAN Port (AP Router mode only)
4. LAN Ports
5. Reset Button
6. WPS Button

2.3 Hardware Installation

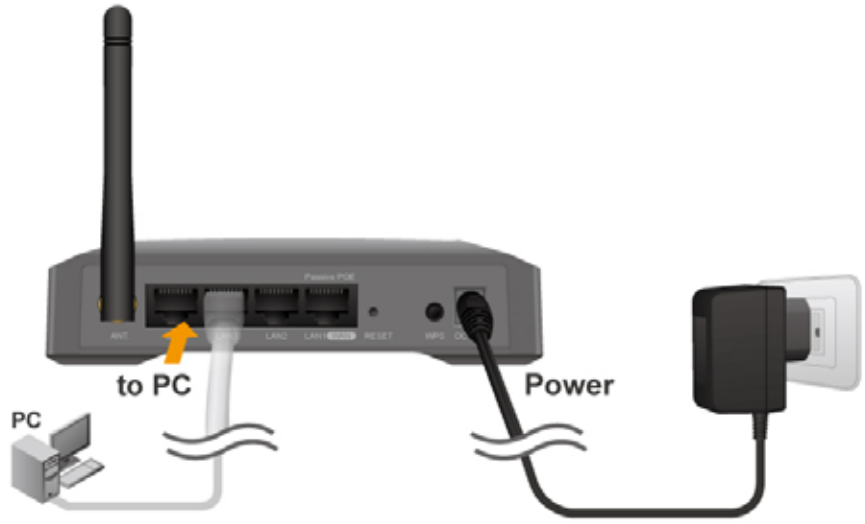
※Note	Before you starting hardware connection, you are advised to find an appropriate location to place the Access Point. Usually, the best place for the Access Point is at the center of your wireless network, with line of straight to all your wireless stations. Also, remember to adjust the antenna; usually the higher the antenna is placed; the better will be the performance.

1. Please install the antennas by turning clock wise into the RF antenna connectors

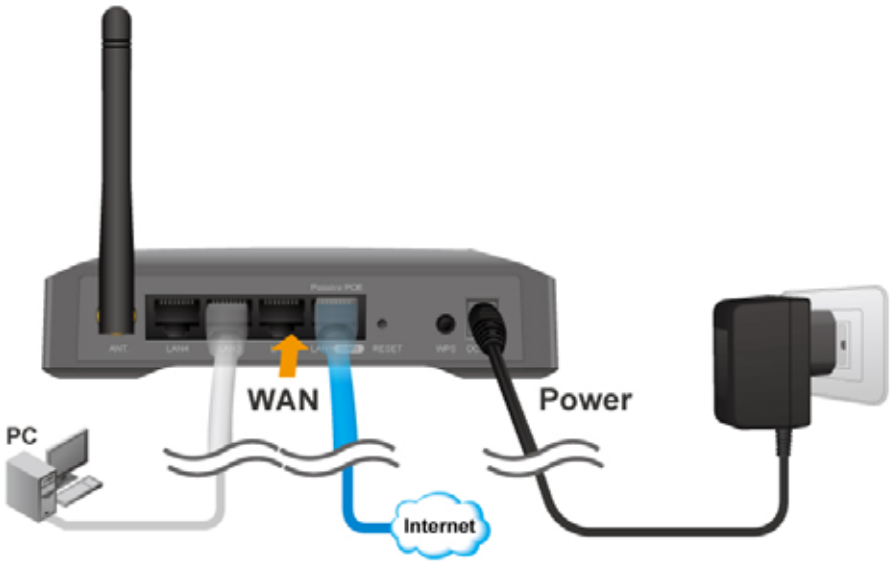
2. Now connect the power adapter to the AP60



3. Connect the Ethernet cable to one of the LAN port and the other end to your PC.

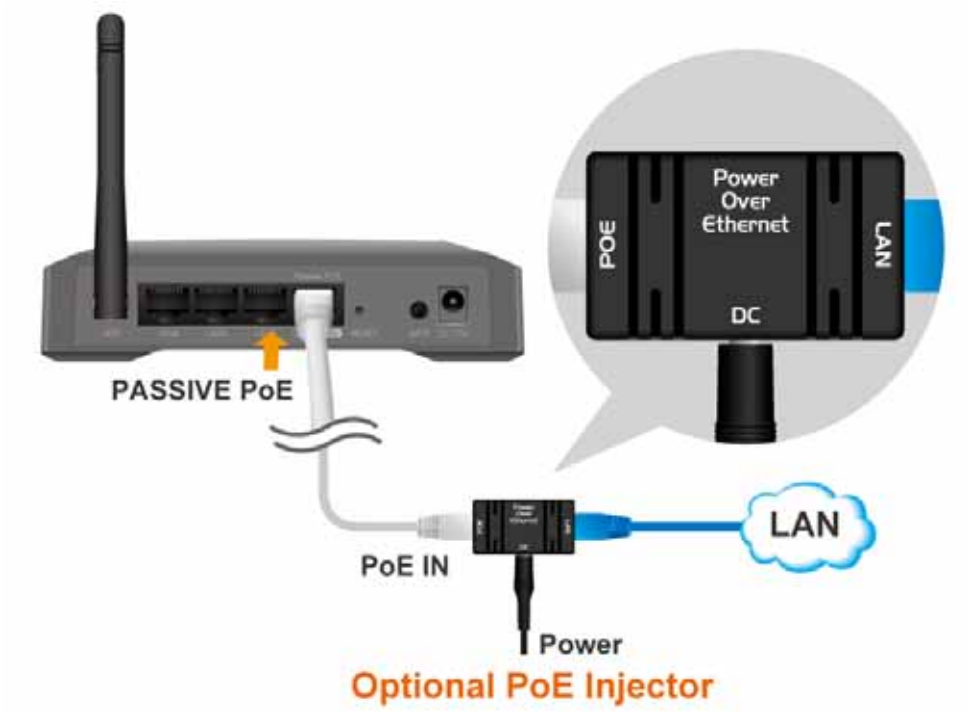


4. If you have broadband connection, please connect the Internet cable to “WAN port”.



Passive PoE Installation

If you want to supply the power by using Passive PoE, please follow the installation diagram below. Please note that the passive DC Injector is not included with AP60, it needs to be purchased separately (AirLive Model: PoE-1P). Air3G uses 12V passive PoE system. it is recommend to use a power adapter of 12Vdc at 1.25A.



2.4 LED Table

This section describes the LED behavior of AP60.

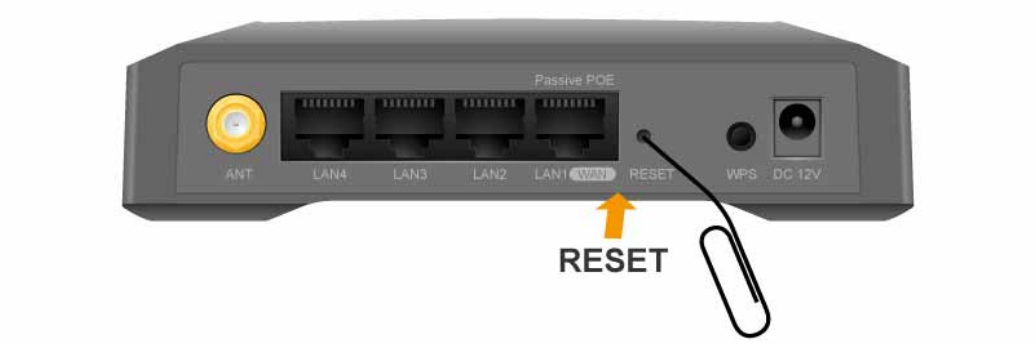
You can find the LED in front of the AP60.

LED	Display	Color	Indication
1	Power	Green	Lights on when the device is powered.
2	WPS	Green	Blinking: WPS is enabled to make a connection OFF: Radio Disabled
3	WLAN	Green	Slow Flashing : Radio is active Fast Flashing: Transmitting Data OFF: Radio Disabled

4	LAN1	Green	Lights on when the port is actively connected, blinking when transmitting or receiving data.
5	LAN2		
6	LAN3		
7	LAN4		

2.5 Restore Settings to Default

If you have forgotten your AP60's IP address or password, you can restore your AP60 to the default settings by pressing on the "reset button" for more than 5 seconds. Performing the Factory Reset will erase all previously entered device settings. The reset button is in back of the case. Please see diagram below for details.



3 Configuring the AP60

The AP60 offers web browser (http) as management interface. In this chapter, we will explain Air3G's management interface and how to get into them.

3.1 Important Information

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

- ❑ The default IP address is: 192.168.100.252 Subnet Mask: 255.255.255.0
- ❑ The default user's name is: admin
- ❑ The default password is: airlive
- ❑ The default SSID is: airlive
- ❑ The default wireless mode is : AP mode
- ❑ After power on, please wait for 1 minutes for AP60 to finish boot up
- ❑ Please remember to click on "Apply" for new settings to take effect
- ❑ **You must reboot the AP60 after you finish all the settings for changes to take effect**
- ❑ When you change to "AP Router" mode, the LAN port 1 will become WAN port.
- ❑ The default regulatory domain is "ETSI" for Europe. If you are not living in EU countries, you might wish to change the regulatory domain. However, please do not choose regulatory domain that does not apply to your country. Using wrong regulatory domain might be illegal.
- ❑ By Default, the DHCP server is turned off, please to configure your PC's IP address manually.

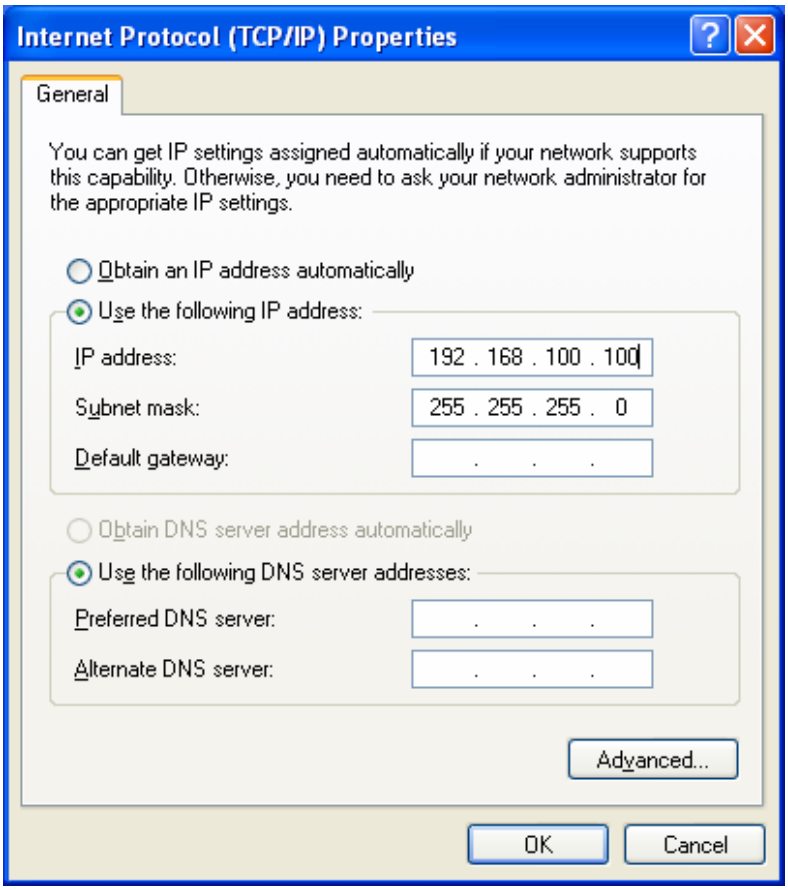
3.2 Prepare your PC

The AP60 can be managed remotely by a PC through either the wired or wireless network. The default IP address of the AP60 is **192.168.100.252** with a *subnet mask* of 255.255.255.0. This means the IP address of the PC should be in the same subnet of the AP60.

To prepare your PC for management with the AP60, please do the following:

1. Connect your PC directly to the LAN port of AP60

2. Set your PC's IP address manually to 192.168.100.100 (or other address in the same subnet)



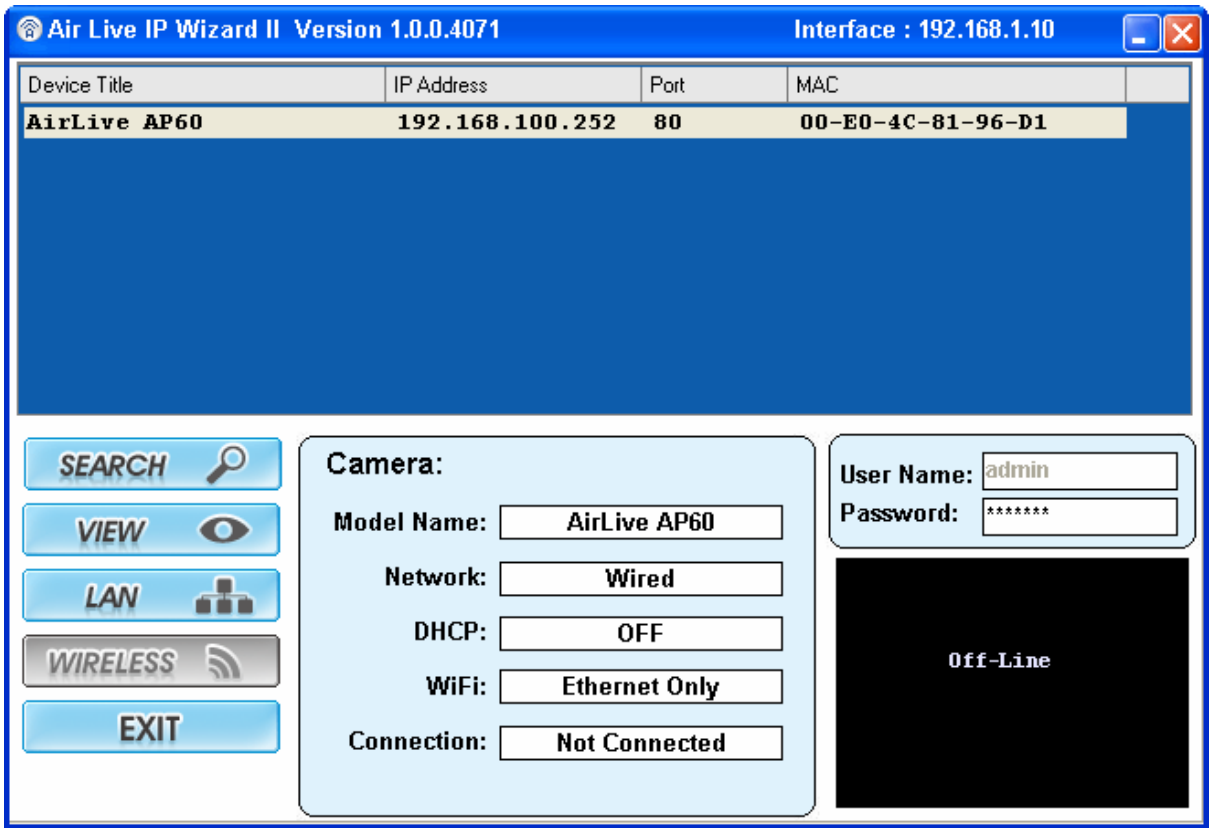
You are ready now to configure the AP60 using your PC.

3.3 Introduction to IP Finder

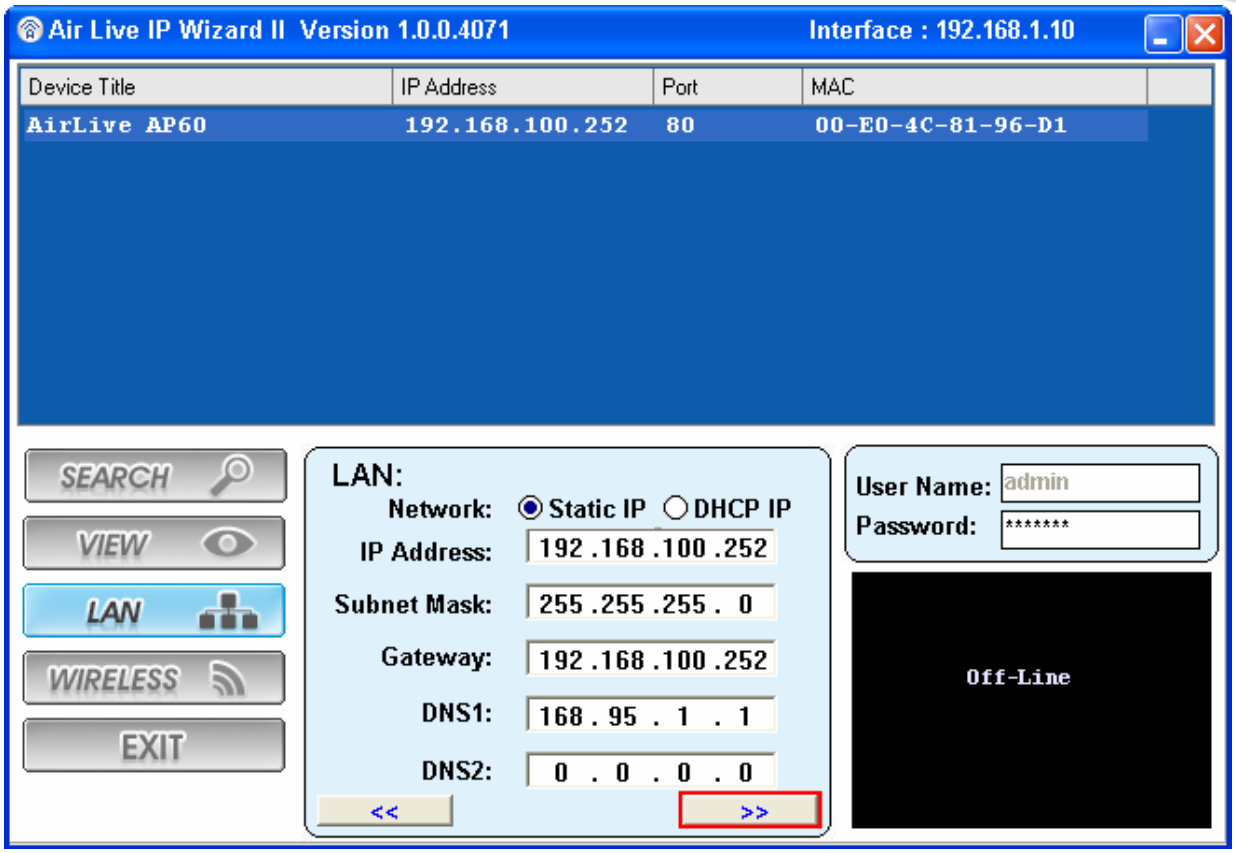
The AP60 provides IP Finder utility and you can get into web management easily. IP Finder is included in the CD. Just click and follow the step by step instruction to install.

While entering the IP Finder utility, the IP Finder will automatically search the AP available on the network. IP Finder will show the Device Name, IP Address, HTTP Port, and Ethernet MAC Address.

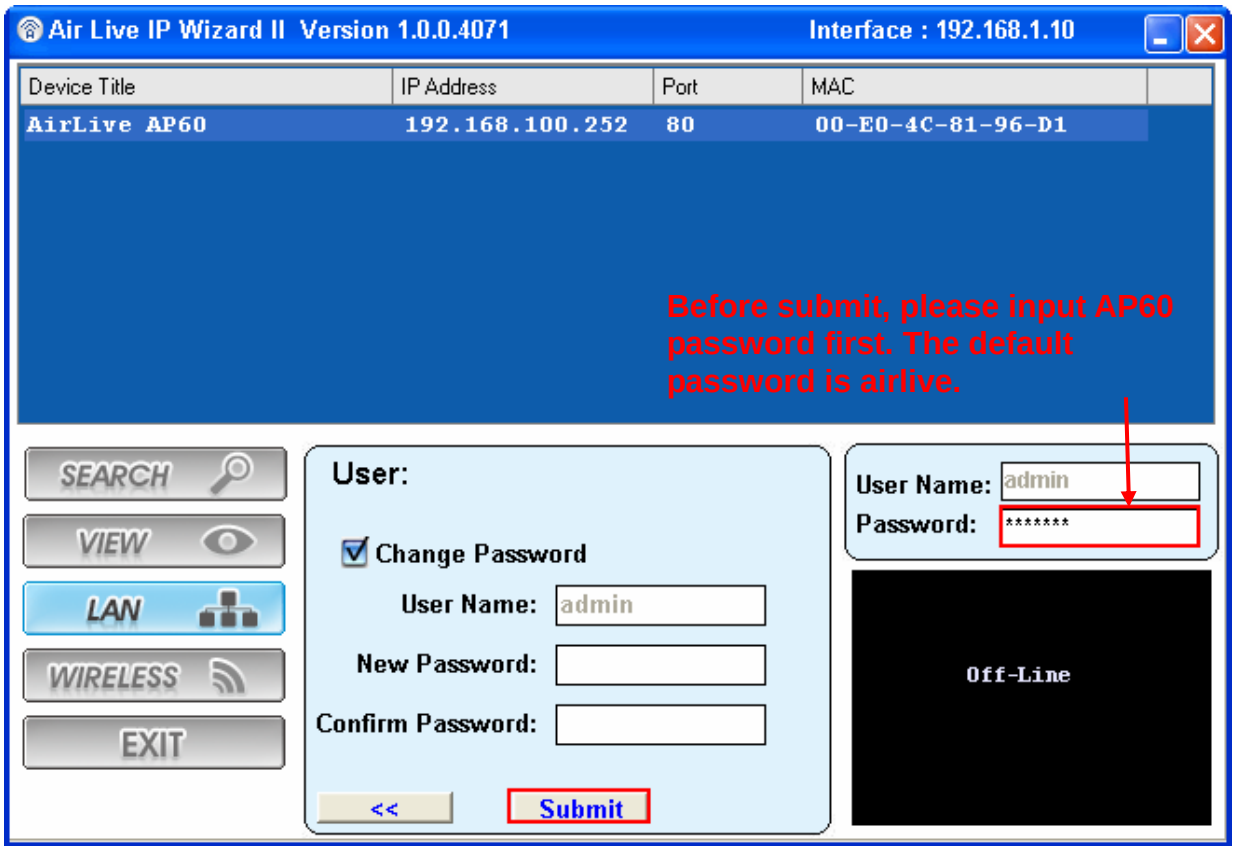
Before start using IP Finder, make sure you disable personal firewall installed in you PC. (Ex. Windows XP personal firewall)



- Search: By clicking Search, IP Finder will try to discover the AP60 on the network.
- View: The function is for IP Camera only. It does not work for PC.
- LAN: You can configure the AP60 LAN IP address here. After enter the IP Address, press >> to the next page. If you would like to change the AP60 login password, please check the box and enter the new password. Please note that the password should be filled before click submit.
- Exit: Click to close IP Finder.



