Air Live®
Powered by OvisLink Corp.

# AirMax2

802.11g Outdoor CPE

## User's Manual


## Copyright & Disclaimer

# 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.

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

# Table of Contents

# 1 Introduction

## 1.1 Overview

The AIRMAX2 is a wireless outdoor multi-function device based on IEEE 802.11g/b 2.4GHz radio technologies. When installed in upright position, it is rain and splash proof. It features an integrated 8.03dBi patch antenna and passive POE to simplify the installation. The built-in antenna can provide up to 3km* of distance depending on conditions. If more distance is required.

The firmware of the AP provides up to 9 operation modes* to satisfy different application environments.

## 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 firmwares that either increase software functions or provide bug fixes for AirMax2. 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

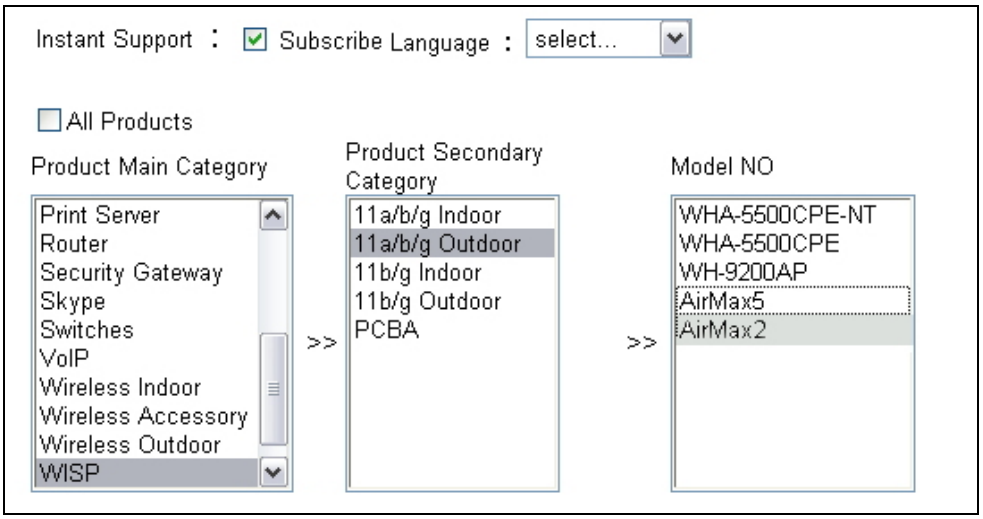



Figure 1.4: AirLive Newsletter Suppport System

## 1.3 Features

- 802.11g/b Hi Powered Chipset
- 4MB Flash and 16MB 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
- 10Bi Integrated Patch Antenna: Vertical Polarization. 70 degree Horizontal and 38 degree Vertical coverage in the forward direction.

- Built from High Temperature resistant ABS material with Anti-UV protection
- Power by passive PoE: 12V Adapter and injector included.
- Slide out housing design for easy maintenance.
- Pole Mount strap included. Optional metal mount and wall mount available
- Interface and IP/MAC Bandwidth Control
- Site Survey, Signal Survey, and Signal Strength LED indicator.
- ClearSignal Interference Resistant Technology
- Emergency firmware recovery mode
- Web, HTTPS, SSH, Telnet managements

## 1.4 Wireless Operation Modes

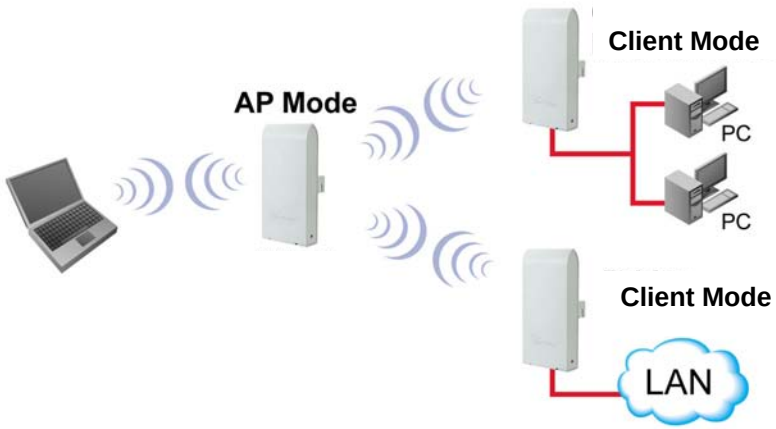
The AirMax2 can perform as a multi-function wireless device. Through the AirLogic web interface, users can easily select which wireless mode they wish the AirMax2 to perform.

| AirMax2 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 |

### 1.4.1 Access Point Mode

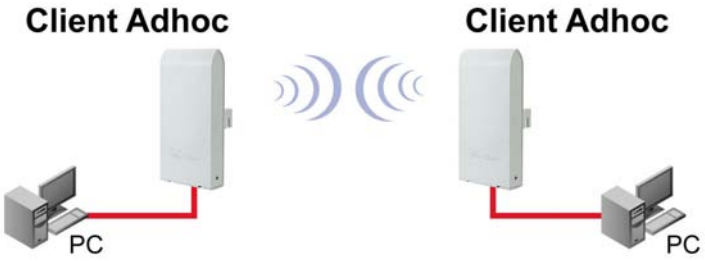
When operating in the Access Point mode, the AIRMAX2 becomes the center hub of the wireless network. All wireless cards and clients connect and communicate through AirMax2. This type of network is known as “Infrastructure network”. Other AirMax2 or 802.11a CPE can connect to AP mode through “Client Mode”.




### 1.4.2 Client Mode

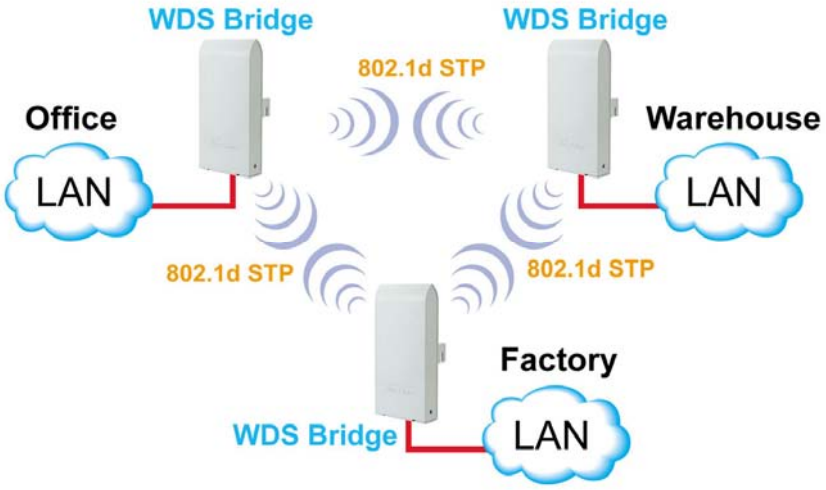
This mode is also known as “Client” mode. For AirMax2, there are 2 types of Client modes: Infrastructure and Adhoc mode. In Infrastructure mode, the AIRMAX2 acts as if it is a wireless adapter to connect with a remote Access Point. Users can attach a computer or a router to the LAN port of AirMax2 to get network access. This mode is often used by WISP on the subscriber’s side.

In Client Ad Hoc mode, AIRMAX2 can connect to other wireless adapters without access point. Users can attach a computer or a router to the LAN port of AirMax2 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 AIRMAX2 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.

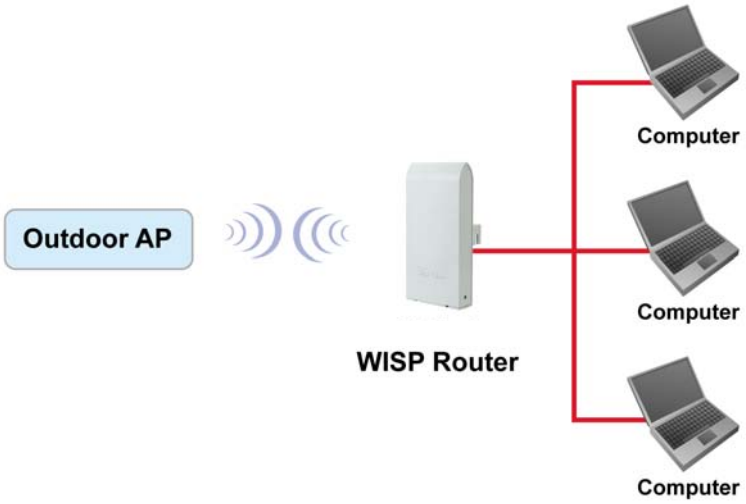



## 1.4.4 WDS Repeater Mode

In WDS Repeater mode, the AIRMAX2 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

### 1.4.6 WISP Router Mode

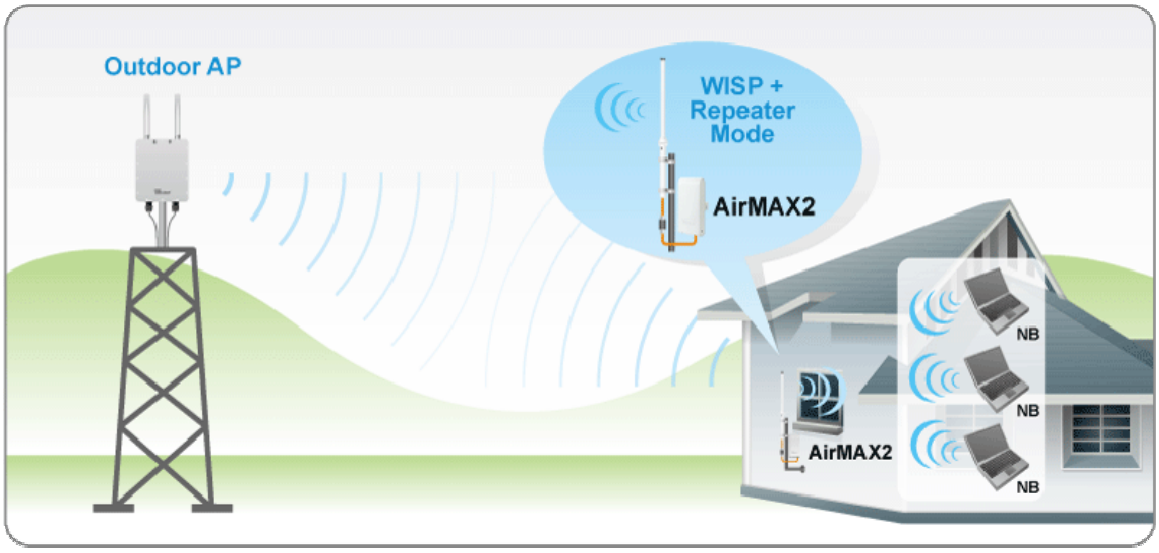
In WISP Router Mode, AIRMAX2 connects to the remote Access Point as in Client Infrastructure Mode. On the LAN side, it acts like a wired router for IP sharing function. This mode is best used for IP sharing application for WISP subscribers. In this mode, the WAN is the wireless client side, the LAN is 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. The use of external Omni-Directional Antenna .

If you are a WISP operator, it is highly recommended that you use a 2-radio product like AirLive G.DUO(dual 11g AP) or WLA-9000AP(A+G AP) for this purpose.



### 1.4.8 AP Router Mode

In AP Router Mode, the AirMax2 behaves like a wireless router. The LAN port of the AirMax2 will become WAN port. The wireless network of AirMax2 becomes the LAN side. Please note when this mode is used, the only way to manage the AirMax2 is through the wireless side unless remote management is opened.


### 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.

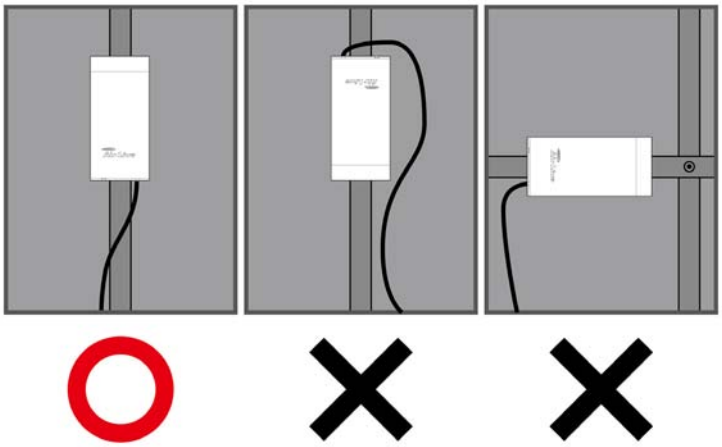
# 2 Installing the AirMax2

This section describes the hardware features and the hardware installation procedure for the AIRMAX2. For software configuration, please go to chapter 3 for more details.

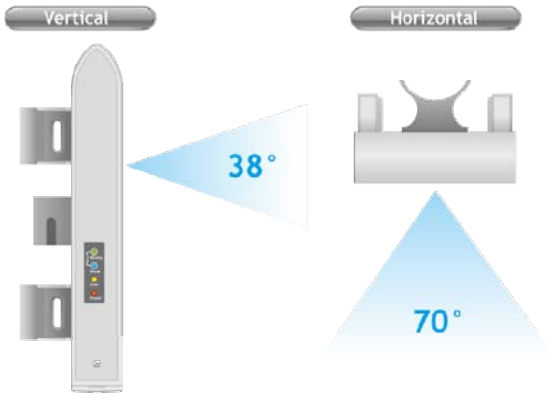
## 2.1 Before You Start

It is important to read through this section before you install the AirMax2

- The AirMax2 comes with everything you need to start installation with exception of the PoE Ethernet Cable. You can use a good quality CAT-5E outdoor graded Ethernet cable (shielded with anti-UV) according to the length you need.
- The AirMax2 must be installed in the upright position if the unit is located in outdoor or wet environments.



- The integrated antenna has forward coverage angle of 70 degree horizontal and 38 degree vertical.



## 2.2 Package Content

The AIRMAX2 package contains the following items:

- One AirMax2 main unit
- One 12V 1A DC power adapter
- Passive PoE DC Injector
- 2 x Plastic Straps
- User's Guide CD
- Quick Start Guide


The PoE Ethernet cable is not included in the package. You may choose an outdoor specification Ethernet cable according to the length you need.

## 2.3 Optional Accessories

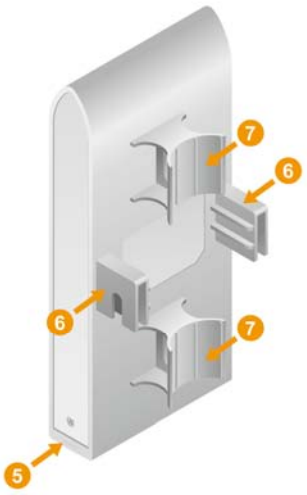
The AirMax2 have the following optional accessories which you can purchase from AirLive

- Tilting Metal Wall/Pole Mount (*Model: WMK-AIRMAX*): This kit allows your AirMax2 to tilt in pole mount, it also allow you to install the AirMax2 to the wall.
- 25 meter PoE cable (*Model: OD-25M*): high quality outdoor graded anti-UI PoE Ethernet Cable.

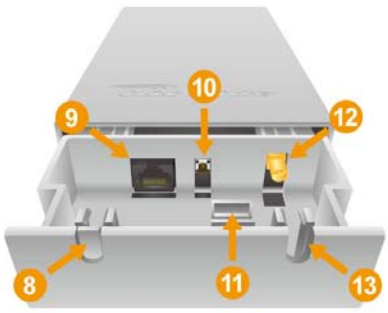

## 2.4 Knowing Your AirMax2

Below are descriptions and diagrams of the product:


1. Case Screws
2. LED Indicators
3. Top Case
4. Bottom Case



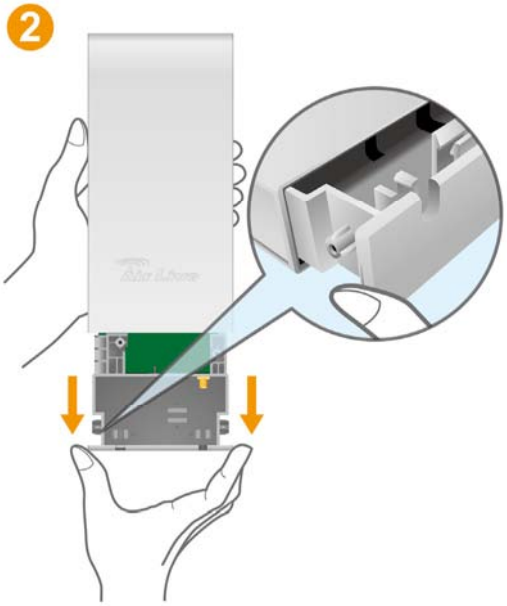

5. Bottom Case Pull-Out Holders
6. Mounting for optional Metal mount kit
7. Pole Mount Holders

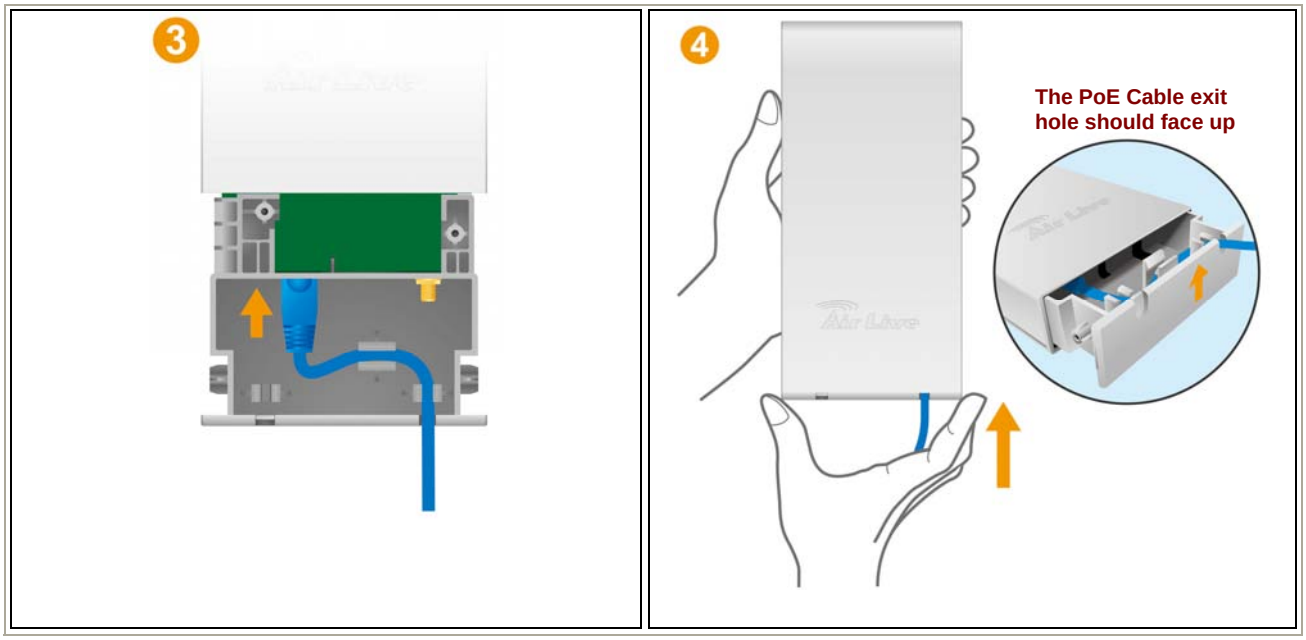



8 Antenna Cable Exit Hole
9 PoE Ethernet Port
10 Reset Button
11 Cable Guard
12 R-SMA External Antenna Connector
13 PoE Cable exit port

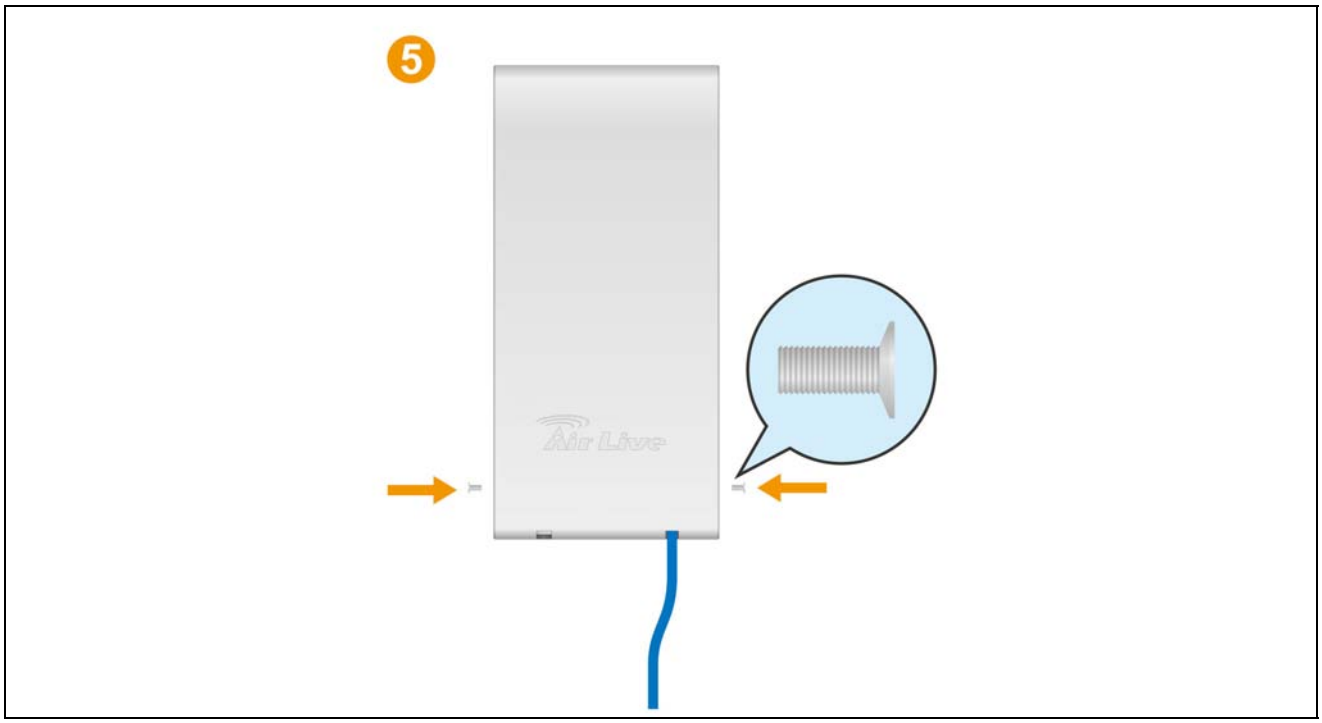
## 2.5 Hardware Installation

Please prepare a screw driver and an outdoor graded PoE Ethernet cable with adequate length according to your need.

