



AIRMAX5

802.11a 108Mbps Outdoor CPE

User's Manual

Version 2.0





Version 2.0

This guide is written for firmware version 1.00e13b 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

All Trademarks are properties of their respective holders.

Safety Instruction

During Installation and Application

- Appropriate space for heat dissipation is required to prevent the product from overheating
- If any abnormal phenomenon appear on this product (such as smoke, weird sound and/or smell), unplug the power adapter.
- Keep the product away from heat sources. Avoid the product working in high-temperature or direct sunshine environment.
- Please use under the situation with temperature range from 5°C to 40°C and humid from 35% to 85%

FCC Statement

Federal Communication Commission Interference Statement This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules.

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

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

FCC Caution

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

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

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



IMPORTANT NOTE

FCC Radiation Exposure Statement:

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



© 2009 OvisLink Corporation, All Rights Reserved

Table of Contents

1. Introduction	1
1.1 Overview	1
1.2 How to Use This Guide	1
1.3 Firmware Upgrade and Tech Support	3
1.4 Features	4
1.5 Wireless Operation Modes.....	5
1.5.1 Access Point Mode	5
1.5.2 Repeater Mode	5
1.5.3 WDS Bridge Mode	6
1.5.4 Bridge Infrastructure Mode	6
1.5.5 Client Infrastructure Mode	7
1.5.6 Client Ad Hoc Mode	8
1.5.7 WISP Router Mode.....	8
1.5.8 AP Router Mode	9
2. Installing the AirMax5	10
2.1 Before You Start	10
2.2 Package Content	11
2.3 Optional Accessories	11
2.4 Knowing your AirMax5	12
2.5 Hardware Installation	13
2.6 LED Table	15
2.7 Restore Settings to Default	15
3. Configuring the AirMax5	16
3.1 Important Information.....	16
3.2 Prepare your PC	16
3.3 Management Interface	17
Web Management (HTTP):.....	17
Secured Web Management (HTTPS):.....	18
Command Line Interface (Telnet):	18
Secure Shell (SSH, SSH2)	19
SNMP Management	21
3.4 Introduction to Web Management.....	21
3.4.1 Getting into Web Management	22
3.4.2 Welcome Screen and Login.....	24

3.5 Initial Configurations	26
3.5.1 Choose the wireless Operation Modes	26
3.5.2 Change the Device's IP Address	27
3.5.3 Set the Time and Date	28
3.5.4 Change System Management	28
3.5.5 Change Password	29
4. Web Management: Wireless and WAN Settings	30
4.1 About AirMax5's Menu Structure	30
4.2 Operation Modes (Wireless and WAN Settings)	31
4.2.1 Regulatory Domain	32
4.2.2 Network SSID	33
4.2.3 Site Survey	33
4.2.4 Signal Survey	34
4.2.5 Lock-to-AP	34
4.2.6 Radio Mode (11a, SuperA, TurboA)	35
4.2.7 SuperA Option	35
4.2.8 Channel	36
4.2.9 Channel Width	37
4.2.10 Security Settings	37
4.2.11 Distance	42
4.2.12 Antenna Settings	42
4.2.13 Transmit Power	42
4.2.14 Advance Settings (Wireless)	43
4.2.15 Access Control (ACL)	45
4.2.16 Multiple SSID	46
4.2.17 WMM QoS	50
4.2.18 RADIUS Settings	53
4.2.19 Bandwidth Control	54
4.2.20 RSSI LED Threshold	59
4.3 WDS Settings	60
4.4 Router Mode Settings	62
4.4.1 WISP Router Mode	62
4.4.2 AP Router Mode	62
4.4.3 WAN Port Settings	63
4.4.4 Dynamic DNS Settings	64
4.4.5 Remote Management Settings	64
4.4.6 IP Routing Settings	65
4.4.7 DHCP Server	66
4.4.8 Multiple DMZ	67
4.4.9 Virtual Server Settings	67
4.4.10 Special Applications	68
4.4.11 IP Filtering Settings	69
5. Web Management 2: System Configuration and Status	70
5.1 System Configuration	70

5.1.1 Device IP Settings	70
5.1.2 Time Settings.....	72
5.1.3 Password Settings.....	72
5.1.4 System Management.....	73
5.1.5 SNMP Settings	74
5.1.6 Ping Watchdog	75
5.1.7 Firmware Upgrade.....	76
5.1.8 Configuration Save and Restore.....	77
5.1.9 Factory Default	77
5.2 Device Status	78
5.2.1 Device Information.....	78
5.2.2 Wireless Information	78
5.2.3 Internet Information	79
5.2.4 Wireless Client Table	79
5.2.5 System Log.....	80
6. Command Line Interface	81
6.1 System Commands.....	81
6.2 Debugging Commands	83
6.3 Show Commands.....	84
6.4 Set Commands	90
6.5 Enable/Disable Commands	97
6.6 Add/Delete Commands.....	99
7. Antenna Alignment	103
7.1 About AirMax5's Antenna	103
7.1.1 Polarization.....	104
7.1.2 Mounting Adjustment	105
7.2 About RSSI Signal Level.....	106
7.3 Preparation before Installation	106
7.4 Antenna Alignment using RSSI LED	107
7.5 Antenna Alignment using Signal Survey	112
8. Application Example: Infrastructure	115
8.1 Application Environment	115
8.2 Device A: Access Point Mode	116
8.2.1 Device A Wireless Settings	117
8.2.2 Device A Bandwidth Management	119
8.3 Device B: Bridge Infrastructure Mode	121

8.3.1 Device B Wireless Settings.....	121
8.3.2 Device B Total Bandwidth Control.....	123
8.4 Device C: Client Infrastructure Mode	124
8.4.1 Device C IP Address.....	124
8.4.2 Device C Wireless Settings	125
9. Application Example 2: Bridge Network	127
9.1 Preparation for Building Outdoor Bridge Networks	127
9.2 WDS Bridge vs. Bridge Infrastructure	129
9.3 WDS Bridge Network Example	131
10. Application Example 3: Router and Repeater	137
10.1 Application Environment	137
10.2 AirMax5 in WISP Router Mode	138
10.2.1 WISP Router: Wireless Settings	138
10.2.2 WISP Router: WAN Port and Virtual Server	140
10.3 AirMax5 in Repeater Mode	143
10.3.1 Repeater Router: Wireless Settings	143
11. Emergency Firmware Recovery	146
11.1 How Emergency Upgrade Works.....	146
11.2 Emergency Upgrade Procedure.....	146
12. Frequent Asked Questions	149
13. Specifications.....	153
13.1 Hardware Features	153
13.1.1 General Hardware Feature	153
13.1.2 Antenna	153
13.1.3 Power Supply	153
13.1.4 Dimension and Weight.....	154
13.2 Radio Specifications	154
13.2.1 Frequency Band	154
13.2.2 Rate and Modulation.....	154
13.2.3 TX Output Power	154
13.2.4 Receiver Sensitivity	154
13.2.5 Supported WLAN Mode.....	155
13.3 Software Feature	155
13.3.1 Operation Mode.....	155
13.3.2 Management Interface.....	155
13.3.3 Channel Width (Rate Mode)	156



13.3.4 Advance Functions	156
14. Wireless Network Glossary.....	157

1

Introduction

1.1 Overview

The AIRMAX5 is a wireless outdoor multi-function device based on IEEE 802.11a 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 3km* of distance depending on conditions. The firmware of the AP provides up to 8 operations modes* to satisfy different application environments.

1.2 How to Use This Guide

AirMax5 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, HTTPS, Telnet, and SSH configurations.
 - **3.4 Introduction to Web Management:** This section tells you how to get into the Web UI using HTTP and HTTPS. 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 – Wireless and WAN Settings:** This chapter explain the wireless functions and router mode settings in the AirMax5. If time permitted, you should read through the entire chapter.

- **4.2 Operation Mode (wireless):** Operation mode is the page where all the wireless settings and router mode settings are. Therefore, it is advised that you must read through the entire section.
 - **4.2.3 Site Survey:** Site Survey is the connection wizard that will search for available networks and let you connect with the select network by simply clicking. It also includes RSSI signal survey for antenna alignment.
 - **4.2.8 and 4.2.9 Channel and Channel Width:** This part explains the concept of variable Channel Width and how to use them. Channel Width can be 40MHz, 20MHz, 10MHz, or 5MHz.
 - **4.2.13 Bandwidth Management:** Be sure to read about AirMax5's powerful Bandwidth Control that allow you to limit up/downlink speed by interface, IP, MAC address, or IP segment. This section provides step-by-step examples also.
- **4.3 WDS Settings:** Here explains the WDS setting page. After reading this section, please go to **Chapter 9: Bridge Network example** to see step-by-step instructions on setting up a multi-point WDS Bridge network.
- **4.4 Router Modes:** This section includes WAN port, virtual server, remote management, virtual servers and all router related settings.
- **Chapter 5: Web Management 2: Configurations and Status**

This chapter explains all the non-wireless settings and status such as IP settings, Ping Watchdog.

 - **5.1.6 PING Watchdog:** PING watchdog is a crucial function to keep your wireless connection alive. When AirMax5 can't get a response from remote devices, it will attempt to re-establish the connection. AirMax5's PING watchdog goes the extra step to allow 2 sets of IP to avoid false alarm.
 - **5.1.8 Configurartion Save and Restore:** You should always backup your configurations so you can restore in the event of system crash.
- **Chapter 6: Command Line Interface**

This chapter explains all the commands in the Telnet and SSH interface. Be sure to "save config" after making all changes. In case you forget a command, just type "help" to display all available commands and their usage.
- **Chapter 7: Antenna Alignment**

This chapter provides detail information about AirMax5's antenna. It also provides step-by-step instructions on how to make antenna alignment using LED indicator or Signal Survey function.
- **Chapter 8: 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: Application Example 2: WDS Bridge**

This chapter tells you the basic knowledge about building a long distance connection. Then it will describe the differences between WDS bridge and Bridge Infrastructure mode, and how to make a choice between them. At last, a step-by-step instruction on how to build a multipoint WDS network is provided.

❑ **Chapter 10: Application Example 3: Repeater and WISP Router**

A step-by-step application example on Repeater and WISP router

❑ **Chapter 11: Emergency Firmware Recovery**

It your AirMax5 can no longer be access due to firmware crash. You might be able to recover it following the procedure on this chapter.

❑ **Chapter 12: Frequent Asked Questions**

If you have a question about AirMax5 that is not found on other part of this guide, you might find your answer here. Including how to make connection with Mikrotik AP, how to save password settings on the browser...etc.

❑ **Chapter 14: Wireless Network Glossary**

Explanations on wireless network technical terms from A to Z. Highly recommended for referencing when you encounter an unfamiliar term.

1.3 Firmware Upgrade and Tech Support

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

In addition, you might find new firmwares that either increase software functions or provide bug fixes for AirMax5. You can reach our on-line support center at the following link: http://www.airlive.com/support/support_2.jsp

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

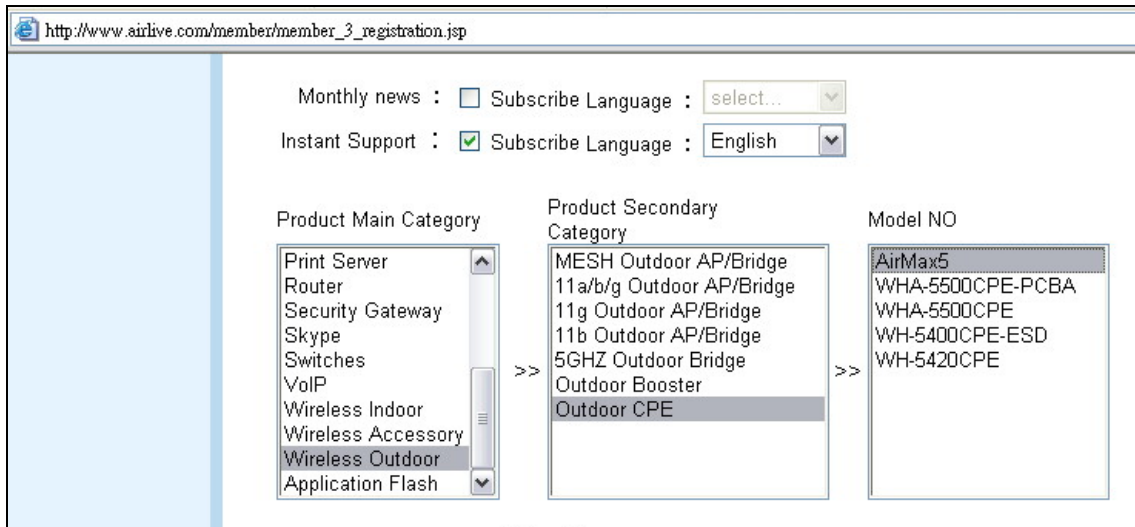


Figure 1.4: AirLive Newsletter Support System

1.4 Features

- Atheros AR-2313 + AR-5112 108mbps 802.11a chipset
- 8MB Flash and 32MB SDRAM
- 8 wireless multi-function modes: Access Point, Repeater, WDS Bridge, Bridge Infrastructure, Client Infrastructure, Client Ad Hoc, WISP Router, AP Router.
- 14dBi Integrated Antenna: Vertical Polarization, Horizontal Polarization. 30 degree Horizontal and Vertical coverage in the forward direction.
- Built from High Temperature resistant ABS material with Anti-UV protection
- Power by passive PoE: 12V Adapter and injector included. Accept up to 22Vdc input on the PoE port.
- Slide out housing design for easy maintenance.
- Pole Mount strap included. Optional metal mount and wall mount available
- Total Bandwidth and Per-User Bandwidth Control
- Limit Bandwidth of HTTP, FTP, Torrent, and eDonkey traffic in router mode
- Site Survey, RSSI signal Survey, and RSSI LED indicator.
- Multi-SSID, TAG VLAN, WMM, TOS
- ACK Timeout Adjustment for long distance connection.
- Emergency firmware recovery mode
- Web, HTTPS, SSH/SSH2, Telnet, and SNMP managements

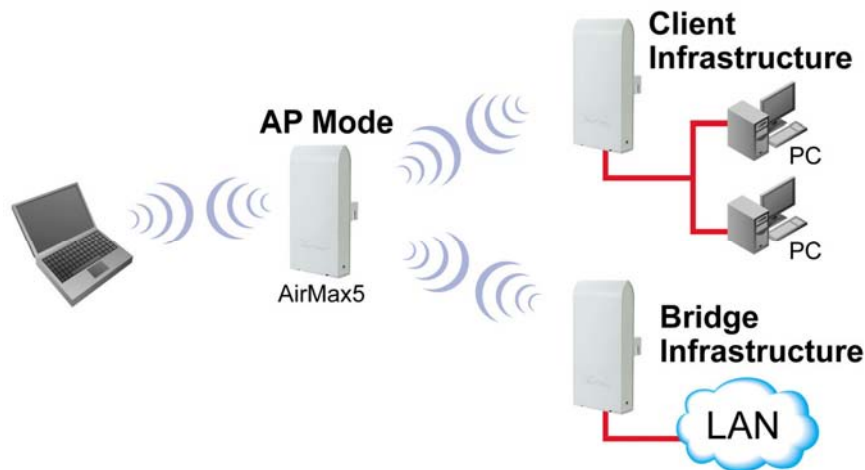
1.5 Wireless Operation Modes

The AirMax5 can perform as a multi-function wireless device. Through the AirLogic web interface, users can easily select which wireless mode they wish the AirMax5 to perform.

The AirMax5 can be configured to operate in the following wireless operation modes:

1.5.1 Access Point Mode

When operating in the Access Point mode, the AIRMAX5 becomes the center hub of the wireless network. All wireless cards and clients connect and communicate through AirMax5. This type of network is known as “Infrastructure network”. Other AirMax5 or 802.11a CPE can connect to AP mode through “Client Infrastructure Mode” or “Bridge Infrastructure Mode”. The Access Point mode will act as “WDS AP” when connecting with the “Bridge Infrastructure mode”. *Please see Chapter 8 for step-by-step application example of this operation mode.*



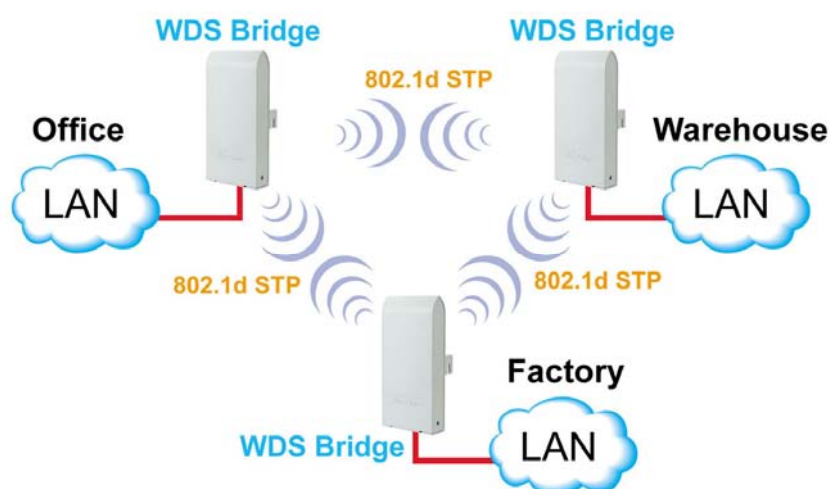
1.5.2 Repeater Mode

In Repeater mode, the AIRMAX5 functions as a repeater that extends the range of remote wireless LAN. The AirMax5’s repeater mode is a universal repeater, not WDS repeater. Because the radio is divided into client + AP mode, the Repeater mode will have less performance and distance. We recommended using a dual radio product like AirLive WLA-9000AP or WH-9200AP if you require full performance in this application. *Please see Chapter 10 for step-by-step application example of this operation mode.*



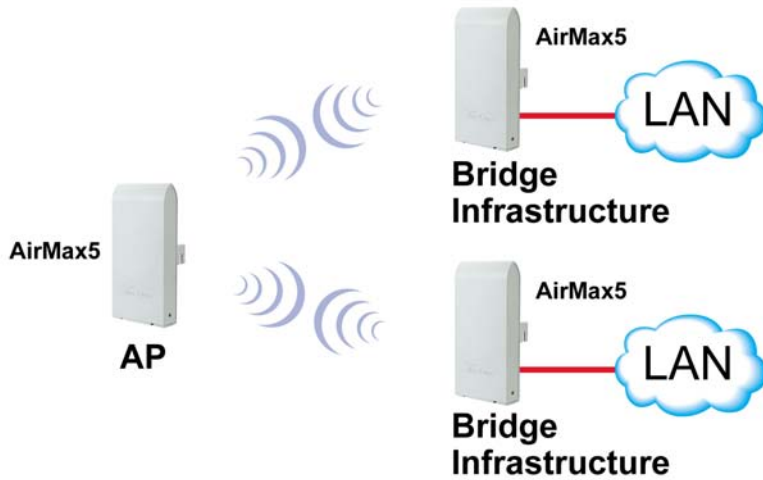
1.5.3 WDS Bridge Mode

This mode is also known as “WDS Pure MAC mode”. When configured to operate in the Wireless Distribution System (WDS) Mode, the AIRMAX5 provides bridging functions with remote LAN networks in the WDS system. The system will support up to total of 8 bridges in a WDS network (by daisy chain). However, each bridge can only associate with maximum of 4 other bridges in the WDS configuration. This mode is best used when you want to connect LAN networks together wirelessly (for example, between office and warehouse). If you have more than 2 AP in WDS Bridges mode, please remember to turn on the “802.1d Spanning Tree” or “STP” option on to avoid network loop. This mode usually delivers faster performance than infrastructure mode. *Please see Chapter 9 for step-by-step application example of this operation mode.*



1.5.4 Bridge Infrastructure Mode

This mode is also known as "WDS Station" or "Client mode with MAC address transparency". The Bridge Infrastructure mode can only connect with “Access Point” mode. 2 Bridge Infrastructure can not connect with each other. It works like client mode with MAC address transparency function. In another word, the MAC addresses of the PCs will be passed instead of the AP's wireless MAC address. If you require Bridge connection with WPA-PSK or WPA-PSK2 connection, please use this mode instead. **However, this mode might not work with some outdoor APs. If it occurs, please use Client Infrastructure or WDS Bridge instead.** *Please see Chapter 8 for step-by-step application example of this operation mode.*

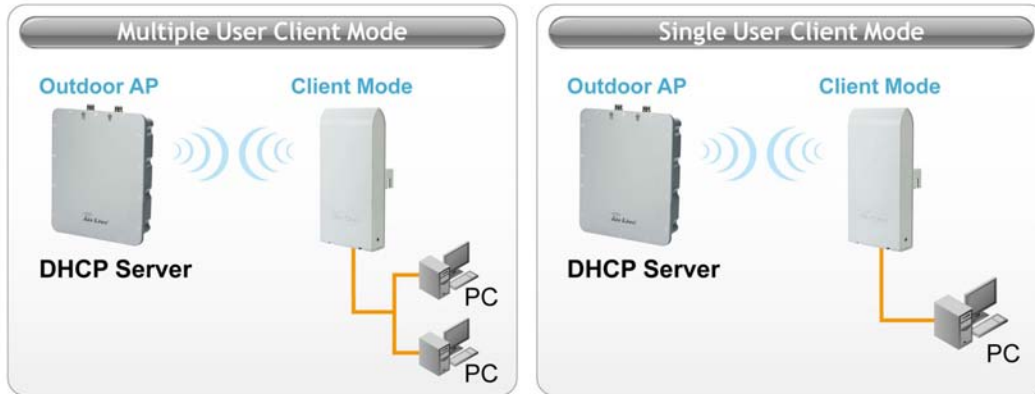


1.5.5 Client Infrastructure Mode

This mode is also known as “Client” mode. In Client Infrastructure mode, the AIRMAX5 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 AirMax5 to get network access. This mode is often used by WISP on the subscriber’s side. *Please see Chapter 8 for step-by-step application example of this operation mode.*

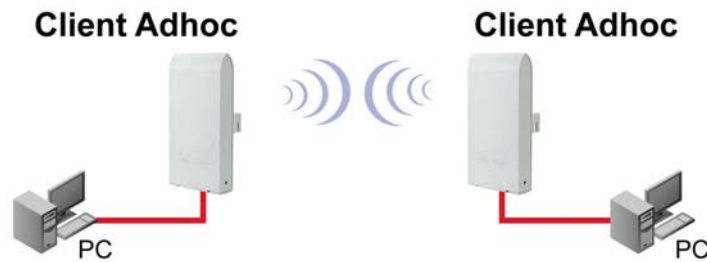


For AirMax5, there are 2 types of Client Infrastructure Mode: “Single User” and “Multiple-User”. When “Single User” is chosen, only one PC that is connected behind the AirMax can get IP address from remote DHCP server. When “multiple user” is chosen, more than one PC can get IP address from remote DHCP server. However, in Client Infrastructure mode, the AirMax5 always sends the AirMax5’s wireless MAC address to the remote AP. If you want the AirMax5 to send the PC’s MAC addresses to remote AP, then you should use the “Bridge Infrastructure” mode. Bridge Infrastructure provides the “Mac Address Transparency” functionality.



