

# **CERIO Corporation**

**CenOS 5.0**

**User Manual**

**for**

**OW-408 A1-MESH**

**eXtreme Power Wave2 4X 2x2 +8dBi Dual-Band  
MAN-MESH Outdoor CPE/AP**



## Content

|       |   |    |
|-------|---|----|
| 1.    | Device and Software Configuration .....                     | 7  |
| 1.1   | Device & Antenna appearance & RJ-45 Ports description ..... | 7  |
| 1.2   | Setup preparation of AP.....                                | 7  |
| 1.3   | Login Web Page .....  | 10 |
| 2.    | Operating Mode Introduction .....                           | 11 |
| 2.1   | MAN-Mesh Mode (Default ).....                               | 11 |
| 2.2   | Access Point Mode .....                                     | 12 |
| 2.3   | Client Bridge + Repeater Mode.....                          | 14 |
| 2.4   | WISP + Repeater AP Mode .....                               | 15 |
| 2.5   | CAP mode (Centralizes Access Point).....                    | 16 |
| 3.    | System Configuration .....                                  | 17 |
| 3.1   | Management.....   | 17 |
| 3.2   | Configure Time Server .....                                 | 20 |
| 3.3   | SNMP .....  | 21 |
| 3.4   | Configure Time Policy .....                                 | 22 |
| 4.    | MAN-MESH Mode .....   | 24 |
| 4.1   | VLAN Setup .....  | 26 |
| 4.1.1 | VLAN List .....   | 26 |
| 4.1.2 | VLAN Wireless Access Point Network Setup .....              | 28 |
| #     | Network Pull-down menu .....                                | 29 |
| 4.1.3 | IPv4 Bridge .....   | 30 |
| 4.1.4 | DHCP Server .....   | 37 |
| 4.1.5 | Radio 0(2.4G)/Radio 1(5G) Access Point Setup.....           | 42 |
| 4.1.6 | MAC Filter .....  | 45 |
| 4.1.7 | 802.11r Fast Roaming Setup.....                             | 46 |
| 4.2   | Wireless Configuration .....                                | 48 |

|       |   |    |
|-------|---|----|
| 4.2.1 | Mesh Radio 0 (2.4G) Setup.....                    | 48 |
| 4.2.2 | Mesh Radio 1 (5G) Setup.....                      | 51 |
| 4.2.3 | Advanced Setup.....                               | 55 |
| 4.2.3 | WMM Setup .....                                   | 57 |
| 4.3   | MAN-Mesh.....                                     | 60 |
| 4.3.1 | MAN-Mesh Common Setup.....                        | 60 |
| 4.3.2 | MAN-Mesh Device Setup .....                       | 63 |
| 4.4   | Change Other Setup modes.....                     | 68 |
| 5.    | Access Point mode .....                           | 69 |
| 5.1   | Change Setup mode.....                            | 69 |
| 5.2   | VLAN Setup .....                                  | 69 |
| #     | Network Setup.....                                | 71 |
| #     | Network Pull-down menu .....                      | 72 |
| 5.2.1 | DHCP Server .....                                 | 73 |
| 5.2.2 | Bandwidth Control .....                           | 75 |
| 5.2.3 | Radio 0(2.4G)/Radio 1(5G) Access Point Setup..... | 76 |
| 5.2.4 | MAC Filter .....                                  | 79 |
| 5.2.5 | 802.11r Fast Roaming Setup.....                   | 80 |
| 5.3   | Authentication .....                              | 82 |
| 5.3.1 | Enable Authentication function.....               | 82 |
| 5.3.2 | Set Authentication function .....                 | 84 |
| #     | Google OAuth2.0 setup sample .....                | 86 |
| #     | Facebook OAuth2.0 setup sample .....              | 90 |
| 5.3.3 | POP3/IMAP Server .....                            | 93 |
| 5.3.4 | Customize Page .....                              | 94 |
| i.    | Language.....                                     | 96 |

|       |                                 |     |
|-------|---------------------------------|-----|
| ii.   | Walled Garden .....             | 97  |
| iii.  | Privilege Address .....         | 97  |
| iv.   | Bulk MAC Address .....          | 98  |
| v.    | Profile .....                   | 99  |
| 5.4   | RADIUS Server .....             | 100 |
| 5.5   | RADIUS Account Setup.....       | 100 |
| 5.6   | Wireless Configuration .....    | 102 |
| 5.6.1 | Radio 0 (2.4G) Setup .....      | 102 |
| 5.6.2 | Radio 1(5G) Setup.....          | 104 |
| 5.6.3 | Advanced Setup.....             | 106 |
| 5.6.4 | WMM Setup .....                 | 108 |
| 5.6.5 | WDS Setup .....                 | 110 |
| 5.6.6 | WDS Status.....                 | 113 |
| 6.    | Client Bridge Mode.....         | 114 |
| 6.1   | Change Setup mode.....          | 114 |
| 6.2   | Configure LAN Setup.....        | 114 |
| 6.3   | Configure DHCP Setup .....      | 117 |
| 6.4   | Wireless General Setup.....     | 119 |
| 6.4.1 | Radio 0(2.4G) Basic Setup ..... | 119 |
| 6.4.2 | Radio 1 (5G) Basic Setup .....  | 121 |
| 6.4.3 | Advanced Setup.....             | 123 |
| 6.4.4 | WMM Setup .....                 | 126 |
| 6.4.5 | Station Setup.....              | 128 |
| 6.4.6 | Repeater AP Setup.....          | 130 |
| 6.4.7 | MAC Filter Setup.....           | 132 |
| 6.4.8 | 802.11r Fast Roaming Setup..... | 133 |



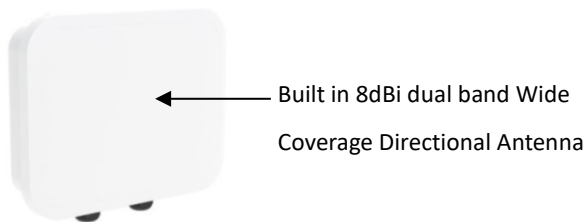
|           |                                  |            |
|-----------|----------------------------------|------------|
| <b>7.</b> | <b>WISP Mode .....</b>           | <b>136</b> |
| 7.1       | Change Setup mode .....          | 136        |
| 7.2       | Configure WAN Setup .....        | 136        |
| 7.3       | Configure LAN Setup .....        | 140        |
| 7.4       | Configure DHCP Setup .....       | 143        |
| 7.5       | Wireless General Setup .....     | 145        |
| 7.5.1     | Radio 0 (2.4G) Basic Setup ..... | 145        |
| 7.5.2     | Radio 1 (5G) Basic Setup .....   | 147        |
| 7.5.3     | Advanced Setup .....             | 150        |
| 7.5.4     | WMM Setup .....                  | 152        |
| 7.5.5     | Station Setup .....              | 154        |
| 7.5.6     | Repeater AP Setup .....          | 156        |
| 7.5.7     | MAC Filter Setup .....           | 158        |
| 7.5.8     | 802.11r Fast Roaming Setup ..... | 159        |
| 7.6       | Advanced Setup .....             | 162        |
| 7.6.1     | DMZ .....                        | 162        |
| 7.6.2     | IP Filter .....                  | 163        |
| 7.6.3     | MAC Filter .....                 | 165        |
| 7.6.4     | Virtual Server .....             | 165        |
| 7.6.5     | Access Control .....             | 167        |
| <b>8.</b> | <b>CAP Mode .....</b>            | <b>169</b> |
| 8.1       | Change Setup mode .....          | 169        |
| 8.2       | VLAN Setup .....                 | 169        |
| 8.3       | AP Control .....                 | 172        |
| 8.3.1     | Scan Device .....                | 172        |
| 8.3.2     | Batch Setup .....                | 174        |

|   |  |     |
|---|--|-----|
| 8.3.3                                     | AP Setup .....   | 177 |
| 8.3.4                                     | Group Setup .....                                      | 178 |
| 8.3.5                                     | Map Setup.....   | 178 |
| 8.3.6                                     | Authentication Profile.....                            | 181 |
| 8.3.7                                     | Status.....  | 181 |
| 8.4                                       | MAN-Mesh Control.....                                  | 183 |
| 8.4.1                                     | MAN-Mesh Device list .....                             | 183 |
| 8.4.2                                     | MAN-Mesh Status .....                                  | 183 |
| 9.  | Utilities .....  | 184 |
| 9.1                                       | Profile Setting.....                                   | 184 |
| 9.2                                       | System Upgrade .....                                   | 185 |
| 9.3                                       | Network Utility.....                                   | 187 |
| 9.4                                       | Reboot .....   | 188 |
| 10.                                       | Status .....   | 188 |
| 10.1                                      | Overview.....  | 189 |
| 10.2                                      | Wireless Client.....                                   | 190 |
| 10.3                                      | Online Users.....                                      | 191 |
| 10.4                                      | Authentication Log .....                               | 192 |
| 10.5                                      | MAN-Mesh Link Chart.....                               | 193 |
| 10.6                                      | MAN-Mesh Client .....                                  | 195 |
| 10.7                                      | System Log .....                                       | 196 |
| 11.                                       | [ Other technical documents] .....                     | 197 |
| 11.1                                      | Point to Point / Multi-Point for WDS settings .....    | 197 |
| 11.2                                      | Apply CERIO web authentication login page sample ..... | 198 |
| Appendix A. WEB GUI Valid Characters..... |  | 205 |

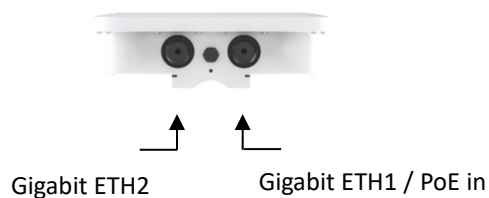
## 1. Device and Software Configuration

### 1.1 Device & Antenna appearance & RJ-45 Ports description

#### 1. 2x2 Antenna Description



#### 2. RJ-45 Ports Description

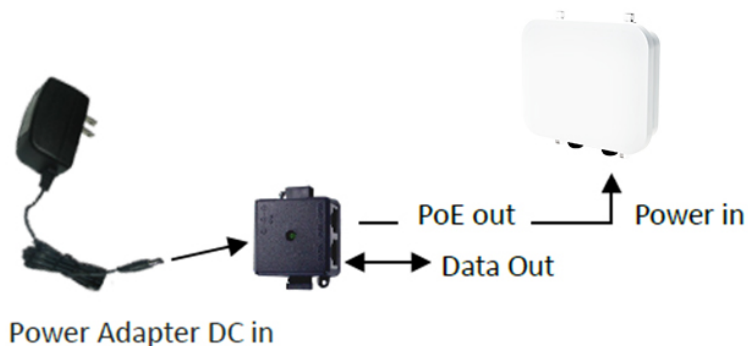


### 1.2 Setup preparation of AP

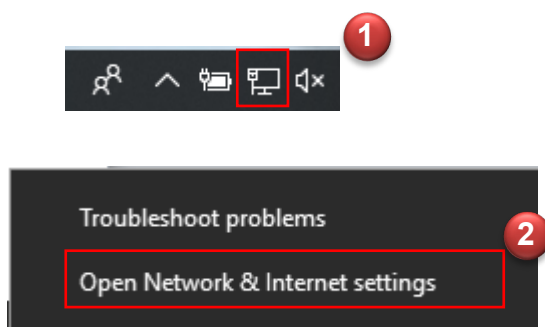
Please PC link to Device used cat5/6 Ethernet cable.

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

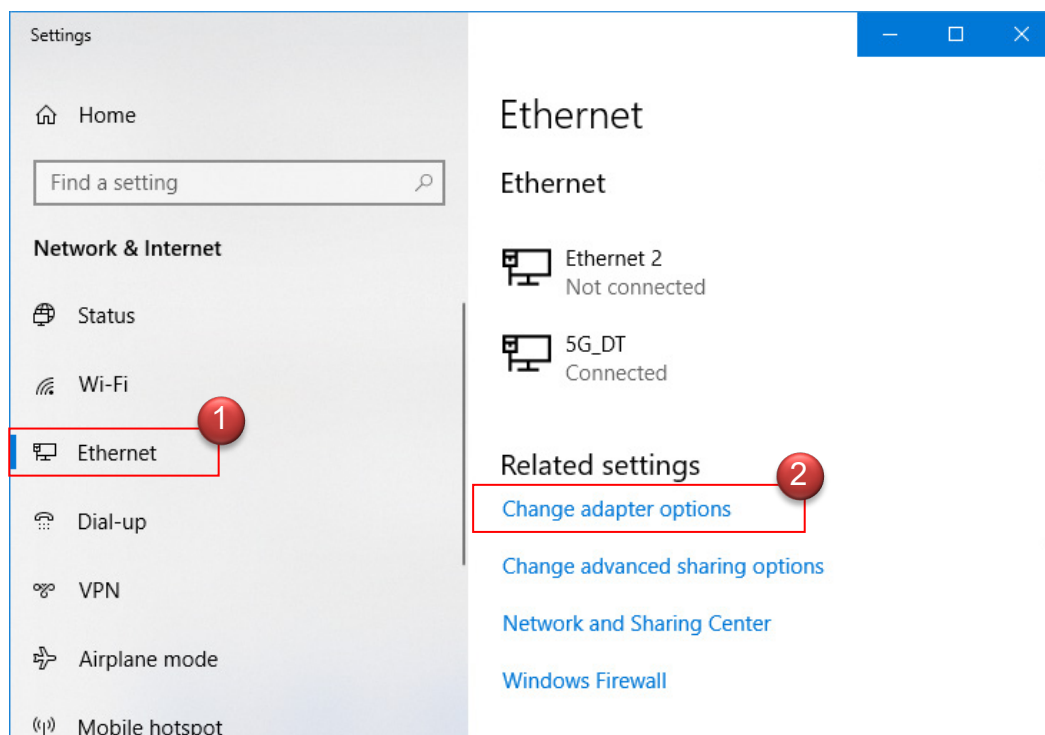
Basic connection diagram:



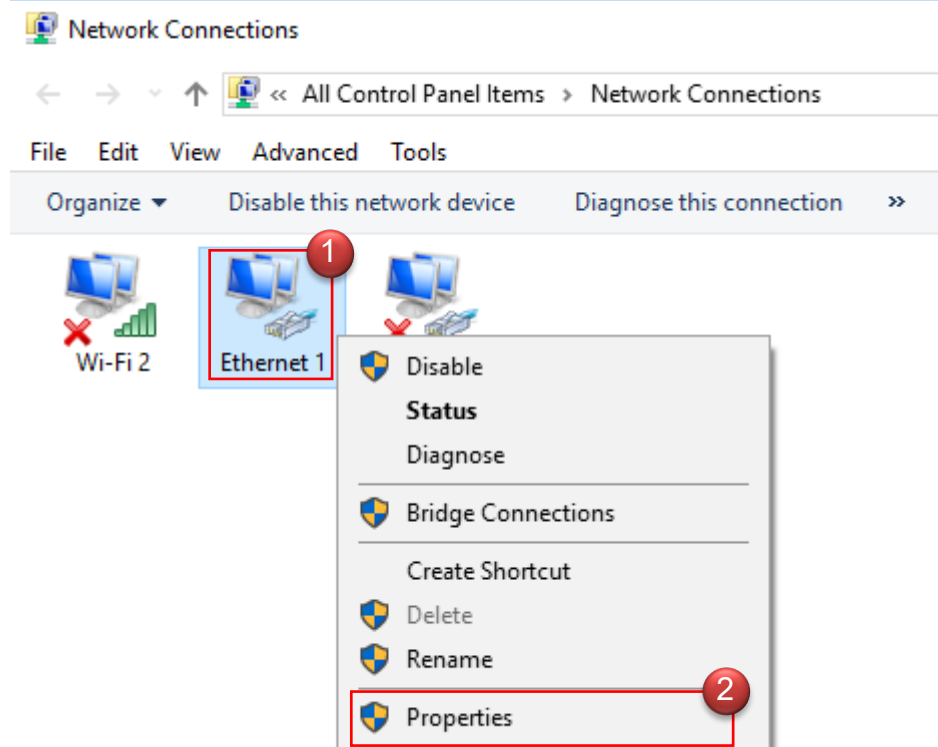
**Step 1:** Please click on the computer icon in the bottom right window, and click “Open Network and Internet settings”



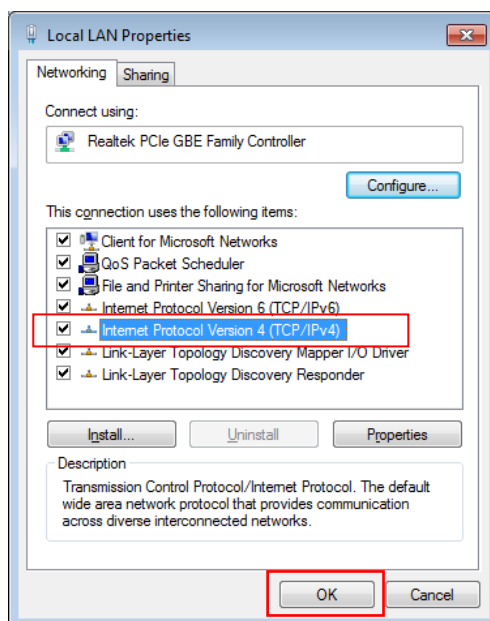
**Step 2:** After click left side "Ethernet" function, click on the right side “Change adapter options” again.



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



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



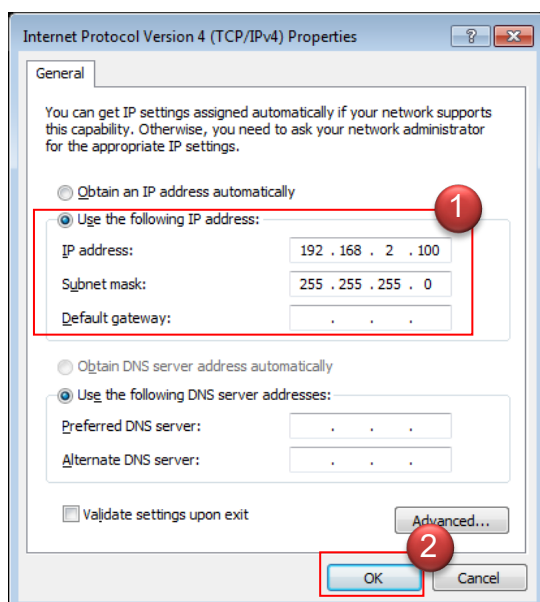
**Step 5 :**

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

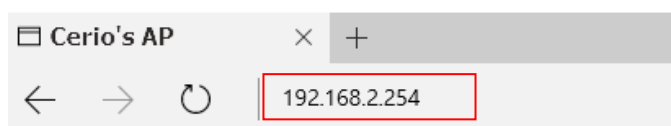
And Click "**OK**" to complete the fixed computer IP setting



## 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.



### System Login

Sign in  
<http://192.168.2.254>  
 Your connection to this site is not private

|          |         |
|----------|---------|
| Username | root    |
| Password | default |

Sign in Cancel

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



The screenshot displays the CERIO web interface. On the left, the 'Overview' tab is active, showing system information: Mode (Mesh Mode), System Name (OW-408\_A1), System Time (2015/01/01 08:49:30), System Uptime (49:47), Firmware Version (Pme-CPE-IPQ40XX-CERIO V1.0.7), Firmware Date (2020/04/29 14:40:53), ETH0 MAC Address (00:11:a3:dd:00:11), Wifi0 MAC Address (00:11:a3:dd:00:13), Wifi1 MAC Address (00:11:a3:dd:00:14), Gateway (10.0.2.1), DNS1 (192.168.2.1), DNS2, and Port Link status. On the right, the 'Information' tab shows three gauges: CPU Usage (8%), Memory (40%), and Wireless Client (0). Below these, the 'Radio 0' configuration is shown with Band Mode (802.11b/g/n), Channel (7), and Rate (400.0 Mb/s). The 'Radio 1' configuration shows Band Mode (802.11ac), Channel (153), and Rate (866.7 Mb/s).

## 2. Operating Mode Introduction

### Notice

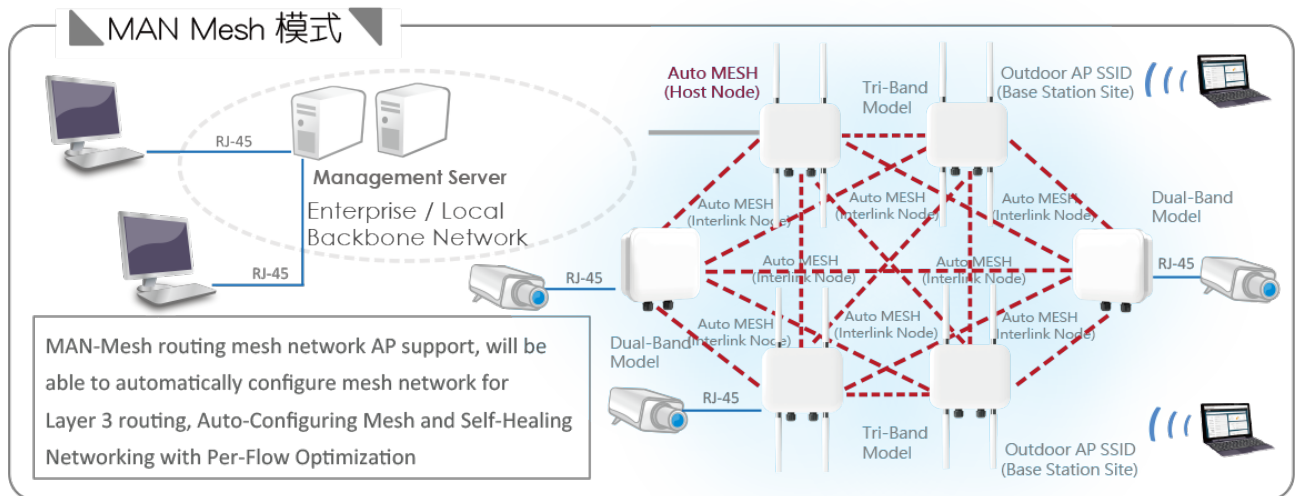
The default mode for the first login of the system is "MAN-Mesh mode". Please decide which mode to use the application requirements. You can refer to the following model application instructions to use the correct model.

If administrators need to switch to other modes, they can apply the change mode under "System Management → Mode Setup" in the menu (refer to manual 4.4 "Switch to other setting operation modes" to setting your instructions)

### 2.1 MAN-Mesh Mode (Default )

After switching MAN-Mesh mode, at first, set one as MAN-Mesh AP "host node", and then successively to set other stations as the MAN-Mesh AP "interlink node", and sequentially expand the network nodes to increase the coverage.

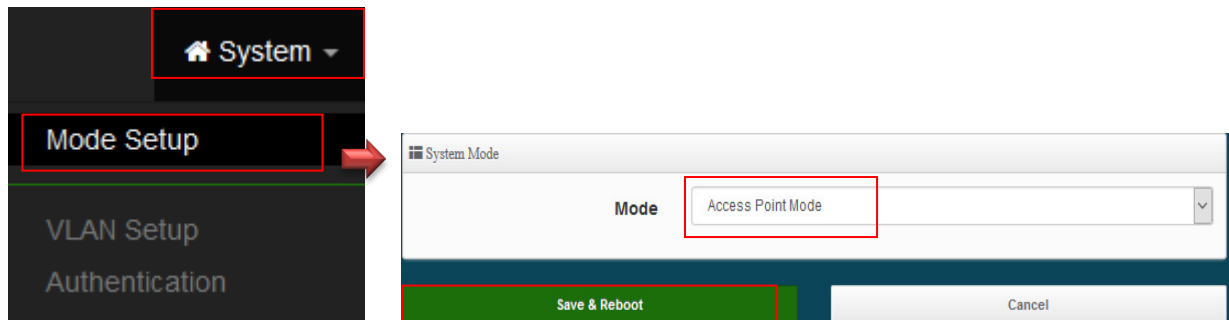
MAN-Mesh mode is a mesh network wireless system, using Layer3 Intelligent WiFi Mesh technology, which is simple to set up, easy to deploy and supports characteristics of multi-node architecture. The The MAN-Mesh mode is a mesh network wireless system, using Layer3 Intelligent WiFi Mesh technology, which is simple to set up, easy to deploy and supports characteristics of multi-node architecture. The MAN-MESH provides Intelligent WiFi Mesh technology with Multi-Channel Routing wireless mechanism.



It's suitable for a backbone network development and solution for backhaul deployment of Semi-Mobile mesh network, such as data transmission of the public transport system (ex. Railways, Ships, Bus, MRT, Gondola, etc.) In addition, it's also the perfect solution for the Intersection monitor Backhaul Deployment.

## 2.2 Access Point Mode

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

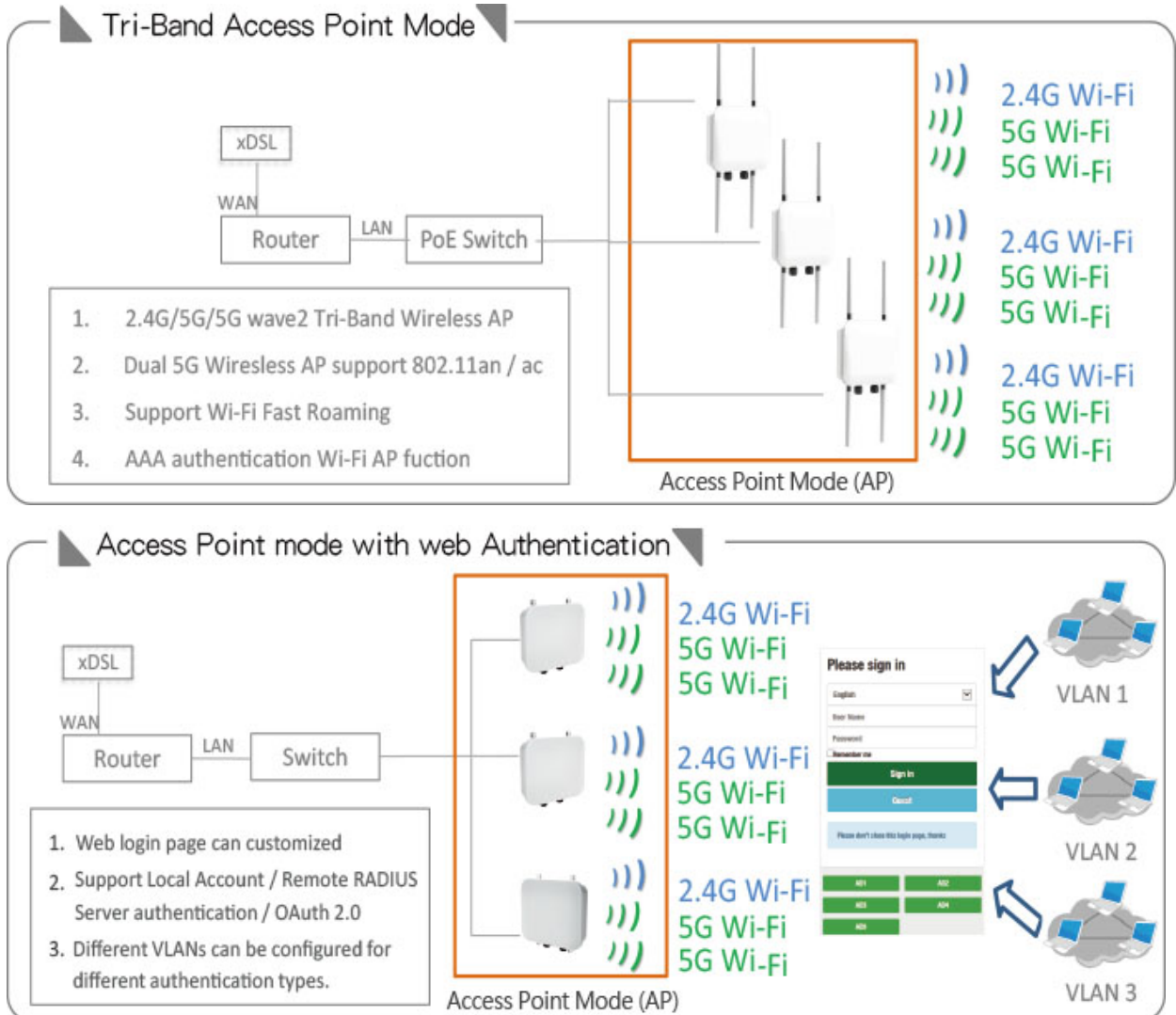


When you want to use the wireless method to access the Internet, you can convert the device to the Access Point mode..

- 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

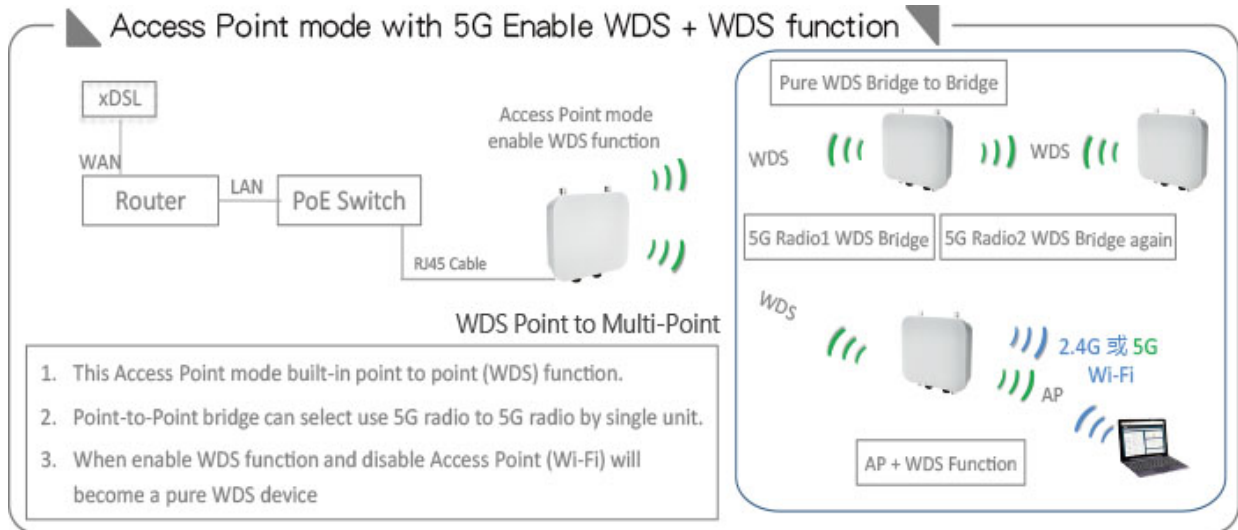


- This enables the wireless interconnection of Access Point in a IEEE802.11 network and accepts wireless
- Support Captive Portal authentication.



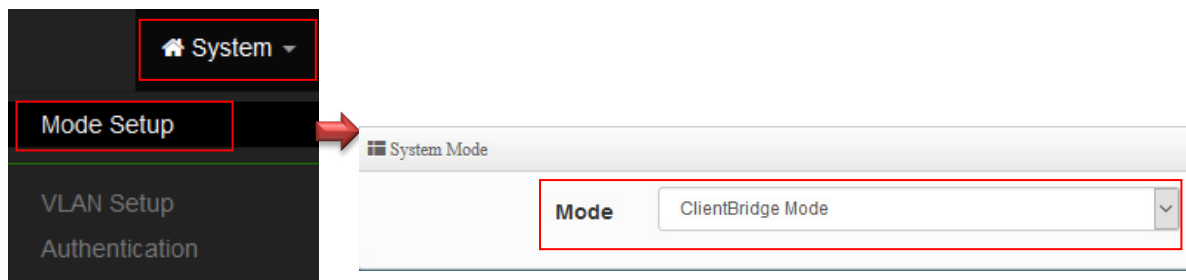
## Application of WDS function in Access Point mode

WDS can be used for long-distance point-to-point wireless connections, as well as applications for long-distance point-to-multipoint wireless connections. You can enable the WDS function under the Access Point (AP Mode), which is an application of AP + WDS, which means that the device can also use the services of the Access Point (AP station), it can be used for long distance with another AP through WDS.



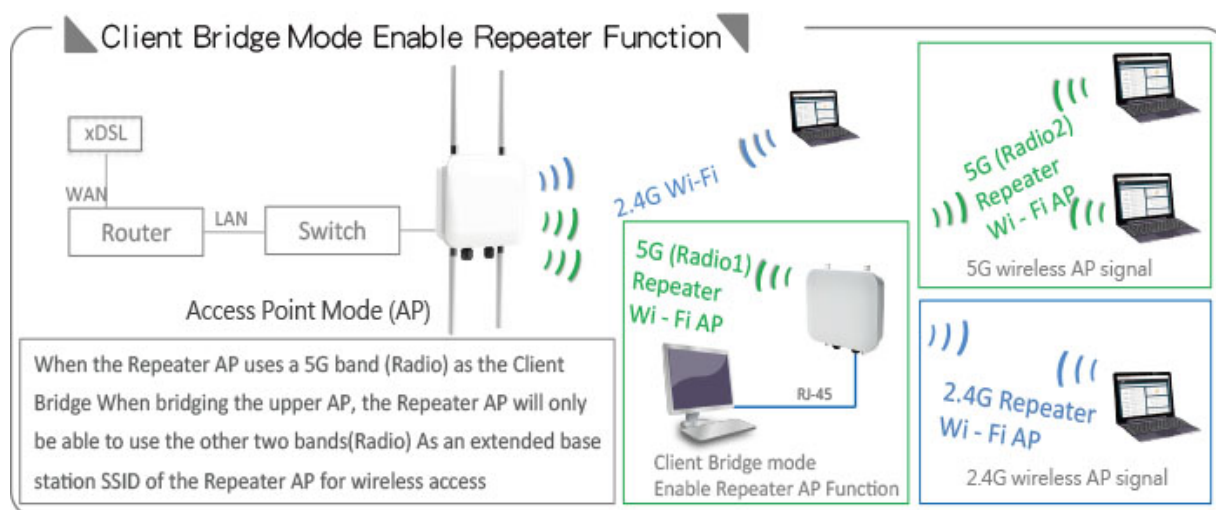
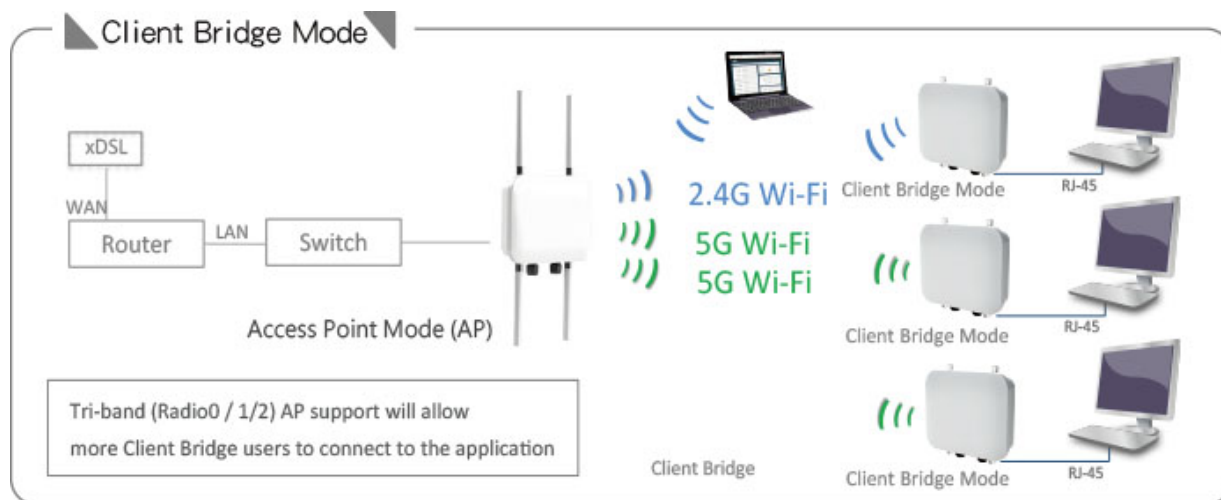
## 2.3 Client Bridge + Repeater Mode

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



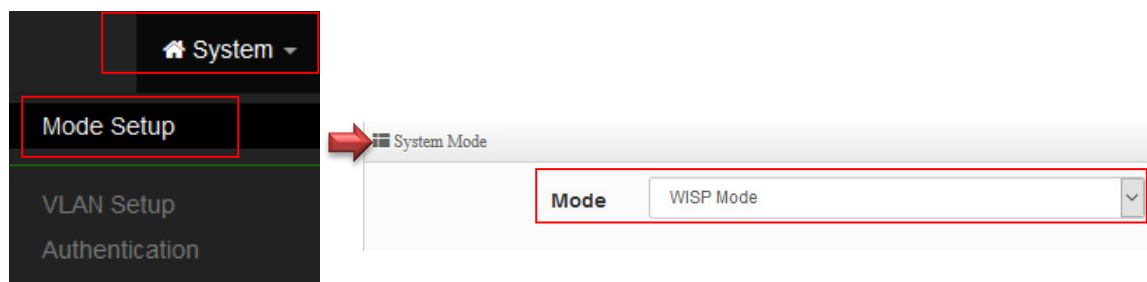
Client Bridge mode, which is responsible for wireless connection with the upper Access Point station(AP). the device must be bridged with the upper Access Point station(AP) for normal operation, and the Repeater extended Access Point station(AP) can be used normally after bridging with the upper AP.

- 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 AP and it accepts wireless connections from client devices. You can disabled the repeater extending AP function, which will enable the “AP Client ” function



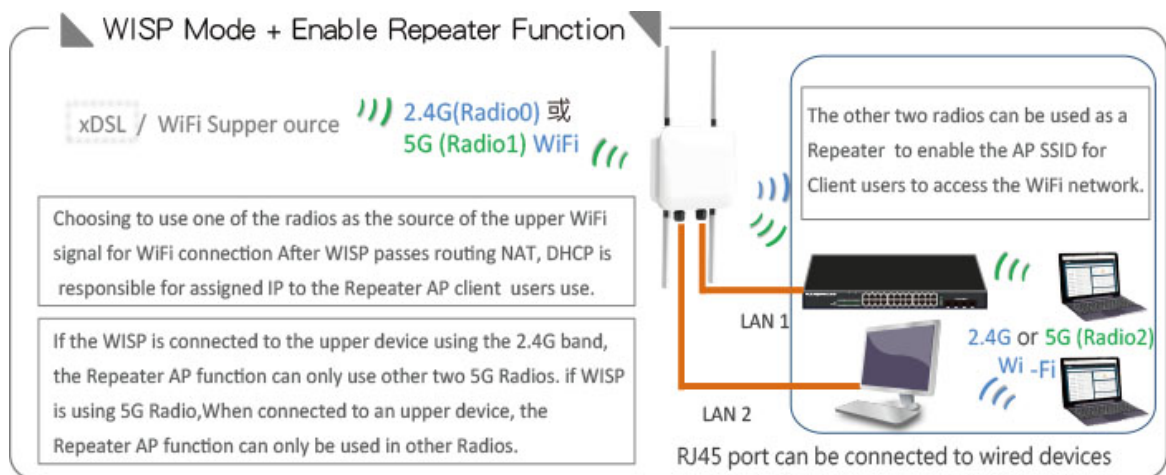
## 2.4 WISP + Repeater AP Mode

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



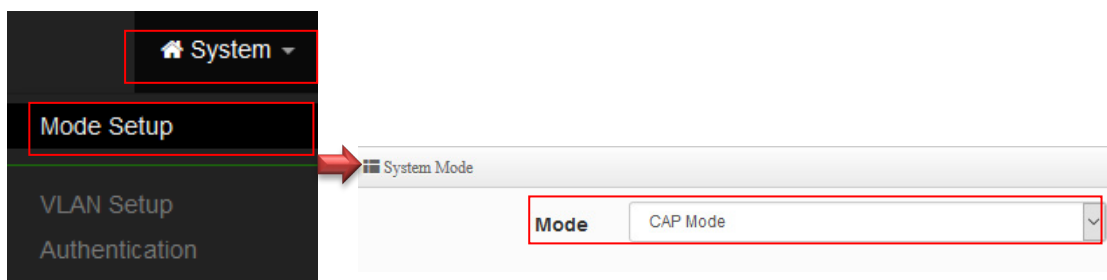
WISP's WAN end wirelessly bridges the upper xDSL AP. The connection method supports dynamic IP, static IP, PPPoE and PPTP. When sharing to all network through NAT.

