

CERIO Corporation

OW-400-A2

**eXtreme Power AC1200 2.4GHz / 5GHz 2x2 Ceiling / Wall
PoE Access Point (800mW)**



CenOS5.0 User Manual

1.	Introduction	5
1.1	Overview	5
1.2	Software Configuration	7
1.3	Login OW-400-A2 Web Page	11
2.	Software Setting	12
2.1	Operating Mode Introduction	12
3.	Access Point mode	16
3.1	Select AP Mode	16
3.2	VLAN Setup	16
3.2.1	Network Button	17
3.2.2	Network Pull-down menu	18
#	DHCP Server	19
#	Radio 0/1 Access Point	20
#	MAC Filter	23
#	802.11r/802.11k Fast Roaming	23
3.3	Authentication	25
#	Authentication Button:	26
#	Authentication Dropdown Button	27
3.3.1	Guest	27
3.3.2	Local User	28
3.3.3	OAuth2.0	29
※	Sample for Google OAuth2.0 setup	29
※	Sample for Facebook OAuth2.0 setup	32
3.3.4	Customize Page	36
3.3.5	Language	38
3.3.6	Walled Garden	38
3.3.7	Privilege Address	39
3.3.8	Profile	39
3.4	RADIUS Server	40
3.5	Radius Account Setup	40
3.6	Wireless Basic Setup	41
3.6.1	Radio 0 Basic Setup (2.4G)	41
3.6.2	Radio 1 Basic Setup (5G)	44
3.6.3	Advanced Setup	47
3.6.4	WMM Setup	49
3.6.5	WDS Setup	52

4.	CAP Mode	55
4.1	System VLAN Setup	55
4.2	AP Control	57
#	Centralized Management APs operating Instructions:	57
4.2.1	Scan Device	58
4.2.2	Batch Setup	59
4.2.3	AP Setup	62
4.2.4	Group Setup	62
4.2.5	Map Setup	63
4.2.6	Authentication Profile	65
5.	Client Bridge Mode	66
5.1	Configure LAN Setup	67
5.2	Configure DHCP Setup	69
5.3	Wireless General Setup	71
5.3.1	Radio 0(2.4G) Basic Setup	71
5.3.2	Radio 1(5G) Basic Setup	73
5.3.3	Advanced Setup	74
5.3.4	WMM Setup	77
5.3.5	Station Setup	79
5.3.6	Repeater AP Setup	80
5.3.7	MAC Filter	82
5.3.8	802.11r/802.11k Fast Roaming	83
6.	WISP Mode	86
6.1	Configure WAN Setup	86
6.2	Configure LAN Setup	90
6.3	Configure DHCP Server	90
6.4	Wireless General Setup	92
6.4.1	Radio 0(2.4G) Basic Setup	93
6.4.2	Radio 1(5G) Basic Setup	94
6.4.3	Advanced Setup	96
6.4.4	WMM Setup	99
6.4.5	Station Setup	101
6.4.6	Repeater AP Setup	102
6.4.7	MAC Filter	104
6.4.8	802.11r/802.11k Fast Roaming	105
7.	Router Mode	107
7.1	Configure WAN Setup	107
7.2	Configure LAN Setup	111

7.2.1	Network Button	112
7.2.2	Network Pull-down menu	113
	# DHCP Server	113
	# Radio 0/1 Access Point	114
	# MAC Filter.....	117
	# 802.11r/802.11k Fast Roaming	118
7.3	Wireless Basic Setup	120
7.3.1	Radio 0 Basic Setup (2.4G)	120
7.3.2	Radio 1 Basic Setup (5G)	123
7.3.3	Advanced Setup	126
7.3.4	WMM Setup	128
8.	Advanced Setup By WISP & Router Mode	131
8.1	DMZ	131
8.2	IP Filter	131
8.3	MAC Filter	134
8.4	Virtual Server	134
8.5	Access Control	136
8.6	Time Policy	137
9.	System Management	138
9.1	Configure system management	138
9.2	Configure Time Server	140
9.3	Control PoE Bridge	142
9.4	Configure SNMP Setup	142
10.	Utilities	143
10.1	Profile Setting	143
10.2	System Upgrade	145
10.3	Network Utility	146
10.4	Reboot	146
11.	Status	147
11.1	Overview	147
11.2	Wireless Client	147
11.3	Online Users by Captive Portal	148
11.4	Authentication Log by Captive Portal	149
11.5	System Log	149
	Appendix A. WEB GUI Valid Characters.....	150

1. Introduction

1.1 Overview

CERIO's OW-400-A2 eXtreme Power AC1200 2.4GHz/5GHz 2x2 +17dBi +Heater Outdoor Bridge/AP (800mW) is a dual band outdoor AP that combined superior functionality with an elegant and highly durable housing design. This 11ac outdoor concurrent dual band access point supports a maximum throughput of **1200Mbps**, up to **300Mbps** on the 2.4GHz frequency band and **867Mbps** on the 5GHz frequency band. **OW-400-A2 utilizes 2 spatial streams**, each of which can operate on the 2.4GHz or 5GHz frequency band. OW-400-A2's high performance and **IP67 weather-proof** durable design makes it perfect for deployment in enterprise, government, public environments, and WISP application.

OW-400-A2 utilizes an 800mW high power design with a **built-in 17dBi 5GHz directional panel antenna** and **four external N-Type antenna connectors**. Two of the N-Type connectors are assigned to the 2.4GHz band and two are assigned to the 5GHz band. OW-400-A2 supports both a built-in directional panel antenna or 2 N-Type external antenna connectors in the 5GHz band, however only supports N-Type connectors in the 2.4GHz band (users must enter the software UI to select either built-in antennas or external N-Type antennas for the 5GHz band, they cannot be used simultaneously). OW-400-A2's quality hardware design incorporates a **built-in heater with a smart temperature sensor**. This heater automatically turns on when the PCB temperature falls below 0°C, making OW-400-A2 perfect for low temperature deployment environments. This device is powered through 802.3af/at Power over Ethernet, allowing both power and data to be provided through CAT5 cabling. OW-400-A2's supports fast wireless roaming 802.11r/k protocol for seamless roaming and smart client handoff.

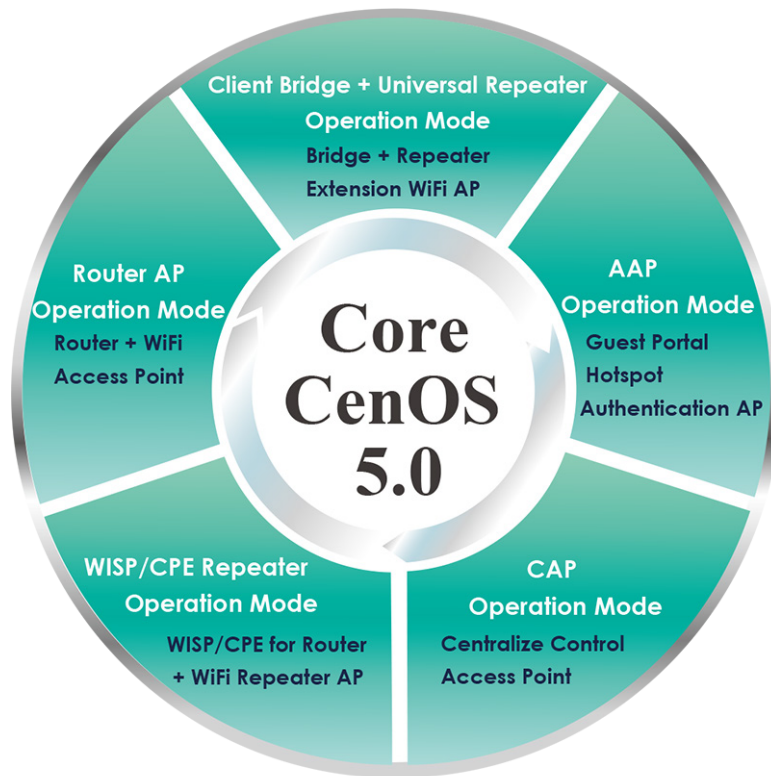
CenOS 5.0 Description

CenOS 5.0 combines aspects of CenOS 3.0 and CenOS 4.0 cores. Supported operation modes include Access Point Mode (including Authentication AP **[AAP]** Mode, Pure AP Mode, and AP with WDS Mode), Control Access Point **[CAP]** (Centralized AP Controller), Router AP Mode, Client Bridge + Repeater Mode, and finally WISP / CPE Repeater + AP Mode.

CenOS 5.0's AAP mode includes new features such as built-in 802.1x RADIUS authentication support. Through AAP and CAP Mode, wireless clients can be securely authenticated through a customized login page that supports OAuth2.0 credentials (Facebook Login, Google Login, etc). This opens up network access conveniently to users, while simultaneously maintaining network security and network management.

Administrators can use CenOS 5.0 CAP Mode to centrally manage AAP devices within the same network. Using CAP Mode's Batch Setup, administrators can make setting changes such as: Wireless Settings, Security Settings / User Authentication / Firmware Upgrade / System Time / Traffic Monitoring / Status Overview and more. CAP Mode also allows users to limit client access and bandwidth to effectively load balance the network.

Cerio's innovative AAP design allows users to create customized login pages (Captive Portal) for user authentication. This not only provides a platform for marketing, but also provides a security barrier by allowing clients to use third-party credentials such as Facebook and Google to login into the network. Using only the customized login page for authentication deviates from traditional security encryptions, which actually slow bandwidth speeds by up to 20%.



Only Cerio's special model supports CAP / Router mode

1.2 Software Configuration

OW-400-A2 supports web-based configuration. Upon the completion of hardware installation, **OW-400-A2** can be configured through a PC/NB by using a web browser such as Internet Explorer 6.0 or later.

- **Default IP Address:** 192.168.2.254
- **Default Subnet Mask:** 255.255.255.0
- **Default Username and Password**

MODE	AP , CAP Mode, Client Bridge , WISP Mode, Router Mode	
Management Account	Root Account	
Username	root	
Password	default	

➤ IP Segment Set-up for Administrator's PC/NB

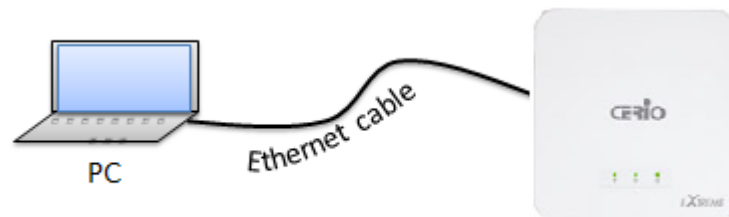
Set the IP segment of the administrator's computer to be in the same range as **OW-400-A2** for accessing the system. Do not duplicate the IP Address used here with IP Address of **OW-400-A2** or any other device within the network.

➤ Example of Segment: (Windows XP)

- Click **Start** -> **Settings** -> **Control Panel**, and then “**Control Panel**” window appears.
Click on “**Network Connections**”, and then “**Network Connections**” window appears.
- Click right on “**Local Area Connection**”, and select **Properties**.

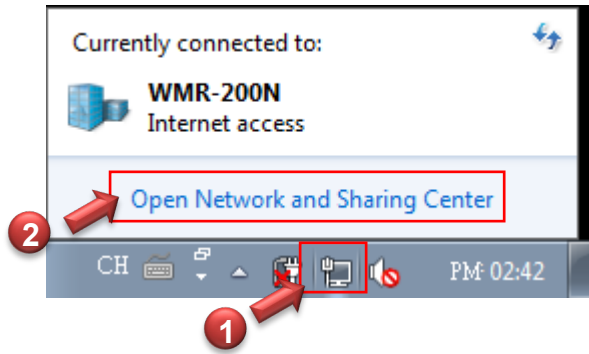
PC link to device setup by OS Windows7

Please PC link to Device used cat5/6 Ethernet cable.



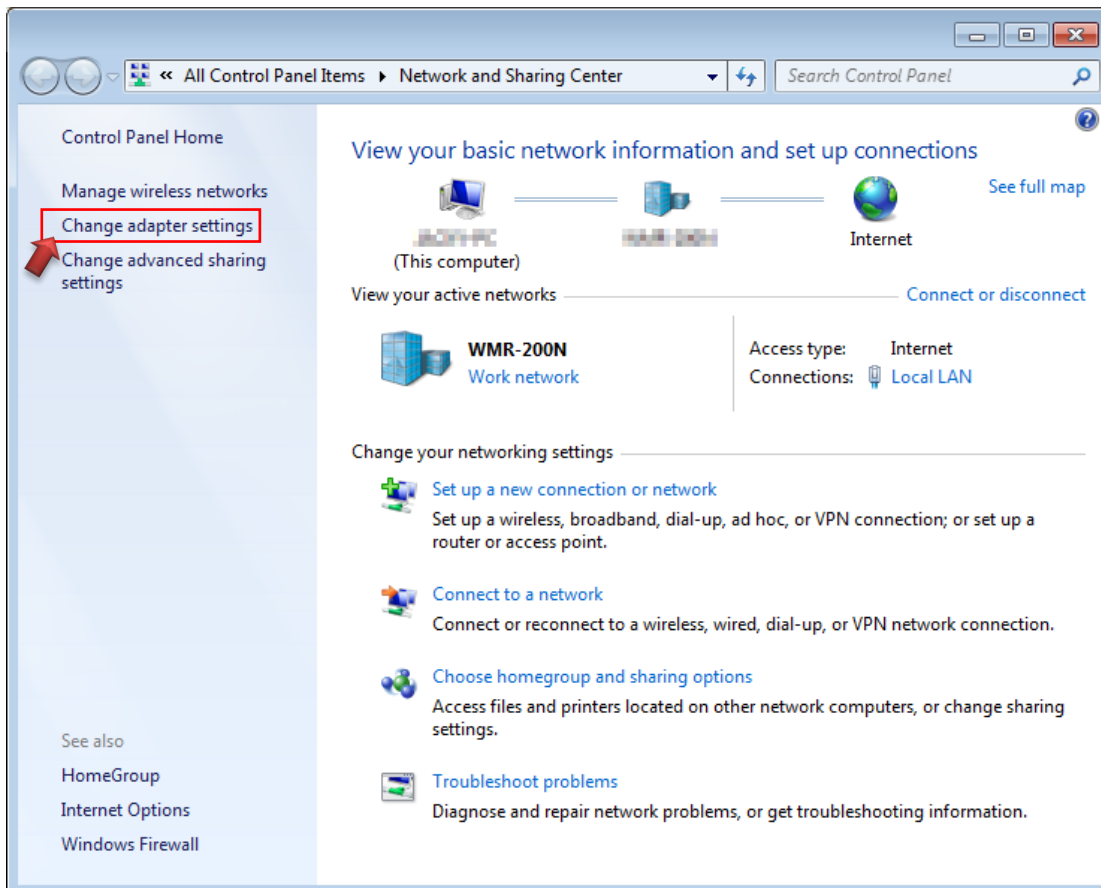
Step 1 :

Please click on the computer icon in the bottom right window, and click “Open Network and Sharing Center”



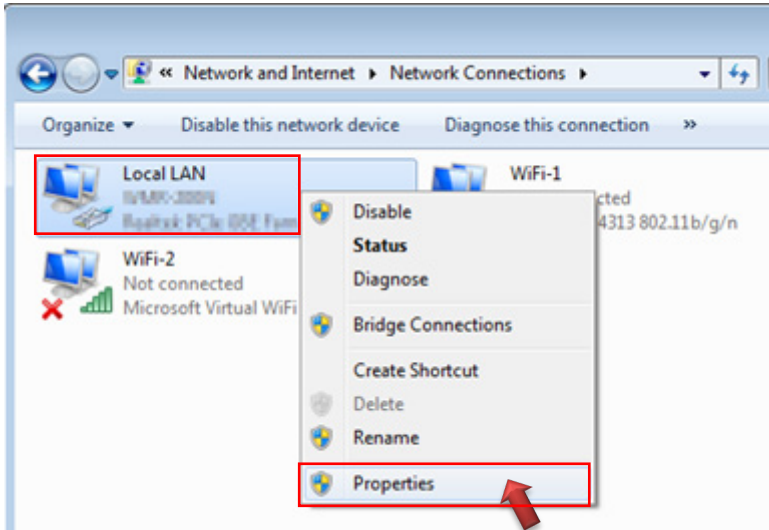
Step 2 :

In the Network and Sharing Center page, Please click on the left side of “Change adapter setting” button



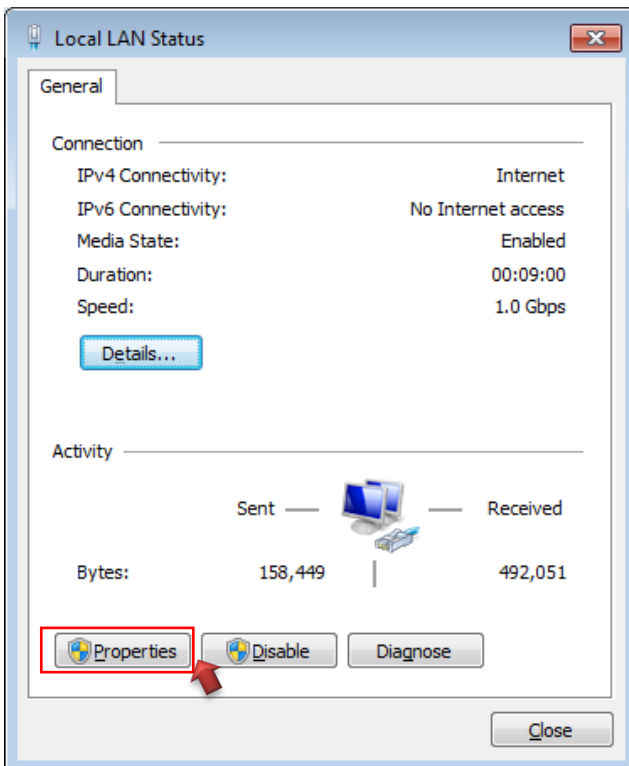
Step 3 :

In “**Change adapter setting**” Page. Please find Local LAN and Click the right button on the mouse and Click “**Properties**”



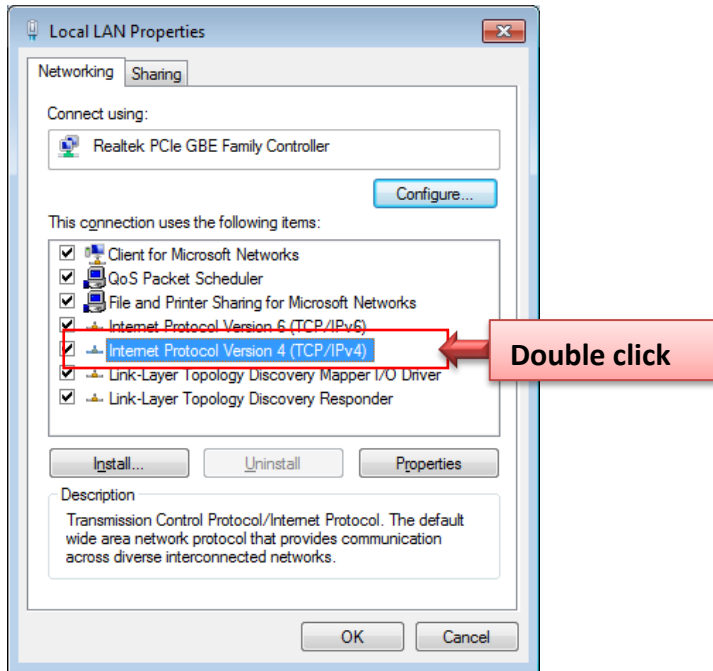
Step 4 :

In “**Properties**” page, please Click “**Properties**” button to TCP/IP setting



Step 5 :

In Properties page to setting IP address, please find **“Internet Protocol Version 4 (TCP/IPv4)”** and double click or click **“Install”** button.

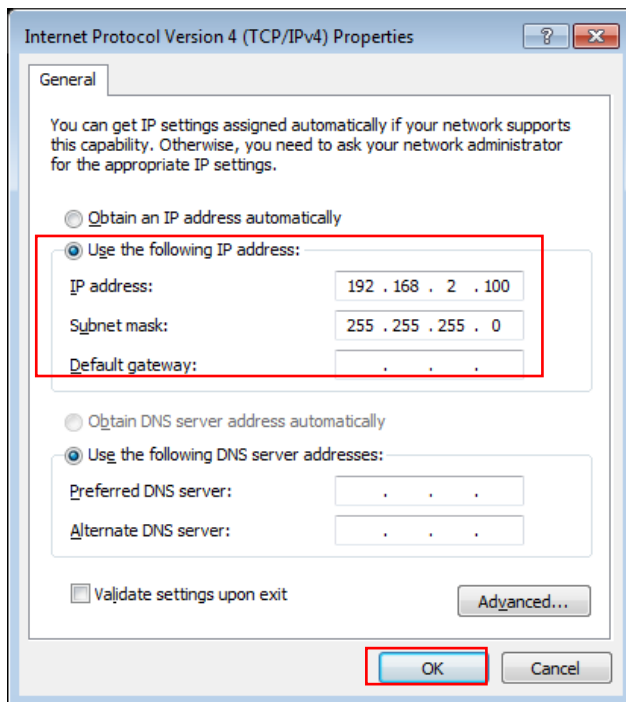


Step 6 :

Select **“Use the following IP address”**, and fix in IP Address : 192.168.2.#
ex. The # is any number by 1 to 253

Subnet mask : 255.255.255.0

And Click **“OK”** to complete the fixed computer IP setting



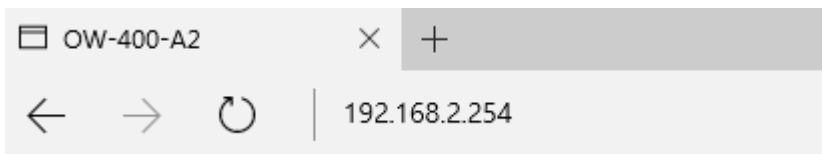
Please Open Web Browser

Without a valid certificate, users may encounter the following problem in IE7 when they try to access system's WMI (<https://192.168.2.254>). There will be a "Certificate Error", because the browser treats system as an illegal website.

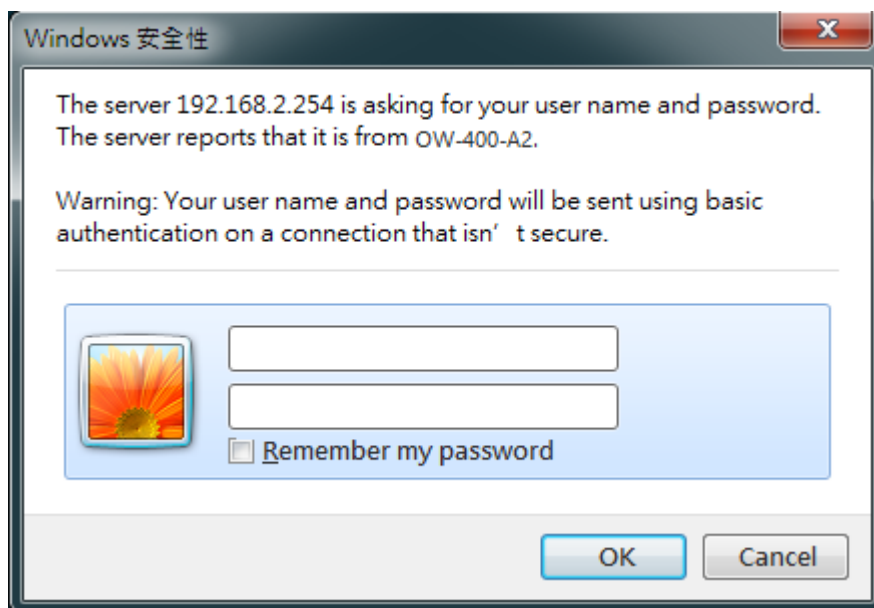
1.3 Login OW-400-A2 Web Page

➤ Launch Web Browser

Launch as web browser to access the web management interface of system by entering the default IP Address, <http://192.168.2.254>, in the URL field, and then press Enter.



➤ System Login



Please use default Users name: "**root**" and default password "**default**" to login.

2. Software Setting

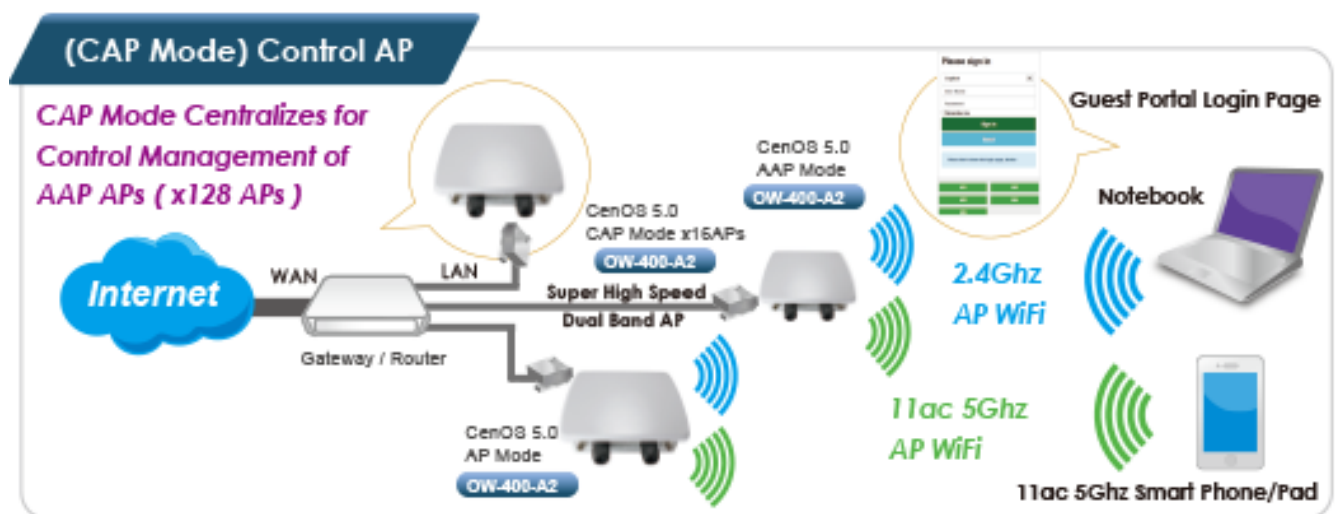
2.1 Operating Mode Introduction

CERIO OW-400-A2 eXtreme Power 11n Dual Band 2x2 Ceiling / Wall PoE Access Point with CenOS5.0 software supports five operational modes: **Access Point Mode, Router Access Point Mode, Control Access Point Mode, Client Bridge Mode, and WISP Mode.** It utilizes built-in remote management features that simplify deployment and reduce costs of continued maintenance of the access point

Because of OW-400-A2's **Dual Band capabilities**, this device possesses more reliable connectivity and allows for higher capacity and performance speeds. OW-400-A2 can operate concurrently on two radio frequencies, simultaneously enabling more flexible deployment without sacrificing bandwidth or risking device overloading. These high performance and high loadbearing capabilities makes OW-400-A2 the perfect device to be deployed in Offices, Hotels, Universities, Hospitals, Airports, Luxury Houses, etc.

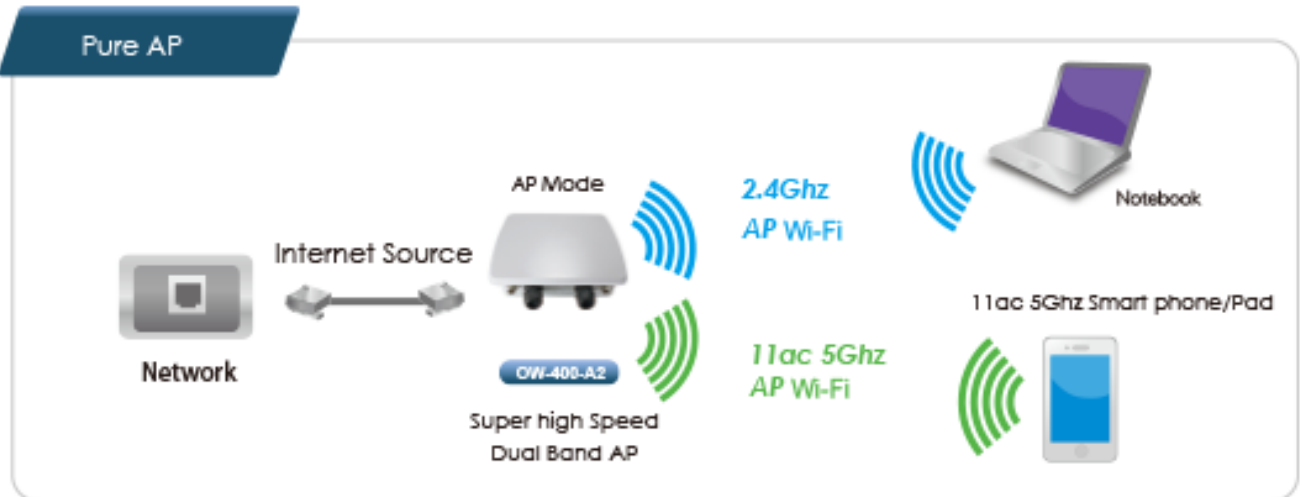
CAP mode (Centralizes Access Point)

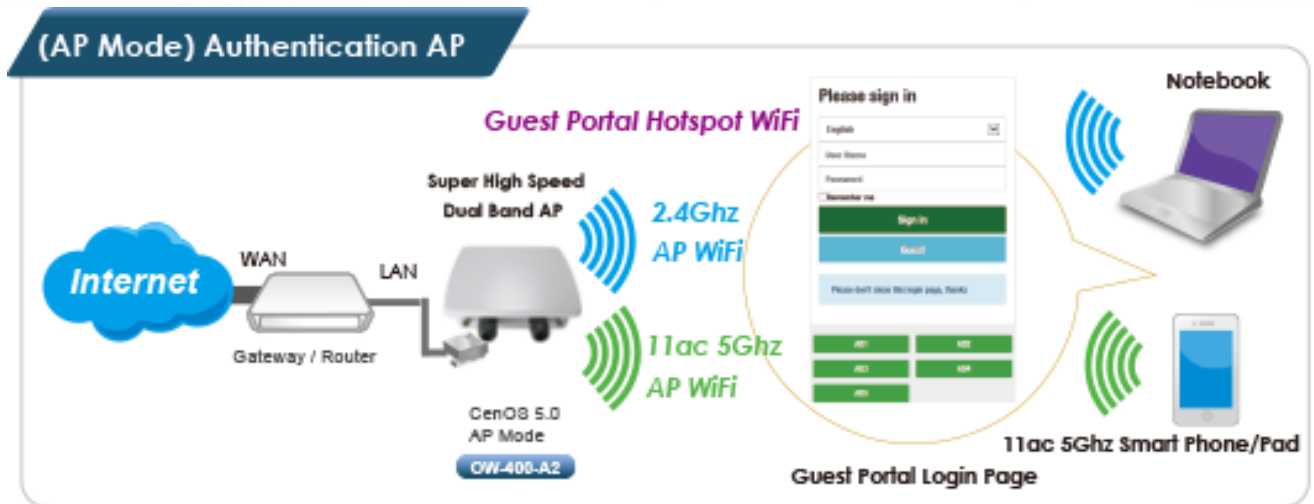
- Control Management of CenOS5.0 APs (x128 APs)
- AP Management support 802.1Q VLAN infrastructure
- Centralized setting Access Point function and firmware upgrade.
- APs Group management for concept.



Access Point Mode (Supports AP+WDS Mode)

- It can be deployed as a traditional fixed wireless Access Point
- It allow wireless clients or Stations (STA) to access
- Supports DHCP Service, allowing for automated assigning of IP addresses to clients connecting to the network
- WDS Setup includes AES (Advanced Encryption Standard) Authentication
- This enables the wireless interconnection of Access Point in a IEEE802.11 network and accepts wireless
- Support Captive Portal authentication.



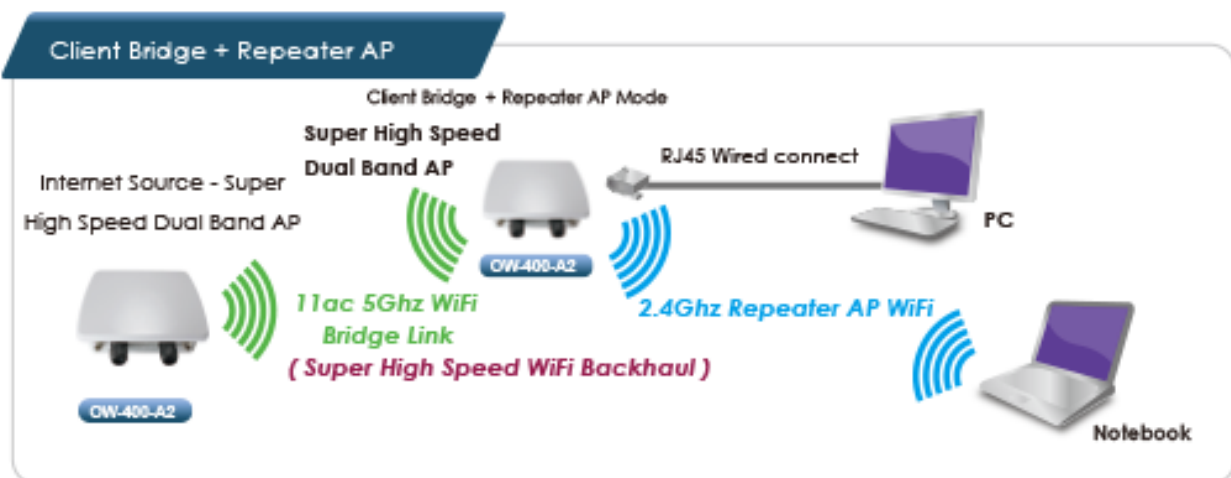


Client Bridge + Repeater Mode

- It can be used as a Client Bridge + Repeater AP to receive wireless signals over last mile applications, helping WISPs deliver wireless broadband Internet service to new residential and business customers
- In this mode, OW-400-A2 is enabled with DHCP Server functions. The wired clients of OW-400-A2 are in the same subnet from Main Base Station and it accepts wireless connections from client devices. You can disabled the repeater extending AP function, which will enable the "AP Client " function



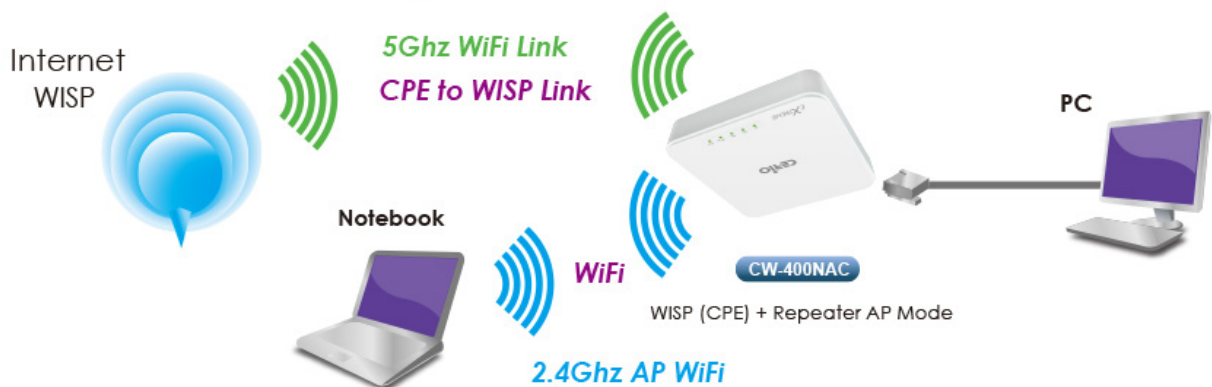
If client bridge used 5Ghz band the Repeater AP only used 2.4Ghz band.



WISP + Repeater AP Mode

- It can be used as an WISP/Outdoor Customer Premises Equipment (CPE) to receive wireless signals over last mile application, helping WISPs deliver wireless broadband Internet service to residents and business customers
- In the WISP (CPE) mode, OW-400-A2 is a gateway enabled with NAT and DHCP Server functions. The wired clients connected to DT-300N are in different subnet from those connected to Main Base Station, and, in WISP (CPE) mode, it does not accept wireless association from wireless clients.

