USER MANUAL

CERIO
Amplify your Wireless Network

CERIO Corporation

CenOS 5.0

User Manual

for

OW-200 A1 / OW-218 A1

1. Software Configuration 6

1.1 Device appearance and RJ-45 reset function kit description 6

1.2 Setup preparation of AP 7

1.3 Login Web Page 10

1.4 Operating Mode Introduction 11

Access Point Mode 11

Client Bridge + Repeater Mode 12

WISP + Repeater AP Mode 14

CAP mode (Centralizes Access Point) 15

2. System Configuration 16

2.1 Management 16

2.2 Configure Time Server 18

2.3 SNMP 19

2.4 Configure Time Policy 21

3. Access Point mode 22

3.1 VLAN Setup 22

# Network Setup 24

# Network Pull-down menu 25

3.1.1 DHCP Server 25

3.1.2 Bandwidth Control 27

3.1.3 Radio 0 Access Point Setup 28

3.1.4 MAC Filter 30

3.1.5 802.11r Fast Roaming Setup 31

3.2 Authentication 33

3.2.1 Enable Authentication function 34

3.2.2 Set Authentication function 36

# Guest 36

# Local User 37

# OAuth2.0 37

Sample for Google OAuth2.0 setup 38

Sample for Facebook OAuth2.0 setup 41

# POP3/IMAP Server 44

# Customize Page 45

# Language 47

# Walled Garden 47

# Privilege Address 47

# Profile 48

3.3 RADIUS Server 49

3.4 RADIUS Account Setup 49

3.5 Wireless Configuration 50

3.5.1 Radio 0 Basic Setup 50

3.5.2 Advanced Setup 52

3.5.3 WMM Setup 54

3.5.4 WDS Setup 56

3.5.5 WDS Status 57

4. Client Bridge Mode 58

4.1 Configure LAN Setup 58

4.2 Configure DHCP Setup 60

4.3 Wireless General Setup 62

4.3.1 Radio 0 Basic Setup 62

4.3.2 Advanced Setup 65

4.3.3 WMM Setup 67

4.3.4 Station Setup 69

4.3.5 Repeater AP Setup 70

4.3.6 MAC Filter Setup 72

4.3.7 802.11r Fast Roaming Setup 73

5. WISP Mode 75

5.1 Configure WAN Setup 75

5.2 Configure LAN Setup 79

5.3 Configure DHCP Server 79

5.4 Wireless General Setup 81

5.4.1 Radio 0 Basic Setup 82

5.4.2 Advanced Setup 84

5.4.3 WMM Setup 86

5.4.4 Station Setup 89

5.4.5 Repeater AP Setup 90

5.4.6 MAC Filter Setup 92

5.4.7 802.11r Fast Roaming Setup 93

5.5 Advanced Setup 95

5.5.1 DMZ 95

5.5.2 IP Filter 96

5.5.3 MAC Filter 97

5.5.4 Virtual Server 98

5.5.5 Access Control 99

6. CAP Mode 101

6.1 VLAN Setup 101

6.2 AP Control 103

6.2.1 Scan Device 104

6.2.2 Batch Setup 105

6.2.3 AP Setup 107

6.2.4 Group Setup 108

6.2.5 Map Setup 108

6.2.6 Authentication Profile 110

6.2.7 Status 111

7. Utilities 111

7.1 Profile Setting 111

7.2 System Upgrade 112

7.3 Network Utility 114

7.4 Reboot 114

8. Status 115

8.1 Overview 115

8.2 Wireless Client 116

8.3 Online Users 116

8.4 Authentication Log 117

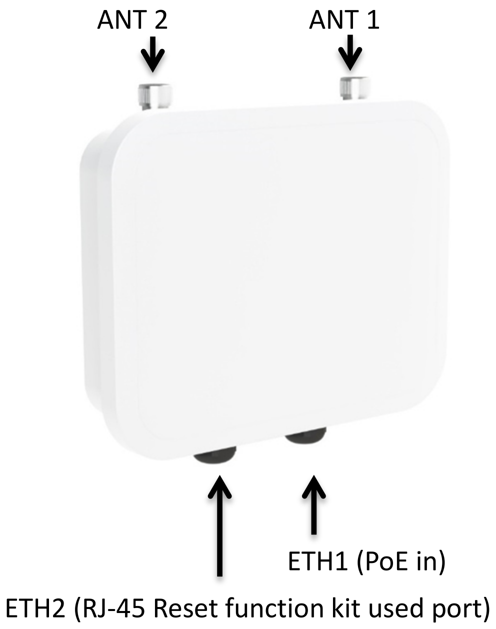
8.5 System Log 117

Appendix A. WEB GUI Valid Characters 119

1. Device and Software Configuration

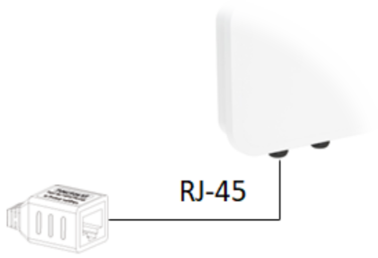
1.1 Device appearance and RJ-45 reset function kit description

Device appearance

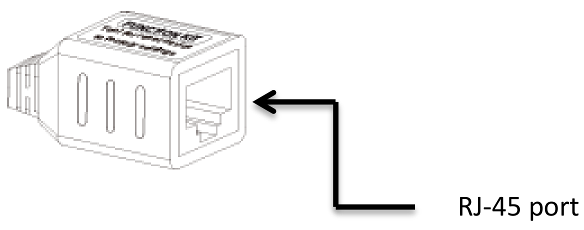


Notice

1. When radio set 1Tx/1Rx then main signal output power is the left N-type (ANT1) connect. As refer 3.5.1 Radio 0 Basic Setup.
2. The device don't add the hardware return factory value button, if software want to reset to default then must use RJ-45 reset function kit (Accessories) , under working of the device (power on state) use RJ-45 cable connection to ETH2 port and function kit, after link about 5 sec remove RJ-45 reset function kit the software will reset to default. As shown.

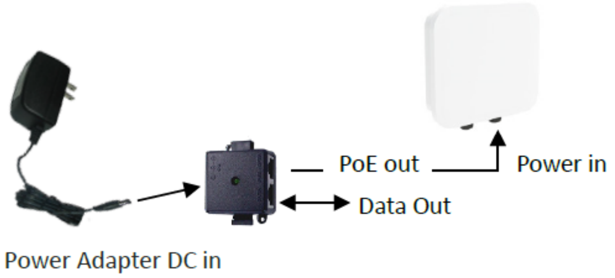


RJ-45 reset function kit



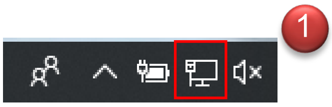
1.2 Setup preparation of AP

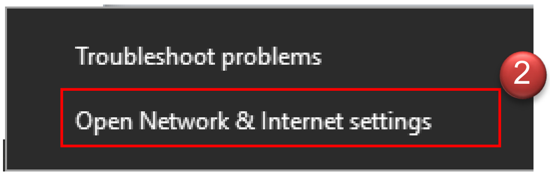
Please PC link to Device used cat5/6 Ethernet cable.



The following setup uses a Windows PC, user OS may vary

Step 1: Please click on the computer icon in the bottom right window, and click **"Open Network and Internet settings"**

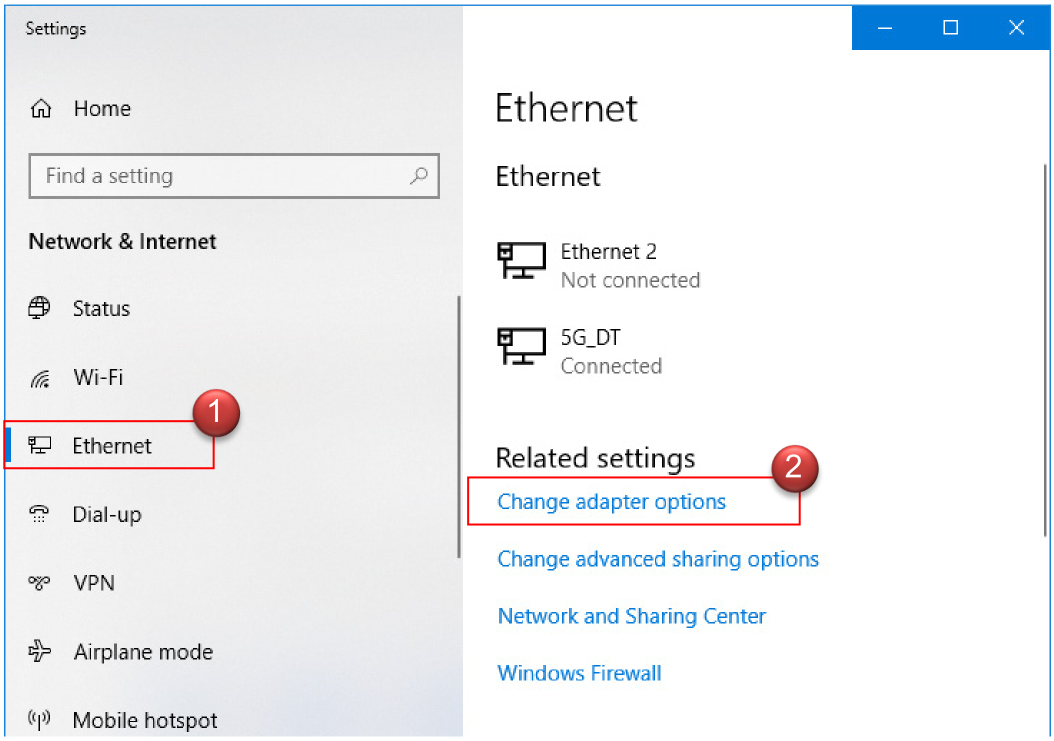




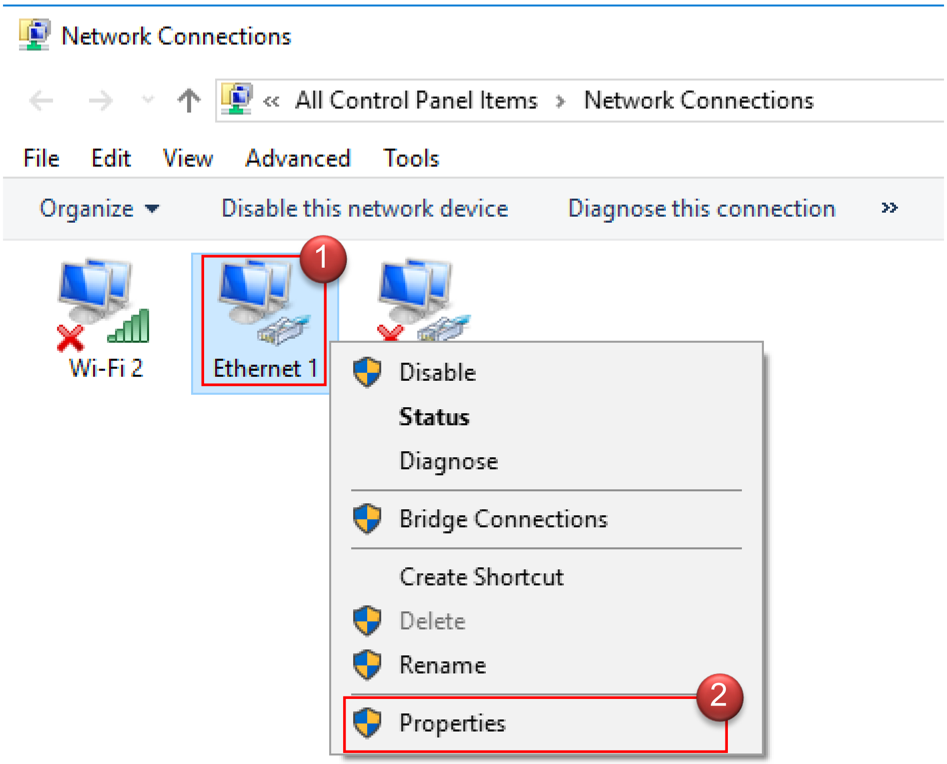
Troubleshoot problems

Open Network & Internet settings

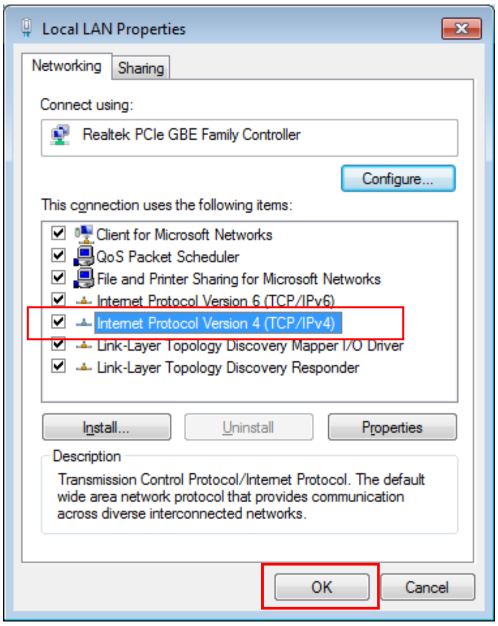
Step 2: After click left side "**Ethernet**" function, click on the right side “**Change adapter options**” again.



Step 3: In **“Change adapter options”** Page. Please find Ethernet (Local LAN) and Click the right button on the mouse and Click **“Properties”**


Network Connections
« All Control Panel Items › Network Connections
File Edit View Advanced Tools
Organize ▾ Disable this network device Diagnose this connection »
Wi-Fi 2
Ethernet 1
Disable
Status
Diagnose
Bridge Connections
Create Shortcut
Delete
Rename
Properties
1
2

Step 4: In Properties page to setting IP address, please find **"Internet Protocol Version 4 (TCP/IPv4)"** and double click or click **"OK"** button.



Local LAN Properties

Networking | Sharing

Connect using:

Realtek PCIe GBE Family Controller

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

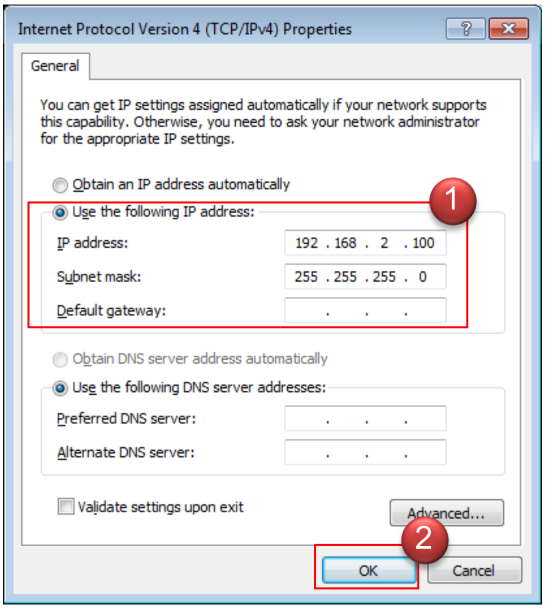
Step 5 :

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



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 2 . 100

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

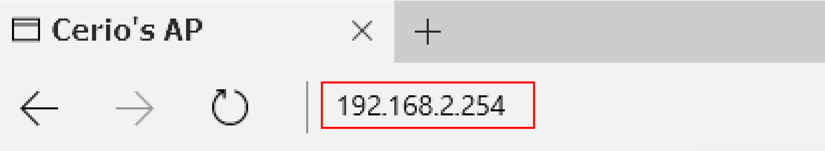
Alternate DNS server: . . .

□ Validate settings upon exit

1.3 Login Web Page

Launch Web Browser

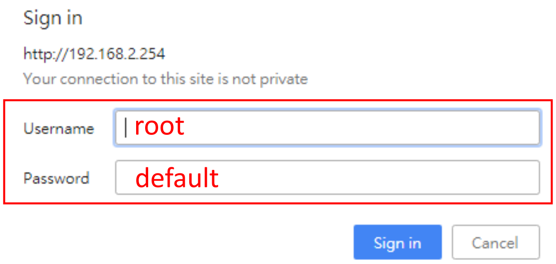
Launch as web browser to access the web management interface of system by entering the default IP Address, http://192.168.2.254, in the URL field, and then press Enter.



Cerio's AP

192.168.2.254

System Login



Sign in

http://192.168.2.254

Your connection to this site is not private

Username | root

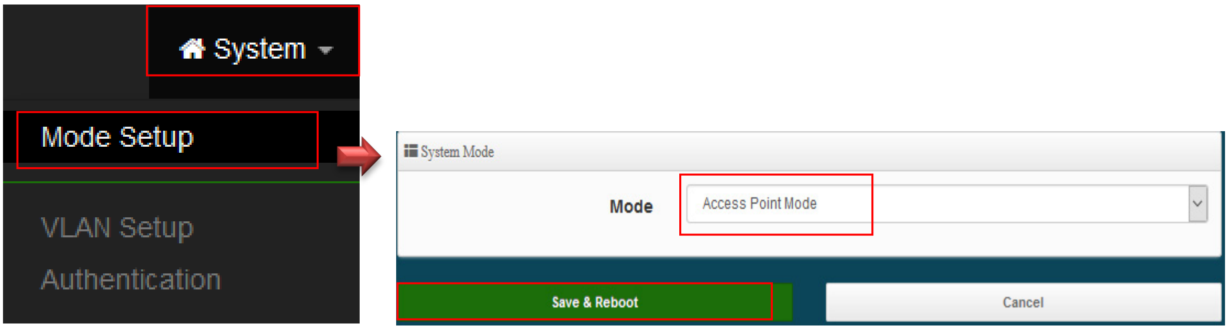
Password default

Default login Username is "**root**"and Password is "**default**"

1.4 Operating Mode Introduction

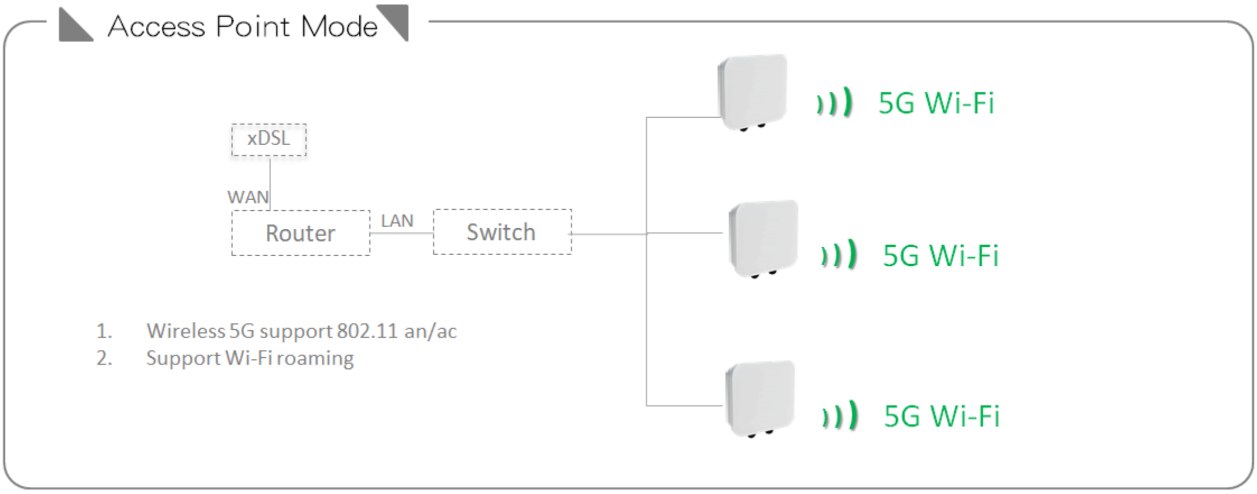
Access Point Mode

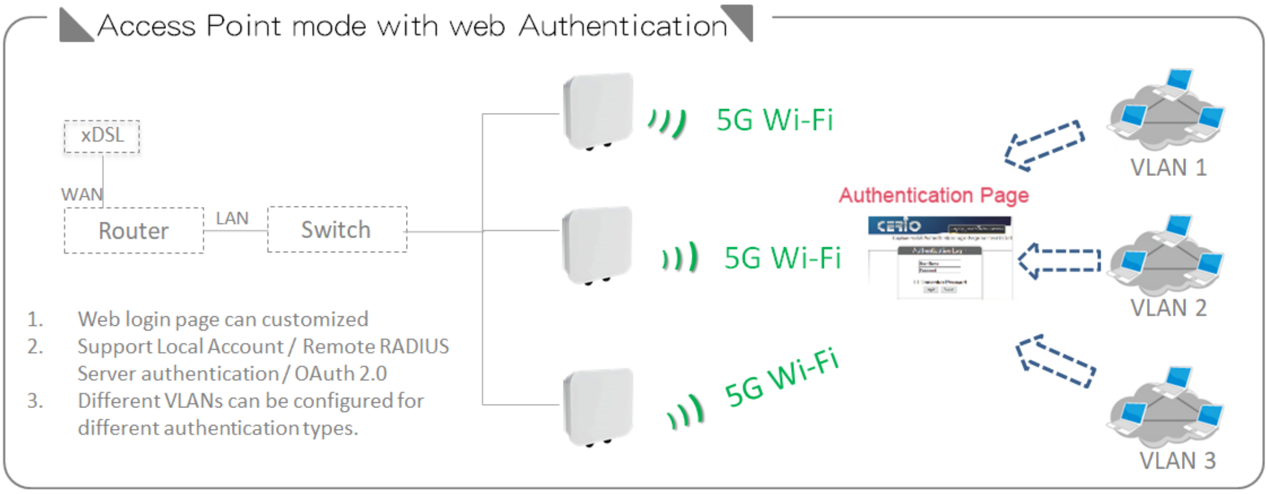
Please click on System ->Mode Setup and choose Access Point Mode



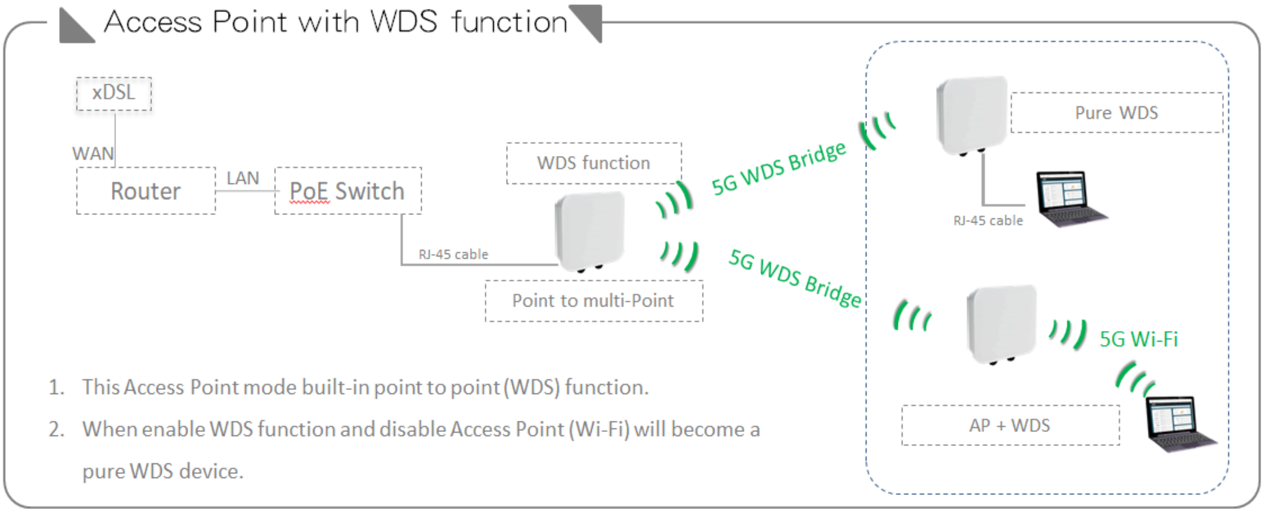
Mode: Access Point Mode

- ➢ 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.





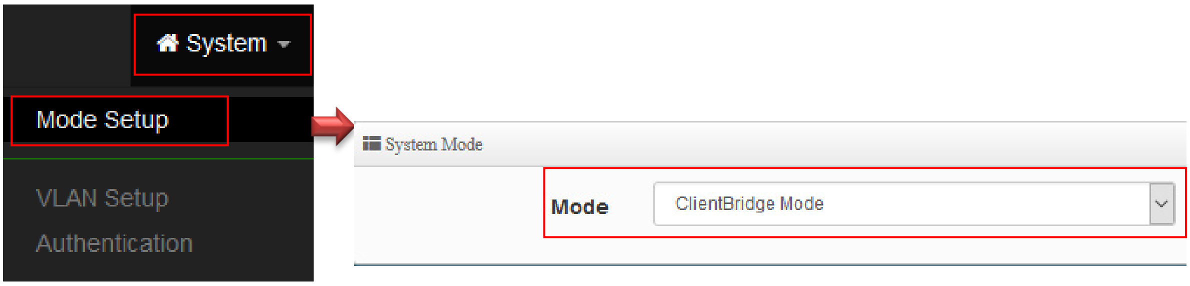
1. Web login page can customized
2. Support Local Account / Remote RADIUS Server authentication / OAuth 2.0
3. Different VLANs can be configured for different authentication types.



1. This Access Point mode built-in point to point (WDS) function.
2. When enable WDS function and disable Access Point (Wi-Fi) will become a pure WDS device.

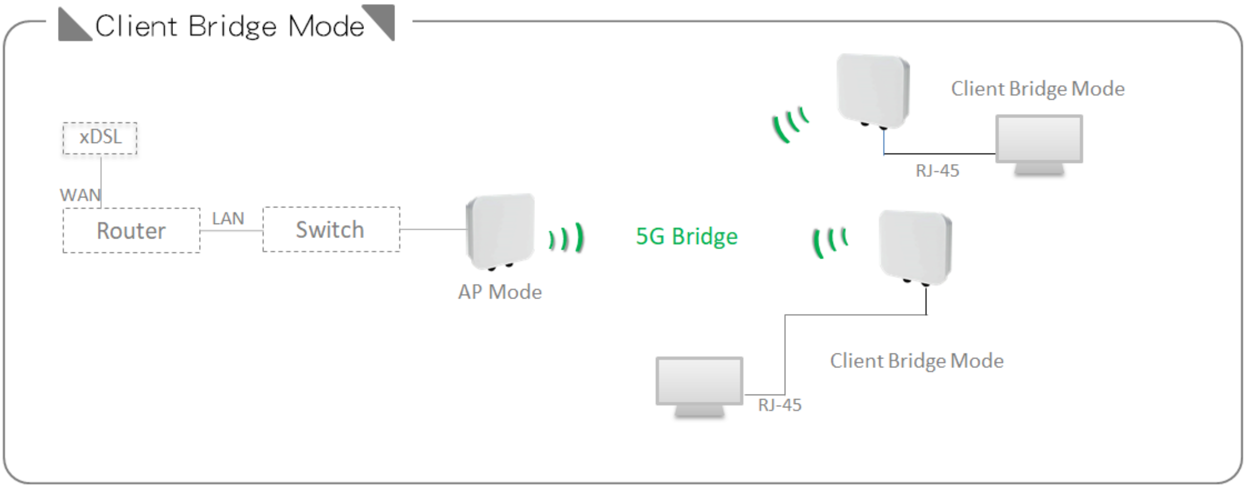
Client Bridge + Repeater Mode

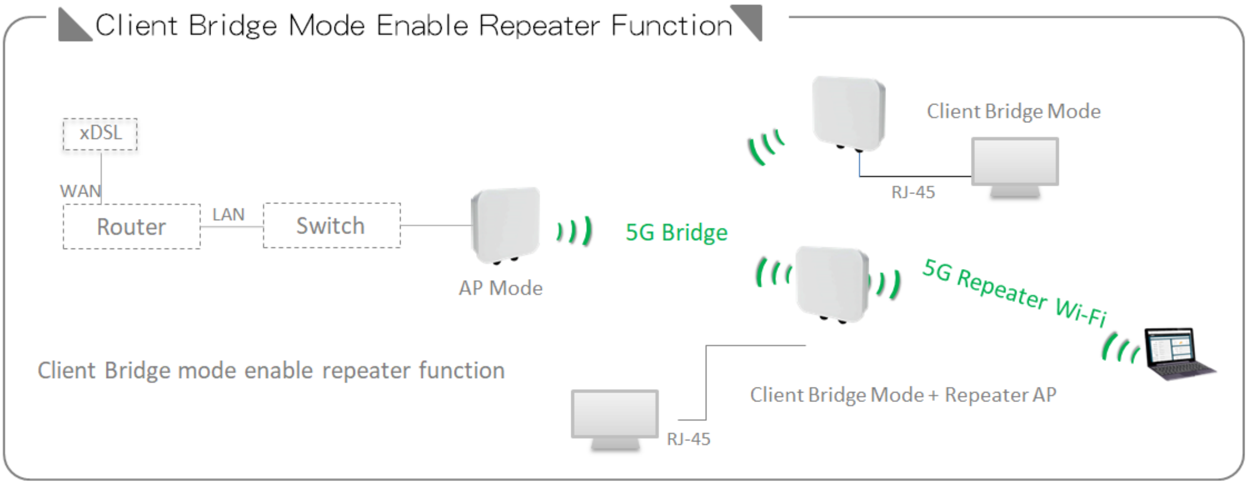
Please click on System ->Mode Setup and choose Client Bridge Mode



Mode ClientBridge Mode

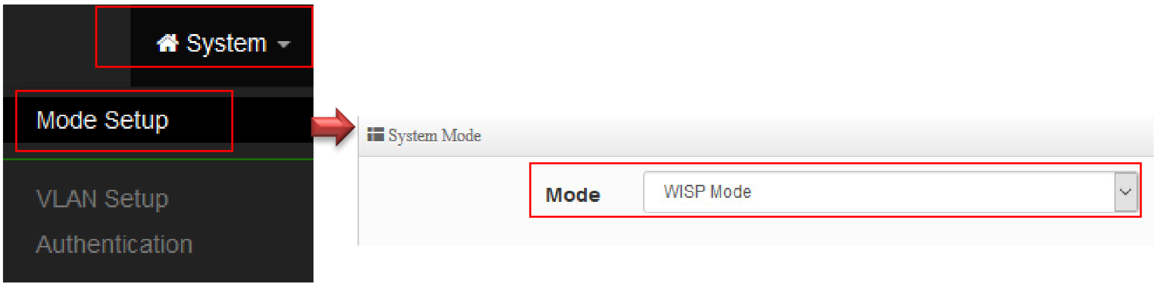
- It can be used as a Client Bridge + Repeater AP to receive wireless signals over last mile applications, helping WISPs deliver wireless broadband Internet service to new residential and business customers
- In this mode, the AP is enabled with DHCP Server functions. The wired clients of the AP are 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




Client Bridge Mode Enable Repeater Function
xDSL
WAN
Router
LAN
Switch
AP Mode
5G Bridge
Client Bridge Mode
RJ-45
5G Repeater Wi-Fi
Client Bridge mode enable repeater function
Client Bridge Mode + Repeater AP
RJ-45

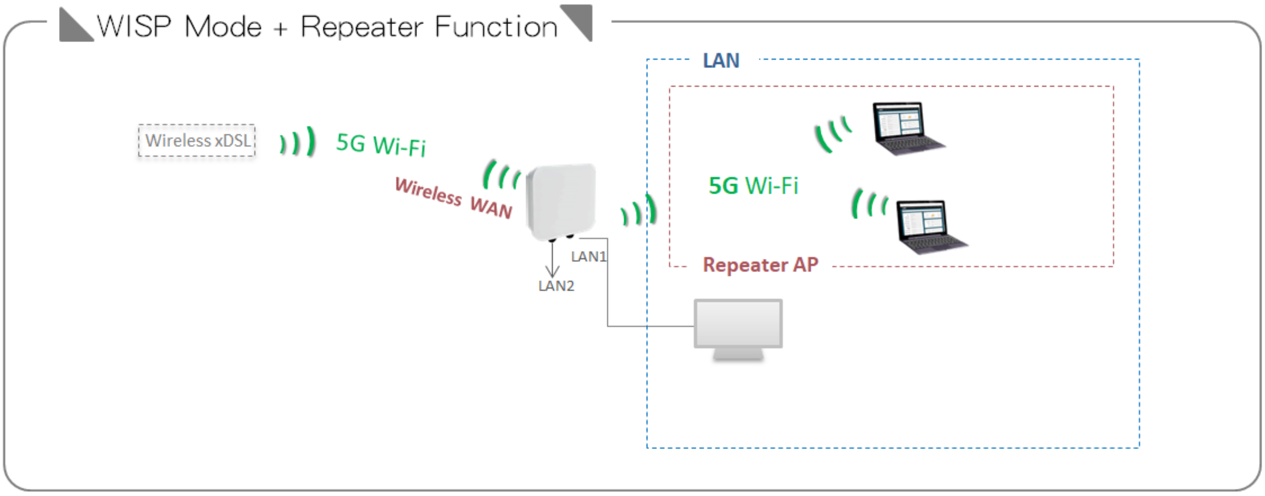
WISP + Repeater AP Mode

Please click on System ->Mode Setup and choose WISP Mode



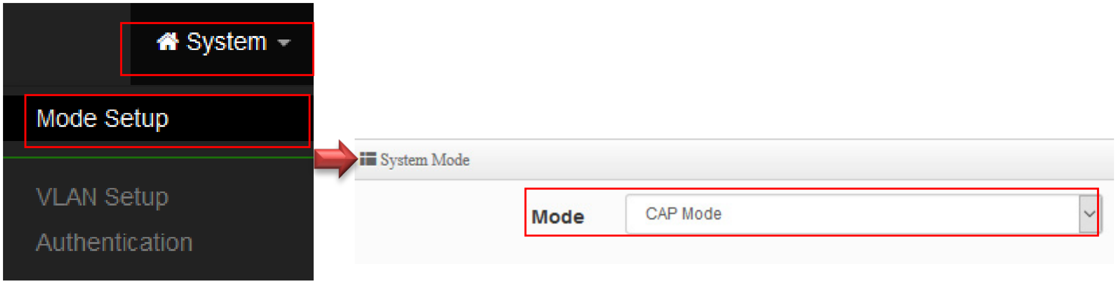
Mode: WISP Mode

- 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, the CenOS 5.0 AP is a gateway enabled with NAT and DHCP Server functions. The wired clients connected to APs 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.



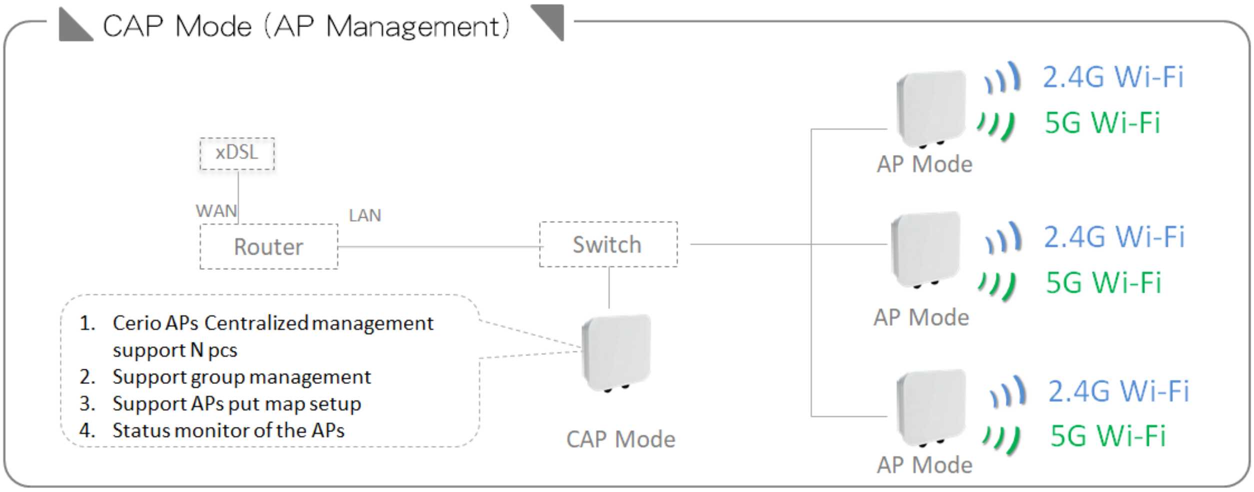
CAP mode (Centralizes Access Point)

Please click on System ->Mode Setup and choose CAP Mode



Mode: CAP Mode

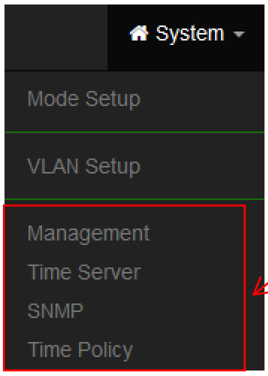
- ➢ Control Management of CenOS5.0 APs
- ➢ AP Management support 802.1Q VLAN infrastructure
- ➢ Centralized setting Access Point function and firmware upgrade.
- ➢ APs Group management for concept.