- It can be used as an WISP (Wireless Internet Service Provide) 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 AP, and, in WISP (CPE) mode, it does not accept wireless association from wireless clients.



## 2.5 CAP mode (Centralizes Access Point)

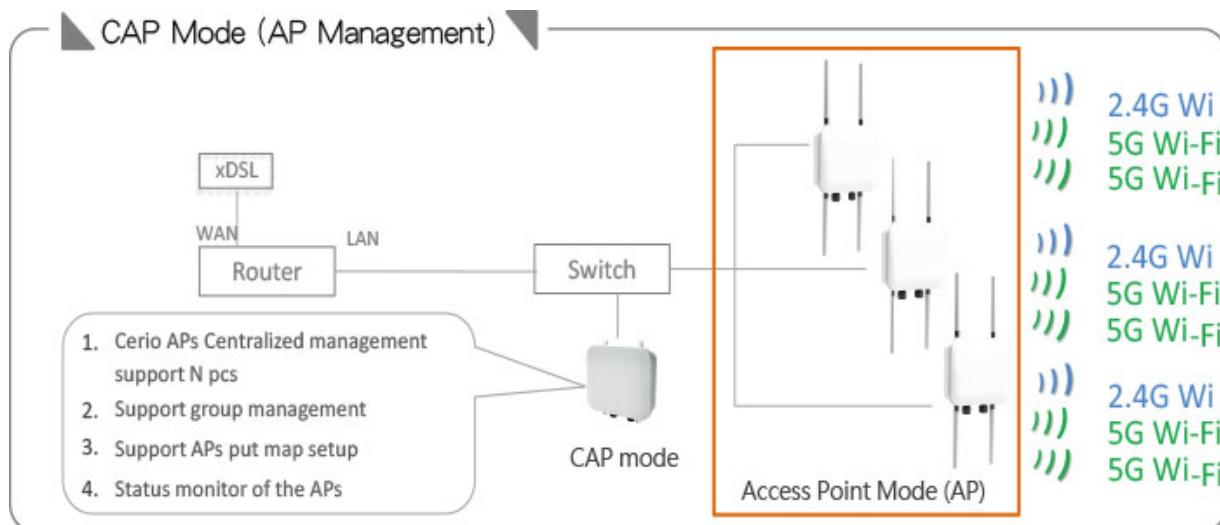
Please click on System -> Mode Setup and choose CAP Mode



After switching the CAP mode, this mode is not a wireless AP, Is a central centralized manager, which for the centralized management of multiple wireless APs in AP mode. It can mainly perform centralized settings, VLAN management, and AP monitoring. All the wireless APs in the CenOS5.0 series are under centralized control and management.

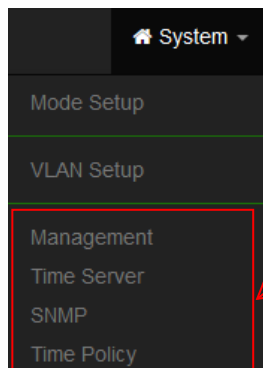
- Control Management of CenOS5.0 APs
- AP Management support 802.1Q VLAN infrastructure
- Centralized setting Access Point function and firmware upgrade.
- APs Group management for concept.





## 3. System Configuration

### Notice

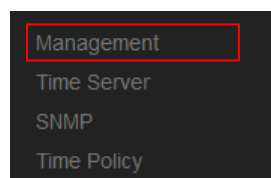


There are common functions in any mode have management / Time Server / SNMP and Time Policy. Please refer to the following detailed instructions.

### 3.1 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.



The screenshot displays the CERIO web interface with the following sections:

- System Language:** A dropdown menu set to "English".
- System Information:** Fields for "System Name" (OW-408\_A1), "Description" (eXtreme Power Wave2 11N/ac 2.4/5Ghz 2x2 +18dBi Out), and "Location".
- Root Password:** Fields for "New Root Password" and "Check Root Password".
- Port Isolate:** Radio buttons for "Enable" and "Disable" (selected).
- LED Control:** Radio buttons for "LED OFF", "Enable", and "Disable" (selected).
- Login Methods:** Checkboxes and port numbers for HTTP (80), HTTPS (443), Telnet (23), and SSH (22). A "Host Key Fingerprint" field shows "ssh-rsa AAAAB3NzaC1yc2EAAAADAQAE" with a "Generate Key" button. An "Access WAN" section has radio buttons for "Enable" and "Disable" (selected).
- System Log Setup:** A "Remote Server" checkbox and a "Port" field set to 514.
- Auto Reboot:** A "Type" dropdown menu set to "Disable".

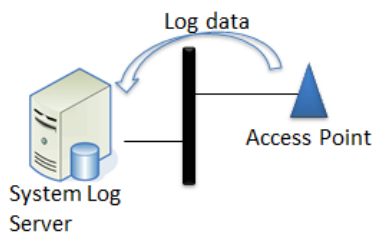
- **System Language:** Administrator can select system language for English and Traditional Chinese
- **System Information:** Administrator can set the system name / Description and Location.
- **Root Password:** Administrator can change system login password.
- **LED Control :** When system working 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.

The screenshot shows the "Ping Watchdog" configuration section with the following fields:

- Ping Watchdog:** A checkbox that is checked, followed by an IP address field containing "8.8.8.8" and a label "IP Address".
- Interval:** A text field containing "30" and a label "Seconds".
- Delay:** A text field containing "100" and a label "Seconds".
- Times of faults:** A text field containing "3" and a label "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.
- **Access WAN:** Administrator can enable and disable login access from WAN Public IP address(This function only for WISP Model)

- **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

☐ Sun
 ☐ Mon
 ☐ Tue
 ☐ Wed
 ☐ Thu
 ☐ Fri
 ☐ Sat

Hour

00

Minute

00

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

Auto Reboot

Type

Month

Monthly

☐ 01
 ☐ 02
 ☐ 03
 ☐ 04
 ☐ 05
 ☐ 06
 ☐ 07
 ☐ 08
 ☐ 09
 ☐ 10
 ☐ 11
 ☐ 12
 ☐ 13
 ☐ 14
 ☐ 15
 ☐ 16
 ☐ 17
 ☐ 18
 ☐ 19
 ☐ 20
 ☐ 21
 ☐ 22
 ☐ 23
 ☐ 24
 ☐ 25
 ☐ 26
 ☐ 27
 ☐ 28
 ☐ 29
 ☐ 30
 ☐ 31

Hour

00

Minute

00

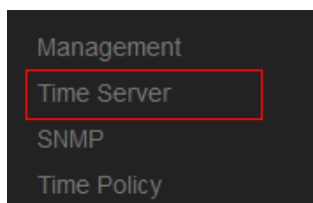
Click **“Save”** button to save your changes. And click **“Reboot”** button to activate your changes

## 3.2 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: 2015/01/01 08:01:19

Mode: ☐ NTP Server ☒ Manual

---

**User Setup** Set Time

Date(Y/M/D): 2019 12 4

Time(H:M:S): 15 59 31 (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 must to set the system time.

**User Setup** Set Time

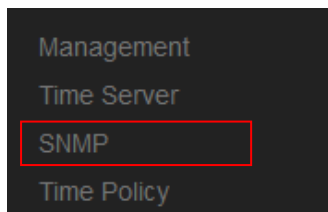
Date(Y/M/D): 2019 12 4

Time(H:M:S): 15 59 31 (GMT+8:00)

Click **"Set Time"** to activate your changes



## 3.3 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

The screenshot shows the 'SNMP v2c' configuration window. It has a title bar with a window icon and the text 'SNMP v2c'. Below the title bar, there are three radio buttons: 'Active', 'Enable', and 'Disable'. The 'Disable' button is selected. Below the radio buttons, there are two text input fields: 'RO Community' and '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

The screenshot shows the 'SNMP v3' configuration window. It has a title bar with a window icon and the text 'SNMP v3'. Below the title bar, there are three radio buttons: 'Active', 'Enable', and 'Disable'. The 'Disable' button is selected. Below the radio buttons, there are four text input fields: 'RO Username', 'RO Password', 'RW Username', and '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

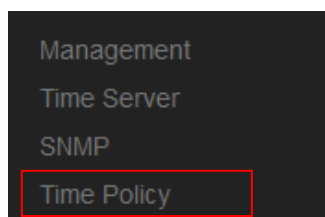
IP 3

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

## 3.4 Configure Time Policy



The administrator can set the time schedule. After setting the time schedule rules, specific functions can be applied.

Please click "System Settings" → "Time Policy" to enter the rule setting list, click the "Edit" button on the list to enter the time setting page.

| Policy List |          |             |                       |
|-------------|----------|-------------|-----------------------|
| #           | Comment  | Mode        | Edit                  |
| 1           | Policy 1 | On Schedule | <button>Edit</button> |
| 2           | Policy 2 | On Schedule | <button>Edit</button> |
| 3           | Policy 3 | On Schedule | <button>Edit</button> |
| 4           | Policy 4 | On Schedule | <button>Edit</button> |
| 5           | Policy 5 | On Schedule | <button>Edit</button> |
| 6           | Policy 6 | On Schedule | <button>Edit</button> |

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

Time Policy Rules

Comment

Mode

☒ On Schedule
 ☐ Out Of Schedule

Policy List

Create New Policy

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

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

### Create New Policy button:

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

Time Policy Rules

Day of Week

☐ Sun
 ☐ Mon
 ☐ Tue
 ☐ Wed
 ☐ Thu
 ☐ Fri
 ☐ Sat

Start Time

End Time

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

### Notice

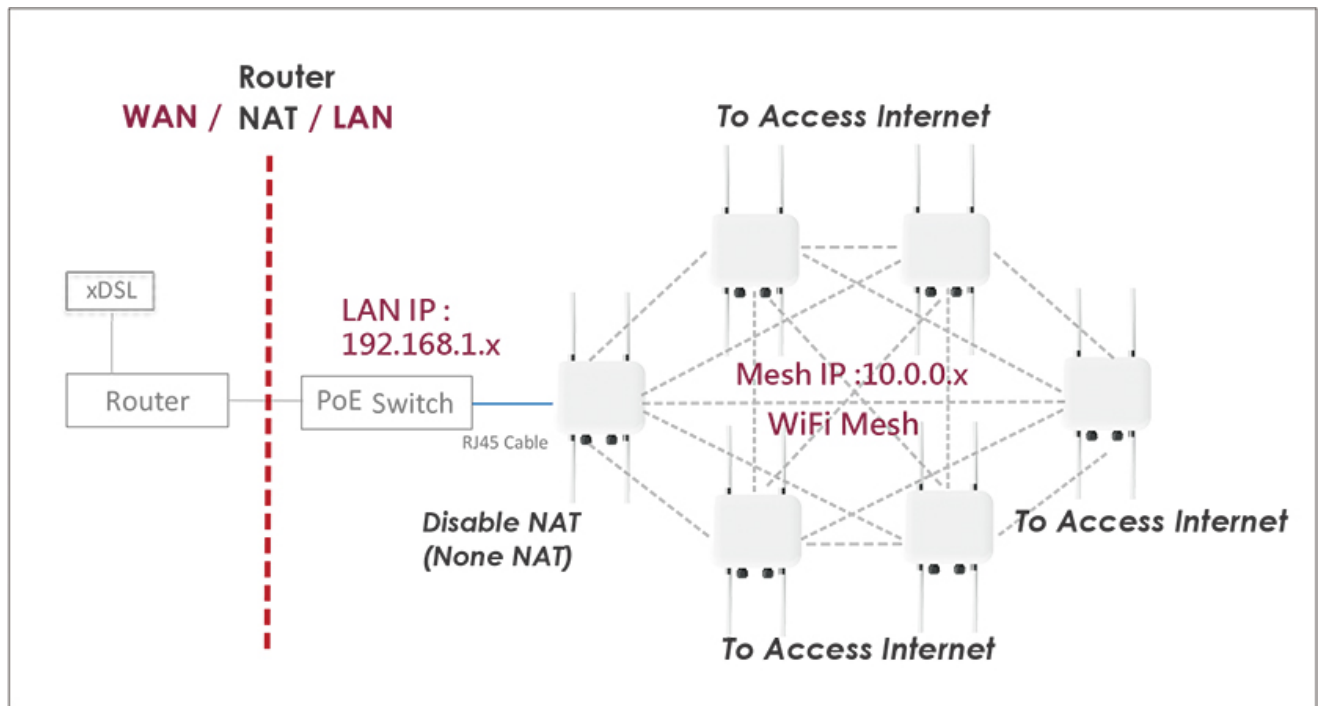
1. If you need to control the wireless signal switch, you must select "Wireless" => "Advanced Setup" => "RF on/off by Schedule" in "MAN MESH Mode" or "Wireless Access Mode" or "Client Bridge Mode" The set time rule group. For details, see [4.2.3 Advanced Setup](#).
2. If you need to control the MAC filter switch, go to "Advanced" => "MAC Filter " in "WISP Mode" and select the set time rule group. See [7.6.3 MAC filter](#) for details.
3. System protection mechanism, the system will confirm whether the system time is consistent with the NTP server time every 10 minutes. If the time is inconsistent, "Time Schedule" will not work to ensure that the machine will not shut down the connection in other time periods.

## 4. MAN-MESH Mode

MAN-Mesh WiFi has the capability of dynamic routing automatic path selection. The dynamic path selection includes the best path transmission of the Mesh Backbone network and the best dynamic path transmission of the WAN / Internet route.

### # Single LAN physical WAN Internet / backhaul access architecture

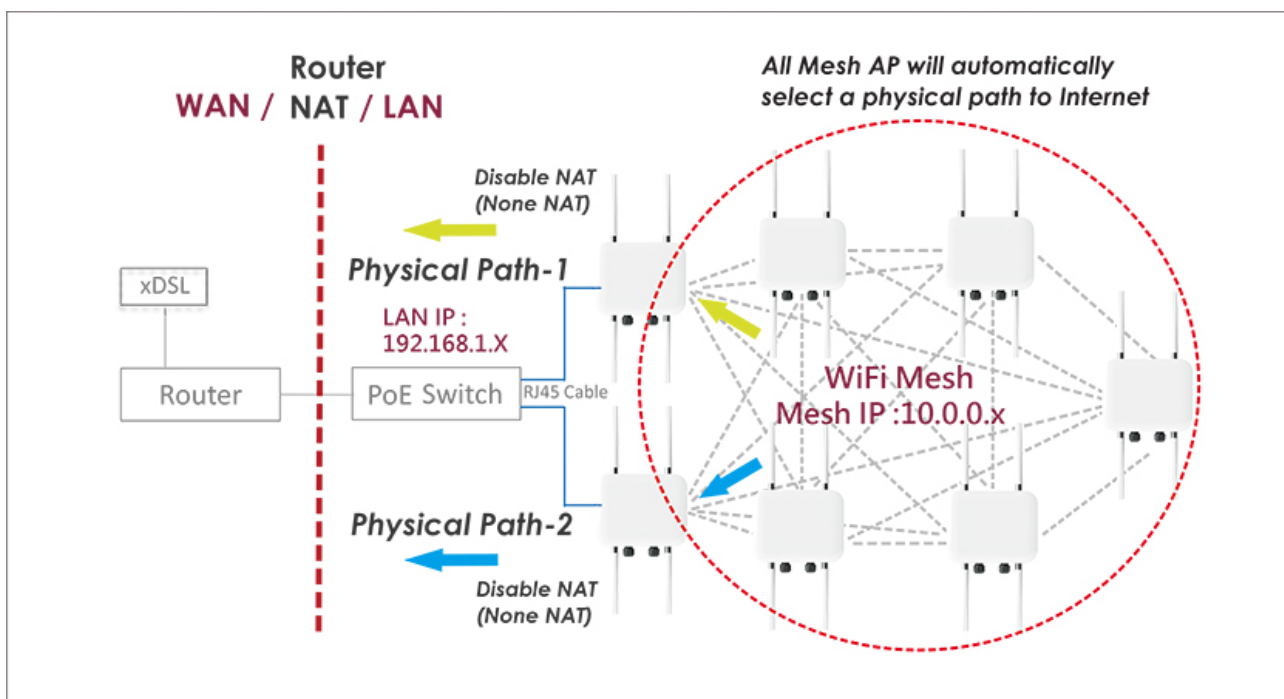
Under the interconnected MAN-Mesh AP environment, all the backhaul or WAN Internet access of the WiFi AP Station extension and its downstream LAN line will be transmitted through the Mesh backbone to the best link path back to the LAN physical line to the upstream connection.



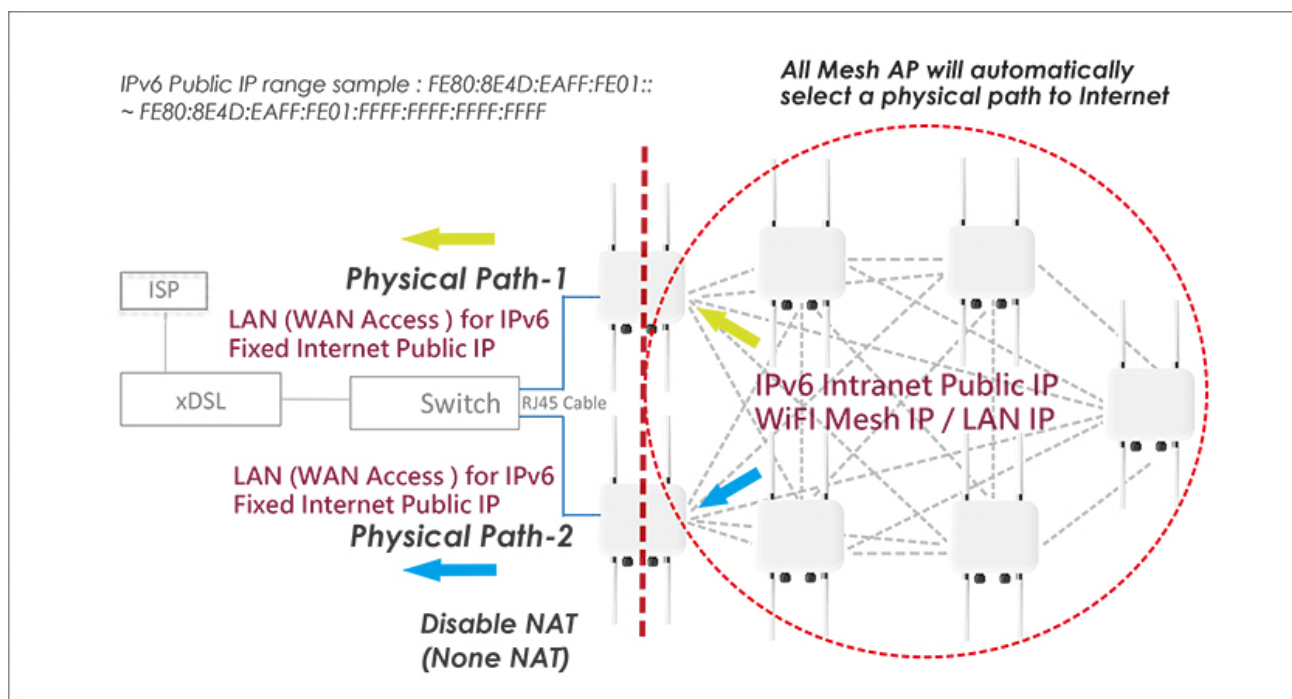
### # Multi-LAN physical WAN Internet / backhaul access architecture:

Under the condition of connecting MAN-Mesh APs, the WiFi AP Station extends all backhaul or WAN of its downstream LAN Internet access, it can transmit back through the best transmission of the mesh network and can be transmitted through the WAN / Internet route of the best dynamic path, automatically select the best available LAN connection, one of connects the upstream to achieve multiple WAN path backup connections.

When IPv4 IP Application :



When IPv6 IP Application :

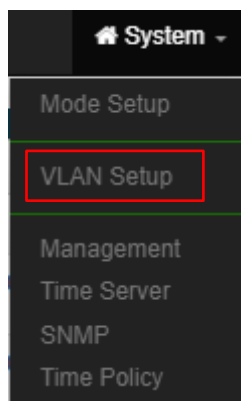
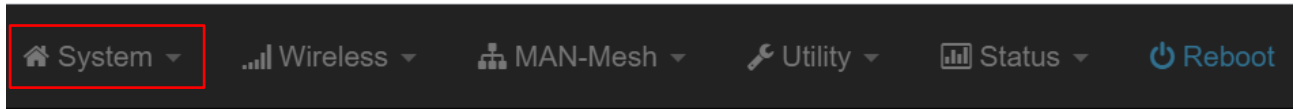




## 4.1 VLAN Setup

Under Man-Mesh mode, the administrator must set up the system's IP address, the network segment must be the same as the internal network domain, and the IP address can't be the same as other devices, otherwise it will cause conflicts

Setting the AP's (LAN) IP address and other functions, please click "System " -> ☐ "VLAN Setup".



After confirmed, it will finish the setting of each virtual network function, gateway and DNS address of the local VLAN.

### 4.1.1 VLAN List

Log in to the MAN-Mesh AP device to start basic LAN IP settings, click "System" -> ☐ "VLAN Setup" Press the network ☐ **Network** button then input the basic information such as IP address, subnet mask, default gateway, DNS ...etc.

#### Notice

If you want to set the virtual network LAN IP address of multiple MAN-Mesh AP devices, please be noticed that the LAN IP addresses of these devices cannot be the same, otherwise IP conflicts will occur and the network will not be connected. The MAN-Mesh AP LAN IP default IP is 192.168.2.254

- **#: Display virtual network group**
- **VLAN Status** : Display the current status of each group of VLANs enabled or disabled.
- **Flag** : Displays the Tag ID information of Virtual VLAN. When ☐ **Native ETH0** displayed , it indicates that the VLAN is currently enabled.
- **IP Address** : Displays the IP address of each VLAN.
- **Netmask** : : Display IP netmask.

- **Radio 0** : It is a 2.4Ghz radio. It can display the SSID name of 2.4Ghz in each VLAN and whether it is enabled (green is enabled, red is disabled).
- **Radio 1** : It is a 5Ghz radio, it can display the SSID name of 5Ghz in each VLAN and whether it is enabled (green is enabled, red means disabled)

| #  | Status | Flag        | IP Address      | Netmask       | Radio 0  | Radio 1 | Action  |
|----|--------|-------------|-----------------|---------------|----------|---------|---------|
| 0  | On     | Native ETH0 | 192.168.101.231 | 255.255.255.0 | 2.4_0_0  | 5G_0_1  | Network |
| 1  | Off    | ETH0.101    | -               | -             | 2.4_1_0  | 5G_1_1  | Network |
| 2  | Off    | ETH0.102    | -               | -             | 2.4_2_0  | 5G_2_1  | Network |
| 3  | Off    | ETH0.103    | -               | -             | 2.4_3_0  | 5G_3_1  | Network |
| 4  | Off    | ETH0.104    | -               | -             | 2.4_4_0  | 5G_4_1  | Network |
| 5  | Off    | ETH0.105    | -               | -             | 2.4_5_0  | 5G_5_1  | Network |
| 6  | Off    | ETH0.106    | -               | -             | 2.4_6_0  | 5G_6_1  | Network |
| 7  | Off    | ETH0.107    | -               | -             | 2.4_7_0  | 5G_7_1  | Network |
| 8  | Off    | ETH0.108    | -               | -             | 2.4_8_0  | 5G_8_1  | Network |
| 9  | Off    | ETH0.109    | -               | -             | 2.4_9_0  | 5G_9_1  | Network |
| 10 | Off    | ETH0.110    | -               | -             | 2.4_10_0 | 5G_10_1 | Network |
| 11 | Off    | ETH0.111    | -               | -             | 2.4_11_0 | 5G_11_1 | Network |
| 12 | Off    | ETH0.112    | -               | -             | 2.4_12_0 | 5G_12_1 | Network |
| 13 | Off    | ETH0.113    | -               | -             | 2.4_13_0 | 5G_13_1 | Network |
| 14 | Off    | ETH0.114    | -               | -             | 2.4_14_0 | 5G_14_1 | Network |
| 15 | Off    | ETH0.115    | -               | -             | 2.4_15_0 | 5G_15_1 | Network |

- **Action** : Click the network **Network** button to enter the LAN setting page. Click the drop-down arrow **Network** button to display the wireless setting function list.
- **Default Gateway** : Setting default gateway IP
- **DNS(1-2)** : Setting DNS(1-2) server IP

|    |     |          |   |   |          |         |         |
|----|-----|----------|---|---|----------|---------|---------|
| 13 | Off | ETH0.113 | - | - | 2.4_13_0 | 5G_13_1 | Network |
| 14 | Off | ETH0.114 | - | - | 2.4_14_0 | 5G_14_1 | Network |
| 15 | Off | ETH0.115 | - | - | 2.4_15_0 | 5G_15_1 | Network |

**Gateway**

Default Gateway

**DNS**

DNS1

DNS2

## Notice

You can set the IP address of the gateway in the architectural environment or the external DNS IP address (if there is no special needs, it is recommended to set at 8.8.8.8 which provided by Google or 168.95.1.1 provided by Chunghwa Telecom for public

### 4.1.2 VLAN Wireless Access Point Network Setup

Click the "Network" **Network** button to virtual network settings

Base on your needs, it can use as the backbone MAN-Mesh AP host, you also set as a wireless AP Station (SSID AP station) for the wireless device access, please turn on or off the wireless radios base on your needs for Access Point 0 (2.4G), Access Point 1 (5G). If enable the AP station function under MAN-Mesh mode, it can be using the backbone network of MAN-Mesh AP and also be used as a AP Station (Wireless AP) at the same time. Allow the wireless users log in and acces. That's MAN-Mesh AP+AP Station function. If you do not need this multiple function (SSID AP station), please skip this part of the setting (the default value is off).

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

## Notice

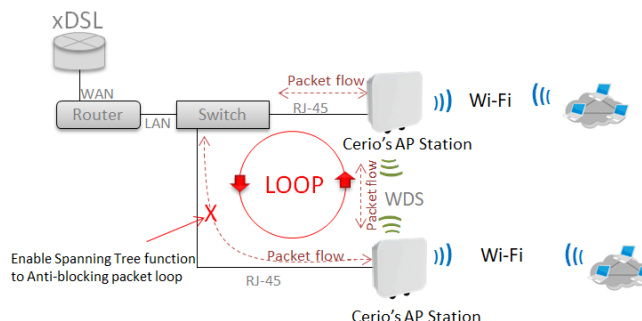
At least one VLAN will always be enabled by default

### Management

- **Access Point 0** : Administrator can Enable or Disable Radio 0(2.4G).
- **Access Point 1** : Administrator can Enable or Disable Radio 1(5G).
- **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



- **IAPP** : Administrator can select radio 2.4G or 5G for IAPP roaming.
- **VLAN Tag Setup**: Set the VLAN used tags.

## Notice

The IAPP condition must use WPA2-PSK Wi-Fi security and AES algorithm)

## Notice

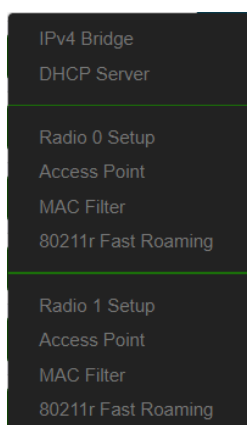
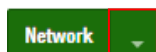
That if ETH0 is set to use a VLAN tag, you must enter the management interface with the same VLAN as the tag to enter the management settings. Otherwise, the VLAN domain is completely blocked.

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

## # Network Pull-down menu

Administrator can set DHCP Server and Radio 0(2.4G)/ Radio 1(5G) security for the access point and set 802.11r fast roaming.

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

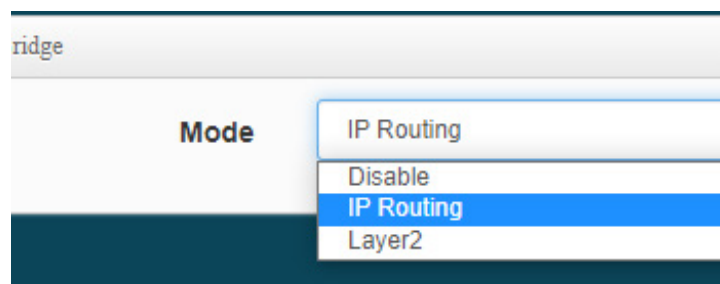
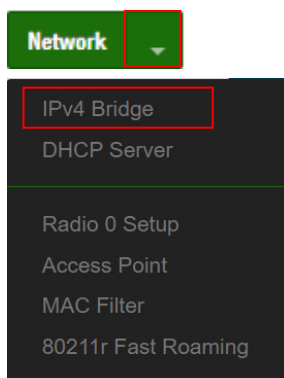


## 4.1.3 IPv4 Bridge

For the MAN-Mesh routing device operating with Layer 3 core in the MESH routing architecture environment, it will determine how to forward data packets based on the data in the Routing Table. Each Mesh host has its own IP address definition for different network segments. The Routing Table exchanges information with each other for communication and interconnection. To ensure that ARP table packets (including Layer 2 DHCP IP designated delivery and forwarding, etc.) calculated by Layer 2 can be successfully recognized in the Layer 3 environment, the Routing mode must be enabled. Or Layer 2's VxLan mode to cooperate.

Click “IPv4 Bridge” settings IPv4 Bridge related functions

### IP Routing Mode



IPv4 Bridge: IP Routing and Layer2 services can be selected.

**IP Routing :** Select and enable this IP Routing mode as the main Bridge mode of IPv4 Bridge.

**Static peer :** It has the same meaning as Static Routing. The manager manually enters and sets the IP location of the back-end LAN device to participate in the Mesh environment interconnection · manually specify the local physical LAN connection manually specify the LAN IP address, must have a LAN IP address which can connect in Mesh environment . Static peer can set up to 11 IP address.

## Notice

When the MAN-Mesh AP is operating, the Mesh WiFi network has its own Mesh WiFi interface IP address, which is different from the existing wired interface LAN IP address of device. When IPv4 Bridge function is enabled, the wired LAN user access through its own WiFi Mesh interface, other Mesh devices in the environment can be identified and communicated with each other. When you only need Internet Gateway WAN function under each MAN-Mesh LAN device but the devices without seeing or access each other. You don't need to enable this function.

## Notice

In the case of Mesh interconnection, if you want to migrate and change the originally specified Static Peer IP host address and set it to the Static Peer IP setting of the MAN-Mesh AP of another station, please be sure to delete the Static Peer in the original Mesh AP first Host IP address. After all the routing designation rules of the Mesh environment are released, proceed to another Mesh AP host to add the static Peer host address setting to be migrated.

Static Peer

IP Address

192.168.2.10

Add

**Static peer List :** It shows the LAN IP address of the LAN device that needs to communicate with the MAN-Mesh IP address.

| Static Peer List |              |        |
|------------------|--------------|--------|
| #                | IP Address   | Action |
| 1                | 192.168.2.10 | Delete |

**Notice**

Wrong static routing settings, such as adding a non-own MAN-Mesh AP back-end device to the MAN-Mesh AP settings of different stations (different network segments), or cross-setting or repeating to static backends of other stations (different network segments) When Peer (Static Routing) specifies the host IP, it will cause a conflict error in the specified Mesh routing.

**Notice**

To enable the normal operation of the network equipment at the lower end of the MESH, two methods can be used:

1. To use the IP routing mode, the upper router device needs to provide a static routing table, and fill in the bridge address IP of the MESH in the table. (If the upper router does not have this function, this method cannot be used)
2. Use Layer 2 VxLan mode. (You can connect and operate without complicated settings. If you have other connection requirements, please refer to the Layer2 mode settings below)

## Layer2 Mode

The screenshot displays the configuration interface for Layer2 Mode. It includes several sections:
 

- IPv4 Bridge:** Mode is set to Layer2.
- VXLAN Settings:** VXLAN VNI is 0, and Bridge Address is 10.0.1.1.
- Auto Link:** Auto Link is enabled, Interval is 180 seconds, Auto Link Layer is 3, and ARP Keepalive is enabled.
- Uplink Backup:** Uplink Backup is disabled, Ping Alive Interval is 5 seconds, and Failure Count is 3 times.
- Uplink IP Address List:** A table with 5 rows for IP addresses, with the first row containing 10.1.1.2.
- Auto Link Allow Address:** A field for Allow Address/Mask with an Add button.
- Auto Link Allow Address List:** A table with columns for #, IP Address/Mask, and Action.

**Layer2 :** Select and enable the Vxlan mode of this Layer 2 as the IPv4 Bridge.

This close-up shows the 'IPv4 Bridge' section with the 'Mode' dropdown menu set to 'Layer2'.

### Notice

The Layer2 Vxlan mode establishes a logical connection between entities between networks, and handles flow control and error detection during transmission. Layer2 encapsulates the digital signal of the physical layer into a data frame, where the frame contains the data link layer The MAC address used to identify the source address of the host data. Mainly used as an overlay (over a layer3 network) environment application.

### ➤ VXLAN Setting

The screenshot shows the 'VXLAN Settings' section with the following values:
 

- VXLAN VNI:** 0
- Bridge Address:** 10.0.1.1

- **VXLAN VNI** : Virtual Network ID ( VNI ) Virtual identification designation, the specified value of the virtual identification of each MAN-Mesh host connected to each other in the environment must be the same, and a maximum of 16,000,000 VxLAN logical network virtual identifications are supported. If there is no need for large-scale or multi-VLAN custom settings, it is recommended to keep the default tag value as 0.
- **Bridge Address** : Using Bridge to display the external operating IP. (The default display of this IP address is the minimum value of the IPv4 address customized for the connected MAN-Mesh device).

## ➤ Auto Link

The screenshot shows the 'Auto Link' configuration window. It includes the following elements:

- Auto Link**: A section header with a small icon.
- Auto Link**: Two radio buttons, 'Enable' (selected) and 'Disable'.
- Interval**: A text input field containing '180' and a dropdown menu currently showing 'Second'.
- Auto Link Layer**: A text input field containing '3'.
- ARP Keepalive**: Two radio buttons, 'Enable' (selected) and 'Disable'.

- **Auto Link** : You can choose to enable or disable, the default is "Enable".
- **Interval** : The reaction speed of mesh reconnection.
- **Auto Link Layer** : Automatically learning the ARP range of all the devices in the connection, the default is "3" Layer (layer jump), if the device is directly connected to the 5th unit, it can be set to "4" Layer (layer jump)
- **ARP Keepalive** : Information used to automatically monitor whether interconnected devices are working properly or prevent link interruption. The default value is enabled. If you specify the Bridge Uplink IP to manually set a custom design environment, you can disable this function without enabling automatic monitoring.



## ➤ Uplink Backup

Uplink Backup

Uplink Backup

☐ Enable
 ☒ Disable

Ping Alive Interval

5

Second

Failure Count

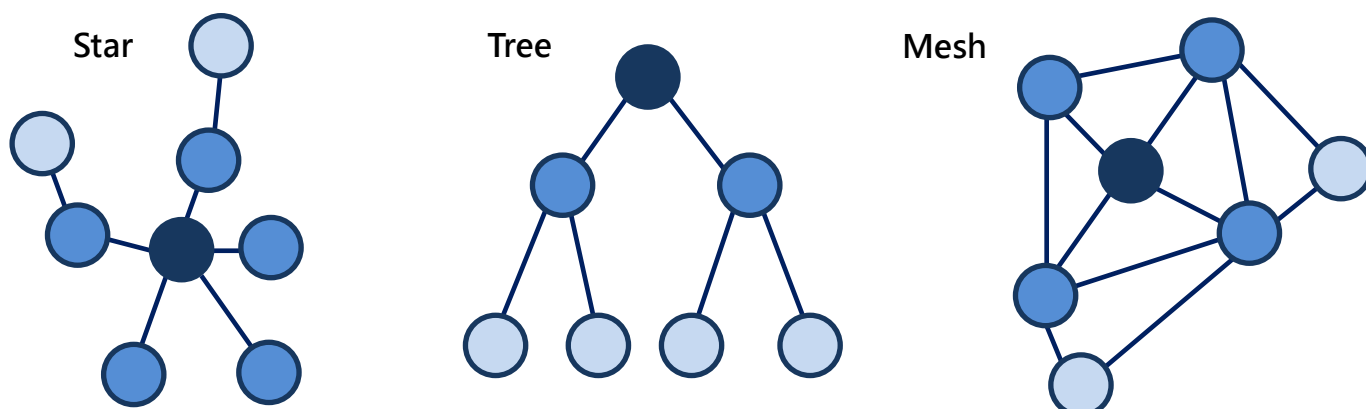
3

Times

- **Uplink IP Address** : You can choose to enable or disable, the default is "off", when the "off" state, it will automatically monitor the connection.
  - When Uplink Backup is enabled, the five groups of IPv4 bridge Uplink IP in the Uplink IP Address List: will always choose one group for use. The priority order is the first group. If the first group is lost and cannot be obtained, the second group will be used. Group IPv4 bridge Uplink IP... (The first group is the highest priority connection, only one group is connected at a time, if the first group is disconnected, the second group is connected, and so on).
  - When Uplink Backup is turned off, the five groups of IPv4 bridge Uplink IP settings in Uplink IP Address List: will take effect at the same time and be used at the same time.
- **Ping Alive Interval** : The number of seconds for the AP to ping Uplink IP Address.
- **Failure Count** : The allowable number of failures of the AP's ping Uplink IP Address. (If the AP pings the Uplink IP 3 times, but still fails, it will postpone the ping of the second group of Uplink IP)

### Notice

When setting, please do not set the Uplink IP Address to any of your own IP in the MAN-Mesh AP you are setting up the machine, including your own LAN IP address and MAN-MESH WiFi IP and your own Bridge Address. "Display IP (IPv4) Bridge IP) address, if the same Uplink IP specified host address is generated in the environment where the Mesh is interconnected, it will cause a conflict error in the Mesh routing designation.



## ➤ Uplink IP Address List

| # | IP位址                                  |
|---|---------------------------------------|
| 1 | <input type="text" value="10.0.1.2"/> |
| 2 | <input type="text"/>                  |
| 3 | <input type="text"/>                  |
| 4 | <input type="text"/>                  |
| 5 | <input type="text"/>                  |

- **Uplink IP Address List:** Display and fill in the IPv4 list of MAN-Mesh devices with priority designated connection. Currently there are five groups of customizable fill-in settings open. The fill-in value in this part is based on the IPv4 “Bridge address” system displayed by the host system of other stations (to be uplinked) as the main fill-in IP identification value.