Click to the next page



Click Submit to save the configuration.

3.4 Introduction to Web Management

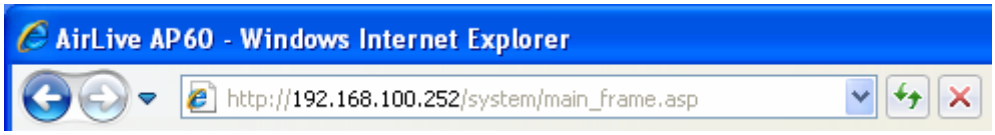
The AP60 can be configured using the Web management interfaces by simply typing its IP address in the web browser. Most functions of AP60 can be accessed by it.

If you are placing the AP60 behind router or firewall, you might need to open the port 80 at virtual server on your firewall/router. This procedure is not necessary in most cases unless there is a router/firewall between your PC and AP60.

3.4.1 Getting into Web Management

You can enter the web management by entering IP address into the web browser's address field.

- To get into the Normal Web Management, simply type in the AP60's IP address (default IP is 192.168.100.252) into the web browser's address field.



3.4.2 Main Menu

After key in the correct username and password, you will enter the main Web management screen.

- **Wireless Settings**: You will find all the settings for wireless and WAN settings in this page. The AP60's wireless settings are different between wireless modes. Only functions that are applicable to the wireless mode will show to simplify configuration. For example, WAN Port is only displayed in WISP Router and AP Router modes.
- **Wireless Mode:** On the left hand side bar, you will find the "Wireless Mode" pull down menu. The menu will display what is the current wireless mode. You can change mode by the pull down menu. The AP will ask you to confirm for the mode change and reboot to the new wireless mode.
- **System Configuration:** All non-wireless and router mode settings are in this category. The system configurations including changing password, upload firmware, backup configuration, settings PING watchdog, and setting management.
- **Device Status**: This section for monitoring the status of AP60. It provides information on device status, Ethernet status, wireless status, wireless client table, and system log.
- **Reboot:** Please remember to save changes and reboot after you finish all settings. The changes will take effect only after reboot.
- **Language Bar:** You can select different language for the web management interface here.

3.5 Initial Configurations

We recommend users to browse through AP60's web management interface to get an overall picture of the functions and interface. Below are the recommended initial configurations for first time login:

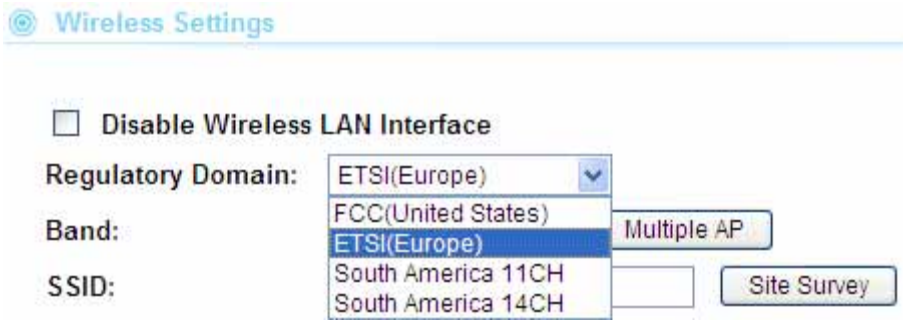
3.5.1 Changing the Regulatory Domain

The Regulatory Domain decides what channels and Tx output power levels are available for your country. In most cases, the Regulatory Domain is already selected correctly for your country. Please note that using the wrong Regulatory Domain is strictly prohibited. If you live inside EU, you must use the ETSI Regulatory Domain. If you live in United States, you must use FCC domain.

The AP60 is available with the following Regulatory Domain:

Regulatory Domain	Available Channels	Maximum Tx Output Power
ETSI (Europe)	1 ~13	20dBm
FCC (United States)	1~11	23dBm
South America(11 CH)	1~11	29dBm
South America(14 CH)	1~14	29dBm

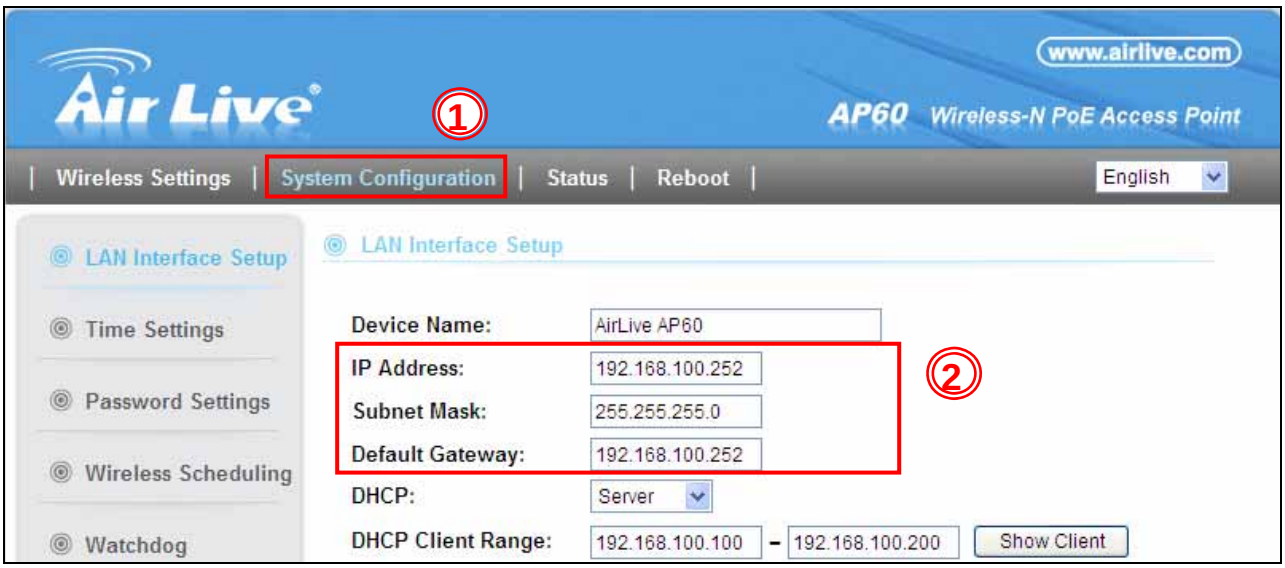
To change Regulatory Domain, please go to the "Wireless Settings" page.



3.5.2 Change the Device's IP Address

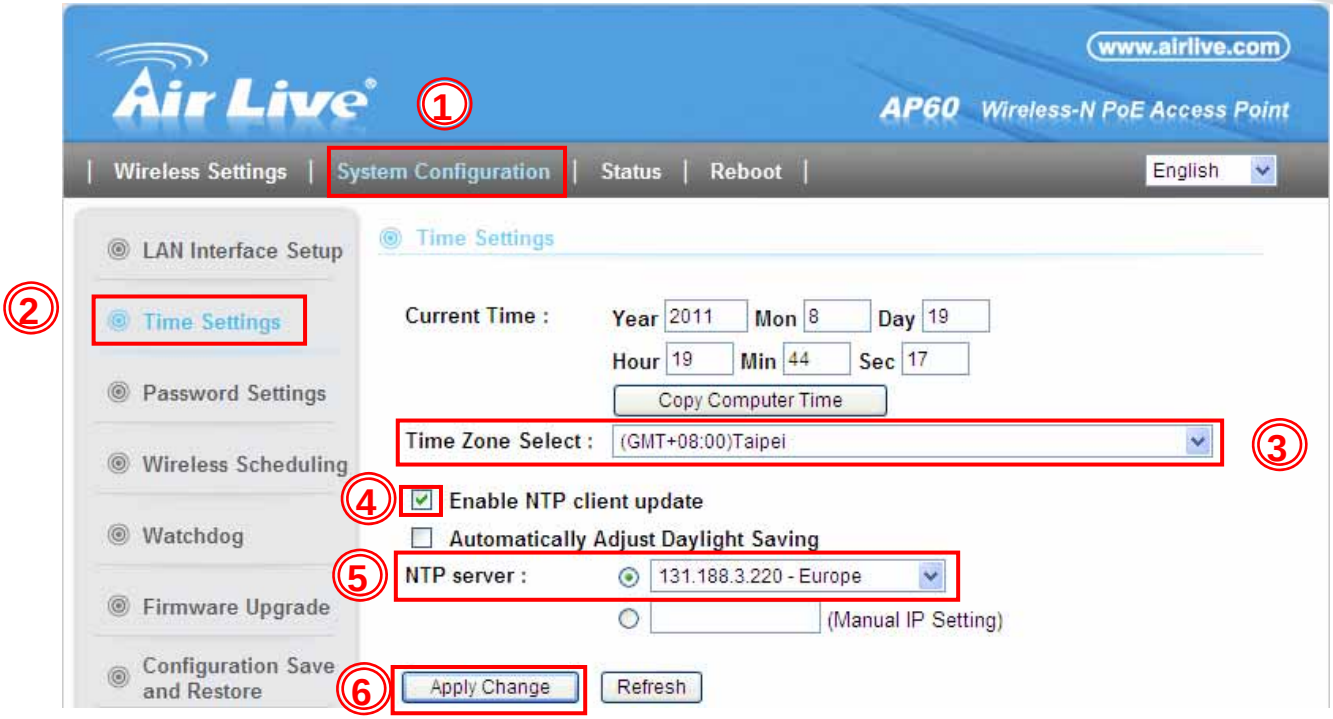
The default IP address is at 192.168.100.252. You should change it to the same subnet as your network. Also, if you want to manage AP60 remotely, you have to set the Gateway and DNS server information.

To setup the IP settings for AP60, please select "System Configuration" -> Device IP Settings". After entering the IP information, click on "Apply Changes" to finish.



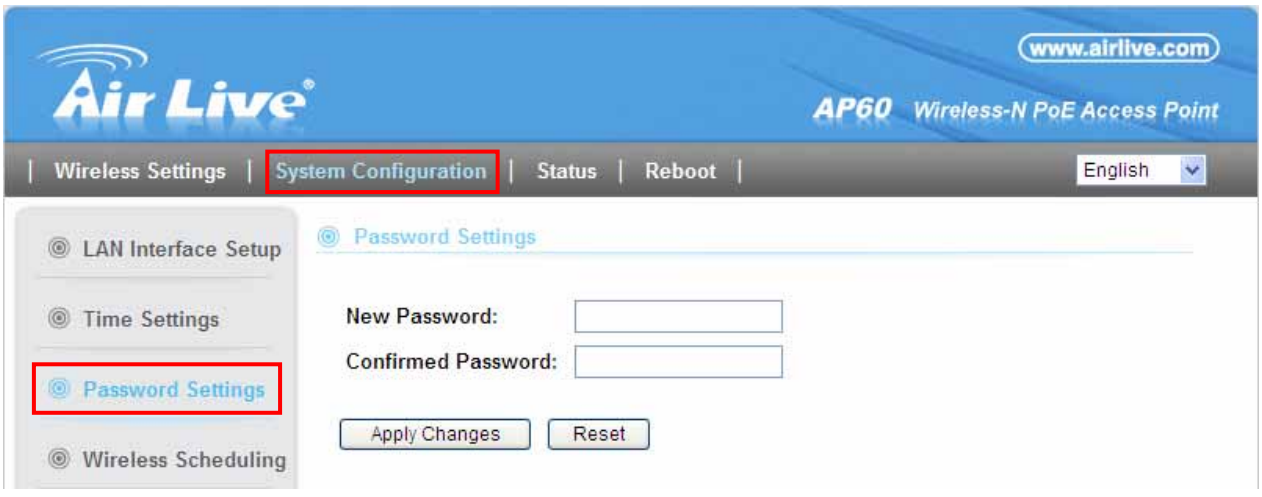
3.5.3 Set the Time and Date

It is important that you set the date and time for your AP60 so that the system log will record the correct date and time information. Please go to "*System Configuration" ->Time Settings*. We recommend you choose "Enable NTP" so the time will be keep even after reboot. If your AP60 is not connected to Internet, please enter the time manually. Please remember to select your local time zone and click "Apply" to finish.



3.5.4 Change Password

You should change the password for AP60 at the first login. To change password, please go to *"System Configuration" -> "Password Settings"* menu.



4 Wireless Settings

In this chapter, we will explain about the wireless settings in web management interface. Please be sure to read through Chapter1's Wireless Operation Mode and Chapter 3's "*Introduction to Web Management"* and *"Initial Configurations"* first.

Although router mode settings (WAN port, Virtual Server…etc) are part of the wireless settings menu, they will be explained in Chapter 5.

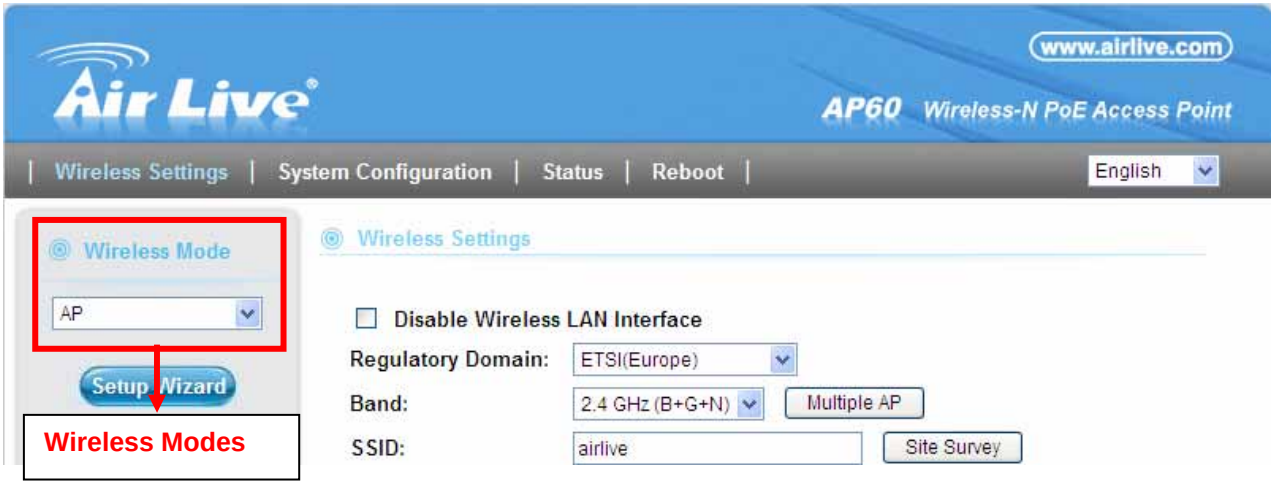
4.1 About Wireless Modes

The AP60 has total of 9 operation modes to suit different application requirements. In this section, we will explain how to change between wireless operation modes. For explanation on each different operation mode, please read Chapter 1 section 1.4 first.

Below is the summary table for different wireless modes:

AP60 Wireless Operation Mode			
Wireless Mode	**Radio**	**WAN**	**Application**
Access Point	AP	None	Hotspot (Indoor and Outdoor)
Client	Client	None	WISP Client
WISP Router	Client	Wireless	WISP Client Router
Bridge	Bridge	None	Building to Building network
WDS Repeater	AP + Client	None	Extend distance of another WDS AP/Router
Universal Repeater	AP + Client	None	Extend distance of any AP Router
WISP + Repeater	AP + Client	Wireless	WISP 2-Way CPE (One radio only)
AP Router	AP	LAN Port	Broadband Sharing
WDS Station	Bridge	None	Bridge with SSID

To change between different wireless modes, please to go the “Wireless Settings” menu, on the left hand side bar, you will see the “Wireless Mode” pull down menu which displays the current operation mode.



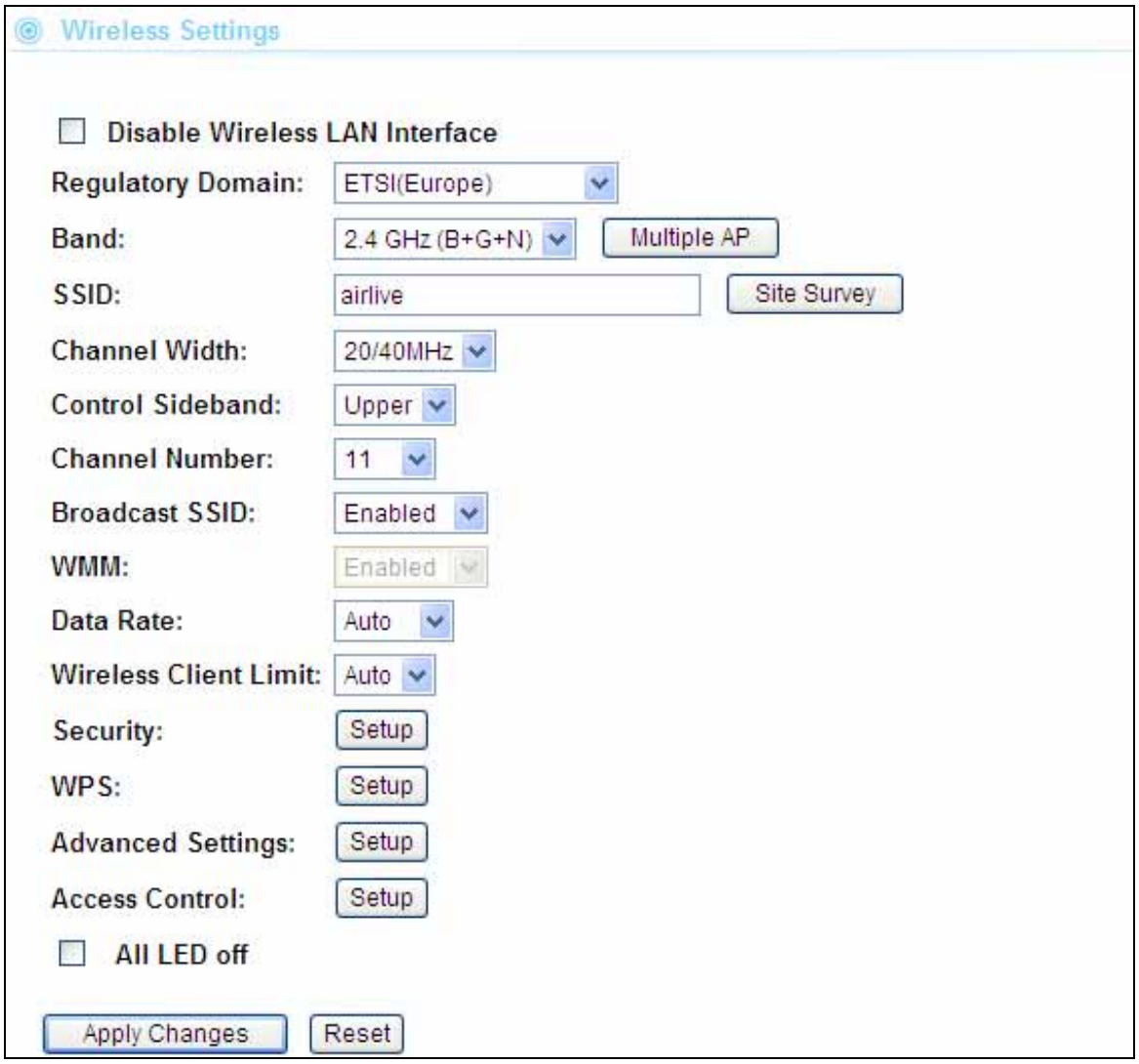
To change wireless mode, please select the new wireless mode from the pull-down menu. The AP60 will ask you to confirm about the mode change. After your confirmation, the AP will reboot itself to the new mode.

After you change to the “AP Router” mode, the LAN port 1 will become WAN port. And the WAN Access Type will be changed to DHCP Client.

4.2 General Wireless Functions

This section will explain the general wireless functions. Not all functions are available in every wireless mode. Please refer to the web interface what is available of each mode.

When you select "*Wireless Settings*" on the top menu; the following screen will appear:



4.2.1 Regulatory Domain

Wireless Settings -> Regulatory Domain

The Regulatory Domain decides what channels and Tx output power levels are available for your country. In most cases, the Regulatory Domain is already selected correctly for your country. Please note that using the wrong Regulatory Domain is strictly prohibited. If you live inside EU, you must use the ETSI Regulatory Domain. If you live in United States, you must use FCC domain.

The AP60 is available with the following Regulatory Domain:

Regulatory Domain	Available Channels	Maximum Tx Output Power
ETSI (Europe)	1 ~13	20dBm
FCC (United States)	1~11	23dBm
South America(11 CH)	1~11	29dBm
South America(14 CH)	1~14	29dBm

4.2.2 Band

Wireless Settings -> Band

AP60 has 6 different options for WLAN transmission. All devices in the same network should use the same WLAN mode.

- **2.4 GHz (B):** The radio will only connect at 11b mode.
- **2.4 GHz (G):** The radio will only connect at 11g mode.
- **2.4 GHz (N):** The radio will only connect at 11n mode.
- **2.4 GHz (B+G):** The radio will auto adjust between 11g and 11b mode.
- **2.4 GHz (G+N):** The radio will auto adjust between 11n and 11g mode.
- **2.4 GHz (B+G+N):** The radio will auto adjust between 11n, 11g and 11b mode. It is recommended to use this mode.

