



AC.TOP

11 AC Wide Range Ceiling
Mount PoE Access Point

User's Manual



www.airlive.com



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.

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



FCC Statement

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

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

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

FCC Caution

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

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

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

IMPORTANT NOTE

FCC Radiation Exposure Statement:

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



© 2009 OvisLink Corporation, All Rights Reserved

Table of Contents

1. Introduction.....	1
1.1 Overview.....	1
1.2 Firmware Upgrade and Tech Support	1
1.3 Features	2
1.4 Wireless Operation Modes.....	2
1.4.1 Access Point Mode	2
1.4.2 WDS Repeater Mode.....	3
2. Installing the AC.TOP	4
2.1 Package Content	4
2.2 Knowing your AC.TOP	4
2.3 Hardware Installation	5
2.3.1 Ceiling Mount.....	5
2.3.2 Install in T-Rail Mount.....	6
2.3.3 Power up the AC.TOP.....	8
2.4 LED Indicators	9
3. Configuring the AC.TOP.....	10
3.1 Important Information.....	10
3.2 Prepare your PC	10
3.3 Introduction to IP Finder.....	11
3.4 Introduction to Web Management	12
3.4.1 Getting into Web Management.....	12
3.4.2 Main Menu	13
3.5 Configuring with Setup Wizard.....	14
3.6 Initial Configurations	16
3.6.1 Change the Device's IP Address	16



3.6.2	Set the Time and Date.....	17
3.6.3	Change Password.....	18
4.	Wireless Settings.....	19
4.1	About Wireless Modes.....	19
4.2	Basic Wireless Functions.....	20
4.2.1	Wireless Mode.....	20
4.2.2	Band.....	21
4.2.3	Network Name (SSID).....	22
4.2.4	Broadcast SSID.....	22
4.2.5	Multiple SSID.....	22
4.2.6	Auto Channel.....	23
4.2.7	Channel.....	23
4.2.8	Channel Width.....	24
4.2.9	Wireless Client Limit.....	24
4.2.10	Security.....	25
4.2.11	WMM.....	28
4.2.12	Data Rate.....	28
4.2.13	RF Power.....	28
4.3	Advance Settings.....	29
4.4	Access Control.....	31
4.5	Site Survey.....	31
4.6	WPS.....	33
4.7	Wireless Scheduling.....	34
4.8	RADIUS.....	34
4.8.1	RADIUS Settings.....	35
4.8.2	Internal Server.....	36
4.8.3	RADIUS Accounts.....	37
5.	System Configurations.....	40
5.1	Menu Structure.....	40
5.2	LAN Interface Setup.....	40



5.2.1	DHCP Settings	41
5.2.2	Set Static DHCP	42
5.2.3	Domain Name	42
5.2.4	802.11d Spanning Tree.....	42
5.2.5	Clone MAC Address	42
5.2.6	Enable AirLive IP Finder Management	42
5.3	Time Settings.....	43
5.4	Password Settings.....	43
5.5	Management.....	44
5.6	Firmware Upgrade	45
5.7	Configuration Save and Restore	46
5.8	Factory Default	46
6.	Status Menu	47
6.1	Menu Structure	47
6.2	Device Information.....	48
6.3	Statistic	50
6.4	Log	50
7.	Frequent Asked Questions	52
8.	Specifications	54
8.1	Hardware Features	54
8.1.1	General Hardware Feature	54
8.1.2	Antenna	54
8.1.3	Power Supply.....	54
8.1.4	Dimension and Weight.....	54
8.1.5	Certification.....	54
8.2	Radio Specifications	54
8.2.1	Frequency Band	54
8.2.2	Output Power and Sensitivity	55
8.2.3	TX Output Power	55



8.2.4 Supported WLAN Mode	55
8.2.5 Supported WLAN Encryption	56
8.3 Software Feature	56
8.3.1 Operation Mode	56
8.3.2 Management Interface	56
8.3.3 Advance Functions.....	56
8.4 Environment	56
8.4.1 Environment.....	56
9. Wireless Network Glossary.....	57



1

Introduction



1.1 Overview

The AC.TOP is a ceiling mount wireless multi-function AP based on 1200Mbps 2T2R Wireless AC+ b/g/n MIMO standard radio technologies. It is 2.4G/5G dual band concurrent. The Wireless Access Point is equipped with one Gigabit Auto-sensing Ethernet ports for connecting to LAN and also for cascading to next Wireless Access Point. It has built-in 802.3af PoE port for installation up to 100 meter away from the power source.

1.2 Firmware Upgrade and Tech Support

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

In addition, you might find new firmware that either increase software functions or provide bug fixes for AC.TOP in our website.



1.3 Features

- 1200Mbps 802.11AC+b/g/n Standard
- Up to 23dBm output power (limited to 20dBm in EU)
- Built-in MIMO Antennas
- 8MB Flash and 64MB SDRAM
- 2 wireless multi-function modes: AP, WDS repeater
- 1 x 10/100/1000 Mbps Ethernet Port with IEEE 802.3af PoE support
- Web management
- Easy Setup Wizard
- Wireless Access Control ,Multiple SSID up to 32 and Virtual AP
- Wireless Client Limit, Client Isolation and Watchdog
- IP Finder Management Utility
- AirLive Central Wireless Management
- Green WLAN for Power Saving

1.4 Wireless Operation Modes

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

AC.TOP Wireless Operation Mode			
Wireless Mode	Radio 5G	Radio 2.4G	Application
Access Point	AP	AP	Hotspot (Indoor and Outdoor)
WDS Repeater	WDS	WDS	Extend distance of another WDS AP/Router

AC.TOP are dual radio device, you also can change the operation mode for each radio. Each radio can be set to difference Operation Mode such as AP mode in 2.4G and WDS repeater mode in 5G

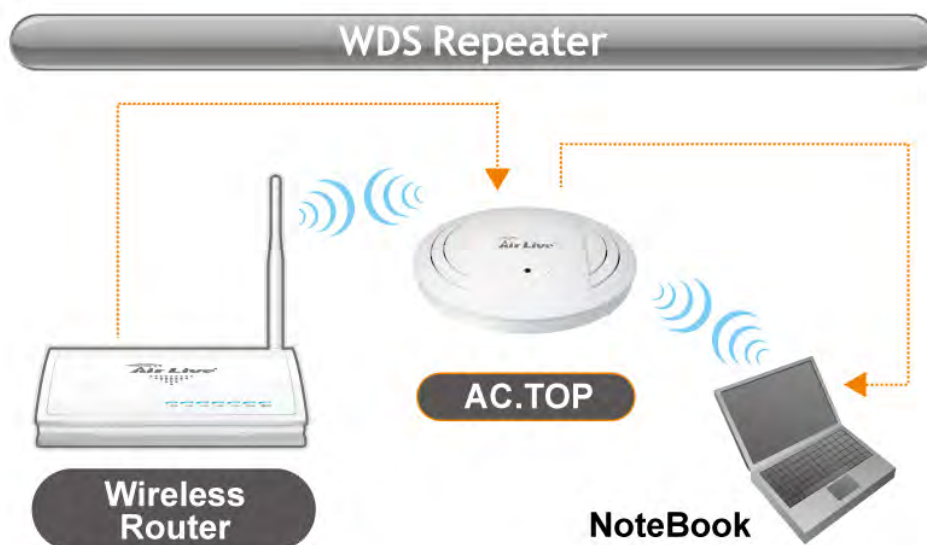
1.4.1 Access Point Mode

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



1.4.2 WDS Repeater Mode

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





2

Installing the AC.TOP

This section describes the installation procedure for the AC.TOP. It starts with a summary of the content of the package you have purchased, followed by steps of how to power up and connect the AC.TOP. Finally, this section explains how to configure a Windows PC to communicate with the AC.TOP.

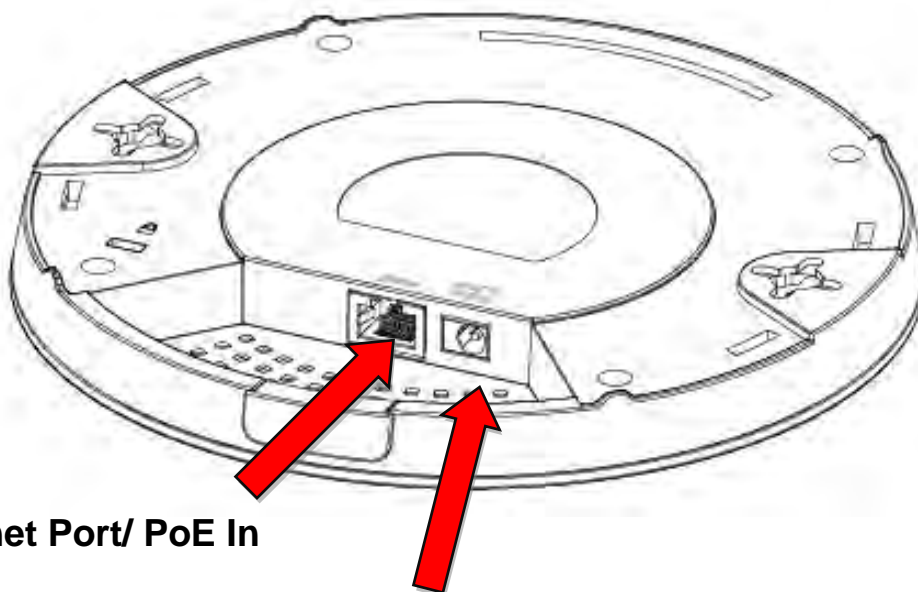
2.1 Package Content

The AC.TOP package contains the following items:

- One AC.TOP main unit
- One 12V DC power adapter
- One CD of the AC.TOP
- Quick Installation Guide

2.2 Knowing your AC.TOP

Below are descriptions and diagrams of the product:



Ethernet Port/ PoE In

Power Jack (DC IN)



2.3 Hardware Installation

*Note	Before you starting hardware connection, you are advised to find an appropriate location to place the Access Point. Usually, the best place for the Access Point is at the center of your wireless network, with line of straight to all your wireless stations.
--------------	--

