



AirMax5X Series
5G High Throughput Outdoor
CPE with PoE Pass through
User's Manual



www.airlive.com



Version 3.0

This guide is written for firmware version 3.0 or later.

Copyright & Disclaimer

No part of this publication may be reproduced in any form or by any means, whether electronic, mechanical, photocopying, or recording without the written consent of OvisLink Corp.

OvisLink Corp. has made the best effort to ensure the accuracy of the information in this user's guide. However, we are not liable for the inaccuracies or errors in this guide. Please use with caution. All information is subject to change without notice

This product requires professional installation. Please do not attempt to install the device without the necessary knowledge in regards to your country's wireless regulations.

Functions and features in your product's firmware might be different due to regulations in your country.



Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- . Reorient or relocate the receiving antenna.
- . Increase the separation between the equipment and receiver.
- . Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- . Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: To assure continued compliance, any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. (Example - use only shielded interface cables when connecting to computer or peripheral devices).

FCC Radiation Exposure Statement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

The antennas used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

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.

All Trademarks are properties of their respective holders.

Table of Contents

1. Introduction	1
1.1 Overview	1
1.2 Special Notice	2
1.3 How to Use This Guide	2
1.4 Firmware Upgrade and Tech Support	3
1.5 Features	4
1.6 Wireless Operation Modes	4
1.6.1 Access Point Mode	4
1.6.2 WDS station Mode	5
1.6.3 WDS AP Mode (WDS + AP)	5
1.6.4 Client Infrastructure Mode	6
1.6.5 Wireless ISP Mode	6
1.6.6 AP Router Mode	7
2. Installing the AirMax5X	8
2.1 Before You Start	8
2.2 Package Content	9
2.3 Knowing your AirMax5X	10
2.4 Hardware Installation	11
2.4.1 Standard Pole Mount	12
2.5 Restore Settings to Default	13
3. Configuring the AirMax5X	14
3.1 Important Information	14
3.2 Prepare your PC	14
3.3 Management Interface	15
3.4 Introduction to Web Management	16
3.4.1 Welcome Screen and Login	16

3.5 Initial Configurations	18
3.5.1 Choose the wireless Operation Modes	18
3.5.2 Change the Device's IP Address	19
3.5.3 Set the Time and Date	20
3.5.4 Change Password	21
4. Web Management: Operation Mode Settings	22
4.1 About AirMax5X's Menu Structure	22
4.2 Operation Modes (Wireless and WAN Settings)	23
4.2.1 Access Point Mode setting	24
4.2.2 Client infrastructure mode setting	32
4.2.3 WDS Access Point Mode	35
4.2.4 WDS Station Mode setting	35
4.2.5 AP Router Mode Setting	35
4.2.5.1 WAN Port Settings	36
4.2.5.2 Dynamic DNS Settings	36
4.2.5.3 Remote Management Settings	37
4.2.5.4 DHCP Server	37
4.2.5.5 DMZ	38
4.2.5.6 Virtual Server Settings	38
4.2.5.7 IP Filtering Settings	39
4.2.5.8 MAC Filtering Settings	39
4.2.5.9 Port Filtering Settings	40
4.2.5.10 Bandwidth Control	40
4.2.6 Wireless ISP Mode Setting	41
4.2.6.1 Remote AP SSID and Site survey	41
5. Web Management: System Configuration and Status	43
5.1 System Configuration	43
5.1.1 Device IP Settings	43
5.1.2 Time Settings	44
5.1.3 Password Settings	45
5.1.4 System Management	45
5.1.5 Ping Watchdog	46
5.1.6 Firmware Upgrade	46
5.1.7 Configuration Save and Restore	47
5.1.8 Factory Default	48

5.2 Device Status	49
5.2.1 Device Information.....	49
5.2.2 Wireless Information	50
5.2.3 Internet Information	50
5.2.4 Wireless Client Table	51
5.2.5 System Log.....	51
5.3 PoE Pass-through (Power up another Device)	52
6. Antenna Alignment	53
6.1 About AirMax5X's Antenna.....	53
6.1.1 Mounting Adjustment	54
6.2 Preparation before Installation	54
6.3 Antenna Alignment using Signal Survey	54
6.4 Antenna Alignment using RSSI LED	56
7. Application Example: Infrastructure	58
7.1 Application Environment	58
7.2 Central AP: Access Point Mode	59
7.2.1 AP Wireless Settings	60
7.3 Client: Client Mode.....	62
7.3.1 Device IP Address	63
7.3.2 Client Wireless Settings.....	63
7.4 WDS AP Mode and WDS Station Mode.....	65
8. Specifications.....	66
8.1 Features.....	66
8.1.1 General Feature	66
8.2 Specifications.....	66
9. Wireless Network Glossary.....	69

1

Introduction



1.1 Overview

The AirMax5X is a 2T2R wireless outdoor multi-function device based on IEEE 802.11a/n 5-GHz radio technologies. When installed in upright position, it is rain and splash proof. It features an integrated 14dBi patch antenna and passive POE to simplify the installation. The built-in antenna can provide up to 20km of distance depending on conditions. The firmware of the AP provides up to 6 operations modes to satisfy different application environments.

1.2 Special Notice

This product requires professional installation. Please do not attempt to install the device without the necessary knowledge in regards to your country's wireless regulations.

Functions and features in your product's firmware might be different due to regulations in your country.

1.3 How to Use This Guide

AirMax5X is an advanced wireless CPE with many functions. It is recommended that you read through the entire user's guide whenever possible. The user guide is divided into different chapters. You should read at least go through the first 3 chapters before attempting to install the device.

Recommended Reading

Chapter 1

■ 1.5 Operation Modes:

This section explains the usage of each wireless operation mode. It is a must read.

Chapter 2:

This chapter is about hardware installation. You should read through the entire chapter.

Chapter 3:

■ **3.1 Important Information:** This section has default settings information such as IP, password, SSID, and recommended browser

■ **3.3 Management Interface:** This section introduces Web, Telnet, and configurations.

■ **3.4 Introduction to Web Management:** This section tells you how to get into the Web UI using HTTP. In addition, it also explains about the basic menu structure.

■ **3.5 Initial Configurations:** This section guide you through the essential initial configurations such as choosing operation mode, set device IP, password, and change frequency domain.

Chapter 4 Web Management – Operation mode Settings:

This chapter explain the wireless functions and router mode settings in the AirMax5X. If time permitted, you should read through the entire chapter.

■ 4.2 Access Point Mode:

This section is the page where Access Point mode is chosen. Therefore, it is advised that you must read through the entire section.

- **4.3 Client Mode:**
Here explains the WDS setting page.
- **4.4 WDS Access Point Mode**
- **4.5 WDS Station Mode**
- **4.6 AP Router Mode**
- **4.7 Wireless ISP Mode**
- **Chapter 5: Web Management 2: Configurations and Status**
This chapter explains all the non-wireless settings and status such as IP settings, Ping Watchdog.
 - **5.1.5 PING Watchdog:**
PING watchdog is a crucial function to keep your wireless connection alive. When AirMax5X can't get a response from remote devices, it will attempt to re-establish the connection.
 - **5.1.7 Configuration Save and Restore:**
You should always backup your configurations so you can restore in the event of system crash.
 - **5.3 PoE Pass-through (Power up another device)**
- **Chapter 7: Application Example: Infrastructure**
In this chapter, you will learn how to use AP mode, Client Infrastructure Mode, and Bridge Infrastructure mode in one application example. In addition, you will also learn how to make multiple SSID and bandwidth control.
- **Chapter 9: Wireless Network Glossary**
Explanations on wireless network technical terms from A to Z. Highly recommended for referencing when you encounter an unfamiliar term.

1.4 Firmware Upgrade and Tech Support

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

In addition, you might find new firmware that either increase software functions or provide bug fixes for AirMax5X. 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.php

1.5 Features

- 2T2R 300Mbps
- IEEE 802.11a/n
- Runs from 5.18GHz to 5.7GHz for Europe domain
- Runs from 5.745GHz to 5.825Ghz for FCC domain
- 2 x 10/100 Ethernet Port with one Passive PoE port
- Built-in 14dBi Antenna
- AP, Repeater, Bridge, Client, Router, WISP Modes
- Passive 48V PoE Powered
- PoE Power Pass-through
- Reset button on the POE Injector
- Support Wireless Access Control, Client Isolation

1.6 Wireless Operation Modes

The AirMax5X can perform as a multi-function wireless device. Through the AirLive web interface, users can easily select which wireless mode they wish the AirMax5X to perform. The AirMax5X can be configured to operate in the following wireless operation modes:

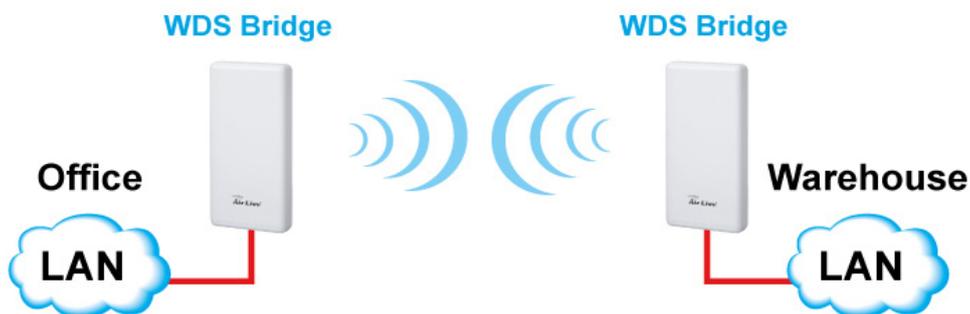
1.6.1 Access Point Mode

When operating in the Access Point mode, the AirMax5X becomes the center hub of the wireless network. All wireless cards and clients connect and communicate through AirMax5X. This type of network is known as “Infrastructure network”. Other AirMax5X or 802.11a/n CPE can connect to AP mode through “Client Infrastructure Mode”.



1.6.2 WDS station Mode

In WDS station mode, the AirMax5X functions similar as client mode. In this mode, the remote client must have WDS (Wireless Distribution System) capability. If you require the PC's or client's MAC addresses to be preserved when the data pass through the Access Point, it is necessary to use the WDS AP mode for remote side AirMax5X and another AirMax5X running for WDS station.



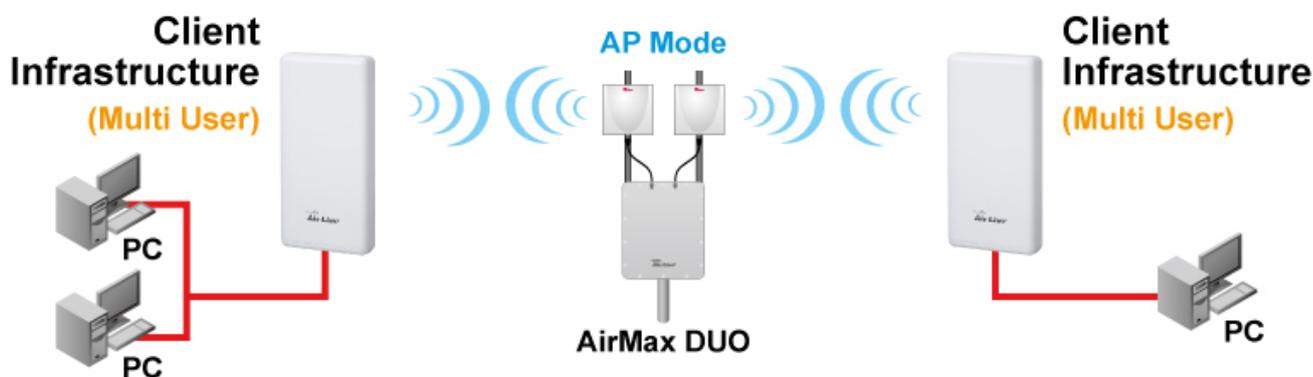
1.6.3 WDS AP Mode (WDS + AP)

In WDS Access Point mode, the AirMax5X functions similar as Access Point. In this mode, the remote client must have WDS (Wireless Distribution System) capability. If you require the PC's or client's MAC addresses to be preserved when the data pass through the Access Point, it is necessary to use the WDS AP mode for remote side AirMax5X and another AirMax5X running for WDS station in Client side.



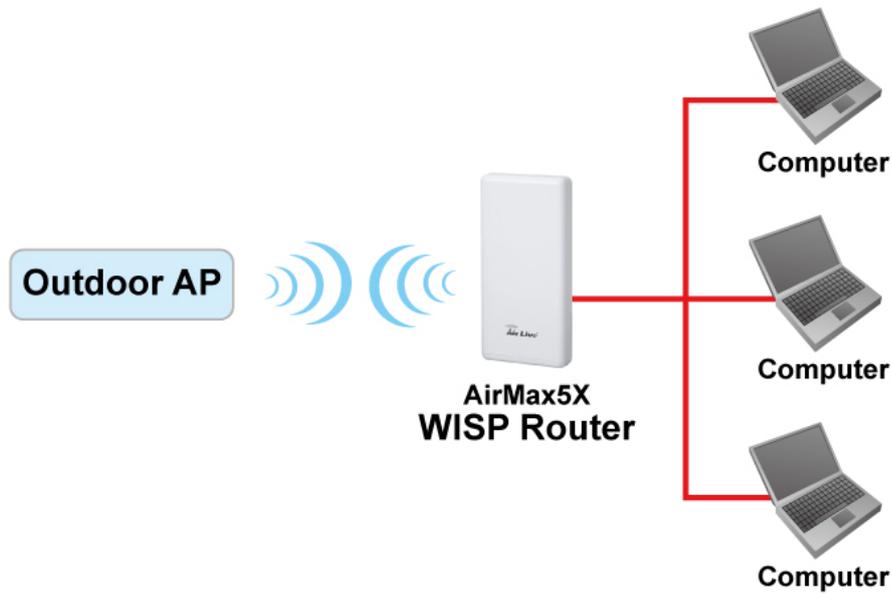
1.6.4 Client Infrastructure Mode

This mode is also known as “Client” mode. In Client Infrastructure mode, the AirMax5X 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 AirMax5X to get network access. This mode is often used by WISP on the subscriber’s side.



1.6.5 Wireless ISP Mode

In Wireless ISP Mode, AirMax5X 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.



1.6.6 AP Router Mode

In AP Router Mode, the AirMax5X behaves like a wireless router. The non-PoE port of the AirMax5X will become WAN port. Both the wireless and the passive PoE port of AirMax5X becomes the LAN side. User can manage the AirMax5X through the wireless or passive PoE port. And if the remote management is opened, user can also get to manage AirMax5X via the WAN side.



2

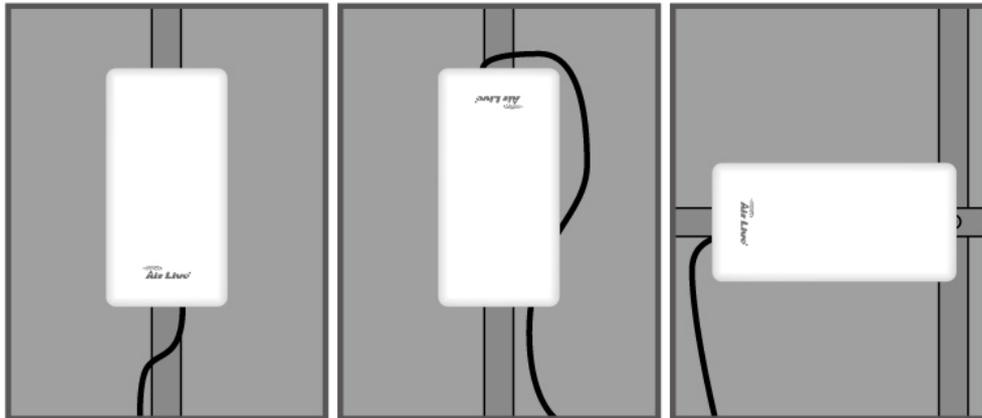
Installing the AirMax5X

This section describes the hardware features and the hardware installation procedure for the AirMax5X. 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 AirMax5X

- The AirMax5X 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 AirMax5X must be installed in the upright position if the unit is located in outdoor or wet environments.



- The use of 5GHz spectrum, the allowed channels can be very in different country. Please consult with your country's telecom regulation first.
- The integrated antenna has forward coverage angle of 20 degree in vertical and 30 degree in horizontal direction.
- The AirMax5X is a 5GHz CPE device only; it cannot operate in 2.4GHz.

2.2 Package Content

The AirMax5X package contains the following items:

- One AirMax5X main unit
- One 48V 1A DC power adapter
- Passive PoE DC Injector
- 1 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.