1. Cerio APs Centralized management support N pcs
2. Support group management
3. Support APs put map setup
4. Status monitor of the APs

2. System Configuration

Notice

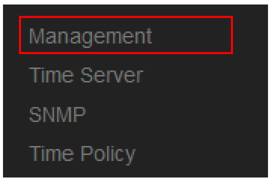


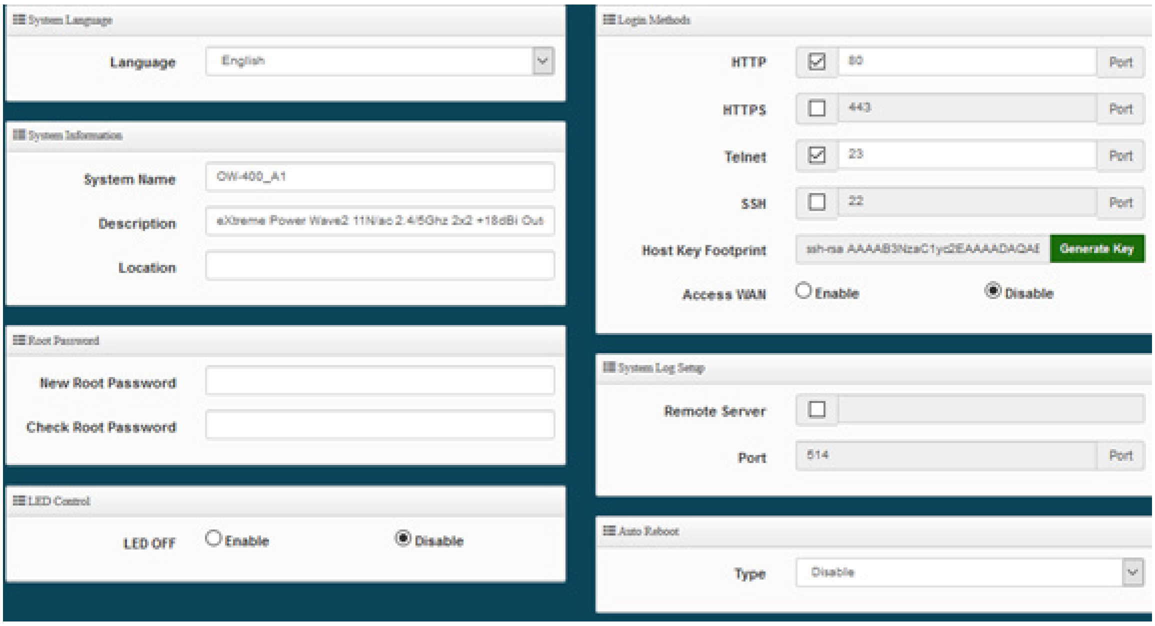
There are common functions in any mode have management / Time Server / SNMP and Time Policy. Please refer to the following detailed instructions.

2.1 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

System Information

System Name: OW-400_A1

Description: eXtreme Power Wave2 11N/ac 2.4/5Ghz 2x2 +18dBi Out

Location:

Root Password

New Root Password:

Check Root Password:

LED Control

LED OFF: ○ Enable ● Disable

Login Methods

HTTP: ☑ 80 Port

HTTPS: □ 443 Port

Telnet: ☑ 23 Port

SSH: □ 22 Port

Host Key Footprint: ssh-rsa AAAAB3NzaC1yc2EAAAADAQAE Generate Key

Access WAN: ○ Enable ● Disable

System Log Setup

Remote Server: □

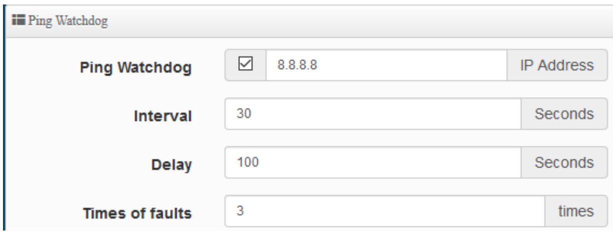
Port: 514 Port

Auto Reboot

Type: Disable

- **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.
- **Ping Watchdog:** Ping Watchdog helps administrator to automatically reboot the system when ever there is a network or AP issue.

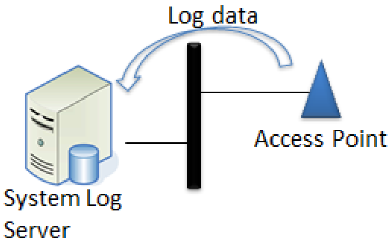


Ping Watchdog

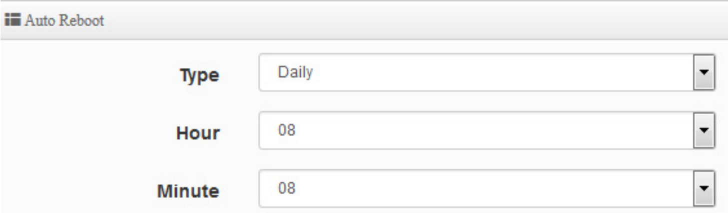
Ping Watchdog	☑ 8.8.8.8	IP Address
Interval	30	Seconds
Delay	100	Seconds
Times of faults	3	times

- **Ping Watchdog:** Enter IP address of remote device
- **Interval:** Ping interval of time.
- **Delay:** After system start, the set time value starts execution Ping watchdog.
- **Times of faults:** After the error exceeds the set value, system will auto reboot.

- **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.



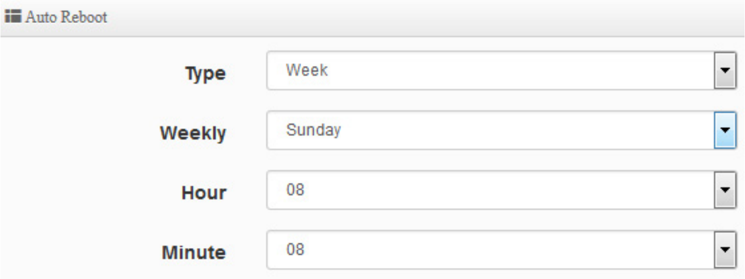
- **Auto Reboot:** The functions can Auto-reboot the system by Date/time management.
  - **Daily：** Setting time to system reboot.



Auto Reboot

Type	Daily
Hour	08
Minute	08

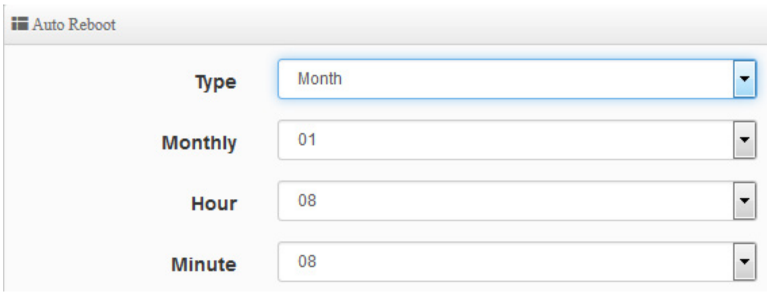
  - **Weekly :** Setting frequency (ex. Weekly) and time of system reboot



Auto Reboot

Type	Week
Weekly	Sunday
Hour	08
Minute	08

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

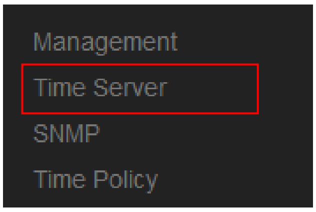


Auto Reboot

Type	Month
Monthly	01
Hour	08
Minute	08

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

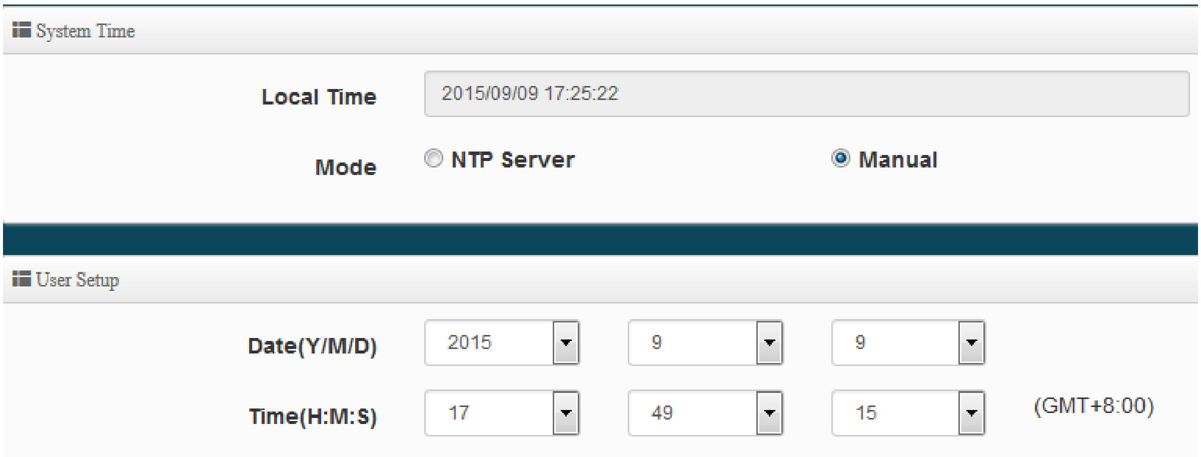
2.2 Configure Time Server



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.



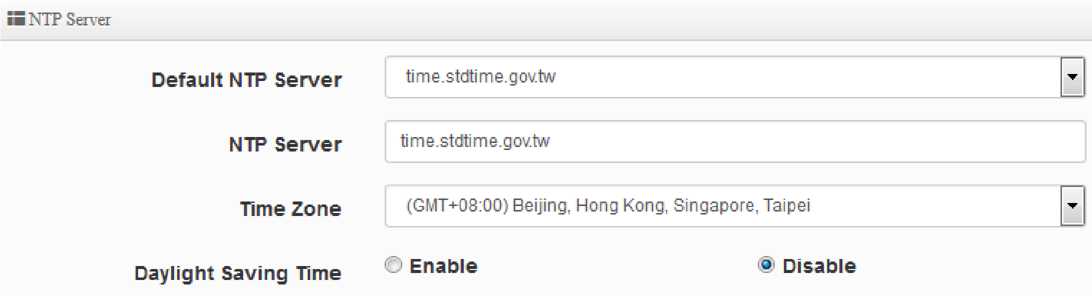
System Time

Local Time	2015/09/09 17:25:22
Mode	○ NTP Server ● Manual

User Setup

Date(Y/M/D)	2015	9	9	
Time(H:M:S)	17	49	15	(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.

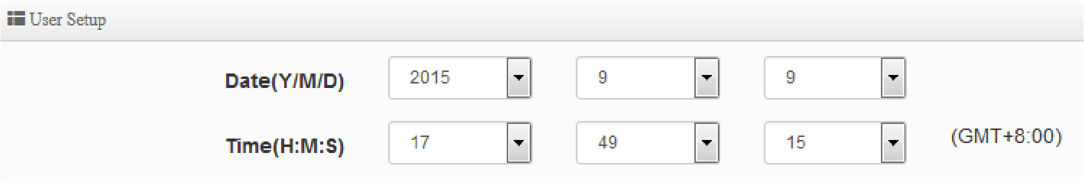


NTP Server

Default NTP Server	time.stdtime.gov.tw	
NTP Server	time.stdtime.gov.tw	
Time Zone	(GMT+08:00) Beijing, Hong Kong, Singapore, Taipei	
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.

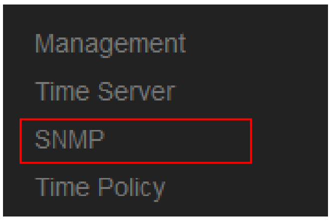


User Setup

Date(Y/M/D)	2015	9	9	
Time(H:M:S)	17	49	15	(GMT+8:00)

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

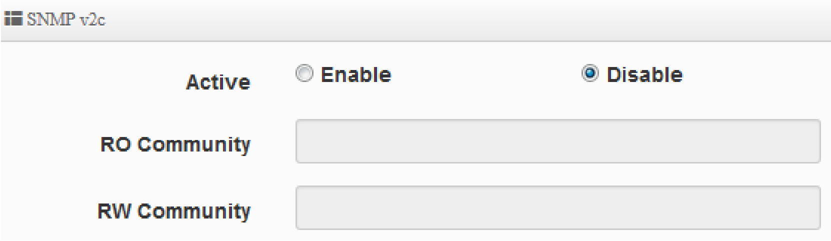
2.3 SNMP



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

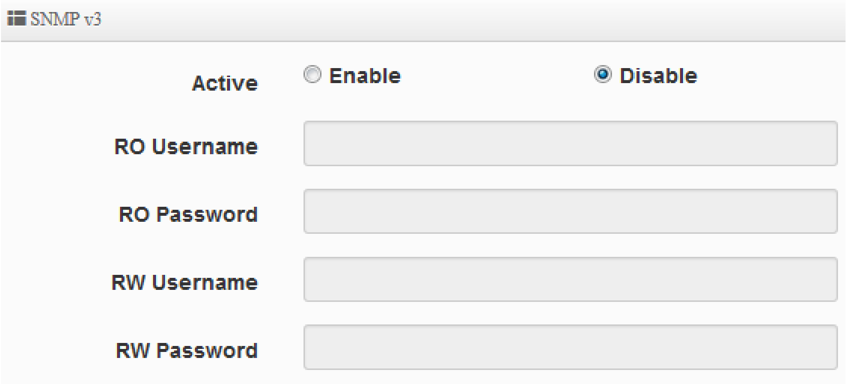


SNMP v2c

Active	○ Enable	● Disable
RO Community		
RW Community		

- ➢ **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



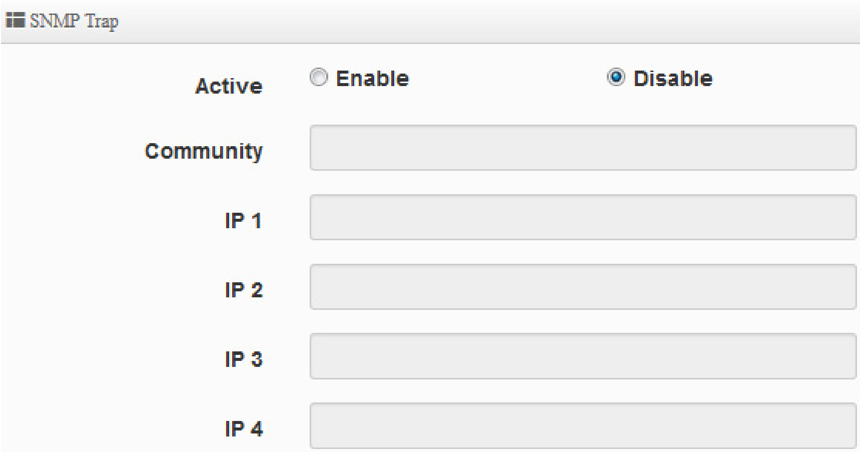
SNMP v3

Active	○ Enable ● Disable
RO Username	
RO Password	
RW Username	
RW Password	

- ➢ **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.



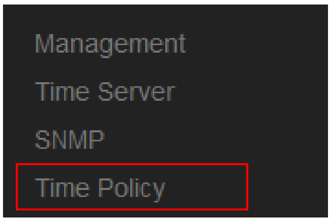
SNMP Trap

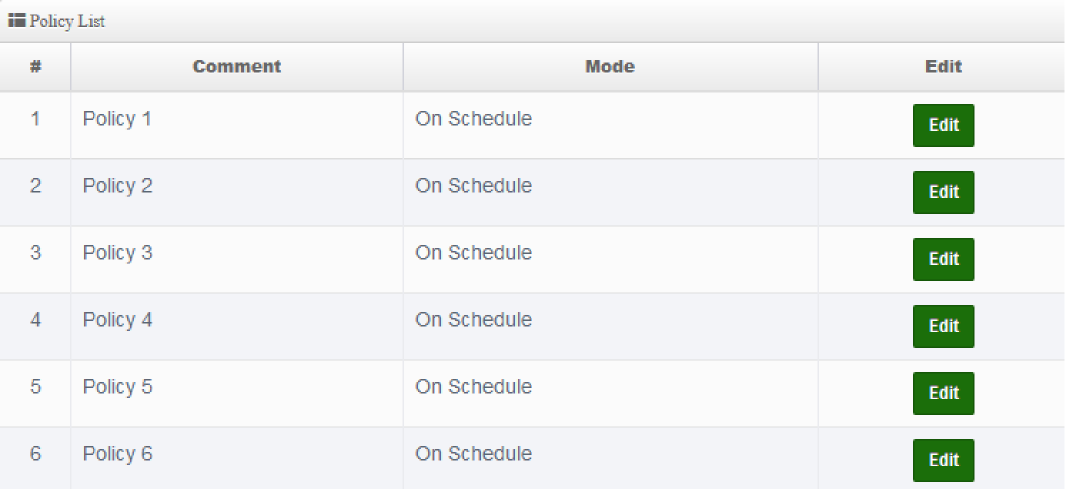
Active	○ Enable ● Disable
Community	
IP 1	
IP 2	
IP 3	
IP 4	

- ➢ **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

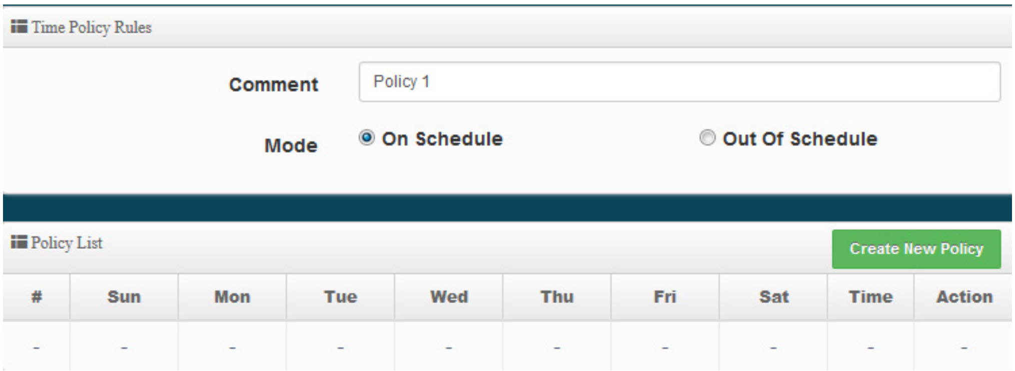
2.4 Configure Time Policy




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: Policy 1

Mode: ● On Schedule ○ Out Of Schedule

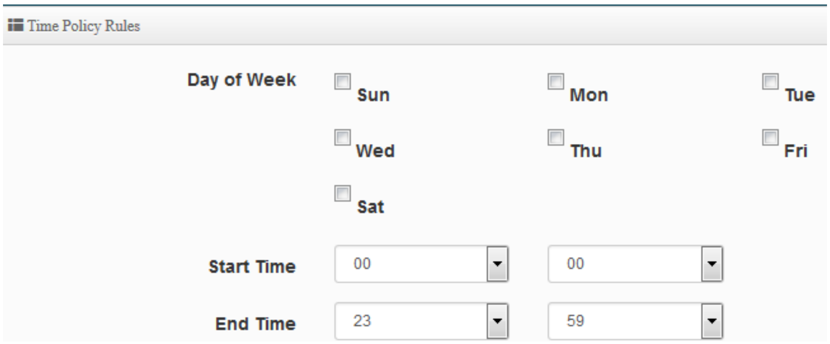
Policy List

#	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.

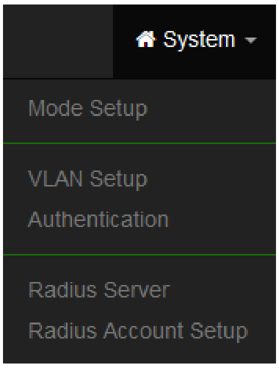


Time Policy Rules

Day of Week	□ Sun	□ Mon	□ Tue
	□ Wed	□ Thu	□ Fri
	□ Sat		
Start Time	00	00	
End Time	23	59	

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.

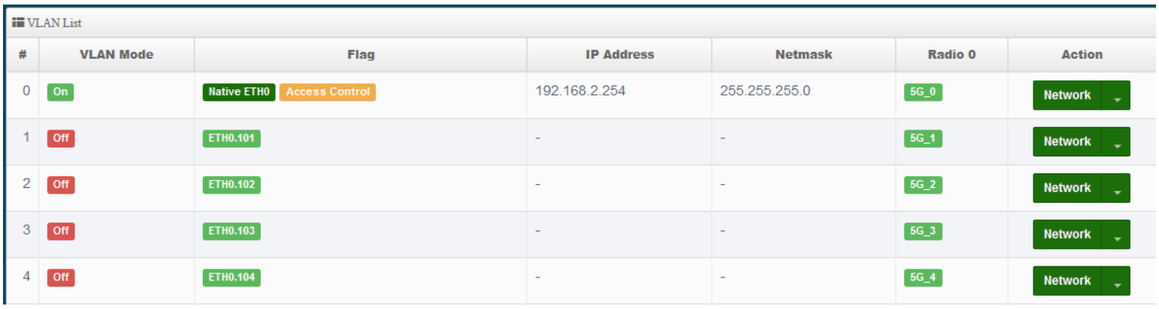
3. Access Point mode



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.

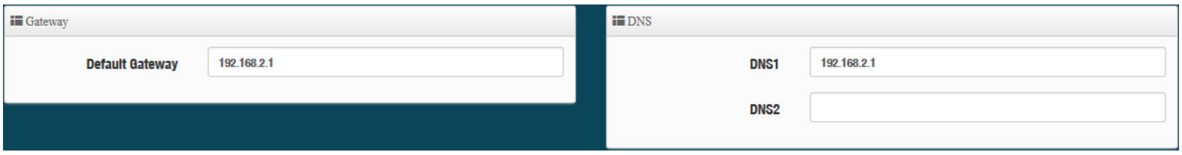
3.1 VLAN Setup

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



VLAN List

#	VLAN Mode	Flag	IP Address	Netmask	Radio 0	Action
0	On	Native ETH0 Access Control	192.168.2.254	255.255.255.0	5G_0	Network
1	Off	ETH0.101	-	-	5G_1	Network
2	Off	ETH0.102	-	-	5G_2	Network
3	Off	ETH0.103	-	-	5G_3	Network
4	Off	ETH0.104	-	-	5G_4	Network



Gateway

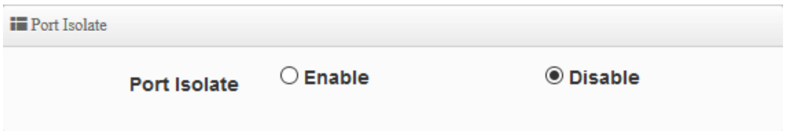
Default Gateway 192.168.2.1

DNS

DNS1 192.168.2.1

DNS2

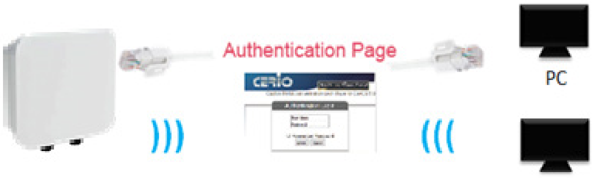
- **VLAN Mode**：Display on/off for the VLAN network.
- **Flag**：Display master VLAN and VLAN Tag No. information.
- **IP Address**：Display IP Address for VLAN Network.
- **NetMask**：Display IP netmask.
- **Radio 0**：Display radio 5G SSID name.
- **Default Gateway:** Set Gateway IP address.
- **Port Isolate :** When enable web authentication function, administrator can chooses Ethernet port whether used web authentication.*(This function need enable System →Authentication function)*



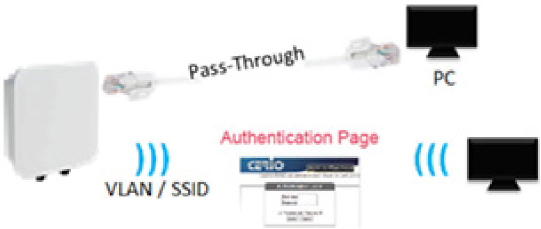
Port Isolate

Port Isolate ○ Enable ● Disable

- **Enable:** If chooses enable this function then client connection Ethernet port will need web authentication too. When enable this function system will only 1 VLAN and 1 ESSID.



- **Disable:** If chooses disable this function then client connection Ethernet port will not be intercepted using web authentication. Wired client network basis on VLAN0. When disable this function system can use 16 VLAN and 16 ESSID.

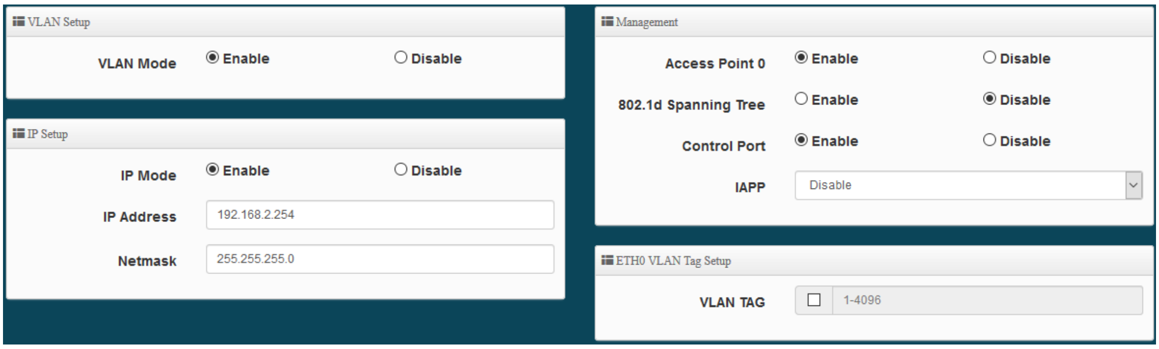


- **DNS:** Set DNS IP address.
- **Action**：The button can set VLAN network functions and radio functions.

# Network Setup

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	192.168.2.254	
Netmask	255.255.255.0	

Management

Access Point 0	● Enable	○ Disable
802.1d Spanning Tree	○ Enable	● Disable
Control Port	● Enable	○ Disable
IAPP	Disable	

ETH0 VLAN Tag Setup

VLAN TAG	□ 1-4096

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

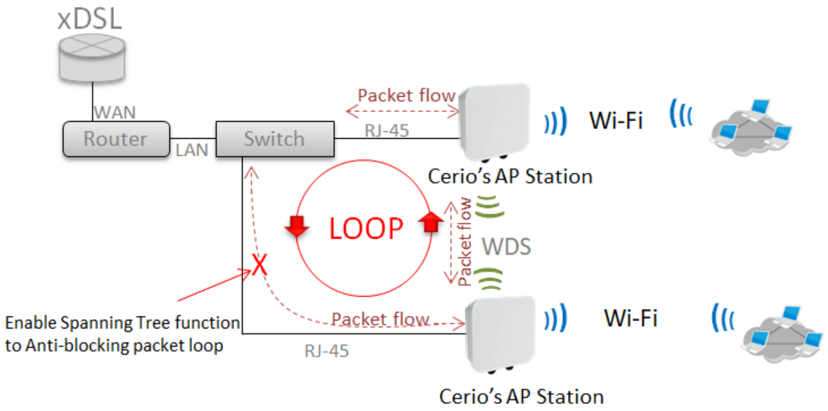
Notice

At least one VLAN will always be enabled by default

- ➢ **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 5G 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

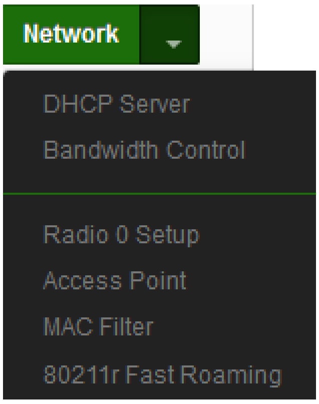


- ➢ **Control Port**：Administrator can select one of the VLAN as managed AP.
- ➢ **IAPP**：Administrator can select radio 5G for IAPP roaming.*(the IAPP condition must use WPA2-PSK Wi-Fi security and AES algorithm)*
- ➢ **VLAN Tag Setup:** Set the VLAN used tags.

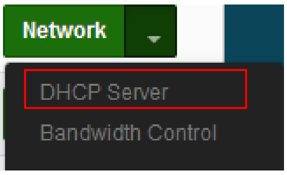
# Network Pull-down menu

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

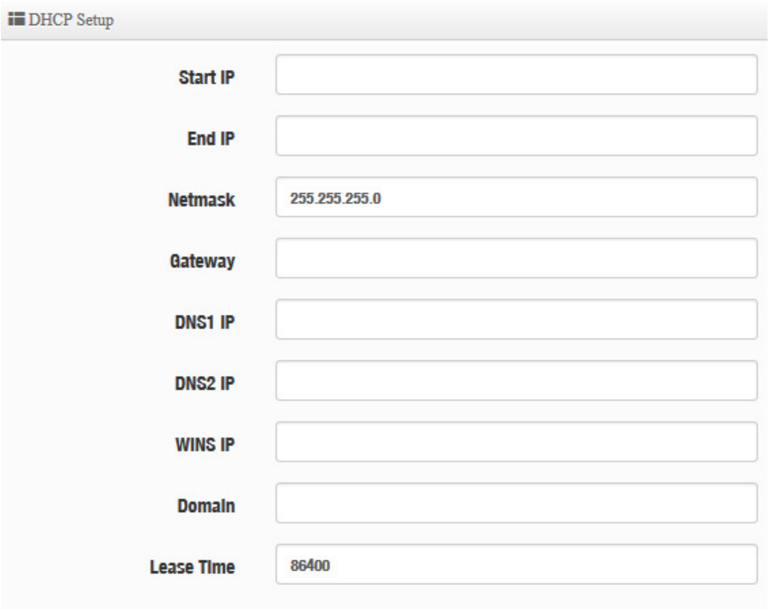
Please click pull-down button.



3.1.1 DHCP Server



Administrator can select enable / disable the function



DHCP Setup

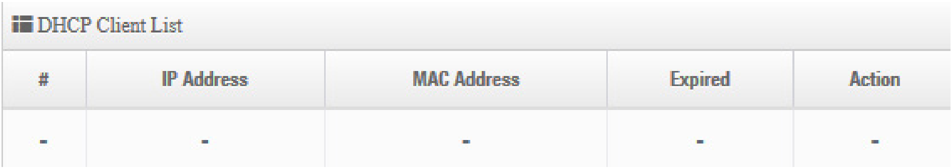
Start IP	
End IP	
Netmask	255.255.255.0
Gateway	
DNS1 IP	
DNS2 IP	
WINS IP	
Domain	
Lease Time	86400

- **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.

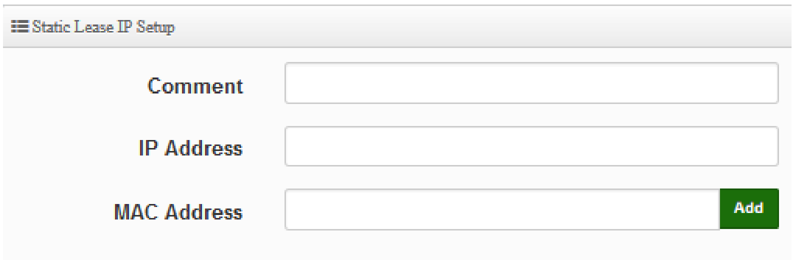


DHCP Client List

#	IP Address	MAC Address	Expired	Action
-	-	-	-	-

Static Lease IP Setup

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



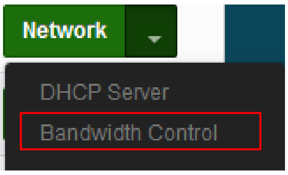
Static Lease IP Setup

Comment	
IP Address	
MAC Address	Add

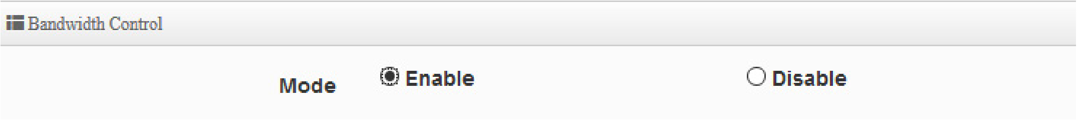
- **Comment :** Enter rule description.
- **IP Address :** Enter access point IP.
- **MAC Address :** Enter Client MAC Address of PC network.

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

3.1.2 Bandwidth Control



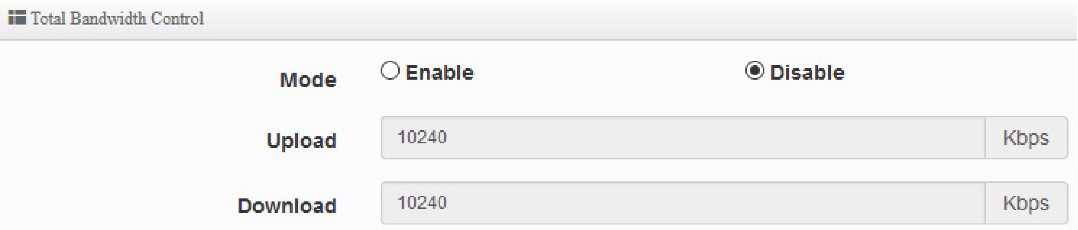
Administrators can set bandwidth limit the max/min bandwidth of the Wi-Fi users, Bandwidth control can set IP/MASK , IP Range, Port(Service), SIP, RTP/RTSP and WEB.



Bandwidth Control

Mode ● Enable ○ Disable

Administrator can enable or disable the function.



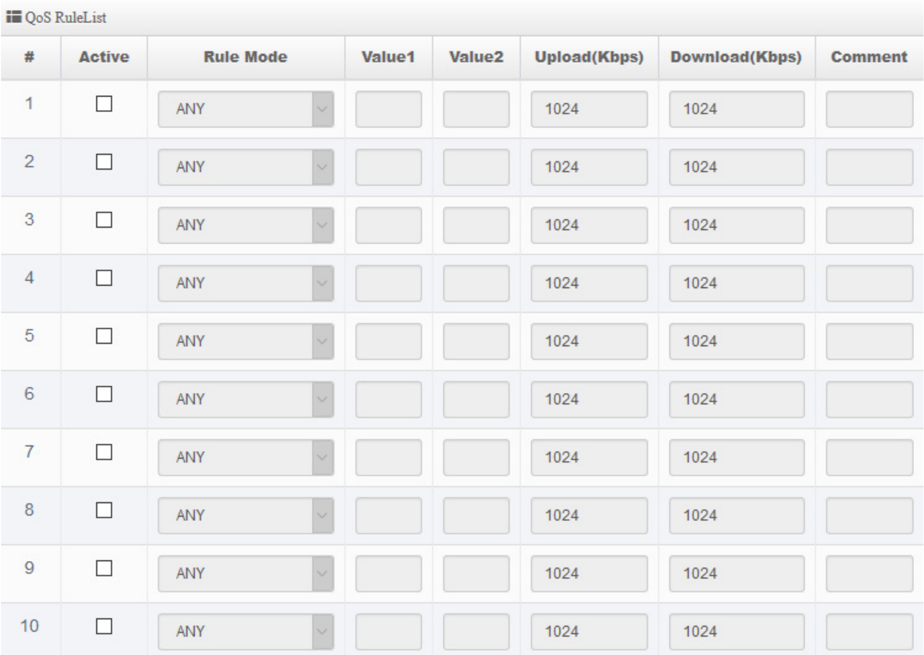
Total Bandwidth Control

Mode ○ Enable ● Disable

Upload 10240 Kbps

Download 10240 Kbps

- Administrator can set total bandwidth used limit in VLAN.



QoS RuleList

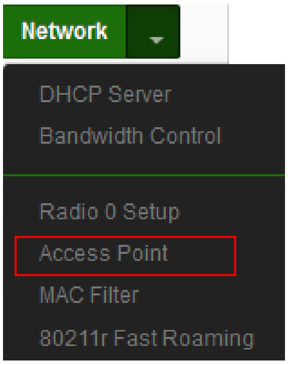
#	Active	Rule Mode	Value1	Value2	Upload(Kbps)	Download(Kbps)	Comment
1	□	ANY			1024	1024	
2	□	ANY			1024	1024	
3	□	ANY			1024	1024	
4	□	ANY			1024	1024	
5	□	ANY			1024	1024	
6	□	ANY			1024	1024	
7	□	ANY			1024	1024	
8	□	ANY			1024	1024	
9	□	ANY			1024	1024	
10	□	ANY			1024	1024	

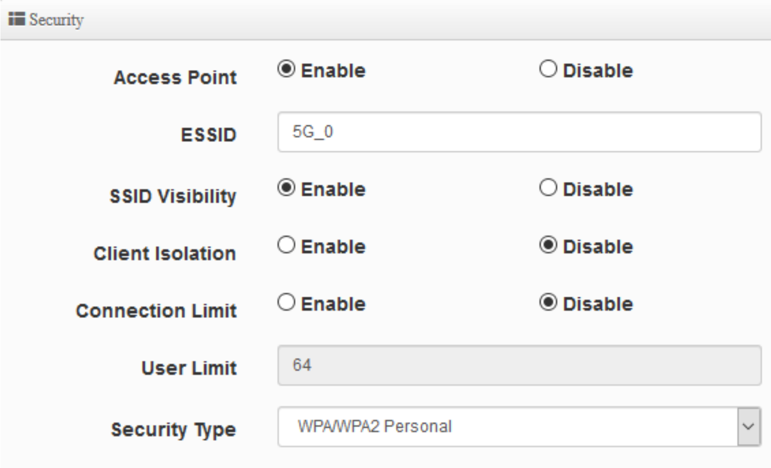
- **QoS Rule List:** Administrator can set bandwidth limit by IP/MASK, IP Range, Port(Service), SIP, RTP/RTSP, WEB protocol , each VLAN can set 10 bandwidth management rule.