There are two methods to mound the AC.TOP. Ceiling mount and T-rail Mount

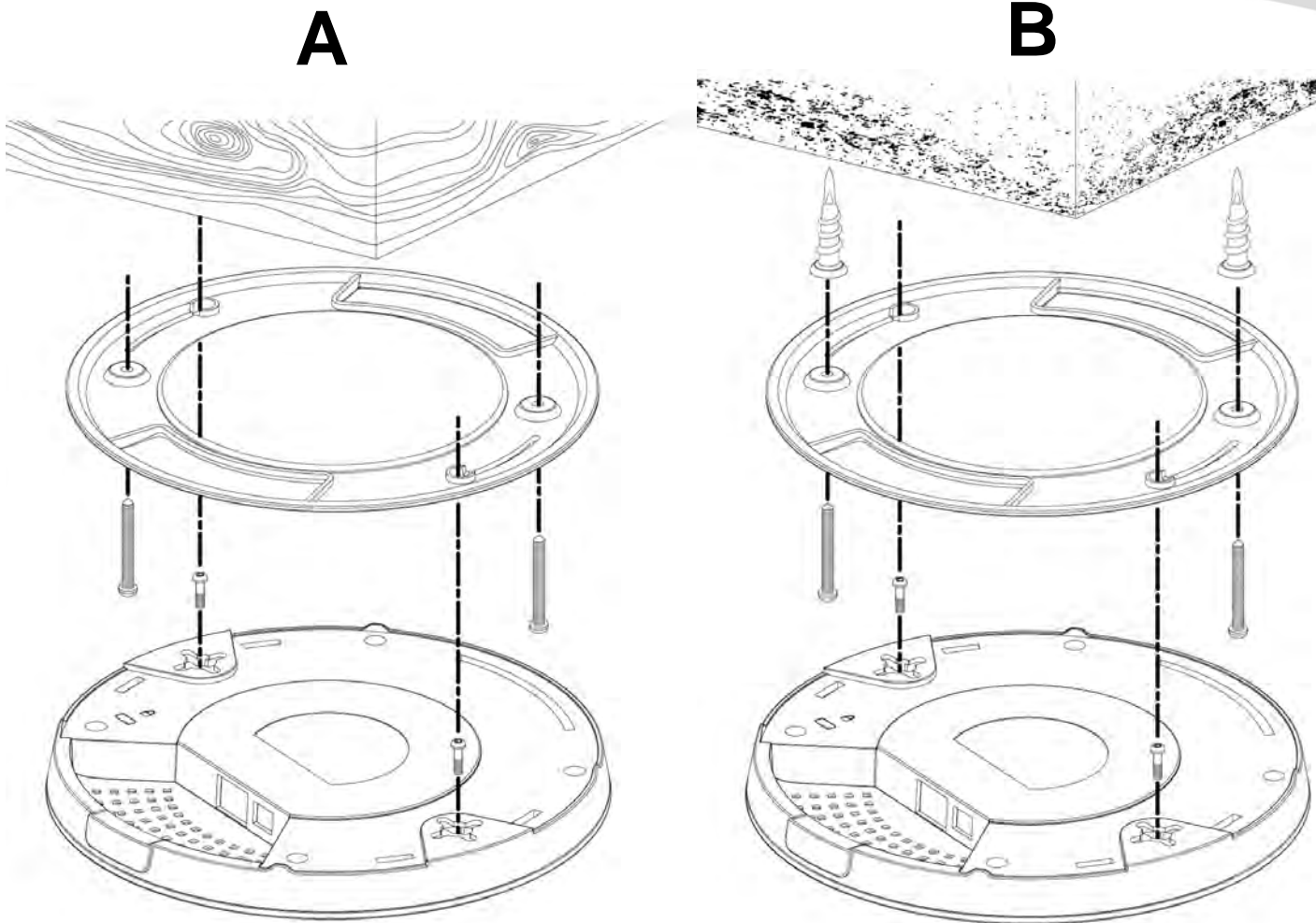
2.3.1 Ceiling Mount

If you want to mount the AC.TOP into wood ceiling

1. Place the ceiling mount bracket to a ceiling in your desired location and insert screw through hole (x 2) and tighten to fix the bracket in place.
2. When the ceiling bracket is in place, inset screw into hole (x 2) on the access point.
3. Fix the access point to the ceiling bracket by inserting the attached screws into hole and twisting the access point.
4. Lock the access point firmly into place when by twisting it to align screws with the grooves in the ceiling mount.

If you want to mount the AC.TOP into other ceilings

1. Place the ceiling mount bracket to a ceiling in your desired location and insert screw through hole (x 2) and tighten to fix the bracket in place, as shown in **A**.
2. Insert screw through hole and into the rear of screw and tighten to provide additional strength.
3. When the ceiling bracket is in place, insert screw into hole (x 2) on the access point.
4. Fix the access point to the ceiling bracket by inserting the attached screws into hole and twisting the access point.
5. Lock the access point firmly into place by twisting it to align screws with the grooves in the ceiling mount.



2.3.2 Install in T-Rail Mount

To mount the access point to a T-Rail, please follow the instructions below and refer to diagram **C**, **D** & **E**.

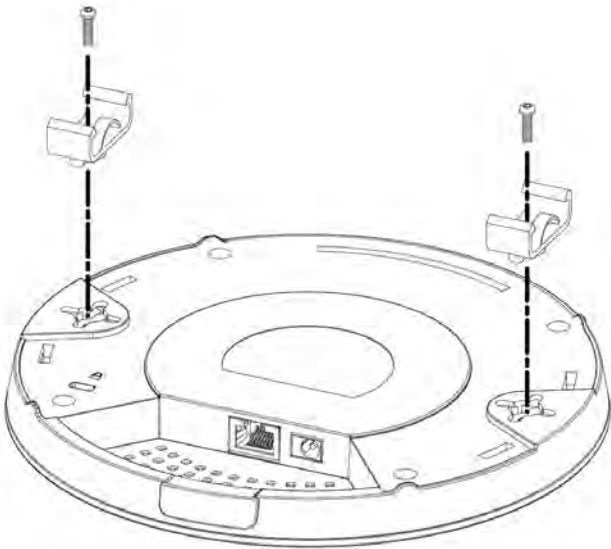
1. Select the correct size T-Rail bracket from the two sizes which are included in the package contents.
2. Attach the T-Rail bracket to hole using screw (x 2) as shown in **C**.



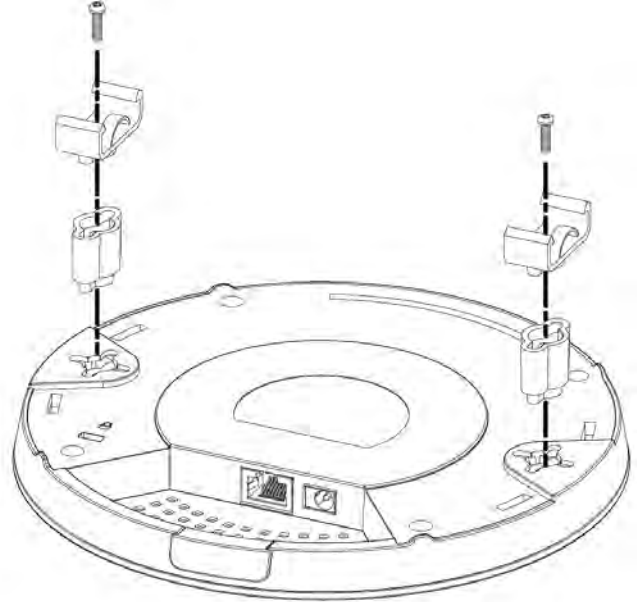
If you need more space between the access point and the T-Rail, then additionally use bracket between bracket and hole (x 2), and use the longer screws (x 2) included in the package contents.