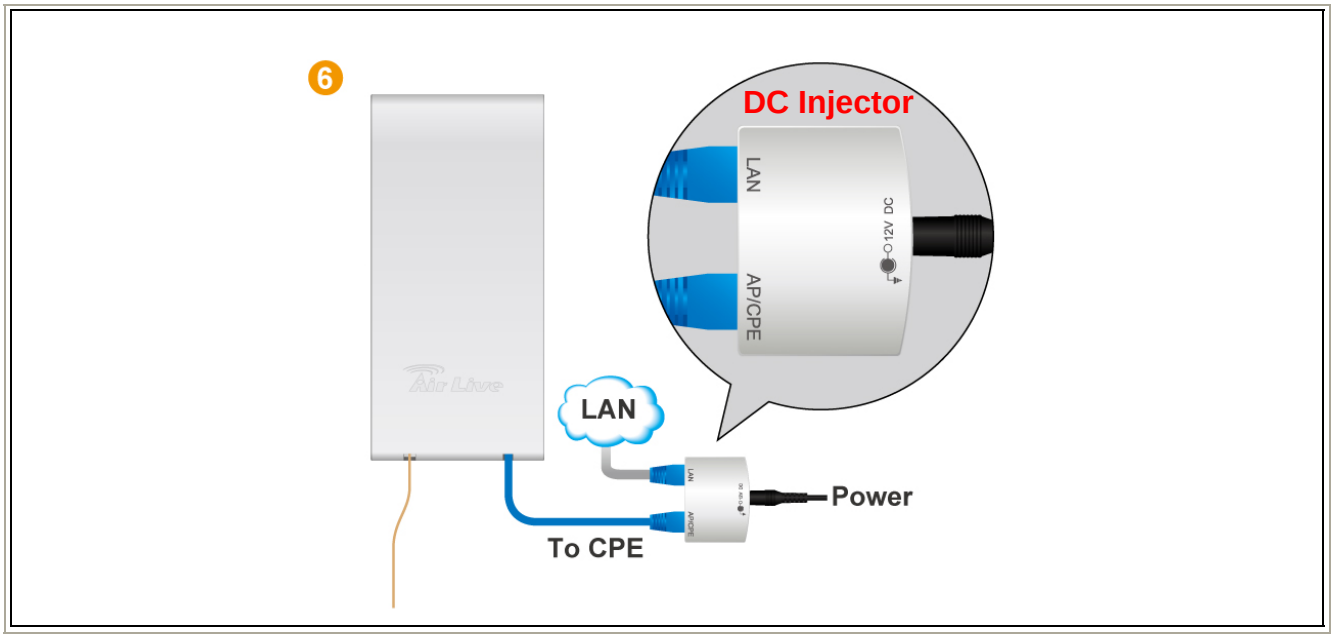
| 1. Remove the screws from the sides of the case. | 2. Hold the sides of the bottom cases and pull out in the downward direction. |
|---|---|
|  |  |
| 3. Install the PoE cable to the PoE Port. Follow the cable guard direction. | 4. Slide back the bottom case |
| | |




. 5. Put the case screws back.

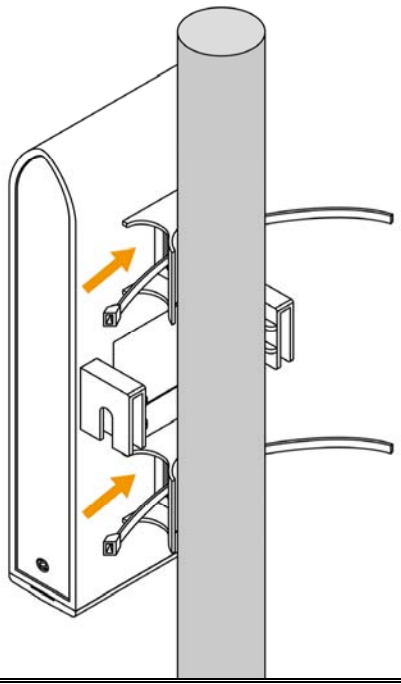
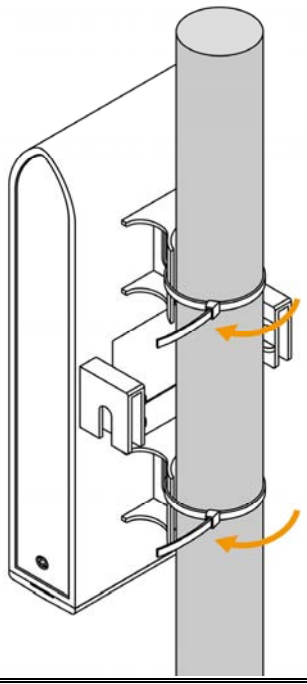



6. Install the PoE Cable and the Power Adapter to the DC Injector. Please make sure to read the markings on the DC Injector carefully and connect the cables correctly. You can connect your PC directly to the “LAN” port of the DC Injector.




## 2.5.1 Standard Pole Mount

Your AirMax2 comes standard with 2 plastic straps for pole mounting. Please follow the procedure below to install:

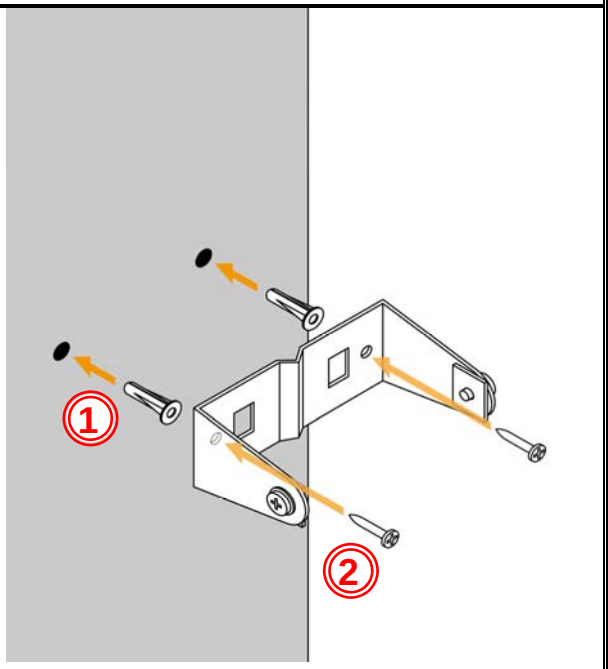
| 1. Put the plastic strap through the holes on the Pole Mount holders. | 2. Thread the thinner end of the strap into the opening on the other end. Then tighten the strap around the pole as tightly as possible. |
|---|---|
|  |  |

## 2.5.2 Optional Tilting Metal Pole/ Wall Mount

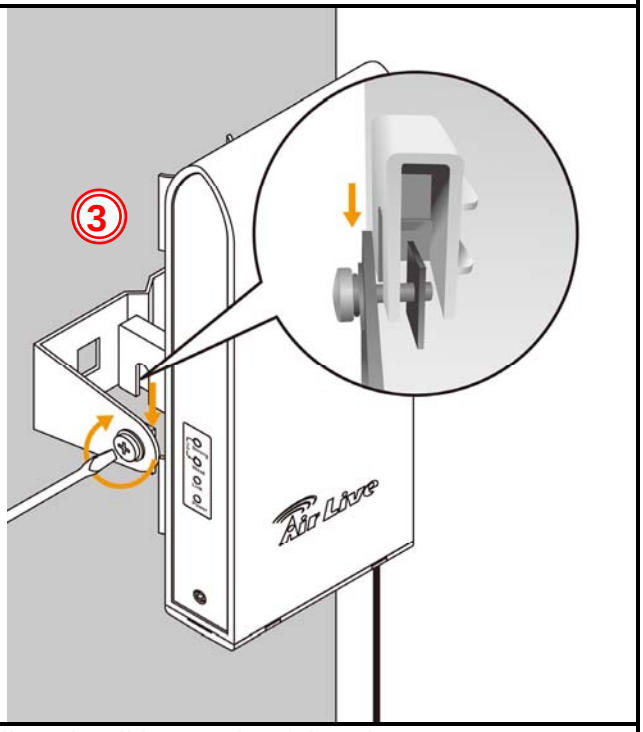
The optional **WMK-AIRMAX** metal pole/wall mount kit allows your AirMax2 to be mounted on the wall and pole. It enables you to tilt the AirMax2 to the desire vertical angle. If you have purchased such kit, please follow the instruction below to mount your AirMax

**Wall Mount Installation using WMK-AIRMAX**

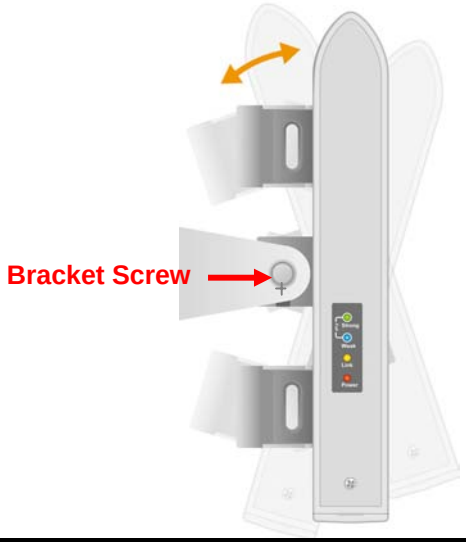
1. Please first install the screw anchors into the wall
2. Secure the screws through the Metal Bracket into the screw anchors




3. Install the AirMax2 into the Metal Bracket and tighten the screws on the bracket.

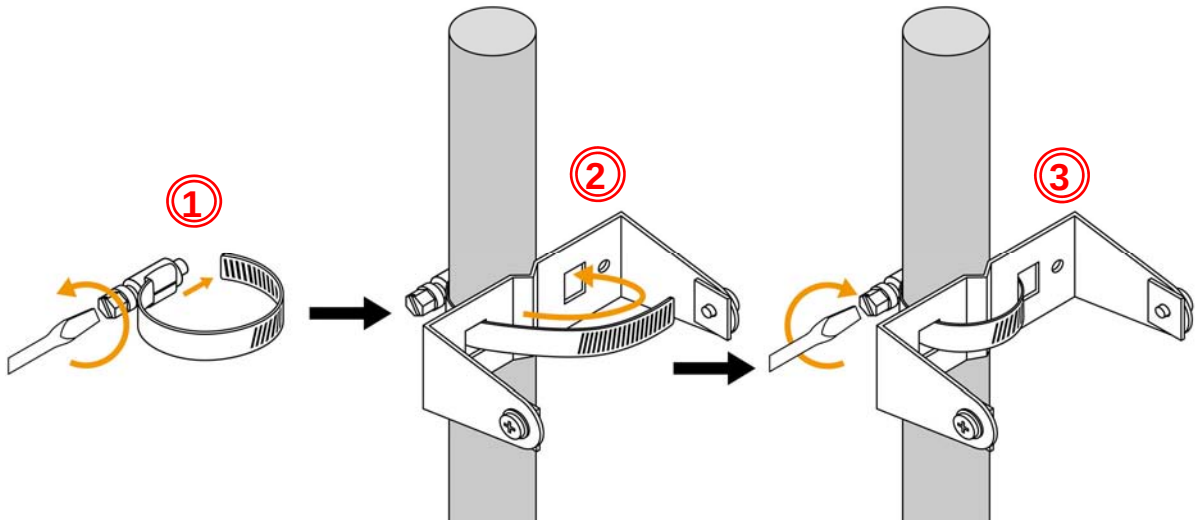



4. By adjusting the bracket screws, you can adjust the tilting angle of the AirMax2

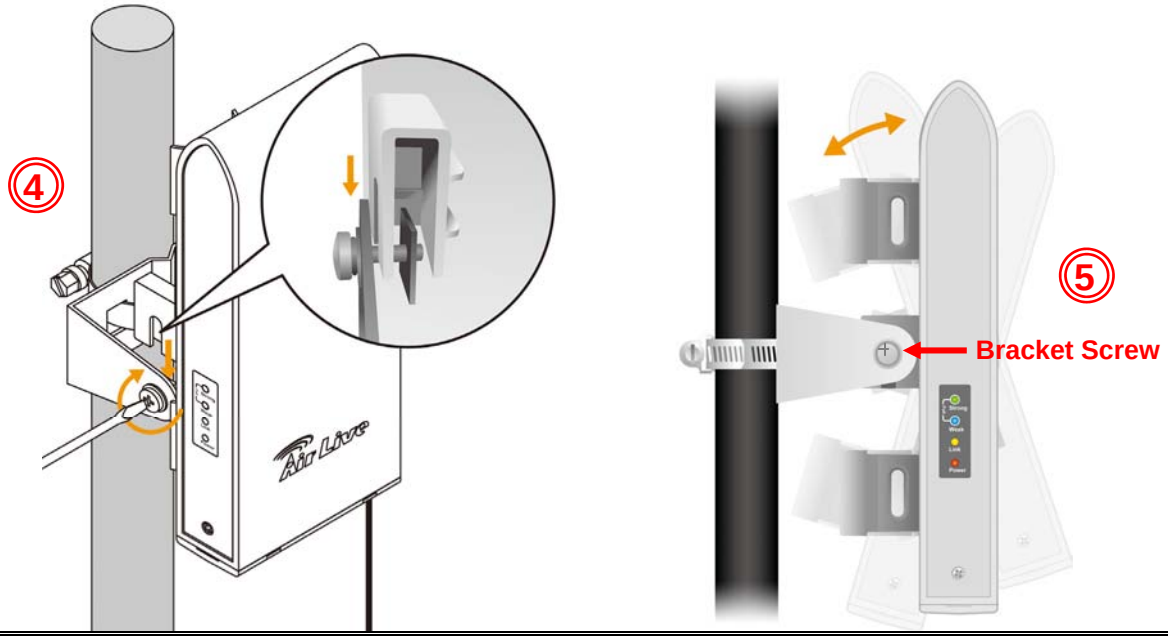


## Pole Mount Installation using WMK-AIRMAX

1. Unscrew the metal ring(pipe fastener) until one end of the ring come off completely
2. Put the metal ring through the holes on the bracket and wrap it around the pole.
3. Tighten the screw on the ring until the ring is very tight around the pole.



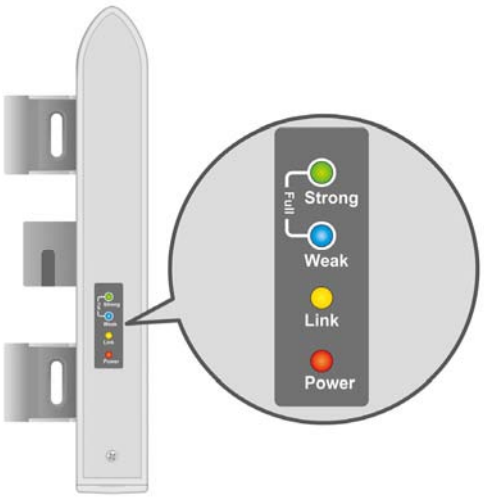

4. Now, install the AirMax 5 into the metal bracket and tighten the screws on the bracket
5. By adjusting the bracket screws, you can adjust the tilting angle of the AirMax2



## 2.6 LED Table

This section describes the LED behavior of AirMax2.

You can find the LED on the left side of the AirMax2.



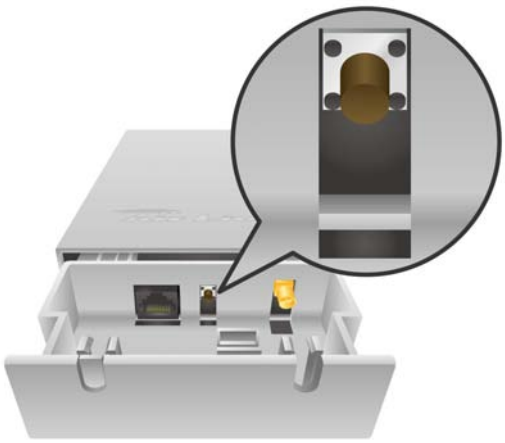

**Power**
- Steady Red – Normal Operation
- OFF – No Power

**Link**
- Steady Yellow: Link is active
- Flashing Yellow: Transmit or receive data
- OFF: No connection

WLAN Signal Strength LEDs
- Weak :Low signal strength
- Strong :Better signal strength
- Weak + Strong: Full Signal strength
- *No connection/Bad signal strength*

## 2.7 Restore Settings to Default

If you have forgotten your AirMax2's IP address or password, you can restore your AirMax2 to the default settings by pressing on the "reset button" for more than 5 seconds. The reset button is inside the bottom case. Please see diagram below for details.



# 3 Configuring the AirMax2

The AirMax2 offers many different types of management interface. You can configure through standard web browser (http), secured web (https), command line (telnet), sand ecured command shell (SSH). In this chapter, we will explain AirMax2's available management interfaces 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.

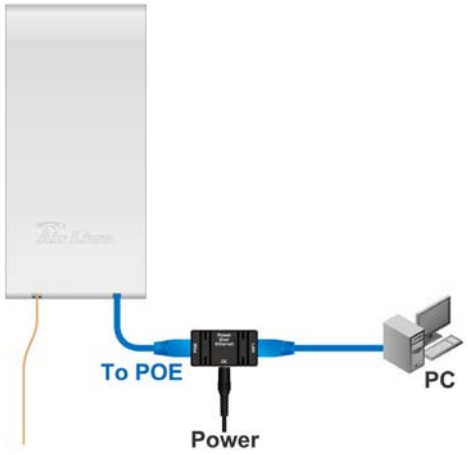
- The default IP address is: 192.168.1.1 Subnet Mask: 255.255.255.0
- The default user's name is: admin
- The default password is: airlive
- The default SSID is: airlive
- The default wireless mode is : Client mode
- After power on, please wait for 2 minutes for AirMax2 to finish boot up
- Please remember to click on "Apply" for new settings to take effect
- **You must reboot the AirMax2 after you finish all the settings for changes to take effect**
- The ClearSignal Technology is "OFF" by default. If there are heavy interference around your environment. Please turn it on.
- When you change to "AP Router" mode, the LAN port will become WAN port. The IP address is changed to "192.168.2.1".