## ➤ Auto Link Allow Address :

| Auto Link Allow Address |  |
|-------------------------|--|
| Allow Address/Mask      | <input type="text" value="10.0.1.1"/> <input type="button" value="Add"/> |

- **Allow Address/Mask :** Manage the IPv4 list of specific WiFi MAN-Mesh devices that can



be set to allow connection. The Link IP of the opposite host that is not on the list cannot be connected. It is a whitelist for WiFi MAN-Mesh MESH connection, which can avoid automatic interconnection and access of other unnecessary MESH devices. (The allowed IP is the IPv4 address of MESH/ Mask is the subnet mask)

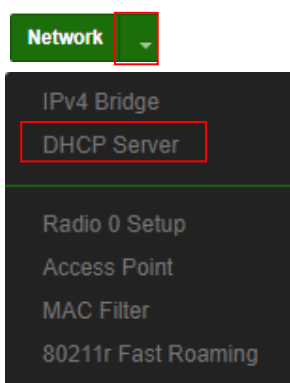
## ➤ Auto Link Allow Address List:

| Auto Link Allow Address List |                 |                        |
|------------------------------|-----------------|------------------------|
| #                            | IP Address/Mask | Action                 |
| 1                            | 10.0.1.1/32     | <a href="#">Delete</a> |

**Auto Link Allow Address List:** Display the IPv4 list of MAN-Mesh devices allowed to connect. All newly added host MAC addresses of MAN-Mesh IPv4 Address will be displayed here and can be deleted. (There are three groups available)

### 4.1.4 DHCP Server

Click "DHCP Server" Setting DHCP Server

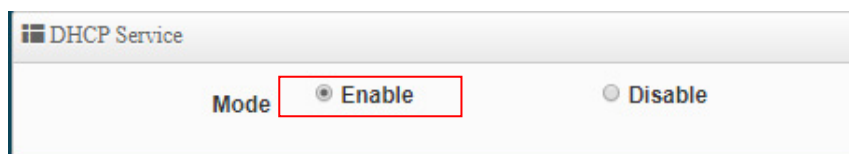


**Notice**

The DHCP server includes "DHCP service" and "DHCP Relay ", it can only choose one way to enable, if your DHCP Client IP and DHCP Server IP in the same "net segment / subnet", it is able to set and obtain the dynamically assigned IP address through the DHCP service, if it is not in the same "net segment / subnet", you must be choose DHCP Relay mode setting, DHCP Relay can forward the message and assign it to a different network segment / subnet or DHCP Server can also broadcast and forward the messages back to the Client (server) from different "net segments / subnets" you can set a different "net segment / subnet" and allow clients to receive and dispatch dynamic allocations from different network segments.

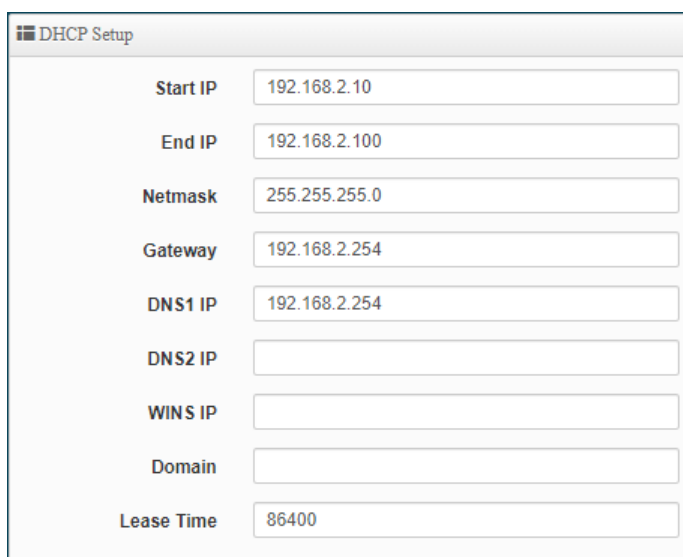
**DHCP Service** : Enable or Disable DHCP Service

Setting IP address distribution to network users automatically, please set the IP address distribution interval, gateway address and DNS server address of the network correctly



➤ **DHCP Service** : DHCP Service : enable or disable DHCP Service

If there is no DHCP server in the network structure or if you want to use the second DHCP server to assign different VLAN IPs, the administrator can enable this function to set the network segment to assign IP addresses.



## Notice

If there are 2 DHCP servers in the network environment, please pay attention to the distribution of IP addresses, do not repeat, to avoid IP conflicts

- **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 |
| -                | -          | -           | -       | -      |

- **IP Address** : Display the IP address sent to the client device
- **MAC Address**: Display the MAC address of the client device
- **Expired**: Display the expiration time of IP lease
- **Active**: To list this device (MAC) as a fixed IP address distribution

### ➤ Static Lease IP Setup

- **Static Lease IP Setup** : If the client device needs to obtain a fixed IP from the dhcp server, please enter a comment, ip address, mac address in "Static Lease IP Setup"

➤ **Static Lease IP List**

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

**Static Lease IP List** : After finished Static Lease IP Setup, the information will be added to this list.

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

**DHCP Relay** : Enable or Disable the DHCP relay (DHCPD) as a relay bridge function, because DHCP servers on different subnets / segments cannot assign IP to DHCP clients. You need to enable DHCP Relay to access different subnets / segments The DHCP server on the server assigns IP to the DHCP client.

## Notice

This function only works under the MAN-Mesh mode, other modes are not supported

DHCP Relay

Relay

☒ Enable
 ☐ Disable

Relay Interface

Mesh

Relay To

☐ IP Address
 ☐ Default Gateway

IP Address

Static Lease IP Setup

Comment

IP Address

MAC Address

Add

## Notice

DHCP Relay (DHCPR), the relay service can exchange DHCP packets between DHCP clients and DHCP servers located in different "network segments / subnets". Relay service is used to send DHCP Client IP request packets from different subnets / segments to the DHCP server when the DHCP Client sends an IP request to the server, so that the DHCP server can assign IP to different subnets / network segments DHCP Client.

- **Relay Interface** : You can be set to choose the interface of the DHCP server to be forwarded through Relay for DHCP clients located in different "segments / subnets". It can select the "Mesh" WiFi or virtual LAN interface VLAN 0 ~ VLAN 15.
- **Relay To** : After selecting the relay interface, set the DHCP server address for different "segment / subnet". The address can be "IP address" or "default gateway"
- **IP Address** : You can set the address of the DHCP server.

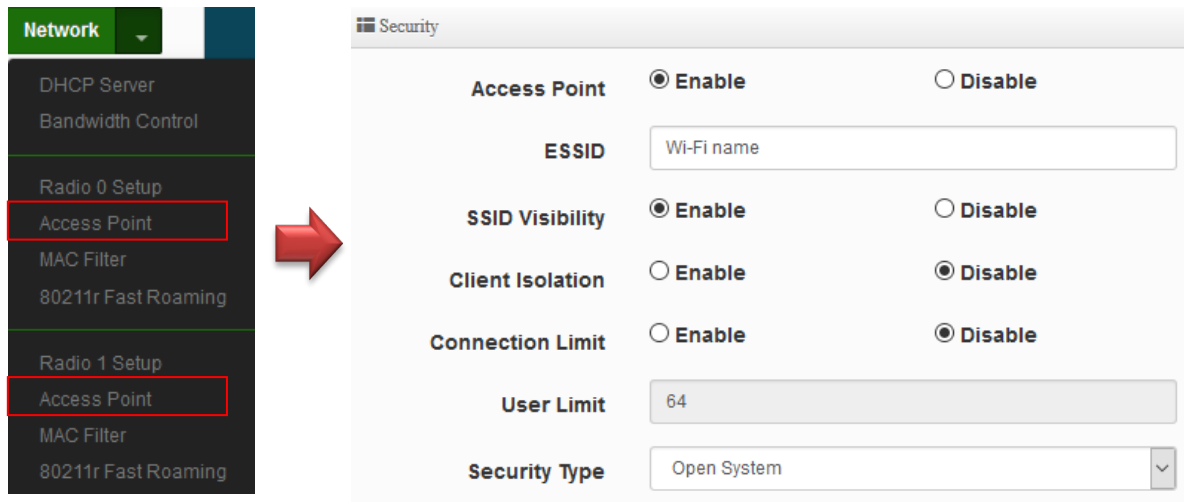
## Notice

When using the DHCP Relay (DHCPR) application, please make sure your DHCP server type (PC Server or Layer 3 switch with DHCP server function) must supports "DHCP multi-segment", In order to use the full function of DHCP Relay (DHCPR) in MAN-Mesh.

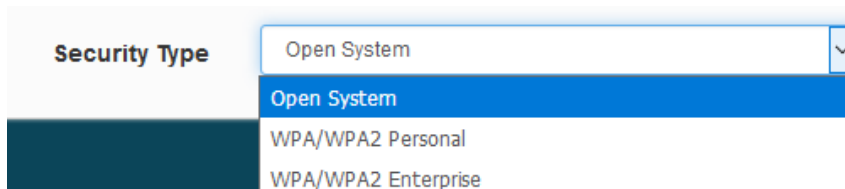
Click **"Save"** button to save your changes. Then click **Reboot** button to activate your changes.

## 4.1.5 Radio 0(2.4G)/Radio 1(5G) Access Point Setup

Administrator can Enable or Disable Radio 0(2.4G)/Radio 1(5G)Wi-Fi. If Radio are enabled, administrators can set the SSID and security for the Radio 0(2.4G) and Radio 1(5G) access point.



- **Access Point:** Administrator can Enable or Disable the Radio 0(2.4G)/Radio 1(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 2.4G/5G limit 40/60 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.



- **Open System:** Data is not unencrypted during transmission when this option is selected.
- **WPA/WAP2- 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.

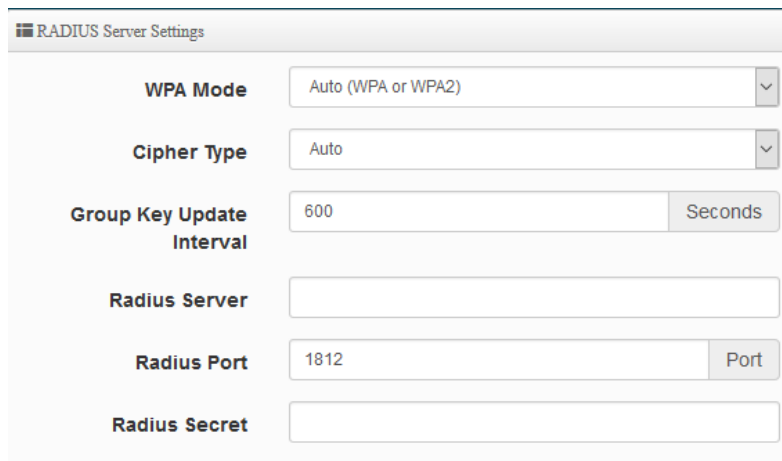
- ✓ **WPA Mode:** Administrator can select security for Auto or only WPA or only WPA2.
- ✓ **Cipher Type:** Administrator can select use AES or TKIP with WPA / WPA2 encryption method.

**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.

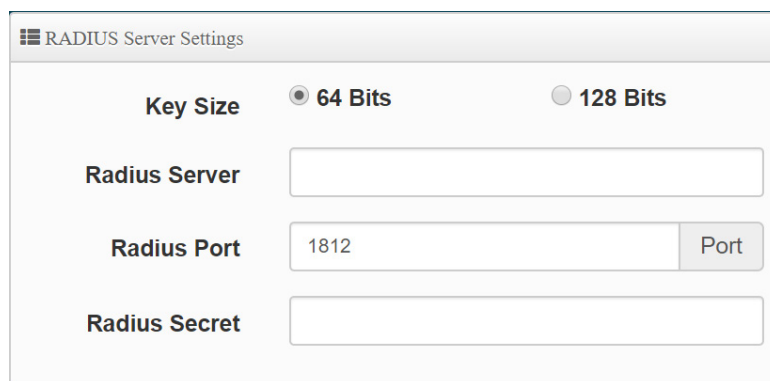
- ✓ **Group Key Update Interval:** The time interval is for re-keying GTK (broadcast/multicast encryption keys) in seconds. Enter the time-length required; the default time is 600 seconds.
- ✓ **Pass Phrase:** Enter the ESSID pass phrase.
- ✓ **WPS:** Administrator can use WPS function to link WiFi client. If enabled, administrator can click the WPS Push Button.

## ● WPA/WAP2-Enterprise



- **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.

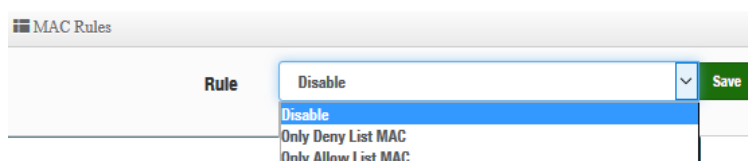
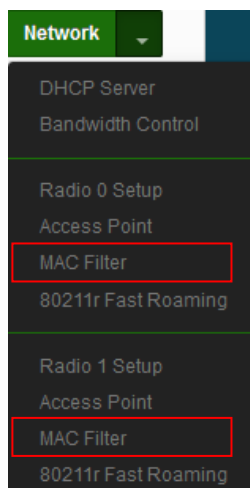
## ● 802.1x RADIUS Server Settings



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

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

## 4.1.6 MAC Filter



**(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.

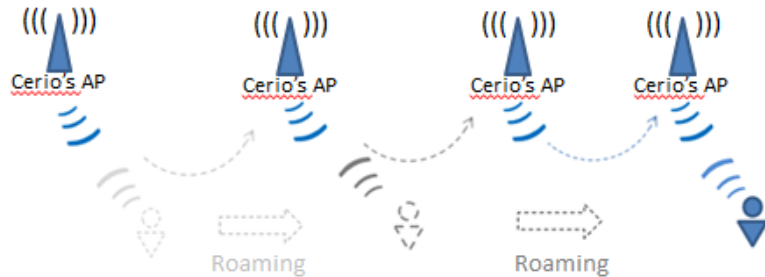
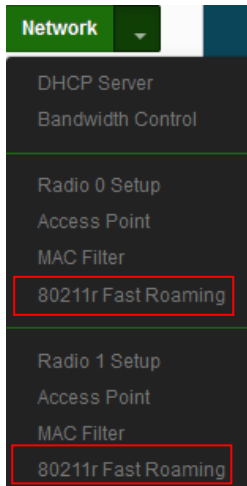
**(2) Only Allow List MAC :** Administrator can add wireless users MAC address in MAC list. The access point will allow connection in MAC address list.

The screenshot shows the 'Add MAC Address' interface. It has a text input field for 'MAC Address' and an 'Add' button. Below this is the 'MAC Address List' section, which contains a table with the following columns: #, MAC Address, Action, #, MAC Address, and Action. The table is currently empty, showing only dashes in the rows.

- **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.

## 4.1.7 802.11r Fast Roaming Setup



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

### Notice

If this feature is enabled when using 802.11r fast roaming, the wireless user equipment must support 802.11k functionality to work properly

- **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.

### Notice

This setting must be 2-octet of hex string codes. For example, enter 8c4d

- **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

NAS Identifier

128-bit Key

Add

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

| # | 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

R1 Identifier

128-bit Key

Add

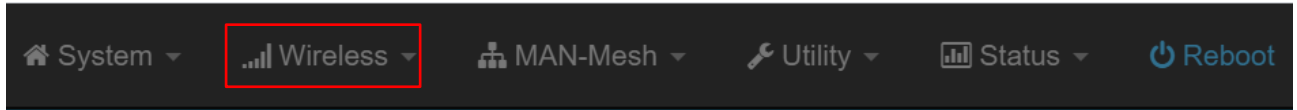
- **MAC Address:** Enter the main roaming device MAC address
- **R1 Identifier:** Enter Shared identifier.
- **128-bit Key:** Enter Shared Key of 128 bit.

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

## 4.2 Wireless Configuration

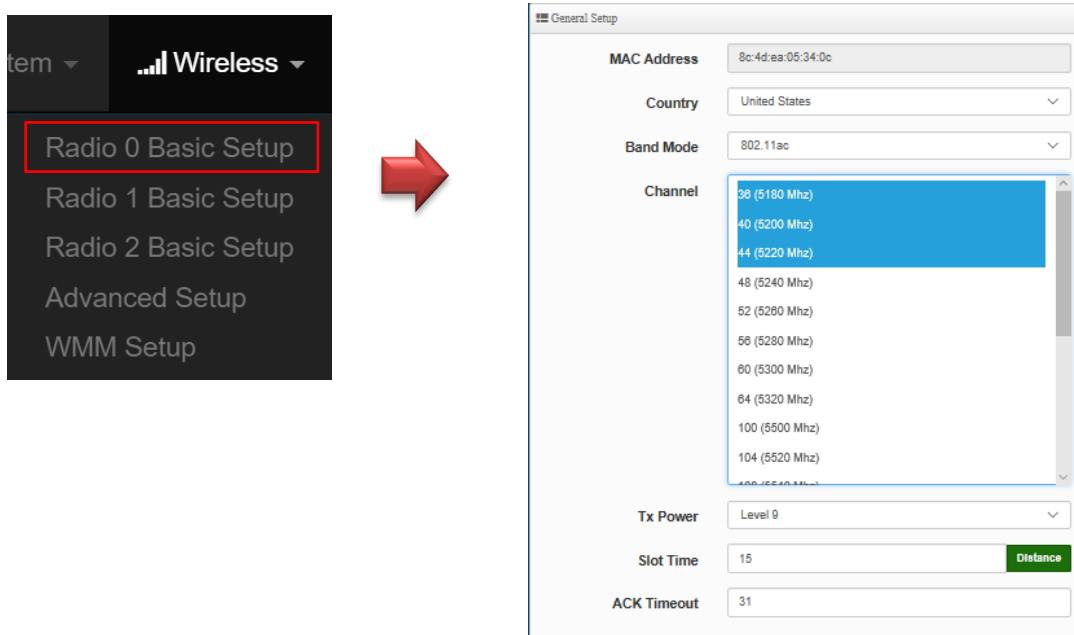
Radio 0 (2.4G) or Radio 1 (5G) AP station, channel, advanced function and WMM setup..etc.

Setting the AP's (LAN) IP address and other functions, please click "System " -> ☐ "VLAN Setup".



Click the "Wireless " to set Radio 0 (2.4G), Radio 1 (5G) MAN-Mesh basic setup, click "Radio 0 or Radio 1" or select the regional for settings, and select the " wireless operation mode" Priority auto-connected multi-channel tag selection in the MAN-Mesh network. Please save your setting after the installation is completed

### 4.2.1 Mesh Radio 0 (2.4G) Setup



- **MAC Address:** Display 2.4G WiFi MAC address.
- **Country:** Administrator can select country: United States(US) , Europe(EU) or Taiwan(TW).
- **Band Mode:** Administrator can select 802.11 b, 802.11 b/g, 802.11 b/g/n, 802.11 n for the 2.4G Band.
- **Channel:** Administrator can make select 1 to 11 CH.Priority automatic connection channel selection of mark in the MAN-Mesh environment. it will have different channel selections in different wireless operation modes in different regions according to regulations.The Channel



settings can be changed in “HT Physical Mode” → “Extension Channel” can select **Upper** or **Lower** channels.



## Notice

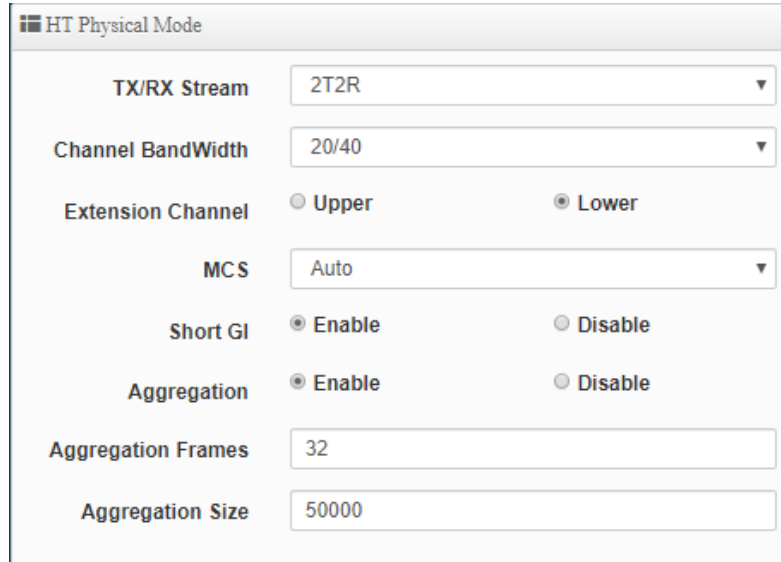
The MAN-Mesh AP provides intelligent and quickly automatic connections between multiple channels. When selected more channels then the search range becomes bigger then the longer time will be required. Appropriate channel selection will help to speed up MAN-Mesh APs to automatically connect to each other. It is recommended that the number of channels selected can be 3 to 5 channels.

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



Setting Slot Time and ACK Timeout can strengthen long-distance connection. Adjustment the value to achieve an optimal setting. If the value is too low, the transmission will be reduced. If the value is too high, the connection may be disconnected.

## HT Physical Mode



- **TX / RX Stream:** Build in 2.4GHz 2 antennas and support 2TX/2RX streams. Administrator can select 1 or 2 TX/RX. The default is 2TX/2RX.



This product has a built-in 2x2 (2T2R) antenna for 2.4Ghz, which has been matched with the default setting of 2T2R. If there is no special demand, please keep this default setting .

- **Channel Bandwidth:** The "20/40" MHz option is usually best. The other option is available for special circumstances.



This product with Wave2 chip solution, 2.4G (Radio 0) using 20/40 mode, the maximum data rate is 400Mbps

- **Extension Channel:** Sets channel select to Upper or Lower. The Upper supports 1 to 7 range CH and Lower supports 5 to 11 range CH.
- **MCS:** This parameter represents transmission rate. By default (Auto) the fastest possible

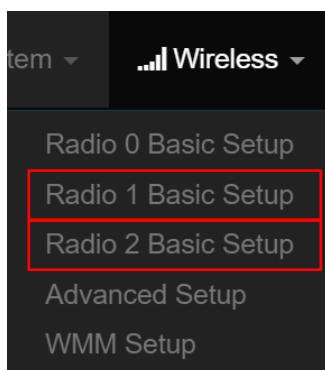
transmission rate will be selected. You have the option of selecting the speed if necessary.

- **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 “Enabled”. Select “Disable” to deactivate Aggregation.  
A part of the 802.11n standard (or draft-standard), it allows sending multiple frames per single access to the medium by combining frames together into one larger frame. It creates the larger frame by combining smaller frames with the same physical source and destination end points and traffic class (i.e. QoS) into one large frame with a common MAC header.
- **Aggregation Frames:** 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.

## Notice

If the packet aggregation Size is not particularly necessary, please do not modify the default setting, which will affect the transmission rate quality

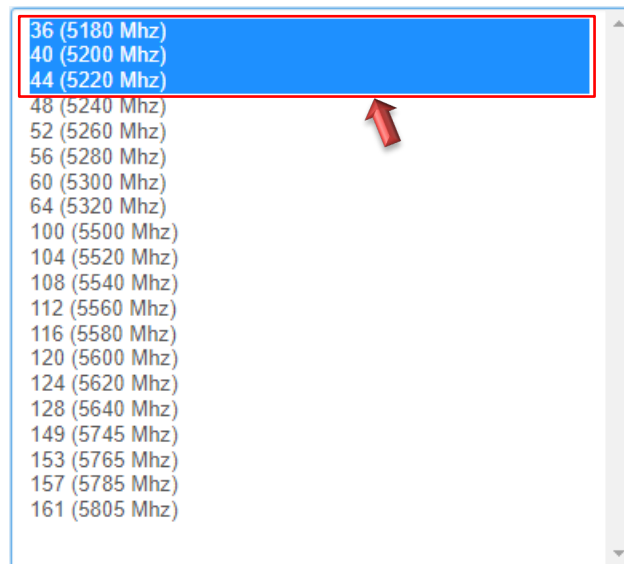
### 4.2.2 Mesh Radio 1 (5G) Setup



The 'General Setup' window displays the following configuration:

- MAC Address:** 8c:4d:ea:05:34:0c
- Country:** United States
- Band Mode:** 802.11ac
- Channel:** A list of channels is shown, with 36 (5180 Mhz), 40 (5200 Mhz), and 44 (5220 Mhz) highlighted in blue.
- Tx Power:** Level 9
- Slot Time:** 15 (with a 'Distance' button next to it)
- ACK Timeout:** 31

- **MAC Address:** Display Radioi 1(5G) WiFi MAC address.
- **Country:** Administrator can select country: United States(US) , Europe(EU) or Taiwan(TW).
- **Band Mode:** Administrator can select 5G Band for 802.11a or 802.11a/n or 802.11n(5G) or 802.11ac. The default is 802.11ac etc..
- **Channel:** Administrator can select priority automatic connection channel selection of mark in the MAN-Mesh environment. it will have different channel selections in different wireless operation modes in different regions according to regulations.



## Notice

The MAN-Mesh AP provides intelligent and quickly automatic connections between multiple channels. When selected more channels then the search range becomes bigger then the longer time will be required. Appropriate channel selection will help to speed up MAN-Mesh APs to automatically connect to each other. It is recommended that the number of channels selected can be 3 to 5 channels.

According to information released by NCC, Taiwan opens the following three 5GHz bands:

1. 5280 ~ 5350MHz (CH56 5280MHz, CH60 5300MHz, CH64 5320MHz)
2. 5470 ~ 5725MHz (CH100 5500MHz, CH104 5520MHz, CH108 5540MHz, CH112 5560MHz, CH116 5580MHz, CH120 5600MHz, CH124 5620MHz, CH128 5640MHz, CH132 5660MHz)

5660MHz, CH136 5680MHz, CH140 5700MHz)

3. 5725 ~ 5825MHz (CH149 5745MHz, CH153 5765MHz, CH157 5785MHz, CH161 5805MHz, CH165 5825MHz)


Among them, the frequency band 5470 ~ 5725MHz conflicts with the military and meteorological Doppler radar frequencies. Under the logic of military priority and civilians, if these frequencies are to be used, it is equipped with equipment that starts DFS and TPC (EIRP value greater than 500mW ) Function, when the device senses that other people in the military are using the current frequency, DFS will automatically jump to other frequencies; 5250 ~ 5350MHz open indoor use. (Related specifications in Taiwan can be found on NCC for "Technical Specifications for Low Power RF Motors")

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



Setting Slot Time and ACK Timeout can strengthen long-distance connection. Adjustment the value to achieve an optimal setting. If the value is too low, the transmission will be reduced. If the value is too high, the connection may be disconnected.

## HT Physical Mode

 HT Physical Mode

|                    |   |
|--------------------|---|
| TX/RX Stream       | 2T2R  |
| Channel BandWidth  | 80  |
| Min MCS            | 4   |
| Max MCS            | 9   |
| Short GI           | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| Aggregation        | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| Aggregation Frames | 32  |
| Aggregation Size   | 50000   |

**TX / RX Stream:** Administrator can select 1 or 2 TX/RX. The default is 2TX/2RX



This product has a built-in 2x2 (2T2R) antenna for 5Ghz, which has been matched with the default setting of 2T2R. If there is no special demand, please keep this default setting .

- **Channel Bandwidth:** The "20/40 and 802.11ac 80" MHz option is usually the best. The other option is available for special circumstances.
- **Min MCS:** This parameter represents transmission rate. By default (0) the fastest possible transmission rate will be selected. You have the option of selecting the speed if necessary.
- **Max MCS:** This parameter represents transmission rate. By default (9) the fastest possible transmission rate will be selected. You have the option of selecting the speed if necessary.
- **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 "Enabled". Select "Disable" to deactivate Aggregation.
- **Aggregation Frames :** The frame size of the packet aggregation. The factory default is "32"
- **Aggregation Size :** The size of the packet aggregation. The factory default is "50000".

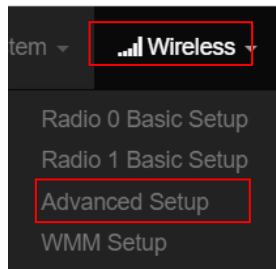


## Notice

If the packet aggregation Size is not particularly necessary, please do not modify the default setting, which will affect the transmission rate quality

After setting, please click the "Save" button to save your settings, and press the "Restart" button to complete the application of the new settings.

### 4.2.3 Advanced Setup



| Advanced Setup        |   |
|-----------------------|---|
| Beacon Interval       | 100   |
| DTIM Interval         | 1   |
| Fragment Threshold    | 2346  |
| RTS Threshold         | 2346  |
| Short Preamble        | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| IGMP Snooping         | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| Greenfield            | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| Band Steering         | <input type="checkbox"/> 10 <input type="button" value="RSSI Limit"/> |
| RF on/off by Schedule | Always <input type="button" value="v"/>                               |
| Location Tracking Log | <input type="checkbox"/> 600 <input type="button" value="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.

