Cerio Corporation

CenOS5.0 User Manual

(For Indoor and Outdoor Wireless Devices)

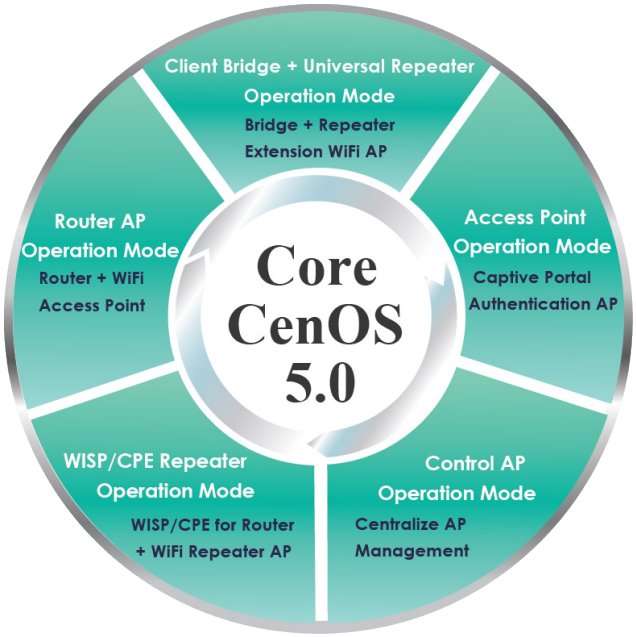
1. Introduction 5
1.1 Overview 5
1.2 Software Configuration 6
1.3 Login Web Page 9
2. Software Setting 10
2.1 Operating Mode Introduction 10
3. Access Point mode 13
3.1 Select AP Mode 13
3.2 VLAN Setup 14
3.2.1 Network Button 15
3.2.2 Network Pull-down menu 16
DHCP Server 16
 # Radio 0/1 Access Point 18
MAC Filter 21
802.11r/802.11k Fast Roaming 21
3.3 Authentication 23
Authentication Button: 24
Authentication Dropdown Button 25
3.3.1 Guest 26
3.3.2 Local User 26
3.3.3 OAuth2.0 27
※ Sample for Google OAuth2.0 setup 27
※ Sample for Facebook OAuth2.0 setup 30
3.3.4 POP3 Server 34
The purpose of this integrated function is to allow clients to link a POP3 server for receiving emails from a remote server. 34
3.3.5 Customize Page 34
3.3.6 Language 36
3.3.7 Walled Garden 36
3.3.8 Privilege Address 37
3.3.9 Profile 37
3.4 RADIUS Server 38
3.5 Radius Account Setup 38
3.6 Wireless Basic Setup 39
3.6.1 Radio 0 Basic Setup (2.4G) 39
3.6.2 Radio 1 Basic Setup (5G) 42
3.6.3 Advanced Setup 45
3.6.4 WMM Setup 47

3.6.5 WDS Setup 50
4. CAP Mode....52
4.1 System VLAN Setup....52
4.2 AP Control 55
Centralized Management APs operating Instructions:....55
4.2.1 Scan Device 55
4.2.2 Batch Setup 57
4.2.3 AP Setup 60
4.2.4 Group Setup 60
4.2.5 Map Setup 61
4.2.6 Authentication Profile 63
5. Client Bridge Mode 64
5.1 Configure LAN Setup....65
5.2 Configure DHCP Setup 66
5.3 Wireless General Setup 68
5.3.1 Radio 0(2.4G) Basic Setup....69
5.3.2 Radio 1(5G) Basic Setup....71
5.3.3 Advanced Setup 72
5.3.4 WMM Setup....75
5.3.5 Station Setup....77
5.3.6 Repeater AP Setup....78
5.3.7 MAC Filter 80
5.3.8 802.11r/802.11k Fast Roaming 81
6. WISP Mode....83
6.1 Configure WAN Setup 83
6.2 Configure LAN Setup....87
6.3 Configure DHCP Server 88
6.4 Wireless General Setup 90
6.4.1 Radio 0(2.4G) Basic Setup....90
6.4.2 Radio 1(5G) Basic Setup....92
6.4.3 Advanced Setup 93
6.4.4 WMM Setup....96
6.4.5 Station Setup....98
6.4.6 Repeater AP Setup....99
6.4.7 MAC Filter 101
6.4.8 802.11r/802.11k Fast Roaming 102
7. Router Mode 104
7.1 Configure WAN Setup 104