3. Clip the access point onto your T-Rail using the now attached T-Rail bracket.

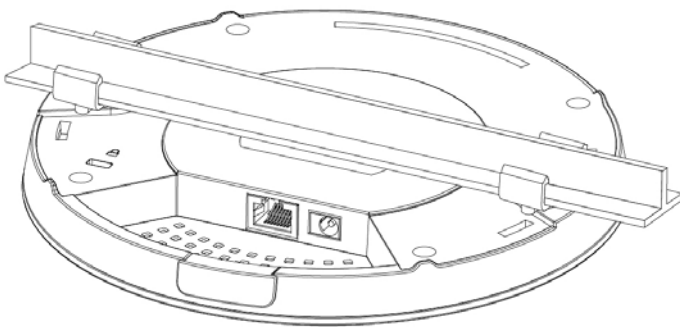
C



D



E



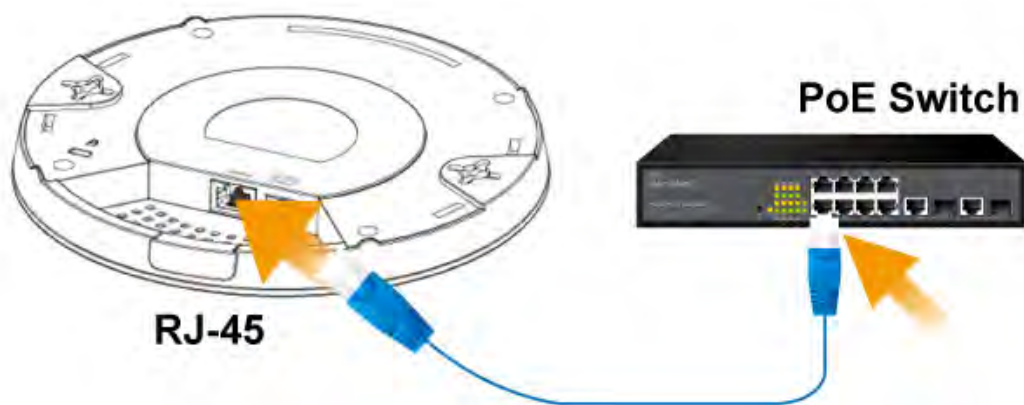


2.3.3 Power up the AC.TOP

There are two way to power up the AC.TOP

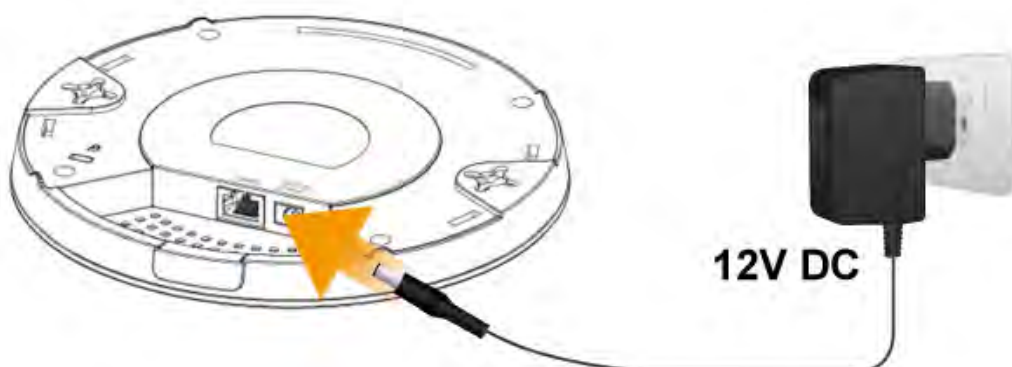
1. Power by PoE

AC.TOP is equipped with 802.3at compliant PoE port. You can select AirLive PoE-48PB v2 or PoE switch such as POE-GSH2004L-370 for the deployment of the PoE network environment. The POE-48PB v2 and POE-GSH2004L-370 is an optional accessory that must be purchased separately. **You must use Cat.5E or better graded Ethernet Cable for PoE Installation.**



2. Power by Power Adapter

Connect 12V adaptor to Power up the AC.TOP



Do not use the power adapter if you are using a PoE switch.



2.4 LED Indicators

This section describes the LED behavior of AC.TOP.
You can find the LED in front of the AC.TOP.



LED Color	LED Status	Description
Blue	On	The access point is starting up.
Purple	On	The access point is on.
Amber	Flashing	Error.
Off	Off	The access point is off.



3

Configuring the AC.TOP

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

3.1 Important Information

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

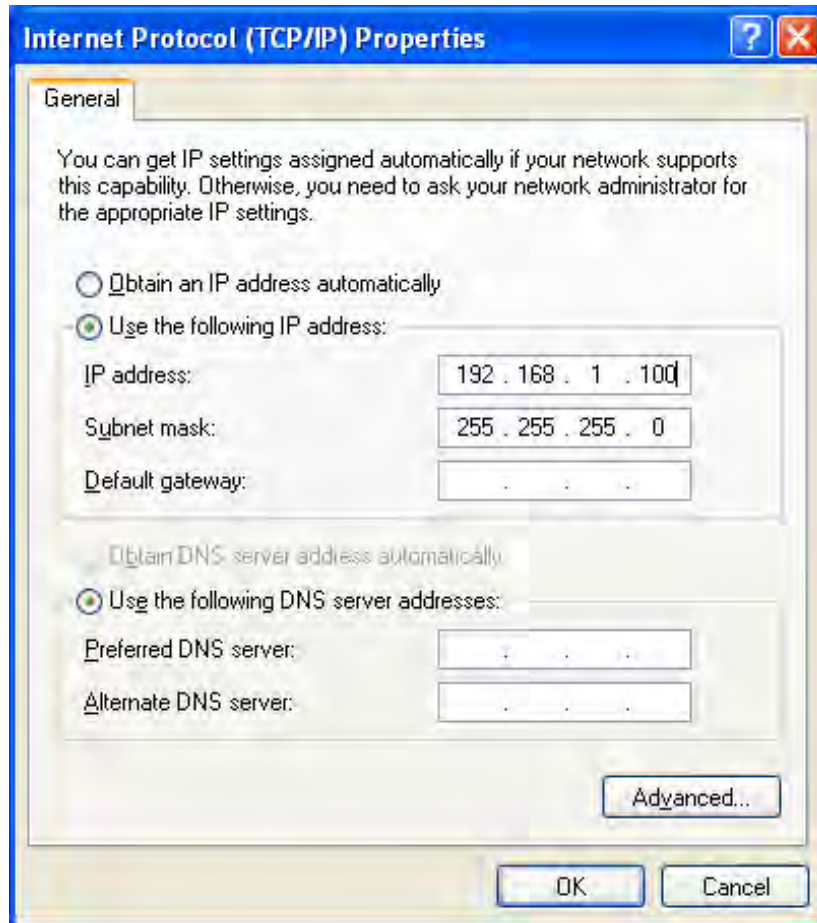
- The default IP address is: **192.168.1.254** Subnet Mask: **255.255.255.0**
- The default user's name is: **admin**
- The default password is: **airlive**
- The default SSID for 2.4G is: **airlive**
- The default SSID for 5G is: **airlive 5g**
- The default wireless mode is : **AP mode**
- After power on, please wait for 1 minutes for AC.TOP to finish boot up
- Please remember to click on "**Apply**" for new settings to take effect
- You must reboot the AC.TOP after you finish all the settings for changes to take effect**
- By Default, the DHCP server is turned off, please to configure your PC's IP address manually.

3.2 Prepare your PC

The AC.TOP can be managed remotely by a PC through either the wired or wireless network. The default IP address of the AC.TOP is **192.168.1.254** with a *subnet mask* of 255.255.255.0. This means the IP address of the PC should be in the same subnet of the AC.TOP.

To prepare your PC for management with the AC.TOP, please do the following:

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



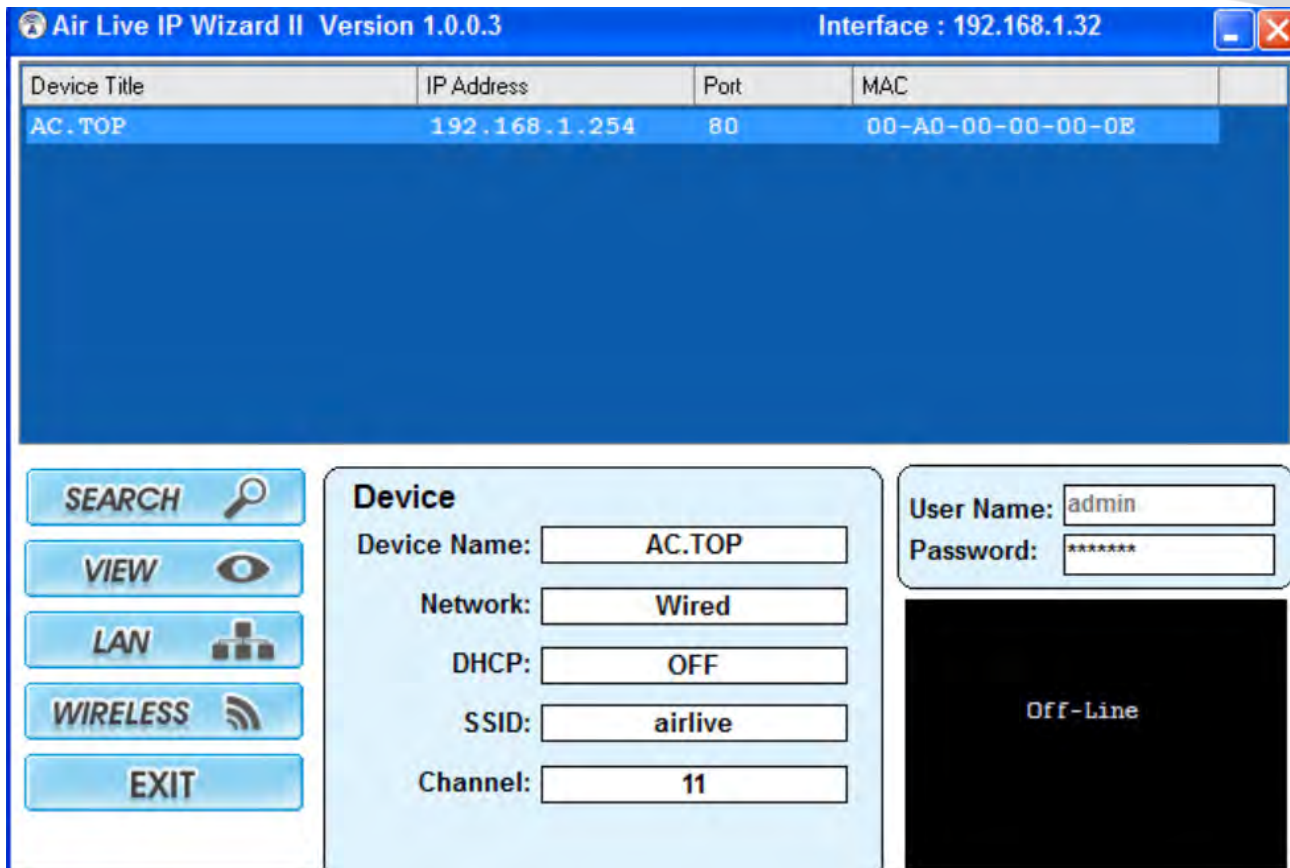
You are ready now to configure the AC.TOP using your PC.

3.3 Introduction to IP Finder

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

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

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



- **Search:** By clicking Search, IP Finder will try to discover the AC.TOP on the network.
- **View:** The function is for IP Camera only. It does not work for AC.TOP.
- **Exit:** Click to close IP Finder.

3.4 Introduction to Web Management

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

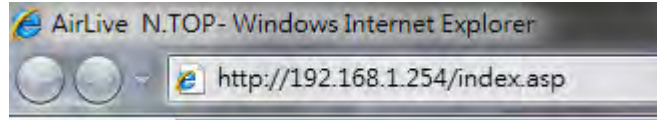
If you are placing the AC.TOP behind router or firewall, you might need to open the port 80 at virtual server on your firewall/router. This procedure is not necessary in most cases unless there is a router/firewall between your PC and AC.TOP.