- **Band Streeing:** When 2.4GHz and 5GHz network cards coexist, the 5GHz network cable is automatically used as the main connection to improve the performance. The threshold for connecting RSSI can be set, that is, when the signal value of the wireless user and the AP is better, the local machine will automatically interrupt the 2.4G user and force the use of 5G.
- **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=84-7-08-11-10 rssi=-67
Jan 1 08:27:00 Wifilogd: tm=1420072020 vlan=0 radio=0 bssid=8c:4d:ea:05:1c:7a climac=84-7-08-11-10 rssi=-68
Jan 1 08:26:00 Wifilogd: tm=1420071960 vlan=0 radio=0 bssid=8c:4d:ea:05:1c:7a climac=84-7-08-11-10 rssi=-67
```

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

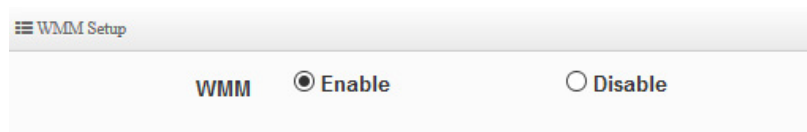
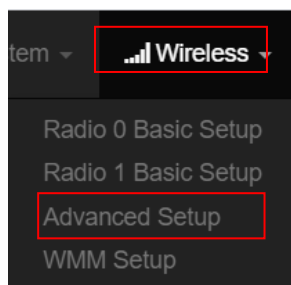
## 4.2.3 WMM Setup

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

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

➤ **AC Type :**

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

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

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

- **AIFS** : The Arbitration Inter-Frame Spacing Number specifies a wait time (in milliseconds) for data frames. ◦
- **TxOP Limit**: Transmission Opportunity is an interval of time when a WME AP has the right to initiate transmissions onto the wireless medium (WM). This value specifies (in milliseconds) the Transmission Opportunity (TXOP) for AP; that is, the interval of time when the WMM AP has the right to initiate transmissions on the wireless network. ◦
- **ACM bit**: Admission Control Mandatory, ACM only takes effect on AC\_VI and AC\_VO. When you do not click Checkbox, it means that the ACM is controlled by the connecting AP. If you click Checkbox, it means that the Client is in charge. ◦
- **No ACK policy bit**: Acknowledgment Policy, WMM defines two ACK policies: **Normal ACK** and **No ACK**. Click "**Checkbox**" indicates "**No ACK**"

When the no acknowledgement (No ACK) policy is used, the recipient does not acknowledge received packets during wireless packet exchange. This policy is suitable in the environment where communication quality is fine and interference is weak.

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

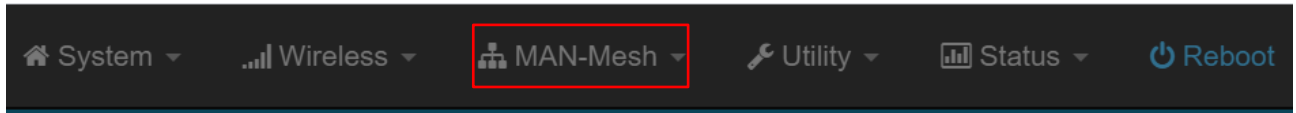
When the Normal ACK policy is used, the recipient acknowledges each received uncast packet.

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



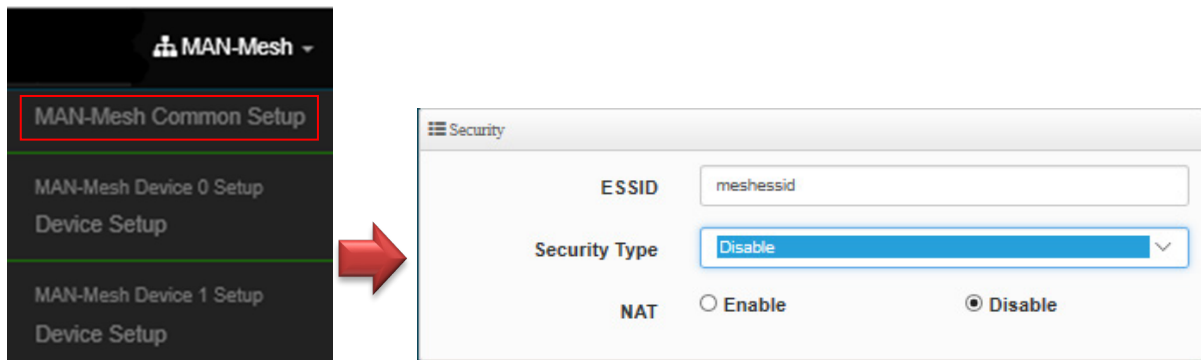
## 4.3 MAN-Mesh

MAN-Mesh common Setup and MAN-Mesh Device 0,1,2 Setup.



### 4.3.1 MAN-Mesh Common Setup

Click "MAN-Mesh" → "MAN-Mesh Common Setup", setting MAN-Mesh AP SSID, MAN-Mesh AP Security Type, MAN-Mesh NAT setup, after completed please save your setting.



- **SSID:** In the same MAN-Mesh architecture, the SSID must be the same which can work properly. Please set a proprietary MAN-Mesh connection SSID for yourself. The default SSID of the MAN-Mesh AP is meshssid
- **Security Type:** Enable or Disable AES 128bit encryption function, AES encryption custom key can input 0 ~ 9 numbers or A ~ Z uppercase and lowercase English format, it can support 8 ~ 32 characters key encryption algorithm in each MAN-Mesh AP connecting each other with secure encrypted transmission.

#### Notice

When this encryption function is enabled, each MAN-Mesh AP device in the Mesh architecture environment needs to synchronize the same encryption settings. If disable the Mesh connection encryption function, to avoid the possibility of connecting to other mesh groups that also use the default SSID (meshssid), it is strongly recommended to change your own Mesh AP SSID in the Mesh environment



Security

ESSID: meshessid

Security Type: AES

PassPhrase: 0123456789ABCDEFGHIJKabodefgghijk

NAT: ☐ Enable ☒ Disable

- **NAT** : Enable or disable the NAT network address conversion function of the MAN-Mesh AP. The administrator can selectively enable this NAT function for a specific node in the environment when the Mesh is connected. The default value is disabled.

## Notice

When the backbone mesh interconnection completed by the MAN-Mesh is completed. NAT applications can be performed on any MAN-Mesh host. More that do not enable for "None NAT" applications information, please refer to Chapter 4. LAN physical line "None NAT" application illustration

- **WAN Interface** : When the NAT network address conversion function of a specific node is enabled, you must select the source interface of the WAN. You can select the WiFi interface "Mesh" or LAN interface virtual network "VLAN 0 ~ VLAN 15".

Security

ESSID: meshessid

Security Type: AES

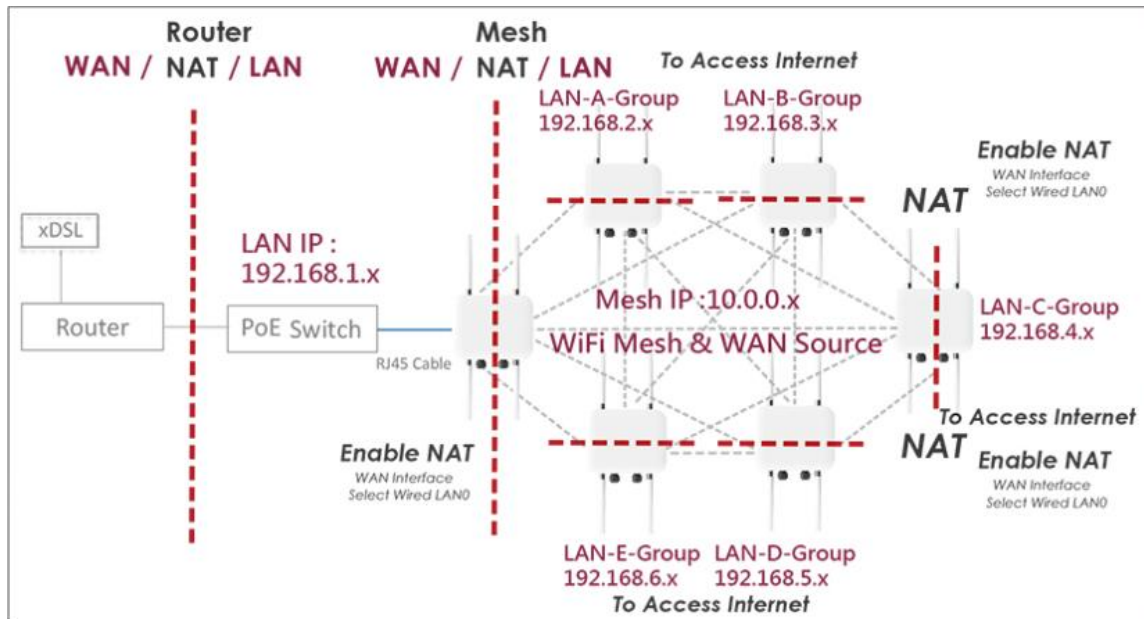
PassPhrase: 0123456789ABCDEFGHIJKabodefgghijk

NAT: ☒ Enable ☐ Disable

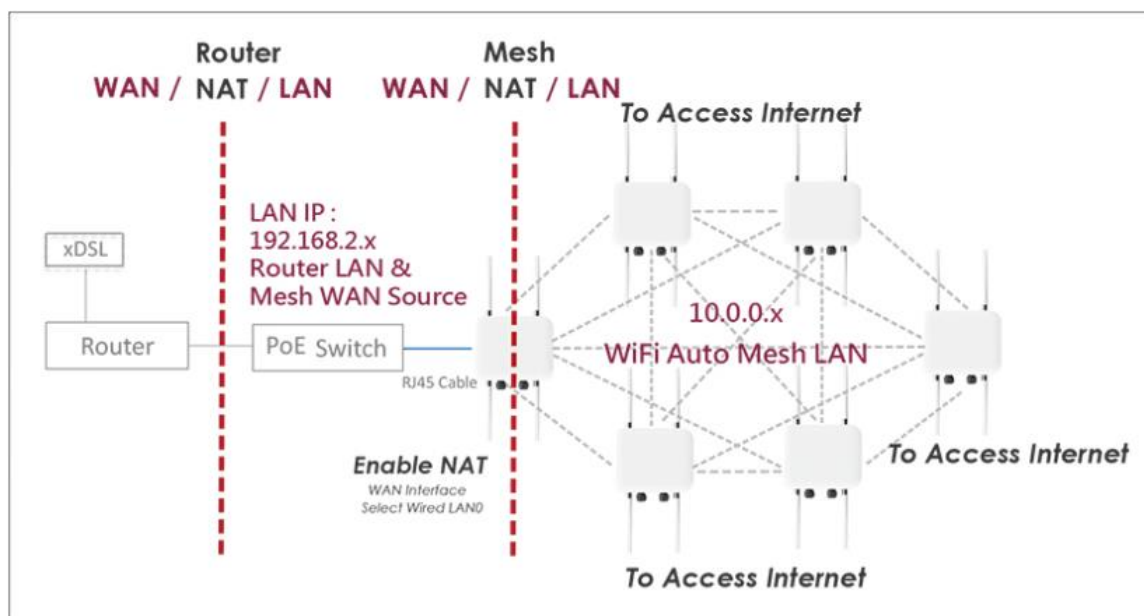
WAN Interface: Mesh

Mesh  
VLAN 0  
VLAN 1  
VLAN 2  
VLAN 3  
VLAN 4  
VLAN 5  
VLAN 6  
VLAN 7  
VLAN 8  
VLAN 9  
VLAN 10  
VLAN 11  
VLAN 12  
VLAN 13  
VLAN 14  
VLAN 15

If the source interface of WAN selects wireless "Mesh" as the upper layer interface (NAT WAN), other interfaces of the host (including wired VLAN (0 ~ 15) and wireless AP) will become the lower layer interface (NAT LAN), this application Designed to allow the use of every Mesh NAT AP unit (small block) environment host that is not connected to each other and users can connect to the Internet Host planning the entire MAN-Mesh environment.



If the selected virtual network (0 ~ 15) as interface (NAT WAN), other interfaces of the host (including wireless AP and wireless mesh interface) will become the lower layer interface (NAT LAN). The design purpose of NAT is to make the entire MAN-Mesh environment in a large LAN communication state. At the same time, all Mesh users can access the Internet through Mesh AP with NAT router function.



## 4.3.2 MAN-Mesh Device Setup

Click "MAN-Mesh" → "MAN-Mesh Device 0 Setup" → Device Setup to set MAN-Mesh Device 0 / "MAN-Mesh Device 1 Setup" → Device Setup to set MAN-Mesh Device 1, enable or disable MAN-Mesh AP radio 0,1 , MAN-Mesh IPv4 / IPv6 setup , MAN-Mesh deployment method, MAN-Mesh mandatory MAC address, MAN-Mesh MAC address list: °



MAN-Mesh Setup

MAN-Mesh
☒ Enable
☐ Disable

MAN-Mesh IPv4 Setup

IPv4 Mode
☒ Enable
☐ Disable

IPv4 Address

Netmask

MAN-Mesh IPv6 Setup

Link-local address

IPv6 Mode
☐ Enable
☒ Disable

IPv6 Address

Subnet Prefix Length

MAN-Mesh Deployment

Multi-hop Layout
☐ Host Node
☒ Interlink Node

MAN-Mesh Force MAC Address

MAC Address

MAN-Mesh MAC Address List

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

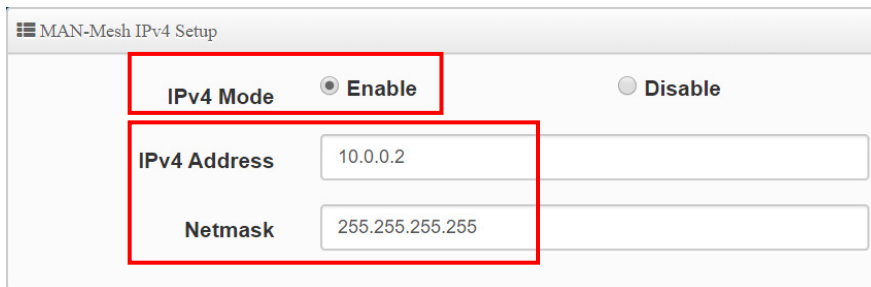
- **MAN-Mesh Setup** : Enable or disable the radio of MAN-Mesh AP. Enable or disable this radio be used as the MAN-Mesh radio for mesh auto link . The default value is “Disable”.



## Notice

When any Radio of MAN-Mesh AP is enabled, At the same time, you must set Mesh interface IP address of Mesh AP. The IP address of the MAN-Mesh AP can be set in both IPv4 and IPv6 formats. If you are not familiar with or do not have an IPv6 address, it is recommended using IPv4 mode to set the Mesh interface IP address of each MAN-Mesh AP. Please note that the Mesh AP's external DNS or Gateway address is set by the relevant of its wired LAN virtual IP address. (Remind: IPv6 format, IP usage acquisition , please contact your ISP provider)

## MAN-Mesh IPv4 Setup



- **IPv4 Mode** : Enable or Disable for IPv4 mode
- **IPv4 Address**: In the Mesh architecture, the IP address used by the MAN-Mesh AP in the Mesh operating environment is different from the LAN IP address (virtual network IP address) selected in the environment when setting the Mesh IP address network segment. For example, if the default LAN IP is same address segment of 192.168.2.XXX, In the mesh environment, please select other virtual IP segments as Mesh IP address segments such as 172.16.2. XXX. The Mesh IP default values: 10.0.0.1, 10.0.1.1, 10.0.2.1.
- **Netmask** : Please input MAN-Mesh AP IPv4 Netmask

## Notice

Note: Mesh interface IP is different from the LAN interface IP of the device. When each MAN-Mesh AP sets its own unique Mesh interface IP address, please be note when setting the IP address, it can't be the same as the IP address of other interfaces of it own or any interface of other MAN-Mesh APs in the environment

## Notice

The IPv4 format is from 0.0.0.0 to 255.255.255.255. Except for the following private IP is not used by international ownership, The remaining IPs are real IPs that are owned or used internationally. To avoid the IP error occurs, please use the following recommended range to choose your own private IP :

- ✓ Private network Class A : 10.0.0.0~10.255.255.255
- ✓ Private network Class B : 172.16.0.0~172.31.255.255
- ✓ Private network Class C : 192.168.0.0~192.168.255.255

## MAN-Mesh IPv6 Setup

MAN-Mesh IPv6 Setup

Link-local address: FE80::8E4D:EAFF:FE05:3406

IPv6 Mode: ☒ Enable ☐ Disable

IPv6 Address: 2001:8E4D:EAFF:FE01:0000:0000:0000:0002

Subnet Prefix Length: 64

- **Link-Local address** : This section automatically displays the Link Local address of the local unique identification interface required by the IPv6 mode address operation specifications, for example, it is displayed as FE80 :: 8E4D: EAFF: FE05: 3406.
- **IPv6 Mode** : Enable or Disable for IPv6 mode
- **IPV6 Address** : This is the IP address used by the MAN-Mesh AP in the Mesh operating



environment Example of IPv6 input network range: 2001: 8E4D: EAFF: FE01: 0000: 0000: 0000: 0002 ~ FFFF: FFFF: FFFF: FFFE. (For IPv6 IP acquisition, please contact your ISP provider )

- **Sub Prefix Length** : the Sub Prefix Length of the IPv6 address of the MAN-Mesh AP device . The default value is 64

## MAN-Mesh Deployment

MAN-Mesh Deployment

Multi-hop Layout
☒ Host Node
☐ Interlink Node

**Multi-hop Layout** : MAN-Mesh AP multi-hop layout role setting selection, you can choose the layout of the Host node or Interlink node

- ✓ **Host Node** : In the MAN-Mesh mesh network environment, it must deploy a unique "host node" so that the "interlink node" can automatically establish a connection with each other. The "host node" will always play the role of search multiple fixed and usable channels in the Mesh environment, in order to create and assist other "interlink node" can quickly and connect to each other to completed Mesh automatic connection architecture.

### Notice

In a MAN-Mesh network environment, only needs to be set one "host node". If more than two "host node", it will cause MAN-Mesh AP to misjudge the role of "interlink node". then when the hosts are connected to each other, the automatic connection will fail.

- ✓ **Interlink Node** : In the Mesh environment, the MAN-Mesh AP of "interlink node" creates a pre-assisted layout according to the channel of the "host node", and can quickly connect with all the MAN-Mesh AP of "interlink nodes".

### Notice

In a Mesh environment, you only need to take one MAN-Mesh AP host as the layout of the "host node" role. And all other MAN-Mesh AP hosts are set as the layout of the "interlink nodes" role

**MAN-Mesh Force MAC Address** : MAN-Mesh Force MAC Address is based on the IPv4 MAC address,



Priority the connection of nearby MAN-Mesh AP that can be meshed, and add a designated priority MAN-Mesh AP.

MAN-Mesh Force MAC Address

MAC Address

Add

**MAN-Mesh MAC Address List** : Manage the MAC list of designated priority links. The MAC addresses of all hosts added by MAN-Mesh Force MAC Address will be displayed here, and you can choose to delete them.

| MAN-Mesh MAC Address List |                   |        |    |                   |        |
|---------------------------|-------------------|--------|----|-------------------|--------|
| #                         | MAC Address       | Action | #  | MAC Address       | Action |
| 1                         | 8c:4d:ea:05:33:01 | Delete | 2  | 8c:4d:ea:05:33:02 | Delete |
| 3                         | 8c:4d:ea:05:33:03 | Delete | 4  | 8c:4d:ea:05:33:04 | Delete |
| 5                         | 8c:4d:ea:05:33:05 | Delete | 6  | 8c:4d:ea:05:33:06 | Delete |
| 7                         | 8c:4d:ea:05:33:07 | Delete | 8  | 8c:4d:ea:05:33:08 | Delete |
| 9                         | 8c:4d:ea:05:33:09 | Delete | 10 | 8c:4d:ea:05:33:0a | Delete |

**MAN-Mesh Block MAC Address :** In the case of automatic interconnection, you can set the specified model to block the MAC of the MAN-Mesh AP host. Please add the specified non-connected MAN-Mesh AP host based on the IPv4 MAC address.

MAN-Mesh Block MAC Address

MAC Address

8c:4d:ea:05:34:1d

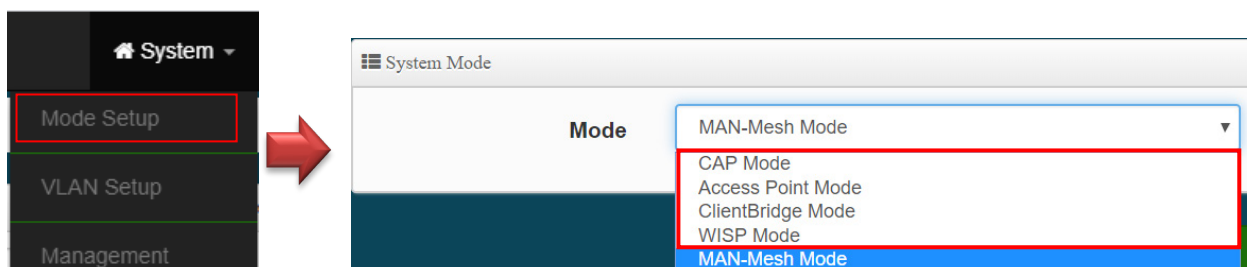
Add

**MAN-Mesh Block MAC Address List :** Manage the MAC list that specifies the priority to block connections. The MAC addresses of all hosts added by MAN-Mesh Force MAC Address will be displayed here, and you can choose to delete them.

| MAN-Mesh Block MAC Address List |                   |        |   |             |        |
|---------------------------------|-------------------|--------|---|-------------|--------|
| #                               | MAC Address       | Action | # | MAC Address | Action |
| 1                               | 8c:4d:ea:05:34:1d | Delete | - | -           | -      |

## 4.4 Change Other Setup modes

If the administrator needs to switch to other modes, click "System"-> " Mode Setup " to change other modes.



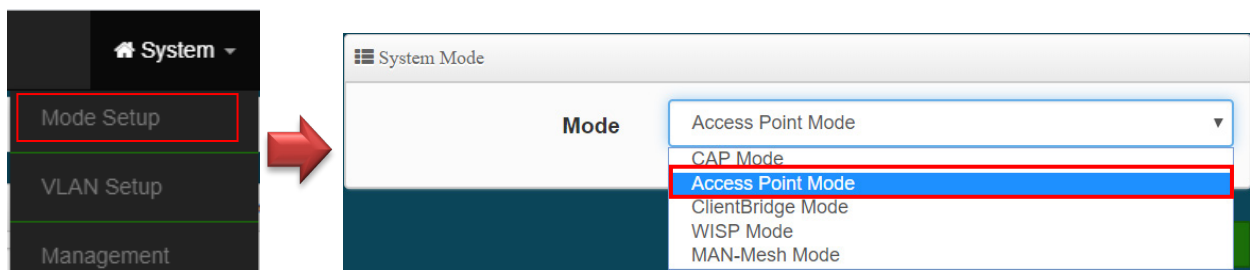
Please click "System " → "Setup Mode", select the MAN-Mesh mode, after confirmation, "press Save & Restart" button

## 5. 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.

### 5.1 Change Setup mode

If the administrator needs to switch to Access Point mode, Please click "System" -> " Mode Setup " to change Access Point mode.

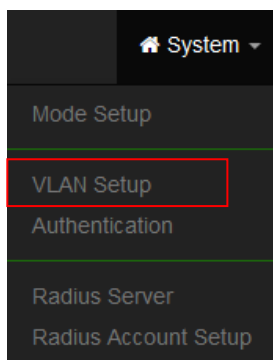


#### Notice

Please note that the LAN IP addresses in each mode are different from each other and will not continue. For the first time after switching modes, always perform access management on the LAN default IP address of 192.168.2.254

### 5.2 VLAN Setup

Start by setting the AP's (LAN) IP address, Please Click " System " → " VLAN Setup "



Here are the instructions to setup the local IP Address / Netmask / Gateway / DNS and management Access Point Radio 0(2.4G) or Radio 1(5G) 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  | Radio 1 | Radio 2 | Action  |
| 0         | On        | Native ETH0 Access Control | 192.168.2.254 | 255.255.255.0 | 2.4G_0_0 | 5G_0_1  | 5G_0_2  | Network |
| 1         | Off       | ETH0.101                   | -             | -             | 2.4G_1_0 | 5G_1_1  | 5G_1_2  | Network |
| 2         | Off       | ETH0.102                   | -             | -             | 2.4G_2_0 | 5G_2_1  | 5G_2_2  | Network |
| 3         | Off       | ETH0.103                   | -             | -             | 2.4G_3_0 | 5G_3_1  | 5G_3_2  | Network |
| 4         | Off       | ETH0.104                   | -             | -             | 2.4G_4_0 | 5G_4_1  | 5G_4_2  | Network |
| 5         | Off       | ETH0.105                   | -             | -             | 2.4G_5_0 | 5G_5_1  | 5G_5_2  | Network |

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

- **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 0(2.4G) SSID name.
- **Radio 1** : Display Radio 1(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**
☐ 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

| DNS  |             |
|------|-------------|
| DNS1 | 192.168.2.1 |
| DNS2 |             |

### Notice

You can set the gateway IP address or external DNS IP address in the architecture environment. You can use Google's DNS IP of 8.8.8.8

- **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   | Management  |
|--|---|
| <b>VLAN Mode</b> <input checked="" type="radio"/> Enable <input type="radio"/> Disable | <b>Access Point 0</b> <input checked="" type="radio"/> Enable <input type="radio"/> Disable       |
|  | <b>Access Point 1</b> <input checked="" type="radio"/> Enable <input type="radio"/> Disable       |
|  | <b>Access Point 2</b> <input checked="" type="radio"/> Enable <input type="radio"/> Disable       |
| <b>IP Setup</b>  | <b>802.1d Spanning Tree</b> <input type="radio"/> Enable <input checked="" type="radio"/> Disable |
| <b>IP Mode</b> <input checked="" type="radio"/> Enable <input type="radio"/> Disable   | <b>Control Port</b> <input checked="" type="radio"/> Enable <input type="radio"/> Disable         |
| <b>IP Address</b> 192.168.2.254  | <b>IAPP</b> Disable   |
| <b>Netmask</b> 255.255.255.0   |   |
|  | <b>ETH0 VLAN Tag Setup</b>  |
|  | <b>VLAN TAG</b> 1-4096  |

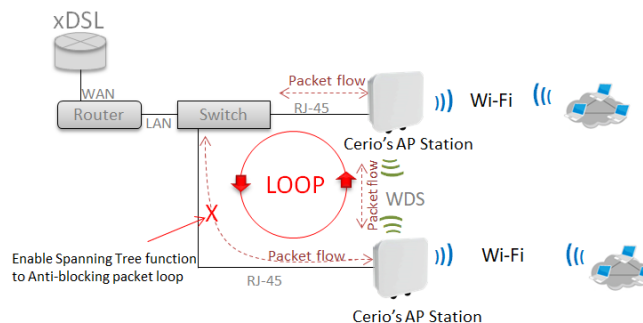
- **VLAN Mode :** Administrator can select Enable or disable for the VLAN Network.
- **IP Mode :** Administrator can select enable or disable function for VLAN IP.
- **IP Address/ NetMask :** Administrator can set IP address and netmask for the VLAN.

## Notice

At least one VLAN will always be enabled by default

## Management

- **Access Point 0** : Administrator can Enable or Disable Radio 0(2.4G).
- **Access Point 1** : Administrator can Enable or Disable Radio 1(5G).
- **802.1d Spanning Tree** : The spanning tree network protocol provides a loop free topology for a bridged LAN between LAN interface and 8 WDS interfaces from wds0 to wds7. The Spanning Tree Protocol, which is also referred to as STP, is defined in the IEEE Standard 802.1d



- **Control Port** : Administrator can select one of the VLAN as managed AP.
- **IAPP** : Administrator can select radio 2.4G or 5G for IAPP roaming.
- **VLAN Tag Setup**: Set the VLAN used tags.

## Notice

The IAPP condition must use WPA2-PSK Wi-Fi security and AES algorithm)

## Notice

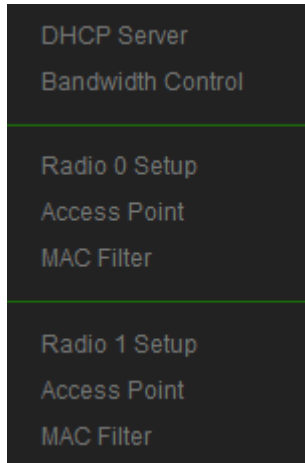
That if ETH0 is set to use a VLAN tag, you must enter the management interface with the same VLAN as the tag to enter the management settings. Otherwise, the VLAN domain is completely blocked.

## # Network Pull-down menu

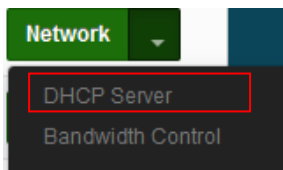
Administrator can set DHCP Server and Radio 0(2.4G)/ Radio 1(5G) security for the access point and set 802.11r fast roaming.



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



## 5.2.1 DHCP Server



If there is no DHCP server in the network or if you want to use a second DHCP server to assign IP, the administrator can enable this function to set the network segment to assign IP addresses.

### Notice

If there are two DHCP servers in the network environment, please do not repeat the IP address assignment of the two DHCP servers to avoid causing IP conflicts.

DHCP Setup

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

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

## DHCP Client List

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

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

## Static Lease IP Setup

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

Static Lease IP Setup

Comment

IP Address

MAC Address

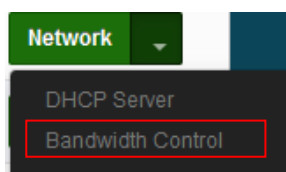
Add

- **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.

## 5.2.2 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

Airtime Fairness

☐ Enable
 ☒ Disable

- **Mode**: Administrator can Enable or Disable the function.
- **Airtime Fairness**: TX/RX traffic balancing, if device use point-to-point ( WDS or AP mode + Client Bridge) then recommended to enable it.

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            | <input type="checkbox"/> | ANY       |        |        | 1024         | 1024           |         |
| 2            | <input type="checkbox"/> | ANY       |        |        | 1024         | 1024           |         |
| 3            | <input type="checkbox"/> | ANY       |        |        | 1024         | 1024           |         |
| 4            | <input type="checkbox"/> | ANY       |        |        | 1024         | 1024           |         |
| 5            | <input type="checkbox"/> | ANY       |        |        | 1024         | 1024           |         |
| 6            | <input type="checkbox"/> | ANY       |        |        | 1024         | 1024           |         |
| 7            | <input type="checkbox"/> | ANY       |        |        | 1024         | 1024           |         |
| 8            | <input type="checkbox"/> | ANY       |        |        | 1024         | 1024           |         |
| 9            | <input type="checkbox"/> | ANY       |        |        | 1024         | 1024           |         |
| 10           | <input type="checkbox"/> | 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.

## 5.2.3 Radio 0(2.4G)/Radio 1(5G) Access Point Setup

Administrator can Enable or Disable Radio 0(2.4G)/Radio 1(5G) Wi-Fi. If Radio are enabled, administrators can set the SSID and security for the Radio 0(2.4G) and Radio 1(5G) access point.

**Network**

- DHCP Server
- Bandwidth Control
- Radio 0 Setup
- Access Point**
- MAC Filter
- 80211r Fast Roaming
- Radio 1 Setup
- Access Point**
- MAC Filter
- 80211r Fast Roaming

**Security**

**Access Point**
☒ Enable
 ☐ Disable

**ESSID**

**SSID Visibility**
☒ Enable
 ☐ Disable

**Client Isolation**
☐ Enable
 ☒ Disable

**Connection Limit**
☐ Enable
 ☒ Disable

**User Limit**

**Security Type**

- **Access Point:** Administrator can Enable or Disable the Radio 0(2.4G)/Radio 1(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 2.4G/5G limit 40/60 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.

The screenshot shows a web interface for selecting a security type. A dropdown menu is open, displaying three options: 'Open System' (highlighted in blue), 'WPA/WPA2 Personal', and 'WPA/WPA2 Enterprise'. The label 'Security Type' is visible to the left of the dropdown.

- **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.

The screenshot shows a 'PassPhrase Settings' window. It contains several configuration fields: 'WPA Mode' set to 'Auto (WPA or WPA2)', 'Cipher Type' set to 'Auto', 'Group Key Update Interval' set to '600' seconds, a 'PassPhrase' input field, 'WPS' radio buttons for 'Enable' and 'Disable' (with 'Disable' selected), and a 'WPS Push Button' labeled 'Push Button'.

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

**AES** is short for “**Advanced Encryption Standard**”, The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plaintext into

the final output of ciphertext. Each round consists of several processing steps, including one that depends on the encryption key. A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key. **TKIP** is short for “**Temporal Key Integrity Protocol**”, TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven’t been tampered with.

- ✓ **Group Key Update Interval:** 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.

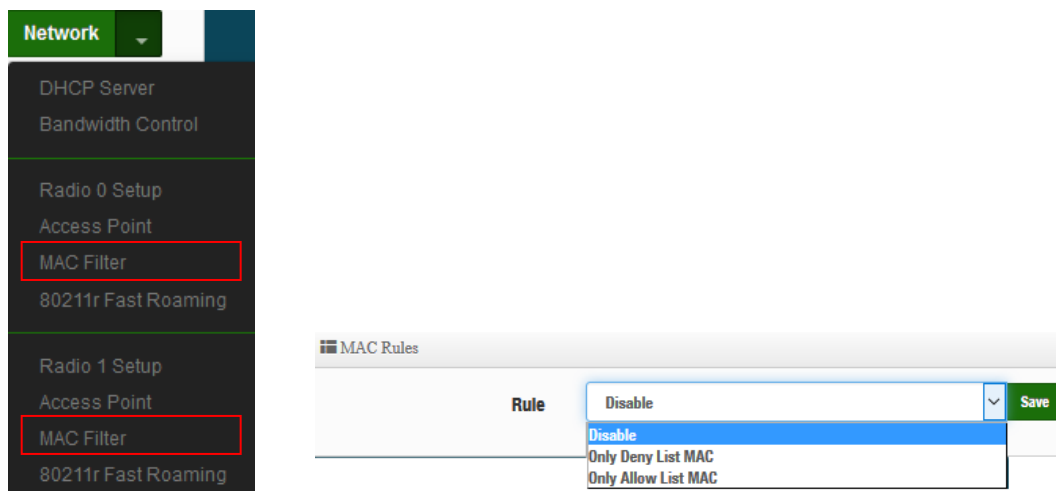
## ● WPA/WAP2-Enterprise

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

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

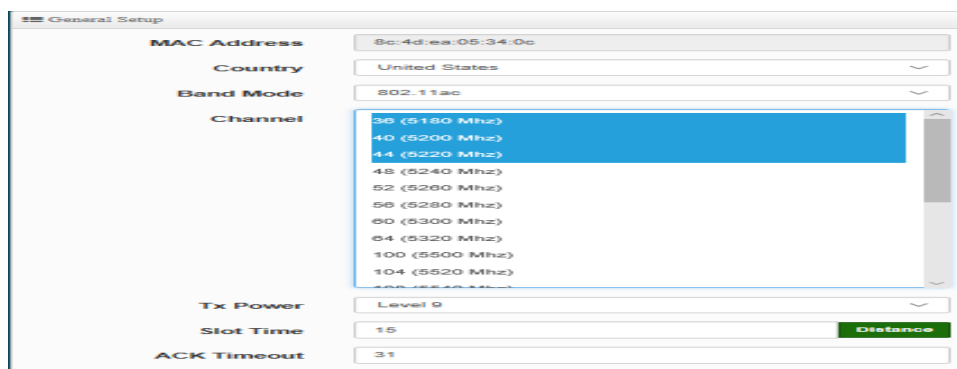


## 5.2.4 MAC Filter



(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.

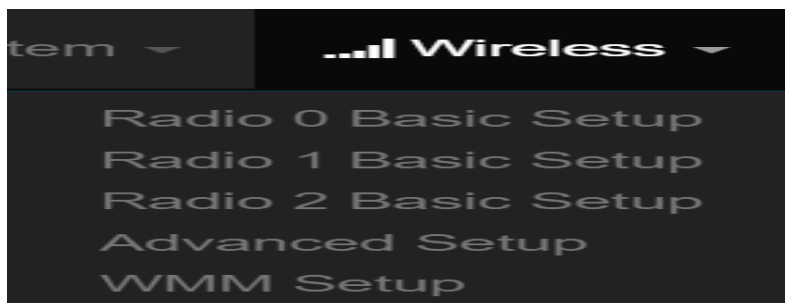
(2) **Only Allow List MAC** : Administrator can add wireless users MAC address in MAC list. The access point will allow connection in MAC address list.



- **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.

## 5.2.5 802.11r Fast Roaming Setup



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

### Notice

If this feature is enabled when using 802.11r fast roaming, the wireless user equipment must support 802.11k functionality to work properly

A screenshot of the 'Fast Roaming Settings' form in the Cerio web interface. The form contains several input fields and a radio button group. The fields are: 'Mobility Domain' (value: a1b2), 'R0 Key Lifetime' (value: 10000), 'Reassoc deadline' (value: 1000), 'R0/NAS Identifier' (value: ap.example.com), and 'R1 Identifier' (value: 000102030405). At the bottom, there is a radio button group for 'R1 Push' with 'Enable' and 'Disable' options. The 'Disable' option is selected.

- **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.

### Notice

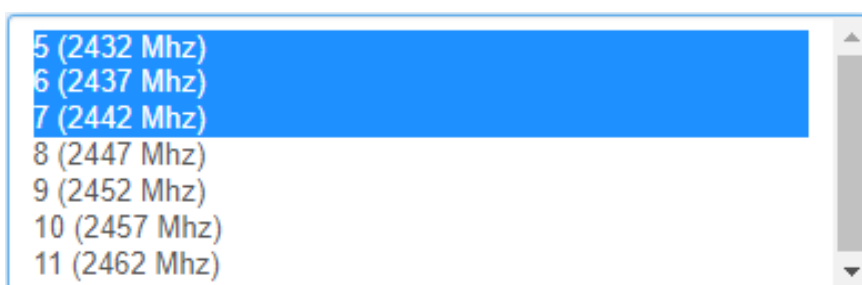
This setting must be 2-octet of hex string codes. For example, enter 8c4d

- **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.



- **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.

| # | 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

R1 Identifier

128-bit Key

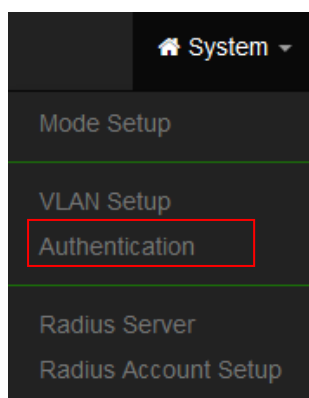
- **MAC Address:** Enter the main roaming device MAC address
- **R1 Identifier:** Enter Shared identifier.
- **128-bit Key:** Enter Shared Key of 128 bit.

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

## 5.3 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 **Manual 5.2 "VLAN Setup"**. If the gateway IP address is set error then web authentication page will 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 5.2 VLAN Setup)
- **Authentication** : Displays VLAN# whether enable or disable web authentication.
- **Action** : The function has 2 buttons (Authentication and Dropdown)

### 5.3.1 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= dport=443      |
|            |          |             |               | MAC= :13 auth=64<000> User account  |
| 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= dport=443      |
|            |          |             |               | MAC= auth=64<000> Used IP address of User   |
| 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= dport=443      |
|            |          |             |               | MAC= auth=64<000> MAC address of user device  |
| 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= dport=443      |
|            |          |             |               | MAC= 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= dport=443      |
|            |          |             |               | MAC= 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= dport=443      |
|            |          |             |               | MAC= 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= dport=443 MAC= |
|            |          |             |               | auth=64<000>  |

- **Local User** : Administrator can enable authentication for local user.
- **RADIUS** : Authentication support remote RADIUS Server. Administrator can enter security

information for remote RADIUS Server.

Radius Setup

Radius

☒ Enable
 ☐ Disable

Display Name

Primary Server IP

Secondary Server IP

Authentication Port

Port

Accounting Service

☐ 1813
 

Port

Authentication Type

☐ PAP
 ☒ CHAP

Secret Key

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

## 5.3.2 Set Authentication function

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

Authentication

Guest

Local User

OAuth 2.0

POP3/IMAP Server

Customize Page

Language

Walled Garden

Privilege Address

Profile



## # Guest

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

- **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.

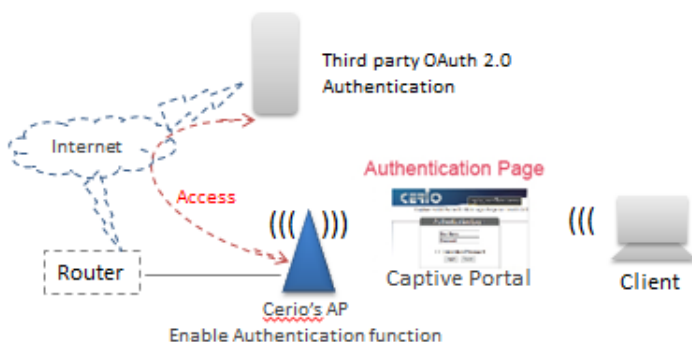
## # Local User

Administrator can create local user account for web login.

- **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 <span>Create New Provider</span> |                  |          |                   |
|--|------------------|----------|-------------------|
| #  | Active           | Provider | Action            |
| 1  | <span>Off</span> | Google   | <span>Edit</span> |
| 2  | <span>Off</span> | Facebook | <span>Edit</span> |

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

## # Google OAuth2.0 setup sample

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 ?

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

[Show advanced options...](#)

Create
Cancel

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

### API API Manager

Overview
**Credentials**

#### 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.

Create credentials ▾

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

### Create client ID

**Application type**

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

Create
Cancel

Name

Web client 1

## Restrictions

Enter JavaScript origins, redirect URIs, or both

### Authorized JavaScript origins

For use with requests from a browser. This is the origin URL 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 | <input type="checkbox"/> 3  | User(s) |
| Login Timeout  | 10  | Minutes |
| Redirect URL   | http://www.google.com   |         |
| Login URL      | domain0.login.com   |         |
| Session Log    | <input type="radio"/> Enable <input checked="" type="radio"/> 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 URL 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 URL.

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

googleusercontent.com

Here is your client secret

YwM

OK

OAuth 2.0 Setup

Advanced

Client ID

ps.googleuse

Client Secret

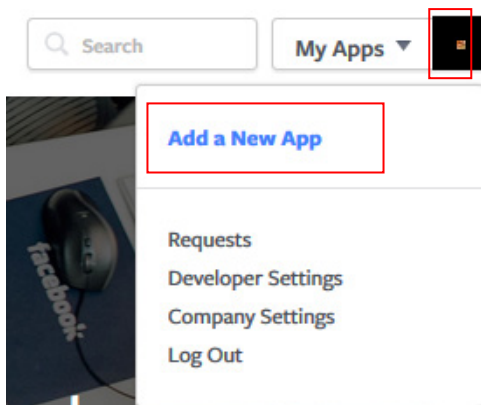
YwM

Save and reboot the AP system, complete the setup.

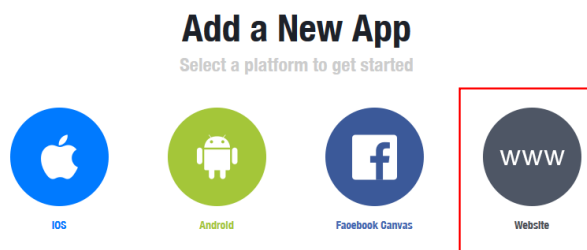
## # Facebook OAuth2.0 setup sample

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



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

**Step.3** Administrator must set www for your information.

### Create a New App ID

Get started integrating Facebook into your app or website

Display Name

The name of your app or website

Namespace

A unique identifier for your app (optional)

Contact Email

Used for important communication about your app

Category

Choose a Category

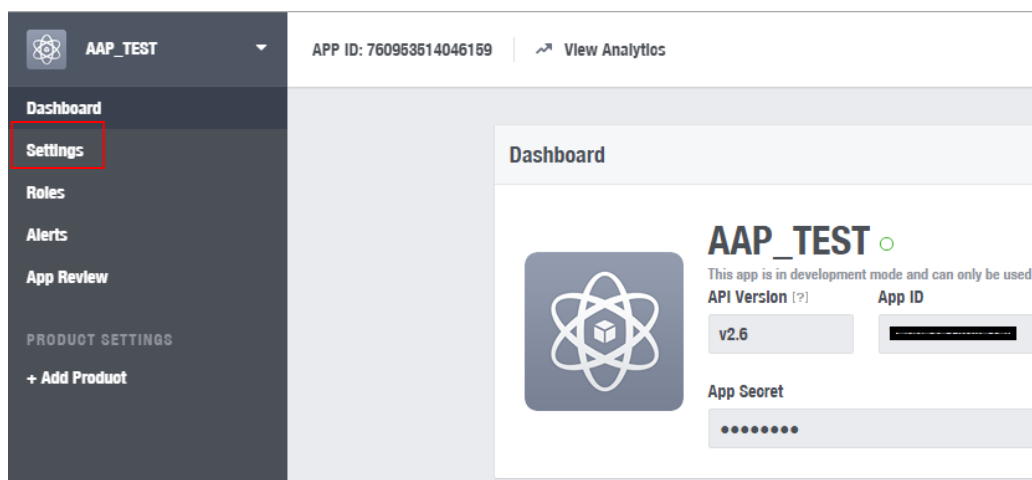
By proceeding, you agree to the [Facebook Platform Policies](#)

Cancel

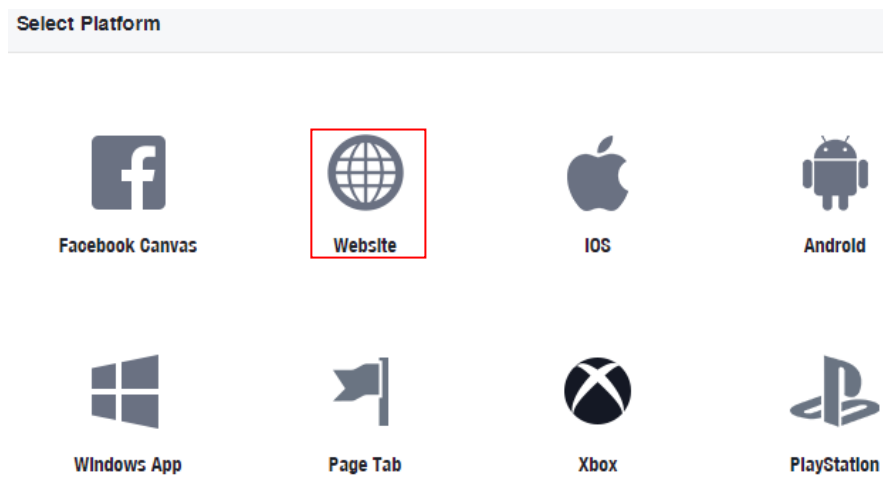
Create App ID

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





## Step.5 Select Platform for “Website”



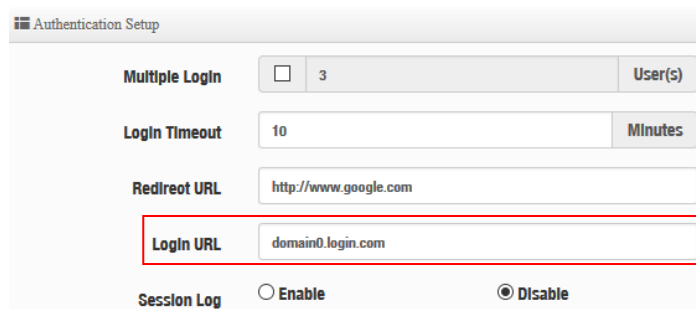
## Step.6 Enter URL is **http://domain0.login.com/login/index.cgi?cgi=CALLBACK**

Site URL

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

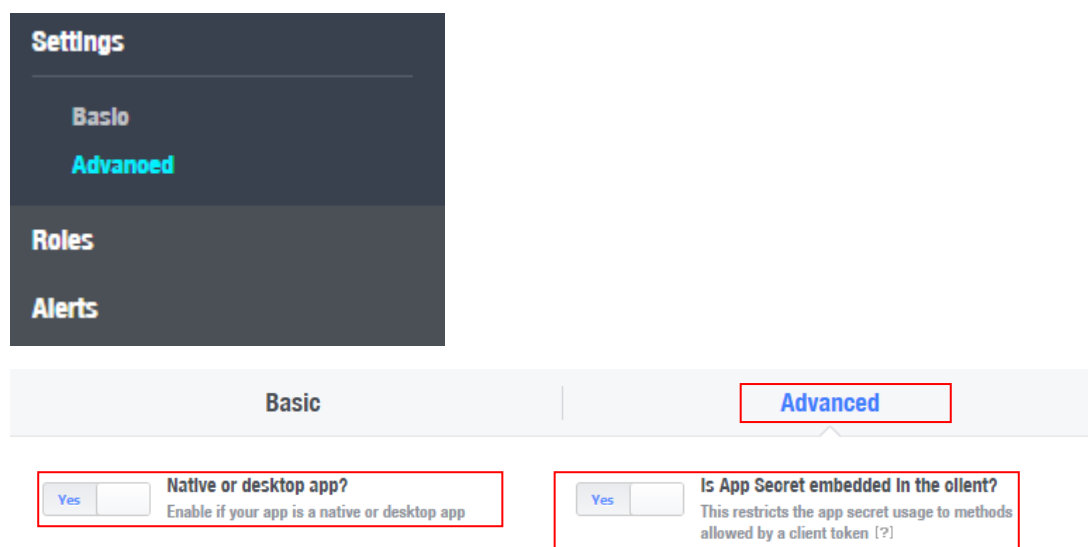
Redirect URL http://www.google.com

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?”



Settings

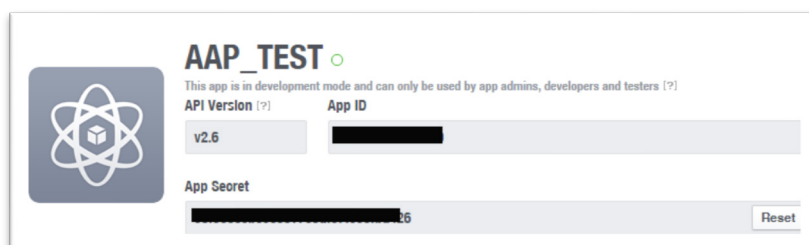
- Basic
- Advanced
- Roles
- Alerts

Basic | Advanced

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

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

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



**AAP\_TEST** ○

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

API Version [?] v2.6 App ID [REDACTED]

App Secret [REDACTED] Reset

OAuth 2.0 Setup

Advanced

Client ID

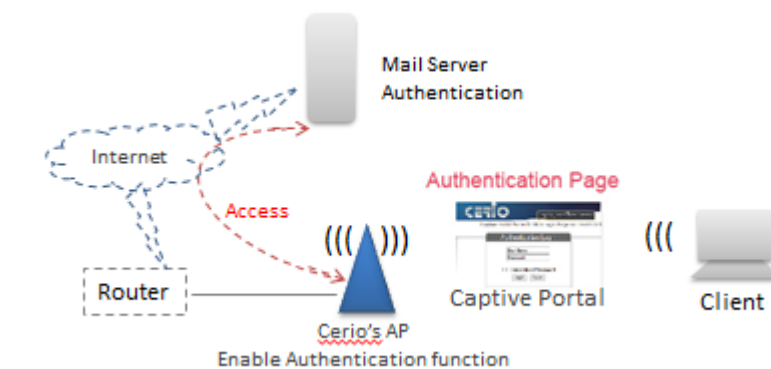
Client Secret

## 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.

## 5.3.3 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

Test

- **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

## 5.3.4 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** : 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>
    
```

Do not delete the red part of the default source code. The other parts can be edited through html syntax or css.