4.2.3 SSID

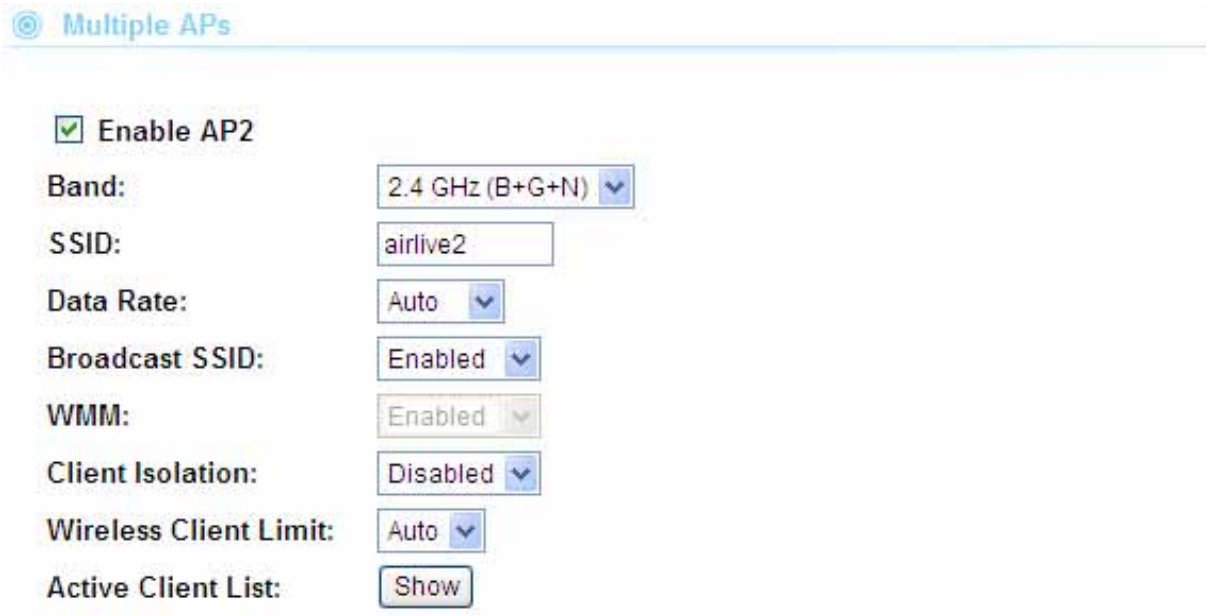
Wireless Settings -> SSID

The SSID is the network name used to identify a wireless network. The SSID must be the same for all devices in the same wireless network. The SSID length is up to 32 characters. The default SSID is "**airlive**".

4.2.4 Multiple SSID

Wireless Settings -> Multiple SSID

Multiple SSID allows Air3G to create up to **4** different wireless networks (SSID). It is also known as “Virtual AP” function. Each SSID can have its Encryption policy. The SSID1 is the main SSID under Wireless Setting page.

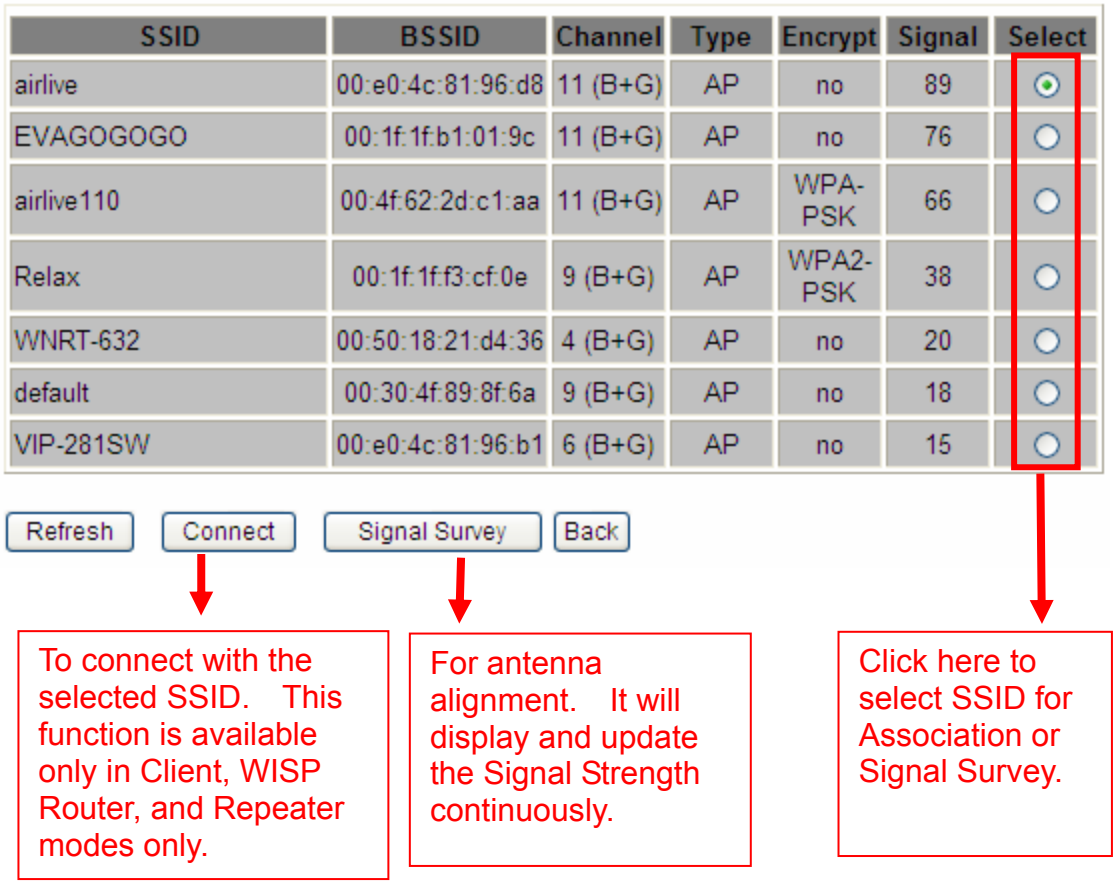


4.2.5 Site Survey

Wireless Settings -> Site Survey

You can scan for wireless networks around your location using the Site Survey function. From the site survey function, you can also perform antenna alignment and establish wireless connection

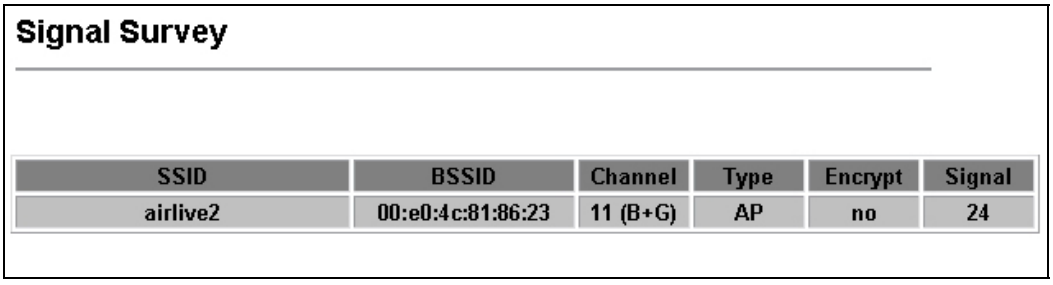
When you click on Site Survey, the following screen will appear. It might take awhile depending on number of available APs in the area.



4.2.6 Signal Survey

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

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



- **BSSID**: This is the remote AP's MAC address.
- **Channel**: The current scanned channel
- **Signal Strength**: This is signal strength number in percentage in 0 to 100 scale. The higher the number, the better signal.

4.2.7 Channel Width

Wireless Settings -> Channel Width

You can choose 20MHz or 20/40MHz channel width. Choose 20MHz for compliance with laws in some countries. 40MHz offers faster performance than 20MHz

4.2.8 Channel Sideband

Wireless Settings -> Channel Sideband

This function will be available under 2.4GHz (N), 2.4GHz (G+N), and 2.4GHz (B + G+ N) mode. Select upper or lower form the pull-down list, default is upper.

4.2.9 Channel

Wireless Settings -> Channel

The channel is the frequency range used by radio. In 802.11n/g/b standard, there are maximum of 14 Channels. However, the available channels in each country are dependant on the local regulation. If you are living in Europe, you can use channel 1 to 13. If you are living in the United States, you can use channel 1 to 11.

Each wireless channel takes between 22 to 25MHz of frequency width. But the channels are only 5MHz apart. Therefore, only every 5 channels can be free of interference with each other. It is recommended that you can do a site survey to find about what channels are used by surrounding AP and choose a channel that is not used by other APs.

Channel	Frequency (MHz)	U.S.A.	Europe
1	2412	O	O
2	2417	O	O
3	2422	O	O

4	2427	O	O
5	2432	O	O
6	2437	O	O
7	2442	O	O
8	2447	O	O
9	2452	O	O
10	2457	O	O
11	2462	O	O
12	2467	-	O
13	2472	-	O
14	2484	-	-

4.2.10 Broadcast SSID

Wireless Settings -> Broadcast SSID

When this function is disabled, the wireless network will become invisible. Only people who know the SSID name can join the network. It is recommended to use this feature to protect the network from intruders. However, once this function is disabled, it might be necessary to configure the wireless connection manually. This option is available in AP mode, AP Router mode, and Repeater modes only.

4.2.11 WMM

Wireless Settings -> WMM

Wi-Fi Multimedia (WMM) is a standard to prioritize traffic for multimedia applications. The WMM prioritize traffic\ on Voice-over-IP (VoIP), audio, video, and streaming media as well as traditional IP data over the AP.

The Wi-Fi Multiple Media function is available under 2.4GHz (B), 2.4GHz (G) and 2.4GHz (B+G) band, and it is enabled under 2.4GHz (N), 2.4GHz (G+N) and 2.4GHz (B+G+N) band.

4.2.12 Data Rate

Wireless Settings -> Data Rate

Data Rate is the physical speed of transmission. The default setting is Auto. In “Auto” mode, the data rate will adjust according to the connection condition. It is advised to put the data rate in Auto.

However, you can also force the radio to operate at specific data rate. The highest for 11b is 11Mbps, 11g is 54Mbps, and 11n is MCS7.

4.2.13 Wireless Client Limit

Wireless Settings -> Wireless Client Limit

This limitation applies to number of wireless clients the device can associate. If you need to serve wireless connection to large number of users in one location. You can deploy many APs and limit the number of wireless clients, so any additional wireless connection attempt will be rejected (therefore, redirect to other AP). The range of user limitation is from 1 to 31.

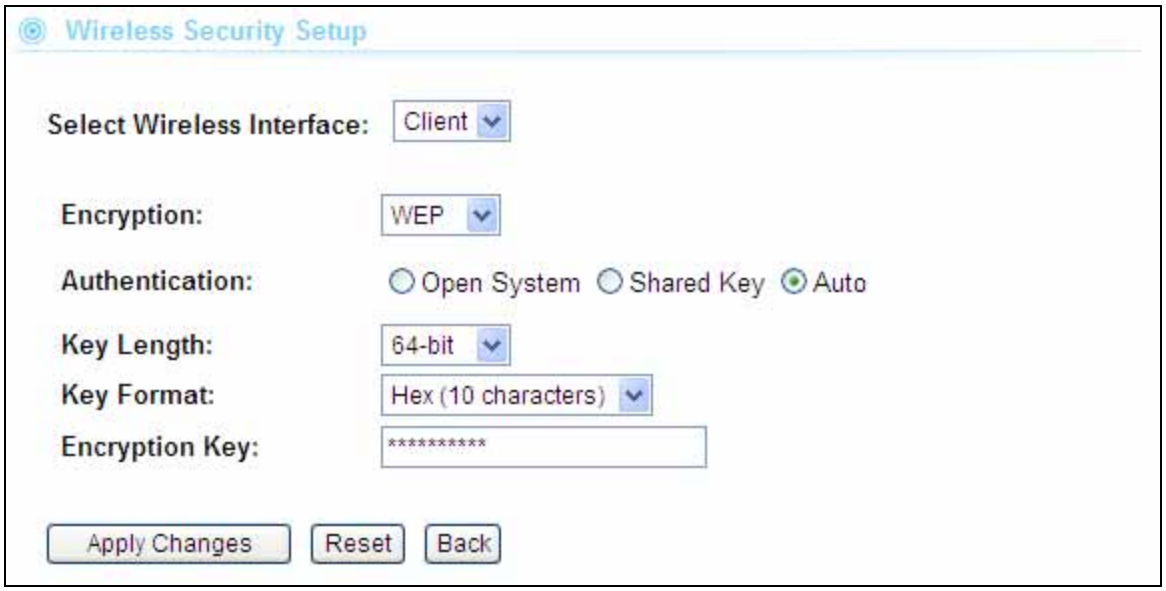
4.2.14 Client Mode Security Settings

Wireless Settings -> Security Settings

Security settings allow you to use encryption to secure your data from eavesdropping. You can select different security policy to provide association authentication and/or data encryption. The AP60 features various security policies including WEP, 802.1x, WPA, WPA Personal, WPA2, WPA2 Personal.

WEP

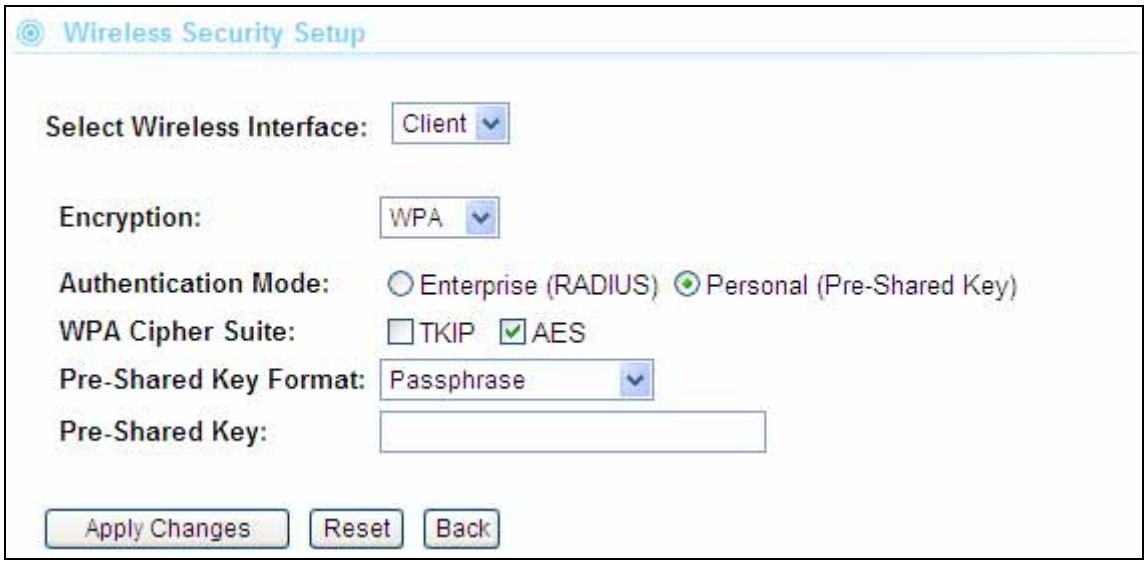
WEP Encryption is the oldest and most available encryption method. However, it is also the least secure.



- **Select Wireless Interface:** When AP60 is configured as repeater mode, you can set the security separately. Change the interface by selecting pull-down menu and configure the security.
- **Authentication:** 2 types of Authentication are offered. Open system and Shared key. If you are not sure which one to use, please select “Auto”.
- **Key Length:** The AP60 offers 64bit and 128 bit for WEP key length. The longer the Key Length, the more secure the encryption is.
- **Key Format:** 2 types are available: ASCII and HEX. ASCII is a string of ASCII code including alphabetical characters, space, signs and numbers (i.e. “airlivepass12”). HEX is a string of 16-bit hexadecimal digits (0..9, a, b, c, d, e, f). All wireless devices on the network must match the exact key length and Key type. Some Wireless clients only allow HEX type for WEP.
- **ASCII-64:** This is a key with 64-bit key length of ASCII type. Please enter **5** ASCII Characters if you choose this option. For example, “passw”
- **HEX-64:** This is a key with 64-bit key length of HEX type. Please enter **10** Hexadecimal digits if you choose this option. For example, “12345abcdef”
- **ASCII-128:** This is a key with 64-bit key length of ASCII type. Please enter **13** ASCII Characters if you choose this option. For example, “airlivewepkey”
- **HEX-128:** This is a key with 128-bit key length of HEX type. Please enter **26** Hexadecimal digits if you choose this option. For example, “1234567890abcdef1234567890”

WPA-PSK, WPA2-PSK

Wi-Fi Protected Access (WPA) introduces the Temporal Key Integrity Protocol (TKIP) that provides added security. WPA2 adds full support for 802.11i standard and the CCMP (AES Encryption). The WPA Mixed tries to authenticate wireless clients using both WPA-PSK and WPA2-PSK.



- **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 **TKIP** and **AES** to allow TKIP clients and CCMP clients to connect to the Access Point at the same time.
- **Pre-Shared Key Format**: You can select between Passphrase(ASCII) or HEX format. Please select Passphrase if you are not sure what to use.
- **Pre-Shared Key**: Enter the password key here..

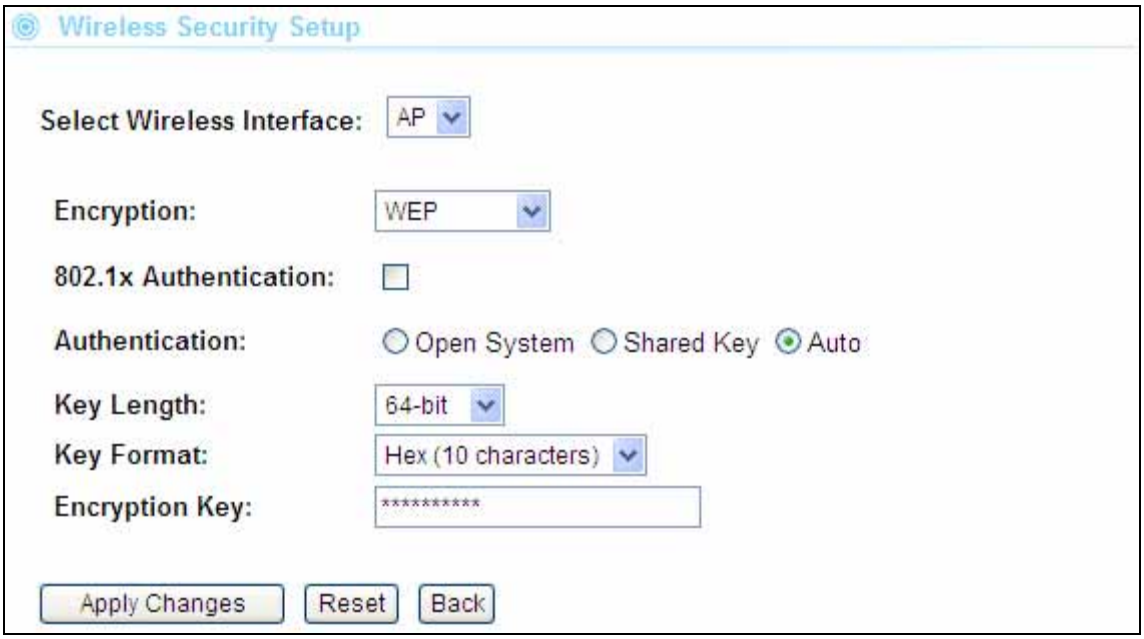
4.2.15 AP Mode Security Settings

Wireless Settings -> Security Settings

Security settings allow you to use encryption to secure your data from eavesdropping. You can select different security policy to provide association authentication and/or data encryption. The AP60 features various security policies including WEP, 802.1x, WPA, WPA Personal, WPA2, WPA2 Personal.

WEP

WEP Encryption is the oldest and most available encryption method. However, it is also the least secure.

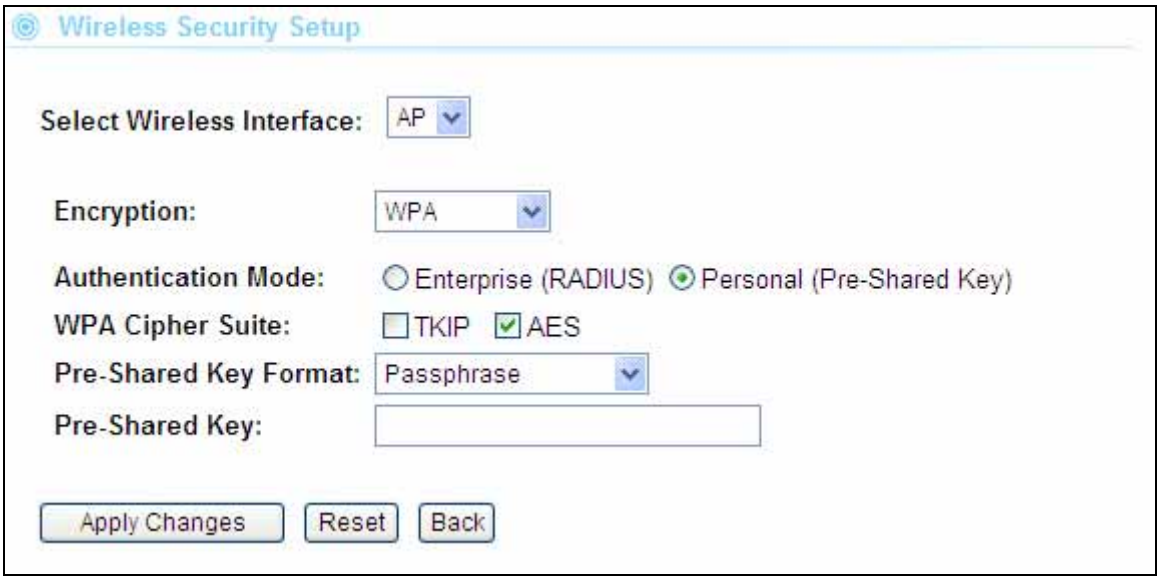


- **802.1x Authentication:** Check the box to enable the 802.1x authentication.
- **Authentication:** 2 types of Authentication are offered. Open system and Shared key. If you are not sure which one to use, please select “Auto”.
- **Key Length:** The AP60 offers 64bit and 128 bit for WEP key length. The longer the Key Length, the more secure the encryption is.
- **Key Format:** 2 types are available: ASCII and HEX. ASCII is a string of ASCII code including alphabetical characters, space, signs and numbers (i.e. “airlivepass12”). HEX is a string of 16-bit hexadecimal digits (0..9, a, b, c, d, e, f). All wireless devices on the network must match the exact key length and Key type. Some Wireless clients only allow HEX type for WEP.
- **ASCII-64:** This is a key with 64-bit key length of ASCII type. Please enter **5** ASCII Characters if you choose this option. For example, “passw”
- **HEX-64:** This is a key with 64-bit key length of HEX type. Please enter **10** Hexadecimal digits if you choose this option. For example, “12345abcdef”
- **ASCII-128:** This is a key with 64-bit key length of ASCII type. Please enter **13** ASCII Characters if you choose this option. For example, “airlivewepkey”

- **HEX-128:** This is a key with 128-bit key length of HEX type. Please enter **26** Hexadecimal digits if you choose this option. For example, "1234567890abcdef1234567890"

WPA-Personal, WPA2-Personal, WPA-Mixed

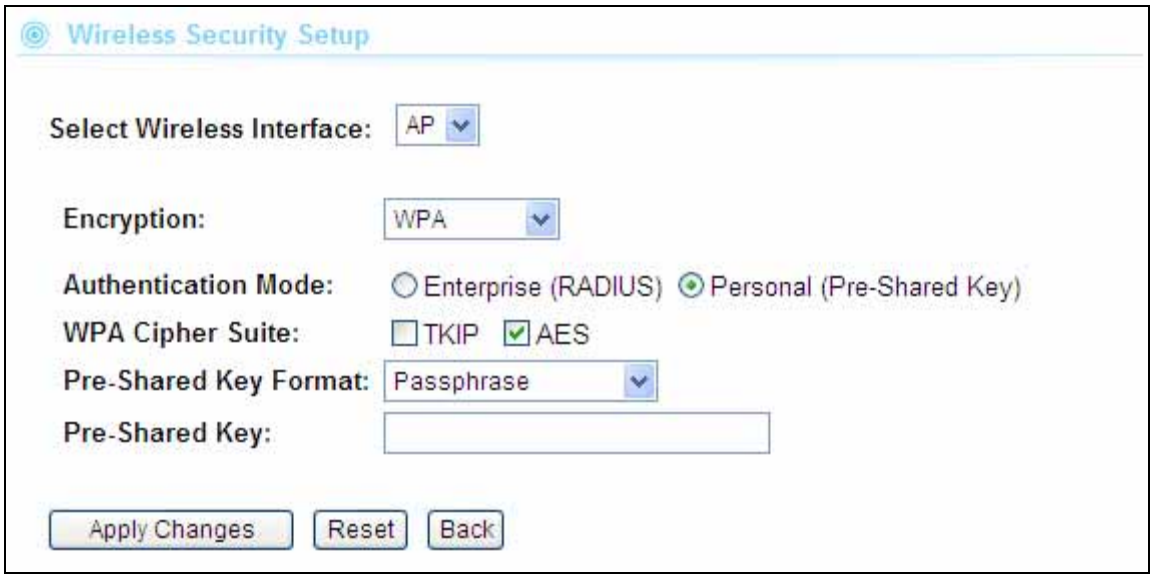
The WPA Personal is also known as "WPA-PSK" encryption. Wi-Fi Protected Access (WPA) introduces the Temporal Key Integrity Protocol (TKIP) that provides added security. WPA2 adds full support for 802.11i standard and the CCMP (AES Encryption). The WPA-Mixed tries to authenticate wireless clients using both WPA-PSK or WPA2-PSK.