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

3.1.3 Radio 0 Access Point Setup

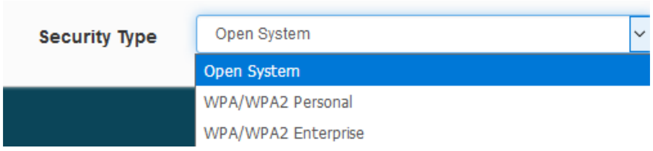
Administrator can Enable or Disable radio 0 (5G) Wi-Fi. If radio 0 (5G) are enabled, administrators can set the SSID and security for the 5G access point.



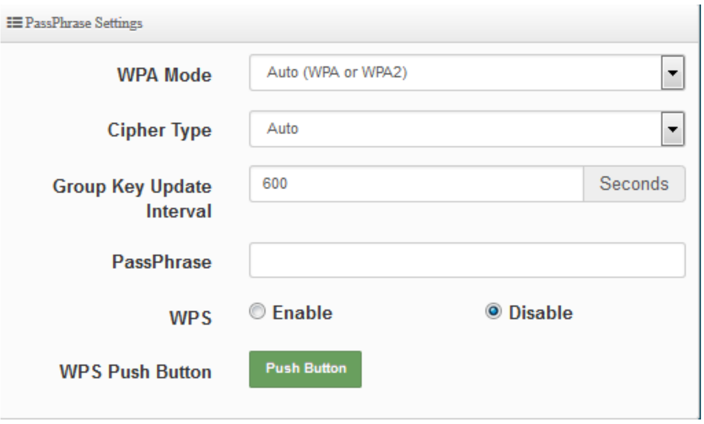

Security

Access Point	● Enable	○ Disable
ESSID	5G_0	
SSID Visibility	● Enable	○ Disable
Client Isolation	○ Enable	● Disable
Connection Limit	○ Enable	● Disable
User Limit	64	
Security Type	WPA/WPA2 Personal	

- **Access Point:** Administrator can Enable or Disable the radio 0 (5G).
- **ESSID:** Administrator can set Wi-Fi SSID name
- **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.(Recommended limit 60 Wi-Fi Users)
- **Security Type:** Select the desired security type from the drop-down list; the options are Open System, WPA-PSK/WPA2-PSK and WPA/WPA2-Enterprise.


Security Type: Open System

- **Open System:** Data is not unencrypted during transmission when this option is selected.
- **WPA-PSK/WPA2-PSK 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

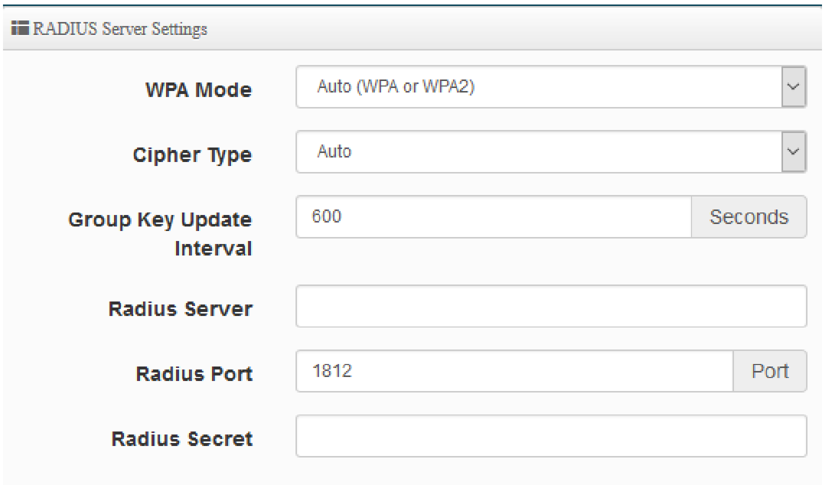
WPA Mode	Auto (WPA or WPA2)
Cipher Type	Auto
Group Key Update Interval	600 Seconds
PassPhrase	
WPS	○ Enable ● Disable

- ✓ **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.

- **WPA/WAP2-Enterprise**



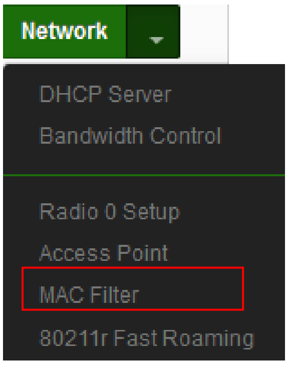
RADIUS Server Settings

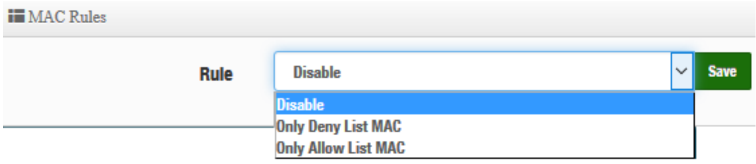
WPA Mode	Auto (WPA or WPA2)
Cipher Type	Auto
Group Key Update Interval	600 Seconds
Radius Server	
Radius Port	1812 Port
Radius Secret	

- **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.

After the above function is setup, please click "**Save**" button and **reboot** system will apply new profile and working normally.

3.1.4 MAC Filter





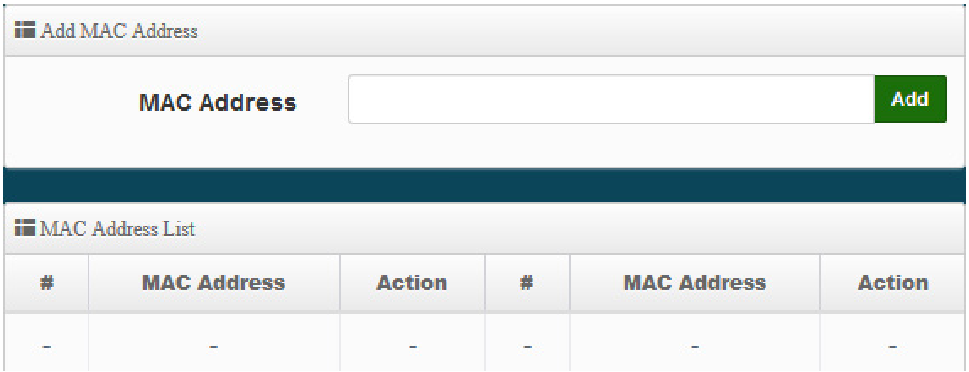
MAC Rules

Rule: Disable

(1) Only Deny List MAC：Administrator can add wireless users MAC address in MAC list. The access point will deny connection in MAC address list.

(2) Only Allow List MAC：Administrator can add wireless users MAC address in MAC list. The access point will allow connection in MAC address list.

After the above function is setup, please click "**Save**" button and **reboot** system will apply new profile and working normally.



Add MAC Address

MAC Address Add

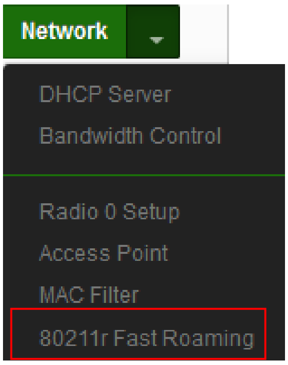
MAC Address List

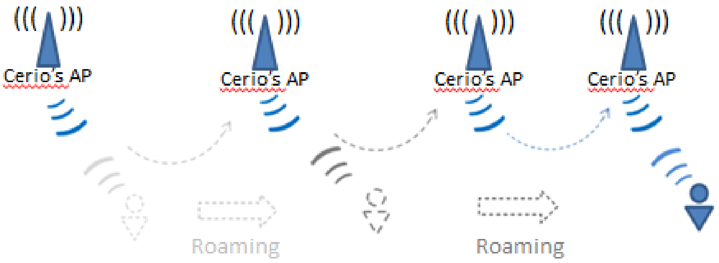
#	MAC Address	Action	#	MAC Address	Action
-	-	-	-	-	-

- **MAC Address:** Set managed MAC address of the client.
- **MAC Address List:** Display managed MAC address list.

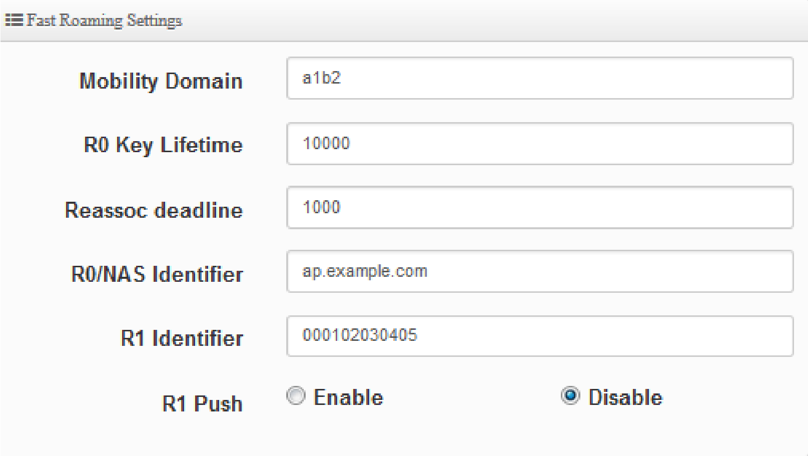
Click “**Save”** button to save your changes. Then click **Reboot** button to activate your changes.

3.1.5 802.11r Fast Roaming Setup





The dual band Access Point supports 802.11r/802.11k function for 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.



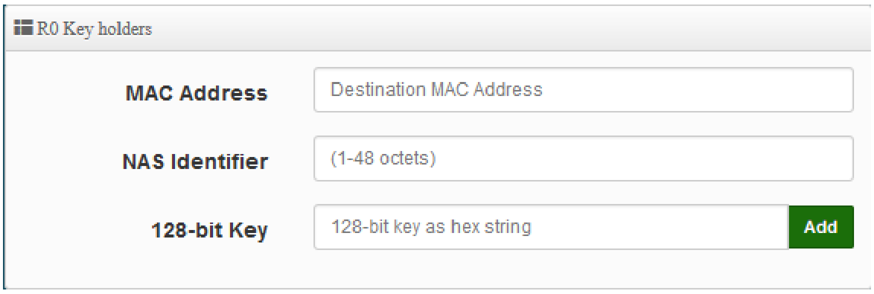
Fast Roaming Settings

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 Holder:

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.

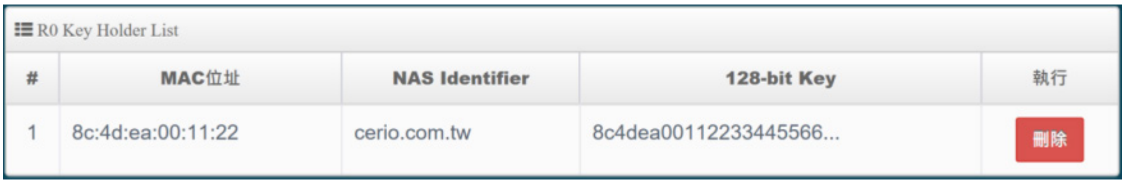


R0 Key holders

MAC Address	Destination MAC Address
NAS Identifier	(1-48 octets)
128-bit Key	128-bit key as hex string

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

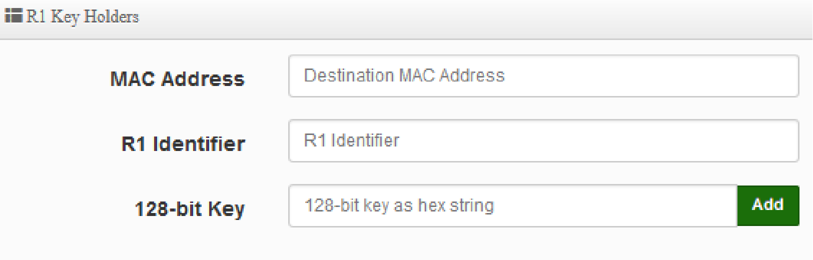
- **128-bit Key:** Enter Shared Key of 128 bit.



R0 Key Holder List

#	MAC位址	NAS Identifier	128-bit Key	執行
1	8c:4d:ea:00:11:22	cerio.com.tw	8c4dea00112233445566...	刪除

R1 Key holders : Enter a unified set of R1 Key Holder identification certification.



R1 Key Holders

MAC Address	Destination MAC Address
R1 Identifier	R1 Identifier
128-bit Key	128-bit key as hex string

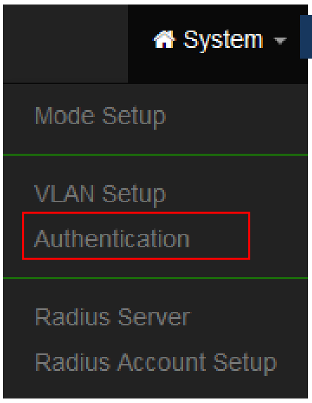
- **MAC Address:** Enter the main roaming device MAC address
- **R1 Identifier:** Enter Shared identifier.
- **128-bit Key:** Enter Shared Key of 128 bit.

After the above function is setup, please click "**Save**" button and **reboot** system will apply new profile and working normally.

3.2 Authentication

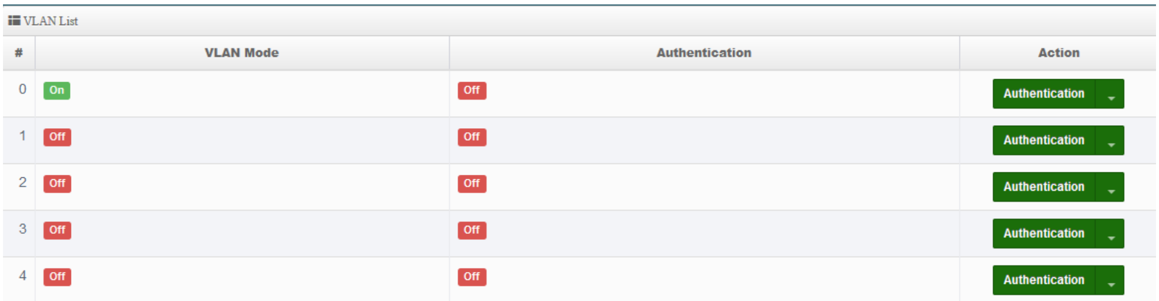
This function used to operate in **Access Point** mode**,** the function is for Web Authentication. It supports authentication for local users / RADIUS Server / OAuth2.0 and Guest. The system supports in N VLANs with web authentication.

Please click on System -> Authentication



Notice

When enable web authentication function, please does make the Access Point can be connected to gateway. Please refer to 3.1 VLAN Setup. If the gateway IP address is set error then web authentication page will be can't display.



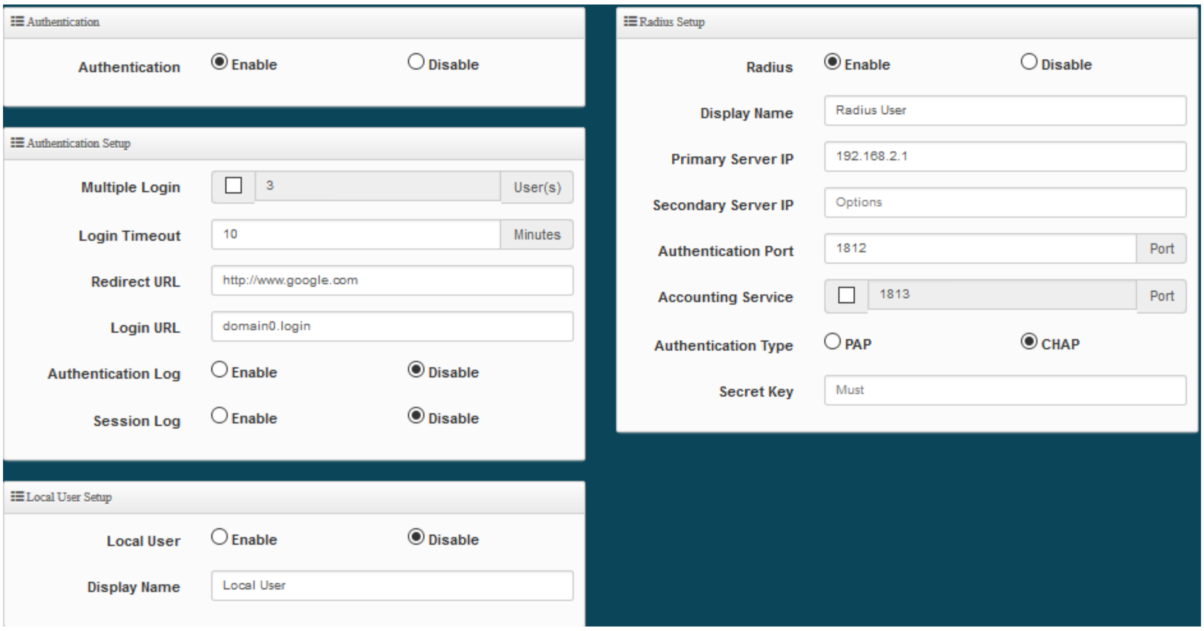
VLAN List

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

- **#**：Display VLANs number.
- **VLAN Mode**：Displays VLAN on/off status. (Please refer to 3.2 VLAN Setup)
- **Authentication**：Displays VLAN# whether enable or disable web authentication.
- **Action**：The function has 2 buttons (Authentication and Dropdown)

3.2.1 Enable Authentication function

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



Authentication

Authentication	● Enable	○ Disable

Authentication Setup

Multiple Login	□ 3	User(s)
Login Timeout	10	Minutes
Redirect URL	http://www.google.com	
Login URL	domain0.login	
Authentication Log	○ Enable	● Disable
Session Log	○ Enable	● Disable

Local User Setup

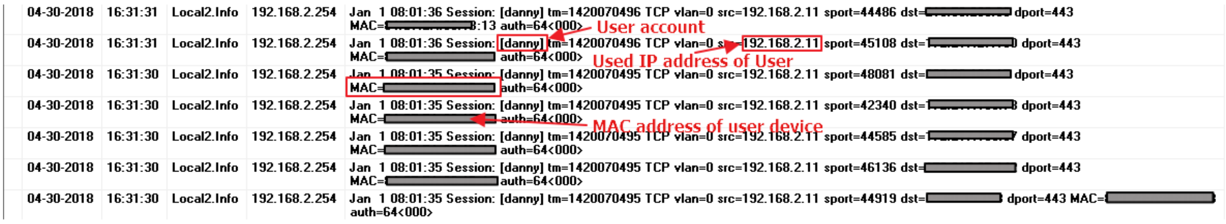
Local User	○ Enable	● Disable
Display Name	Local User	

Radius Setup

Radius	● Enable	○ Disable
Display Name	Radius User	
Primary Server IP	192.168.2.1	
Secondary Server IP	Options	
Authentication Port	1812	Port
Accounting Service	□ 1813	Port
Authentication Type	○ PAP	● CHAP
Secret Key	Must	

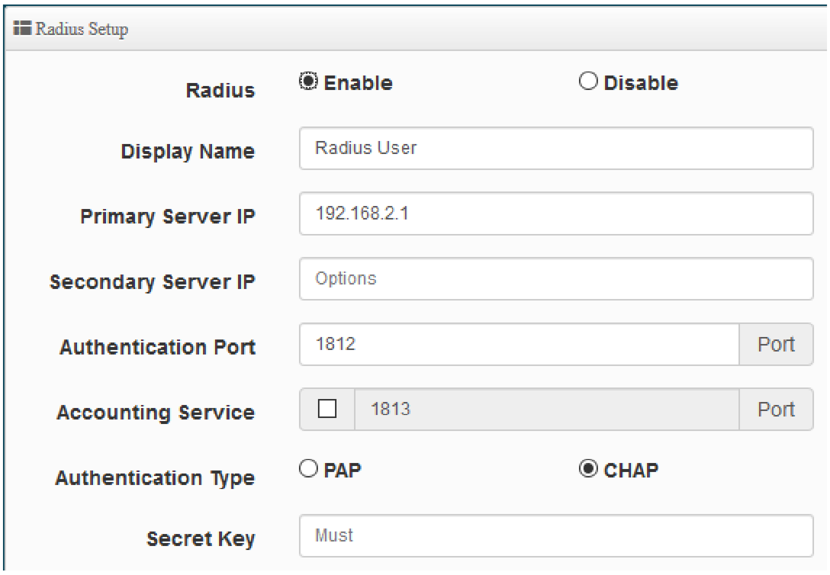
- **Authentication**：Administrator can enable or disable authentication function.
- **Multiple Login**：Administrator can set one account to multiple users simultaneously login and the users can set limit.(0 = not limited)
- **Login Timeout**：After account login for some time no traffic, system will automatic 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.



```
04-30-2018  16:31:31  Local2.Info  192.168.2.254  Jan  1 08:01:36 Session: [danny] tm=1420070496 TCP vlan=0 src=192.168.2.11 sport=44486 dst=[redacted] dport=443
                                                  MAC=[redacted]:13 auth=64<000>
04-30-2018  16:31:31  Local2.Info  192.168.2.254  Jan  1 08:01:36 Session: [danny] tm=1420070496 TCP vlan=0 src=192.168.2.11 sport=45108 dst=[redacted] dport=443
                                                  MAC=[redacted] auth=64<000>
04-30-2018  16:31:30  Local2.Info  192.168.2.254  Jan  1 08:01:35 Session: [danny] tm=1420070495 TCP vlan=0 src=192.168.2.11 sport=48081 dst=[redacted] dport=443
                                                  MAC=[redacted] auth=64<000>
04-30-2018  16:31:30  Local2.Info  192.168.2.254  Jan  1 08:01:35 Session: [danny] tm=1420070495 TCP vlan=0 src=192.168.2.11 sport=42340 dst=[redacted] dport=443
                                                  MAC=[redacted] auth=64<000>
04-30-2018  16:31:30  Local2.Info  192.168.2.254  Jan  1 08:01:35 Session: [danny] tm=1420070495 TCP vlan=0 src=192.168.2.11 sport=44585 dst=[redacted] dport=443
                                                  MAC=[redacted] auth=64<000>
04-30-2018  16:31:30  Local2.Info  192.168.2.254  Jan  1 08:01:35 Session: [danny] tm=1420070495 TCP vlan=0 src=192.168.2.11 sport=46136 dst=[redacted] dport=443
                                                  MAC=[redacted] auth=64<000>
04-30-2018  16:31:30  Local2.Info  192.168.2.254  Jan  1 08:01:35 Session: [danny] tm=1420070495 TCP vlan=0 src=192.168.2.11 sport=44919 dst=[redacted] dport=443 MAC=[redacted]
                                                  auth=64<000>
```

- **Local User**：Administrator can enable authentication for local user. Create user account can to reference **"3.2.2 Local User"** setup**.**
- **RADIUS**： Authentication support remote RADIUS Server. Administrator can enter security information for remote RADIUS Server.



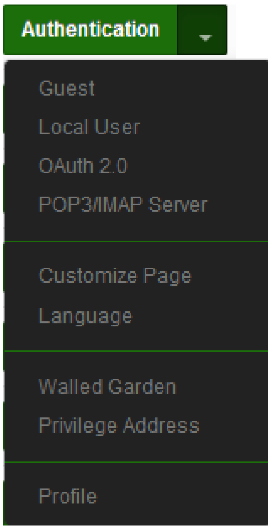
Radius Setup

Radius	● Enable	○ Disable
Display Name	Radius User	
Primary Server IP	192.168.2.1	
Secondary Server IP	Options	
Authentication Port	1812	Port
Accounting Service	□ 1813	Port
Authentication Type	○ PAP	● CHAP
Secret Key	Must	

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

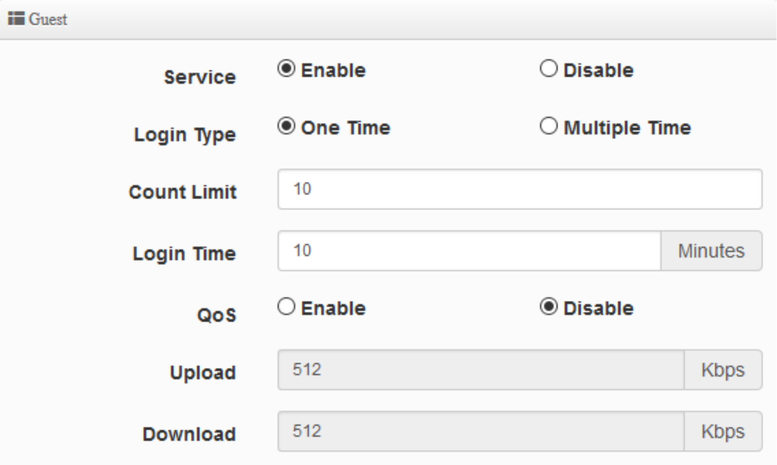
3.2.2 Set Authentication function

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



# 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

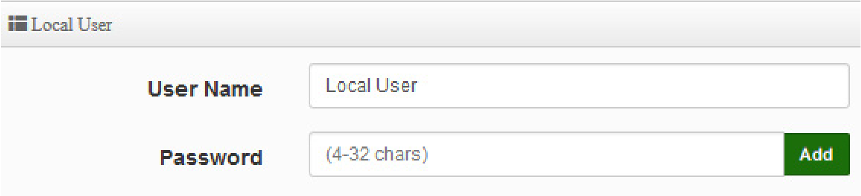
Service	● Enable	○ Disable
Login Type	● One Time	○ Multiple Time
Count Limit	10	
Login Time	10 Minutes	
QoS	○ Enable	● Disable
Upload	512 Kbps	
Download	512 Kbps	

- ➢ **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.

# Local User

Administrator can create local user account for web login.



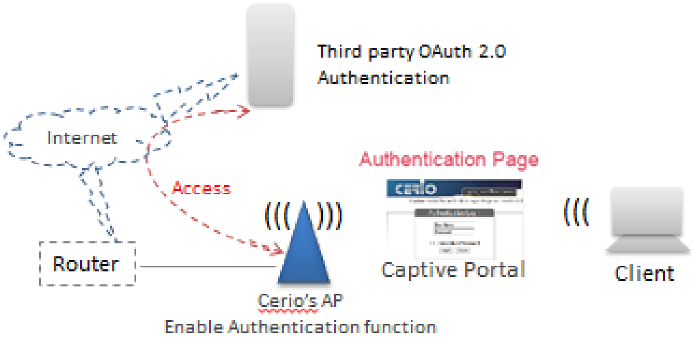
Local User

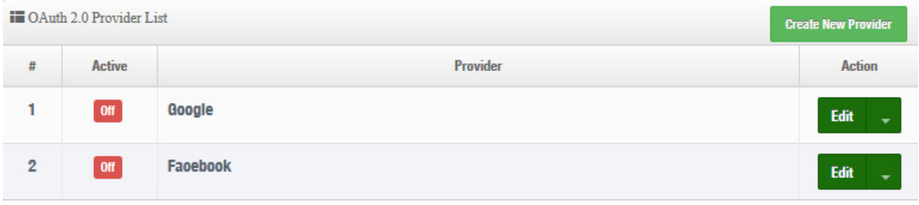
User Name	Local User
Password	(4-32 chars) Add

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

# 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	Off	Google	Edit ⌄
2	Off	Facebook	Edit ⌄

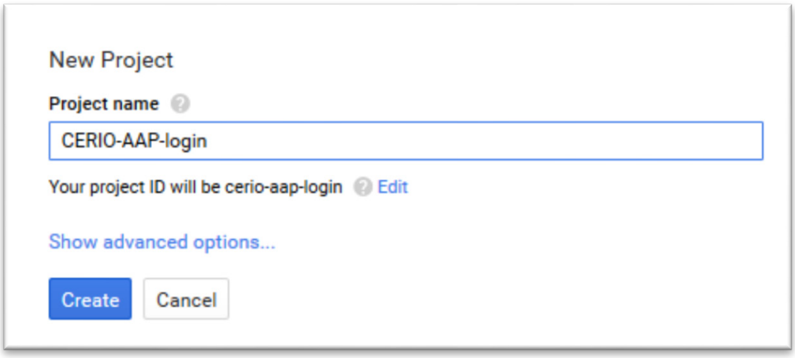
- **#：**Display items.
- **Active：**Display on/off status for the authentication.
- **Provider：**Display authentication server. The system default use authentication server for Google and Facebook

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)

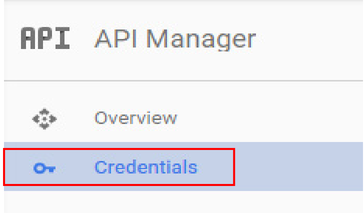


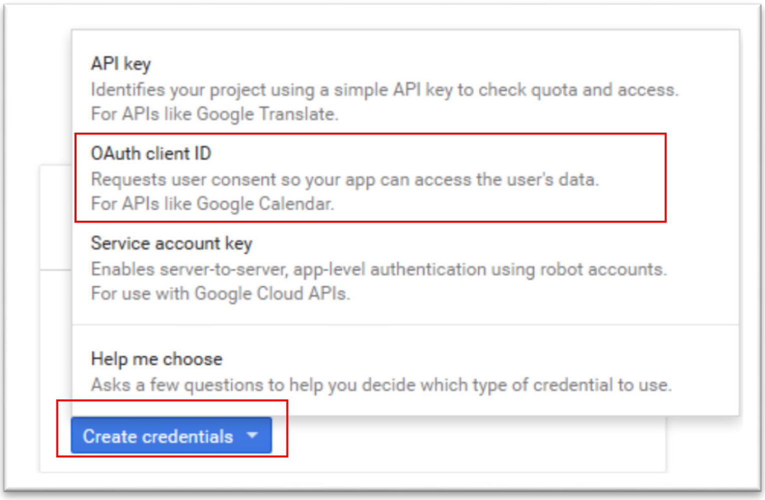
New Project

Project name: CERIO-AAP-login

Your project ID will be cerio-aap-login Edit

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





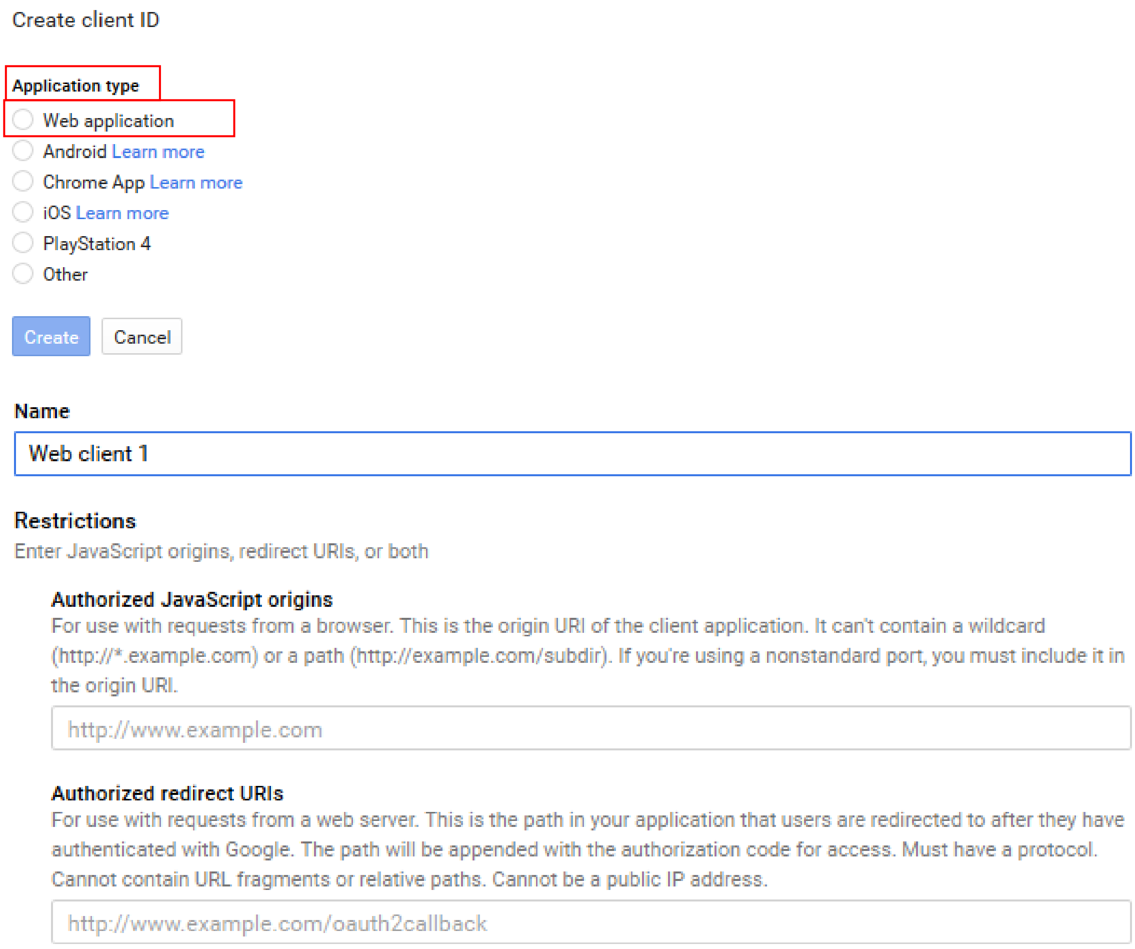
API key
Identifies your project using a simple API key to check quota and access.
For APIs like Google Translate.

OAuth client ID
Requests user consent so your app can access the user's data.
For APIs like Google Calendar.

Service account key
Enables server-to-server, app-level authentication using robot accounts.
For use with Google Cloud APIs.

Help me choose
Asks a few questions to help you decide which type of credential to use.

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

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

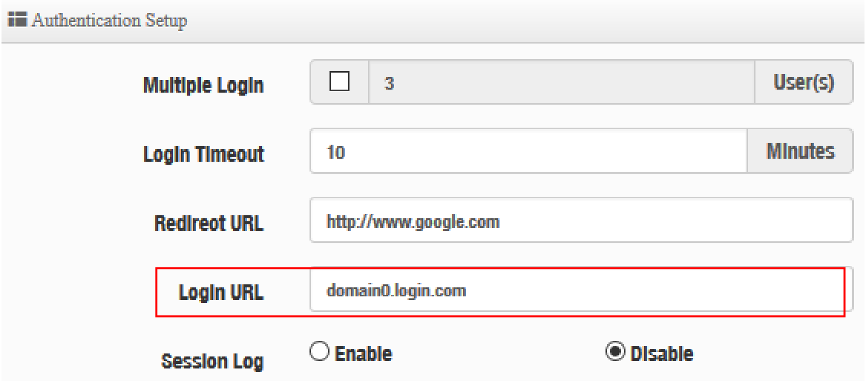
For use with requests from a web server. This is the path in your application that users are redirected to after they have authenticated with Google. The path will be appended with the authorization code for access. Must have a protocol. Cannot contain URL fragments or relative paths. Cannot be a public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



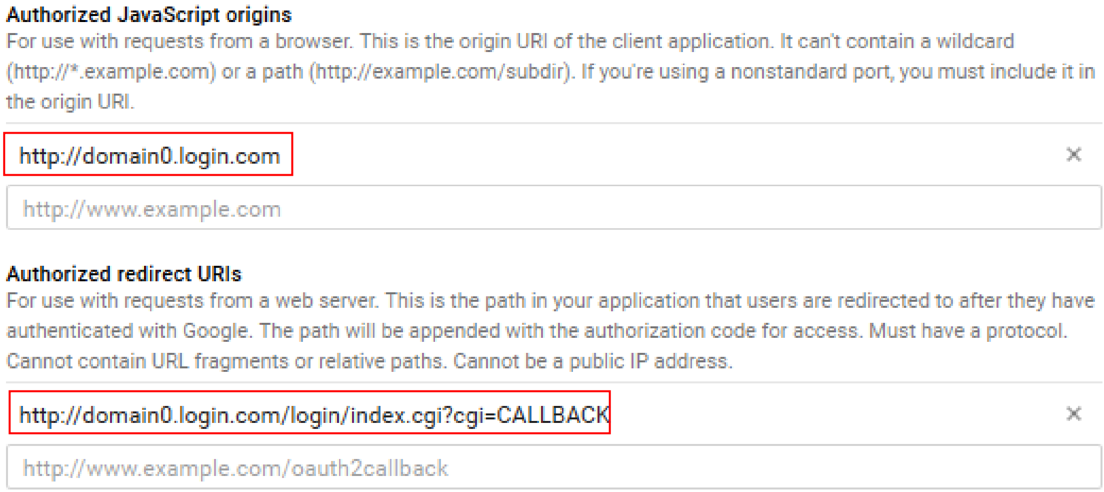
Authentication Setup

Multiple Login	□ 3 User(s)
Login Timeout	10 Minutes
Redirect URL	http://www.google.com
Login URL	domain0.login.com
Session Log	○ Enable ● Disable

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.

http://domain0.login.com ×

http://www.example.com

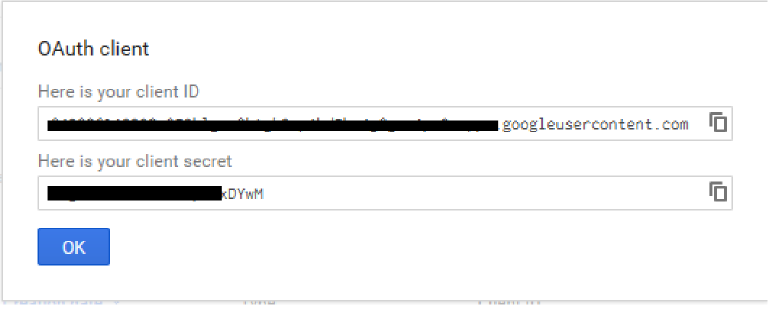
Authorized redirect URIs

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://domain0.login.com/login/index.cgi?cgi=CALLBACK ×

http://www.example.com/oauth2callback

Step.5 After completing the "Restrictions" setup, click the create button. An 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.