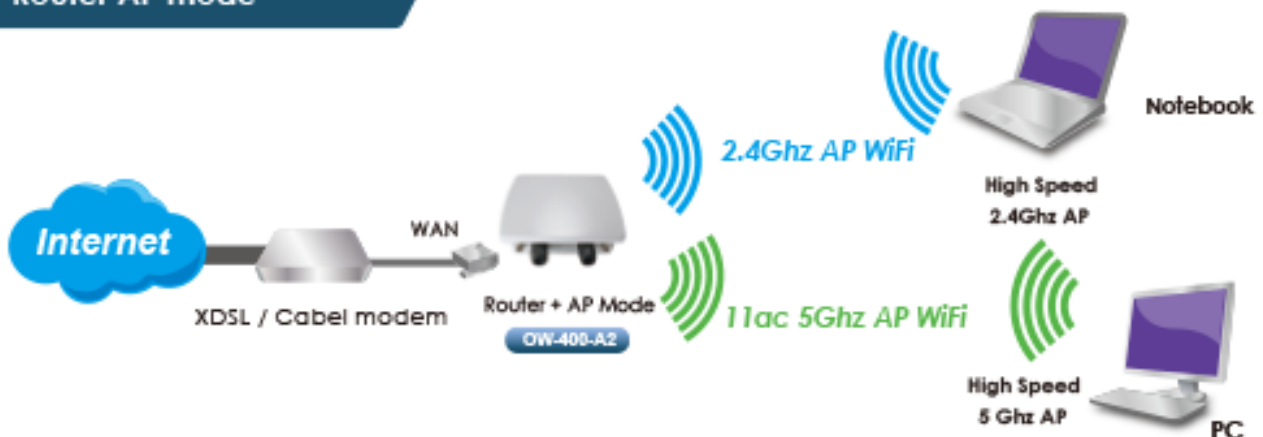
WISP + Repeater AP Mode



Route AP Mode

- Router AP without WDS , It can be deployed as a gateway with wireless Access Point
- Router AP with WDS, It can be deployed as a gateway with wireless Access Point and provide WDS link for network extension

Router AP mode



3. Access Point mode

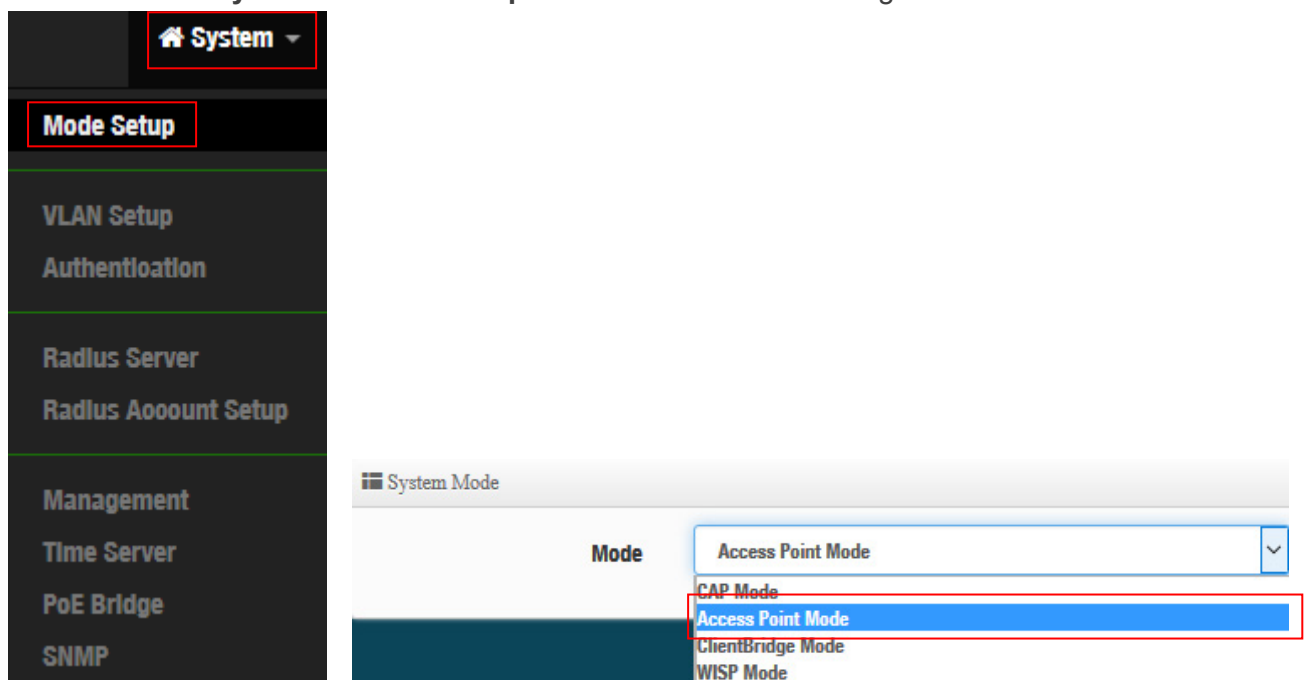
When AP mode is chosen, the system can be configured as an Access Point. This section provides detailed explanation for users to configure in the AP mode with help of illustrations. In the AP mode, functions listed in the table below are also available from the Web-based GUI interface.

3.1 Select AP Mode

The system administrator can set the desired mode via this page, and then configure the system according to their deployment needs.

When select Authentication AP mode, administrator can use Hotspot Portal function.

Please click on **System -> Mode Setup** and follow the below setting.



3.2 VLAN Setup

Here are the instructions to setup the local IP Address / Netmask / Gateway / DNS and management Access Point 2.4G or 5G Radio on/off. Administrators can change settings such as LAN Spanning Tree and Tag VLAN functions.

#	VLAN Mode	Flag	IP Address	Netmask	Radio 0	Radio 1	Action
0	On	Native ETH0 Access Control	192.168.2.254	255.255.255.0	2.4G_0_0	5G_0_1	Network
1	Off	ETH0.101	-	-	2.4G_1_0	5G_1_1	Network
2	Off	ETH0.102	-	-	2.4G_2_0	5G_2_1	Network
3	Off	ETH0.103	-	-	2.4G_3_0	5G_3_1	Network
4	Off	ETH0.104	-	-	2.4G_4_0	5G_4_1	Network
5	Off	ETH0.105	-	-	2.4G_5_0	5G_5_1	Network
6	Off	ETH0.106	-	-	2.4G_6_0	5G_6_1	Network

Gateway

Default Gateway:

DNS

DNS1:

DNS2:

- **VLAN Mode** : Display on/off for the VLAN network.
- **Flag** : Display master VLAN and VLAN Tag No. information.
- **IP Address** : Display IP Address for VLAN Network.
- **NetMask** : Display IP netmask.
- **Radio 0** : Display radio 2.4G SSID name.
- **Radio 1** : Display radio 5G SSID name.
- **Action** : The button can set VLAN network functions and radio functions.

3.2.1 Network Button

Administrator can click Network button to set VLAN network functions.

VLAN Setup

VLAN Mode: Enable Disable

IP Setup

IP Mode: Enable Disable

IP Address:

Netmask:

Management

Access Point 0: Enable Disable

Access Point 1: Enable Disable

802.1d Spanning Tree: Enable Disable

Control Port: Enable Disable

IAPP:

ETH0 VLAN Tag Setup

ETH0: Enable Disable

VLAN TAG: 1-4096

- **VLAN Mode** : Administrator can select Enable or disable for the VLAN Network.

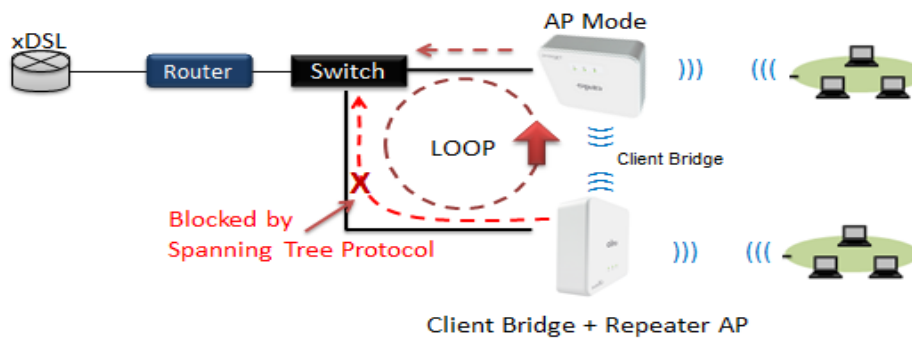


The VLAN list at least one must is enable.

- **IP Mode** : Administrator can select enable or disable function for VLAN IP.
- **IP Address/ NetMask** : Administrator can set IP address and netmask for the VLAN.

Management

- **Access Point 0** : Administrator can Enable or Disable 2.4G Radio.
- **Access Point 0** : Administrator can Enable or Disable 2.4G Radio.
- **802.1d Spanning Tree** : The spanning tree network protocol provides a loop free topology for a bridged LAN between LAN interface and 8 WDS interfaces from wds0 to wds7. The Spanning Tree Protocol, which is also referred to as STP, is defined in the IEEE Standard 802.1d

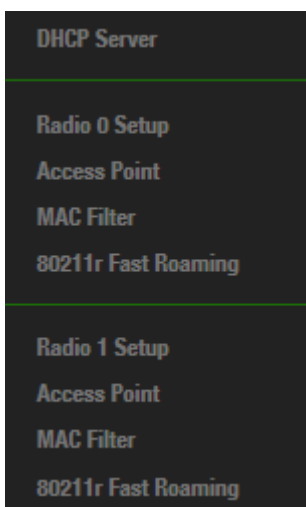


- **Control Port** : Administrator can select one of the VLAN as managed AP.
- **IAPP** : Administrator can select radio 2.4G or 5G for IAPP roaming. *(the IAPP condition must use WPA2-PSK Wi-Fi security and AES algorithm)*

3.2.2 Network Pull-down menu

Administrator can set DHCP Server and 2.4/5G security for the access point and set 802.11r fast roaming.

Please click **Network** pull-down button.



DHCP Server

Administrator can select enable / disable the function

DHCP Setup

Start IP	<input type="text"/>
End IP	<input type="text"/>
Netmask	<input type="text" value="255.255.255.0"/>
Gateway	<input type="text"/>
DNS1 IP	<input type="text"/>
DNS2 IP	<input type="text"/>
WINS IP	<input type="text"/>
Domain	<input type="text"/>
Lease Time	<input type="text" value="86400"/>

- **Start IP** : Set Start IP for DHCP Service.
- **End IP** : Set End IP for DHCP Service.
- **Netmask**: Set IP Netmask, the default is **255.255.255.0**
- **Gateway**: Set Gateway IP for DHCP Service.
- **DNS(1-2) IP** : Set DNS IP for DHCP Service.
- **WINS IP** : Enter IP address of the Windows Internet Name Service (WINS) server; this is optional.
- **Domain** : Enter the domain name for this network.
- **Lease Time** : The IP addresses given out by the DHCP server will only be valid for the duration specified by the lease time. Increasing the time ensure client operation without interruptions, but could introduce potential conflicts. Lowering the lease time will avoid potential address conflicts, but might cause more interruptions to the client while it will acquire new IP addresses from the DHCP server. Default is **86400** seconds

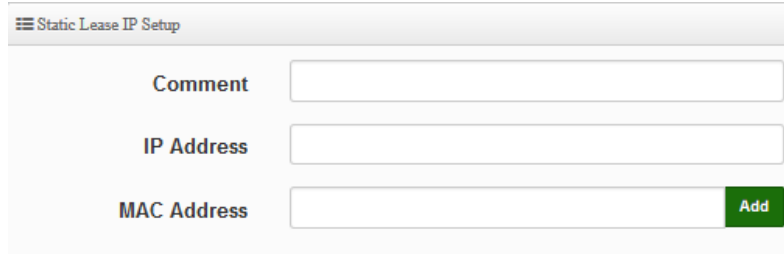
DHCP Client List

Administrator can view IP address used status of client users on each DHCP Server.

DHCP Client List				
#	IP Address	MAC Address	Expired	Action
-	-	-	-	-

Static Lease IP Setup

Administrator can set be delivered fixed IP address to the users.

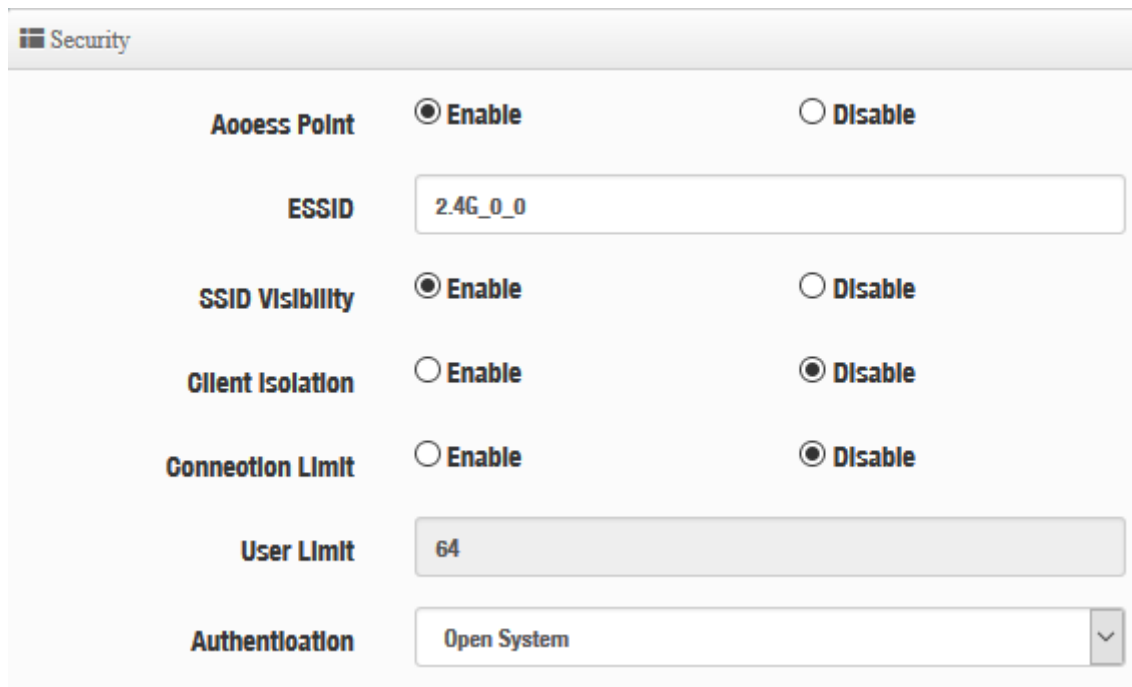


The form is titled "Static Lease IP Setup" and contains three input fields: "Comment", "IP Address", and "MAC Address". A green "Add" button is located to the right of the "MAC Address" field.

- **Comment** : Enter rule description.
- **IP Address** : Enter access point IP.
- **MAC Address** : Enter Client MAC Address of PC network.

Radio 0/1 Access Point

Administrator can Enable or Disable radio 0/1 (2.4/5G) Wi-Fi, if enable radio 0/1 (2.4/5G) administrator can set SSID and security for the 2.4/5G access point.

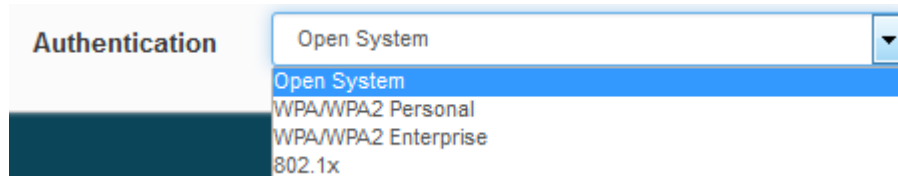


The form is titled "Security" and contains several configuration options:

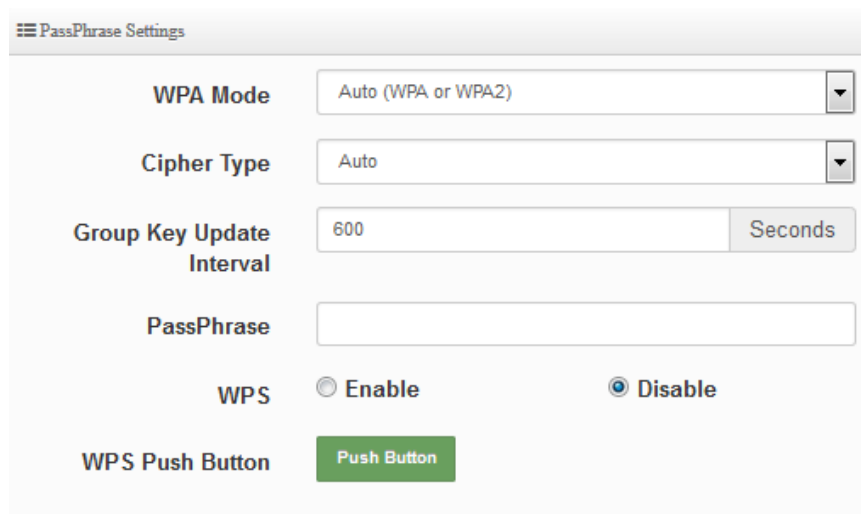
- Access Point**: Radio buttons for Enable and Disable.
- ESSID**: Text input field containing "2.4G_0_0".
- SSID Visibility**: Radio buttons for Enable and Disable.
- Client Isolation**: Radio buttons for Enable and Disable.
- Connection Limit**: Radio buttons for Enable and Disable.
- User Limit**: Text input field containing "64".
- Authentication**: Dropdown menu showing "Open System".

- **Access Point**: Administrator can Enable or Disable the radio 0 (2.4G).
- **ESSID**: Administrator can set Wi-Fi SSID name for the 2.4G.

- **SSID Visibility:** Administrator can select Enable or Disable the Visibility.
- **Client Isolation:** Enable or Disable the client isolation function.
- **Connection Limit:** Administrator can select Enable or Disable WiFi connection Limit.
- **User Limit:** If select enable of the connection Limit function, administrator can set users connection limit.
- **Authentication:** Select the desired security type from the drop-down list; the options are WPA-PSK, WPA2-PSK, WPA/WPA2-Enterprise and WEP 802.1X.



- **Open System:** Data is not unencrypted during transmission when this option is selected.
- **WPA/WPA2 Personal:** WPA/WPA2 is short for W-Fi Protected Access-Pre-Shared Key. WPA/WPA2 uses the same encryption way with WPA, and the only difference between them is that WPA/WPA2 recreates a simple shared key, instead of using the user's certification.



- ✓ WPA Mode: Administrator can select security for Auto or only WPA or only WPA2.
- ✓ Cipher Type: Administrator can select use AES or TKIP with WPA / WPA2 encryption method.

AES is short for “**Advanced Encryption Standard**”, The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plaintext into the final output of ciphertext. Each round consists of several processing steps, including one that depends on the encryption key. A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key.

TKIP is short for “**Temporal Key Integrity Protocol**”, TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven’t been tampered with.

- ✓ **Group Key Update Interval:** The time interval is for re-keying GTK (broadcast/multicast encryption keys) in seconds. Enter the time-length required; the default time is 600 seconds.
- ✓ **Pass Phrase:** Enter the ESSID pass phrase.
- ✓ **WPS:** Administrator can used WPS function to link WiFi client. If enabled, administrator can click the WPS Push Button.
- **802.1X security:** When 802.1x Authentication is enabled, please refer to the following Dynamic WEP and RADIUS settings to complete the configuration.

The screenshot shows the 'RADIUS Server Settings' configuration page. At the top, there is a title bar with a hamburger menu icon and the text 'RADIUS Server Settings'. Below this, there are two radio buttons for 'Key Size': '64 Bits' (which is selected) and '128 Bits'. Underneath, there are three input fields: 'Radius Server' (empty), 'Radius Port' (containing '1812' with a 'Port' button to its right), and 'Radius Secret' (empty).

- ✓ **Key Size:** Check on the respected button to enable either 64bits or 128bits key length. The system will automatically generate WEP keys for encryption.
- ✓ **Radius Server:** Enter the IP address of the Authentication RADIUS server.
- ✓ **Radius Port:** The port number used by Authentication RADIUS server. Use the default 1812 or enter port number specified.
- ✓ **Radius Secret:** The secret key for system to communicate with Authentication RADIUS server. Support 1 to 64 characters.

Click “**Save**” button to save your changes. Then click **Reboot** button to activate your changes.

MAC Filter

Administrator can set allow or reject Wi-Fi users connection access point.

Rule	Save
Disable	Save
Only Deny List MAC	
Only Allow List MAC	

- **Disable** : Disable MAC Filter function.
- **Only Deny List MAC** : Administrator can add wireless users MAC address in MAC list. The access point will deny connection in MAC address list.
- **Only Allow List MAC** : Administrator can add wireless users MAC address in MAC list. The access point will Allow connection in MAC address list.

Click “**Save**” button to save your changes. Then click **Reboot** button to activate your changes.

802.11r/802.11k Fast Roaming

The dual band Access Point supports 802.11r/802.11k function for 2.4G and 5G radio. 802.11r, which is the IEEE standard for fast roaming, introduces a new concept of roaming where the initial handshake with the new AP is done even before the client roams to the target AP.

Fast Roaming Settings

Mobility Domain: a1b2

R0 Key Lifetime: 10000

Reassoc deadline: 1000

R0/NAS Identifier: ap.example.com

R1 Identifier: 000102030405

R1 Push: Enable Disable

- **Mobility Domain:** MDID is used to indicate a group of APs (within an ESS, i.e., sharing the same SSID) between which a STA can use Fast BSS Transition. Please enter 2-octet identifier as a hex string.
- **R0 Key Lifetime:** Default lifetime of the PMK-RO in minutes, the default is 10000, administrator can setting 1~65535.
- **Reassoc deadline:** Reassociation deadline in time units (TUs / 1.024 ms; range 1000~65535). The default is 1000.

- **R0/NAS Identifier:** PMK-R0 Key Holder identifier. When using IEEE 802.11r, nas_identifier must be set and must be between 1 and 48 octets long.
- **R1 Identifier:** PMK-R1 Key Holder identifier 6-octet identifier as a hex string.
- **R1 Push:** Administrator can select Enable or disable. If enable the function will automatically sent the R1 Key.

R0 Key Address:

To enable roaming between multiple AP devices, AP1 must key in the MAC Address of AP2, and AP2 must key in the MAC Address of AP1. The NAS Identifier and 128-bit Key should be identical in both AP settings. This will enable device roaming between the two Access Points.

R0 Key holders

MAC Address	<input type="text" value="Destination MAC Address"/>
NAS Identifier	<input type="text" value="(1-48 octets)"/>
128-bit Key	<input type="text" value="128-bit key as hex string"/> Add

- **MAC Address:** Administrators must enter the MAC Address of other AP
- **NAS Identifier:** Enter 1~48 octets of network domain name.
- **128-bit Key:** Enter Shared Key of 128 bit.

R0 Key Holder List:

After setting "R0 Key holders" function the information will appear in list.

R0 Key Holder List				
#	MAC Address	NAS Identifier	128-bit Key	Action
-	-	-	-	-

R1 Key Holder List:

Enter a unified set of R1 Key Holder identification certification.

R1 Key Holders

MAC Address	<input type="text" value="Destination MAC Address"/>
R1 Identifier	<input type="text" value="R1 Identifier"/>
128-bit Key	<input type="text" value="128-bit key as hex string"/> Add

- **MAC Address:** Enter the main roaming device MAC address
- **R1 Identifier:** Enter Shared identifier.
- **128-bit Key:** Enter Shared Key of 128 bit.

R1 Key Holder List:

After setting "R1 Key holders" function the information will appear in list.

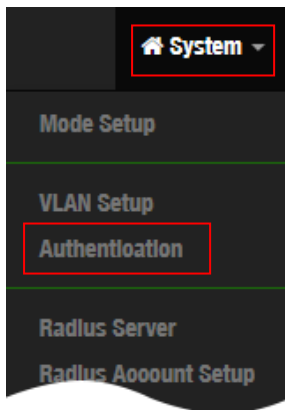
R1 Key Holder List				
#	MAC Address	NAS Identifier	128-bit Key	Action
-	-	-	-	-

Click **Save** button to save your changes. Then click **Reboot** button to activate your changes.

3.3 Authentication

The function is for Web Authentication. It supports authentication for local users / RADIUS Server / OAuth2.0 and Guest. The system support 16 VLAN with web authentication.

Please click on **System -> Authentication**



VLAN List			
#	VLAN Mode	Authentication	Action
0	On	Off	Authentication
1	Off	Off	Authentication
2	Off	Off	Authentication
3	Off	Off	Authentication
4	Off	Off	Authentication
5	Off	Off	Authentication

- # : Display 16 VLAN number.
- **VLAN Mode** : Displays VLAN on/off status.
- **Authentication** : Displays VLAN# whether enable or disable web authentication.
- **Action** : The function has 2 buttons (Authentication and Dropdown)

Authentication Button:



: By clicking the Authentication button, administrator can enable or disable this function.

<div style="border: 1px solid #ccc; padding: 5px;"> <p>Authentication</p> <p>Authentication <input checked="" type="radio"/> Enable <input type="radio"/> Disable</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 5px;"> <p>Authentication Setup</p> <p>Multiple Login <input type="checkbox"/> 3 User(s)</p> <p>Login Timeout 10 Minutes</p> <p>Redirect URL http://www.google.com</p> <p>Login URL domain6.login</p> <p>Session Log <input type="radio"/> Enable <input checked="" type="radio"/> Disable</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 5px;"> <p>Local User Setup</p> <p>Local User <input type="radio"/> Enable <input checked="" type="radio"/> Disable</p> </div>	<div style="border: 1px solid #ccc; padding: 5px;"> <p>Radius Setup</p> <p>Radius <input type="radio"/> Enable <input checked="" type="radio"/> Disable</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 5px;"> <p>Bandwidth Control</p> <p>Peer Users <input type="radio"/> Enable <input checked="" type="radio"/> Disable</p> <p>Total <input type="radio"/> Enable <input checked="" type="radio"/> Disable</p> </div>
--	--

- **Authentication** : Administrator can enable or disable authentication function.
- **Multiple Login** : Administrator can set one account to multiple users simultaneously login and the users can set limit.(0 = not limited)
- **Login Timeout** : After account login for some time no traffic, system will automatic timeout for account. Administrator can enter a time(Minutes).
- **Redirect URL** : After the success of the login, system will redirect to URL. Administrator can enter web site URL.
- **Login URL** : Administrator can set URL for login page.
- **Session Log** : If network have Syslog server. Administrator can to system→management setting IP address for syslog server and enable the function. Account session log will copy to syslog server.
- **Local User** : Administrator can enable authentication for local user. Create user account can to reference “3.3.2 Local User”.

- **RADIUS** : Authentication support remote RADIUS Server. Administrator can enter security information for remote RADIUS Server.
- **Bandwidth Control** : Administrator can be control traffic by Users or total.

Bandwidth Control

Peer Users Enable Disable

Upload 512 Kbps

Download 512 Kbps

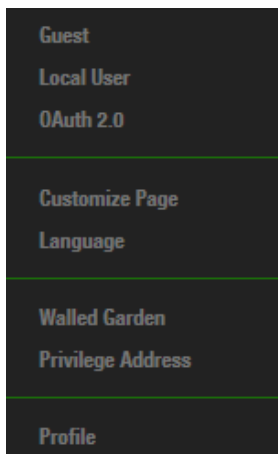
Total Enable Disable

Upload 512 Kbps

Download 512 Kbps

Authentication Dropdown Button

Authentication  : By Clicking the Dropdown button, Administrators can set authentication functions.



3.3.1 Guest

Administrator can enable or disable guest authentication. If enabled, the administrator can set guest Count Limit / login time and type and flow control.

Guest

Service Enable Disable

Login Type One Time Multiple Time

Count Limit

Login Time **Minutes**

QoS Enable Disable

Upload **Kbps**

Download **Kbps**

- **Service** : Administrator can select enable or disable this function.
- **Login Type** :
 - **One Time**: Login to start counting until the end of time.
 - **Multiple Times**: logout time will stop counting until the next re-login to time start counting.
- **Count Limit**: Administrator can set guest limit.
- **Login Time**: Within a certain timeframe with no traffic, the system will auto logout.
- **QoS**: Administrator can restrict the traffic of guest. Traffic management can set users upload and download traffic.

3.3.2 Local User

Administrator can create local user account for web login.

Local User

User Name

Password **Add**

Local User List

#	Name	Action
1	oerio	Delete
2	danny	Delete

- **User Name** : Administrator can create users account.
- **Password** : Set account password.

3.3.3 OAuth2.0

The OAuth2.0 function supports Facebook and Google by default. Users can add additional OAuth2.0 servers through UI settings.

OAuth 2.0 Provider List			Create New Provider
#	Active	Provider	Action
1	<input type="checkbox"/> Off	Google	<input type="button" value="Edit"/>
2	<input type="checkbox"/> Off	Facebook	<input type="button" value="Edit"/>

- **#** : Display items.
- **Active** : Display on/off status for the authentication.
- **Provider** : Display authentication server. The system default use authentication server for Google and Facebook

※ Sample for Google OAuth2.0 setup

Please complete the application on the Google website to receive an account ID and password, follow the steps below.

Step.1 Please go to the **Google Developers Console page** and **create a project**

(Reference <https://developers.google.com/identity/protocols/OAuth2>)

New Project

Project name [?]

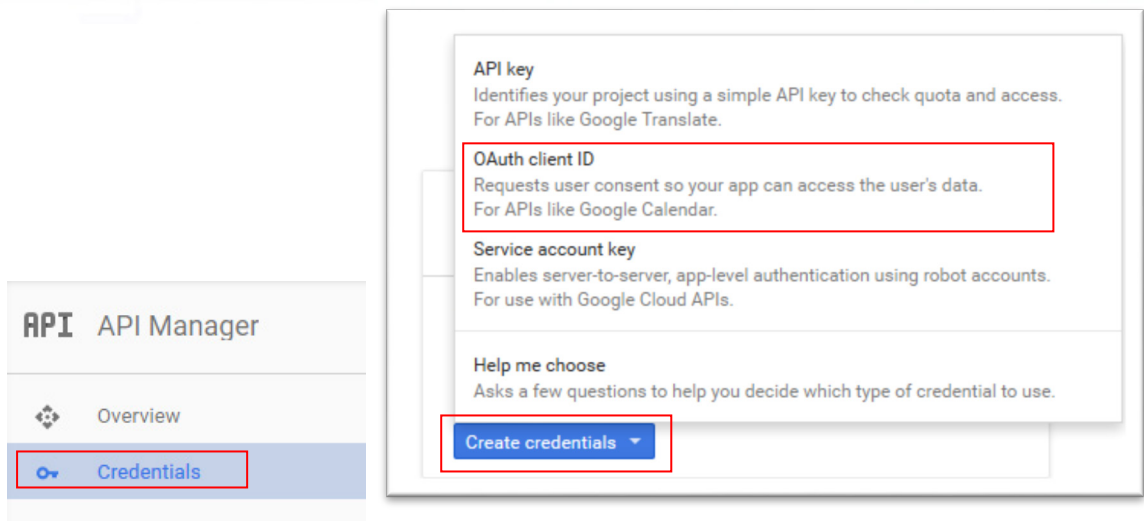
CERIO-AAP-login

Your project ID will be cerio-aap-login [?] Edit

Show advanced options...

Create Cancel

Step.2 Click Credentials to create OAuth client ID in the API manager page.



Step.3 Select web application in the “Application Type” section and set “Restrictions” URL.

Create client ID

Application type

- Web application
- Android [Learn more](#)
- Chrome App [Learn more](#)
- iOS [Learn more](#)
- PlayStation 4
- Other

Create

Cancel

Name

Web client 1

Restrictions

Enter JavaScript origins, redirect URIs, or both

Authorized JavaScript origins

For use with requests from a browser. This is the origin URI of the client application. It can't contain a wildcard (http://*.example.com) or a path (http://example.com/subdir). If you're using a nonstandard port, you must include it in the origin URI.

http://www.example.com

Authorized redirect URIs

For use with requests from a web server. This is the path in your application that users are redirected to after they have authenticated with Google. The path will be appended with the authorization code for access. Must have a protocol. Cannot contain URL fragments or relative paths. Cannot be a public IP address.

http://www.example.com/oauth2callback

Step.4 Set Authorized JavaScript origins and Authorized redirect URLs (**important**)

Administrator must set login URL in the device function. After complete set of login URL go to the “**Restrictions**” function in web page. Follow the steps below to set login URLs

- Setup login URL in the device. Please Click **system**➔**Authentication** and enable the function.
- The “Authentication Setup” page to set Login URL

After complete set of login URL go to the “**Restrictions**” function in web page. Copy and paste the login URL from the system display into the “Restriction” page on the Google Developer website.

- Google Authorized JavaScript origins URL is **http://domain0.login.com** (same as Login URL)
- Google Authorized redirect URLs is **http://domain0.login.com/login/index.cgi?cgi=CALLBACK**

Authorized JavaScript origins

For use with requests from a browser. This is the origin URI of the client application. It can't contain a wildcard (http://*.example.com) or a path (http://example.com/subdir). If you're using a nonstandard port, you must include it in the origin URI.

Authorized redirect URIs

For use with requests from a web server. This is the path in your application that users are redirected to after they have authenticated with Google. The path will be appended with the authorization code for access. Must have a protocol. Cannot contain URL fragments or relative paths. Cannot be a public IP address.

Step.5 After completing the “Restrictions” setup, click the create button. A OAuth Client page will pop-up with your “client ID” and “client secret”. Administrators must copy and paste their client ID and secret into the OAuth 2.0 Setup page in our software UI.

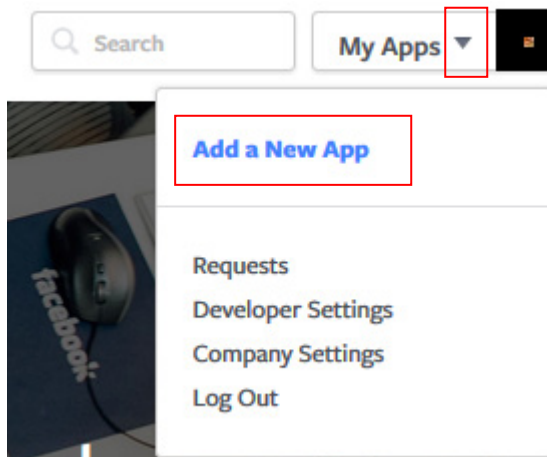
The image shows two screenshots of the Cerio software interface. The top screenshot is a modal window titled "OAuth client". It contains two text input fields: "Here is your client ID" with a value ending in "googleusercontent.com" and "Here is your client secret" with a value ending in "kDYwM". There is a blue "OK" button at the bottom. The bottom screenshot is the "OAuth 2.0 Setup" page, which has a green "Advanced" button in the top right. It features two input fields: "Client ID" with a value ending in "pps.googleuse" and "Client Secret" with a value ending in "YwM".

Save and reboot the AP system, complete the setup.

※ **Sample for Facebook OAuth2.0 setup**

Please complete the application on the Facebook website to receive an account ID and password, follow the steps below.

Step.1 Please to Facebook developers page and add a New App



Step.2 Select WWW function

Add a New App

Select a platform to get started



IOS



Android



Facebook Canvas



Website

If you're developing on another platform or want to skip this step for now, use the [basic setup](#).

Step.3 Administrator must set www for your information.