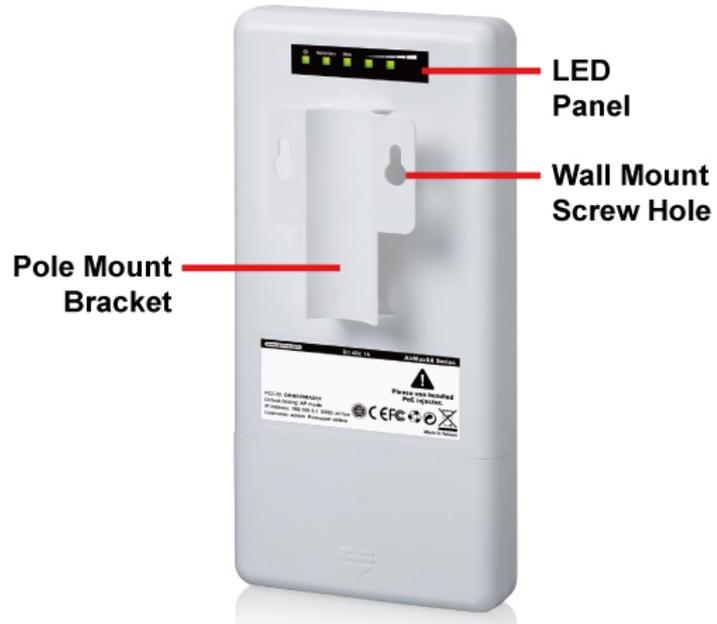
2.3 Knowing your AirMax5X

Below are descriptions and diagrams of the product:

Front

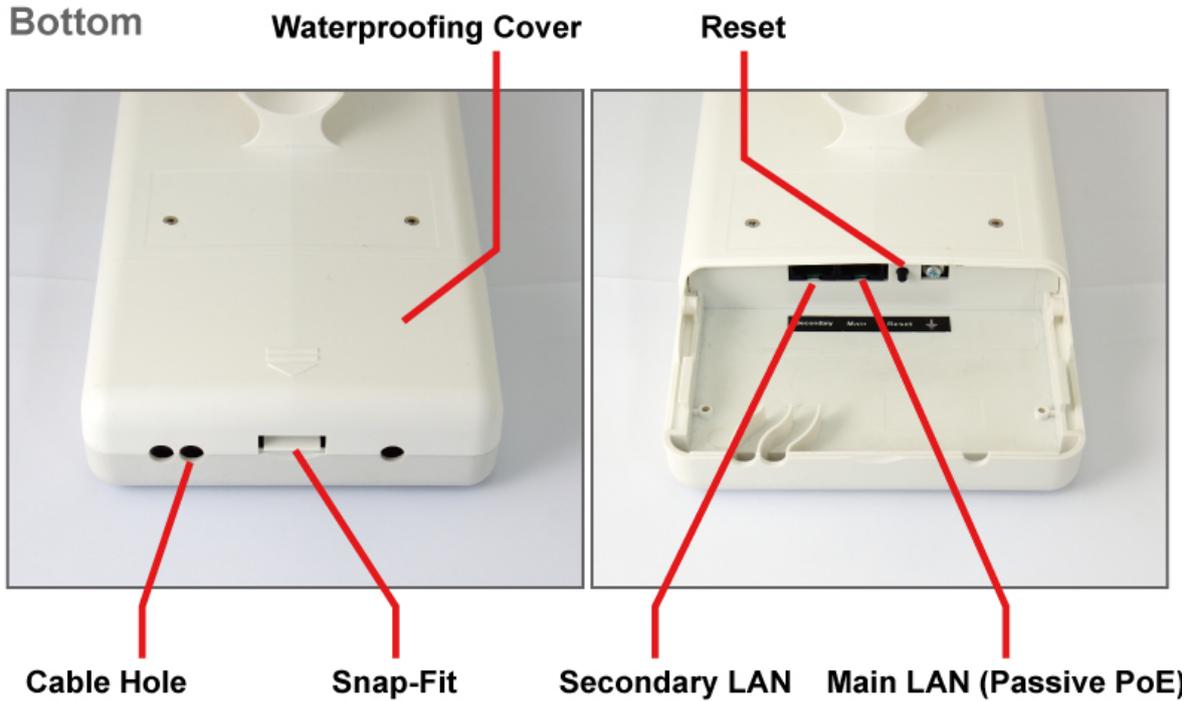


Back



LED Behavior

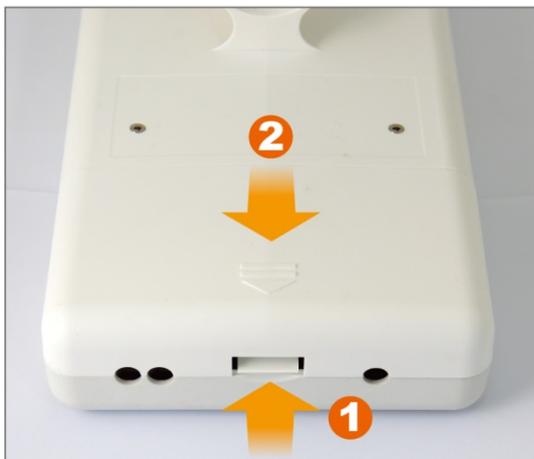
LED Indicator	State	Description
1. PWR LED	ON	The AirMax5X is powered ON.
	Off	The AirMax5X is powered Off.
2. Secondary Port LED	ON	Port linked.
	Off	No link.
	Flashing	Data is transmitting or receiving on the LAN interface.
3. Main Port LED	ON	Port linked.
	Off	No link.
	Flashing	Data is transmitting or receiving on the LAN interface.



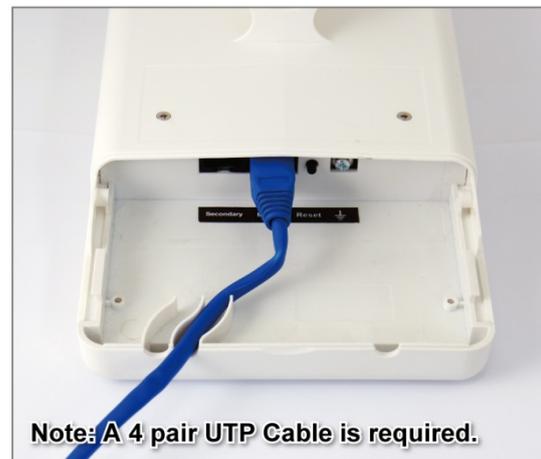
2.4 Hardware Installation

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

1. Push the button in the side to remove upper housing.



2. Pass through Ethernet cable from the hole; insert the cable to Secondary port.



3. Install the upper housing and make sure the housing is well installed.



4. Install POE Injector

DC: Insert adapter

POE: This hole is linked to Secondary port of the Outdoor Router with RJ-45.

LAN: This hole is linked to LAN side PC/Hub or Router/ADSL modem device with RJ-45



2.4.1 Standard Pole Mount

Your AirMax5X comes standard with 1 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 Restore Settings to Default

If you have forgotten your AirMax5X's IP address or password, you can restore your AirMax5X to the default settings by pressing on the "reset button" for more than 5 seconds. The reset button is located on the PoE Kit. Please see diagram below for details.



3

Configuring the AirMax5X

In this chapter, we will explain AirMax5X's available management interfaces and how to get into them. Then, we will provide the introduction on Web Management and recommended initial settings. For detail explanations on Web Management functions, please go to Chapter 4 and 5.

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.

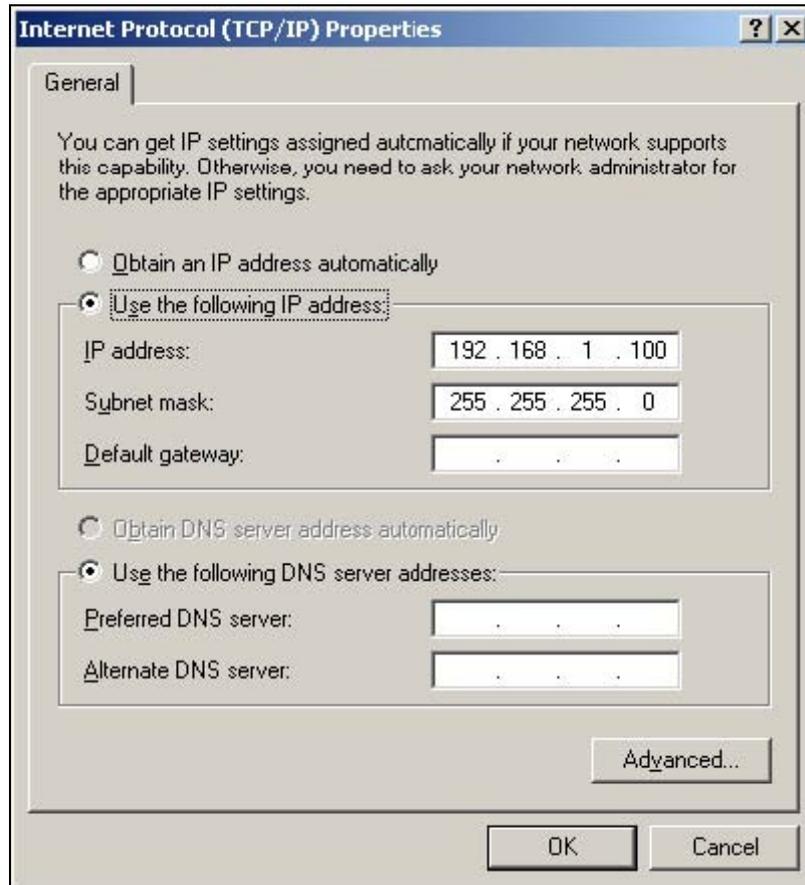
- The default IP address is:** 192.168.1.1 **Subnet Mask:** 255.255.255.0
- The default user's name is:** admin
- The default password is:** airlive
- The default wireless mode is :** Access Point mode
- After power on, please wait for 2 minutes for AirMax5X to finish boot up
- Please remember to click on "**Apply**" for new settings to take effect

3.2 Prepare your PC

The AirMax5X can be managed remotely by a PC through either the wired or wireless network. The default IP address of the AirMax5X 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 AirMax5X, please do the following:

1. Connect your PC directly to the LAN port on the DC Injector of AirMax5X
2. Set your PC's IP address manually to 192.168.1.100 (or other address in the same subnet)



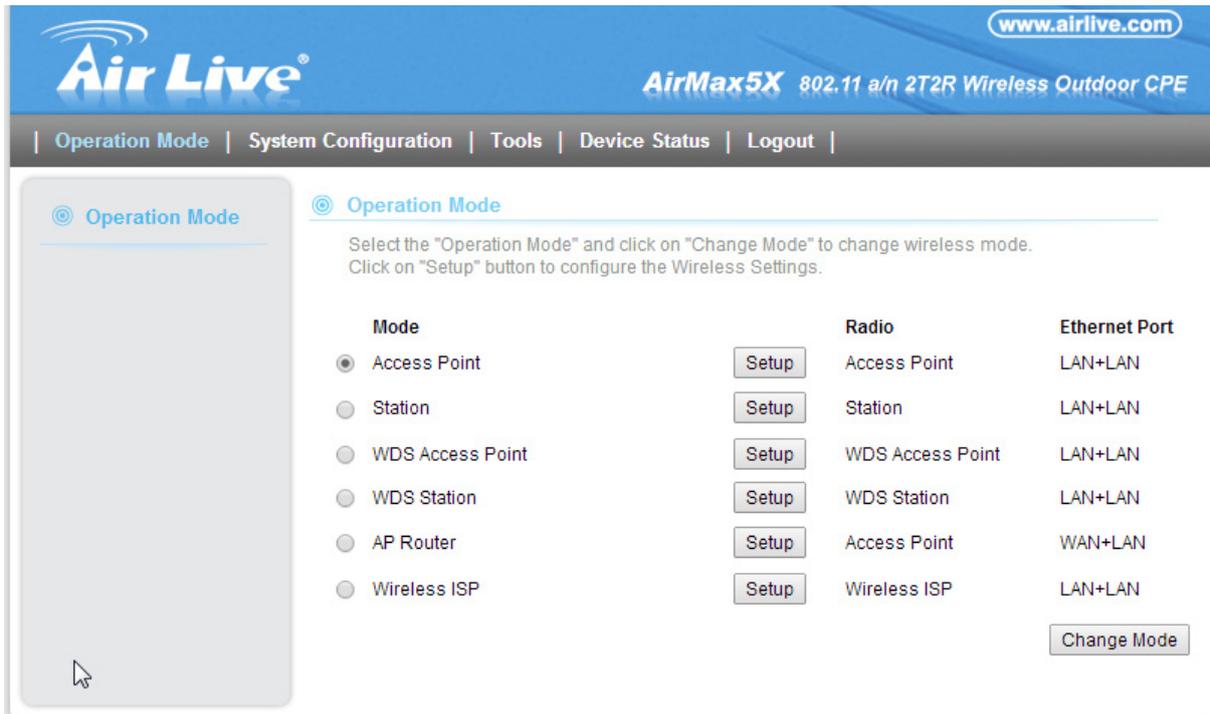
You are ready now to configure the AirMax5X using your PC.

3.3 Management Interface

The AirMax5X can be configured using the web interfaces:

Web Management (HTTP)

You can manage your AirMax5X by simply typing its IP address in the web browser. Most functions of AirMax5X can be accessed by web management interface. We recommend using this interface for initial configurations. To begin, simply enter AirMax5X's IP address (default is 192.168.1.1) on the web browser. The default username is "admin" and password is "airlive".



3.4 Introduction to Web Management

3.4.1 Welcome Screen and Login

After the procedure above, the Welcome Screen will appear. Welcome Screen gives a brief introduction of the AirMax5X’s main function category. By click on the function category, it will direct you to the corresponding web management menu.



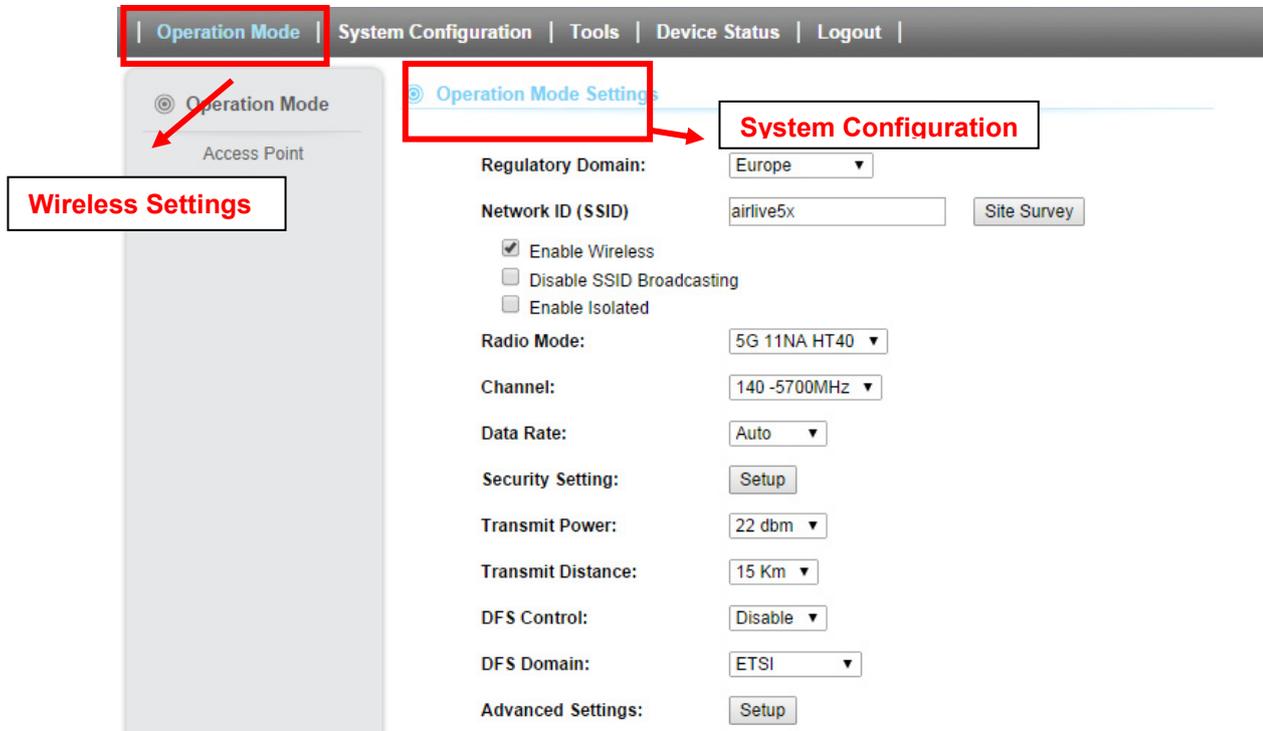
- **Wireless Settings:** Click on this part will bring you to the wireless operation mode menu. The AirMax5X's wireless settings are different between wireless modes. Only functions that are applicable to the wireless mode will show to simplify configuration. For example, multiple SSID option is workable for Access Point, AP Router, and WDS + AP mode. Therefore, the function will only appear in these 3 modes. For this reason, the first step to configure the AirMax5X is to select the wireless mode. The router mode specific functions are also in this menu category. For explanation of different wireless modes, please refer to Chapter 1.
- **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 AirMax5X. It provides information on device status, Ethernet status, wireless status, wireless client table, and system log.

TIPS: You can choose any menu categories to begin; you can switch to other menu later.

When you access to the AirMax5X, it will require you to enter the username and password. Please enter “**admin**” for the User Name, and “**airlive**” (all lower cases) for password.



After you enter the correct password, the welcome screen will appear. Then chose the corresponding menu you needed, and the web interface will be arranged as below:



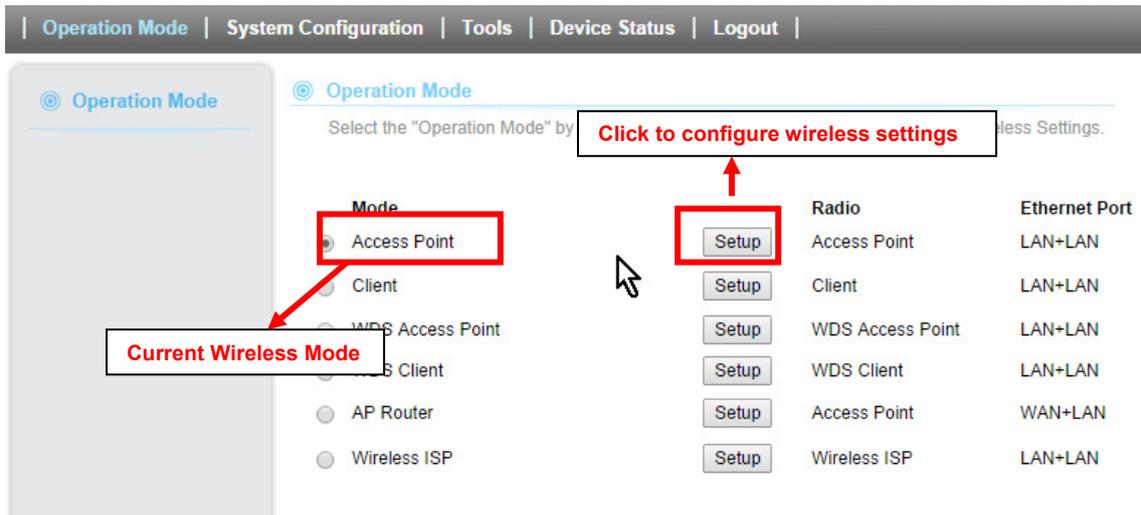
3.5 Initial Configurations

We recommend users to browse through AirMax5X’s web management interface to get an overall picture of the functions and interface. Below are the recommended initial configurations for first time login:

3.5.1 Choose the wireless Operation Modes

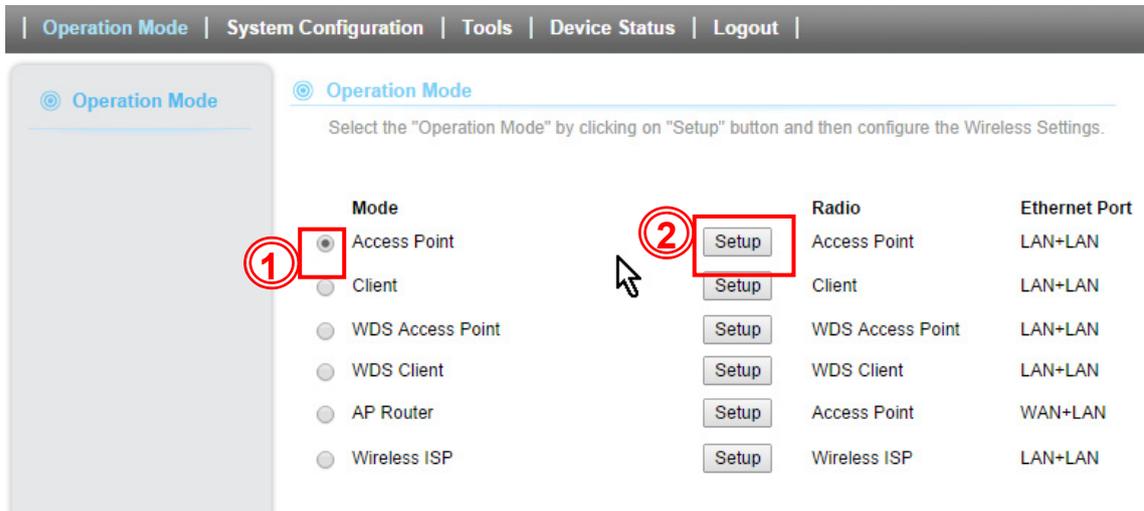
The wireless settings of AirMax5X are dependent on the wireless operation mode you choose. Therefore, the first step is to choose the operation mode. For explanation on when to use what operation mode, please refer to Chapter 1

When you click on the “Wireless Settings” on the welcome screen or the “Operation Mode” on the top menu bar, the following screen will appear.