3.4.1 Getting into Web Management

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



- To get into the Normal Web Management, simply type in the AC.TOP's IP address (default IP is **192.168.1.254**) into the web browser's address field.



3.4.2 Main Menu

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

The screenshot displays the AirLive web management interface for an AC.TOP device. The page title is "AC.TOP 11 AC wide range Ceiling Mount PoE Access Point". The navigation menu includes "Wizard", "Wireless", "System", "Status", and "Reboot". The main content area shows the "Wireless 5G Settings" page with the following configuration options:

- Enable Wireless LAN Interface
- Wireless Mode: WDS Repeater
- Band: 5 GHz (802.11 ac/a/n)
- SSID: TOOP5G
- Broadcast ESSID: Enable
- Multiple SSID: Setup
- Auto Channel: Disable
- Channel: Ch 36, 5.18GHz
- Channel Width: Auto 80/40/20 MHz
- Wireless Client Limit: 32
- Security: Setup
- Data Rate: Auto
- RF Power: 90 %
- WDS: Setup

Buttons for "Apply" and "Cancel" are visible at the bottom of the settings area.

- **Wizard:**

The wizard will guide you to configure access point for first time. Please follow the setup wizard step by step.



- **Wireless:**

You will find all the settings for wireless settings in this page. The AC.TOP's wireless settings are different between wireless modes.

- **System:**

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.

- **Status:**

This section for monitoring the status of AC.TOP. It provides information on device status, Ethernet status, wireless status, wireless client table, and system log.

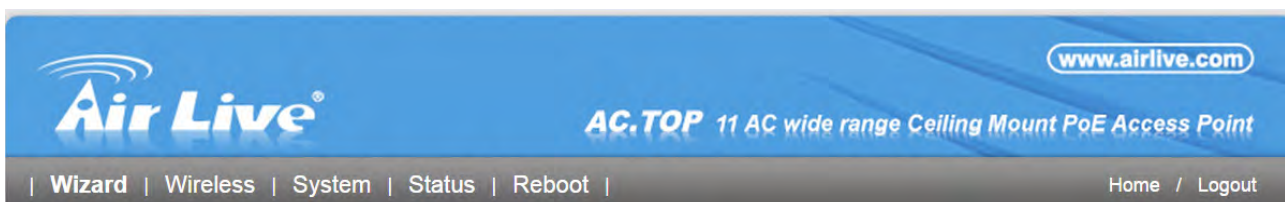
- **Reboot:**

Please remember to save changes and reboot after you finish all settings. The changes will take effect only after reboot.

3.5 Configuring with Setup Wizard

You can browse to activate the Setup Wizard

Step1: Login the Web UI of AC.TOP, select “**Wizard**” for basic settings with simple way.



Step2: Select wireless mode that you deserved, and click “**Next**” to continue.

Setup Wizard



Step 1: Select Wireless Mode

Mode

- Access Point
- WDS Repeater

next



Use this mode to extend the wireless coverage of another AP/Router. The remote AP/Router must also have WDS function. The wireless MAC addresses of the PC are preserved in this mode.

Step3: Setup your wireless settings for 2.4G band such as **SSID**, **Wireless Channel** and **Encryption Key**...etc, and click “**Next**” to apply the setting or click on “**Previous**” to the previous settings.



Step 2: Wireless Settings (2.4GHz)

Enable Wireless LAN Interface

Band: 2.4 GHz (B+G+N) ▼

SSID: AceTop24

Auto Channel: Disable ▼

Channel: Ch 3 ▼

Channel Width: 40 MHz, +Ch 7 ▼

Broadcast ESSID: Enable ▼

Encryption Key: 1234567890

previous

next



In this mode, the AC.TOP will act as a center hub for the wireless network. Please choose this mode if you already have a router and want to create a new wireless network.



Step 4: Setup your wireless settings for 5G band such as **SSID**, **Wireless Channel** and **Encryption Key**...etc, and click “**Finish**” to apply the setting or click on “**Previous**” to the previous settings.

Step 3: Wireless Settings (5GHz)

Enable Wireless LAN Interface

Band

SSID

Auto Channel

Channel

Channel Width

Broadcast ESSID

Encryption Key

AP Mode

In this mode, the AC.TOP will act as a center hub for the wireless network. Please choose this mode if you already have a router and want to create a new wireless network.

3.6 Initial Configurations

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

3.6.1 Change the Device's IP Address

The default IP address is at **192.168.1.254**. You should change it to the same subnet as your network. Also, if you want to manage AC.TOP remotely, you have to set the Gateway and DNS server information.

To setup the IP settings for AC.TOP, please select “System” -> LAN Interface Setup”. After entering the IP information, click on “Apply Changes” to finish.

1

| Wizard | Wireless | **System** | Status | Reboot |

LAN Interface Setup

IP Address Assignment Static IP

Device Name test

IP Address 192.168.1.254

IP Subnet Mask 255.255.255.0

Default Gateway User-Defined 192.168.1.254

DHCP Disabled

DHCP Leased Time One Hour

DHCP Client Range 192.168.1.120 - 192.168.1.140 Show Client

Static DHCP Set Static DHCP

DNS1 8.8.8.8

DNS2

Domain Name AC.TOP

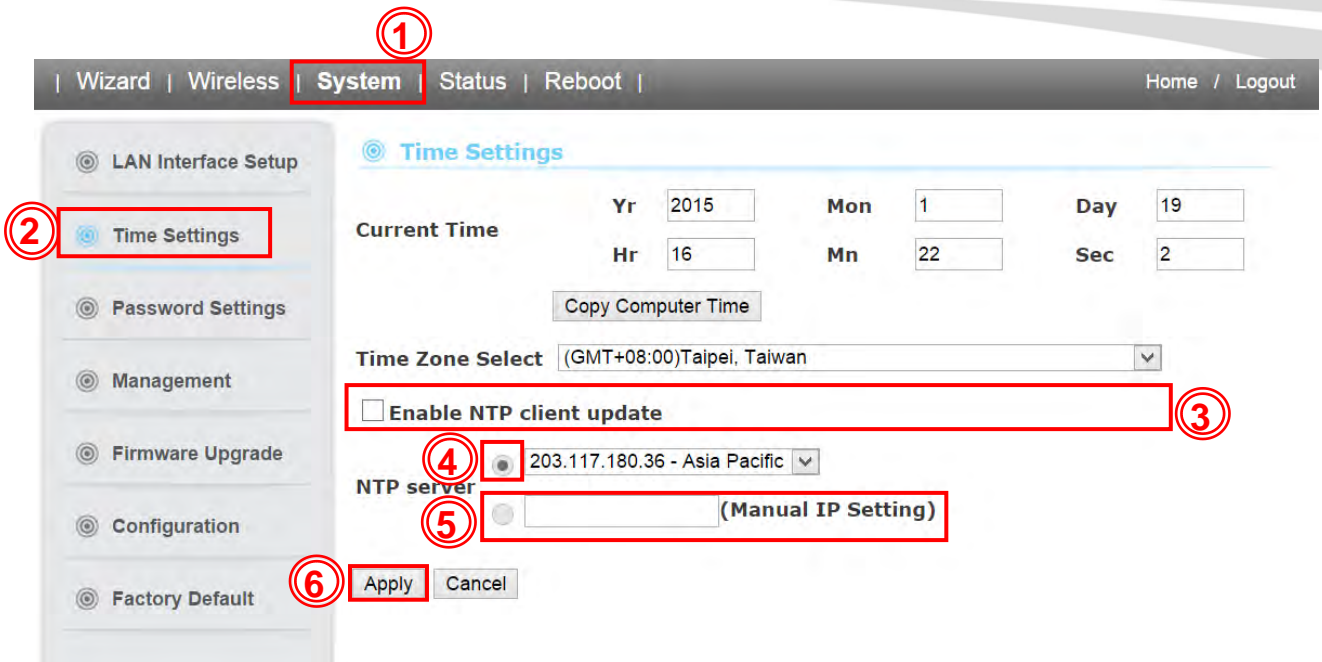
Enable AirLive IP Finder Management

Apply Cancel

2

3.6.2 Set the Time and Date

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



3.6.3 Change Password

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





4

Wireless Settings

In this chapter, we will explain about the wireless settings in web management interface. Please be sure to read through Chapter 1's Wireless Operation Mode and Chapter 3's "Introduction to Web Management" and "Initial Configurations" first.

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

4.1 About Wireless Modes

The AC.TOP has 2 operation modes to suit different application requirements. In this section, we will explain how to change between wireless operations modes. For explanation on each different operation mode, please read Chapter 1 section 1.4 first.

Below is the summary table for different wireless modes:

AC.TOP Wireless Operation Mode			
Wireless Mode	Radio	WAN	Application
Access Point	AP	None	Hotspot (Indoor and Outdoor)
WDS Repeater	AP + Client	None	Extend distance of another WDS AP/Router
Universal Repeater	AP + Client	None	Extend distance of any AP Router

To change between different wireless modes, please to go the "Wireless" menu, on the left hand side bar you can select Wireless 2.4G or Wireless 5G to change the Operation mode for each band, in the webpage you will see the "Wireless Mode" pull down menu which displays the current operation mode.



| Wizard | **Wireless** | System | Status | Reboot |

- Wireless 2.4G
- Wireless 5G
- Advanced Settings
- Access Control
- Site Survey
- WPS
- WLAN Schedule
- RADIUS

Wireless 2.4G Settings

Enable Wireless LAN Interface

Wireless Mode WDS Repeater ▼

Band 2.4 GHz (802.11b/g/n) ▼

SSID AceTop24

Broadcast ESSID Enable ▼

Multiple SSID Setup

Auto Channel Disable ▼

Channel Ch 3 ▼

Channel Width 40 MHz, +Ch 7 ▼

Wireless Client Limit 29 ▼

Security Setup

To change wireless mode, please select the new wireless mode from the pull-down menu and click “apply” button. The AC.TOP will ask you to confirm about the mode change. After your confirmation, the AP will reboot itself to the new mode.