Create a New App ID

Get started integrating Facebook into your app or website

Display Name

The name of your app or website'

Namespace

'A unique identifier for your app (optional)'

Contact Email

Used for important communication about your app

Category

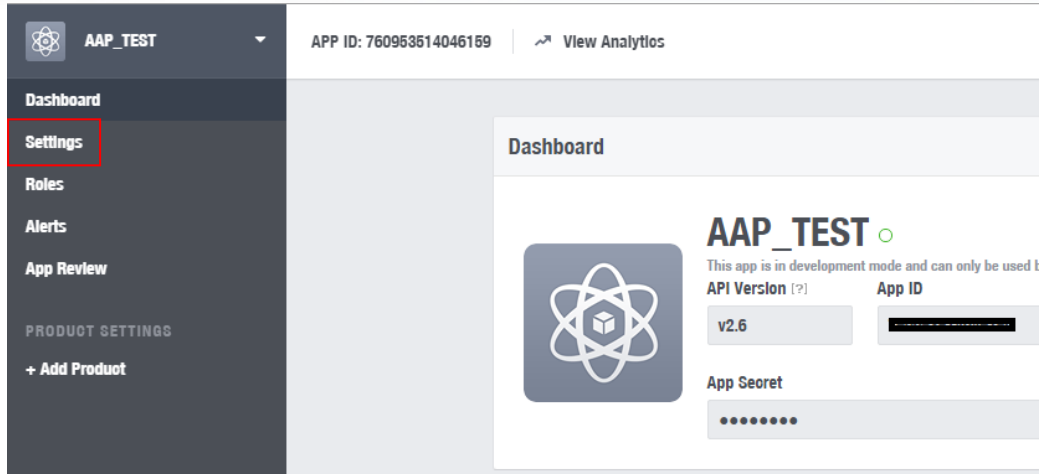
Choose a Category ▾

By proceeding, you agree to the [Facebook Platform Policies](#)

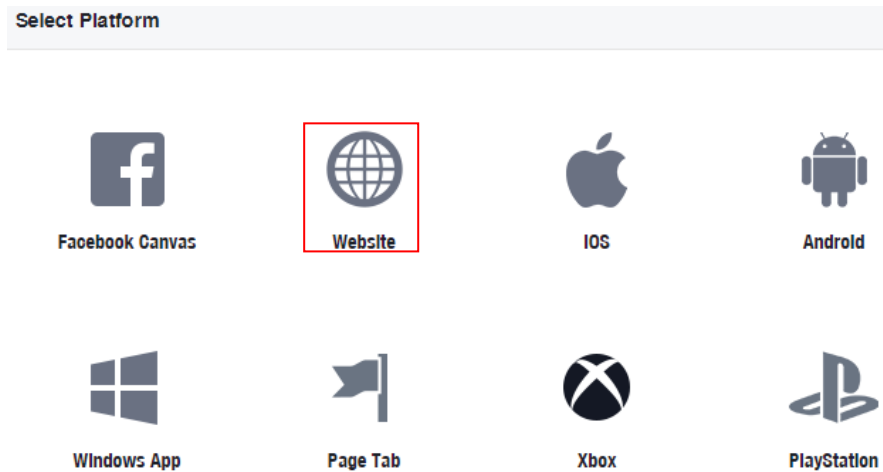
Cancel

Create App ID

Step.4 Please click “**Setting**” and add Platform



Step.5 Select Platform for “Website”



Step.6 Enter URL is **http://domain0.login.com/login/index.cgi?cgi=CALLBACK**

Site URL

Administrator must set login URL in the device function. After complete set of login URL go to the “Facebook Site URL” function in web page. Follow the steps below to set login URLs

- Setup login URL in the device. Please Click **system** → **Authentication** and enable the function.
- The “**Authentication Setup**” page to set Login URL

Authentication Setup

Multiple Login 3 User(s)

Login Timeout 10 Minutes

Redireot URL http://www.google.com

Login URL domain0.login.com

Session Log Enable Disable

After complete set of login URL go to the “Facebook Site URL” function in web page. Copy and paste the login URL from the system display into the “Site URL” page on the Facebook website.

Step.7 Click Advanced function to enable the “Native or desktop app?” and “Is App Secret embedded in the client?”

Settings


- Basic
- Advanced**
- Roles
- Alerts

Basic | **Advanced**

Yes **Native or desktop app?**
Enable if your app is a native or desktop app

Yes **Is App Secret embedded in the client?**
This restricts the app secret usage to methods allowed by a client token [?]

Step.8 After completing the “Facebook Site URL” setup. Administrators must copy and paste their App ID and App secret into the OAuth 2.0 Setup page in our software UI.

AAP_TEST 

This app is in development mode and can only be used by app admins, developers and testers [?]

API Version [?] v2.6

App ID [REDACTED]

App Secret [REDACTED]26

The screenshot shows the 'OAuth 2.0 Setup' configuration page. At the top right, there is a green 'Advanced' button. Below the title, there are two input fields: 'Client ID' with a value ending in '9' and 'Client Secret' with a value ending in '26'. Both fields are partially obscured by black redaction bars.



Client ID and Client Secret setup by third parties such as Facebook and Google are subject to change. The instructions above follow the 2016 setup procedure. Any future changes to the Facebook/Google process may lead to our instructions becoming invalid.

3.3.4 Customize Page

This function is to customized the user Login Page. This supports Multiple Language and allows comprehensive customization through HTML editing.

The screenshot displays the 'Page Setup' and 'Preview' interface. The 'Page Setup' panel on the left includes:

- Page Setup:** 'Template' with radio buttons for 'Enable' (selected) and 'Disable'; 'Multiple Language' with radio buttons for 'Enable' and 'Disable' (selected).
- Page Color Setup:** 'Style' dropdown set to 'Default' with an 'Apply' button; 'Body Background' (#EEEEEE); 'Content Background' (#FFFFFF); 'Font Color' (#333333); 'Content Width' (350 px); 'AD Background' (#47A747); 'AD Font Color' (#FFFFFF).

The 'Preview' panel on the right shows a login form titled 'Please sign in' with fields for 'User Name' and 'Password', a 'Remember me' checkbox, a green 'Sign in' button, and a blue 'Guest' button. Below the form are six green buttons labeled AD1 through AD6.

Page Setup

- **Template** : Administrator can select Enable or disable.
 - Select enable to active default Login Page

Please sign in

Remember me

Sign in

Guest

AD1

AD2

AD3

AD4

AD6

- Select disable to active HTML Source code window for customization

Customize HTML Source code

```

<html>
  <head>
    <title>Hotspot</title>
    <script src="/jscripts/login.js" charset="utf-8" type="text/javascript"></script>
  </head>
  <body>
    <div class="container"></div>
  </body>
</html>

```

Sample: See sample login page below that is customized by html coding (*sample login page html code templates are available on Cerio website*)

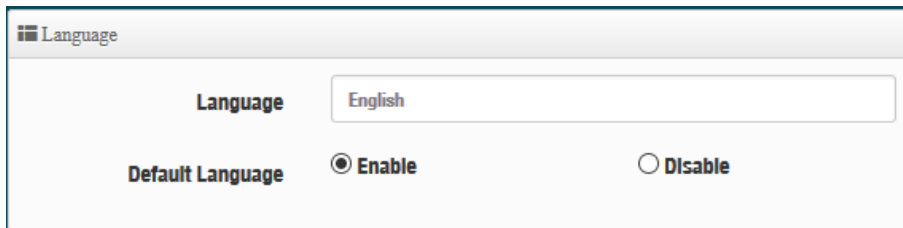


The following function is by Template Enable

- **Multiple Language** : Administrator can select enable or disable multiple language for login page. Administrator must to Language function create new language.
- **Page Color Setup** : Administrator can change the login page color.

3.3.5 Language

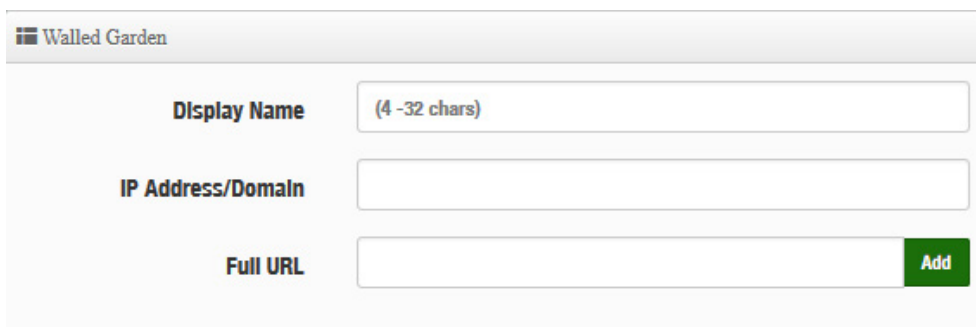
Administrator can create other language for login page.



Language configuration interface showing a dropdown menu for Language (English) and radio buttons for Default Language (Enable/Disable).

3.3.6 Walled Garden

This function provides certain free services or advertisement web pages for users to access the websites listed before login and authentication. User without the network access right can still have a chance to experience the actual network service free of charge in Walled Garden URL list.

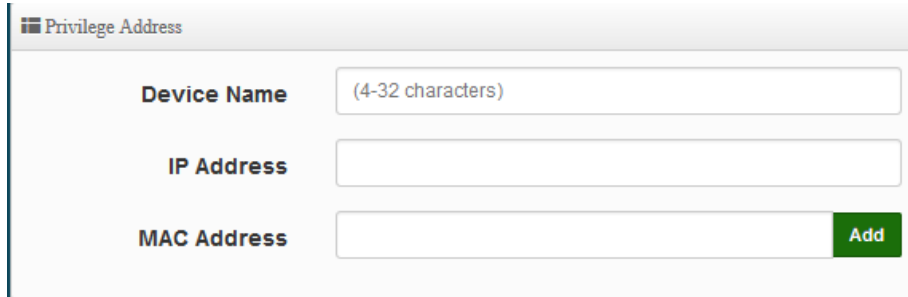


Walled Garden configuration interface showing input fields for Display Name (4 -32 chars), IP Address/Domain, and Full URL, with an Add button.

- **Display Name**: Set name of Website.
- **IP Address/Domain**: Set IP or Domain of the Open the website.
- **Full URL**: Set full website name.

3.3.7 Privilege Address

This function provides local device can access Internet without authentication. If there are some workstations belonging NGS Access Point that need to access to network without authentication, enter the IP or MAC address of these workstations in this list.



Privilege Address

Device Name (4-32 characters)

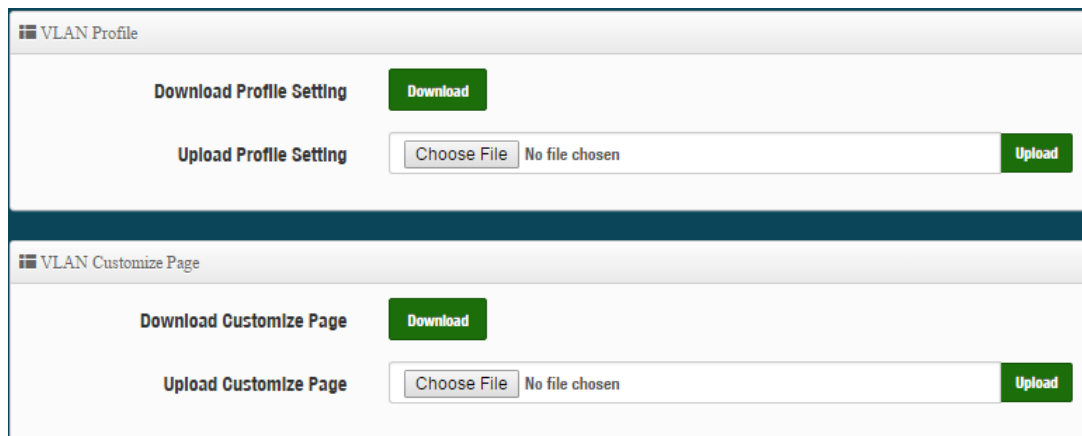
IP Address

MAC Address

- **Device Name:** Enter Device or Users Name.
- **IP Address:** Enter used IP Address of Device or Users PC.
- **MAC Address:** Enter MAC Address of Device or Users PC.

3.3.8 Profile

Administrator can backup current authentication configuration and login page for HTML Source code. But also can recover.



VLAN Profile

Download Profile Setting

Upload Profile Setting No file chosen

VLAN Customize Page

Download Customize Page

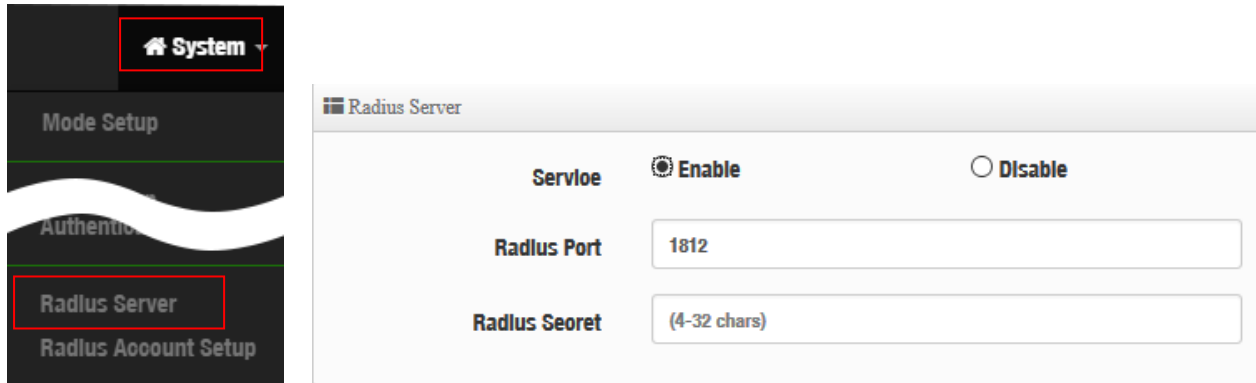
Upload Customize Page No file chosen

Click **“Save”** button to save your changes. Then click **Reboot** button to activate your changes.

3.4 RADIUS Server

The function is 802.1x RADIUS Server. Administrator can enable or disable Server.

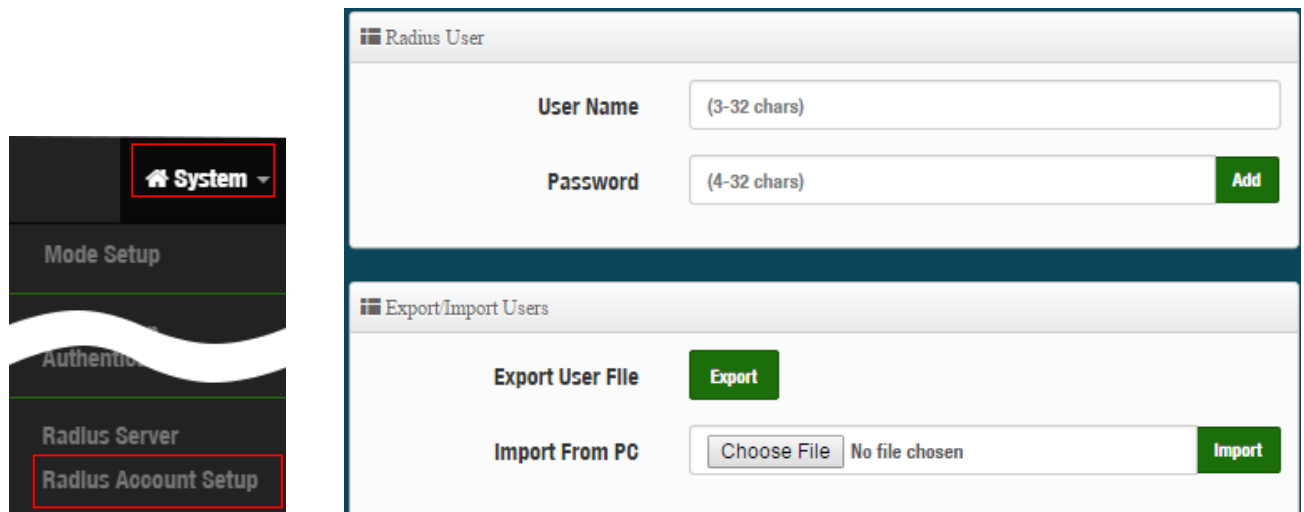
Please click on **System** → **RADIUS Server**



- **Service** : Administrator can select Enable or disable the function.
- **Radius** : Administrator must to set remote RADIUS Server use Port.
- **Radius Secret** : Administrator must to set remote RADIUS Server use Key.

3.5 Radius Account Setup

When enabled RADIUS Server, administrator can add RADIUS account and password in the function. But also can recover or backup the RADIUS account



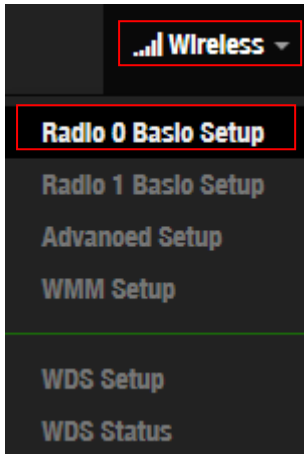
- **User Name** : Create users name for RADIUS account.
- **Password** : Enter password for user name.
- **Export User File** : Administrator can export account list in RADIUS Server.
- **Import From PC** : Administrator can import account list to the RADIUS Server.

Click **“Save”** button to save your set function. Then click Reboot button to activate your changes.

3.6 Wireless Basic Setup

This section includes the main base station setup procedures for 2.4G / 5G Wifi functions · Wi-Fi Advanced setup · WMM · WDS and WDS Status

3.6.1 Radio 0 Basic Setup (2.4G)



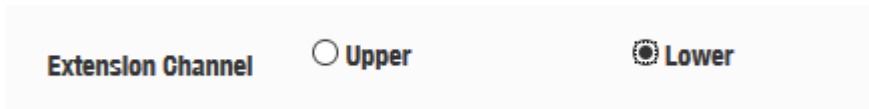
General setup

A screenshot of the 'General Setup' configuration page. The page title is 'General Setup'. The configuration fields are as follows:

MAC Address	8c:4d:ea:04:d0:69
Country	Taiwan
Band Mode	802.11n
Auto Channel	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Channel	5 (2432 Mhz)
Tx Power	Level 9
Slot Time	13 Distance
ACK Timeout	93

- **MAC Address:** Display 2.4G WiFi MAC address.
- **Country:** Administrator can select country: US or EU or Taiwan.
- **Band Mode:** Administrator can select 802.11b/g/n for the 2.4G Band.
- **Auto Channel:** Administrator can Enable or Disable the function. If disabled, the WiFi channel will be fixed to the manually selected channel.

- **Channel:** Administrator can select 1 to 11 CH. The Channel settings can be changed in “HT Physical Mode” →” **Extension Channel**” can select **Upper** or **Lower** channels.



- **Tx Power:** Administrator can control the WiFi Tx output power. The power Max. Level 9.
- **Slot Time :** Slot time is in the range of **9~1489** and set in unit of **microsecond**. The default value is **9** microsecond.

Slot time is the amount of time a device waits after a collision before retransmitting a packet. Reducing the slot time decreases the overall back-off, which increases throughput. Back-off, which is a multiple of the slot time, is the random length of time a station waits before sending a packet on the LAN. For a sender and receiver own right of the channel the shorter slot time help manage shorter wait time to re-transmit from collision because of hidden wireless clients or other causes. When collision sources can be removed sooner and other senders attempting to send are listening the channel(CSMA/CA) the owner of the channel should continue ownership and finish their transmission and release the channel. Then, following ownership of the channel will be sooner for the new pair due to shorter slot time. However, when long duration of existing collision sources and shorter slot time exist the owners might experience subsequent collisions. When adjustment to longer slot time can't improve performance then RTS/CTS could supplement and help improve performance.

- **ACK Timeout :** ACK timeout is in the range of **1~372** and set in unit of **microsecond**. The default value is **64** microsecond.

All data transmission in 802.11b/g request an “Acknowledgement” (ACK) send by receiving radio. The transmitter will resend the original packet if correspondent ACK failed to arrive within specific time interval, also refer to as “ACK Timeout”.

ACK Timeout is adjustable due to the fact that distance between two radio links may vary in different deployment. ACK Timeout makes significant influence in performance of long distance radio link. If ACK Timeout is set too short, transmitter will start to “Resend” packet before ACK is received, and throughput become low due to excessively high re-transmission.

ACK Timeout is best determined by distance between the radios, data rate of average environment. The Timeout value is calculated based on round-trip time of packet with a little tolerance, So, if experiencing re-transmissions or poor performance the ACK Timeout could be made longer to accommodate.



Slot Time and ACK Timeout settings are for long distance links. It is important to tweak settings to achieve the optimal result based on requirement.

HT Physical Mode

HT Physical Mode

TX/RX Stream

Channel BandWidth 20 20/40

Extension Channel Upper Lower

MCS

Short GI Enable Disable

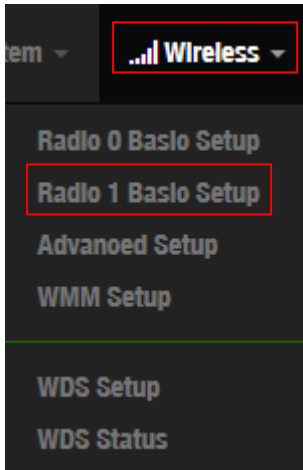
Aggregation Enable Disable

Aggregation Frames

Aggregation Size

- **TX/RX Stream:** The OW-400-A2 utilizes 2 antenna and supports 2TX/2RX streams. Administrator can select 1 or 2 TX/RX. The default is 2TX/2RX.
- **Channel Bandwidth:** The "20/40" MHz option is usually best. The other option is available for special circumstances.
- **Extension Channel:** Sets channel select to Upper or Lower. The Upper supports 1 to 7 range CH and Lower supports 5 to 11 range CH.
- **MCS:** This parameter represents transmission rate. By default (Auto) the fastest possible transmission rate will be selected. You have the option of selecting the speed if necessary.
- **Short GI:** Short Guard Interval is "Enabled" by default to increase throughput. However, it can also increase error rate in some installations, due to increased sensitivity to radio-frequency reflections. Select the option that works best for your installation.
- **Aggregation:** By default, it's "Enabled". Select "Disable" to deactivate Aggregation. A part of the 802.11n standard (or draft-standard), it allows sending multiple frames per single access to the medium by combining frames together into one larger frame. It creates the larger frame by combining smaller frames with the same physical source and destination end points and traffic class (i.e. QoS) into one large frame with a common MAC header.
- **Aggregation Frames :** The Aggregation Frames is in the range of 2~64, default is 32. It determines the number of frames combined on the new larger frame.
- **Aggregation Size :** The Aggregation Size is in the range of 1024~65535, default is 50000. It determines the size (in Bytes) of the larger frame.

3.6.2 Radio 1 Basic Setup (5G)



General Setup

A screenshot of the 'General Setup' configuration page. The page contains the following fields and options:

- MAC Address:** 8c:4d:ea:04:d0:6a
- Country:** Taiwan
- Band Mode:** 802.11ac
- Auto Channel:** Enable Disable
- Channel:** 100 (5500 Mhz)
- Tx Power:** Level 9
- Slot Time:** 9 (with a 'Distance' button)
- ACK Timeout:** 30

- **MAC Address:** Display 2.4G WiFi MAC address.
- **Country:** Administrator can select country: US or EU or Taiwan.
- **Band Mode:** Administrator can select 5G Band for 802.11a/n or 802.11ac. The default is 802.11ac
- **Auto Channel:** Administrator can Enable or Disable the function. If select disabled function the WiFi channel can be manually fixed.
- **Channel:** Supports US and EU country 5G Channel standards.
- **Tx Power:** Administrator can control the WiFi Tx output power. The power Max. Level 9.

- **Slot Time** : Slot time is in the range of **9~1489** and set in unit of **microsecond**. The default value is **9** microsecond.

Slot time is the amount of time a device waits after a collision before retransmitting a packet. Reducing the slot time decreases the overall back-off, which increases throughput. Back-off, which is a multiple of the slot time, is the random length of time a station waits before sending a packet on the LAN. For a sender and receiver own right of the channel the shorter slot time help manage shorter wait time to re-transmit from collision because of hidden wireless clients or other causes. When collision sources can be removed sooner and other senders attempting to send are listening the channel(CSMA/CA) the owner of the channel should continue ownership and finish their transmission and release the channel. Then, following ownership of the channel will be sooner for the new pair due to shorter slot time. However, when long duration of existing collision sources and shorter slot time exist the owners might experience subsequent collisions. When adjustment to longer slot time can't improve performance then RTS/CTS could supplement and help improve performance.

- **ACK Timeout** : ACK timeout is in the range of **1~372** and set in unit of **microsecond**. The default value is **64** microsecond.

All data transmission in 802.11b/g request an "Acknowledgement" (ACK) send by receiving radio. The transmitter will resend the original packet if correspondent ACK failed to arrive within specific time interval, also refer to as "ACK Timeout".

ACK Timeout is adjustable due to the fact that distance between two radio links may vary in different deployment. ACK Timeout makes significant influence in performance of long distance radio link. If ACK Timeout is set too short, transmitter will start to "Resend" packet before ACK is received, and throughput become low due to excessively high re-transmission.

ACK Timeout is best determined by distance between the radios, data rate of average environment. The Timeout value is calculated based on round-trip time of packet with a little tolerance, So, if experiencing re-transmissions or poor performance the ACK Timeout could be made longer to accommodate.



Slot Time and ACK Timeout settings are for long distance links. It is important to tweak settings to achieve the optimal result based on requirement.

HT Physical Mode

HT Physical Mode

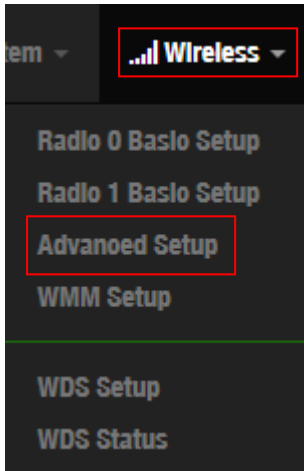
TX/RX Stream	<input type="text" value="2T2R"/>
Channel BandWidth	<input type="text" value="80"/>
Short GI	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Aggregation	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Aggregation Frames	<input type="text" value="32"/>
Aggregation Size	<input type="text" value="50000"/>

- **TX/RX Stream:** The OW-400-A2 utilizes 2 antennas and supports 2TX/2RX streams. Administrator can select 1 or 2 TX/RX. The default is 2TX/2RX.
- **Channel Bandwidth:** The "20/40 and 802.11ac 80" MHz option is usually the best. The other option is available for special circumstances.
- **Short GI:** Short Guard Interval is "Enabled" by default to increase throughput. However, it can also increase error rate in some installations, due to increased sensitivity to radio-frequency reflections. Select the option that works best for your installation.
- **Aggregation:** By default, it's "Enable". Select "Disable" to deactivate Aggregation. A part of the 802.11n standard (or draft-standard). It allows sending multiple frames per single access to the medium by combining frames together into one larger frame. It creates the larger frame by combining smaller frames with the same physical source and destination end points and traffic class (i.e. QoS) into one large frame with a common MAC header.
- **Aggregation Frames :** The Aggregation Frames is in the range of 2~64, default is 32. It determines the number of frames combined on the new larger frame.
- **Aggregation Size :** The Aggregation Size is in the range of 1024~65535, default is 50000. It determines the size (in Bytes) of the larger frame.

Click "Save" button to save your set function. Then click "Reboot" button to activate your changes.

3.6.3 Advanced Setup

The administrator can change the Slot Time, ACK Timeout, RTS threshold and fragmentation threshold settings for the system. Please click on **Wireless -> Advanced Setup** and follow the below setting.



A screenshot of the 'Advanced Setup' configuration page. The page contains the following settings:

- Beacon Interval:** 100
- DTIM Interval:** 1
- Fragment Threshold:** 2346
- RTS Threshold:** 2346
- Short Preamble:** Enable Disable
- IGMP Snooping:** Enable Disable
- Greenfield:** Enable Disable
- Band Steering:** 10 **RSSI Limit**

- **Beacon Interval:** Beacon Interval is in the range of **40~3500** and set in unit of *millisecond*. The default value is **100** msec.
Access Point (AP) in IEEE 802.11 will send out a special approximated 50-byte frame, called "Beacon". Beacon is broadcast to all the stations, provides the basic information of AP such as SSID, channel, encryption keys, signal strength, time stamp, support data rate. All the radio stations received beacon recognizes the existence of such AP, and may proceed next actions if the information from AP matches the requirement. Beacon is sent on a periodic basis, the time interval can be adjusted.

By increasing the beacon interval, you can reduce the number of beacons and associated overhead, but that will likely delay the association and roaming process because stations scanning for available access points may miss the beacons. You can decrease the beacon interval, which increases the rate of beacons. This will make the association and roaming process very responsive; however, the network will incur additional overhead and throughput will go down.

- **DTIM Interval** : The DTIM interval is in the range of **1~255**. The default is **1**.
DTIM is defined as *Delivery Traffic Indication Message*. It is used to notify the wireless stations, which support power saving mode, when to wake up to receive multicast frame. DTIM is necessary and critical in wireless environment as a mechanism to fulfill power-saving synchronization.
A DTIM interval is a count of the number of beacon frames that must occur before the access point sends the buffered multicast frames. For instance, if DTIM Interval is set to 3, then the Wi-Fi clients will expect to receive a multicast frame after receiving three Beacon frame. The higher DTIM interval will help power saving and possibly decrease wireless throughput in multicast applications.
- **Fragmentation Threshold**: Fragmentation Threshold is one more parameter which is given in all stations and Access points. Fine tuning Fragmentation Threshold parameter can result in good throughput but not using it properly can results in low throughput. In simple words it does the same thing which MTU do in Ethernet. Both are different parameters but the work done is same, it fragments the data packets.
Fragmentation threshold will be used when we have more data packet size to be transmitted and we have less fragment threshold value. Lets say from Ethernet we have to send 1400 byte packet but the fragmentation threshold is set as 400. In this case when the packet is to be transmitted on air it will fragment the packet in to 4 small packet 400+400+400+200 and send on air. This includes MAC header+ frame body and CRC so 400 byte will be in total including headers. This helps in increasing the throughput. The default is 2346.
- **RTS Threshold**: TRTS Threshold is in the range of **1~2347** byte. The default is **2347** byte. The main purpose of enabling RTS by changing RTS threshold is to reduce possible collisions due to hidden wireless clients. RTS in AP will be enabled automatically if the packet size is larger than the Threshold value. By default, RTS is disabled in a normal environment supports non-jumbo frames.
- **Short Preamble**: By default, this function is "**Enabled**". **Disabling** will automatically use the Long 128-bit Preamble Synchronization field. The preamble is used to signal "here is a train of data coming" to the receiver. The short preamble provides 72-bit Synchronization field to improve WLAN transmission efficiency with less overhead.

- **IGMP Snooping:** The process of listening to Internet Group Management Protocol (IGMP) network traffic. The feature allows a network switch to listen in on the IGMP conversation between hosts and routers. By listening to these conversations the switch maintains a map of which links need which IP multicast streams. Multicasts may be filtered from the links which do not need them and thus controls which ports receive specific multicast traffic.
- **Greenfield:** In wireless WLAN technology, greenfield mode is a feature of major components of the 802.11n specification. The greenfield mode feature is designed to improve efficiency by eliminating support for 802.11b/g devices in an all draft-n network. In greenfield mode the network can be set to ignore all earlier standards.
- **Band Steering: Dual band operation with Band Steering** detects clients capable of 5 GHz operation and steers them to that frequency which leaves the more crowded 2.4 GHz band available for legacy clients. This helps improve end user experience by reducing channel utilization, especially in high density environments. The default RSSI Limit :10

3.6.4 WMM Setup

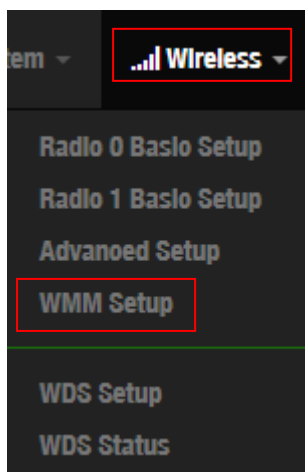
This affects traffic flowing from the access point to the client station.

Configuring QoS options consists of setting parameters on existing queues for different types of wireless traffic. You can configure different minimum and maximum wait times for the transmission of packets in each queue based on the requirements of the media being sent.

Queues automatically provide minimum transmission delay for Voice, Video, multimedia, and mission critical applications, and rely on best-effort parameters for traditional IP data.

As an Example, time-sensitive Voice & Video, and multimedia are given effectively higher priority for transmission (lower wait times for channel access), while other applications and traditional IP data which are less time-sensitive but often more data-intensive are expected to tolerate longer wait times.

Please click on **Wireless -> WMM Setup**



WMM Setup

WMM Enable Disable

➤ **WMM:** Administrator can select Enable or Disable the services of WMM.

WMM Parameters of Access Point

AC Type	CWmin	CWmax	AIFS	TxOp Limit	No ACK Policy bit
AC_BE(0)	4	6	3	0	<input type="checkbox"/>
AC_BK(1)	4	10	7	0	<input type="checkbox"/>
AC_VI(2)	3	4	1	3008	<input type="checkbox"/>
AC_VO(3)	2	3	1	1504	<input type="checkbox"/>

WMM Parameters of Station

AC Type	CWmin	CWmax	AIFS	TxOp Limit	ACM bit
AC_BE(0)	4	10	3	0	<input type="checkbox"/>
AC_BK(1)	4	10	7	0	<input type="checkbox"/>
AC_VI(2)	3	4	2	3008	<input type="checkbox"/>
AC_VO(3)	2	3	2	1504	<input type="checkbox"/>

✓ **AC Type :**

Queue	Data Transmitted AP to Clients	Priority	Description
AC_BK	Background	Low	High throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).
AC_BE	Best Effort	Medium	Medium throughput and delay. Most traditional IP data is sent to this queue.
AC_VI	Video	High	Minimum delay. Time-sensitive video data is automatically sent to this queue.
AC_VO	Voice	High	Time-sensitive data like VoIP and streaming media are automatically sent to this queue.

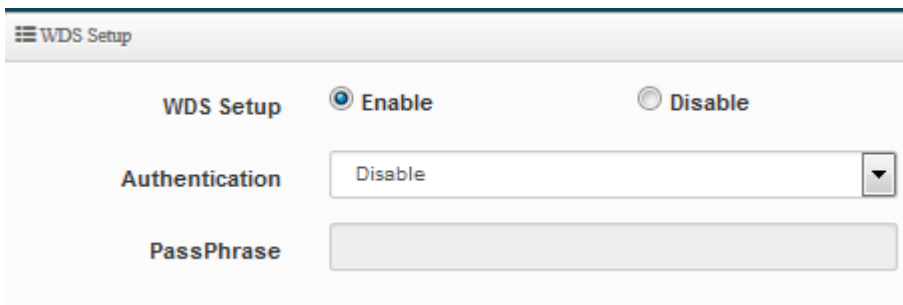
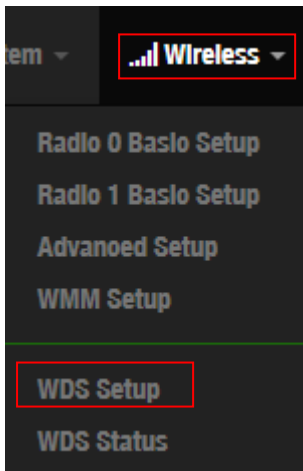
- ✓ **CWmin** :
Minimum Contention Window. This parameter is input to the algorithm that determines the initial random backoff wait time ("window") for retry of a transmission. The value specified here in the Minimum Contention Window is the upper limit (in milliseconds) of a range from which the initial random backoff wait time is determined.
- ✓ **CWmax** : Maximum Contention Window. The value specified here in the Maximum Contention Window is the upper limit (in milliseconds) for the doubling of the random backoff value. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached. Once the Maximum Contention Window size is reached, retries will continue until a maximum number of retries allowed is reached. Valid values for the "cwmax" are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024. The value for "cwmax" must be higher than the value for "cwmin". ◦
- ✓ **AIFS** : The Arbitration Inter-Frame Spacing Number specifies a wait time (in milliseconds) for data frames ◦
- ✓ **TxOP Limit** : Transmission Opportunity is an interval of time when a WME AP has the right to initiate transmissions onto the wireless medium (WM). This value specifies (in milliseconds) the Transmission Opportunity (TXOP) for AP; that is, the interval of time when the WMM AP has the right to initiate transmissions on the wireless network. ◦
- ✓ **ACM bit** : Admission Control Mandatory, ACM only takes effect on AC_VI and AC_VO. When you do not click Checkbox, it means that the ACM is controlled by the connecting AP. If you click Checkbox, it means that the Client is in charge ◦
- ✓ **No ACK policy bit** : Acknowledgment Policy, WMM defines two ACK policies: **Normal ACK** and **No ACK**. Click "**Checkbox**" indicates "**No ACK**"
When the no acknowledgement (No ACK) policy is used, the recipient does not acknowledge received packets during wireless packet exchange. This policy is suitable in the environment where communication quality is fine and interference is weak.
While the No ACK policy helps improve transmission efficiency, it can cause increased packet loss when communication quality deteriorates. This is because when this policy is used, a sender does not retransmit packets that have not been received by the recipient. When the Normal ACK policy is used, the recipient acknowledges each received unicast packet. ◦

3.6.5 WDS Setup

The administrator can create WDS Links for expanding wireless network via this page. When you enable “**WDS**” function in AP Mode both Wireless and Ethernet user can connect your local network at the same time through **AP**.

The WDS link supports 2.4G/5G radio and can support VLAN tag pass through

Please click on **Wireless -> WDS Setup**



- **WDS Setup:** Administrator can select Enable or Disable.
- **Authentication:** Administrator can use AES security.
- **WDS Client Setup:** Administrator can used 2.4G or 5G for WDS Links. A Single Radio supports up to 8 WDS links.