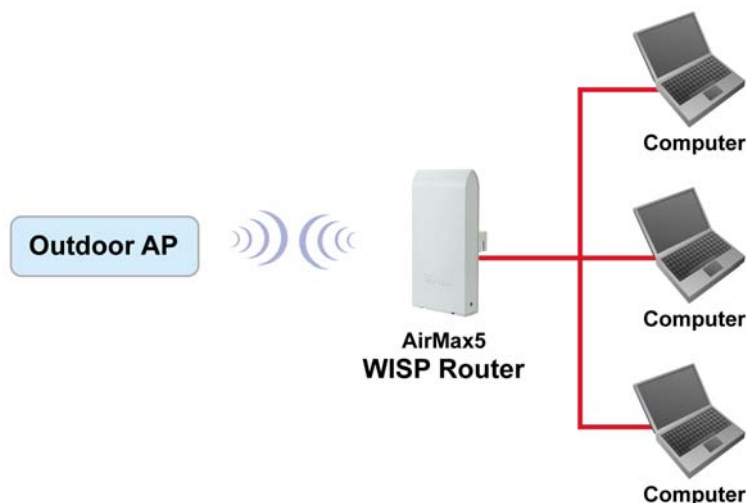
1.5.6 Client Ad Hoc Mode

In Client Ad Hoc mode, AIRMAX5 can connect to other wireless adapters without access point. Users can attach a computer or a router to the LAN port of AirMax5 to get network access.



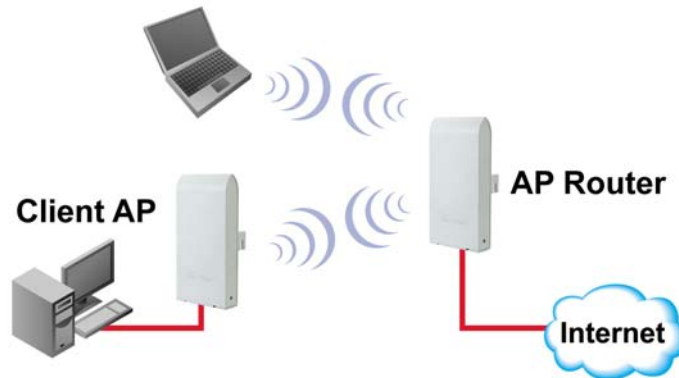
1.5.7 WISP Router Mode

In WISP Router Mode, AIRMAX5 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. *Please see Chapter 10 for step-by-step application example of this operation mode.*



1.5.8 AP Router Mode

In AP Router Mode, the AirMax5 behaves like a wireless router. The LAN port of the AirMax5 will become WAN port. The wireless network of AirMax5 becomes the LAN side. Please note when this mode is used, the only way to manage the AirMax5 is through the wireless side unless remote management is opened.



2

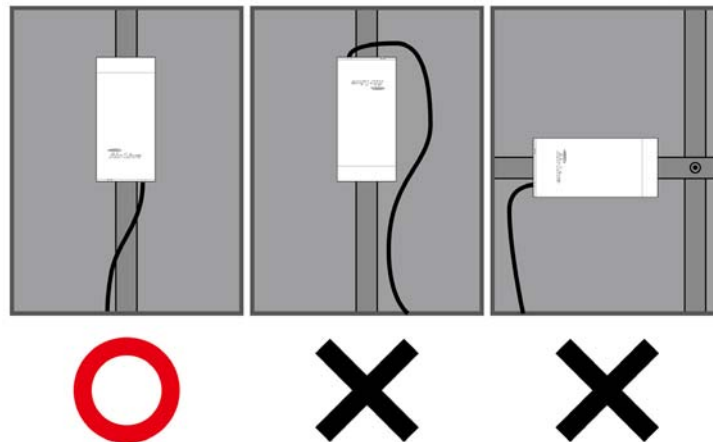
Installing the AirMax5

This section describes the hardware features and the hardware installation procedure for the AIRMAX5. 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 AirMax5

- The AirMax5 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 AirMax5 must be installed in the upright position if the unit is located in outdoor or wet environments.



- The use of 5GHz spectrum, Turbo modes, and 5/10MHz channel bandwidth might be prohibited in some countries. Please consult with your country's telecom regulation first.
- You must set the distance parameter to make long distance connection work. Please refer to chapter 4 of this user's guide for details.
- The integrated antenna has forward coverage angle of 30 degree both in vertical and horizontal direction.
- The AirMax5 is a 5GHz CPE device only, it can not operate in 2.4GHz.

2.2 Package Content

The AIRMAX5 package contains the following items:

- One AIRMAX5 main unit
- One 12V 1A DC power adapter
- Passive PoE DC Injector
- 2 x Plastic Straps
- User's Guide CD
- Quick Start Guide



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

2.3 Optional Accessories

The AirMax5 have the following optional accessories which you can purchase from AirLive

- Tilting Metal Wall/Pole Mount (*Model: WMK-AIRMAX*): This kit allows your AirMax5 to tilt in pole mount, it also allow you to install the AirMax5 to the wall.
- 25 meter PoE cable (*Model: OD-25M*): high quality outdoor graded anti-UI PoE Ethernet Cable.

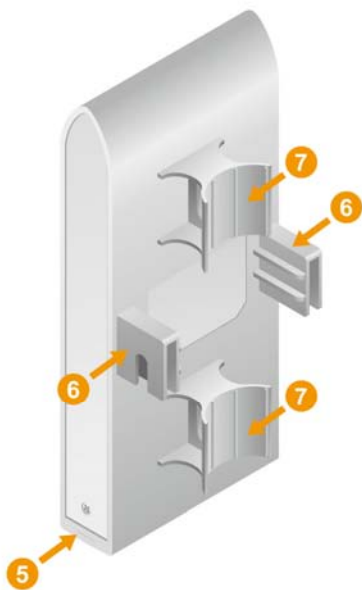


2.4 Knowing your AirMax5

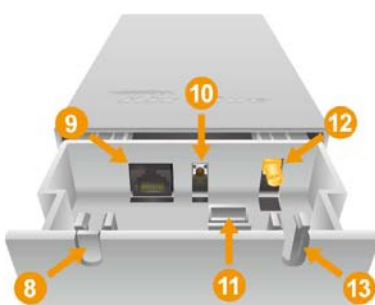
Below are descriptions and diagrams of the product:



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




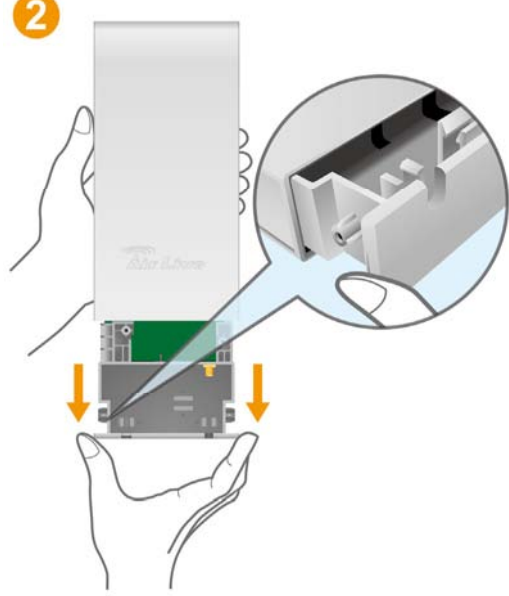
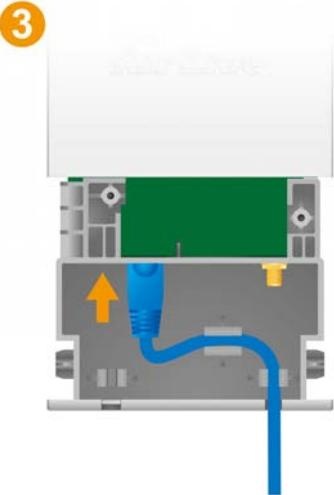
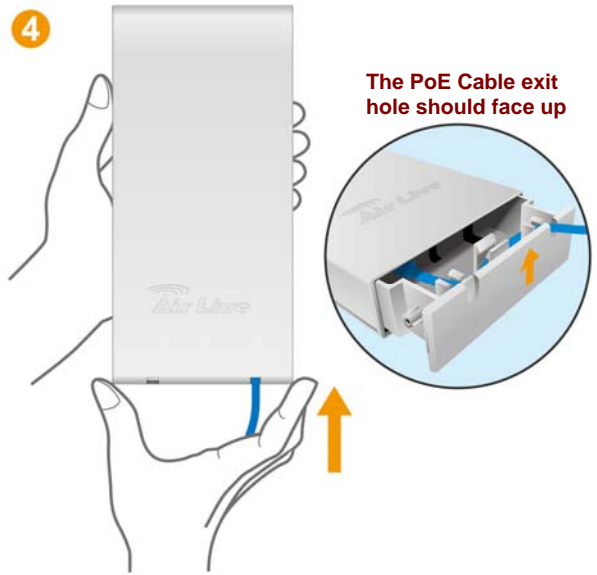
- 5 Bottom Case Pull-Out Holders
- 6 Mounting for optional Metal mount kit
- 7 Pole Mount Holders



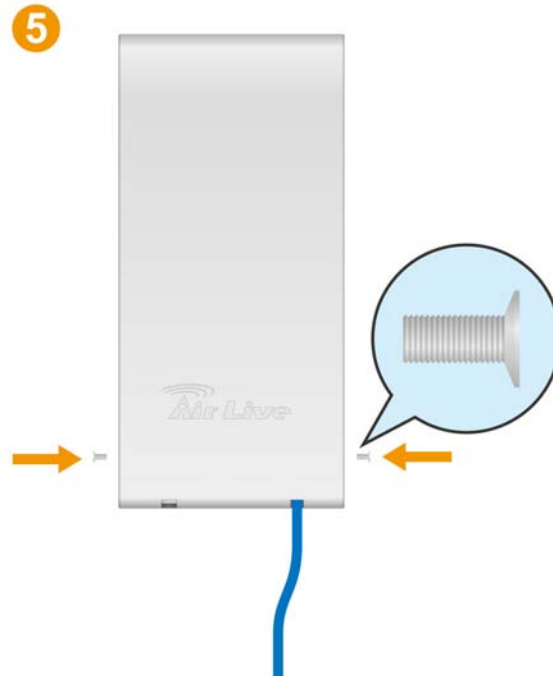
- 8 Antenna Cable Exit Hole
- 9 PoE Ethernet Port
- 10 Reset Button
- 11 Cable Guard
- 12 R-SMA External Antenna Connector
- 13 PoE Cable exit port

2.5 Hardware Installation

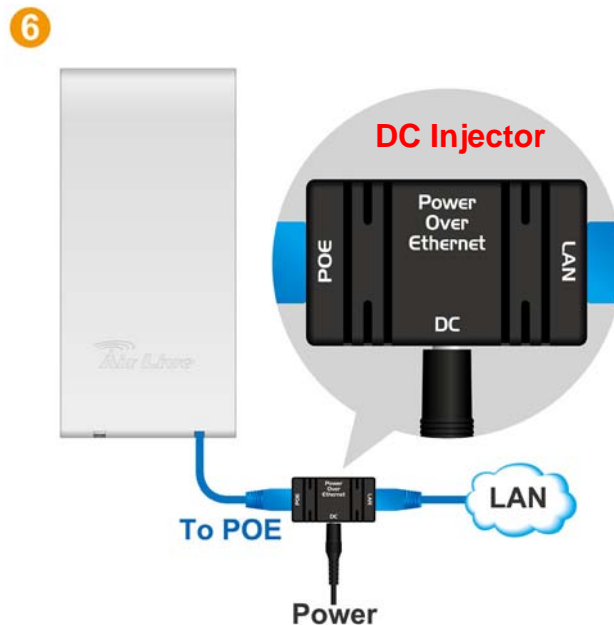
Please prepare a screw driver and an outdoor graded PoE Ethernet cable with adequate length according to your need.

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

5. Put the case screws back.



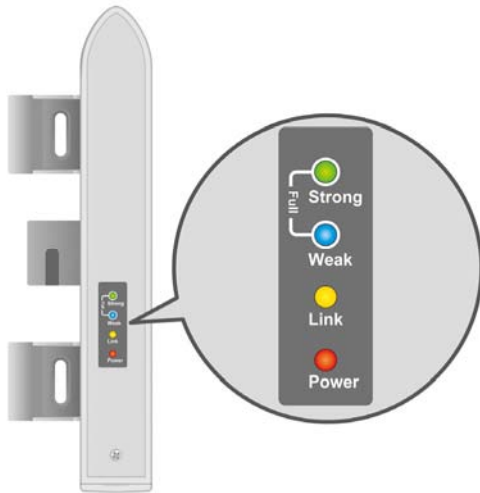
6. Install the PoE Cable and the Power Adapter to the DC Injector. Please make sure to read the markings on the DC Injector carefully and connect the cables correctly. You can connect your PC directly to the "LAN" port of the DC Injector.



2.6 LED Table

This section describes the LED behavior of AirMax5. For more information on how to use the LED for antenna alignment, please refer to Chapter 5: How to make Antenna Alignment for details.

You can find the LED on the left side of the AirMax5.



Power

- Steady Red – Normal Operation
- OFF – No Power

Link

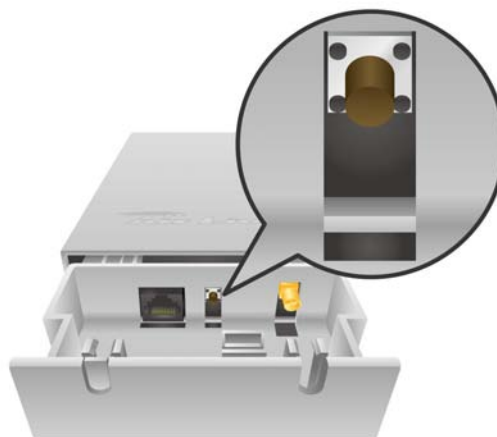
- Steady Yellow: Link is active
- Flashing Yellow: Transmit or receive data
- OFF: No connection

WLAN Signal Strength LEDs

- Weak :Low signal strength
- Strong :Better signal strength
- Weak + Strong: Full Signal strength
- ● No connection/Bad signal strength

2.7 Restore Settings to Default

If you have forgotten your AirMax5's IP address or password, you can restore your AirMax5 to the default settings by pressing on the "reset button" for more than 5 seconds. The reset button is inside the bottom case. Please see diagram below for details.



3

Configuring the AirMax5

The AirMax5 offers many different types of management interface. You can configure through standard web browser (http), secured web (https), command line (telnet), secured command shell (SSH, SSH2), and SNMP management. In this chapter, we will explain AirMax5'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. For Command-Line interface, please go to Chapter 6.

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: airlive
- The default password is: airlive
- When using SSH/SSH2, there are 2-levels login
 - First Level:
 - Login : root
 - Password: Nothing, just press enter key
 - Second Level:
 - Password: airlive. When you change your password, this will change also.
- The default SSID is: airlive
- The default wireless mode is : Client mode
- After power on, please wait for 2 minutes for AirMax5 to finish boot up
- Please remember to click on "Apply" for new settings to take effect
- Please remember to enter the correct "Distance" parameter in wireless settings. Failure to do so can result in poor performance.

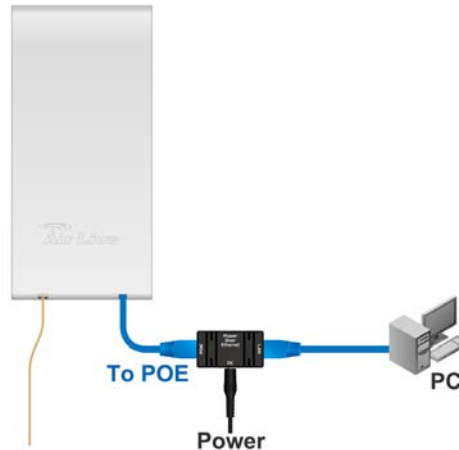
3.2 Prepare your PC

The AIRMAX5 can be managed remotely by a PC through either the wired or wireless network. The default IP address of the AIRMAX5 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

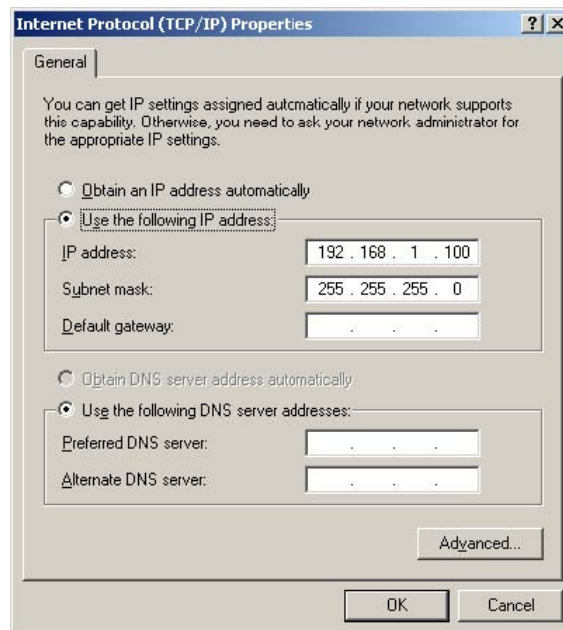
192.168.1.2 to 192.168.1.254.

To prepare your PC for management with the AirMax5, please do the following:

1. Connect your PC directly to the LAN port on the DC Injector of AirMax5



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 AirMax5 using your PC.

3.3 Management Interface

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

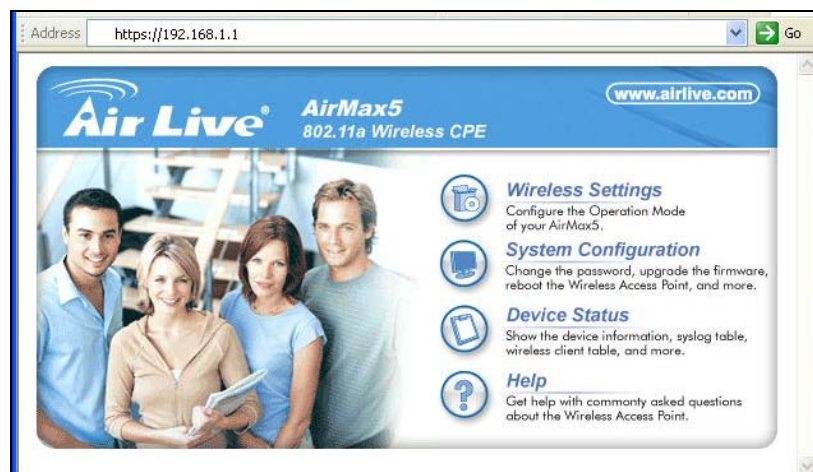
- **Web Management (HTTP):** You can manage your AirMax5 by simply typing its IP address in the web browser. Most functions of AirMax5 can be accessed by web

management interface. We recommend using this interface for initial configurations. To begin, simply enter AirMax5's IP address (default is 192.168.1.1) on the web browser. The default username and password are both "airlive".



- **Secured Web Management (HTTPS):** HTTPS is also using web browser for configuration. But all the data transactions are securely encrypted using SSL encryption. Therefore, it is a safe and easy way to manage your AirMax5. We highly recommend WISP and service provider to use HTTPS for management.

To begin, simply enter <https://192.168.1.1> on your web browser. A security alert screen from your browser will pop up. Please grant all permission and get certificate to AirMax5. After you pass the security warning screen, you will enter the secured web management interface. The default username and password are both "airlive".

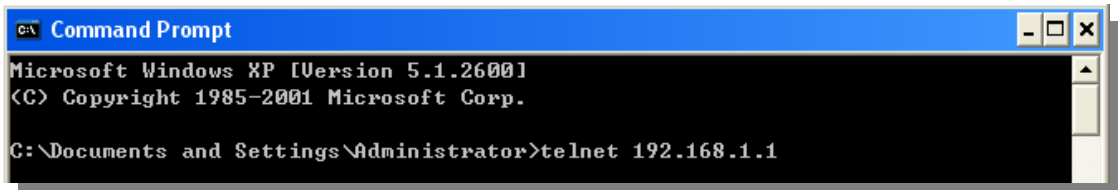


For more information about Web Management and HTTPS, please make sure to read through "Introduction to Web Management" in this chapter, Chapter 4, and Chapter 5

- **Command Line Interface (Telnet):** AirMax5 can be managed through the

command line interface (CLI). It is possible to write a text script file, and then paste it into the CLI to execute several commands at once. However, Telnet does not encrypt its message. Therefore, it is not secure. The default Telnet management port is TCP port 23.

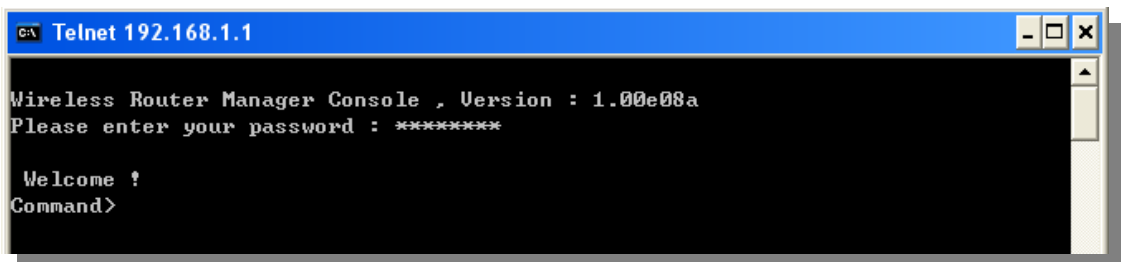
To use the CLI, please open the command line window. Then type “telnet 192.168.1.1” to start.



```
C:\ Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>telnet 192.168.1.1
```

When asked for password, please enter “airlive”.



```
C:\ Telnet 192.168.1.1

Wireless Router Manager Console , Version : 1.00e08a
Please enter your password : *****

Welcome !
Command>
```

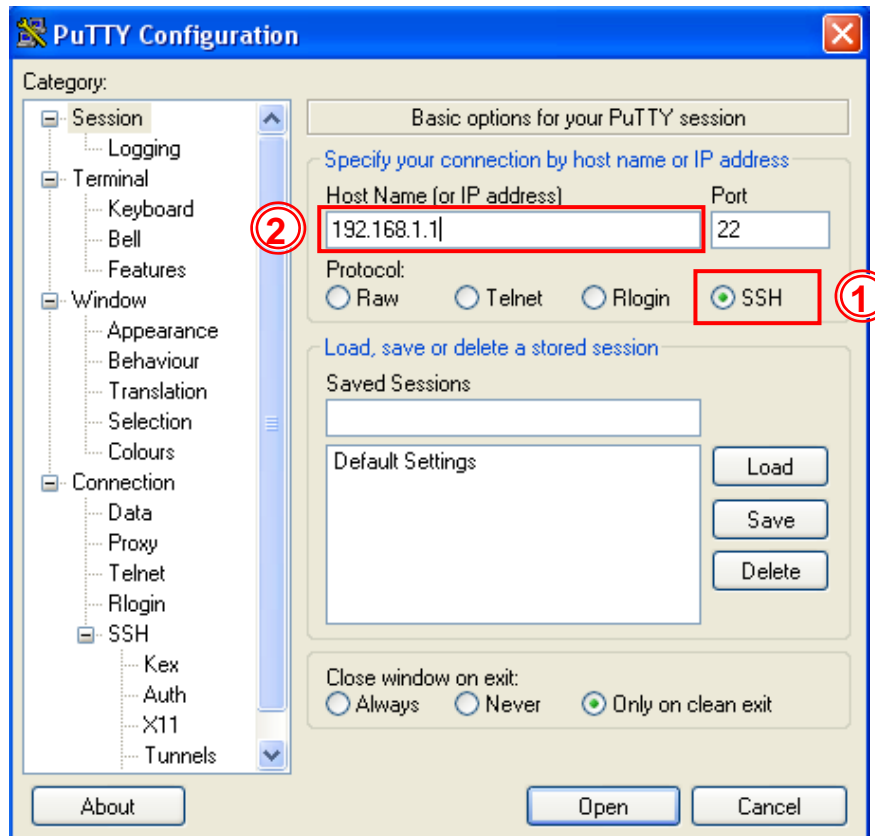
To get a list of available command and their usage, please type “help” on the command prompt.