4.2 Basic Wireless Functions

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

When you select “**Wireless**” on the top menu; the following screen will appear:

4.2.1 Wireless Mode

Wireless -> Wireless

There are 2 wireless modes such as AP, and WDS Repeater for you can work in different application environments

- Wireless 2.4G
- Wireless 5G
- Advanced Settings
- Access Control
- Site Survey
- WPS
- WLAN Schedule
- RADIUS

Wireless 2.4G Settings

Enable Wireless LAN Interface

Wireless Mode

Band

SSID

Broadcast ESSID

Multiple SSID

Auto Channel

Channel

Channel Width

Wireless Client Limit

Security

Data Rate

RF Power

4.2.2 Band

Wireless -> Band

AC.TOP has 4 different options in 2.4G band and 3 for 5G band for WLAN transmission.

All devices in the same network should use the same WLAN mode.

- **2.4 GHz (B):** The radio will only connect at 11b mode.
- **2.4 GHz (G):** The radio will only connect at 11g mode.
- **2.4 GHz (B+G):** The radio will auto adjust between 11g and 11b mode.
- **2.4 GHz (B+G+N):** The radio will auto adjust between 11n, 11g and 11b mode. It is recommended to use this mode for 2.4G Band.
- **5 GHz (A):** The radio will only connect at 11a mode.
- **5 GHz (A+N):** The radio will auto adjust between 11a and 11n mode.
- **5GHz (AC+N+A):** The radio will auto adjust between 11ac, 11n and 11a mode. It is recommended to use this mode for 5G Band.



4.2.3 Network Name (SSID)

Wireless -> Network Name (SSID)

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

4.2.4 Broadcast SSID

Wireless Settings -> Broadcast SSID

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

4.2.5 Multiple SSID

Wireless -> Multiple SSID

Multiple SSID allows AC.TOP to create up to **16** different wireless networks (SSID) each band. It is also known as “**Virtual AP**” function. Each SSID can have its Encryption policy and VLAN ID. The SSID1 is the main SSID under Wireless Setting page.

2.4GHz WLAN Multiple ESSID

This page allows you to configure the wireless settings for Multiple ESSIDs. The wireless security settings for these ESSIDs can be configured in Security page.(VLAN ID:0~4094)

Enable SSID number :

NO.	Basic Setting	Advanced Settings		
	SSID	Broadcast SSID	WMM	VLAN ID
ESSID1	<input type="text" value="AceTop24"/>	<input type="text" value="Enable"/> <input type="button" value="v"/>	<input type="text" value="Enable"/> <input type="button" value="v"/>	<input type="text" value="1"/>
ESSID2	<input type="text" value="22"/>	<input type="text" value="Enable"/> <input type="button" value="v"/>	<input type="text" value="Enable"/> <input type="button" value="v"/>	<input type="text" value="2"/>
ESSID3	<input type="text" value="33"/>	<input type="text" value="Enable"/> <input type="button" value="v"/>	<input type="text" value="Enable"/> <input type="button" value="v"/>	<input type="text" value="3"/>
ESSID4	<input type="text" value="44"/>	<input type="text" value="Enable"/> <input type="button" value="v"/>	<input type="text" value="Enable"/> <input type="button" value="v"/>	<input type="text" value="14"/>
ESSID5	<input type="text" value="55"/>	<input type="text" value="Enable"/> <input type="button" value="v"/>	<input type="text" value="Enable"/> <input type="button" value="v"/>	<input type="text" value="8"/>



4.2.6 Auto Channel

When Auto Channel is enable, AC.TOP will automatically select and change wifi channel. In 2.4G radio, AC.TOP will change the channel between 1~11. In 5G radio, user can select the channel Band according to the regulation and AC.TOP will select the channel in the selected band.

4.2.7 Channel

Wireless -> Channel

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

In 802.11 ac/a/n standard, there are four channel can be used in Europ, which are channel 36,40,44,48. Please make sure the client can receive those channel.

Each wireless channel takes between 20 to 40 MHz of frequency width in 2.4G and 20 to 80 MHz in 5G. But the channels are only 5MHz apart in 2.4G. Therefore, only every 5 channels can be free of interference with each other for 2.4G band. It is recommended that you can do a site survey to find about what channels are used by surrounding AP and choose a channel that is not used by other APs.

Channel	Frequency (MHz)	U.S.A.	Europe
1	2412	○	○
2	2417	○	○
3	2422	○	○
4	2427	○	○
5	2432	○	○
6	2437	○	○
7	2442	○	○
8	2447	○	○
9	2452	○	○
10	2457	○	○
11	2462	○	○



12	2467	-	O
13	2472	-	O
14	2484	-	-
36	5180	O	O
40	5200	O	O
44	5220	O	O
48	5240	O	O
149	5745	O	O
153	5765	O	O
157	5785	O	O
161	5805	O	O
165	5825	O	O

 Note: 1. For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible. 2. This device is restricted to indoor use

4.2.8 Channel Width

Wireless -> Channel Width

You can choose 20MHz or 20/40MHz channel width in Wireless 2.4G and 20MHz, 40MHz and Auto (80/40/20 MHz) . Choose 20MHz for compliance with laws in some countries. 40MHz offers faster performance than 20MHz, 80MHz in 5G in order to have 802.11 ac performance.

4.2.9 Wireless Client Limit

Wireless -> Wireless Client Limit

This limitation applies to number of wireless clients the device can associate. If you need to serve wireless connection to large number of users in one location, you can deploy many APs and limit the number of wireless clients, so any additional wireless connection attempt will be rejected (therefore, redirect to other AP). The range of user limitation is from 1 to 32 in each radio. Total users are 64.



4.2.10 Security

Wireless -> Security

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 AC.TOP features various security policies including WEP, 802.1x, WPA, WPA Personal, WPA2, WPA2 Personal and WPA Radius.

Wireless 2.4G Settings

Enable Wireless LAN Interface

Wireless Mode AP

Band 2.4 GHz (802.11b/g/n)

SSID AceTop24

Broadcast ESSID Enable

Multiple SSID Setup

Auto Channel Disable

Channel Ch 3

Channel Width 40 MHz, +Ch 7

Wireless Client Limit 29

Security Setup

Data Rate Auto

RF Power 75 %

Apply Cancel

WEP

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



• Select SSID	
SSID choice	AceTop24 ▼
• Security Settings	
Client Isolation	Disable ▼
Encryption	WEP ▼
Key Length	64-bit ▼
Key type	Hex (10characters) ▼
Default key	Key 1 ▼
Encryption Key 1	1234567890
Encryption Key 2	
Encryption Key 3	
Encryption Key 4	
Additional Authentication	No additional authentication ▼

- **Key Length:** The AC.TOP offers 64bit and 128 bit for WEP key length. The longer the Key Length, the more secure the encryption is.
- **Key Format:** 2 types are available: ASCII and HEX. ASCII is a string of ASCII code including alphabetical characters, space, signs and numbers (i.e. “airlivepass12”). HEX is a string of 16-bit hexadecimal digits (0..9, a, b, c, d, e, f). All wireless devices on the network must match the exact key length and Key type. Some Wireless clients only allow HEX type for WEP.

WPA(TKIP), WPA(AES), WPA Mixed

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

• Security Settings	
Client Isolation	Disable
Encryption	WPA per-shared key
WPA type	WPA2 Only
Encryption Type	AES
Pre-shared Key Type	Passphrase
Pre-shared Key	1234567890
Additional Authentication	No additional authentication

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

WPA Radius

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

• Select SSID	
SSID choice	TOOP5G
• Security Settings	
Client Isolation	SSID Separator
Encryption	WPA RADIUS
WPA type	WPA/WPA2 mixed mode-EAP
Encryption Type	TKIP/AES Mixed Mode
Additional Authentication	No additional authentication

802.1x/EAP

AC.TOP also supports the 802.1x/EAP as security



• Select SSID	
SSID choice	actop24 ▼
• Security Settings	
Client Isolation	Disable ▼
Encryption	IEEE802.1x/EAP ▼
Key Length	64-bit ▼
Additional Authentication	No additional authentication ▼

- **Key Length:** Select 64-bit or 128-bit. 128-bit is more secure than 64-bit and is recommended.

4.2.11 WMM

Wireless -> Multi SSID ->WMM

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

4.2.12 Data Rate

Wireless -> Data Rate

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

4.2.13 RF Power

Wireless -> RF Power

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



4.3 Advance Settings

Wizard Wireless System Status Reboot		Home / Logout	
<ul style="list-style-type: none"> <input type="radio"/> Wireless 2.4G <input type="radio"/> Wireless 5G <input checked="" type="radio"/> Advanced Settings <input type="radio"/> Access Control <input type="radio"/> Site Survey <input type="radio"/> WPS <input type="radio"/> WLAN Schedule <input type="radio"/> RADIUS 		<h3><input checked="" type="radio"/> Wireless Advanced Setting</h3>	
Fragment Threshold	<input type="text" value="2346"/>	(256-2346)	
RTS Threshold	<input type="text" value="2347"/>	(1-2347)	
Beacon Interval	<input type="text" value="90"/>	(20-1000 ms)	
Preamble Type	<input type="radio"/> Long Preamble <input checked="" type="radio"/> Short Preamble		
CTS Protection	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		
Aggregation	<input type="text" value="AMPDU"/>		
Short GI	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		
Ack Timeout	<input type="text" value="1"/>	(0-255,0:Auto adjustment, Unit:4usec)	
			<input type="button" value="Apply"/> <input type="button" value="Cancel"/>

- **Fragmentation:** When the size of a unicast frame exceeds the fragmentation threshold, it will be fragmented before the transmission. It should have a value of 256-2346 bytes, with a default of 2346. If you experience a high packet error rate, you should slightly decrease the Fragmentation Threshold.
- **RTS Threshold:** RTS/CTS frames are used to gain control of the medium for transmission. Any unicast (data or control) frames larger than specified RTS threshold must be transmitted following the RTS/CTS handshake exchange mechanism. The RTS threshold should have a value between 256-2347 bytes, with a default of **2347**. It is recommended that this value does not deviate from the default too much.
- **Beacon Interval:** The device broadcasts beacon frames regularly to announce its existence. The beacon Interval specifies how often beacon frames are transmitted in time unit of milliseconds. The default value is **100**, and a valid value should be between 1 and 65,535.
- **Preamble Type:** A preamble is a signal used in wireless environment to synchronize the transmitting timing including Synchronization and Start frame delimiter. In a "noisy" network environment, the Preamble Type should be set to Long Preamble. The Short Preamble is intended for applications where minimum overhead and maximum performance is desired. If in a "noisy" network environment, the performance will be decreased.