Follow the example below to change to "Access Point" mode

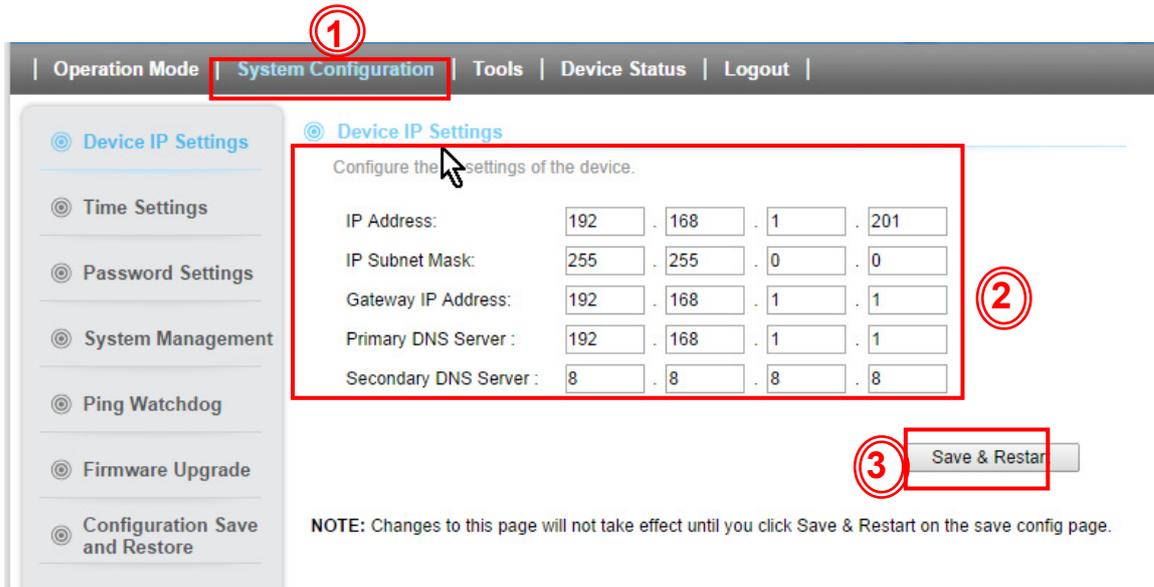
1. Select "Access Point" mode.
2. Click on "setup" button then "save and Restart"
3. The AP will reboot, for about one minute
- 4.



3.5.2 Change the Device's IP Address

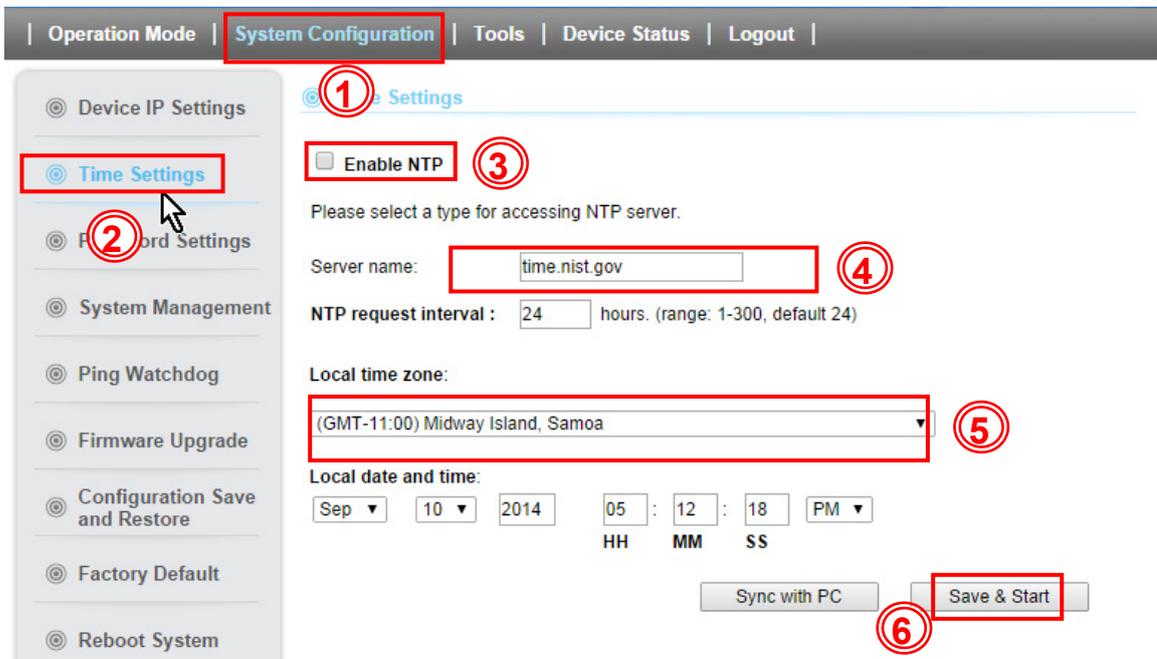
The default IP address is at 192.168.1.1. You should change it to the same subnet as your network. Also, if you want to manage AirMax5X remotely, you have to set the Gateway and DNS server information.

To setup the IP settings for AirMax5X, please select "System Configuration" -> Device IP Settings". After entering the IP information, click on "Apply" to finish.



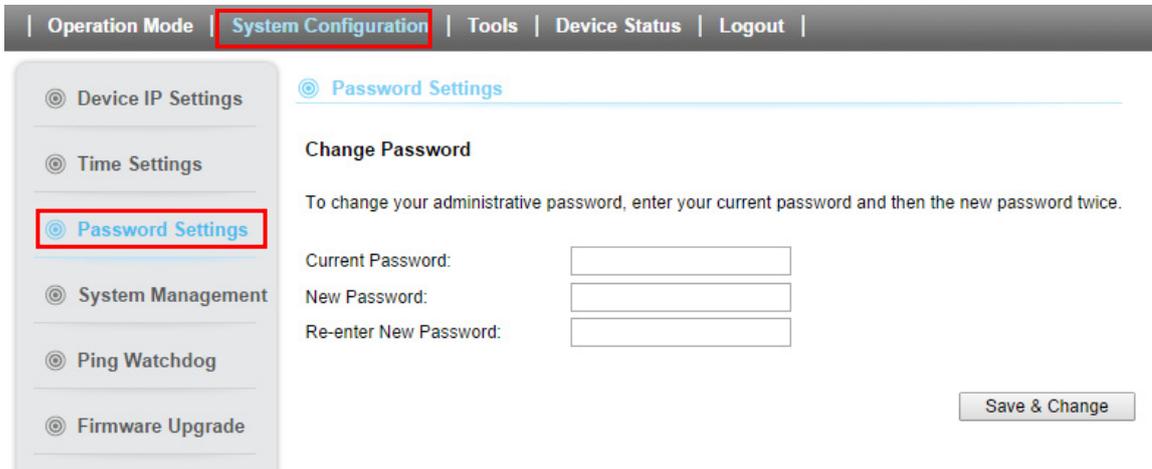
3.5.3 Set the Time and Date

It is important that you set the date and time for your AirMax5X 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 AirMax5X is not connected to Internet, please enter the time manually. Please remember to select your local time zone and click "Apply" to finish.



3.5.4 Change Password

You should change the password for AirMax5X at the first login. To change password, please go to “System Configuration” -> “Password Settings” menu.



The screenshot shows the web interface for configuring the AirMax5X. At the top, there is a navigation bar with the following items: "Operation Mode", "System Configuration" (highlighted with a red box), "Tools", "Device Status", and "Logout". Below the navigation bar is a sidebar menu with the following items: "Device IP Settings", "Time Settings", "Password Settings" (highlighted with a red box), "System Management", "Ping Watchdog", and "Firmware Upgrade". The main content area is titled "Password Settings" and contains the following text: "Change Password", "To change your administrative password, enter your current password and then the new password twice.", "Current Password:", "New Password:", and "Re-enter New Password:". Each of these labels is followed by an empty text input field. At the bottom right of the form is a "Save & Change" button.

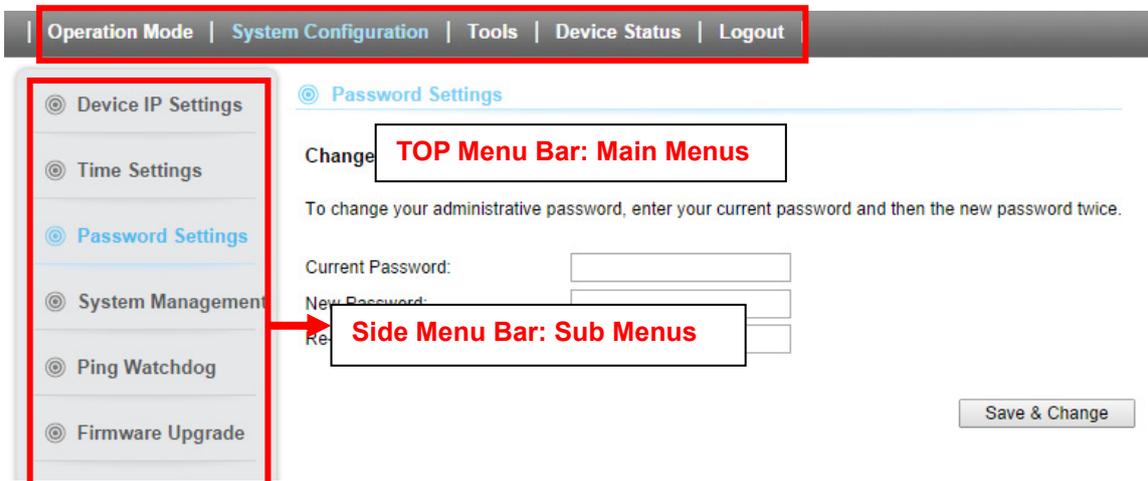
4

Web Management: Operation Mode Settings

In this chapter, we will explain about the wireless settings and router mode settings in web management interface. Please be sure to read through Chapter 3's "Introduction to Web Management" and "Initial Configurations" first. For system configurations, device status, and other non-wireless related settings; please go to Chapter 5.

4.1 About AirMax5X's Menu Structure

The AirMax5X's web management menu is divided into 3 main menus: *Operation Modes*, *System Configurations*, and *Device Status*. The main menus are displayed in "Top Menu Bar". Within each main menu category, there are sub-menu options which are displayed on the "Side Menu Bar".



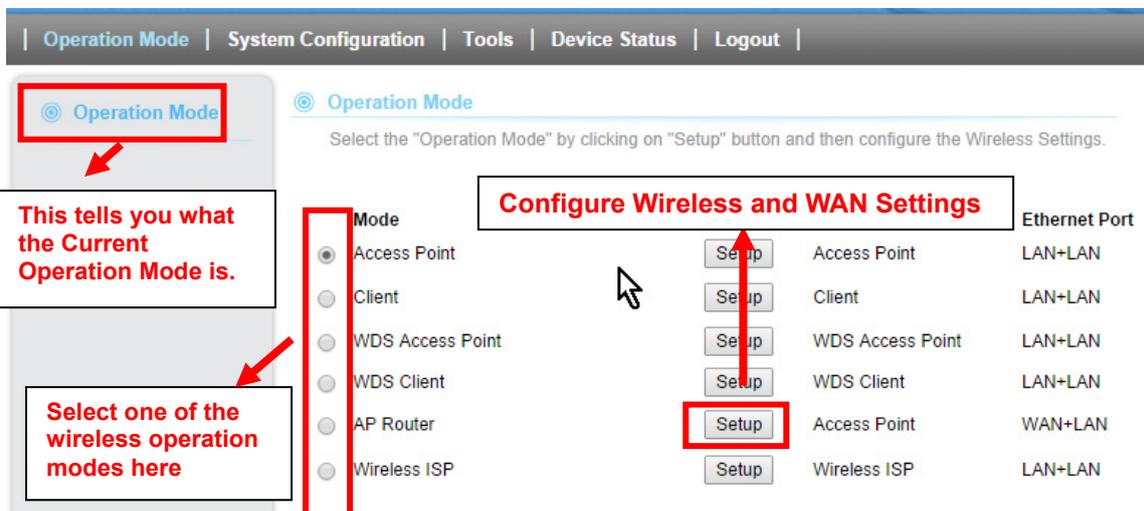
- Operation Mode:** This menu is where you will find wireless and WAN settings. The AirMax5X's wireless settings are dependent on the wireless operation mode you choose; only the applicable wireless settings for selected operation mode are shown. For example; WAN port setting is available only for AP Router and WISP Router mode, it will only be shown in those modes. To access wireless settings, click on the "Setup" button within each operation mode. For explanation on different wireless modes, please refer to Chapter 1. We will talk about functions in this menu for this chapter.

- **System Configuration:** All settings besides Wireless and WAN functions are in this category. The system configuration including changing password, upload firmware, backup configuration, settings PING watchdog, and setting management interface. We will talk about this menu's function in Chapter 5.
- **Device Status:** This section for monitoring the status of AirMax5X. It provides information on device status, Ethernet status, wireless status, wireless client table, and system log.
- **Logout:** Please make sure to Logout after you finish all settings.

4.2 Operation Modes (Wireless and WAN Settings)

The wireless settings of AirMax5X are dependent on the wireless operation mode you choose. Therefore, the first step is to choose the operation mode. For explanation on when to use what operation mode, please refer to Chapter 1.

When you select "Wireless Settings" in the welcome screen, or click on the "Operation Mode" on the top menu; the following screen will appear:



The screenshot shows the 'Operation Mode' configuration page. At the top, there is a navigation bar with links: 'Operation Mode', 'System Configuration', 'Tools', 'Device Status', and 'Logout'. Below the navigation bar, the page title is 'Operation Mode' with a sub-instruction: 'Select the "Operation Mode" by clicking on "Setup" button and then configure the Wireless Settings.' The main content area is a table with columns for 'Mode', 'Setup', and 'Ethernet Port'. The 'Mode' column lists: Access Point (selected), Client, WDS Access Point, WDS Client, AP Router, and Wireless ISP. The 'Setup' column has a 'Setup' button for each mode. The 'Ethernet Port' column lists: LAN+LAN, LAN+LAN, LAN+LAN, LAN+LAN, WAN+LAN, and LAN+LAN. A red box highlights the 'Operation Mode' header, and another red box highlights the 'Setup' button for 'Access Point' in the 'WAN+LAN' mode. Red arrows point from text boxes to these elements.

Mode	Setup	Ethernet Port
<input checked="" type="radio"/> Access Point	Setup	LAN+LAN
<input type="radio"/> Client	Setup	LAN+LAN
<input type="radio"/> WDS Access Point	Setup	LAN+LAN
<input type="radio"/> WDS Client	Setup	LAN+LAN
<input type="radio"/> AP Router	Setup	WAN+LAN
<input type="radio"/> Wireless ISP	Setup	LAN+LAN

- **Mode:** The available wireless operation modes for AirMax5X. Select one and click on "Change Mode" button to switch between modes.
- **Setup:** Click here to configure the Wireless and WAN (in router mode) settings.
- **Radio:** This explain how the radio function in the particular operation mode
- **Ethernet Port:** The Ethernet Port function. In AP router mode, the secondary LAN Port is working as WAN and Main LAN Port is working as LAN Port. In rest of the operation mode , all two Ethernet LAN Port are working as the LAN Port

4.2.1 Access Point Mode setting

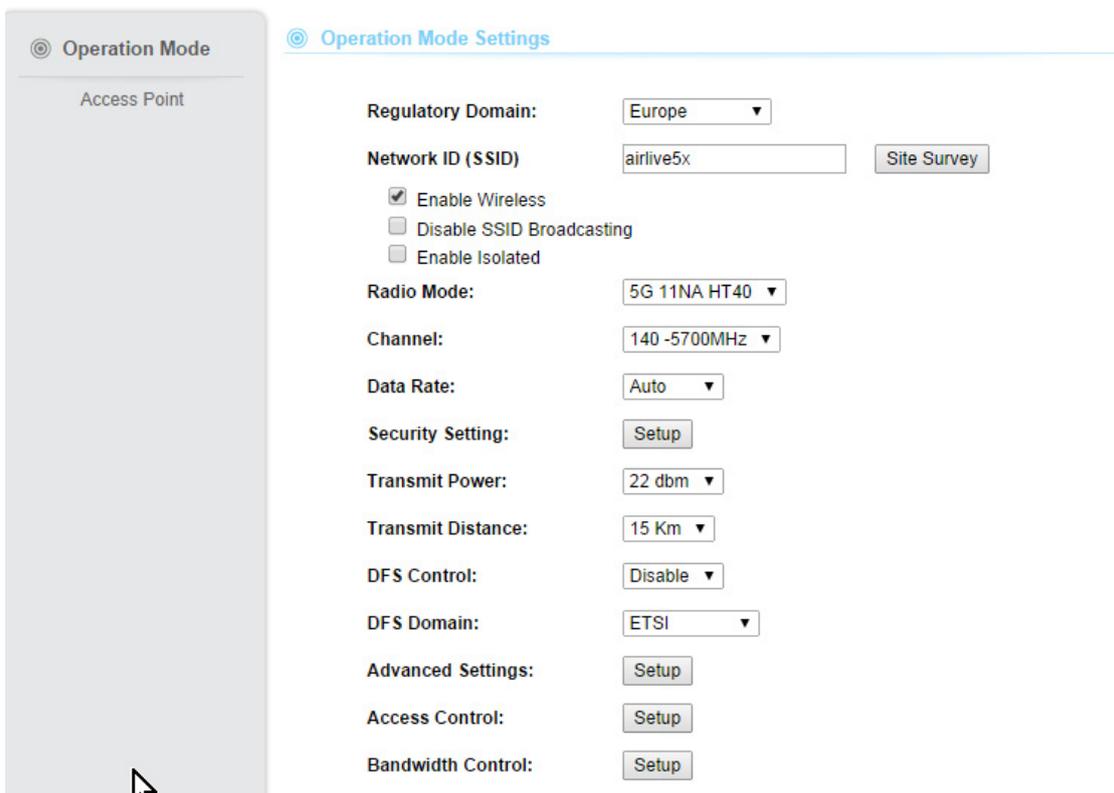
When operating in the Access Point mode, the AirMax5X becomes the center hub of the wireless network. All wireless cards and clients connect and communicate through AirMax5X. This type of network is known as “Infrastructure network”. Other AirMax5X or 802.11a/n CPE can connect to AP mode through “Client Infrastructure Mode”.