- **Secure Shell (SSH, SSH2):** SSH is an encrypted Command Line Interface that allow user to send text commands through SSL encryption. Therefore, it provides the added advantage of security comparing to Telnet. As with Telnet, the SSH and SSH2 provide the possibility to write a text script and paste into the CLI interface for multiple command execution. It also makes configuration change across many AirMax5s easier. The default management port for SSH/SSH2 is TCP/UDP port 22.

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

Once you have download and install Putty. Please follow the figure below to make a connection with AirMax5:

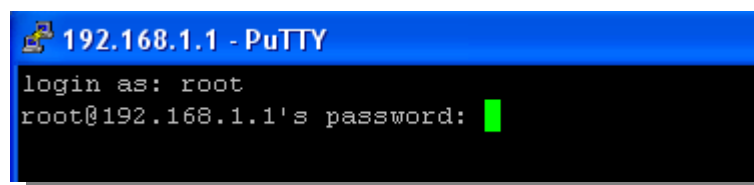
1. Choose “SSH” as indicated in the diagram
2. Enter the IP address of AirMax5
3. Click on “Open” to start the SSH session.



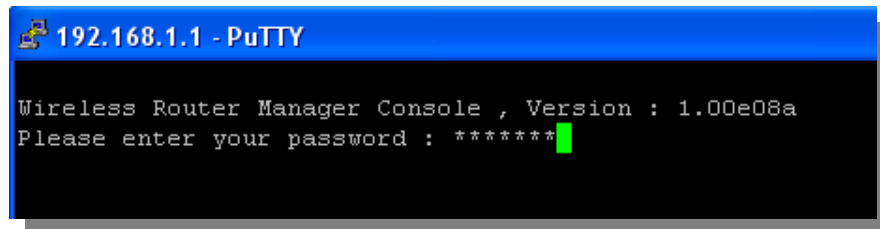
When the following screen appear, click on “Yes” to continue



When the following screen appears, enter “root” for login. Then press Enter when password for root is requested, do not enter any password

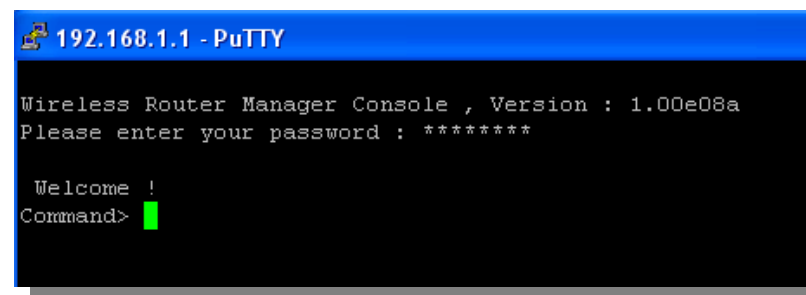


When the “Wireless Router Manager Console” appears, please enter “airlive” for password. This password will change when you change the password.



```
192.168.1.1 - PuTTY
Wireless Router Manager Console , Version : 1.00e08a
Please enter your password : *****
```

Now you are ready to enter commands



```
192.168.1.1 - PuTTY
Wireless Router Manager Console , Version : 1.00e08a
Please enter your password : *****

Welcome !
Command>
```

To get a list of available command and their usage, please type “help” on the command prompt.

 *For more information about Telnet and SSH configuration, please go to Chapter 7 Command Line Interface.*

■ **SNMP Management:** The AirMax5 support SNMPv1/v2 management. If you have a SNMP management software, it can manage the AirMax5. The AirMax5’s SNMP support is as followed:

- SNMP v1/v2 support
- SNMP Read/Write Community String
- SNMP Trap support
- MIB and MIB II Support
- Ether-like MIB
- IEEE802dot11 MIB
- Private MIB
 - A copy of the AirMax5’s Private MIB can be found in the “Private MIB” directory on the installation CD. Please also visit our website to check if a new version is available.

3.4 Introduction to Web Management

The AirMax5 offers both normal (http) and secured (https) Web Management interfaces. Their share the same interface and functions, and they can both be accessed through web

browsers. The only difference is HTTPS are encrypted for extra security. Therefore, we will discuss them together as “Web Management” on this guide.

If you are placing the AirMax5 behind router or firewall, you might need to open virtual server ports to AirMax5 on your firewall/router

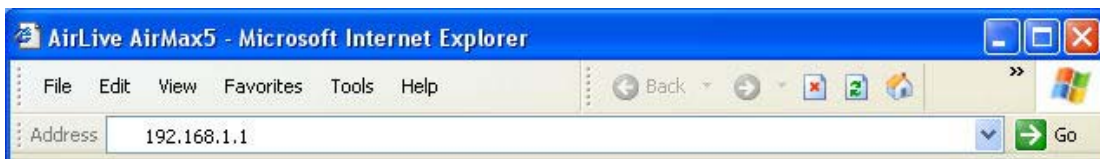
- HTTP: TCP Port 80
- HTTPS: TCP/UDP Port 443

This procedure is not necessary in most cases unless there is a router/firewall between your PC and AirMax5.

3.4.1 Getting into Web Management

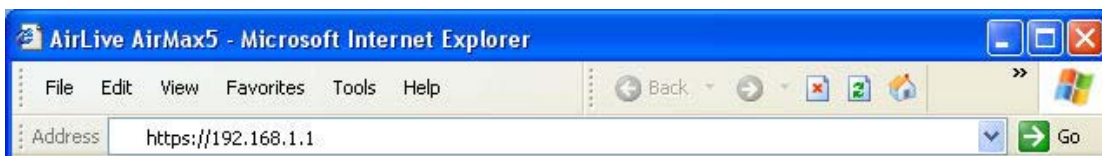
Normal Web Management (HTTP)

To get into the Normal Web Management, simply type in the AirMax5’s IP address (default IP is 192.168.1.1) into the web browser’s address field.



Secured Web Management (HTTPS)

To get into the Secured Web Management, just type “https://192.168.1.1 ” into the web browser’s address field. The “192.168.1.1” is AirMax5’s default IP address. If the IP address is changed, the address entered in the browser should change also.



A security warning screen from your browser will then pop-up depending on the browser you use. Please follow step below to clear the security screen.

- Internet Explorer: Select “Yes” to proceed



❑ Firefox:

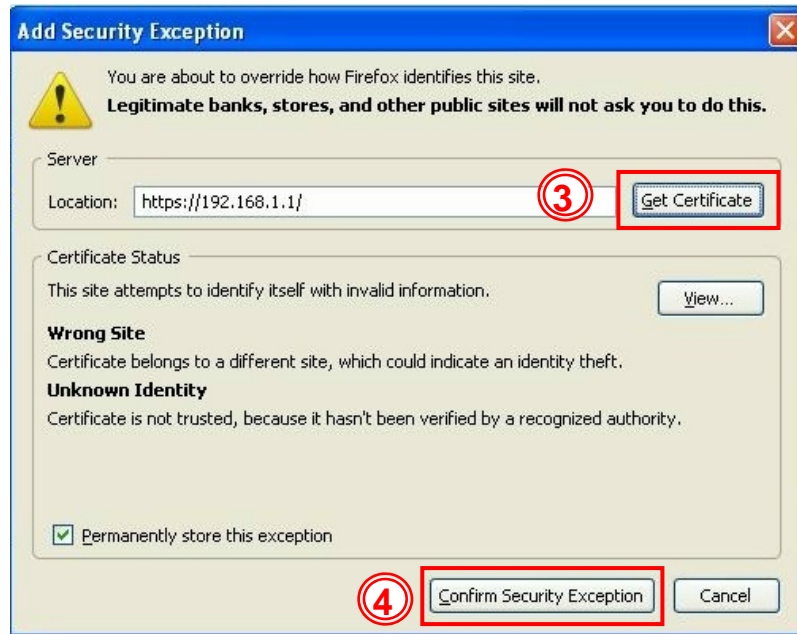
1. Select “or you can add an exception”



2. Click on “Add Exception”



3. Click on “Get Certificate”. Then, please enter AirMax5’s IP address. Finally, please click on “Confirm Security Exception.”



3.4.2 Welcome Screen and Login

After the procedure above, the Welcome Screen will appear. Welcome Screen gives a brief introduction of the AirMax5’s main function category. By click on the function category, it will direct you to the corresponding web management menu.

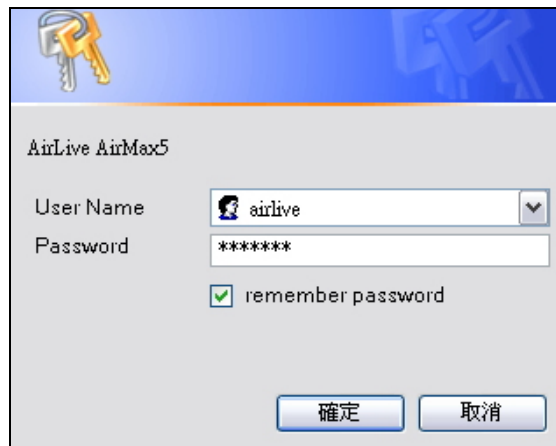


- **Wireless Settings:** Click on this part will bring you to the wireless operation mode menu. The AirMax5’s wireless settings are different between wireless modes. Only functions that are applicable to the wireless mode will show to simplify configuration. For example, multiple SSID option is only workable for Access Point and AP Router mode. Therefore, the function will only appear in these 2 modes. For this reason, the first step to configure the AirMax5 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.

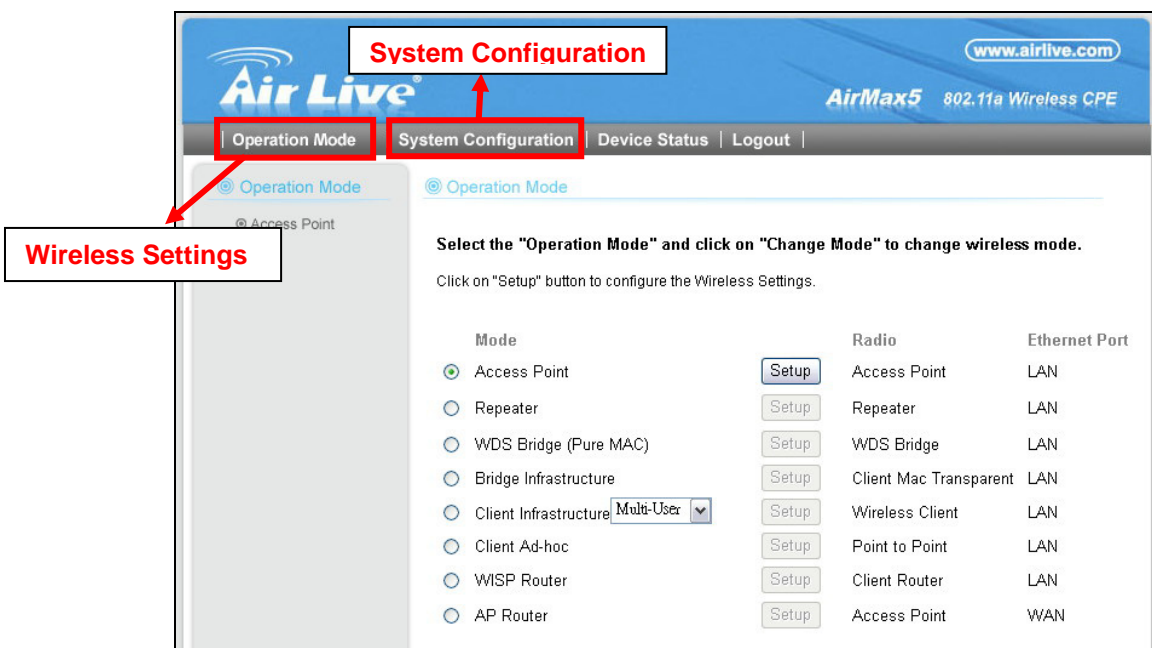
- **System Configuration:** All non-wireless and router mode settings are in this category. The system configurations including changing password, upload firmware, backup configuration, settings PING watchdog, and setting management interface. The default management timeout is 10 minutes; we recommend you should change password and management timeout during the first time login.
- **Device Status:** This section for monitoring the status of AirMax5. It provides information on device status, Ethernet status, wireless status, wireless client table, and system log.
- **Help:** This is the online help system for quick reference. We still recommend you to read this user's guide for more information.

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

When you choose one of the menu categories, the AirMax5 will require you to enter the username and password. Please enter "airlive" (all lower cases) for both username and password.



After you enter the correct password, the following screen will appear corresponding to the menu category you selected.



System Configuration

Wireless Settings

Select the "Operation Mode" and click on "Change Mode" to change wireless mode.
Click on "Setup" button to configure the Wireless Settings.

Mode	Radio	Ethernet Port
<input checked="" type="radio"/> Access Point	<input type="button" value="Setup"/> Access Point	LAN
<input type="radio"/> Repeater	<input type="button" value="Setup"/> Repeater	LAN
<input type="radio"/> WDS Bridge (Pure MAC)	<input type="button" value="Setup"/> WDS Bridge	LAN
<input type="radio"/> Bridge Infrastructure	<input type="button" value="Setup"/> Client Mac Transparent	LAN
<input type="radio"/> Client Infrastructure <input type="button" value="Multi-User"/>	<input type="button" value="Setup"/> Wireless Client	LAN
<input type="radio"/> Client Ad-hoc	<input type="button" value="Setup"/> Point to Point	LAN
<input type="radio"/> WISP Router	<input type="button" value="Setup"/> Client Router	LAN
<input type="radio"/> AP Router	<input type="button" value="Setup"/> Access Point	WAN

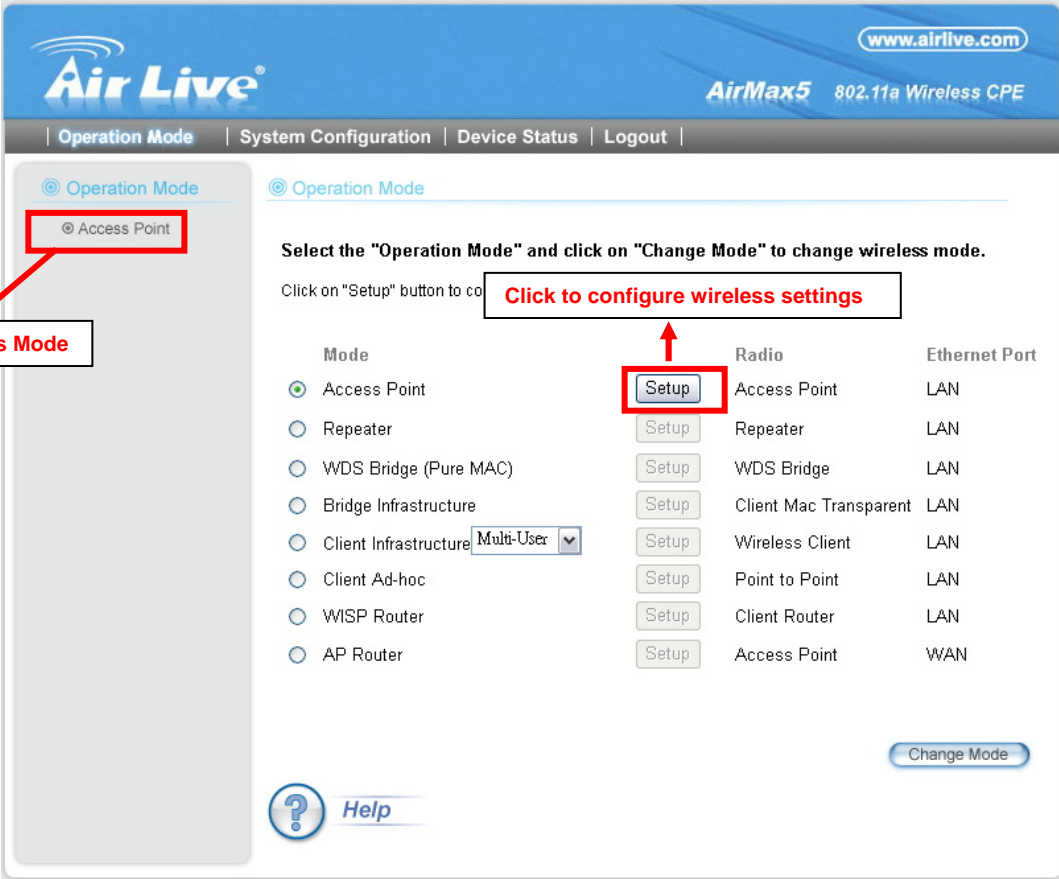
3.5 Initial Configurations

We recommend users to browse through AirMax5'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 AirMax5 are dependant 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.



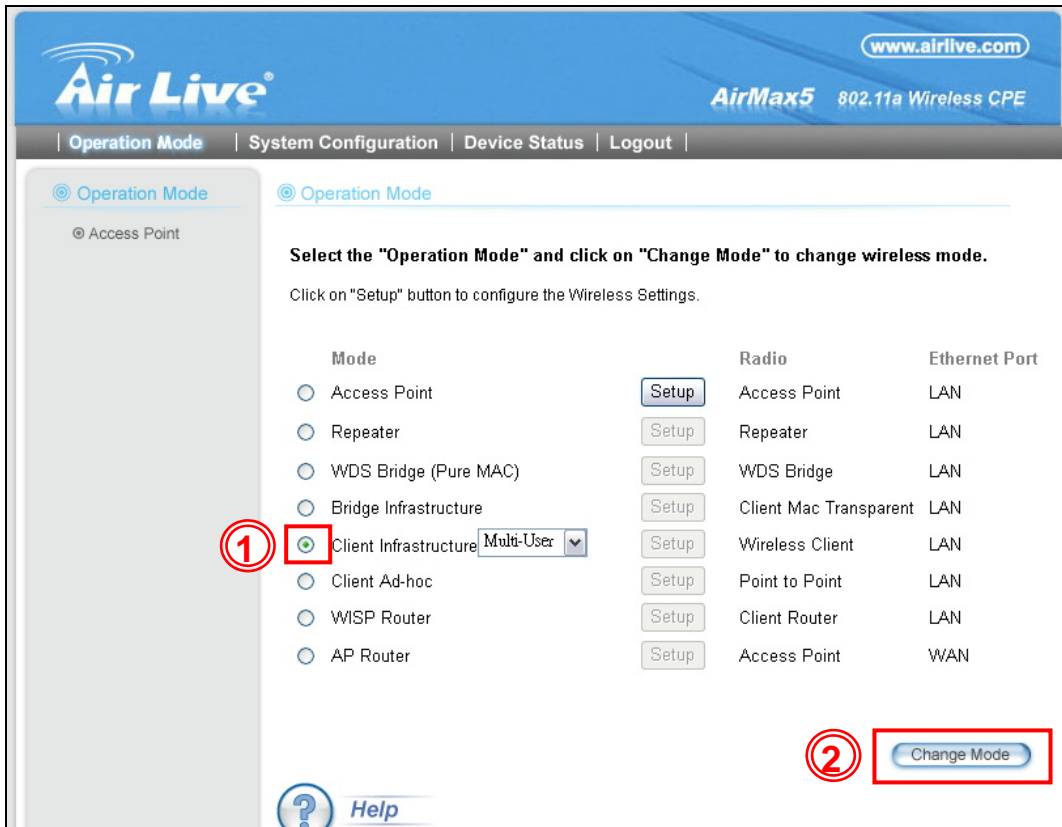
The screenshot displays the AirMax5 web management interface. The top navigation bar includes 'Operation Mode', 'System Configuration', 'Device Status', and 'Logout'. The main content area is titled 'Operation Mode' and contains the following text: 'Select the "Operation Mode" and click on "Change Mode" to change wireless mode. Click on "Setup" button to co **Click to configure wireless settings**'. Below this text is a table of operation modes:

Mode	Radio	Ethernet Port
<input checked="" type="radio"/> Access Point	Setup Access Point	LAN
<input type="radio"/> Repeater	Setup Repeater	LAN
<input type="radio"/> WDS Bridge (Pure MAC)	Setup WDS Bridge	LAN
<input type="radio"/> Bridge Infrastructure	Setup Client Mac Transparent	LAN
<input type="radio"/> Client Infrastructure Multi-User	Setup Wireless Client	LAN
<input type="radio"/> Client Ad-hoc	Setup Point to Point	LAN
<input type="radio"/> WISP Router	Setup Client Router	LAN
<input type="radio"/> AP Router	Setup Access Point	WAN

At the bottom right of the main content area is a 'Change Mode' button. A 'Help' icon is located at the bottom left. A red arrow points from the 'Access Point' mode in the left sidebar to a callout box labeled 'Current Wireless Mode'. Another red arrow points from the 'Setup' button for the 'Access Point' mode to a callout box labeled 'Click to configure wireless settings'.

Follow the example below to change to "Client Infrastructure" mode

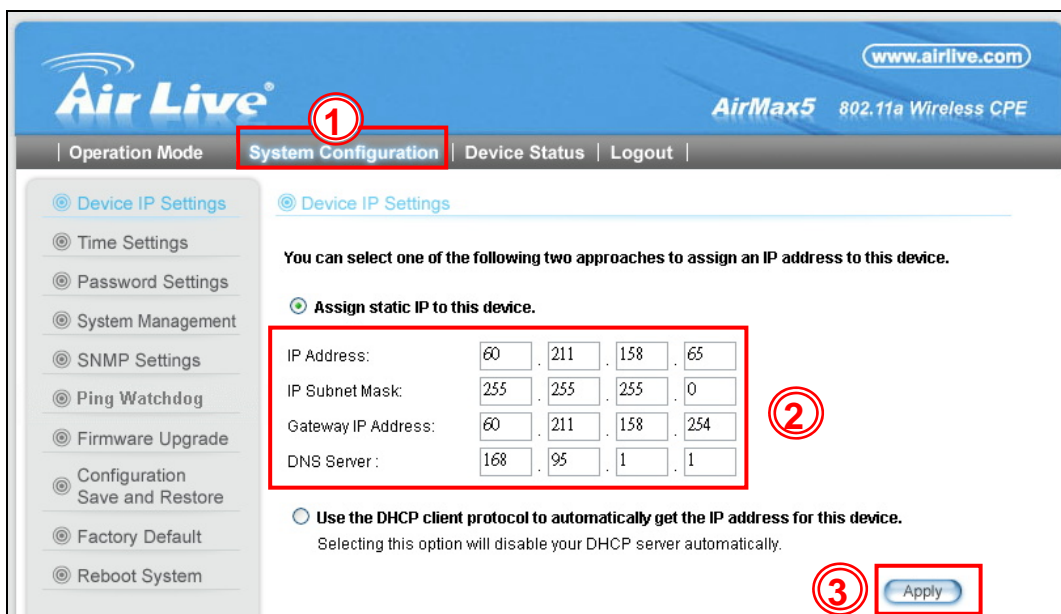
1. Select "Client Infrastructure" mode.
2. Click on "change mode" button
3. The AP will reboot, wait for about one minute



3.5.2 Change the Device's IP Address

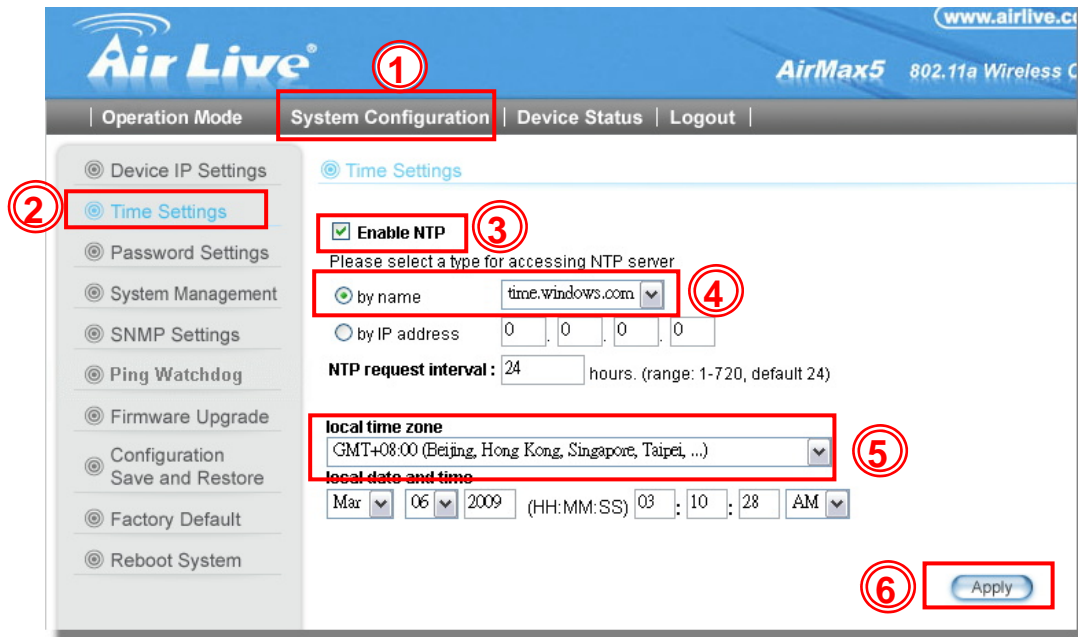
The default IP address is at 192.168.1.1. You should change it to the same subnet as your network. Also, if you want to manage AirMax5 remotely, you have to set the Gateway and DNS server information.