- **IAPP:** IAPP (Inter Access Point Protocol) is designed for the enforcement of unique association throughout a ESS (Extended Service Set) and a secure exchange of station's security context between current access point (AP) and new AP during handoff period.
- **Protection:** Select Enabled or Disabled to execute the security function.
- **Aggregation:** Select Enabled or Disabled to execute this function.
- **Short GI:** Select Enabled or Disabled to execute this function.
- **ACK Timeout:** Acknowledgement Timeout Windows. 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. This is especially true for 802.11a and 802.11g networks.
Setting the correct ACK timeout value need to consider 3 factors: distance, AP response time, and interference. The AC.TOP provides ACK adjustment capability in form of either distance or direct input. When you enter the distance parameter, the AC.TOP will automatically calculate the correct ACK timeout value, it should have a value of 0-255 sec.



4.4 Access Control

Wireless -> Access Control

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

The screenshot shows the Air Live AC.TOP web interface. The top navigation bar includes 'Wizard | Wireless | System | Status | Reboot |' and 'Home / Logout'. The main content area is titled 'Wireless Access Control' and features a form for adding MAC addresses with fields for 'MAC Address' and 'Comment', and buttons for 'Add' and 'Reset'. Below the form is a table titled 'Current Access Control List' with columns for 'MAC Address', 'Comment', and 'Select'. At the bottom of the table are buttons for 'Delete Selected', 'Delete All', and 'Reset'.

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

4.5 Site Survey

Wireless -> Site Survey

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

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



11g

SSID	MAC Address	Channel	Encryption	Signal(%)
SAPIDO_RB-1830_2.4G	00:D0:41:CB:E1:B8	1	NONE	91
HP-Print-78-Officejet Pro 8600	D8:9D:67:ED:B7:78	1	WPA2PSK/AES	29
airlive	00:4F:6A:0B:E4:C5	11	WPA1PSKWPA2PSK/TKIPAES	96
airlive	00:4F:6A:0B:DB:BE	11	NONE	100
airlive	00:4F:6A:0B:EB:66	11	NONE	81
AP60	00:12:0E:F1:43:76	11	WPA2PSK/AES	100
N450R2.4	00:4F:67:05:2B:62	11	WPA2PSK/TKIPAES	100
DSL-6740C	D8:FE:E3:5D:01:65	11	WPA2PSK/AES	20
TIMOTION-WIFI	2A:A4:3C:A3:D0:71	11	WPA1PSKWPA2PSK/TKIPAES	15
TIMOTION-Guest	2E:A4:3C:A3:D0:71	11	NONE	20
airlive	00:4F:6A:0B:EB:5C	2	WPA2PSK/AES	86
Winky Online	00:19:70:2B:F4:1F	3	WPA1PSKWPA2PSK/TKIPAES	100
CHT	00:0F:B5:38:AB:88	6	WPAPSK/TKIP	39
bluesky	00:12:0E:4F:5E:5E	6	WPA2PSK/AES	60
NEWTECH_Guest	62:A4:4C:C7:0C:25	6	WPA2PSK/AES	24
TIMOTION-Guest	0E:18:D6:2F:10:D9	6	NONE	29
WNAP-6308	00:30:4F:77:F5:FA	6	WPA2PSK/AES	34
mitsui	00:1D:60:19:C4:2F	6	WPA2PSK/TKIPAES	34
NEWTECH	60:A4:4C:C7:0C:24	6	WPA2PSK/AES	20
Winky Online	00:19:70:2B:F4:1F	3	WPA1PSKWPA2PSK/TKIPAES	100

- **SSID:** This is the remote AP's SSID.
- **MAC:** This is the remote's AP's MAC address.
- **Channel:** The current scanned channel
- **Type:** The wireless type of remote AP.
- **Encryption:** The wireless encryption of remote AP.
- **Signal:** This is signal strength number in percentage in 0 to 100 scales. The higher the number, the better signal.



4.6 WPS

Wireless Settings -> WPS

Wi-Fi Protected Setup

Enable WPS

Apply Cancel

AP Interface

WPS Current Status Configured Release Configuration

Self-PIN Number 13681562

Push Button Configuration Start to Process

Client PIN Number Start to Process

2.4G

SSID	Authentication	Key
AceTop24	IEEE802.1X/EAP	

5G

SSID	Authentication	Key
TOOP5G	WPA2 Pre-Shared Key	1234567890

- **Disable WPS:** Check the box to disable the WPS function, default setting is enabled.
- **WPS Status:** Here shows the current status of the WPS function. Default setting is configured; click **Reset to UnConfigured** to re-configure the WPS connection.
- **Self-PIN Number:** Here shows the 8-digit numbers PIN code of the router itself. Enter the Self-PIN Number to client (Registrar) end and click the PIN button at the client end to make a WPS connection. It will connect with the wireless router within two minutes and get IP address.
- **Push Button Configuration:** Click **Start PBC** button (or press the physical WPS button on the Wireless Router once), meanwhile, the client should also click the PBC button simultaneously within 2 minutes.
- **Client PIN Number:** Enter the client (Enrollee) PIN code into the blank field then click the **Start PIN** button to make a WPS connection with client. Then, the wireless router will connect to client within 2 minutes and get IP address



4.7 Wireless Scheduling

Wireless -> Wireless Scheduling

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

☉ Wireless Scheduling

Define a schedule for when the 2.4GHz/5GHz Wi-Fi network is enabled or disabled.

Enable Wireless Schedule

Enable	Day	From	To
<input checked="" type="checkbox"/>	Sun	01 (hour) 00 (min)	02 (hour) 00 (min)
<input checked="" type="checkbox"/>	Sun	06 (hour) 00 (min)	10 (hour) 00 (min)
<input type="checkbox"/>	Sun	00 (hour) 00 (min)	00 (hour) 00 (min)
<input type="checkbox"/>	Sun	00 (hour) 00 (min)	00 (hour) 00 (min)
<input type="checkbox"/>	Sun	00 (hour) 00 (min)	00 (hour) 00 (min)
<input type="checkbox"/>	Sun	00 (hour) 00 (min)	00 (hour) 00 (min)
<input type="checkbox"/>	Sun	00 (hour) 00 (min)	00 (hour) 00 (min)
<input type="checkbox"/>	Sun	00 (hour) 00 (min)	00 (hour) 00 (min)
<input type="checkbox"/>	Sun	00 (hour) 00 (min)	00 (hour) 00 (min)
<input type="checkbox"/>	Sun	00 (hour) 00 (min)	00 (hour) 00 (min)

Apply Reset

4.8 RADIUS

Wireless -> RADIUS

The RADIUS menu allows you to configure the access point's RADIUS server settings, categorized into three submenus: RADIUS settings, Internal Server and RADIUS accounts.

A RADIUS server provides user-based authentication to improve security and offer wireless client control – users can be authenticated before gaining access to a network.

The access point can utilize both a primary and secondary (backup) RADIUS server for each of its wireless frequencies (2.4GHz & 5GHz). External RADIUS servers can be used or the access point's internal RADIUS server can be used.



RADIUS

Internal Server

RADIUS Accounts

2.4GHz RADIUS

RADIUS Type Internal External

RADIUS Server

Authentication Port

Shared Secret

Session Timeout second(s)

Accounting Enable Disable

Accounting Port

5GHz RADIUS

RADIUS Type Internal External

RADIUS Server

Authentication Port

Shared Secret

Session Timeout second(s)

Accounting Enable Disable

Accounting Port

4.8.1 RADIUS Settings

Configure the RADIUS server settings for 2.4GHz & 5GHz. Each frequency can use an internal or external RADIUS server.

- **RADIUS Type:** Select “Internal” to use the access point’s built-in RADIUS server or “external” to use an external RADIUS server.
- **RADIUS Server:** Enter the RADIUS server host IP address.
- **Authentication Port:** Set the UDP port used in the authentication protocol of the RADIUS server. Value must be between 1 – 65535



- **Shared Secret:** Enter a shared secret/password between 1 – 99 characters in length. This should match the “MAC-RADIUS” password used in **IV-3-1-3-6** or **IV-3-2-3**.
- **Session Timeout:** Set a duration of session timeout in seconds between 0 – 86400.
- **Accounting:** Enable or disable RADIUS accounting.
- **Accounting Port:** When accounting is enabled (above), set the UDP port used in the accounting protocol of the RADIUS server. Value must be between 1 – 65535.

4.8.2 Internal Server

AC.TOP also features a built-in RADIUS server which can be configured as shown below used when “Internal” is selected for “RADIUS Type” in the “Wireless” → “RADIUS” → “Internal Server”

The screenshot shows the 'Internal Server Setup' configuration page. It includes the following fields and options:

- Enable Internal RADIUS Server
- EAP Internal Authentication: PEAP(MS-PEAP) ▼
- EAP Certificate File Format: PKCS#12(*.pfx/*.p12)
- EAP Certificate File: Upload
- Shared Secret:
- Session-Timeout: 3600 second(s)
- Termination-Action:
 - Reauthentication(RADIUS-Request)
 - Not-Reauthentication(Default)
 - Not-Send

Buttons: Apply, Cancel

- **Internal Server:** Check/uncheck to enable/disable the access point’s internal RADIUS server.
- **EAP Internal Authentication :** Select EAP internal authentication type from the drop down menu
- **EAP Certificate File Format :** Displays the EAP certificate file format: PCK#12(*.pfx/*.p12)



- **EAP Certificate File:** Click “Upload” to open a new window and select the location of an EAP certificate file to use. If no certificate file is uploaded, the internal RADIUS server will use a self-made certificate.
- **Shared Secret:** Enter a shared secret/password for use between the internal RADIUS server and RADIUS client. The shared secret should be 1 – 99 characters in length. This should match the “MAC-RADIUS” password used in **IV-3-1-3-6** or **IV-3-2-3**.
- **Session Timeout:** Set a duration of session timeout in seconds between 0 – 86400.
- **Termination Action:** Select a termination-action attribute: “Reauthentication” sends a RADIUS request to the access point, “Not-Reauthentication” sends a default termination-action attribute to the access point, “Not-Send” no termination-action attribute is sent to the access point.