In this mode, normally your AirMax5x will not provide the IP to the client (Notebook or PC) , Please make sure that there are another DHCP server which can provide the IP in the network or all of the wireless cards, clients are set the difference IP manually.

All of the Ethernet Ports are LAN ports in Access Point mode



Once you click on the “Setup” page for Access Point Mode, the wireless settings page will appear as below image



In the default, DFS is enabled and wifi channel is “auto” in order to meet the requirement from EU. SSID is **airlive**

4.2.1.1 Regulatory domain

The default Regulatory domain is “**European**”, if you are located in America you can change to “**America**” in order to meet the regulation of FCC.

4.2.1.2 Network ID(SSID)

The SSID is the network name used to identify a wireless network. In AP mode, SSID is the ID that AirMax5X broadcast. It can be modified and The SSID length is up to 32 characters. The default SSID is “**airlive**”

- **Enable Wireless:** The default wireless is on. You can uncheck this box to disable wireless interface. When the box is uncheck. Clients cannot find this AirMax5X from their wireless interface.
- **Disable SSID Broadcast:** If you check this box, the SSID will be hidden; only users who know the SSID can associate with this network.

4.2.1.3 Radio Mode

AirMax5X is 802.11n 2T2R wireless outdoor CPE, but it is backward compatible with 802.11a. The default radio mode is auto select; however you can fix at 11n mode or 11 a mode.

4.2.1.4 Channel

The channel is to select the wireless channel for AirMax5X. The channel which can be selected is difference in each Regulatory domain.

When in ETSI domain, CH36 ~ Channel 140 can be selected.

When in FCC domain, CH149 ~ CH165 can be selected

You can select the channel which has less interference.

Channel	CH 36 ~ 140 (5.18 ~ 5.700GHz) for Europe Domain CH 149 ~ 165 (5.745 ~ 5.825GHz) for American Domain
---------	--

However, the channel available for use in your device depends on your country's regulations. This is subject to change depending on regulations of your country. Your device is preloaded with firmware according to the regulations. If your device's firmware is not conforming to your country's latest regulation, please write to tech@airlive.com.

4.2.1.5 Data Rate

Operation Mode -> Setup -> Data Rate

Use this function; you can lock the data rate of your AirMax5X to a specified value. For 802.11a radio mode, the data rate supports from 1Mbps to 54Mbps. For 802.11n, the data rate will be specified in MCS value. For AirMax5X, it will support from MCS0 to MCS7.

4.2.1.6 Security Setting

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. The AirMax5X features various security policies including WEP, 802.1x, WPA-RADIUS, WPA-PSK, WPA2-RADIUS, WPA2-PSK, and WPA-PSK. Please note not all security policies are available in all operation modes. All wireless devices on the same network must use the same security policy. We recommend using WPA-PSK or WPA2-PSK whenever possible. For WDS Bridge, we recommend using AES encryption.

WEP

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

Security Settings

ClientMode

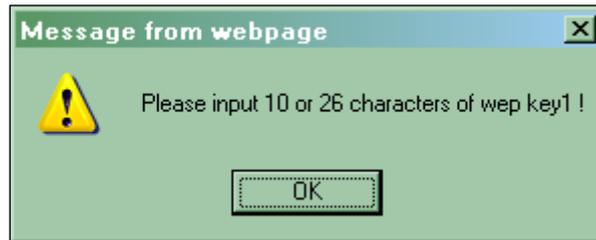
Select Security Policy:

Select one of the WEP keys for the wireless network:

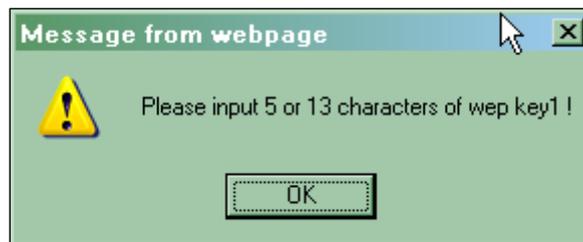
WEP Key 1:	<input type="text"/>	<input type="text" value="ASCII"/>
WEP Key 2:	<input type="text"/>	<input type="text" value="ASCII"/>
WEP Key 3:	<input type="text"/>	<input type="text" value="ASCII"/>
WEP Key 4:	<input type="text"/>	<input type="text" value="ASCII"/>

- **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.

- WEP Keys:** Please enter the WEP keys used for encryption. You need to fill at least the “Select WEP Key”. For example; if you choose “*Select one of the WEP keys for the wireless network: Key 1*” in the previous field, then it is necessary to fill WEP Key 1. The restriction to the Key length is depending on the Key type you selected.
- Hex:** The Key length can be 10 or 26 character to Hex Key type, and the character can be 1~0, and A~F. If the Key length is not 10 nor 26, the alert message should pop up as below:



- ASCII:** The Key length can be 5 or 13 character to ASCII Key type, and the character can be any ASCII character. If the length is not 5 nor 13, the alert message should pop up as below:



802.1x

Security Settings

Select SSID: Airlive

Select Security Policy: 802.1X

WEP: Disable Enable

Radius Server

IP Address:

Port:

Shared Secret:

Session Timeout:

Idle Timeou:

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

WPA-RADIUS, WPA2-RADIUS

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). It requires a RADIUS server available in order to do authentication (same as 802.1x), thus there is no shared key required.

Security Settings

Select SSID:

Select Security Policy:

Encryption Type: TKIP AES TKIPAES

Key Renewal Interval: seconds (60 ~ 9999)

PMK Cache Period: minute

Pre-Authentication: Disable Enable

Radius Server

IP Address:

Port:

Shared Secret:

Session Timeout:

Idle Timeou:

- **Encryption Type:** There are two encryption types **TKIP** and **AES (CCMP)**. While AES provides better security than TKIP, some wireless client stations may not be equipped with the hardware to support it. You can select **TKIP/AES** to allow TKIP clients and AES clients to connect to the Access Point at the same time.
- **Key Renewal Interval:** A group key is used for multicast/broadcast data, and the re-key interval is time period that the system will change the group key periodically. The shorter the interval is, the better the security is. The default is 3600 sec.

WPA-PSK, WPA2-PSK

Wi-Fi Protected Access (WPA) with Pre-Shared Key (PSK) provides better security than WEP keys. It does not require a RADIUS server in order to provide association authentication, but you do have to enter a shared key for the authentication purpose. The encryption key is generated automatically and dynamically. WPA2-PSK adds CCMP and AES encryption for even better security.

Security Settings

Select SSID: Airlive

Select Security Policy: WPA-PSK

Encryption Type: TKIP AES TKIPAES

Pre-Shared Key: 12345678

Key Renewal Interval: 3600 seconds (60 ~ 9999)

Apply

Security Settings

Select SSID: Airlive

Select Security Policy: WPA2-PSK

Encryption Type: TKIP AES TKIPAES

Pre-Shared Key: 12345678

Key Renewal Interval: 3600 seconds (60 ~ 9999)

Apply

Pre-shared Key: This is an ASCII string with 8 to 63 characters. Please make sure that both the AirMax5X and the wireless client stations use the same key.

- **Encryption Type:** There are two encryption types **TKIP** and **AES (CCMP)**. While AES provides better security than TKIP, some wireless client stations may not be equipped with the hardware to support it. You can select **TKIP/AES** to allow TKIP clients and AES clients to connect to the Access Point at the same time.
- **Key Renewal Interval:** A group key is used for multicast/broadcast data, and the re-key interval is time period that the system will change the group key periodically. The shorter the interval is, the better the security is. The default is 3600 sec.

4.2.1.7 Transmit Power

Operation Mode -> Setup -> Transmit Power

You can adjust the transmit output power of the AirMax5X's radio from 12 to 27dBm. The higher the output power, the more distance AirMax5X can deliver. However, it is advised that you use just enough output power so it will not create excessive interference for the environment. Also, using too much power at close distance can create serious performance drop due to signal distortion.

4.2.1.8 Transmit Distance

This area is to set the transmit distance. Longer distance between AirMax5X and Client have required longer ask time out. But AirMax5X users do not need to calculate the ACK time out, users just need to put the maximum distance between AP and Client. In real application, we suggest that users and add 2 more Km for transmit distance. For example, if the distance between AP and Client is 10Km, it is better to set the transmit distance to 12Km

4.2.1.9 DFS Control

DFS (dynamic frequency selection) is required to operate WiFi devices in 5GHz. Before you disable the DFS, please make sure your country's regulatory is not violated.

4.2.1.10 Advanced Setting

Operation Mode -> Setup -> Advance Settings

This page includes all the wireless settings that change the RF behaviors of AirMax5X. It is important to read through this section before attempting to make changes. If you are not familiar with those setting, we suggest you use the default setting.

RTS/CTS Threshold	Determines the packet size of a transmission and, through the use of an AP, helps control traffic flow. The range is 0-2346 bytes.
Beacon Interval	Beacons are the packets sending by Access point to synchronize the wireless network. The beacon interval is the time interval between beacons sending by this unit in AP or AP+WDS operation. The default and recommended beacon interval is 100 milliseconds.

DTIM	This is the Delivery Traffic Indication Map. It is used to alert the clients that multicast and broadcast packets buffered at the AP will be transmitted immediately after the transmission of this beacon frame. You can change the value from 1 to 255. The AP will check the buffered data according to this value. For example, selecting “1” means to check the buffered data at every beacon.
Roaming Threshold	Defines the minimum client signal level accepted by the AP for the client to connect.
Short GI	Guard intervals are used to ensure that distinct transmissions do not interfere with one another. Only effect under Mixed Mode.
Fragment Size	A large data frame is fragmented into several fragments each of size equal to fragment threshold. By tuning the fragment threshold value, we can get varying fragment sizes.
Aggregation	A part of the 802.11n standard that allows sending multiple frames per single access to the medium by combining frames together into one larger frame. It creates the larger frame by combining smaller frames with the same physical source, destination end points, and traffic class (QoS) into one large frame with a common MAC header
Aggregated Frames Number	Determines the number of frames combined in the new larger frame.
Maximum Aggregation Size	Determines the size (in bytes) of the larger frame.
Tx/Rx Chain Mask	Displays the number of independent spatial data streams the device is transmitting (TX) and receiving (RX) simultaneously within one spectral channel of bandwidth. Multiple chains increase data transfer performance significantly.

4.2.1.11 Access Control

Operation Mode -> Setup -> Access Control

The AirMax5X 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.

Access Control Settings

This feature allows you to define a list of MAC addresses that are authorized to access or denied from accessing the wireless network.

Select SSID : airlive ▼

Disable MAC address control list
No MAC address filtering is performed.

Enable GRANT address control list
Allow data traffic from devices listed in the table to access the network.

Enable DENY address control list
Deny/discard data traffic from devices listed in the table.

MAC Address: (xx:xx:xx:xx:xx:xx)

Apply
Cancel

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

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

To delete entries, check the corresponding *Select* boxes and then press *Delete Selected*.

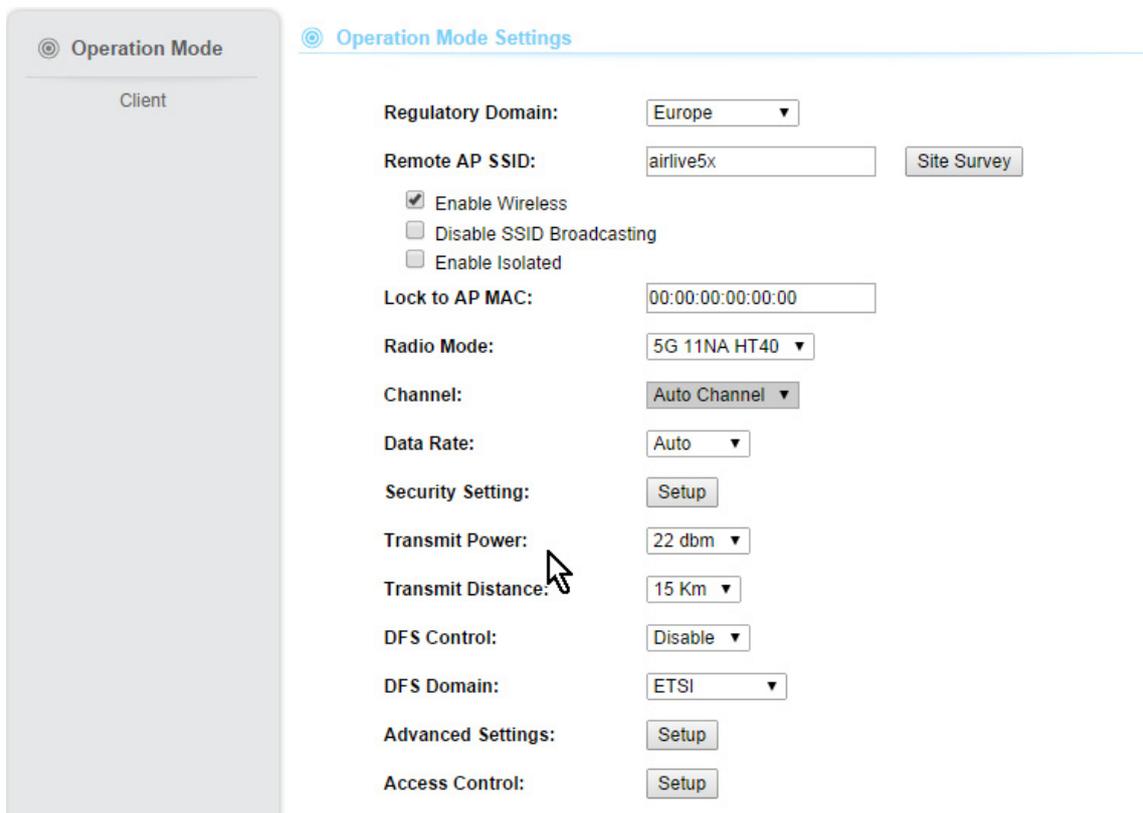
4.2.2 Client infrastructure mode setting

This mode is also known as “Client” mode. In Client Infrastructure mode, the AirMax5X acts as a wireless adapter to connect with a remote Access Point. Users can attach a computer or a router to the LAN port of AirMax5X to get network access. This mode is often used by WISP on the subscriber’s side.

In This mode, all two Ethernet ports act as LAN Port. The setting of Client infrastructure mode is similar of the AP mode, but it need to set the remote AP’s SSID. So please refer the chapter 4.2.1.5 ~ 4.2.1.11



4.2.2.1 Remote AP SSID and Site Survey



The screenshot shows the 'Operation Mode Settings' page for a Client. The page is divided into two main sections: 'Operation Mode' on the left and 'Operation Mode Settings' on the right. The 'Operation Mode' section is currently set to 'Client'. The 'Operation Mode Settings' section contains the following configuration options:

- Regulatory Domain: Europe
- Remote AP SSID: airlive5x (with a 'Site Survey' button)
- Enable Wireless:
- Disable SSID Broadcasting:
- Enable Isolated:
- Lock to AP MAC: 00:00:00:00:00:00
- Radio Mode: 5G 11NA HT40
- Channel: Auto Channel
- Data Rate: Auto
- Security Setting: Setup
- Transmit Power: 22 dbm
- Transmit Distance: 15 Km
- DFS Control: Disable
- DFS Domain: ETSI
- Advanced Settings: Setup
- Access Control: Setup

In Client mode, you need to decide which remote AP that he/she want to associate. User can enter the SSID by themselves or click the site survey button, the AirMax5X will scan the available AP.

After click the “site survey” button, the available AP will pop-up in other page as below.