WDS Client Setup			
Radio 0(2.4G)		Radio 1(5G)	
Enable	MAC Address	Enable	MAC Address
<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/>

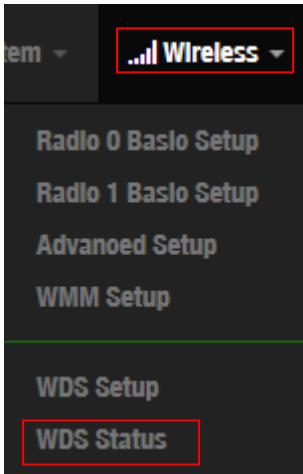
➤ **VLAN Setup:** The WDS aisle support Multi-tag VALN

VLAN Setup						
VLAN#	Radio 0			Radio 1		
	Native	TAG	TAG ID	Native	TAG	TAG ID
VLAN 0	<input checked="" type="radio"/>	<input type="checkbox"/>	<input type="text"/>	<input checked="" type="radio"/>	<input type="checkbox"/>	<input type="text"/>
VLAN 1	<input type="radio"/>	<input type="checkbox"/>	<input type="text" value="101"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="text" value="101"/>
VLAN 2	<input type="radio"/>	<input type="checkbox"/>	<input type="text" value="102"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="text" value="102"/>
VLAN 3	<input type="radio"/>	<input type="checkbox"/>	<input type="text" value="103"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="text" value="103"/>
VLAN 4	<input type="radio"/>	<input type="checkbox"/>	<input type="text" value="104"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="text" value="104"/>
VLAN 5	<input type="radio"/>	<input type="checkbox"/>	<input type="text" value="105"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="text" value="105"/>
VLAN 6	<input type="radio"/>	<input type="checkbox"/>	<input type="text" value="106"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="text" value="106"/>
VLAN 7	<input type="radio"/>	<input type="checkbox"/>	<input type="text" value="107"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="text" value="107"/>

3.6.6 WDS Status

Displays 2.4G and 5G radio WDS link status through MAC and Date (TX/RX)

Please click on **Wireless -> WDS status**



WDS Status	
Radio0 (2.4G) Client	
MAC Address	Rate(RX/TX)
-	-
Radio1 (5G) Client	
MAC Address	Rate(RX/TX)
-	-

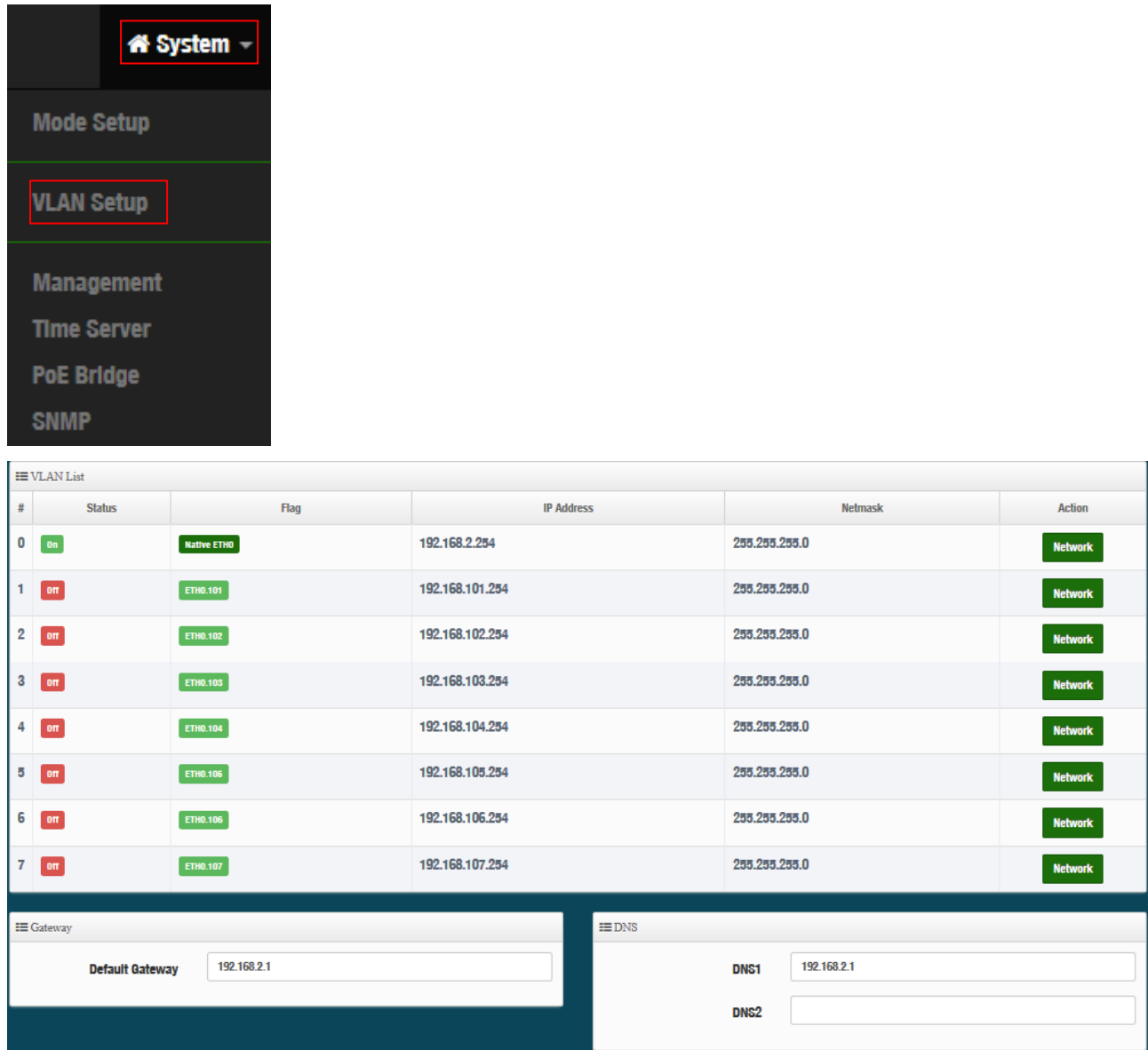
4. CAP Mode

The CAP mode itself isn't Access Point. This mode is primarily to control all the managed AP.

4.1 System VLAN Setup

Setup Control AP of LAN or VLAN IP Address, Gateway, DNS and Ethernet Tag etc.

Please click on **System -> VLAN Setup**



#	Status	Flag	IP Address	Netmask	Action
0	on	Native ETH0	192.168.2.254	255.255.255.0	Network
1	on	ETH0.101	192.168.101.254	255.255.255.0	Network
2	on	ETH0.102	192.168.102.254	255.255.255.0	Network
3	on	ETH0.103	192.168.103.254	255.255.255.0	Network
4	on	ETH0.104	192.168.104.254	255.255.255.0	Network
5	on	ETH0.105	192.168.105.254	255.255.255.0	Network
6	on	ETH0.106	192.168.106.254	255.255.255.0	Network
7	on	ETH0.107	192.168.107.254	255.255.255.0	Network

Gateway: Default Gateway

DNS: DNS1 DNS2

- # : Display VLAN No.
- **VLAN Mode** : Display on /off line status for the VLAN mode
- **IP Address** : Display IP address for the VLAN mode.
- **NetMask** : Display netmask for the VLAN mode.
- **Action** : Administrator can set VLAN IP · Radio 2.4 or 5G on/off · Spanning tree · IAPP and VLAN tag.

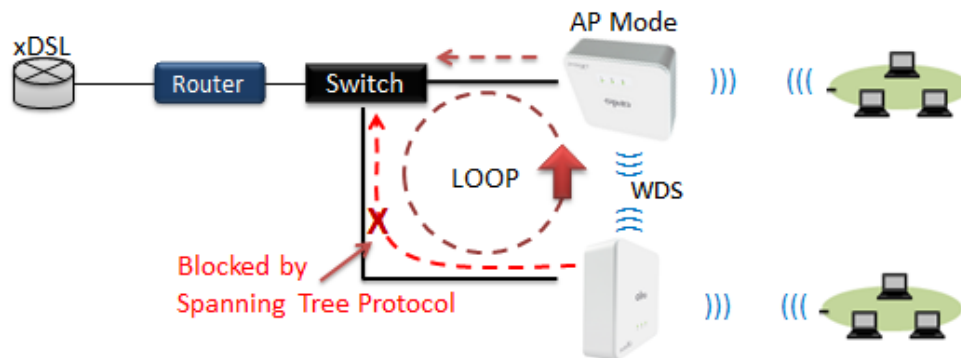
VLAN Setup VLAN Mode <input checked="" type="radio"/> Enable <input type="radio"/> Disable	Management 802.1d Spanning Tree <input type="radio"/> Enable <input checked="" type="radio"/> Disable
IP Setup IP Address 192.168.2.254 Netmask 255.255.255.0	ETH0 VLAN Tag Setup ETH0 <input checked="" type="radio"/> Enable <input type="radio"/> Disable VLAN TAG <input type="checkbox"/> 1-4096

- **VLAN Mode** : Administrator can Enable or disable the VLAN function.



VLAN have 0~7 total 8 VLAN. There must always be at least one VLAN enabled. If the administrator disables all the VLANs, he/she will not be able to login to the manager page. The administrator must then reset to default.

- **IP setup** : Administrator can set the VLAN IP address and NetMask or disable IP.
- **802.1d Spanning Tree** : The spanning tree network protocol provides a loop free topology for a bridged LAN between LAN interface and 8 WDS interfaces from wds0 to wds7. The Spanning Tree Protocol, which is also referred to as STP, is defined in the IEEE Standard 802.1d.



- **ETH0** : Administrator select Enable/disable the Ethernet port.
- **VLAN Tag** : Administrator can set Tag ID for the Ethernet port.

➤ **Set Gateway / DNS address functions.**

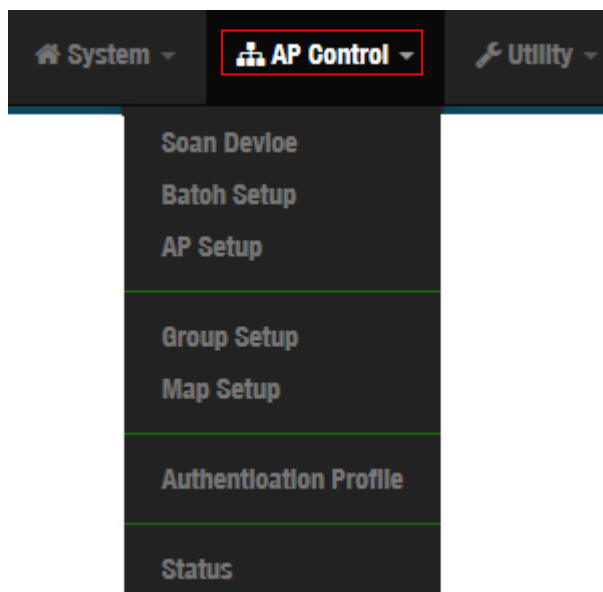
Gateway Default Gateway 192.168.2.1	DNS DNS1 8.8.8.8 DNS2
<input type="button" value="Save"/>	<input type="button" value="Cancel"/>

- **Gateway**: The default Gateway IP Address is 192.168.2.1, Please check your Gateway IP and change.
- **DNS**: Check either “No Default DNS Server” or “Specify DNS Server IP” button as desired to set up the system DNS.

- ✓ **Primary:** The IP address of the primary DNS server.
- ✓ **Secondary:** The IP address of the secondary DNS server.

4.2 AP Control

When CenOS5.0 AP changes to CAP mode, Administrator can use AP Control functions to centralize management of APs in the network architecture. AP control Setting functions have “Scan Device”, “Batch Setup”, “AP Setup”, “Group / Map setup” and Authentication Profile setup etc.. Please click “**AP Control**” to enter AP Management settings

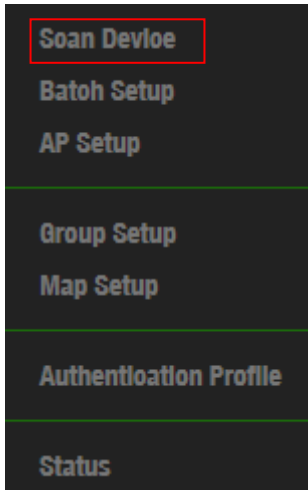


Centralized Management APs operating Instructions:

- 1) Click “**Scan Device**” to discover Access Points in the network architecture.
- 2) Set IP address for all managed Access Points and reboot managed Access Points.
- 3) Re-Scan managed APs and Import to databases.
- 4) Centralize managed AP settings by clicking “**AP control**” → “**Batch setup**”
- 5) After the setup is complete for managed APs function, administrator must reboot all managed APs.

4.2.1 Scan Device

This management page can discover all managed APs in the network. Administrator can set IP address / Password and VLAN tag for managed APs. After the setup is complete, Administrator must import all managed APs to databases.



Filter Device

VLAN#

Default Password

Sort

- **VLAN#** : Administrator can select VLAN network to discovery managed Aps
- **Default Password**: Set login system password by managed Aps.
- **Sort**: Administrator can select discovery managed Aps Type. (IP or MAC)

Scan Result										Default	Import
#	Device	IP Address	MAC Address	Password	Host Name	F/W Version	F/W Date	IP Address	Netmask	Action	
1		192.168.2.253	8c:4d:ea:04:d0:6e	CW-400NAC-E1	Pme-CPE-ACS V1.1.0	2016/05/06 09:19:35	<input type="text" value="192.168.2.253"/>	<input type="text" value="255.255.255.0"/>	<input type="button" value="Info"/>	

- **#** : Display managed APs items.
- **Device** : Administrator can select all or single for managed Aps.
- **IP Address** : Display IP address for managed AP.
- **MAC Address** : Display MAC address for managed AP.
- **Host Name** : Display host name for managed AP.
- **F/W Version** : Display firmware version for managed AP.
- **F/W Date** : Display firmware Release date for managed AP.
- **IP Address** : Administrator can set single IP address for Managed AP.
- **Netmask** : Administrator can set single Netmask for Managed AP.

- **Default** : Administrator click the button will can reset to default for select managed APs.

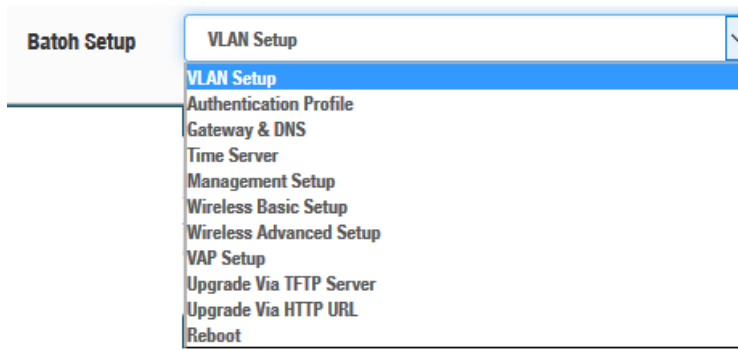
- **Control Port** : Administrator can change VLAN network for managed APs.
- **VLAN TAG** : Administrator can set VLAN TAG ID for managed APs.
- **IP Address** : Administrator can set IP address for managed APs, the IP address is auto-incrementally.
- **NetMask** : Administrator can set NetMask for managed APs.

When the setting managed APs is completed, please click Apply & Reboot button to complete the setup process.

4.2.2 Batch Setup

The AP control function supports centralized configuration of managed APs. Administrator can change VLAN network / Group and batch setup for managed APs.

- **LAN** : When VLAN Tag function is enabled (please refer to 4.1 System VLAN Setup), administrator can change VLAN tag for managed APs.
- **Group** : When AP Groups are created (please refer to 4.2.4 Group setup), Administrators can select and change group settings of managed APs.
- **Batch Setup** : Administrator can centralize setting changes for managed APs.



- **VLAN Setup** : Administrator can set VLAN Tag, IP address and Wi-Fi on/off for the managed APs.

The image shows the 'VLAN Setup' configuration page. It includes an 'Apply' button in the top right corner. The configuration options are as follows:

VLAN	VLAN 0	
VLAN Mode	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
Access Point 0	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
Access Point 1	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
802.1d Spanning Tree	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
Control Port	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
IAPP	Disable	

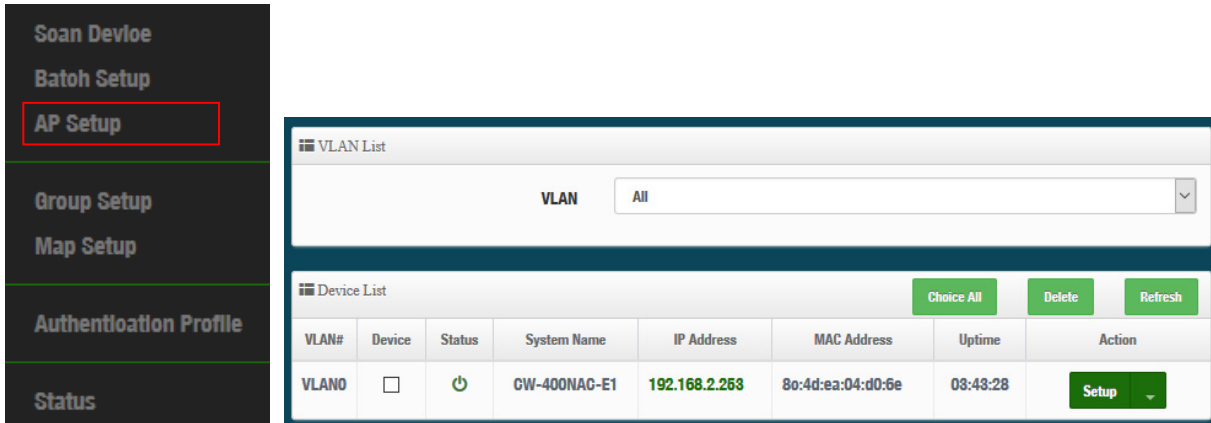
- ✓ **VLAN** : The function can select VLAN (please refer to 3.2 Configure VLAN Setup) for managed APs.
- ✓ **VLAN Mode** : Administrator can enable or disable VLAN mode of the managed APs.
- ✓ **Access Point0/1** : Administrator can enable or disable 2.4 or 5G radio of the managed APs. (Access Point 0 is radio 2.4G, Access Point 1 is radio 5G)
- ✓ **802.1d Spanning Tree** : Administrator can enable or disable the function.(please refer to 3.2.1 Configure Network → 802.1d Spanning Tree)
- ✓ **Control Port** : The function administrator can enable or disable of the managed APs (please refer to 3.2.1 Configure Network → Control Port)
- ✓ **IAPP** : The function administrator can enable or disable of the managed APs (Please refer to 3.2.1 Configure Network → IAPP)

IP Setup	
Apply	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
IP Mode	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
IP Address	<input type="text" value="192.168.2.10"/>
Netmask	<input type="text" value="255.255.255.0"/>
ETH0 VLAN Tag Setup	
ETH0	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
VLAN TAG	<input type="checkbox"/> <input type="text" value="1-4096"/>
ETH1 VLAN Tag Setup	
ETH1	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
VLAN TAG	<input type="checkbox"/> <input type="text" value="1-4096"/>

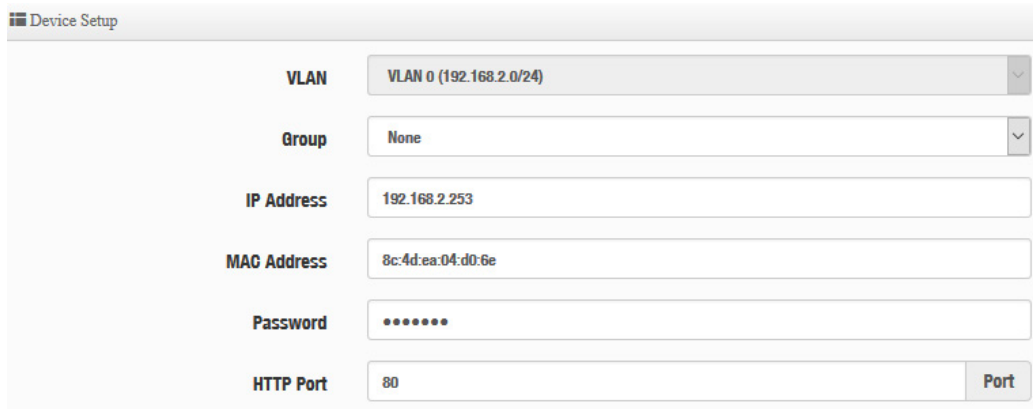
- ✓ **IP Setup** : Administrator can set IP address and Netmask of the managed APs.
 - ✓ **ETH0/1 VLAN Tag Setup** : Administrator can set VLAN Tag or disable VLAN function of the managed APs.
- **Authentication Profile** : After creating Profiles, See: “4.2.6 Authentication Profile” users can conveniently apply Authentication profiles
 - **Gateway & DNS**: Setting Gateway and DNS for managed APs.
 - **Time Server**: Setting System Time for managed APs. (Please refer to 5.2 Configure Time Server)
 - **Management Setup**: Setting system name/ system login port and system log server service for managed APs. (Please refer to 5.1 system management)
 - **Wireless Batch Setup**: Setting Wi-Fi configurations for managed APs. (Please refer to 3.6 Wireless Basic Setup)
 - **Wireless Advanced Setup**: Setting Wi-Fi Advanced settings for managed APs. (Please refer to 3.6.3 Wireless Advanced Setup)
 - **VAP Setup** : Wi-Fi SSID / channel or security settings for managed APs. (Please refer to 3.2.3 Configure Radio 0/1)
 - **Upgrade via TFTP Server**: Administrator can centrally upgrade firmware via TFTP Server for the managed APs.
 - **Upgrade via HTTP Server**: Administrator can centrally upgrade firmware via HTTP Server for the managed APs.
 - **Reboot**: Administrator can reboot managed APs.

4.2.3 AP Setup

Administrator can monitor statuses and modify managed APs information.

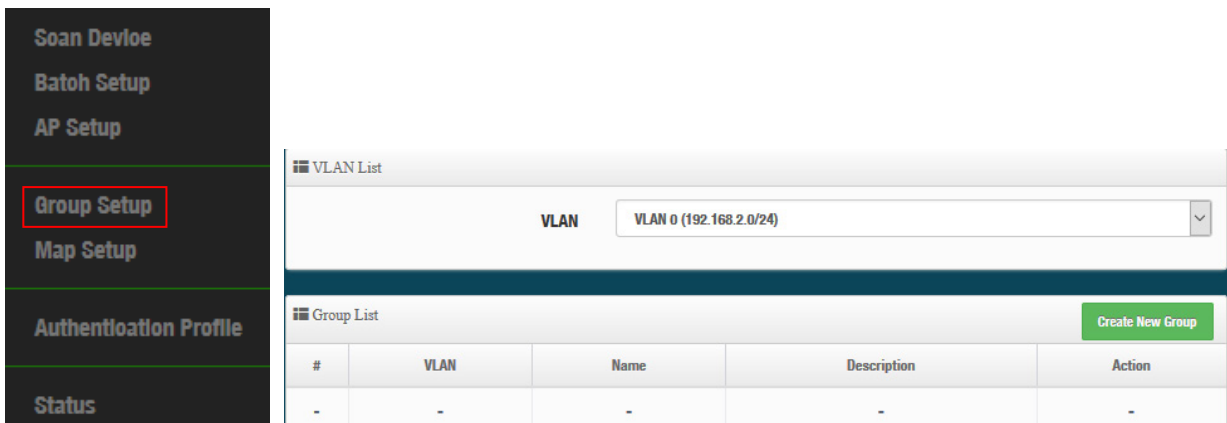


- **VLAN** : Select desired VLAN for AP setup
- **Setup** : Administrator can modify IP addresses, system login passwords, and web login port for managed APs. If administrator has change AP devices, administrator can modify MAC address of the new managed AP.



4.2.4 Group Setup

Administrator can create Groups within the same VLAN.



- **VLAN** : Select VLAN.
- **Create New Group** : Click the button to create a new AP Group

Group List				Create New Group
#	VLAN	Name	Description	Action
1	VLAN 0	test	Offloe group	Device ▾

- ✓ **Device button** : Administrator can select managed APs and import them into the Group.

4.2.5 Map Setup

The Map Setup feature allows administrators to upload a floor plan image to a web server, then use the image URL to import the map into the AP user interface. Once the image is uploaded, administrators can use the Map Setup function to map out the locations of the AP network.

Scan Device

Batch Setup

AP Setup

Group Setup

Map Setup

Authentication Profile

Status

Map List				Create New Map
#	Name	Description	Action	
1	1F_plan	Location Map for man...	View ▾	

- **Create New Map** : Click the button to create map.

Map Setting

Map Name

Image URL

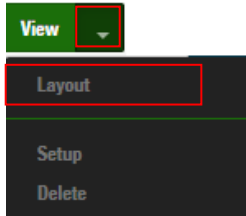
Description

Image

- **Map Name** : Enter map name.
- **Image URL** : Paste Map image url
- **Description** : Enter the description for the map.

After the Map URL setup confirmation, please reboot the system.

View : Once the Map is created and properly in the Map List, administrators can click the “Layout” button in the action tab to map out the AP network. Managed APs will appear in the “Device List” section of the layout page. Administrators can simply drag the AP (IP Address) to the correct installation location.

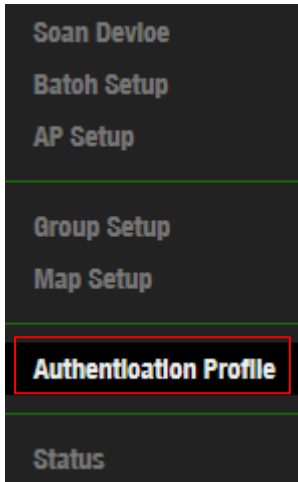


Map List			Create New Map
#	Name	Description	Action
1	1F_plan	Location Map for man...	View

View : Once complete, administrators can click the “View” button to monitor AP statuses and locations.



4.2.6 Authentication Profile

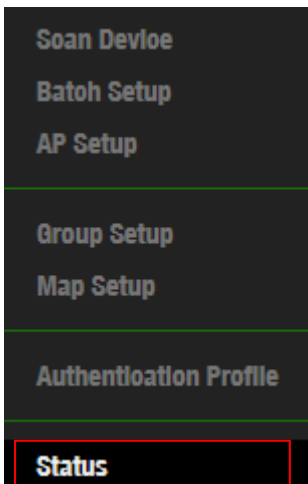


Administrator can pre-set authentication conditions in the profile, the authentication set can refer 3.3 Authentication.

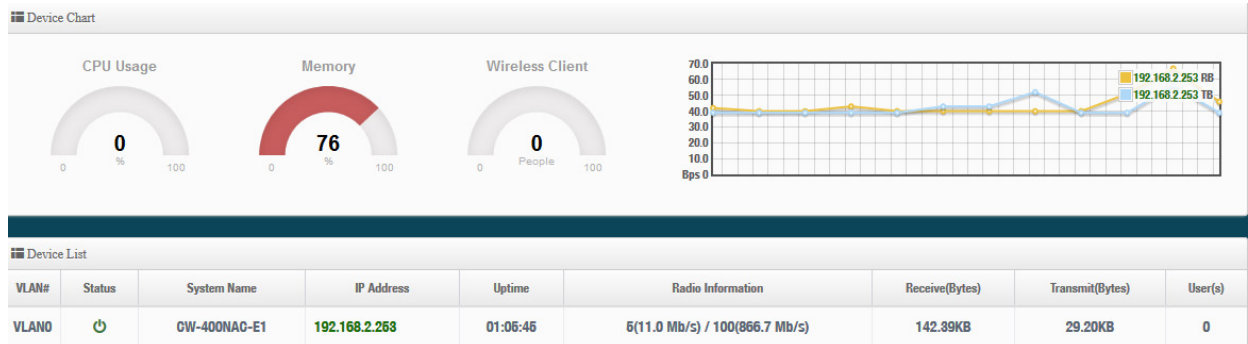
Authentication Profile List Create New Profile					
#	Name	Description	Authentication	Edit	Action
1	Authentioation-test1		Off	Authentication	Setup

- **Create New Profile** : Administrator can create authentication profile.
- **Edit** : **Authentication** Click the Authentication button to Enable or Disable authentication function. For more details, refer to “3.3 Authentication”.
- **Authentication** Click Dropdown to set authentication functions. Refer to “3.3 Authentication” dropdown functions.
- **Action**: **Setup** The button can modify or delete for the authentication profile.

4.2.7 Status



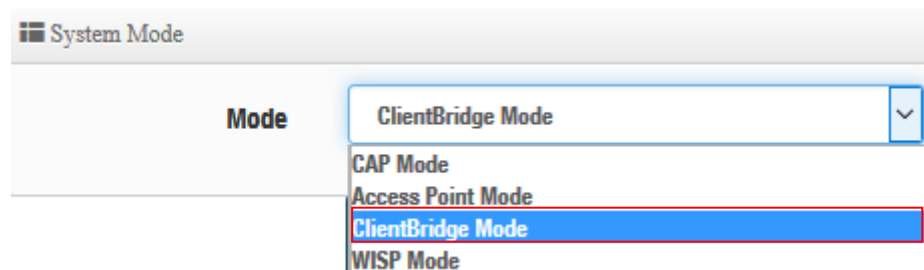
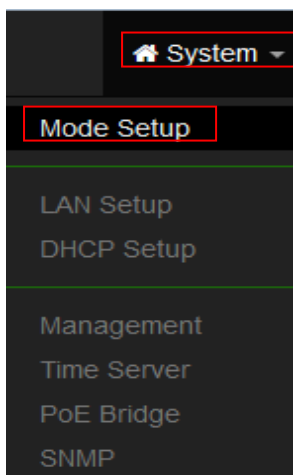
Administrator can monitor Tx/Rx flow information, show online users and check system CPU / Memory information and on/off line for the managed APs. The information data display support graphical interface.



5. Client Bridge Mode

When Client Bridge is chosen, the system can be configured as a Client Bridge and support Repeater AP function. This section provides detailed explanation for users to configure in the Client Bridge Mode and Repeater AP function with help of illustrations.

The system administrator can set the desired mode via this page, and then configure the system according to their deployment needs, Please click on **System -> Mode Setup** and follow the below setting.



If Client Bridge used 2.4G radio link to AP station, the Repeater AP only used 5G radio.
So Client Bridge used 5G radio link to AP station, the Repeater AP only used 2.4G radio.

5.1 Configure LAN Setup

Here are the instructions for how to setup the local IP Address and Netmask. Please click on **System -> LAN** and follow the below setting.

Ethernet Connection Type

Mode Static IP Dynamic IP

Mode: Administrator can select the IP used Static or Dynamic IP address.

➤ **Static IP:**

Static IP

IP Address

Netmask

Gateway

- **IP address:** The IP address is 192.168.2.254
 - **Netmask:** The default Netmask is 255.255.255.0
 - **Gateway:** The default Gateway IP Address is 192.168.2.1, Please check your Gateway IP and change.
- **DNS:** Enter IP address of domain name service.

DNS

Primary DNS

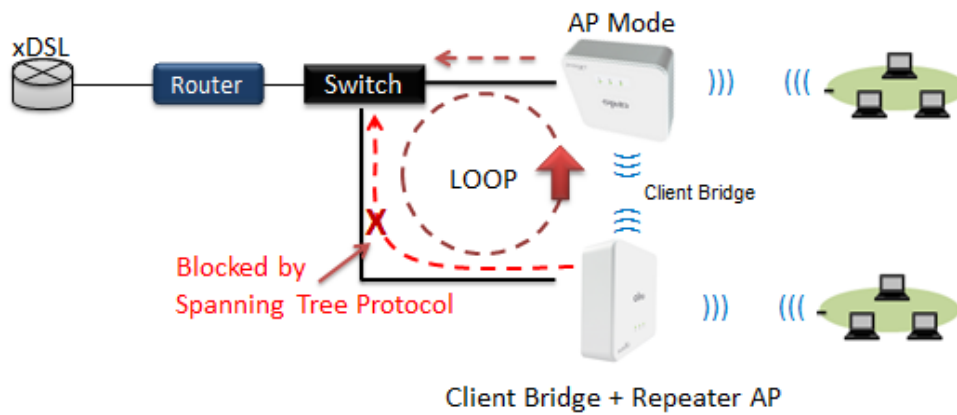
Secondary DNS

- **Primary DNS:** The IP address of the primary DNS server.
 - **Secondary:** The IP address of the secondary DNS server.
- **802.1d Spanning Tree :**

802.1d Spanning Tree

802.1d Spanning Tree Enable Disable

The spanning tree network protocol provides a loop free topology for a bridged LAN between LAN interface and 8 WDS interfaces from wds0 to wds7. The Spanning Tree Protocol, which is also referred to as STP, is defined in the IEEE Standard 802.1d.



- **DHCP Forward:** When the AP Mode device and Client Bridge AP are linked, and DHCP Service is "Enabled", the Client Bridge AP must also enable DHCP Forward to allow connecting clients to receive the IP Address from the source AP (AP Mode Device). By default, DHCP Forward is disabled in Client Bridge devices. This function must be enabled to allow clients connecting to the Client Bridge device to receive IP Addresses from the source AP.

DHCP Forward	
DHCP Forward	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

5.2 Configure DHCP Setup

The DHCP Service function in the Client Bridge device can select a separate IP Address range within the same network segment of the source AP, and allocate those IP Addresses to connecting clients.

DHCP Service	
Mode	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

DHCP Setup	
Start IP	<input type="text" value="192.168.2.100"/>
End IP	<input type="text" value="192.168.2.140"/>
Netmask	<input type="text" value="255.255.255.0"/>
Gateway	<input type="text" value="192.168.2.1"/>
DNS1 IP	<input type="text" value="192.168.2.1"/>
DNS2 IP	<input type="text"/>
WINS IP	<input type="text"/>
Domain	<input type="text"/>
Lease Time	<input type="text" value="86400"/>

- **Start IP / End IP:** Specify the range of IP addresses to be used by the DHCP server when assigning IP address to clients.
- **Netmask:** The netmask default is 255.255.255.0.
- **Gateway:** Enter source gateway IP address.
- **DNS1:** Enter IP address of the first DNS server; this field is required.
- **DNS2:** Enter IP address of the second DNS server; this is optional.
- **WINS IP :** Enter IP address of the Windows Internet Name Service (WINS) server; this is optional.
- **Domain:** Enter the domain name for this network.
- **Lease Time:** The IP addresses given out by the DHCP server will only be valid for the duration specified by the lease time. Increasing the time ensure client operation without interruptions, but could introduce potential conflicts. Lowering the lease time will avoid potential address conflicts, but might cause more interruptions to the client while it will acquire new IP addresses from the DHCP server. Default is **86400** seconds

DHCP Clients List: When users link OW-400-A2 and use IP address of the DHCP service, the DHCP Client List will display users the information and used IP address.

DHCP Client List				
#	IP Address	MAC Address	Expired	Action
-	-	-	-	-

- **IP Address:** Display users used IP address.
- **MAC Address:** Display MAC Address of users used device.
- **Expired:** Display Lease expiration time of IP address.
- **Action:** Kicked user button.

Static Lease IP Setup: Administrator can set as static IP address for users.

Static Lease IP Setup	
Comment	<input type="text"/>
IP Address	<input type="text"/>
MAC Address	<input type="text"/> <input type="button" value="Add"/>

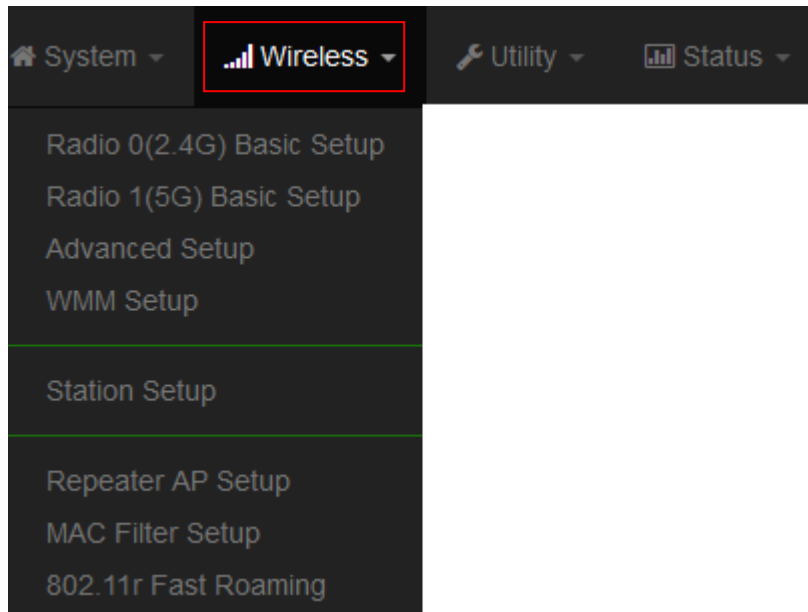
- **Comment:** Enter description for the information.
- **IP Address:** Set static IP address for users.
- **MAC Address:** Set MAC address of user device.