4.8.3 RADIUS Accounts

The internal RADIUS server can authenticate up to 256 user accounts. The “RADIUS Accounts” page allows you to configure and manage users.



RADIUS Accounts

User Name

Add

Reset

User Registration List

Select	User Name	Password	Customize
<input type="checkbox"/>	airlive	Configured	Edit

Add/edit User Registration List

User Name	<input type="text" value="airlive"/>
Password	<input type="password" value="...."/>

- **User Name:** Enter the user names here, separated by commas.
- **Add :** Click “Add” to add the user to the user registration list
- **Reset:** Clear text from the user name box.
- **Select:** Check the box to select a user.
- **User Name:** Displays the user name.
- **Password:** Displays if specified user name has a password (configured) or not (not configured).



- **Customize:** Click “Edit” to open a new field to set/edit a password for the specified user name (below).
- **Delete Selected:** Delete selected user from the user registration list.
- **Delete All :** Delete all users from the user registration list.



5

System Configurations

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

5.1 Menu Structure

When you click on the “**System**” 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 displays 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 **AC.TOP 11 AC wide range Ceiling Mount PoE Access Point**. The main menu bar contains links for Wizard, Wireless, **System**, Status, and Reboot. A Home / Logout link is also present.

The **LAN Interface Setup** configuration page is shown, featuring a sidebar with the following menu items: LAN Interface Setup (selected), Time Settings, Password Settings, Management, Firmware Upgrade, Configuration, and Factory Default.

The main configuration area for **LAN Interface Setup** includes the following fields:

- IP Address Assignment:** Dynamic IP (dropdown menu)
- Device Name:** test (text input)
- IP Address:** 192.168.1.254 (text input)
- IP Subnet Mask:** 255.255.255.0 (text input)
- Default Gateway:** User-Defined (dropdown menu) and 192.168.1.254 (text input)

Buttons for **Apply** and **Cancel** are located at the bottom of the configuration area.

5.2 LAN Interface Setup

System >> LAN Interface Setup

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

Wizard | Wireless | System | Status | Reboot | H

- LAN Interface Setup
- Time Settings
- Password Settings
- Management
- Firmware Upgrade
- Configuration
- Factory Default

LAN Interface Setup

IP Address Assignment Static IP

Device Name test

IP Address 192.168.1.254

IP Subnet Mask 255.255.255.0

Default Gateway User-Defined 192.168.1.254

DHCP Disabled

DHCP Leased Time One Hour

DHCP Client Range 192.168.1.120 - 192.168.1.140 Show Client

Static DHCP Set Static DHCP

DNS1

DNS2

Domain Name AC.TOP

Enable AirLive IP Finder Management

Apply Cancel

← Device IP Settings

↑ DHCP Settings

5.2.1 DHCP Settings

- **DHCP Service:** You can enable or disable DHCP server here.
 - **Disable(default):** Disable DHCP server
 - **Enable:** The AC.TOP will act as DHCP server to provide IP addresses to the clients on the LAN/Wireless interface. By default, the DHCP server is on.

- **DHCP Client Range:** You can define the IP pool from which the DHCP clients can get IP address. Click on “**Show Client**” to see the current DHCP client table.

- **DHCP Release Time:** You can define how long the AC.TOP will reserve IP address for a particular PC or Device here.



5.2.2 Set Static DHCP

Static DHCP

- **Static DHCP Lease Table**
It allows 10 entries only.

NO.	IP Address	MAC Address	Select
<input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/> <input type="button" value="Reset"/>			
<input type="checkbox"/> Enable Static DHCP IP			
IP Address		MAC Address	
<input style="width: 100%;" type="text"/>		<input style="width: 100%;" type="text"/>	
<input type="button" value="Add"/>		<input type="button" value="Clear"/>	
<input type="button" value="Apply"/>			

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

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

5.2.3 Domain Name

You can enter the network area name here.

5.2.4 802.11d Spanning Tree

Select Disabled or Enabled form the pull-down list.

5.2.5 Clone MAC Address

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

5.2.6 Enable AirLive IP Finder Management

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



5.3 Time Settings

System -> Time Settings

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

The screenshot shows the 'Time Settings' configuration page. On the left is a navigation menu with options: LAN Interface Setup, Time Settings (selected), Password Settings, Management, Firmware Upgrade, Configuration, and Factory Default. The main content area is titled 'Time Settings' and includes the following fields and controls:

- Current Time:** Yr: 2015, Mon: 1, Day: 17, Hr: 11, Mn: 16, Sec: 6. A 'Copy Computer Time' button is located below these fields.
- Time Zone Select:** A dropdown menu showing '(GMT+08:00)Taipei, Taiwan'.
- Enable NTP client update:** A checked checkbox.
- NTP server:** A radio button selected for '203.117.180.36 - Asia Pacific' and another radio button for '(Manual IP Setting)' with an empty input field.
- Buttons:** 'Apply' and 'Cancel' buttons at the bottom.

Below is the procedure to set your NTP server

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

5.4 Password Settings

System -> Password Settings

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



⊙ Password

This page is used to set the account to access the web server of Access Point. Empty user name and password will disable the protection.

Current Password

New Password

Confirm Password

5.5 Management

System ->Management

The Management page allow users to enable or disable the manage methods which they want to uses.

⊙ Management

- HTTP
- HTTPS
- TELNET
- SSH
- SNMP

SNMP Version

SNMP Get Community

SNMP Set Community

SNMP Trap

SNMP Trap Community

SNMP Trap Manager

- **HTTP:** means AC.TOP can be access via http port
- **Watch Host:** means AC.TOP can be access via https port.
- **SNMP:** AC.TOP can be management via SNMP v1/v2c



- **SNMP Get Community:** set the Get community (password)
- **SNMP Set Community:** set the Set Community (password)
- **SNMP Trap:** to Enable SNMP trap
- **SNMP Trap Community:** to set the trap community (password)
- **SNMP Trap Manager:** to set the IP address which SNMP trap server locate.

5.6 Firmware Upgrade

System -> Firmware Upgrade

You can upgrade the firmware of your AC.TOP (the software that controls your AC.TOP's operation). Normally, this is done when a new version of firmware offers new features that you want, or solves problems that you have encountered with the current version.

- **Upgrade Firmware:**

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

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



5.7 Configuration Save and Restore

System -> Configuration Save and Restore

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

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

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



Step 2 Click on **“Save Setting to File”** and enter the path of the configuration file to save-to.

Restore Setting:

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

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

5.8 Factory Default

System Configuration -> Factory Default

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





6

Status Menu

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

6.1 Menu Structure

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

Device Information	
System	
Uptime	0 day 18:23:59
Hardware version	Rev. A
Runtime code version	0.1.0
2.4G Wireless Configuration	
Mode	AP
Associated Clients	0 <input type="button" value="Show Active Clients"/>
SSID 1	
SSID	AceTop24
Channel	3
Security	WEP
BSSID	74:DA:38:14:E0:5C
SSID 2	
SSID	22
Channel	3
Security	Disable
BSSID	76:DA:38:10:E0:5C
SSID 3	
SSID	33
Channel	3
Security	Disable
BSSID	76:DA:38:11:E0:5C



6.2 Device Information

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

- **Uptime:** This displays the time since system last boot up. This is a good indication for how long the system has been alive.
- **Hardware Version:** It displays the hardware version.
- **Runtime Code Version:** This place will display the current firmware version.

System	
Uptime	0 day 18:24:57
Hardware version	Rev. A
Runtime code version	0.1.0

- **Wireless:** This page displays the current settings and status of the radio. It includes the BSSID and connection status. The BSSID is also the wireless MAC address that is needed for the WDS entry.



2.4G Wireless Configuration	
Mode	AP
Associated Clients	0 <input type="button" value="Show Active Clients"/>
SSID 1	
SSID	AceTop24
Channel	3
Security	WEP
BSSID	74:DA:38:14:E0:5C
SSID 2	
SSID	22
Channel	3
Security	Disable
BSSID	76:DA:38:10:E0:5C
SSID 3	
SSID	33
Channel	3
Security	Disable
BSSID	76:DA:38:11:E0:5C

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

LAN Configuration	
IP Address	192.168.1.254
Subnet Mask	255.255.255.0
DHCP Server	Disabled
MAC Address	74:DA:38:14:E0:5C



6.3 Statistic

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

Statistics

This page shows the packet counters for transmission and reception regarding to networks.