## 3.2 Prepare your PC

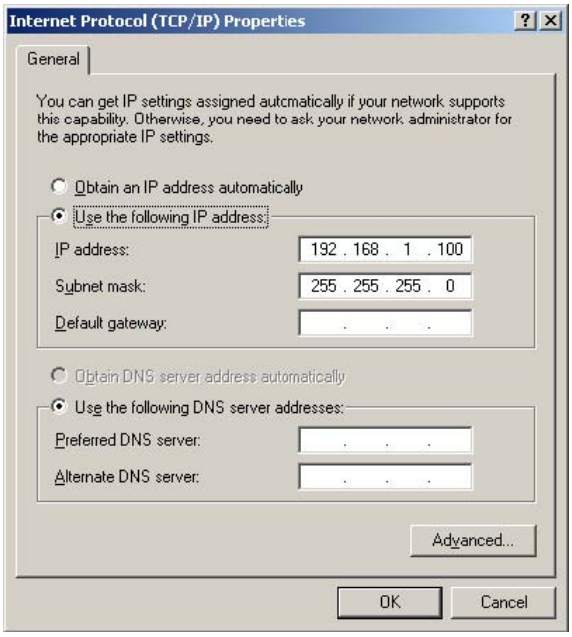
The AIRMAX2 can be managed remotely by a PC through either the wired or wireless network. The default IP address of the AIRMAX2 is **192.168.1.1** with a *subnet mask* of 255.255.255.0. This means the IP address of the PC should be in the range of 192.168.1.2 to 192.168.1.254.

To prepare your PC for management with the AirMax2, please do the following:

**1.** Connect your PC directly to the LAN port on the DC Injector of AirMax2




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




You are ready now to configure the AirMax2 using your PC.

## 3.3 Management Interface

The AirMax can be configured using one the management interfaces below:

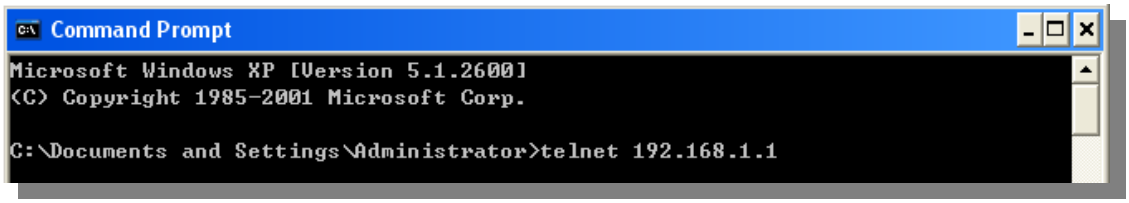
- **Web Management (HTTP):** You can manage your AirMax2 by simply typing its IP address in the web browser. Most functions of AirMax2 can be accessed by web management interface. We recommend using this interface for initial configurations. To begin, simply enter AirMax2's IP address (default is 192.168.1.1) on the web browser. The default username is "admin" and password is "airlive".


- **Secured Web Management (HTTPS):** HTTPS is also using web browser for configuration. But all the data transactions are securely encrypted using SSL encryption. Therefore, it is a safe and easy way to manage your AirMax2. We highly recommend WISP and service provider to use HTTPS for management.

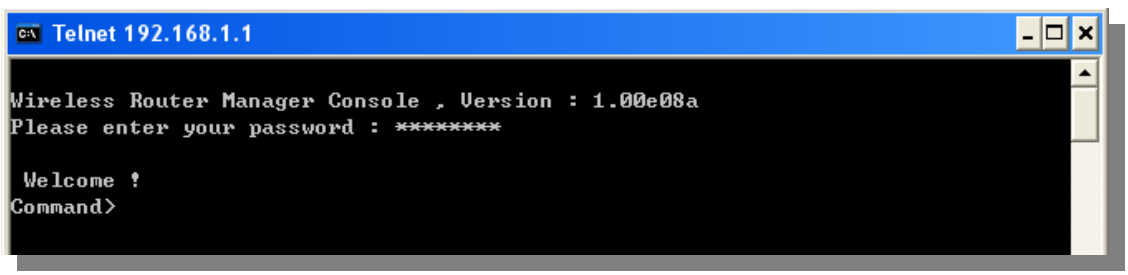
  To begin, simply enter https://192.168.1.1 on your web browser. A security alert screen from your browser will pop up. Please grant all permission and get certificate to AirMax2. After you pass the security warning screen, you will enter the secured web management interface. The default username is "admin" and password is "airlive".


- **Command Line Interface (Telnet):** AirMax2 can be managed through the command line interface (CLI). It is possible to write a text script file, and then paste it into the CLI to execute several commands at once. However, Telnet does not encrypt its message. Therefore, it is not secure. The default Telnet management port is TCP port 23.

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




  When asked for password, please enter "airlive".



■ **Secure Shell (SSH, SSH2)**: SSH is an encrypted Command Line Interface that allow user to send text commands through SSL encryption. Therefore, it provides the added advantage of security comparing to Telnet. As with Telnet, the SSH and SSH2 provide the possibility to write a text script and paste into the CLI interface for multiple command execution. It also makes configuration change across many AirMax2s easier. The default management port for SSH/SSH2 is TCP/UDP port 22.

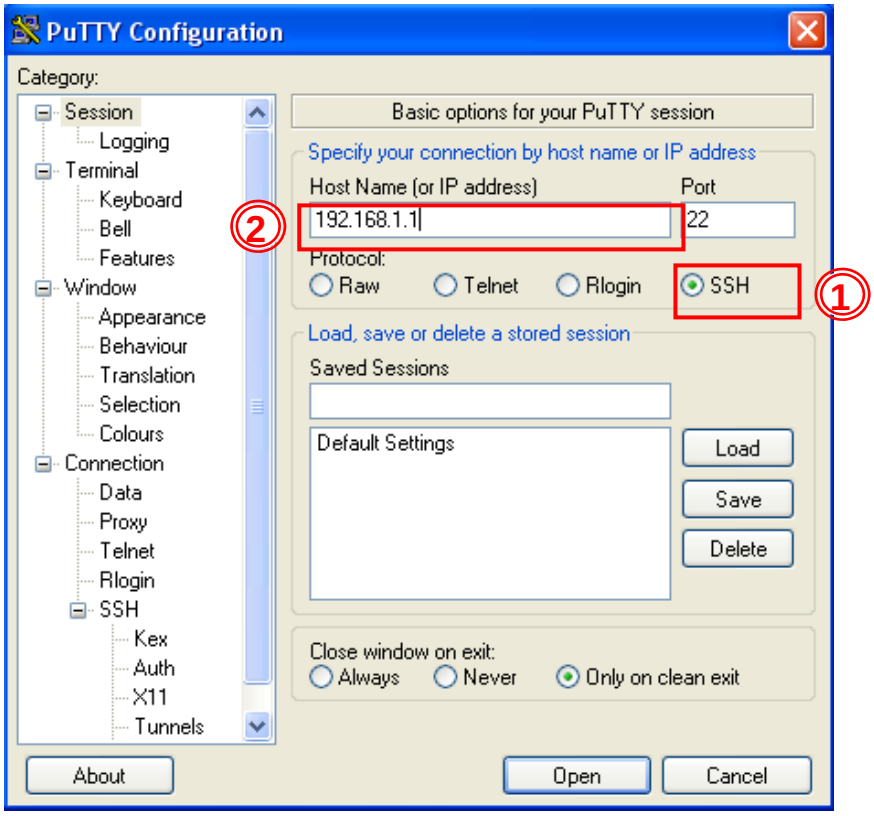
To manage via the SSH/SSH2 protocol, you would need a SSH client. Free SSH clients are widely available on the Internet. You can find where to download them by using Internet search engine such as Google. In this guide, we will use a popular SSH/Telnet utility called "Putty".

Once you have download and install Putty. Please follow the figure below to make a connection with AirMax2:

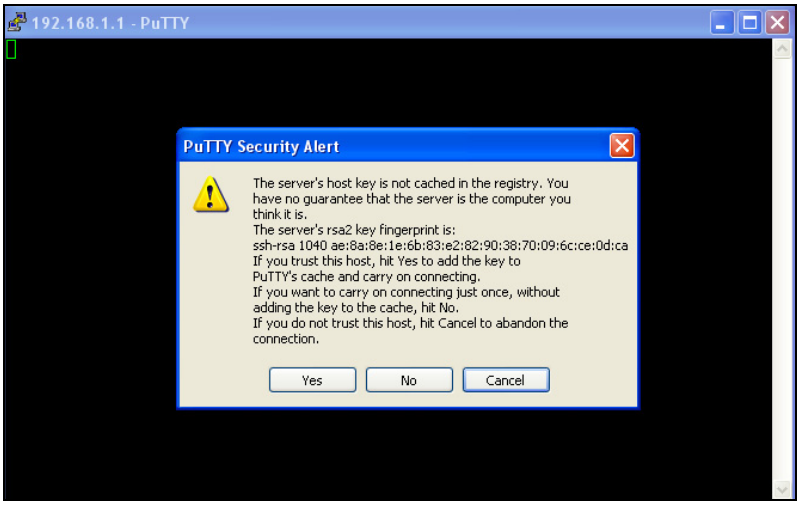
**1.** Choose "SSH" as indicated in the diagram

**2.** Enter the IP address of AirMax2

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




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




When asked for username, please enter “admin”. When asked for password, please enter “airlive” as factory default. This password will change when you change the password.


## 3.4 Introduction to Web Management

The AirMax2 offers both normal (http) and secured (https) Web Management interfaces. Their share the same interface and functions, and they can both be accessed through web browsers. The only difference is HTTPS are encrypted for extra security. Therefore, we will discuss them together as “Web Management” on this guide.

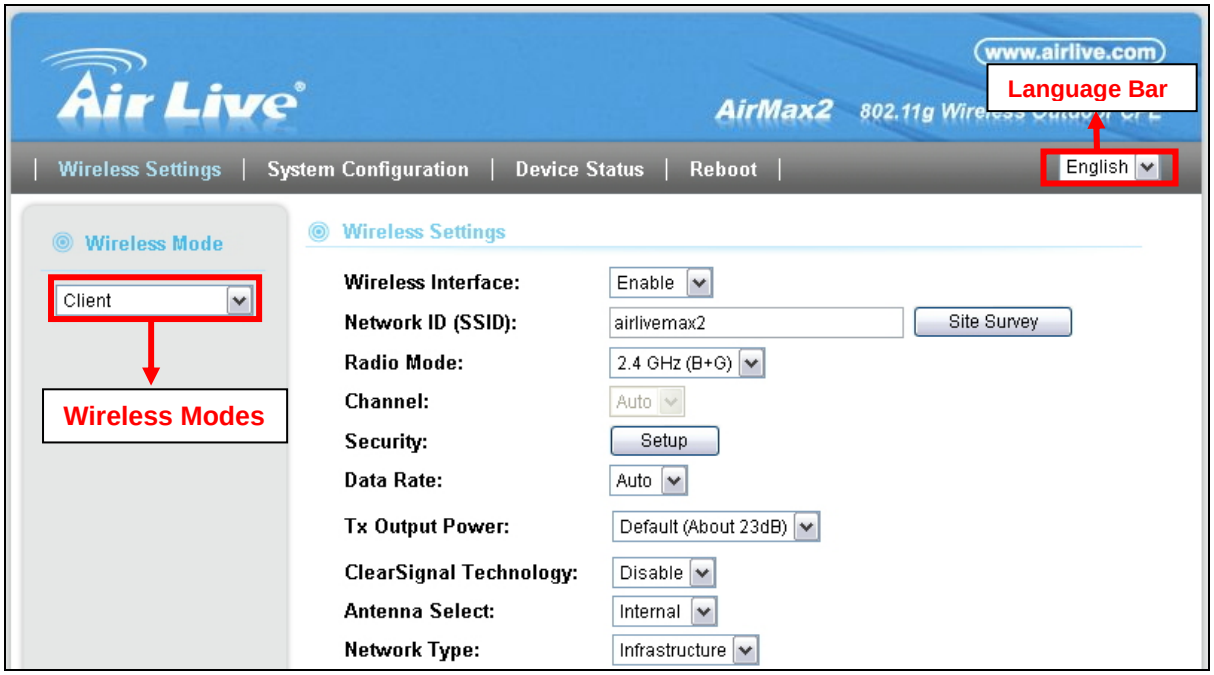
If you are placing the AirMax2 behind router or firewall, you might need to open virtual server ports to AirMax2 on your firewall/router

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

This procedure is not necessary in most cases unless there is a router/firewall between your PC and AirMax2.

### 3.4.1 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 AirMax2'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 interface.
- **Device Status**: This section for monitoring the status of AirMax2. 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.

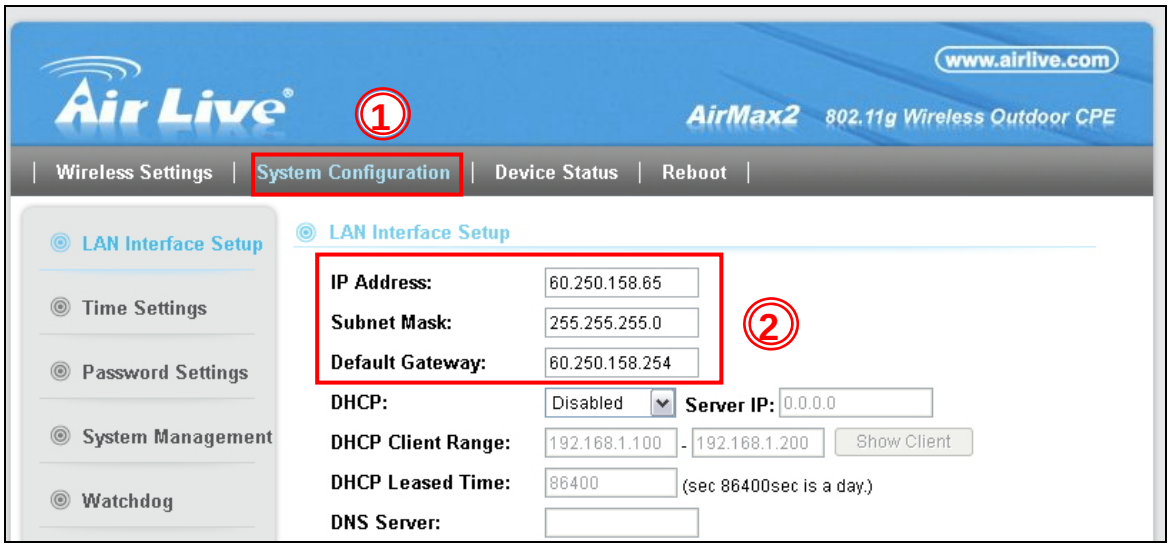
## 3.5 Initial Configurations

We recommend users to browse through AirMax2's web management interface to get an overall picture of the functions and interface. Below are the recommended initial configurations for first time login:

### 3.5.2 Change the Device's IP Address

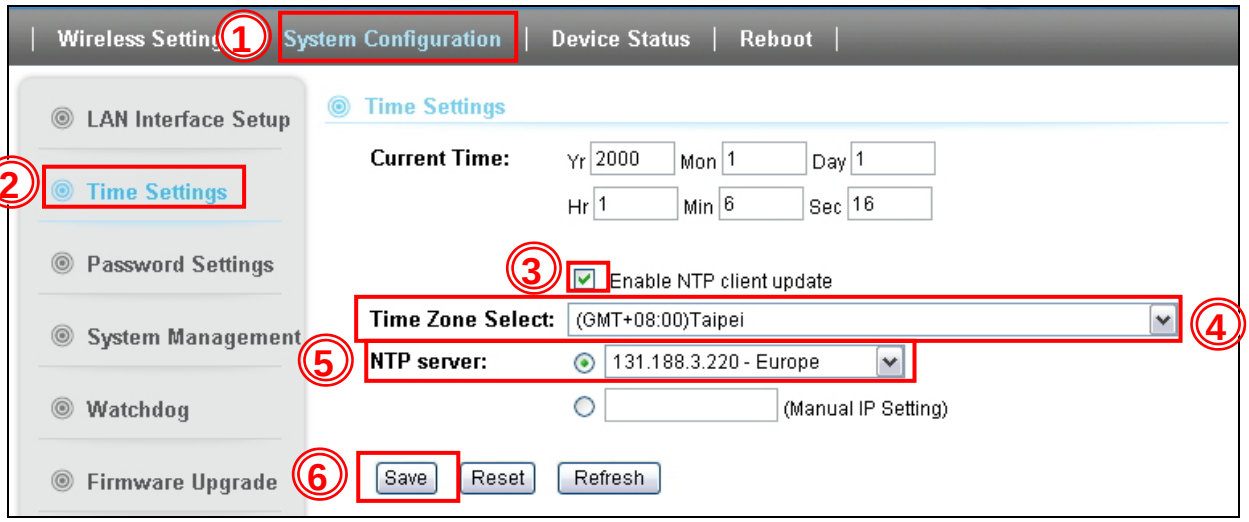
The default IP address is at 192.168.1.1. You should change it to the same subnet as your network. Also, if you want to manage AirMax2 remotely, you have to set the Gateway and DNS server information.

To setup the IP settings for AirMax2, please select “System Configuration” -> Device IP Settings”. After entering the IP information, click on “Apply Changes” to finish.



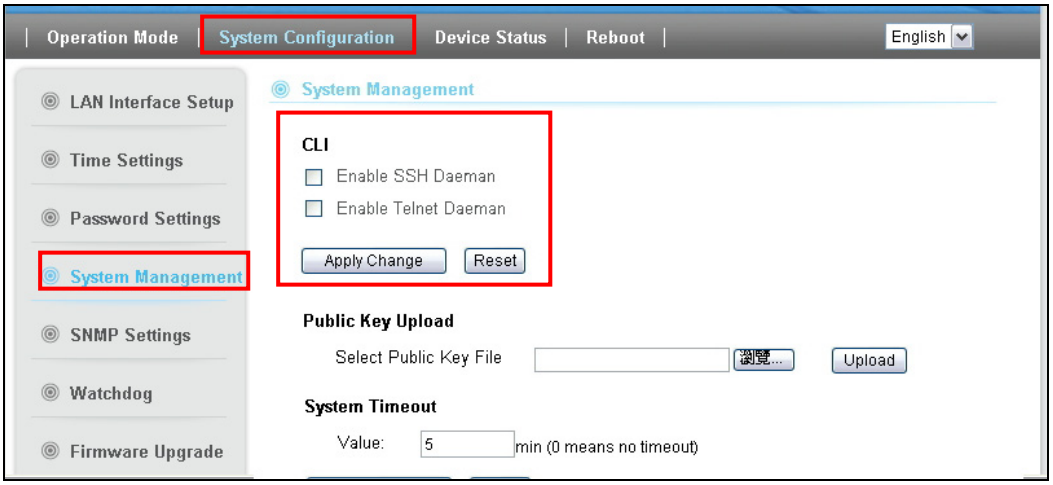

## 3.5.3 Set the Time and Date

It is important that you set the date and time for your AirMax2 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 AirMax2 is not connected to Internet, please enter the time manually. Please remember to select your local time zone and click “Apply” to finish.



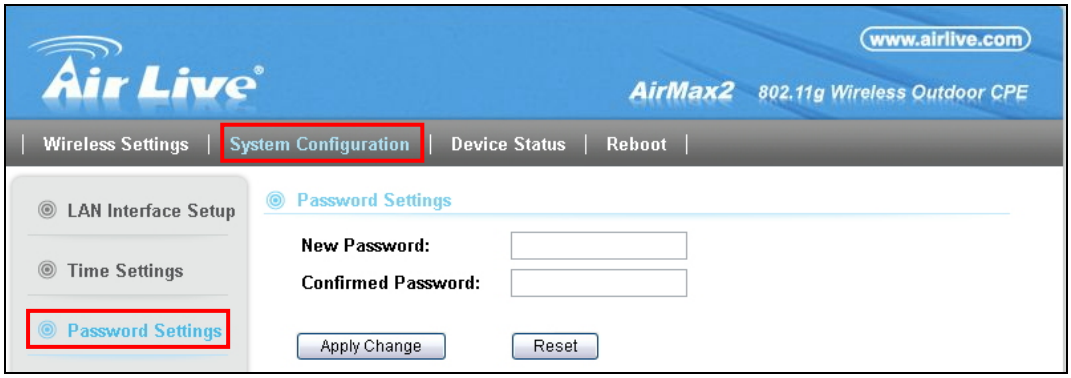
### 3.5.4 Enable/Disable Telnet and SSH Management

The Telnet and SSH management interface are turned off by default. If you wish to use them, please go to the “System Configuration -> System Management” menu. Check “Telnet” or “SSH”, then click on “Apply Change” button.




### 3.5.5 Change Password

You should change the password for AirMax2 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.