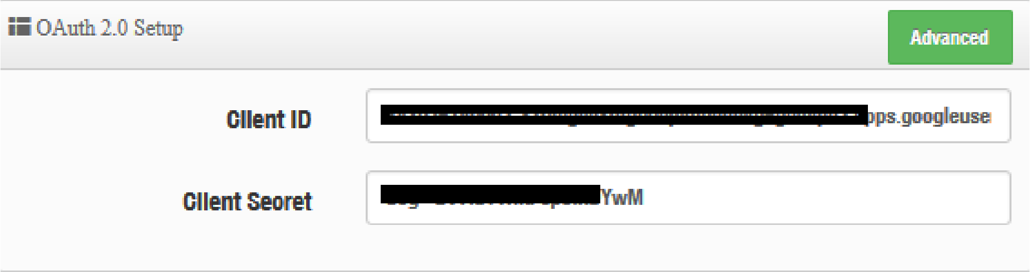
OAuth client

Here is your client ID

[redacted]googleusercontent.com

Here is your client secret

[redacted]kDYwM



OAuth 2.0 Setup

Client ID [redacted]pps.googleuse

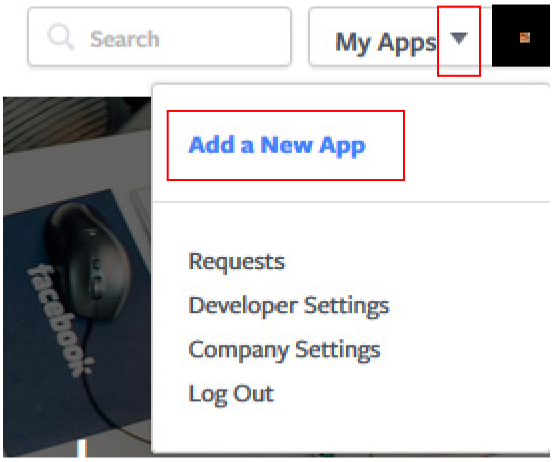
Client Secret [redacted]YwM

Save and reboot the AP system, complete the setup.

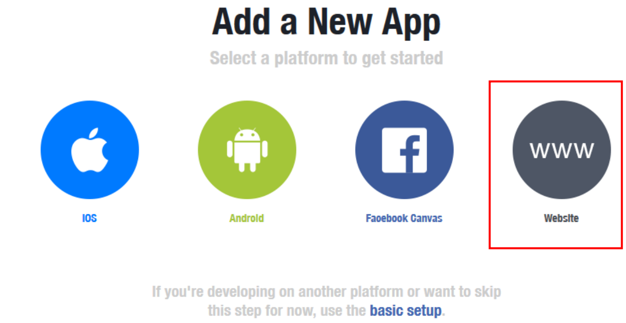
Sample for Facebook OAuth2.0 setup

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

Step.1 Please to Facebook developer's page and add a New App



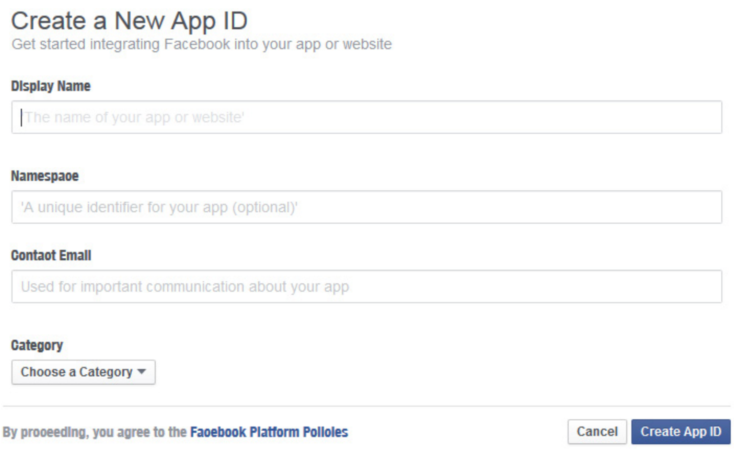
Step.2 Select WWW function


Add a New App

Select a platform to get started

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'

Namespaoe

'A unique identifier for your app (optional)'

Contaot Emall

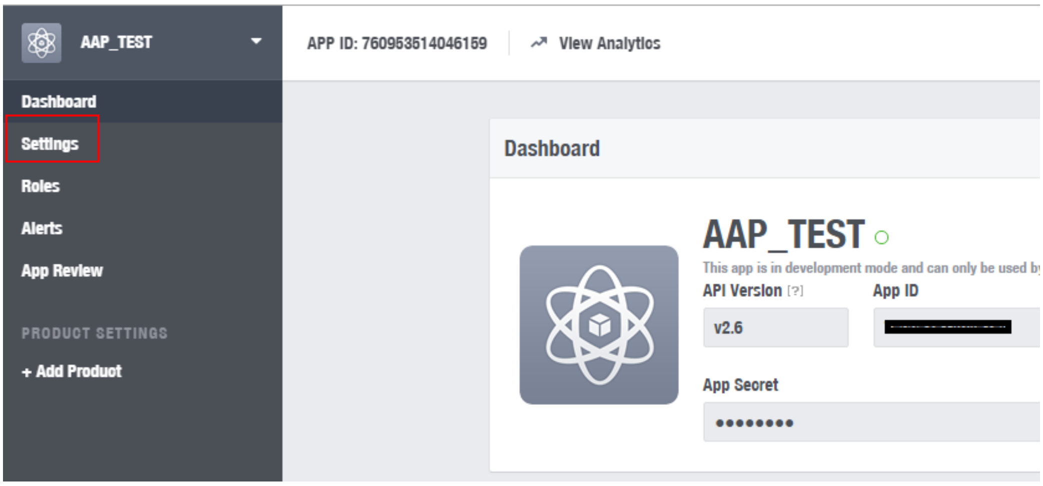
Used for important communication about your app

Category

Choose a Category ▾

By prooeedlng, you agree to the Faoebook Platform Pollcles

Step.4 Please click **"Setting"** and add Platform



APP ID: 760953614046159

Dashboard

AAP_TEST

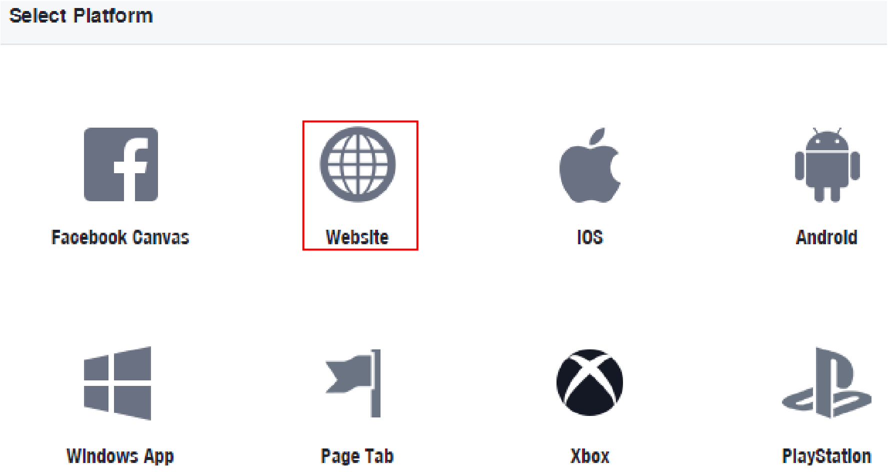
This app is in development mode and can only be used b

API Version [?]: v2.6

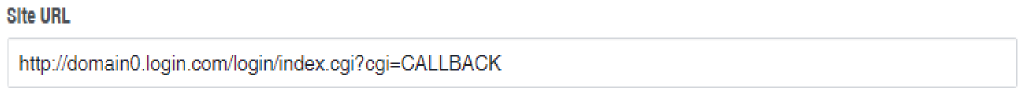
App ID: [redacted]

App Secret: ••••••••

Step.5 Select Platform for "**Website**"



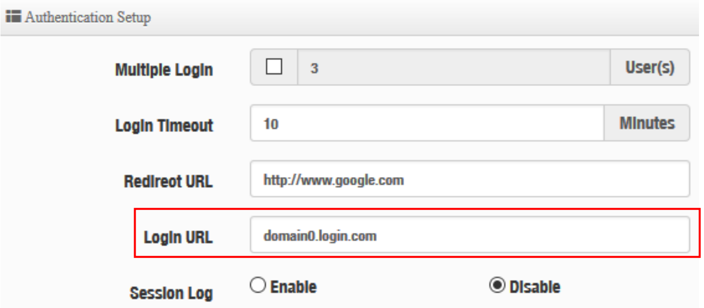
Step.6 Enter URL is **http://domain0.login.com/login/index.cgi?cgi=CALLBACK**



Site URL: http://domain0.login.com/login/index.cgi?cgi=CALLBACK

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

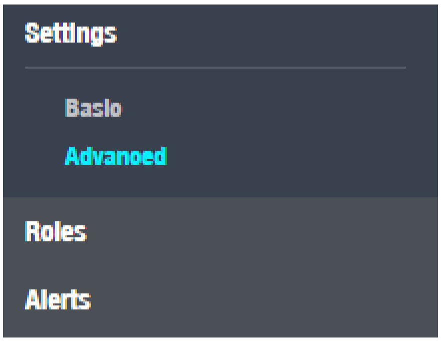


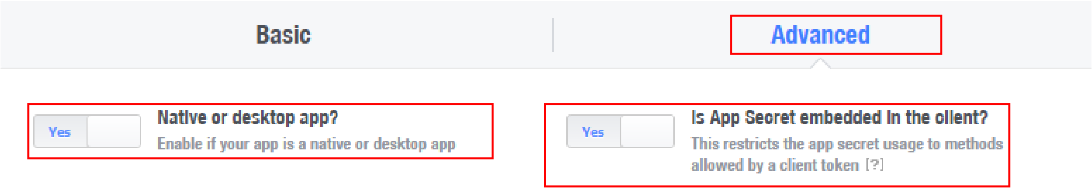
Authentication Setup

Multiple Login	☐ 3	User(s)
Login Timeout	10	Minutes
Redirect 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? "**

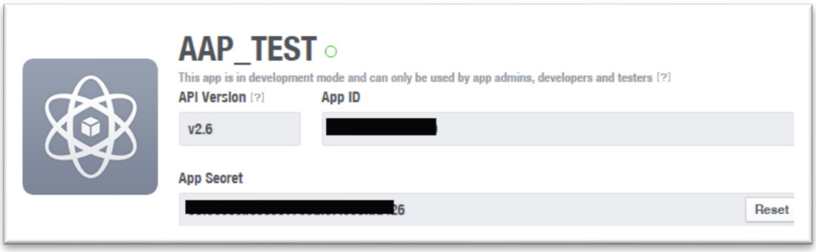




Yes — Native or desktop app?
Enable if your app is a native or desktop app

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.



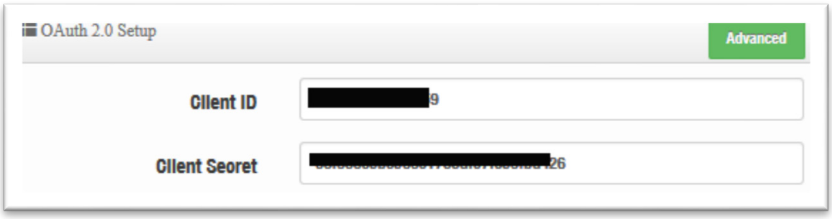
AAP_TEST ○

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]



OAuth 2.0 Setup

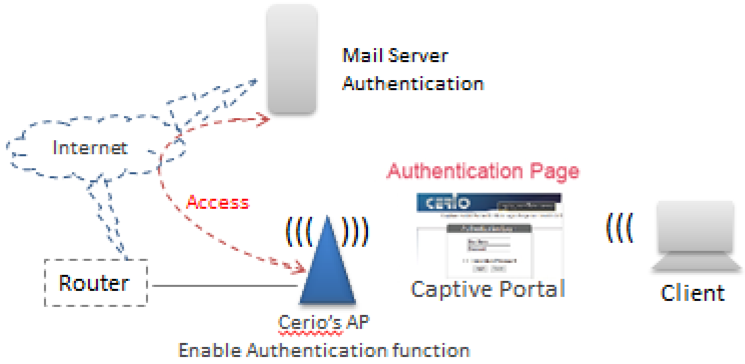
Client ID	[redacted]
Client Secret	[redacted]

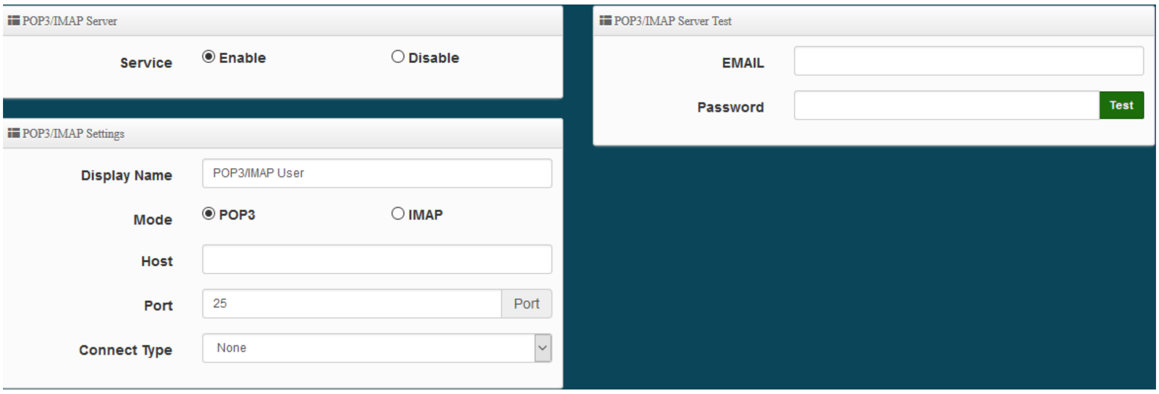
Notice

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.

# POP3/IMAP Server

The purpose of this integrated function is to allow clients to link a POP3 server for receiving emails from a remote server.





POP3/IMAP Server

Service	● Enable	○ Disable

POP3/IMAP Settings

Display Name	POP3/IMAP User	
Mode	● POP3	○ IMAP
Host		
Port	25	Port
Connect Type	None	

POP3/IMAP Server Test

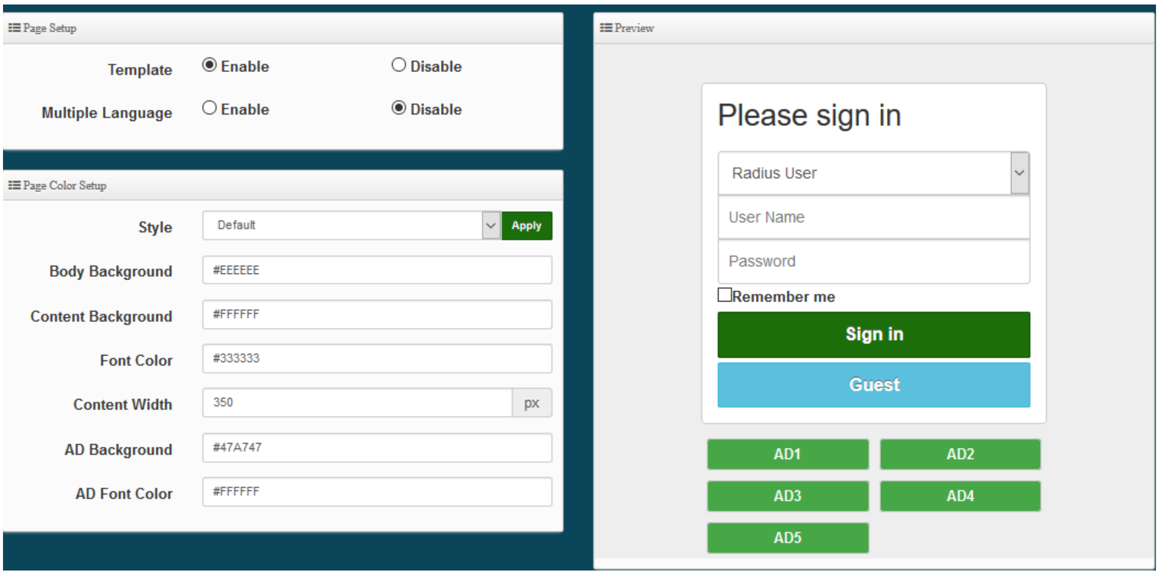
EMAIL	
Password	

- **Service:** Administrator can choose Enable or Disable the PoP3 authentication.
- **Display Name**：Set the "Display Name" based on the appropriate POP3 user or client.

- **Host :** Define the desired Host server name.
- **Port :** Input the proper port number for the corresponding server.
- **Connect Type :** Select the Connect type with options of “STARTTLS”, “SSL/TTL”, or “None”.
- **POP3 Server Test :** Use this tool to test if the POP3 server is operating correctly with your selected email

# Customize Page

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



Page Setup

Template	◉ Enable	○ Disable
Multiple Language	○ Enable	◉ Disable

Page Color Setup

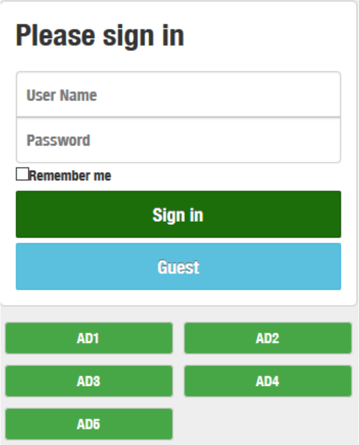
Style	Default Apply
Body Background	#EEEEEE
Content Background	#FFFFFF
Font Color	#333333
Content Width	350 px
AD Background	#47A747
AD Font Color	#FFFFFF

Preview

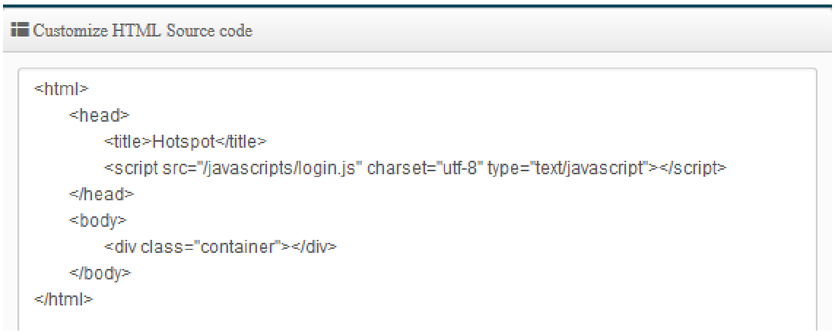
Page Setup

➢ **Template** : Administrator can select Enable or disable.

- Select enable to active default Login Page



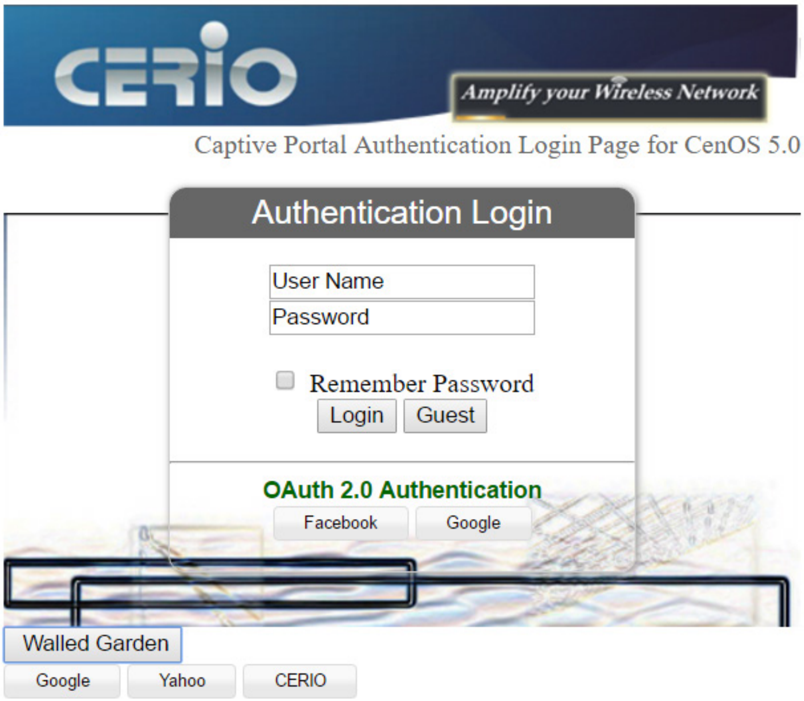
- Select disable to active HTML Source code window for customization



Customize HTML Source code

```
<html>
    <head>
        <title>Hotspot</title>
        <script src="/javascripts/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)*

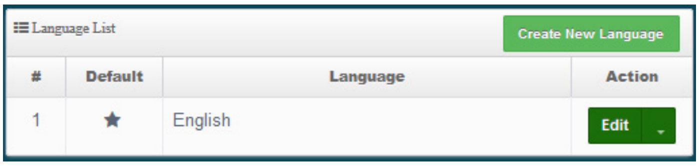


The following function uses the enabled Template

- **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.

# Language

Administrator can create other language for login page.

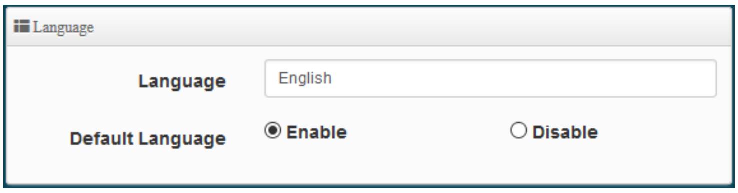


☰ Language List

Create New Language

#	Default	Language	Action
1	★	English	Edit ⌄

Click “Create New Language” button go to add or edit language for login page.



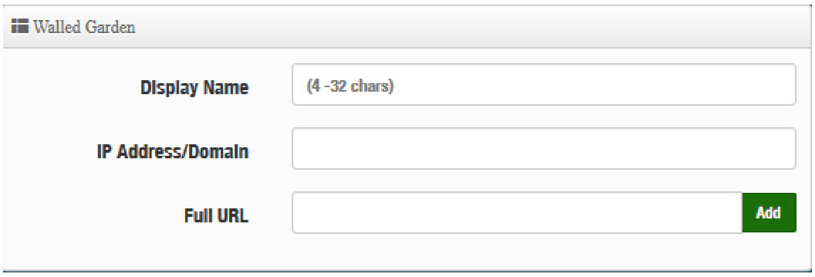
☰ Language

Language	English
Default Language	● Enable ○ Disable

- ➢ Language: Set description of language.
- ➢ Default Language: Display default language.

# 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.



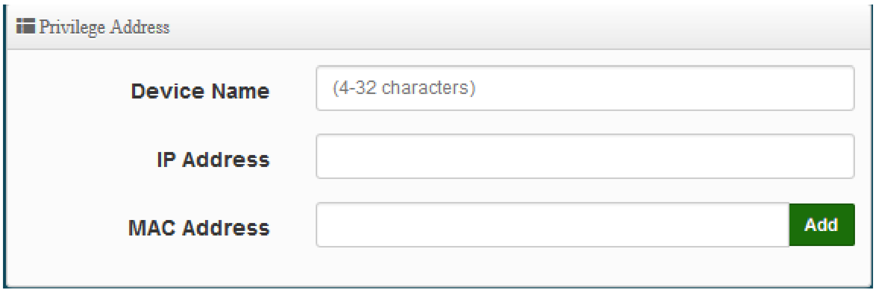
☰ Walled Garden

Display Name	(4 -32 chars)
IP Address/Domain	
Full URL	Add

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

# 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:

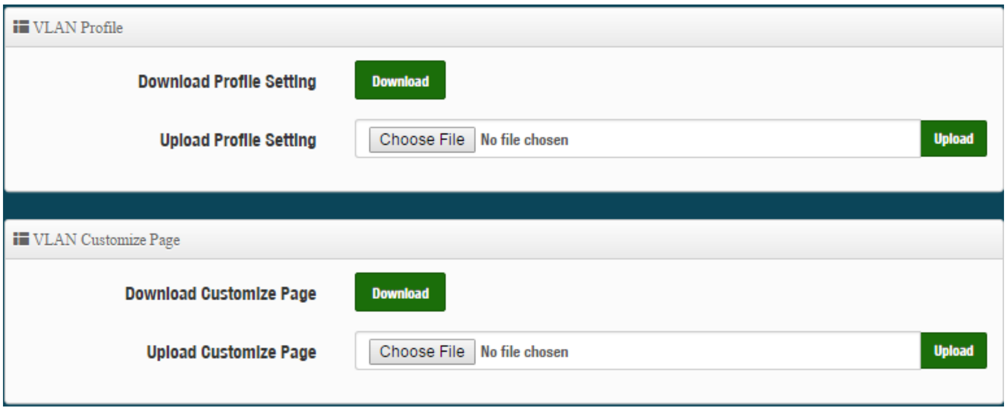
MAC Address:

- **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.

After the above function is setup, please click "**Save**" button and **reboot** system will apply new profile and working normally.

# 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

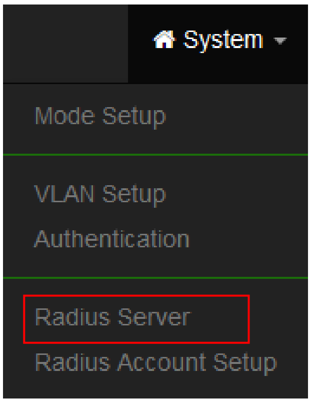
VLAN Customize Page

Download Customize Page

Upload Customize Page: No file chosen

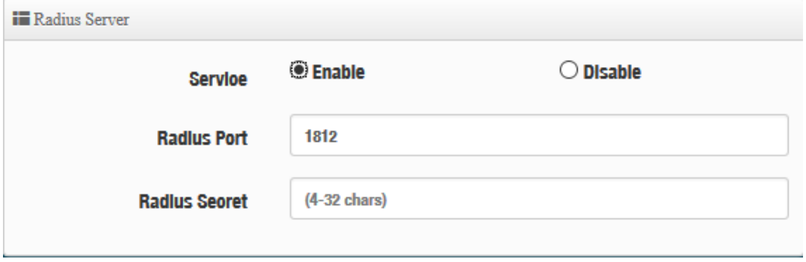
Click “**Save”** button to save your changes. Then click **Reboot** button to activate your changes.

3.3 RADIUS Server



Notice

This function only used to operate in **Access Point** mode.


Radius Server

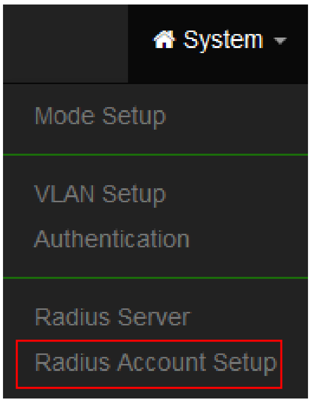
Service	● Enable	○ Disable
Radius Port	1812	
Radius Secret	(4-32 chars)	

- ➢ **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.

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

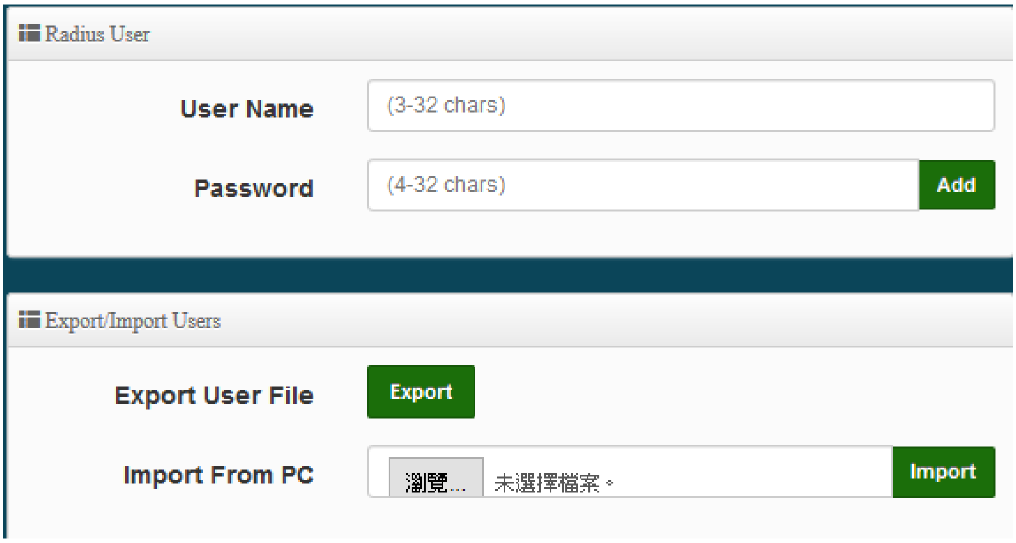
3.4 RADIUS Account Setup

When enabled RADIUS Server, administrator can add RADIUS account and password in the function. But also can recover or backup the RADIUS account. Account can create 50 users limit



Notice

This function only used in **Access Point** mode.



Radius User

User Name	(3-32 chars)
Password	(4-32 chars) Add

Export/Import Users

Export User File	Export
Import From PC	瀏覽... 未選擇檔案。 Import

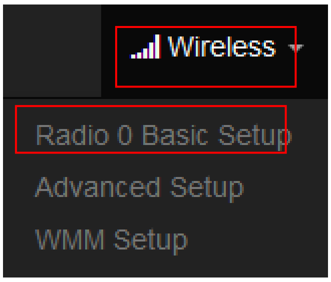
- **User Name**：Create users name for RADIUS account.
- **Password**：Enter password for user name.
- **Export User File**：Administrator can export account list in RADIUS Server.
- **Import From PC**：Administrator can import account list to the RADIUS Server.

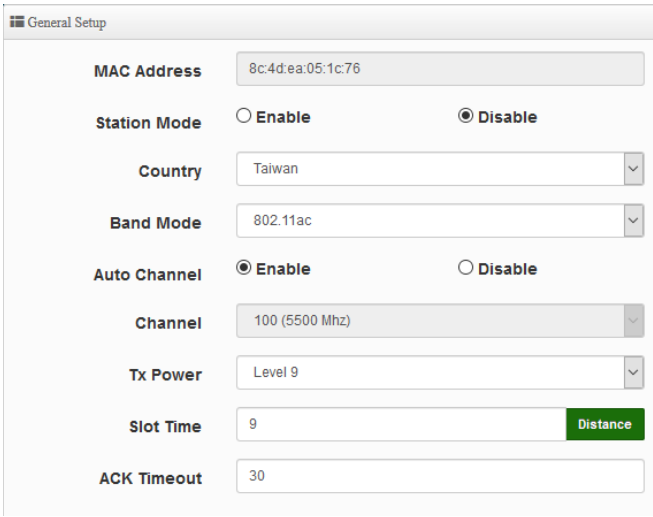
Click **"Save"** button to save your set function. Then click Reboot button to activate your changes.

3.5 Wireless Configuration

This wireless functions administrator can set radio 0 (5G) application of the Access Point.

3.5.1 Radio 0 Basic Setup





General Setup

MAC Address	8c:4d:ea:05:1c:76	
Station Mode	○ Enable	● Disable
Country	Taiwan	
Band Mode	802.11ac	
Auto Channel	● Enable	○ Disable
Channel	100 (5500 Mhz)	
Tx Power	Level 9	
Slot Time	9	Distance
ACK Timeout	30	

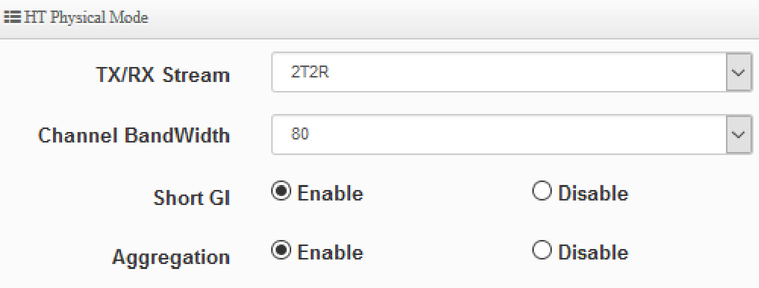
- **MAC Address:** Display 5G WiFi MAC address.
- **Country:** Administrator can select country: US or EU or Taiwan.
- **Band Mode:** Administrator can select 5G Band for 802.11a/n or 802.11ac. The default is 802.11ac
- **Auto Channel:** Administrator can Enable or Disable the function. If select disabled 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 Timout :** You can enter the slot time value here. When the distance is long or short, the waiting time for packet transmission will be adjusted fast and slow.

  Distance: When the "Distance" button is clicked, the point-to-point bridge distance can be entered. The system will automatically calculate the ideal reference value for the Slot Time and ACK Timeout. The input distance is calculated in units (meters).
- **ACK Timout :** When waiting for the "ACKnowledgment frame" interval is too long to be received, the ACK will be retransmitted. A higher ACK Timeout will reduce packet loss, but the transmission efficiency will be poor.

Notice

Setting Slot Time and ACK Timeout can strengthen the long-distance connection. Changing the value can optimize the setting. If the value is too low, the length transmission will be reduced. If the value is too high, there may be disconnection.

HT Physical Mode



HT Physical Mode

TX/RX Stream	2T2R	
Channel BandWidth	80	
Short GI	● Enable	○ Disable
Aggregation	● Enable	○ Disable

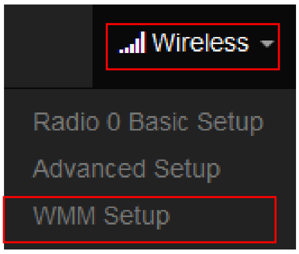
- **TX/RX Stream:** Administrator can select 1 or 2 TX/RX. The default is 2TX/2RX. If administratior adopt model is OW-200 A1 and select use 1Tx/1Rx funciton then please note external N-type connector only one have signal output, as shown below.

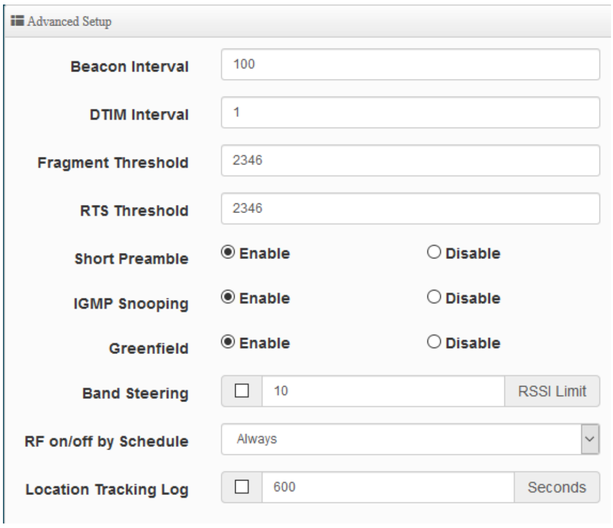
This N-type is main signal output power

- **Channel Bandwidth:** The "**20/40 and 802.11ac 80**" MHz option is usually the best. The other option is available for special circumstances.
- **Shout 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.

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

3.5.2 Advanced Setup





Advanced Setup

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
RF on/off by Schedule	Always	
Location Tracking Log	□ 600	Seconds

- **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

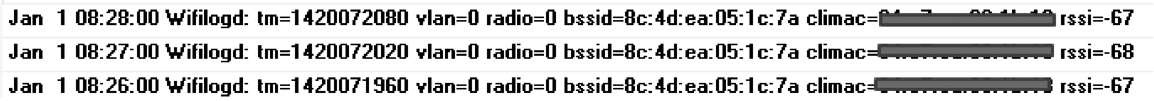
next actions if the information from AP matches the requirement. Beacon is sent on a periodic basis, the time interval can be adjusted.

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. Let's 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.
- **RF on/off by schedule:** Administrator can apply Time Policy to on or off wireless signal.
- **Location Tracking Log:** The system can detect the signal strength of the wireless client to determine the location of the Access Point and send to database.