Select	SSID	MAC Address	Channel	Signal Strength(%)	Security
<input type="radio"/>	ASMT-7F-PM-5G	14:D6:4D:CC:25:52	52	-94 dBm	WPA/WPA2/YesTKIP/CCMP/PSK
<input type="radio"/>	CL-WLAN-a	00:0B:86:AA:14:10	56	-85 dBm	WPA/YesCCMP/802.1x
<input type="radio"/>	CL-WLAN	00:1A:1E:67:ED:10	64	-83 dBm	WPA/YesTKIP/802.1x
<input type="radio"/>	tyler_5G	60:A4:4C:67:20:0D	149		WPA2/YesCCMP/PSK
<input type="radio"/>	ac5g	80:1F:02:75:EE:4B	153		WPA2/YesCCMP/PSK
<input type="radio"/>	default_5G	00:30:4F:A1:C7:24	149		WPA2/YesCCMP/PSK
<input type="radio"/>	uest_5G_2	02:30:4F:A1:C7:25	149		WPA2/YesCCMP/PSK
<input type="radio"/>	CL-GUEST	00:1A:1E:67:ED:11	64	-84 dBm	none

Click here to select SSID for Association or Signal Survey

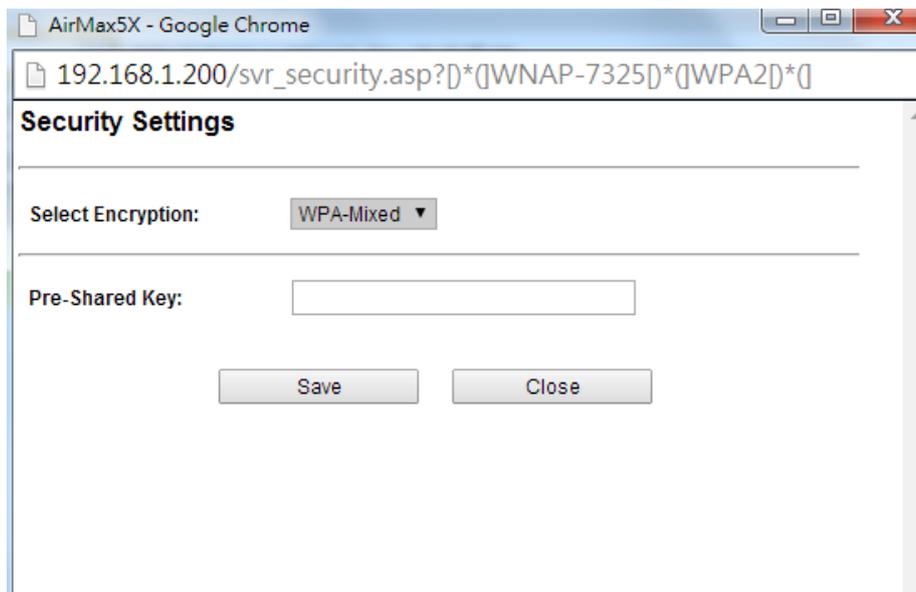
For antenna alignment. It will display signal

ASSOCIATE RESCAN CLOSE

To connect with the selected SSID. This function is available only in Client or Bridge Mode

Select the SSID which you want to connect , and click the “SET SECURITY”, type in the key if required. Then Click “Save” Button. If the key is correct , the AirMax5X will ask users to reboot the device.

After reboot is finished , the AirMax5X is connected with another remote AP. It is important that AirMax5X need to set the” transmit distance”. If the AirMax5X can not connected with remote AP , please change the setting of “transmit distance”. Detail of the setting, please refer the chapter 4.2.2.2



Tips: Even the IP address of AirMax5X does not need to be the same subnet with the remote IP. We suggest that it is better to set the same subnet with difference IP address of remote IP.

4.2.2.2 Radio Mode

To setup the Radio Mode, Please set is same radio mode as your remote AP.

4.2.2.3 Transmit Distance

This area is to set the transmit distance. Longer distance between AirMax5X and Client required longer ask time out. But AirMax5X users do not need to calculate the ACK time out, users just need to put the maximum distance between AP and Client. In real application, we suggest that users and add 2 more Km for transmit distance. For example, if the distance between AP and Client is 10Km, it is better to set the transmit distance to 12Km

4.2.3 WDS Access Point Mode

In WDS Access Point mode, the AirMax5X functions as a WDS bridge with Access Point Mode. For WDS Access Point, it can be connected by other AirMax5X which using the WDS station. In this mode, the setting is same as Access Point Mode. Please refer chapter 4.2.1 for the detail setting

4.2.4 WDS Station Mode setting

In WDS Station mode, the AirMax5X functions as a client which can connect with remote WDS Access Point.. In this mode, the setting is same as client infrastructure mode. Please refer chapter 4.2.2 for the detail setting

4.2.5 AP Router Mode Setting

In AP Router Mode, the AirMax5X behaves like a wireless router. The secondary Ethernet port of the AirMax5X will become WAN port. Both the wireless and the main Ethernet port becomes the LAN side. User can manage the AirMax5X through the wireless or main Ethernet port. And if the remote management is opened, user can also get to manage AirMax5X via the WAN side.



When you select the AP Router mode, additional wireless settings will appear for WAN port settings.

WAN Port Settings:	<input type="button" value="Setup"/>
Dynamic DNS Settings:	<input type="button" value="Setup"/>
Remote Management:	<input type="button" value="Setup"/>
DHCP Server Settings:	<input type="button" value="Setup"/>
DMZ Settings:	<input type="button" value="Setup"/>
Virtual Server Settings:	<input type="button" value="Setup"/>
Filtering Settings:	<input type="button" value="Setup"/>
Bandwidth Control:	<input type="button" value="Setup"/>

There are two important steps to set up the AP Router mode. First, you need to know what kind of WAN that your ISP or your network provided. Secondary you need to decide whether the AirMax5X will provide the DHCP IP via the LAN port or wireless Interface. If the AirMax5X does not provide the IP, the client needs to assign the IP by themselves.

4.2.5.1 WAN Port Settings

Operation Mode -> Setup -> WAN Port Settings

The AirMax5X support different authentication and IP assignment standards for the WAN port. It includes fixed IP, DHCP, PPPoE, PPTP and L2TP protocols. Please consult with your ISP about what authentication type is used for the WAN port connection.

WAN Port Settings

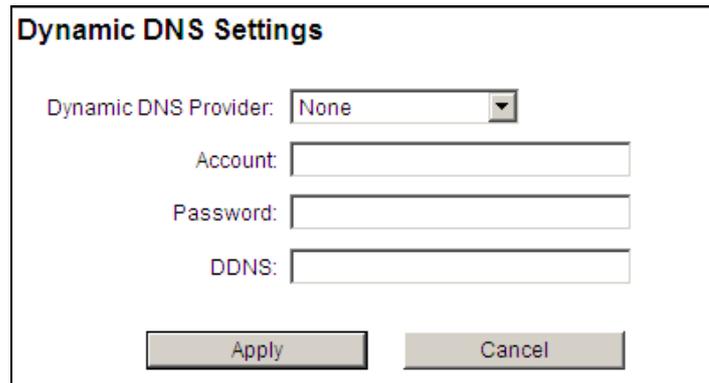
WAN Connection Type:

Host Name(optional):

4.2.5.2 Dynamic DNS Settings

Operation Mode -> Setup -> Dynamic DNS Settings

Dynamic DNS (DDNS) allows you to create a hostname that points to your dynamic IP or static IP address or URL. AirMax5X provide Dynamic DNS client using DynDNS, please visit <http://www.dyndns.org> for detail.



Dynamic DNS Settings

Dynamic DNS Provider:

Account:

Password:

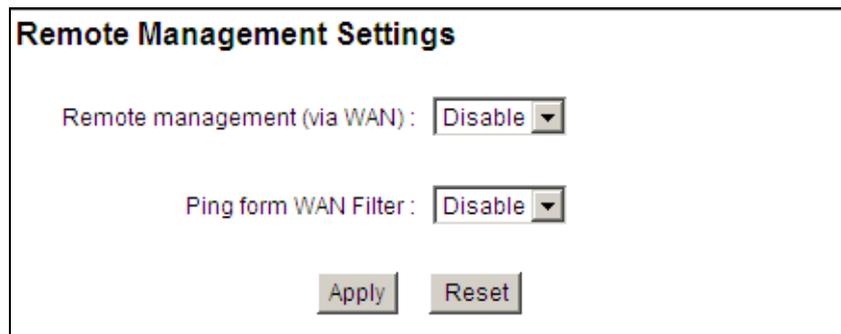
DDNS:

4.2.5.3 Remote Management Settings

Operation Mode -> Setup -> Remote Management

Remote Management allows administrator to manage the AirMax5X from WAN side. You can enable or disable.

- **HTTP Web Server Access:** You can enable or disable HTTP service from WAN side
- **Response to WAN ping:** You can disable or enable whether AirMax5X will response to PING command.



Remote Management Settings

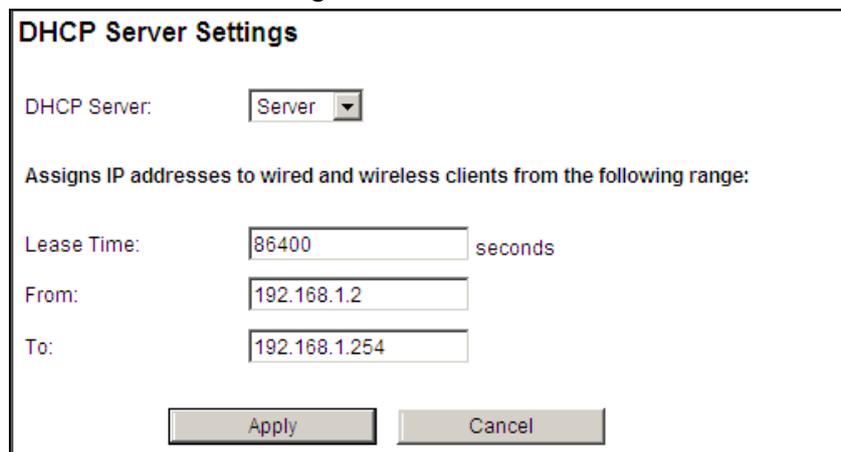
Remote management (via WAN) :

Ping form WAN Filter :

4.2.5.4 DHCP Server

Operation Mode -> Setup -> DHCP Server Settings

DHCP Server Settings is to assign private IP address to the devices in your local area network (LAN). The default LAN IP address of AirMax5X is 192.168.1.1, changing AirMax5X's IP address will also change the DHCP server's IP subnet.



DHCP Server Settings

DHCP Server:

Assigns IP addresses to wired and wireless clients from the following range:

Lease Time: seconds

From:

To:

4.2.5.5 DMZ

Operation Mode -> Setup ->DMZ Settings

DMZ opens all TCP/UDP ports to particular IP address on the LAN side. It allows setting up servers behind the AirMax5X.

DMZ Settings

DMZ Settings:

DMZ IP Address:

Enable the DMZ function and then enter the local DMZ IP address.

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

4.2.5.6 Virtual Server Settings

Operation Mode -> Setup ->Virtual Setting

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

Virtual Server Settings

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

Virtual Server:

Protocol:

IP Address:

Port Range: -

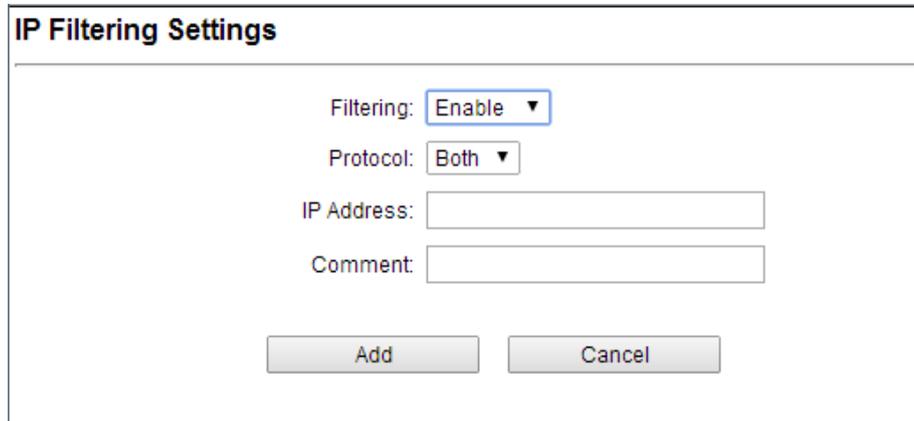
Comment:

No.	IP Address	Protocol	Port Range	Comment	Delete
1	192.168.1.60	BOTH	30-40	123	<input type="checkbox"/>

4.2.5.7 IP Filtering Settings

Operation Mode -> Setup -> IP Filtering Settings

IP filtering is simply a mechanism that decides which types of IP datagram will be processed normally and which will be discarded.



The screenshot shows a web form titled "IP Filtering Settings". It contains the following elements:

- Filtering:** A dropdown menu with "Enable" selected.
- Protocol:** A dropdown menu with "Both" selected.
- IP Address:** A text input field.
- Comment:** A text input field.
- Buttons:** "Add" and "Cancel" buttons at the bottom.

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

MAC/IP/Port Filtering: Select **Enable** or **Disable** the MAC/IP/Port Filtering function.

MAC address: Fill in the MAC address of source NIC, to restrict data transmission.

Port Range: Fill in the start-port and end-port number of source, to restrict data transmission.

Dest IP Address: Fill in the IP address of destination, to restrict data transmission.

Source IP Address: Fill in the IP address of source, to restrict data transmission.

Protocol: Select the protocol that you want to restrict. There are four options: None, TCP, UDP and ICMP.

Comment: Make a comment for the filtering policy.

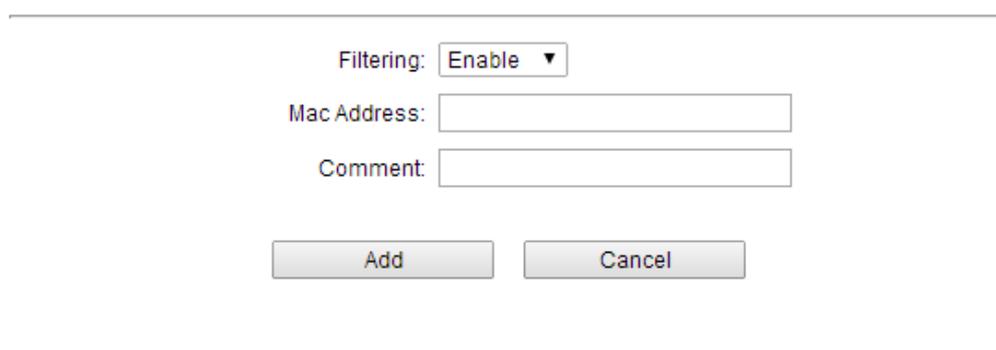
Apply: To grant or deny IP address, select **ADD** or **Delete Selected**.

4.2.5.8 MAC Filtering Settings

Operation Mode -> Setup -> MAC Filtering Settings

MAC filtering is simply a mechanism that decides which MAC address will be processed normally and which will be discarded.

Mac Filtering Settings



The screenshot shows a web form titled "Mac Filtering Settings". It contains the following elements:

- Filtering:** A dropdown menu with "Enable" selected.
- Mac Address:** A text input field.
- Comment:** A text input field.
- Buttons:** "Add" and "Cancel" buttons at the bottom.

4.2.5.9 Port Filtering Settings

Operation Mode -> Setup -> Port Filtering Settings

Port filtering is simply a mechanism that decides which Port will be processed normally and which will be discarded.

Port Filtering Settings

Filtering: ▾
Protocol: ▾
Port Range: -
Comment:

4.2.5.10 Bandwidth Control

Operation Mode -> Setup -> Bandwidth Control

Bandwidth Control can limit the maximum speed of individual device. It is also known as Traffic Shaping. The AirMax5X provides Per-IP Bandwidth Control for both uplink and downlink speed. It controls the speed of both wireless and wired interface.

To configure, please click on the “Bandwidth Control” button under wireless settings. The following screen will appear:

Bandwidth Control Settings

Quality of Service ▾
Local IP Address: -
Uplink BandWidth (Kbps):
Downlink BandWidth (Kbps):
Comment:

- **Enable:** Select to enable Bandwidth Control. The default value is disabled.
- **Local IP Address:** Fill in the local IP address
- **Uplink Bandwidth:** Input uplink Maximum upload bandwidth
- **Downlink Bandwidth:** Input downlink Maximum upload bandwidth.

4.2.6 Wireless ISP Mode Setting

In Wireless ISP Mode, AirMax5X 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.

Once you click on the “Setup” page, the wireless settings will appear.

Wireless ISP

Regulatory Domain:	Europe ▼	
Remote AP SSID:	airlive5x	Site Survey
<input checked="" type="checkbox"/> Enable Wireless <input type="checkbox"/> Disable SSID Broadcasting <input type="checkbox"/> Enable Isolated		
Lock to AP MAC:	00:00:00:00:00:00	
Radio Mode:	5G 11NA HT40 ▼	
Channel:	Auto Channel ▼	
Data Rate:	Auto ▼	
Security Setting:	Setup	
Transmit Power:	22 dbm ▼	
Transmit Distance:	15 Km ▼	
DFS Control:	Disable ▼	
DFS Domain:	ETSI ▼	
Advanced Settings:	Setup	
Access Control:	Setup	
WAN Port Settings:	Setup	

4.2.6.1 Remote AP SSID and Site survey

In Wireless ISP mode, you need to decide which remote AP that you want to associate. User can enter the SSID by themselves or click the site survey button, the AirMax5X will scan the available AP.

After click the “site survey” button, the available AP will pop-up in other page as below

Select	SSID	MAC Address	Channel	Signal Strength(%)	Security
<input type="radio"/>	ASMT-7F-PM-5G	14:D6:4D:CC:25:52	52	-94 dBm	WPA/WPA2/YesTKIP/CCMP/PSK
<input type="radio"/>	CL-WLAN-a	00:0B:86:AA:14:10	56	-85 dBm	WPA/YesCCMP/802.1x
<input type="radio"/>	CL-WLAN	00:1A:1E:67:ED:10	64	-83 dBm	WPA/YesTKIP/802.1x
<input type="radio"/>	tyler_5G	60:A4:4C:67:20:0D	149		WPA2/YesCCMP/PSK
<input type="radio"/>	ac5g	80:1F:02:75:EE:4B	153		WPA2/YesCCMP/PSK
<input type="radio"/>	default_5G	00:30:4F:A1:C7:24	149		WPA2/YesCCMP/PSK
<input type="radio"/>	test_5G_2	02:30:4F:A1:C7:25	149		WPA2/YesCCMP/PSK
<input type="radio"/>	...-GUEST	00:1A:1E:67:ED:11	64	-84 dBm	none

Click here to select SSID for Association or Signal Survey

For antenna alignment. It will display signal

ASSOCIATE RESCAN CLOSE

To connect with the selected SSID. This function is available only in Client or Bridge Mode.

Select the SSID which you want to connect , and click the “SET SECURITY” , type in the key if required. Then Click “Save” Button. If the key is correct , the AirMax5X will ask users to reboot the device.

After reboot is finished , the AirMax5X is connected with another remote AP.

The rest of the setting in wireless ISP is same as the AP Router mode. Please refer the chapter 4.2.5

- **Add (to WDS):** Please choose a SSID before click on this button. This button is available only in Client, WDS or WDS + AP modes. Once you click on this button, AirMax5X will attempt to make a connection with the selected network. If there is encryption needed, the AirMax5X will prompt you to enter the encryption key. Please make sure you enter the correct encryption key, the AirMax5X will not check whether the encryption key is correct.
- **Signal Strength:** This is a value to show the signal level of the AirMax5X. In general, remote APs with stronger signal will display higher level.