Static Lease IP List: Display users list of static IP address.

Static Lease IP List				
#	Comment	IP Address	MAC Address	Action
-	-	-	-	-

5.3 Wireless General Setup

The main setting for Client Bridge mode link to AP Station, Repeater AP functions setting, MAC filter, WMM and 802.11r/802.11k Fast Roaming etc.



5.3.1 Radio 0(2.4G) Basic Setup

Administrator can change the data transmission, channel and output power settings for the system.

General Setup

Station Mode Enable Disable

Country

Band Mode

Tx Power

- **Station Mode:** Administrator can Enable or Disable the radio.
- **Country:** Administrator can select country used channel by US and EU.
- **Band Mode:** Select an appropriate wireless band; bands available are **801.11 b/g/n mixed mode**.
- **Tx Power:** Administrator can adjust the output power of the system to get the appropriate coverage for your wireless network. Specify digit numbers between level **1** to level **9** (the unit is %) for your environment. If you are not sure which setting to choose, then keep the default setting level **9 (100%)**.

HT Physical Mode

HT Physical Mode

TX/RX Stream

Channel BandWidth 20 20/40

Extension Channel Upper Lower

MCS

Short GI Enable Disable

Aggregation Enable Disable

Aggregation Frames

Aggregation Size

- **TX/RX Stream:** OW-400-A2 utilizes 2 antennas, supporting 2TX/2RX streams. Administrator can select 1 or 2 TX/RX. The default is 2TX/2RX.
- **Channel Bandwidth:** The "20/40" MHz option is usually best. The other option is available for special circumstances.
- **Extension Channel:** Set channel select of Upper or Lower, the Upper support 1 to 7 range CH and Lower support 5 to 11 range CH.
- **MCS:** This parameter represents transmission rate. By default (Auto) the fastest possible transmission rate will be selected. You have the option of selecting the speed if necessary.
- **Short GI:** Short Guard Interval, by default, it's "Enable". it's can increase throughput. However, it can also increase error rate in some installations, due to increased sensitivity to radio-frequency reflections. Select the option that works best for your installation.
- **Aggregation:** By default, it's "Enable". To "Disable" to deactivated Aggregation. A part of the 802.11n standard (or draft-standard). It allows sending multiple frames per single access to the medium by combining frames together into one larger frame. It creates the larger frame by combining smaller frames with the same physical source and destination end points and traffic class (i.e. QoS) into one large frame with a common MAC header.
- **Aggregation Frames :** The Aggregation Frames is in the range of 2~64, the default is 32. It determines the number of frames combined on the new larger frame.
- **Aggregation Size :** The Aggregation Size is in the range of 1024~65535, the default is 50000. It determines the size (in Bytes) of the larger frame.

5.3.2 Radio 1(5G) Basic Setup

General Setup

Station Mode	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Country	<input type="text" value="United States"/>
Band Mode	<input type="text" value="802.11ac"/>
Auto Channel	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Channel	<input type="text" value="36 (5180 Mhz)"/>
Tx Power	<input type="text" value="Level 9"/>

- **Station Mode:** Administrator can Enable or Disable the radio.
- **Country:** Administrator can select a country: US or EU.
- **Band Mode:** Administrator can select 5G Band for 802.11a/n or 802.11ac. The default is 802.11ac
- **Auto Channel:** Administrator can Enable or Disable the function. If select disable function the WiFi channel can be fixed a channel.
- **Channel:** Support US and Eu country by 5G Channel.
- **Tx Power:** Administrator can control the WiFi Tx output power. The power Max. Level 9.

HT Physical Mode

HT Physical Mode

TX/RX Stream	<input type="text" value="2T2R"/>
Channel BandWidth	<input type="text" value="80"/>
Short GI	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Aggregation	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Aggregation Frames	<input type="text" value="32"/>
Aggregation Size	<input type="text" value="50000"/>

- **TX/RX Stream:** The OW-400-A2 utilizes 2 antenna and supports 2TX/2RX streams. Administrator can select 1 or 2 TX/RX. The default is 2TX/2RX.
- **Channel Bandwidth:** The "20/40 and 802.11ac 80" MHz option is usually best. The other option is available for special circumstances.

- **Shout GI:** Short Guard Interval, by default, it's "Enable". it's can increase throughput. However, it can also increase error rate in some installations, due to increased sensitivity to radio-frequency reflections. Select the option that works best for your installation.
- **Aggregation:** By default, it's "Enable". To "Disable" to deactivated Aggregation. A part of the 802.11n standard (or draft-standard). It allows sending multiple frames per single access to the medium by combining frames together into one larger frame. It creates the larger frame by combining smaller frames with the same physical source and destination end points and traffic class (i.e. QoS) into one large frame with a common MAC header.
- **Aggregation Frames :** The Aggregation Frames is in the range of **2~64**, default is **32**. It determines the number of frames combined on the new larger frame.
- **Aggregation Size :** The Aggregation Size is in the range of **1024~65535**, default is **50000**. It determines the size (in Bytes) of the larger frame.

5.3.3 Advanced Setup

The administrator can change the Slot Time, ACK Timeout, RTS threshold and fragmentation threshold settings for the system.

Advanced Setup

Slot Time	<input type="text" value="9"/>	<input type="button" value="Distance"/>
ACK Timeout	<input type="text" value="64"/>	
Beacon Interval	<input type="text" value="100"/>	
DTIM Interval	<input type="text" value="1"/>	
Fragment Threshold	<input type="text" value="2346"/>	
RTS Threshold	<input type="text" value="2346"/>	
Short Preamble	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
IGMP Snooping	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
Greenfield	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable

- **Slot Time** : Slot time is in the range of **9~1489** and set in unit of **microsecond**. The default value is **9** microsecond.

Slot time is the amount of time a device waits after a collision before retransmitting a packet. Reducing the slot time decreases the overall back-off, which increases throughput. Back-off, which is a multiple of the slot time, is the random length of time a station waits before sending a packet on the LAN. For a sender and receiver own right of the channel the shorter slot time help manage shorter wait time to re-transmit from collision because of hidden wireless clients or other causes. When collision sources can be removed sooner and other senders attempting to send are listening the channel(CSMA/CA) the owner of the channel should continue ownership and finish their transmission and release the channel. Then, following ownership of the channel will be sooner for the new pair due to shorter slot time. However, when long duration of existing collision sources and shorter slot time exist the owners might experience subsequent collisions. When adjustment to longer slot time can't improve performance then RTS/CTS could supplement and help improve performance.

- **ACK Timeout** : ACK timeout is in the range of **1~372** and set in unit of **microsecond**. The default value is **64** microsecond.

All data transmission in 802.11b/g request an "Acknowledgement" (ACK) send by receiving radio. The transmitter will resend the original packet if correspondent ACK failed to arrive within specific time interval, also refer to as "ACK Timeout".

ACK Timeout is adjustable due to the fact that distance between two radio links may vary in different deployment. ACK Timeout makes significant influence in performance of long distance radio link. If ACK Timeout is set too short, transmitter will start to "Resend" packet before ACK is received, and throughput become low due to excessively high re-transmission.

ACK Timeout is best determined by distance between the radios, data rate of average environment. The Timeout value is calculated based on round-trip time of packet with a little tolerance, So, if experiencing re-transmissions or poor performance the ACK Timeout could be made longer to accommodate.



Slot Time and ACK Timeout settings are for long distance links. It is important to tweak settings to achieve the optimal result based on requirement.

- **Beacon Interval:** Beacon Interval is in the range of **40~3500** and set in unit of *millisecond*. The default value is **100** msec.
Access Point (AP) in IEEE 802.11 will send out a special approximated 50-byte frame, called "Beacon". Beacon is broadcast to all the stations, provides the basic information of AP such as SSID, channel, encryption keys, signal strength, time stamp, support data rate. All the radio stations received beacon recognizes the existence of such AP, and may proceed next actions if the information from AP matches the requirement. Beacon is sent on a periodic basis, the time interval can be adjusted.
By increasing the beacon interval, you can reduce the number of beacons and associated overhead, but that will likely delay the association and roaming process because stations scanning for available access points may miss the beacons. You can decrease the beacon interval, which increases the rate of beacons. This will make the association and roaming process very responsive; however, the network will incur additional overhead and throughput will go down.
- **DTIM Interval :** The DTIM interval is in the range of **1~255**. The default is **1**.
DTIM is defined as *Delivery Traffic Indication Message*. It is used to notify the wireless stations, which support power saving mode, when to wake up to receive multicast frame. DTIM is necessary and critical in wireless environment as a mechanism to fulfill power-saving synchronization.
A DTIM interval is a count of the number of beacon frames that must occur before the access point sends the buffered multicast frames. For instance, if DTIM Interval is set to 3, then the Wi-Fi clients will expect to receive a multicast frame after receiving three Beacon frame. The higher DTIM interval will help power saving and possibly decrease wireless throughput in multicast applications.
- **Fragmentation Threshold:** Fragmentation Threshold is one more parameter which is given in all stations and Access points. Fine tuning Fragmentation Threshold parameter can result in good throughput but not using it properly can results in low throughput. In simple words it does the same thing which MTU do in Ethernet. Both are different parameters but the work done is same , it fragments the data packets.
Fragmentation threshold will be used when we have more data packet size to be transmitted and we have less fragment threshold value. Lets say from Ethernet we have to send 1400 byte packet but the fragmentation threshold is set as 400. In this case when the packet is to be transmitted on air it will fragment the packet in to 4 small packet 400+400+400+200 and send on air.This includes MAC header+ frame body and CRC so 400 byte will be in total including headers. This helps in increasing the throughput. The default is 2346.

- **RTS Threshold:** TRTS Threshold is in the range of **1~2347** byte. The default is **2347** byte. The main purpose of enabling RTS by changing RTS threshold is to reduce possible collisions due to hidden wireless clients. RTS in AP will be enabled automatically if the packet size is larger than the Threshold value. By default, RTS is disabled in a normal environment supports non-jumbo frames.
- **Short Preamble:** By default, it's "**Enable**". To **Disable** is to use Long 128-bit Preamble Synchronization field. The preamble is used to signal "here is a train of data coming" to the receiver. The short preamble provides 72-bit Synchronization field to improve WLAN transmission efficiency with less overhead.
- **IGMP Snooping:** the process of listening to Internet Group Management Protocol (IGMP) network traffic. The feature allows a network switch to listen in on the IGMP conversation between hosts and routers. By listening to these conversations the switch maintains a map of which links need which IP multicast streams. Multicasts may be filtered from the links which do not need them and thus controls which ports receive specific multicast traffic.
- **Greenfield:** In wireless WLAN technology, greenfield mode is a feature of major components of the 802.11n specification. The greenfield mode feature is designed to improve efficiency by eliminating support for 802.11b/g devices in an all draft-n network. In greenfield mode the network can be set to ignore all earlier standards.

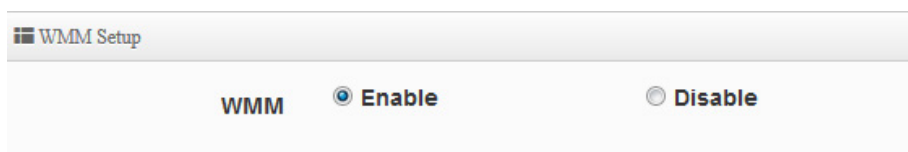
5.3.4 WMM Setup

This affects traffic flowing from the access point to the client station.

Configuring QoS options consists of setting parameters on existing queues for different types of wireless traffic. You can configure different minimum and maximum wait times for the transmission of packets in each queue based on the requirements of the media being sent.

Queues automatically provide minimum transmission delay for Voice, Video, multimedia, and mission critical applications, and rely on best-effort parameters for traditional IP data.

As an Example, time-sensitive Voice & Video, and multimedia are given effectively higher priority for transmission (lower wait times for channel access), while other applications and traditional IP data which are less time-sensitive but often more data-intensive are expected to tolerate longer wait times.



WMM Parameters of Access Point					
AC Type	CWmin	CWmax	AIFS	TxOp Limit	No ACK Policy bit
AC_BE(0)	4	6	3	0	<input type="checkbox"/>
AC_BK(1)	4	10	7	0	<input type="checkbox"/>
AC_VI(2)	3	4	1	3008	<input type="checkbox"/>
AC_VO(3)	2	3	1	1504	<input type="checkbox"/>

WMM Parameters of Station					
AC Type	CWmin	CWmax	AIFS	TxOp Limit	ACM bit
AC_BE(0)	4	10	3	0	<input type="checkbox"/>
AC_BK(1)	4	10	7	0	<input type="checkbox"/>
AC_VI(2)	3	4	2	3008	<input type="checkbox"/>
AC_VO(3)	2	3	2	1504	<input type="checkbox"/>

✓ **AC Type :**

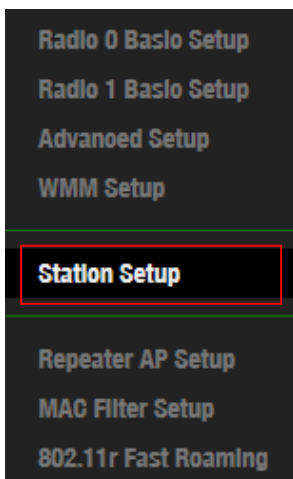
Queue	Data Transmitted AP to Clients	Priority	Description
AC_BK	Background	Low	High throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).
AC_BE	Best Effort	Medium	Medium throughput and delay. Most traditional IP data is sent to this queue.
AC_VI	Video	High	Minimum delay. Time-sensitive video data is automatically sent to this queue.
AC_VO	Voice	High	Time-sensitive data like VoIP and streaming media are automatically sent to this queue.

✓ **CWmin :**

Minimum Contention Window. This parameter is input to the algorithm that determines the initial random backoff wait time ("window") for retry of a transmission. The value specified here in the Minimum Contention Window is the upper limit (in milliseconds) of a range from which the initial random backoff wait time is determined. ◦

- ✓ **CWmax** : Maximum Contention Window. The value specified here in the Maximum Contention Window is the upper limit (in milliseconds) for the doubling of the random backoff value. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached. Once the Maximum Contention Window size is reached, retries will continue until a maximum number of retries allowed is reached. Valid values for the "cwmax" are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024. The value for "cwmax" must be higher than the value for "cwmin". ◦
- ✓ **AIFS** : The Arbitration Inter-Frame Spacing Number specifies a wait time (in milliseconds) for data frames ◦
- ✓ **TxOP Limit** : Transmission Opportunity is an interval of time when a WME AP has the right to initiate transmissions onto the wireless medium (WM). This value specifies (in milliseconds) the Transmission Opportunity (TXOP) for AP; that is, the interval of time when the WMM AP has the right to initiate transmissions on the wireless network. ◦
- ✓ **ACM bit** : Admission Control Mandatory, ACM only takes effect on AC_VI and AC_VO. When you do not click Checkbox, it means that the ACM is controlled by the connecting AP. If you click Checkbox, it means that the Client is in charge ◦
- ✓ **No ACK policy bit** : Acknowledgment Policy, WMM defines two ACK policies: **Normal ACK** and **No ACK**. Click "**Checkbox**" indicates "**No ACK**"
When the no acknowledgement (No ACK) policy is used, the recipient does not acknowledge received packets during wireless packet exchange. This policy is suitable in the environment where communication quality is fine and interference is weak. While the No ACK policy helps improve transmission efficiency, it can cause increased packet loss when communication quality deteriorates. This is because when this policy is used, a sender does not retransmit packets that have not been received by the recipient. When the Normal ACK policy is used, the recipient acknowledges each received unicast packet. ◦

5.3.5 Station Setup



The functions setting functions include Client Bridge link to AP station. Administrator can used “site survey” function to Search for AP stations.

The screenshot shows the Cerio web interface. On the left, there are two configuration panels. The top panel is titled "Security" and contains fields for "ESSID" (TEST-AP), "Authentication" (WPA/WPA2 Personal), and a "WPS Push Button" with a green "Push Button" button. The bottom panel is titled "PassPhrase Settings" and contains fields for "WPA Mode" (Auto (WPA or WPA2)), "Cipher Type" (Auto), and "PassPhrase" (masked with dots). At the bottom of these panels are "Save" and "Cancel" buttons. On the right, there is a "MAC Address List" table with a "Site Survey" button in the top right corner. The table has columns for Channel, Signal, BSSID, ESSID, Authentication, and Setup, with all cells currently containing dashes.

Channel	Signal	BSSID	ESSID	Authentication	Setup
-	-	-	-	-	-

- **MAC Address List** : The function main discovery AP Station and select want to link the AP station.
- **Security/ PassPhrase Settings**: If link as AP station the AP station have used security, administrator can select AP station used authentication mode and enter password in the functions.

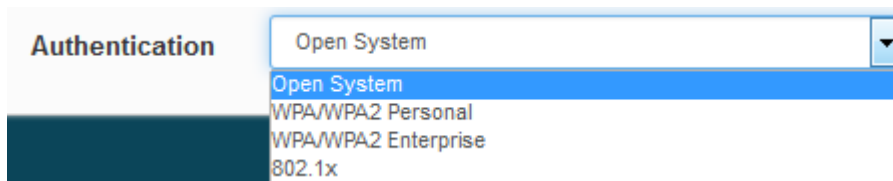
5.3.6 Repeater AP Setup

Administrators can configure ESSID, SSID broadcasting, Maximum number of client associations.

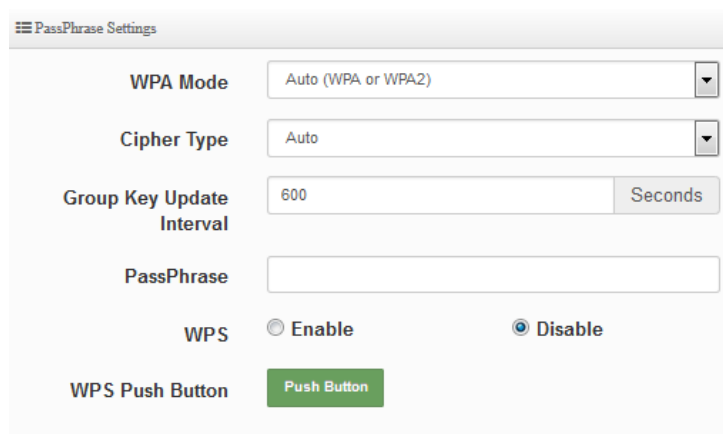
The screenshot shows the "Security" configuration panel for a Repeater AP. It includes radio buttons for "Access Point" (Enable selected, Disable unselected), "SSID Visibility" (Enable selected, Disable unselected), "Client Isolation" (Enable unselected, Disable selected), and "Connection Limit" (Enable unselected, Disable selected). There is a "User Limit" input field with the value 64. The "ESSID" field contains "CW-400NAC" and the "Authentication" dropdown is set to "WPA/WPA2 Personal".

- **Access Point**: Administrator can Enable or Disable the Repeater AP function.
- **ESSID**: Enter the Repeater AP of ESSID name.

- **SSID Visibility:** The default it's Enable. When select Disable the SSID will not be discovered.
- **Client Isolation:** This function is Disabled by default. All clients will be isolated from each other, which mean they can't reach each other.
- **Connection Limit:** This function is Disabled by default. If select Enable, Administrator can limit Wi-Fi users the Quantity.
- **Authentication:** Select the desired security type from the drop-down list; the options are WPA-PSK, WPA2-PSK, WPA/WPA2-Enterprise and WEP 802.1X.



- **Open System:** Data are not unencrypted during transmission when this option is selected.
- **WPA/WPA2 Personal:** WPA/WPA2 is short for W-Fi Protected Access-Pre-Shared Key. WPA/WPA2 uses the same encryption way with WPA, and the only difference between them is that WPA/WPA2 recreates a simple shared key, instead of using the user's certification.



- ✓ **WPA Mode:** Administrator can select security for Auto or only WPA or only WPA2.
- ✓ **Cipher Type:** Administrator can select use AES or TKIP with WPA / WPA2 encryption method.

AES is short for “**Advanced Encryption Standard**”, The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plaintext into the final output of ciphertext. Each round consists of several processing steps, including one that depends on the encryption key. A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key.

TKIP is short for “**Temporal Key Integrity Protocol**”, TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with.

- ✓ **Group Key Update Interval:** This time interval for re-keying GTK (broadcast/multicast encryption keys) in seconds. Enter the time-length required; the default time is 600 seconds.
- ✓ **Pass Phrase:** Enter the ESSID pass phrase.
- ✓ **WPS:** Administrator can used WPS function link WiFi client, if select enable the function, administrator can click the WPS Push Button.
- **802.1X security:** When 802.1x Authentication is enabled, please refer to the following Dynamic WEP and RADIUS settings to complete the configuration.

☰ RADIUS Server Settings

Key Size 64 Bits 128 Bits

Radius Server

Radius Port Port

Radius Secret

- ✓ **Key Size:** Check on the respected button to enable either 64bits or 128bits key length. The system will automatically generate WEP keys for encryption.
- ✓ **Radius Server:** Enter the IP address of the Authentication RADIUS server.
- ✓ **Radius Port:** The port number used by Authentication RADIUS server. Use the default 1812 or enter port number specified.
- ✓ **Radius Secret:** The secret key for system to communicate with Authentication RADIUS server. Support 1 to 64 characters.

5.3.7 MAC Filter

The administrator can allow or reject WiFi clients to access AP.

☰ MAC Rules

Rule Save

Add MAC Address

MAC Address **Add**

MAC Address List

#	MAC Address	Action	#	MAC Address	Action
-	-	-	-	-	-

- **Rule:** Select the desired access control type from the drop-down list; the options are Disable, Allow or Reject.

MAC Rules

Rule **Save**

- Disable
- Only Deny List MAC
- Only Allow List MAC

- **Only Allow List MAC:** Define certain wireless clients in the list which will have granted access to the Access Point while the access will be denied for all the remaining clients – Action Type is set to “**Only Allow List MAC**”.
 - **Only Deny List MAC:** Define certain wireless clients in the list which will have denied access to the Access Point while the access will be granted for all the remaining clients – Action Type is set to “**Only Deny List MAC**”.
- **MAC Address:** Enter MAC Address for WiFi Clients.
 - **MAC Address List:** Display the MAC address of WiFi Clients.

5.3.8 802.11r/802.11k Fast Roaming

The system support 802.11r/802.11k function for 2.4G and 5G radio. 802.11r, which is the IEEE standard for fast roaming, introduces a new concept of roaming where the initial handshake with the new AP is done even before the client roams to the target AP.

Fast Roaming Settings

Mobility Domain	<input type="text" value="a1b2"/>
R0 Key Lifetime	<input type="text" value="10000"/>
Reassoc deadline	<input type="text" value="1000"/>
R0/NAS Identifier	<input type="text" value="ap.example.com"/>
R1 Identifier	<input type="text" value="000102030405"/>
R1 Push	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

- **Mobility Domain:** MDID is used to indicate a group of APs (within an ESS, i.e., sharing the same SSID) between which a STA can use Fast BSS Transition. Please enter 2-octet identifier as a hex string.
- **R0 Key Lifetime:** Default lifetime of the PMK-RO in minutes, the default is 10000, administrator can setting 1~65535.
- **Reassoc deadline:** Reassociation deadline in time units (TUs / 1.024 ms; range 1000~65535). The default is 1000.
- **R0/NAS Identifier:** PMK-R0 Key Holder identifier. When using IEEE 802.11r, nas_identifier must be set and must be between 1 and 48 octets long.
- **R1 Identifier:** PMK-R1 Key Holder identifier 6-octet identifier as a hex string.
- **R1 Push:** Administrator can select Enable or disable. If enable the function will automatically sent the R1 Key.

R0 Key Address:

To enable roaming between multiple AP devices, AP1 must key in the MAC Address of AP2, and AP2 must key in the MAC Address of AP1. The NAS Identifier and 128-bit Key should be identical in both AP settings. This will enable device roaming between the two Access Points.

R0 Key holders

MAC Address	<input type="text" value="Destination MAC Address"/>
NAS Identifier	<input type="text" value="(1-48 octets)"/>
128-bit Key	<input type="text" value="128-bit key as hex string"/> <input style="background-color: #006633; color: white; padding: 2px 5px; border: none;" type="button" value="Add"/>

- **MAC Address:** Enter must key in the MAC Address of other AP
- **NAS Identifier:** Enter 1~48 octets of network domain name.
- **128-bit Key:** Enter Shared Key of 128 bit.

R0 Key Holder List:

After setting "R0 Key holders" function the information will appear in list.

R0 Key Holder List				
#	MAC Address	NAS Identifier	128-bit Key	Action
-	-	-	-	-

R1 Key Holder List:

Enter a unified set of R1 Key Holder identification certification.

R1 Key Holders	
MAC Address	<input type="text" value="Destination MAC Address"/>
R1 Identifier	<input type="text" value="R1 Identifier"/>
128-bit Key	<input type="text" value="128-bit key as hex string"/> <input type="button" value="Add"/>

- **MAC Address:** Enter the main roaming device MAC address
- **R1 Identifier:** Enter Shared identifier.
- **128-bit Key:** Enter Shared Key of 128 bit.

R1 Key Holder List:

After setting "R1 Key holders" function the information will appear in list.

R1 Key Holder List				
#	MAC Address	NAS Identifier	128-bit Key	Action
-	-	-	-	-

6. WISP Mode

WISP Mode is a router function, if the Telecom company permits wireless connection to their WAN, administrators can change OW-400-A2 to WISP Mode to connect to the wifi network.

The WISP Mode support PPPoE / Static IP / Dynamic IP and PPTP for WAN, and support Repeater AP function.



If wireless WAN used 2.4G radio connection to Telecom company station, the Repeater AP radio only used 5G radio. So wireless WAN used 5G radio connection to Telecom company station, the Repeater AP radio only used 2.4G radio.

6.1 Configure WAN Setup

There are four connection types for the WAN port : **Static IP**, **Dynamic IP**, **PPPoE** and **PPTP**.

Please click on **System -> WAN** and follow the below setting.

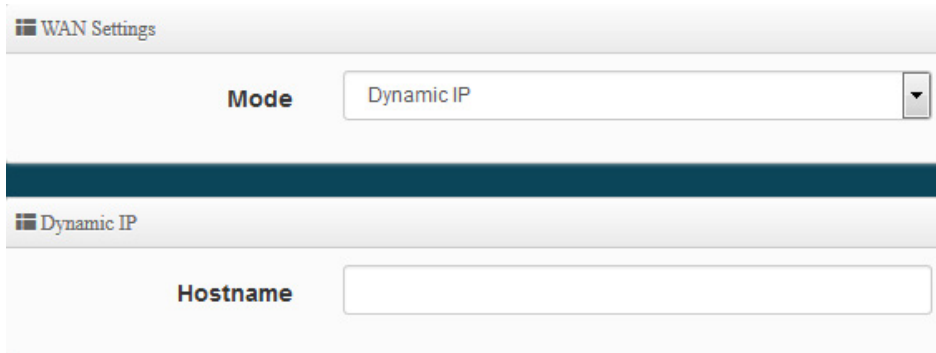
The screenshot shows the WAN Settings configuration page. The 'Mode' dropdown is set to 'Static IP'. Below it, there are input fields for 'IP Address', 'Netmask', and 'Gateway'. To the right, the 'MAC Clone' section is set to 'Default MAC Address'. The 'DNS' section has 'Primary DNS' set to '8.8.8.8' and 'Secondary DNS' is empty. The 'NAT' section has 'Enable' selected.

WAN Setting

The close-up shows the 'Mode' dropdown menu with the following options: Static IP (selected), Dynamic IP, PPPoE, and PPTP.

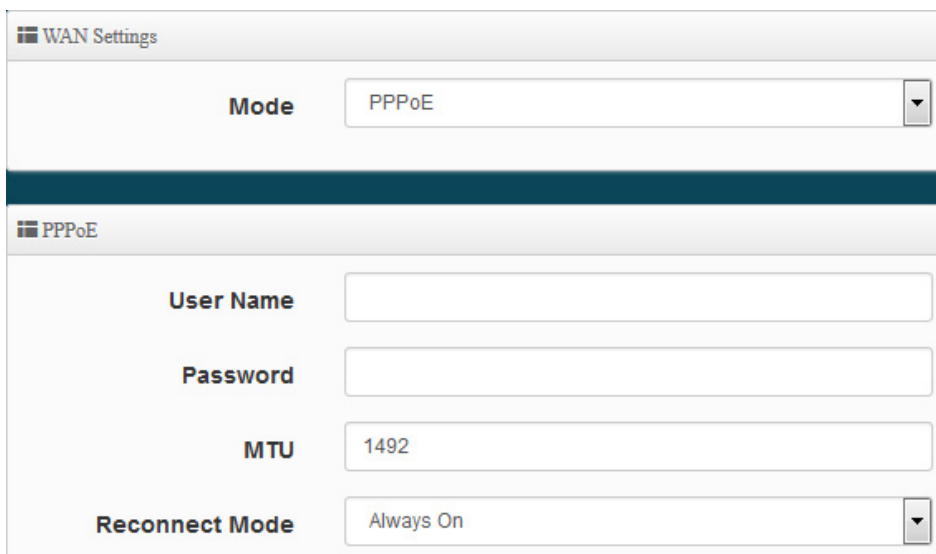
- **Static IP** : Users can manually setup the WAN IP address with a static IP provided by WISP.
 - **IP Address** : The IP address of the WAN port.
 - **IP Netmask** : The Subnet mask of the WAN port.
 - **IP Gateway** : The default gateway of the WAN port.

- **Dynamic IP** : Please consult with WISP for correct wireless settings to associate with WISP AP before a dynamic IP, along with related IP settings. If IP Address is not assigned, please double check with your wireless settings and ensure successful association. Also, you may go to **“WAN Information”** in the Overview page to click **Release** button to release IP address and click **Renew** button to renew IP address again.



The screenshot shows the 'WAN Settings' configuration page. Under the 'Dynamic IP' section, the 'Mode' is set to 'Dynamic IP' and the 'Hostname' field is empty.

- **Hostname** : The Hostname of the WAN port
- **PPPoE** : To create wireless PPPoE WAN connection to a PPPoE server in network.



The screenshot shows the 'WAN Settings' configuration page for PPPoE. The 'Mode' is set to 'PPPoE'. Under the 'PPPoE' section, the 'User Name' and 'Password' fields are empty, 'MTU' is set to 1492, and 'Reconnect Mode' is set to 'Always On'.

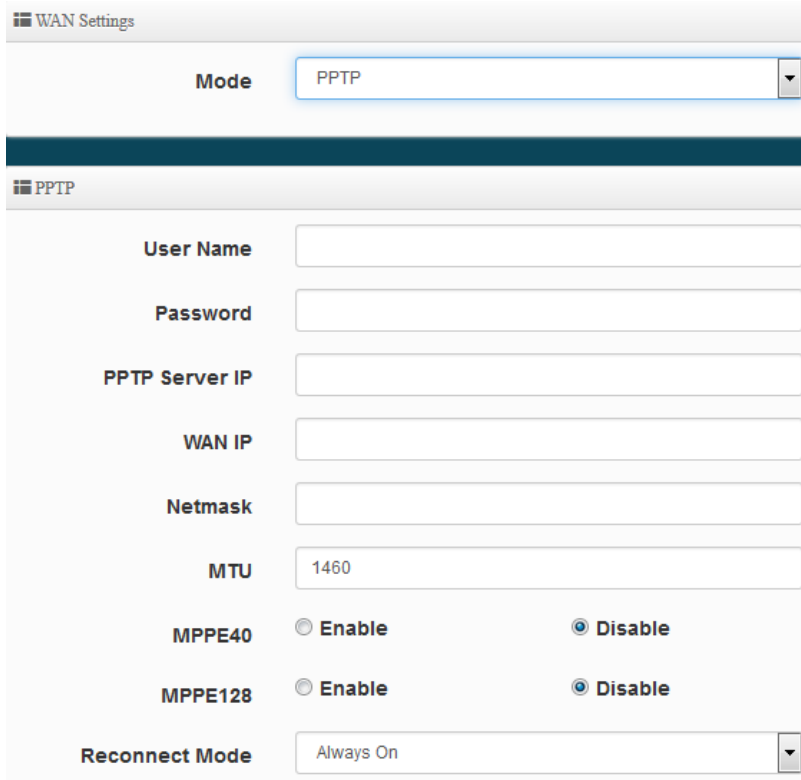
- **User Name** : Enter User Name for PPPoE connection
- **Password** : Enter Password for PPPoE connection
- **MTU** : By default, MTU is set to **1492** bytes. MTU stands for Maximum Transmission Unit. Consult with WISP for a correct MTU setting.
- **Reconnect Mode** : Administrator can select three function for Always On / On Demand / Manual.
 - ✓ **Always on** – A connection to Internet is always maintained.
 - ✓ **On Demand** – A connection to Internet is made as needed.



*When **Time Server** is enabled at the “On Demand” mode, the “Reconnect Mode” will turn out “Always on”.*

- ✓ **Manual** – Click the “**Connect**” button on “**WAN Information**” in the Overview page to connect to the Internet.


- **PPTP** : The Point-to-Point Tunneling Protocol (PPTP) mode enables the implementation of secure multi-protocol Virtual Private Networks (VPNs) through public networks.



The screenshot shows the WAN Settings interface. At the top, the 'Mode' is set to 'PPTP'. Below this, the PPTP configuration section includes the following fields and options:

- User Name**: Text input field.
- Password**: Text input field.
- PPTP Server IP**: Text input field.
- WAN IP**: Text input field.
- Netmask**: Text input field.
- MTU**: Text input field with the value '1460'.
- MPPE40**: Radio buttons for 'Enable' and 'Disable', with 'Disable' selected.
- MPPE128**: Radio buttons for 'Enable' and 'Disable', with 'Disable' selected.
- Reconnect Mode**: Dropdown menu set to 'Always On'.

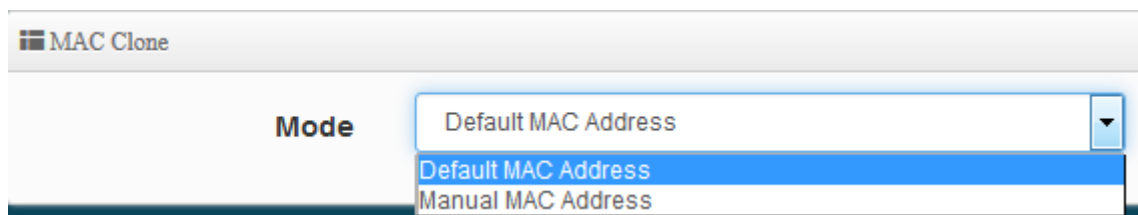
- **User Name**: Enter account for PPTP.
- **Password**: Enter user name account used password for PPTP.
- **PPTP Server IP**: Enter remote IP address of PPTP Server.
- **WAN IP**: The IP address of the WAN port.
- **Netmask** : The Subnet mask of the WAN port.
- **MTU** : By default, it's **1460** bytes. MTU stands for Maximum Transmission Unit. Consult with WISP for a correct MTU setting.
- **MPPE40/128**: Microsoft Point-to-Point Encryption (MPPE) encrypts data in Point-to-Point Protocol(PPP)-based dial-up connections or Point-to-Point Tunneling Protocol (PPTP) virtual private network (VPN) connections. **128-bit** key (strong) and **40-bit** key (standard) MPPE encryption schemes are supported. MPPE provides data security for the PPTP connection that is between the VPN client and the VPN server.
- **Reconnect Mode** : Administrator can select three function for Always On / On Demand / Manual.
 - ✓ **Always on** – A connection to Internet is always maintained.
 - ✓ **On Demand** – A connection to Internet is made as needed.

 **Notice** When **Time Server** is enabled at the “On Demand” mode, the “Reconnect Mode” will turn out “Always on”.

- ✓ **Manual** – Click the “**Connect**” button on “**WAN Information**” in the Overview page to connect to the Internet.

➤ **MAC Clone**

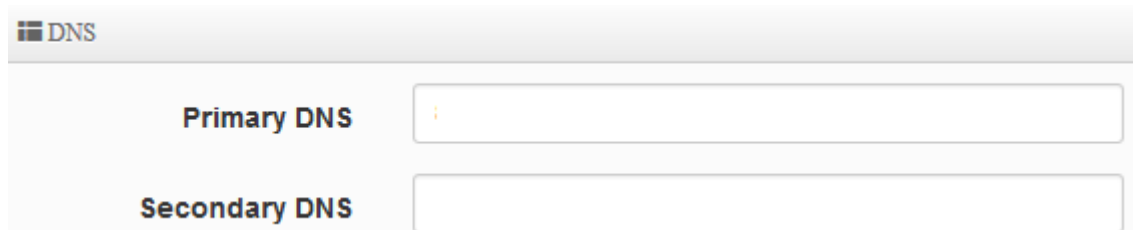
The MAC address is a 12-digit HEX code uniquely assigned to hardware as identification. Some ISPs require you to register a MAC address in order to access to Internet. If not, you could use default MAC or clone MAC from a PC.