```
Jan  1 08:28:00 Wifilogd: tm=1420072080 vlan=0 radio=0 bssid=8c:4d:ea:05:1c:7a climac=[redacted] rssi=-67
Jan  1 08:27:00 Wifilogd: tm=1420072020 vlan=0 radio=0 bssid=8c:4d:ea:05:1c:7a climac=[redacted] rssi=-68
Jan  1 08:26:00 Wifilogd: tm=1420071960 vlan=0 radio=0 bssid=8c:4d:ea:05:1c:7a climac=[redacted] rssi=-67
```

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

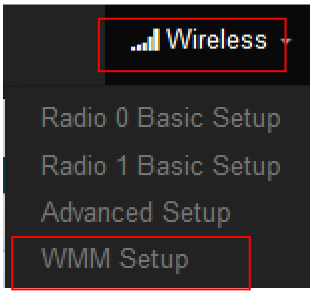
3.5.3 WMM Setup

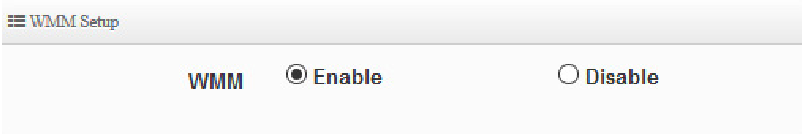
This affects traffic flowing from the access point to the client station.

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.

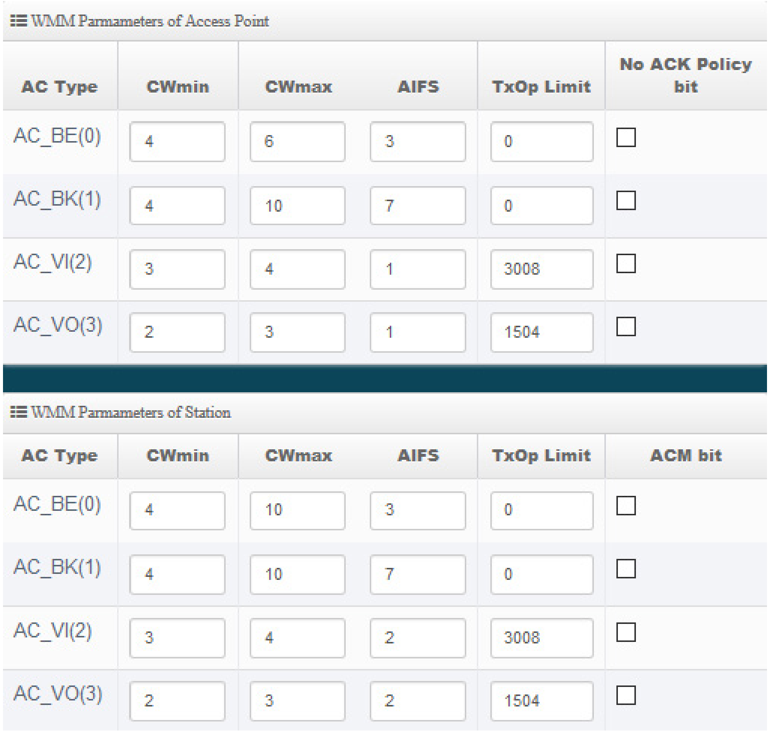
As an Example, time-sensitive Voice & Video, and multimedia are given effectively higher priority for transmission (lower wait times for channel access), while other applications and traditional IP data which are less time-sensitive but often more data-intensive are expected to tolerate longer wait times.

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





WMM ● Enable ○ Disable



☷ WMM Parmameters of Access Point

AC Type	CWmin	CWmax	AIFS	TxOp Limit	No ACK Policy bit
AC_BE(0)	4	6	3	0	□
AC_BK(1)	4	10	7	0	□
AC_VI(2)	3	4	1	3008	□
AC_VO(3)	2	3	1	1504	□

☷ WMM Parmameters of Station

AC Type	CWmin	CWmax	AIFS	TxOp Limit	ACM bit
AC_BE(0)	4	10	3	0	□
AC_BK(1)	4	10	7	0	□
AC_VI(2)	3	4	2	3008	□
AC_VO(3)	2	3	2	1504	□

- **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

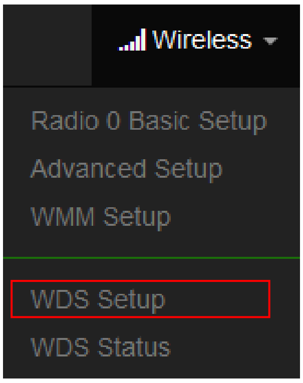
is reached. Once the Maximum Contention Window size is reached, retries will continue until a maximum number of retries allowed is reached. Valid values for the "cwmax" are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024. The value for "cwmax" must be higher than the value for "cwmin". 。

- **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 uncast packet.

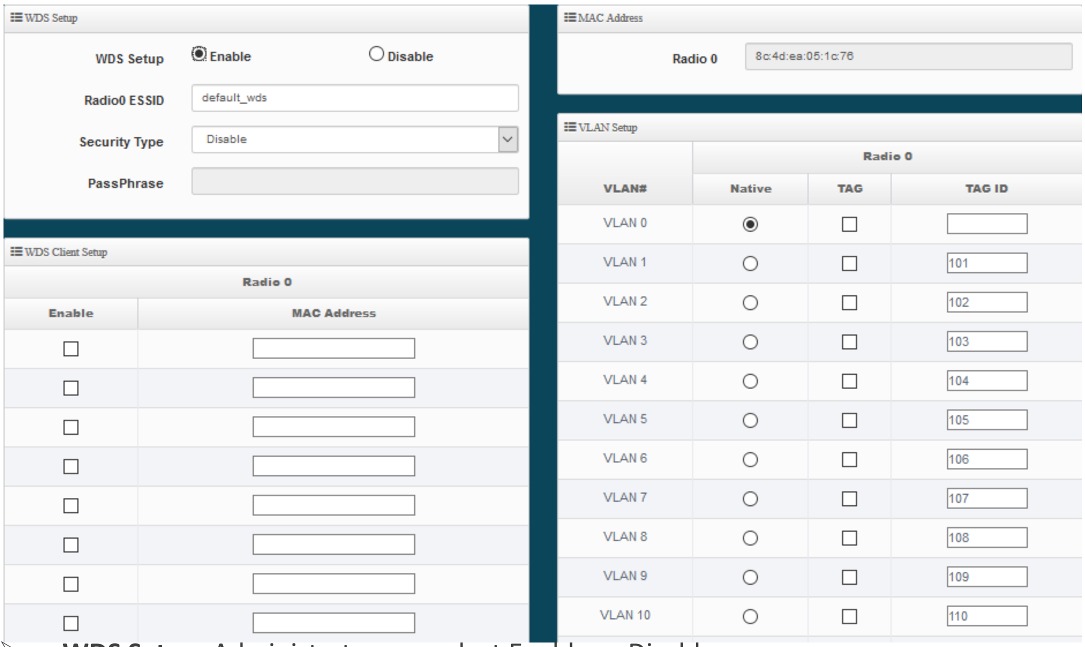
Click **"Save"** button to save your set function. Then click "Reboot" button to activate your changes.

3.5.4 WDS Setup

Please click on Wireless -> 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 5G radio and can support VLAN tag pass through



WDS Setup

WDS Setup	● Enable	○ Disable
Radio0 ESSID	default_wds	
Security Type	Disable	
PassPhrase		

WDS Client Setup

	Radio 0
Enable	MAC Address
□	
□	
□	
□	
□	
□	
□	
□	

MAC Address

Radio 0	8c:4d:ea:05:1c:76

VLAN Setup

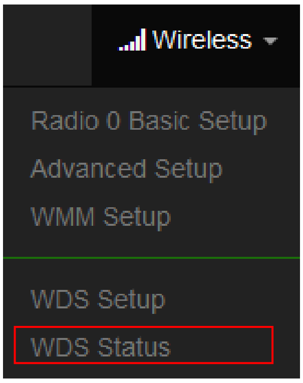
	Radio 0		
VLAN#	Native	TAG	TAG ID
VLAN 0	●	□	
VLAN 1	○	□	101
VLAN 2	○	□	102
VLAN 3	○	□	103
VLAN 4	○	□	104
VLAN 5	○	□	105
VLAN 6	○	□	106
VLAN 7	○	□	107
VLAN 8	○	□	108
VLAN 9	○	□	109
VLAN 10	○	□	110

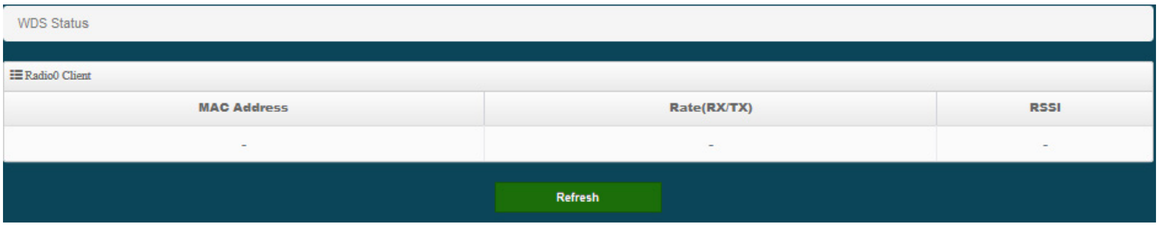
- **WDS Setup:** Administrator can select Enable or Disable.
- **Authentication:** Administrator can use AES security.
- **WDS Client Setup:** Administrator can used 5G for WDS Links. A Single Radio supports up to 8 WDS links.
- **VLAN Setup:** The WDS aisle support Multi-tag VALN

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

3.5.5 WDS Status

Displays 5G radio WDS link status through MAC and Date (TX/RX)
Please click on **Wireless -> WDS status**





WDS Status

Radio0 Client

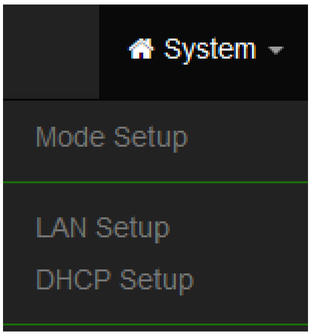
MAC Address	Rate(RX/TX)	RSSI
-	-	-

- **MAC Address**：Display connected MAC Address.。
- **Rate(TX/RX)**：Display Tx/Rx rate of the point to point。
- **RSSI:** Display signal connection value of RSSI

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

4. Client Bridge Mode

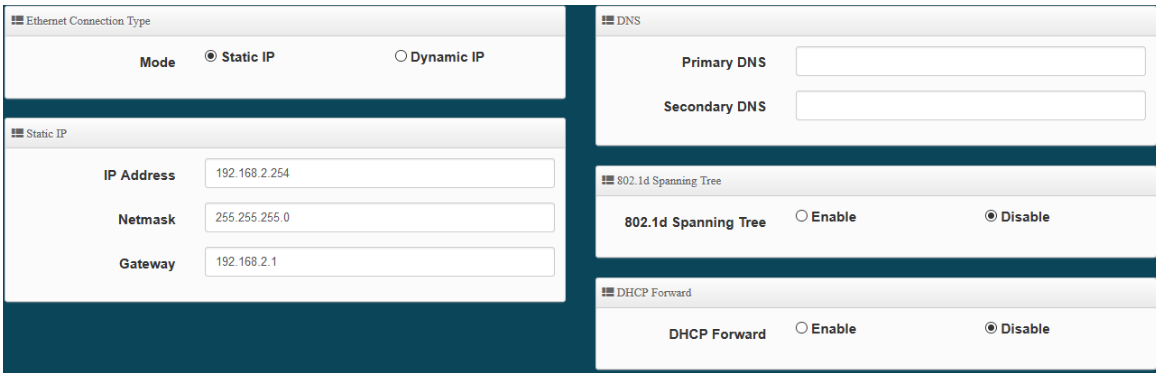
When Client Bridge is chosen, the system can be configured as a Client Bridge and support Repeater AP function. This can setup VLAN and DHCP server in the system menu.



This section provides detailed explanation for users to configure in the Client Bridge Mode and Repeater AP function with help of illustrations.

4.1 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

Static IP

IP Address 192.168.2.254

Netmask 255.255.255.0

Gateway 192.168.2.1

DNS

Primary DNS

Secondary DNS

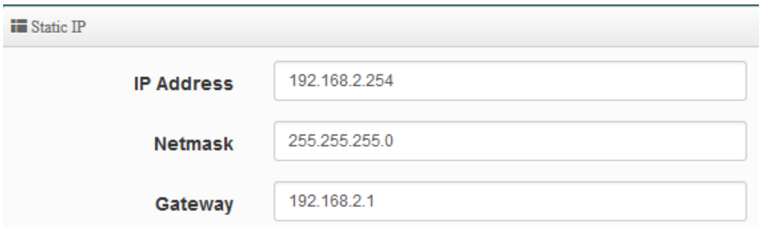
802.1d Spanning Tree

802.1d Spanning Tree ○ Enable ● Disable

DHCP Forward

DHCP Forward ○ Enable ● Disable

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



Static IP

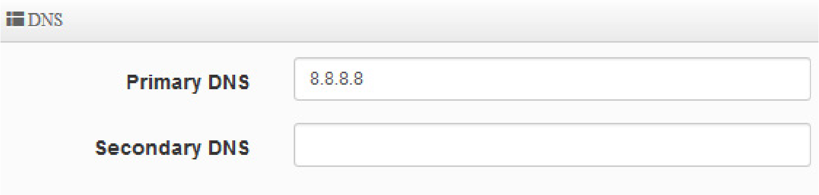
IP Address 192.168.2.254

Netmask 255.255.255.0

Gateway 192.168.2.1

- **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.



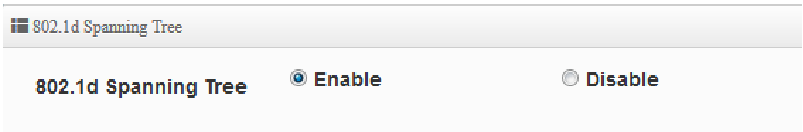
DNS

Primary DNS 8.8.8.8

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 :**

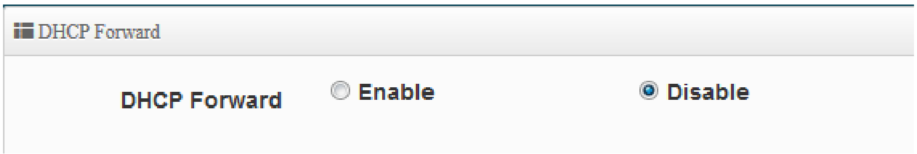


802.1d Spanning Tree

802.1d Spanning Tree ● Enable ○ Disable

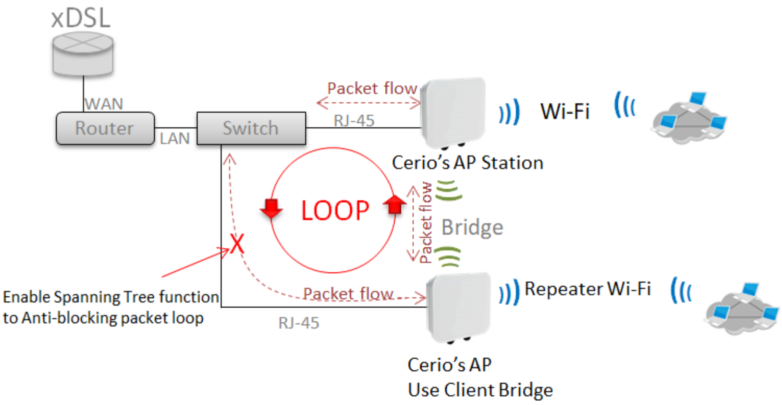
The spanning tree network protocol provides a loop free topology for a bridged LAN between LAN interface and 8 WDS interfaces from wds0 to wds7. The Spanning Tree Protocol, which is also referred to as STP, is defined in the IEEE Standard 802.1d.

- **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

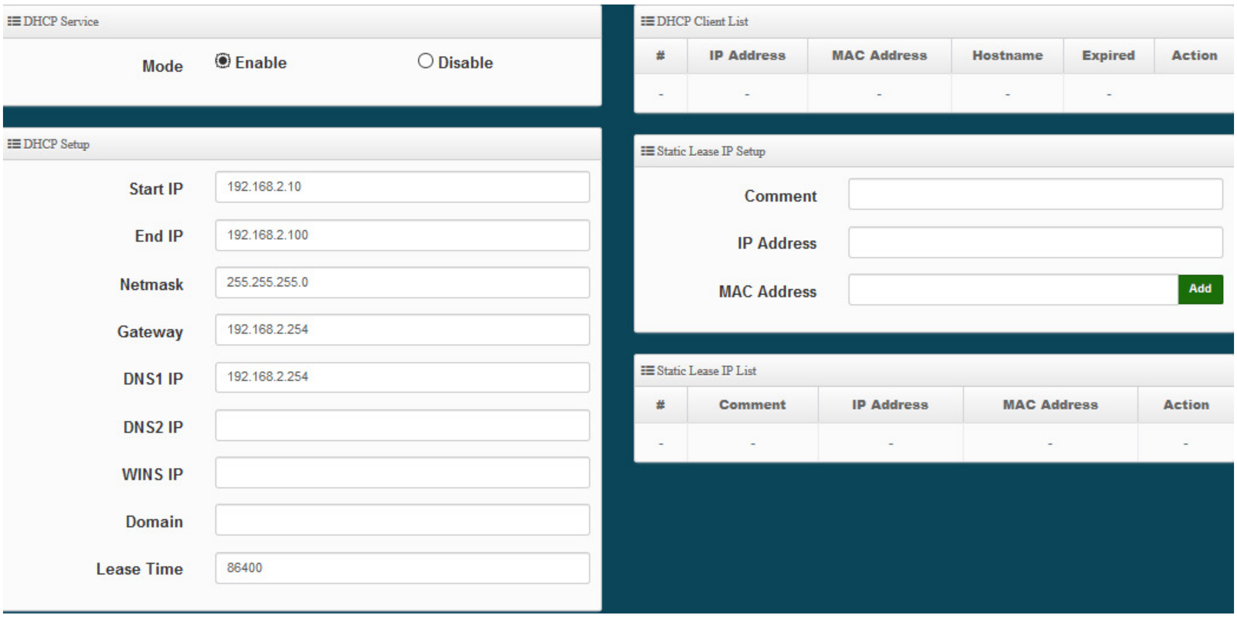
DHCP Forward	○ Enable	● Disable



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

4.2 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	● Enable	○ Disable

DHCP Setup

Start IP	192.168.2.10
End IP	192.168.2.100
Netmask	255.255.255.0
Gateway	192.168.2.254
DNS1 IP	192.168.2.254
DNS2 IP	
WINS IP	
Domain	
Lease Time	86400

DHCP Client List

#	IP Address	MAC Address	Hostname	Expired	Action
-	-	-	-	-	

Static Lease IP Setup

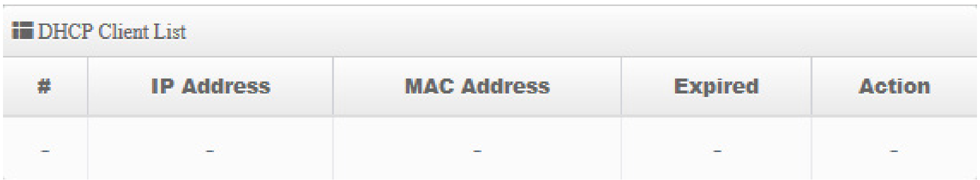
Comment	
IP Address	
MAC Address	

Static Lease IP List

#	Comment	IP Address	MAC Address	Action
-	-	-	-	-

- **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 to CenOS 5.0 AP and use IP address of the DHCP service, the DHCP Client List will display users the information and used IP address.

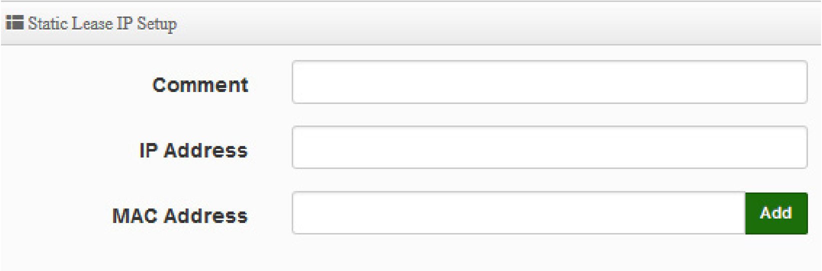


DHCP Client List

#	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.

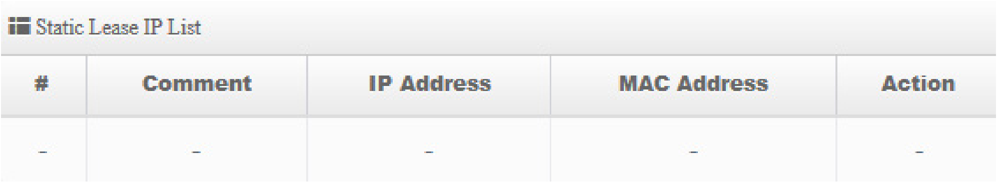


Static Lease IP Setup

Comment	
IP Address	
MAC Address	

- **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.



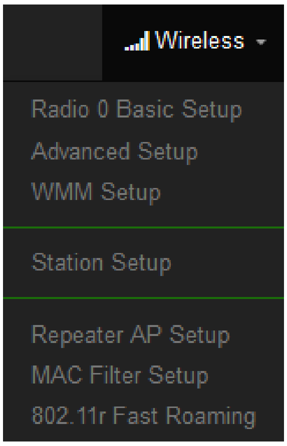
Static Lease IP List

#	Comment	IP Address	MAC Address	Action
-	-	-	-	-

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

4.3 Wireless General Setup

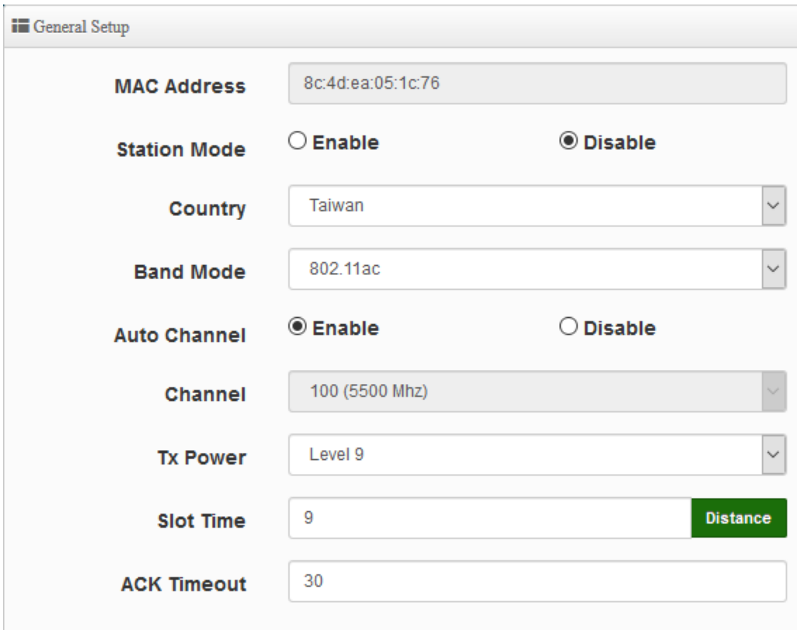
The main setup Client Bridge connection to AP Station and Repeater AP functions setting, MAC filter, WMM and 802.11r/802.11k Fast Roaming etc in wireless menu.



Notice

If want to use Repeater AP function then Clinet Bridge must determine connection to Access Point then Repeater AP can operate normally.

4.3.1 Radio 0 Basic Setup



General Setup

MAC Address	8c:4d:ea:05:1c:76	
Station Mode	○ Enable	● Disable
Country	Taiwan	
Band Mode	802.11ac	
Auto Channel	● Enable	○ Disable
Channel	100 (5500 Mhz)	
Tx Power	Level 9	
Slot Time	9	Distance
ACK Timeout	30	

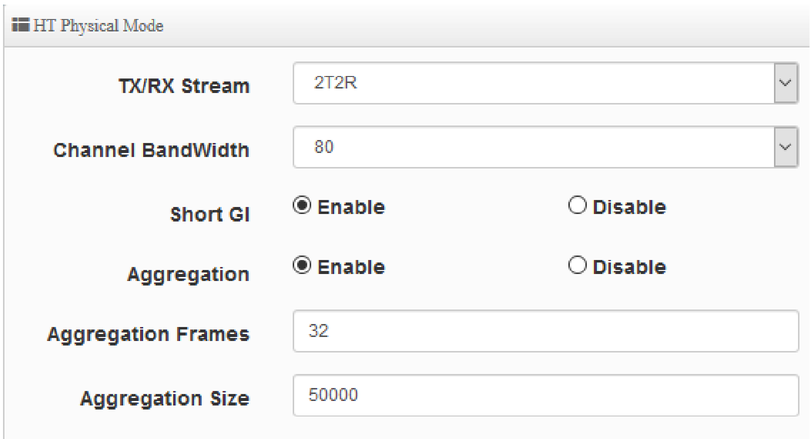
- **MAC Address:** Display radio 1 use MAC address.
- **Country:** Administrator can select country used channel by US / EU and Taiwan.
- **Band Mode:** If Client Bridge want to use 5G link to Access Point then administrator can enable the function (radio 1).
- **Auto Channel:** Administrator can Enable or Disable the function. If select disable function the WiFi channel can be fixed a channel.
- **Channel:** Support US / EU / Taiwan country by 5G Channel.
- **Tx Power:** Administrator can control the WiFi Tx output power. The power Max. Level 9.
- **Slot Timout :** You can enter the slot time value here. When the distance is long or short, the waiting time for packet transmission will be adjusted fast and slow.

  Distance: When the "Distance" button is clicked, the point-to-point bridge distance can be entered. The system will automatically calculate the ideal reference value for the Slot Time and ACK Timeout. The input distance is calculated in units (meters).
- **ACK Timout :** When waiting for the "ACKnowledgment frame" interval is too long to be received, the ACK will be retransmitted. A higher ACK Timeout will reduce packet loss, but the transmission efficiency will be poor.

Notice

Setting Slot Time and ACK Timeout can strengthen the long-distance connection. Changing the value can optimize the setting. If the value is too low, the length transmission will be reduced. If the value is too high, there may be disconnection.

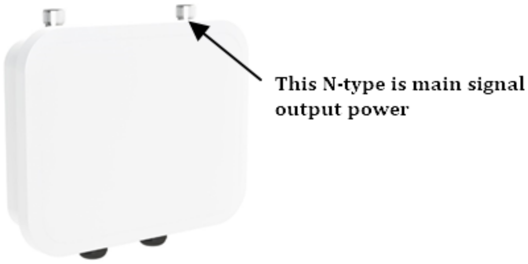
HT Physical Mode



HT Physical Mode

TX/RX Stream	2T2R	
Channel BandWidth	80	
Short GI	● Enable	○ Disable
Aggregation	● Enable	○ Disable
Aggregation Frames	32	
Aggregation Size	50000	

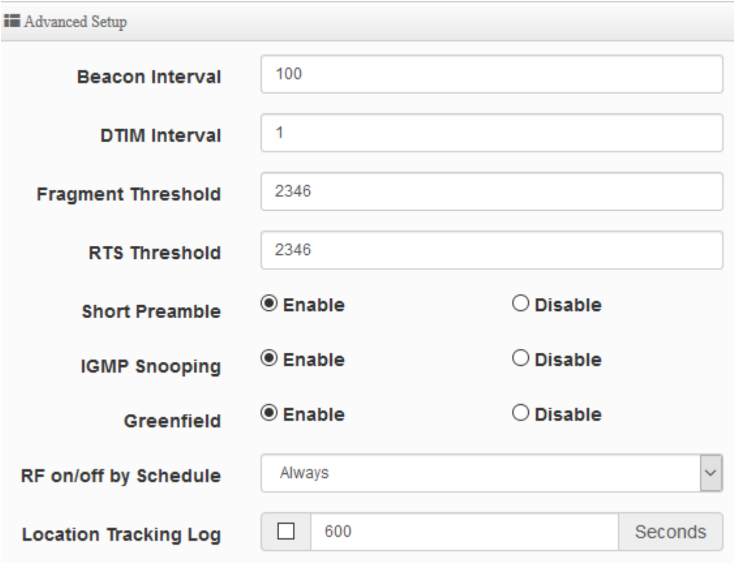
- **TX/RX Stream:** Administrator can select 1 or 2 TX/RX. The default is 2TX/2RX. If administratior adopt model is OW-200 A1 and select use 1Tx/1Rx funciton then please note external N-type connector only one have signal output, as shown below.



- **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:** Set frames size of Aggregation, the size recommend use default value is 32.
- **Aggregation Size:** Set aggregation size, the size recommends use default value is 500000.

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

4.3.2 Advanced Setup



Advanced Setup

Beacon Interval	100	
DTIM Interval	1	
Fragment Threshold	2346	
RTS Threshold	2346	
Short Preamble	● Enable	○ Disable
IGMP Snooping	● Enable	○ Disable
Greenfield	● Enable	○ Disable
RF on/off by Schedule	Always	
Location Tracking Log	□ 600	Seconds

- **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.

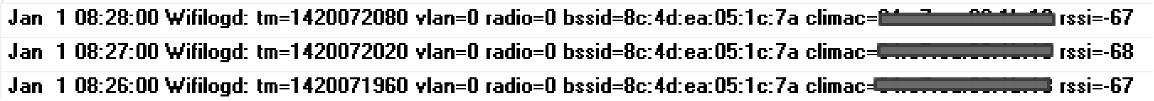
- **RTS Threshold:** TRTS Threshold is in the range of **1~2347** byte. The default is **2347** byte.

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.
- **RF on/off by Schedule:** When system enable and set time policy function then RF on/off can apply time policy in the function.(Time Policy function set please go to system ➔ Time Policy)
- **Location Tracking Log:** This feature can provides information to third-party positioning systems.