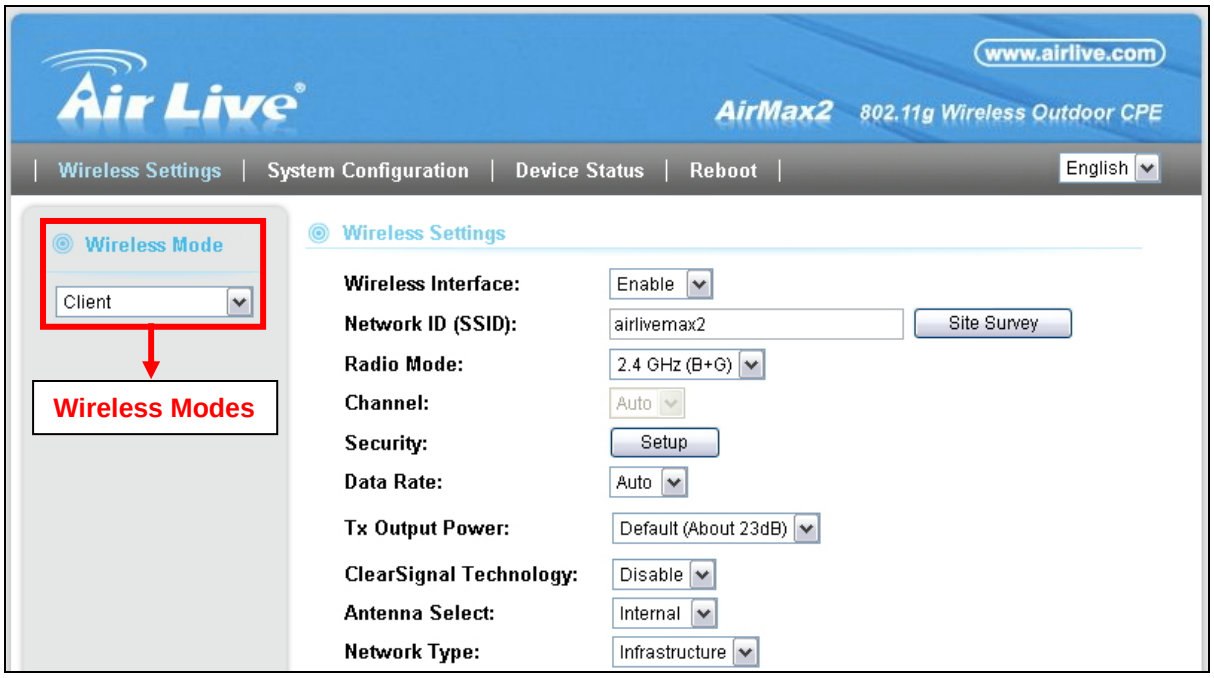
## 4.1 About Wireless Modes

The AirMax2 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.

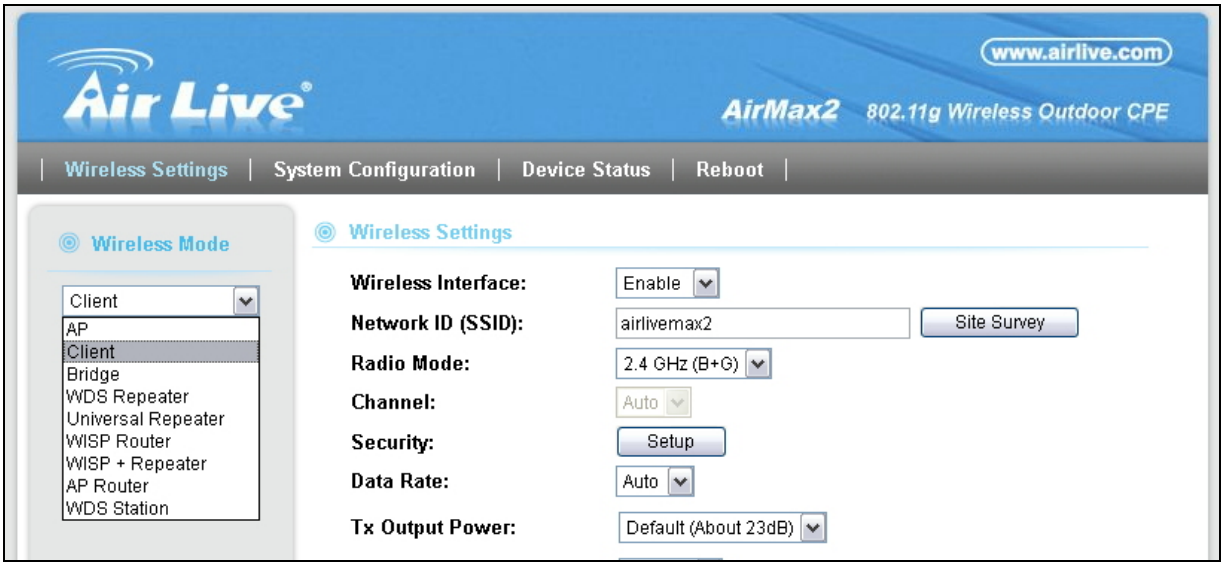
Below is the summary table for different wireless modes:

| AirMax2 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 mode, 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 pulldown menu. The AirMax2 will ask you to confirm about the mode change. After your confirmation, the AP will reboot itself to the new mode.




*The AirMax2 only have one LAN port. After you change to the "AP Router" mode, the LAN port will become WAN port. And the IP address will be changed to 192.168.2.1.*

## 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 AirMax2 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 | 26dBm |
| South America(14 CH) | 1~14 | 26dBm |

## 4.2.2 Network SSID

***Wireless Settings -> Network SSID***

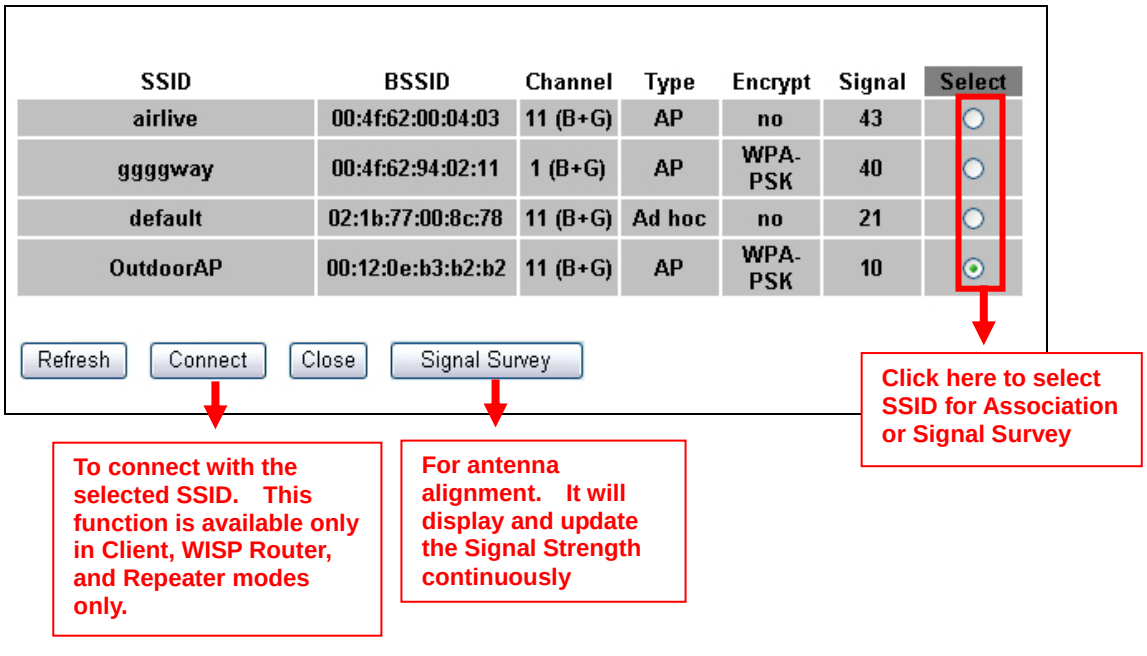
The SSID is the network name used to identify a wireless network. The SSID must be the same for all devices in the same wireless network. The SSID length is up to 32 characters. The default SSID is "**airlive**".

## 4.2.3 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

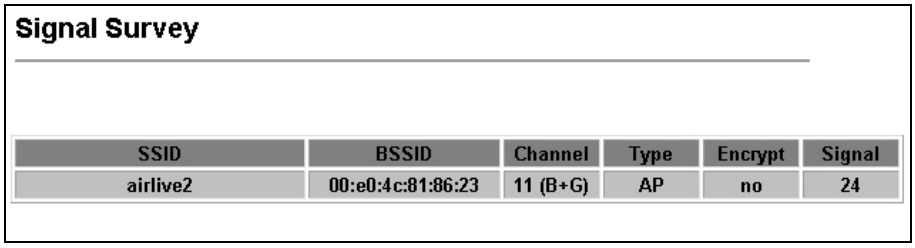
When you click on Site Survey, the following screen will appear. It might take awhile depending on number of available APs in the area.



## 4.2.4 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.

## 4.2.5 Hide SSID

***Wireless Settings -> Hide SSID***

When this function is enabled, 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 enabled, it might be necessary to configure the wireless connection manually. This option is available in AP mode, AP Router mode, and Repeater modes only.

## 4.2.6 Radio Mode

***Wireless Settings -> Radio Mode***

AirMax2 has 3 different options for WLAN transmission. All devices in the same network should use the same WLAN mode.

- **802.11g/b:** The radio will auto adjust between 11g and 11b mode. It is recommended to use this mode.
- **802.11g Only:** The radio will only connect at 11g mode.
- **802.11b Only:** The radio will only connect at 11b mode.

## 4.2.7 Channel

***Wireless Settings -> Channel***

The channel is the frequency range used by radio. In 802.11g/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 | - | - |

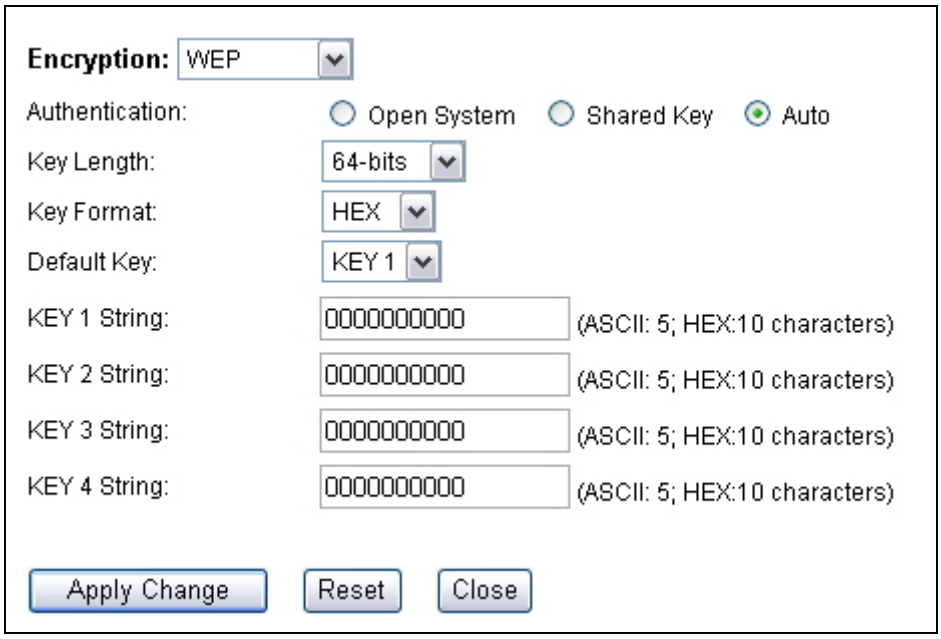
## 4.2.8 Client Mode Security Settings

***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 AIRMAX2 features various security policies including WEP, 802.1x, WPA, WPA Personal, WPA2, WPA2 Personal , WPA Mixed.

## WEP

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



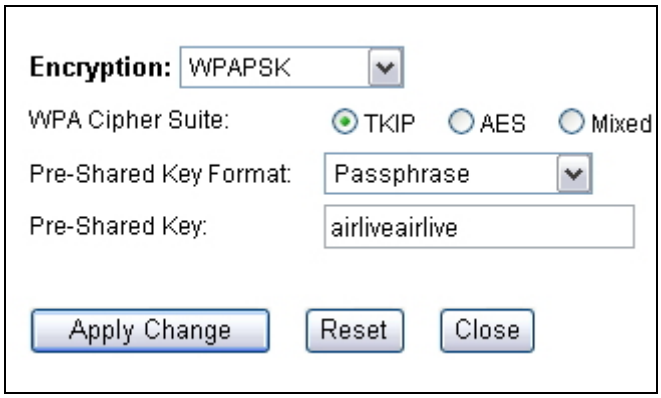

- **Select one of the WEP key for wireless network:** There are total of 4 possible keys for WEP encryption. You need to choose which key will be used for encryption. All wireless devices on the same network have to use the same settings. We recommend using WEP Key 1 as in default setting.

  - **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 AIRMAX2 offers 64bit and 128 bit for WEP key length. The longer the Key Length, the more secure the encryption is.
  - **Key Type:** 2 types are available: ASCII and HEX. ASCII is a string of ASCII code including alphabetical characters, space, signs and numbers (i.e. “airlivepass12”). HEX is a string of 16-bit hexadecimal digits (0..9, a, b, c, d, e, f). All wireless devices on the network must match the exact key length and Key type. Some Wireless clients only allow HEX type for WEP.
  - **ASCII-64:** This is a key with 64-bit key length of ASCII type. Please enter **5** ASCII Characters if you choose this option. For example, “passw”
  - **HEX-64:** This is a key with 64-bit key length of HEX type. Please enter **10** Hexadecimal digits if you choose this option. For example, “12345abcdef”
  - **ASCII-128:** This is a key with 64-bit key length of ASCII type. Please enter **13** ASCII Characters if you choose this option. For example, “airlivewepkey”
  - **HEX-128:** This is a key with 128-bit key length of HEX type. Please enter **26**

Hexadecimal digits if you choose this option. For example, "1234567890abcdef1234567890"

### WPA-PSK, WPA2-PSK, WPA-AUTO

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

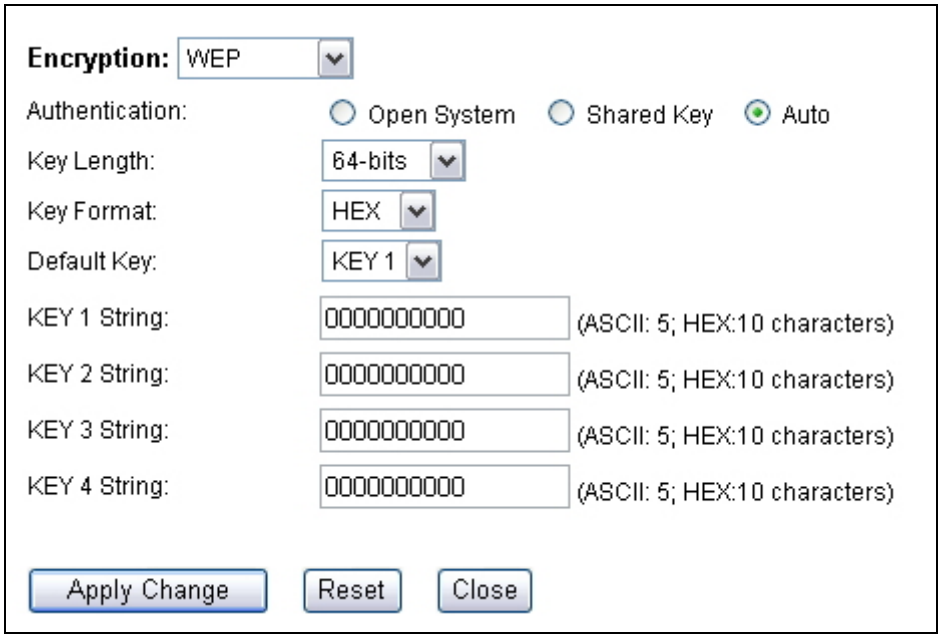
## 4.2.9 AP Mode Security Settings

***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 AIRMAX2 features various security policies including WEP, 802.1x, WPA, WPA Personal, WPA2, WPA2 Personal, WPA Mixed.

### WEP

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

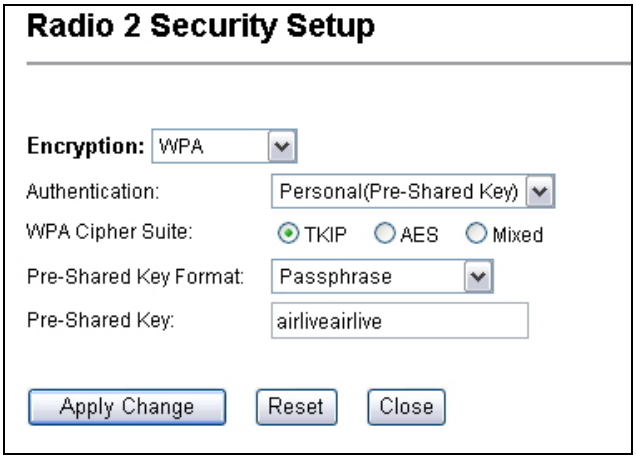



- **Select one of the WEP key for wireless network:** There are total of 4 possible keys for WEP encryption. You need to choose which key will be used for encryption. All wireless devices on the same network have to use the same settings. We recommend using WEP Key 1 as in default setting.

  - **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 AIRMAX2 offers 64bit and 128 bit for WEP key length. The longer the Key Length, the more secure the encryption is.
  - **Key Type:** 2 types are available: ASCII and HEX. ASCII is a string of ASCII code including alphabetical characters, space, signs and numbers (i.e. “airlivepass12”). HEX is a string of 16-bit hexadecimal digits (0..9, a, b, c, d, e, f). All wireless devices on the network must match the exact key length and Key type. Some Wireless clients only allow HEX type for WEP.
  - **ASCII-64:** This is a key with 64-bit key length of ASCII type. Please enter **5** ASCII Characters if you choose this option. For example, “passw”
  - **HEX-64:** This is a key with 64-bit key length of HEX type. Please enter **10** Hexadecimal digits if you choose this option. For example, “12345abcdef”
  - **ASCII-128:** This is a key with 64-bit key length of ASCII type. Please enter **13** ASCII Characters if you choose this option. For example, “airlivewepkey”
  - **HEX-128:** This is a key with 128-bit key length of HEX type. Please enter **26** Hexadecimal digits if you choose this option. For example, “1234567890abcdef1234567890”

## WPA-Personal, WPA2-Personal, WPA-Mixed (Pre-Shared Key)

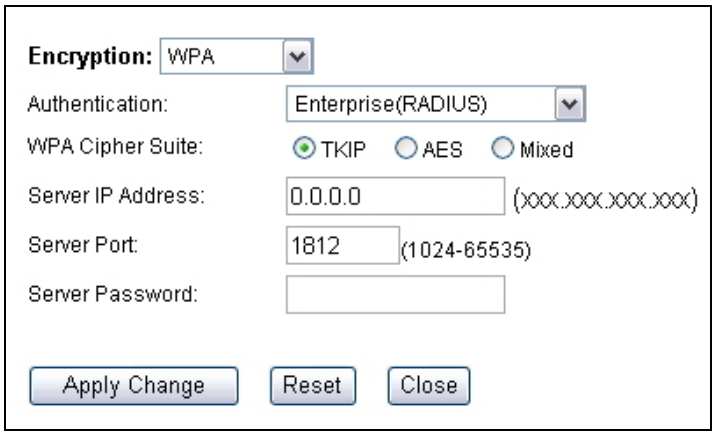
The WPA Personal is also known as “WPA-PSK” encryption. Wi-Fi Protected Access (WPA) introduces the Temporal Key Integrity Protocol (TKIP) that provides added security. WPA2 adds full support for 802.11i standard and the CCMP (AES Encryption). The WPA-Mixed tries to authenticate wireless clients using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



## 4.2.10 Client Isolation

***Wireless Settings -> 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.

## 4.2.11 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 11g/b and 11g Radio mode is 54Mbps.

## 4.2.13 Clear Signal Technology

***Wireless Settings -> ClearSignal Technology***

The default setting is “Off”. ClearSignal Technology uses the combination of sensitivity adjustment and hardware filtering to reduce the effect of interference. If you are experiencing unstable performance caused by interference, please try to turn on this setting. However, turn on this function will also reduce the radio’s sensitivity. Therefore, it is advised only in heavy interference condition.

## 4.2.14 Antenna Select

***Wireless Settings -> Antenna Select***

You can choose to use the built-in Internal Antenna through this setting.
Please remember to reboot the AP after “Apply Changes” to take effect.

## 4.2.15 Auto Clone MAC (Client Mode Only)

***Wireless Settings -> Auto Clone MAC***

When this function is selected, the AirMax2(in client mode) will use MAC address of the first PC that went through the LAN port as the wireless MAC address.

## 4.2.16 Manual MAC Clone (Client Mode Only)

***Wireless Settings -> Manual MAC Clone***

If you wish to change the wireless MAC address of the AirMax2 manually, please enter the MAC address here.

## 4.2.17 Access Control

***Wireless Settings -> Access Control***

The AIRMAX2 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.