- **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 **TKIP** and **AES** to allow TKIP clients and CCMP clients to connect to the Access Point at the same time.
- **Pre-Shared Key Format**: You can select between Passphrase(ASCII) or HEX format. Please select Passphrase if you are not sure what to use.
- **Pre-Shared Key**: Enter the password key here..

WPA-Enterprise, WPA2-Enterprise, WPA-Mixed Enterprise (Radius)

Wi-Fi Protected Access (WPA) Enterprise uses Radius Server as the authenticator. WPA2 adds full support for 802.11i standard and the CCMP (AES Encryption). The WPA-Mixed tries to authenticate wireless clients using both WPA or WPA2.



4.2.16 WPS

Wireless Settings -> WPS

- **Disable WPS**: Check the box to disable the WPS function, default setting is enabled.

- **WPS Status**: Here shows the current status of the WPS function. Default setting is configured; click Reset to UnConfigured to re-configure the WPS connection.

- **Self-PIN Number**: Here shows the 8-digit numbers PIN code of the router itself. Enter the Self-PIN Number to client (Registrar) end and click the PIN button at the client end to make a WPS connection. It will connect with the wireless router within two minutes and get IP address.

- **Push Button Configuration**: Click Start PBC button (or press the physical WPS button on the Wireless Router once), meanwhile, the client should also click the PBC button simultaneously within 2 minutes.

- **Client PIN Number**: Enter the client (Enrollee) PIN code into the blank field then click the Start PIN button to make a WPS connection with client. Then, the wireless router will connect to client within 2 minutes and get IP address

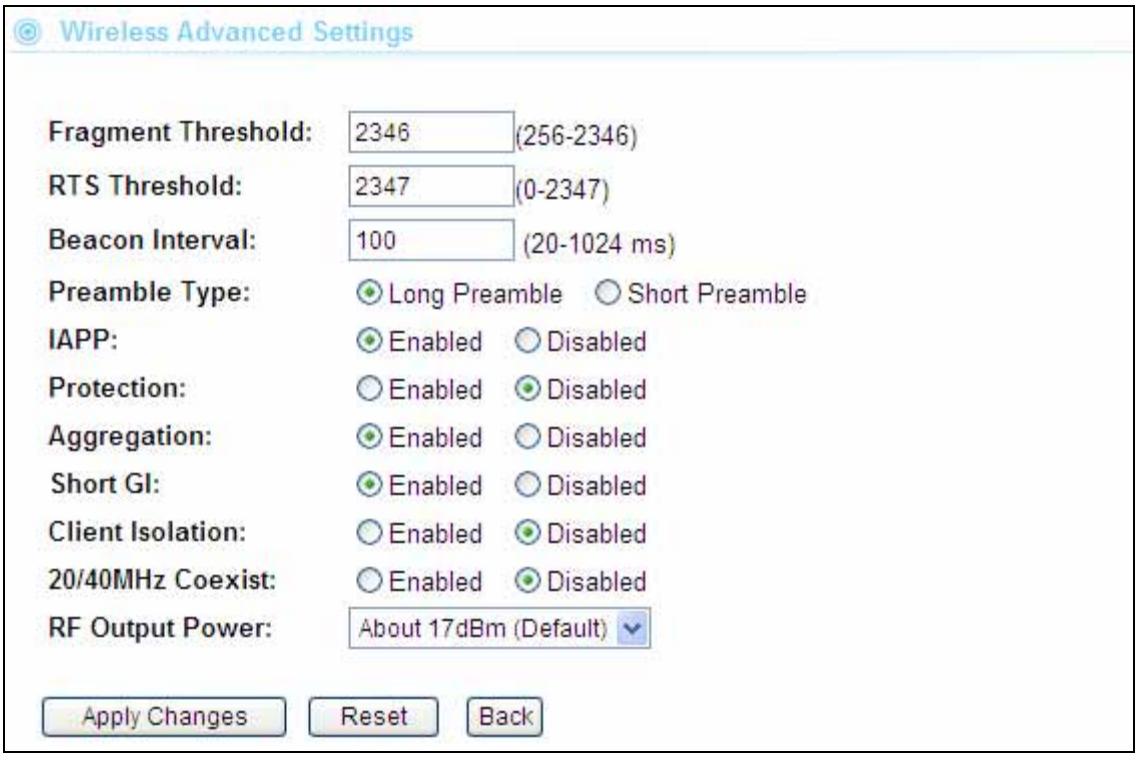
4.2.17 Access Control

Wireless Settings -> Access Control

The AP60 allows you to define a list of MAC addresses that are allowed or denied to access the wireless network. This function is available only for Access Point and AP Router modes. This function is available only for Access Point and Gateway modes.

- **Disable:** When selected, no MAC address filtering will be performed.
- **Allow list:** When selected, data traffic from only the specified devices in the table will be allowed in the network.
- **Deny list:** When selected, data traffic from the devices specified in the table will be denied/discarded by the network.

4.3 Advance Settings



- **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.

- **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.

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

- **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.

- **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.

- **Protection:** Select Enabled or Disabled to execute the security function.

- **Aggregation:** Select Enabled or Disabled to execute this function.

- **Short GI:** Select Enabled or Disabled to execute this function.

- **Client Isolation:** The default setting is "Disable". When enabled, the wireless clients will not be able to communicate with each other. This feature is useful for public WiFi, WISP operators, and Hotspot operators.

- **20/40MHz Coexist:** Select Enabled or Disabled to execute this function. The default is Disabled.

- **RF Output Power**: You can adjust the transmit output power of the AP60's radio. The higher the output power, the more distance AP60 can deliver. However, it is advised that you use just enough output power so it will not create excessive interference for the environment. Also, using too much power at close distance can create serious performance drop due to signal distortion.

  If you are not getting good signal, you can try to increase the output power. However; if your signal appear to be strong but the performance is low, it is advised to reduce the output power.

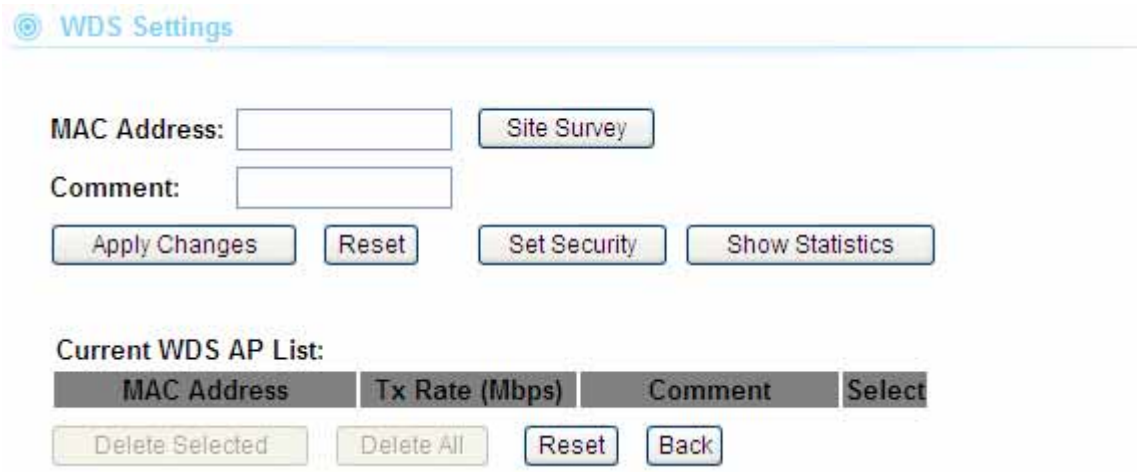
Please make sure not to exceed the legal limit of output power in your country. For EU, it is limited to 20dBm. For U.S.A., the limit is 23dBm.

4.4 Bridge Mode Settings

4.4.1 WDS Settings

Wireless Settings -> WDS

For Bridge network, it is required to enter the Wireless MAC address of all remote bridges that is connected directly to your AP60. The wireless MAC address is also known as BSSID that is display on your site survey result.



- **MAC Address:** Please enter the Wireless MAC address or BSSID of the remote Bridge. You can usually find it at remote Bridge's device label.
- **Comment:** If you input anything that will help remind you about which remote Bridge it is.

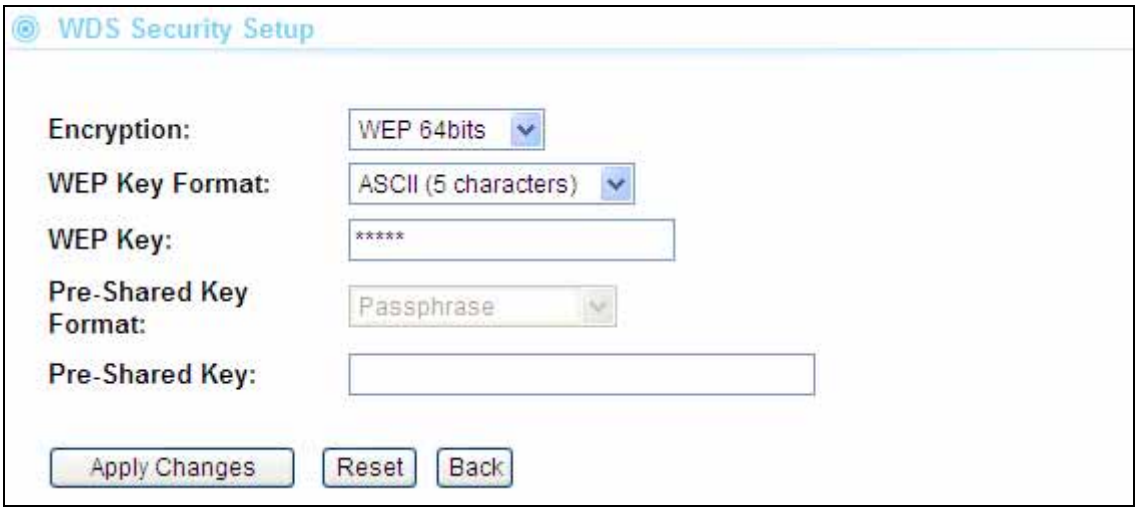
4.4.2 WDS Security

Operation Mode -> WDS -> Set Security -> WDS Security Settings

Security settings allow you to use encryption to secure your data from eavesdropping. You can select different security policy to provide association authentication and/or data encryption.

WEP

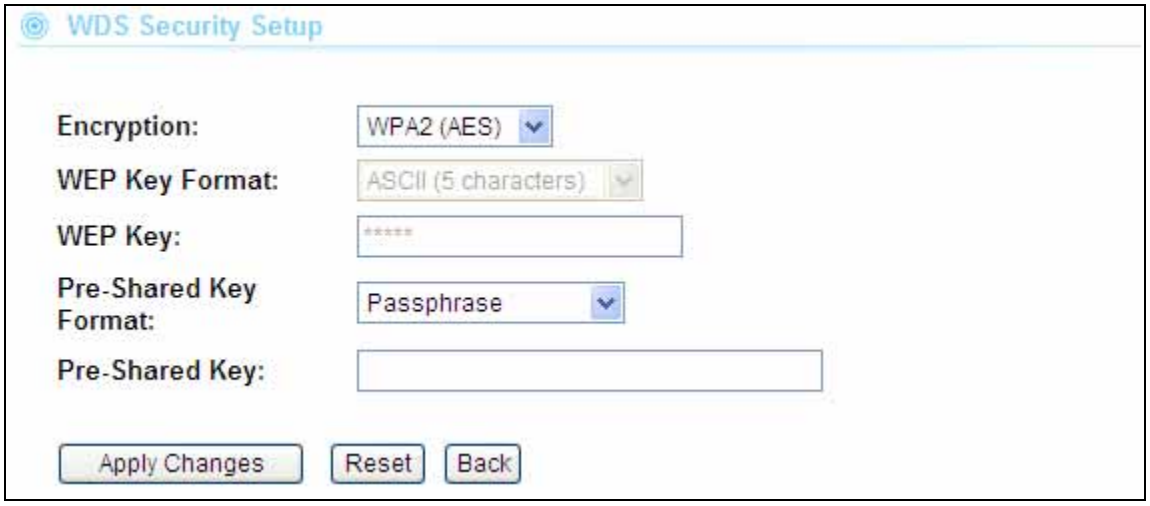
WEP Encryption is the oldest and most available encryption method. However, it is also the least secure.



- **Key Length:** The AP60 offers 64bit and 128 bit for WEP key length. The longer the Key Length, the more secure the encryption is.
- **Key Format:** 2 types are available: ASCII and HEX. ASCII is a string of ASCII code including alphabetical characters, space, signs and numbers (i.e. “airlivepass12”). HEX is a string of 16-bit hexadecimal digits (0..9, a, b, c, d, e, f). All wireless devices on the network must match the exact key length and Key type. Some Wireless clients only allow HEX type for WEP.
- **ASCII-64:** This is a key with 64-bit key length of ASCII type. Please enter **5** ASCII Characters if you choose this option. For example, “passw”
- **HEX-64:** This is a key with 64-bit key length of HEX type. Please enter **10** Hexadecimal digits if you choose this option. For example, “12345abcdef”
- **ASCII-128:** This is a key with 64-bit key length of ASCII type. Please enter **13** ASCII Characters if you choose this option. For example, “airlivewepkey”
- **HEX-128:** This is a key with 128-bit key length of HEX type. Please enter **26** Hexadecimal digits if you choose this option. For example, “1234567890abcdef1234567890”

WPA-PSK, WPA2-PSK

Wi-Fi Protected Access (WPA) introduces the Temporal Key Integrity Protocol (TKIP) that provides added security. WPA2 adds full support for 802.11i standard and the CCMP (AES Encryption).



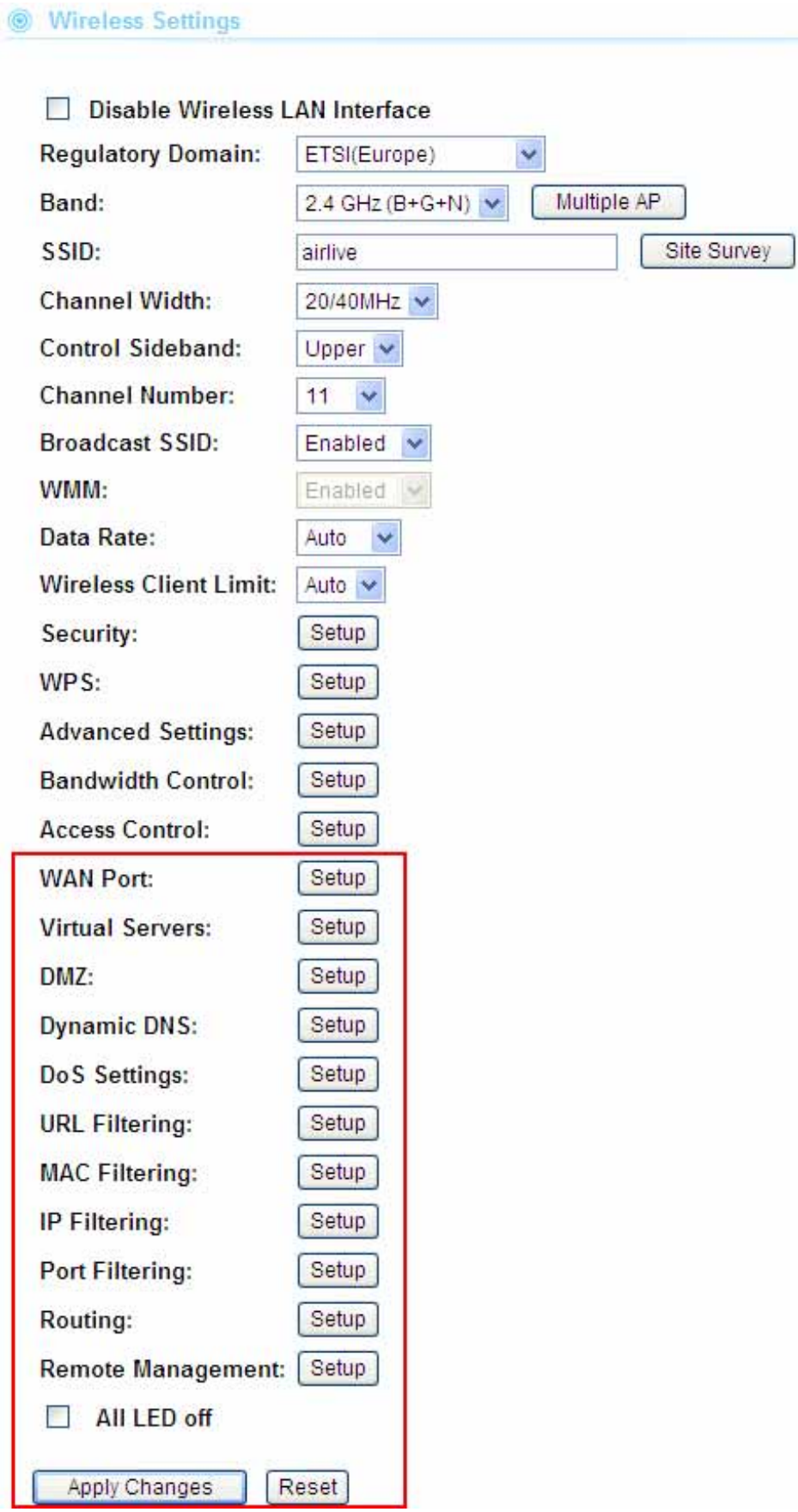
- **Pre-Shared Key Format**: You can select between Passphrase(ASCII) or HEX format. Please select Passphrase if you are not sure what to use.
- **Pre-Shared Key**: Enter the password key here..

5 Wireless Menu: Router Mode Settings

In this chapter, we will explain about Route mode settings in web management interface. The Router mode settings are available in WISP Router, AP Router, and WISP + Repeater mode. Please be sure to read through Chapter 3's "*Introduction to Web Management*" and *"Initial Configurations"* first. .

5.1 Router Mode Settings under Wireless Menu

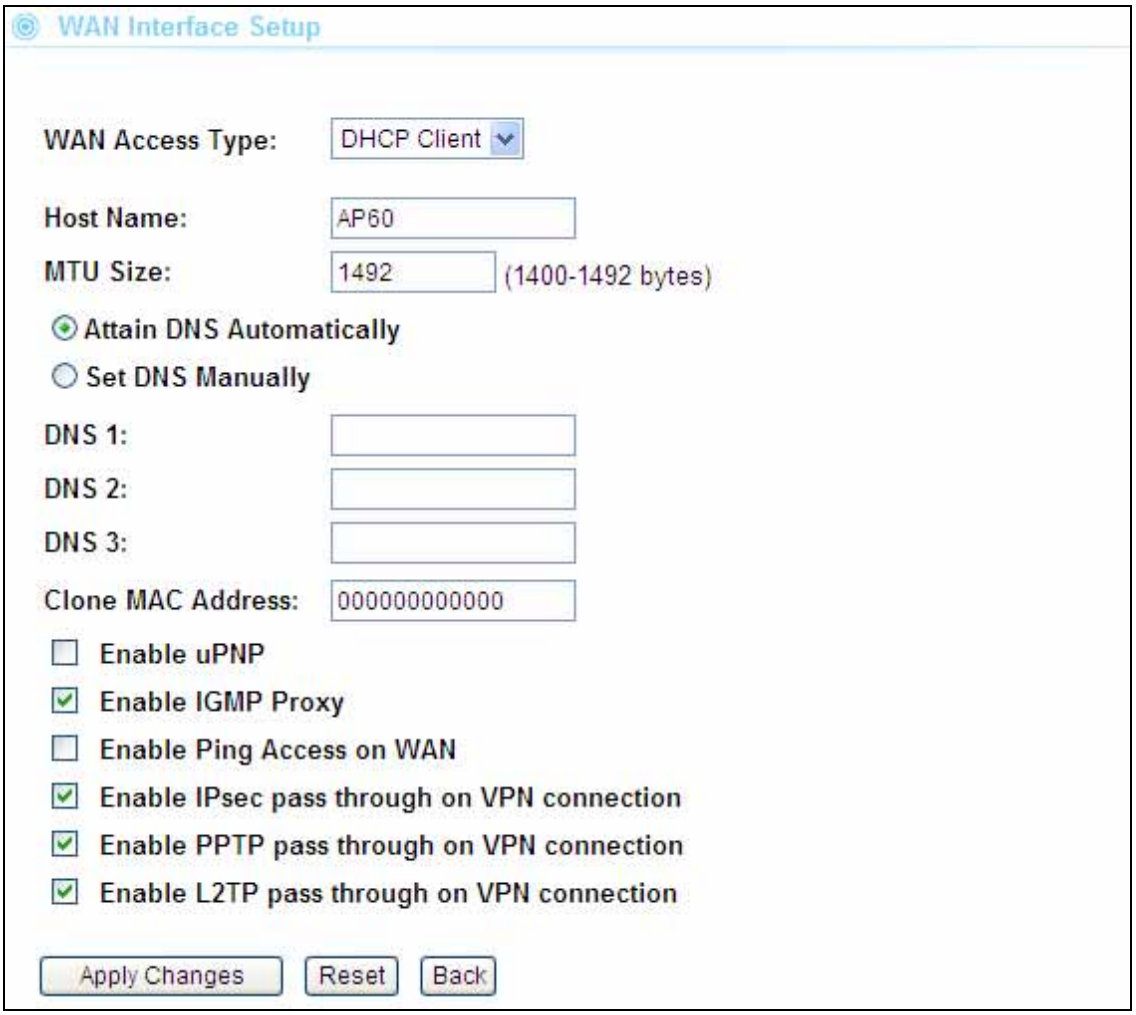
When you choose AP Router, WISP Router, or WISP + Universal modes; the Wireless Setting page will feature router mode functions as indicated on the image below.