To setup the IP settings for AirMax5, please select "System Configuration" -> "Device IP Settings". After entering the IP information, click on "Apply" to finish.



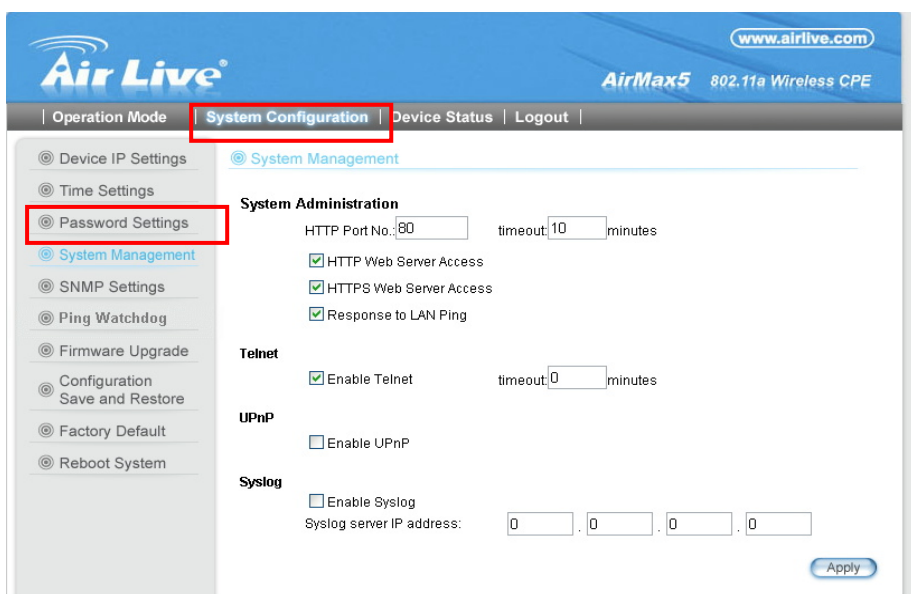
3.5.3 Set the Time and Date

It is important that you set the date and time for your AirMax5 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 AirMax5 is not connected to Internet, please enter the time manually. Please remember to select your local time zone and click “Apply” to finish.



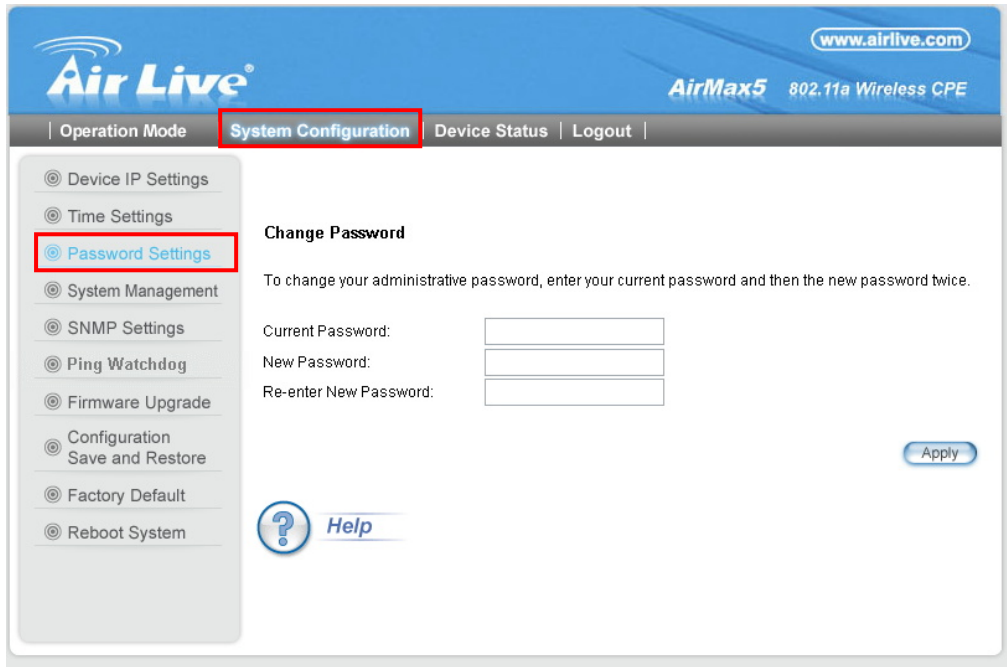
3.5.4 Change System Management

It is recommended that you change the system management settings first. Please go to “System Configuration”-> “System Management”. The default web management time out is 10 minutes, you can set to longer period if needed. For WISP administrators, you can consider turning off HTTP and Telnet for security purpose.



3.5.5 Change Password

You should change the password for AirMax5 at the first login. To change password, please go to “System Configuration” -> “Password Settings” menu.



The screenshot displays the Air Live web interface for the AirMax5 802.11a Wireless CPE. The top navigation bar includes 'Operation Mode', 'System Configuration' (highlighted with a red box), 'Device Status', and 'Logout'. The left sidebar menu lists various settings, with 'Password Settings' (highlighted with a red box) selected. The main content area is titled 'Change Password' and contains the following text: 'To change your administrative password, enter your current password and then the new password twice.' Below this text 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. A 'Help' link with a question mark icon is also visible at the bottom left of the main content area.

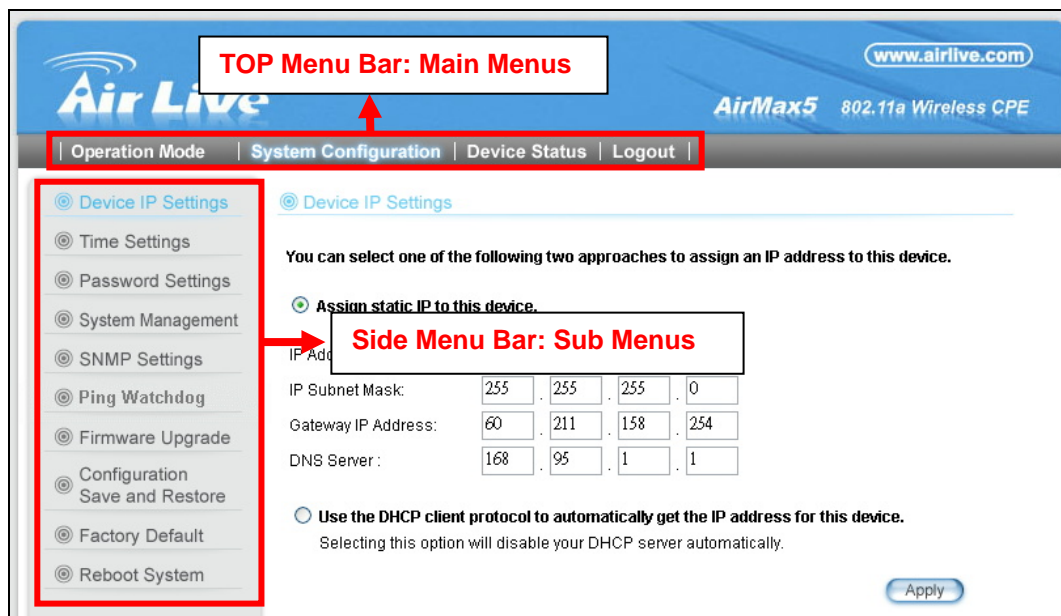
4

Web Management: Wireless and WAN 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 AirMax5's Menu Structure

The AirMax5'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 AirMax5's wireless settings are dependant 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

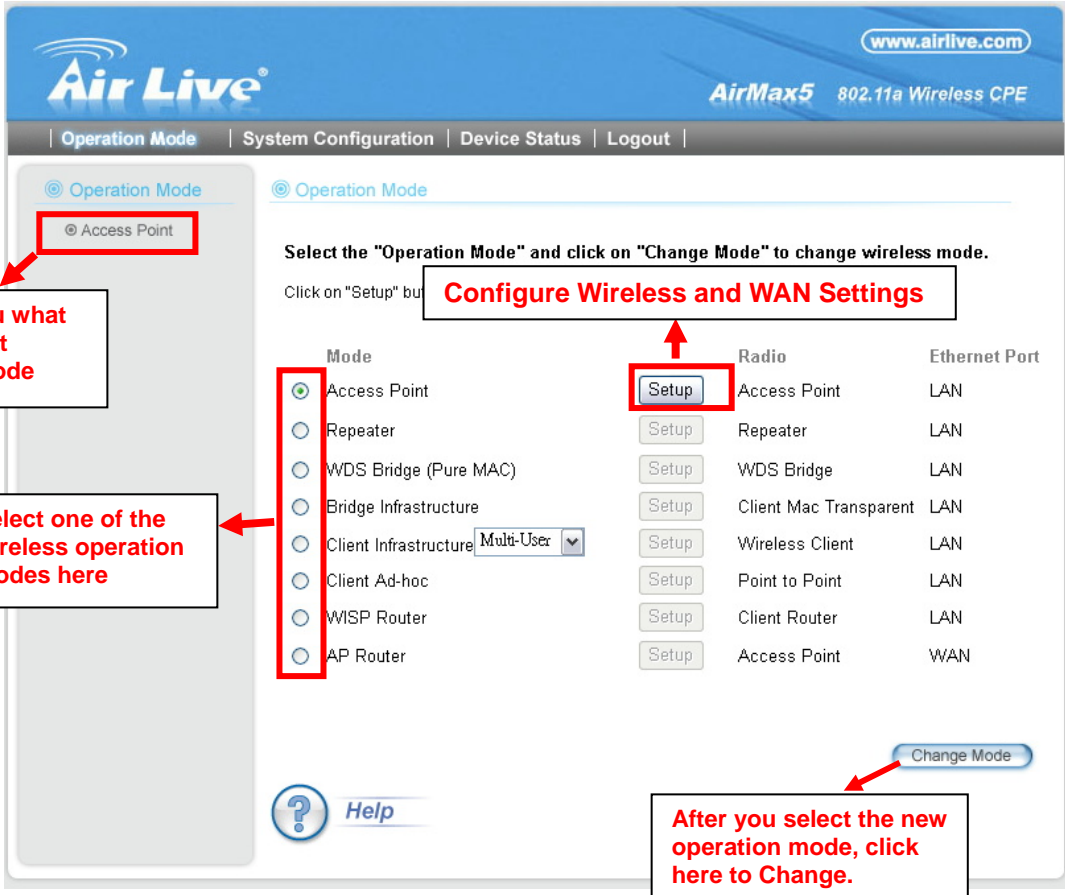
this menu for this chapter.

- **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 AirMax5. 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 AirMax5 are dependant 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:



This tells you what is the Current Operation Mode

Select one of the wireless operation modes here

Configure Wireless and WAN Settings

After you select the new operation mode, click here to Change.

Mode	Radio	Ethernet Port
<input checked="" type="radio"/> Access Point	Setup Access Point	LAN
<input type="radio"/> Repeater	Setup Repeater	LAN
<input type="radio"/> WDS Bridge (Pure MAC)	Setup WDS Bridge	LAN
<input type="radio"/> Bridge Infrastructure	Setup Client Mac Transparent	LAN
<input type="radio"/> Client Infrastructure <small>Multi-User</small>	Setup Wireless Client	LAN
<input type="radio"/> Client Ad-hoc	Setup Point to Point	LAN
<input type="radio"/> WISP Router	Setup Client Router	LAN
<input type="radio"/> AP Router	Setup Access Point	WAN

- **Mode:** The available wireless operation modes for AirMax5. 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:** This shows whether the radio

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



4.2.1 Regulatory Domain

Operation Mode -> Setup -> Regulatory Domain

There is a special domain called “*Test Domain*” which will show all the channels. It is for compatibility testing only. Please make sure the channel you used is allowed in your country when select this special domain.

4.2.2 Network SSID

Operation Mode -> Setup -> Network SSID

The SSID is the network name used to identify a wireless network. The SSID must be the same for all devices in the same wireless network. In AirMax5; it is possible to create more than one SSID in AP and AP Router mode, please check the “Multiple SSID & VLAN” section in this chapter. Conversely, several access points on a network can have the same SSID. 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.
- **Disable SSID Broadcast:** If you check this box, the SSID will be hidden; only users who know the SSID can associate with this network.

4.2.3 Site Survey

Operation Mode -> Setup -> Site Survey

The Site Survey function in AirMax5 provides 4 important functions

- In Client and Bridge Infrastructure mode, site survey will scan for available AP network. Then allow user to select and connect to the AP. This greatly simplify the installation
- Once Site Survey displays the available AP or Bridge networks, you can select a particular SSID to display its RSSI value continuously. This function is called “Signal Survey”. Signal Survey can be used for antenna alignment. For detail explanation of about RSSI value, please visit “How to Make Antenna Alignment” Chapter.
- For WDS Bridge mode, the Site Survey will scan for available AP and Bridge networks. User can then find the MAC address (BSSID) of the remote Bridges.
- For AP and AP router mode, the Site Survey allows administrator to check what channels are already occupied for choosing a cleaner channel.

When you click on Site Survey, the following screen will appear. It might take a few minutes to scan all the channels in the 5GHz spectrum.

Site survey

Site survey list :

Select	ESSID	MAC Address	Conn Mode	Channel	Turbo	Super	XR	WME	Signal Strength(dbm)	Security	Network
<input type="radio"/>	AirLive2	00:4f:69:6f:ee:a5	A	56	-	-	-	*	-34	None	AP
<input type="radio"/>	test	00:4f:69:52:2b:89	A	64	-	-	-	*	-61	None	AP
<input type="radio"/>	AirLive1	00:4f:69:6f:ee:a4	A	36	-	-	-	*	-41	None	AP

NOTE:
The sitesurvey will show both Ap and Bridge connections. Device without ESSID is more likely to be a Bridge device.

REFRESH SIGNAL SURVEY ASSOCIATE

Click here to select SSID for Association or Signal Survey

For antenna alignment. It will display and update RSSI value once a second.

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

- **Associate:** Please choose a SSID before click on this button. This button is available only in Client Infrastructure or Bridge Infrastructure modes. Once you click on this button, AirMax5 will attempt to make a connection with the selected ESSID. If there is encryption needed, the AirMax5 will prompt you to enter the encryption key. Please make sure you enter the correct encryption key, the Airmax5 will not check whether the encryption key is correct.
- **RSSI:** RSSI is a value to show the Receiver Sensitivity of the AirMax5. 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.

4.2.4 Signal Survey

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

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

BSSID:	<input type="text" value="00"/> - <input type="text" value="4F"/> - <input type="text" value="69"/> - <input type="text" value="6F"/> - <input type="text" value="EE"/> - <input type="text" value="A4"/>
Channel:	<input type="text" value="36"/>
Signal Strength:	<input type="text" value="-38"/> dbm

- **BSSID:** This is the remote AP’s MAC address.
- **Channel:** The current scanned channel
- **Signal Strength:** This is the RSSI value. It will refresh itself every second. The smaller the absolute value of the RSSI, the stronger the signal. For example -38dbm is stronger than -70dBm.

4.2.5 Lock-to-AP

Operation Mode -> Setup -> Lock-to-AP

This function is applicable only to Client mode, Bridge Infrastructure, and WISP Router mode. When this function is enables, the AirMax5 will put priority to associate with AP on the list. If “*Force connect with AP added below*” is selected, the AirMax5 will only connect with AP on the list.

4.2.6 Radio Mode (11a, SuperA, TurboA)

Operation Mode -> Setup -> Radio Mode

AirMax5 has 4 different options for WLAN transmission. All devices in the same network should use the same WLAN mode.

- **11a mode** (normal-A): This is the IEEE standard for WiFi operating in 5GHz frequency band. 11a is the most stable mode. If you are getting packet loss or disconnection using Super-A or Turbo-A mode. Please use 11a mode instead.
- **SuperA:** Super-A add Bursting, Compression, and Fast Frames to increase the speed over 11a mode. If you live in countries that prohibit the channel binding technology (i.e. Europe), you should choose “Super-A” If you need more speed than 11a mode. However, this mode is not as stable as 11a mode.
- **Super-A with Static Turbo:** Turbo mode uses channel binding technology to increase the speed further over Super-A mode. This mode might not be allowed in countries that prohibit channel binding (i.e. some EU countries). This mode will always turn on the turbo mode in all conditions
- **Super-A with Dynamic Turbo:** Dynamic Turbo mode will be turn on only when adjacent channel is not used. It is also know as intelligent turbo mode. This mode might not be allowed in countries that prohibit channel binding (i.e. some EU countries). In addition, this mode does not work in WDS Bridge mode



If you select “11a” or “Super-A” mode, you can still combined them with Turbo mode when you select “40MHz” Channel Width.

4.2.7 SuperA Option

Operation Mode -> Setup -> SuperA Option

When you select Radio Mode with “Super-A”, the SuperA Options will be available.

- **Bursting:** Allow more data frame to be sent over given period of time by overhead reduction.
- **Compression:** Increasing throughput by compressing data frame in real time
- **Fast Frame:** Utilizing frame aggregation and removing interframe pauses to increase the throughput.

It is recommended to select all 3 options except for compatibility reasons with remote AP.

4.2.8 Channel

Operation Mode -> Setup -> Channel

The channel is the frequency range used by radio. In 802.11a standard, each channel occupies 20MHz width. For 2 wireless devices to connect, they must use the same channel. The number of available legal channels might be different between countries. For example, Channel 149 to 161 are available only to United States and a few other countries. If you are living outside EU, please change the country from the “*Regulatory Domain*” option in this page. Below is the table list of channels and frequency.

Frequency Domain	Channel	Frequency (MHz)
5.15 to 5.25GHz U-NII Low ETSI Band1	36	5180
	40	5200
	44	5220
	48	5240
5.25 to 5.35GHz U-NII Mid ETSI Band1	52	5260
	56	5280
	60	5300
	64	5320
5.47 to 5.725GHz U-NII World Wide ETSI Band3	100	5500
	104	5520
	108	5540
	112	5560
	116	5580
	120	5600
	124	5620
	128	5640
	132	5660
	136	5680
U-NII Upper	140	5700
	149	5745
	153	5765
	157	5785
ISM	161	5805
	165	5825

- **Show All Channels:** Firmware starting from 1.00e14 version will have this option. It will display all the channel numbers regardless of what channel width is elected. For example, when you select “20MHz” for channel width, check this option will display channels “36,37,38, 39, 40...” Instead of “36, 40, 44...etc). This allow you to use a non-standard channel to avoid interference or for privacy purpose.

4.2.9 Channel Width

Operation Mode -> Setup -> Channel Width

In 802.11a spec, each channel occupies 20MHz channel width. Therefore, each channel will jump by number of 4 (i.e. 36, 40, 44...etc). You can change the Channel Width to 40MHz(Turbo), 10MHz(Half) or 5MHz(Quarter) to either increase performance or reduce the interference problem.

- **Turbo (40MHz):** Each channel will use 40MHz, double the normal size, to increase the performance by channel binding. This option is not allowed in countries inside EU
- **Normal (20MHz):** This is the default channel width specified by IEEE 802.11a specification
- **Half (10MHz):** Using this option will double the available channels for deployment in congested areas. However, the performance will also drop by half when using this option.
- **Quarter (5MHz):** Using this option will increase the available channels by 4 times. It is a good choice for deployment in very congested areas. However, the performance will also drop greatly when using this option.

4.2.10 Security Settings

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 AirMax5 features various security policies including WEP, 802.1x, WPA, WPA-PSK, WPA2, WPA2-PSK, WPA-Auto, and WPA-PSK-Auto. Please note not all security policies are available in all operation modes. For example, only WEP is available currently in WDS Bridge mode and Client Adhoc mode. 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 and Client Adhoc mode, we recommend using WEP-152 encryption.

WEP

WEP Encryption is the oldest and most available encryption method. However, it is also the least secure. Due to the limitation of the chipset, only WEP encryption is available for WDS Bridge Pure MAC mode and Client Adhoc mode.

Select Security Policy: WEP

Encryption
 Enabling encryption will secure data and prevent unauthorized users from accessing your wireless network. Identical encryption keys must be entered on all authorized wireless clients.

Authentication type AUTO

Select one of the WEP keys for the wireless network:
Encrypt data transmitting with WEP Key 1

WEP Key 1	WEP64-ASCII	<input style="width: 95%;" type="text"/>
WEP Key 2	WEP64-ASCII	<input style="width: 95%;" type="text"/>
WEP Key 3	WEP64-ASCII	<input style="width: 95%;" type="text"/>
WEP Key 4	WEP64-ASCII	<input style="width: 95%;" type="text"/>

APPLY

NOTE: To access the wireless network, user must have correct SSID and encryption key, if enabled.

- **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 “Encrypt Data with WEP Key 1” in the previous field, then it is necessary to fill WEP Key 1. The length of key is dependant on the Key Length and Key type you choose.

 - **Key Length:** The AirMax5 offers 64bit, 128 bit, and 152 bit for WEP key length. The longer the Key Length, the more secure the encryption is.
 - **Key Type:** 2 types are available: ASCII and HEX. ASCII is a string of ASCII code including alphabetical characters, space, signs and numbers (i.e. “airlivepass12”). HEX is a string of 16-bit hexadecimal digits (0..9, a, b, c, d, e, f). All wireless devices on the network must match the exact key length and Key type. Some Wireless clients only allow HEX type for WEP.
 - **ASCII-64:** This is a key with 64-bit key length of ASCII type. Please enter **5** ASCII Characters if you choose this option. For example, “passw”
 - **HEX-64:** This is a key with 64-bit key length of HEX type. Please enter **10** Hexadecimal digits if you choose this option. For example, “12345abcdef”
 - **ASCII-128:** This is a key with 64-bit key length of ASCII type. Please enter **13** ASCII Characters if you choose this option. For example, “airlivewepkey”
 - **HEX-128:** This is a key with 128-bit key length of HEX type. Please enter **26** Hexadecimal digits if you choose this option. For example, “1234567890abcdef1234567890”
 - **ASCII-152:** This is a key with 64-bit key length of ASCII type. Please enter **16** ASCII Characters if you choose this option. For example, “airlivewepkey123”

- **HEX-152:** This is a key with 128-bit key length of HEX type. Please enter **32** Hexadecimal digits if you choose this option. For example, "1234567890abcdef1234567890abcdef"

802.1x

Select Security Policy:

Select key length for WEP rekeying:

Rekey interval: sec.(0 means keying once)

NOTE:To access the wireless network, user must have correct SSID and encryption key, if enabled.