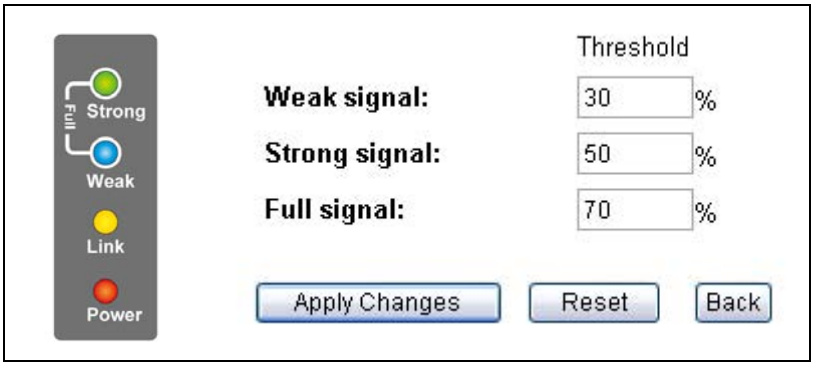
## 4.3 LED Threshold

***Wireless Settings -> LED Threshold***

This function is available only for Client, Bridge, and WISP Router mode.

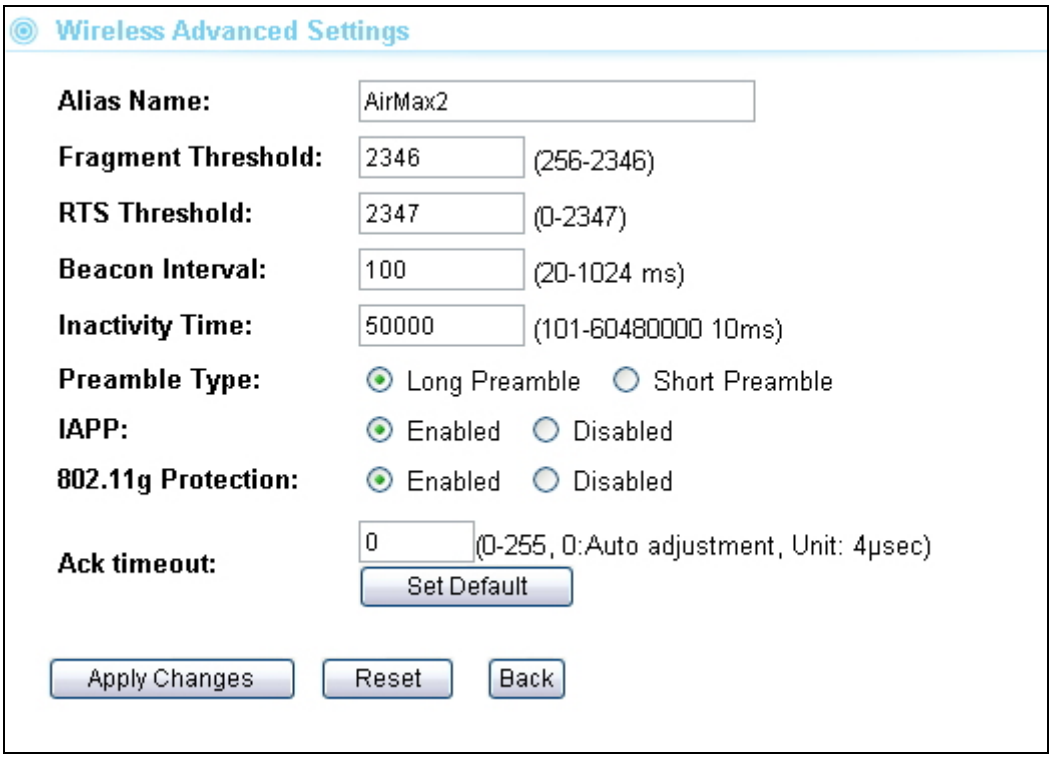
The AirMax2 is equipped with 2 LEDs on the Left side of the housing to indicate the signal strength of current connection. It is very useful in helping you to align the antenna. The signal level are classified into 4 levels, you can change the Thresholds (dividing line) between levels in this setting. The unit for Signal Strength is in Percentage from 0 to 100. The higher.the value, the stronger the signal.

- **No Signal**: When signal strength is less than “Weak Signal Threshold”(for example, 20%) . Both LED are off.
- **Weak Signa**l: When signal strength is greater or equal than the “Weak Signal Threshold”(for example 35%). Only the Blue LED is on.
- **Strong Signal**: When signal strength is greater or equal than the “Strong Signal Threshold”(for example 60%). Only the Green LED is on.
- **Full Signal**: When signal strength is greater or equal than the “Full Signal Threshold”(for example 75%). Both Green and Blue LEDs are on




The Signal LEDs are working only when the connection is established. Therefore, please make sure all wireless settings are correct and the connection is established.

## 4.4 Advance Settings




- **Alias Name:** This function is available only for AP and AP Router mode. You can define the name of the AP in this field.

- **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.

- **Inactivity Time:** The wireless client will be dropped from the network when they are inactive for this amount of time.

- **AckTimeOut:** 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. In most conditions, please put ACKtimeout value at zero(default value). The AP will calculate the ACKtimeout automatically when the value is zero. However, you can also enter the ACKtimeout manually.

- **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.

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

## 4.5 Bridge Mode Settings

### 4.5.1 WDS Settings

For Bridge network, it is required to enter the Wireless MAC address of all remote bridges that is connect directly to your AirMax2. 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.

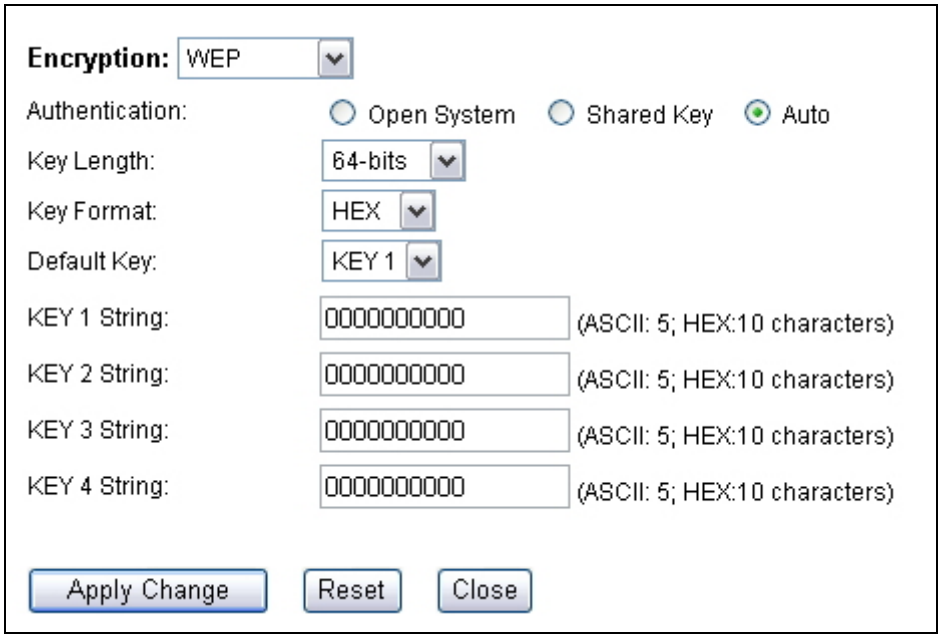
### 4.5.2 WDS Security

***Operation Mode -> Setup -> Security Settings***

Security settings allow you to use encryption to secure your data from eavesdropping. You can select different security policy to provide association authentication and/or data encryption. AirMax2 features various security policies including WEP, 802.1x, WPA, WPA Personal, WPA2, WPA2 Personal , WPA Mixed.

#### WEP

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

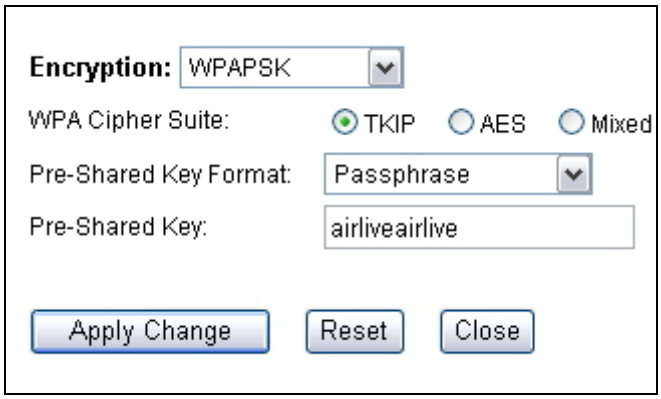



- **Select one of the WEP key for wireless network:** There are total of 4 possible keys for WEP encryption. You need to choose which key will be used for encryption. All wireless devices on the same network have to use the same settings. We recommend using WEP Key 1 as in default setting.

  - **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 AIRMAX2 offers 64bit and 128 bit for WEP key length. The longer the Key Length, the more secure the encryption is.
  - **Key Type:** 2 types are available: ASCII and HEX. ASCII is a string of ASCII code including alphabetical characters, space, signs and numbers (i.e. “airlivepass12”). HEX is a string of 16-bit hexadecimal digits (0..9, a, b, c, d, e, f). All wireless devices on the network must match the exact key length and Key type. Some Wireless clients only allow HEX type for WEP.
  - **ASCII-64:** This is a key with 64-bit key length of ASCII type. Please enter **5** ASCII Characters if you choose this option. For example, “passw”
  - **HEX-64:** This is a key with 64-bit key length of HEX type. Please enter **10** Hexadecimal digits if you choose this option. For example, “12345abcdef”
  - **ASCII-128:** This is a key with 64-bit key length of ASCII type. Please enter **13** ASCII Characters if you choose this option. For example, “airlivewepkey”
  - **HEX-128:** This is a key with 128-bit key length of HEX type. Please enter **26** Hexadecimal digits if you choose this option. For example, “1234567890abcdef1234567890”

## 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 or WPA2-PSK.



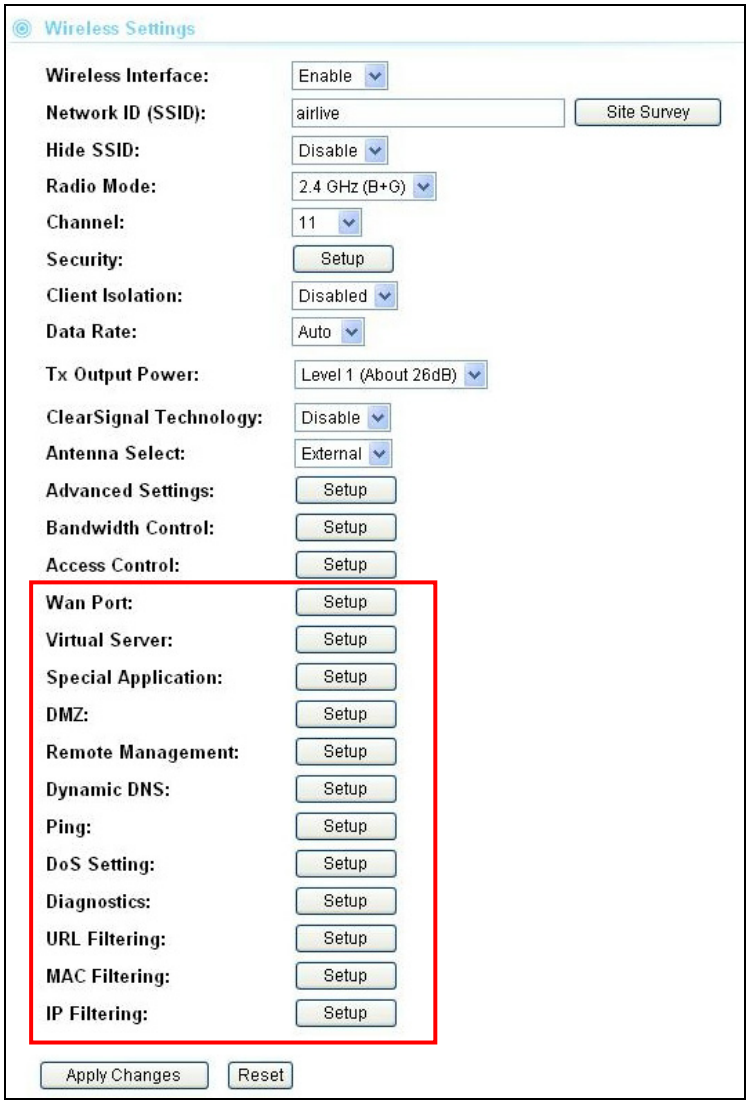

- **Encryption Type**: There are two encryption types **TKIP** and **CCMP (AES)**. While CCMP provides better security than TKIP, some wireless client stations may not be equipped with the hardware to support it. You can select **Mixed** to allow TKIP clients and CCMP clients to connect to the Access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

# 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

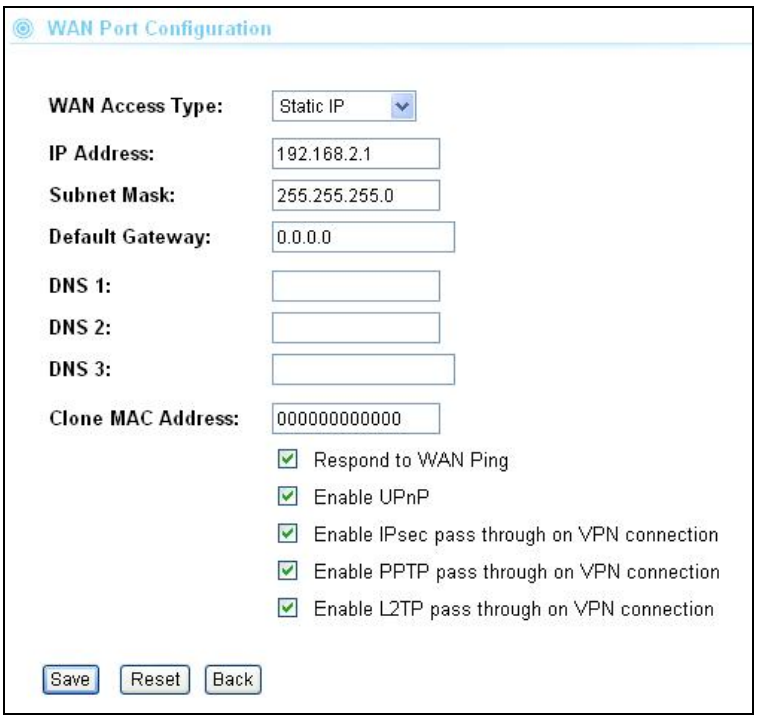
When you choose AP Router, WISP Router, or WISP+Universal modes; the Wireless Setting page will feature router mode functions as indicated on the image below.



## 5.1.1 WAN Port

***Operation Mode -> Setup -> WAN Port***

The AIRMAX2 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

## 5.1.2 DMZ

***Advanced Settings >> Multiple DMZ***

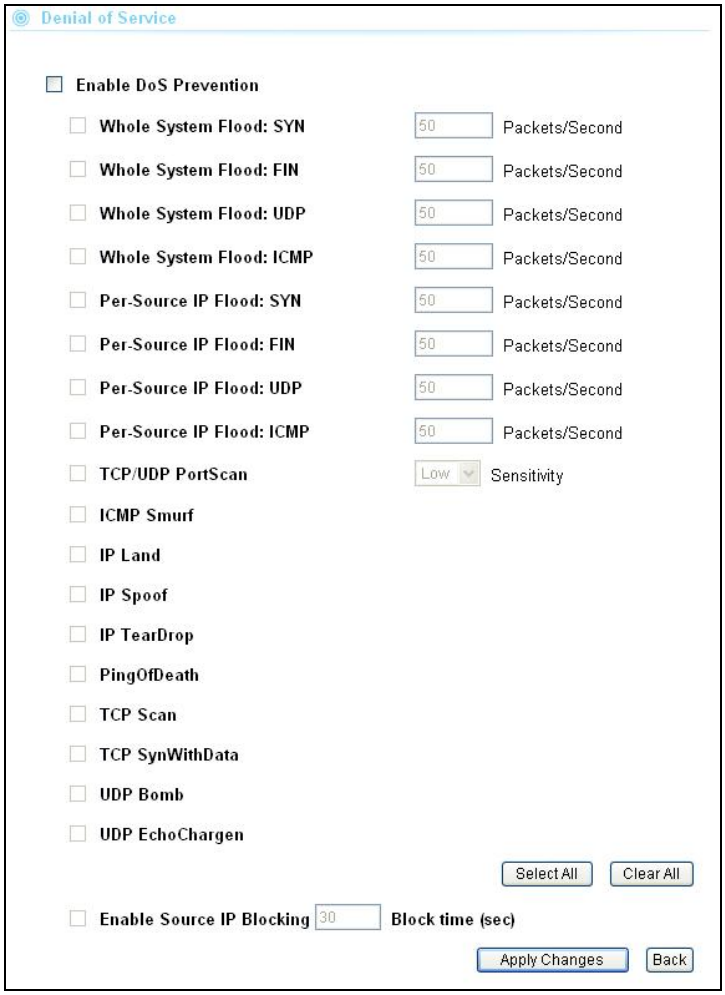
DMZ opens all TCP/UDP ports to particular IP address on the LAN side. It allows setting up servers behind the AIRMAX2.


## 5.1.3 Dynamic DNS

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. The AIRMAX2 support “Dyndns” and “TZO” service.

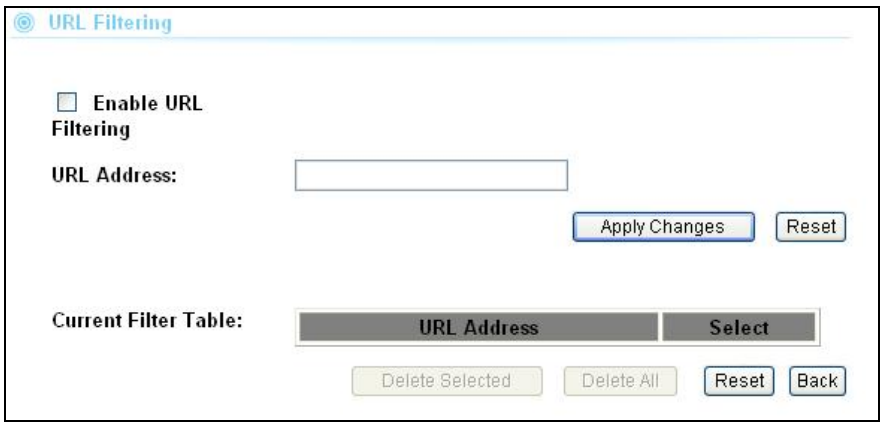

## 5.1.4 DoS (Denial of Service)

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.



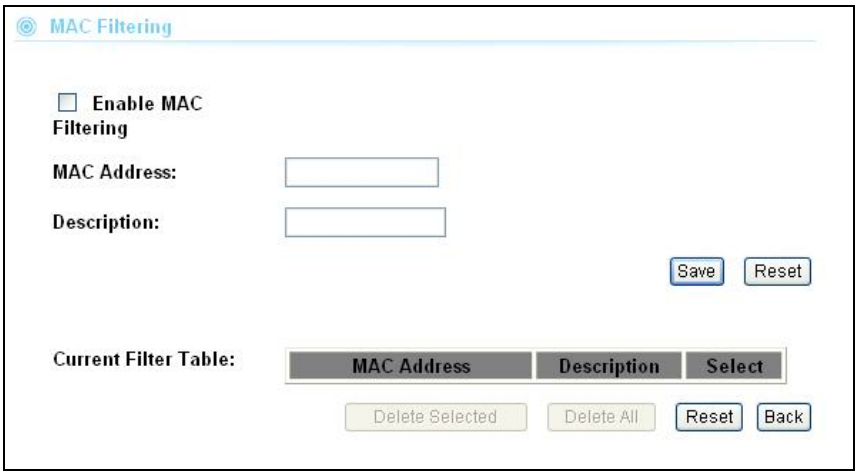
### 5.1.5 URL Filter

The AIRMAX2 provide URL filter function to stop access to certain website. It is especially useful for parents to stop children from accessing some websites.