## Notice

When using html and css and other syntax editing, it is recommended that editors have html and css and other editing capabilities. Cerio does not support the use of assisted teaching of grammar. The field must be within 190 lines. If you write the source code such as HTML / CSS After a certain amount of time, it is recommended to save the CSS source code to the remote Web server, and then enter the IP address of the remote web server into Walled Garden.

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



## Notice

1. This editing html system has a certain length limit, and at the same time, it is not possible to upload the image file to the system, so if there is CSS syntax or image file, it must be uploaded to the web server first, and the image file is linked by hyperlink.
2. In the system's Walled Garden function, you must add the IP address of the server to upload the image file or CSS file.

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.

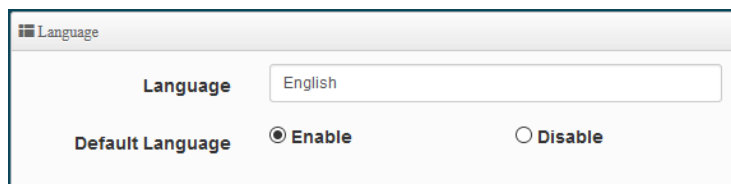
## i. Language

Administrator can create other language for login page.

| Language List |         |          |        | Create New Language |
|---------------|---------|----------|--------|---------------------|
| #             | Default | Language | Action |                     |
| 1             | ★       | English  | Edit   |                     |



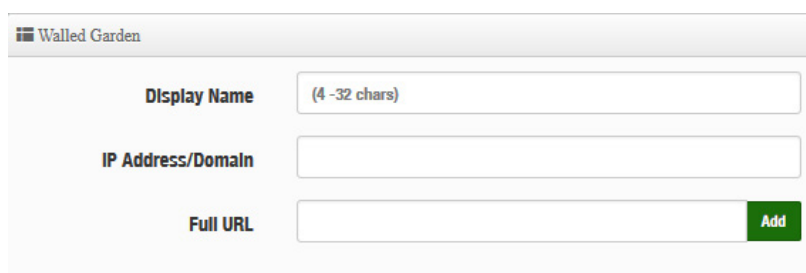
Click “Create New Language” button go to add or edit language for login page.



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

## ii. Walled Garden

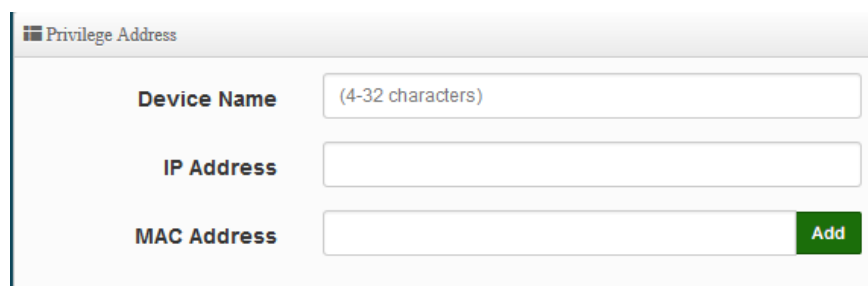
This function provides certain free services or advertisement web pages for users to access the websites listed before login and authentication. User without the network access right can still have a chance to experience the actual network service free of charge in Walled Garden URL list.



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

## iii. 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.



- **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.

A list of up to 10 websites can be created in the form.

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

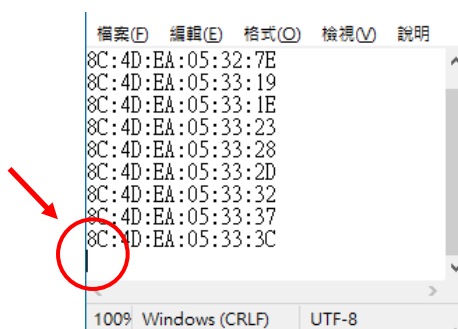
#### iv. Bulk MAC Address

The function is MAC whitelist. Administrator can upload batch MAC address °



#### Notice

When upload MAC whitelist file, the extension name must use csv file. Ex. aaa.csv . The TXT file can also be used. When using TXT file, please pay attention to the following steps: fill in the MAC one per line, and the cursor needs to click on the bottom blank when saving as a new file, please pay attention to the coding principle when saving as, it is recommended to choose ANSI.



- **Rule :** Administrator can select enable or disable the MAC address verification.
- **Upload MAC Address :** Administrator can click to find file and upload file.

When the confirmation is complete, click Restart the system to make the function work normally.

| MAC Address List |                   |    |                   |    |                   |
|------------------|-------------------|----|-------------------|----|-------------------|
| #                | MAC Address       | #  | MAC Address       | #  | MAC Address       |
| 1                | 80:4D:EA:04:A6:5F | 2  | 80:4D:EA:04:A6:62 | 3  | 80:4D:EA:04:A6:65 |
| 6                | 80:4D:EA:04:A6:6E | 7  | 80:4D:EA:04:A6:71 | 8  | 80:4D:EA:04:A6:74 |
| 11               | 80:4D:EA:04:A6:7D | 12 | 80:4D:EA:04:A6:80 | 13 | 80:4D:EA:04:A6:83 |
| 16               | 80:4D:EA:04:A6:8C | 17 | 80:4D:EA:04:A6:8F | 18 | 80:4D:EA:04:A6:92 |
| 21               | 80:4D:EA:04:A6:9B | 22 | 80:4D:EA:04:A6:9E | 23 | 80:4D:EA:04:A6:A1 |
| 4                | 80:4D:EA:04:A6:68 | 5  | 80:4D:EA:04:A6:6B | 9  | 80:4D:EA:04:A6:77 |
|                  |                   | 10 | 80:4D:EA:04:A6:7A | 14 | 80:4D:EA:04:A6:86 |
|                  |                   | 15 | 80:4D:EA:04:A6:89 | 19 | 80:4D:EA:04:A6:95 |
|                  |                   | 20 | 80:4D:EA:04:A6:98 | 24 | 80:4D:EA:04:A6:A4 |
|                  |                   | 25 | 80:4D:EA:04:A6:A7 |    |                   |

## v. Profile

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

VLAN Profile

Download Profile Setting
Download

Upload Profile Setting
Choose File No file chosen
Upload

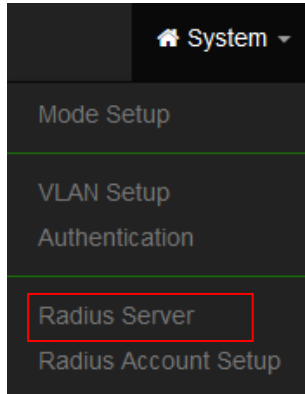
VLAN Customize Page

Download Customize Page
Download

Upload Customize Page
Choose File No file chosen
Upload

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

## 5.4 RADIUS Server



### Notice

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

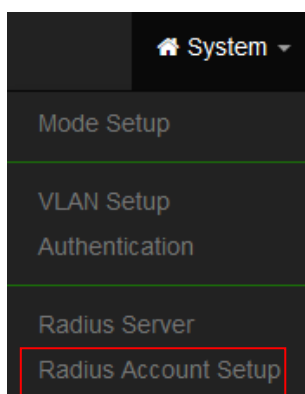
A screenshot of the 'Radius Server' configuration page. It features a 'Service' section with radio buttons for 'Enable' (selected) and 'Disable'. Below this are two input fields: 'Radius Port' with the value '1812' and 'Radius Secret' with a placeholder '(4-32 chars)'.

- **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.

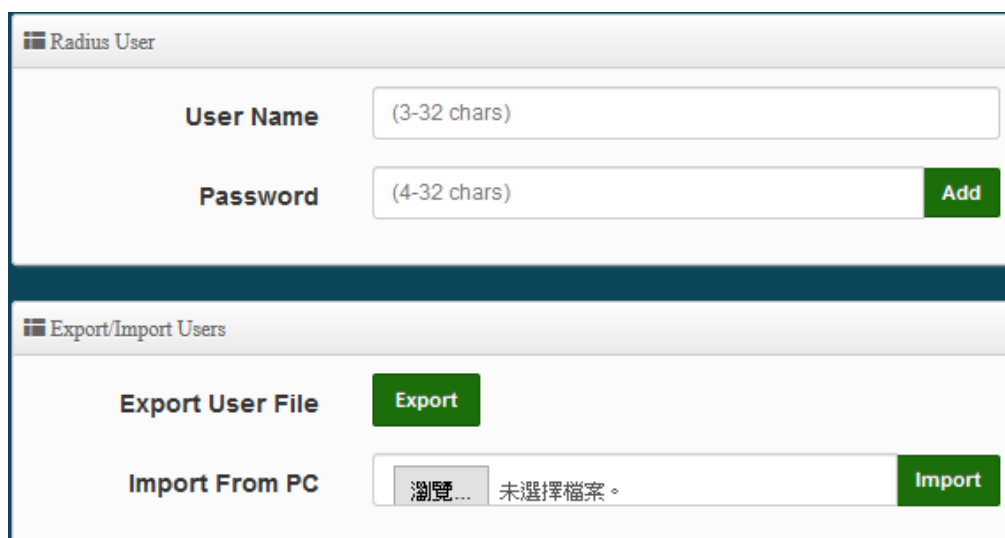
## 5.5 RADIUS Account Setup

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



### Notice

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



The screenshot displays two sections of the CERIO web interface. The top section, titled "Radius User", contains two input fields: "User Name" with a "(3-32 chars)" hint and "Password" with a "(4-32 chars)" hint. A green "Add" button is positioned to the right of the Password field. The bottom section, titled "Export/Import Users", contains two options: "Export User File" with a green "Export" button, and "Import From PC" with a file selection button labeled "瀏覽..." (Browse...) and "未選擇檔案" (No file selected), followed by a green "Import" button.

- **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.

## 5.6 Wireless Configuration

This wireless functions administrator can set Radio 0(2.4G) or Radio 1(5G) application of the Access Point.

### 5.6.1 Radio 0 (2.4G) Setup

- **MAC Address:** Display 2.4G WiFi MAC address.
- **Country:** Administrator can select country: United States(US) , Europe(EU) or Taiwan(TW).
- **Band Mode:** Administrator can select 802.11 b, 802.11 b/g, 802.11 b/g/n, 802.11 n for the 2.4G Band.
- **Auto Channel:** Administrator can Enable or Disable the function. If disabled, the WiFi channel will be fixed to the manually selected channel.
- **Channel:** Administrator can select 1 to 11 CH. The Channel settings can be changed in “HT Physical Mode” ➔ “Extension Channel” can select **Upper** or **Lower** channels.

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

20/40

Extension Channel

☐ Upper
 ☒ Lower

MCS

Auto

Short GI

☒ Enable
 ☐ Disable

Aggregation

☒ Enable
 ☐ Disable

- **TX/RX Stream:** Build in 2.4GHz 2 antennas and support 2TX/2RX streams. Administrator can select 1 or 2 TX/RX. The default is 2TX/2RX.

## Notice

This product has a built-in 2x2 (2T2R) antenna for 2.4Ghz, which has been matched with the default setting of 2T2R. If there is no special demand, please keep this default setting .

- **Channel Bandwidth:** The "20/40" MHz option is usually best. The other option is available for special circumstances.
- **Extension Channel:** Sets channel select to Upper or Lower. The Upper supports 1 to 7 range CH and Lower supports 5 to 11 range CH.
- **MCS:** This parameter represents transmission rate. By default (Auto) the fastest possible transmission rate will be selected. You have the option of selecting the speed if necessary.
- **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 "Enabled". Select "Disable" to deactivate Aggregation. A part of the 802.11n standard (or draft-standard), it allows sending multiple frames per single access to the medium by combining frames together into one larger frame. It creates the larger frame by combining smaller frames with the same physical source and destination end points and traffic class (i.e. QoS) into one large frame with a common MAC header.

## 5.6.2 Radio 1(5G) Setup

The screenshot displays the 'General Setup' window for 'Radio 1 Basic Setup'. The left sidebar contains a 'Wireless' dropdown menu with options: Radio 0 Basic Setup, Radio 1 Basic Setup (selected), Advanced Setup, WMM Setup, WDS Setup, and WDS Status. The main configuration area includes the following fields:

- MAC Address:** 8c:4d:ea:05:23:28
- Country:** Taiwan
- Band Mode:** 802.11ac
- Auto Channel:** ☒ Enable ☐ Disable
- Channel:** 153 (5765 Mhz)
- Tx Power:** Level 9
- Slot Time:** 12 (with a green 'Distance' button)
- ACK Timeout:** 28

- **MAC Address:** Display Radio1(5G) WiFi MAC address.
- **Country:** Administrator can select country: United States(US) , Europe(EU) or Taiwan(TW).
- **Band Mode:** Administrator can select 5G Band for 802.11a or 802.11a/n or 802.11n(5G) or 802.11ac. The default is 802.11ac etc..
- **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 Timeout :** 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 Timeout :** 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

80

BandWidth

Min MCS

4

Max MCS

9

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.

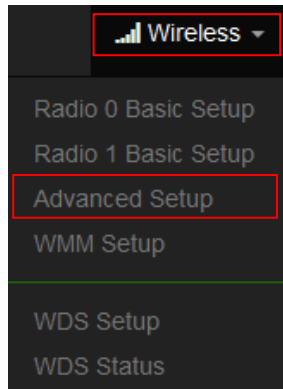
## Notice

This product has a built-in 2x2 (2T2R) antenna for 5Ghz, which has been matched with the default setting of 2T2R. If there is no special demand, please keep this default setting .

- **Channel Bandwidth:** The "20/40 and 802.11ac 80" MHz option is usually the best. The other option is available for special circumstances.
- **MIN MCS:** This parameter represents transmission rate. By default (4) the fastest possible transmission rate will be selected. You have the option of selecting the speed if necessary.
- **MAX MCS:** This parameter represents transmission rate. By default (9) the fastest possible transmission rate will be selected. You have the option of selecting the speed if necessary.
- **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.

## 5.6.3 Advanced Setup



- **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 result 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 into 4 small packets 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:** RTS Threshold is in the range of **1~2347** byte. The default is **2347** byte.  
The main purpose of enabling RTS by changing RTS threshold is to reduce possible collisions due to hidden wireless clients. RTS in AP will be enabled automatically if the packet size is larger than the Threshold value. By default, RTS is disabled in a normal environment supports non-jumbo frames.
- **Short Preamble:** By default, this function is **"Enabled"**. **Disabling** will automatically use the Long 128-bit Preamble Synchronization field. The preamble is used to signal "here is a train of data coming" to the receiver. The short preamble provides 72-bit Synchronization field to improve WLAN transmission efficiency with less overhead.
- **IGMP Snooping:** The process of listening to Internet Group Management Protocol (IGMP) network traffic. The feature allows a network switch to listen in on the IGMP conversation between hosts and routers. By listening to these conversations the switch maintains a map of which links need which IP multicast streams. Multicasts may be filtered from the links which do not need them and thus controls which ports receive specific multicast traffic.
- **Greenfield:** In wireless WLAN technology, greenfield mode is a feature of major components of the 802.11n specification. The greenfield mode feature is designed to improve efficiency by eliminating support for 802.11b/g devices in an all draft-n network. In greenfield mode the network can be set to ignore all earlier standards.
- **Band Steering:** When 2.4GHz and 5GHz network cards coexist, the 5GHz network card is automatically used as the main connection to improve the performance. The threshold for connecting RSSI can be set, that is, when the signal value of the wireless user and the AP is better, the local machine will automatically interrupt the 2.4G user and force the use of 5G.
- **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.

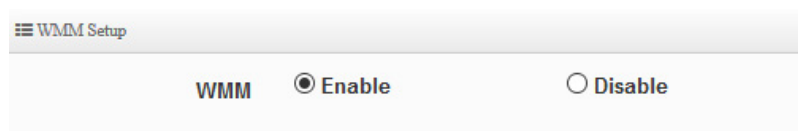
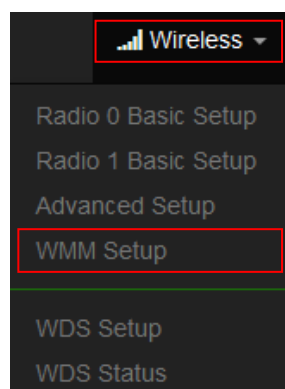
## 5.6.4 WMM Setup

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

Configuring QoS options consists of setting parameters on existing queues for different types of wireless traffic. You can configure different minimum and maximum wait times for the transmission of packets in each queue based on the requirements of the media being sent. Queues automatically provide minimum transmission delay for Voice, Video, multimedia, and mission critical applications, and rely on best-effort parameters for traditional IP data.

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

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





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

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

➤ **AC Type :**

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

- **CWmin:** Minimum Contention Window. This parameter is input to the algorithm that determines the initial random backoff wait time ("window") for retry of a transmission. The value specified here in the Minimum Contention Window is the upper limit (in milliseconds) of a range from which the initial random backoff wait time is determined.
- **CWmax:** Maximum Contention Window. The value specified here in the Maximum Contention Window is the upper limit (in milliseconds) for the doubling of the random backoff value. This doubling continues until either the data frame is sent or the Maximum Contention Window size

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

- **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.

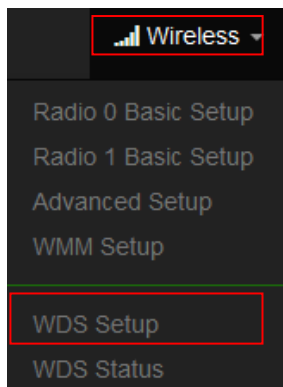
While the No ACK policy helps improve transmission efficiency, it can cause increased packet loss when communication quality deteriorates. This is because when this policy is used, a sender does not retransmit packets that have not been received by the recipient.

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.

## 5.6.5 WDS Setup

Please click on Wireless -> WDS Setup



### Notice

When the WDS function is enabled, it can be set to use Radio 0 (2.4G) for WDS or Radio 1 (5G) for WDS, etc., and a maximum of 24 groups can be set up to bridge to 2.4G + 5G + 5G. In WDS The function supports VLAN tag transmission. If there is a tag set in the network domain, WDS can bring multiple groups of tags to another bridge endpoint.

WDS Setup

WDS Setup

☒ Enable
 ☐ Disable

Radio0 ESSID

default\_wds0

Radio1 ESSID

default\_wds1

Radio2 ESSID

default\_wds2

Security Type

Disable

PassPhrase

MAC Address

Radio 0

00:11:a3:1e:00:03

Radio 1

00:11:a3:1e:00:04

Radio 2

00:11:a3:1e:00:05

WDS Client Setup

| Radio 0                  |             | Radio 1                  |             | Radio 2                  |             |
|--------------------------|-------------|--------------------------|-------------|--------------------------|-------------|
| Enable                   | MAC Address | Enable                   | MAC Address | Enable                   | MAC Address |
| <input type="checkbox"/> |             | <input type="checkbox"/> |             | <input type="checkbox"/> |             |
| <input type="checkbox"/> |             | <input type="checkbox"/> |             | <input type="checkbox"/> |             |
| <input type="checkbox"/> |             | <input type="checkbox"/> |             | <input type="checkbox"/> |             |
| <input type="checkbox"/> |             | <input type="checkbox"/> |             | <input type="checkbox"/> |             |
| <input type="checkbox"/> |             | <input type="checkbox"/> |             | <input type="checkbox"/> |             |
| <input type="checkbox"/> |             | <input type="checkbox"/> |             | <input type="checkbox"/> |             |
| <input type="checkbox"/> |             | <input type="checkbox"/> |             | <input type="checkbox"/> |             |
| <input type="checkbox"/> |             | <input type="checkbox"/> |             | <input type="checkbox"/> |             |

VLAN Setup

| VLAN#   | Radio 0                          |                          |        | Radio 1                          |                          |        | Radio 2                          |                          |        |
|---------|----------------------------------|--------------------------|--------|----------------------------------|--------------------------|--------|----------------------------------|--------------------------|--------|
|         | Native                           | TAG                      | TAG ID | Native                           | TAG                      | TAG ID | Native                           | TAG                      | TAG ID |
| VLAN 0  | <input checked="" type="radio"/> | <input type="checkbox"/> |        | <input checked="" type="radio"/> | <input type="checkbox"/> |        | <input checked="" type="radio"/> | <input type="checkbox"/> |        |
| VLAN 1  | <input type="radio"/>            | <input type="checkbox"/> | 101    | <input type="radio"/>            | <input type="checkbox"/> | 101    | <input type="radio"/>            | <input type="checkbox"/> | 101    |
| VLAN 2  | <input type="radio"/>            | <input type="checkbox"/> | 102    | <input type="radio"/>            | <input type="checkbox"/> | 102    | <input type="radio"/>            | <input type="checkbox"/> | 102    |
| VLAN 3  | <input type="radio"/>            | <input type="checkbox"/> | 103    | <input type="radio"/>            | <input type="checkbox"/> | 103    | <input type="radio"/>            | <input type="checkbox"/> | 103    |
| VLAN 4  | <input type="radio"/>            | <input type="checkbox"/> | 104    | <input type="radio"/>            | <input type="checkbox"/> | 104    | <input type="radio"/>            | <input type="checkbox"/> | 104    |
| VLAN 5  | <input type="radio"/>            | <input type="checkbox"/> | 105    | <input type="radio"/>            | <input type="checkbox"/> | 105    | <input type="radio"/>            | <input type="checkbox"/> | 105    |
| VLAN 6  | <input type="radio"/>            | <input type="checkbox"/> | 106    | <input type="radio"/>            | <input type="checkbox"/> | 106    | <input type="radio"/>            | <input type="checkbox"/> | 106    |
| VLAN 7  | <input type="radio"/>            | <input type="checkbox"/> | 107    | <input type="radio"/>            | <input type="checkbox"/> | 107    | <input type="radio"/>            | <input type="checkbox"/> | 107    |
| VLAN 8  | <input type="radio"/>            | <input type="checkbox"/> | 108    | <input type="radio"/>            | <input type="checkbox"/> | 108    | <input type="radio"/>            | <input type="checkbox"/> | 108    |
| VLAN 9  | <input type="radio"/>            | <input type="checkbox"/> | 109    | <input type="radio"/>            | <input type="checkbox"/> | 109    | <input type="radio"/>            | <input type="checkbox"/> | 109    |
| VLAN 10 | <input type="radio"/>            | <input type="checkbox"/> | 110    | <input type="radio"/>            | <input type="checkbox"/> | 110    | <input type="radio"/>            | <input type="checkbox"/> | 110    |
| VLAN 11 | <input type="radio"/>            | <input type="checkbox"/> | 111    | <input type="radio"/>            | <input type="checkbox"/> | 111    | <input type="radio"/>            | <input type="checkbox"/> | 111    |
| VLAN 12 | <input type="radio"/>            | <input type="checkbox"/> | 112    | <input type="radio"/>            | <input type="checkbox"/> | 112    | <input type="radio"/>            | <input type="checkbox"/> | 112    |
| VLAN 13 | <input type="radio"/>            | <input type="checkbox"/> | 113    | <input type="radio"/>            | <input type="checkbox"/> | 113    | <input type="radio"/>            | <input type="checkbox"/> | 113    |
| VLAN 14 | <input type="radio"/>            | <input type="checkbox"/> | 114    | <input type="radio"/>            | <input type="checkbox"/> | 114    | <input type="radio"/>            | <input type="checkbox"/> | 114    |
| VLAN 15 | <input type="radio"/>            | <input type="checkbox"/> | 115    | <input type="radio"/>            | <input type="checkbox"/> | 115    | <input type="radio"/>            | <input type="checkbox"/> | 115    |

- **WDS Setup:** Administrator can select Enable or Disable.
- **Security Type:** Enable or Disable AES 128bit encryption function.
- **Pass Phrase :** AES encryption custom key can input 0 ~ 9 numbers or A ~ Z uppercase and lowercase English format, it can support 8 ~ 32 characters key encryption algorithm in each WDS connecting each other with secure encrypted transmission.
- **MAC Address :** Enter the MAC address of the other party's host to agree to accept the connection.
- **WDS Client Setup:** Administrator can used Radio 0(2.4G) or Radio 1(5G) for WDS Links. A Single Radio supports up to 8 WDS links.

## Notice

### WDS considerations

1. When two wireless APs want to use WDS connection, the channels of the two must be the same.
2. If the two base AP stations are A and B, the WDS Client Setup of station A needs to set the wireless MAC address of station B, and the WDS Client Setup of station B needs to set the wireless MAC address of station A.
3. If tags must be used in the architecture, the APs on both sides can select multiple sets of tags in the virtual network settings.
4. WDS encryption setting is by optional use.

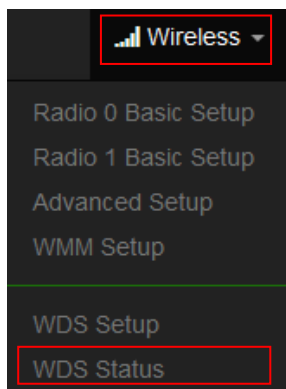
- **VLAN Setup:** The WDS aisle support Multi-tag VALN

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

## 5.6.6 WDS Status

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

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



| Radio0 Client |             |      |
|---------------|-------------|------|
| MAC Address   | Rate(RX/TX) | RSSI |
| -             | -           | -    |

| Radio1 Client |             |      |
|---------------|-------------|------|
| MAC Address   | Rate(RX/TX) | RSSI |
| -             | -           | -    |

| Radio2 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

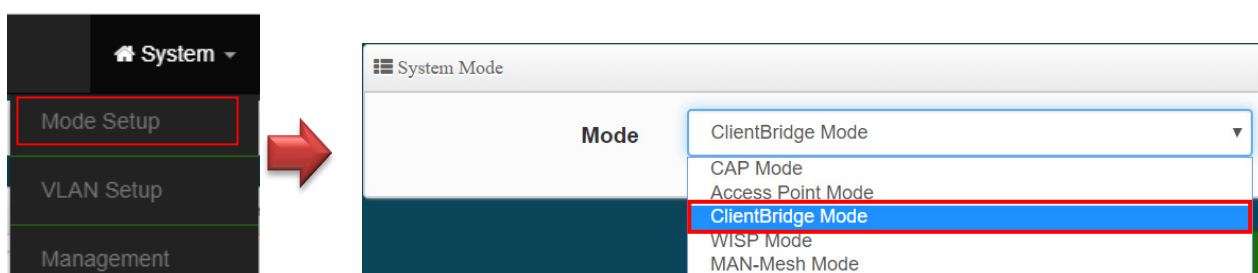
Click **“Save”** button to save your set function. Then click **“Reboot”** button to activate your changes.

## 6. 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.

### 6.1 Change Setup mode

If the administrator needs to switch to Client Bridge mode, Please click "System"-> " Mode Setup " to change Client Bridge mode.



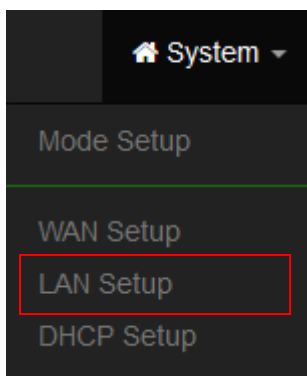
#### Notice

Please note that the LAN IP addresses in each mode are different from each other and will not continue. For the first time after switching modes, always perform access management on the LAN default IP address of 192.168.2.254

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

### 6.2 Configure LAN Setup

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





|   |  |   |  |
|---|--|---|--|
| <b>Ethernet Connection Type</b><br>Mode <input checked="" type="radio"/> Static IP <input type="radio"/> Dynamic IP   |  | <b>DNS</b><br>Primary DNS <input type="text"/><br>Secondary DNS <input type="text"/>                                      |  |
| <b>Static IP</b><br>IP Address <input type="text" value="192.168.2.254"/><br>Netmask <input type="text" value="255.255.255.0"/><br>Gateway <input type="text" value="192.168.2.1"/> |  | <b>802.1d Spanning Tree</b><br>802.1d Spanning Tree <input type="radio"/> Enable <input checked="" type="radio"/> Disable |  |
|   |  | <b>DHCP Forward</b><br>DHCP Forward <input type="radio"/> Enable <input checked="" type="radio"/> Disable                 |  |

- **Mode:** Administrator can select the IP used Static or Dynamic IP address.
  - Static IP : A set of fixed IP addresses can be manually set for the system to use.
  - Dynamic IP : If there is a DHCP server on the top, you can use the dynamic IP address to let the system obtain a set of IP automatically.

## Notice

That when using a dynamic IP, the system will automatically obtain the IP address sent by DHCP, and the obtained IP address will be obtained after the operation is confirmed by the upper DHCP server. Obtaining the IP address is not fixed. For system management, the upper DHCP server must query the IP address obtained by the current system.

- **Static IP:**

|                  |  |
|------------------|--|
| <b>Static IP</b> |  |
| IP Address       | <input type="text" value="192.168.2.254"/> |
| Netmask          | <input type="text" value="255.255.255.0"/> |
| Gateway          | <input type="text" value="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.

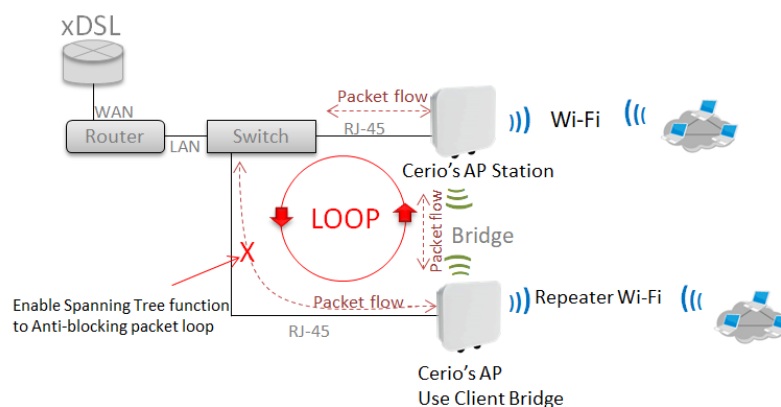
## ➤ 802.1d Spanning Tree :

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.

## 6.3 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.

The screenshot displays the CERIO web interface for configuring the DHCP service. On the left, a sidebar menu shows 'System', 'Mode Setup', 'WAN Setup', 'LAN Setup', and 'DHCP Setup' (highlighted with a red box). The main content area shows the 'DHCP Service' configuration. Under 'Mode', the 'Enable' radio button is selected. Below this is the 'DHCP Setup' form with the following fields:

| Field      | Value         |
|------------|---------------|
| 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 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               | <input type="text"/>                                    |
| IP Address            | <input type="text"/>                                    |
| MAC Address           | <input type="text"/> <input type="button" value="Add"/> |

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

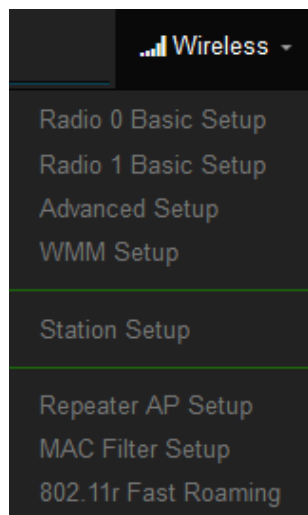
**Static Lease IP List:** Display users list of static IP address.

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

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

## 6.4 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.

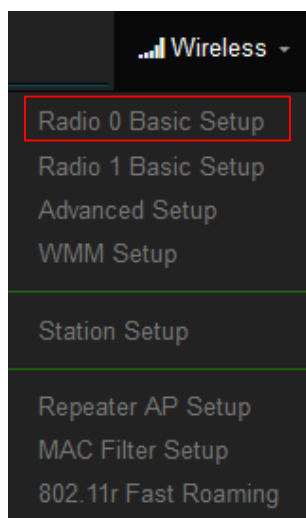


### Notice

When the upper limit of the 2.4G frequency is used, the repeater AP will only be able to use the other two 5G extension Repeater AP APs. If the upper end AP with a Radio 1 (5G) frequency is used, the repeater AP will only Use 2.4G as the extension Repeater AP base.

### 6.4.1 Radio 0(2.4G) Basic Setup

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



| General Setup |   |
|---------------|---|
| MAC Address   | 8c:4d:ea:05:1c:75   |
| Station Mode  | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| Country       | Taiwan  |
| Band Mode     | 802.11b/g/n   |
| Tx Power      | Level 9   |
| Slot Time     | 9 <span>Distance</span>   |
| ACK Timeout   | 64  |

- **Station Mode:** If Client Bridge want to use 2.4G link to Access Point then administrator can enable the function (radio 0).
- **Country:** Administrator can select country used channel by US and EU.
- **Band Mode:** Select an appropriate wireless band; bands available are **801.11 b/g/n mixed mode**.

- **Tx Power:** Administrator can adjust the output power of the system to get the appropriate coverage for your wireless network. Specify digit numbers between level **1** to level 9 (the unit is %) for your environment. If you are not sure which setting to choose, then keep the default setting level 9 (**100%**).
- **Slot Timeout :** 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 Timeout :** 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          |   |
|---------------------------|---|
| <b>TX/RX Stream</b>       | 2T2R  |
| <b>Channel BandWidth</b>  | 20/40   |
| <b>MCS</b>                | Auto  |
| <b>Short GI</b>           | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| <b>Aggregation</b>        | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| <b>Aggregation Frames</b> | 32  |
| <b>Aggregation Size</b>   | 50000   |

- **TX/RX Stream:** Build in 2.4GHz 2 antennas and support 2TX/2RX streams. Administrator can select 1 or 2 TX/RX. The default is 2TX/2RX.

## Notice

This product has a built-in 2x2 (2T2R) antenna for 2.4Ghz, which has been matched with the default setting of 2T2R. If there is no special demand, please keep this default setting .

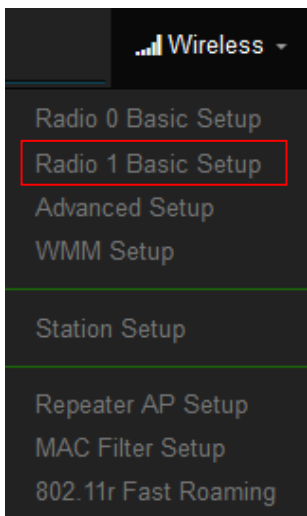
h

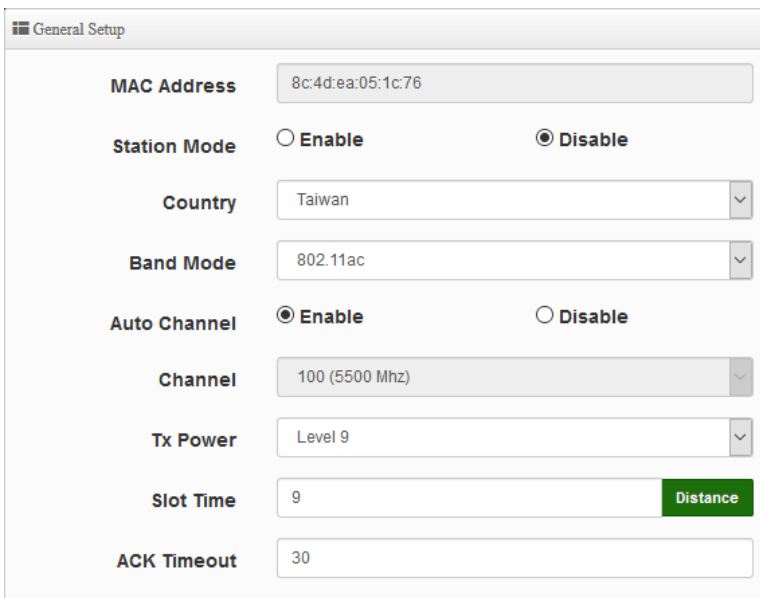


- **Channel Bandwidth:** The "20/40" MHz option is usually best. The other option is available for special circumstances.
- **MCS:** This parameter represents transmission rate. By default (Auto) the fastest possible transmission rate will be selected. You have the option of selecting the speed if necessary.
- **Shout GI:** Short Guard Interval, by default, it's "Enable". it's can increase throughput. However, it can also increase error rate in some installations, due to increased sensitivity to radio-frequency reflections. Select the option that works best for your installation.
- **Aggregation:** By default, it's "Enable". To "Disable" to deactivated Aggregation.  
A part of the 802.11n standard(or draft-standard). It allows sending multiple frames per single access to the medium by combining frames together into one larger frame.  
It creates the larger frame by combining smaller frames with the same physical source and destination end points and traffic class (i.e. QoS) into one large frame with a common MAC header.
- **Aggregation Frames:** 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.

## 6.4.2 Radio 1 (5G) Basic Setup





- **MAC Address:** Display Radio 1(5G) used 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(5G).
- **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 Timeout :** 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 Timeout :** 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

- **TX/RX Stream:** supporting 2TX/2RX streams. Administrator can select 1 or 2 TX/RX. The default is 2TX/2RX.

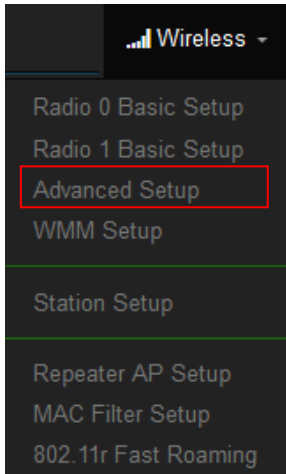
## Notice

This product has a built-in 2x2 (2T2R) antenna for 5Ghz, which has been matched with the default setting of 2T2R. If there is no special demand, please keep this default setting .