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.

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



After you have finished the configuration wizard, you have to configure the RADIUS Settings in "Operation Mode -> Setup -> RADIUS Settings" in order to make the 802.1x function work.

WPA, WPA2, WPA-AUTO

Wi-Fi Protected Access (WPA) introduces the Temporal Key Integrity Protocol (TKIP) that provides added security. WPA2 adds full support for 802.11i standard and the CCMP (AES Encryption). The WPA-AUTO tries to authenticate wireless clients using WPA or WPA2. All 3 requires a RADIUS server available in order to do authentication (same as 802.1x), thus there is no shared key required.

Select Security Policy:

WPA Encryption Type: TKIP CCMP(AES) Both

WPA Group Rekey Interval: sec.(0 means disable rekey)

Select Security Policy:

WPA2 Encryption Type: TKIP CCMP(AES) Both

WPA2 Group Rekey Interval: sec.(0 means disable rekey)

Select Security Policy:

WPA-AUTO Encryption Type: TKIP CCMP(AES) Both

WPA-AUTO Group Rekey Interval: sec.(0 means disable rekey)

- Encryption Type:** There are two encryption types **TKIP** and **CCMP (AES)**. While CCMP provides better security than TKIP, some wireless client stations may not be equipped with the hardware to support it. You can select **Both** to allow TKIP clients and CCMP clients to connect to the Access Point at the same time.
- Group Rekey Interval:** A group key is used for multicast/broadcast data, and the re-key interval is time period that the system will change the group key periodically. The shorter the interval is, the better the security is. The default is 300 sec.

WPA-PSK, WPA2-PSK, WPA-PSK-Auto

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

Select Security Policy:

Pre-shared Key (ASCII string):

(8-63 characters)

WPA Encryption Type: TKIP CCMP(AES) Both

WPA Group Rekey Interval: sec.(0 means disable rekey)

Select Security Policy: <input type="text" value="WPA2-PSK"/>
Pre-shared Key (ASCII string): <input type="text"/> (8-63 characters)
WPA Encryption Type: <input type="radio"/> TKIP <input type="radio"/> CCMP(AES) <input checked="" type="radio"/> Both
WPA2 Group Rekey Interval: <input type="text" value="300"/> sec.(0 means disable rekey)

Select Security Policy: <input type="text" value="WPA-PSK-AUTO"/>
Pre-shared Key (ASCII string): <input type="text"/> (8-63 characters)
WPA-AUTO Encryption Type: <input type="radio"/> TKIP <input type="radio"/> CCMP(AES) <input checked="" type="radio"/> Both
WPA-AUTO Group Rekey Interval: <input type="text" value="300"/> sec.(0 means disable rekey)

- **Pre-shared Key:** This is an ASCII string with 8 to 63 characters. Please make sure that both the AIRMAX5 and the wireless client stations use the same key.
- **Encryption Type:** There are two encryption types **TKIP** and **CCMP (AES)**. While CCMP provides better security than TKIP, some wireless client stations may not be equipped with the hardware to support it. You can select **Both** to allow TKIP clients and CCMP clients to connect to the Access Point at the same time.
- **Group Rekey Interval:** A group key is used for multicast/broadcast data, and the re-key interval is time period that the system will change the group key periodically. The shorter the interval is, the better the security is. The default is 300 sec.

4.2.11 Distance

Operation Mode -> Setup -> Distance

Please enter the distance to the remote wireless device here. The AirMax5 will then calculate the appropriate ACK Timeout value automatically.

It is very important that you enter the correct distance for long distance connection. Failure to do so will result in poor performance.

4.2.12 Antenna Settings

Operation Mode -> Setup -> Antenna Settings

The AirMax5 is equipped with 2 x 14dBi patch antennas. One antenna in horizontal polarization and one in vertical polarization. For 2 wireless devices to connect, their antennas must use the same polarization.

- Vertical:** The polarization of the antenna is vertical, in the same direction as the AirMax5. This settings is the default and most used.
- Horizontal:** The polarization of the antenna is horizontal, 90 degree from the direction of the case.
- Diversity:** The AirMax5 will auto switch between vertical and horizontal antennas based on the RSSI level detected. However, the performance can suffer if the switching happens too frequently.

Please read more about Antenna information on *Chapter 7: Antenna Alignment*.

4.2.13 Transmit Power

Operation Mode -> Setup -> Transmit Power

You can adjust the transmit output power of the AirMax5's radio from 10dBm to 24dBm. The higher the output power, the more distance AirMax5 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.

At less than 200meter distance, the best output power is about 14dBm. At 2km distance; the best output power setting is 18dBm for "11a" and "Super-A without Turbo", 24dBm for "Super-A with Static/Dynamic Turbo".

4.2.14 Advance Settings (Wireless)

Operation Mode -> Setup -> Advance Settings

This page includes all the wireless settings that change the RF behaviors of AirMax5. It is important to read through this section before attempting to make changes.

Advanced Wireless Settings

Beacon Interval: msec. (range: 20-1000, default 100)

RTS Threshold: bytes (range: 0-2347, default 2347)

Fragmentation: bytes (range: 256-2346, default 2346)

DTIM Interval: (range 1-255, default 1)

User Limitation: (range: 1-100, default 100)

Age Out Timer: min. (range: 1-1000, default 5)

Rate Control: Mbps

Noise Immunity:

AckTimeOut: μ S (range: 10-255, default 25)

Enable Radio eXtended Range

Enable privacy separator(Client Isolation)

Enable 802.1d STP

Enable 802.11d global roaming

- **Beacon Interval:** The device broadcasts beacon frames regularly to announce its existence. The beacon Interval specifies how often beacon frames are transmitted in time unit of milliseconds. The default value is **100**, and a valid value should be between 1 and 65,535.
- **RTS Threshold:** RTS/CTS frames are used to gain control of the medium for transmission. Any unicast (data or control) frames larger than specified RTS threshold must be transmitted following the RTS/CTS handshake exchange mechanism. The RTS threshold should have a value between 256-2347 bytes, with a default of **2347**. It is recommended that this value does not deviate from the default too much.
- **Fragmentation:** When the size of a unicast frame exceeds the fragmentation threshold, it will be fragmented before the transmission. It should have a value of 256-2346 bytes, with a default of 2346. If you experience a high packet error rate,

you should slightly decrease the Fragmentation Threshold.

- **DTIM Interval:** The AIRMAX5 buffers packets for stations that operate in the power-saving mode. The Delivery Traffic Indication Message (DTIM) informs such power-conserving stations that there are packets waiting to be received by them. The DTIM interval specifies how often the beacon frame should contain DTIMs. It should have a value between 1 to 255, with a default value of 3.
- **User Limitation:** This limitation applies to number of wireless clients the device can associate. If you need to serve wireless connection to large number of users in one location. You can deploy many APs and limit the number of wireless clients, so any additional wireless connection attempt will be rejected (therefore, redirect to other AP). The range of user limitation is from 1 to 100.
- **Age Out Timer:** Set the age out timer for the wireless client. If there is no traffic from client for more than the timer, the wireless client will be dropped. The default is 300 sec. This function is available only for the Access Point and AP router mode.
- **Rate Control:** Select here to change the Data Rate for the radio. Lower data rate sometimes provide longer distance. In most cases, however, we recommend to keep the setting at “Best”.
- **Noise Immunity:** Adaptive Noise Immunity is one of the new function in Atheros driver to enhance the performance in interference environment.
- **AckTimeOut:** When a packet is sent out from one wireless station to the other, it will wait 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.

The easiest way to enter AckTimeOut value is by entering the distance in “*Operation Mode -> Setup -> Distance*”. The AirMax5 will then calculate and enter the correct value for you.
- **Enable Radio eXtended Range:** XR is Atheros eXtended technology to increase range. When XR is turned on, the radio can increase the receiver sensitivity greatly. However, performance may be reduced significantly also. Use this mode only if you can trade more distance for lower performance.
- **Enable privacy separator:** Select the check box to prohibit data transmission


between client stations. This function is also known as “Client Isolation”.

- **Enable 802.1d:** Enable the Spanning Tree Protocol to prevent forming a network loop. This option is especially important for WDS Bridge mode.
- **Enable 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.

4.2.15 Access Control (ACL)

Operation Mode -> Setup -> Access Control

The AIRMAX5 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.

 **MAC Filtering Settings**

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

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.

Mnemonic Name:

MAC Address: - - - - -

Select	Name	MAC Address
-	-	-

- **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.

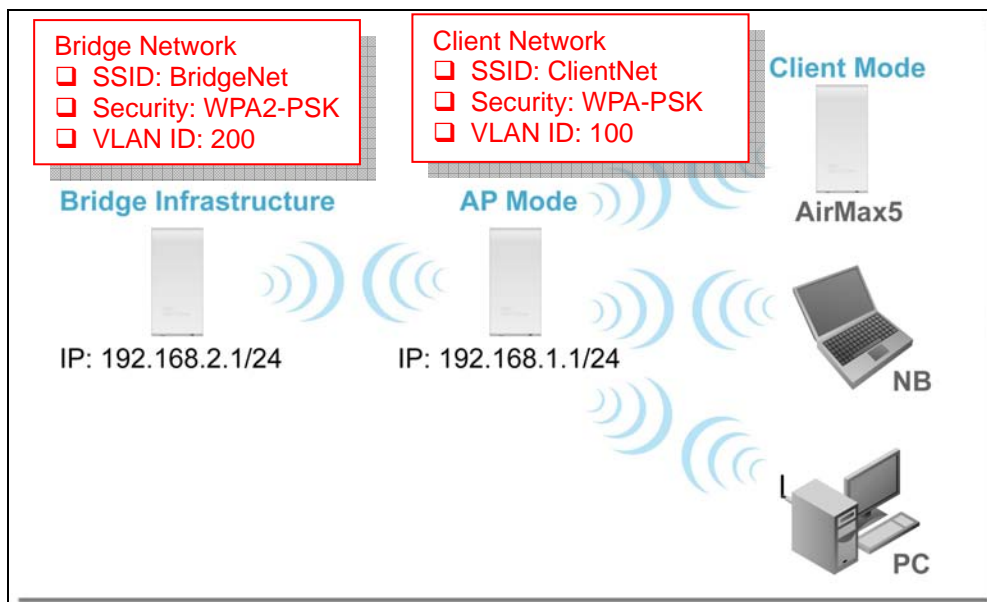
To add a MAC address into the table, enter a *Mnemonic Name* and the *MAC Address*, and then click *Add*. The table lists all configured MAC Filter entries.

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

4.2.16 Multiple SSID

Operation Mode -> Setup -> Multiple SSID

This function is available only for Access Point and AP Router modes. Multiple SSID allows AirMax5 to create up to 4 different wireless networks (SSID). It is also known as “Virtual AP” function. Each SSID can have its Encryption type, VLAN Tag, and TOS settings. In the following diagram, the AirMax5 uses Multiple SSID function to create separate Bridge and Client network. Each has its own encryption policies.



Configuring the Multiple SSID

When you click on the “Multiple SSID” button, the following screen will appear

SSID Settings

This page lets you configure multiple SSIDs and corresponding QoS settings if QoS is enabled.

- Enable VLAN for all SSIDs (All packets are tagged with VLAN ID)
- Enable DiffServ Marking

Apply

SSID Name	VLAN ID/Priority	Security
<input checked="" type="radio"/> airlive	-	Wep

This is the default SSID

NEW

DELETE SELECTED

SSID Name:

- Disable SSID Broadcasting

Select Security Policy:

Click here to apply changes on adding or deleting SSID

Apply

Click here to Apply changes in "VLAN" and "DiffServe Marking"

How to add a SSID

You can add up to 4 SSID in AirMax5. Please follow the procedure below:

1. Enter the SSID name (i.e. BridgeNet)
2. Select the Security Policy (i.e. WPA2-PSK)
3. Enter the Security Key (i.e. BridgeNetKey).
4. Click on "Apply" to add SSID

SSID Settings

This page lets you configure multiple SSIDs and corresponding QoS settings if QoS is enabled.

- Enable VLAN for all SSIDs (All packets are tagged with VLAN ID)
- Enable DiffServ Marking

Apply

SSID Name	VLAN ID/Priority	Security
<input checked="" type="radio"/> airlive	-	Wep

NEW DELETE SELECTED

SSID Name: 1

- Disable SSID Broadcasting

Select Security Policy: 2

Pre-shared Key (ASCII string): 3
(8-63 characters)

WPA2 Encryption Type: TKIP CCMP(AES) Both

WPA2 Group Rekey Interval: sec.(0 means disable rekey)

4 Apply

How to Modify or Delete a SSID

Please follow the procedure below:

1. Select the SSID you want to modify or delete
2. The SSID's settings will be displayed in the box area. Modify any settings.
3. Click on "APPLY" to complete the modification
4. Or click on "Delete Selected" to delete the SSID

SSID Settings

This page lets you configure multiple SSIDs and corresponding QoS settings if QoS is enabled.

Enable VLAN for all SSIDs (All packets are tagged with VLAN ID)

Enable DiffServ Marking

SSID Name	VLAN ID/Priority	Security
<input type="radio"/> airlive	-	None
<input checked="" type="radio"/> BridgeNet	-	Wpa2-Psk

SSID Name:

Disable SSID Broadcasting

Select Security Policy:

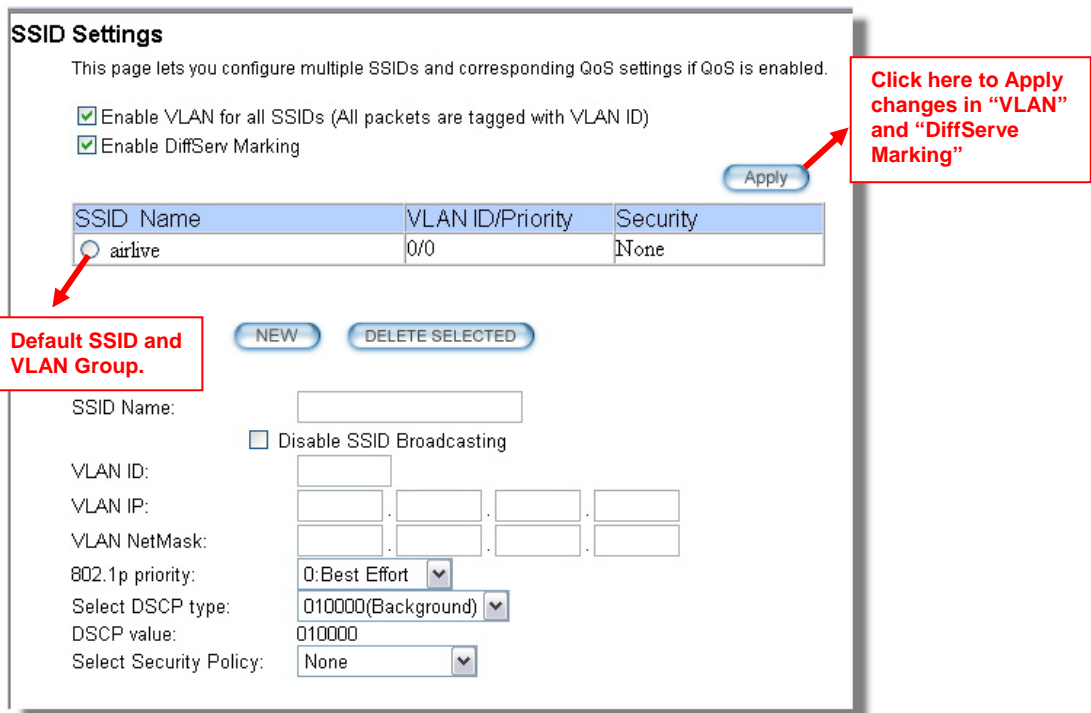
Pre-shared Key (ASCII string):
(8-63 characters)

WPA2 Encryption Type: TKIP CCMP(AES) Both

WPA2 Group Rekey Interval: sec.(0 means disable rekey)

Configure the VLAN and DiffServ Markings

When you check the *Enable VLAN for All SSIDs* and/or *Enable DiffServ Marking*, the following screen will appear:



SSID Settings

This page lets you configure multiple SSIDs and corresponding QoS settings if QoS is enabled.

Enable VLAN for all SSIDs (All packets are tagged with VLAN ID)

Enable DiffServ Marking

Apply

SSID Name	VLAN ID/Priority	Security
airlive	0/0	None

NEW DELETE SELECTED

SSID Name:

Disable SSID Broadcasting

VLAN ID:

VLAN IP: . . .

VLAN NetMask: . . .

802.1p priority: : Best Effort

Select DSCP type: 010000(Background)

DSCP value: 010000

Select Security Policy: None

- **Enable VLAN for All SSIDs:** Once this function is enabled, you can specify an individual VLAN ID and priority tag for each SSID. The packets from a SSID will be forwarded to the Ethernet with the corresponding configured VLAN ID written. *You need to click on the top “APPLY” button after making changes.*
- **Enable DiffServ Marking:** When this function is enabled, you can configure a DSCP value for each SSID. Then a packet from a station using this SSID will be forwarded with the DSCP value labeled. *You need to click on the top “APPLY” button after making changes.*
- **VLAN ID:** Packets going out of this VLAN will be tagged with the VLAN ID. Packets coming into the AP will be dropped if the VLAN Tag does not match. The valid range is between 0 to 4095. The VLAN ID “0” is the default VLAN group.
- **VLAN IP:** Each SSID can be given with different VLAN IP group. Please notice that the management IP in the VLAN will also be changed. For example, if you define the VLAN IP to be 192.168.2.X subnet, then the AirMax5’s management IP in the group will change to 192.168.2.1.
- **VLAN IP NetMask:** Define your VLAN IP scope here
- **802.1p Priority:** Define your 802.1p priority Tag here. Value from 0 to 7
- **Select DSCP TYPE:** Assign the 6-digit DifferServ Code(DSCP) for the packets in the SSID network for QoS purpose. There are 8 preset values. To assign your own value, please select “Best Effort”
- **DSCP Value:** When you select “Best Effort” DSCP Type, you can enter the 6-digit DSCP Value here.
- **Select Security Policy:** Select the encryption used for this SSID VLAN group. This policy can be different in each SSID VLAN group. For example, one SSID

can be using WEP, the other policy can use WPA-PSK.

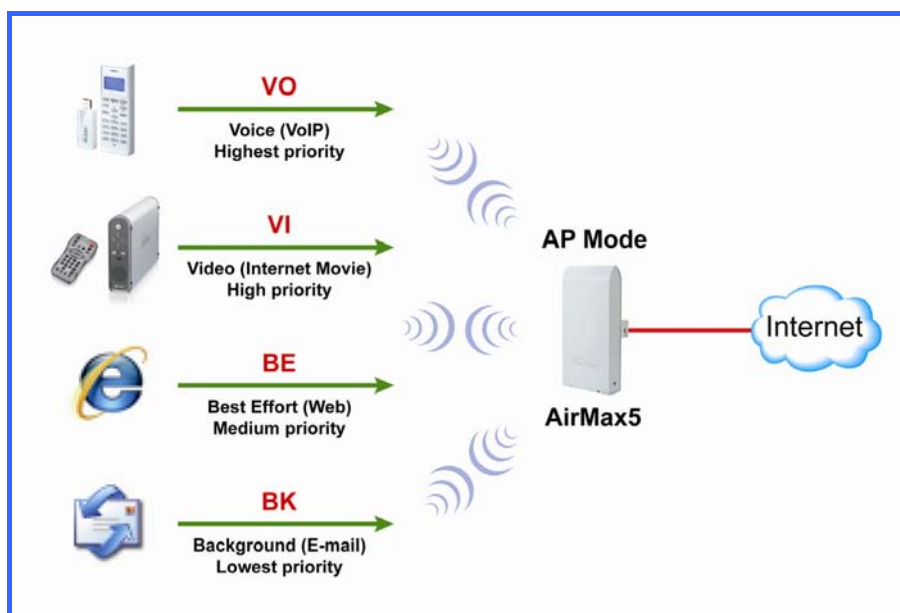


Once you enable the VLAN ID. The incoming packet from Ethernet port to your VLAN group must carry the same VLAN ID tag or the packet will be dropped.

4.2.17 WMM QoS

Operation Mode -> Setup -> WMM QoS

Wi-Fi Multimedia (WMM) is a standard to prioritize traffic for multimedia applications. The WMM Settings is to specify parameters on multiple data queue for better performance of differentiated wireless traffic like Voice-over-IP (VoIP), other types of audio, video, and streaming media as well as traditional IP data over the AP.



Configure the WMM QoS Parameters

QoS Settings

Enable WMM

WMM Parameters of Access Point

AC TYPE	ECWMin	ECWMax	AIFS	TxopLimit-11a(μs)	ACM	Ack-policy
AC_BE(0)	<input type="text" value="4"/>	<input type="text" value="6"/>	<input type="text" value="3"/>	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>
AC_BK(1)	<input type="text" value="4"/>	<input type="text" value="10"/>	<input type="text" value="7"/>	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>
AC_VI(2)	<input type="text" value="3"/>	<input type="text" value="4"/>	<input type="text" value="1"/>	<input type="text" value="3008"/>	<input type="checkbox"/>	<input type="checkbox"/>
AC_VO(3)	<input type="text" value="2"/>	<input type="text" value="3"/>	<input type="text" value="1"/>	<input type="text" value="1504"/>	<input type="checkbox"/>	<input type="checkbox"/>

WMM Parameters of Station

AC TYPE	ECWMin	ECWMax	AIFS	TxopLimit-11a(μs)	ACM
AC_BE(0)	<input type="text" value="4"/>	<input type="text" value="10"/>	<input type="text" value="3"/>	<input type="text" value="0"/>	<input type="checkbox"/>
AC_BK(1)	<input type="text" value="4"/>	<input type="text" value="10"/>	<input type="text" value="7"/>	<input type="text" value="0"/>	<input type="checkbox"/>
AC_VI(2)	<input type="text" value="3"/>	<input type="text" value="4"/>	<input type="text" value="2"/>	<input type="text" value="3008"/>	<input type="checkbox"/>
AC_VO(3)	<input type="text" value="2"/>	<input type="text" value="3"/>	<input type="text" value="2"/>	<input type="text" value="1504"/>	<input type="checkbox"/>

■ AC Type

The queue and associated priorities and parameters for transmission are as follows:

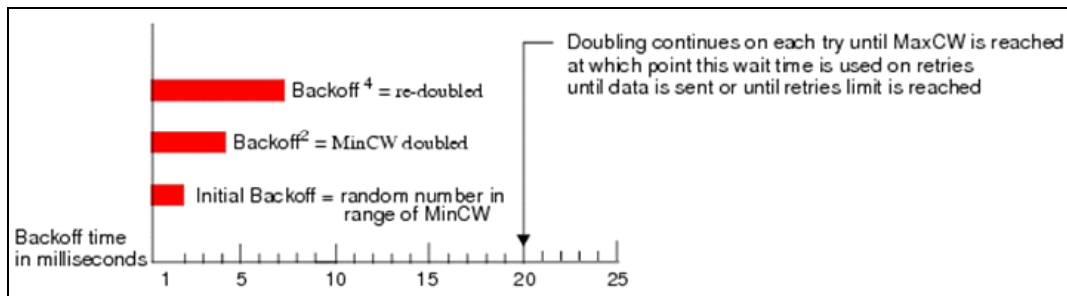
- Data 0 (Best Effort, BE):** Medium priority queue, medium throughput and delay. Most traditional IP data is sent to this queue.
- Data 1 (Background, BK):** Lowest priority queue, high throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example):
- Data 2 (Video, VI):** High priority queue, minimum delay. Time-sensitive data such as Video and other streaming media are automatically sent to this queue.
- Data 3 (Voice, VO):** Highest priority queue, minimum delay. Time-sensitive data such as Voice over IP (VoIP) is automatically sent to this queue.