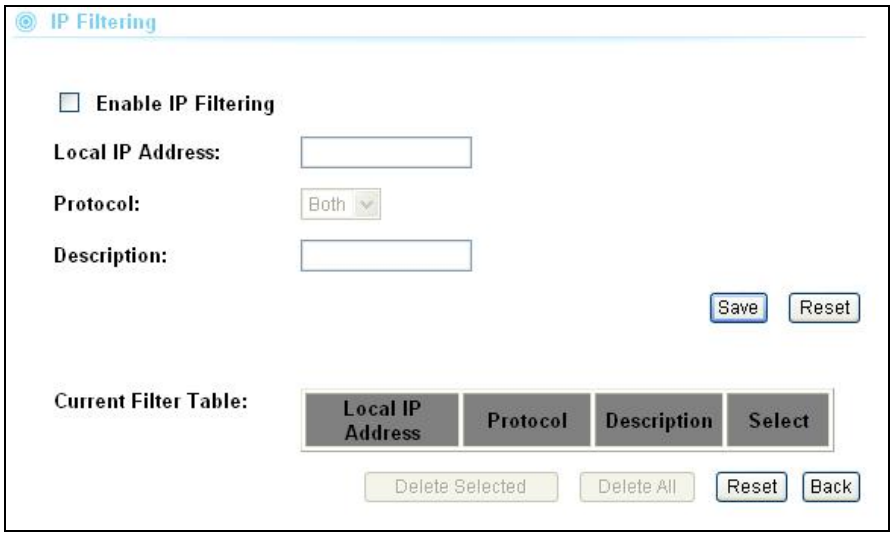

### 5.1.6 MAC Filter

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



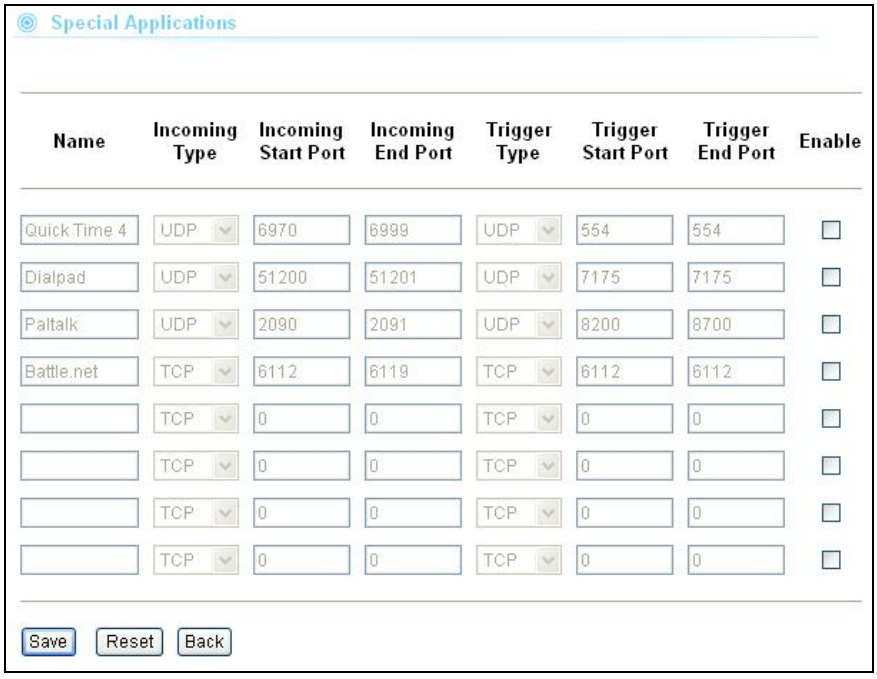

### 5.1.7 IP Filter

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




## 5.1.8 Special Applications

This function enables special Internet audio, video, or game servers that require “Port Trigger” function.

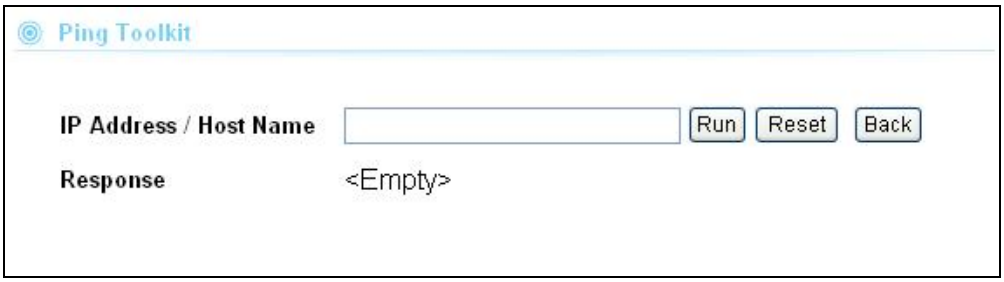



## 5.1.9 Diagnostic (DNS Lookup)

The DNS Lookup can look up for information about a domain name. It will display the IP address and DNS server of a specific domain.

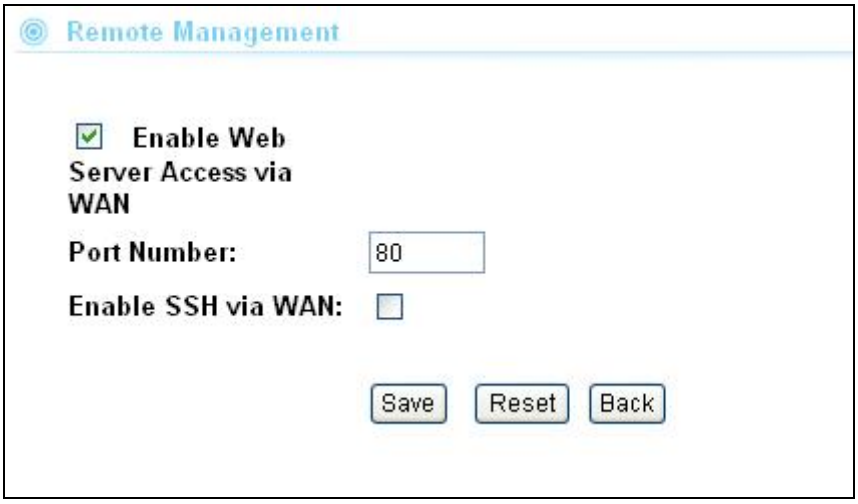

## 5.1.10 PING

The PING function allow you to test whether a remote IP address is accessible from the AirMax2. You can enter either IP address or Domain Name in the foeld.




## 5.1.11 Remote Management

You can enable the web management to allow the AirMax2 be managed from internet. You can change the management port number and/or enable the SSH access from WAN.

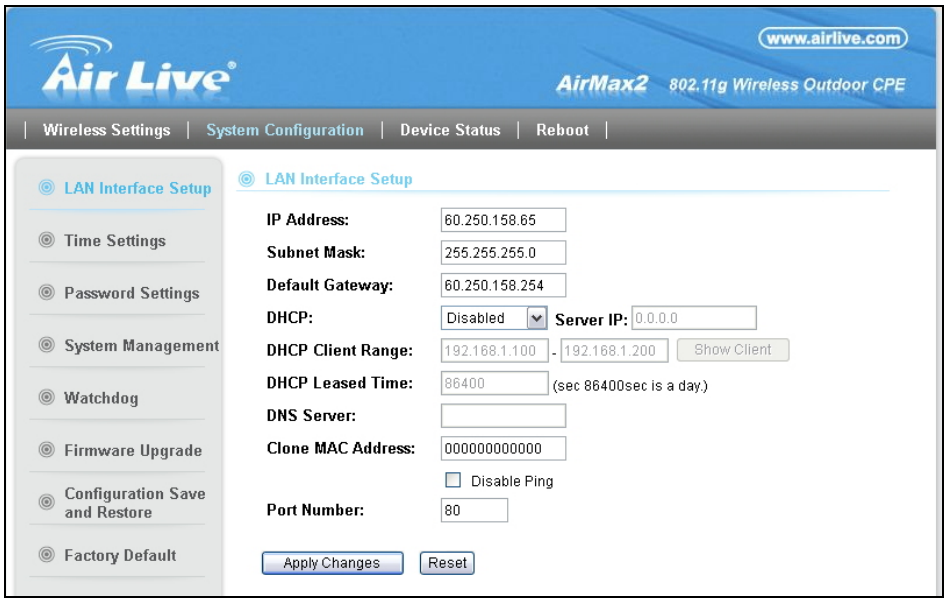


# 6 System Configurations

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

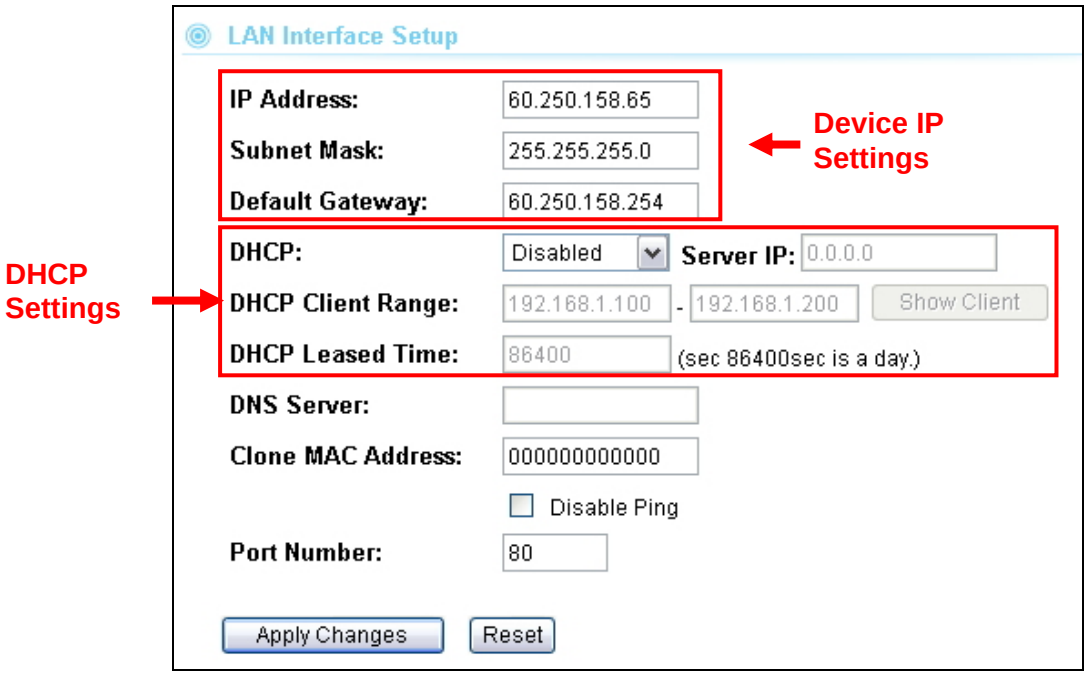
When you click on the "System Configuration" menu on the top menu bar, the following screen will appear. The system configuration includes all non-wireless settings. We will explain their functions here.




## 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 AIRMAX2 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 AIRMAX2 will reserve IP address for a particular PC or Device here.

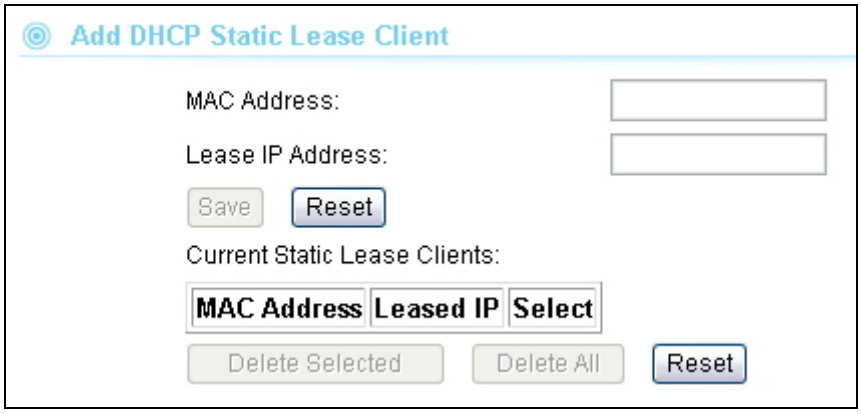
## 6.2.2 Clone MAC Address

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

## 6.2.3 Disable PING

If you do not wish the AIRMAX2 to respond to remote PING command, please disable it here.

### 6.2.4 Add DHCP Static Lease Client



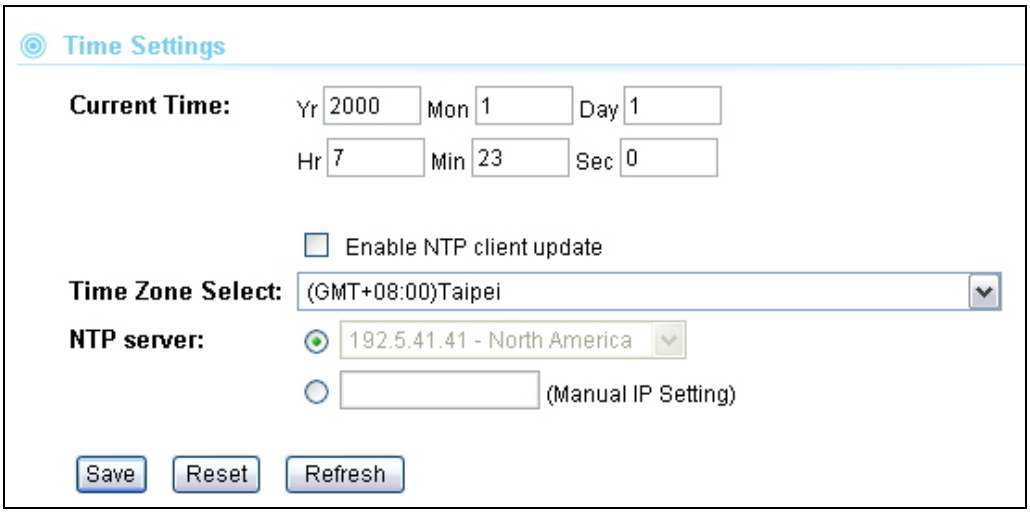

If you want to lock IP address to a MAC address, you should add DHCP clients to the "Static Lease Client". Up to 40 entries can be entered. Below is the procedure for adding an entry:

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

## 6.3 Time Settings

***System Configuration ->Time Settings***

You can set the NTP Time Server for your AIRMAX2's internal clock here. You can use NTP server function so your AIRMAX2 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

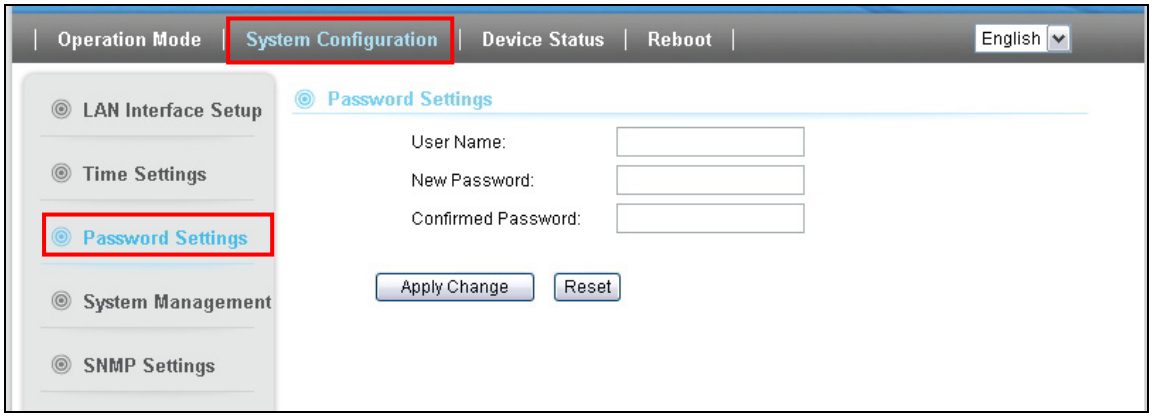
**1.** Check the "Enable NTP Client Update"

2. Select your time Zone
3. Select your NTP server
4. Click on “Apply Change”

## 6.4 Password Settings

***System Configuration -> Password Settings***

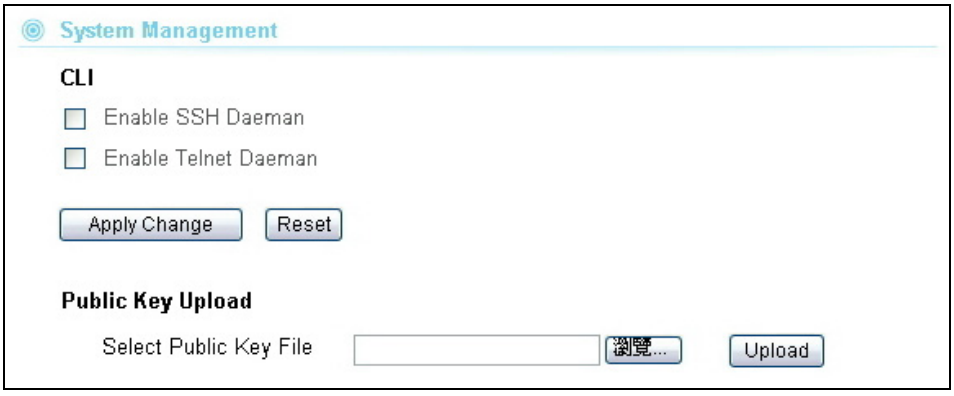
The AIRMAX2’s password protection is turned off by default. To enable password protection or change password, just enter your username and password, and click on “Apply Change” button.




## 6.5 System Management

***System Configuration -> System Management***

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




**CLI (Command Line Interface):**

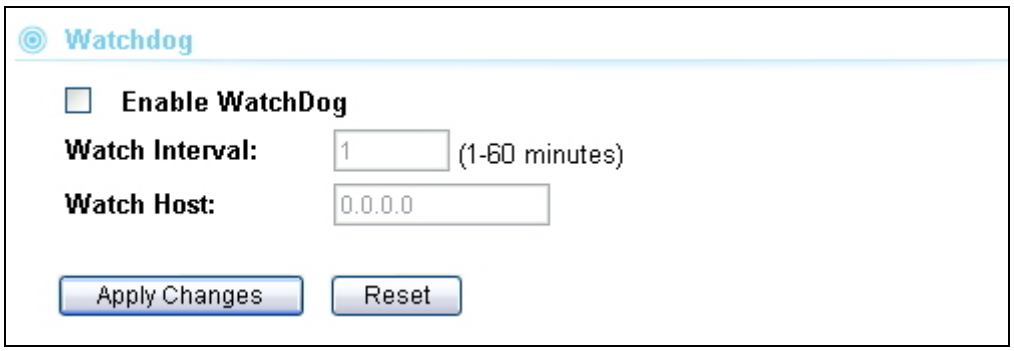
You can enable or disable Telnet and SSH management interface from here.

**Public Key Upload:** You can upload your public for the SSH authentication here.

## 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 can either reconnect or reboot. To prevent the AP from power recycling, the PING watchdog will start 10 minutes after power up to prevent power recycle problem.

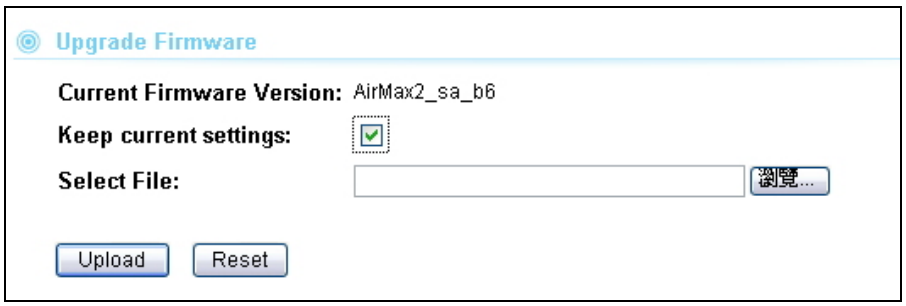



- **Watch Interval:** means: "How often the CPE will PING". For example, it will PING once every "1" minute.
- **Watch Host:** This is the IP address for which the Watchdog will ping.

## 6.7 Firmware Upgrade

***System Configuration -> Firmware Upgrade***

You can upgrade the firmware of your AIRMAX2 (the software that controls your AIRMAX2'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 AIRMAX2 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 AIRMAX2. 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 AIRMAX2 unless the new firmware has new features you need or if it has a fix to a problem that you've encountered.