```
Jan  1 08:28:00 Wifilogd: tm=1420072080 vlan=0 radio=0 bssid=8c:4d:ea:05:1c:7a climac=[redacted] rssi=-67
Jan  1 08:27:00 Wifilogd: tm=1420072020 vlan=0 radio=0 bssid=8c:4d:ea:05:1c:7a climac=[redacted] rssi=-68
Jan  1 08:26:00 Wifilogd: tm=1420071960 vlan=0 radio=0 bssid=8c:4d:ea:05:1c:7a climac=[redacted] rssi=-67
```

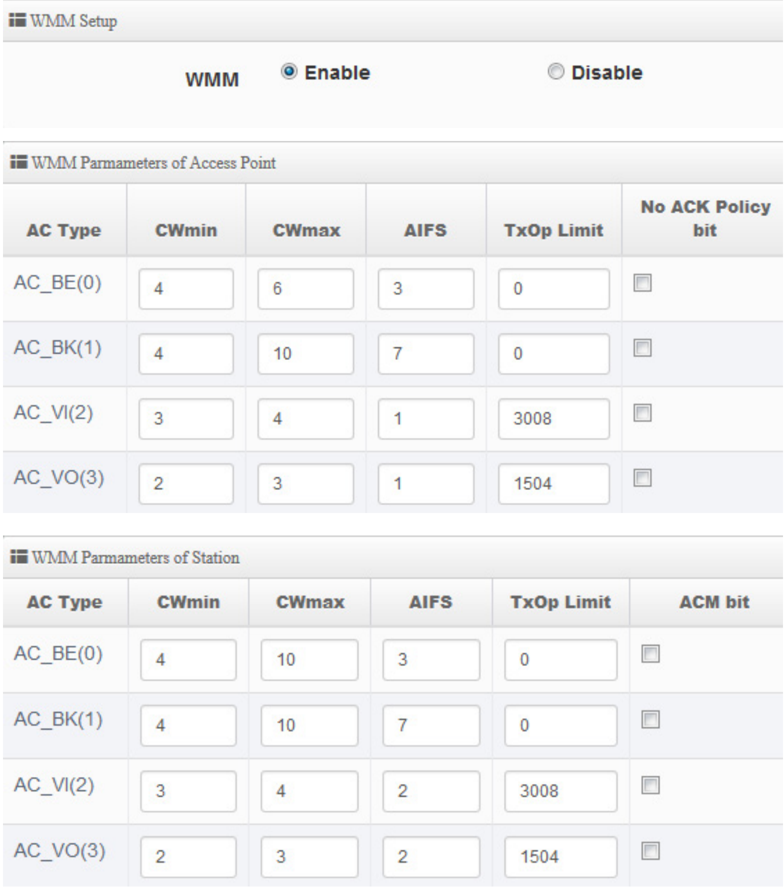
Click **"Save"** button to save your set function. Then click "Reboot" button to activate your changes.

4.3.3 WMM Setup

His 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 Parmameters of Access Point

AC Type	CWmin	CWmax	AIFS	TxOp Limit	No ACK Policy bit
AC_BE(0)	4	6	3	0	□
AC_BK(1)	4	10	7	0	□
AC_VI(2)	3	4	1	3008	□
AC_VO(3)	2	3	1	1504	□

WMM Parmameters of Station

AC Type	CWmin	CWmax	AIFS	TxOp Limit	ACM bit
AC_BE(0)	4	10	3	0	□
AC_BK(1)	4	10	7	0	□
AC_VI(2)	3	4	2	3008	□
AC_VO(3)	2	3	2	1504	□

- **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.

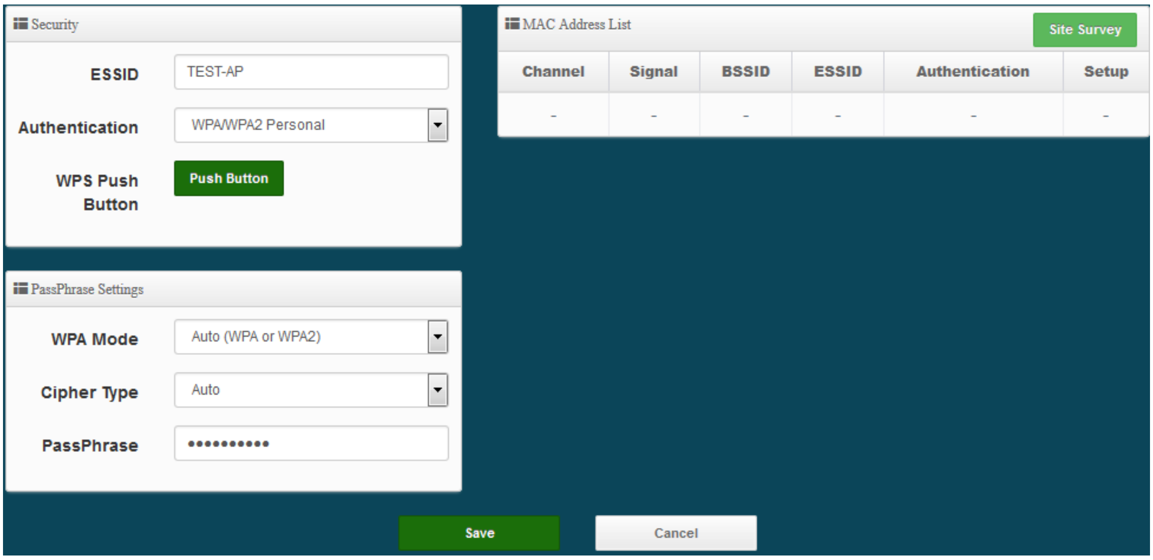
While the No ACK policy helps improve transmission efficiency, it can cause increased packet loss when communication quality deteriorates. This is because when this policy is used, a sender does not retransmit packets that have not been received by the recipient.

When the Normal ACK policy is used, the recipient acknowledges each received uncast packet. ◦

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

4.3.4 Station Setup

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



Security

ESSID: TEST-AP

Authentication: WPA/WPA2 Personal

WPS Push Button: Push Button

PassPhrase Settings

WPA Mode: Auto (WPA or WPA2)

Cipher Type: Auto

PassPhrase: ••••••••••

MAC Address List

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

- ➢ **MAC Address List:** The function can discovery AP Station and select want to link the AP station, please click site survey button.
- ➢ **Security:** After site survey AP station complete will list all AP station, when click AP station setup button then AP station information (ESSID/Security type) will display on page.
- ➢ **PassPhrase Settings:** Administrator need manual set correct ESSID security/Cipher type and pass phrase.

Notice

If Security/Cipher selected or set PassPhrase is wrong, it will not be able to bridge normally.

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

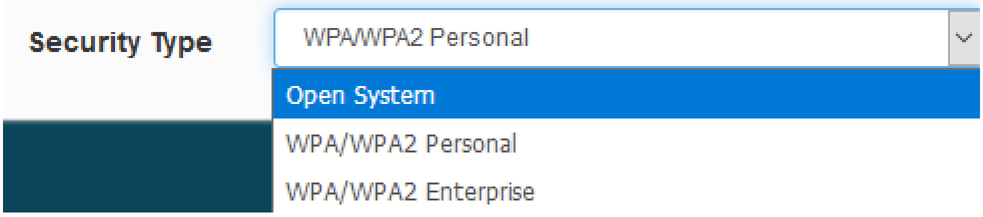
4.3.5 Repeater AP Setup

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

Notice

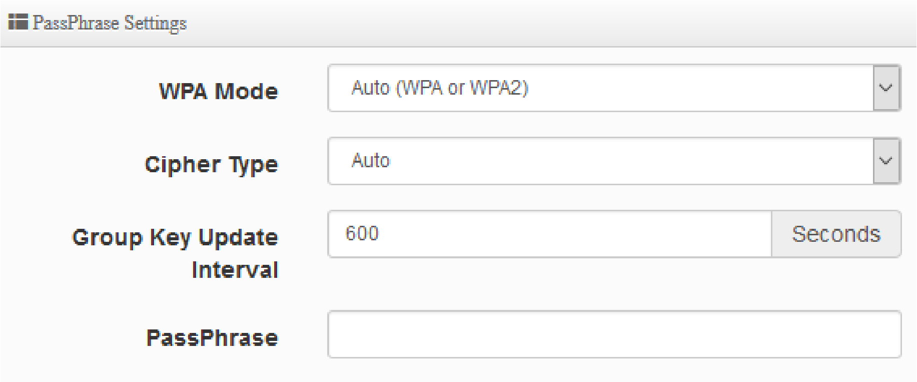
1. If want to use Repeater AP function then Clinet Bridge must determine connection to Access Point then Repeater AP can operate normally.
2. The default is enabling of Repeater AP. If want to used pure Client Bridge will can disable it.

- **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 is 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.



Security Type: WPA/WPA2 Personal

- **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	

- ✓ **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.

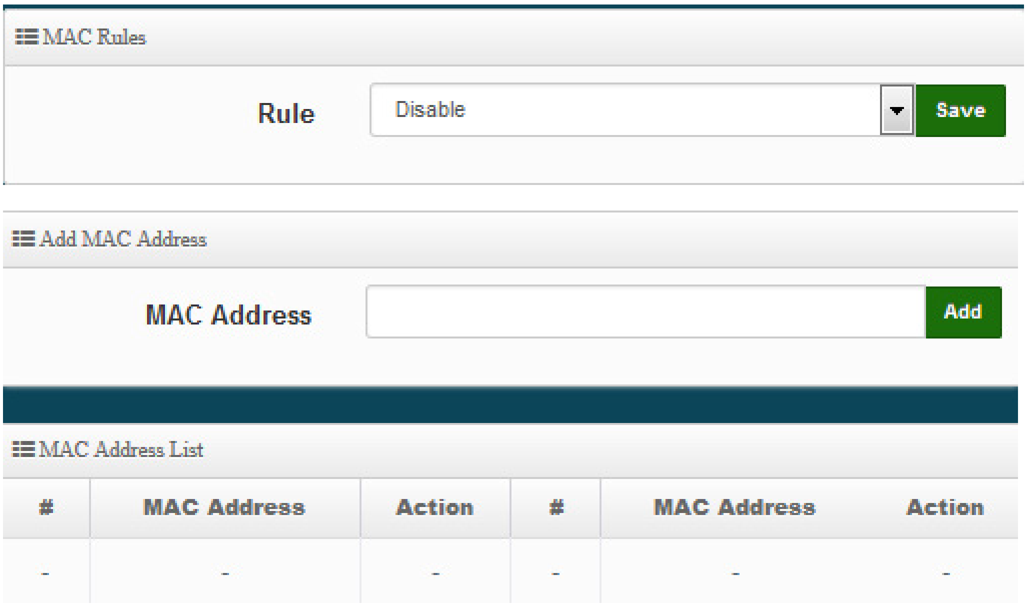
  AES is short for "**Advanced Encryption Standard**", The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plaintext into the final output of ciphertext. Each round consists of several processing steps, including one that depends on the encryption key. 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.

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

4.3.6 MAC Filter Setup

Administrator can setup allow or reject WiFi clients (MAC address) to access Repeater AP.



MAC Rules

Rule: Disable

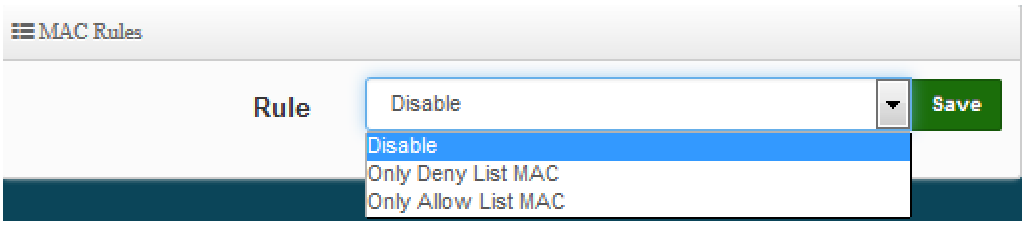
Add MAC Address

MAC Address

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: Disable

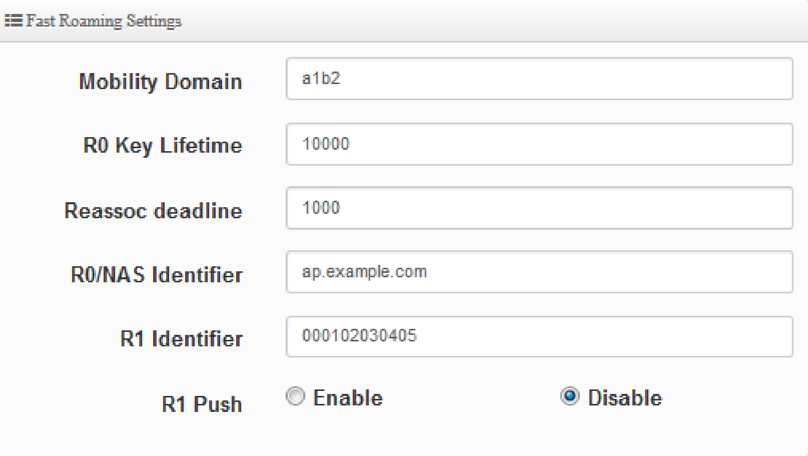
- ● **Only Allow List MAC**: Define certain wireless clients in the list which will have granted access to the Access Point while the access will be denied for all the remaining clients – Action Type is set to "**Only Allow List MAC**".
- ● **Only Deny List MAC**: Define certain wireless clients in the 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.

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

4.3.7 802.11r Fast Roaming Setup

The system support 802.11r/802.11k function for 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.



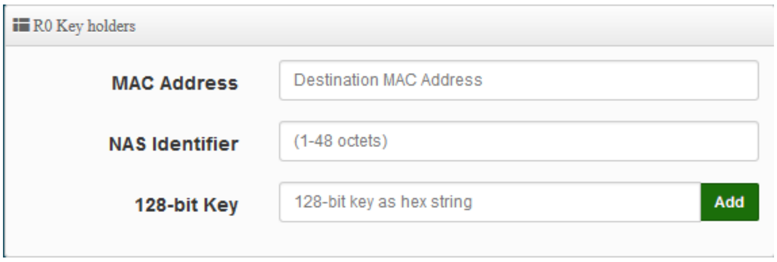
Fast Roaming Settings

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.



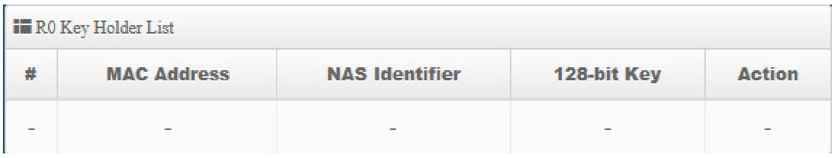
R0 Key holders

MAC Address	Destination MAC Address
NAS Identifier	(1-48 octets)
128-bit Key	128-bit key as hex string

- **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.

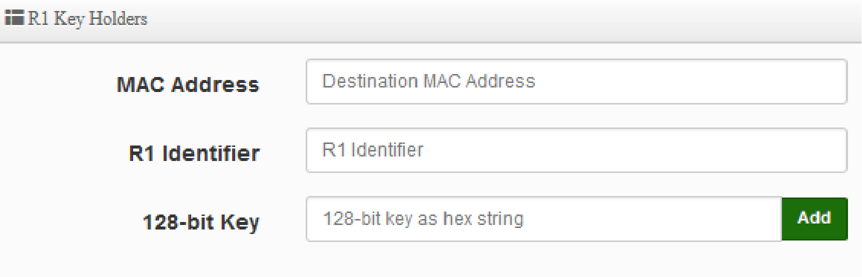


R0 Key Holder List

#	MAC Address	NAS Identifier	128-bit Key	Action
-	-	-	-	-

R1 Key Holder List:

Enter a unified set of R1 Key Holder identification certification.



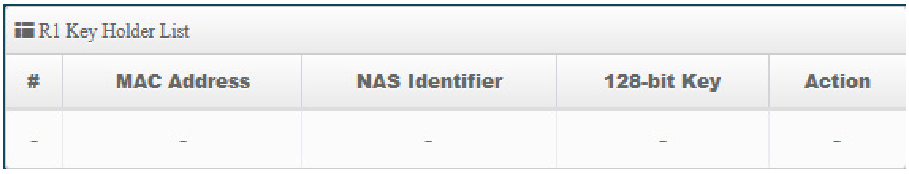
R1 Key Holders

MAC Address	Destination MAC Address
R1 Identifier	R1 Identifier
128-bit Key	128-bit key as hex string

- **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.

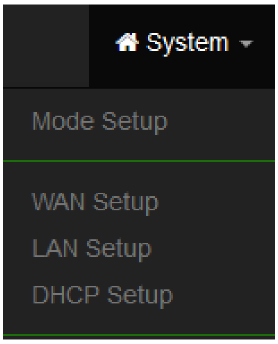


R1 Key Holder List

#	MAC Address	NAS Identifier	128-bit Key	Action
-	-	-	-	-

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

5. WISP Mode

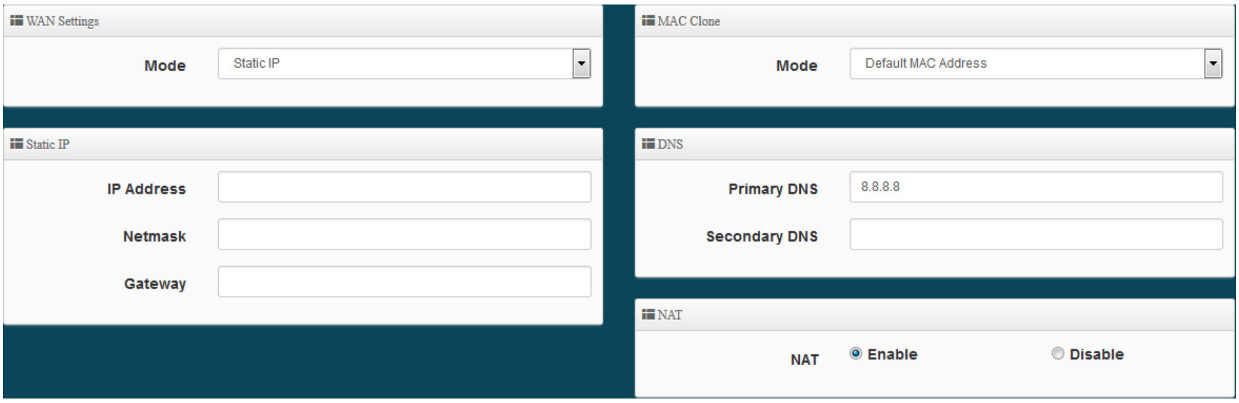


WISP Mode is a router function, if the Telecom company permits wireless connection to their WAN, administrators can change the CenOS 5.0 AP to WISP Mode to connect to the wifi network.

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

5.1 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.



WAN Settings

Mode: Static IP

Static IP

IP Address:

Netmask:

Gateway:

MAC Clone

Mode: Default MAC Address

DNS

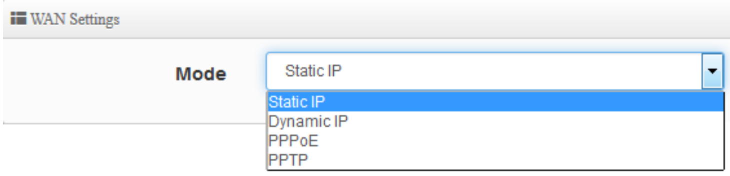
Primary DNS: 8.8.8.8

Secondary DNS:

NAT

NAT: ● Enable ○ Disable

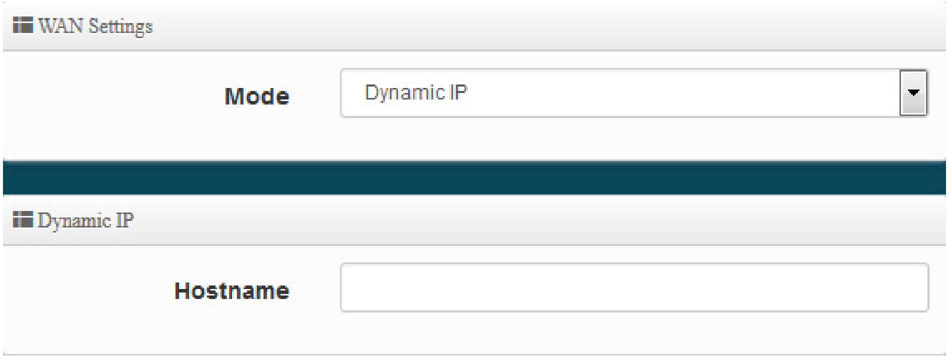
WAN Setting



WAN Settings

Mode: Static IP

- **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.



WAN Settings

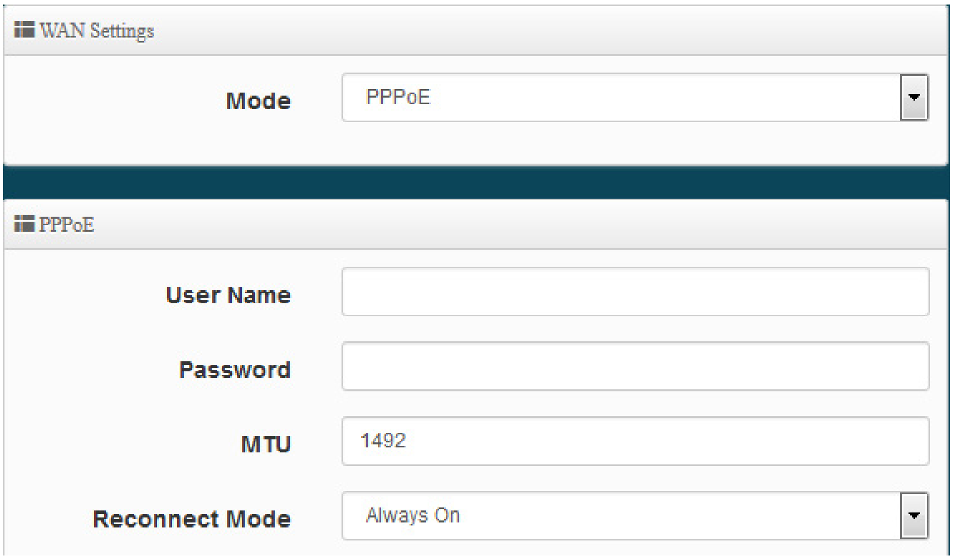
Mode: Dynamic IP

Dynamic IP

Hostname:

- **Hostname :** The Hostname of the WAN port

➢ **PPPoE :** To create wireless PPPoE WAN connection to a PPPoE server in network.



WAN Settings

Mode: PPPoE

PPPoE

User Name:

Password:

MTU: 1492

Reconnect Mode: Always On

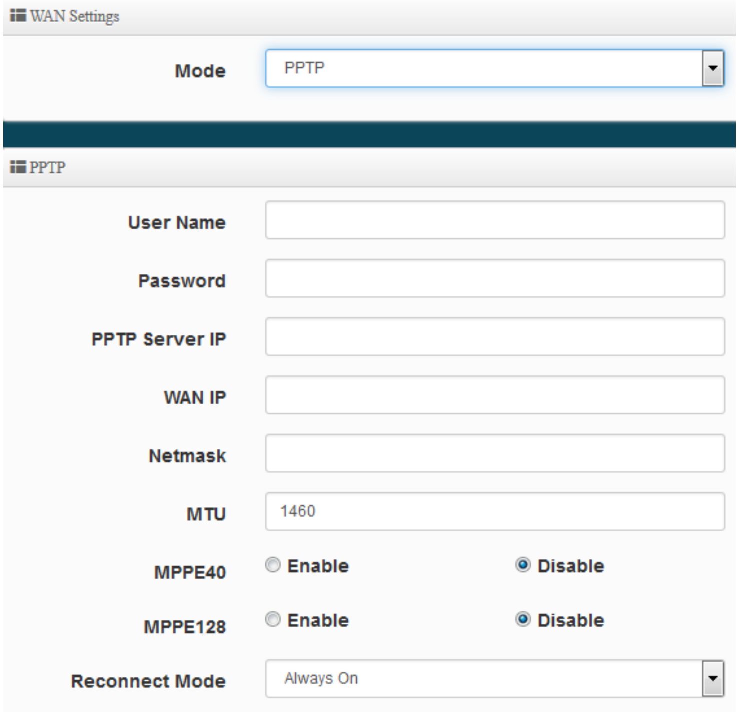
- **User Name :** Enter User Name for PPPoE connection
- **Password :** Enter Password for PPPoE connection
- **MTU:** By default, MTU is set to **1492** bytes. MTU stands for Maximum Transmission Unit. Consult with WISP for a correct MTU setting.
- **Reconnect Mode:** Administrator can select three 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.

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.



WAN Settings

Mode	PPTP

PPTP

User Name		
Password		
PPTP Server IP		
WAN IP		
Netmask		
MTU	1460	
MPPE40	○ Enable	● Disable
MPPE128	○ Enable	● Disable
Reconnect Mode	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.

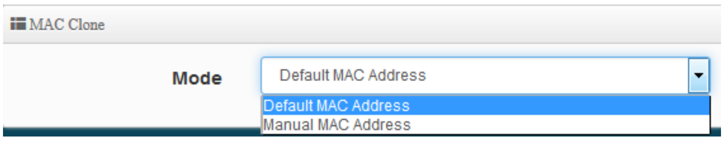
Notice

*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.



MAC Clone

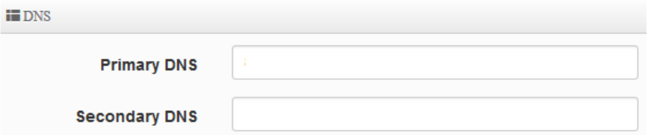
Mode: Default MAC Address

Default MAC Address
Manual MAC Address

- **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.



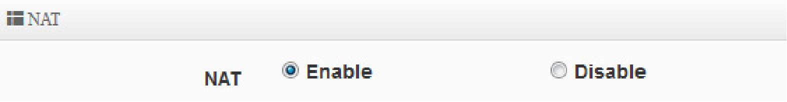
DNS

Primary DNS	
Secondary 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



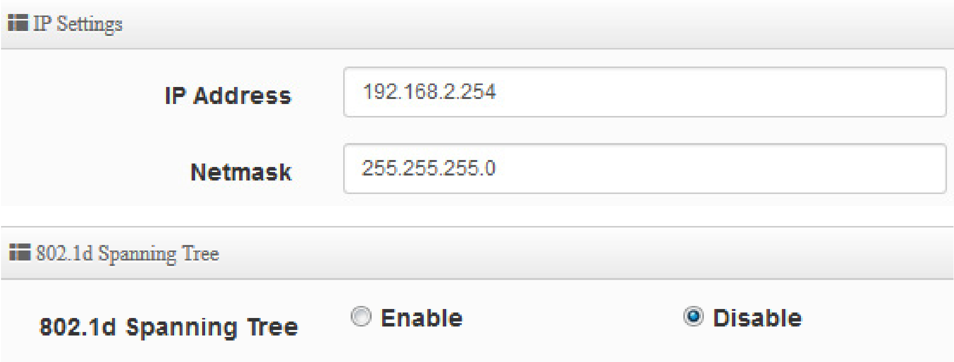
NAT

NAT ● Enable ○ Disable

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

5.2 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

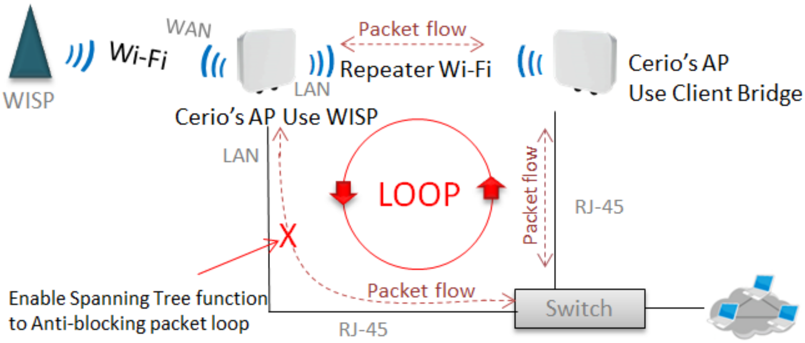
Netmask: 255.255.255.0

802.1d Spanning Tree

802.1d Spanning Tree ○ Enable ● Disable

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

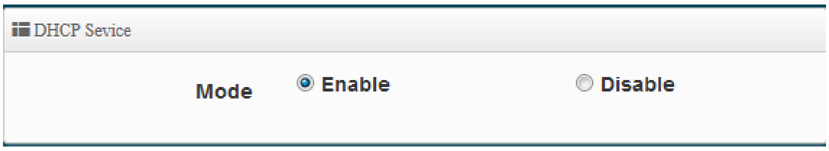
- **IP Address :** The IP address of the LAN port; default IP address is 192.168.2.254
- **IP Netmask :** The Subnet mask of the LAN port; default Netmask is 255.255.255.0
- **802.1d Spanning Tree :** The spanning tree network protocol provides a loop free topology for a bridged LAN between LAN interface 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



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

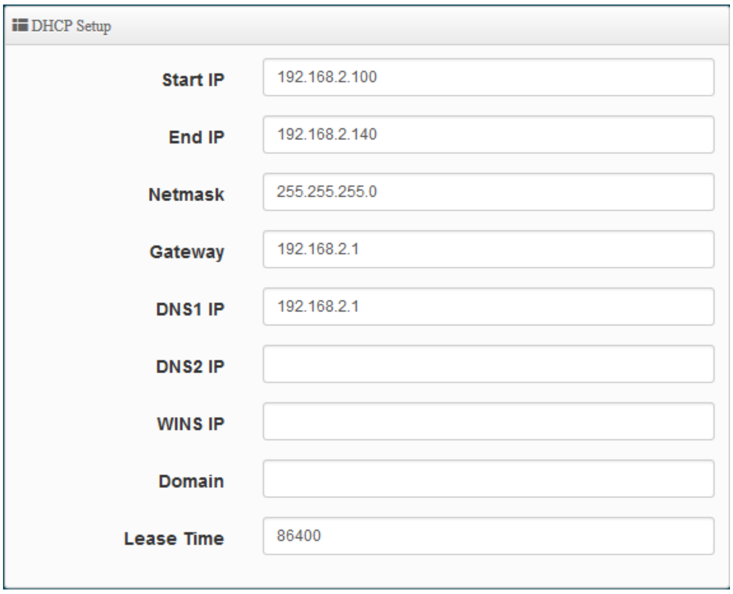
5.3 Configure DHCP Server

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 Sevice

Mode ● Enable ○ Disable

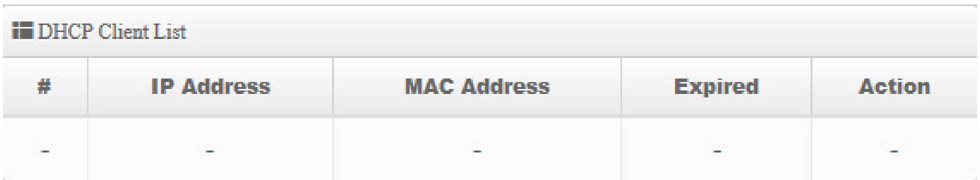


DHCP Setup

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 to the CenOS 5.0 AP and use IP address of the DHCP service, the DHCP Client List will display users the information and used IP address.

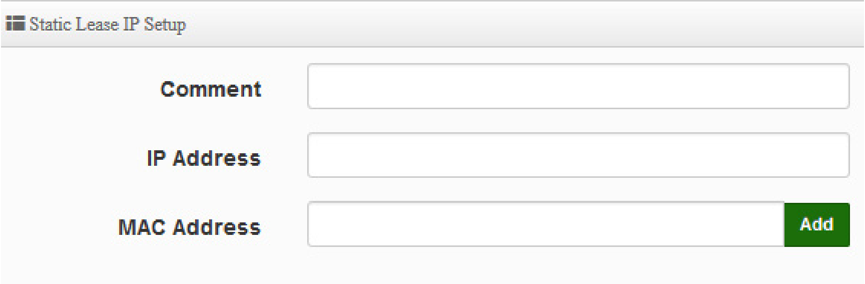


DHCP Client List

#	IP Address	MAC Address	Expired	Action
-	-	-	-	-

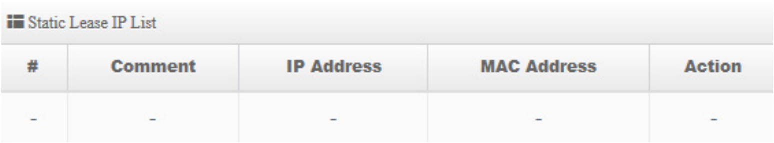
- **IP Address:** Display users used IP address.
- **MAC Address:** Display MAC Address of users used device.
- **Expired:** Display Lease expiration time of IP address.
- **Action:** Kicked user button.

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



- **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.

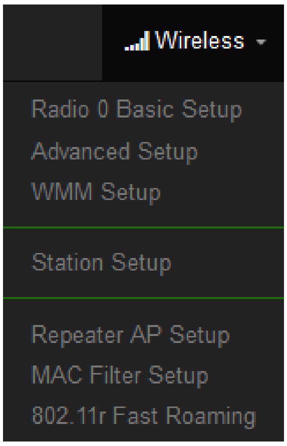

Static Lease IP List

#	Comment	IP Address	MAC Address	Action
-	-	-	-	-

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

5.4 Wireless General Setup

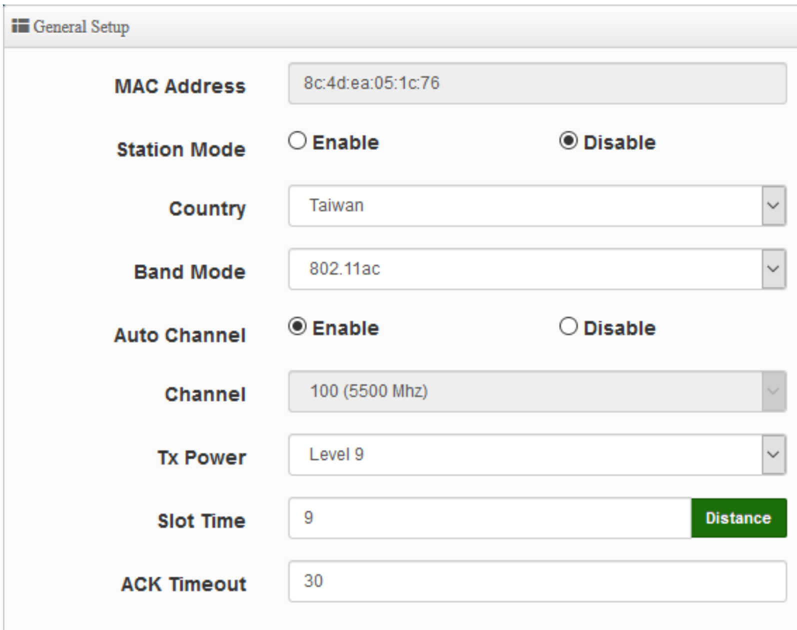
The main setup Client Bridge connection to AP Station and Repeater AP functions setting, MAC filter, WMM and 802.11r/802.11k Fast Roaming etc in wireless menu.



Notice

If want to use Repeater AP function then Clinet Bridge must determine connection to Access Point then Repeater AP can operate normally.

5.4.1 Radio 0 Basic Setup



MAC Address: 8c:4d:ea:05:1c:76

Station Mode: ○ Enable ● Disable

Country: Taiwan

Band Mode: 802.11ac

Auto Channel: ● Enable ○ Disable

Channel: 100 (5500 Mhz)

Tx Power: Level 9

Slot Time: 9 Distance

ACK Timeout: 30

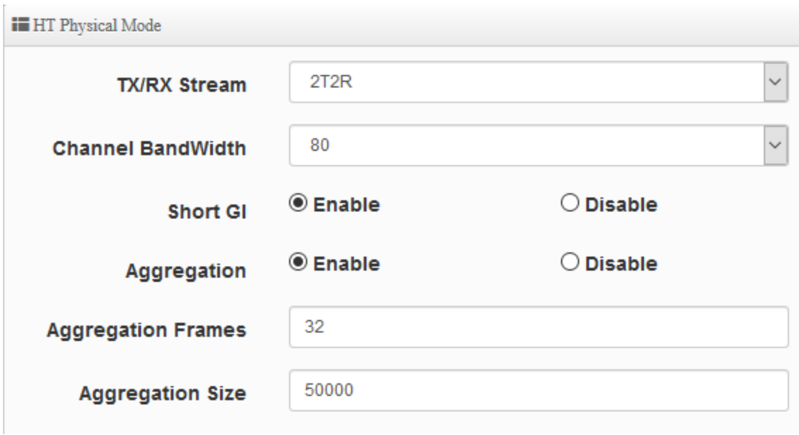
- **MAC Address:** Display radio 1 use MAC address.
- **Country:** Administrator can select country used channel by US / EU and Taiwan.
- **Band Mode:** Administrator can select 5G Band for 802.11a/n or 802.11ac. The default is 802.11ac
- **Auto Channel:** Administrator can Enable or Disable the function. If select disable function the WiFi channel can be fixed a channel.
- **Channel:** Support US / EU / Taiwan country by 5G Channel.
- **Tx Power:** Administrator can control the WiFi Tx output power. The power Max. Level 9.
- **Slot Timout :** You can enter the slot time value here. When the distance is long or short, the waiting time for packet transmission will be adjusted fast and slow.

  Distance: When the "Distance" button is clicked, the point-to-point bridge distance can be entered. The system will automatically calculate the ideal reference value for the Slot Time and ACK Timeout. The input distance is calculated in units (meters).
- **ACK Timout :** When waiting for the "ACKnowledgment frame" interval is too long to be received, the ACK will be retransmitted. A higher ACK Timeout will reduce packet loss, but the transmission efficiency will be poor.

Notice

Setting Slot Time and ACK Timeout can strengthen the long-distance connection. Changing the value can optimize the setting. If the value is too low, the length transmission will be reduced. If the value is too high, there may be disconnection.

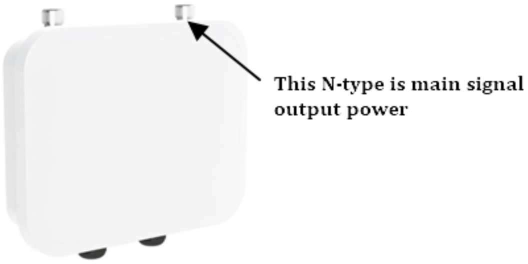
HT Physical Mode



HT Physical Mode

TX/RX Stream	2T2R
Channel BandWidth	80
Short GI	● Enable ○ Disable
Aggregation	● Enable ○ Disable
Aggregation Frames	32
Aggregation Size	50000

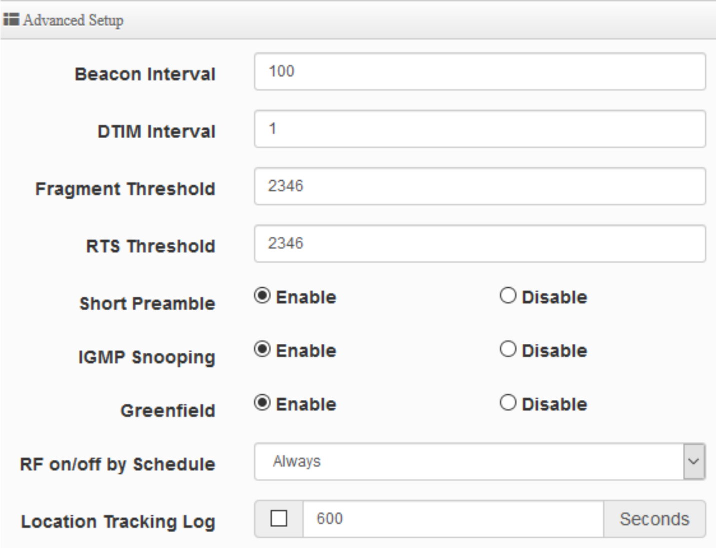
- **TX/RX Stream:** Administrator can select 1 or 2 TX/RX. The default is 2TX/2RX. If administratior adopt model is OW-200 A1 and select use 1Tx/1Rx funciton then please note external N-type connector only one have signal output, as shown below.



- **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:** Set frames size of Aggregation, the size recommend use default value is 32.
- **Aggregation Size:** Set aggregation size, the size recommends use default value is 500000.

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

5.4.2 Advanced Setup



Advanced Setup

Beacon Interval	100	
DTIM Interval	1	
Fragment Threshold	2346	
RTS Threshold	2346	
Short Preamble	● Enable	○ Disable
IGMP Snooping	● Enable	○ Disable
Greenfield	● Enable	○ Disable
RF on/off by Schedule	Always	
Location Tracking Log	□ 600	Seconds

- **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.

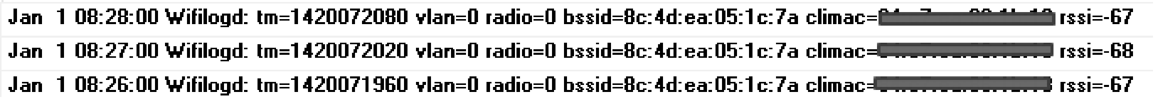
The main purpose of enabling RTS by changing RTS threshold is to reduce possible collisions due to hidden wireless clients. RTS in AP will be enabled automatically if the packet size is larger than the Threshold value. By default, RTS is disabled in a normal environment supports non-jumbo frames.

- **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.
- **RF on/off by Schedule:** When system enable and set time policy function then RF on/off can apply time policy in the function.(Time Policy function set please go to system ➔ Time Policy)
- **Location Tracking Log:** This feature can provides information to third-party positioning systems.