Packets in a higher priority queue will be transmitted before packets in a lower priority queue.

■ ECWmin and ECWmax

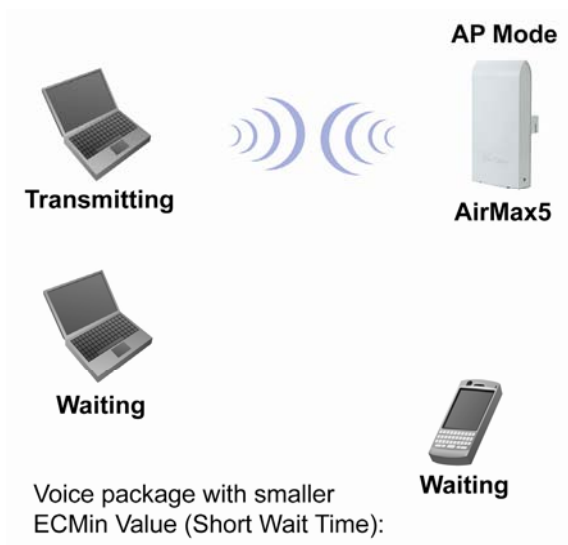
If an access point detects that the medium is in use, it uses the DCF random backoff timer to determine the amount of time to wait before attempting to access a given channel again. Each access point waits some random period of time between retries. The wait time (initially a random value within a range specified as the *Minimum Contention Window* increases exponentially up to a specified limit *Maximum Contention Window*.

The random delay avoids most of the collisions that would occur if multiple APs got access to the medium at the same time and tried to transmit data simultaneously. The more active users you have on a network, the more significant the performance gains of the backoff timer will be in reducing the number of collisions and retransmissions.



The random backoff used by the access point is a configurable parameter. To describe the random delay, a "Minimum Contention Window" (ECWMin) and a "Maximum Contention Window" (ECWMax) is defined.

- ❑ **ECWmin:** The value specified for the Minimum Contention Window is the upper limit of a range for the initial random backoff wait time. The number used in the random backoff is initially a random number between 0 and the number defined for the Minimum Contention Window.
- ❑ **ECWmax:** If the first random backoff time ends before successful transmission of the data frame, the access point increments a retry counter, and doubles the value of the random backoff window. The value specified in the Maximum Contention Window is the upper limit for this doubling of the random backoff. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached.



■ AIFS

The Arbitration Inter-Frame Spacing (AIFS) specifies a wait time (in milliseconds) for data frames. 802.11e uses interframe spaces to regulate which frames get access to available channels and to coordinate wait times for transmission of different types of data. The AIFS ensures that multiple access points do not try sending data at the same time but instead wait until a channel is free. Valid values for AIFS are 1 through 255.

■ Transmission Opportunity

The Transmission Opportunity (TXOP) is an interval of time when a WMM client station has the right to initiate transmissions onto the wireless medium. This value specifies (in milliseconds) the Transmission Opportunity (TXOP) for client stations; that is, the interval of time when a WMM client station has the right to initiate transmissions on the wireless network.



We recommend that you use the default settings on the WMM QoS page. Changing these values can lead to unexpected blockages of traffic on your wireless LAN, and the blockages might be difficult to diagnose.

4.2.18 RADIUS Settings

Operation Mode -> Setup -> RADIUS Setting

RADIUS servers provide centralized authentication services to wireless clients. Two RADIUS servers can be defined: one acts as a primary, and the other acts as a secondary backup. If you choose to use 802.1x, WPA, or WPA2 as security policy, you might need to set the RADIUS server settings.

RADIUS Settings

RADIUS Server

Enable RADIUS Server

Server IP: . . .

Port Number:

RADIUS Type: RADIUS

Shared Secret:

Secondary RADIUS Server

Enable RADIUS Server

Server IP: . . .

Port Number:

RADIUS Type: RADIUS

Shared Secret:

RADIUS Server Reattempt Period Seconds

To Enable RADIUS Server:

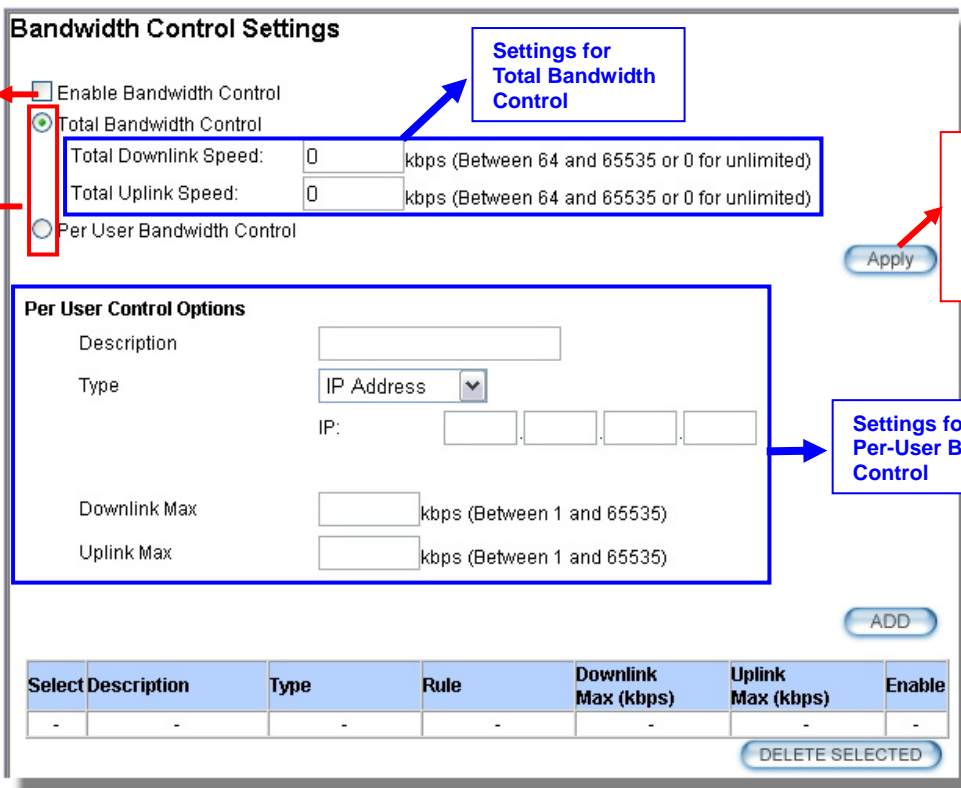
- **Server IP:** The IP address of the RADIUS server.
- **Port Number:** The port number that your RADIUS server uses for authentication. The default setting is 1812.
- **RADIUS Type:** RADIUS
- **Shared Secret:** This is used by your RADIUS server in the Shared Secret field in RADIUS protocol messages. The shared secret configured in the AIRMAX5 must match the shared secret configured in the RADIUS server. The shared secret can contain up to 64 alphanumeric characters.
- **RADIUS Server Reattempt Period:** The number of times the AIRMAX5 should attempt to contact the primary server before giving up

4.2.19 Bandwidth Control

Operation Mode -> Setup -> Bandwidth Control

Bandwidth Control can limit the maximum speed of entire wireless interface or individual device. It is also known as Traffic Shaping. The AirMax5 provides both Total Bandwidth and Per-User 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

Enable Bandwidth Control

Total Bandwidth Control

Total Downlink Speed: kbps (Between 64 and 65535 or 0 for unlimited)

Total Uplink Speed: kbps (Between 64 and 65535 or 0 for unlimited)

Per User Bandwidth Control

Per User Control Options

Description:

Type: IP Address

IP: . . .

Downlink Max: kbps (Between 1 and 65535)

Uplink Max: kbps (Between 1 and 65535)

Select	Description	Type	Rule	Downlink Max (kbps)	Uplink Max (kbps)	Enable
-	-	-	-	-	-	-

- Enable Bandwidth:** Check to enable Bandwidth Control. Uncheck to disable it. The default value is disabled.

You must select between Total Bandwidth and Per-User Bandwidth. They can not be enabled at the same time.

- Total Bandwidth:** Total Bandwidth control limit the bandwidth between Wireless and Ethernet interface. Therefore, it is most suitable for *Client Infrastructure Mode*, *Bridge Mode*, and *WISP Router Mode*. For WISP operator who use AirMax5 as the client side device; setting the Total Bandwidth control on the AirMax5 will easy the loading on the AP for bandwidth management. To begin, please enable the Bandwidth Management first. Then enter the downlink and uplink speed; click on Apply to finish.
 - Total Downlink Speed: Enter speed you wish to limit the download traffic in Kbps units.
 - Total Uplink Speed: Enter the speed you wish to limit the upload traffic in Kbps units.
- Per User Bandwidth Control:** Per user Bandwidth Control can limit speed of individual PC and network device. The AirMax5 allows multiple Per-User bandwidth rules and can limit the bandwidth by IP address, MAC address, or IP segment.

Please first enable the Bandwidth Control, then select “*Per User Bandwidth Control*” to begin. It is recommended to use this type of bandwidth control for Access Point and AP Router mode.

Per User Control Options

Description: Enter a description for the bandwidth policy. For example, “VIP” subscriber

Type: AirMax5 offers 3 types of Per-User Control

■ **IP Address:** To limit the bandwidth of one single IP address.

■ **IP Segment:** To limit the bandwidth the entire IP segment.

For example; if you enter the address of 192.168.1.20 with subnet mask of 255.255.255.248, the AirMax5 will limit bandwidth of IP addresses from 192.168.1.17 to 192.168.1.22. Please use an online IP calculate if you are not familiar with IP segment calculation. Below is an example link:

<http://www.subnet-calculator.com/>

Because the Ethernet interface is also controlled by the Bandwidth Manager, it is recommended that devices on the Ethernet side to use a wider IP subnet mask that will cover the IP range of the controlled IP segment. Therefore, the devices on Ethernet interface will not be limited by bandwidth control and still can communicate with the IP segment. For example, if your IP segment is set to 192.168.1.20 / 255.255.255.248, then the devices on the Ethernet side should be 192.168.1.X / 255.255.255.0.

■ **MAC address:** To limit the bandwidth of one single MAC address.

■ **Port Range:** This is available only in WISP router and AP Router mode. It can limit the bandwidth by application ports.

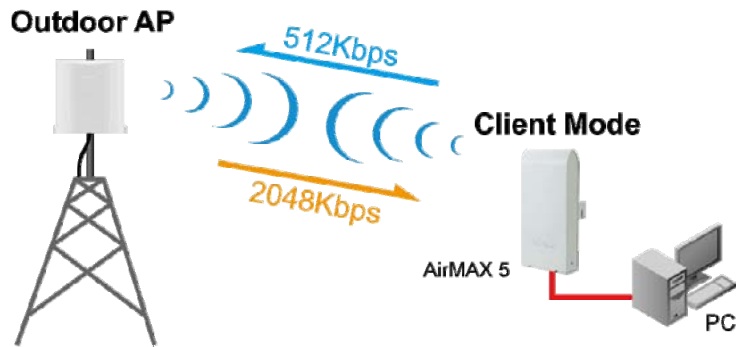
■ **Application:** This option is available only in WISP router and AP Router mode. It can limit the bandwidth of HTTP, FTP, BitTorrent, and eDonkey traffic.

Downlink Max: Enter the speed you wish to limit the download traffic in kbps units.

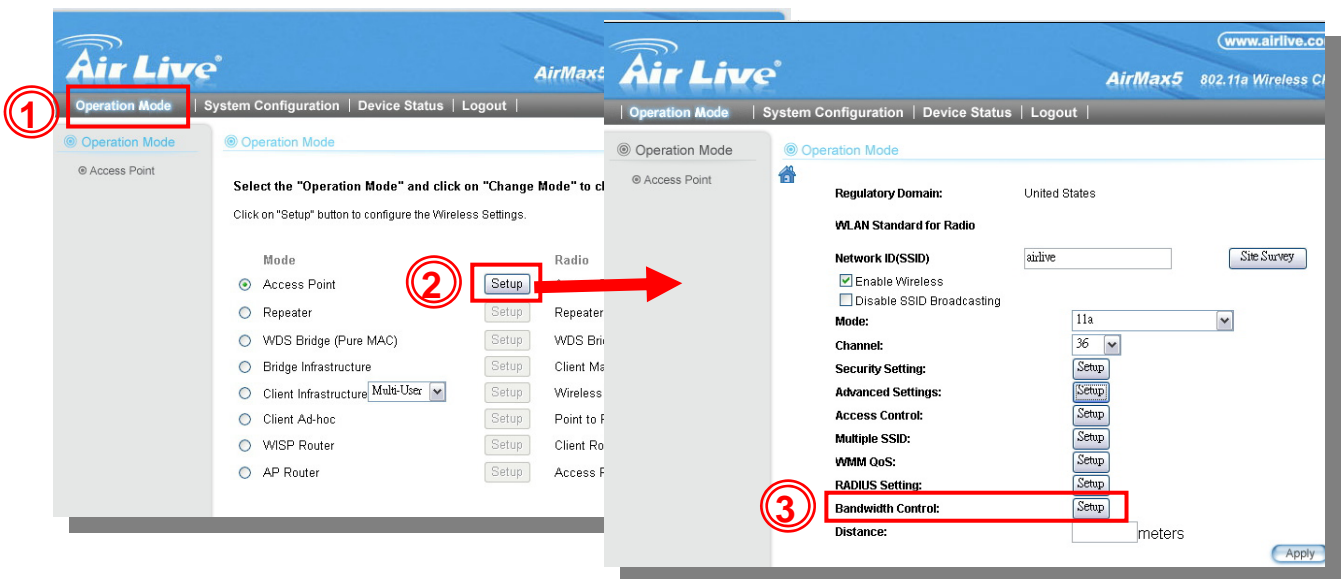
Uplink Max: Enter the speed you wish to limit the upload traffic in kbps units

■ Example 1: Total Bandwidth Control

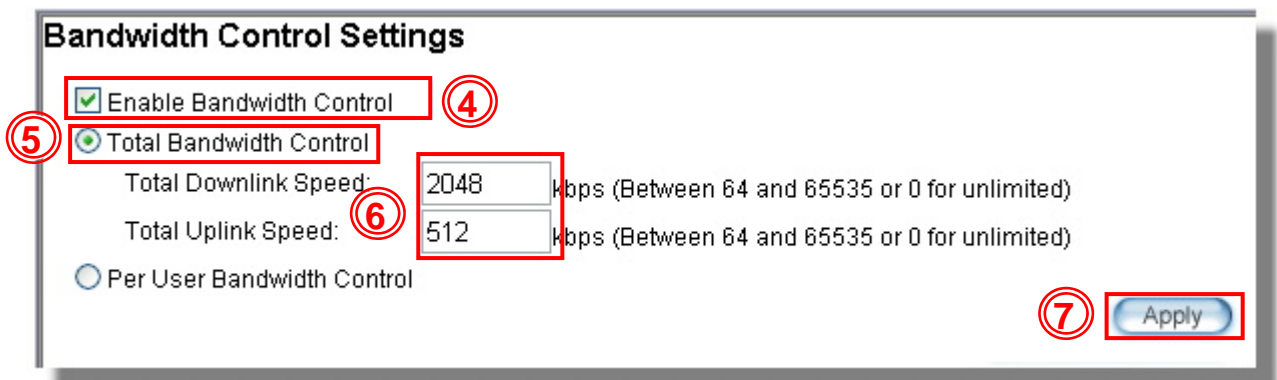
In this example, the AirMax5 is in Client Infrastructure mode connecting to a remote AP. We want to limit the Bandwidth of the link to 2048Kbps download and 512kbps Upload.



- **Step 1 to 3:** From *Operation Mode* menu, select “Setup” -> “Bandwidth Control”

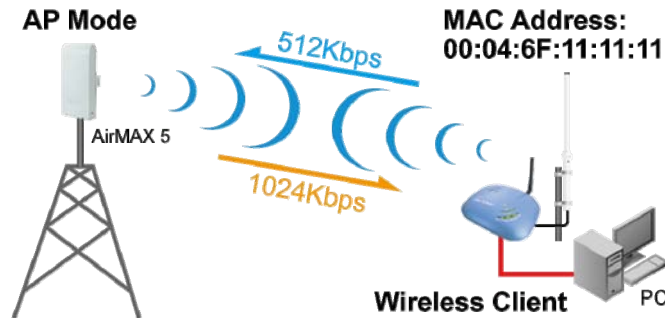


- **Step 4 to 7:** Enable the Bandwidth Control and select the “Total Bandwidth Control”. Then enter the “2048” for *Total Downlink Speed* and “512”kpbs for *Total Uplink Speed*. Click “Apply” to finish



■ **Example 2: Per User Bandwidth Control**

In this example, the AirMax5 is Access Point mode. There is a wireless client connecting to AirMax5 with MAC address of 00:04:6F:11:11:11. We want to limit the bandwidth of the wireless client to 1024 downstream and 512K upstream using AirMax5's Per-User Bandwidth Control.



- Step 1.** Enable Bandwidth Control and select “Per User Bandwidth Control”
- Step 2.** Enter Description for this policy (Wireless Client)
- Step 3.** Select “MAC Address”, then enter the MAC address of the wireless client.
- Step 4.** Enter the downlink speed as “1024” and uplink speed as “512”.
- Step 5.** Click on “Add” button to add the bandwidth policy
- Step 6.** This new policy should appear on the button. You can enable/disable it.

Bandwidth Control Settings

Enable Bandwidth Control

Total Bandwidth Control

Total Downlink Speed: kbps (Between 64 and 65535 or 0 for unlimited)

Total Uplink Speed: kbps (Between 64 and 65535 or 0 for unlimited)

Per User Bandwidth Control Apply

Per User Control Options

Description: ②

Type: ③

MAC: - - - - -

Downlink Max: kbps (Between 1 and 65535) ④

Uplink Max: kbps (Between 1 and 65535)

ADD ⑤

Select	Description	Type	Rule	Downlink Max (kbps)	Uplink Max (kbps)	Enable
⑥ <input checked="" type="checkbox"/>	Wireless Client	MAC Address	00-4F-6F-11-11-11	1024	512	<input checked="" type="checkbox"/>

DELETE SELECTED

4.2.20 RSSI LED Threshold

Operation Mode -> Setup -> RSSI LED Threshold

The AirMax5 is equipped with 2 LEDs to indicate the signal strength of current connection. It is very useful in helping you to align the antenna. The signal level are classified into 4 levels, you can change the Thresholds (dividing line) between levels in this setting. Please note that the smaller the absolute value of RSSI is, the stronger the signal. For example, -50dB is stronger than -80dB. RSSI level stronger with -60dB is considered a very good connection. This setting only appears in Client and Bridge modes.

- No Signal:** When signal strength is less than “Weak Signal Threshold” (i.e. 85dB). Both LED are off.
- Weak Signal:** When signal strength is greater or equal than the “Weak Signal Threshold” (i.e. -75dB). Only the Blue LED is on.
- Strong Signal:** When signal strength is greater or equal than the “Strong Signal Threshold” (i.e. -55dB). Only the Green LED is on.
- Full Signal:** When signal strength is greater or equal than the “Full Signal Threshold” (i.e. -45dB). Both Green and Blue LEDs are on

● Strong

● Weak

● Link

● Power

RSSI Signal setting for Antenna Alignment:

	Threshold
Weak signal:	-80
Strong signal:	-60
Full signal:	-50

Apply
DEFAULT

Be sure to read **Chapter 7: Antenna Alignment** for more information.



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

4.3 WDS Settings

Operation Mode -> Setup -> WDS Settings

WDS Bridge mode can make Point-to-Point and Multi-Point connections. Because of its faster performance, it is frequently used to build point-to-point bridge connection and backbone networks. In a WDS network, each node can *have up to 4 connections*. However, the total number of devices in a WDS network should not exceed 8. Currently, the WDS Bridge mode can only use WEP encryptions policy.

TIPS: For step-by-step instructions on how to build a WDS bridge network, please be sure to read through *Chapter 9: WDS Bridge Example* for details.

In this section, we will talk about the WDS Settings which is available only in WDS Bridge (Pure MAC) mode. WDS Bridges are using BSSID (AP's Wireless MAC address) to authenticate each other. Therefore, it is necessary to know the remote Bridge's wireless MAC addresses. You can always do a "Site Survey" to find out the MAC Addresses.

When you click on WDS settings, the following screen will appear:

WDS Settings

Additional configurations for WDS bridge mode:

WEP key

Prepare the WEP keys for the wireless network.
On Pure MAC mode, all the bridges shared the four keys.

WEP Key 1	WEP152-ASCII	1234567890abcdef
WEP Key 2	WEP152-ASCII	1234123440abcdef
WEP Key 3	WEP152-ASCII	1234562334abcdef
WEP Key 4	WEP152-ASCII	1234567890233def

Name:

SSID:

MAC address: -----

Select Security Policy:

Select	Name	SSID	MAC Address	Security	WEP key Index
-	-	-	-	-	-

Here are the encryption key settings for WEP. Please make sure all bridges in the WDS network enter the same keys.

This is where you enter the remote Bridge's information. The SSID must be different between each Bridge.

After you add a remote Bridge, it will be display here. Up to 4 entries are possible

- ❑ **WEP Key:** You can set up to 4 keys, each key can have different Key Length and Key type. When you add an entry to the WDS setting and select WEP encryption, the system will ask you which key to use. All devices on the network must have the same sets of keys, but each link can have use different key. We recommend using WEP-152 whenever possible for better security.

- ❑ **Adding a new WDS link**

The WDS link are created by entering the remote Bridge's information. This process must be repeated on both side of the bridge.

- **Name:** This is the name for the WDS Link. You can enter any name for your own reference (i.e. WarehouseLink).
- **SSID:** SSID is the network ID for the wireless link. If you have more than one WDS link or if you want to make WDS connection with Mikrotik devices, this field is required. Each WDS Link must have a different SSID name. If you only have one WDS link, you can leave this field empty.
- **MAC Address:** Please enter the remote bridge's wireless MAC address in this field. This wireless SSID can be found on the device label. You can also use Site Survey function to assist you.
- **Select Security Settings:** You can choose to use WEP encryption for better security. It is necessary to enter the same set of keys in the same WDS network. When you select WEP, the AirMax5 will ask you to select from one of the 4 keys. Please be sure to select the same key on both side of the link.
- Press **Add** to finish

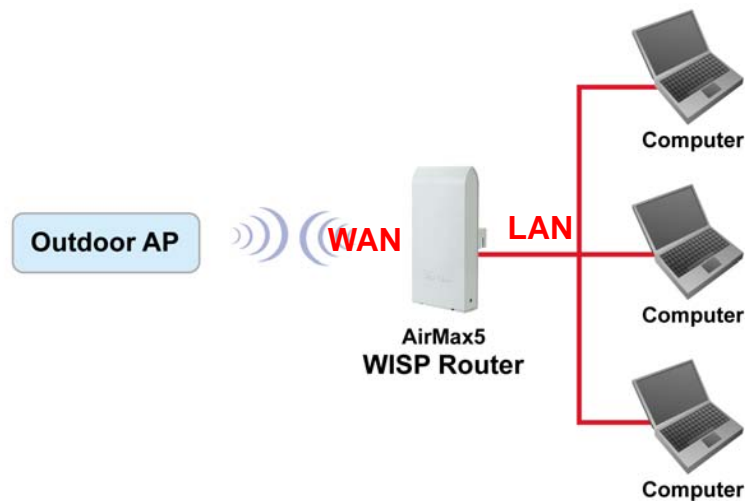
4.4 Router Mode Settings

Operation Mode -> Setup

This section will explain WAN port settings and other functions that are available only in WISP router and AP Router mode.