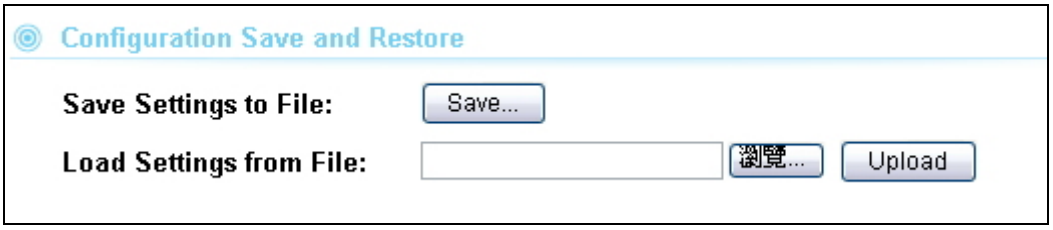
## 6.8 Configuration Save and Restore

***System Configuration -> Configuration Save and Restore***

The AIRMAX2 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 AIRMAX2 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:**

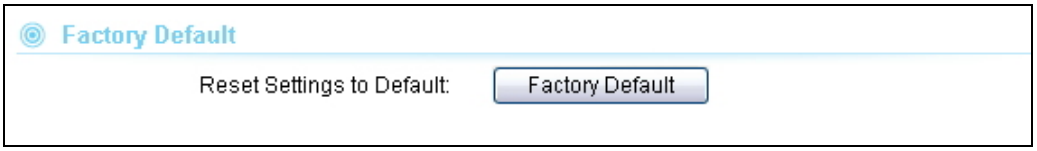
**Step1**: Enter the file name in the “Load Settings from File” field. Or click on “Browse” button to location the location of the file.

**Step2**: Click on “Upload” button to restore settings.

## 6.9 Factory Default

***System Configuration -> Factory Default***

You can reset the configuration of your AIRMAX2 to the factory default settings.

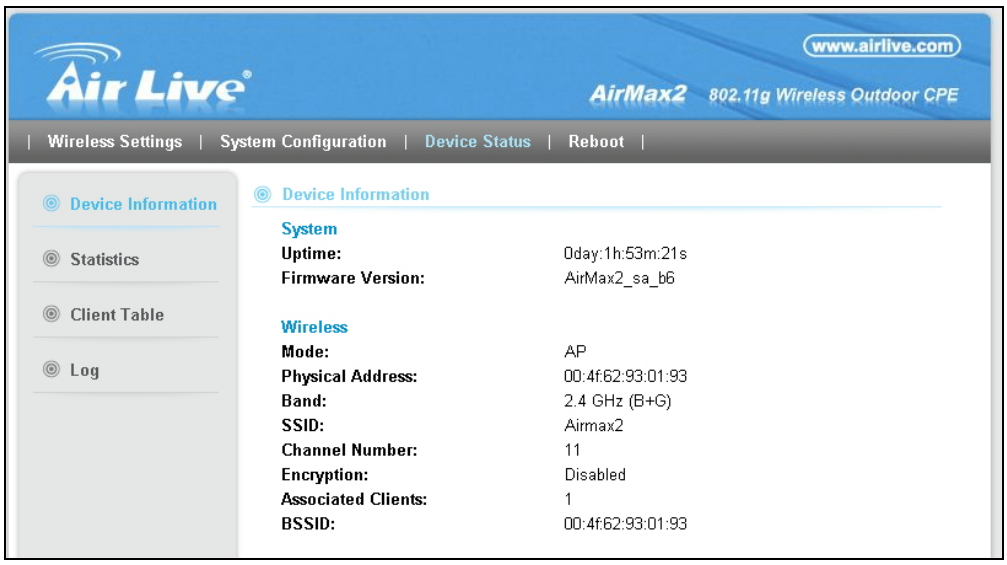


# 7 Device Status Menu

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 AIRMAX2 such as Uptime, Firmware version, Wireless Interface…etc. Below are some additional explanations on some status information of this page:

- **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 AirMax2. 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 | |
|---|---|
| **Mode:** | AP |
| **Physical Address:** | 00:4f:62:93:01:93 |
| **Band:** | 2.4 GHz (B+G) |
| **SSID:** | Airmax2 |
| **Channel Number:** | 11 |
| **Encryption:** | Disabled |
| **Associated Clients:** | 1 |
| **BSSID:** | 00:4f:62:93:01:93 |

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

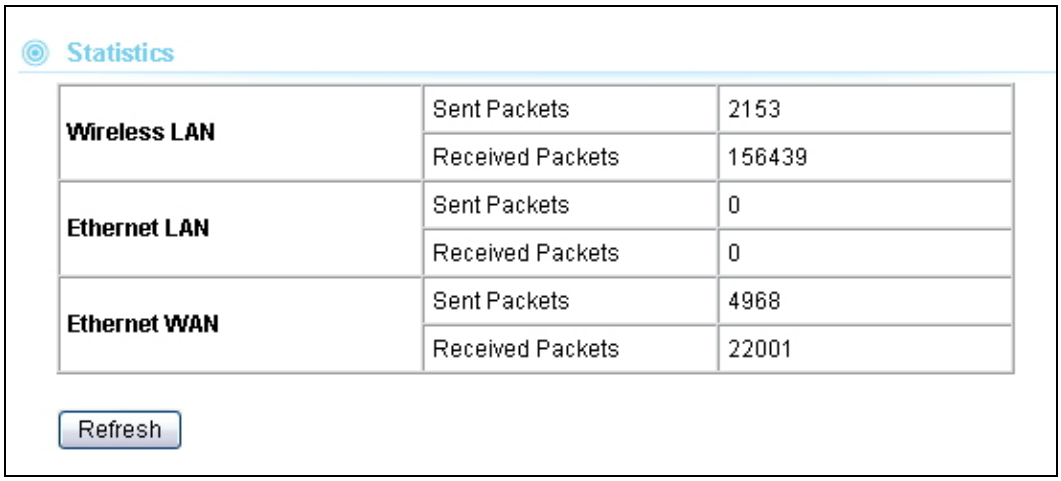
| LAN Configuration | |
|---|---|
| **Connection Method:** | Fixed IP |
| **Physical Address:** | 00:4f:62:93:01:91 |
| **IP Address:** | 192.168.1.1 |
| **Network Mask:** | 255.255.255.0 |
| **DHCP Server:** | ON |
| **DHCP Start IP Address:** | 192.168.1.100 |
| **DHCP Finish IP Address:** | 192.168.1.200 |

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

| Internet Configuration | |
|---|---|
| **Connection Method:** | PPPoE Connected |
| **Physical Address:** | 00:4f:62:93:01:92 |
| **IP Address:** | 61.217.146.176 |
| **Network Mask:** | 255.255.255.255 |
| **Default Gateway:** | 61.217.144.254 |

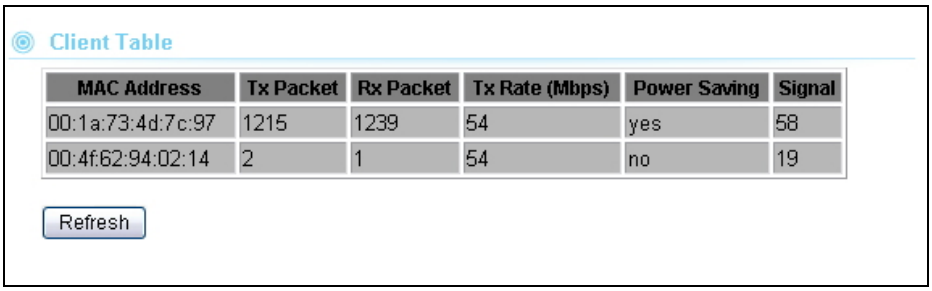
## 7.3 Statistic

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




## 7.4 Client Table

It will show all wireless device connected to the AIRMAX2. 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).




## 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**: register all logs
  - **Wireless**: register wireless log only

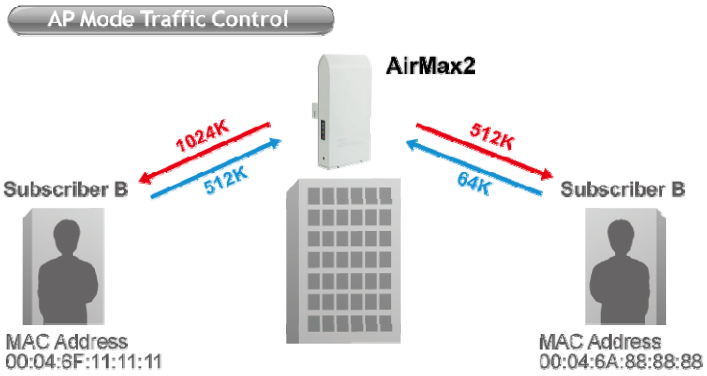
.

# 8 Bandwidth Control

In this chapter, you will learn how to utilize AirMax2's Bandwidth Control function. The Bandwidth Control settings can be found in the "Wireless Settings" page on the AirMax2'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 operators can offer different class of connection speeds for different subscription fees - just like the ADSL service! The AirLive advance firmware can control the bandwidth by Interface or IP/MAC.




## 8.2 Type of Bandwidth Control

AirMax2's Bandwidth Control function limits the "Maximum Data Rate". There are 2 types of Bandwidth Control it offers.

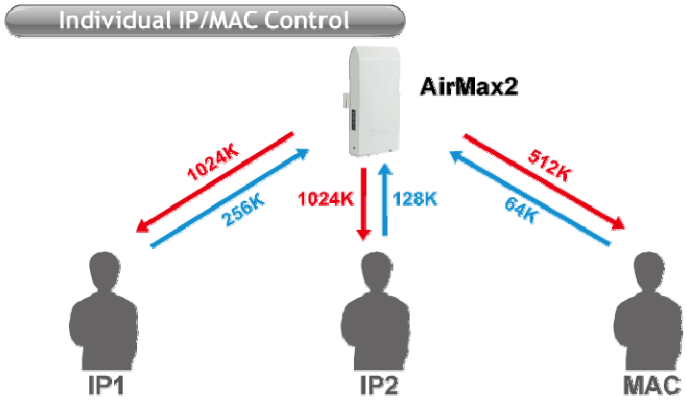
### 8.2.1 Interface Control

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

data rate


### 8.2.2 Individual IP/MAC Control

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

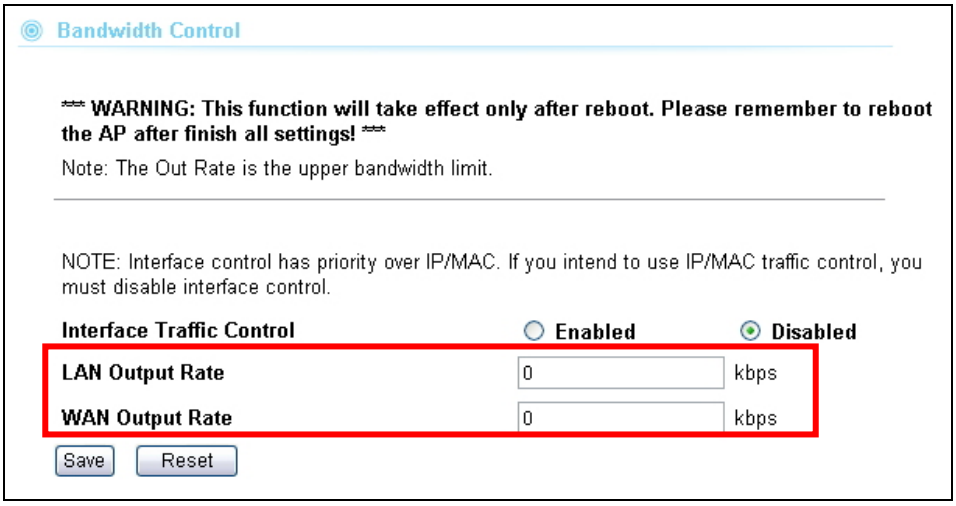



## 8.3 What is “Out Rate”?

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

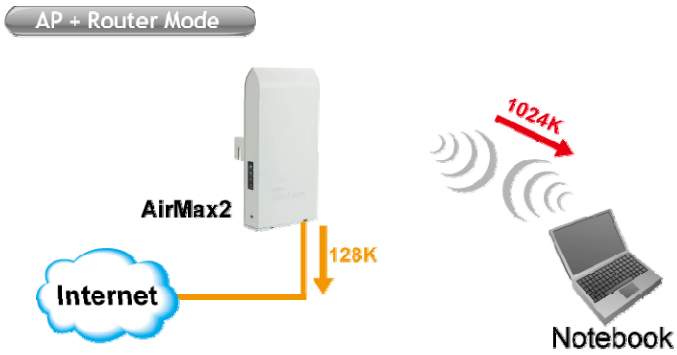
1. **LAN Output Rate**: This is the speed of the traffic out of the LAN port. In gateway mode, the LAN Output Rate includes both the wired LAN and WLAN interface.
2. **WLAN Output Rate**: This is the speed of the traffic out of the Wireless LAN
3. **WAN Output Rate**: This is the speed of the traffic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

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




In the below Diagram:

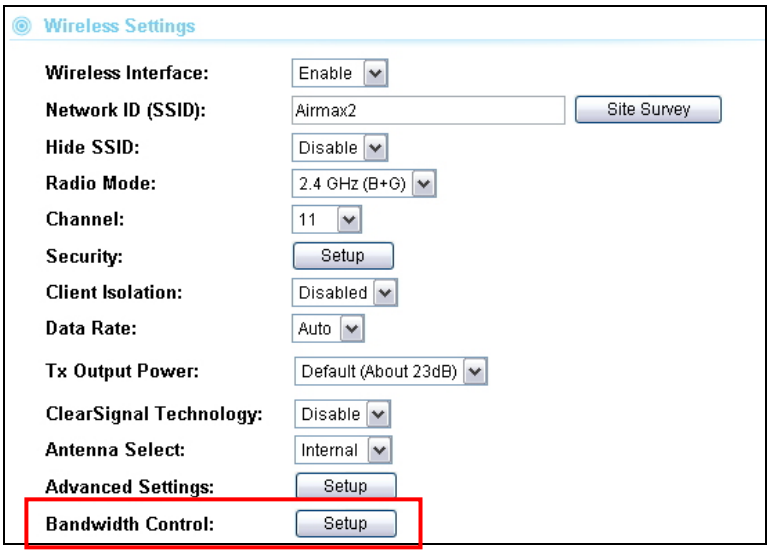
- The AP is in Gateway Mode
- The WAN Output Rate is 128K
- The LAN/WLAN Output Rate is 1024K



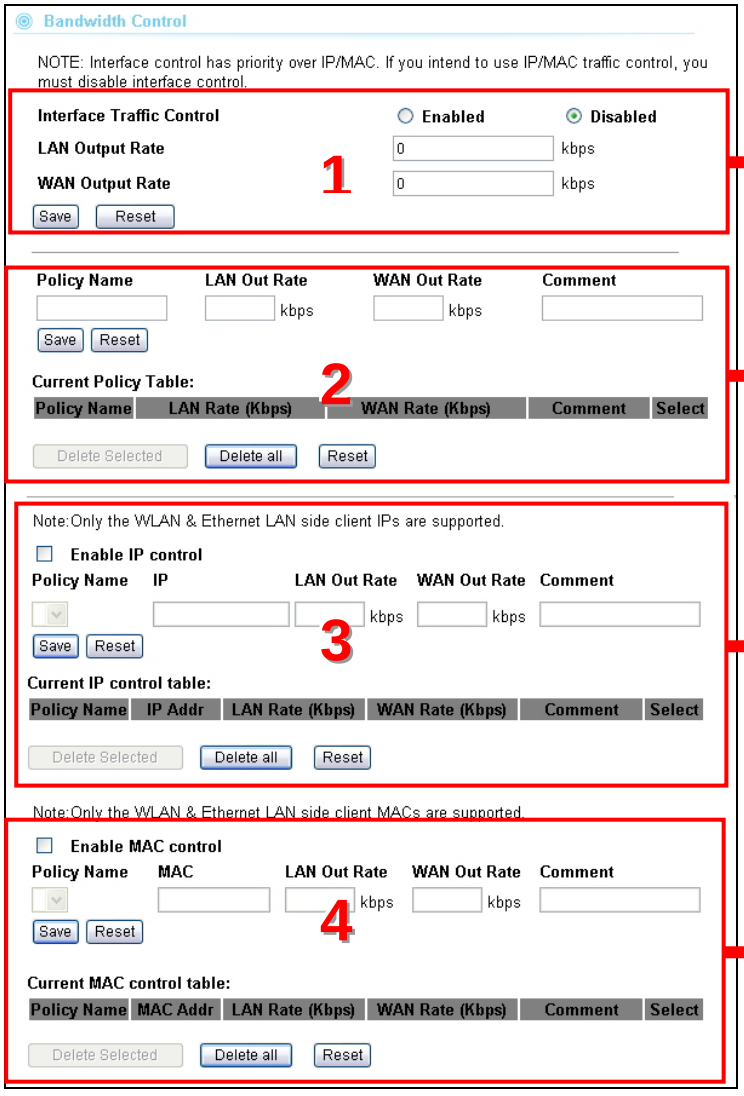

In this setup, the notebook users get an upstream bandwidth of 128K and downstream bandwidth of 1024K.

## 8.4 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.



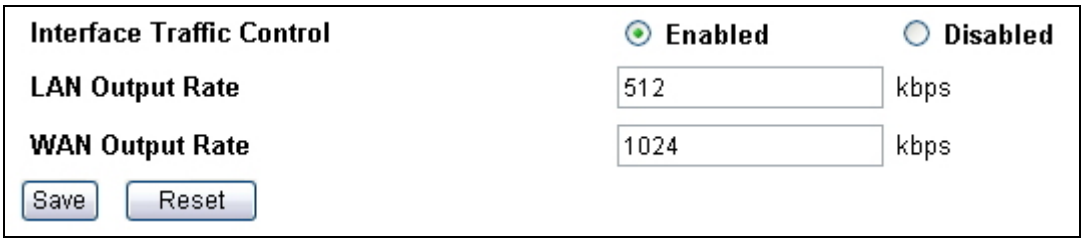

This section is the "Interface Control" session. You must disable the "interface Bandwidth Control" if you want to use the "IP/MAC Bandwidth Control"

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

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

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

## 8.4.1 Interface Control Settings

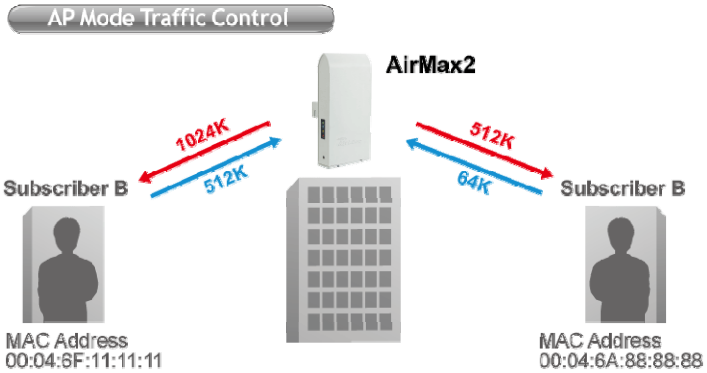



In the Interface Control Settings, the AP only controls the total bandwidth limit of an interface. For example, if you want to limit the output data rate of the LAN to 512K and the output data rate of WLAN to 1024K. You should perform the following steps:

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

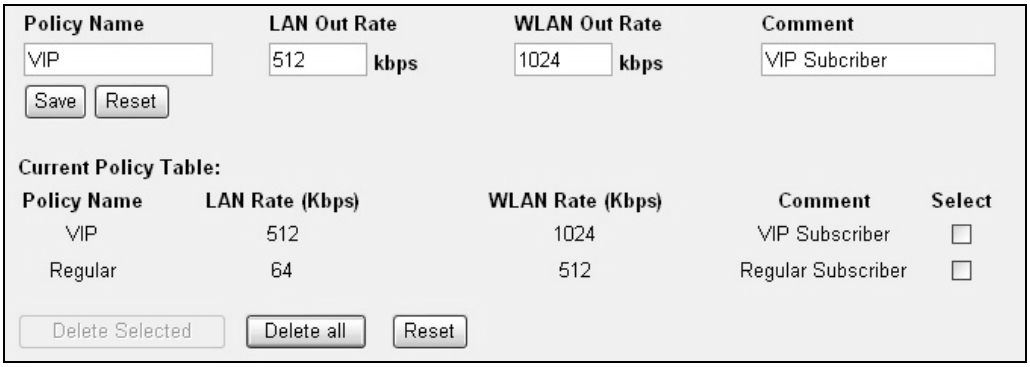

## 8.4.2 Define Policy

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



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

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




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

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

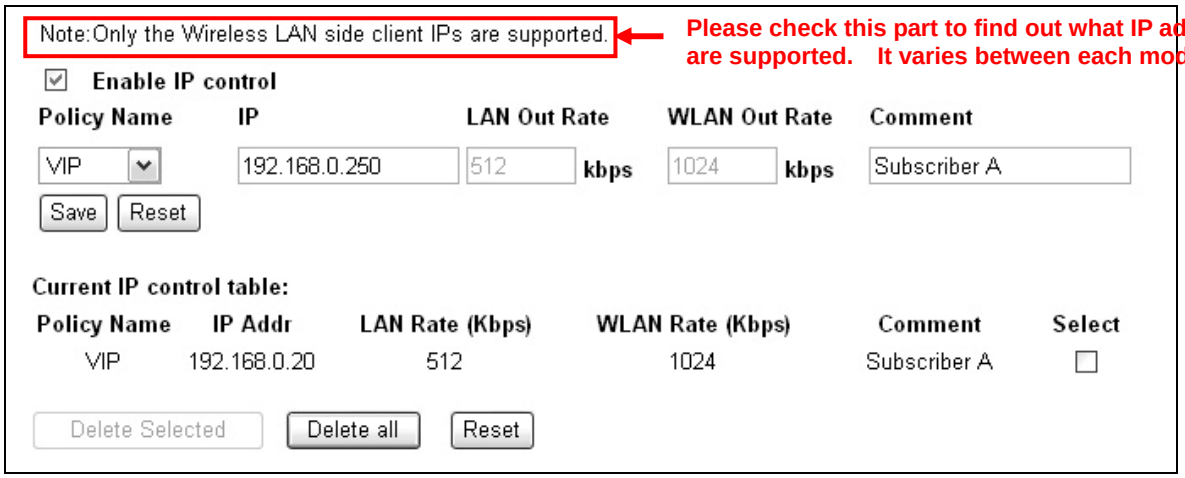
Once finished, the administrator will be able to choose the policy “VIP” for their IP/MAC Bandwidth Control.