Wireless Settings
Disable Wireless LAN Interface
Regulatory Domain: ETSI(Europe)
Band: 2.4 GHz (B+G+N) Multiple AP
SSID: airlive Site Survey
Channel Width: 20/40MHz
Control Sideband: Upper
Channel Number: 11
Broadcast SSID: Enabled
WMM: Enabled
Data Rate: Auto
Wireless Client Limit: Auto
Security: Setup
WPS: Setup
Advanced Settings: Setup
Bandwidth Control: Setup
Access Control: Setup
WAN Port: Setup
Virtual Servers: Setup
DMZ: Setup
Dynamic DNS: Setup
DoS Settings: Setup
URL Filtering: Setup
MAC Filtering: Setup
IP Filtering: Setup
Port Filtering: Setup
Routing: Setup
Remote Management: Setup
All LED off
Apply Changes
Reset

5.1.1 WAN Port

Operation Mode -> Setup -> WAN Port

The AP60 support different authentication and IP assignment standards for the WAN port. It includes fixed IP, DHCP, PPPoE, PPTP, L2TP, and Big Pond protocols. Please consult with your ISP about what authentication type is used for the WAN port connection.



- **Clone MAC Address**: In this place, you can assign a MAC address for the WAN port. In case of WISP mode, it is Radio1's MAC address. For Gatway mode, it is the WAN/LAN1 MAC address.
- **Enable UPnP:** Check this field will enable Universal Plug n Play protocol
- **Enable Web Server Access on WAN:** Check this field will enable remote management from WAN side.

5.1.2 Virtual Server Settings

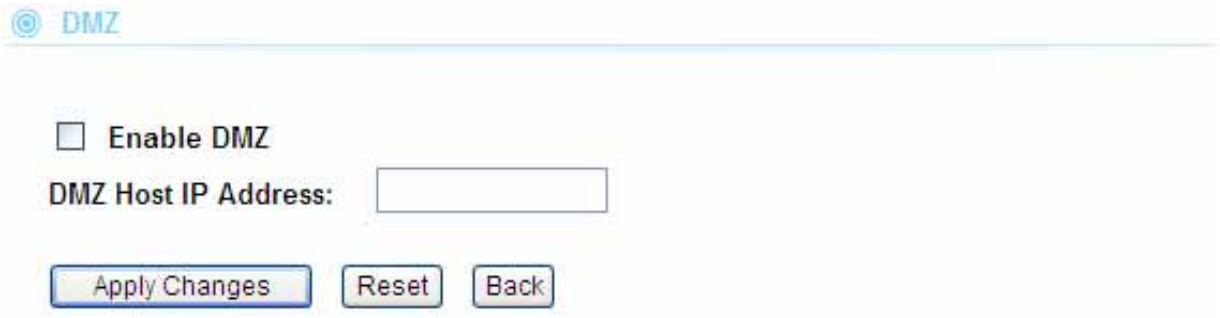
Virtual server allows you to specify one or more applications running on server computers on the LAN that may be accessed by any Internet user. Internet data destined for the specified public port will be directed to the specified private port number on the LAN client with the specified private IP address.

If you want to allow your web server, ftp server, or email server to be accessible from Internet, you would need to open specific port on the virtual server to your local IP address.

For a list of most frequent used TCP and UDP ports. Please visit
http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

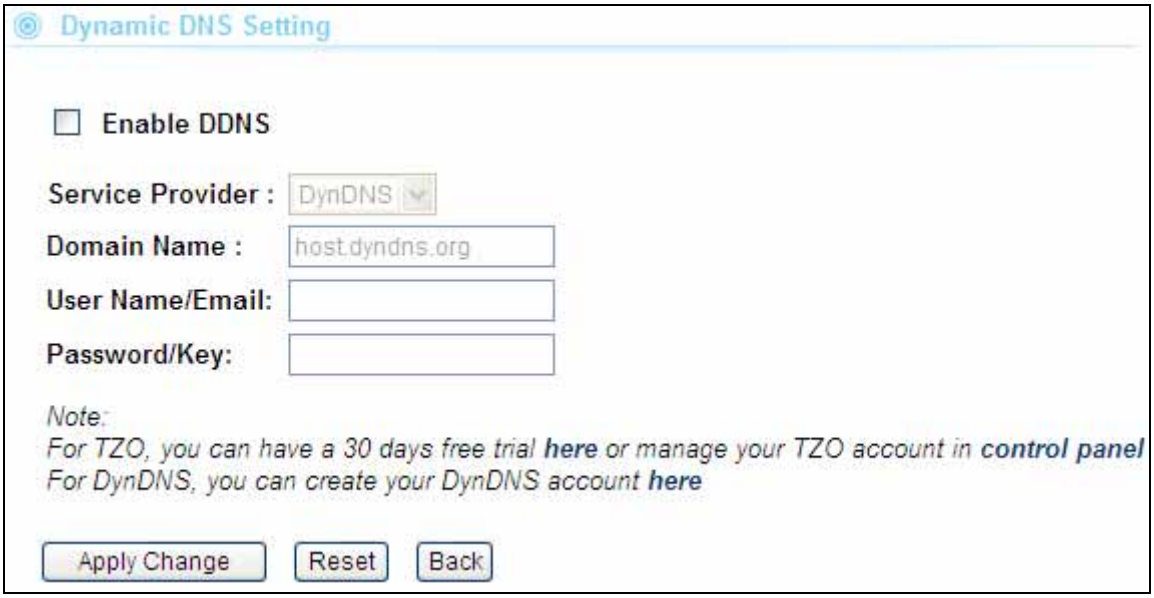
5.1.3 DMZ

DMZ opens all TCP/UDP ports to particular IP address on the LAN side. It allows setting up servers behind the AP60.



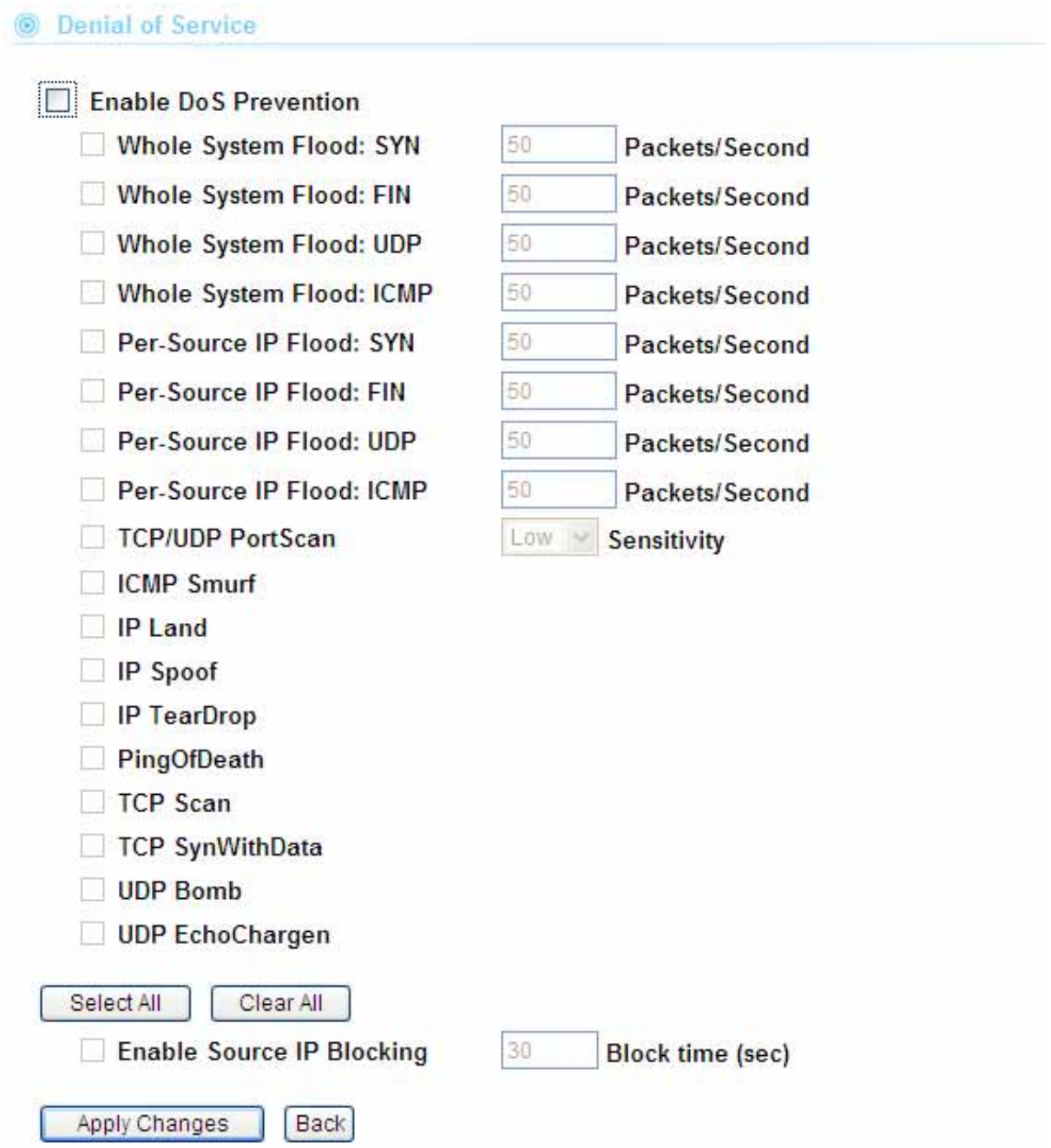
5.1.4 Dynamic DNS

Dynamic Domain Name System. An algorithm allows the use of dynamic IP address for hosting Internet Server. A DDNS service provides each user account with a domain name. The AP60 support “Dyndns” and “TZO” service.



5.1.5 DoS (Denial of Service)

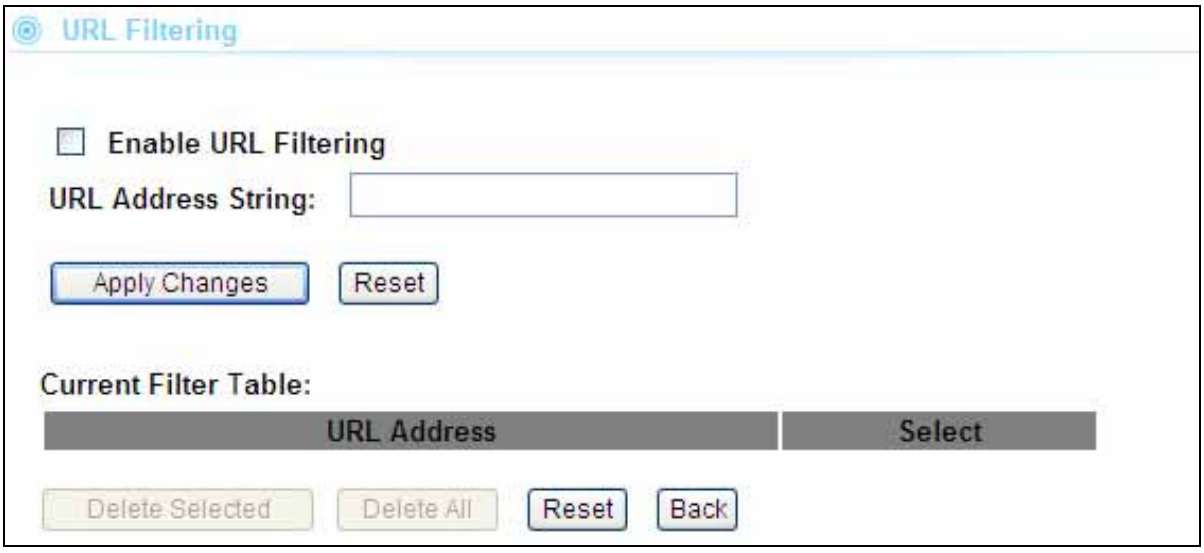
Denial of Service is a type of network attack that floods the network with useless traffic. Many DoS attacks, such as the Ping of Death and Teardrop attacks, exploit limitations in the TCP/IP protocols.



5.1.6 URL Filter

The AP60 provide URL filter function to stop access to certain website. It is especially

useful for parents to stop children from accessing some websites.

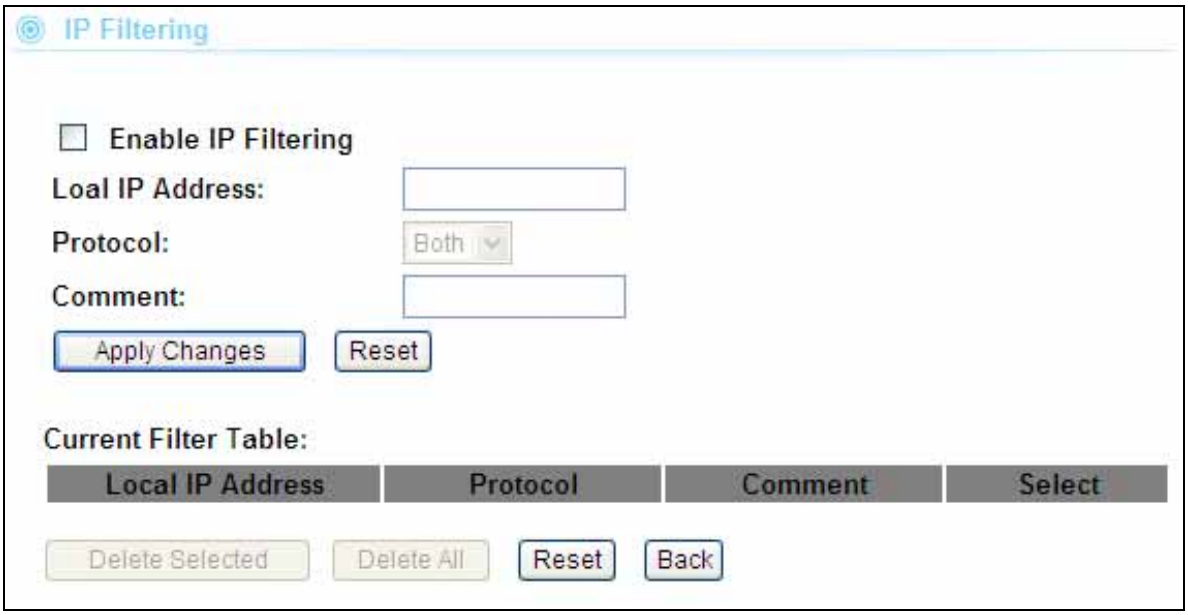


5.1.7 MAC Filter

MAC filter can filter out traffic from certain MAC addresses. It can prevent access to internet from certain station in the local LAN.

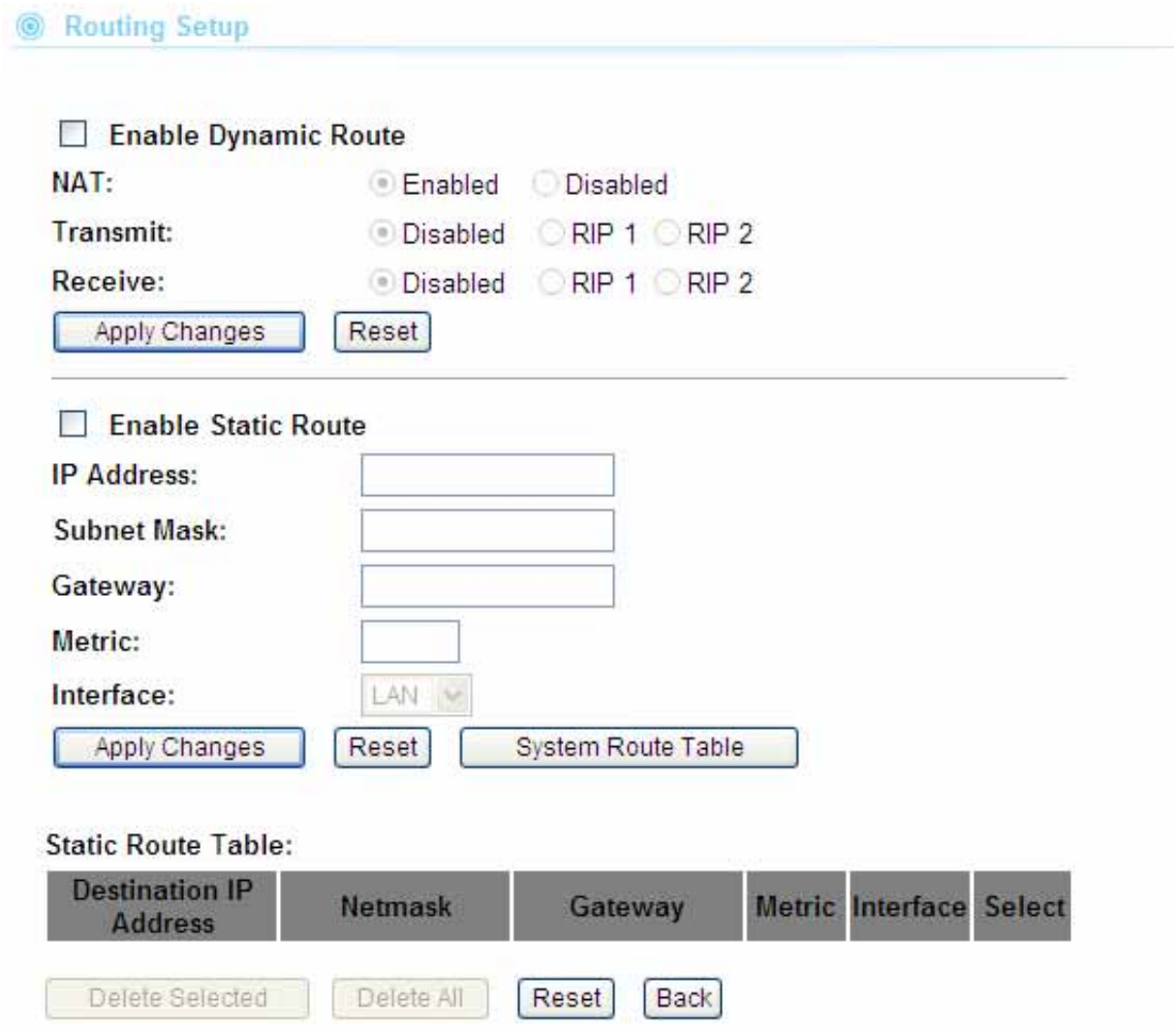
5.1.8 IP Filter

IP filtering allows you to block certain IP addresses from accessing the internet.



5.1.9 Routing

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



- **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.

- **Static Route 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.

5.1.10 Remote Management

You can enable the web management to allow the AP60 be managed from internet. You

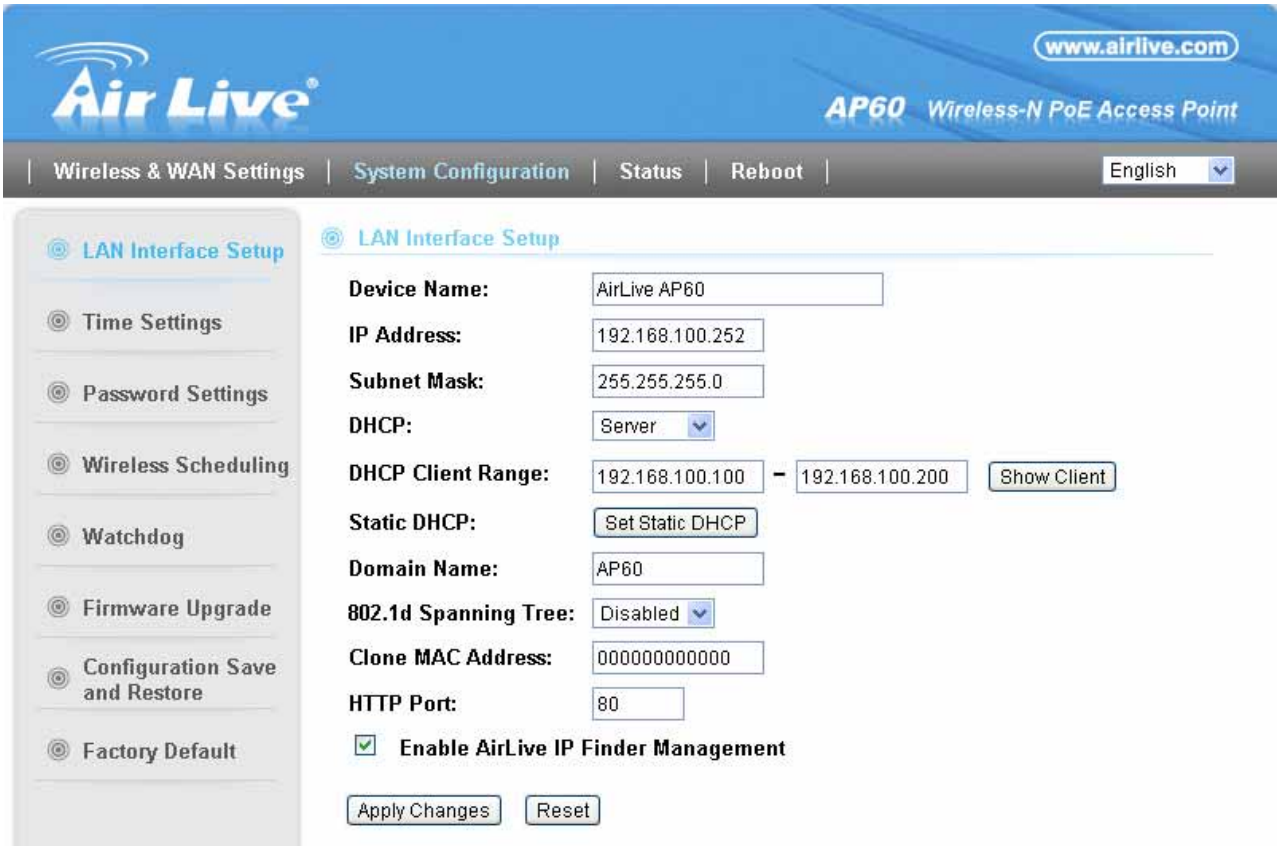
can change the management port number.