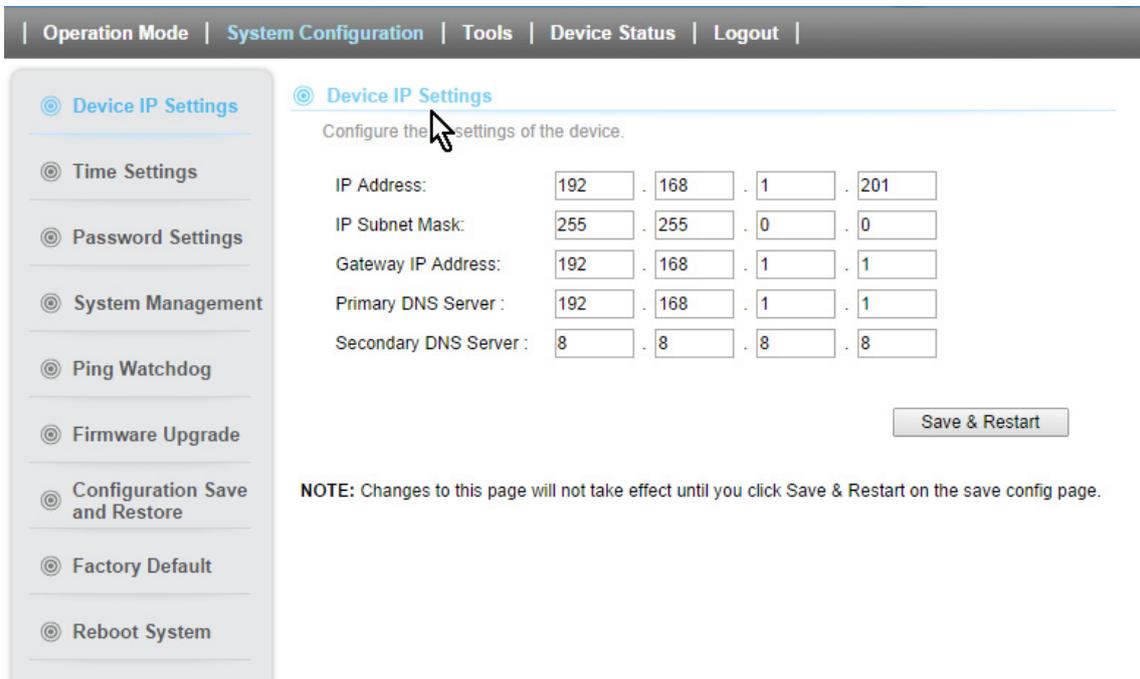
5

Web Management: System Configuration and Status

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. .

5.1 System Configuration

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.



5.1.1 Device IP Settings

System Configurations>> Device IP Settings

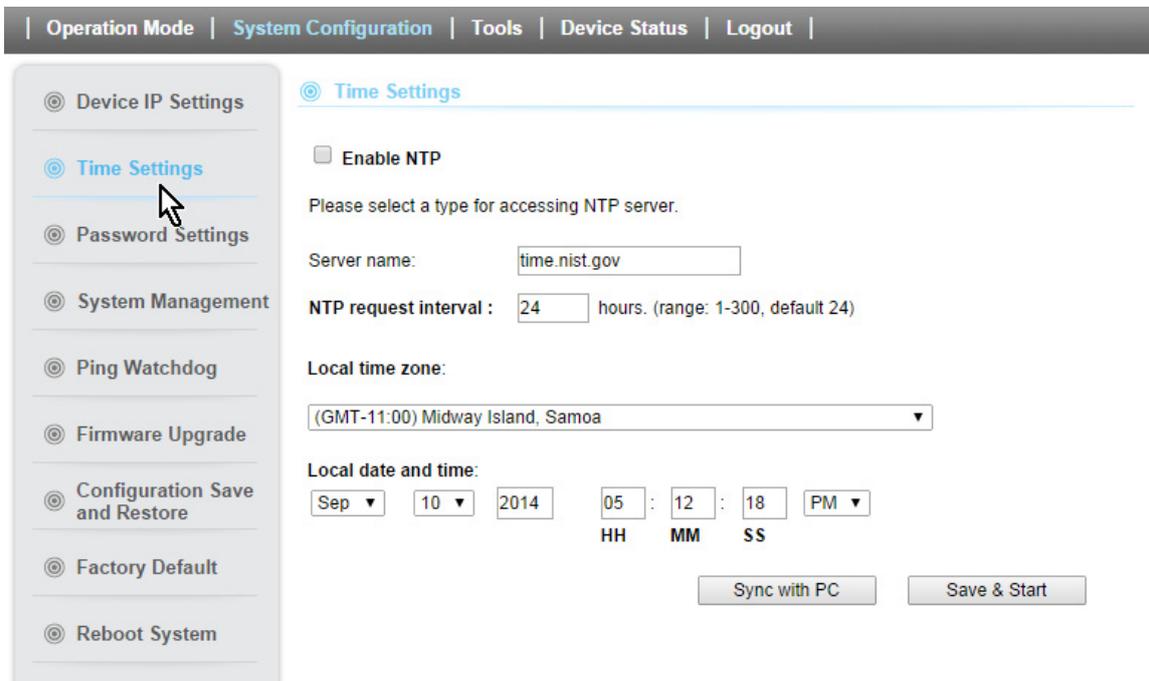
The Device IP Settings screen allows you to configure the IP address and subnet of the device.

- **IP Address and IP Subnet Mask:** Default values are 192.168.1.1 and 255.255.255.0 respectively. It is important to note that there are similar addresses falling in the standard private IP address range and it is an essential security feature of the device. Because of this private IP address, the device can no longer be accessed (seen) from the Internet.
- **Gateway IP Address:** Enter the IP address of your default gateway.
- **DNS Server:** The Domain Name System (DNS) is a server on the Internet that translates logical names such as “www.yahoo.com” to IP addresses like 66.218.71.80. In order to do this, a query is made by the requesting device to a DNS server to provide the necessary information. If your system administrator requires you to manually enter the DNS Server addresses, you should enter them here.
- Click **Save and Restart** to go to the next screen.

5.1.2 Time Settings

System Configuration ->Time Settings

It is important that you set the date and time for your AirMax5X so that the system log will record the correct date and time information. We recommend you choose “Enable NTP” so the time will be keep even after reboot. If your AirMax5X is not connected to Internet, please enter the time manually. Please remember to select your local time zone and click “Apply” to finish.



The screenshot shows the web management interface with a navigation bar at the top containing: Operation Mode | System Configuration | Tools | Device Status | Logout |. On the left is a sidebar menu with options: Device IP Settings, Time Settings (highlighted with a mouse cursor), Password Settings, System Management, Ping Watchdog, Firmware Upgrade, Configuration Save and Restore, Factory Default, and Reboot System. The main content area is titled "Time Settings" and contains the following configuration options:

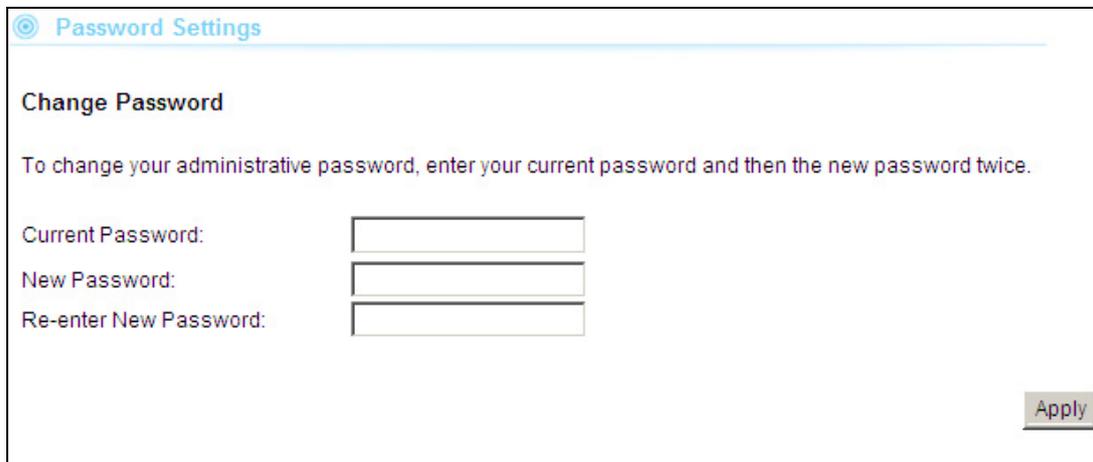
- Enable NTP
- Please select a type for accessing NTP server.
- Server name:
- NTP request interval: hours. (range: 1-300, default 24)
- Local time zone:
- Local date and time: : :

At the bottom right of the configuration area are two buttons: "Sync with PC" and "Save & Start".

5.1.3 Password Settings

System Configuration -> Time Settings

To change password, please go to “System Configuration” -> “Password Settings” menu.

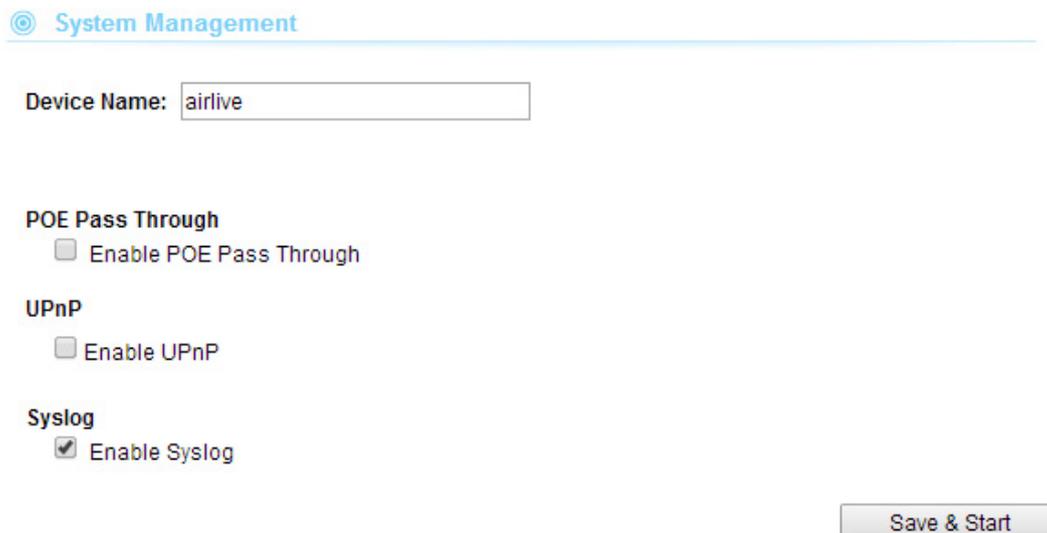


The screenshot shows the 'Password Settings' page. At the top, there is a title 'Password Settings' with a home icon. Below the title is the section 'Change Password'. A descriptive text reads: 'To change your administrative password, enter your current password and then the new password twice.' There are three input fields: 'Current Password:', 'New Password:', and 'Re-enter New Password:'. An 'Apply' button is located at the bottom right of the form.

5.1.4 System Management

System Configuration -> System Management

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



The screenshot shows the 'System Management' page. At the top, there is a title 'System Management' with a home icon. Below the title is a 'Device Name' field containing the text 'airlive'. There are three sections with checkboxes: 'POE Pass Through' with 'Enable POE Pass Through' (unchecked), 'UPnP' with 'Enable UPnP' (unchecked), and 'Syslog' with 'Enable Syslog' (checked). A 'Save & Start' button is located at the bottom right of the form.

- **PoE Pass Through:** To Enable PoE Pass Through. The detail introduction of PoE Pass Through please refer the chapter 5.3
- **UPnP:** Administrator can enable or disable the UPnP function here.
- **Syslog:** To enable or disable the syslog here.

5.1.5 Ping Watchdog

System Configuration -> Ping 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.

⊙ Ping Watchdog

The Ping Watchdog will ping up to a IP addresses for connection status. If the remote IP addresses do not respond to Ping, the device will either reconnect or power reboot.

Ping Watchdog: Enable Disable

IP Address 1: . . .

Ping Frequency: Seconds (10 to 999, default is: 120)

Failed tries: (default is 2 tries)

Action:

NOTE: Watchdog will take effect 10 minutes after startup. when filled, IP Address 1 must fail to respond for watchdog to take action.

Save & Start

- **PING Frequency:** means "How often the CPE will PING". For example, it will PING once every "120" seconds.
- **Fail Tries** means "How many times fails before the CPE will judge the PING failed". For example "2" means the CPE will reconnect if the PING doesn't respond for 2 times.

When you set the Ping Frequency to every "120" seconds and Fail Tries to "2". It means the CPE will ping every 120 seconds, after the second failure, it will reconnect.

Actions:

- Reboot: the AirMax5X will do a power recycle after Ping Failed.

5.1.6 Firmware Upgrade

System Configuration -> Firmware Upgrade

You can upgrade the firmware of your AirMax5X (the software that controls your AirMax5X'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.

© Firmware Upgrade

Select the firmware file by clicking Browse, and click UPGRADE.

WARNING : Don't use wireless connection to upload the firmware, To avoid system crashes.

NOTE:

1. Do not power off the router while upgrading the firmware.
2. Some browsers would fail to locate the firmware file when there is any localized character in the firmware file path.

■ Upgrade Firmware:

To update the AirMax5X firmware, first download the firmware from AirLive website to your local disk, and then from the above screen enter the path and filename of the firmware file (or click **Browse** to locate the firmware file). Next, Click the **Upgrade** button to start.

The new firmware will be loaded to your AirMax5X. 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 AirMax5X unless the new firmware has new features you need or if it has a fix to a problem that you've encountered. For the data structure might be change after firmware upgrade, it's better for the administrator to reset the device to factory default for cleaning the original configuration data.

5.1.7 Configuration Save and Restore

System Configuration -> Configuration Save and Restore

You can save system configuration settings to a file, and later download it back to the AirMax5X by following the steps.

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

Configuration Save and Restore

Click SAVE to save the configuration to a management host.

SAVE

Select the text configure file by clicking Browse, then click RESTORE.

Browse...

RESTORE

NOTE: Some browsers would fail to locate the configuration file when there is any localized character in the configuration file path.

- Step 2** Click the SAVE button to save the current configuration into the specified file. Or click the *Browse* button to locate the configuration file, and then click the RESTORE button to restore the system configuration from the specified file.

5.1.8 Factory Default

System Configuration -> Factory Default

You can reset the configuration of your AirMax5X to the factory default settings.

- Step 1** Select *Factory Default* from the *System Configuration* menu.

Factory Default

Do you really want to restore the configuration to factory defaults? YES

CAUTION: Restoring factory default settings will erase all your previous settings.

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

5.2 Device Status

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

Device Information

Firmware Version:	1.0.2 (Jul 31 2014)
Device IP:	192.168.1.200
Device MAC:	00:1A:EF:AB:00:16
Gateway IP:	192.168.1.200
DNS IP:	192.168.1.1
Wireless MAC:	00:1A:EF:AB:00:18
Uptime: (dd:hh:mm:ss)	0 day 21:46:8
CPU Loading:	<div style="width: 0%;"><div style="width: 0%;"></div></div> 0%

Memory Information

Total Available:	<div style="width: 73%;"><div style="width: 73%;"></div></div> 73%	47844KB / 65536KB
Used:	<div style="width: 15%;"><div style="width: 15%;"></div></div> 15%	7140KB / 47844KB
Free:	<div style="width: 85%;"><div style="width: 85%;"></div></div> 85%	40704KB / 47844KB
Buffers:	<div style="width: 0%;"><div style="width: 0%;"></div></div> 0%	0KB / 7140KB
Cached:	<div style="width: 13%;"><div style="width: 13%;"></div></div> 13%	908KB / 7140KB

ARP Table

IP Address	MAC Address	Interface
192.168.1.218	bc:ae:c5:0d:89:f0	br0

5.2.1 Device Information

This page shows the general information about AirMax5X such as firmware version, device IP/MAC, WAN IP/MAC (in router modes), Gateway IP(in router modes), DNS IP...etc.

Below are some additional explanations on some status information of this page:

- **CPU Loading** Display the CPU usage.
- **Memory Information** Display how much memory is used and free.
- **Firmware version:** Shows the current firmware version installed in this AirMax5X
- **Wireless MAC:** This is the wireless MAC address (BSSID) of this AiMax5N.
- **Uptime:** This is the time that the AirMax5X has been running since last power up.
- **ARP Table:** Display the corresponding IP and MAC address Table.

5.2.2 Wireless Information

This page shows the information about wireless status such as current operation mode, wireless traffic, error packets, device's BSSD, connecting State, channel, and encryption used.

Wireless Information

Operation Mode: Access Point
Physical Address: 00:1A:EF:21:7E:BA
Band: IEEE 802.11a/n
Radio Channel: 48
Encryption: OPEN-NONE

SSID	BSSID	Encryption
airlive	00:4F:60:21:7E:BA	NONE

WLAN Statistics

	Bytes	Packets	Errors
Received:	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
Transmitted:	<input type="text" value="82560"/>	<input type="text" value="264"/>	<input type="text" value="0"/>

5.2.3 Internet Information

This page shows the information about WAN port of the AirMax5X. It includes the type of WAN port authentication used and the IP address information about the WAN port.