- **Channel Bandwidth:** The "20/40 and 802.11ac 80" MHz option is usually best. The other option is available for special circumstances.
- **MIN MCS:** This parameter represents transmission rate. By default (4) the fastest possible transmission rate will be selected. You have the option of selecting the speed if necessary.
- **MAX MCS:** This parameter represents transmission rate. By default (9) the fastest possible transmission rate will be selected. You have the option of selecting the speed if necessary.
- **Shout GI:** Short Guard Interval, by default, it's "Enable". it's can increase throughput. However, it can also increase error rate in some installations, due to increased sensitivity to radio-frequency reflections. Select the option that works best for your installation.
- **Aggregation:** By default, it's "Enable". To "Disable" to deactivated Aggregation.  
A part of the 802.11n standard(or draft-standard). It allows sending multiple frames per single access to the medium by combining frames together into one larger frame. It creates the larger frame by combining smaller frames with the same physical source and destination end points and traffic class (i.e. QoS) into one large frame with a common MAC header.
- **Aggregation Frames:** 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.

## 6.4.3 Advanced Setup



Wireless ▾

- Radio 0 Basic Setup
- Radio 1 Basic Setup
- Advanced Setup**
- WMM Setup
- Station Setup
- Repeater AP Setup
- MAC Filter Setup
- 802.11r Fast Roaming

**Advanced Setup**

|                       |   |
|-----------------------|---|
| Beacon Interval       | <input type="text" value="100"/>                                      |
| DTIM Interval         | <input type="text" value="1"/>  |
| Fragment Threshold    | <input type="text" value="2346"/>                                     |
| RTS Threshold         | <input type="text" value="2346"/>                                     |
| Short Preamble        | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| IGMP Snooping         | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| Greenfield            | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| RF on/off by Schedule | <input type="text" value="Always"/> ▾                                 |
| Location Tracking Log | <input type="checkbox"/> <input type="text" value="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 result 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:** RTS 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.

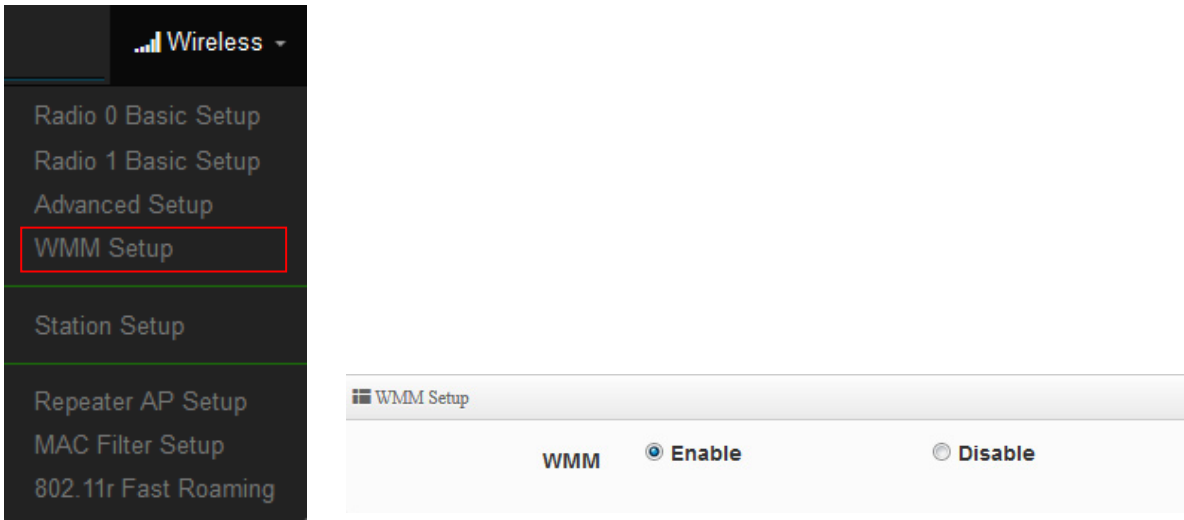
```
Jan 1 08:28:00 Wifilogd: tm=1420072080 vlan=0 radio=0 bssid=8c:4d:ea:05:1c:7a climac=81-7-28-11-19 rssi=-67
Jan 1 08:27:00 Wifilogd: tm=1420072020 vlan=0 radio=0 bssid=8c:4d:ea:05:1c:7a climac=81-7-28-11-19 rssi=-68
Jan 1 08:26:00 Wifilogd: tm=1420071960 vlan=0 radio=0 bssid=8c:4d:ea:05:1c:7a climac=81-7-28-11-19 rssi=-67
```

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



6.4.4 WMM Setup

This affects traffic flowing from the access point to the client station. Configuring QoS options consists of setting parameters on existing queues for different types of wireless traffic. You can configure different minimum and maximum wait times for the transmission of packets in each queue based on the requirements of the media being sent. Queues automatically provide minimum transmission delay for Voice, Video, multimedia, and mission critical applications, and rely on best-effort parameters for traditional IP data.



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

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



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

➤ **AC Type :**

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

➤ **CWmin :**

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

➤ **CWmax :** Maximum Contention Window. The value specified here in the Maximum Contention Window is the upper limit (in milliseconds) for the doubling of the random backoff value. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached. Once the Maximum Contention Window size is reached, retries will continue until a maximum number of retries allowed is reached. Valid values for the "cwmax" are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024. The value for "cwmax" must be higher than the value for "cwmin". ◦

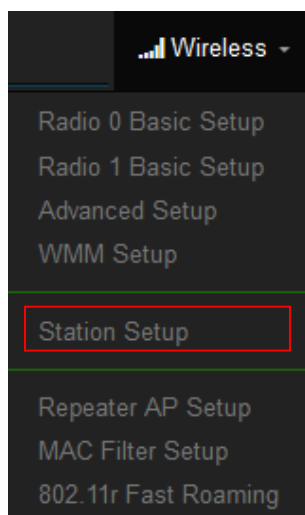
➤ **AIFS :** The Arbitration Inter-Frame Spacing Number specifies a wait time (in milliseconds) for data frames ◦

- **TxOP Limit** : Transmission Opportunity is an interval of time when a WME AP has the right to initiate transmissions onto the wireless medium (WM). This value specifies (in milliseconds) the Transmission Opportunity (TXOP) for AP; that is, the interval of time when the WMM AP has the right to initiate transmissions on the wireless network. ◦
- **ACM bit** : Admission Control Mandatory, ACM only takes effect on AC\_VI and AC\_VO. When you do not click Checkbox, it means that the ACM is controlled by the connecting AP. If you click Checkbox, it means that the Client is in charge ◦
- **No ACK policy bit** : Acknowledgment Policy, WMM defines two ACK policies: **Normal ACK** and **No ACK**. Click “**Checkbox**” indicates “**No ACK**”  
 When the no acknowledgement (No ACK) policy is used, the recipient does not acknowledge received packets during wireless packet exchange. This policy is suitable in the environment where communication quality is fine and interference is weak.  
 While the No ACK policy helps improve transmission efficiency, it can cause increased packet loss when communication quality deteriorates. This is because when this policy is used, a sender does not retransmit packets that have not been received by the recipient.  
 When the Normal ACK policy is used, the recipient acknowledges each received unicast packet. ◦

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

## 6.4.5 Station Setup

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



**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 |
|---------|--------|-------|-------|----------------|-------|
| -       | -      | -     | -     | -              | -     |

Site Survey

Save Cancel

- **MAC Address List:** The function can discovery AP Station and select want to link the AP station, please click site survey button.

## Notice

If want to discovery 2.4G station then administrator need to enable station mode in Radio 0 (2.4G) function page (reference manual 6.4.1 “Radio 0 Basic Setup”). Same practice if want to discovery 5G station will need to enable station mode in Radio 1(5G) function page (reference manual 6.4.2 “Radio 1(5G) Basic Setup”).

Station Mode ☒ Enable ☐ Disable

- **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.

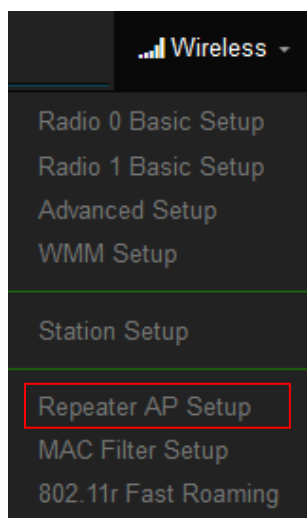
## Notice

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.

## 6.4.6 Repeater AP Setup

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



### Notice

1. If want to use Repeater AP function then Client 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.
  3. When Client Bridge used 2.4G to connection station then Repeater AP function only used the other 5G Wi-Fi. Same practice If Client Bridge used Radio 1(5G) then Repeater AP only used Radio 0 (2.4G) Wi-Fi.
- **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.

|                      |                     |
|----------------------|---------------------|
| <b>Security Type</b> | WPA/WPA2 Personal   |
|                      | Open System         |
|                      | WPA/WPA2 Personal   |
|                      | WPA/WPA2 Enterprise |

- **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.

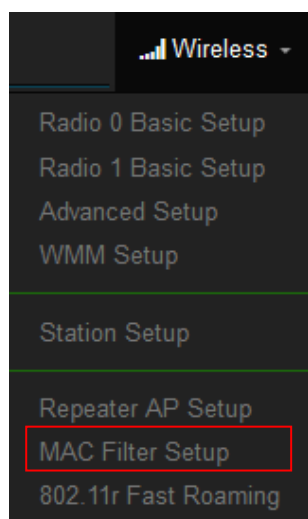
**TKIP** is short for “**Temporal Key Integrity Protocol**”, TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with.

- ✓ **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.

## 6.4.7 MAC Filter Setup

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



A screenshot of the 'MAC Rules' configuration page. It includes a 'Rule' dropdown menu set to 'Disable' with a 'Save' button. Below this is an 'Add MAC Address' section with a text input field and an 'Add' button. At the bottom is a 'MAC Address List' table with columns for #, MAC Address, and Action.

| # | 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.

A screenshot of the 'MAC Rules' configuration page with the 'Rule' dropdown menu open. The dropdown options are: Disable, Only Deny List MAC, and Only Allow List MAC. The 'Save' button is visible to the right of the dropdown.

- **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.

## 6.4.8 802.11r Fast Roaming Setup

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

The screenshot displays the CERIO web interface. At the top, a 'Wireless' dropdown menu is open, showing options: Radio 0 Basic Setup, Radio 1 Basic Setup, Advanced Setup, WMM Setup, Station Setup, Repeater AP Setup, MAC Filter Setup, and 802.11r Fast Roaming (which is highlighted with a red box). Below this, the 'Fast Roaming Settings' page is shown with the following fields:

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

- **Mobility Domain:** MDID is used to indicate a group of APs (within an ESS, i.e., sharing the same SSID) between which a STA can use Fast BSS Transition.

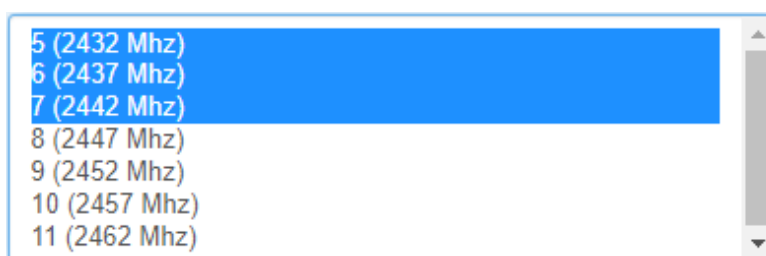
## Notice

Please enter 2-octet identifier as a hex string.

- **R0 Key Lifetime:** Default lifetime of the PMK-R0 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.



- **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.

## 7. WISP Mode

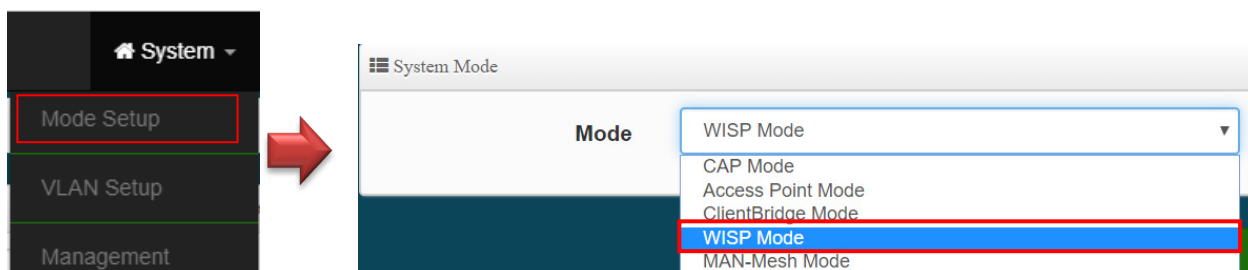
WISP Mode is a router function, if the Telecom company permits wireless connection to their WAN, administrators can change the CenOS 5.0 AP to WISP Mode to connect to the wifi network. The WISP Mode support PPPoE / Static IP / Dynamic IP and PPTP for WAN, and support Repeater AP function.

### Notice

Relevant to Dual Band Devices Only: If wireless WAN used 2.4G radio connection to Telecom company station, the Repeater AP radio only used 5G radio. So wireless WAN used 5G radio connection to Telecom company station, the Repeater AP radio only used 2.4G radio.

### 7.1 Change Setup mode

If the administrator needs to switch to WISP mode, Please click "System"-> " Mode Setup " to change WISP mode.

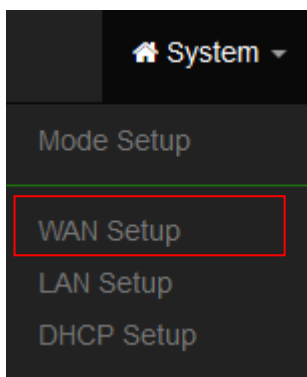


### Notice

Please note that the LAN IP addresses in each mode are different from each other and will not continue. For the first time after switching modes, always perform access management on the LAN default IP address of 192.168.2.254

### 7.2 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.

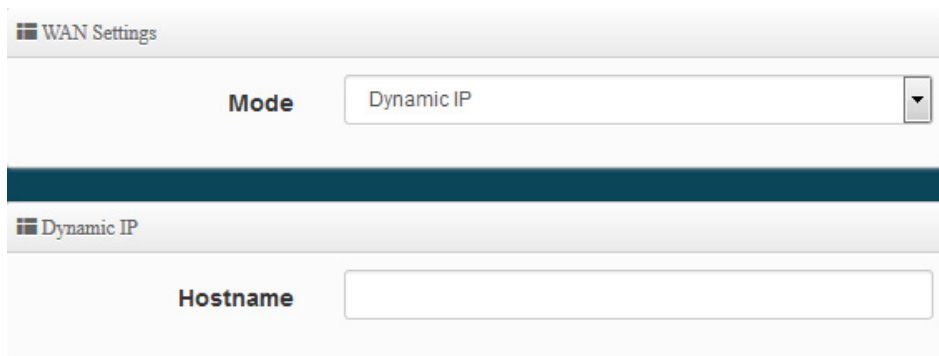


Two side-by-side configuration panels from the Cerio web interface. The left panel is titled 'WAN Settings' and shows the 'Mode' set to 'Static IP'. Below this, under a 'Static IP' sub-header, are input fields for 'IP Address', 'Netmask', and 'Gateway'. The right panel is titled 'MAC Clone' and shows the 'Mode' set to 'Default MAC Address'. Below this, under a 'DNS' sub-header, are input fields for 'Primary DNS' (containing '8.8.8.8') and 'Secondary DNS'. At the bottom of the right panel, under a 'NAT' sub-header, are radio buttons for 'Enable' (selected) and 'Disable'.

## WAN Setting

A close-up screenshot of the 'Mode' dropdown menu in the 'WAN Settings' panel. The dropdown is open, showing four options: 'Static IP' (highlighted in blue), 'Dynamic IP', 'PPPoE', and 'PPTP'.

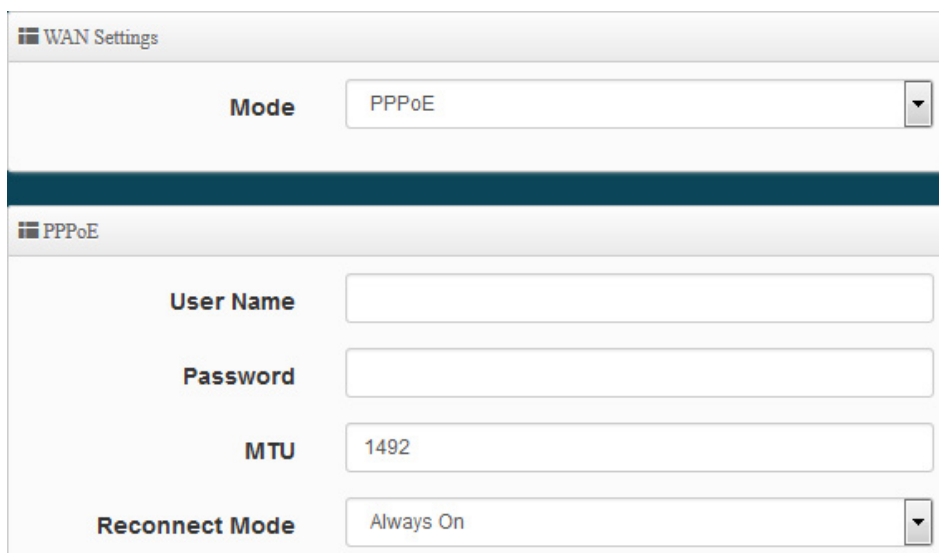
- **Static IP:** Users can manually setup the WAN IP address with a static IP provided by WISP.
  - **IP Address:** The IP address of the WAN port.
  - **IP Netmask:** The Subnet mask of the WAN port.
  - **IP Gateway:** The default gateway of the WAN port.
- **Dynamic IP:** Please consult with WISP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



The screenshot shows the 'WAN Settings' window. The 'Mode' dropdown menu is set to 'Dynamic IP'. Below this, the 'Dynamic IP' section is active, showing a 'Hostname' text input field.

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

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



The screenshot shows the 'WAN Settings' window with 'Mode' set to 'PPPoE'. The 'PPPoE' section is active, displaying fields for 'User Name', 'Password', 'MTU' (set to 1492), and 'Reconnect Mode' (set to 'Always On').

- **User Name** : Enter User Name for PPPoE connection
  - **Password** : Enter Password for PPPoE connection
  - **MTU**: By default, MTU is set to **1492** bytes. MTU stands for Maximum Transmission Unit. Consult with WISP for a correct MTU setting.
  - **Reconnect Mode**: Administrator can select three function for Always On / On Demand / Manual.
    - ✓ **Always on** – A connection to Internet is always maintained.
    - ✓ **On Demand** – A connection to Internet is made as needed.
    - ✓ **Manual** – Click the “**Connect**” button on “**WAN Information**” in the Overview page to connect to the Internet.
- **PPTP**: The Point-to-Point Tunneling Protocol (PPTP) mode enables the implementation of secure multi-protocol Virtual Private Networks (VPNs) through public networks.



The screenshot shows the 'WAN Settings' window with the 'Mode' dropdown set to 'PPTP'. Below this, the 'PPTP' configuration section includes fields for 'User Name', 'Password', 'PPTP Server IP', 'WAN IP', 'Netmask', and 'MTU' (set to 1460). There are also radio button options for 'MPPE40' and 'MPPE128', both with 'Enable' and 'Disable' choices. The 'Reconnect Mode' dropdown is set to 'Always On'.

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

## 7.3 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.

System

Mode Setup

WAN Setup

**LAN Setup**

DHCP Setup

|   |  |   |  |
|---|--|---|--|
| <b>Ethernet Connection Type</b><br>Mode <input checked="" type="radio"/> Static IP <input type="radio"/> Dynamic IP   |  | <b>DNS</b><br>Primary DNS <input type="text"/><br>Secondary DNS <input type="text"/>                                      |  |
| <b>Static IP</b><br>IP Address <input type="text" value="192.168.2.254"/><br>Netmask <input type="text" value="255.255.255.0"/><br>Gateway <input type="text" value="192.168.2.1"/> |  | <b>802.1d Spanning Tree</b><br>802.1d Spanning Tree <input type="radio"/> Enable <input checked="" type="radio"/> Disable |  |
|   |  | <b>DHCP Forward</b><br>DHCP Forward <input type="radio"/> Enable <input checked="" type="radio"/> Disable                 |  |

- **Mode:** Administrator can select the IP used Static or Dynamic IP address.
  - Static IP : A set of fixed IP addresses can be manually set for the system to use.
  - Dynamic IP : If there is a DHCP server on the top, you can use the dynamic IP address to let the system obtain a set of IP automatically.

## Notice

That when using a dynamic IP, the system will automatically obtain the IP address sent by DHCP, and the obtained IP address will be obtained after the operation is confirmed by the upper DHCP server. Obtaining the IP address is not fixed. For system management, the upper DHCP server must query the IP address obtained by the current system.

## ➤ Static IP:

|                  |  |
|------------------|--|
| <b>Static IP</b> |  |
| IP Address       | <input type="text" value="192.168.2.254"/> |
| Netmask          | <input type="text" value="255.255.255.0"/> |
| Gateway          | <input type="text" value="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 :

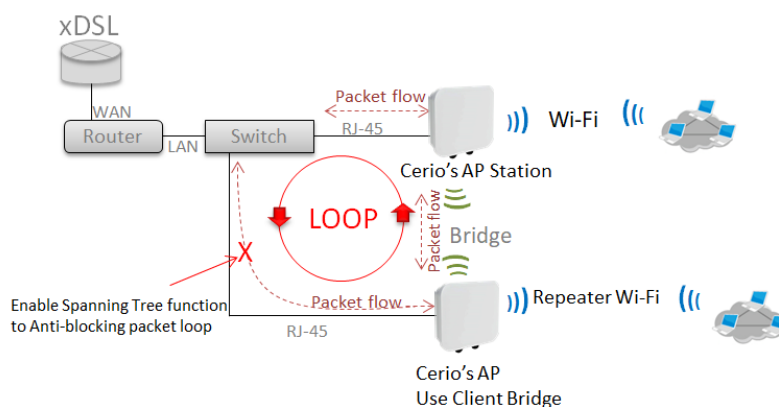
**802.1d Spanning Tree**

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.

## 7.4 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.

The screenshot displays the CERIO web interface for configuring DHCP. On the left, a sidebar menu under 'System' includes 'Mode Setup', 'WAN Setup', 'LAN Setup', and 'DHCP Setup' (which is highlighted with a red box). The main content area shows the 'DHCP Service' configuration. The 'Mode' is set to 'Enable' (indicated by a selected radio button). Below this, the 'DHCP Setup' form contains the following fields:

- 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:** (empty field)
- WINS IP:** (empty field)
- Domain:** (empty field)
- 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 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 |   |
|-----------------------|---|
| <b>Comment</b>        | <input type="text"/>                                    |
| <b>IP Address</b>     | <input type="text"/>                                    |
| <b>MAC Address</b>    | <input type="text"/> <input type="button" value="Add"/> |

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

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

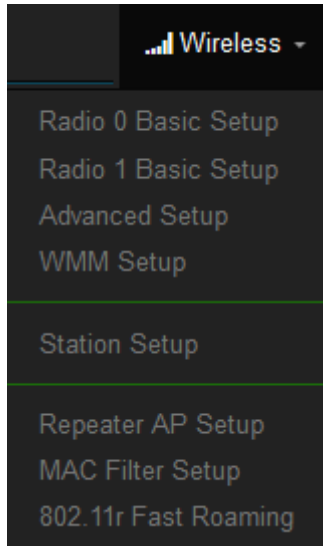
| Static Lease IP List |         |            |             |        |
|----------------------|---------|------------|-------------|--------|
| #                    | Comment | IP Address | MAC Address | Action |
| -                    | -       | -          | -           | -      |

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



## 7.5 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.

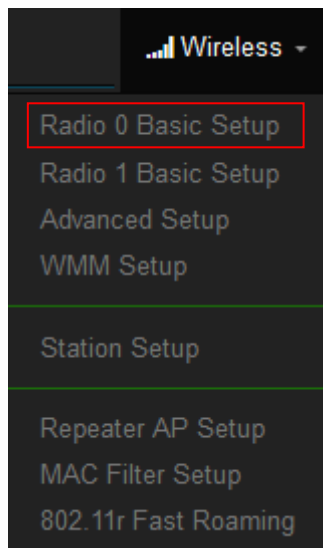


### Notice

When the upper limit of the 2.4G frequency is used, the repeater AP will only be able to use the other two 5G extension Repeater AP APs. If the upper end AP with a Radio 1 (5G) frequency is used, the repeater AP will only Use 2.4G as the extension Repeater AP base.

### 7.5.1 Radio 0 (2.4G) Basic Setup

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



| General Setup |   |
|---------------|---|
| MAC Address   | 8c:4d:ea:05:1c:75   |
| Station Mode  | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| Country       | Taiwan  |
| Band Mode     | 802.11b/g/n   |
| Tx Power      | Level 9   |
| Slot Time     | 9 <span>Distance</span>   |
| ACK Timeout   | 64  |

- **Station Mode:** If Client Bridge want to use 2.4G link to Access Point then administrator can enable the function (radio 0).
- **Country:** Administrator can select country used channel by US and EU.
- **Band Mode:** Select an appropriate wireless band; bands available are **801.11 b/g/n mixed mode**.

- **Tx Power:** Administrator can adjust the output power of the system to get the appropriate coverage for your wireless network. Specify digit numbers between level **1** to level 9 (the unit is %) for your environment. If you are not sure which setting to choose, then keep the default setting level 9 (**100%**).
- **Slot Timeout :** 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 Timeout :** 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

20/40

MCS

Auto

Short GI

☒ Enable
 ☐ Disable

Aggregation

☒ Enable
 ☐ Disable

Aggregation Frames

32

Aggregation Size

50000

- **TX/RX Stream:** Build in 2.4GHz 2 antennas and support 2TX/2RX streams. Administrator can select 1 or 2 TX/RX. The default is 2TX/2RX.

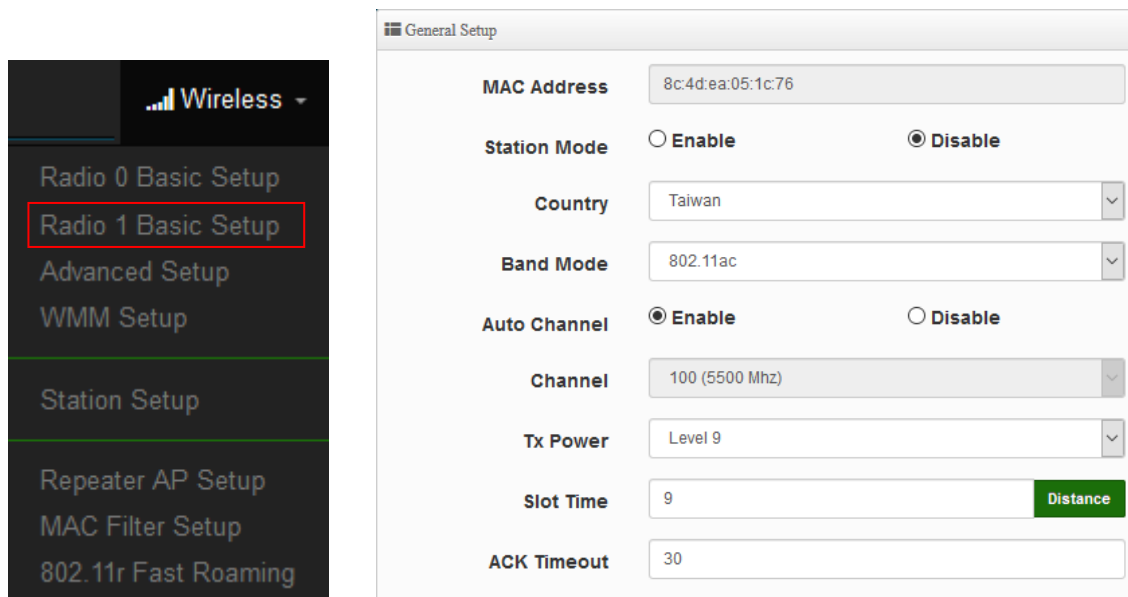
## Notice

This product has a built-in 2x2 (2T2R) antenna for 2.4Ghz, which has been matched with the default setting of 2T2R. If there is no special demand, please keep this default setting .

- **Channel Bandwidth:** The "20/40" MHz option is usually best. The other option is available for special circumstances.
- **MCS:** This parameter represents transmission rate. By default (Auto) the fastest possible transmission rate will be selected. You have the option of selecting the speed if necessary.
- **Shout GI:** Short Guard Interval, by default, it's "Enable". it's can increase throughput. However, it can also increase error rate in some installations, due to increased sensitivity to radio-frequency reflections. Select the option that works best for your installation.
- **Aggregation:** By default, it's "Enable". To "Disable" to deactivated Aggregation.  
A part of the 802.11n standard(or draft-standard). It allows sending multiple frames per single access to the medium by combining frames together into one larger frame.  
It creates the larger frame by combining smaller frames with the same physical source and destination end points and traffic class (i.e. QoS) into one large frame with a common MAC header.
- **Aggregation Frames:** 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.

## 7.5.2 Radio 1 (5G) Basic Setup



The screenshot shows the Cerio configuration interface. On the left is a sidebar menu with the following items: Wireless (with a signal icon), Radio 0 Basic Setup, Radio 1 Basic Setup (highlighted with a red box), Advanced Setup, WMM Setup, Station Setup, Repeater AP Setup, MAC Filter Setup, and 802.11r Fast Roaming. The main area displays the 'General Setup' form for Radio 1. The form contains the following fields and options:

- MAC Address:** 8c:4d:ea:05:1c:76
- Station Mode:** Radio buttons for ☐ Enable and ☒ Disable
- Country:** Taiwan (dropdown menu)
- Band Mode:** 802.11ac (dropdown menu)
- Auto Channel:** Radio buttons for ☒ Enable and ☐ Disable
- Channel:** 100 (5500 Mhz) (dropdown menu)
- Tx Power:** Level 9 (dropdown menu)
- Slot Time:** 9 (text input) with a green 'Distance' button
- ACK Timeout:** 30 (text input)

- **MAC Address:** Display Radio 1(5G) used 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(5G).

- **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 Timeout :** 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 Timeout :** 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

80

BandWidth

Min MCS

4

Max MCS

9

Short GI

☒ Enable
 ☐ Disable

Aggregation

☒ Enable
 ☐ Disable

Aggregation Frames

32

Aggregation Size

50000

- **TX/RX Stream:** supporting 2TX/2RX streams. Administrator can select 1 or 2 TX/RX. The default is 2TX/2RX.

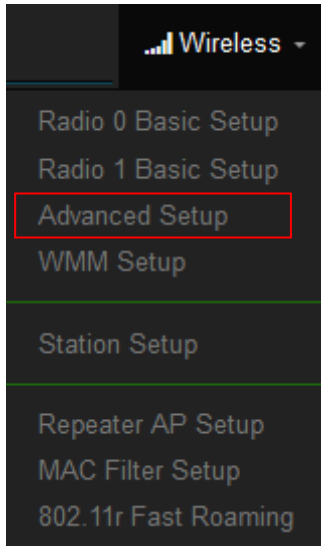
## Notice

This product has a built-in 2x2 (2T2R) antenna for 5Ghz, which has been matched with the default setting of 2T2R. If there is no special demand, please keep this default setting .

- **Channel Bandwidth:** The "20/40 and 802.11ac 80" MHz option is usually best. The other option is available for special circumstances.
- **MIN MCS:** This parameter represents transmission rate. By default (4) the fastest possible transmission rate will be selected. You have the option of selecting the speed if necessary.
- **MAX MCS:** This parameter represents transmission rate. By default (9) the fastest possible transmission rate will be selected. You have the option of selecting the speed if necessary.
- **Shout GI:** Short Guard Interval, by default, it's "Enable". it's can increase throughput. However, it can also increase error rate in some installations, due to increased sensitivity to radio-frequency reflections. Select the option that works best for your installation.
- **Aggregation:** By default, it's "Enable". To "Disable" to deactivated Aggregation.  
A part of the 802.11n standard(or draft-standard). It allows sending multiple frames per single access to the medium by combining frames together into one larger frame. It creates the larger frame by combining smaller frames with the same physical source and destination end points and traffic class (i.e. QoS) into one large frame with a common MAC header.
- **Aggregation Frames:** 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.

## 7.5.3 Advanced Setup



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

- Beacon Interval:** 100
- DTIM Interval:** 1
- Fragment Threshold:** 2346
- RTS Threshold:** 2346
- Short Preamble:** ☒ Enable ☐ Disable
- IGMP Snooping:** ☒ Enable ☐ Disable
- Greenfield:** ☒ Enable ☐ Disable
- RF on/off by Schedule:** Always (dropdown menu)
- 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 result 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.