- **Default MAC Address:** Keep the default MAC address of WAN port on the system.
- **Manual MAN Address:** Enter the MAC address registered with your ISP.

➤ **DNS**

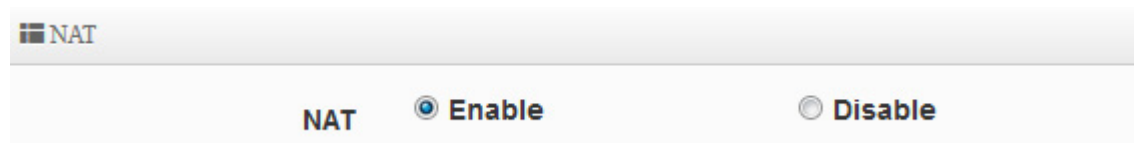
Check “No Default DNS Server” or “Specify DNS Server IP” radial button as desired to set up system DNS.



- **Primary DNS:** The IP address of the primary DNS server.
- **Secondary DNS:** The IP address of the secondary DNS server.

➤ **NAT**

The NAT support Enable and Disable Service



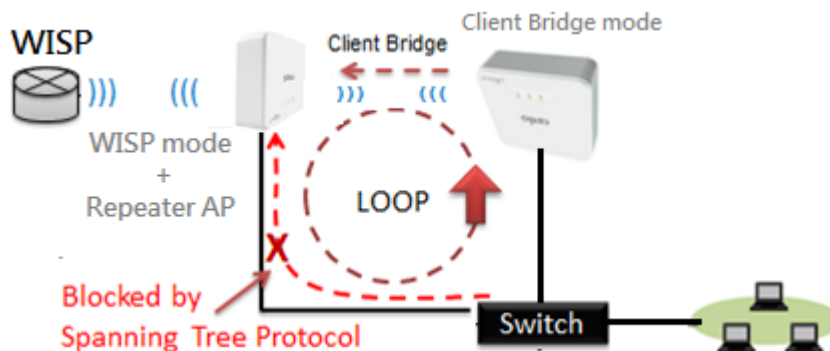
6.2 Configure LAN Setup

Here are the instructions for how to setup the local IP Address and Netmask. Please click on **System -> LAN** and follow the below setting.

IP Settings	
IP Address	192.168.2.254
Netmask	255.255.255.0
802.1d Spanning Tree	
802.1d Spanning Tree	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

IP Setup : The administrator can manually setup the LAN IP address.

- **IP Address :** The IP address of the LAN port; default IP address is 192.168.2.254
- **IP Netmask :** The Subnet mask of the LAN port; default Netmask is 255.255.255.0
- **802.1d Spanning Tree :** The spanning tree network protocol provides a loop free topology for a bridged LAN between LAN interface and 8 WDS interfaces from wds0 to wds7. The Spanning Tree Protocol, which is also referred to as STP, is defined in the IEEE Standard 802.1d



6.3 Configure DHCP Server

The DHCP Service function in the Client Bridge device can select a separate IP Address range within the same network segment of the source AP, and allocate those IP Addresses to connecting clients.

DHCP Service	
Mode	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

DHCP Setup	
Start IP	192.168.2.100
End IP	192.168.2.140
Netmask	255.255.255.0
Gateway	192.168.2.1
DNS1 IP	192.168.2.1
DNS2 IP	
WINS IP	
Domain	
Lease Time	86400

- **Start IP / End IP:** Specify the range of IP addresses to be used by the DHCP server when assigning IP address to clients.
- **Netmask:** The netmask default is 255.255.255.0.
- **Gateway:** Enter source gateway IP address.
- **DNS1:** Enter IP address of the first DNS server; this field is required.
- **DNS2:** Enter IP address of the second DNS server; this is optional.
- **WINS IP :** Enter IP address of the Windows Internet Name Service (WINS) server; this is optional.
- **Domain:** Enter the domain name for this network.
- **Lease Time:** The IP addresses given out by the DHCP server will only be valid for the duration specified by the lease time. Increasing the time ensure client operation without interruptions, but could introduce potential conflicts. Lowering the lease time will avoid potential address conflicts, but might cause more interruptions to the client while it will acquire new IP addresses from the DHCP server. Default is **86400** seconds

DHCP Clients List: When users link OW-400-A2 and use IP address of the DHCP service, the DHCP Client List will display users the information and used IP address.

DHCP Client List				
#	IP Address	MAC Address	Expired	Action
-	-	-	-	-

- **IP Address:** Display users used IP address.
- **MAC Address:** Display MAC Address of users used device.

- **Expired:** Display Lease expiration time of IP address.
- **Action:** Kicked user button.

Static Lease IP Setup: Administrator can set as static IP address for users.

Static Lease IP Setup

Comment

IP Address

MAC Address Add

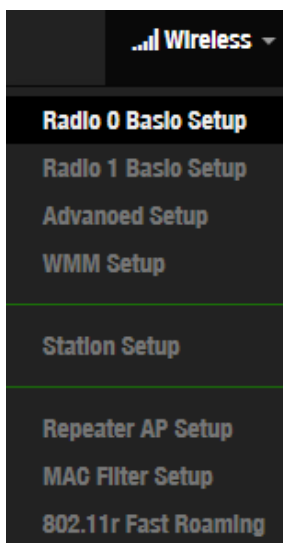
- **Comment:** Enter description for the information.
- **IP Address:** Set static IP address for users.
- **MAC Address:** Set MAC address of user device.

Static Lease IP List: Display users list of static IP address.

Static Lease IP List				
#	Comment	IP Address	MAC Address	Action
-	-	-	-	-

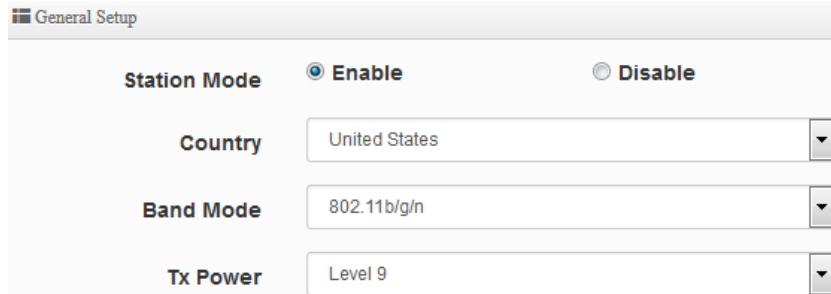
6.4 Wireless General Setup

The main setting for Client Bridge mode link to AP Station, Repeater AP functions setting, MAC filter, WMM and 802.11r/802.11k Fast Roaming etc.



6.4.1 Radio 0(2.4G) Basic Setup

Administrator can change the data transmission, channel and output power settings for the system.



General Setup

Station Mode Enable Disable

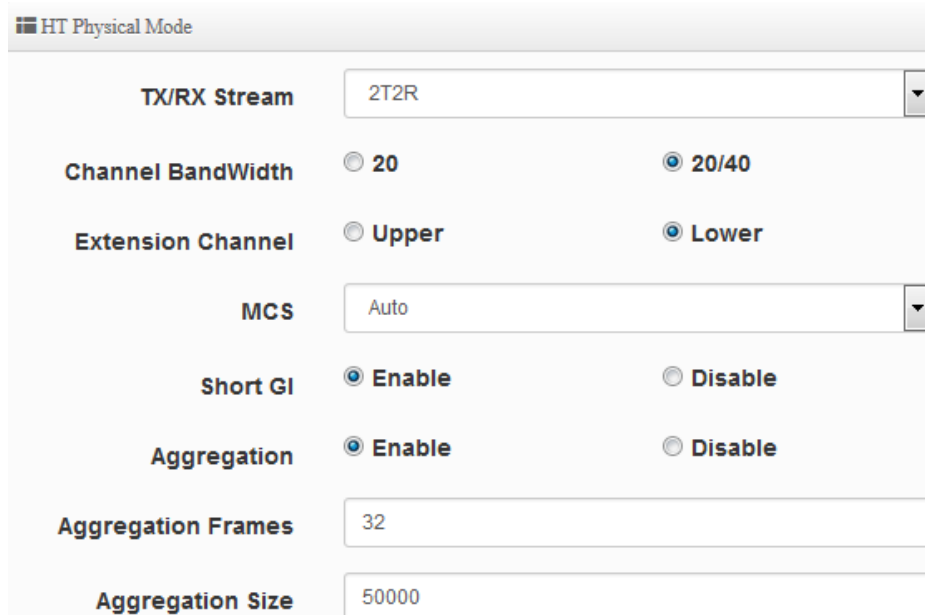
Country

Band Mode

Tx Power

- **Station Mode:** Administrator can Enable or Disable the radio.
- **Country:** Administrator can select country used channel by US and EU.
- **Band Mode:** Select an appropriate wireless band; bands available are **801.11 b/g/n mixed mode**.
- **Tx Power:** Administrator can adjust the output power of the system to get the appropriate coverage for your wireless network. Specify digit numbers between level **1** to level **9** (the unit is %) for your environment. If you are not sure which setting to choose, then keep the default setting level **9 (100%)**.

HT Physical Mode



HT Physical Mode

TX/RX Stream

Channel BandWidth 20 20/40

Extension Channel Upper Lower

MCS

Short GI Enable Disable

Aggregation Enable Disable

Aggregation Frames

Aggregation Size

- **TX/RX Stream:** OW-400-A2 utilizes 2 antennas, supporting 2TX/2RX streams. Administrator can select 1 or 2 TX/RX. The default is 2TX/2RX.
- **Channel Bandwidth:** The "**20/40**" MHz option is usually best. The other option is available for special circumstances.

- **Extension Channel:** Set channel select of Upper or Lower, the Upper support 1 to 7 range CH and Lower support 5 to 11 range CH.
- **MCS:** This parameter represents transmission rate. By default (Auto) the fastest possible transmission rate will be selected. You have the option of selecting the speed if necessary.
- **Shout GI:** Short Guard Interval, by default, it's "Enable". it's can increase throughput. However, it can also increase error rate in some installations, due to increased sensitivity to radio-frequency reflections. Select the option that works best for your installation.
- **Aggregation:** By default, it's "Enable". To "Disable" to deactivated Aggregation. A part of the 802.11n standard (or draft-standard). It allows sending multiple frames per single access to the medium by combining frames together into one larger frame. It creates the larger frame by combining smaller frames with the same physical source and destination end points and traffic class (i.e. QoS) into one large frame with a common MAC header.
- **Aggregation Frames :** The Aggregation Frames is in the range of **2~64**, the default is **32**. It determines the number of frames combined on the new larger frame.
- **Aggregation Size :** The Aggregation Size is in the range of **1024~65535**, the default is **50000**. It determines the size (in Bytes) of the larger frame.

6.4.2 Radio 1(5G) Basic Setup

General Setup

Station Mode	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Country	<input type="text" value="United States"/>	
Band Mode	<input type="text" value="802.11ac"/>	
Auto Channel	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Channel	<input type="text" value="36 (5180 Mhz)"/>	
Tx Power	<input type="text" value="Level 9"/>	

- **Station Mode:** Administrator can Enable or Disable the radio.
- **Country:** Administrator can select a country: US or EU.
- **Band Mode:** Administrator can select 5G Band for 802.11a/n or 802.11ac. The default is 802.11ac
- **Auto Channel:** Administrator can Enable or Disable the function. If select disable function the WiFi channel can be fixed a channel.
- **Channel:** Support US and Eu country by 5G Channel.

- **Tx Power:** Administrator can control the WiFi Tx output power. The power Max. Level 9.

HT Physical Mode

HT Physical Mode

TX/RX Stream	<input type="text" value="2T2R"/>
Channel BandWidth	<input type="text" value="80"/>
Short GI	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Aggregation	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Aggregation Frames	<input type="text" value="32"/>
Aggregation Size	<input type="text" value="50000"/>

- **TX/RX Stream:** The OW-400-A2 utilizes 2 antenna and supports 2TX/2RX streams. Administrator can select 1 or 2 TX/RX. The default is 2TX/2RX.
- **Channel Bandwidth:** The "20/40 and 802.11ac 80" MHz option is usually best. The other option is available for special circumstances.
- **Shout GI:** Short Guard Interval, by default, it's "Enable". it's can increase throughput. However, it can also increase error rate in some installations, due to increased sensitivity to radio-frequency reflections. Select the option that works best for your installation.
- **Aggregation:** By default, it's "Enable". To "Disable" to deactivated Aggregation. A part of the 802.11n standard (or draft-standard). It allows sending multiple frames per single access to the medium by combining frames together into one larger frame. It creates the larger frame by combining smaller frames with the same physical source and destination end points and traffic class (i.e. QoS) into one large frame with a common MAC header.
- **Aggregation Frames :** The Aggregation Frames is in the range of 2~64, default is 32. It determines the number of frames combined on the new larger frame.
- **Aggregation Size :** The Aggregation Size is in the range of 1024~65535, default is 50000. It determines the size (in Bytes) of the larger frame.

6.4.3 Advanced Setup

The administrator can change the Slot Time, ACK Timeout, RTS threshold and fragmentation threshold settings for the system.

Advanced Setup	
Slot Time	9 Distance
ACK Timeout	64
Beacon Interval	100
DTIM Interval	1
Fragment Threshold	2346
RTS Threshold	2346
Short Preamble	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
IGMP Snooping	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Greenfield	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

- **Slot Time** : Slot time is in the range of **9~1489** and set in unit of **microsecond**. The default value is **9** microsecond.
 Slot time is the amount of time a device waits after a collision before retransmitting a packet. Reducing the slot time decreases the overall back-off, which increases throughput. Back-off, which is a multiple of the slot time, is the random length of time a station waits before sending a packet on the LAN. For a sender and receiver own right of the channel the shorter slot time help manage shorter wait time to re-transmit from collision because of hidden wireless clients or other causes. When collision sources can be removed sooner and other senders attempting to send are listening the channel(CSMA/CA) the owner of the channel should continue ownership and finish their transmission and release the channel. Then, following ownership of the channel will be sooner for the new pair due to shorter slot time. However, when long duration of existing collision sources and shorter slot time exist the owners might experience subsequent collisions. When adjustment to longer slot time can't improve performance then RTS/CTS could supplement and help improve performance.
- **ACK Timeout** : ACK timeout is in the range of **1~372** and set in unit of **microsecond**. The default value is **64** microsecond.

All data transmission in 802.11b/g request an “Acknowledgement” (ACK) send by receiving radio. The transmitter will resend the original packet if correspondent ACK failed to arrive within specific time interval, also refer to as “ACK Timeout”.

ACK Timeout is adjustable due to the fact that distance between two radio links may vary in different deployment. ACK Timeout makes significant influence in performance of long distance radio link. If ACK Timeout is set too short, transmitter will start to “Resend” packet before ACK is received, and throughput become low due to excessively high re-transmission.

ACK Timeout is best determined by distance between the radios, data rate of average environment. The Timeout value is calculated based on round-trip time of packet with a little tolerance, So, if experiencing re-transmissions or poor performance the ACK Timeout could be made longer to accommodate.



Slot Time and ACK Timeout settings are for long distance links. It is important to tweak settings to achieve the optimal result based on requirement.

- **Beacon Interval:** Beacon Interval is in the range of **40~3500** and set in unit of *millisecond*. The default value is **100** msec.
Access Point (AP) in IEEE 802.11 will send out a special approximated 50-byte frame, called “Beacon”. Beacon is broadcast to all the stations, provides the basic information of AP such as SSID, channel, encryption keys, signal strength, time stamp, support data rate. All the radio stations received beacon recognizes the existence of such AP, and may proceed next actions if the information from AP matches the requirement. Beacon is sent on a periodic basis, the time interval can be adjusted.
By increasing the beacon interval, you can reduce the number of beacons and associated overhead, but that will likely delay the association and roaming process because stations scanning for available access points may miss the beacons. You can decrease the beacon interval, which increases the rate of beacons. This will make the association and roaming process very responsive; however, the network will incur additional overhead and throughput will go down.
- **DTIM Interval :** The DTIM interval is in the range of **1~255**. The default is **1**.
DTIM is defined as *Delivery Traffic Indication Message*. It is used to notify the wireless stations, which support power saving mode, when to wake up to receive multicast frame. DTIM is necessary and critical in wireless environment as a mechanism to fulfill power-saving synchronization.

A DTIM interval is a count of the number of beacon frames that must occur before the access point sends the buffered multicast frames. For instance, if DTIM Interval is set to 3, then the Wi-Fi clients will expect to receive a multicast frame after receiving three Beacon frame. The higher DTIM interval will help power saving and possibly decrease wireless throughput in multicast applications.

- **Fragmentation Threshold:** Fragmentation Threshold is one more parameter which is given in all stations and Access points. Fine tuning Fragmentation Threshold parameter can result in good throughput but not using it properly can results in low throughput. In simple words it does the same thing which MTU do in Ethernet. Both are different parameters but the work done is same , it fragments the data packets.

Fragmentation threshold will be used when we have more data packet size to be transmitted and we have less fragment threshold value. Lets say from Ethernet we have to send 1400 byte packet but the fragmentation threshold is set as 400. In this case when the packet is to be transmitted on air it will fragment the packet in to 4 small packet 400+400+400+200 and send on air. This includes MAC header+ frame body and CRC so 400 byte will be in total including headers. This helps in increasing the throughput. The default is 2346.

- **RTS Threshold:** TRTS Threshold is in the range of **1~2347** byte. The default is **2347** byte. The main purpose of enabling RTS by changing RTS threshold is to reduce possible collisions due to hidden wireless clients. RTS in AP will be enabled automatically if the packet size is larger than the Threshold value. By default, RTS is disabled in a normal environment supports non-jumbo frames.

- **Short Preamble:** By default, it's "**Enable**". To **Disable** is to use Long 128-bit Preamble Synchronization field.

The preamble is used to signal "here is a train of data coming" to the receiver. The short preamble provides 72-bit Synchronization field to improve WLAN transmission efficiency with less overhead.

- **IGMP Snooping:** the process of listening to Internet Group Management Protocol (IGMP) network traffic. The feature allows a network switch to listen in on the IGMP conversation between hosts and routers. By listening to these conversations the switch maintains a map of which links need which IP multicast streams. Multicasts may be filtered from the links which do not need them and thus controls which ports receive specific multicast traffic.

- **Greenfield:** In wireless WLAN technology, greenfield mode is a feature of major components of the 802.11n specification. The greenfield mode feature is designed to improve efficiency by eliminating support for 802.11b/g devices in an all draft-n network. In greenfield mode the network can be set to ignore all earlier standards.

6.4.4 WMM Setup

This affects traffic flowing from the access point to the client station.

Configuring QoS options consists of setting parameters on existing queues for different types of wireless traffic. You can configure different minimum and maximum wait times for the transmission of packets in each queue based on the requirements of the media being sent.

Queues automatically provide minimum transmission delay for Voice, Video, multimedia, and mission critical applications, and rely on best-effort parameters for traditional IP data.

As an Example, time-sensitive Voice & Video, and multimedia are given effectively higher priority for transmission (lower wait times for channel access), while other applications and traditional IP data which are less time-sensitive but often more data-intensive are expected to tolerate longer wait times.

WMM Setup

WMM **Enable** **Disable**

WMM Parameters of Access Point

AC Type	CWmin	CWmax	AIFS	TxOp Limit	No ACK Policy bit
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"/>
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="1"/>	<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="1"/>	<input type="text" value="1504"/>	<input type="checkbox"/>

WMM Parameters of Station

AC Type	CWmin	CWmax	AIFS	TxOp Limit	ACM bit
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 :**

Queue	Data Transmitted AP to Clients	Priority	Description
AC_BK	Background	Low	High throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).
AC_BE	Best Effort	Medium	Medium throughput and delay. Most traditional IP data is sent to this queue.
AC_VI	Video	High	Minimum delay. Time-sensitive video data is automatically sent to this queue.
AC_VO	Voice	High	Time-sensitive data like VoIP and streaming media are automatically sent to this queue.

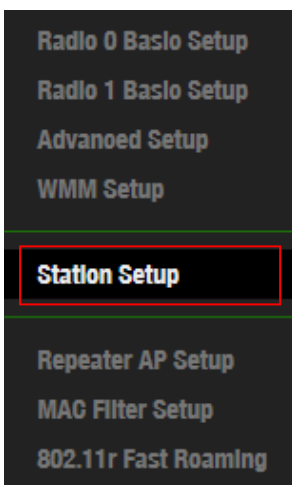
✓ **CWmin :**

Minimum Contention Window. This parameter is input to the algorithm that determines the initial random backoff wait time ("window") for retry of a transmission. The value specified here in the Minimum Contention Window is the upper limit (in milliseconds) of a range from which the initial random backoff wait time is determined. ◦

- ✓ **CWmax :** Maximum Contention Window. The value specified here in the Maximum Contention Window is the upper limit (in milliseconds) for the doubling of the random backoff value. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached. Once the Maximum Contention Window size is reached, retries will continue until a maximum number of retries allowed is reached. Valid values for the "cwmax" are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024. The value for "cwmax" must be higher than the value for "cwmin". ◦
- ✓ **AIFS :** The Arbitration Inter-Frame Spacing Number specifies a wait time (in milliseconds) for data frames ◦
- ✓ **TxOP Limit :** Transmission Opportunity is an interval of time when a WME AP has the right to initiate transmissions onto the wireless medium (WM). This value specifies (in milliseconds) the Transmission Opportunity (TXOP) for AP; that is, the interval of time when the WMM AP has the right to initiate transmissions on the wireless network. ◦
- ✓ **ACM bit :** Admission Control Mandatory, ACM only takes effect on AC_VI and AC_VO. When you do not click Checkbox, it means that the ACM is controlled by the connecting AP. If you click Checkbox, it means that the Client is in charge ◦
- ✓ **No ACK policy bit :** Acknowledgment Policy, WMM defines two ACK policies: **Normal ACK** and **No ACK**. Click "Checkbox" indicates "No ACK"

When the no acknowledgement (No ACK) policy is used, the recipient does not acknowledge received packets during wireless packet exchange. This policy is suitable in the environment where communication quality is fine and interference is weak. While the No ACK policy helps improve transmission efficiency, it can cause increased packet loss when communication quality deteriorates. This is because when this policy is used, a sender does not retransmit packets that have not been received by the recipient. When the Normal ACK policy is used, the recipient acknowledges each received unicast packet. ◦

6.4.5 Station Setup



The functions setting functions include Client Bridge link to AP station. Administrator can used “site survey” function to Search for AP stations.

Channel	Signal	BSSID	ESSID	Authentication	Setup
-	-	-	-	-	-

- **MAC Address List** : The function main discovery AP Station and select want to link the AP station.

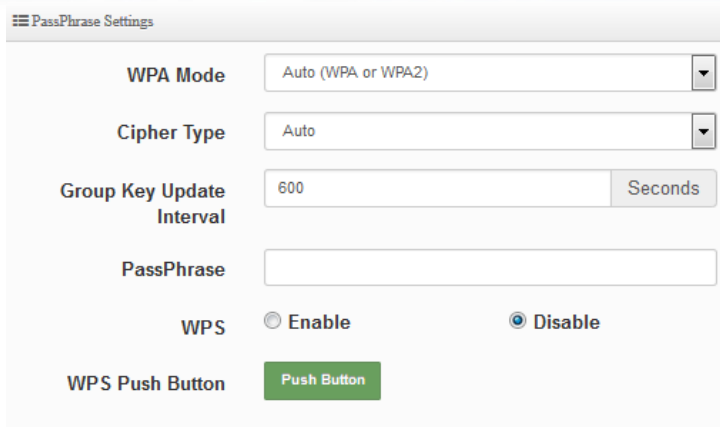
- **Security/ PassPhrase Settings:** If link as AP station the AP station have used security, administrator can select AP station used authentication mode and enter password in the functions.

6.4.6 Repeater AP Setup

Administrators can configure ESSID, SSID broadcasting, Maximum number of client associations.

- **Access Point:** Administrator can Enable or Disable the Repeater AP function.
- **ESSID:** Enter the Repeater AP of ESSID name.
- **SSID Visibility:** The default it's Enable. When select Disable the SSID will not be discovered.
- **Client Isolation:** This function is Disabled by default. All clients will be isolated from each other, which mean they can't reach each other.
- **Connection Limit:** This function is Disabled by default. If select Enable, Administrator can limit Wi-Fi users the Quantity.
- **Authentication:** Select the desired security type from the drop-down list; the options are WPA-PSK, WPA2-PSK, WPA/WPA2-Enterprise and WEP 802.1X.

- **Open System:** Data are not unencrypted during transmission when this option is selected.
- **WPA/WPA2 Personal:** WPA/WPA2 is short for W-Fi Protected Access-Pre-Shared Key. WPA/WPA2 uses the same encryption way with WPA, and the only difference between them is that WPA/WPA2 recreates a simple shared key, instead of using the user's certification.



PassPhrase Settings

WPA Mode: Auto (WPA or WPA2)

Cipher Type: Auto

Group Key Update Interval: 600 Seconds

PassPhrase: [Empty text box]

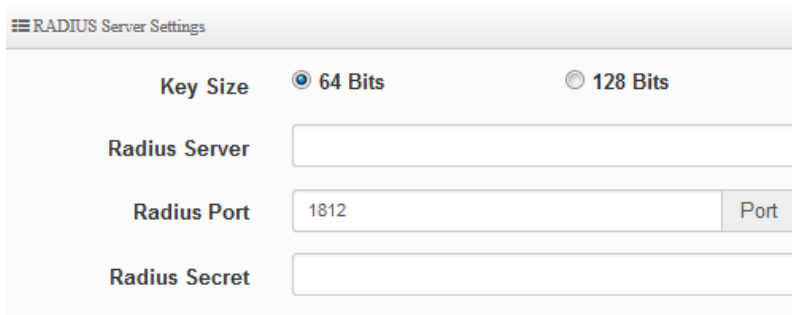
WPS: Enable Disable

WPS Push Button: Push Button

- ✓ **WPA Mode:** Administrator can select security for Auto or only WPA or only WPA2.
- ✓ **Cipher Type:** Administrator can select use AES or TKIP with WPA / WPA2 encryption method.

AES is short for “**Advanced Encryption Standard**”, The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plaintext into the final output of ciphertext. Each round consists of several processing steps, including one that depends on the encryption key. A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key.

TKIP is short for “**Temporal Key Integrity Protocol**”, TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven’t been tampered with.
- ✓ **Group Key Update Interval:** This time interval for re-keying GTK (broadcast/multicast encryption keys) in seconds. Enter the time-length required; the default time is 600 seconds.
- ✓ **Pass Phrase:** Enter the ESSID pass phrase.
- ✓ **WPS:** Administrator can used WPS function link WiFi client, if select enable the function, administrator can click the WPS Push Button.
- **802.1X security:** When 802.1x Authentication is enabled, please refer to the following Dynamic WEP and RADIUS settings to complete the configuration.



RADIUS Server Settings

Key Size: 64 Bits 128 Bits

Radius Server: [Empty text box]

Radius Port: 1812 Port

Radius Secret: [Empty text box]

- ✓ **Key Size:** Check on the respected button to enable either 64bits or 128bits key length. The system will automatically generate WEP keys for encryption.
- ✓ **Radius Server:** Enter the IP address of the Authentication RADIUS server.

- ✓ **Radius Port:** The port number used by Authentication RADIUS server. Use the default 1812 or enter port number specified.
- ✓ **Radius Secret:** The secret key for system to communicate with Authentication RADIUS server. Support 1 to 64 characters.

6.4.7 MAC Filter

The administrator can allow or reject WiFi clients to access AP.

The screenshot shows the MAC Filter configuration interface with three main sections:

- MAC Rules:** A form with a 'Rule' dropdown menu currently set to 'Disable' and a green 'Save' button.
- Add MAC Address:** A form with a 'MAC Address' input field and a green 'Add' button.
- MAC Address List:** A table with the following structure:

#	MAC Address	Action	#	MAC Address	Action
-	-	-	-	-	-

- **Rule:** Select the desired access control type from the drop-down list; the options are Disable, Allow or Reject.

This close-up shows the dropdown menu for the 'Rule' field. The options are:

- Disable
- Only Deny List MAC
- Only Allow List MAC

 The 'Only Deny List MAC' option is currently selected and highlighted in blue.

- **Only Allow List MAC:** Define certain wireless clients in the list which will have granted access to the Access Point while the access will be denied for all the remaining clients – Action Type is set to “**Only Allow List MAC**”.
- **Only Deny List MAC:** Define certain wireless clients in the list which will have denied access to the Access Point while the access will be granted for all the remaining clients - Action Type is set to “**Only Deny List MAC**”.
- **MAC Address:** Enter MAC Address for WiFi Clients.
- **MAC Address List:** Display the MAC address of WiFi Clients.

6.4.8 802.11r/802.11k Fast Roaming

The system support 802.11r/802.11k function for 2.4G and 5G radio. 802.11r, which is the IEEE standard for fast roaming, introduces a new concept of roaming where the initial handshake with the new AP is done even before the client roams to the target AP.

Fast Roaming Settings

Mobility Domain	<input type="text" value="a1b2"/>
R0 Key Lifetime	<input type="text" value="10000"/>
Reassoc deadline	<input type="text" value="1000"/>
R0/NAS Identifier	<input type="text" value="ap.example.com"/>
R1 Identifier	<input type="text" value="000102030405"/>
R1 Push	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

- **Mobility Domain:** MDID is used to indicate a group of APs (within an ESS, i.e., sharing the same SSID) between which a STA can use Fast BSS Transition. Please enter 2-octet identifier as a hex string.
- **R0 Key Lifetime:** Default lifetime of the PMK-RO in minutes, the default is 10000, administrator can setting 1~65535.
- **Reassoc deadline:** Reassociation deadline in time units (TUs / 1.024 ms; range 1000~65535). The default is 1000.
- **R0/NAS Identifier:** PMK-R0 Key Holder identifier. When using IEEE 802.11r, nas_identifier must be set and must be between 1 and 48 octets long.
- **R1 Identifier:** PMK-R1 Key Holder identifier 6-octet identifier as a hex string.
- **R1 Push:** Administrator can select Enable or disable. If enable the function will automatically sent the R1 Key.

R0 Key Address:

To enable roaming between multiple AP devices, AP1 must key in the MAC Address of AP2, and AP2 must key in the MAC Address of AP1. The NAS Identifier and 128-bit Key should be identical in both AP settings. This will enable device roaming between the two Access Points.

R0 Key holders

MAC Address	<input type="text" value="Destination MAC Address"/>
NAS Identifier	<input type="text" value="(1-48 octets)"/>
128-bit Key	<input type="text" value="128-bit key as hex string"/> <input style="float: right; background-color: #006633; color: white; padding: 2px 5px; border: none;" type="button" value="Add"/>

- **MAC Address:** Enter must key in the MAC Address of other AP
- **NAS Identifier:** Enter 1~48 octets of network domain name.
- **128-bit Key:** Enter Shared Key of 128 bit.

R0 Key Holder List:

After setting "R0 Key holders" function the information will appear in list.

R0 Key Holder List				
#	MAC Address	NAS Identifier	128-bit Key	Action
-	-	-	-	-

R1 Key Holder List:

Enter a unified set of R1 Key Holder identification certification.

R1 Key Holders

MAC Address	<input type="text" value="Destination MAC Address"/>
R1 Identifier	<input type="text" value="R1 Identifier"/>
128-bit Key	<input type="text" value="128-bit key as hex string"/> <input style="float: right; background-color: #006633; color: white; padding: 2px 5px; border: none;" type="button" value="Add"/>

- **MAC Address:** Enter the main roaming device MAC address
- **R1 Identifier:** Enter Shared identifier.
- **128-bit Key:** Enter Shared Key of 128 bit.

R1 Key Holder List:

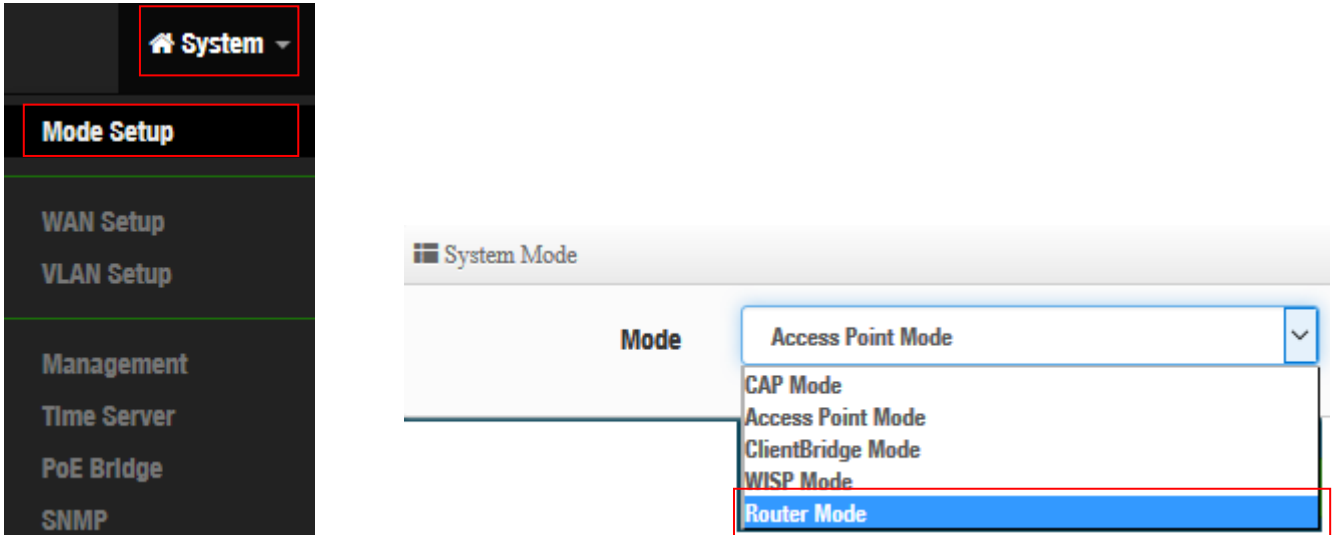
After setting "R1 Key holders" function the information will appear in list.

R1 Key Holder List				
#	MAC Address	NAS Identifier	128-bit Key	Action
-	-	-	-	-

7. Router Mode

When Router AP mode is chosen, the system can be configured as an Router AP mode. This section provides detailed explanation for users to configure in the Router AP mode with help of illustrations. In the Router AP mode, functions listed in the table below are also available from the Web-based GUI interface.

Please click “**System**”→” **Mode Setup**” to change Router Mode.



7.1 Configure WAN Setup

There are four connection types for the WAN port : **Static IP**, **Dynamic IP**, **PPPoE** and **PPTP**.

Please click on **System -> WAN** and follow the below setting.

The image shows the 'WAN Settings' configuration page. It is divided into several sections: 'WAN Settings' with a 'Mode' dropdown set to 'Static IP'; 'Static IP' with input fields for 'IP Address', 'Netmask', and 'Gateway'; 'MAC Clone' with a 'Mode' dropdown set to 'Default MAC Address'; 'DNS' with input fields for 'Primary DNS' (containing '8.8.8.8') and 'Secondary DNS'; and 'NAT' with radio buttons for 'Enable' (selected) and 'Disable'.

WAN Setting

The screenshot shows the 'WAN Settings' section. The 'Mode' dropdown menu is open, displaying the following options: Static IP (selected), Dynamic IP, PPPoE, and PPTP.


- **Static IP** : Users can manually setup the WAN IP address with a static IP provided by WISP.
 - **IP Address** : The IP address of the WAN port.
 - **IP Netmask** : The Subnet mask of the WAN port.
 - **IP Gateway** : The default gateway of the WAN port.
- **Dynamic IP** : Please consult with WISP for correct wireless settings to associate with WISP AP before a dynamic IP, along with related IP settings. If IP Address is not assigned, please double check with your wireless settings and ensure successful association. Also, you may go to **“WAN Information”** in the Overview page to click **Release** button to release IP address and click **Renew** button to renew IP address again.

The screenshot shows the 'WAN Settings' section with 'Dynamic IP' selected in the 'Mode' dropdown. Below this, there is a sub-section titled 'Dynamic IP' with a 'Hostname' text input field.