6 System Configurations

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

6.1 Menu Structure

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



6.2 LAN Interface Setup

System Configurations>> LAN Interface Setup

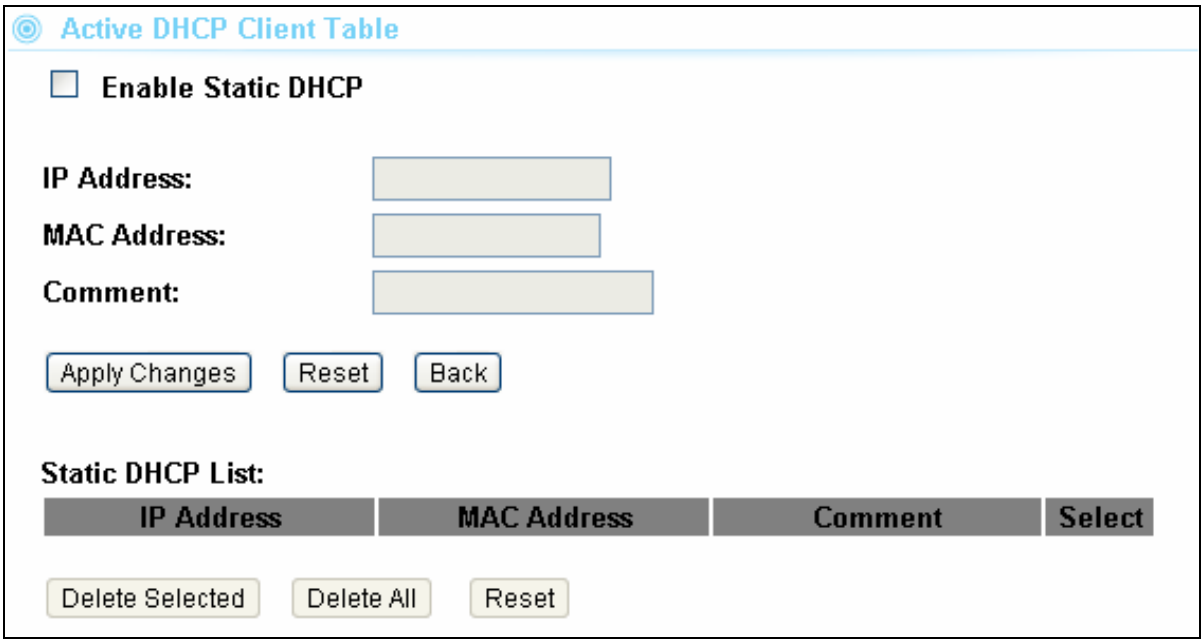
This menu is where you can configuration all the aspect about LAN interface including IP address, DHCP server settings etc.

6.2.1 DHCP Settings

- **DHCP Service:** You can enable or disable DHCP server here.
  - **Disable**: Disable DHCP server
  - **Client:** The LAN interface will get IP address from DHCP server
  - **Server (default):** The AP60 will act as DHCP server to provide IP addresses to the clients on the LAN/Wireless interface. By default, the DHCP server is on.
  - **DCHP Relay Agent**: This function should be chosen in Universal Repeater mode in order to assign IP address from remote DHCP server.

- **DHCP Client Range**: You can define the IP pool from which the DHCP clients can get IP address.. Click on “Show Clients” to see the current DHCP client table.
- **DHCP Release Time:** You can define how long the AP60 will reserve IP address for a particular PC or Device here.

6.2.2 Set Static DHCP



If you want to lock IP address to a MAC address, you should add DHCP clients to the “Static Lease Client”. Up to 40 entries can be entered. Below is the procedure for adding an entry:

1. Enter the MAC address of the device
2. Enter the IP address of the device
3. Click on the “Add” button

6.2.3 Domain Name

You can enter the network area name here.

6.2.4 802.11d Spanning Tree

Select Disabled or Enabled form the pull-down list.

6.2.5 Clone MAC Address

You can change the MAC address of your LAN port to other value here.

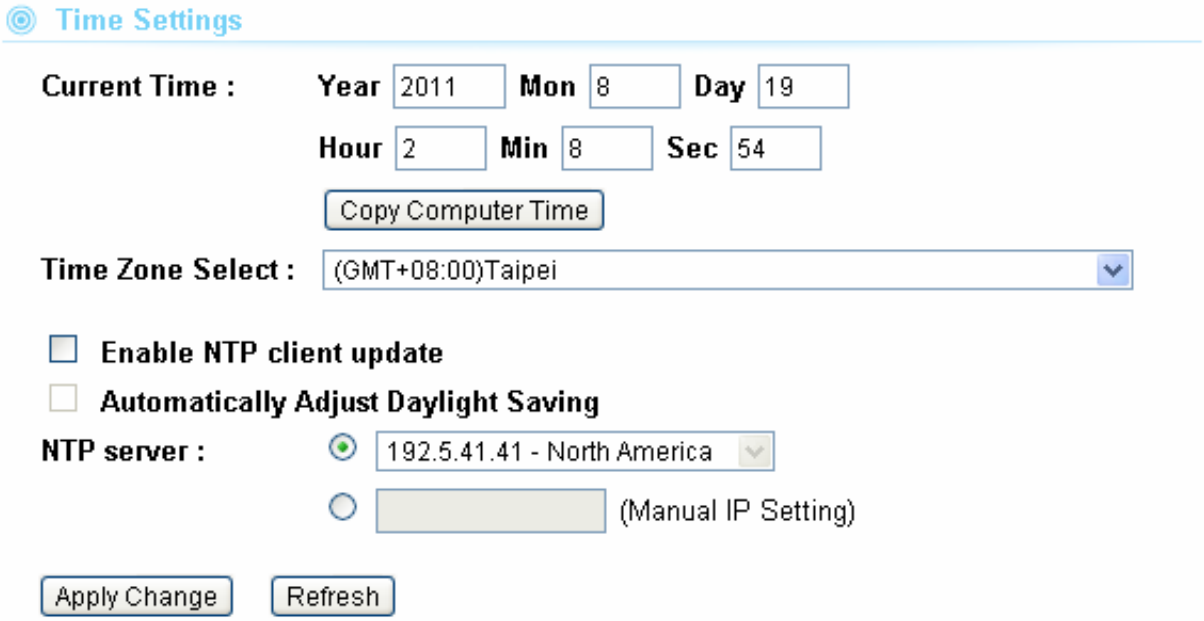
6.2.6 Enable AirLive IP Finder Management

By enabling the function, IP Finder could discover the AP60 in the LAN.

6.3 Time Settings

System Configuration ->Time Settings

You can set the NTP Time Server for your AP60's internal clock here. You can use NTP server function so your AP60 will check with NTP to set time automatically upon each startup. Thus, it prevents the clock losing track of time during reboot or power outage.



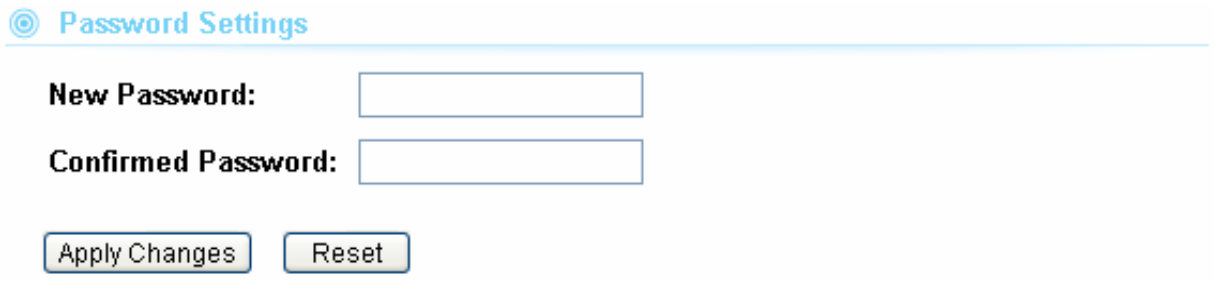
Below is the procedure to set your NTP server

1. Check the "Enable NTP Client Update"
2. Select your time Zone
3. Select your NTP server
4. Click on "Apply Change"

6.4 Password Settings

System Configuration -> Password Settings

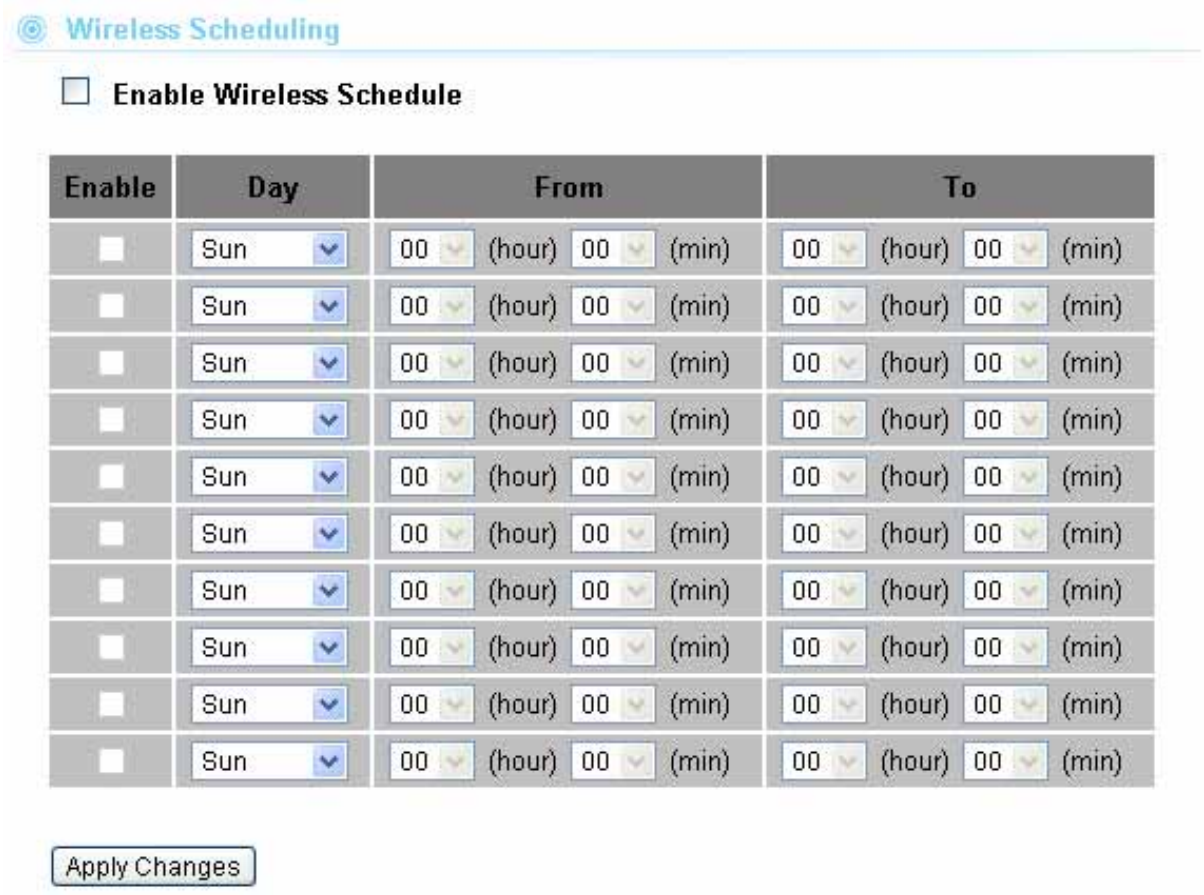
The AP60's password protection is turned off by default. To enable password protection or change password, just enter your username and password, and click on "Apply Change" button.



6.5 Wireless Scheduling

System Configuration -> Wireless Scheduling

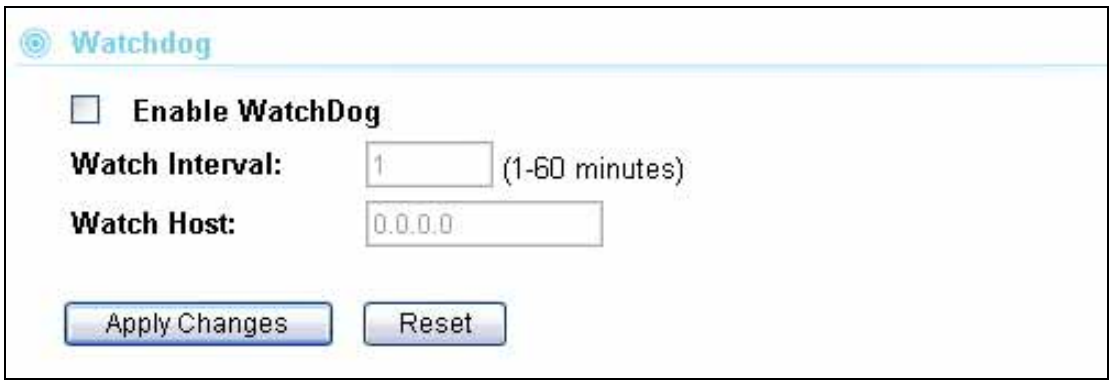
Check the box to enable the schedule function. Set up the time to schedule the wireless access rule. Select the day and time you want to enable the wireless function.



6.6 Watchdog

System Configuration -> Watchdog

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



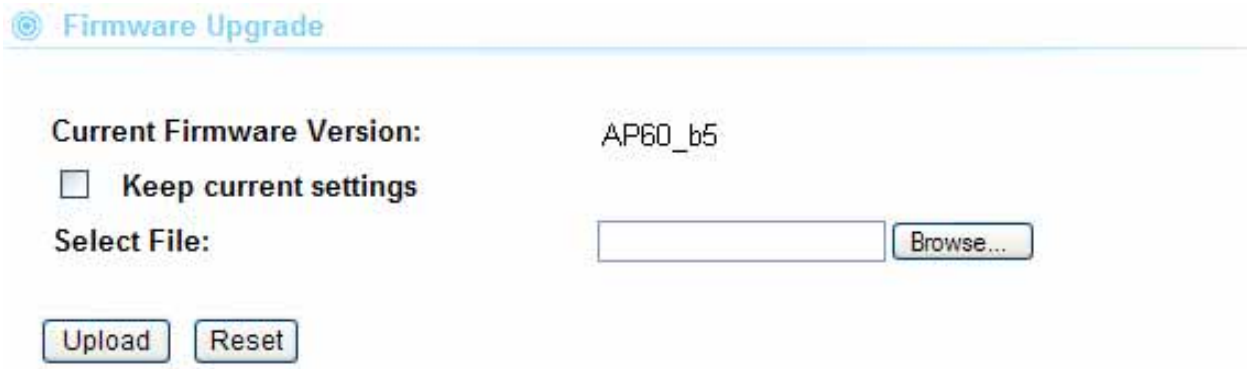
- **Watch Interval:** means: "How often the AP60 will PING". For example, it will PING once every "1" minute.

- **Watch Host:** This is the IP address for which the Watchdog will ping.

6.7 Firmware Upgrade

System Configuration -> Firmware Upgrade

You can upgrade the firmware of your AP60 (the software that controls your AP60'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.



- **Upgrade Firmware:**

  To update the AP60 firmware, first download the firmware from AirLive web site to your local disk. 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.

  Please make sure to check the "Keep Settings" box if you want the settings to be kept after firmware upgrade.

  The new firmware will be loaded to your AP60. 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 AP60 unless the new firmware has new features you need or if it has a fix to a problem that you've encountered.

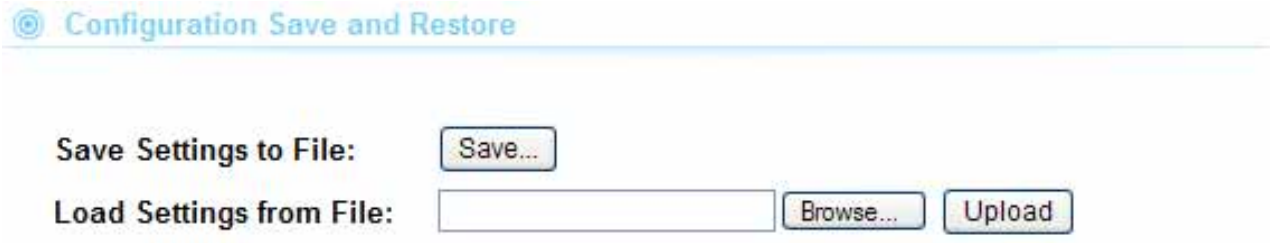
6.8 Configuration Save and Restore

System Configuration -> Configuration Save and Restore

The AP60 can save and restore the settings to a file. In addition, it has the unique capability to restore only the network or wireless settings. This makes changes of wireless settings across the entire network of AP much easier.

You can save system configuration settings to a file, and later download it back to the AP60 by following the steps.

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



Step 2 Click on "Save to" and Enter the path of the configuration file to save-to.

Restore Setting:

Step1: Enter the file name in the "Load Settings from File" field. Or click on "Browse" button to location the location of the file.

Step2: Click on "Upload" button to restore settings.

6.9 Factory Default

System Configuration -> Factory Default

You can reset the configuration of your AP60 to the factory default settings.

7 Device Status Menu

In this chapter, we will explain the “Device Status” menu in the web management interface. Before you read this chapter, please make sure to read through chapter 3 on “Introduction to Web Management Interface.

7.1 Menu Structure

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

7.2 Device Information

This page shows the general information about AP60 such as Uptime, Firmware version, Wireless Interface…etc. Below are some additional explanations on some status information of this page:

- **Device Name:** You can change AP60 device name in the column.
- **Uptime:** This displays the time since system last boot up. This is a good indication for how long the system has been alive.
- **Firmware version**: This place will display the current firmware version of your AP60. In general, AirLive will refer to its firmware as exx (such as e10) version on the release note
- **Wireless:** This page displays the current settings and status of the radio. It includes the BSSID and connection status. The BSSID is also the wireless MAC address that is needed for the WDS entry.

Wireless Configuration	
Mode	AP
Band	2.4 GHz (B+G+N)
SSID	airlive
Channel Number	11
Encryption	Disabled
BSSID	00:e0:4c:81:96:d1
Associated Clients	0

- **LAN Configuration:** This page displays the status of the LAN port such as MAC address, DHCP status.

TCP/IP Configuration	
Attain IP Protocol	Fixed IP
IP Address	192.168.100.252
Subnet Mask	255.255.255.0
DHCP Server	Enabled
MAC Address	00:e0:4c:81:96:d1

- **Internet Configuration:** Internet configuration tells you the current status of WAN port such as IP address, WAN Type and connection status.

WAN Configuration

Attain IP Protocol	DHCP
IP Address	192.168.1.105
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
MAC Address	00:e0:4c:81:96:d9

7.3 Statistic

This page shows the sent and received packet information for Radio1, Radio2, LAN, and WAN interface.

Statistics

Wireless LAN	Sent Packets	1
	Received Packets	752
Ethernet LAN	Sent Packets	3807
	Received Packets	3892
Ethernet WAN	Sent Packets	3141
	Received Packets	3489

Refresh

7.4 Client Table

It will show all wireless device connected to the AP60. It will show the packet sent and received. Whether the wireless client is using power saving mode and the signal strength level (in percentage from 0 to 100).

Client Table

MAC Address	Mode	Tx Packet	Rx Packet	Tx Rate (Mbps)	Power Saving	Signal
00:21:00:b1:43:3c	11g	5	235	54	no	68

Refresh

7.5 Log

The log function is where you can check for error messages for diagnostic purpose.

- **Enable Log: Check this box to enable log function.**
- **System All**: Activates all logging functions
- **Wireless**: Only logs related to the wireless LAN will be recorded
- **DoS**: Only logs related to the DoS protection will be recorded.
- **Enable Remote Log**: Only logs related to the Remote control will be recorded.
- **Log Server IP Address**: Only logs related to the server will be recorded.

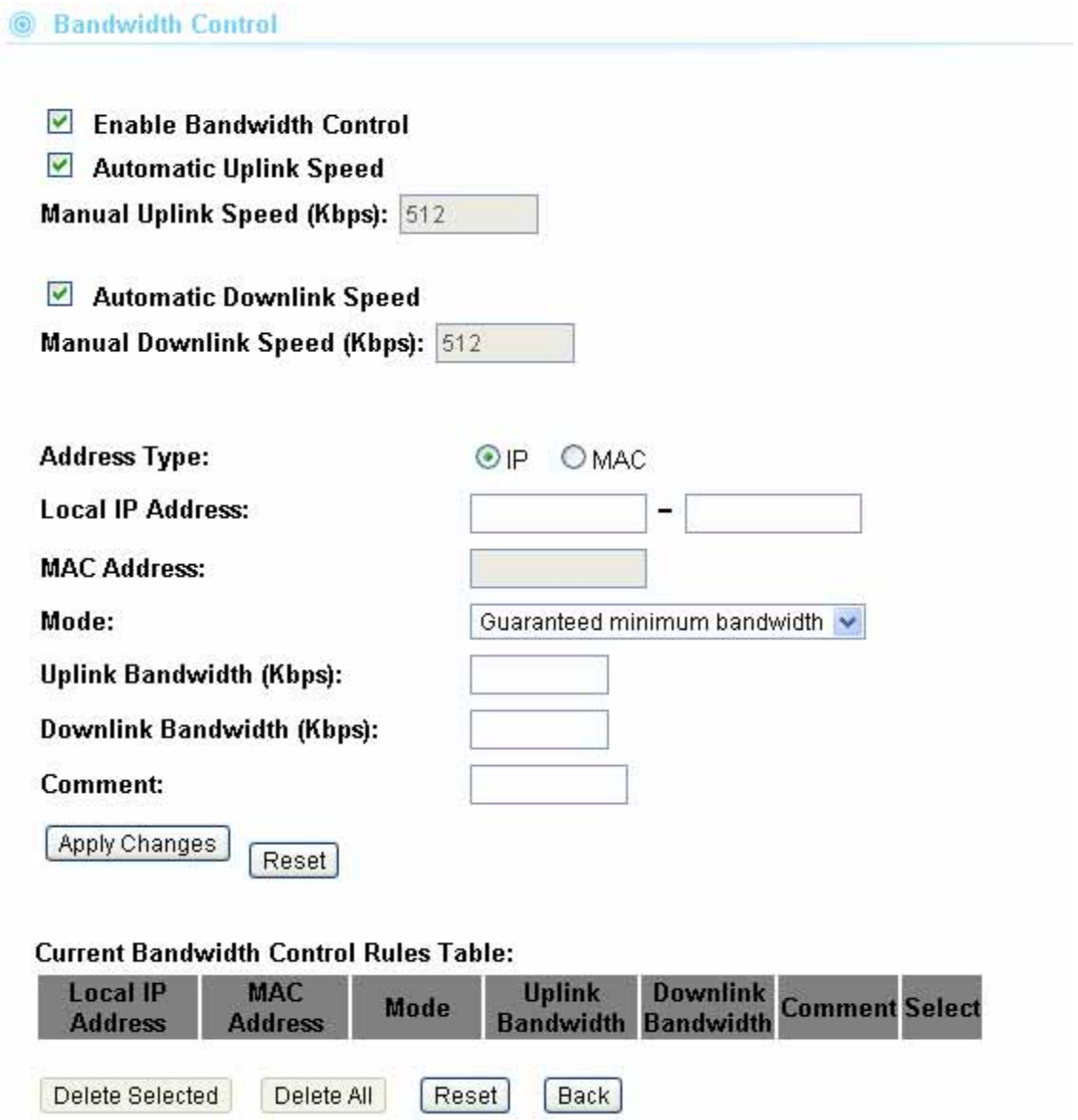
.