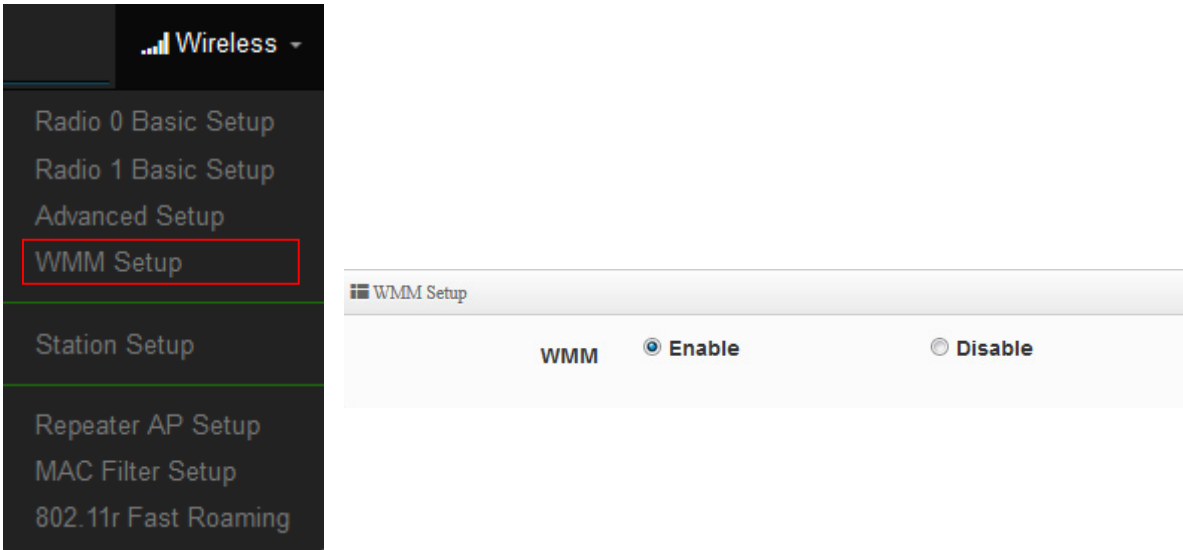
- **RTS Threshold:** RTS Threshold is in the range of **1~2347** byte. The default is **2347** byte. The main purpose of enabling RTS by changing RTS threshold is to reduce possible collisions due to hidden wireless clients. RTS in AP will be enabled automatically if the packet size is larger than the 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=8c:4d:ea:05:1c:7a rssi=67
Jan 1 08:27:00 Wifilogd: tm=1420072020 vlan=0 radio=0 bssid=8c:4d:ea:05:1c:7a climac=8c:4d:ea:05:1c:7a rssi=68
Jan 1 08:26:00 Wifilogd: tm=1420071960 vlan=0 radio=0 bssid=8c:4d:ea:05:1c:7a climac=8c:4d:ea:05:1c:7a rssi=67
```

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

**7.5.4 WMM Setup**

This affects traffic flowing from the access point to the client station. Configuring QoS options consists of setting parameters on existing queues for different types of wireless traffic. You can configure different minimum and maximum wait times for the transmission of packets in each queue based on the requirements of the media being sent. Queues automatically provide minimum transmission delay for Voice, Video, multimedia, and mission critical applications, and rely on best-effort parameters for traditional IP data.



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

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

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

➤ **AC Type :**

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

➤ **CWmin :**

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

➤ **CWmax :** Maximum Contention Window. The value specified here in the Maximum Contention Window is the upper limit (in milliseconds) for the doubling of the random backoff value. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached. Once the Maximum Contention Window size is reached, retries will continue until a maximum number of retries allowed is reached. Valid values for the "cwmax" are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024. The value for "cwmax" must be higher than the value for "cwmin". ◦

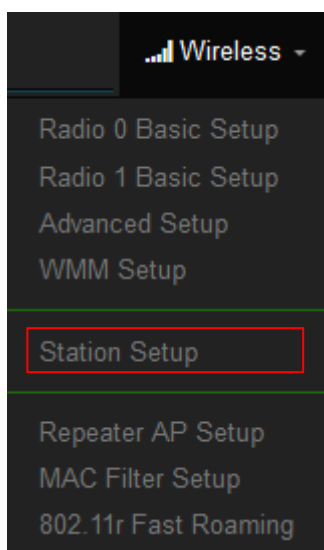
➤ **AIFS :** The Arbitration Inter-Frame Spacing Number specifies a wait time (in milliseconds) for data frames ◦

- **TxOP Limit** : Transmission Opportunity is an interval of time when a WME AP has the right to initiate transmissions onto the wireless medium (WM). This value specifies (in milliseconds) the Transmission Opportunity (TXOP) for AP; that is, the interval of time when the WMM AP has the right to initiate transmissions on the wireless network. ◦
- **ACM bit** : Admission Control Mandatory, ACM only takes effect on AC\_VI and AC\_VO. When you do not click Checkbox, it means that the ACM is controlled by the connecting AP. If you click Checkbox, it means that the Client is in charge ◦
- **No ACK policy bit** : Acknowledgment Policy, WMM defines two ACK policies: **Normal ACK** and **No ACK**. Click “**Checkbox**” indicates “**No ACK**”  
 When the no acknowledgement (No ACK) policy is used, the recipient does not acknowledge received packets during wireless packet exchange. This policy is suitable in the environment where communication quality is fine and interference is weak.  
 While the No ACK policy helps improve transmission efficiency, it can cause increased packet loss when communication quality deteriorates. This is because when this policy is used, a sender does not retransmit packets that have not been received by the recipient.  
 When the Normal ACK policy is used, the recipient acknowledges each received unicast packet. ◦

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

## 7.5.5 Station Setup

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



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

.....

Save

Cancel

MAC Address List

Site Survey

| 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.

## Notice

If want to discovery 2.4G station then administrator need to enable station mode in Radio 0 (2.4G) function page (reference manual 7.5.1 “Radio 0 Basic Setup”). Same practice if want to discovery 5G station will need to enable station mode in Radio 1(5G) function page (reference manual 7.5.2 “Radio 1(5G) Basic Setup”).

Station Mode    ☒ Enable    ☐ Disable

- **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.

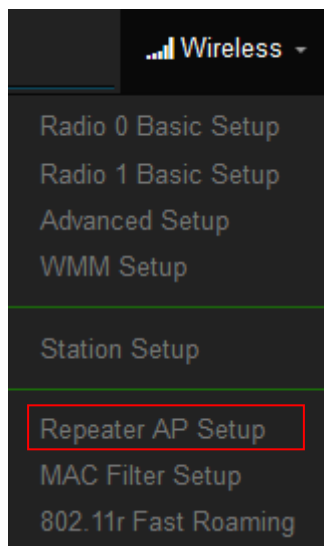
## Notice

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.

## 7.5.6 Repeater AP Setup

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



### Notice

1. If want to use Repeater AP function then Client 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.
3. When Client Bridge used 2.4G to connection station then Repeater AP function only used the other 5G Wi-Fi. Same practice If Client Bridge used Radio 1(5G) then Repeater AP only used Radio 0 (2.4G) Wi-Fi.

- 
- 
- **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.



|                      |                     |   |
|----------------------|---------------------|---|
| <b>Security Type</b> | WPA/WPA2 Personal   | ▼ |
|                      | Open System         |   |
|                      | WPA/WPA2 Personal   |   |
|                      | WPA/WPA2 Enterprise |   |

- **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.

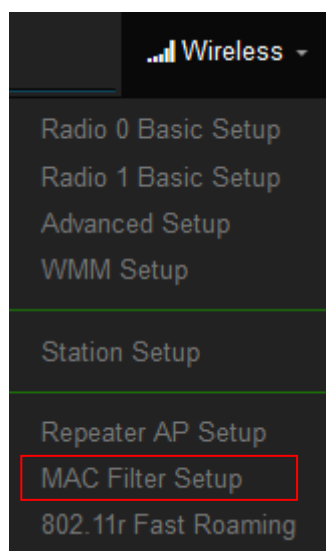
**TKIP** is short for “**Temporal Key Integrity Protocol**”, TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with.

- ✓ **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.

## 7.5.7 MAC Filter Setup

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



A screenshot of the 'MAC Rules' configuration page. It features a 'Rule' dropdown menu currently set to 'Disable' and a 'Save' button. Below this is an 'Add MAC Address' section with a text input field and an 'Add' button. At the bottom, there is a 'MAC Address List' table with columns for '#', 'MAC Address', and 'Action'. The table currently contains one row with dashes in all three columns.

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

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

A screenshot of the 'MAC Rules' configuration page, showing the 'Rule' dropdown menu open. The menu lists three options: 'Disable', 'Only Deny List MAC', and 'Only Allow List MAC'. The 'Only Allow List MAC' option is highlighted in blue. The 'Save' button is visible to the right of the dropdown.

- **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**”.

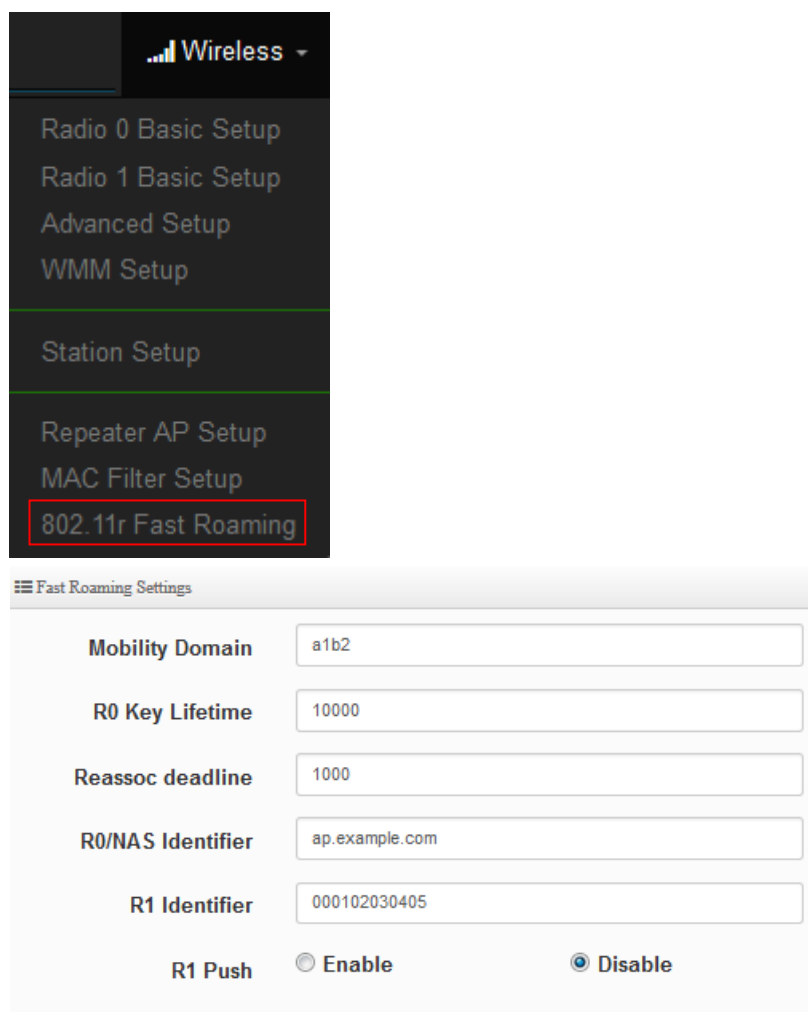
- **Only Deny List MAC:** Define certain wireless clients in the list which will have denied access to the Access Point while the access will be granted for all the remaining clients - Action Type is set to “**Only Deny List MAC**”.

- **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.

## 7.5.8 802.11r Fast Roaming Setup

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



The screenshot displays the CERIO web interface. At the top, a 'Wireless' menu is open, showing options like 'Radio 0 Basic Setup', 'Radio 1 Basic Setup', 'Advanced Setup', 'WMM Setup', 'Station Setup', 'Repeater AP Setup', 'MAC Filter Setup', and '802.11r Fast Roaming' (which is highlighted with a red box). Below this, the 'Fast Roaming Settings' page is shown with the following fields:

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

- **Mobility Domain:** MDID is used to indicate a group of APs (within an ESS, i.e., sharing the same SSID) between which a STA can use Fast BSS Transition.

## Notice

Please enter 2-octet identifier as a hex string.

- **R0 Key Lifetime:** Default lifetime of the PMK-R0 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.

- **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

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

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

### R1 Key Holder List:

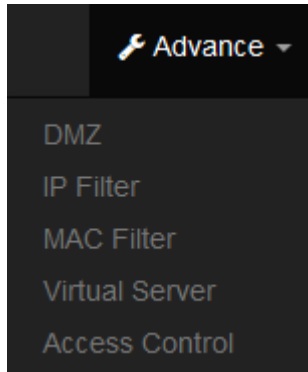
After setting "R1 Key holders" function the information will appear in list.

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

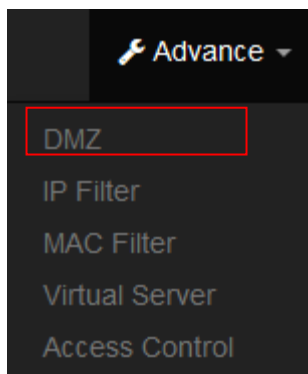
Click **"Save"** button to save your set function. Then click **"Reboot"** button to activate your changes.

## 7.6 Advanced Setup

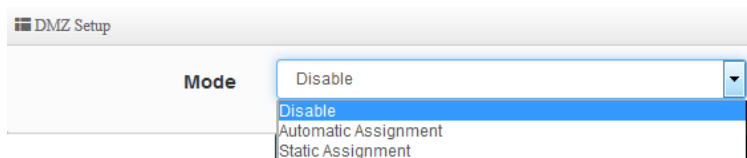
Administrator can set basic routing security functions, including DMZ / IP and MAC filtering / virtual servers and access control management (basic firewall rules) in Advance menu.



### 7.6.1 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.



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



- **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

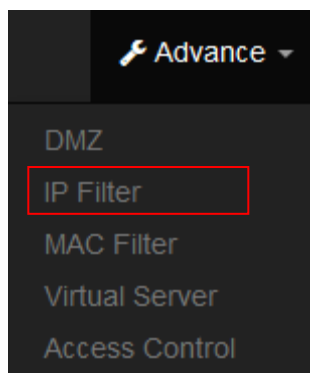
Internal IP Address

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.

## 7.6.2 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.

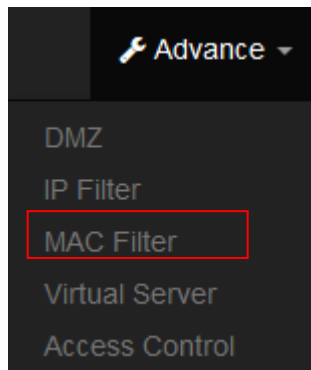
- **Active:** Administrator can select Enable or Disable the service.
- **Comment:** Enter the description of IP filter rule.
- **Policy:** Administrator can select the IP flow rule of Deny or Pass.
- **In/ Out:** Administrator can select the IP flow rule of In/out bound.
- **Protocol:** Set used service 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.

## 7.6.3 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.

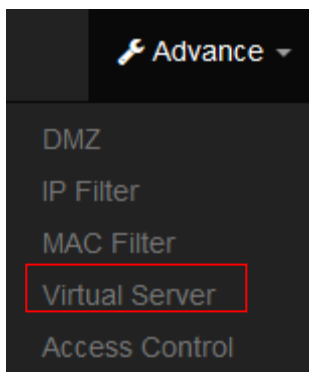
The screenshot shows the 'MAC Filter Rules' configuration page. At the top, there's a 'Mode' dropdown menu with options: Disable, Deny, and Allow. Below this is the 'MAC Filter List' table.

| # | Active                   | Comment | MAC Address | Policy     |
|---|--------------------------|---------|-------------|------------|
| 1 | <input type="checkbox"/> |         |             | Always Run |
| 2 | <input type="checkbox"/> |         |             | Always Run |
| 3 | <input type="checkbox"/> |         |             | Always Run |
| 4 | <input type="checkbox"/> |         |             | Always Run |
| 5 | <input type="checkbox"/> |         |             | 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.

## 7.6.4 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.

| # | 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.

## 7.6.5 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**

Active ☒ Enable ☐ Disable

Comment:

Protocol:

Schedule:

**MAC Address Setup**

MAC Address:

**MAC Address List**

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

**IP Address Setup**

Local IP Address:  -

Local Port:

Destination IP Address:  -

Destination Port:

## # Access control rules :

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

**Protocol**

ANY

TCP

UDP

ICMP

Content Filter

Application

Domain Filter

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

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



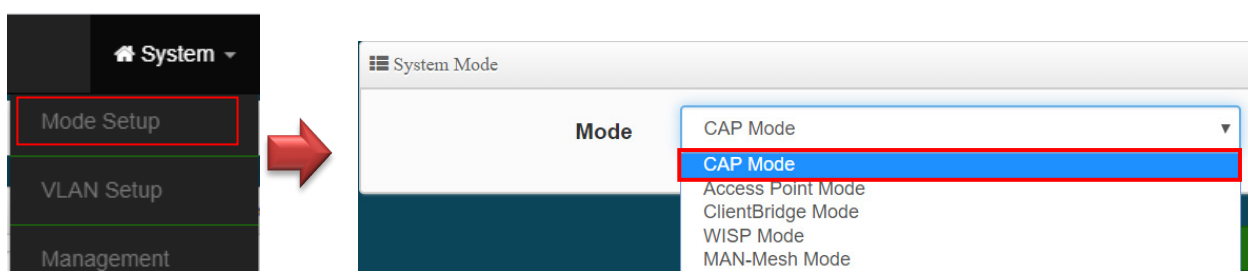
## 8. CAP Mode

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

### 8.1 Change Setup mode

If the administrator needs to switch to CAP mode, Please click "System"-> " Mode Setup " to change CAP mode.

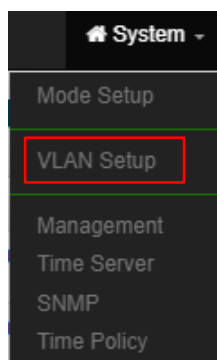


#### Notice

Please note that the LAN IP addresses in each mode are different from each other and will not continue. For the first time after switching modes, always perform access management on the LAN default IP address of 192.168.2.254

### 8.2 VLAN Setup

Start by setting the AP's (LAN) IP address, Please Click " System " → " VLAN Setup "



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

#### Notice

This VLANs support max 16 IEEE 802.1q tag VLANs.

| VLAN List |        |             |                 |               |         |
|-----------|--------|-------------|-----------------|---------------|---------|
| #         | Status | Flag        | IP Address      | Netmask       | Action  |
| 0         | On     | Native ETH0 | 192.168.101.48  | 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 |
| 8         | Off    | ETH0.108    | 192.168.108.254 | 255.255.255.0 | Network |
| 9         | Off    | ETH0.109    | 192.168.109.254 | 255.255.255.0 | Network |
| 10        | Off    | ETH0.110    | 192.168.110.254 | 255.255.255.0 | Network |
| 11        | Off    | ETH0.111    | 192.168.111.254 | 255.255.255.0 | Network |
| 12        | Off    | ETH0.112    | 192.168.112.254 | 255.255.255.0 | Network |
| 13        | Off    | ETH0.113    | 192.168.113.254 | 255.255.255.0 | Network |
| 14        | Off    | ETH0.114    | 192.168.114.254 | 255.255.255.0 | Network |
| 15        | Off    | ETH0.115    | 192.168.115.254 | 255.255.255.0 | Network |

- # : 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 0(2.4) or Radio 1(5G) on/off、Spanning tree、IAPP and VLAN tag.

✕ Enter the "Network" setting page as follows

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

**VLAN Setup**

**VLAN Mode**
☒ Enable
 ☐ Disable

**IP Setup**

**IP Address**

**Netmask**

**Save**

**Management**

**802.1d Spanning Tree**
☐ Enable
 ☒ Disable

**ETH0 VLAN Tag Setup**

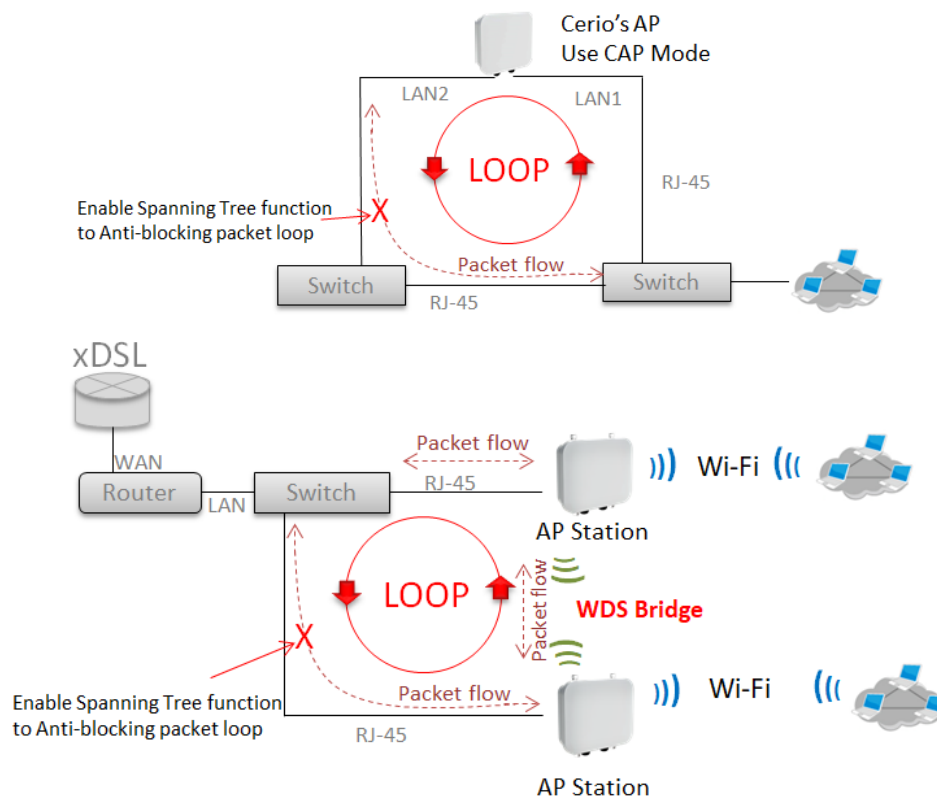
**VLAN TAG**

**Cancel**

## 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.

The screenshot shows the configuration interface for the Gateway and DNS settings. The "Gateway" section has a "Default Gateway" field set to "192.168.2.1". The "DNS" section has a "DNS1" field set to "192.168.2.1" and an empty "DNS2" field. At the bottom, there are "Save" and "Cancel" buttons.

- **Gateway**: The default Gateway IP Address is 192.168.2.1, Please check your Gateway IP and change.

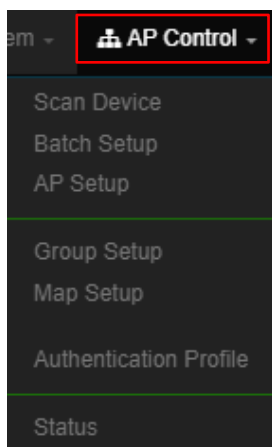
- **DNS:** Check either “No Default DNS Server” or “Specify DNS Server IP” button as desired to set up the system DNS.
  - ✓ **Primary:** The IP address of the primary DNS server.
  - ✓ **Secondary:** The IP address of the secondary DNS server.

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

## 8.3 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

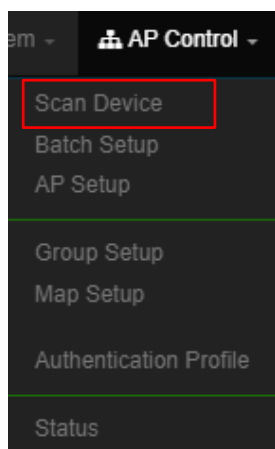


### # Centralized Management APs operating Instructions:

- 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.

#### 8.3.1 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.



The 'Filter Device' window contains the following fields:
 

- VLAN#**: A dropdown menu showing 'VLAN 0 (192.168.2.0/24)'.
- Default Password**: A text input field filled with ten dots.
- Sort**: A dropdown menu showing 'IP Address'.
- A green **Scan** button is located to the right of the Sort dropdown.

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

Scan Result

Default

Import

| # | Device                            | IP Address    | MAC Address       | Password | Host Name    | F/W Version        | F/W Date            | IP Address    | Netmask       | Action                                |
|---|-----------------------------------|---------------|-------------------|----------|--------------|--------------------|---------------------|---------------|---------------|---------------------------------------|
| 1 | <div><div></div><div></div></div> | 192.168.2.253 | 8c-4d-ea-04-d0-6e | *****    | CW-400NAC-E1 | Pme-CPE-ACS V1.1.0 | 2016/05/06 09:19:35 | 192.168.2.253 | 255.255.255.0 | <div><div>Info</div><div></div></div> |

- **#** : 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.

The 'Update IP Address & Netmask' window contains the following fields:
 

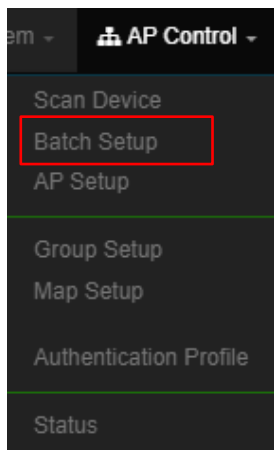
- Control Port**: A dropdown menu showing 'VLAN 0 (192.168.2.0/24)'.
- VLAN TAG**: A checkbox followed by a text input field containing '1-4096'.
- IP Address**: A text input field containing '192.168.2.10'.
- Netmask**: A text input field containing '255.255.255.0'.
- A green **Apply&Reboot** button is located to the right of the Netmask field.

- **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.

## 8.3.2 Batch Setup



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

The image shows a 'VLAN List' configuration window with three dropdown menus:
 

- VLAN**: VLAN 0 (192.168.2.0/24)
- Group**: None
- Batch Setup**: VLAN Setup

- **LAN** : When VLAN Tag function is enabled (**please refer to Manual 5.2 Access Point System VLAN Setup**), administrator can change VLAN tag for managed APs.
- **Group** : When AP Groups are created (**please refer to Manual 8.3.4 Group setup**), Administrators can select and change group settings of managed APs.
- **Batch Setup** : Administrator can centralize setting changes for managed APs.

The image shows the 'Batch Setup' dropdown menu. The 'VLAN Setup' option is selected and highlighted in blue. Other options in the list include: Authentication Profile, Gateway & DNS, Time Server, Management Setup, Wireless Basic Setup, Wireless Advanced Setup, VAP Setup, Upgrade Via TFTP Server, Upgrade Via HTTP URL, and Reboot.



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

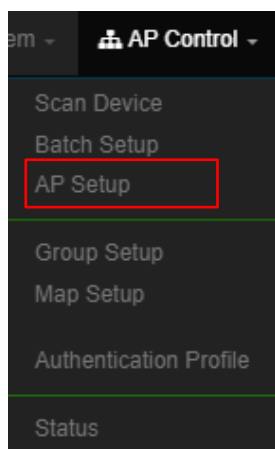
- ✓ **VLAN** : The function can select VLAN (please refer to 5.2 Configure Access Point VLAN Setup) for managed Aps.
- ✓ **VLAN Mode** : Administrator can enable or disable VLAN mode of the managed APs.
- ✓ **Access Point 0** : Administrator can enable or disable 2.4G radio 0 of the managed APs.
- ✓ **Access Point 1** : Administrator can enable or disable 5G radio 1 of the managed APs.
- ✓ **802.1d Spanning Tree** : Administrator can enable or disable the function.( please refer to 5.2 Configure Network → 802.1d Spanning Tree)
- ✓ **Control Port** : The function administrator can enable or disable of the managed APs (please refer to 5.2 Configure Network → Control Port)
- ✓ **IAPP** : The function administrator can enable or disable of the managed APs (Please refer to 5.2 Configure Network → IAPP)

The screenshot displays three configuration sections in the CERIO web interface:

- IP Setup:** Contains fields for 'Apply' (radio buttons for Enable and Disable), 'IP Mode' (radio buttons for Enable and Disable), 'IP Address' (text box with value 192.168.2.10), and 'Netmask' (text box with value 255.255.255.0).
- ETH0 VLAN Tag Setup:** Contains a radio button for 'ETH0' (Enable/Disable) and a 'VLAN TAG' section with a checkbox and a text box containing '1-4096'.
- ETH1 VLAN Tag Setup:** Contains a radio button for 'ETH1' (Enable/Disable) and a 'VLAN TAG' section with a checkbox and a text box containing '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: “8.3.6 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 3.2 Configure Time Server)
- **Management Setup:** Setting system name/ system login port and system log server service for managed APs. (Please refer to 3.1 system management)
- **Wireless Batch Setup:** Setting Wi-Fi configurations for managed APs. (Please refer to 5.6 Wireless Basic Setup)
- **Wireless Advanced Setup:** Setting Wi-Fi Advanced settings for managed APs. (Please refer to 5.6.3 Wireless Advanced Setup)
- **VAP Setup** : Wi-Fi SSID / channel or security settings for managed APs. (Please refer to 5.2.3 Configure Radio 0/1)
- **Upgrade via TFTP Server:** Administrator can centrally upgrade firmware via TFTP Server for the managed APs.
- **Upgrade via HTTP Server:** Administrator can centrally upgrade firmware via HTTP Server for the managed APs.
- **Reboot:** Administrator can reboot managed APs.

## 8.3.3 AP Setup



Administrator can monitor statuses and modify managed APs information.

VLAN List

VLAN

All

Device List

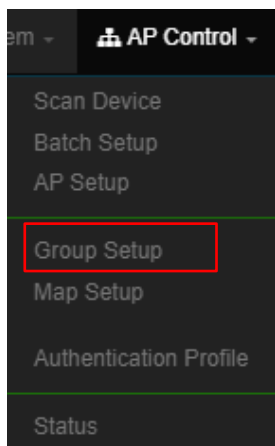
Choice AllDeleteRefresh

| VLAN# | Device                   | Status | System Name  | IP Address    | MAC Address       | Uptime   | Action           |
|-------|--------------------------|--------|--------------|---------------|-------------------|----------|------------------|
| VLAN0 | <input type="checkbox"/> |        | CW-400NAG-E1 | 192.168.2.253 | 8c:4d:ea:04:d0:6e | 03:43:28 | <div>Setup</div> |

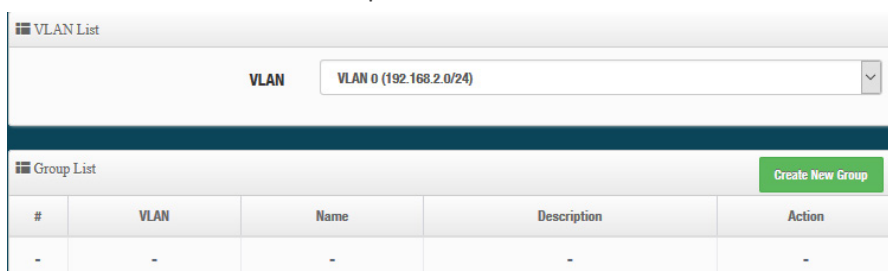
- **VLAN** : Select desired VLAN for AP setup
- **Setup** : Administrator can modify IP addresses, system login passwords, and web login port for managed APs. If administrator has change AP devices, administrator can modify MAC address of the new managed AP.

| Device Setup |                         |
|--------------|-------------------------|
| VLAN         | VLAN 0 (192.168.2.0/24) |
| Group        | None                    |
| IP Address   | 192.168.2.253           |
| MAG Address  | 8c:4d:ea:d0:6e          |
| Password     | *****                   |
| HTTP Port    | 80                      |

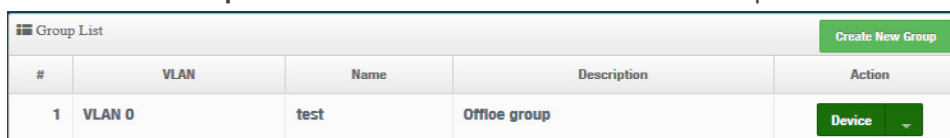
## 8.3.4 Group Setup



Administrator can create Groups within the same VLAN.

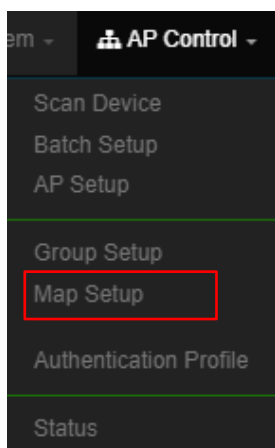


- **VLAN** : Select VLAN.
- **Create New Group** : Click the button to create a new AP Group



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

## 8.3.5 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 |         |                         | Create New Map |
|----------|---------|-------------------------|----------------|
| #        | Name    | Description             | Action         |
| 1        | 1F_plan | Location Map for man... | View           |

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

Map Setting

Map Name

Image URL

Description

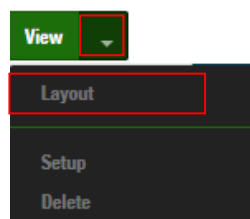
Image

View

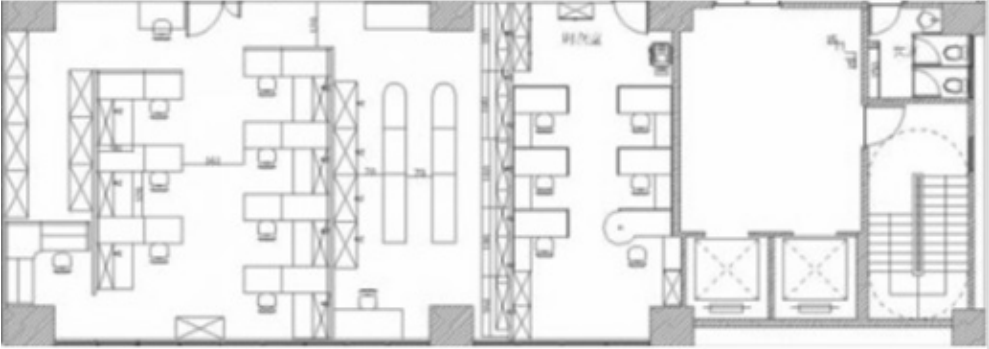
- **Map Name** : Enter map name.
- **Image URL** : Paste Map image url
- **Description** : Enter the description for the map.

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.



192.168.2.253



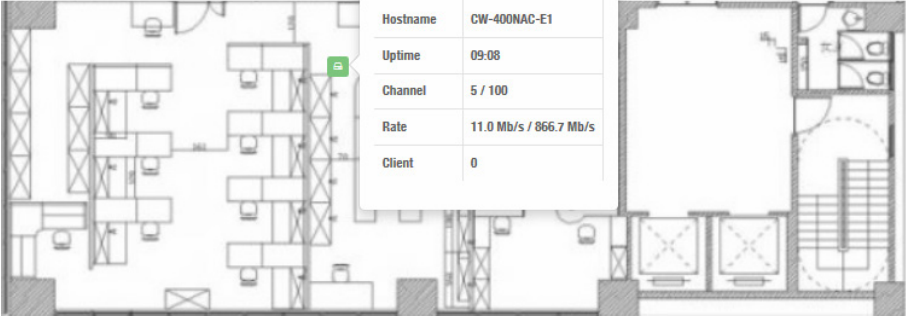
Save Close

Map List

Create New Map

| # | Name    | Description             | Action          |
|---|---------|-------------------------|-----------------|
| 1 | 1F_plan | Looation Map for man... | <div>View</div> |

**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:d0:6e

Hostname

CW-400NAC-E1

Uptime

09:08

Channel

5 / 100

Rate

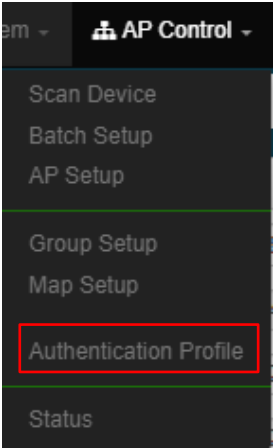
11.0 Mb/s / 866.7 Mb/s

Client

0



8.3.6 Authentication Profile

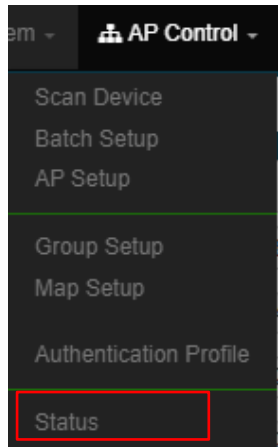


Administrator can pre-set authentication conditions in the profile, the authentication set can refer to manual “5.2 Authentication”.

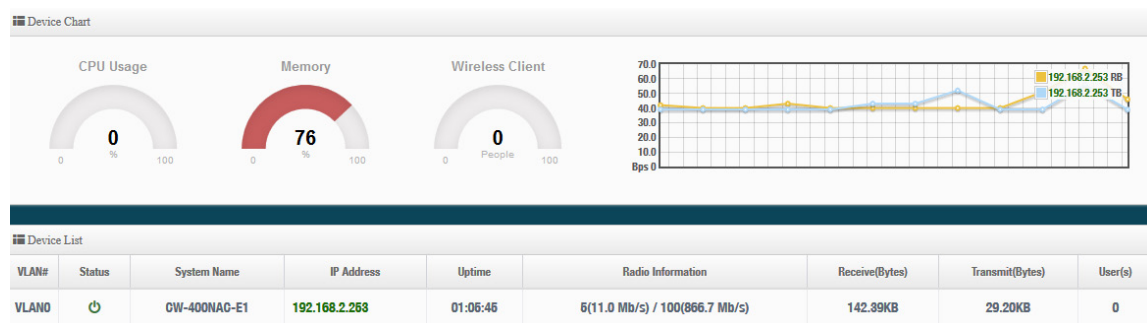
| Authentication Profile List |                      |             |                |                |        | Create New Profile |
|-----------------------------|----------------------|-------------|----------------|----------------|--------|--------------------|
| #                           | Name                 | Description | Authentication | Edit           | Action |                    |
| 1                           | Authentloation-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 **Manual“5.3 Authentication”**.  
**Authentication** Click Dropdown to set authentication functions. Refer to **Manual “5.3 Authentication”** dropdown functions.
- **Action**: **Setup** The button can modify or delete for the authentication profile.

8.3.7 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 #: Display the virtual local area network information.
- System status: Shows the operating status of the managed AP, whether it is offline or online.
- System name: Display the name information of the managed AP
- IP address: Displays the IP address information of the managed AP.
- Connection time: display the operating time of the managed AP.
- Radio information: displays the frequency and channel information enabled by the managed AP.
- Receive: Shows how much packet traffic is received by the managed AP.
- Transmission: Shows how much packet traffic is transmitted by the managed AP.
- User (s): Display the current number of Wi-Fi connected APs.

## 8.4 MAN-Mesh Control

### 8.4.1 MAN-Mesh Device list

Create Man-Mesh device IP address and comment of MAN-Mesh devices to be monitored.


| MAN-Mesh Device List |               |         | Create MAN-Mesh Device |
|----------------------|---------------|---------|------------------------|
| #                    | IP Address    | Comment | Action                 |
| 1                    | 192.168.2.253 | test    | Edit                   |

Item Action “edit” the status of the MAN-Mesh Device's IP address, annotations, (root) password, HTTP port number, and delete MAN-Mesh Device.

| MAN-Mesh Device Setup |   |
|-----------------------|---|
| IP Address            | <input type="text" value="192.168.2.253"/>                          |
| Comment               | <input type="text" value="test"/>                                   |
| Password              | <input type="password" value="*****"/>                              |
| HTTP Port             | <input type="text" value="80"/> <input type="button" value="Port"/> |

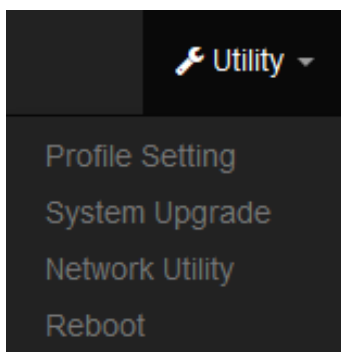
### 8.4.2 MAN-Mesh Status

Display the system status, IP address, comment, Uptime, firmware version, and firmware release date of the newly added MAN-Mesh Device.

| MAN-Mesh Device List |   |               |         |        |                  | Refresh       |
|----------------------|---|---------------|---------|--------|------------------|---------------|
| #                    | Status  | IP Address    | Comment | Uptime | Firmware Version | Firmware Date |
| 1                    |  | 192.168.2.253 | test    | -      | -                | -             |

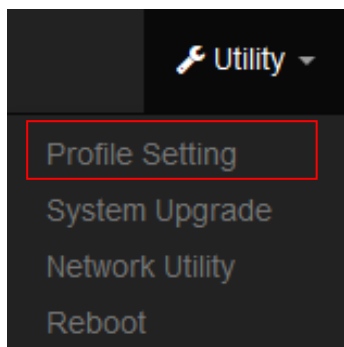
## 9. Utilities

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



### 9.1 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

Save

Load Settings From PC

瀏覽... 未選擇檔案。

Upload

Reset To Factory Default

Default

---

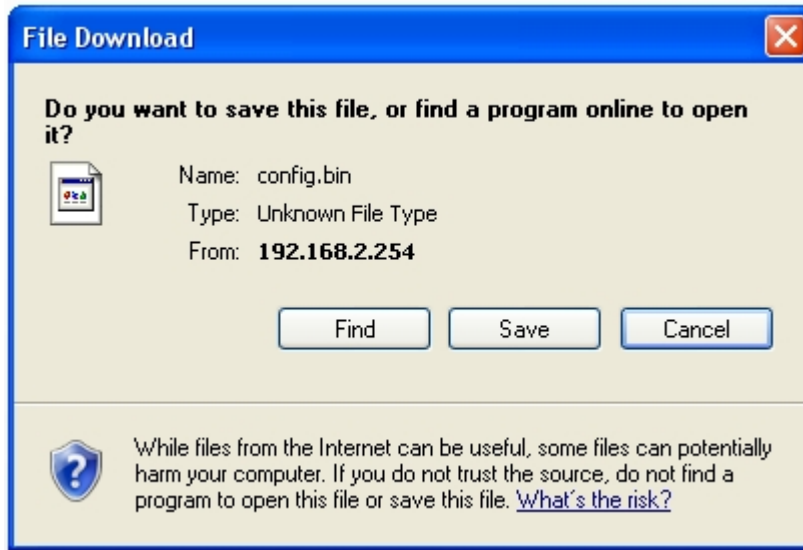
Update SSL Certification From Local Hard Drive

Certificate File

瀏覽... 未選擇檔案。

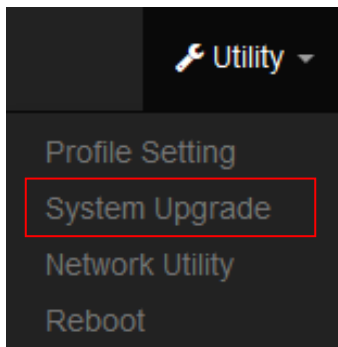
Upload

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



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

## 9.2 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.

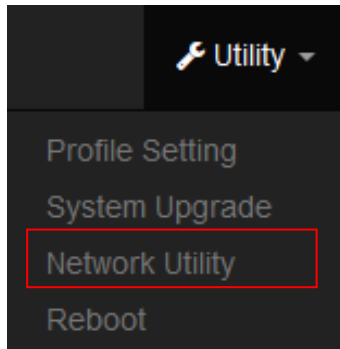
### Notice

*We strongly recommend that you perform the firmware update by following these steps:*

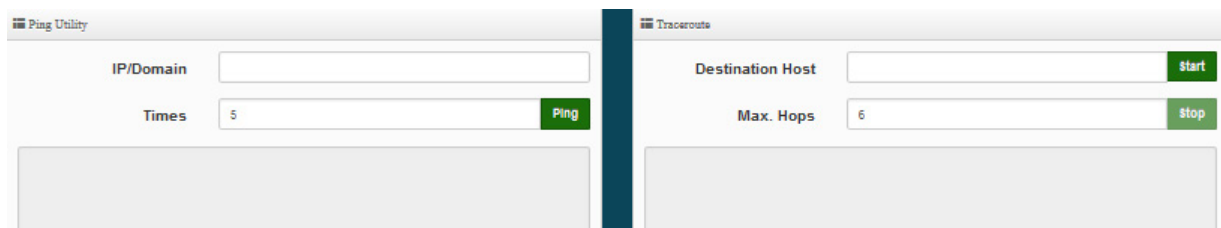
- 1. Please use a RJ-45 network cable to connect the computer and the wireless base AP mode to perform the update operation. Do not use a wireless connection for firmware update operations.*
- 2. During the update process, please do not turn off or power off the system.*
- 3. Make sure to update using a compatible web browser to avoid update failures.*
- 4. After the update is complete, make sure to perform a factory default reset operation and restart the wireless AP mode.*
- 5. If the update operation is not performed according to the above steps, if the update fails and the system cannot provide services or cannot operate normally, please forgive us for treating this situation as a human error and you will lose the product warranty. Service and you will be charged for related maintenance.*



## 9.3 Network Utility

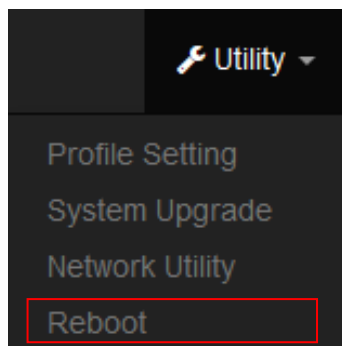


The administrator can diagnose network connectivity via the PING or TRACEROUTE utility. Please click on **Utilities** -> **Network Utility** and follow the below setting.

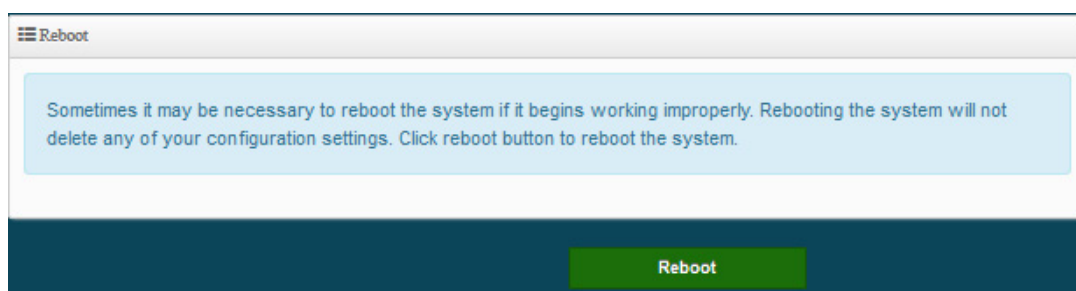


- **Ping:** This utility will help ping other devices on the network to verify connectivity. Ping utility, using ICMP packets, detects connectivity and latency between two network nodes. As result of that, packet loss and latency time are available in the **Result** field while running the PING test.
  - **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.

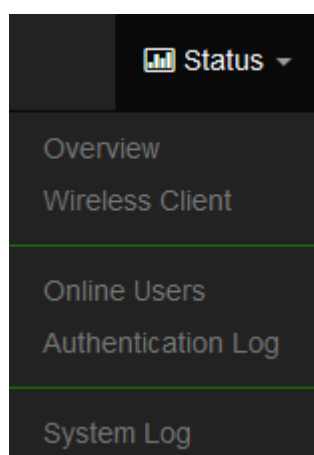
## 9.4 Reboot



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.



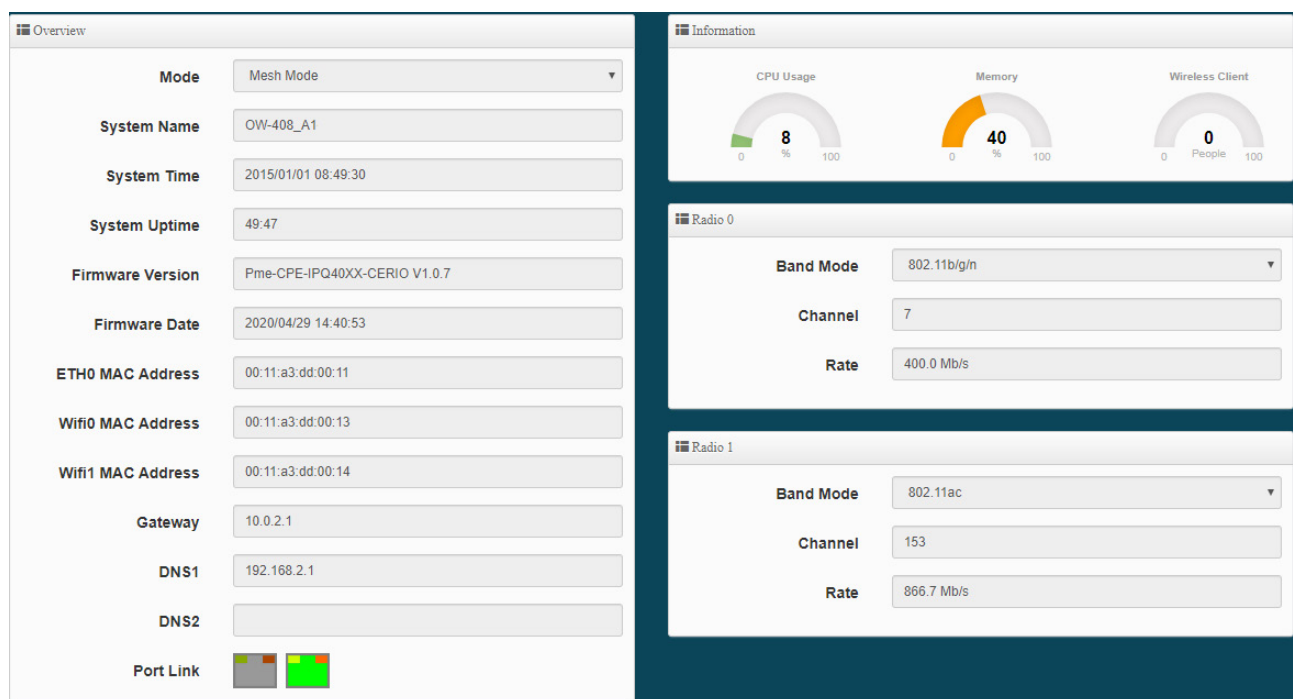
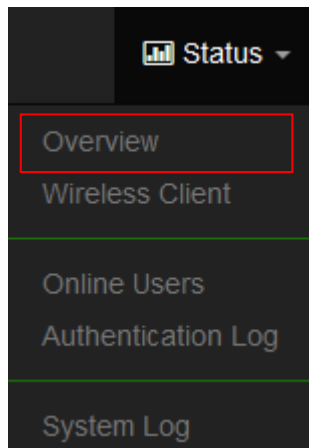
## 10. Status



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

## 10.1 Overview

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

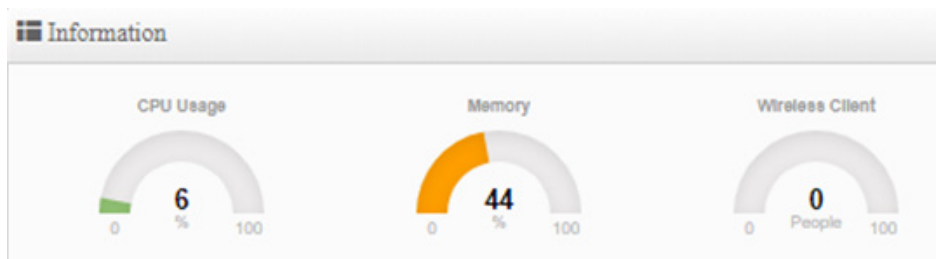


### Overview :

It mainly displays the current mode, name, time, firmware version, network card address and related network settings.

### Information :

Shows the performance / memory usage of the total CPU space used by the current system and the current number of connected wireless users. °



## Radio 0 / Radio 1 wireless Information :

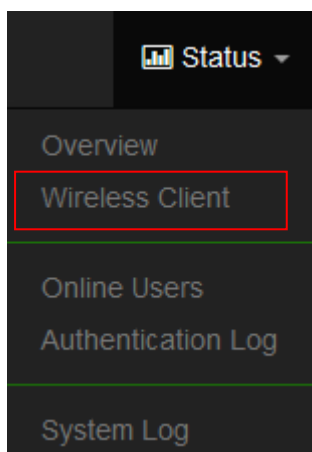
Displays the basic operating mode information of the current Radio 0 (2.4GHz) / Radio 1 (5GHz) wireless AP.

| Radio 0   |             |
|-----------|-------------|
| Band Mode | 802.11b/g/n |
| Channel   | 5           |
| Rate      | 400.0 Mb/s  |

| Radio 1   |          |
|-----------|----------|
| Band Mode | 802.11ac |
| Channel   | 132      |
| Rate      | 0.0 Mb/s |

## 10.2 Wireless Client

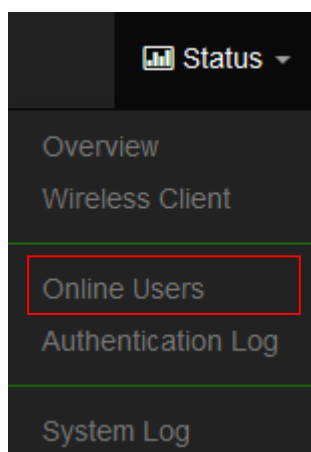


The page can be display Wireless user information link to access point. Administrator can monitor MAC address / rate and RSSI for the wireless users. (In addition to CAP mode)

| VLAN 0 |             |             |      |
|--------|-------------|-------------|------|
| Radio  | MAC Address | Rate(RX/TX) | RSSI |
| -      | -           | -           | -    |

- **Radio** : Display information for wireless client connection Radio 0 or 1
- **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.

## 10.3 Online Users



### Notice

This function works in the wireless AP mode. When the web authentication function is activated, the current connection status and related information of online users who have passed the authentication will be displayed. **(Please refer to Manual 5.3“Authentication” Function)**

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)

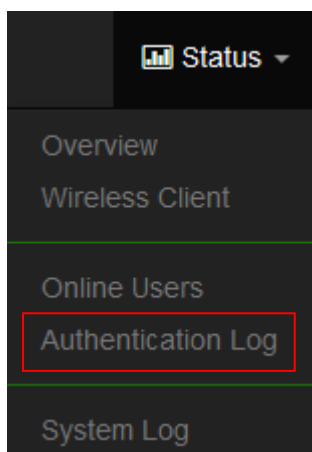
| Authentication Zone Online Users |                |            |                  |                |                |              |        |
|----------------------------------|----------------|------------|------------------|----------------|----------------|--------------|--------|
| VLAN#                            | 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 | 00:0C:29:00:00:00:2A | 2016/01/01 00:23:41 | 76842            | 17677          | 98.41MB        | 2.09MB       | <a href="#">Logout</a> |

- **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.

## 10.4 Authentication Log



### Notice

This function works in the wireless AP mode. When the web authentication function is activated, the current connection status and related information of online users who have passed the authentication will be displayed. **(Please refer to Manual 5.3 “Authentication” Function)**

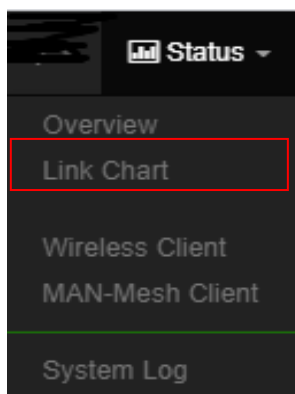
The authentication log can monitor account login/logout type and account use time. (This page only used AP mode)

| Authentication Zone Log |       |        |
|-------------------------|-------|--------|
| Date                    | VLAN# | Detail |
| -                       | -     | -      |

- **Date**: Administrator can select dates.
- **VLAN**: Administrator can select VLANs.
- **Detail**: Administrator can click button to open detail information.



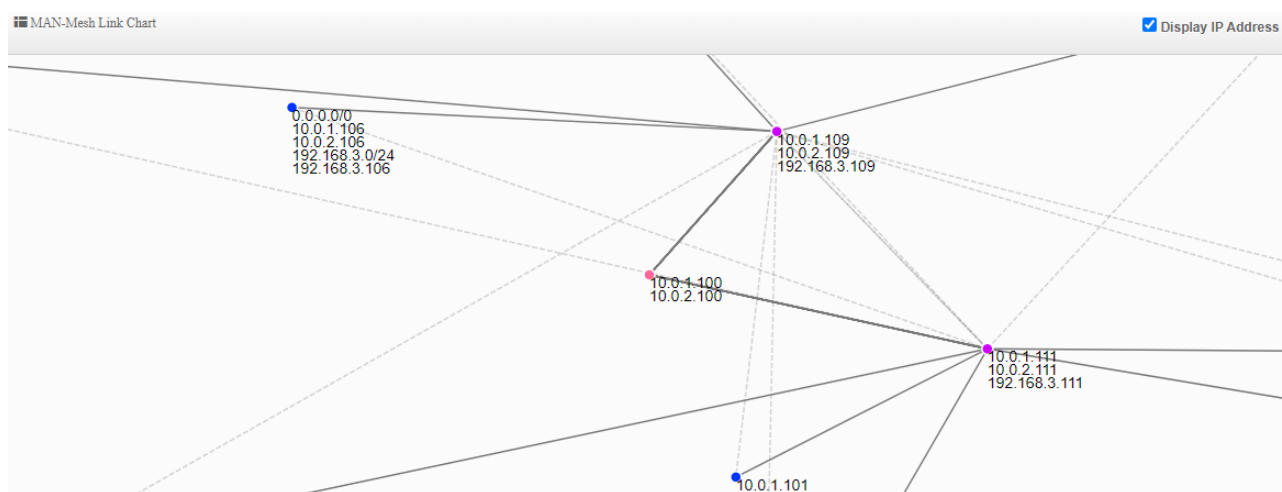
## 10.5 MAN-Mesh Link Chart



This function works in MAN-Mesh mode. When the MAN-Mesh function is enable, the MAN-Mesh APs connection information will be displayed. (Please refer to the manual 4.3 "MAN-Mesh" function)

Display MAN-Mesh connection information(MAN-Mesh Link Chart) or MAN-Mesh signal status(MAN-Mesh Client) to view MAN-Mesh related information.

### MAN-Mesh Link Chart



Using WI-FI multi-angle positioning-related address to display MAN-Mesh link chart

**Check Display IP Address to view the LAN IP and MESH IP of all MESH connected machines.**

## MAN-Mesh Neighbours

| MAN-Mesh Routes    |        |           |                         |                          |           |           |
|--------------------|--------|-----------|-------------------------|--------------------------|-----------|-----------|
| Prefix             | Metric | Refmetric | ID                      | Via                      | Interface | Installed |
| 192.168.101.224/32 | 512    | 256       | 02:11:a3:ff:fe:1d:00:05 | fe80::211:a3ff:fe1d:4    | mesh11    | no        |
| 192.168.2.254/32   | 65535  | 256       | 02:11:a3:ff:fe:1d:00:05 | fe80::211:7fff:fe1b:f952 | mesh11    | no        |
| 192.168.101.224/32 | 65535  | 256       | 02:11:a3:ff:fe:1d:00:05 | fe80::211:7fff:fe1b:f952 | mesh11    | no        |
| 192.168.2.252/32   | 512    | 256       | 02:11:a3:ff:fe:1d:00:01 | fe80::211:7fff:fe1b:f950 | mesh11    | no        |
| 192.168.2.252/32   | 256    | 0         | 02:11:a3:ff:fe:1d:00:01 | fe80::211:a3ff:fe1d:4    | mesh11    | yes       |
| 192.168.101.217/32 | 256    | 0         | 02:11:a3:ff:fe:1d:00:01 | fe80::211:a3ff:fe1d:4    | mesh11    | yes       |
| 192.168.2.0/24     | 384    | 128       | 02:11:a3:ff:fe:1d:00:01 | fe80::211:a3ff:fe1d:4    | mesh11    | yes       |
| 192.168.2.252/32   | 65535  | 0         | 02:11:a3:ff:fe:1d:00:01 | fe80::211:7fff:fe1b:f952 | mesh11    | no        |
| 192.168.101.217/32 | 65535  | 0         | 02:11:a3:ff:fe:1d:00:01 | fe80::211:7fff:fe1b:f952 | mesh11    | no        |
| 192.168.2.0/24     | 65535  | 128       | 02:11:a3:ff:fe:1d:00:01 | fe80::211:7fff:fe1b:f952 | mesh11    | no        |


## MAN-Mesh Routes

| MAN-Mesh Redistributed Routes |        |
|-------------------------------|--------|
| Prefix                        | Metric |
| 192.168.2.0/24                | 128    |
| 192.168.2.1/32                | 128    |
| 192.168.2.10/32               | 128    |
| 192.168.2.253/32              | 0      |
| 192.168.101.221/32            | 0      |
| 192.168.101.222/32            | 0      |

## MAN-Mesh Redistributed Routes

| MAN-Mesh Neighbours      |           |       |         |         |       |
|--------------------------|-----------|-------|---------|---------|-------|
| Address                  | Interface | Reach | RX Cost | TX Cost | Cost  |
| fe80::211:7fff:fe1b:f952 | mesh11    | ffff  | 256     | 65535   | 65535 |
| fe80::211:7fff:fe1b:f952 | mesh21    | ffff  | 256     | 256     | 256   |
| fe80::211:a3ff:fe1d:4    | mesh11    | ffff  | 256     | 256     | 256   |
| fe80::211:a3ff:fe1d:8    | mesh21    | ffff  | 256     | 256     | 256   |
| fe80::211:7fff:fe1b:f950 | mesh11    | ffff  | 256     | 256     | 256   |

## 10.6 MAN-Mesh Client

|  <b>Status</b> |               |      |
|---|---------------|------|
| MAN-Mesh Client   |               |      |
| radio 0   |               |      |
| MAC Address   | Rate(RX/TX)   | RSSI |
| -   | -             | -    |
| radio 1   |               |      |
| MAC Address   | Rate(RX/TX)   | RSSI |
| 00:11:a3:1d:00:04   | 6Mb / 866Mb   | 48   |
| 00:11:7f:1b:f9:52   | 650Mb / 650Mb | 33   |
| 00:11:7f:1b:f9:50   | 6Mb / 866Mb   | 52   |
| radio 2   |               |      |
| MAC Address   | Rate(RX/TX)   | RSSI |
| 00:11:7f:1b:f9:52   | 6Mb / 780Mb   | 40   |
| 00:11:a3:1d:00:08   | 6Mb / 866Mb   | 55   |
| 00:11:a3:1d:00:04   | 650Mb / 650Mb | 36   |

Display MAN-Mesh connection status of MAN-Mesh wireless signal .

### MAN-Mesh Client

#### MAN-Mesh Radio 0 (2.4G)

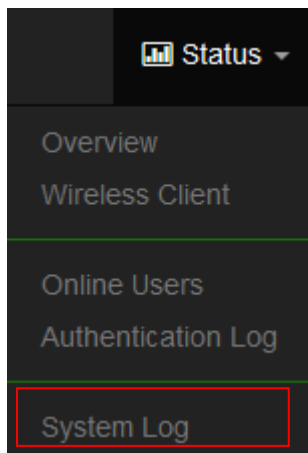
- **MAC Address** : Peripheral MAN-Mesh MAC address connected to Radio 0

- **Rate(RX/TX)** : Peripheral MAN-Mesh equipment connected to Radio 0 transmission rate , RX receive rate and TX transmit rate
- **RSSI** : Display the signal value between wireless users and Radio 0

## MAN-Mesh Radio 1 (5G)

- **MAC Address** : Peripheral MAN-Mesh MAC address connected to Radio 1
- **Rate(RX/TX)** : Peripheral MAN-Mesh equipment connected to Radio 1 transmission rate , RX receive rate and TX transmit rate
- **RSSI** : Display the signal value between wireless users and Radio 1

## 10.7 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 <span>Refresh</span> <span>Clear</span> |          |          |  |
|--|----------|----------|--|
| 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.

## 11. [ Other technical documents]

### 11.1 Point to Point / Multi-Point for WDS settings

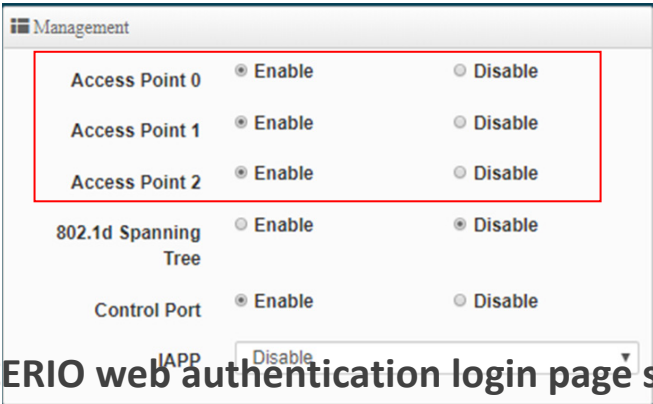
The WDS function is applied in the wireless AP mode. This function is mainly used for point-to-point wireless AP bridging. For the setting method, You can **refer to the manual 5.6.5 "WDS Setting"**. This document mainly guides the key WDS procedures. Can easily structure WDS point-to-point or point to multi point applications

- 1) If point-to-point bridging is used for WDS function, it is recommended to use our products to avoid compatibility issues.
- 2) If point-to-point bridging is used for WDS function, it is recommended to use our products to avoid compatibility issues.
- 3) According to the requirements to be applied to 2.4G or 5G, please make sure that each wireless AP sets a set of same channels (**please refer to the manual 5.6 "Wireless Configuration" (Radio 0 or Radio 1 Setup)**)
- 4) Restart after confirmation will complete WDS point-to-point bridging, **please refer to the manual 5.6.6 "WDS Status"** to confirm the RSSI value. The value If show to "-1" indicates that the connection is not successful, please re-confirm whether the configuration file follows the above instructions, or between APs. Signals are blocked by interference.
- 5) Please refer to WDS setting page, please set the MAC address information of other wireless for the wireless AP correctly. If two bridges, Radio A and Radio B, are used as examples, the MAC address information of Radio B must be entered in the MAC address list of Radio A of the site, and, the MAC address information of Radio A must be entered in the MAC address list of Radio B of the site.  
**Ps, The RSSI value is recommended to fall between 40 ~ 60. If over the RSSI value means the AP is too close to the AP. If below the RSSI value means the signal is not right or the distance is too far.**

**Remark:**

Because the WDS application is in the wireless AP mode, if the WDS function is enabled, it will be an AP + WDS application. If the wireless AP is not required to use the WDS function purely, **you**

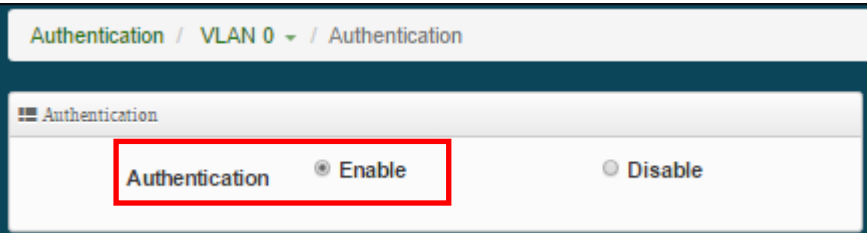
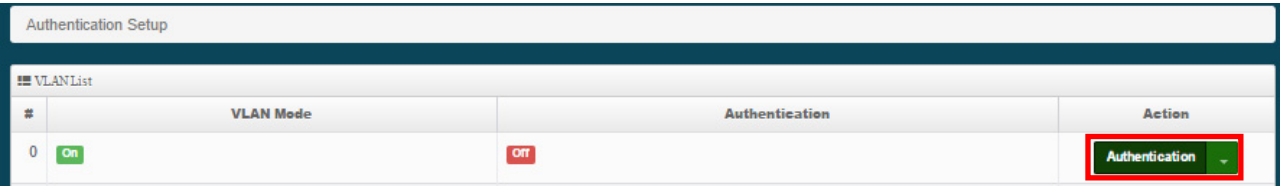
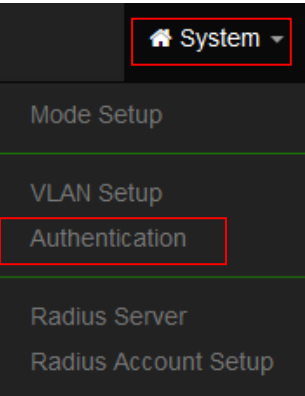
can refer to the manual 5.2 "VLAN Setup" instructions, turn off the wireless AP, as shown below.



11.2 Apply CERIO web authentication login page sample

If the device uses our company's wireless AP CenOS5.0, and the web authentication function is enabled, you will be able to customize the web authentication page. You can follow the steps below to easily complete the sample login page.

Step 1 : Start the web page authentication function first, and in the "System" settings => "Authentication" function (refer to Manual 5.3 "Authentication" function)



**Step 2 :** After confirming the activation, you can choose what type of login account to use. This step uses "Local User" as an example, and will "enable to create a Local User". After confirming the activation, and "Save it", See as follows.



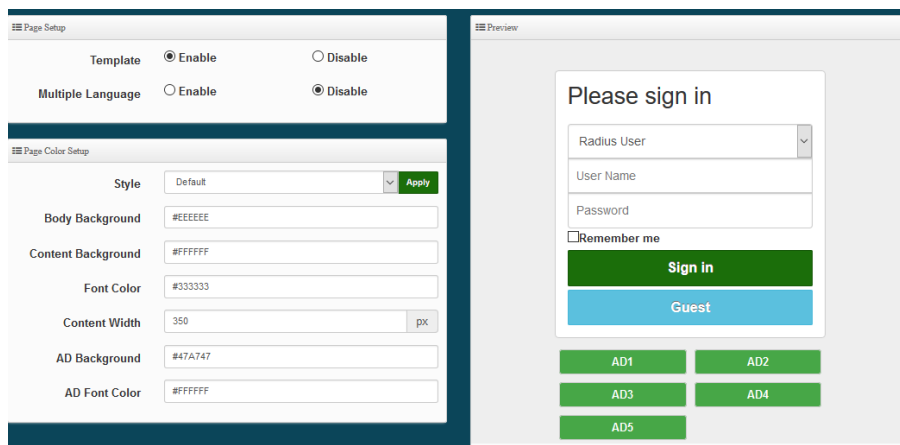
**Step 3 :** Please go to the pull-down function button of the authentication function, and enter the “User Name” and “password” , See as follows.

- \* If want to use the system preset page, please refer to **step 4**,
- \* If want to apply our template, please refer to below for **step 5**,
- \* If want to edit the webpage by yourself, please refer to **step 7**.

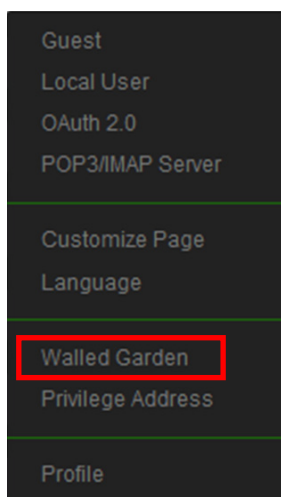
## Notice

If you want to edit the webpage by yourself, it is recommended that the administrator must have the basic ability to make webpages in HTML / CSS.) This department has no responsibility for webpage syntax guidance.

**Step 4 :** If you want to use the preset authentication page, you can refer to the instruction **manual 5.3.4 “Customized Page”**, you will be able to set the preset Format for color editing and revision, if you need to customize the page and apply our template, **please refer to step 5**

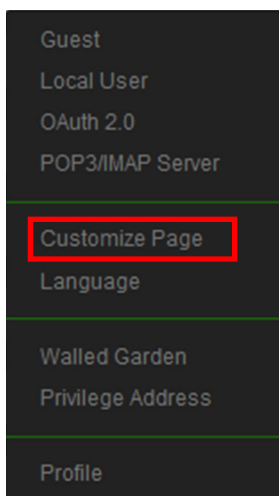


**Step 5 :** The image file of the login page must be placed on the website server, the website address must be whitelisted. The background image of this example is stored on below second server (URL: [www.serio.com.tw](http://www.serio.com.tw)), so please make sure Enter into Walled Garden.

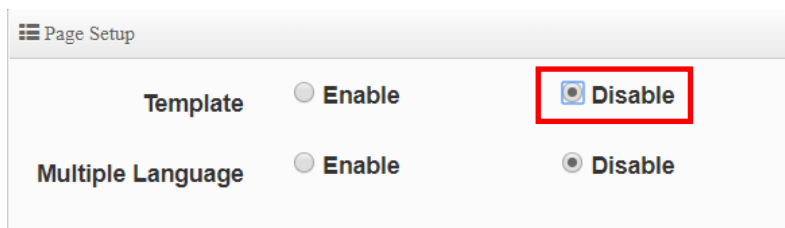



**Step 6 :** Go to the company's Cerio website to download the sample file first. And open your download sample, select all the HTML syntax and copy it, then paste it on the custom edit page of the system and save it.

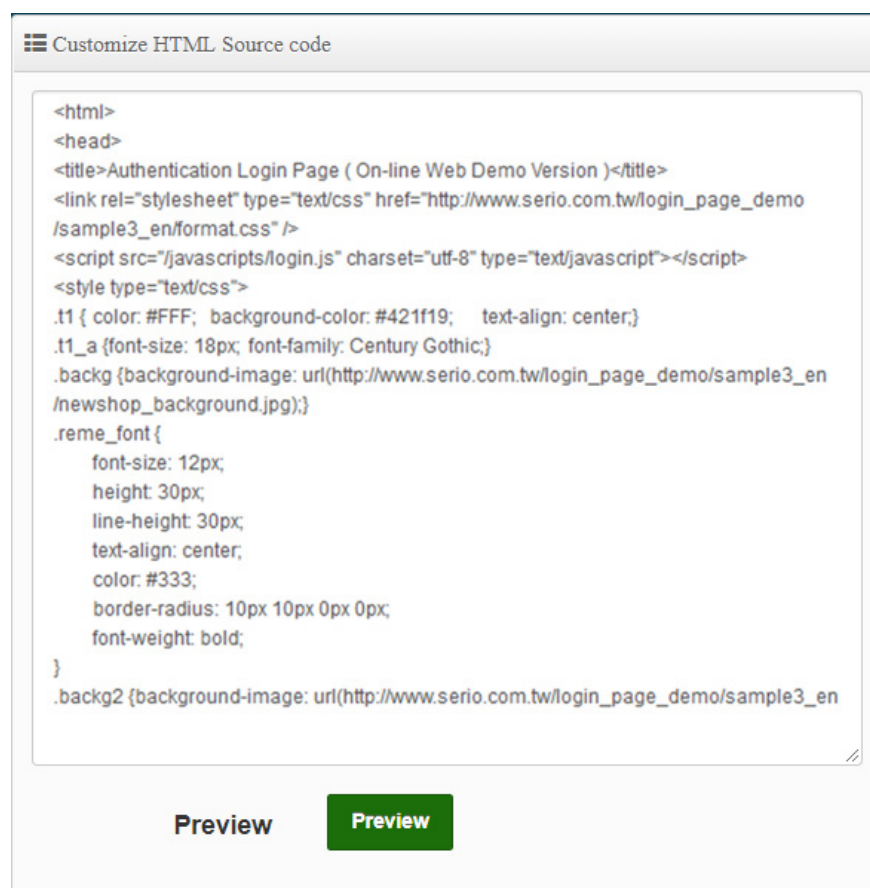
Download example address: [www.cerio.com.tw/eng/extreme-indoor/customized-page/](http://www.cerio.com.tw/eng/extreme-indoor/customized-page/)



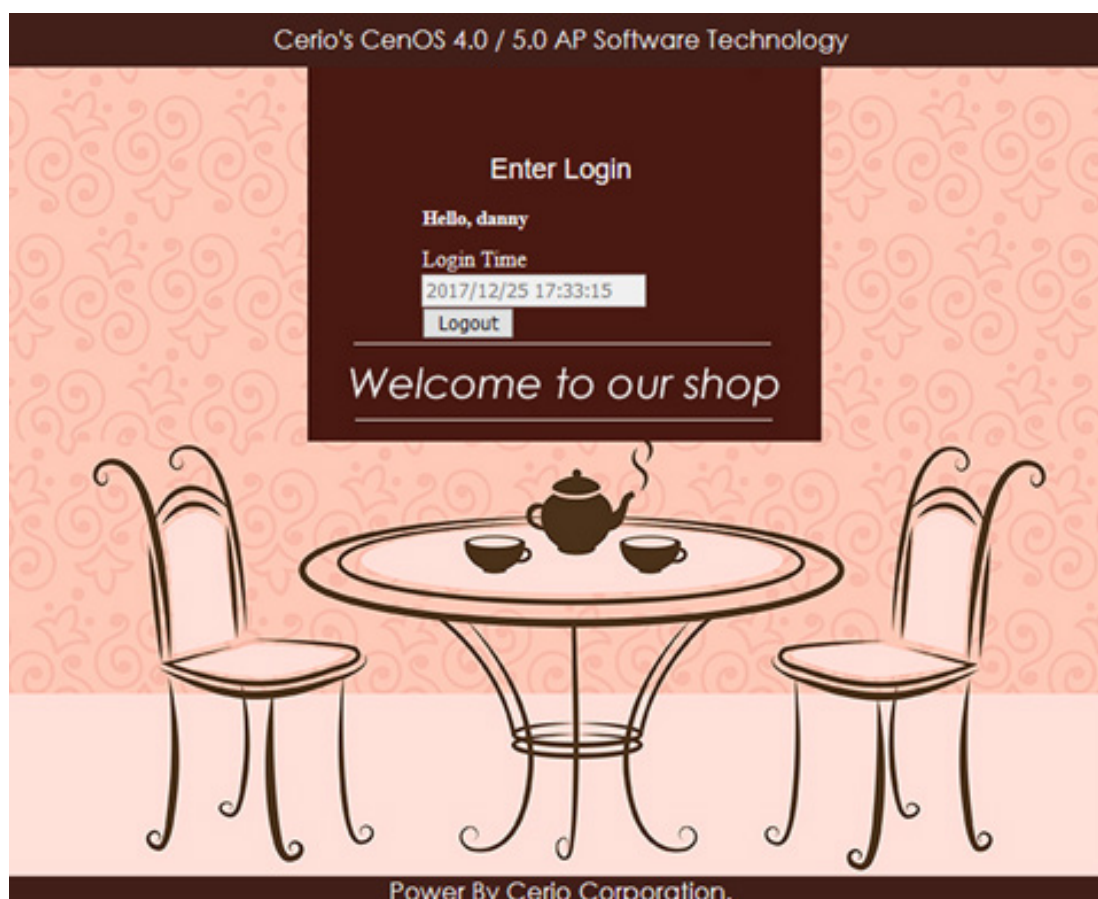
Close "Template" first, then copy the sample html\_code syntax and replace it in the HTML source code edit "Customize HTML Source code" bar.



After clearing the HTML source code content, then paste all the downloaded source code into the field, save and restart the device, and you can finish editing the login page.



Login page for template below :





**Notice**

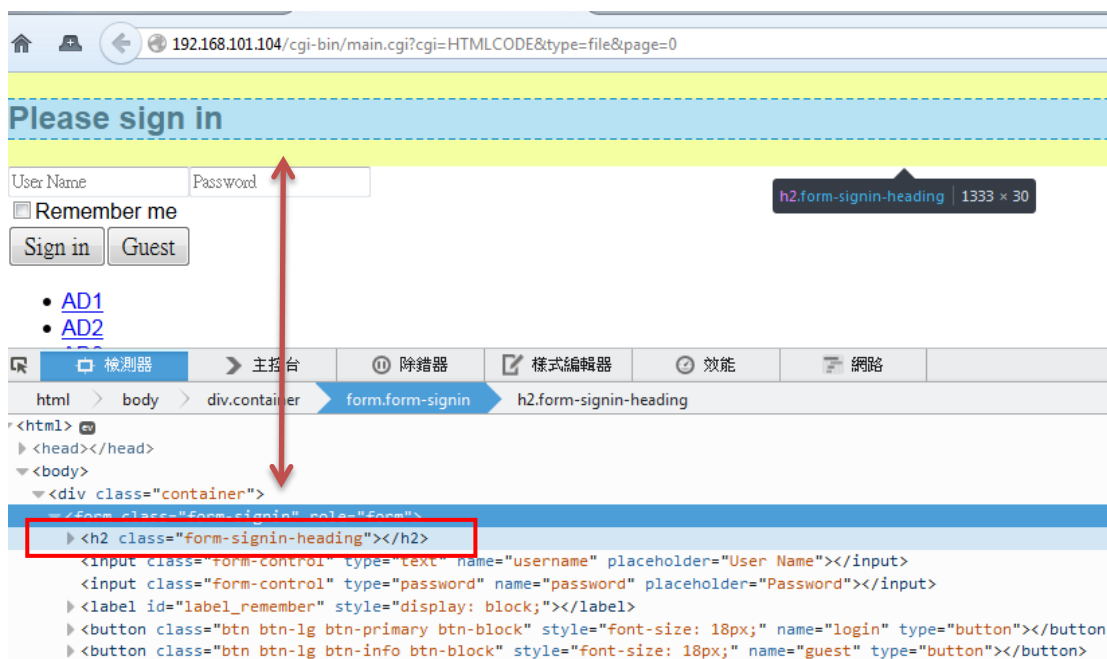
1. This part must be within 190 lines. If the written HTML / CSS and other source code exceeds a certain line, it is recommended to save the CSS source code to the remote Web server, and then enter the IP address of the remote web server. Within Walled Garden. **(Please refer to the manual 5.3.4 "Walled Garden" setting instructions)**
2. This device does not support the storage space of picture files. If necessary, store the picture files on a remote web server and call the address recently, See as above.

**Step 7 :** If the custom page is to be make by yourself, the original code of the following scarlet letters must not be removed, others will be able to make by themselves