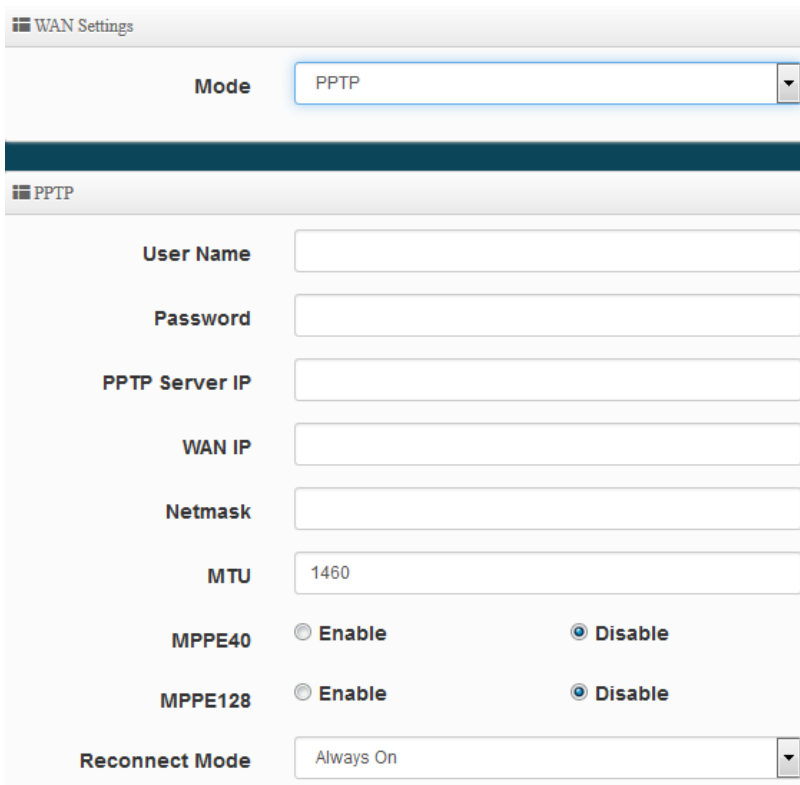
- **Hostname** : The Hostname of the WAN port
- **PPPoE** : To create wireless PPPoE WAN connection to a PPPoE server in network.

The screenshot shows the 'WAN Settings' section with 'PPPoE' selected in the 'Mode' dropdown. Below this, there is a sub-section titled 'PPPoE' with the following fields: 'User Name' (text input), 'Password' (text input), 'MTU' (text input with value 1492), and 'Reconnect Mode' (dropdown menu with 'Always On' selected).

- **User Name** : Enter User Name for PPPoE connection
- **Password** : Enter Password for PPPoE connection
- **MTU** : By default, MTU is set to **1492** bytes. MTU stands for Maximum Transmission Unit. Consult with WISP for a correct MTU setting.
- **Reconnect Mode** : Administrator can select three function for Always On / On Demand / Manual.
 - ✓ **Always on** – A connection to Internet is always maintained.
 - ✓ **On Demand** – A connection to Internet is made as needed.

 **Notice** When **Time Server** is enabled at the “On Demand” mode, the “Reconnect Mode” will turn out “Always on”.


- ✓ **Manual** – Click the “**Connect**” button on “**WAN Information**” in the Overview page to connect to the Internet.
- **PPTP** : The Point-to-Point Tunneling Protocol (PPTP) mode enables the implementation of secure multi-protocol Virtual Private Networks (VPNs) through public networks.



The screenshot shows the WAN Settings interface. At the top, the 'Mode' dropdown is set to 'PPTP'. Below this, the PPTP configuration section includes several input fields: 'User Name', 'Password', 'PPTP Server IP', 'WAN IP', and 'Netmask'. The 'MTU' field is pre-filled with '1460'. There are two rows of radio buttons for 'MPPE40' and 'MPPE128', both with 'Disable' selected. At the bottom, the 'Reconnect Mode' dropdown is set to 'Always On'.

- **User Name**: Enter account for PPTP.
- **Password**: Enter user name account used password for PPTP.
- **PPTP Server IP**: Enter remote IP address of PPTP Server.
- **WAN IP**: The IP address of the WAN port.
- **Netmask** : The Subnet mask of the WAN port.

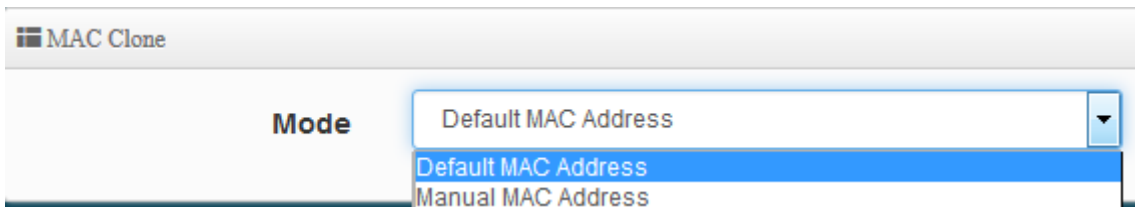
- **MTU** : By default, it's **1460** bytes. MTU stands for Maximum Transmission Unit. Consult with WISP for a correct MTU setting.
- **MPPE40/128**: Microsoft Point-to-Point Encryption (MPPE) encrypts data in Point-to-Point Protocol(PPP)-based dial-up connections or Point-to-Point Tunneling Protocol (PPTP) virtual private network (VPN) connections. **128-bit** key (strong) and **40-bit** key (standard) MPPE encryption schemes are supported. MPPE provides data security for the PPTP connection that is between the VPN client and the VPN server.
- **Reconnect Mode** : Administrator can select three function for Always On / On Demand / Manual.
 - ✓ **Always on** – A connection to Internet is always maintained.
 - ✓ **On Demand** – A connection to Internet is made as needed.

 *When **Time Server** is enabled at the “On Demand” mode, the “Reconnect Mode” will turn out “Always on”.*

- ✓ **Manual** – Click the “**Connect**” button on “**WAN Information**” in the Overview page to connect to the Internet.

➤ **MAC Clone**

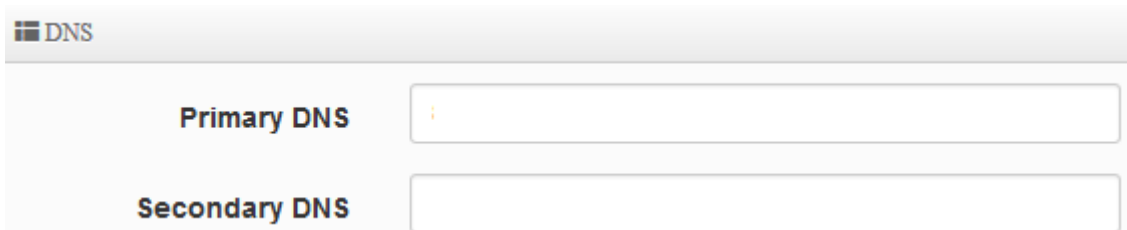
The MAC address is a 12-digit HEX code uniquely assigned to hardware as identification. Some ISPs require you to register a MAC address in order to access to Internet. If not, you could use default MAC or clone MAC from a PC.



- **Default MAC Address**: Keep the default MAC address of WAN port on the system.
- **Manual MAN Address**: Enter the MAC address registered with your ISP.

➤ **DNS**

Check “No Default DNS Server” or “Specify DNS Server IP” radial button as desired to set up system DNS.



- **Primary DNS**: The IP address of the primary DNS server.

- **Secondary DNS:** The IP address of the secondary DNS server.

➤ **NAT**

The NAT support Enable and Disable Service

NAT

NAT **Enable** **Disable**

7.2 Configure LAN Setup

Here are the instructions to setup the local IP Address / Netmask / Gateway / DNS and management Access Point 2.4G or 5G Radio on/off. Administrators can change settings such as LAN Spanning Tree and Tag VLAN functions.

#	VLAN Mode	Flag	IP Address	Netmask	Radio 0	Radio 1	Action
0	On	Native ETH0 Access Control	192.168.2.254	255.255.255.0	2.4G_0_0	5G_0_1	Network
1	Off	ETH0.101	-	-	2.4G_1_0	5G_1_1	Network
2	Off	ETH0.102	-	-	2.4G_2_0	5G_2_1	Network
3	Off	ETH0.103	-	-	2.4G_3_0	5G_3_1	Network
4	Off	ETH0.104	-	-	2.4G_4_0	5G_4_1	Network
5	Off	ETH0.105	-	-	2.4G_5_0	5G_5_1	Network
6	Off	ETH0.106	-	-	2.4G_6_0	5G_6_1	Network

<p>Gateway</p> <p>Default Gateway: <input type="text" value="192.168.2.1"/></p>	<p>DNS</p> <p>DNS1: <input type="text" value="192.168.2.1"/></p> <p>DNS2: <input type="text"/></p>
--	---

- **VLAN Mode** : Display on/off for the VLAN network.
- **Flag** : Display master VLAN and VLAN Tag No. information.
- **IP Address** : Display IP Address for VLAN Network.
- **NetMask** : Display IP netmask.
- **Radio 0** : Display radio 2.4G SSID name.
- **Radio 1** : Display radio 5G SSID name.
- **Action** : The button can set VLAN network functions and radio functions.

7.2.1 Network Button

Administrator can click **Network** button to set VLAN network functions.

VLAN Setup VLAN Mode <input checked="" type="radio"/> Enable <input type="radio"/> Disable <hr/> IP Setup IP Mode <input checked="" type="radio"/> Enable <input type="radio"/> Disable IP Address <input type="text" value="192.168.2.254"/> Netmask <input type="text" value="255.255.255.0"/>	Management Access Point 0 <input checked="" type="radio"/> Enable <input type="radio"/> Disable Access Point 1 <input checked="" type="radio"/> Enable <input type="radio"/> Disable 802.1d Spanning Tree <input type="radio"/> Enable <input checked="" type="radio"/> Disable Control Port <input checked="" type="radio"/> Enable <input type="radio"/> Disable IAPP <input type="text" value="Disable"/>
ETH0 VLAN Tag Setup ETH0 <input checked="" type="radio"/> Enable <input type="radio"/> Disable VLAN TAG <input type="checkbox"/> 1-4096	

- **VLAN Mode** : Administrator can select Enable or disable for the VLAN Network.

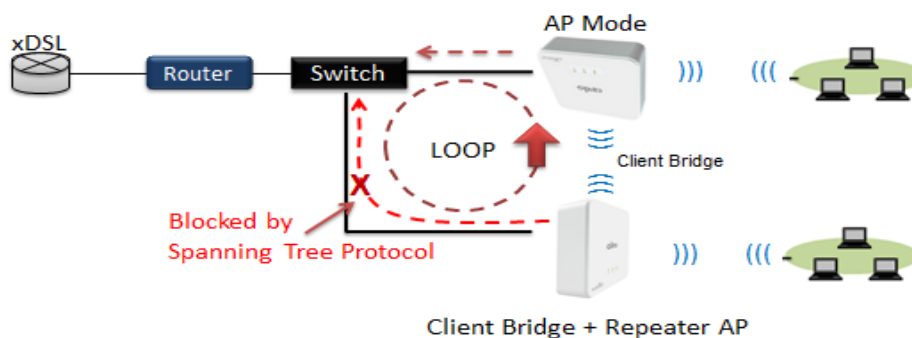


The VLAN list at least one must is enable.

- **IP Mode** : Administrator can select enable or disable function for VLAN IP.
- **IP Address/ NetMask** : Administrator can set IP address and netmask for the VLAN.

Management

- **Access Point 0** : Administrator can Enable or Disable 2.4G Radio.
- **Access Point 1** : Administrator can Enable or Disable 2.4G Radio.
- **802.1d Spanning Tree** : The spanning tree network protocol provides a loop free topology for a bridged LAN between LAN interface and 8 WDS interfaces from wds0 to wds7. The Spanning Tree Protocol, which is also referred to as STP, is defined in the IEEE Standard 802.1d

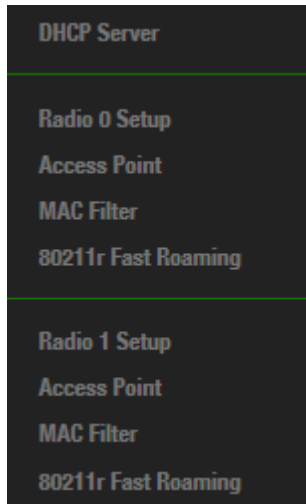


- **Control Port** : Administrator can select one of the VLAN as managed AP.
- **IAPP** : Administrator can select radio 2.4G or 5G for IAPP roaming. *(the IAPP condition must use WPA2-PSK Wi-Fi security and AES algorithm)*

7.2.2 Network Pull-down menu

Administrator can set DHCP Server and 2.4/5G security for the access point and set 802.11r fast roaming.

Please click **Network** pull-down button.



DHCP Server

Administrator can select enable / disable the function

DHCP Setup

Start IP	<input type="text"/>
End IP	<input type="text"/>
Netmask	<input type="text" value="255.255.255.0"/>
Gateway	<input type="text"/>
DNS1 IP	<input type="text"/>
DNS2 IP	<input type="text"/>
WINS IP	<input type="text"/>
Domain	<input type="text"/>
Lease Time	<input type="text" value="86400"/>

- **Start IP** : Set Start IP for DHCP Service.
- **End IP** : Set End IP for DHCP Service.
- **Netmask**: Set IP Netmask, the default is **255.255.255.0**
- **Gateway**: Set Gateway IP for DHCP Service.
- **DNS(1-2) IP** : Set DNS IP for DHCP Service.

- **WINS IP** : Enter IP address of the Windows Internet Name Service (WINS) server; this is optional.
- **Domain** : Enter the domain name for this network.
- **Lease Time** : The IP addresses given out by the DHCP server will only be valid for the duration specified by the lease time. Increasing the time ensure client operation without interruptions, but could introduce potential conflicts. Lowering the lease time will avoid potential address conflicts, but might cause more interruptions to the client while it will acquire new IP addresses from the DHCP server. Default is **86400** seconds

DHCP Client List

Administrator can view IP address used status of client users on each DHCP Server.

DHCP Client List				
#	IP Address	MAC Address	Expired	Action
-	-	-	-	-

Static Lease IP Setup

Administrator can set be delivered fixed IP address to the users.

Static Lease IP Setup	
Comment	<input type="text"/>
IP Address	<input type="text"/>
MAC Address	<input type="text"/> <input type="button" value="Add"/>

- **Comment** : Enter rule description.
- **IP Address** : Enter access point IP.
- **MAC Address** : Enter Client MAC Address of PC network.

Radio 0/1 Access Point

Administrator can Enable or Disable radio 0/1 (2.4/5G) Wi-Fi, if enable radio 0/1 (2.4/5G) administrator can set SSID and security for the 2.4/5G access point.

Security	
Access Point	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
ESSID	<input type="text" value="2.4G_0_0"/>
SSID Visibility	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Client Isolation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Connection Limit	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
User Limit	<input type="text" value="64"/>
Authentication	<input type="text" value="Open System"/>

- **Access Point:** Administrator can Enable or Disable the radio 0 (2.4G).
- **ESSID:** Administrator can set Wi-Fi SSID name for the 2.4G.
- **SSID Visibility:** Administrator can select Enable or Disable the Visibility.
- **Client Isolation:** Enable or Disable the client isolation function.
- **Connection Limit:** Administrator can select Enable or Disable WiFi connection Limit.
- **User Limit:** If select enable of the connection Limit function, administrator can set users connection limit.
- **Authentication:** Select the desired security type from the drop-down list; the options are WPA-PSK, WPA2-PSK, WPA/WPA2-Enterprise and WEP 802.1X.

Authentication	<input type="text" value="Open System"/> <ul style="list-style-type: none"> Open System WPA/WPA2 Personal WPA/WPA2 Enterprise 802.1x
-----------------------	--

- **Open System:** Data is not unencrypted during transmission when this option is selected.
- **WPA/WPA2 Personal:** WPA/WPA2 is short for W-Fi Protected Access-Pre-Shared Key. WPA/WPA2 uses the same encryption way with WPA, and the only difference between them is that WPA/WPA2 recreates a simple shared key, instead of using the user's certification.

- ✓ **WPA Mode:** Administrator can select security for Auto or only WPA or only WPA2.
- ✓ **Cipher Type:** Administrator can select use AES or TKIP with WPA / WPA2 encryption method.

AES is short for “**Advanced Encryption Standard**”, The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plaintext into the final output of ciphertext. Each round consists of several processing steps, including one that depends on the encryption key. A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key.

TKIP is short for “**Temporal Key Integrity Protocol**”, TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven’t been tampered with.

- ✓ **Group Key Update Interval:** The time interval is for re-keying GTK (broadcast/multicast encryption keys) in seconds. Enter the time-length required; the default time is 600 seconds.
- ✓ **Pass Phrase:** Enter the ESSID pass phrase.
- ✓ **WPS:** Administrator can used WPS function to link WiFi client. If enabled, administrator can click the WPS Push Button.
- **802.1X security:** When 802.1x Authentication is enabled, please refer to the following Dynamic WEP and RADIUS settings to complete the configuration.

RADIUS Server Settings

Key Size **64 Bits** **128 Bits**

Radius Server

Radius Port

Radius Secret

- ✓ **Key Size:** Check on the respected button to enable either 64bits or 128bits key length. The system will automatically generate WEP keys for encryption.
- ✓ **Radius Server:** Enter the IP address of the Authentication RADIUS server.
- ✓ **Radius Port:** The port number used by Authentication RADIUS server. Use the default 1812 or enter port number specified.
- ✓ **Radius Secret:** The secret key for system to communicate with Authentication RADIUS server. Support 1 to 64 characters.

Click “**Save**” button to save your changes. Then click **Reboot** button to activate your changes.

MAC Filter

Administrator can set allow or reject Wi-Fi users connection access point.

MAC Rules

Rule	
Disable	<input type="button" value="Save"/>

- **Disable** : Disable MAC Filter function.
- **Only Deny List MAC** : Administrator can add wireless users MAC address in MAC list. The access point will deny connection in MAC address list.
- **Only Allow List MAC** : Administrator can add wireless users MAC address in MAC list. The access point will Allow connection in MAC address list.

Click “**Save**” button to save your changes. Then click **Reboot** button to activate your changes.

802.11r/802.11k Fast Roaming

The dual band Access Point supports 802.11r/802.11k function for 2.4G and 5G radio. 802.11r, which is the IEEE standard for fast roaming, introduces a new concept of roaming where the initial handshake with the new AP is done even before the client roams to the target AP.

Fast Roaming Settings	
Mobility Domain	<input type="text" value="a1b2"/>
R0 Key Lifetime	<input type="text" value="10000"/>
Reassoc deadline	<input type="text" value="1000"/>
R0/NAS Identifier	<input type="text" value="ap.example.com"/>
R1 Identifier	<input type="text" value="000102030405"/>
R1 Push	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

- **Mobility Domain:** MDID is used to indicate a group of APs (within an ESS, i.e., sharing the same SSID) between which a STA can use Fast BSS Transition. Please enter 2-octet identifier as a hex string.
- **R0 Key Lifetime:** Default lifetime of the PMK-RO in minutes, the default is 10000, administrator can setting 1~65535.
- **Reassoc deadline:** Reassociation deadline in time units (TUs / 1.024 ms; range 1000~65535). The default is 1000.
- **R0/NAS Identifier:** PMK-R0 Key Holder identifier. When using IEEE 802.11r, nas_identifier must be set and must be between 1 and 48 octets long.
- **R1 Identifier:** PMK-R1 Key Holder identifier 6-octet identifier as a hex string.
- **R1 Push:** Administrator can select Enable or disable. If enable the function will automatically sent the R1 Key.

R0 Key Address:

To enable roaming between multiple AP devices, AP1 must key in the MAC Address of AP2, and AP2 must key in the MAC Address of AP1. The NAS Identifier and 128-bit Key should be identical in both AP settings. This will enable device roaming between the two Access Points.

R0 Key holders

MAC Address

NAS Identifier

128-bit Key Add

- **MAC Address:** Administrators must enter the MAC Address of other AP
- **NAS Identifier:** Enter 1~48 octets of network domain name.
- **128-bit Key:** Enter Shared Key of 128 bit.

R0 Key Holder List:

After setting "R0 Key holders" function the information will appear in list.

R0 Key Holder List				
#	MAC Address	NAS Identifier	128-bit Key	Action
-	-	-	-	-

R1 Key Holder List:

Enter a unified set of R1 Key Holder identification certification.

R1 Key Holders

MAC Address

R1 Identifier

128-bit Key Add

- **MAC Address:** Enter the main roaming device MAC address
- **R1 Identifier:** Enter Shared identifier.
- **128-bit Key:** Enter Shared Key of 128 bit.

R1 Key Holder List:

After setting "R1 Key holders" function the information will appear in list.

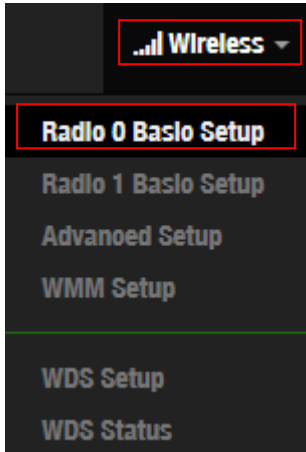
R1 Key Holder List				
#	MAC Address	NAS Identifier	128-bit Key	Action
-	-	-	-	-

Click "**Save**" button to save your changes. Then click **Reboot** button to activate your changes.

7.3 Wireless Basic Setup

This section includes the main base station setup procedures for 2.4G / 5G Wifi functions · Wi-Fi Advanced setup · WMM · WDS and WDS Status

7.3.1 Radio 0 Basic Setup (2.4G)

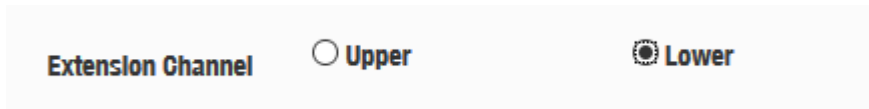


General setup

A screenshot of the 'General Setup' configuration page. The page has a light gray header with a hamburger menu icon and the text 'General Setup'. Below the header, there are several configuration fields: 'MAC Address' with the value '8c:4d:ea:04:d0:69'; 'Country' with a dropdown menu showing 'Taiwan'; 'Band Mode' with a dropdown menu showing '802.11n'; 'Auto Channel' with radio buttons for 'Enable' and 'Disable' (selected); 'Channel' with a dropdown menu showing '5 (2432 Mhz)'; 'Tx Power' with a dropdown menu showing 'Level 9'; 'Slot Time' with a text input '13' and a green 'Distance' button; and 'ACK Timeout' with a text input '93'.

- **MAC Address:** Display 2.4G WiFi MAC address.
- **Country:** Administrator can select country: US or EU or Taiwan.
- **Band Mode:** Administrator can select 802.11b/g/n for the 2.4G Band.
- **Auto Channel:** Administrator can Enable or Disable the function. If disabled, the WiFi channel will be fixed to the manually selected channel.

- **Channel:** Administrator can select 1 to 11 CH. The Channel settings can be changed in “HT Physical Mode” →” **Extension Channel**” can select **Upper** or **Lower** channels.



- **Tx Power:** Administrator can control the WiFi Tx output power. The power Max. Level 9.
- **Slot Time :** Slot time is in the range of **9~1489** and set in unit of **microsecond**. The default value is **9** microsecond.

Slot time is the amount of time a device waits after a collision before retransmitting a packet. Reducing the slot time decreases the overall back-off, which increases throughput. Back-off, which is a multiple of the slot time, is the random length of time a station waits before sending a packet on the LAN. For a sender and receiver own right of the channel the shorter slot time help manage shorter wait time to re-transmit from collision because of hidden wireless clients or other causes. When collision sources can be removed sooner and other senders attempting to send are listening the channel(CSMA/CA) the owner of the channel should continue ownership and finish their transmission and release the channel. Then, following ownership of the channel will be sooner for the new pair due to shorter slot time. However, when long duration of existing collision sources and shorter slot time exist the owners might experience subsequent collisions. When adjustment to longer slot time can't improve performance then RTS/CTS could supplement and help improve performance.

- **ACK Timeout :** ACK timeout is in the range of **1~372** and set in unit of **microsecond**. The default value is **64** microsecond.

All data transmission in 802.11b/g request an “Acknowledgement” (ACK) send by receiving radio. The transmitter will resend the original packet if correspondent ACK failed to arrive within specific time interval, also refer to as “ACK Timeout”.

ACK Timeout is adjustable due to the fact that distance between two radio links may vary in different deployment. ACK Timeout makes significant influence in performance of long distance radio link. If ACK Timeout is set too short, transmitter will start to “Resend” packet before ACK is received, and throughput become low due to excessively high re-transmission.

ACK Timeout is best determined by distance between the radios, data rate of average environment. The Timeout value is calculated based on round-trip time of packet with a little tolerance, So, if experiencing re-transmissions or poor performance the ACK Timeout could be made longer to accommodate.



Slot Time and ACK Timeout settings are for long distance links. It is important to tweak settings to achieve the optimal result based on requirement.

HT Physical Mode

HT Physical Mode

TX/RX Stream

Channel BandWidth 20 20/40

Extension Channel Upper Lower

MCS

Short GI Enable Disable

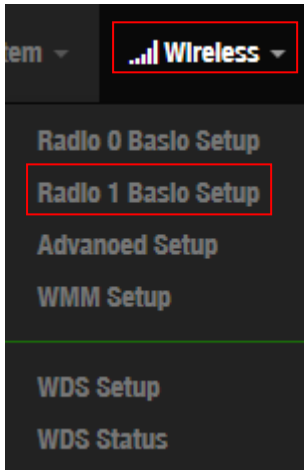
Aggregation Enable Disable

Aggregation Frames

Aggregation Size

- **TX/RX Stream:** The OW-400-A2 utilizes 2 antenna and supports 2TX/2RX streams. Administrator can select 1 or 2 TX/RX. The default is 2TX/2RX.
- **Channel Bandwidth:** The "20/40" MHz option is usually best. The other option is available for special circumstances.
- **Extension Channel:** Sets channel select to Upper or Lower. The Upper supports 1 to 7 range CH and Lower supports 5 to 11 range CH.
- **MCS:** This parameter represents transmission rate. By default (Auto) the fastest possible transmission rate will be selected. You have the option of selecting the speed if necessary.
- **Short GI:** Short Guard Interval is "Enabled" by default to increase throughput. However, it can also increase error rate in some installations, due to increased sensitivity to radio-frequency reflections. Select the option that works best for your installation.
- **Aggregation:** By default, it's "Enabled". Select "Disable" to deactivate Aggregation. A part of the 802.11n standard (or draft-standard), it allows sending multiple frames per single access to the medium by combining frames together into one larger frame. It creates the larger frame by combining smaller frames with the same physical source and destination end points and traffic class (i.e. QoS) into one large frame with a common MAC header.
- **Aggregation Frames :** The Aggregation Frames is in the range of 2~64, default is 32. It determines the number of frames combined on the new larger frame.
- **Aggregation Size :** The Aggregation Size is in the range of 1024~65535, default is 50000. It determines the size (in Bytes) of the larger frame.

7.3.2 Radio 1 Basic Setup (5G)



General Setup

General Setup	
MAC Address	8c:4d:ea:04:d0:6a
Country	Taiwan
Band Mode	802.11ac
Auto Channel	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Channel	100 (5500 Mhz)
Tx Power	Level 9
Slot Time	9 Distance
ACK Timeout	30

- **MAC Address:** Display 2.4G WiFi MAC address.
- **Country:** Administrator can select country: US or EU or Taiwan.
- **Band Mode:** Administrator can select 5G Band for 802.11a/n or 802.11ac. The default is 802.11ac
- **Auto Channel:** Administrator can Enable or Disable the function. If select disabled function the WiFi channel can be manually fixed.
- **Channel:** Supports US and EU country 5G Channel standards.
- **Tx Power:** Administrator can control the WiFi Tx output power. The power Max. Level 9.

- **Slot Time** : Slot time is in the range of **9~1489** and set in unit of **microsecond**. The default value is **9** microsecond.

Slot time is the amount of time a device waits after a collision before retransmitting a packet. Reducing the slot time decreases the overall back-off, which increases throughput. Back-off, which is a multiple of the slot time, is the random length of time a station waits before sending a packet on the LAN. For a sender and receiver own right of the channel the shorter slot time help manage shorter wait time to re-transmit from collision because of hidden wireless clients or other causes. When collision sources can be removed sooner and other senders attempting to send are listening the channel(CSMA/CA) the owner of the channel should continue ownership and finish their transmission and release the channel. Then, following ownership of the channel will be sooner for the new pair due to shorter slot time. However, when long duration of existing collision sources and shorter slot time exist the owners might experience subsequent collisions. When adjustment to longer slot time can't improve performance then RTS/CTS could supplement and help improve performance.

- **ACK Timeout** : ACK timeout is in the range of **1~372** and set in unit of **microsecond**. The default value is **64** microsecond.

All data transmission in 802.11b/g request an "Acknowledgement" (ACK) send by receiving radio. The transmitter will resend the original packet if correspondent ACK failed to arrive within specific time interval, also refer to as "ACK Timeout".

ACK Timeout is adjustable due to the fact that distance between two radio links may vary in different deployment. ACK Timeout makes significant influence in performance of long distance radio link. If ACK Timeout is set too short, transmitter will start to "Resend" packet before ACK is received, and throughput become low due to excessively high re-transmission.

ACK Timeout is best determined by distance between the radios, data rate of average environment. The Timeout value is calculated based on round-trip time of packet with a little tolerance, So, if experiencing re-transmissions or poor performance the ACK Timeout could be made longer to accommodate.



Slot Time and ACK Timeout settings are for long distance links. It is important to tweak settings to achieve the optimal result based on requirement.

HT Physical Mode

HT Physical Mode

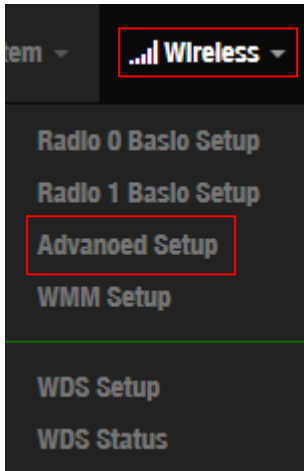
TX/RX Stream	<input type="text" value="2T2R"/>
Channel BandWidth	<input type="text" value="80"/>
Short GI	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Aggregation	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Aggregation Frames	<input type="text" value="32"/>
Aggregation Size	<input type="text" value="50000"/>

- **TX/RX Stream:** The OW-400-A2 utilizes 2 antennas and supports 2TX/2RX streams. Administrator can select 1 or 2 TX/RX. The default is 2TX/2RX.
- **Channel Bandwidth:** The "20/40 and 802.11ac 80" MHz option is usually the best. The other option is available for special circumstances.
- **Short GI:** Short Guard Interval is "Enabled" by default to increase throughput. However, it can also increase error rate in some installations, due to increased sensitivity to radio-frequency reflections. Select the option that works best for your installation.
- **Aggregation:** By default, it's "Enable". Select "Disable" to deactivate Aggregation. A part of the 802.11n standard (or draft-standard). It allows sending multiple frames per single access to the medium by combining frames together into one larger frame. It creates the larger frame by combining smaller frames with the same physical source and destination end points and traffic class (i.e. QoS) into one large frame with a common MAC header.
- **Aggregation Frames :** The Aggregation Frames is in the range of 2~64, default is 32. It determines the number of frames combined on the new larger frame.
- **Aggregation Size :** The Aggregation Size is in the range of 1024~65535, default is 50000. It determines the size (in Bytes) of the larger frame.

Click "Save" button to save your set function. Then click "Reboot" button to activate your changes.

7.3.3 Advanced Setup

The administrator can change the Slot Time, ACK Timeout, RTS threshold and fragmentation threshold settings for the system. Please click on **Wireless -> Advanced Setup** and follow the below setting.



A screenshot of the 'Advanced Setup' configuration page. The page contains the following settings:

- Beacon Interval:** 100
- DTIM Interval:** 1
- Fragment Threshold:** 2346
- RTS Threshold:** 2346
- Short Preamble:** Enable Disable
- IGMP Snooping:** Enable Disable
- Greenfield:** Enable Disable
- Band Steering:** 10

- **Beacon Interval:** Beacon Interval is in the range of **40~3500** and set in unit of *millisecond*. The default value is **100** msec.
Access Point (AP) in IEEE 802.11 will send out a special approximated 50-byte frame, called "Beacon". Beacon is broadcast to all the stations, provides the basic information of AP such as SSID, channel, encryption keys, signal strength, time stamp, support data rate. All the radio stations received beacon recognizes the existence of such AP, and may proceed next actions if the information from AP matches the requirement. Beacon is sent on a periodic basis, the time interval can be adjusted.

By increasing the beacon interval, you can reduce the number of beacons and associated overhead, but that will likely delay the association and roaming process because stations scanning for available access points may miss the beacons. You can decrease the beacon interval, which increases the rate of beacons. This will make the association and roaming process very responsive; however, the network will incur additional overhead and throughput will go down.

- **DTIM Interval** : The DTIM interval is in the range of **1~255**. The default is **1**.
DTIM is defined as *Delivery Traffic Indication Message*. It is used to notify the wireless stations, which support power saving mode, when to wake up to receive multicast frame. DTIM is necessary and critical in wireless environment as a mechanism to fulfill power-saving synchronization.
A DTIM interval is a count of the number of beacon frames that must occur before the access point sends the buffered multicast frames. For instance, if DTIM Interval is set to 3, then the Wi-Fi clients will expect to receive a multicast frame after receiving three Beacon frame. The higher DTIM interval will help power saving and possibly decrease wireless throughput in multicast applications.
- **Fragmentation Threshold**: Fragmentation Threshold is one more parameter which is given in all stations and Access points. Fine tuning Fragmentation Threshold parameter can result in good throughput but not using it properly can results in low throughput. In simple words it does the same thing which MTU do in Ethernet. Both are different parameters but the work done is same, it fragments the data packets.
Fragmentation threshold will be used when we have more data packet size to be transmitted and we have less fragment threshold value. Lets say from Ethernet we have to send 1400 byte packet but the fragmentation threshold is set as 400. In this case when the packet is to be transmitted on air it will fragment the packet in to 4 small packet 400+400+400+200 and send on air. This includes MAC header+ frame body and CRC so 400 byte will be in total including headers. This helps in increasing the throughput. The default is 2346.
- **RTS Threshold**: TRTS Threshold is in the range of **1~2347** byte. The default is **2347** byte. The main purpose of enabling RTS by changing RTS threshold is to reduce possible collisions due to hidden wireless clients. RTS in AP will be enabled automatically if the packet size is larger than the Threshold value. By default, RTS is disabled in a normal environment supports non-jumbo frames.
- **Short Preamble**: By default, this function is "**Enabled**". **Disabling** will automatically use the Long 128-bit Preamble Synchronization field. The preamble is used to signal "here is a train of data coming" to the receiver. The short preamble provides 72-bit Synchronization field to improve WLAN transmission efficiency with less overhead.

- **IGMP Snooping:** The process of listening to Internet Group Management Protocol (IGMP) network traffic. The feature allows a network switch to listen in on the IGMP conversation between hosts and routers. By listening to these conversations the switch maintains a map of which links need which IP multicast streams. Multicasts may be filtered from the links which do not need them and thus controls which ports receive specific multicast traffic.
- **Greenfield:** In wireless WLAN technology, greenfield mode is a feature of major components of the 802.11n specification. The greenfield mode feature is designed to improve efficiency by eliminating support for 802.11b/g devices in an all draft-n network. In greenfield mode the network can be set to ignore all earlier standards.
- **Band Steering: Dual band operation with Band Steering** detects clients capable of 5 GHz operation and steers them to that frequency which leaves the more crowded 2.4 GHz band available for legacy clients. This helps improve end user experience by reducing channel utilization, especially in high density environments. The default RSSI Limit :10

7.3.4 WMM Setup

This affects traffic flowing from the access point to the client station.

Configuring QoS options consists of setting parameters on existing queues for different types of wireless traffic. You can configure different minimum and maximum wait times for the transmission of packets in each queue based on the requirements of the media being sent.

Queues automatically provide minimum transmission delay for Voice, Video, multimedia, and mission critical applications, and rely on best-effort parameters for traditional IP data.

As an Example, time-sensitive Voice & Video, and multimedia are given effectively higher priority for transmission (lower wait times for channel access), while other applications and traditional IP data which are less time-sensitive but often more data-intensive are expected to tolerate longer wait times.

Please click on **Wireless -> WMM Setup**



WMM Setup

WMM **Enable** **Disable**

➤ **WMM:** Administrator can select Enable or Disable the services of WMM.