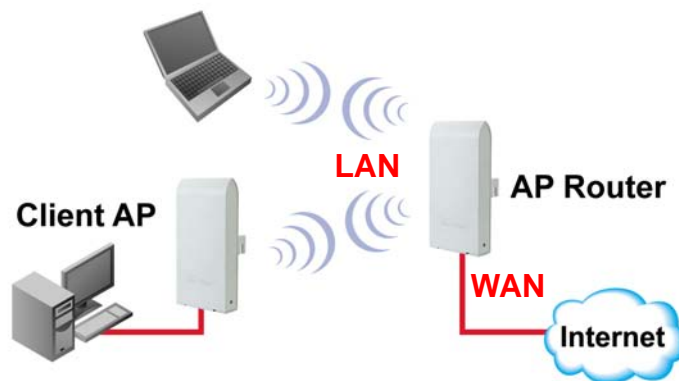
4.4.1 WISP Router Mode

The WISP Router mode is also known as Client Router. The wireless side is connected to the remote AP as in Client Infrastructure mode. Between the wireless and LAN is the IP sharing router function. This is used to share WISP connection. The WAN is on the wireless side.

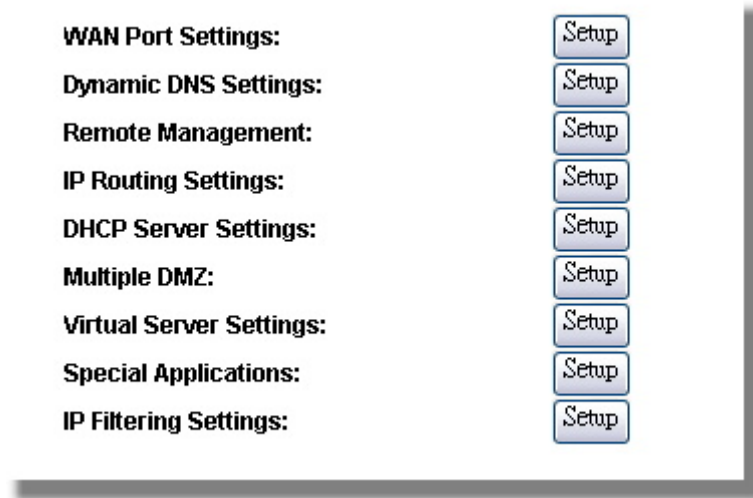


4.4.2 AP Router Mode

In AP Router mode, the POE port of the AirMax5 will turn into the WAN port. The wireless interface will become the LAN side. It will turn AirMax5 into a wireless router. Since the Ethernet interface becomes WAN; if your PC is connected to the POE port, the management IP will change to the WAN IP (192.168.2.1). The remote management will be automatically turned on to allow you managing the device from the POE WAN port.




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



4.4.3 WAN Port Settings

Operation Mode -> Setup -> WAN Port Settings

The AirMax5 support different authentication and IP assignment standards for the WAN port. It includes fixed IP, DHCP, PPPoE and PPTP protocols. Please consult with your ISP about what authentication type is used for the WAN port connection.

 **WAN Port Settings**

If your ISP has assigned you a **static IP** address, select this button and enter the information below:

IP Address Assigned by Your ISP:

IP Subnet Mask:

ISP Gateway IP Address:

DNS IP Address:

If your ISP already provides you with **PPPoE** authentication information, select this button and enter the information below:

User Name:

Password:

Service name:

Connection Type: ▼

MTU: Bytes (128-1500)

MRU: Bytes (1-1500)

Session Type: ▼

- **Clone MAC Address:** Some service provider (Cable Modem provider) lock to certain MAC address. In this situation, the WAN port of AirMax5 need to clone the MAC address. Please check the “Clone MAC address” box and enter the address that need to be cloned.

Cloned MAC Address :


If your ISP requires you to use a specific WAN Ethernet MAC address, check this box and enter the MAC address here.

MAC Address: - - - - -

4.4.4 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. AirMax5 provide Dynamic DNS client using DynDNS, please visit <http://www.dyndns.org> for detail.


 **Dynamic DNS Settings**

Enable Dynamic DNS Client using [DynDNS.org](http://www.dyndns.org)

Hostname:

Username:

Password:

 [Help](#)

4.4.5 Remote Management Settings

Operation Mode -> Setup -> Remote Management

Remote Management allows administrator to manage the AirMax5 from WAN side. You can also change the management port and other settings here.

- **HTTP Port No:** The default port for HTTP is Port 80, you can change the value here
- **Timeout:** The default management timeout is 10 minutes. After timeout, the AirMax5 will ask you to login again. You can change the timeout value here.
- **HTTP Web Server Access:** You can enable or disable HTTP service from WAN side

- **HTTPS Web server Access:** You can enable or disable HTTPS Web Server Access from WAN side
- **Response to WAN ping:** You can disable or enable whether AirMax5 will response to PING command.

Remote Management Settings

HTTP Port No.: timeout: minutes

HTTP Web Server Access

HTTPS Web Server Access

Response to WAN Ping

4.4.6 IP Routing Settings

Operation Mode -> Setup -> IP Routing Settings

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

IP Routing Settings

Dynamic Routing

Select the routing protocol scheme used for the router's LAN / WAN port.

Disable

RIP

Static Routing

This allows you to manually configure static network routes. Static routes will override routes learned by standard routing protocol discover methods.

Destination IP Address: . . .

Subnet Mask: . . .

Gateway IP Address: . . .

Interface:

Metric Count:

To add a static route, enter the information above and click **ADD**.

IP Routing Table

Select	Destination IP Address	Subnet Mask	Gateway IP Address	Interface	Flag	Metric
-	192.168.1.0	255.255.255.0	-	lan	U	0
-	239.0.0.0	255.0.0.0	-	lan	U	0

- **Dynamic Routing:**
Select the routing protocol scheme used for the router's LAN / WAN port.
- **Static Routing:**
This allows you to manually configure static network routes. Static routes will override routes learned by standard routing protocol discover methods.
- **IP Routing Table:**
To delete a static route from the table, select the route and click DELETE SELECTED.

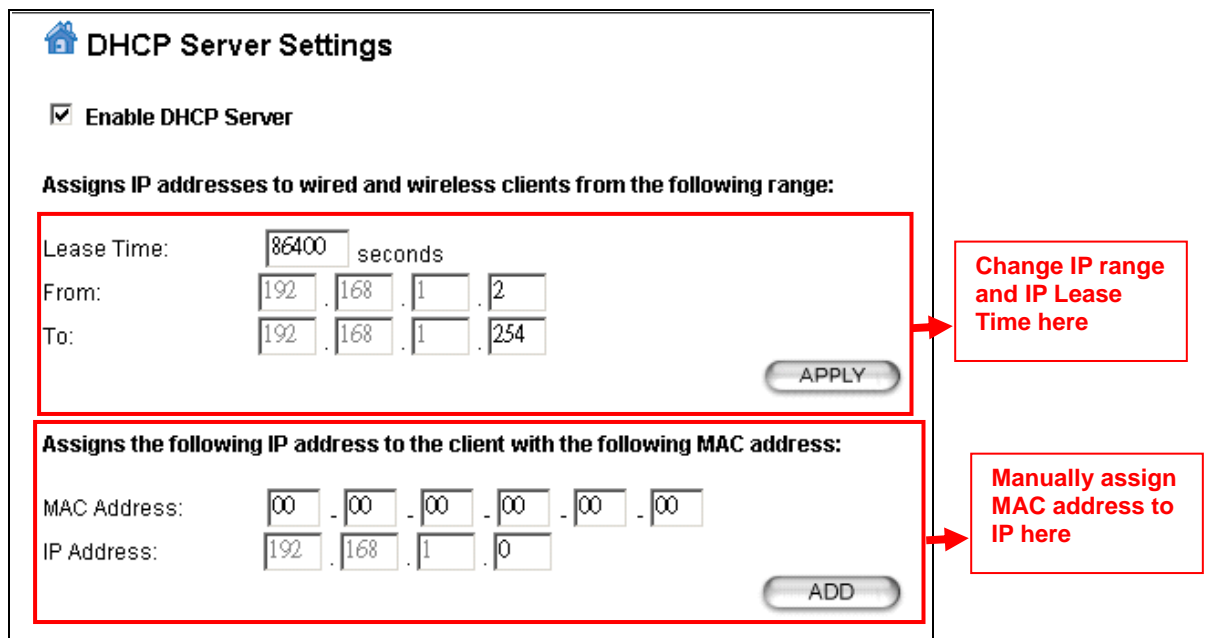
Note: Changes to the routing table will take effect immediately.

4.4.7 DHCP Server

Operation Mode -> Setup -> IP Routing 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 AirMax5 is 192.168.1.1, changing AirMax5's IP address will also change the DHCP server's IP subnet.

You can also lock IP address to MAC address manually; the DHCP server will keep the IP for the MAC address.



The screenshot shows the 'DHCP Server Settings' page. It includes a checked 'Enable DHCP Server' option. Below, there are two main sections:

- Assigns IP addresses to wired and wireless clients from the following range:** This section contains a 'Lease Time' field set to 86400 seconds, and 'From' and 'To' IP address ranges. The 'From' range is 192.168.1.2 and the 'To' range is 192.168.1.254. An 'APPLY' button is located to the right of these fields.
- Assigns the following IP address to the client with the following MAC address:** This section contains a 'MAC Address' field with six boxes (00, 00, 00, 00, 00, 00) and an 'IP Address' field with four boxes (192, 168, 1, 0). An 'ADD' button is located to the right of these fields.

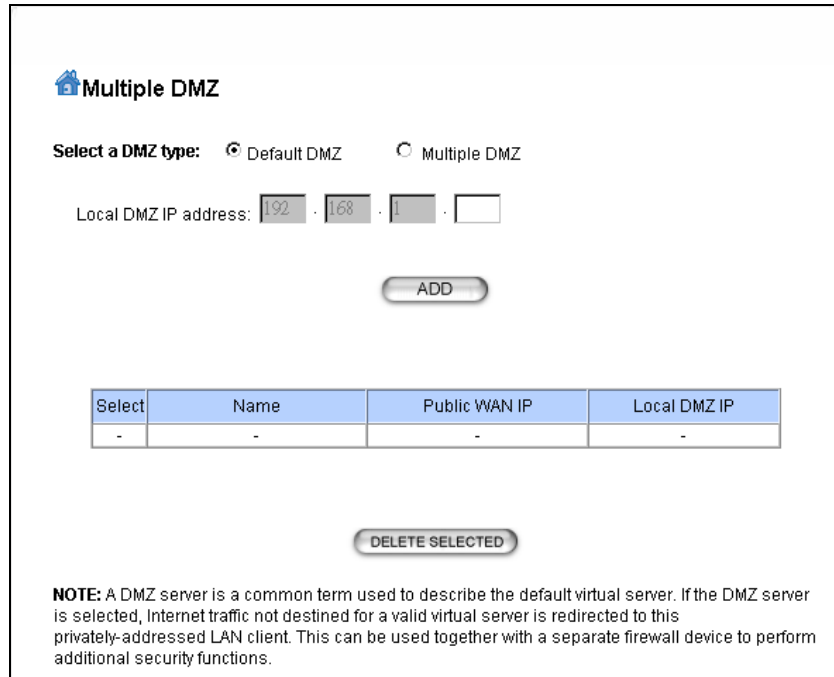
Two red callout boxes with arrows point to specific areas:

- One callout box points to the IP range and lease time fields, containing the text: "Change IP range and IP Lease Time here".
- Another callout box points to the MAC and IP address fields, containing the text: "Manually assign MAC address to IP here".

4.4.8 Multiple DMZ

Advanced Settings >> Multiple DMZ

Multiple DMZ opens all TCP/UDP ports to particular IP address on the LAN side. It allows setting up servers behind the AirMax5.



Multiple DMZ

Select a DMZ type: Default DMZ Multiple DMZ

Local DMZ IP address: . . .

ADD

Select	Name	Public WAN IP	Local DMZ IP
-	-	-	-

DELETE SELECTED

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

Select a DMZ type 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.

4.4.9 Virtual Server Settings

Advanced Settings >> Virtual Setting

This allows you to specify one or more applications running on server computers on the LAN that may be accessed by any Internet user. Internet data destined for the specified public port will be directed to the specified private port number on the LAN client with the specified private IP address. For step-by-step example on Virtual Server settings, please go to section 10.2.2.

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.

Service Name: HTTP

Public Port No.: Single 80
 Range [] ~ []

Local IP Address: 192 . 168 . 1 . []

Local Port No. Starts From: 80

ADD

Select	Service	Public Port No(s)	Local IP Address	Local Port No(s)
-	-	-	-	-

DELETE SELECTED

4.4.10 Special Applications

Advanced Setting >> Special Applications

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

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

Special Applications

Some Internet applications such as Instant Messaging or Games in particular use groups of ports, and are not easy to work behind a firewall. To work well with these special applications we will open ports to let traffic pass through. Before you set up special application, please see your applications' help for such information.

Select an Application: -- select one --

Name: []

Trigger Ports: []

Trigger Protocol: BOTH

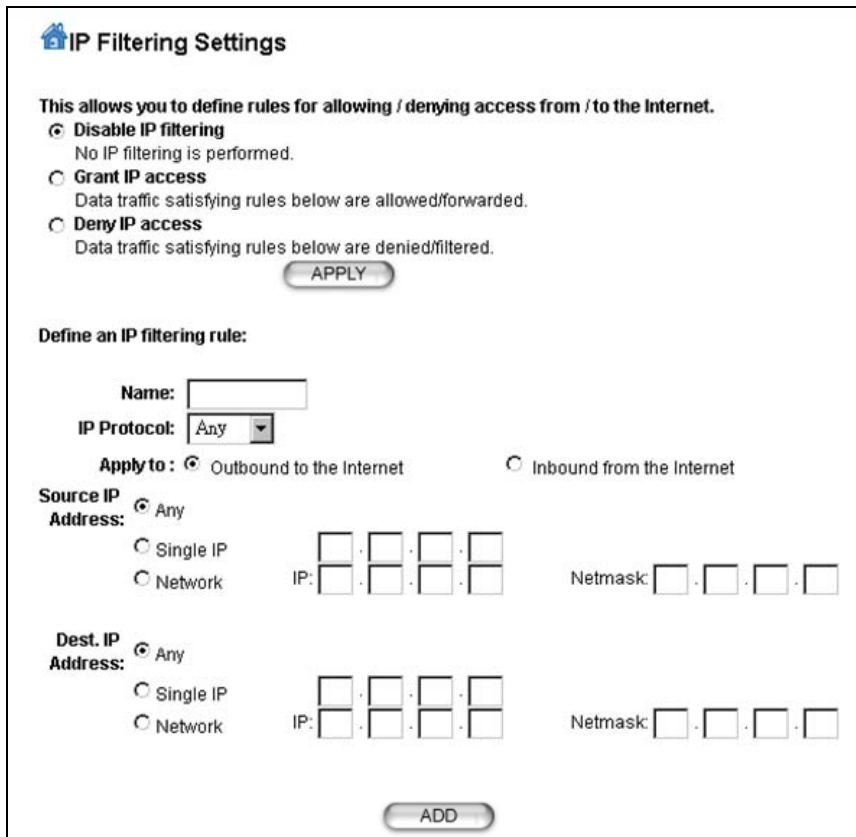
Opened Ports: [] ~ []

Opened Protocol: BOTH

4.4.11 IP Filtering Settings

Advanced Setting>>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.



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

Please do set both inbound/outbound in order to get complete connection. Only inbound or outbound will not allow to get response from the destination IP.

Disable IP filtering: No IP filtering is performed.

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

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

You can also define IP filtering rule, such as:

Name; IP Protocol; Apply to either Outbound to the Internet or Inbound from the Internet; Source IP Address and Dest. (Destination) IP Address.

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

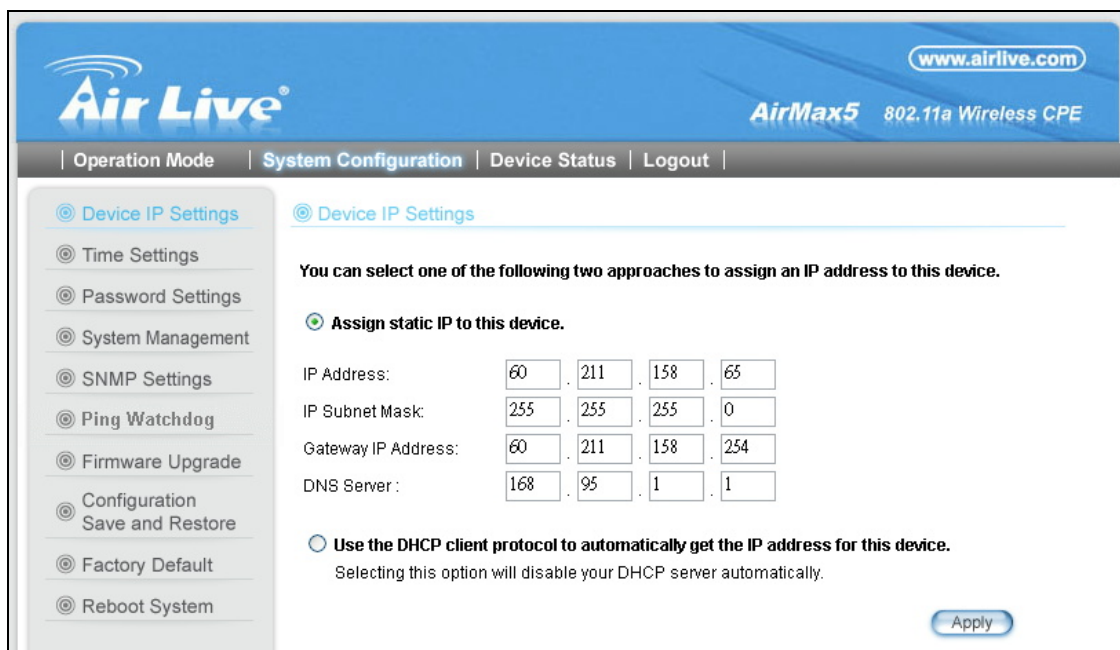
5

Web Management 2: 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.



The screenshot shows the 'Device IP Settings' page in the Air Live web management interface. The page title is 'Device IP Settings' and it includes a navigation menu with 'Operation Mode', 'System Configuration', 'Device Status', and 'Logout'. The main content area is titled 'Device IP Settings' and contains the following text: 'You can select one of the following two approaches to assign an IP address to this device.' There are two radio button options: 'Assign static IP to this device.' (which is selected) and 'Use the DHCP client protocol to automatically get the IP address for this device.' Below the static IP option, there are four input fields for IP Address (60, 211, 158, 65), IP Subnet Mask (255, 255, 255, 0), Gateway IP Address (60, 211, 158, 254), and DNS Server (168, 95, 1, 1). An 'Apply' button is located at the bottom right of the form.

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. Although you can rely on a DHCP server to assign an IP address to the AIRMAX5 automatically, it is recommended that you configure a static IP address manually in most applications.

Device IP Settings

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

Assign static IP to this device.

IP Address: . . .

IP Subnet Mask: . . .

Gateway IP Address: . . .

DNS Server : . . .

Use the DHCP client protocol to automatically get the IP address for this device.
Selecting this option will disable your DHCP server automatically.

Assign Static IP to the Device

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

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

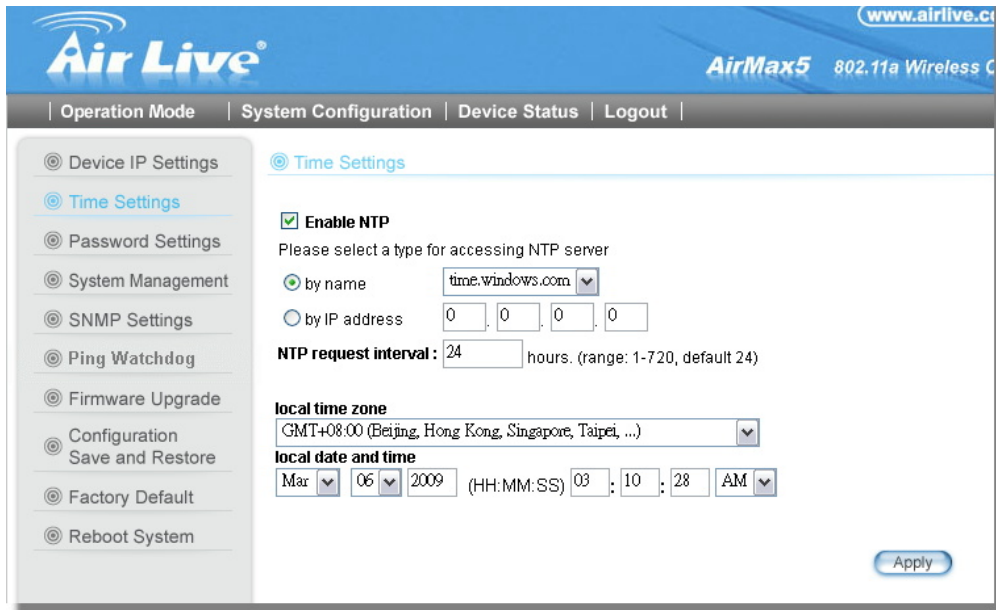
Use DHCP Client Protocol to Get IP automatically

If you choose to use a DHCP Server to acquire an IP address for the AIRMAX5 automatically, enable the checkbox “Use the DHCP client protocol to automatically get the IP address for this device”. Then click Next to go to the next screen. As a reminder, you might lose the IP address of AirMax5 when IP is assigned dynamically.

5.1.2 Time Settings

System Configuration ->Time Settings

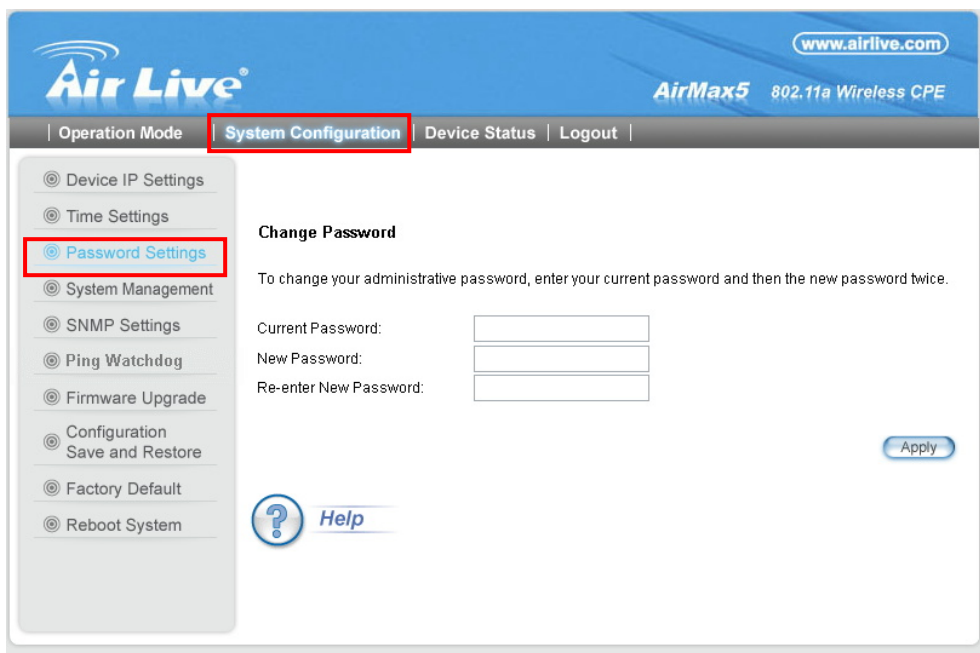
It is important that you set the date and time for your AirMax5 so that the system log will record the correct date and time information. We recommend you choose “Enable NTP” so the time will be keep even after reboot. If your AirMax5 is not connected to Internet, please enter the time manually. Please remember to select your local time zone and click “Apply” to finish.