Device Information

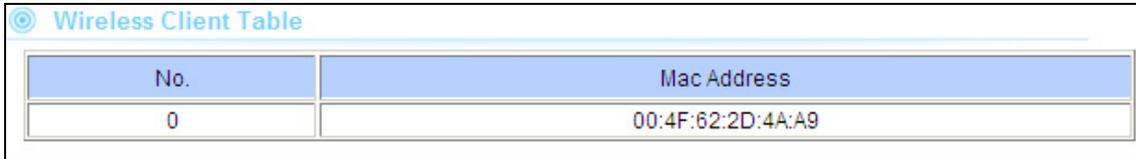
Connection Method: STATIC
Physical Address: 00:1A:EF:21:7E:BA
IP Address: 172.16.1.1
Network Mask: 255.255.0.0
Default Gateway: 172.16.254.254
Connect State: Disassociated

WAN STATISTICS

	Bytes	Packets	Errors
Received:	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
Transmitted:	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>

5.2.4 Wireless Client Table

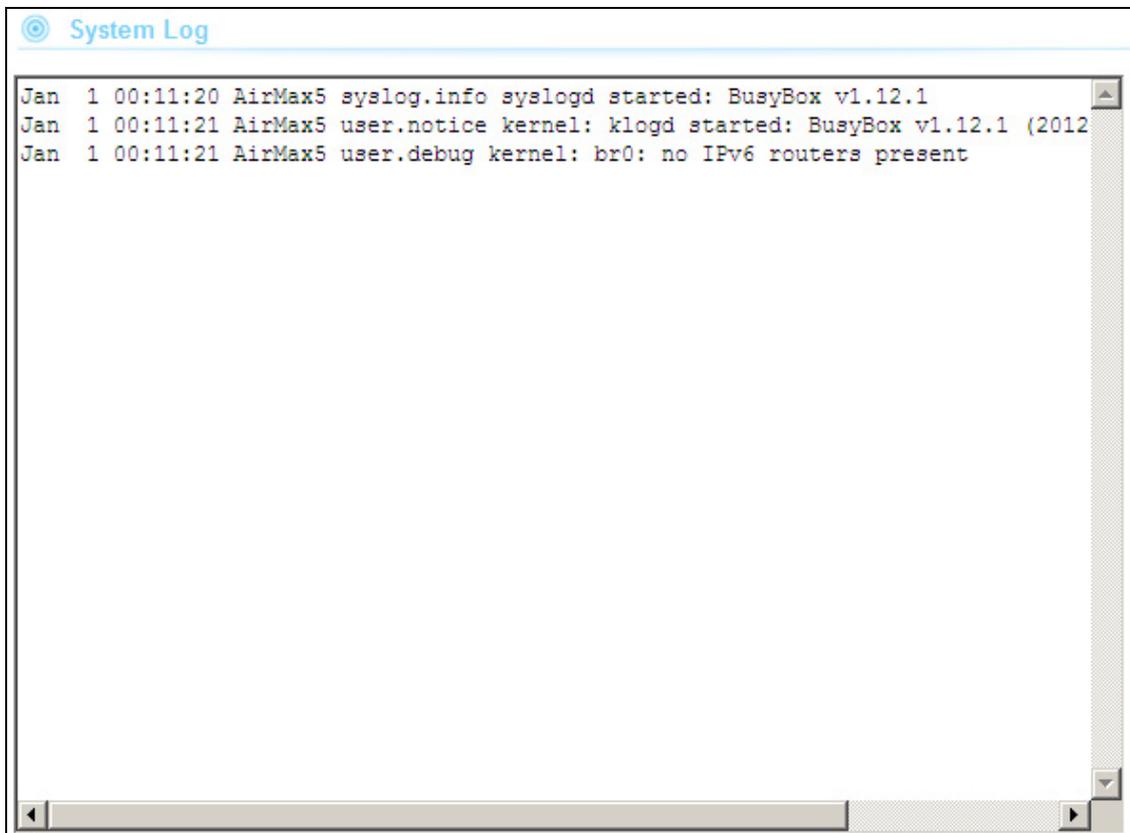
This function displays the information about wireless clients that are associated with AirMax5X. It includes signal strength, TX and RX data rate, MAC address, and the state.



No.	Mac Address
0	00:4F:62:2D:4A:A9

5.2.5 System Log

The System Log displays the system activities, login, and system error report. If you need to report a problem to Air Live, please be sure to send us the System Log information also.



```
Jan 1 00:11:20 AirMax5 syslog.info syslogd started: BusyBox v1.12.1
Jan 1 00:11:21 AirMax5 user.notice kernel: klogd started: BusyBox v1.12.1 (2012
Jan 1 00:11:21 AirMax5 user.debug kernel: br0: no IPv6 routers present
```

5.3 PoE Pass-through (Power up another Device)

The AirMax5X have a special feature which is PoE Pass through, the PoE pass-through. The PoE pass-through allows the AirMax5X to have 48V output in order to power up another AirMax5X or IP cameras.

The PoE pass-through function is disabled at default settings. Before enable the PoE Pass-through function, please make sure the device you want to power up is connect to the secondly port and the device can accept 48V input.

To enable the PoE pass through, please follow below steps:

1. Connect the AirMax5X's mainly port to PoE injector's PoE port
2. Connect the PC/NB in PoE injector's LAN port
3. Connect the device you want to power up to the secondly port of the AirMax5X
4. Visit AirMax5X's web UI and enable the PoE pass-through function in **System Configuration -> System Management**
5. The device should be power up



6

Antenna Alignment

It is important to align your antenna correctly with the remote device to get the best signal and performance. The AirMax5X is equipped with a 14dBi antenna. There is a connector for external antenna if more distance or different angle coverage is required. In this chapter, we will first explain the design and function of the built-in antenna.

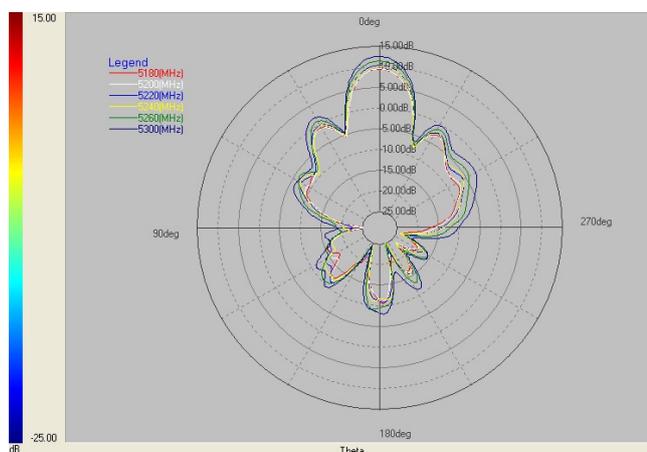
We will provide instructions on the two alignment methods later in this chapter.

6.1 About AirMax5X's Antenna

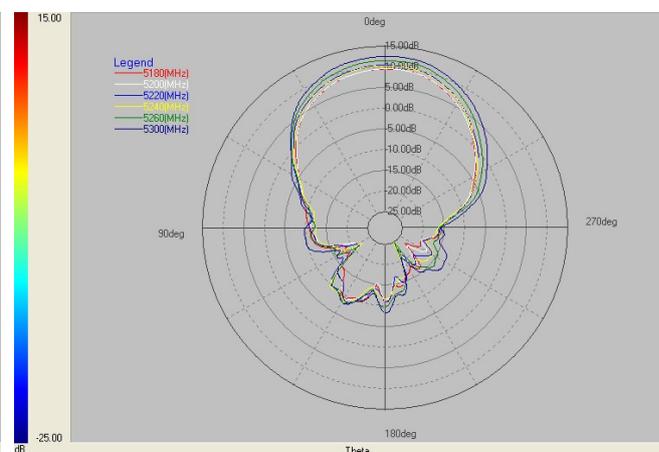
The AirMax5X's built-in 2T2R antenna has the following characteristics:

- **Gain:** 14dBi
- **Type:** Patch Antenna
- **Vertical Coverage Angle:** 20 degree forward
- **Horizontal Coverage Angle:** 30 degree forward

Vertical Pattern



Horizontal Pattern



6.1.1 Mounting Adjustment

The degree you can adjust the AirMax5X's antenna depends on what mounting kit you use. Using the standard strap mount allows you to rotate the CPE in the horizontal plane only. As long as 2 wireless devices are at about the same elevation, this adjustment is already enough.

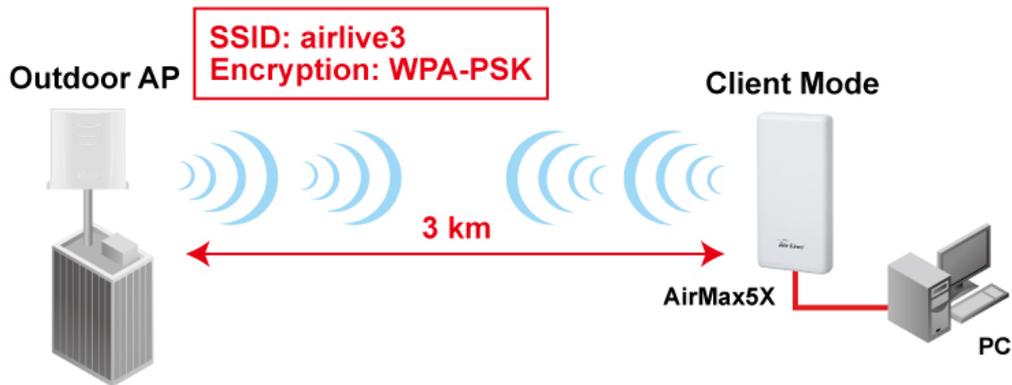
6.2 Preparation before Installation

The antenna alignment is for small adjustment only, you should not use it find remote AP. The correct way is to use a Graphic Information System (GIS) program such as "Google Earth" to find the locations of the installation site and the nearest AP/Bridge. Then measure the approximate direction and angle. It will also help to bring a pair of hi power binocular for sight survey.



6.3 Antenna Alignment using Signal Survey

Signal Survey function can display the Signal Strength value in real time to help you with antenna alignment. The Signal Survey is a subnet of the Site Survey function; you do not need to enter the wireless settings in advance. Please follow the example below to complete antenna alignment using Signal Survey function.



Step 1 Go to the Sit Survey function

Wireless Settings

Regulatory Domain: All Channel

Remote AP SSID:

Network ID (SSID): Airlive

Site Survey

Select	SSID	MAC Address	Channel	Signal Strength(%)	Security
<input type="radio"/>	ASMT-7F-PM-5G	14:D6:4D:CC:25:52	52	-94 dBm	WPA/WPA2/YesTKIP/CCMP/PSK
<input type="radio"/>	CL-WLAN-a	00:0B:86:AA:14:10	56	-85 dBm	WPA/YesCCMP/802.1x
<input type="radio"/>	CL-WLAN	00:1A:1E:67:ED:10	64	-83 dBm	WPA/YesTKIP/802.1x
<input type="radio"/>	tyler_5G	60:A4:4C:67:20:0D	149	-88 dBm	WPA2/YesCCMP/PSK
<input type="radio"/>	ac5g	80:1F:02:75:EE:4B	153	-69 dBm	WPA2/YesCCMP/PSK
<input type="radio"/>	Default_5G	00:30:4F:A1:C7:24	149	-89 dBm	WPA2/YesCCMP/PSK
<input type="radio"/>	Guest_5G_2	02:30:4F:A1:C7:25	149	-82 dBm	WPA2/YesCCMP/PSK
<input type="radio"/>	CL-GUEST	00:1A:1E:67:ED:11	64	-84 dBm	none

ASSOCIATE RESCAN CLOSE

- Step 2** Check the Signal Strength of the desired AP. For identify the AP quicker, we suggest you to written the MAC address of the desired AP and using the MAC to filter out your target.
- Step 3** If the Signal Strength is too weak to make a connection, please adjust the antenna.
- Step 4** Refresh the Site Survey page and check the Signal Strength again.

Select	SSID	MAC Address	Channel	Signal Strength(%)	Security
<input type="radio"/>	ASMT-7F-PM-5G	14:D6:4D:CC:25:52	52	-94 dBm	WPA/WPA2/YesTKIP/CCMP/PSK
<input type="radio"/>	CL-WLAN-a	00:0B:86:AA:14:10	56	-85 dBm	WPA/YesCCMP/802.1x
<input type="radio"/>	CL-WLAN	00:1A:1E:67:ED:10	64	-83 dBm	WPA/YesTKIP/802.1x
<input type="radio"/>	tyler_5G	60:A4:4C:67:20:0D	149	-88 dBm	WPA2/YesCCMP/PSK
<input type="radio"/>	ac5g	80:1F:02:75:EE:4B	153	-69 dBm	WPA2/YesCCMP/PSK
<input type="radio"/>	Default_5G	00:30:4F:A1:C7:24	149	-89 dBm	WPA2/YesCCMP/PSK
<input type="radio"/>	Guest_5G_2	02:30:4F:A1:C7:25	149	-82 dBm	WPA2/YesCCMP/PSK
<input type="radio"/>	CL-GUEST	00:1A:1E:67:ED:11	64	-84 dBm	none

Step 5 Once the Signal is good enough, please check the radio box in front of the desired AP and then click on the ASSOCIATE button for building the connection.

6.4 Antenna Alignment using RSSI LED

There are 3 LED indicators on the back of the AirMax5x that is dedicated to display the RSSI signal strength after device is connecting.

6.4.1 RSSI LED Table

The RSSI LED will only function when the wireless link is established. Therefore, you should enter all the wireless settings correctly before installation. So the connection will establish while doing antenna adjustment.

Below table is RSSI Level for AirMax 5X's LED.

Number of LED lighting	RSSI Level (dBm)
3	-35 ~ -60
2	-65 ~ -75
1	-75 ~ -95
Non	>-35 or <-95

6.4.2 Antenna Alignment Procedures using RSSI LED

At the first, please configure the Airmax 5x into client mode or WDS station mode. Please refer the chapter 4.2.2 for the detail setting.

After setting is finished, you can take the AirMax5 to the installation site and adjust the antenna by looking at the LED indicator. You might never get the full signal, but you can find the best position where the signal is strongest



7

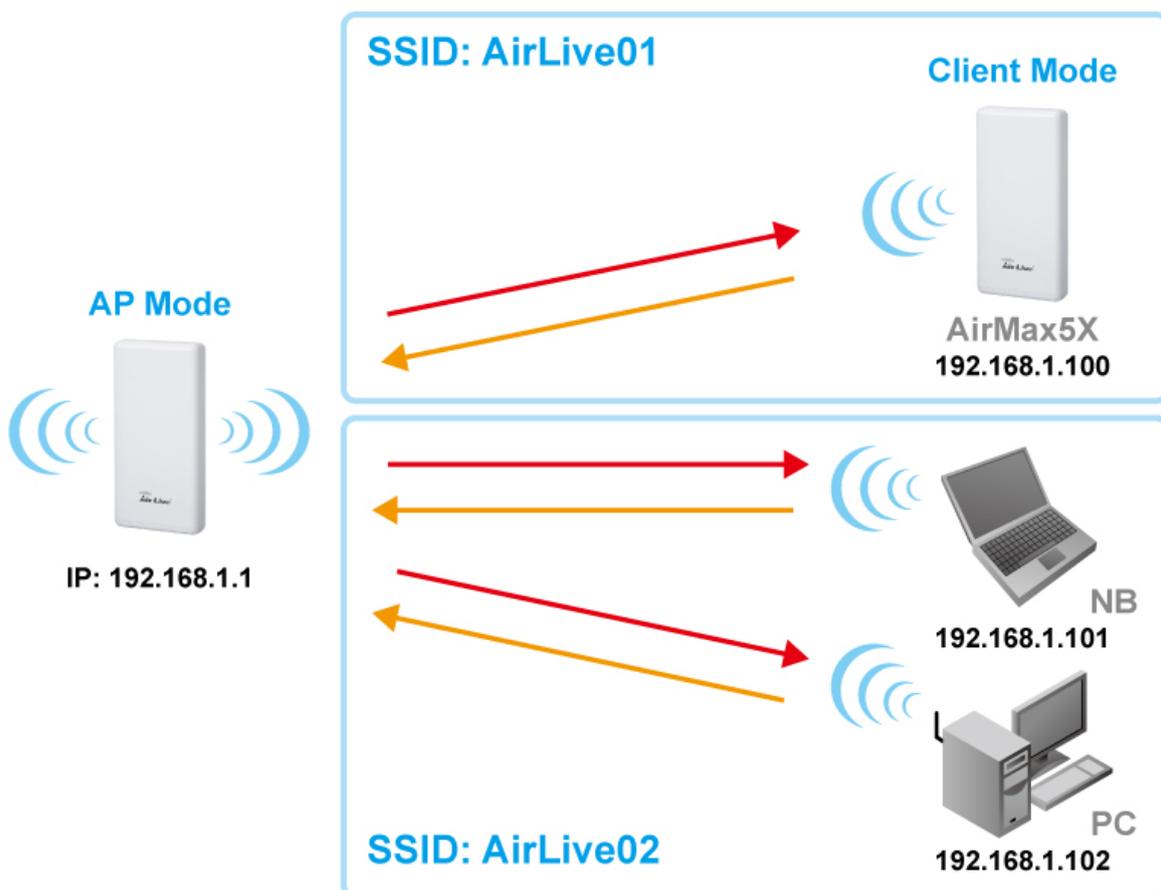
Application Example: Infrastructure

In this chapter, you will learn how to utilize AirMax5X's Access Point mode, Client Infrastructure Mode, and WDS AP/Station mode in one application example.

7.1 Application Environment

In this application example, an AirMax5X in Access Point mode is in the center of an infrastructure topology with two virtual wireless networks. Each wireless network has its own SSID, security Policy and Bandwidth policy.

Below is the general description about the devices of the network.