```
Jan  1 08:28:00 Wifilogd: tm=1420072080 vlan=0 radio=0 bssid=8c:4d:ea:05:1c:7a climac=[redacted] rssi=-67
Jan  1 08:27:00 Wifilogd: tm=1420072020 vlan=0 radio=0 bssid=8c:4d:ea:05:1c:7a climac=[redacted] rssi=-68
Jan  1 08:26:00 Wifilogd: tm=1420071960 vlan=0 radio=0 bssid=8c:4d:ea:05:1c:7a climac=[redacted] rssi=-67
```

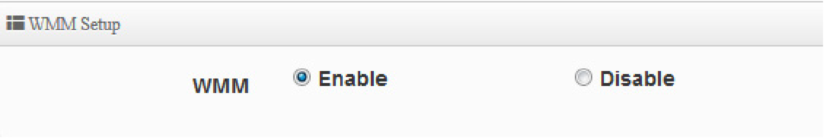
Click **"Save"** button to save your set function. Then click "Reboot" button to activate your changes.

5.4.3 WMM Setup

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

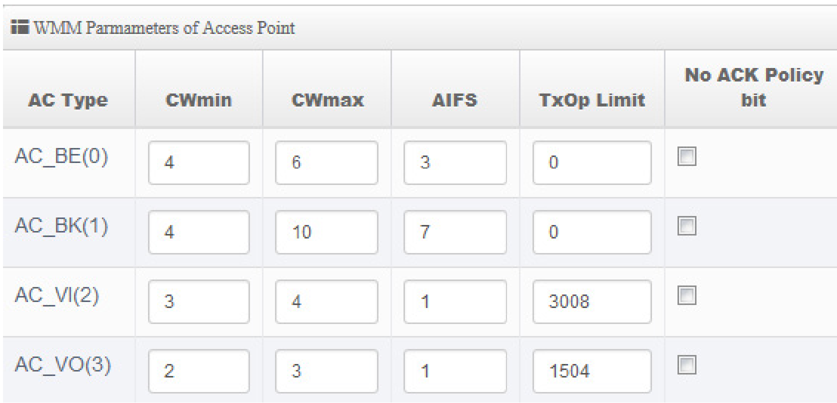
Configuring QoS options consists of setting parameters on existing queues for different types of wireless traffic. You can configure different minimum and maximum wait times for the transmission of packets in each queue based on the requirements of the media being sent. Queues automatically provide minimum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



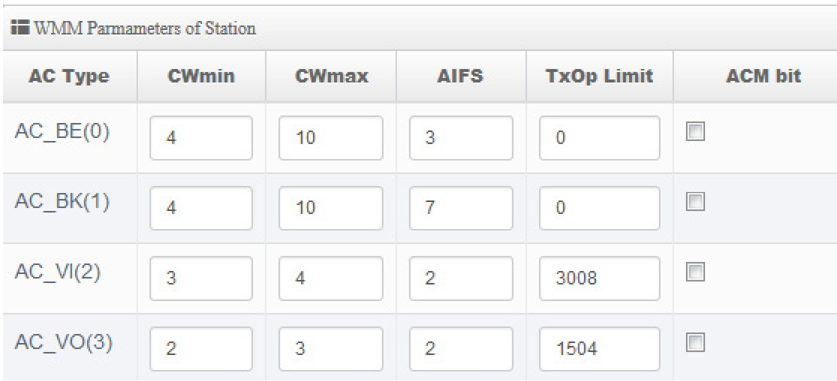
WMM Setup

WMM ● Enable ○ Disable



WMM Parmameters of Access Point

AC Type	CWmin	CWmax	AIFS	TxOp Limit	No ACK Policy bit
AC_BE(0)	4	6	3	0	□
AC_BK(1)	4	10	7	0	□
AC_VI(2)	3	4	1	3008	□
AC_VO(3)	2	3	1	1504	□



WMM Parmameters of Station

AC Type	CWmin	CWmax	AIFS	TxOp Limit	ACM bit
AC_BE(0)	4	10	3	0	□
AC_BK(1)	4	10	7	0	□
AC_VI(2)	3	4	2	3008	□
AC_VO(3)	2	3	2	1504	□

- **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".◦

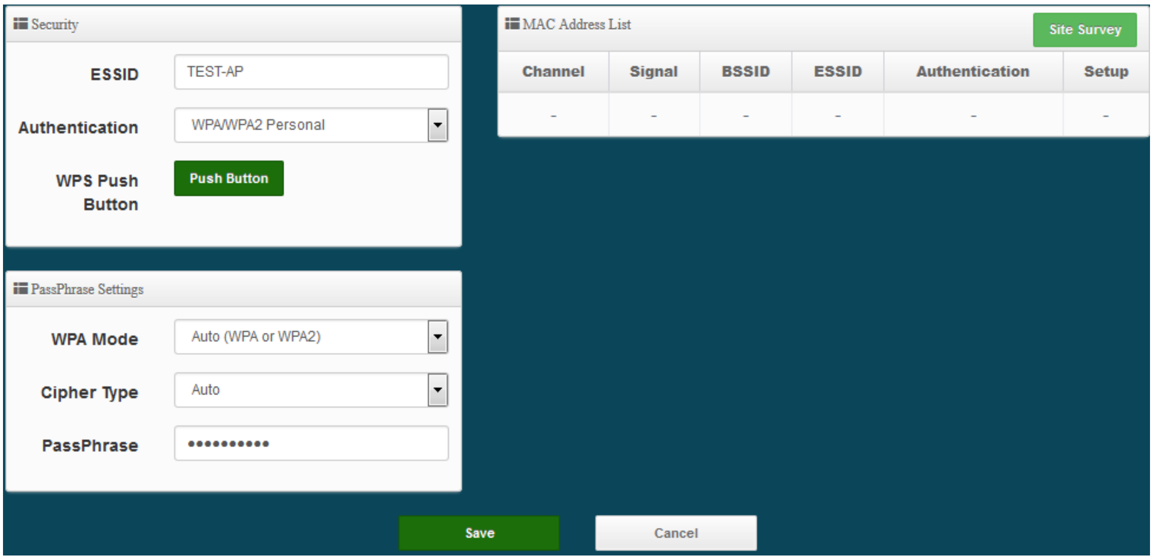
- **AIFS**：The Arbitration Inter-Frame Spacing Number specifies a wait time (in milliseconds) for data frames◦

- **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 uncast packet.◦

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

5.4.4 Station Setup

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



Security

ESSID	TEST-AP
Authentication	WPA/WPA2 Personal
WPS Push Button	Push Button

MAC Address List

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

PassPhrase Settings

WPA Mode	Auto (WPA or WPA2)
Cipher Type	Auto
PassPhrase	••••••••••

- **MAC Address List:** The function can discovery AP Station and select want to link the AP station, please click site survey button.
- **Security:** After site survey AP station complete will list all AP station, when click AP station setup button then AP station information (ESSID/Security type) will display on page.
- **PassPhrase Settings:** Administrator need manual set correct ESSID security/Cipher type and pass phrase.

Notice

If Security/Cipher selected or set PassPhrase is wrong, it will not be able to bridge normally.

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

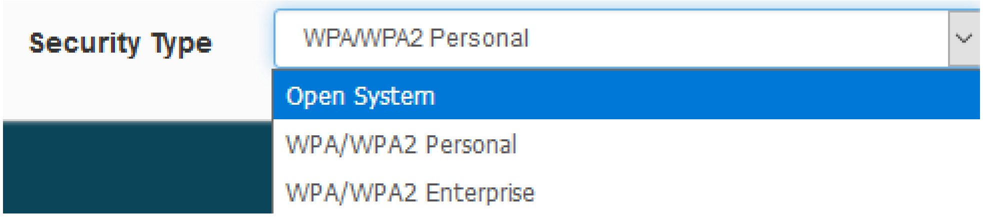
5.4.5 Repeater AP Setup

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

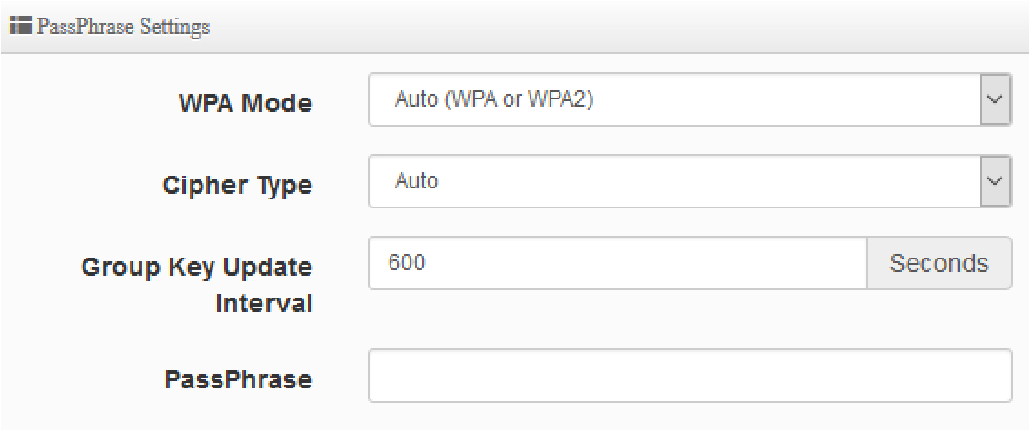
Notice

1. If want to use Repeater AP function then Clinet Bridge must determine connection to Access Point then Repeater AP can operate normally.
2. The default is enabling of Repeater AP. If want to used pure Client Bridge will can disable it.

- **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 is 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.


Security Type: WPA/WPA2 Personal

- **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:

- ✓ **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.

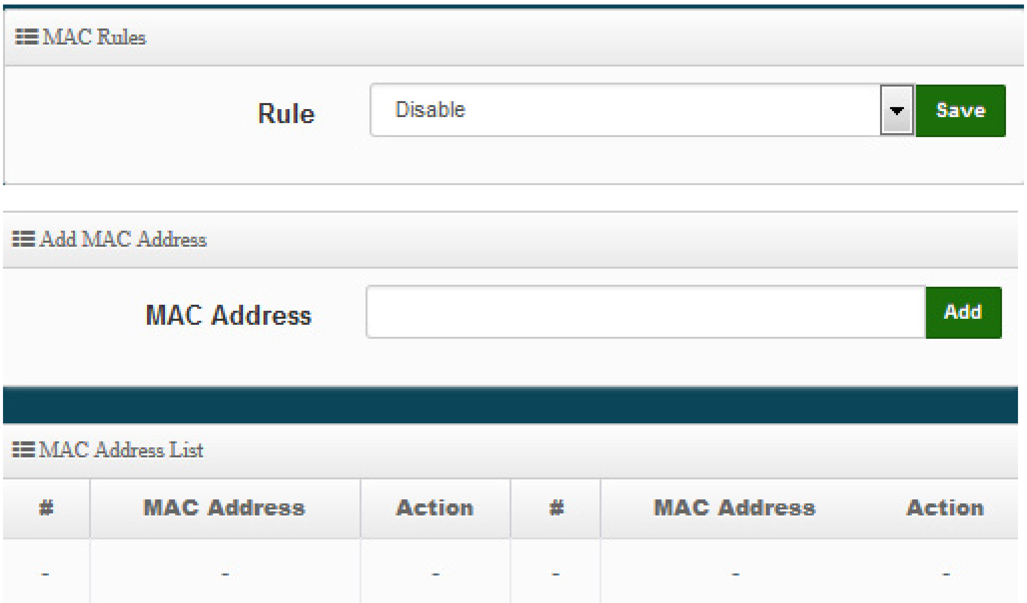
  AES is short for "**Advanced Encryption Standard**", The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plaintext into the final output of ciphertext. Each round consists of several processing steps, including one that depends on the encryption key. 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.

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

5.4.6 MAC Filter Setup

Administrator can setup allow or reject WiFi clients(MAC address) to access Repeater AP.

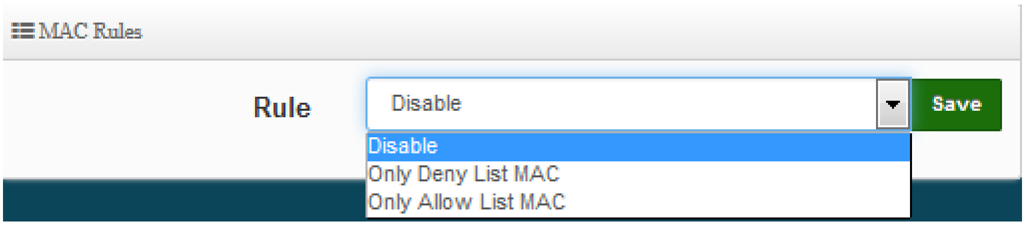


Rule: Disable

MAC Address:

#	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.



Rule: Disable

- **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 -

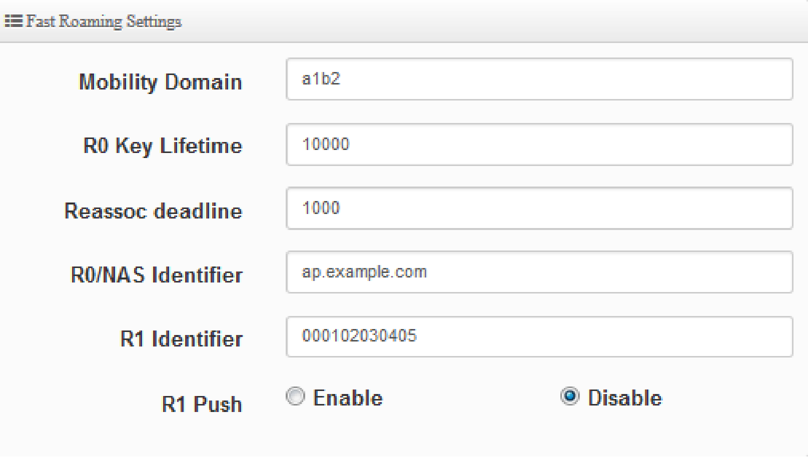
Action Type is set to “**Only Deny List MAC**”.

- **MAC Address:** Enter MAC Address for WiFi Clients.
- **MAC Address List:** Display the MAC address of WiFi Clients.

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

5.4.7 802.11r Fast Roaming Setup

The system support 802.11r/802.11k function for 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.



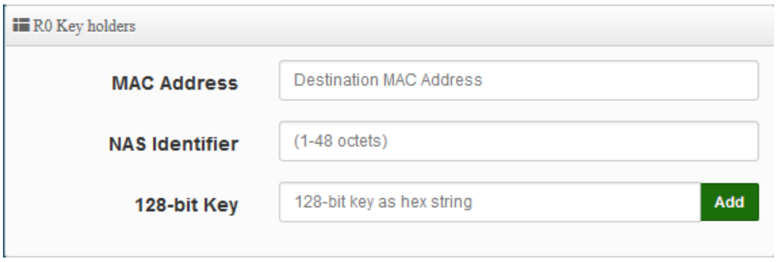
Fast Roaming Settings

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.



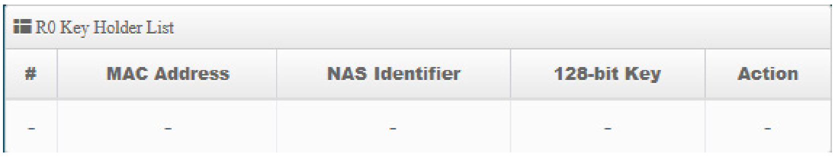
R0 Key holders

MAC Address	Destination MAC Address
NAS Identifier	(1-48 octets)
128-bit Key	128-bit key as hex string 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.

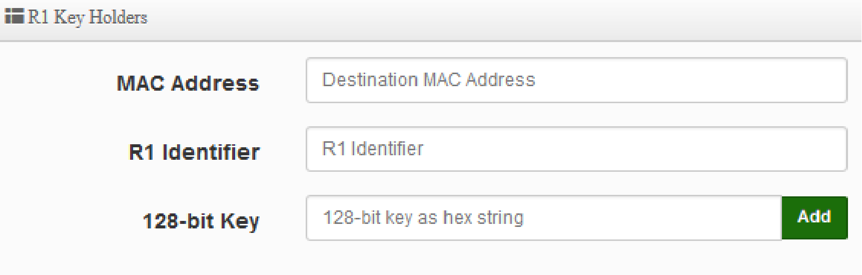


R0 Key Holder List

#	MAC Address	NAS Identifier	128-bit Key	Action
-	-	-	-	-

R1 Key Holder List:

Enter a unified set of R1 Key Holder identification certification.



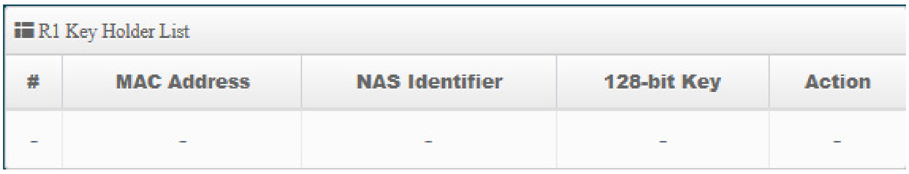
R1 Key Holders

MAC Address	Destination MAC Address
R1 Identifier	R1 Identifier
128-bit Key	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.



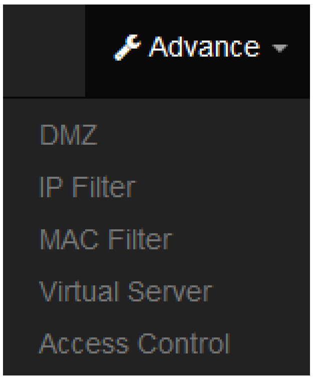
R1 Key Holder List

#	MAC Address	NAS Identifier	128-bit Key	Action
-	-	-	-	-

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

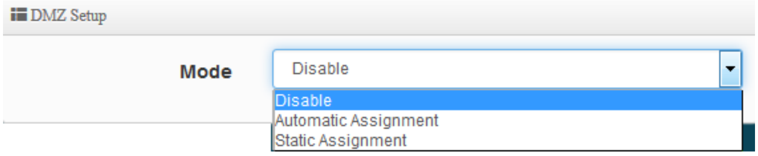
5.5 Advanced Setup

Administrator can set basic routing security functions, including DMZ / IP and MAC filtering / virtual servers and access control management (basic firewall rules) in Advance memu.



5.5.1 DMZ

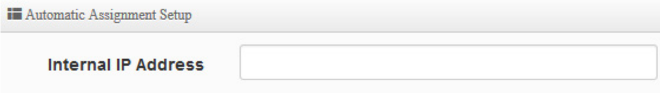
DMZ is commonly work with the NAT functionality as an alternative of Virtual Server(Port Forwarding*)* while wanting all ports of DMZ host visible to Internet users. Virtual Server rules have precedence over the DMZ rule. In order to use a range of ports available to access to different internal hosts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



DMZ Setup

Mode: Disable

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

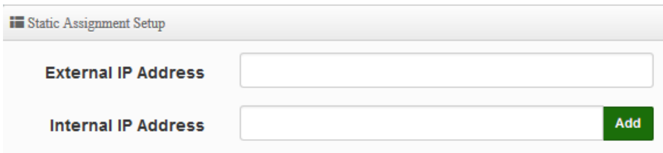


Automatic Assignment Setup

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



Static Assignment Setup

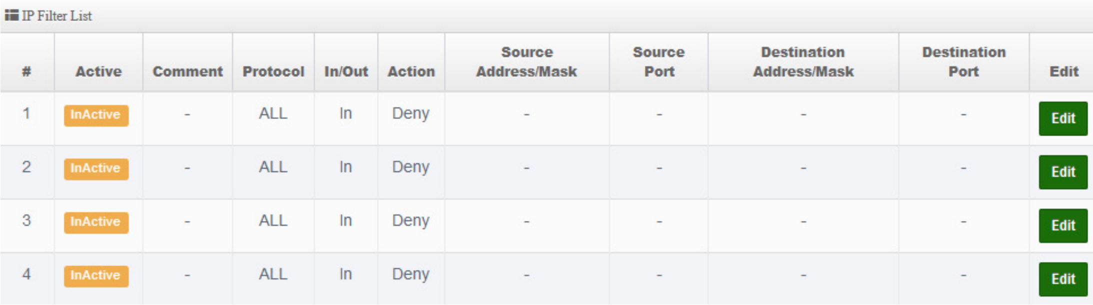
External IP Address	
Internal IP Address	Add

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

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

5.5.2 IP Filter

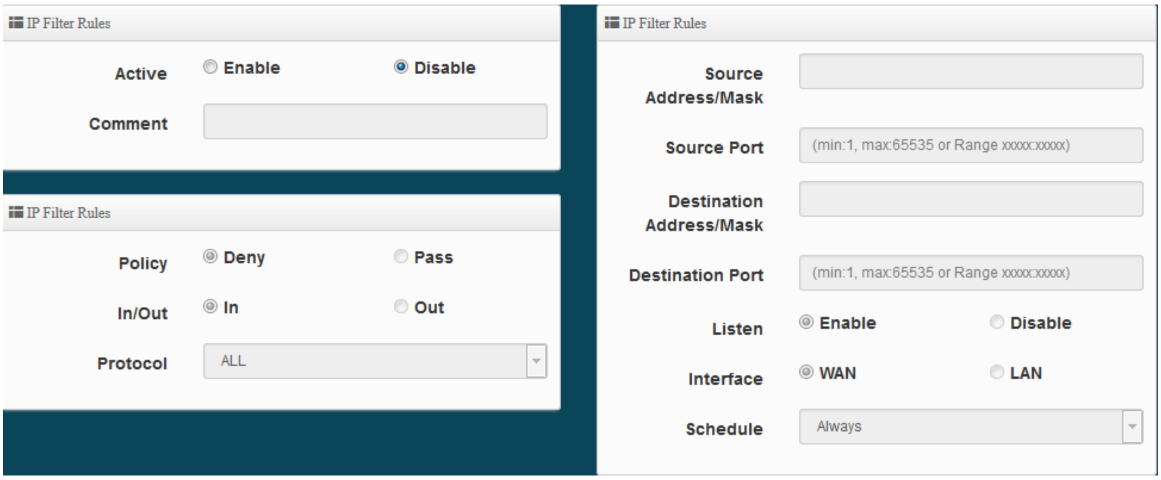
Can allow or deny filter ingress or egress packets from specific source and/or to destination IP address on wired (LAN) or Wireless (WAN) ports. Filter rules could be used to filter unicast or multicast packets on different protocols as shown in the IP Filter Setup. Important to note that IP filter rules has precedence over Virtual server rules. Total of **20** rules maximum allowed in the IP Filter List. All rules can be edited or removed from the List.



IP Filter List

#	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 ALL

IP Filter Rules

Source Address/Mask

Source Port (min:1, max:65535 or Range xxxxx:xxxxx)

Destination Address/Mask

Destination Port (min:1, max:65535 or Range xxxxx:xxxxx)

Listen ● Enable ○ Disable

Interface ● WAN ○ LAN

Schedule Always

➢ **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".**

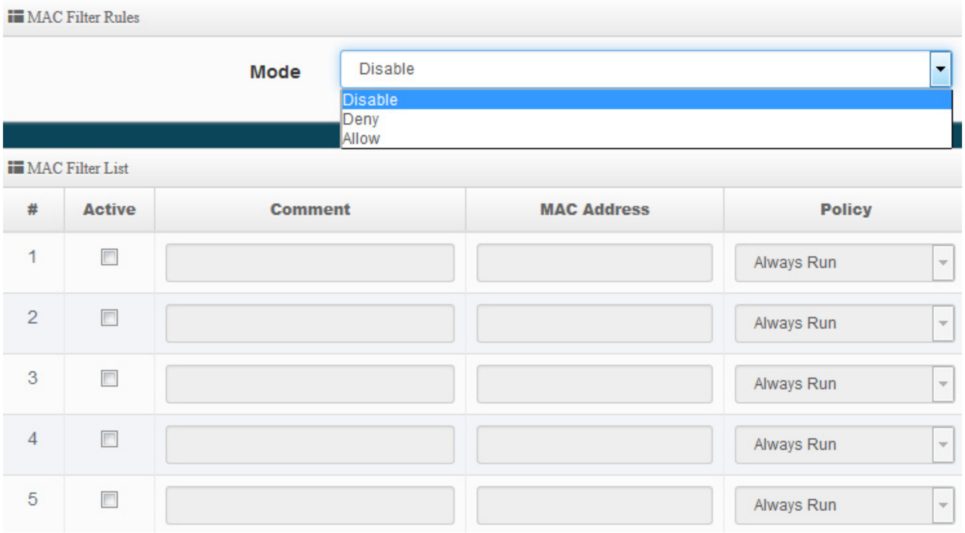
Notice

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

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

5.5.3 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

MAC Filter List

#	Active	Comment	MAC Address	Policy
1	□			Always Run
2	□			Always Run
3	□			Always Run
4	□			Always Run
5	□			Always Run

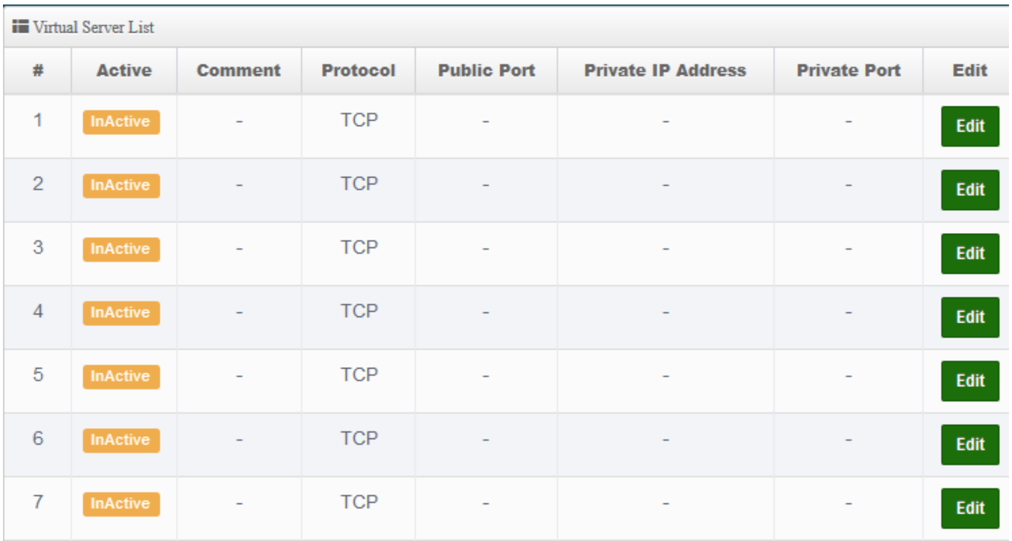
- **Mode:** Administrator can select Deny or Allow.
  - **Deny:** The MAC Filter List will be **denied** to access (LAN to WAN). Others will be allowed.
  - **Allow:** The MAC Filter List will be **allowed** to access (LAN to WAN). Others will be denied.
- **Comment:** Enter the description of MAC filter 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 use rule by **"Time Policy".**

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

5.5.4 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.

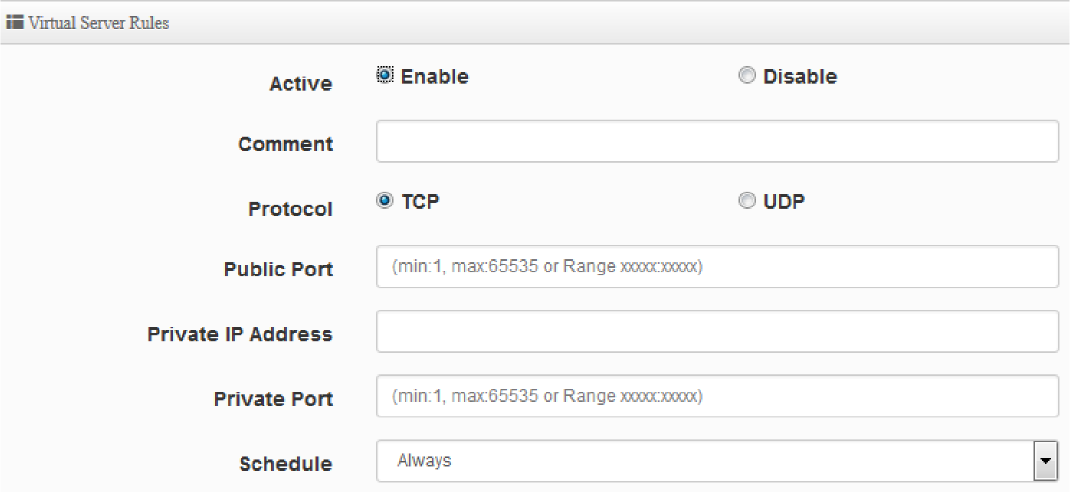
Suppose you want to assign ports 21-25 to one FTP, Telnet and SMTP server (A in the example), and port 80 to another (B in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.



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	● Enable ○ Disable
Comment	
Protocol	● TCP ○ UDP
Public Port	(min:1, max:65535 or Range xxxxx:xxxxx)
Private IP Address	
Private Port	(min:1, max:65535 or Range xxxxx:xxxxx)
Schedule	Always

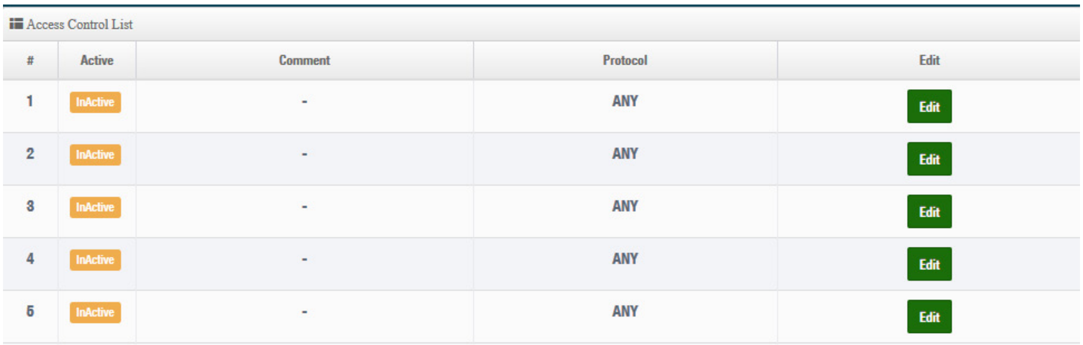
- **Active:** Administrator can select Virtual server rule to Enable or disable.
- **Comment:** Enter the description of virtual server rule.
- **Protocol:** Administrator can select service protocol of TCP or UDP.
- **Public Port:** Enter service port No. for public.
- **Private IP Address:** Enter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

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

5.5.5 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.

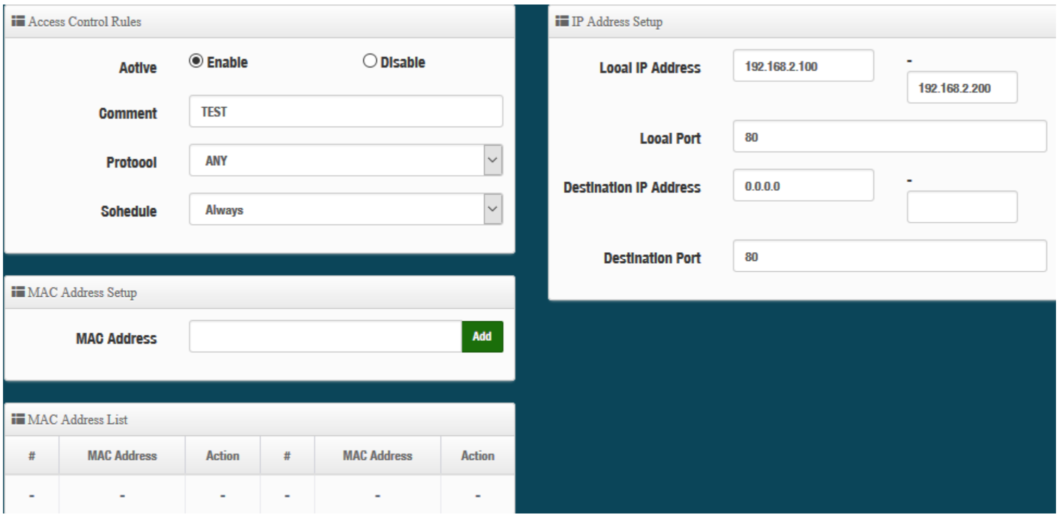
Please click on **Advance -> Access Control** and follow the below setting.



Access Control List

#	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

Aotive ● Enable ○ Disable

Comment: TEST

Protoool: ANY

Sohedule: Always

MAC Address Setup

MAC Address: Add

MAC Address List

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

IP Address Setup

Looal IP Address: 192.168.2.100 - 192.168.2.200

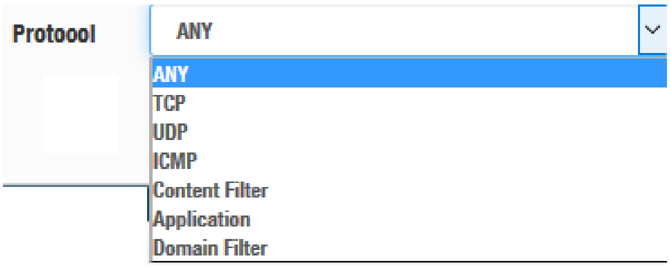
Looal Port: 80

Destination IP Address: 0.0.0.0 -

Destination Port: 80

# 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.

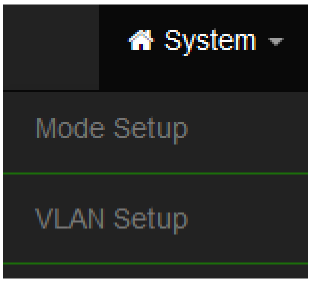


- ✓ **ANY:** Select **"Any"** is all deny Protocol, administrator can filter local IP / IP range go to destination IP / IP range and use protocol.
- ✓ **TCP:** Deny TCP Protocol, Administrator can set TCP protocol and assign IP / IP range.
- ✓ **UDP:** Deny UDP Protocol, Administrator can set UDP protocol 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.

6. CAP Mode

The CAP mode itself isn't Access Point. This mode is primarily to control all the managed AP.
The following describes setup function in system menu

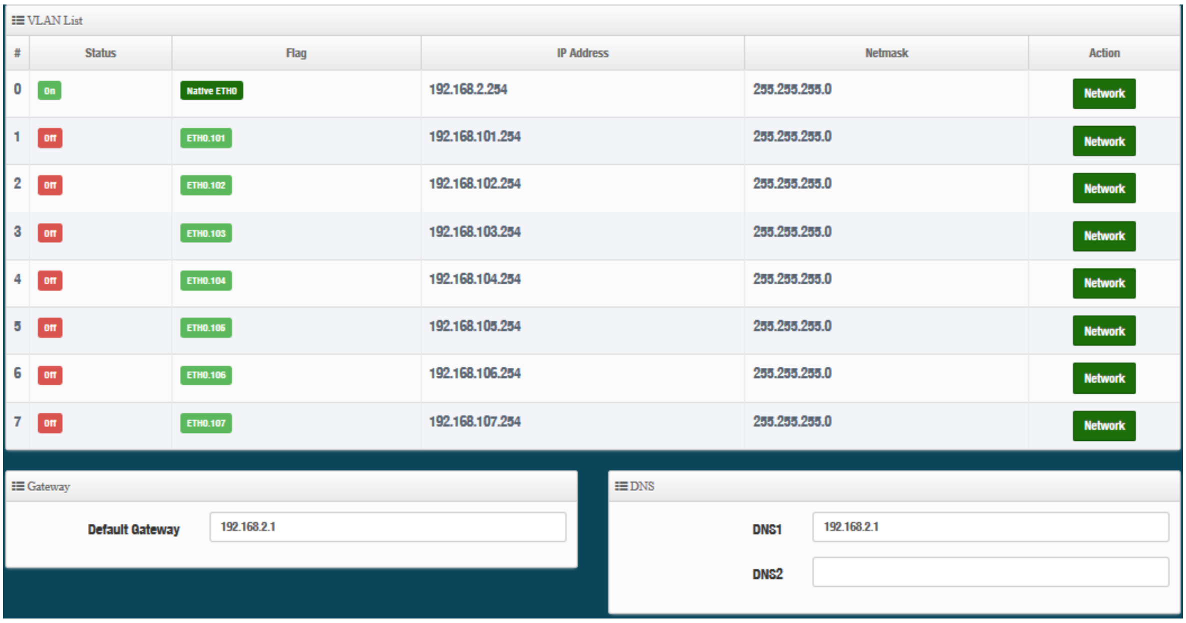


6.1 VLAN Setup

Setup Control AP of LAN or VLAN IP Address, Gateway, DNS and Ethernet Tag etc.
Please click on **System -> VLAN Setup**

Notice

This VLANs support max 16 IEEE 802.1q tag VLANs.



VLAN List

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

Gateway

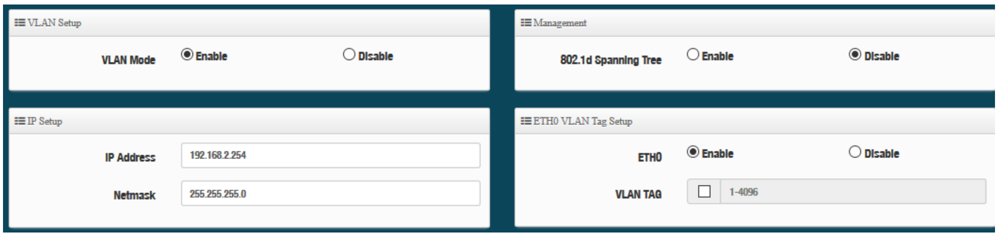
Default Gateway: 192.168.2.1

DNS

DNS1: 192.168.2.1

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: ● Enable ○ Disable

Management

802.1d Spanning Tree: ○ Enable ● Disable

IP Setup

IP Address: 192.168.2.254

Netmask: 255.255.255.0

ETH0 VLAN Tag Setup

ETH0: ● Enable ○ Disable

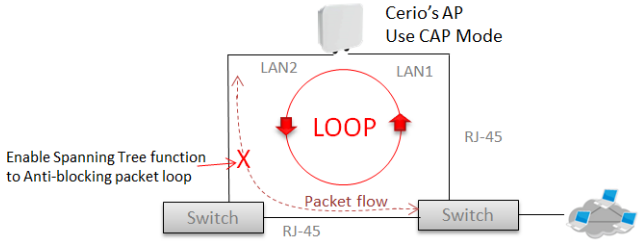
VLAN TAG: □ 1-4096

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

Notice

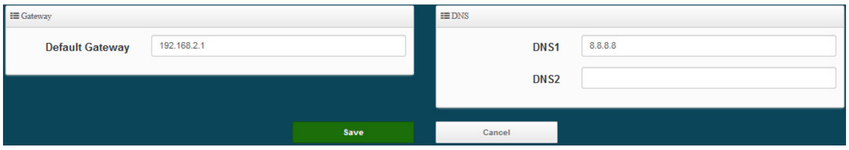
There must always be at least one VLAN enabled. If the administrator disables all the VLANs, he/she will not be able to login to the manager page. The administrator must then reset to default.

- **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.**



Default Gateway: 192.168.2.1

DNS1: 8.8.8.8

DNS2:

- **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.

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

6.2 AP Control

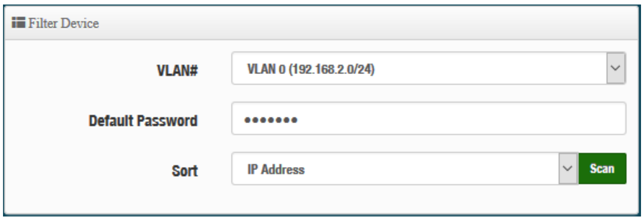
When CenOS5.0 AP changes to CAP mode, Administrator can use AP Control functions to centralize management of APs in the network architecture. AP control Setting functions have "Scan Device", "Batch Setup", "AP Setup", "Group / Map setup" and Authentication Profile setup etc..
Please click **"AP Control"**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

6.2.1 Scan Device

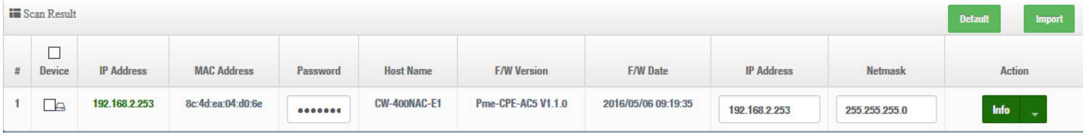
This management page can discover all managed APs in the network. Administrator can set IP address / Password and VLAN tag for managed APs. After the setup is complete, Administrator must import all managed APs to databases.



Filter Device

VLAN#	VLAN 0 (192.168.2.0/24)
Default Password	•••••••
Sort	IP Address

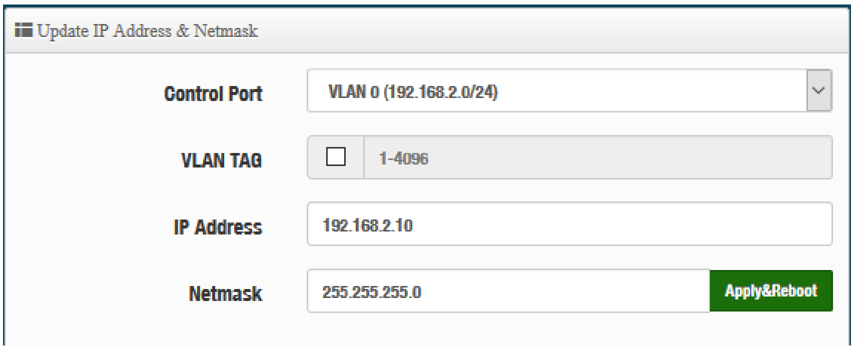