WMM Parameters of Access Point

AC Type	CWmin	CWmax	AIFS	TxOp Limit	No ACK Policy bit
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"/>
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="1"/>	<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="1"/>	<input type="text" value="1504"/>	<input type="checkbox"/>

WMM Parameters of Station

AC Type	CWmin	CWmax	AIFS	TxOp Limit	ACM bit
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 :**

Queue	Data Transmitted AP to Clients	Priority	Description
AC_BK	Background	Low	High throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).
AC_BE	Best Effort	Medium	Medium throughput and delay. Most traditional IP data is sent to this queue.
AC_VI	Video	High	Minimum delay. Time-sensitive video data is automatically sent to this queue.
AC_VO	Voice	High	Time-sensitive data like VoIP and streaming media are automatically sent to this queue.

- ✓ **CWmin** :
Minimum Contention Window. This parameter is input to the algorithm that determines the initial random backoff wait time ("window") for retry of a transmission. The value specified here in the Minimum Contention Window is the upper limit (in milliseconds) of a range from which the initial random backoff wait time is determined.
- ✓ **CWmax** : Maximum Contention Window. The value specified here in the Maximum Contention Window is the upper limit (in milliseconds) for the doubling of the random backoff value. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached. Once the Maximum Contention Window size is reached, retries will continue until a maximum number of retries allowed is reached. Valid values for the "cwmax" are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024. The value for "cwmax" must be higher than the value for "cwmin". ◦
- ✓ **AIFS** : The Arbitration Inter-Frame Spacing Number specifies a wait time (in milliseconds) for data frames ◦
- ✓ **TxOP Limit** : Transmission Opportunity is an interval of time when a WME AP has the right to initiate transmissions onto the wireless medium (WM). This value specifies (in milliseconds) the Transmission Opportunity (TXOP) for AP; that is, the interval of time when the WMM AP has the right to initiate transmissions on the wireless network. ◦
- ✓ **ACM bit** : Admission Control Mandatory, ACM only takes effect on AC_VI and AC_VO. When you do not click Checkbox, it means that the ACM is controlled by the connecting AP. If you click Checkbox, it means that the Client is in charge ◦
- ✓ **No ACK policy bit** : Acknowledgment Policy, WMM defines two ACK policies: **Normal ACK** and **No ACK**. Click "**Checkbox**" indicates "**No ACK**"
When the no acknowledgement (No ACK) policy is used, the recipient does not acknowledge received packets during wireless packet exchange. This policy is suitable in the environment where communication quality is fine and interference is weak.
While the No ACK policy helps improve transmission efficiency, it can cause increased packet loss when communication quality deteriorates. This is because when this policy is used, a sender does not retransmit packets that have not been received by the recipient. When the Normal ACK policy is used, the recipient acknowledges each received unicast packet. ◦

8. Advanced Setup By WISP & Router Mode

8.1 DMZ

DMZ is commonly work with the NAT functionality as an alternative of Virtual Server(Port Forwarding) while wanting all ports of DMZ host visible to Internet users. Virtual Server rules have precedence over the DMZ rule. In order to use a range of ports available to access to different internal hosts Virtual Server rules are needed.

The screenshot shows the 'DMZ Setup' configuration page. The 'Mode' dropdown menu is open, displaying the following options: 'Disable', 'Automatic Assignment', and 'Static Assignment'. The 'Disable' option is currently selected.

- **Automatic Assignment:** Enter Internal IP address of DMZ host and only one DMZ host is supported.

The screenshot shows the 'Automatic Assignment Setup' configuration page. It contains a single text input field labeled 'Internal IP Address'.

- **Internal IP Address:** Enter Virtual IP for service device.
- **Static Assignment:** Enter external and internal IP address of DMZ host. The function only external IP to Internal IP address

The screenshot shows the 'Static Assignment Setup' configuration page. It contains two text input fields: 'External IP Address' and 'Internal IP Address'. A green 'Add' button is located to the right of the 'Internal IP Address' field.

- **External IP Address:** Enter external IP address
- **Internal IP Address:** Enter Virtual IP for service device.

8.2 IP Filter

Can allow or deny filter ingress or egress packets from specific source and/or to destination IP address on wired (LAN) or Wireless (WAN) ports. Filter rules could be used to filter unicast or multicast packets on different protocols as shown in the IP Filter Setup. Important to note that IP filter rules has precedence over Virtual server rules.

#	Active	Comment	Protocol	In/Out	Action	Source Address/Mask	Source Port	Destination Address/Mask	Destination Port	Edit
1	InActive	-	ALL	In	Deny	-	-	-	-	Edit
2	InActive	-	ALL	In	Deny	-	-	-	-	Edit
3	InActive	-	ALL	In	Deny	-	-	-	-	Edit
4	InActive	-	ALL	In	Deny	-	-	-	-	Edit

Please click **Edit** button to setting IP filter.

IP Filter Rules

Active Enable Disable

Comment

IP Filter Rules

Policy Deny Pass

In/Out In Out

Protocol

IP Filter Rules

Source Address/Mask

Source Port

Destination Address/Mask

Destination Port

Listen Enable Disable

Interface WAN LAN

Schedule

- **Active:** Administrator can select Enable or Disable the service.
- **Comment:** Enter the description of IP filter rule.
- **Policy:** Administrator can select the IP flow rule of Deny or Pass.
- **In/ Out:** Administrator can select the IP flow rule of In/out bound.
- **Protocol:** Set used service Port of **TCP**, **UDP** or **ICMP**.
- **Source Address/Mask :** Enter desired source IP address and netmask. i.e. 192.168.2.10/32 or 192.168.2.10/255.255.255.0
- **Source Port :** Enter a port or a range of ports as **start:end**. i.e. port 20:80
- **Destination Address/Mask :** Enter desired destination IP address and netmask. i.e. 192.168.1.10/32 or 192.168.2.10/255.255.255.0
- **Destination Port :** Enter a port or a range of ports as **start:end**. i.e. port 20:80
- **Listen:** Select Enable radial button to match TCP packets only with the SYN flag.
- **Interface :** The interface that a filter rule applies.
- **Schedule :** Can choose to use rule by **"Time Policy"**.



All packets are allowed by default. Deny rules could be added to the filter list to filter out unwanted packets and leave remaining allowed.

When you create rules in the IP Filter List, the prior rules maintain higher priority. To allow limited access from a subnet to a destination network manager needs to create allow rules first and followed by deny rules. So, if you just want one IP address to access the system via telnet from your subnet, not others, the Example 1 demonstrates it, not rules in the Example 2.

Example 1 :

Create a higher priority rule to allow IP address 192.168.2.2 Telnet access from LAN port first, and deny Telnet access from remaining IP addresses in the same subnet.

Rule	Source		Destination		In/Out	Protocol	Listen	Action	Side
	IP/Mask	Port	IP/Mask	Port					
1	192.168.2.2/32		192.168.2.254/32	22	In	TCP	n	Pass	LAN
2	192.168.2.0/24		192.168.2.254/32	22	In	TCP	n	Deny	LAN

Example 2 :

All Telnet access to the system from the IP addresses of subnet 192.168.2.x works with the rule 1 of Example 2. The rule 2 won't make any difference.

Rule	Source		Destination		In/Out	Protocol	Listen	Action	Side
	IP/Mask	Port	IP/Mask	Port					
1	192.168.2.0/24		192.168.2.254/32	22	In	TCP	n	Pass	LAN
2	192.168.2.2/32		192.168.2.254/32	22	In	TCP	n	Deny	LAN

Click "**Save**" button to add IP filter rule. Total of **20** rules maximum allowed in the IP Filter List. All rules can be edited or removed from the List. Click **Reboot** button to activate your changes.

8.3 MAC Filter

Allows creating MAC filter rules to allow or deny unicast or multicast packets from limited number of MAC addresses. Important and must note. That MAC filter rules have precedence over IP Filter rules.

MAC Filter Rules

Mode Disable

Disable
 Deny
 Allow

MAC Filter List

#	Active	Comment	MAC Address	Policy
1	<input type="checkbox"/>	<input style="width: 95%;" type="text"/>	<input style="width: 95%;" type="text"/>	Always Run ▼
2	<input type="checkbox"/>	<input style="width: 95%;" type="text"/>	<input style="width: 95%;" type="text"/>	Always Run ▼
3	<input type="checkbox"/>	<input style="width: 95%;" type="text"/>	<input style="width: 95%;" type="text"/>	Always Run ▼
4	<input type="checkbox"/>	<input style="width: 95%;" type="text"/>	<input style="width: 95%;" type="text"/>	Always Run ▼
5	<input type="checkbox"/>	<input style="width: 95%;" type="text"/>	<input style="width: 95%;" type="text"/>	Always Run ▼

- **Mode:** Administrator can select Deny or Allow.
 - **Deny:** The MAC Filter List will be **denied** to access (LAN to WAN). Others will be allowed.
 - **Allow:** The MAC Filter List will be **allowed** to access (LAN to WAN). Others will be denied.
- **Comment:** Enter the description of MAC filter rule.
- **MAC Address :** Enter MAC address (e.g. aa:bb:cc:00:00:0a) and click “**Add**” button, then the MAC address should display in the MAC Filter List.
- **Policy:** Administrator can select to used rule by “**Time Policy**”.

8.4 Virtual Server

The “**Virtual Server**” can also referred to as “Port Forward” as well and used interchangeably. Resources in the network can be exposed to the Internet users in a controlled manner including on-line gaming, video conferencing or others via Virtual Server setup. Don’t repeat ports’ usage to avoid confusion.

Suppose you want to assign ports 21-25 to one FTP, Telnet and SMTP server (A in the example), and port 80 to another (B in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

Virtual Server List							
#	Active	Comment	Protocol	Public Port	Private IP Address	Private Port	Edit
1	InActive	-	TCP	-	-	-	Edit
2	InActive	-	TCP	-	-	-	Edit
3	InActive	-	TCP	-	-	-	Edit
4	InActive	-	TCP	-	-	-	Edit
5	InActive	-	TCP	-	-	-	Edit
6	InActive	-	TCP	-	-	-	Edit
7	InActive	-	TCP	-	-	-	Edit

Please click **Edit** button to setting Virtual Server rules.

Virtual Server Rules	
Active	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Comment	<input type="text"/>
Protocol	<input checked="" type="radio"/> TCP <input type="radio"/> UDP
Public Port	<input type="text" value="(min:1, max:65535 or Range xxxxx:xxxxx)"/>
Private IP Address	<input type="text"/>
Private Port	<input type="text" value="(min:1, max:65535 or Range xxxxx:xxxxx)"/>
Schedule	<input type="text" value="Always"/> <input type="button" value="v"/>

- **Active:** Administrator can select Virtual server rule to Enable or disable.
- **Comment:** Enter the description of virtual server rule.
- **Protocol:** Administrator can select service protocol of TCP or UDP.
- **Public Port:** Enter service port No. for public.
- **Private IP Address:** Enter corresponding IP address for internal.
- **Private Port:** Enter internal service port No. for private.
- **Schedule :** Administrator can select to used rule of “Time Policy”

8.5 Access Control

The Access Control function administrator can to block or allow specific kinds of TCP/UDP/ICMP protocol, such as Internet access, designated services, and websites. The Access Control function can set 20 profiles.

Please click on **Advance -> Access Control** and follow the below setting.

#	Active	Comment	Protocol	Edit
1	InActive	-	ANY	Edit
2	InActive	-	ANY	Edit
3	InActive	-	ANY	Edit
4	InActive	-	ANY	Edit
5	InActive	-	ANY	Edit

- **#** : Display access control list.
- **Active** : Display Active or InActive for the access control rule.
- **Comment**: Display information for the rule.
- **Protocol** : Display information for the protocol.
- **Edit** : Administrator can click the button to set Access Control rule.

Access Control Rules

Active Enable Disable

Comment:

Protocol:

Schedule:

MAC Address Setup

MAC Address:

MAC Address List

#	MAC Address	Action	#	MAC Address	Action
-	-	-	-	-	-

IP Address Setup

Local IP Address: -

Local Port:

Destination IP Address: -

Destination Port:

Access control rules :

- **Active** : Administrator can select Enable or Disable for the Access control rule.
- **Comment** : Administrator can enter comment for the role.
- **Protocol** : Administrator can to select management protocol by TCP/UDP/ICMP/Content Filter/Application and Domain Filter.

Protocol ANY ▼

- ANY
- TCP
- UDP
- ICMP
- Content Filter
- Application
- Domain Filter

- ✓ **ANY** : Select "Any" is all deny Protocol, administrator can filter local IP / IP range go to destination IP / IP range and use protocol.
- ✓ **TCP** : Deny TCP Protocol, Administrator can set TCP protocol and assign IP / IP range.
- ✓ **UDP** : Deny UDP Protocol, Administrator can set UDP protocol and assign IP / IP range.
- ✓ **ICMP** : Deny ICMP Protocol, Administrator can assign IP / IP range.
- ✓ **Content Filter** : Administrator can set web Keyword to filter.
- ✓ **Application** : System built-in multiple applications data, Administrator can select application data to filter.
- ✓ **Domain** : Administrator can set domain name to filter.
 - **Schedule** : The rule can apply Time Policy.

8.6 Time Policy

Policy List			
#	Comment	Mode	Edit
1	Policy 1	On Schedule	Edit
2	Policy 2	On Schedule	Edit
3	Policy 3	On Schedule	Edit
4	Policy 4	On Schedule	Edit
5	Policy 5	On Schedule	Edit
6	Policy 6	On Schedule	Edit

Please click **Edit** button to setting Time Policy rules.

Time Policy Rules

Comment

Mode On Schedule Out Of Schedule

Policy List Create New Policy

#	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Time	Action
-	-	-	-	-	-	-	-	-	-

- **Comment:** Enter the description of Time Policy rule.
- **Mode:** Administrator can select On schedule or Out of schedule to execution the rules.

Create New Policy button:

Administrator can set time for week / start time and end time.

Time Policy Rules

Day of Week

Sun Mon Tue

Wed Thu Fri

Sat

Start Time

End Time

Click "Save" button to add schedule to policy. There are 10 schedule maximum allowed in the each time policy. All schedules can be edited or removed in the each time policy. Click **Reboot** button to activate your changes.

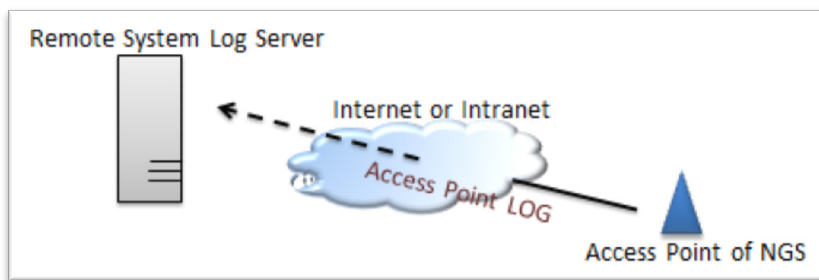
9. System Management

9.1 Configure system management

Administrators can specify geographical location of the system via instructions in this page and modify system login password and select use system login protocol by 80, 443, 23, 22 Port. The management page adds LED control on/off and system auto reboot function.

System Language Language: English	Login Methods HTTP: <input checked="" type="checkbox"/> 80 Port HTTPS: <input type="checkbox"/> 443 Port Telnet: <input checked="" type="checkbox"/> 23 Port SSH: <input type="checkbox"/> 22 Port Host Key Footprint: ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQgIXQjW Generate Key
System Information System Name: CW-400NAC-E1 Description: eXtreme Power AC1200 2.4GHz / 5GHz 2x2 Ceiling / Wall PoE Access P Location:	System Log Setup Remote Server: <input type="checkbox"/> Port: 514 Port
Root Password New Root Password: <input type="text"/> Check Root Password: <input type="text"/>	Auto Reboot Type: Disable
LED Control LED OFF <input type="radio"/> Enable <input type="radio"/> Disable <input checked="" type="radio"/>	

- **System Language:** Administrator can select system language for English and Traditional Chinese
- **System Information:** Administrator can set the system name / Description and Location.
- **Root Password:** Administrator can change system login password.
- **LED Control :** When system working the moment, device LED will flashes. Administrator can select close the LED flashes in the function.
- **Login Methods:** Administrator can set system login protocol of the http/https/telnet and ssh.
- **System Log Setup:** Administrator can be backup system log or authentication log to remote server. Please enter IP address and port of remote syslog server.



- **Auto Reboot:** The functions can Auto-reboot the system by Date/time management.
 - **Daily :** Setting time to system reboot.

Auto Reboot

Type: Daily

Hour: 08

Minute: 08

- **Weekly** : Setting frequency (ex. Weekly) and time of system reboot

Auto Reboot

Type: Week

Weekly: Sunday

Hour: 08

Minute: 08

- **Monthly** : Setting Every month, fixed date and time to system reboot

Auto Reboot

Type: Month

Monthly: 01

Hour: 08

Minute: 08

Click “**Save**” button to save your changes. And click “**Reboot**” button to activate your changes

9.2 Configure Time Server

Administrator can select manual or via a NTP server to modify system time for the right local time. If select update the system time for manual, when administrator reboot system the system time will reply default.

If select update the system time for the NTP Server, system must set gateway and DNS server, the system can be connected internet.

System Time

Local Time

Mode NTP Server Manual

User Setup

Date(Y/M/D)

Time(H:M:S) (GMT+8:00)

- **Mode:** Administrator can select NTP Server or Manual.
 - **NTP Server:** System can auto update the system time. Administrator needs setting as NTP Server.

NTP Server

Default NTP Server

NTP Server

Time Zone

Daylight Saving Time Enable Disable

- ✓ **Default NTP Server:** Administrator can select NTP Server.
- ✓ **NTP Server:** Administrator can setting as NTP Server.
- ✓ **Time Zone:** Administrator can select a desired time zone from the drop-down list.
- ✓ **Daylight saving Time:** Enable or disable Daylight saving.
- **Manual:** Administrator need to set the system time.

User Setup

Date(Y/M/D)

Time(H:M:S) (GMT+8:00)

Click “**Save**” button to save your changes. And click “**Reboot**” button to activate your changes

9.3 Control PoE Bridge

This device supports Cerio's smart PoE Bridge function. Enabling PoE Bridge function will allow this device to provide PoE power to subsequent standard PD devices such as Cerio APs or as IP Cameras.

- **PoE Bridge:** Administrator can select Enable or Disable.

Click **“Save”** button to save your changes. And click **“Reboot”** button to activate your changes

9.4 Configure SNMP Setup

SNMP is an application-layer protocol that provides a message format for communication between SNMP managers and agents. By enabling SNMP function, the administrator can obtain the system information remotely.

Please click on **System -> SNMP** and follow the below setting.

SNMP v2c function

- **Active:** Administrator can select Enable or Disable the service.
- **RO Community:** Set a community string to authorize read-only access.
- **RW Community:** Set a community string to authorize read/write access.

SNMP v3 function

- **Active:** Administrator can select Enable or Disable the service.

- **RO username:** Set a community string to authorize read-only access.
- **Ro password:** Set a password to authorize read-only access.
- **RW username:** Set a community string to authorize read/write access.
- **RW password:** Set a password to authorize read/write access.

SNMP Trap

Events such as cold start interface up & down, and association & disassociation will report to an assigned server.



SNMP Trap

Active Enable **Disable**

Community

IP 1

IP 2

IP 3

IP 4

- **Active:** Administrator can select Enable or Disable the service.
- **Community:** Set a community string required by the remote host computer that will receive trap messages or notices send by the system.
- **IP(1~4) :** Enter the IP addresses of the remote hosts to receive trap messages.

Click "**Save**" button to save your changes. And click "**Reboot**" button to activate your changes

10. Utilities

10.1 Profile Setting

This Functions purpose is to backup current configuration, restore prior configuration or reset back to factory default configurations.

Please click on **Utilities -> Profile Setting** and follow the below setting

Profile Setting

In this page, you can save your current configuration, restore a previously saved configuration, or restore all of the settings in the system to the factory (default) settings.

Save Settings To PC

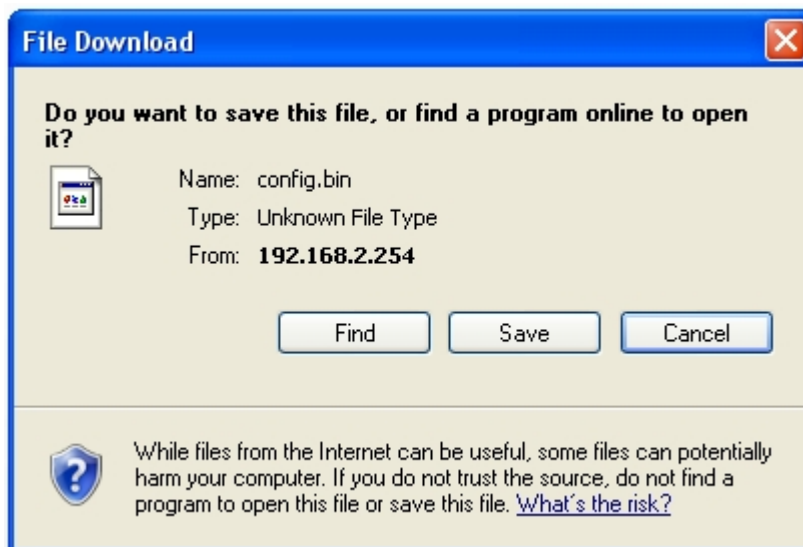
Load Settings From PC 未選擇檔案。

Reset To Factory Default

Update SSL Certification From Local Hard Drive

Certificate File 未選擇檔案。

- **Save Settings to PC** : Click **Save** button to save the current configuration to a local disk.



- **Load Settings from PC**: Click **Browse** button to locate a configuration file to restore, and then click **Upload** button to upload.
- **Reset To Factory Default**: Click **Default** button to reset back to the factory default settings and expect **Successful** loading message. Then, click **Reboot** button to activate.

10.2 System Upgrade

Firmware is the main software image that system needs to respond to requests and to manage real time operations. Firmware upgrades are sometimes required to include new features or bugs fix. It takes around 2 minutes to upgrade due to complexity of firmware. To upgrade system firmware, click Browse button to locate the new firmware, and then click Upgrade button to upgrade.

Firmware Information:

Display the system firmware information.

Firmware Information

Sometimes it may be necessary to reboot the system if it begins working improperly. Rebooting the system will not delete any of your configuration settings. Click reboot button to reboot the system.

Firmware Version	Pme-CPE-AC5 V0.0.22
Firmware Date	2015/07/17 15:18:58

Upgrade Via Local PC and TFTP Server:

The upgrade firmware will support via local PC and TFTP Server and HTTP URL to upgrade system.

Upgrade Via Local PC

Select File

- **Select File:** Administrator can select Firmware file in Local PC.

Upgrade Via TFTP Server

TFTP Server IP

File Name

- **TFTP Server:** Enter IP address for TFTP Server.
- **File Name:** Enter file name.



1. To prevent data loss during firmware upgrade, please back up current settings before proceeding
2. Do not interrupt during firmware upgrade including power on/off as this may damage system.

10.3 Network Utility

The administrator can diagnose network connectivity via the PING or TRACEROUTE utility. Please click on **Utilities** -> **Network Utility** and follow the below setting.

The screenshot shows two side-by-side utility panels. The left panel is titled 'Ping Utility' and contains a text input field for 'IP/Domain', a numeric input field for 'Times' set to '5', and a green 'Ping' button. The right panel is titled 'Traceroute' and contains a text input field for 'Destination Host', a green 'Start' button, a numeric input field for 'Max. Hops' set to '6', and a green 'Stop' button. Both panels have a large grey rectangular area below the input fields for displaying results.

- **Ping** : This utility will help ping other devices on the network to verify connectivity. Ping utility, using ICMP packets, detects connectivity and latency between two network nodes. As result of that, packet loss and latency time are available in the **Result** field while running the PING test.
 - **IP/Domain** : Enter desired domain name, i.e. www.google.com, or IP address of the destination, and click ping button to proceed. The ping result will be shown in the Result field.
 - **Count** : By default, it's 5 and the range is from 1 to 50. It indicates number of connectivity test.
- **Traceroute** : Allows tracing the hops from the OW-400-A2 device to a selected outgoing IP address. It should be used for the finding the route taken by ICMP packets across the network to the destination host. The test is started using the **Start** button, click **Stop** button to stopped test.
 - **Destination Host** : Specifies the Destination Host for the finding the route taken by ICMP packets across the network.
 - **MAX Hop** : Specifies the maximum number of hops(max time-to-live value) trace route will probe.

10.4 Reboot

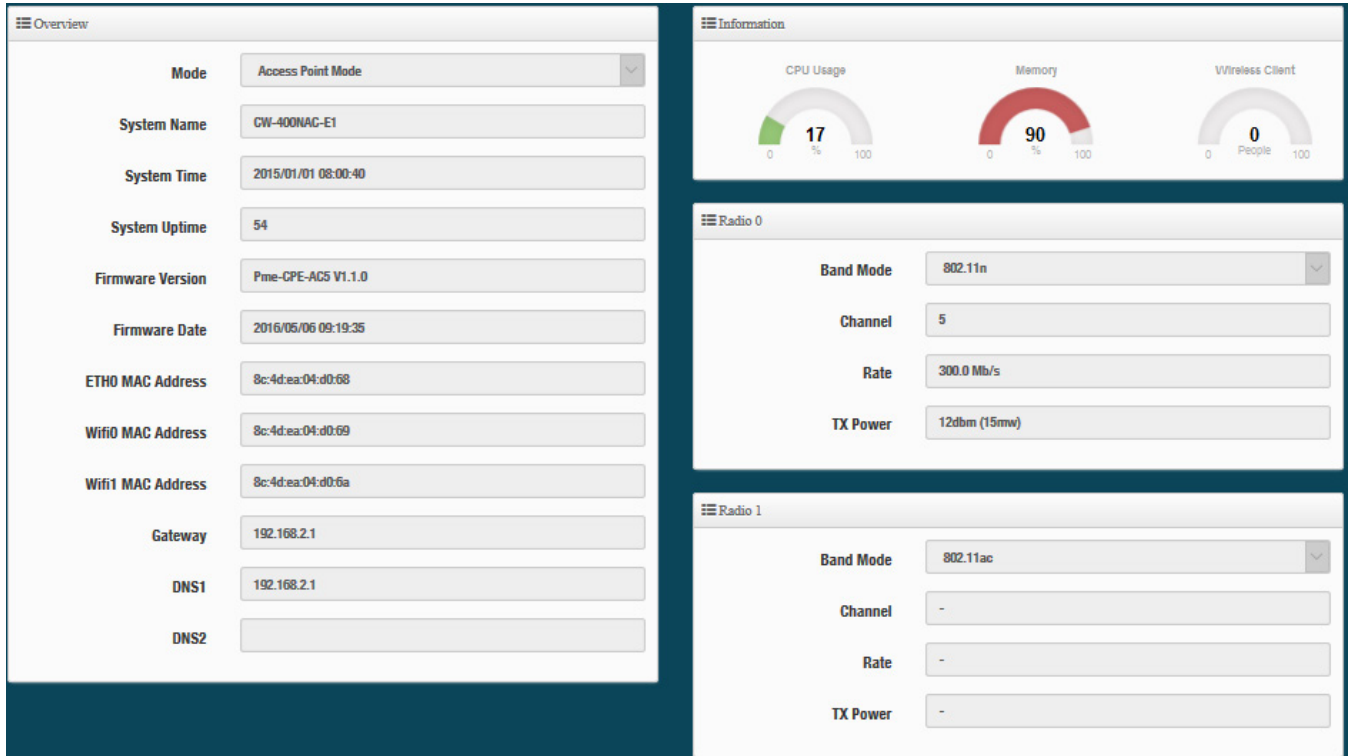
This function allows user to restart system with existing or most current settings when changes are made. Click **Reboot** button to proceed and take around three minutes to complete.

The screenshot shows a 'Reboot' utility window. At the top left, there is a menu icon and the text 'Reboot'. Below this is a light blue informational box containing the text: 'Sometimes it may be necessary to reboot the system if it begins working improperly. Rebooting the system will not delete any of your configuration settings. Click reboot button to reboot the system.' At the bottom center of the window is a large green button labeled 'Reboot'.

11. Status

11.1 Overview

Detailed information on System, Network can be reviewed via this page.



The screenshot displays the 'Overview' page with the following sections:

- Mode:** Access Point Mode
- System Name:** CW-400NAC-E1
- System Time:** 2015/01/01 08:00:40
- System Uptime:** 54
- Firmware Version:** Pme-CPE-AC5 V1.1.0
- Firmware Date:** 2016/05/06 09:19:35
- ETH0 MAC Address:** 8c:4d:ea:04:d0:68
- Wifi0 MAC Address:** 8c:4d:ea:04:d0:69
- Wifi1 MAC Address:** 8c:4d:ea:04:d0:6a
- Gateway:** 192.168.2.1
- DNS1:** 192.168.2.1
- DNS2:** (empty)

Information Section:

- CPU Usage:** 17%
- Memory:** 90%
- Wireless Client:** 0 People

Radio 0 Section:

- Band Mode:** 802.11n
- Channel:** 5
- Rate:** 300.0 Mb/s
- TX Power:** 12dbm (15mw)

Radio 1 Section:

- Band Mode:** 802.11ac
- Channel:** -
- Rate:** -
- TX Power:** -

11.2 Wireless Client

The page can be display Wireless user information link to access point. Administrator can monitor MAC address / rate and RSSI for the wireless users.

VLAN 0

Radio	MAC Address	Rate(RX/TX)	RSSI
-	-	-	-

11.3 Online Users by Captive Portal

The status can display online users by Captive Portal. Administrator can monitor user's login / logout time and account type for the authentication account.

Authentication Zone Online Users							
VLAN#	Authentication	User Count	Download Packets	Upload Packets	Download Bytes	Upload Bytes	Action
0	ON	1	76842	17677	98.41MB	2.09MB	Detail
1	OFF	0	0	0	0B	0B	-

- **VALN#** : Display VLAN number.
- **Authentication** : Display Captive Portal authentication function is on/off in the VLANs.
- **Users Count** : Display the VLAN network connected user's amount.
- **Download Packets** : Display total download packets amount information of the VLAN.
- **Upload Packets** : Display total upload packets amount information of the VLAN.
- **Download Bytes** : Display total download flow information of the VLAN.
- **Upload Bytes** : Display total upload flow information of the VLAN.
- **Action** : Administrator can click "**Detail**" button to monitor all user's use network information.

Authentication Zone 0 Online Users										
#	Auth Type	Username	IP Address	MAC Address	Login Time	Download Packets	Upload Packets	Download Bytes	Upload Bytes	Action
1	Local	test	192.168.2.21	08:00:27:00:00:02:A	2016/01/01 00:23:41	76842	17677	98.41MB	2.09MB	Logout

- **Auth Type** : Display authentication login type.
- **User name** : Display authentication account.
- **IP Address** : Display IP address for user.
- **MAC Address** : Display MAC address for user.
- **Download Packets** : Display total download packets amount information by user.
- **Upload Packets** : Display total upload packets amount information by user.
- **Download Bytes** : Display total download flow information by user.
- **Upload Bytes** : Display total upload flow information by user.

11.4 Authentication Log by Captive Portal

The authentication log can monitor account login/logout type and account use time.

#	Date/Time	Status	User	IP Address	MAC Address	Download Packets	Upload Packets	Download Bytes	Upload Bytes
1	2016/01/01 00:01:53	LOGIN	test	192.168.2.22	██████████7	0	0	0B	0B
2	2016/01/01 00:26:12	LOGOUT	test	192.168.2.22	██████████7	1028	890	761.08KB	107.40KB
3	2016/01/01 00:26:12	LOGIN	test	192.168.2.23	██████████9:50	0	0	0B	0B

11.5 System Log

The system log displays system events when system is up and running. Also, it becomes very useful as a troubleshooting tool when issues are experienced in system.

System Log Refresh Clear			
Time	Facility	Severity	Message
-	-	-	-

- **Time** : The date and time when the event occurred.
- **Facility** : It helps users to identify source of events such “System” or “User”
- **Severity** : Severity level that a specific event is associated such as “info”, “error”, “warning”, etc.
- **Message** : Description of the event.
- Click “**Refresh**” button to renew the log
- Click “**Clear**” button to clear all the record.

Appendix A. WEB GUI Valid Characters

Table B WEB GUI Valid Characters

Block	Field	Valid Characters
LAN	IP Address	IP Format; 1-254
	IP Netmask	128.0.0.0 ~ 255.255.255.252
	IP Gateway	IP Format; 1-254
	Primary DNS	IP Format; 1-254
	Secondary DNS	IP Format; 1-254
	Hostname	Length : 32 0-9, A-Z, a-z ~!@#% ^ * () _ + - { } : < > ? [] / ; ` , . =
WAN	Manual MAC Address	12 HEX chars
	IP Address	IP Format; 1-254
	IP Netmask	128.0.0.0 ~ 255.255.255.252
	IP Gateway	IP Format; 1-254
	Hostname	Length : 32 0-9, A-Z, a-z ~!@#% ^ * () _ + - { } : < > ? [] / ; ` , . =
	User name	Length : 32 0-9, A-Z, a-z
	Password	~!@#% ^ * () _ + - { } : < > ? [] / ; ` , . =
	MTU	576 ~ 1492 for PPPoE; 1400 ~ 1460 for PPTP
	Idle Time	0 ~ 60 minutes
	Primary DNS	IP Format; 1-254
	Secondary DNS	IP Format; 1-254
DHCP Server	Start IP	IP Format; 1-254
	End IP	IP Format; 1-254
	DNS1 IP	IP Format; 1-254
	DNS2 IP	IP Format; 1-254
	WINS IP	IP Format; 1-254
	Domain	Length : 32 0-9, A-Z, a-z ~!@#% ^ * () _ + - { } : < > ? [] / ; ` , . =
	Lease Time	600 ~ 99999999

Table B WEB GUI Valid Characters (continued)

Block	Field	Valid Characters
Management	System Name/ Location	Length : 32 0-9, A-Z, a-z Space ~!@#\$%^*()_+ -{ :<>?[]/;'` , . =
	Description	32 chars
	Password	Length : 4 ~ 30 0-9, A-Z, a-z ~!@#\$%^*()_+ -{ :<>?[]/;'` , . =
	HTTP/ HTTPS Port	1 ~ 65535
	Telnet/ SSH Port	1 ~ 65535
SNMP	RO/RW community	Length : 32 0-9, A-Z, a-z ~!@#\$%^*()_+ -{ :<>?[];'` , . =
	RO/RW user	Length : 31 0-9, A-Z, a-z ~!@#\$%^*()_+ -{ :<>?[];'` , . =
	RO/RW password	Length : 8 ~ 32 0-9, A-Z, a-z ~!@#\$%^*()_+ -{ :<>?[];'` , . =
	Community	Length : 32 0-9, A-Z, a-z ~!@#\$%^*()_+ -{ :<>?[];'` , . =
	IP	IP Format; 1-254
General Setup	Tx Power	1-100 %
Wireless Profile	Profile Name	32 chars
	ESSID	Length : 31 Space 0-9, A-Z, a-z ~!@#\$%^*()_+ -{ :<>?[]/;'` , . =
	WEP Key	10, 26 HEX chars or 5, 13 ASCII chars
	Pre-shared Key	8 ~ 63 ASCII chars; 64 HEX chars
Advanced Setup	Beacon Interval	20 ~ 1024
	Date Beacon Rate	1 ~ 255
	Fragment Threshold	256 ~ 2346
	RTS Threshold	1 ~ 2347

Table B WEB GUI Valid Characters (continued)

Block	Field	Valid Characters
Virtual AP Setup	ESSID	Length : 31 Space 0-9, A-Z, a-z ~!@#\$%^*()_+ -{ :<>?[]/;'` , . =
	Maximum Clients	1 ~ 32
	VLAN ID	1 ~ 4094
	WEP Key	10, 26 HEX chars or 5, 13 ASCII chars
	Group Key Update Period	>=60 seconds
	PMK Cache Period	> 0 minute
	Pre-Shared Key	8 ~ 63 ASCII chars; 64 HEX chars
	Radius Server IP	IP Format; 1-254
	Radius Port	1 ~ 65535
	Shared Secret	8 ~ 64 characters
	Session Timeout	>= 60 seconds; 0 is disable
WDS Setup	WEP Key	10, 26 HEX chars or 5, 13 ASCII chars
	TKIP Key	8 ~ 63 ASCII chars; 64 HEX chars
	AES Key	8 ~ 63 ASCII chars; 64 HEX chars
	Peer's MAC Address	12 HEX chars
	Description	32 chars
IP Filter	Source Address	IP Format; 1-254
	Source Mask	0 ~ 32
	Source Port	1 ~ 65535
	Destination Address	IP Format; 1-254
	Destination Mask	0 ~ 32
	Destination Port	1 ~ 65535
MAC Filter	MAC address	MAC Format; 12 HEX chars
Virtual Server	Description	32 chars
	Private IP	IP Formate; 1-254
	Private/ Public Port	1 ~ 65535
	DMZ	IP Address