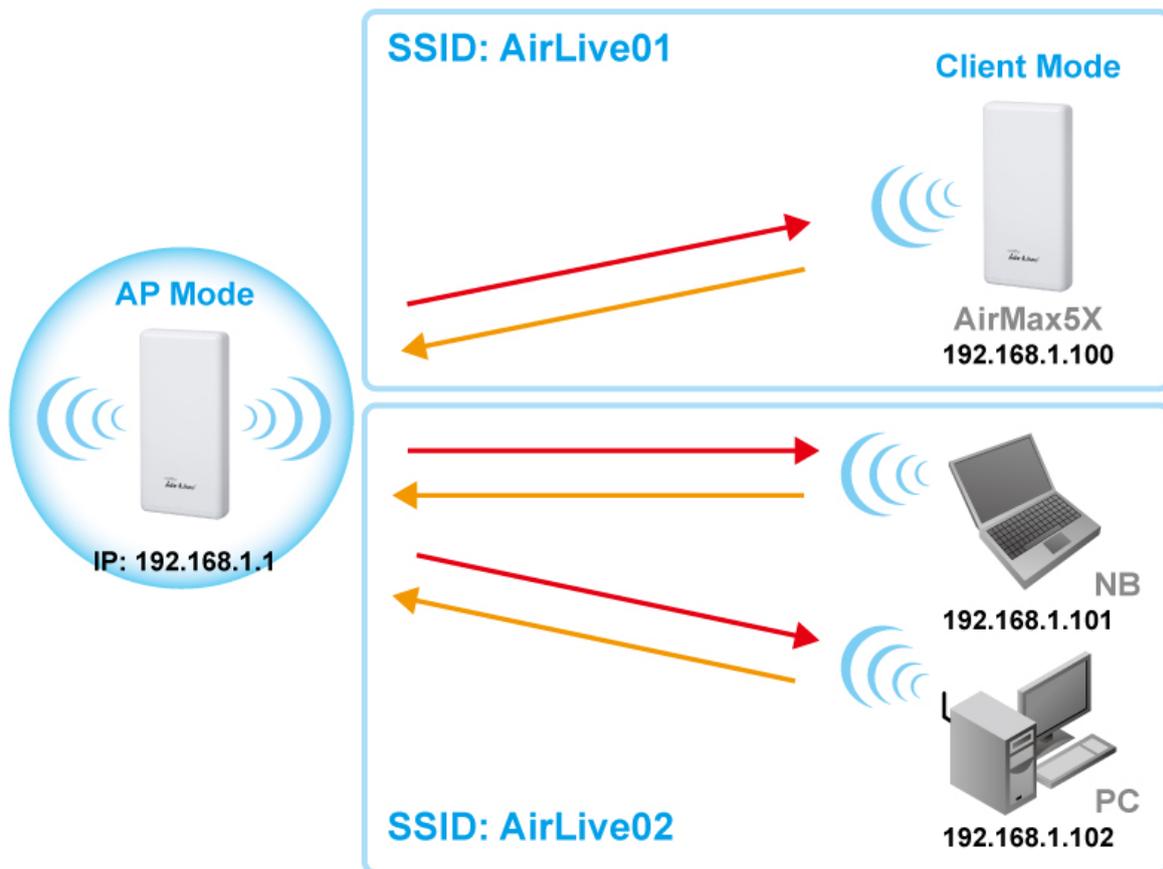


Central AP: AirMax5X in Access Point Mode

Client: AirMax5X in Client Mode

- Associate the AirLive01 and share the bandwidth to remote LAN

7.2 Central AP: Access Point Mode



The configuration of Central AP involves the followings:

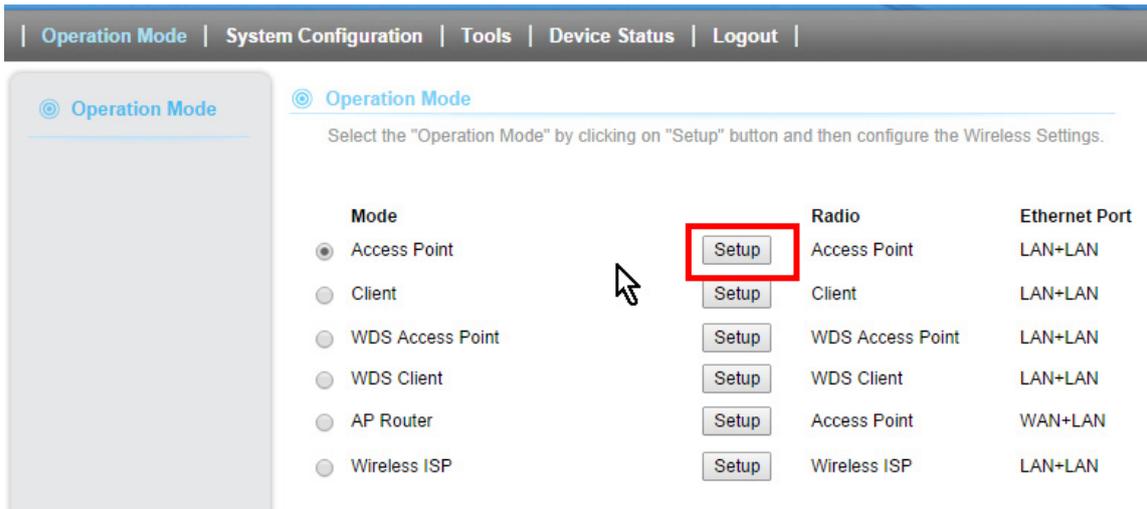
- Set SSID to **Airlive**
- Set the Transmit Distance to the longest distance between AP to the Client. For example: There are two Clients. One is 5Km away the central AP, the other is 1Km. Please set the **Transmit Distance** longer than 5Km

7.2.1 AP Wireless Settings

AP : AirMax5X in AP Mode

- Set device IP to 192.168.1.1 with subnet mask of 255.255.255.248
- Connect to the Access Point using *AP mode*.

Step 1 Click on “setup” button on the “Operation Mode” page



The screenshot shows the web interface for configuring the AirMax5X device. The top navigation bar includes 'Operation Mode', 'System Configuration', 'Tools', 'Device Status', and 'Logout'. The main content area is titled 'Operation Mode' and contains a list of modes and their corresponding radio and Ethernet port configurations. The 'Access Point' mode is selected, and its 'Setup' button is highlighted with a red box.

Mode	Radio	Ethernet Port
<input checked="" type="radio"/> Access Point	Access Point	LAN+LAN
<input type="radio"/> Client	Client	LAN+LAN
<input type="radio"/> WDS Access Point	WDS Access Point	LAN+LAN
<input type="radio"/> WDS Client	WDS Client	LAN+LAN
<input type="radio"/> AP Router	Access Point	WAN+LAN
<input type="radio"/> Wireless ISP	Wireless ISP	LAN+LAN

Step 2 On the wireless setting page; please enter the SSID, Channel and Transmit distance, then press “Apply” to make changes.

Operation Mode Settings

Network ID (SSID):

Enable Wireless
 Disable SSID Broadcasting
 Enable Isolated

Radio Mode:

Channel:

Data Rate:

Security Setting:

Transmit Power:

Transmit Distance:

DFS Control:

DFS Domain:

Advanced Settings:

Access Control:

Bandwidth Control:

Step 3 Go to the Security Setting and set the security policy separately.

Security Settings

Select SSID:

Select Security Policy:

Encryption Type: TKIP AES TKIPAES

Pre-Shared Key:

Key Renewal Interval: seconds (60 ~ 9999)

Security Settings

Select SSID:

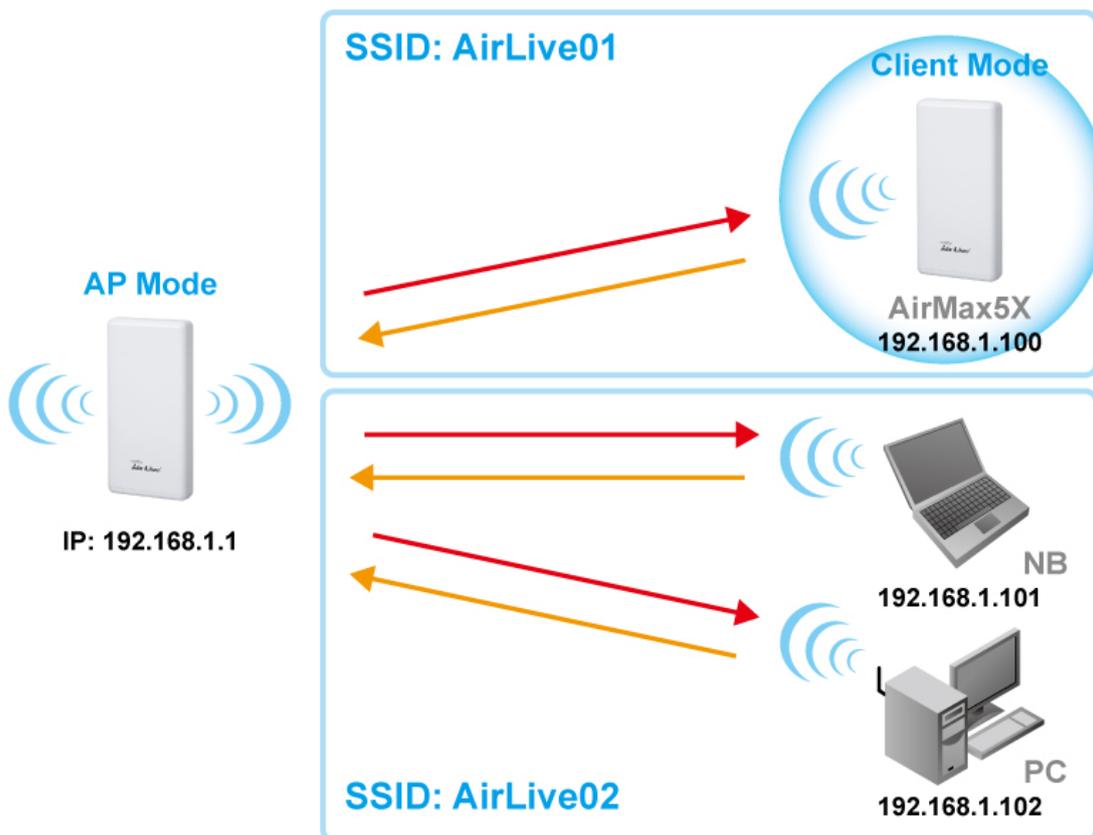
Select Security Policy:

Encryption Type: TKIP AES TKIPAES

Pre-Shared Key:

Key Renewal Interval: seconds (60 ~ 9999)

7.3 Client: Client Mode



Client : AirMax5X in Client Infrastructure Mode

- Set device IP to 192.168.1.100 with subnet mask of 255.255.255.248
- Connect to the Access Point using *Client mode*.
- Use Site Survey to connect and associate with AP.
- Set the transmit distance to correct value.

7.3.1 Device IP Address

Step 1 Go to “System Configuration -> Device IP settings”. Select “Assign Static IP to this device”. Then enter the IP address and Subnet Mask as bellowed. Click Apply when finished.

Device IP Settings

You can select one of the following two approaches to assign an IP address to this device.

IP Address:	192	.	168	.	1	.	200
IP Subnet Mask:	255	.	255	.	255	.	0
Gateway IP Address:	192	.	168	.	1	.	200
Primary DNS Server:	192	.	168	.	1	.	1
Secondary DNS Server:	8	.	8	.	8	.	8

Save & Restart

7.3.2 Client Wireless Settings

Step 1 Go to “Operation Mode” menu. Select “Client”, and then click on “Change Mode” button.

Operation Mode | System Configuration | Tools | Device Status | Logout

Operation Mode

Select the "Operation Mode" by clicking on "Setup" button and then configure the Wireless Settings.

Mode	Radio	Ethernet Port
<input checked="" type="radio"/> Access Point	Access Point	LAN+LAN
<input type="radio"/> Client	Client	LAN+LAN
<input type="radio"/> WDS Access Point	WDS Access Point	LAN+LAN
<input type="radio"/> WDS Client	WDS Client	LAN+LAN
<input type="radio"/> AP Router	Access Point	WAN+LAN
<input type="radio"/> Wireless ISP	Wireless ISP	LAN+LAN

Step 2 Press “Setup” to enter the wireless settings page. Click on the Site Survey button for searching the remote AP.

© Operation Mode Settings

Regulatory Domain: United States ▼

Remote AP SSID:

Enable Wireless
 Disable SSID Broadcasting
 Enable Isolated

Radio Mode: 5G 11NA HT40 ▼

Channel: Auto Channel ▼

Data Rate: Auto ▼

Security Setting:

Transmit Power: 27 dbm ▼

Transmit Distance:

Step 3 After pressing “Site Survey” button, the following page should appear. Select “AirLive01” and press “Associate” button to connect

Select	SSID	MAC Address	Channel	Signal Strength(%)	Security
<input type="radio"/>	ASMT-7F-PM-5G	14:D6:4D:CC:25:52	52	-94 dBm	WPA/WPA2/YesTKIP/CCMP/PSK
<input type="radio"/>	CL-WLAN-a	00:0B:86:AA:14:10	56	-85 dBm	WPA/YesCCMP/802.1x
<input checked="" type="radio"/>	CL-WLAN	00:1A:1E:67:ED:10	64	-83 dBm	WPA/YesTKIP/802.1x
<input type="radio"/>	tyler_5G	60:A4:4C:67:20:0D	149	-88 dBm	WPA2/YesCCMP/PSK
<input type="radio"/>	ac5g	80:1F:02:75:EE:4B	153	-69 dBm	WPA2/YesCCMP/PSK
<input type="radio"/>	Default_5G	00:30:4F:A1:C7:24	149	-89 dBm	WPA2/YesCCMP/PSK
<input type="radio"/>	Guest_5G_2	02:30:4F:A1:C7:25	149	-82 dBm	WPA2/YesCCMP/PSK
<input type="radio"/>	CL-GUEST	00:1A:1E:67:ED:11	64	-84 dBm	none

Step 4 The AirMax5X will prompt you to enter security policy information. Select WPA-PSK and enter your Pre-Shared Key.

Security Settings

Client Mode

Select Security Policy:

Encryption Type: TKIP AES

Pre-Shared Key:

Step 5 Click on “Apply”. After a few seconds, the following screen will appear to show successful connection.



You have now setup a successful Infrastructure network with AirMax5X in Access Point and Client modes

7.4 WDS AP Mode and WDS Station Mode

If you require the PC's or client's MAC addresses to be preserved when the data pass through the Access Point, it is necessary to use the WDS AP mode for remote side AirMax5X and another AirMax5X running for WDS station in Client side.

To set the AirMax5X, it is very simple. All of the setting is same as the access point mode and client mode. Please refer the chapter 7.2 for WDS AP mode and 7.3 for WDS Station Mode.

8

Specifications

The specification of AirMax5X is subject to change without notice. Please use the information with caution.

8.1 Features

8.1.1 General Feature

- 2T2R 300Mbps
- IEEE 802.11a/n
- Runs from 5.1GHz to 5.8GHz Spectrum
- 2 x 10/100 Ethernet Port
- Built-in 14 dBi 2T2R Antenna
- Up to 27dBm Output Power Max(limited according to regulations in EU and U.S.)
- AP, Client, Router, WISP Modes, WDS AP, WDS Station
- Passive 48V PoE Powered
- PoE Pass Through
- Support Wireless Access Control, Client Isolation

8.2 Specifications

Hardware

2T2R Wireless 802.11 a/n Standard

2 x 10/100 Ethernet Port

48V Passive PoE (accept from 24V~48V)

Reset Button on PoE Injector and AirMax5X

Antenna

Built-in Directional Antenna: 14dBi

Frequency Band

In 5GHz spectrum. Available frequency range varies according to the regulations in each country or region.

Data Rate

802.11a: up to 54Mbps
802.11n (20MHz): up to 144Mbps
802.11n (40MHz): up to 300Mbps

Power Supply

Power Adapter with PoE Injector: 48V/1A output

Media Access Control

CSMA/CA

Sensitivity

90dBm@802.11a
88dBm@802.11n

Output Power

(Limited according to regulation in EU and United States)

802.11a: up to 27 ± 1 dBm
802.11n: up to 22 ± 1 dBm

Mode

AP, Client, Router, WISP Modes, WDS AP , WDS Station

Security

64/128bit WEP
WPA (TKIP with IEEE 802.11x)
WPA2 (AES with IEEE 802.11x)

Software

Site Survey with RSSI Signal Survey
User Friendly Web Management
Channel list selection
Support adjustable output power
WEP over WDS support
AP, Client, Router, WISP Modes, WDS AP, WDS Station
Support DHCP Server, Client and Relay
Support Wireless Access Control, Client Isolation
Support Virtual Server, DMZ, Port Forwarding
Support Dynamic, Static IP, PPPoE,

QoS bandwidth management
Firewall, IP, Port, MAC filtering
Firmware upgrade and configuration backup via Web UI

Certificate

FCC, CE

Product Size (L x W x H (mm))

254.1mm X 127.1mm X 64.0mm

9

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.

802.11a

An IEEE specification for wireless networking that operates in the 5 GHz frequency range (5.425 GHz to 5.750 GHz) with a maximum of 54 Mbps data transfer rate. The 5 GHz frequency band is not as crowded as the 2.4 GHz band. In addition, the 802.11a have 12 non-overlapping channels, comparing to 802.11b/g's 3 non-overlapping channels. This means the possibility to build larger non-interfering networks. However, the 802.11a deliver shorter distance at the same output power when comparing to 802.11g.

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 advice 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.

802.11h

This IEEE standard define the TPC (transmission power control) and DFS(dynamic frequency selection) required to operate WiFi devices in 5GHz for EU.

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.

802.11n

The IEEE 802.11 standard improves network throughput over 802.11a and 802.11g, with a significant increase in the maximum data rate from 54 Mbps to 600 Mbps. 802.11n standardized support for multiple-input multiple-output (MIMO) and frame aggregation, and security improvements.

802.1Q Tag VLAN

In 802.1Q VLAN, the VLAN information is written into the Ethernet packet itself. Each packet carries a VLAN ID(called Tag) as it traveled across the network. Therefore, the VLAN configuration can be configured across multiple switches. In 802.1Q spec, possible 4096 VLAN ID can be created. Although for some devices, they can only view in frames of 256 ID at a time.

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 AirMax5X provide ACK adjustment capability in form of either distance or direct input. When you enter the distance parameter, the AirMax5X will automatically calculate the correct ACK timeout value.

Bandwidth Management

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. The AirMax5X's features both "Per-user Bandwidth Control" and "Total Bandwidth Control". "Per-user Bandwidth Control" allow administrator to define the maximum bandwidth of each user by IP, IP Group, or MAC address. Total Bandwidth define the maximum bandwidth of wireless or Ethernet interface.

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 domain 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.

Full Duplex

The ability of a networking device to receive and transmit data simultaneously. In wireless environment, this is usually done with 2 or more radios doing load balancing.

Gateway

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

Hotspot

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

IGMP Snooping

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

Infrastructure Mode

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

IP address

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

IPsec

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

LACP (802.3ad) Trunking

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

MAC

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

Mbps

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

MESH

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

MIMO

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

NAT

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

Node

A network connection end point, typically a computer.

Packet

A unit of data sent over a network.

Passphrase

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

POE

Power over Ethernet. A standard to deliver both power and data through one single Ethernet cable (UTP/STP). It allows network device to be installed far away from power 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.

RSSI

Receiver Sensitivity Index. RSSI is a value to show the Receiver Sensitivity of the remote wireless device. In general, remote APs with stronger signal will display higher RSSI values. For RSSI 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.

Super A

Super A is an Atheros proprietary turbo mode to increase speed over standard 802.11a mode. It adds Bursting and Compression to increase the speed. If you live in countries that prohibit the channel binding technology (i.e. Europe), you should choose "Super-A without Turbo) if you need more speed than 11a mode

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.

Turbo A

Turbo A is an Atheros proprietary turbo mode to increase speed over standard 802.11a mode. It uses channel binding technology to increase speed. There are 2 types of Turbo A modes: Dynamic Turbo and Static Turbo. In Dynamic Turbo, the channel binding will be used only if necessary. In Static Turbo, the channel binding is always on. This protocol may be combined with Super-A model to increase the performance even more. The used of channel binding might be prohibited in EU countries.

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.

Walled Garden

On the Internet, a walled garden refers to a browsing environment that controls the information and Web sites the user is able to access. This is a popular method used by ISPs in order to keep the user navigating only specific areas of the Web

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 original 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.