5.1.3 Password Settings

System Configuration ->Time Settings

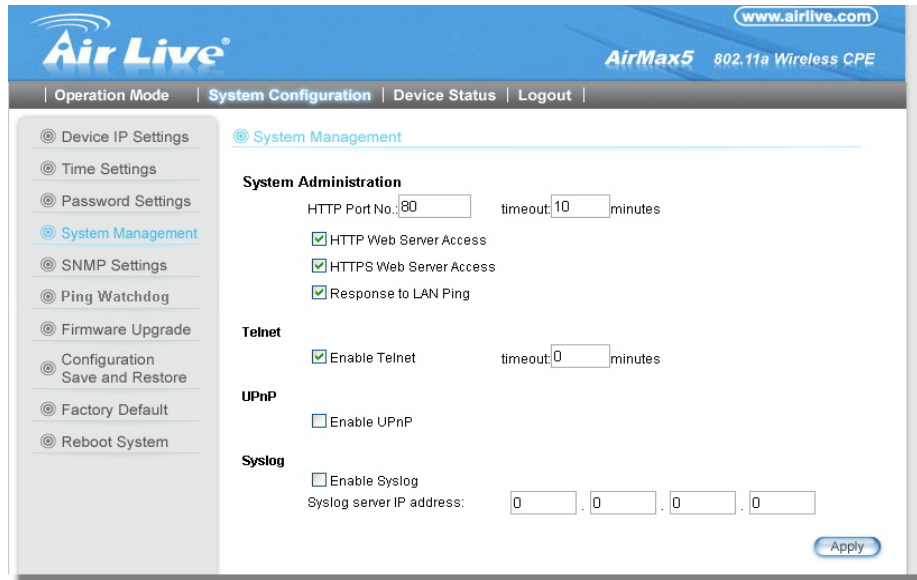
To change password, please go to “System Configuration” -> “Password Settings” menu.



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 Air Live web management interface for an AirMax5 802.11a Wireless CPE. The page is titled "System Management" and includes a navigation menu on the left with options like "Device IP Settings", "Time Settings", "Password Settings", "System Management", "SNMP Settings", "Ping Watchdog", "Firmware Upgrade", "Configuration Save and Restore", "Factory Default", and "Reboot System". The main content area is divided into sections: "System Administration" (HTTP Port No: 80, timeout: 10 minutes, checkboxes for HTTP/HTTPS Web Server Access and Response to LAN Ping), "Telnet" (checkbox for Enable Telnet, timeout: 0 minutes), "UPnP" (checkbox for Enable UPnP), and "Syslog" (checkbox for Enable Syslog, Syslog server IP address: 0.0.0.0). An "Apply" button is located at the bottom right.

System Administration

- **HTTP Port No:** The default port for HTTP is Port 80, you can change the value here
- **Timeout:** The default management timeout is 10 minutes. After timeout, the AirMax5 will ask you to login again. You can change the timeout value here.
- **HTTP Web Server Access:** You can enable or disable HTTP service from WAN side
- **HTTPS Web server Access:** You can enable or disable HTTPS Web Server Access from WAN side
- **Response to WAN ping:** You can disable or enable whether AirMax5 will response to PING command.

Telnet: Disable/Enable Telnet Interface. It is recommend that you disable the Telnet interface and use SSH instead

UPnP: Click here to enable UPnP. It is recommended not to open UPnP for security reason.


Syslog: Syslog is an IETF (Internet Engineering Task Force - the Internet standards body)-conformant standard for logging system events (RFC-3164). When the AIRMAX5 encounters an error or warning condition (ie., a log-in attempt with an invalid password), it will create a log in the system log table. To be able to remotely view such system log events, you need to check the *Enable Syslog* box and configure the IP address of a Syslog daemon. When doing so, the AIRMAX5 will send logged events over network to the daemon for future reviewing.

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

5.1.5 SNMP Settings

System Configuration -> SNMP Settings

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

 **SNMP Settings**

Enable SNMP

Assign system information:

System Name:

System Location:

System Contact:

Assign the SNMP community string:

Community String For Read:

Community String For Write:

Assign a specific name and IP address for your SNMP trap manager:

Name:

IP Address:

- **System Name:** A name that you assign to your 802.11a+g Router. It is an alphanumeric string of up to 30 characters.
- **System Location:** Enter a system location.
- **System Contact:** Contact information for the system administrator responsible for managing the AirMax5. It is an alphanumeric string of up to 60 characters.
- **Community String For Read:** If you intend the router to be managed from a remote SNMP management station, you need to configure a read-only “community string” for read-only operation. The community string is an alphanumeric string of up to 15 characters.
- **Community String For Write:** For read-write operation, you need to configure a write “community string”.

■ **Assign a specific name and IP address for your SNMP trap manager:**

A trap manager is a remote SNMP management station where special SNMP trap messages are generated (by the router) and sent to in the network.

You can define trap managers in the system.

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

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

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

5.1.6 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. To prevent the AP from power recycling, the PING watchdog will start 10 minutes after power up to prevent power recycle problem.

⊙ Ping Watchdog

The Ping Watchdog will ping up to 2 IP addresses for connection status. If the remote IP addresses do not respond to Ping, the device will either reconnect or power reboot .

Enable
 Disable

IP Address 1: . . . (Must fill)

IP Address 2: . . . (Optional)

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

Failed tries: (default is 2 tries)

Action:

Note: Watchdog will take effect 10 minutes after startup. IP Address 2 is optional, when filled, both IP Address 1 and IP Address 2 must fail to respond for watchdog to take action.

- **PING Frequency** means: "How often the CPE will PING". For example, it will PING once every "1" minute.
- **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 "2" minutes and Fail Tries to "2". It means the CPE will ping every 2 minutes, after the second failure, it will reconnect.


Actions:

- Reconnect: the AirMax5 will attempt to re-establish the connection. It is recommend to use this option for WDS Bridge connection.
- Reboot: the AirMax5 will do a power recycle.

5.1.7 Firmware Upgrade

System Configuration -> Firmware Upgrade

can upgrade the firmware of your AIRMAX5 (the software that controls your AIRMAX5'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.



The screenshot shows a web interface titled "Firmware Upgrade". It includes a home icon, the title "Firmware Upgrade", and instructions: "Select the firmware file by clicking **Browse**, then click **UPGRADE**." Below this is a text input field and a "Browse..." button. To the right is an "UPGRADE" button. A "NOTE:" section contains two red warnings: "1. Do not power off the router while upgrading the firmware." and "2. Some browsers would fail to locate the firmware file when there is any localized character in the firmware file path." At the bottom left is a "Help" link with a question mark icon.

- **Upgrade Firmware:**

To update the AIRMAX5 firmware, first download the firmware from AirLive web site to your local disk, and then from the above screen enter the path and filename of the firmware file (or click **Browse** to locate the firmware file). Next, Click the **Upgrade** button to start.

The new firmware will be loaded to your AIRMAX5. After a message appears telling you that the operation is completed, you need to reset the system to have the new firmware take effect.



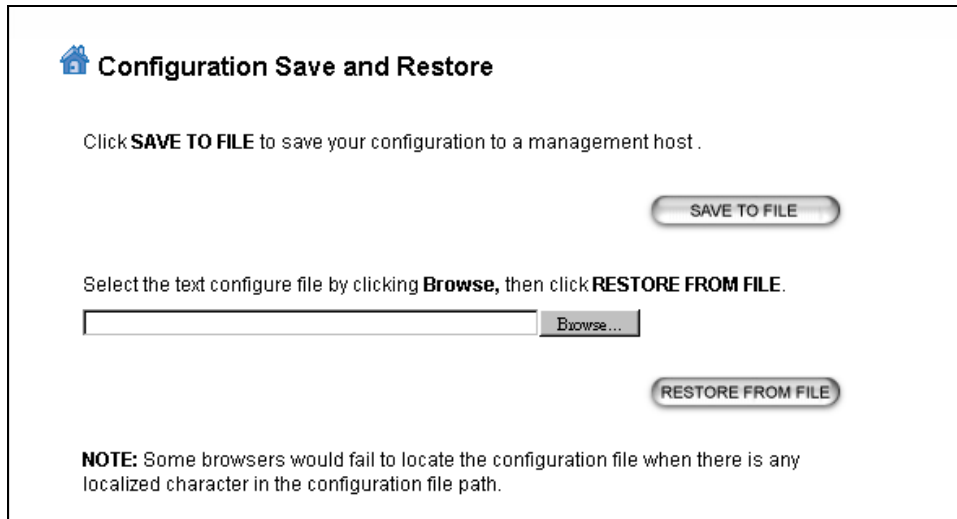
Do not power off the device while upgrading the firmware. It is recommended that you do not upgrade your AIRMAX5 unless the new firmware has new features you need or if it has a fix to a problem that you've encountered.

5.1.8 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 AIRMAX5 by following the steps.

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



The screenshot shows a web interface titled "Configuration Save and Restore". It contains the following elements:

- A home icon followed by the title "Configuration Save and Restore".
- Text: "Click **SAVE TO FILE** to save your configuration to a management host."
- A button labeled "SAVE TO FILE".
- Text: "Select the text configure file by clicking **Browse**, then click **RESTORE FROM FILE**."
- An input field with a "Browse..." button next to it.
- A button labeled "RESTORE FROM FILE".
- A **NOTE**: "Some browsers would fail to locate the configuration file when there is any localized character in the configuration file path."

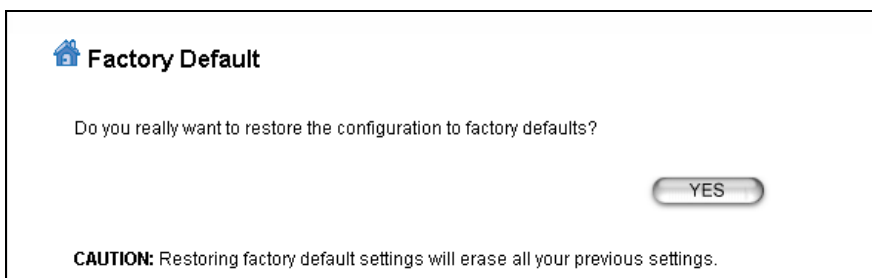
Step 2 Enter the path of the configuration file to save-to/restore-from (or click the *Browse* button to locate the configuration file). Then click the *SAVE TO FILE* button to save the current configuration into the specified file, or click the *RESTORE FROM FILE* button to restore the system configuration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

5.1.9 Factory Default

System Configuration -> Factory Default

You can reset the configuration of your AIRMAX5 to the factory default settings.

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



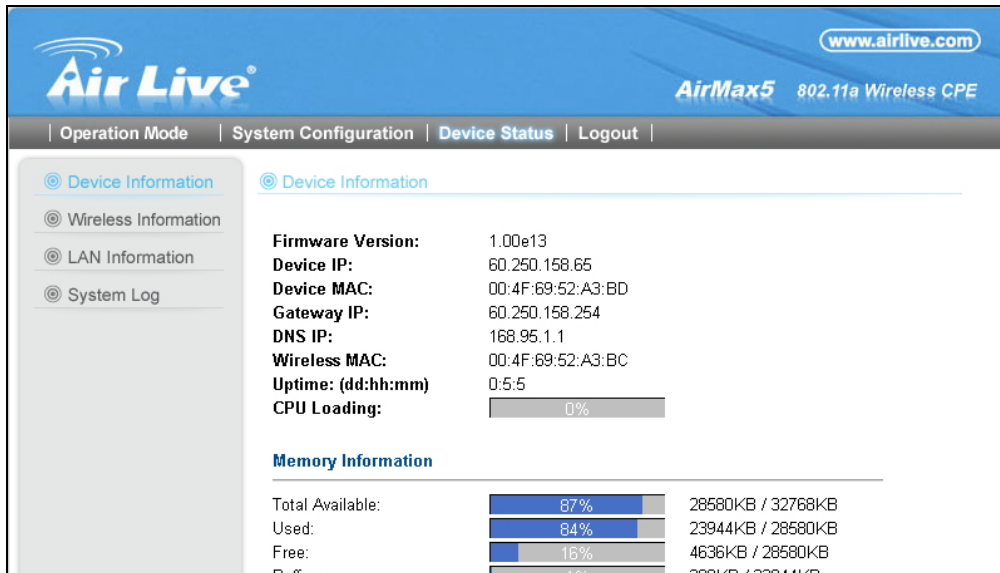
The screenshot shows a confirmation dialog titled "Factory Default". It contains the following elements:

- A home icon followed by the title "Factory Default".
- Text: "Do you really want to restore the configuration to factory defaults?"
- A button labeled "YES".
- A **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.



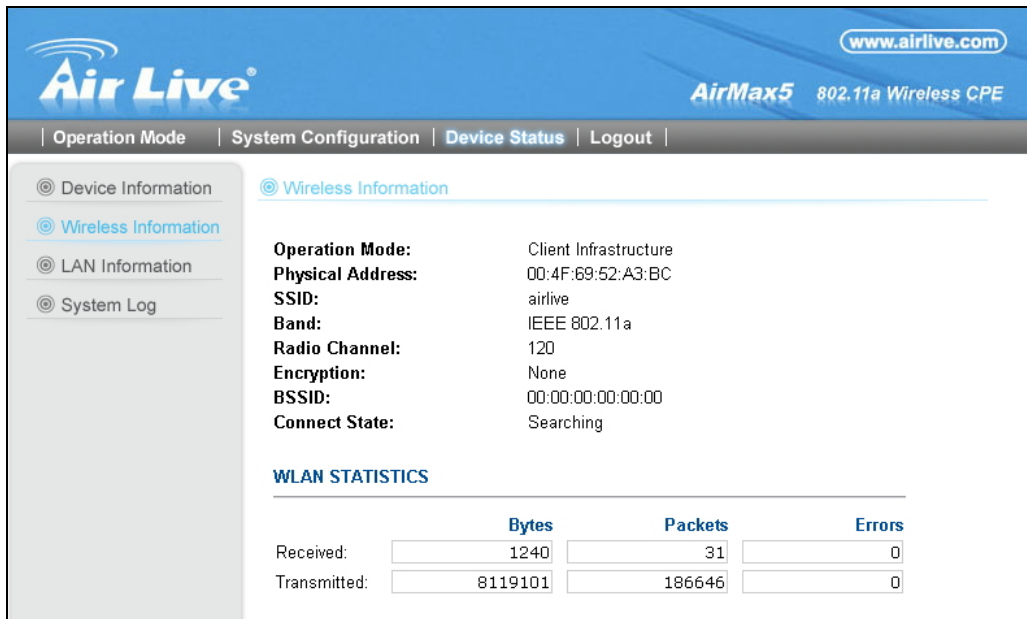
5.2.1 Device Information

This page shows the general information about AirMax5 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:** The first AirMax5 firmware release is 1.00e10. In general, AirLive will refer to its firmware as exx (such as e10) version on the release note
- **Wireless MAC:** This is the wireless MAC address (BSSID) of this AiMax5. This is the address to enter on the remote WDS Bridge for the WDS link.
- **Uptime:** This is the time that the AirMax5 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, RSSI, Remote device’s BSSD, connecting State, channel, and encryption used.



The screenshot shows the Air Live web interface for the AirMax5 802.11a Wireless CPE. The page is titled "Wireless Information" and displays the following details:

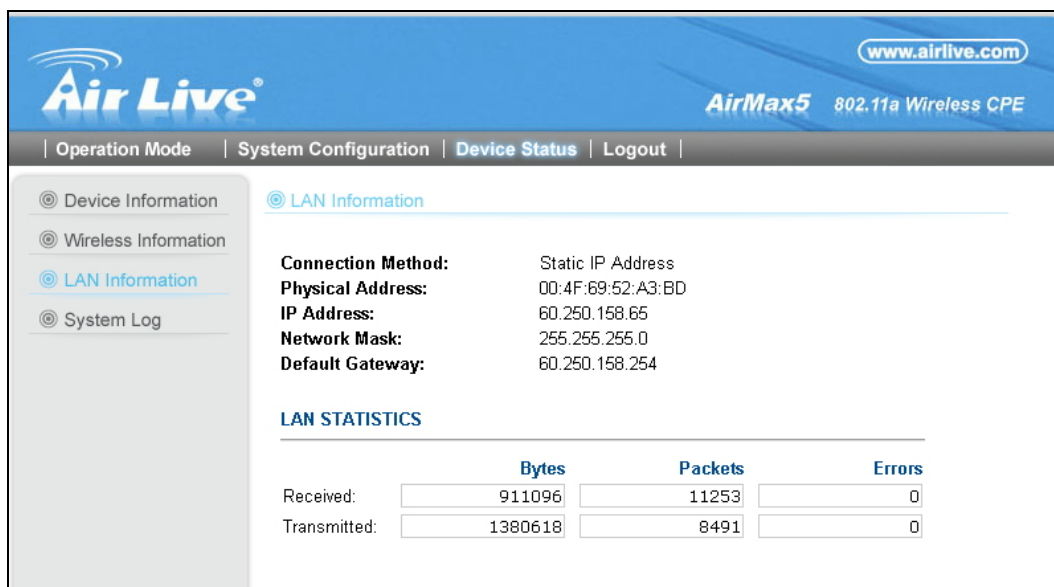
- Operation Mode:** Client Infrastructure
- Physical Address:** 00:4F:69:52:A3:BC
- SSID:** airlive
- Band:** IEEE 802.11a
- Radio Channel:** 120
- Encryption:** None
- BSSID:** 00:00:00:00:00:00
- Connect State:** Searching

Below the details is a "WLAN STATISTICS" table:

	Bytes	Packets	Errors
Received:	1240	31	0
Transmitted:	8119101	186646	0

5.2.3 Internet Information

This page shows the information about WAN port of the AirMax5. It includes the type of WAN port authentication used and the IP address information about the WAN port.



The screenshot shows the Air Live web interface for the AirMax5 802.11a Wireless CPE. The page is titled "LAN Information" and displays the following details:

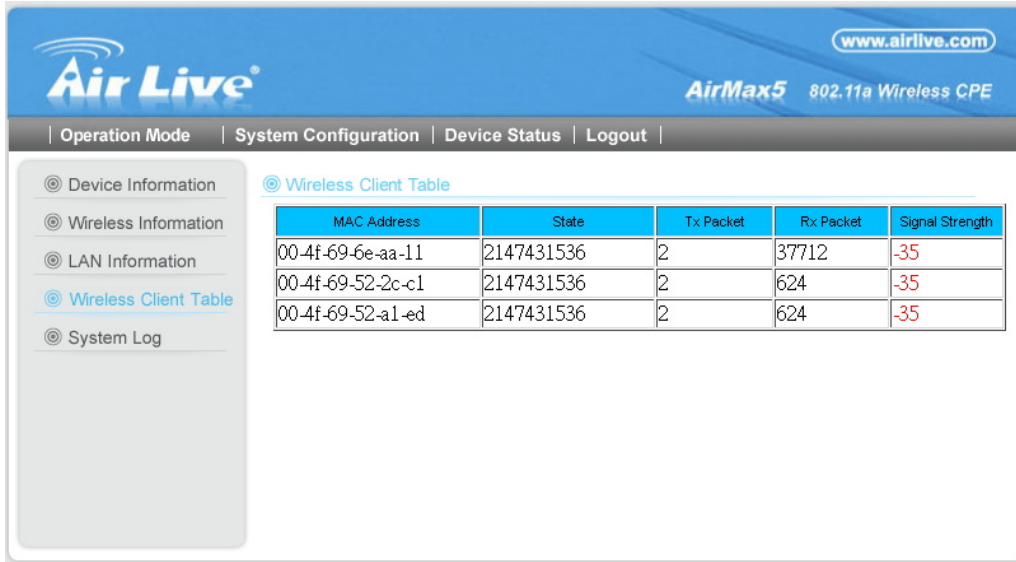
- Connection Method:** Static IP Address
- Physical Address:** 00:4F:69:52:A3:BD
- IP Address:** 60.250.158.65
- Network Mask:** 255.255.255.0
- Default Gateway:** 60.250.158.254

Below the details is a "LAN STATISTICS" table:

	Bytes	Packets	Errors
Received:	911096	11253	0
Transmitted:	1380618	8491	0

5.2.4 Wireless Client Table

This function is available in AP mode and AP Router mode only. It displays the information about wireless clients that are associated with AirMax5. It includes signal strength, TX and RX data rate, MAC address, and the state.

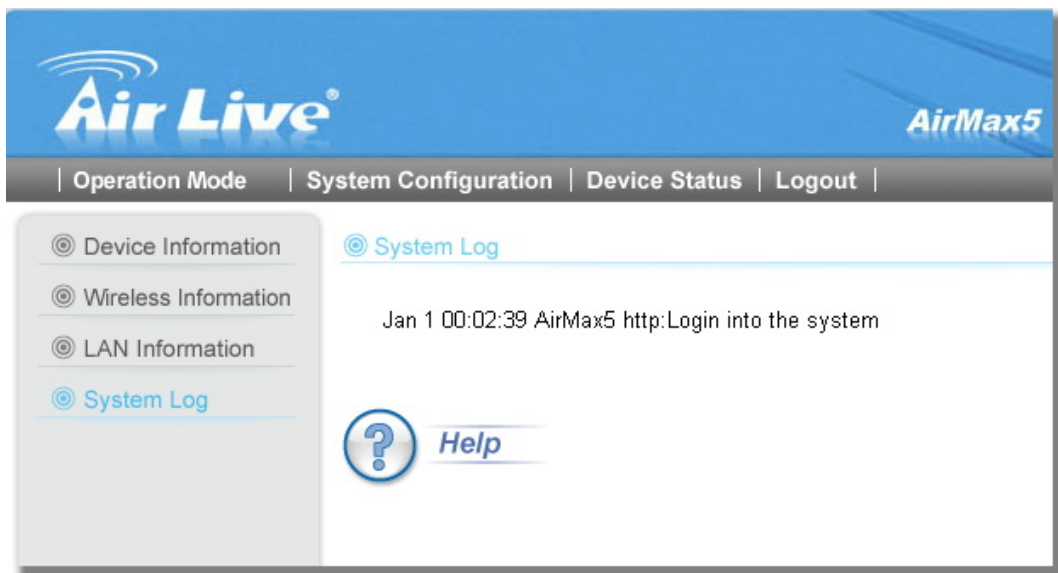


The screenshot shows the Air Live web management interface. The top navigation bar includes the Air Live logo, the website URL www.airlive.com, and the device model AirMax5 802.11a Wireless CPE. Below the navigation bar, there are tabs for Operation Mode, System Configuration, Device Status, and Logout. The main content area is divided into a left sidebar with menu items: Device Information, Wireless Information, LAN Information, Wireless Client Table (selected), and System Log. The main content area displays the Wireless Client Table with the following data:

MAC Address	State	Tx Packet	Rx Packet	Signal Strength
00-4f-69-6e-aa-11	2147431536	2	37712	-35
00-4f-69-52-2c-c1	2147431536	2	624	-35
00-4f-69-52-a1-ed	2147431536	2	624	-35

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.



The screenshot shows the Air Live web management interface with the System Log selected. The top navigation bar and sidebar are the same as in the previous screenshot. The main content area displays the System Log with the following entry:

Jan 1 00:02:39 AirMax5 http:Login into the system

Below the log entry, there is a help icon (a question mark inside a circle) and the word "Help".