2.4G Wireless LAN	<i>Sent Packets</i>	0
	<i>Received Packets</i>	1505
5G Wireless LAN	<i>Sent Packets</i>	0
	<i>Received Packets</i>	0
Ethernet	<i>Sent Packets</i>	96408
	<i>Received Packets</i>	533105

6.4 Log

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

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



System Log

Enable Remote Log

Log Server IP Address:

Apply Changes

```

Jan 17 08:04:36 [DHCPC]: DHCP Client, Lease obtained: 192.168.0.47; lea
Jan 17 05:04:36 [DHCPC]: DHCP Client, Lease obtained: 192.168.0.47; lea
Jan 17 02:04:36 [DHCPC]: DHCP Client, Lease obtained: 192.168.0.47; lea
Jan 16 23:04:36 [DHCPC]: DHCP Client, Lease obtained: 192.168.0.47; lea
Jan 16 20:04:35 [DHCPC]: DHCP Client, Lease obtained: 192.168.0.47; lea
Jan 16 18:44:33 [SYSTEM]: NET, Firewall Disabled
Jan 16 18:44:33 [SYSTEM]: NET, NAT Disabled
Jan 16 18:44:33 [SYSTEM]: NET, stop Firewall
Jan 16 18:44:33 [SYSTEM]: NET, stop NAT
Jan 16 18:44:33 [SYSTEM]: SCHEDULE, Schedule Stopping
Jan 16 18:44:33 [SYSTEM]: SCHEDULE, Schedule Stopping
Jan 16 18:44:33 [SYSTEM]: NTP, start NTP Client
Jan 16 18:44:33 [SYSTEM]: SYSTEM, Apply settings for [NTPD][Scheduler]
Jan 16 18:01:15 [SYSTEM]: SNMP, start SNMP server
Jan 16 18:01:15 [SYSTEM]: SNMP, stop SNMP server
Jan 16 18:01:15 [SYSTEM]: LAN, Firewall Disabled
Jan 16 18:01:15 [SYSTEM]: LAN, NAT Disabled
Jan 16 18:01:15 [SYSTEM]: LAN, stop Firewall
Jan 16 18:01:15 [SYSTEM]: LAN, stop NAT

```

Save

Clear

Refresh



7

Frequent Asked Questions

In this chapter, we will address some frequent asked questions about AC.TOP

Q: I forgot my password or the IP address of AC.TOP.

A:

Please restore your settings to default by press the reset button for more than 5 seconds. You should be able to find your AC.TOP at 192.168.1.254 with default username “**admin**” and password “**airlive**”.



Q: AC.TOP is not responding to me when I want to access it by web browser

A:

- a. Please check the connection of power cord and network cable of this access point. All cords and cables should be correctly and firmly inserted to AC.TOP.
- b. If LEDs on this access point are out, please check the status of A/C power adapter, and make sure it's correctly powered.
- c. You must use the same IP address section which AC.TOP uses.
- d. Are you using MAC or IP address filter?
Try to connect the access point by another computer and see if it works; if not, please perform a hard reset (pressing 'reset' button).
- e. Set your computer to obtain an IP address automatically (DHCP), and see if your computer can get an IP address.
- f. If you did a firmware upgrade and this happens, contact your dealer of purchase for help.
- g. If all above solutions don't work, contact the dealer of purchase for help.

**Q: Can't get connected to AC.TOP.****A:**

- a. If encryption is enabled, please re-check WEP or WPA passphrase settings on your wireless client.
- b. Try to move closer to AC.TOP.
- c. Unplug the power plug of AC.TOP and plug it back again after 10 seconds.
- d. If all LEDs on this AC.TOP are out, please check the status of A/C power adapter, and make sure it's correctly powered.

Q: I can't locate my access point by my wireless client**A:**

- a. **'Broadcast ESSID'** set to off?
- b. Is Antenna properly installed and secured?
- c. Are you too far from your AC.TOP? Try to get closer.
- d. Please remember that you have to input ESSID on your wireless client manually, if ESSID broadcast is disabled.

Q: File download is very slow or breaks frequently**A:**

- a. Try to reset the AC.TOP and see if it's better after that.
- b. Try to know what computers do on your local network. If someone's transferring big files, other people will think Internet is really slow.
- c. Change channel number and see if this works.

Q: I can't log onto web management interface: password is wrong**A:**

- a. Make sure you're connecting to the correct IP address of the AC.TOP!
- b. Password is case-sensitive. Make sure the **'Caps Lock'** light is not illuminated.
- c. If you really forget the password, do a hard reset.

Q: AC.TOP become hot**A:**

- a. This is not a malfunction, if you can keep your hand on the AC.TOP's case.
- b. If you smell something wrong or see the smoke coming out from access point or A/C power adapter, please disconnect the access point and A/C power adapter from utility power (make sure it's safe before you're doing this!), and call your dealer of purchase for help.



8

Specifications

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

8.1 Hardware Features

8.1.1 General Hardware Feature

- 1 x 10/100/1000 Mbps Ethernet Port with Auto MDI/MDI-X Support
- 802.3af PoE Port (LAN) LAN, PWR, LED Indicators
- 2.4G and 5G dual band con-current
- 1200Mbps 2T2R 11 ac+b/g/n Radio
- Up to 23dBm Output Power (20dBm in EU, 23dBm in the U.S.)
- 4MB Flash, 32MB SDRAM

8.1.2 Antenna

PiFa Antenna x 4 (2T2R MIMO Technology)

8.1.3 Power Supply

- 12VDC, 1.5A Switching Power Adapter

8.1.4 Dimension and Weight

- Product Weight: 306 g
- Product Size (D x H): 176(D) x 30(H)mm

8.1.5 Certification

- FCC, CE

8.2 Radio Specifications

8.2.1 Frequency Band

- 2.4000~2.4835GHz (Industrial Scientific Medical Band)
- 5180 ~5240GHz (Band1) for ETSI
- 5745 ~ 5825 for FCC



8.2.2 Output Power and Sensitivity

■ Output Power (excluding the antenna gain)

- 2.4GHz:

- 11b(11M): 20 ± 1.5 dBm
- 11g(54M): 19 ± 1.5 dBm
- 11n(20MHz, MCS7): 14 ± 1.5 dBm
- 11n(40MHz, MCS7): 13 ± 1.5 dBm

- 5GHz:

- 11a(54M): 19.5 ± 1.5 dBm
- 11n(20MHz, MCS7): 16.5 ± 1.5 dBm
- 11n(40MHz, MCS7): 17 ± 1.5 dBm
- 11ac(80MHz, VHTMCS9): 12 ± 1.5 dBm

■ Receive Sensitivity

- 2.4GHz:

- 11b(11M): -90 ± 2 dBm
- 11g(54M): -75 ± 2 dBm
- 11n(20MHz, MCS7): -70 ± 2 dBm
- 11n(40MHz, MCS7): -70 ± 2 dBm

- 5GHz:

- 11a(54M): -72 ± 2 dBm
- 11n(20MHz, MCS7): -68 ± 2 dBm
- 11n(40MHz, MCS7): -68 ± 2 dBm
- 11ac(80MHz, VHTMCS9): -58 ± 2 dBm

Note: The real output is dependent on the regulation

8.2.3 TX Output Power

- ETSI (Europe) - About 20dBm max
- FCC (The United States) - About 23dBm max

8.2.4 Supported WLAN Mode

- 2.4 GHz (B + G + N)
- 2.4 GHz (B)
- 2.4 GHz (B + G)
- 5G (A)
- 5G (A+N)
- 5G (AC+A+N)



8.2.5 Supported WLAN Encryption

- 64/128-bit WEP
- WPA/WPA2-PSK support
- WPA/WPA2-EAP support
- 802.1x Radius Support

8.3 Software Feature

8.3.1 Operation Mode

- Access Point Mode (AP mode)
- WDS repeater

8.3.2 Management Interface

- Web HTTP
- IP Finder
- AirLive Central Wireless

8.3.3 Advance Functions

- Setup Wizard
- Multiple SSID, Virtual AP, Watchdog, Hidden SSID
- ACK Timeout Adjustment
- WMM, MAC Access Control, Wireless Client Isolation, Channel, RTS Threshold
- Green AP Energy Saving Feature TX Output Power Adjustment
- Wireless Security: WEP- 64/128bit, WPA, WPA2 and IEEE 802.1x
- Restore to Factory Default
- Configuration Backup and Restore

8.4 Environment

8.4.1 Environment

- Operating temperature: 0~40 Degree C
- Operating humidity (non-condensing): 10~90%
- Storage temperature: -20~60 Degree C
- Storage humidity: 95% Max



9

Wireless Network Glossary

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

802.3ad

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

802.3af

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

802.11b

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

802.1d STP

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

802.11d

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

802.11e

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

802.11g

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

**802.11i**

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

802.1x

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

Adhoc

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

Access Point (AP)

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

ACK Timeout

Acknowledgement Timeout Windows. When a packet is sent out from one wireless station to the other, it will 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. This is especially true for 802.11a and 802.11g networks. Setting the correct ACK timeout value need to consider 3 factors: distance, AP response time, and interference. The AC.TOP provides ACK adjustment capability in form of either distance or direct input. When you enter the distance parameter, the AC.TOP will automatically calculate the correct ACK timeout value.



Bandwidth Management (Bandwidth Control)

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

Bootloader

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

Bridge

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

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

Client

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

CPE Devices

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

CTS

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

**DDNS**

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

DHCP

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

DMZ

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

DNS

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

Domain Name

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

DoS Attack

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

Encryption

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

**ESSID (SSID)**

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

Firewall

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

Firmware

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

FTP

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

Fragment Threshold

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

Gateway

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

Hotspot

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



IGMP Snooping

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

Infrastructure Mode

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

IP address

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

IPsec

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

LACP (802.3ad) Trunking

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

MAC

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

**Mbps**

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

MESH

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

MIMO

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

NAT

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

Node

A network connection end point, typically a computer.

Packet

A unit of data sent over a network.

Passphrase

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

POE

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

**Port**

This word has 2 different meaning for networking.

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

PPPoE

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

PPTP

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

Preamble Type

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

Rate Control

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

RADIUS

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



Receiver Sensitivity

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

RJ-45

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

Router

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

SIGNAL STRENGTH

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

RTS

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

RTS Threshold

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

**SNMP**

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

SSH

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

SSL

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

Subnet Mask

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

Subnetwork or Subnet

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

TCP

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

**TX Output Power**

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

UDP

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

Upgrade

To replace existing software or firmware with a newer version.

Upload

To send a file to the Internet or network device.

URL

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

VPN

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

WAN

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

WEP

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

Wi-Fi

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

**WiMAX**

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

WDS

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

WLAN

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

WMM

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

WMS

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

WPA

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

WPA2

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