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




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

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

### 8.4.4 Control by MAC Address

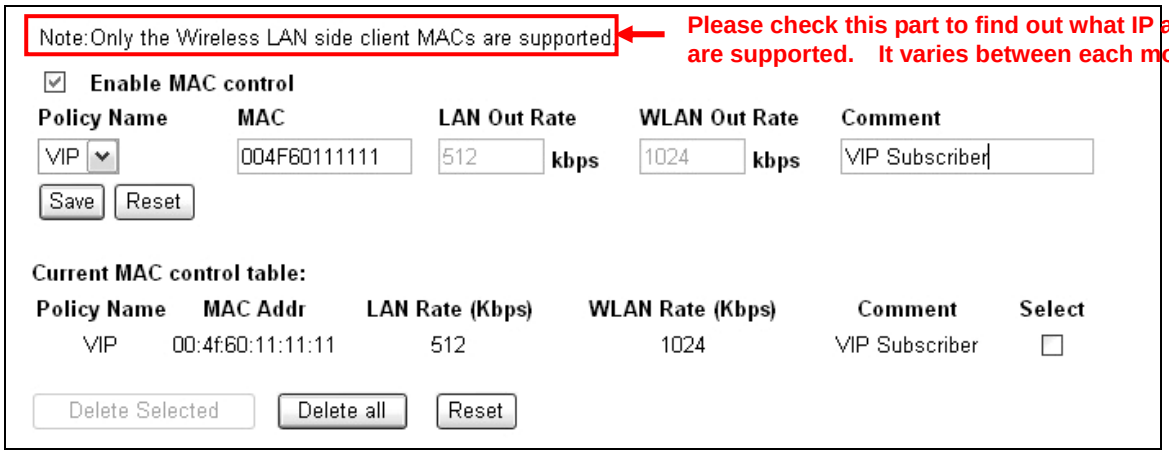
You can set the maximum bandwidth of a PC or a subscriber by using the MAC Control.

Please follow the procedure below to setup MAC Bandwidth Control:

1. Please make sure the “Interface Bandwidth Control” is disabled

2. Before you start, please check the following area to see which client MACs are supported. It differs between each mode.

3. Enable the MAC Control




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

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

# 9 Command Line Interface

In this chapter, we will explain commands that are available through Telnet or SSH interface.

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

- **Telnet**
  - Password: airlive
- **SSH**
  - Login: admin
  - Password: airlive

## 9.1 Available Commands

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

| | | | |
|---|---|---|---|
| | | | <key> |
| | | | wpa [tkip\|aes] <pass\|hex> <key> [gklt] |
| | | | wpa2 [mixed\|aes] <pass\|hex> <key> [gklt] |
| | stp | [on\|off] | |
| | isolation | [on\|off] | |
| wlan | | | |
| | alias | [string] | |
| [Mode] Site Survey | | | |
| wlan | | | |
| | survey | | |
| | | connect | [id] |
| | | | (only support in Client, WISP, Universal Repeater Mode, WISP + Universal Repeater Mode ) |
| [Mode] Security | | | |
| wlan | | | |
| | auth | [open\|share\|auto] | |
| | security | | |
| | | encrypt | [off] |
| | | | wep [64\|128] <ascii\|hex> <1:key1\|2:key2\|3:key3\|4 :key4> <key> |
| | | | wpa [tkip\|aes] <pass\|hex> <key> [gklt] |
| | | | wpa2 [mixed\|aes] <pass\|hex> <key> [gklt] |
| | | 1x | [off\|on <port> <ip_addr> <password> <wep [64\|128]\|wpa [tkip\|aes]\|wpa2 [mixed\|aes]>] |
| | | preauth | [on\|off] |
| | | account | [off\|on <port> <ip_addr> <password>] |
| [Mode] Advanced Settings | | | |
| wlan | | | wlan |
| | preamble | [long\|short] | |
| | bssid | [on\|off] | |
| | iapp | [on\|off] | |
| | protect11g | [on\|off] | |
| | fragment | <256~2346> | |
| | rts | <0~2347> | |
| | beacon | <20~1024> | |
| | inactivity | <100~60480000> | |
| | datarate | <0~12> | |
| | txpower | <1~10> | |
| | watchdog | [off\|on <interval:1~60> <host>] | |
| [Mode] Access Control | | | |
| wlan | | | |
| | acl | | |

| | | | |
|---|---|---|---|
| | | disp | |
| | | off | |
| | | allow | |
| | | deny | |
| | | add [mac] | |
| | | delete [id] | |
| | | clearall | |
| [Mode] Wan Port | | | |
| wan | | | |
| | clone | [mac_addr] | |
| | dns | [auto\|manual] | |
| | static | [ip_addr <netmask> <gateway>] | |
| | dhcp | [on\|release\|renew] | |
| | pppoe | <username> <password> [svname 0\|1 <service_name>] <auth_type> <mppe> <mtu_value> dynwan dynpppoe [connect 0\|1 <timeout>\|2] | |
| | pptp | <ip [server_ip]\|url [server_url]> <username> <password> <auth_type> <mppe> <mtu_value> [static <ip_addr> <netmask> <gateway>\|dynamic] | |
| | l2tp | <ip [server_ip]\|url [server_url]> <username> <password> <auth_type> <mppe> <mtu_value> [static <ip_addr> <netmask> <gateway>\|dynamic] <timeout> | |
| | | auth_type: 0. PAP 1. CHAP 2. MSCHAP 3. MSCHAP2 | |
| | | mppe: 0. none 1. 40bits 2. 56bits 3. 128bits | |
| | link | [status\|set <mode>] | |
| | protocol | status | |
| sys | server | access | icmp <0:disabled\|1:enabled> |
| | passthruvpn | ipsec <0:disabled\|1:enabled> | |
| | passthruvpn | pptp <0:disabled\|1:enabled> | |
| | passthruvpn | l2tp <0:disabled\|1:enabled> | |
| [Mode] Virtual Servers | | | |
| ip | | | |
| | nat | | |
| | | server | |
| | | | disp |

| | | | |
|---|---|---|---|
| | | | delete [id] |
| | | | clearall |
| | | | add <ser_ip> <server> [proto <from_port [to_port]>] |
| | | | server: 0. Customize 1. Web, 2. FTP, 3. POP3, 4. SMTP, 5. DNS, 6. Telnet |
| | | | proto: 1. TCP+UDP, 2. TCP, 3. UDP |
| [Mode] Special Applications | | | |
| ip | | | |
| | nat | | |
| | | service | |
| | | | disp |
| | | | sap1 [on\|off\|clear\|edit <name> <in_proto> <in_from_port> <in_to_port> <trig_proto> <trig_from_port> <trig_to_port>] |
| | | | sap2 [on\|off\|clear\|edit <name> <in_proto> <in_from_port> <in_to_port> <trig_proto> <trig_from_port> <trig_to_port>] |
| | | | sap3 [on\|off\|clear\|edit <name> <in_proto> <in_from_port> <in_to_port> <trig_proto> <trig_from_port> <trig_to_port>] |
| | | | sap4 [on\|off\|clear\|edit <name> <in_proto> <in_from_port> <in_to_port> <trig_proto> <trig_from_port> <trig_to_port>] |
| | | | sap5 [on\|off\|clear\|edit <name> <in_proto> <in_from_port> <in_to_port> <trig_proto> <trig_from_port> <trig_to_port>] |
| | | | sap6 [on\|off\|clear\|edit <name> <in_proto> <in_from_port> <in_to_port> <trig_proto> |

| | | | |
|---|---|---|---|
| | | | <trig_from_port> <trig_to_port>] |
| | | | sap7 [on\|off\|clear\|edit <name> <in_proto> <in_from_port> <in_to_port> <trig_proto> <trig_from_port> <trig_to_port>] |
| | | | sap8 [on\|off\|clear\|edit <name> <in_proto> <in_from_port> <in_to_port> <trig_proto> <trig_from_port> <trig_to_port>] |
| | | | proto: 1. TCP+UDP, 2. TCP, 3. UDP |
| [Mode] Remote Management | | | |
| sys | | | |
| | server | access | web <0:disabled\|1:enabled> |
| | | port | web <portnum> |
| | | access | telnet <0:disabled\|1:enabled> |
| [Mode] URL Filtering | | | |
| ip | | | |
| | urlfilter | | |
| | | customize | |
| | | | disp |
| | | | add [string] |
| | | | delete [id] |
| | | | clearall |
| [Mode] MAC Filtering | | | |
| ip | | | |
| | macfilter | | |
| | | customize | |
| | | | disp |
| | | | add [mac_addr] |
| | | | delete [id] |
| | | | clearall |
| [Mode] IP Filtering | | | |
| ip | | | |
| | ipfilter | | |
| | | customize | |
| | | | disp |
| | | | add [ip_addr] <1:tcp+udp\|2:tcp\|3:udp> |
| | | | delete [id] |
| | | | clearall |
| [Mode] Traffic Control(Qos) | | | |
| qos | | | |
| | disableif | | |
| | enableif | lanoutput [output rate] | |

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

| | | | |
|---|---|---|---|
| | | eath><tcpscan><tcpsynwithdata><udpbomb><udpechochargen><srcipblocktime > | |
| [Mode] Dynamic DNS | | | |
| ddns | | | |
| | enabledyndns | <Domain Name><User Name/Email><Password/Key> | |
| | enabletzo | <Domain Name><User Name/Email><Password/Key> | |
| | disableddns | | |
| | result | | |
| [Status] Statistics | | | |
| ip | | | |
| | status | | |
| [Status] Active Wireless Client Table | | | |
| wlan | | | |
| | association | | |
| [TCP/IP] LAN Interface Setup | | | |
| ip | address | [addr] | |
| | subnetmask | [netmask] | |
| | gateway | [addr] | |
| | dhcp | on | [client\|server\|relay <server_ip>] |
| | | off | |
| | | client | |
| | | | [start_ip <end_ip>] |
| | | status | |
| | dns | | |
| | | server | |
| | | | [ip1 <ip2> <ip3>] |
| | | status | |
| [Reboot] Reboot System | | | |
| reboot | | | |
| [Other] Password | | | |
| sys | | | |
| | password | [pw] | (if [pw] is empty, then clear the password) |
| [Other] Save / Reload Setting | | | |
| save | | | |
| factorydefault | | | |
| [Other] NTP | | | |
| sys | | | |
| | ntp | | |
| | | showcurrenttime | |
| | | setcurrenttime | <yyyy/mm/dd/hh/MM/ss> |
| | | enablentp | |
| | | timezoneselect | <zone num> |
| | | ntpserver | <servernum> |
| | | | manualipsetting <ip> |
| | | disablentp | |
| [Other] System Log | | | |
| sys | | | |

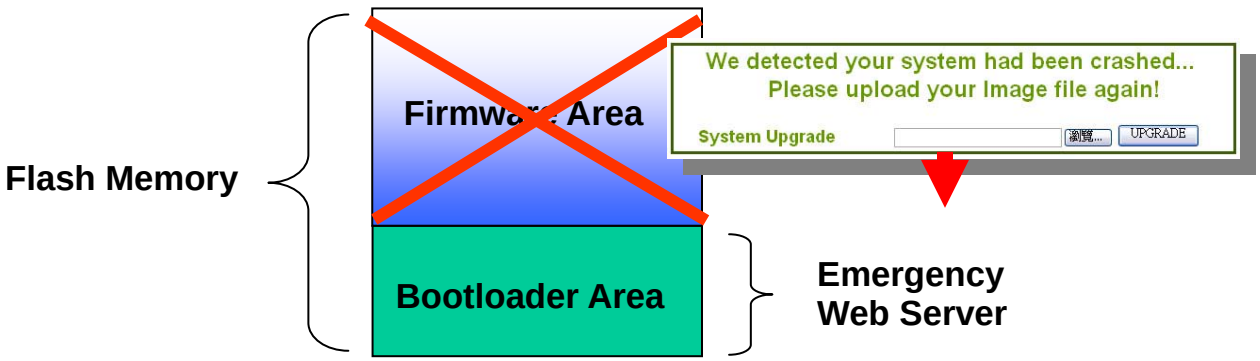
| | | | |
|---|---|---|---|
| | log | | |
| | | disable | |
| | | enablesysall | [showsysall] |
| | | enablewlanonly | [showwlanonly] |
| | | clear | |

# 10 Emergency Firmware Recovery

The AIRMAX2 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 192.168.1.1. If you can't find it, then please perform the emergency upgrade.

## 10.1 How Emergency Upgrade Works?

AIRMAX2'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***.




## 10.2 Emergency Upgrade Procedure

1. Please connect your PC directly to the LAN Port ***of AirMax2***
2. set your PC's IP address to 192.168.1.50
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 "Green Color" LED light on(about 2 seconds). Then release the reset button.

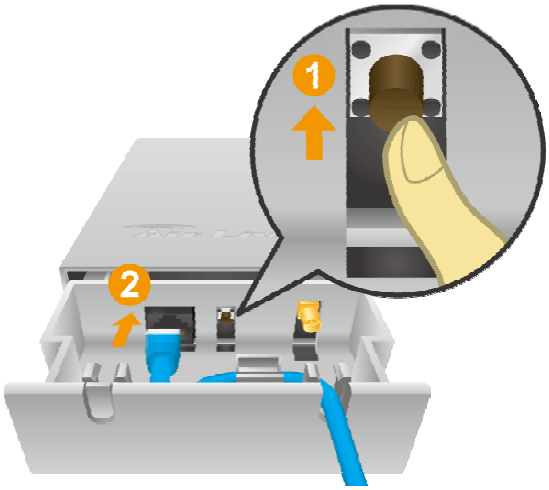



**Fig 1-2 : Press and hold the reset button while plugging in the power.**

6. Open a browser; type “192.168.1.6” for the website address. The following screen should show up


7. Click the “Browse” button, select and open the correct firmware file. Please go to www.airlive.com to AIRMAX2’s support page and download.

8. Click on “UPGRADE” button. Do not touch the AP or PC until the upgrade is completed.

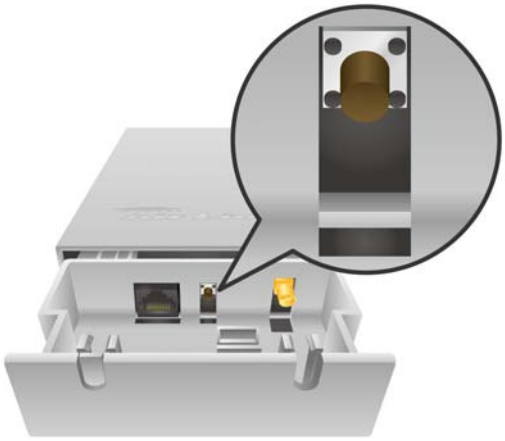
9. Wait for AP to finish reboot. Open the web browser, and type “192.168.1.254”. You should be able to login into the normal Web UI.

# 11 Frequent Asked Questions

In this chapter, we will address some frequent asked questions about AirMax2

**Question:** I forgot my password or the IP address of AirMax2.

**Answer**: Please restore your settings to default by press the reset button for more than 5 seconds. You should be able to find your AirMax2 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 AirMax5 after all the settings are changed.

==========

**Question:** Where can I purchase the optional metal Mounting Kit?

**Answer**: The part number for the mounting kit is “WMK-AIRMAX”. Please ask your authorized AirLive distributor for availability.

==========

==========

**Question:** When I plug in the POE cable and power adapter, the AirMax2'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:** I tried the Emergency Upgrade procedure. But it doesn't work, why?

**Answer**: It is recommended to use IE6, IE8, or Firefox 3.5.4 above.

==========

**Question:** Why can't I receive any signal from AirMax2's built in antenna?

**Answer**: The AirMax2's built-in antenna is a patch antenna that sends and receive signal in the forward direction of the CPE with 70 degree angle horizontal and 38 degree vertically. Please see diagram below:

==========

**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:** When I use “Site Survey”, why does the Signal LED goes off?

**Answer**: When you click on the Site Survey, the AirMax2 thinks you are trying to choose a new network to associate. Therefore, it will disconnect from current connection and wait until you establish a new connection.

==========

# 12 Specifications

The specification of AirMax2 is subject to change without notice. Please use the information with caution.

## 12.1 Hardware Features

### 12.1.1 General Hardware Feature

- 802.11g/b Radio
- 4MB Flash, 16MB SDRAM
- RoHS compliant
- One 10/100 Mbps Ethernet Port / PoE Port with Auto MDI/MDI-X support
- 12V Passive PoE
- 26dBm Transmit Output power (20dBm in EU)
- Rain and splash proof housing
- 4 LED indicators with RSSI LED function
- Optional Metal Wall / Pole Mount Kit

### 12.1.2 Antenna

- Integrated 8.03 dBi patch directional antenn
- Vertical Polarizations

- H-Plane Coverage Angle: 70 degree in the forward direction
- E-Plane Coverage Angle: 38 degree in the forward direction

### 12.1.3 Power Supply

- Power Adapter Voltage : input 100~240Vac/50~60Hz , output 12V/1A
- Advance Passive PoE (Accept 12 volts)
- POE Adapter, DC Injector provided

### 12.1.4 Dimension and Weight

- Dimension: 210 x 100 x 32 mm
- Package Weight: 750g

## 12.2 Radio Specifications

### 12.2.1 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

### 12.2.3 Rate and Modulation

- **Data Rate :** 6, 9, 12, 18, 24, 36, 48, 54Mbps
- **Modulation:**
  - 11g Orthogonal Frequency Division Multiplexing (OFDM)
  - 11b Direct Sequence Spread Spectrum (CCK, DQPSK, DBPSK)

### 12.2.4 TX Output Power

- 20dBm (ETSI: Europe)
- 23dBm (FCC: United States)
- 26dBm (South America)

### 12.2.5 Receiver Sensitivity

| | | | |
|---|---|---|---|
| IEEE 802.11b | Min (dBm) | 1Mbps | -95 |
| | | 2Mbps | -91 |
| | | 5.5Mbps | -90 |
| | | 11Mbps | -86 |
| IEEE 802.11g | Min (dBm) | 6Mbps | -86 |
| | | 9Mbps | -86 |
| | | 12Mbps | -85 |

| | | | |
|---|---|---|---|
| | | 18Mbps | -83 |
| | | 24Mbps | -81 |
| | | 36Mbps | -77 |
| | | 48Mbps | -73 |
| | | 54Mbps | -71 |

### 12.2.6 Supported WLAN Mode

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

## 12.3 Software Feature

### 12.3.1 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

### 12.3.2 Management Interface

- Web HTTP
- Secured Web (HTTPS)
- Telnet (CLI)
- SSH (Secured Shell)

# 13 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 AIRMAX2 provide ACK adjustment capability in form of either distance or direct input. When you enter the distance parameter, the AIRMAX2 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 device must set the trunking feature to work.

**MAC**

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

**Mbps**

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

**MESH**

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

**MIMO**

Multi In Multi Out. A Smart Antenna technology designed to increase the coverage and performance of a WLAN network. In a MIMO device, 2 or more antennas are used to

increase the receiver sensitivity and to focus available power at intended Rx.

**NAT**

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

**Node**

A network connection end point, typically a computer.

**Packet**

A unit of data sent over a network.

**Passphrase**

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

**POE**

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

**Port**

This word has 2 different meaning for networking.

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

**PPPoE**

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

**PPTP**

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

**Preamble Type**

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

**Rate Control**

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

**RADIUS**

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

**Receiver Sensitivity**

Receiver sensitivity means how sensitive is the radio for receiving signal. In general; the

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

**RJ-45**

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

**Router**

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

**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.