- ➢ **VLAN# :** Administrator can select VLAN network to discovery managed Aps
- ➢ **Default Password:** Set login system password by managed Aps.
- ➢ **Sort**: Administrator can select discovery managed Aps Type. (IP or MAC)



Scan Result

#	□ 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-AC5 V1.1.0	2016/05/06 09:19:35	192.168.2.253	255.255.255.0	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.



Update IP Address & Netmask

Control Port	VLAN 0 (192.168.2.0/24)
VLAN TAG	□ 1-4096
IP Address	192.168.2.10
Netmask	255.255.255.0

- ➢ **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

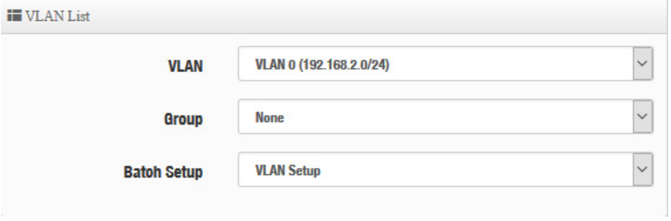
auto-incrementally.

- **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.

6.2.2 Batch Setup

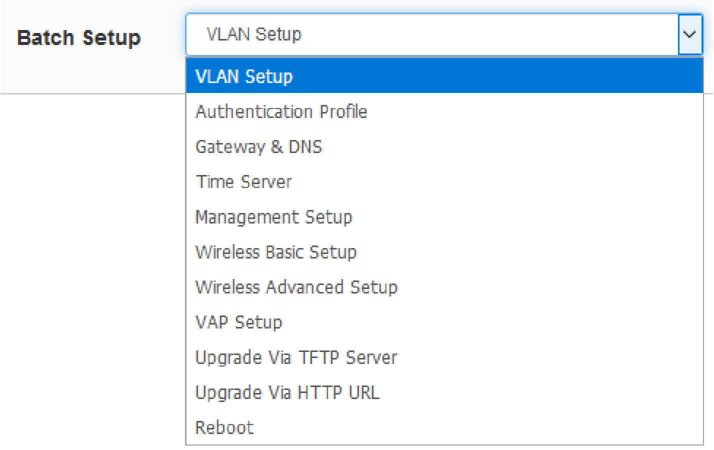
The AP control function supports centralized configuration of managed APs. Administrator can change VLAN network / Group and batch setup for managed APs.



VLAN List

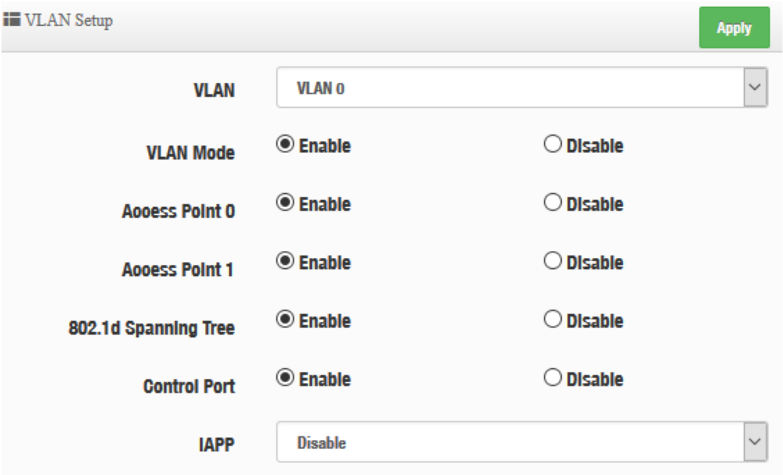
VLAN	VLAN 0 (192.168.2.0/24)
Group	None
Batoh Setup	VLAN Setup

- **LAN**：When VLAN Tag function is enabled (please refer to 3.1 System VLAN Setup), administrator can change VLAN tag for managed APs.
- **Group**：When AP Groups are created (please refer to 6.2.4 Group setup), Administrators can select and change group settings of managed APs.
- **Batch Setup**：Administrator can centralize setting changes for managed APs.



Batch Setup: VLAN Setup

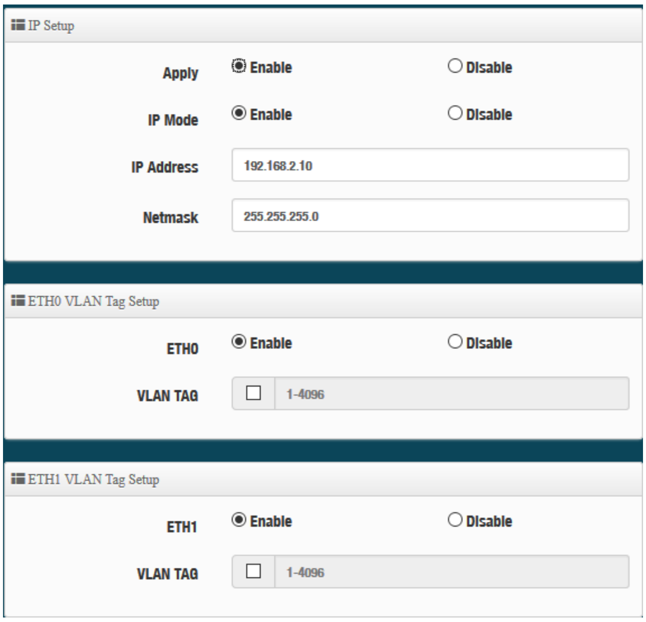
- **VLAN Setup**：Administrator can set VLAN Tag, IP address and Wi-Fi on/off for the managed APs.



VLAN Setup

VLAN	VLAN 0	
VLAN Mode	● Enable	○ Disable
Access Point 0	● Enable	○ Disable
Access Point 1	● Enable	○ Disable
802.1d Spanning Tree	● Enable	○ Disable
Control Port	● Enable	○ Disable
IAPP	Disable	

- ✓ **VLAN：**The function can select VLAN (please refer to 3.1 Configure VLAN Setup) for managed APs.
- ✓ **VLAN Mode：**Administrator can enable or disable VLAN mode of the managed APs.
- ✓ **Access Point0：**Administrator can enable or disable 2.4G radio of the managed APs.
- ✓ **Access Point1：**Administrator can enable or disable 5G radio of the managed APs.
- ✓ **802.1d Spanning Tree：**Administrator can enable or disable the function.(please refer to 3.1 Network Setup ➔ 802.1d Spanning Tree)
- ✓ **Control Port：**The function administrator can enable or disable of the managed APs (please refer to 3.1 Network Setup ➔ Control Port)
- ✓ **IAPP：**The function administrator can enable or disable of the managed APs (Please refer to 3.1 Network Setup ➔ IAPP)



IP Setup

Apply	● Enable	○ Disable
IP Mode	● Enable	○ Disable
IP Address	192.168.2.10	
Netmask	255.255.255.0	

ETH0 VLAN Tag Setup

ETH0	● Enable	○ Disable
VLAN TAG	□ 1-4096	

ETH1 VLAN Tag Setup

ETH1	● Enable	○ Disable
VLAN TAG	□ 1-4096	

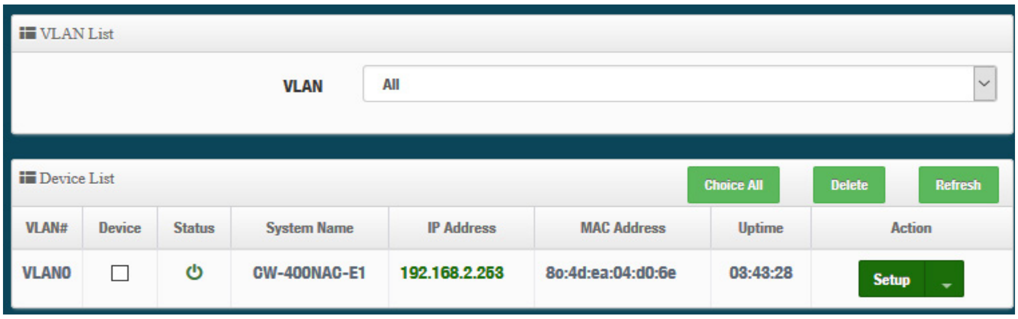
- ✓ **IP Setup：**Administrator can set IP address and Netmask of the managed APs.
- ✓ **ETH0/1 VLAN Tag Setup：**Administrator can set VLAN Tag or disable VLAN function

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 2.2 Configure Time Server)
- **Management Setup:** Setting system name/ system login port and system log server service for managed APs. (Please refer to 2.1 system management)
- **Wireless Batch Setup:** Setting Wi-Fi configurations for managed APs. (Please refer to 3.5.1 Wireless Basic Setup)
- **Wireless Advanced Setup:** Setting Wi-Fi Advanced settings for managed APs. (Please refer to 3.5.2 Wireless Advanced Setup)
- **VAP Setup**：Wi-Fi SSID / channel or security settings for managed APs. (Please refer to 3.1.3 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.

6.2.3 AP Setup

Administrator can monitor statuses and modify managed APs information.



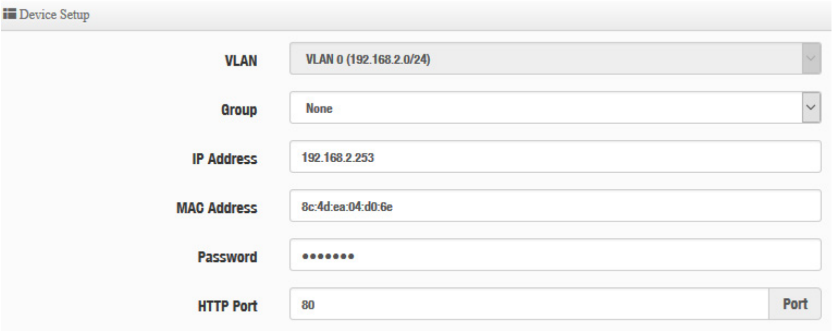
VLAN List

VLAN: All

Device List

VLAN#	Device	Status	System Name	IP Address	MAC Address	Uptime	Action
VLAN0	□	⏻	CW-400NAC-E1	192.168.2.253	8o:4d:ea:04:d0:6e	03:43:28	Setup

- ➢ **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.

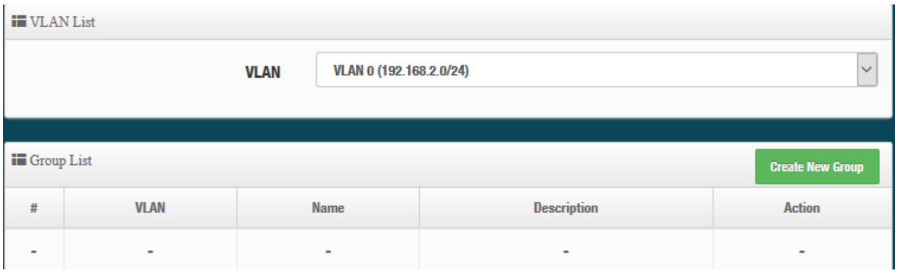


Device Setup

VLAN	VLAN 0 (192.168.2.0/24)
Group	None
IP Address	192.168.2.253
MAC Address	8c:4d:ea:04:d0:6e
Password	•••••••
HTTP Port	80 Port

6.2.4 Group Setup

Administrator can create Groups within the same VLAN.



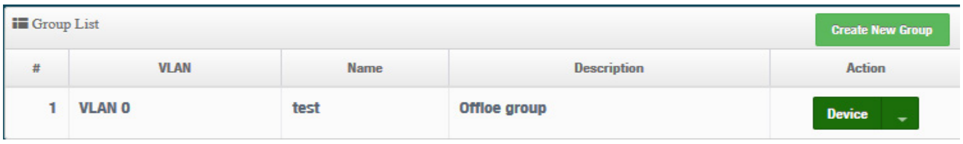
VLAN List

VLAN: VLAN 0 (192.168.2.0/24)

Group List

#	VLAN	Name	Description	Action
-	-	-	-	-

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



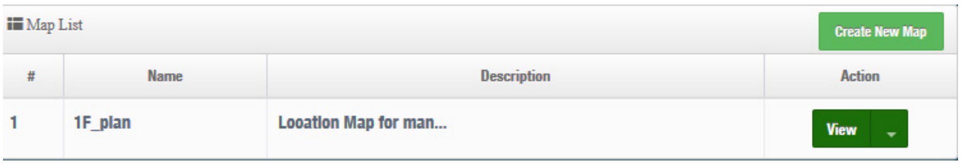
Group List

#	VLAN	Name	Description	Action
1	VLAN 0	test	Offloe group	Device

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

6.2.5 Map Setup

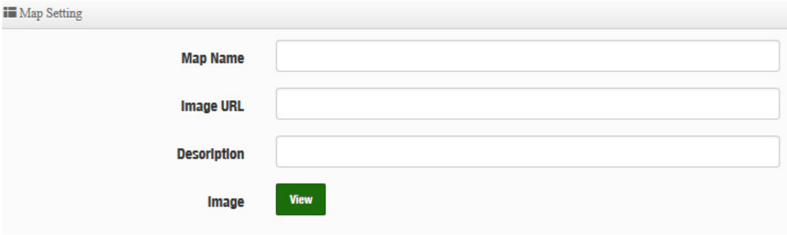
The Map Setup feature allows administrators to upload a floor plan image to a web server, then use the image URL to import the map into the AP user interface. Once the image is uploaded, administrators can use the Map Setup function to map out the locations of the AP network.



Map List

#	Name	Description	Action
1	1F_plan	Looatlon Map for man...	View

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



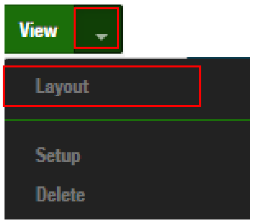
Map Setting

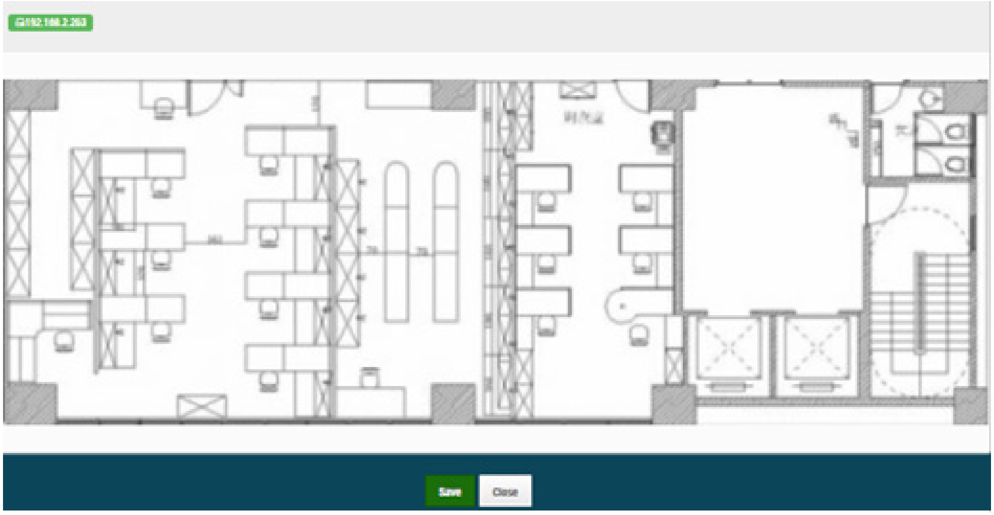
Map Name	
Image URL	
Description	
Image	View

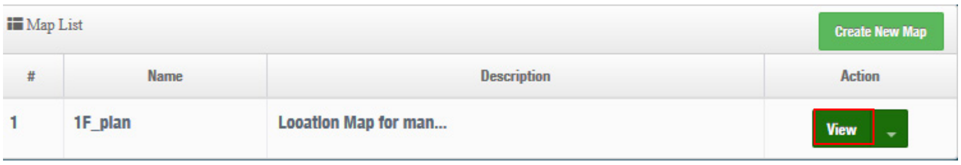
- **Map Name**：Enter map name.
- **Image URL**：Paste Map image url
- **Description**：Enter the description for the map.

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.





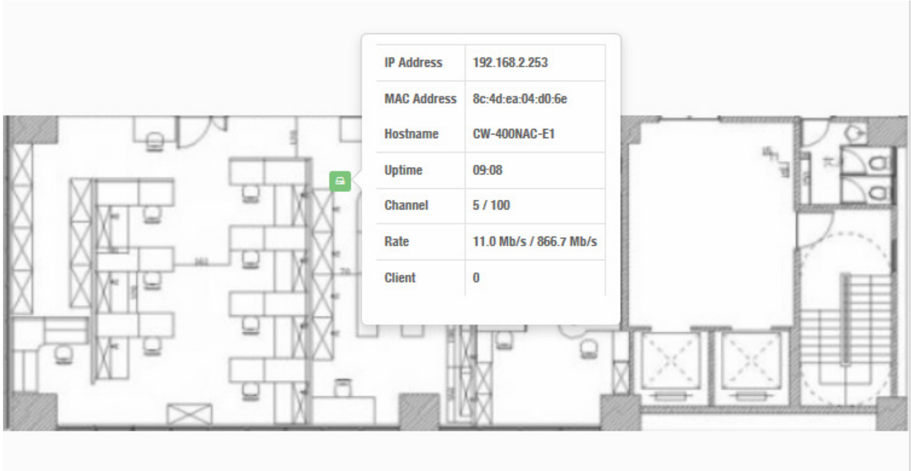


Map List

Create New Map

#	Name	Description	Action
1	1F_plan	Location Map for man...	View ⌄

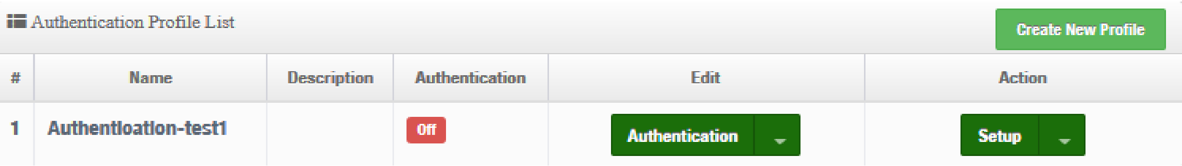
View：Once complete, administrators can click the "View" button to monitor AP statuses and locations.



IP Address	192.168.2.253
MAC Address	8c:4d:ea:04:d0:6e
Hostname	CW-400NAC-E1
Uptime	09:08
Channel	5 / 100
Rate	11.0 Mb/s / 866.7 Mb/s
Client	0

6.2.6 Authentication Profile

Administrator can pre-set authentication conditions in the profile, the authentication set can refer 3.2 Authentication.



Authentication Profile List

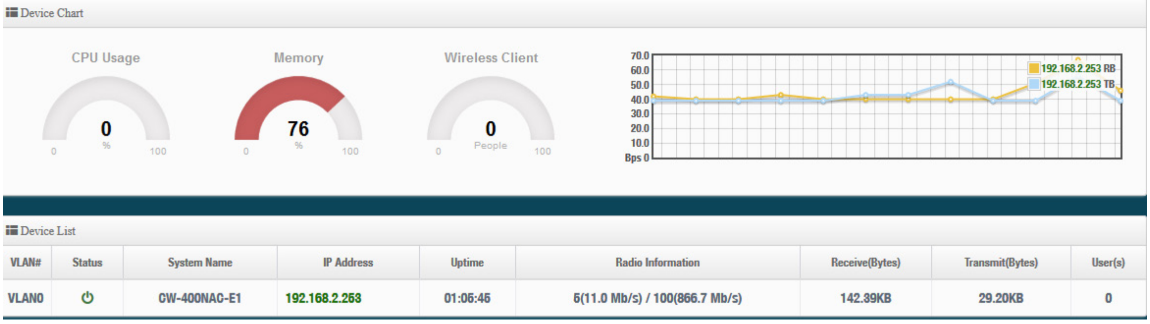
#	Name	Description	Authentication	Edit	Action
1	Authentloatlon-test1		Off	Authentication ⌄	Setup ⌄

- **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 **“3.2.1 Authentication”.**

  Authentication ⌄ Click Dropdown to set authentication functions. Refer to **“3.2.2 Authentication”** dropdown functions.
- **Action:** Setup ⌄ The button can modify or delete for the authentication profile.

6.2.7 Status

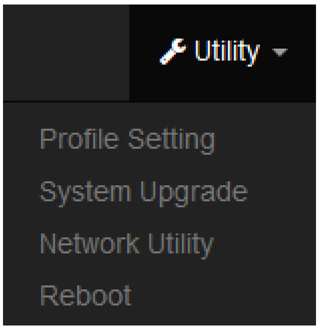
Administrator can monitor Tx/Rx flow information, show online users and check system CPU / Memory information and on/off line for the managed APs. The information data display support graphical interface.



VLAN#	Status	System Name	IP Address	Uptime	Radio Information	Receive(Bytes)	Transmit(Bytes)	User(s)
VLAN0	⏻	CW-400NAC-E1	192.168.2.253	01:06:46	5(11.0 Mb/s) / 100(866.7 Mb/s)	142.39KB	29.20KB	0

7. Utilities

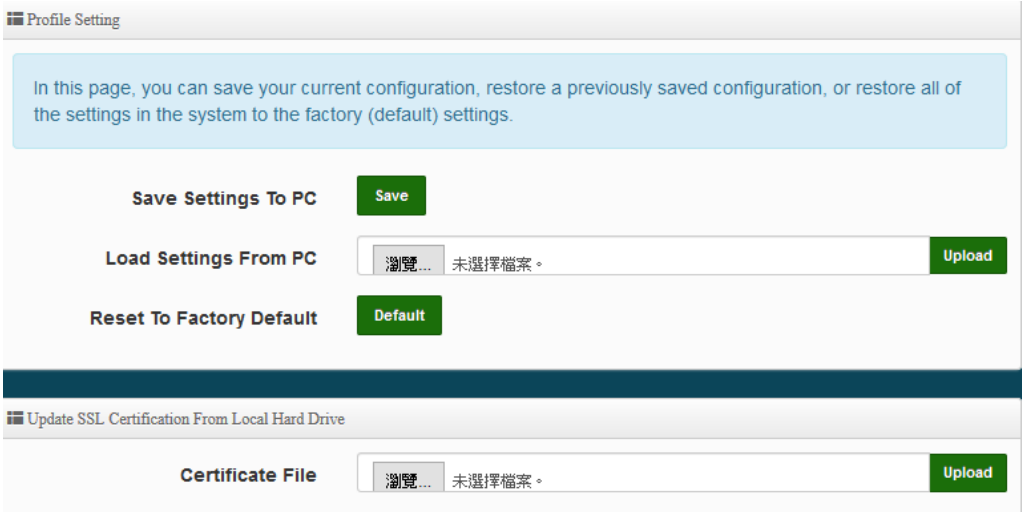
Administrator can backup or restore system configuration / firmware Upgrade / ping tools and system reset to default or reboot system.



7.1 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

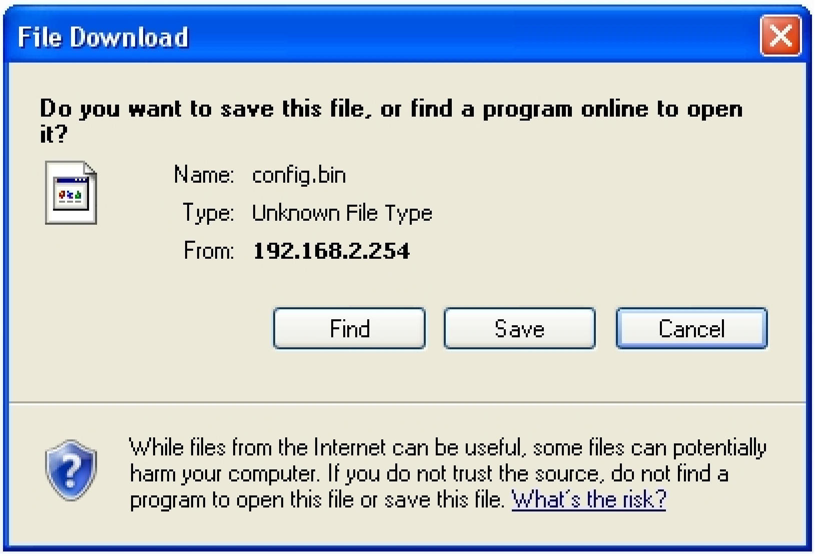
Load Settings From PC

Reset To Factory Default

Update SSL Certification From Local Hard Drive

Certificate File

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



File Download

Do you want to save this file, or find a program online to open it?

Name: config.bin

Type: Unknown File Type

From: 192.168.2.254

While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not find a program to open this file or save this file. What's the risk?

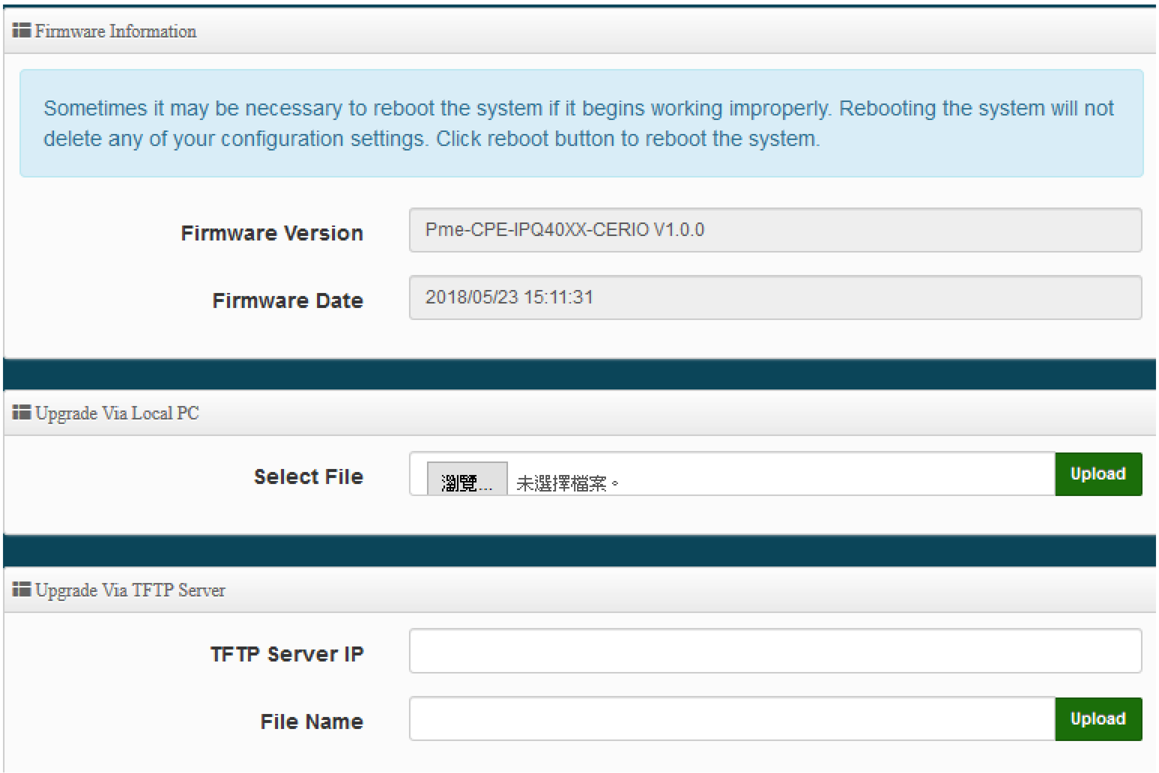
- **Load Settings from PC:** Click ***Browse*** button to locate a configuration file to restore, and then click ***Upload*** button to upload.
- **Reset To Factory Default:** Click ***Default*** button to reset back to the factory default settings and expect **Successful** loading message**.** Then,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

7.2 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-IPQ40XX-CERIO V1.0.0

Firmware Date: 2018/05/23 15:11:31

Upgrade Via Local PC

Select File: 瀏覽... 未選擇檔案。 Upload

Upgrade Via TFTP Server

TFTP Server IP:

File Name: Upload

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

Upgrade Via Local PC and TFTP Server:

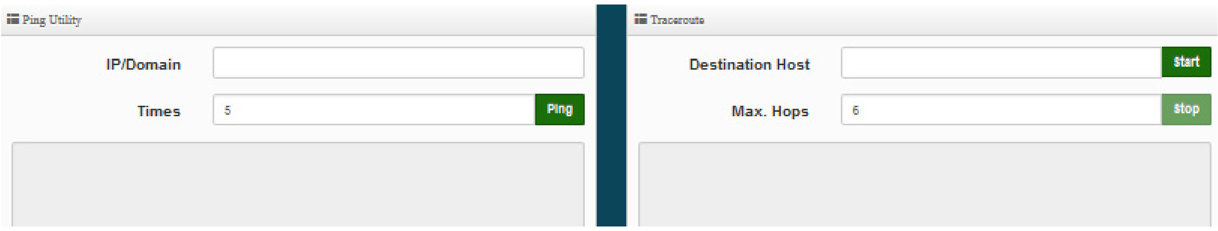
The upgrade firmware will support via local PC and TFTP Server and HTTP URL to upgrade system.

Notice

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.*

7.3 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.



Ping Utility

IP/Domain

Times 5

Traceroute

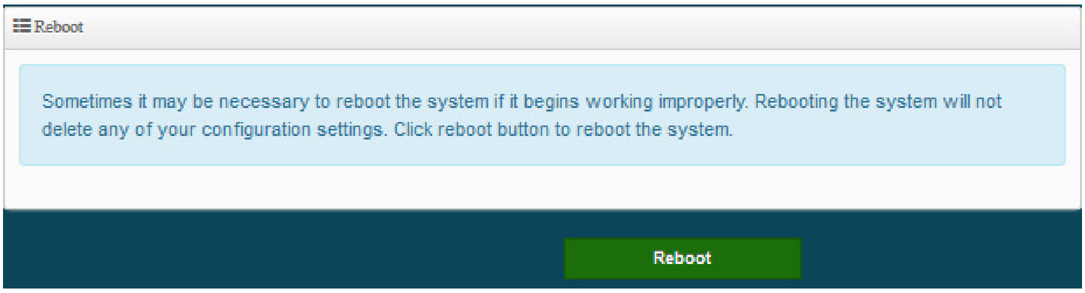
Destination Host

Max. Hops 6

- **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, its 5 and the range is from 1 to 50. It indicates number of connectivity test.
- **Traceroute**： Allows tracing the hops from the CenOS 5.0 AP 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.

7.4 Reboot

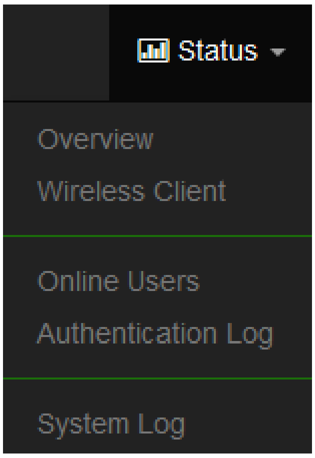
This function allows user to restart system with existing or most current settings when changes are made. Click **Reboot** button to proceed and take around three minutes to complete.



Reboot

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.

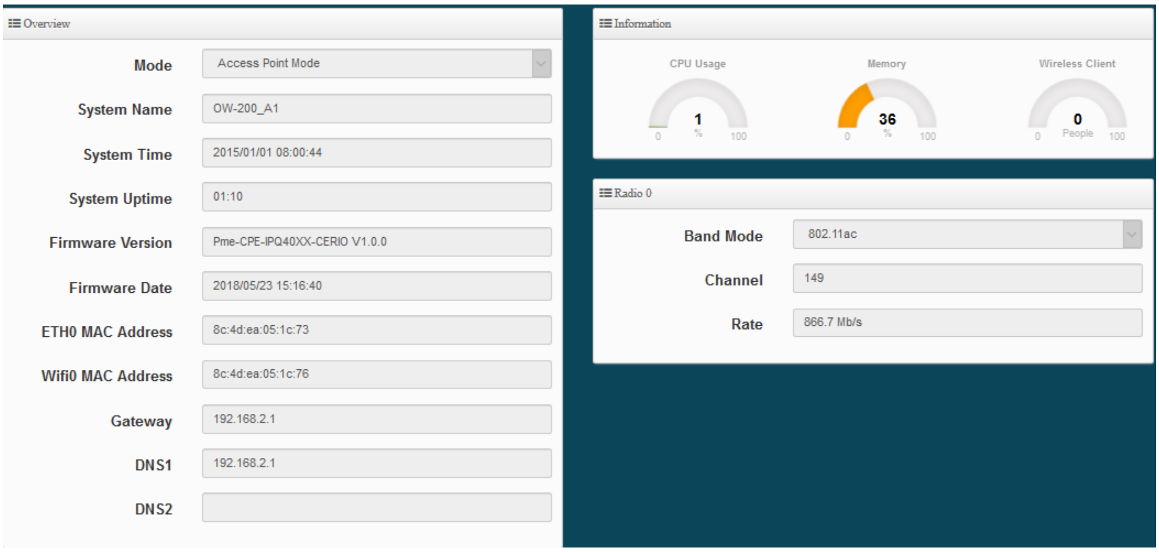
8. Status



The status mainly displays system related information, including system network information, wireless base station information, and wireless user connection information.

8.1 Overview

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



Overview

Mode	Access Point Mode
System Name	OW-200_A1
System Time	2015/01/01 08:00:44
System Uptime	01:10
Firmware Version	Pme-CPE-IPQ40XX-CERIO V1.0.0
Firmware Date	2018/05/23 15:16:40
ETH0 MAC Address	8c:4d:ea:05:1c:73
Wifi0 MAC Address	8c:4d:ea:05:1c:76
Gateway	192.168.2.1
DNS1	192.168.2.1
DNS2	

Information

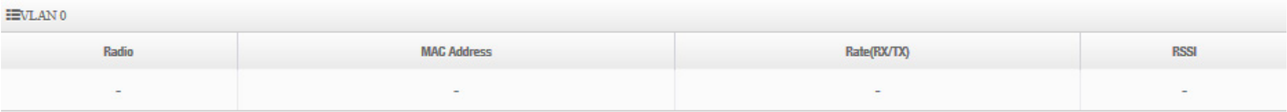
CPU Usage 1 %
Memory 36 %
Wireless Client 0 People

Radio 0

Band Mode	802.11ac
Channel	149
Rate	866.7 Mb/s

8.2 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. (In addition to CAP mode)



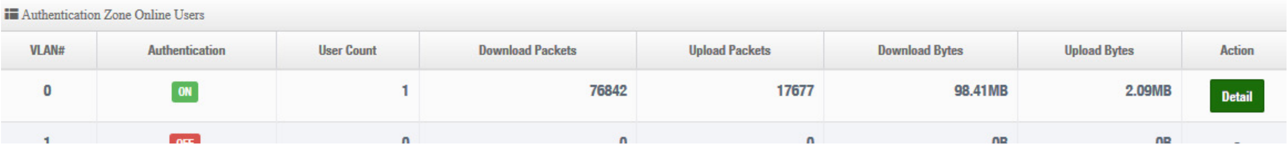
☰VLAN 0

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

- **Radio**：Display information for wireless client connection Radio 0.
- **MAC Address**：Display information of clients Wi-Fi MAC address
- **Rata(Tx/Rx)**：Display information of clients Wi-Fi connection data rete.
- **RSSI**：Display information of clients Wi-Fi connection signal strong and weak.

8.3 Online Users

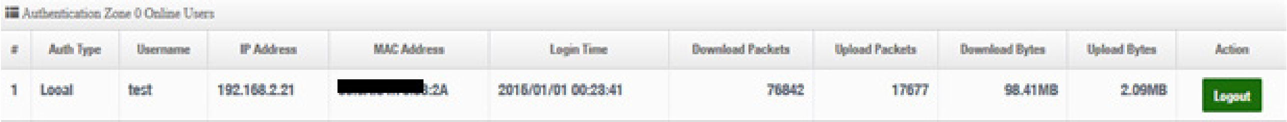
The status can display online users by Captive Portal. Administrator can monitor user’s login / logout time and account type for the authentication account. (This page only used AP mode)



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	-

- **VLAN#**：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.



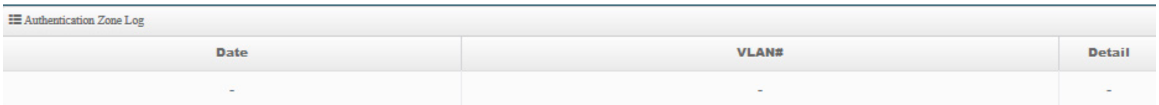
Authentication Zone 0 Online Users

#	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	[redacted]:2A	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.

8.4 Authentication Log

The authentication log can monitor account login/logout type and account use time. (This page only used AP mode)



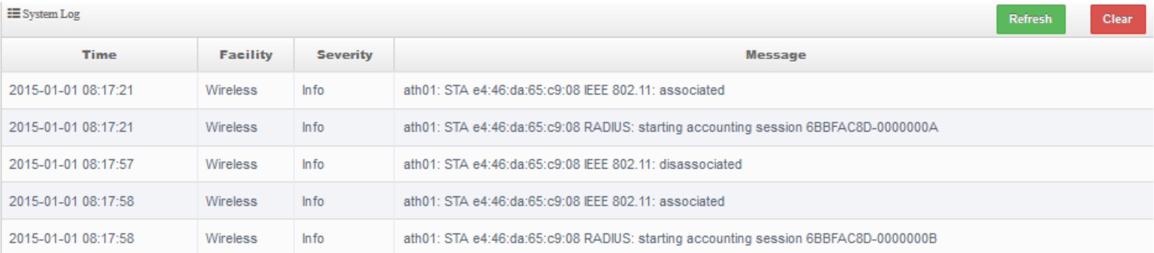
Authentication Zone Log

Date	VLAN#	Detail
-	-	-

- ➢ **Date:** Administrator can select dates.
- ➢ **VLAN:** Administrator can select VLANs.
- ➢ **Detall**: Administrator can clicl button to open detall information.

8.5 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

Time	Facility	Severity	Message
2015-01-01 08:17:21	Wireless	Info	ath01: STA e4:46:da:65:c9:08 IEEE 802.11: associated
2015-01-01 08:17:21	Wireless	Info	ath01: STA e4:46:da:65:c9:08 RADIUS: starting accounting session 6BBFAC8D-0000000A
2015-01-01 08:17:57	Wireless	Info	ath01: STA e4:46:da:65:c9:08 IEEE 802.11: disassociated
2015-01-01 08:17:58	Wireless	Info	ath01: STA e4:46:da:65:c9:08 IEEE 802.11: associated
2015-01-01 08:17:58	Wireless	Info	ath01: STA e4:46:da:65:c9:08 RADIUS: starting accounting session 6BBFAC8D-0000000B

- ➢ **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 ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] / ; ` , . =
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	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