8 Bandwidth Control

In this chapter, you will learn how to utilize AP60's Bandwidth Control function. The Bandwidth Control settings can be found in the "Wireless Settings" page on the AP60's web management.

8.1 What is Bandwidth Control?

Bandwidth Control is a great tool to control the bandwidth of the WISP subscribers. Therefore, the WISP operator can offer different class of connection speeds for different subscription fees-Just like the ADSL service! The AirLive advanced firmware It can also guarantee the speed of certain application or priviledged IP address

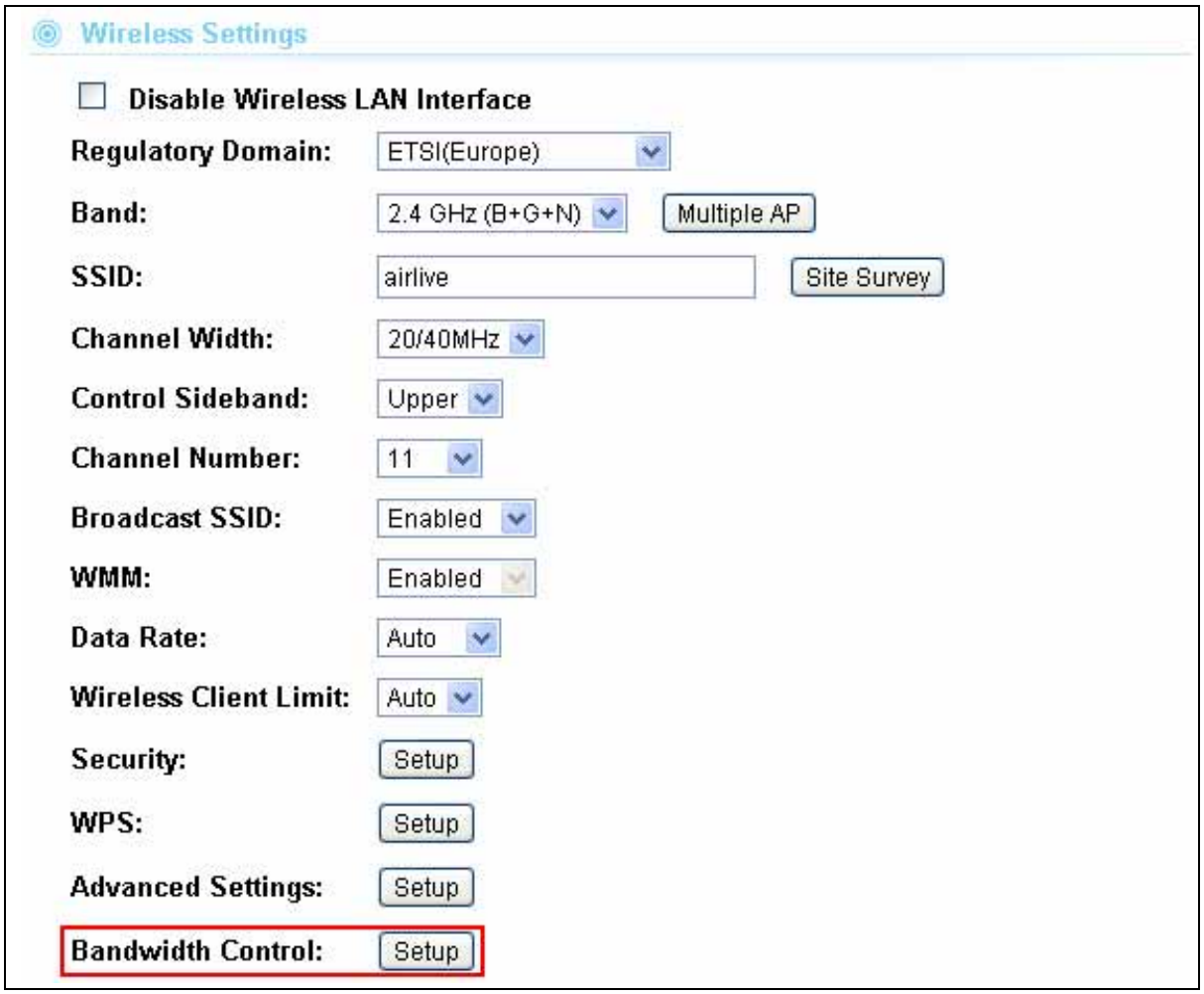


- **Enable Bandwidth Control**: Enable this function can limit the Internet connection speed of individual IP or Application. It can also guarantee the speed of certain special application or privileged IP address.
- **Automatic Uplink/Download Speed**: Check the box to enable the automatic uplink/ download speed function.
- **Manual Uplink/Download Speed**: You can manually enter the uplink/ download transmission rate in the blank field.
- **Address Type**: Select IP or MAC address type.
- **Local IP Address/MAC Address**: Depend on the address type that selected, user can enter the IP address or MAC address of client to set up the bandwidth of the transmission.

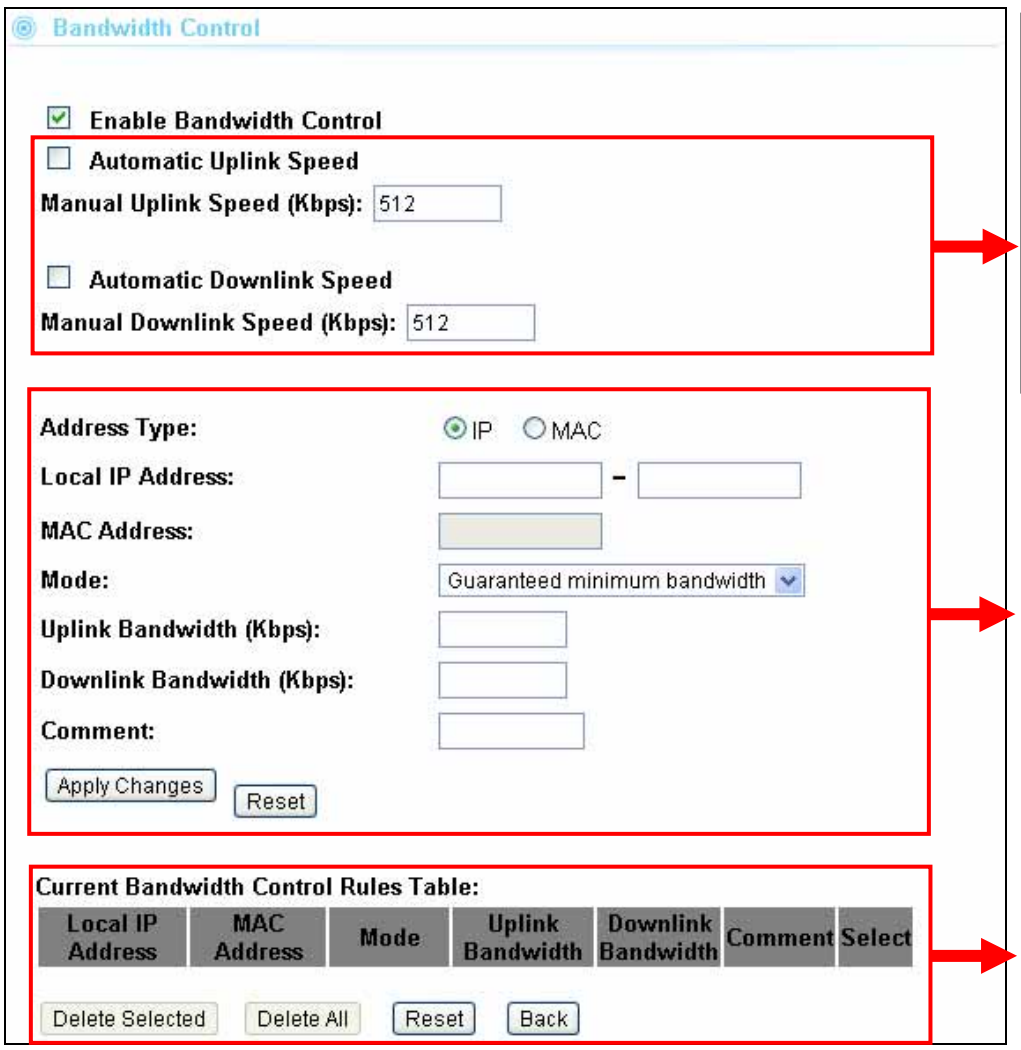
- **Mode**: Select Guaranteed minimum bandwidth or Restricted maximum bandwidth modes.
- **Uplink Bandwidth (Kbps)**: Enter the Uplink Bandwidth (Kbps) in the column.
- **Downlink Bandwidth (Kbps)**: Enter the Downlink Bandwidth (Kbps) in the column.
- Comment: Enter the note for the setting.

8.2 Configure the Bandwidth Control

From the Wireless Setting page, please choose the “Bandwidth Control”



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



This section is the "Interface Control" session. The user which is not in the bandwidth control rules table would be limited. You can uncheck the box and enter the speed manually

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

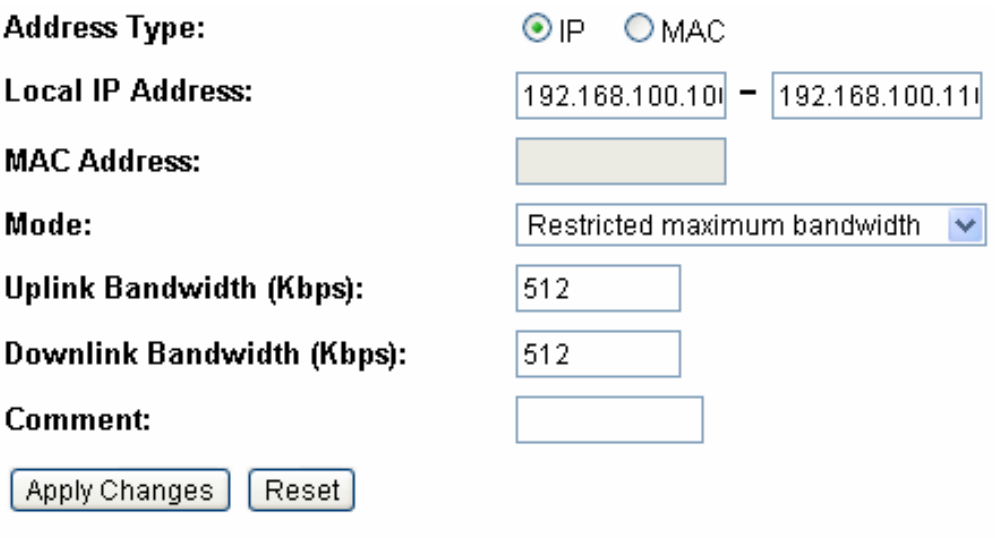
This section shows the IP Address and MAC Address which are controlled.

8.2.1 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 Bandwidth Control:

1. Configure Address Type to IP.



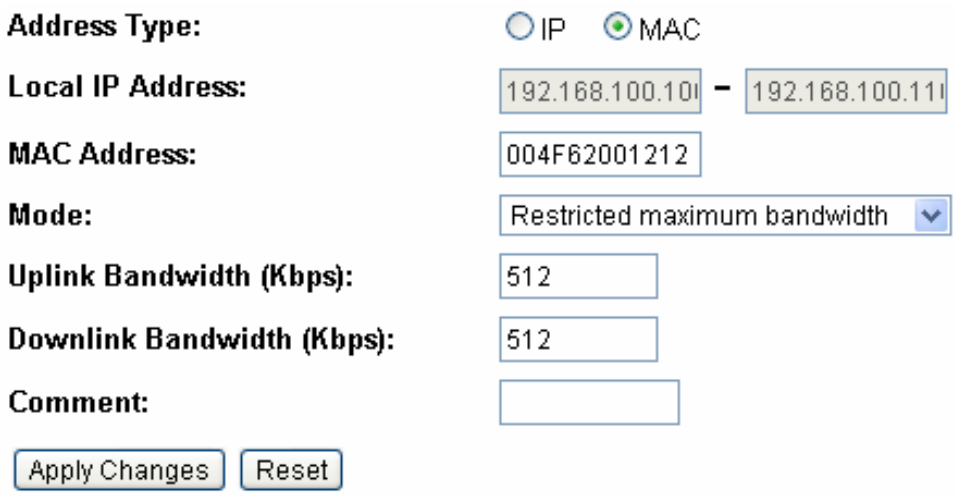
2. Enter the Local IP Address Ranges which will be limited.
3. Select the control mode by pull-down bar.
4. Enter the Uplink/Download Bandwidth.
5. Click Apply Changes to save settings.
6. Reboot your AP.

8.2.2 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 Bandwidth Control:

1. Configure Address Type to MAC.
2. Enter the Local IP Address Ranges which will be limited.
3. Select the control mode by pull-down bar.



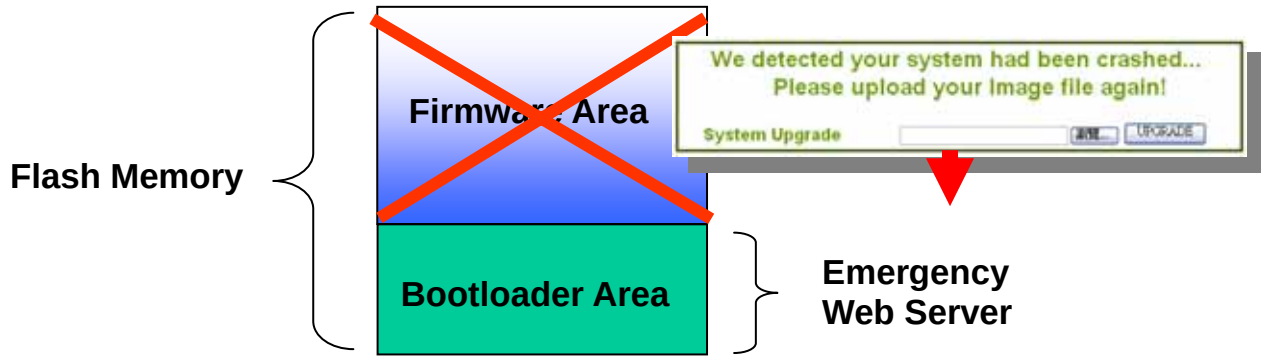
4. Enter the Uplink/Download Bandwidth.
5. Click Apply Changes to save settings.
6. Reboot your AP.

9 Emergency Firmware Recovery

The AP60 features emergency firmware upgrade function that can restore your AP from a firmware crashed. If you can't access your AP anymore, please first try to restore the setting to default by holding the RESET button (in the back) for more than 10 seconds. You should be able to find the AP at 192.168.100.252. If you can't find it, then please perform the emergency upgrade.

9.1 How Emergency Upgrade Works?

AP60's flash memory is divided into "firmware" and "bootloader" area. The bootloader area is protected from writing and has a built-in emergency web server. Therefore, the AP can be recovered from emergency web server after a firmware crash. The emergency web server is enabled when AP is forced into emergency upgrade mode, it's IP will be changed to ***192.168.1.6***.

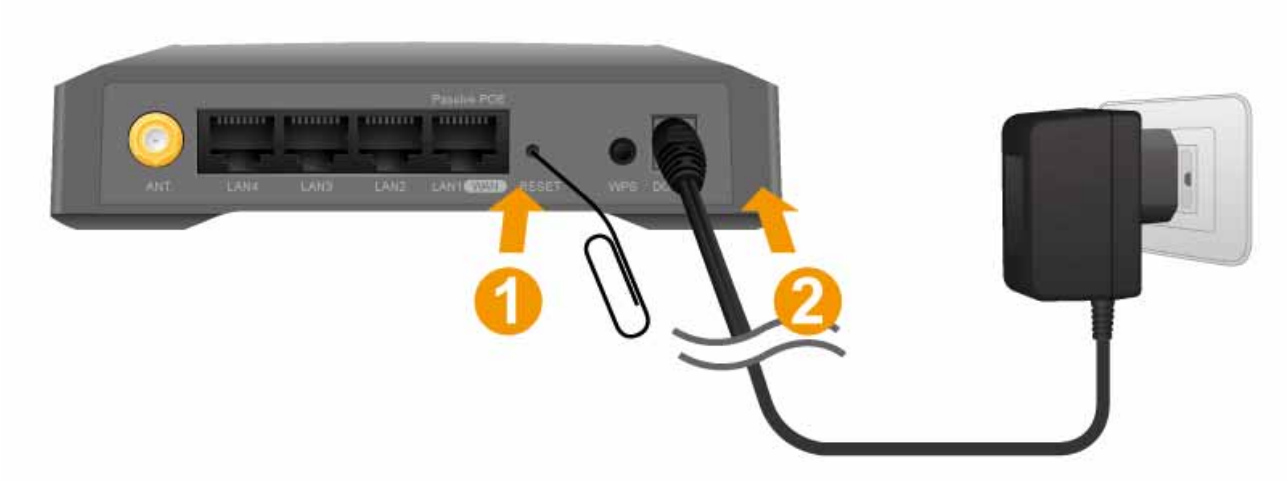


9.2 Emergency Upgrade Procedure

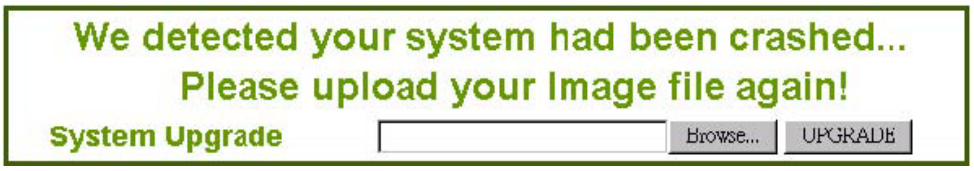
1. Please connect one of your LAN Ports (LAN1~LAN4) to your PC directly.

2. Set your PC's IP address to 192.168.1.100

3. Before connecting the power, please press and holding the "Reset" button (in the back of the AP). Then plug in the power. Keep press and hold the Reset button until the LED of the selected port goes on(about 3 seconds)



4. Open a browser; type "192.168.1.6" for the website address. The following screen should show up



5. Click the "Browse" button, select and open the correct firmware file. Please go to www.airlive.com to AP60's support page and download.

6. Click on "UPGRADE" button. Do not touch the AP or PC until the upgrade is completed.

7. Wait for AP to finish reboot.

8. Set you PC's IP Address to 192.168.100.100.

9. Open the web browser, and type "192.168.100.252". You should be able to login into the normal Web UI.

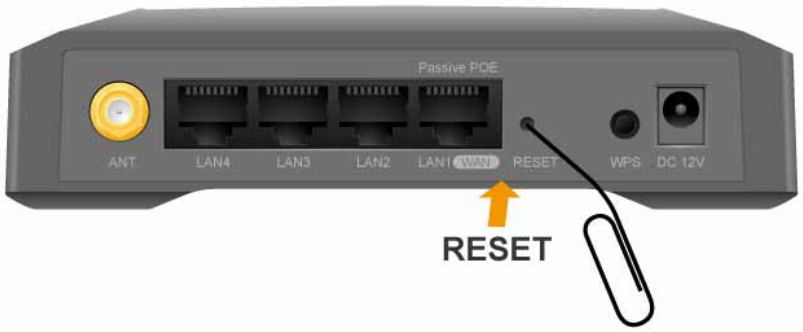
10 Frequent Asked Questions

In this chapter, we will address some frequent asked questions about AP60

==========

Question: I forgot my password or the IP address of AP60.

Answer: Please restore your settings to default by press the reset button for more than 5 seconds. You should be able to find your AP60 at 192.168.1.1 with default username “admin” and password “airlive”.



==========

Question: Why is my settings unchanged after pressing the “Apply” button?

Answer: Please reboot your AP60 after all the settings are changed.

==========

Question: When I plug in the POE cable and power adapter, the AP60’s power LED is not on?

Answer: Please make sure you have connected the PoE cable to the correct port on the DC injector. Moreover, you should use an Ethernet cable with 4 twisted pairs (CAT5 or better) for POE cable.

==========

==========

Question: When I use an external antenna, how much distance can the AP60 reach?

Answer: The distance of a wireless connection depends on many factors such as cable loss and weather conditions. There is an online distance calculator at the AirLive website. The distance calculated is not a guaranteed value; it is for your reference only. If you agree with this limitation, please visit http://www.airlive.com/support/wireless_distance_calculator.jsp

==========

Question: When I wan to use "Site Survey" tool to connect with a AP that has no encryption, why does the AP60 report "encryption type mismatch!" and ask me to configure the wireless security settings?

Answer: When you press "Connect" from site survey, the AP60 will first check if the current wireless encryption setting is correct. If not, it will ask you to modify the setting. Therefore, if your current wireless settings has encryption and the new AP you want to associate does not use encryption, then the AP60 will report the mismatch. In this case, simple select "Disable" in the encryption field and press "Apply Change".

==========

Question: Where is the signal survey function that displays the Signal Strength value continuously?

Answer: The "Signal Survey" function is inside the Site Survey function. You can access from "*Wireless Settings -> Site Survey*" menu.