```
<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>
```

**Step 8 :** The login function of this system is displayed by default. If there are unnecessary fields, specific fields can be hidden by CSS syntax, as explained below

Add the **<style> class** tag in the syntax and then add **{display: none;} </ style>** as the following example, find the ID code of the field to be hidden by the browser, for example, to hide the **"Please Sign in"** description, then find out its Class ID as shown below.



Add `<style> .form-signin-heading {display: none;} </ style>` in the head to hide the description "Please Sign in" as shown in the figure below, and find the Please Sign in word disappeared, and so on.

User Name  Password

☐ Remember me



## 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<br>0-9, A-Z, a-z<br>~ ! @ # \$ % ^ * ( ) _ + - { }   : < > ? [ ] / ; ` , . = |
| 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<br>0-9, A-Z, a-z<br>~ ! @ # \$ % ^ * ( ) _ + - { }   : < > ? [ ] / ; ` , . = |
|             | Lease Time    | 600 ~ 99999999   |

**Table B WEB GUI Valid Characters (continued)**

| Block      | Field                 | Valid Characters  |
|------------|-----------------------|---|
| Management | System Name/ Location | Length : 32<br>0-9, A-Z, a-z<br>Space<br>~ ! @ # \$ % ^ * ( ) _ + - { }   : < > ? [ ] / ; ` , . = |
|            | Description           | 32 chars  |
|            | Password              | Length : 4 ~ 30<br>0-9, A-Z, a-z<br>~ ! @ # \$ % ^ * ( ) _ + - { }   : < > ? [ ] / ; ` , . =      |
|            | HTTP/ HTTPS Port      | 1 ~ 65535   |
|            | Telnet/ SSH Port      | 1 ~ 65535   |

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

**Table B WEB GUI Valid Characters (continued)**

| Block                   | Field                   | Valid Characters  |
|-------------------------|-------------------------|---|
| <b>Virtual AP Setup</b> | ESSID                   | Length : 31<br>Space<br>0-9, A-Z, a-z<br>~ ! @ # \$ % ^ * ( ) _ + - { }   : < > ? [ ] / ; ` , . = |
|                         | 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  |

| Block          | Field                | Valid Characters                 |
|----------------|----------------------|----------------------------------|
| WDS Setup      | Radius Server IP     | IP Format; 1-254                 |
|                | Radius Port          | 1 ~ 65535                        |
|                | Shared Secret        | 8 ~ 64 characters                |
|                | Session Timeout      | >= 60 seconds; 0 is disable      |
|                | AES Key              | 8 ~ 63 ASCII chars; 64 HEX chars |
|                | Peer's MAC Address   | 12 HEX chars                     |
| IP Filter      | Description          | 32 chars                         |
|                | Source Address       | IP Format; 1-254                 |
|                | Source Mask          | 0 ~ 32                           |
|                | Source Port          | 1 ~ 65535                        |
|                | Destination Address  | IP Format; 1-254                 |
|                | Destination Mask     | 0 ~ 32                           |
| MAC Filter     | Destination Port     | 1 ~ 65535                        |
|                | MAC address          | MAC Format; 12 HEX chars         |
| Virtual Server | Description          | 32 chars                         |
|                | Private IP           | IP Formate; 1-254                |
|                | Private/ Public Port | 1 ~ 65535                        |