==========

Question: Where is the POE port for AP60?

Answer: The PoE system used for AP60 is 12~24V Passive PoE. LAN1 is also used as the passive PoE port.

==========

11 Specifications

The specification of AP60 is subject to change without notice. Please use the information with caution.

11.1 Hardware Features

11.1.1 General Hardware Feature

- 802.11b/g/n Radio
- 4MB Flash, 32MB SDRAM
- RoHS compliant
- One 10/100 Mbps Ethernet Port / PoE Port with Auto MDI/MDI-X support
- 12V~24V Passive PoE port (LAN1)

11.1.2 Power Supply

- Power Adapter Voltage : input 100~240Vac/50~60Hz , output 12V/1A
- Advance Passive PoE (Accept 12 volts). Passive PoE DC Injector not included

11.1.3 Dimension and Weight

- Dimension: 137 x 88 x 30 mm
- Package Weight: 151g

11.2 Radio Specifications

11.2.1 Frequency Band

- USA (FCC) 11 Channels: 2.412GHz~2.462GHz
- Europe (ETSI) 13 Channels : 2.412GHz~2.472GHz
- South America 14 channels: 2.412GHz~2.484GHz

11.2.2 Rate and Modulation

- Data Rate:
  - 802.11n
    - 20 MHz BW(LGI): 65, 58.5, 52, 39, 26, 19.5, 13, 6.5
    - 40 MHz BW(LGI): 135, 121.5, 108, 81, 54, 40.5, 27, 13.5
    - 20 MHz BW(SGI): 72.2, 65, 57.8, 43.3, 28.9, 21.7, 14.4, 7.2
    - 40 MHz BW(SGI): 150, 135, 120, 90, 60, 45, 30, 15
  - 802.11g: 54, 48, 36, 24, 18, 12, 9 and 6 Mbps
  - 802.11b: 11, 5.5, 2 and 1 Mbps
- Modulation
  - 802.11n
    - 20 MHz BW(LGI): 65, 58.5, 52, 39, 26, 19.5, 13, 6.5
    - 40 MHz BW(LGI): 135, 121.5, 108, 81, 54, 40.5, 27, 13.5
    - 20 MHz BW(SGI): 72.2, 65, 57.8, 43.3, 28.9, 21.7, 14.4, 7.2
    - 40 MHz BW(SGI): 150, 135, 120, 90, 60, 45, 30, 15
  - 802.11g: 54, 48, 36, 24, 18, 12, 9 and 6 Mbps
  - 802.11b: 11, 5.5, 2 and 1 Mbps

11.2.3 TX Output Power

- ETSI (Europe)
  - About 20dBm max
- FCC (The United States)

- About 23dBm max
- South America
  - About 29dBm max

11.2.4 Supported WLAN Mode

- 802.11n/g/b Auto
- 802.11n/g Auto
- 802.11g/b Auto
- 802.11n only
- 802.11g only
- 802.11b only

11.3 Software Feature

11.3.1 Operation Mode

- Access Point Mode (AP mode)
- Client Mode (Infrastructure and Adhoc)
- WDS Bridge Mode
- WDS Repeater Mode
- Universal Repeater Mode
- WISP Router Mode
- WISP + Universal Mode
- AP Router Mode
- WDS Station Mode

11.3.2 Management Interface

- Web HTTP

11.3.3 Advance Functions

- Site Survey with RSSI Signal Survey
- Total Bandwidth and Per-User Bandwidth Management
- Multiple SSID
- QoS (802.11e WMM)
- Wi-Fi, WPA compatible interoperability
- WPA with PSK/TKIP/AES support ,WPA2 support
- Privacy Separator support
- Support adjustable output power
- 152-bit WEP support (Atheros Proprietary)
- ACK Timeout Adjustment
- Bootloader Protection and Emergency Firmware Upload Code
- Radius Supported
- Firmware upgrade and configuration backup via Web

12 Wireless Network Glossary

The wireless network glossary contains explanation or information about common terms used in wireless networking products. Some of information in this glossary might be outdated, please use with caution.

802.3ad
802.3ad is an IEEE standard for bonding or aggregating multiple Ethernet ports into one virtual port (also known as trunking) to increase the bandwidth.

802.3af
This is the PoE (Power over Ethernet) standard by IEEE committee. 803.af uses 48V POE standard that can deliver up to 100 meter distance over Ethernet cable.

802.11b
International standard for wireless networking that operates in the 2.4 GHz frequency band (2.4 GHz to 2.4835 GHz) and provides a throughput up to 11 Mbps.

802.1d STP
Spanning Tree Protocol. It is an algorithm to prevent network from forming. The STP protocol allows net work to provide a redundant link in the event of a link failure. It is advise to turn on this option for multi-link bridge network.

802.11d
Also known as “Global Roaming”. 802.11d is a standard for use in countries where systems using other standards in the 802.11 family are not allowed to operate.

802.11e
The IEEE QoS standard for prioritizing traffic of the VoIP and multimedia applications. The WMM is based on a subset of the 802.11e.

802.11g
A standard provides a throughput up to 54 Mbps using OFDM technology. It also operates in the 2.4 GHz frequency band as 802.11b. 802.11g devices are backward compatible with 802.11b devices.

802.11i

The IEEE standard for wireless security. 802.11i standard includes TKIP, CCMP, and AES encryption to improve wireless security. It is also know as WPA2.

802.1x

802.1x is a security standard for wired and wireless LANs. In the 802.1x parlance, there are usually supplicants (client), authenticator (switch or AP), and authentication server (radius server) in the network. When a supplicants request a service, the authenticator will pass the request and wait for the authentication server to grant access and register accounting. The 802.1x is the most widely used method of authentication by WISP.

Adhoc

A Peer-to-Peer wireless network. An Adhoc wireless network do not use wireless AP or router as the central hub of the network. Instead, wireless client are connected directly to each other. The disadvantage of Adhoc network is the lack of wired interface to Internet connections. It is not recommended for network more than 2 nodes.

Access Point (AP)

The central hub of a wireless LAN network. Access Points have one or more Ethernet ports that can connect devices (such as Internet connection) for sharing. Multi-function Access Point can also function as an Ethernet client, wireless bridge, or repeat signals from other AP. Access Points typically have more wireless functions comparing to wireless routers.

ACK Timeout

Acknowledgement Timeout Windows. When a packet is sent out from one wireless station to the other, it will waits for an Acknowledgement frame from the remote station. The station will only wait for a certain amount of time, this time is called the ACK timeout. If the ACK is NOT received within that timeout period then the packet will be re-transmitted resulting in reduced throughput. If the ACK setting is too high then throughput will be lost due to waiting for the Ack Window to timeout on lost packets. If the ACK setting is too low then the ACK window will have expired and the returning packet will be dropped, greatly lowering throughput. By having the ability to adjust the ACK setting we can effectively optimize the throughput over long distance links. This is especially true for 802.11a and 802.11g networks. Setting the correct ACK timeout value need to consider 3 factors: distance, AP response time, and interference. The AP60 provide ACK adjustment capability in form of either distance or direct input. When you enter the distance parameter, the AP60 will automatically calculate the correct ACK timeout value.

Bandwidth Management (Bandwidth Control)
Bandwidth Management controls the transmission speed of a port, user, IP address, and application. Router can use bandwidth control to limit the Internet connection speed of individual IP or Application. It can also guarantee the speed of certain special application or privileged IP address - a crucial feature of QoS (Quality of Service) function.

Bootloader
Bootloader is the under layering program that will start at the power-up before the device loads firmware. It is similar to BIOS on a personal computer. When a firmware crashed, you might be able to recover your device from bootloader.

Bridge
A product that connects 2 different networks that uses the same protocol. Wireless bridges are commonly used to link network across remote buildings. For wireless application, there are 2 types of Bridges. WDS Bridge can be used in Point-to-Point or Point-to-Multipoint topology. Bridge Infrastructure works with AP mode to form a star topology.

Cable and Connector Loss: During wireless design and deployment, it is important to factor in the cable and connector loss. Cable and connector loss will reduce the output power and receiver sensitivity of the radio at connector end. The longer the cable length is, the more the cable loss. Cable loss should be subtracted from the total output power during distance calculation. For example, if the cable and connector loss is 3dBm and the output power is 20dBm; the output power at the cable end is only 17dBm.

Client
Client means a network device or utility that receives service from host or server. A client device means end user device such as wireless cards or wireless CPE.

CPE Devices
CPE stands for Customer Premises Equipment. A CPE is a device installed on the end user's side to receive network services. For example, on an ADSL network, the ADSL modem/router on the subscriber's home is the CPE device. Wireless CPE means a complete Wireless (usually an AP with built-in Antenna) that receive wireless broadband access from the WISP. The opposite of CPE is CO.

CTS
Clear To Send. A signal sent by a device to indicate that it is ready to receive data.

DDNS
Dynamic Domain Name System. An algorithm that allows the use of dynamic IP address for hosting Internet Server. A DDNS service provides each user account with a domain name. A router with DDNS capability has a built-in DDNS client that updates the IP address information to DDNS service provider whenever there is a change. Therefore, users can build website or other Internet servers even if they don't have fixed IP connection.

DHCP
Dynamic Hosting Configuration Protocol. A protocol that enables a server to dynamically assign IP addresses. When DHCP is used, whenever a computer logs onto the network, it automatically gets an IP address assigned to it by DHCP server. A DHCP server can either be a designated PC on the network or another network device, such as a router.

DMZ
Demilitarized Zone. When a router opens a DMZ port to an internal network device, it opens all the TCP/UDP service ports to this particular device. The feature is used commonly for setting up H.323 VoIP or Multi-Media servers.

DNS
A program that translates URLs to IP addresses by accessing a database maintained on a collection of Internet servers.

Domain Name
The unique name that identifies an Internet site. Domain Names always have 2 or more parts, separated by dots. In www.airlive.com, the "airlive.com" is the doman name.

DoS Attack
Denial of Service. A type of network attack that floods the network with useless traffic. Many DoS attacks, such as the Ping of Death and Teardrop attacks, exploit limitations in the TCP/IP protocols.

Encryption
Encoding data to prevent it from being read by unauthorized people. The common wireless encryption schemes are WEP, WPA, and WPA2.

ESSID (SSID)
The identification name of an 802.11 wireless network. Since wireless network has no physical boundary liked wired Ethernet network, wireless LAN needs an identifier to distinguish one network from the other. Wireless clients must know the SSID in order to associate with a WLAN network. Hide SSID feature disable SSID broadcast, so users must know the correct SSID in order to join a wireless network.

Firewall
A system that secures a network and prevents access by unauthorized users. Firewalls can be software, router, or gateway. Firewalls can prevent unrestricted access into a network, as well as restricting data from flowing out of a network.

Firmware
The program that runs inside embedded device such as router or AP. Many network devices are firmware upgradeable through web interface or utility program.

FTP
File Transfer Protocol. A standard protocol for sending files between computers over a TCP/IP network and the Internet.

Fragment Threshold
Frame Size larger than this will be divided into smaller fragment. If there are interferences in your area, lower this value can improve the performance. If there are not, keep this parameter at higher value. The default size is 2346. You can try 1500, 1000, or 500 when there are interference around your network.

Gateway
In the global Internet network, the gateways are core routers that connect networks in different IP subnet together. In a LAN environment with an IP sharing router, the gateway is the router. In an office environment, gateway typically is a multi-function device that integrates NAT, firewall, bandwidth management, and other security functions.

Hotspot
A place where you can access Wi-Fi service. The term hotspot has two meanings in wireless deployment. One is the wireless infrastructure deployment, the other is the Internet access billing system. In a hotspot system, a service provider typically need an authentication and account system for billing purposes, and a wireless AP network to provide access for customers.

IGMP Snooping
Internet Group Management Protocol (IGMP) is a Layer 3 protocol to report IP multicast memberships to neighboring multicast switches and routers. IGMP snooping is a feature that allows an Ethernet switch to "listen in" on the IGMP conversation between hosts and routers. A switch support IGMP snooping has the possibility to avoid multicast traffic being treated as broadcast traffic; therefore, reducing the overall traffic on the network.

Infrastructure Mode
A wireless network that is built around one or more access points to provide wireless clients access to wired LAN / Internet service. The opposite of Infrastructure mode is Adhoc mode.

IP address
IP (Internet Protocol) is a layer-3 network protocol that is the basis of all Internet communication. An IP address is 32-bit number that identifies each sender or receiver of information that is sent across the Internet. An IP address has two parts: an identifier of a particular network on the Internet and an identifier of the particular device (which can be a server or a workstation) within that network. The new IPv6 specification supports 128-bit IP address format.

IPsec
IP Security. A set of protocols developed by the IETF to support secure exchange of packets at the IP layer. IPsec has been deployed widely to implement Virtual Private Networks (VPNs). IPsec supports two encryption modes: Transport and Tunnel. Transport mode encrypts only the data of each packet, but leaves the header untouched. The more secure Tunnel mode encrypts both the header and the payload. On the receiving side, an IPSec-compliant device decrypts each packet.

LACP (802.3ad) Trunking
The 802.3ad Link Aggregation standard defines how to combine the several Ethernet ports into one high-bandwidth port to increase the transmission speed. It is also known as port trunking. Both devices must set the trunking feature to work.

MAC
Media Access Control. MAC address provides layer-2 identification for Networking Devices. Each Ethernet device has its own unique address. The first 6 digits are unique for each manufacturer. When a network device have MAC access control feature, only the devices with the approved MAC address can connect with the network.

Mbps
Megabits Per Second. One million bits per second; a unit of measurement for data transmission

MESH
Mesh is an outdoor wireless technology that uses Spanning Tree Protocol (STP) and Wireless Distribution system to achieve self-forming, self-healing, and self-configuring outdoor network. MESH network are able to take the shortest path to a destination that does not have to be in the line of site.

MIMO
Multi In Multi Out. A Smart Antenna technology designed to increase the coverage and performance of a WLAN network. In a MIMO device, 2 or more antennas are used to increase the receiver sensitivity and to focus available power at intended Rx.

NAT
Network Address Translation. A network algorithm used by Routers to enables several PCs to share single IP address provided by the ISP. The IP that a router gets from the ISP side is called Real IP; the IP assigned to PC under the NAT environment is called Private IP.

Node
A network connection end point, typically a computer.

Packet
A unit of data sent over a network.

Passphrase
Used much like a password, a passphrase simplifies the WEP encryption process by automatically generating the WEP encryption keys for the company products.

POE
Power over Ethernet. A standard to deliver both power and data through one single Ethernet cable (UTP/STP). It allows network device to be installed far away from power source. A POE system typically compose of 2 main component: DC Injector (Base Unit) and Splitter (Terminal Unit). The DC injector combines the power and data, and the splitter separates the data and power back. A PoE Access Point or CPE has the splitter built-in to the device. The IEEE 802.3af is a POE spec that uses 48 volt to deliver power up to 100 meter distance.

Port

This word has 2 different meaning for networking.

- The hardware connection point on a computer or networking device used for plugging in a cable or an adapter.
- The virtual connection point through which a computer uses a specific application on a server.

PPPoE

Point-to- Point Protocol over Ethernet. PPPoE relies on two widely accepted standards: PPP and Ethernet. PPPoE is a specification for connecting the users on an Ethernet to the Internet through a common broadband medium, such as a single DSL line, wireless device or cable modem.

PPTP

Point-to-Point Tunneling Protocol: A VPN protocol developed by PPTP Forum. With PPTP, users can dial in to their corporate network via the Internet. If users require data encryption when using the Windows PPTP client, the remote VPN server must support MPPE (Microsoft Point-To-Point Encryption Protocol) encryption. PPTP is also used by some ISP for user authentication, particularly when pairing with legacy Alcatel / Thomson ADSL modem.

Preamble Type

Preamble are sent with each wireless packet transmit for transmission status. Use the long preamble type for better compatibility. Use the short preamble type for better performance

Rate Control

Ethernet switches' function to control the upstream and downstream speed of an individual port. Rate Control management uses "Flow Control" to limit the speed of a port. Therefore, the Ethernet adapter must also have the flow control enabled. One way to force the adapter's flow control on is to set a port to half-duplex mode.

RADIUS

Remote Authentication Dial-In User Service. An authentication and accounting system used by many Internet Service Providers (ISPs). When you dial in to the ISP, you must enter your username and password. This information is passed to a RADIUS server, which checks that the information is correct, and then authorizes access to the ISP system. Radius typically uses port 1812 and port 1813 for authentication and accounting port. Though not an official standard, the RADIUS specification is maintained by a working group of the IETF.

Receiver Sensitivity
Receiver sensitivity means how sensitive is the radio for receiving signal. In general; the slower the transmission speed, the more sensitive the radio is. The unit for Receiver Sensitivity is in dB; the lower the absolute value is, the higher the signal strength. For example, -50dB is higher than -80dB.

RJ-45
Standard connectors for Twisted Pair copper cable used in Ethernet networks. Although they look similar to standard RJ-11 telephone connectors, RJ-45 connectors can have up to eight wires, whereas telephone connectors have only four.

Router
An IP sharing router is a device that allows multiple PCs to share one single broadband connection using NAT technology. A wireless router is a device that combines the functions of wireless Access Point and the IP sharing router.

SIGNAL STRENGTH
Receiver Sensitivity Index. SIGNAL STRENGTH is a value to show the Receiver Sensitivity of the remote wireless device. In general, remote APs with stronger signal will display higher SIGNAL STRENGTH values. For SIGNAL STRENGTH value, the smaller the absolute value is, the stronger the signal. For example, “-50db” has stronger signal than “-80dB”. For outdoor connection, signal stronger than -60dB is considered as a good connection.

RTS
Request To Send. A packet sent when a computer has data to transmit. The computer will wait for a CTS (Clear To Send) message before sending data.

RTS Threshold
RTS (Request to Send). The RTS/CTS(clear to send) packet will be send before a frame if the packet frame is larger than this value. Lower this value can improve the performance if there are many clients in your network. You can try 1500, 1000 or 500 when there are many clients in your AP’s network.

SNMP
Simple Network Management Protocol. A set of protocols for managing complex networks. The SNMP network contains 3 key elements: managed devices, agents, and network-management systems (NMSs). Managed devices are network devices that content SNMP agents. SNMP agents are programs that reside SNMP capable device's firmware to provide SNMP configuration service. The NMS typically is a PC based software such as HP Openview that can view and manage SNMP network device remotely.

SSH
Developed by SSH Communications Security Ltd., Secure Shell is a program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. It provides strong authentication and secure communications over insecure channels. It is a replacement for rlogin, rsh, rcp, and rdist.

SSL
Secure Sockets Layer. It is a popular encryption scheme used by many online retail and banking sites to protect the financial integrity of transactions. When an SSL session begins, the server sends its public key to the browser. The browser then sends a randomly generated secret key back to the server in order to have a secret key exchange for that session. SSL VPN is also known as Web VPN. The HTTPS and SSH management interface use SSL for data encryption.

Subnet Mask
An address code mask that determines the size of the network. An IP subnet are determined by performing a BIT-wise AND operation between the IP address and the subnet mask. By changing the subnet mask, you can change the scope and size of a network.

Subnetwork or Subnet
Found in larger networks, these smaller networks are used to simplify addressing between numerous computers. Subnets connect to the central network through a router, hub or gateway. Each individual wireless LAN will probably use the same subnet for all the local computers it talks to.

TCP
A layer-4 protocol used along with the IP to send data between computers over the Internet. While IP takes care of handling the actual delivery of the data, TCP takes care of keeping track of the packets that a message is divided into for efficient routing through the Internet.

TX Output Power
Transmit Output Power. The TX output power means the transmission output power of the radio. Normally, the TX output power level limit for 2.4GHz 11g/b is 20dBm at the antenna end. The output power limit for 5GHz 802.11a is 30dBm at the antenna end..

UDP
User Datagram Protocol. A layer-4 network protocol for transmitting data that does not require acknowledgement from the recipient of the data.

Upgrade
To replace existing software or firmware with a newer version.

Upload
To send a file to the Internet or network device.

URL
Uniform Resource Locator. The address of a file located on the Internet.

VPN
Virtual Private Network. A type of technology designed to increase the security of information transferred over the Internet. VPN creates a private encrypted tunnel from the end user's computer, through the local wireless network, through the Internet, all the way to the corporate network.

WAN
Wide Area Network. A communication system of connecting PCs and other computing devices across a large local, regional, national or international geographic area. A WAN port on the network device means the port (or wireless connection) that is connected to the Internet side of the network topology.

WEP
Wired Equivalent Privacy. A wireless encryption protocol. WEP is available in 40-bit (64-bit), 108-bit (128-bit) or 152-bit (Atheros proprietary) encryption modes.

Wi-Fi
Wireless Fidelity. An interoperability certification for wireless local area network (LAN) products based on the IEEE 802.11 standards. The governing body for Wi-Fi is called Wi-Fi Alliance (also known as WECA).

WiMAX
Worldwide Interoperability for Microwave Access. A Wireless Metropolitan Network technology that complies with IEEE 802.16 and ETSI Hiperman standards. The orginal 802.16 standard call for operating frequency of 10 to 66Ghz spectrum. The 802.16a amendment extends the original standard into spectrum between 2 and 11 Ghz. 802.16d increase data rates to between 40 and 70 Mbps/s and add support for MIMO antennas, QoS, and multiple polling technologies. 802.16e adds mobility features, narrower bandwidth (a max of 5 mhz), slower speed and smaller antennas. Mobility is allowed up to 40 mph.

WDS
Wireless Distribution System. WDS defines how multiple wireless Access Point or Wireless Router can connect together to form one single wireless network without using wired uplinks. WDS associate each other by MAC address, each device

WLAN
Wireless Local Area Network. A type of local-area network that uses high-frequency radio waves rather than wires to communicate between nodes. The most popular standard for WLAN is the 802.11 standards.

WMM
Wi-Fi Multimedia (WMM) is a standard to prioritize traffic for multimedia applications. The WMM prioritize traffic\ on Voice-over-IP (VoIP), audio, video, and streaming media as well as traditional IP data over the AP.

WMS
Wireless Management System. An utility program to manage multiple wireless AP/Bridges.

WPA
Wi-Fi Protected Access. It is an encryption standard proposed by WiFi for advance protection by utilizing a password key (TKIP) or certificate. It is more secure than WEP encryption. The WPA-PSK utilizes pre-share key for encryption/authentication.

WPA2
Wi-Fi Protected Access 2. WPA2 is also known as 802.11i. It improves on the WPA security with CCMP and AES encryption. The WPA2 is backward compatible with WPA. WPA2-PSK utilizes pre-share key for encryption/authentication.