7.2 Configure LAN Setup 109
7.2.1 Network Button 109
7.2.2 Network Pull-down menu 111
DHCP Server 111
 # Radio 0/1 Access Point 112
MAC Filter 115
802.11r/802.11k Fast Roaming 116
7.3 Wireless Basic Setup 118
7.3.1 Radio 0 Basic Setup (2.4G) 118
7.3.2 Radio 1 Basic Setup (5G) 121
7.3.3 Advanced Setup 124
7.3.4 WMM Setup 126
8. Advanced Setup By WISP & Router Mode 128
8.1 DMZ 128
8.2 IP Filter 129
8.3 MAC Filter 131
8.4 Virtual Server 132
8.5 Access Control 133
8.6 Time Policy 135
9. System Management 136
9.1 Configure system management 136
9.2 Configure Time Server 137
9.3 Control PoE Bridge 138
9.4 Configure SNMP Setup 139
10. Utilities 140
10.1 Profile Setting 140
10.2 System Upgrade 142
10.3 Network Utility 143
10.4 Reboot 143
11. Status 144
11.1 Overview 144
11.2 Wireless Client 144
11.3 Online Users by Captive Portal 145
11.4 Authentication Log by Captive Portal 146
11.5 System Log 146
Appendix A. WEB GUI Valid Characters 147

1. Introduction

1.1 Overview



This versatile and feature packed software allows our wireless devices to handle any challenges and network requirements faced by our customers, providing an all-encompassing wireless solution for all network environments and architectures.

CenOS 5.0 is compatible with all Cerio wireless access points with the exemption of a few models. Devices that are currently operating on legacy software cores can be upgraded to CenOS 5.0 by downloading the CenOS 5.0 firmware from the Cerio website product page.

CenOS 5.0 Demo (CLICK HERE)

Highlight features

- Supports five different operation modes
- Versatile authentication supports **Guest Login**, **Local Account Users**, **OAuth2.0** for **Facebook** and **Google+ Login**, and **Built-in RADIUS**
- Control Access Point Mode (CAP) can centrally manage a maximum of
  - **128 AP Devices** (using 11ac Access Point)
  - **16 AP Devices** (using 11n Access Point)
- Customizable Captive Portal authentication platform for convenient client login
- Supports built-in 802.1x RADIUS authentication server account database for small and medium environments **(for 11ac devices only)**
- QoS (Quality of Service) for bandwidth management and traffic prioritization. Administrators can regulate the maximum Bandwidth Upload/Download speed limit of each network user
- 11ac Access Points support 32 ESSIDs per device (16 ESSID on 2.4Ghz and 16 ESSID on 5Ghz)
- 11n Access Points support 7 ESSIDs per device
- Supports IEEE802.11f IAPP and IEEE802.11r and IEEE802.11k Fast Roaming
- Supports x8 WDS per Radio (2.4Ghz band WDS x8 and 5Ghz band WDSx8) for a total of 16 WDS Links (dual band models only)
- Dual Band devices supports Band steering
- Software UI supports Auto reboot setting function. Software setting allows automatically reboot by Daily/Weekly/Monthly settings

1.2 Software Configuration

CenOS 5.0 APs supports web-based configuration. Upon the completion of hardware installation, **APs** can be configured through a PC/NB by using a web browser such as Internet Explorer 6.0 or later.

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

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

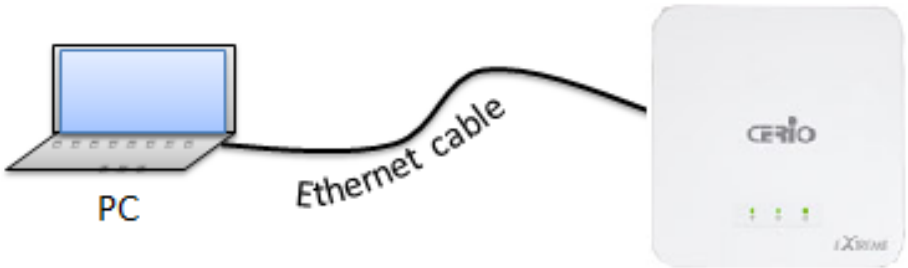
- **IP Segment Set-up for Administrator's PC/NB**

Set the IP segment of the administrator's computer to be in the same range as the **CenOS 5.0 AP** for accessing the system. Do not duplicate the IP Address used here with IP Address of the **CenOS 5.0 AP** or any other device within the network.

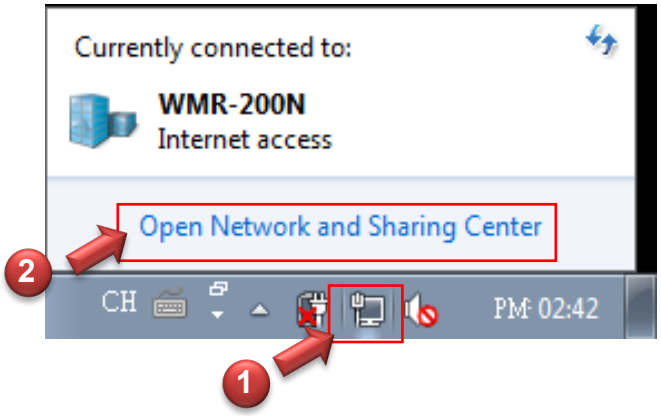
- **Example of Segment: (Windows XP)**
  - Click **Start** -> **Settings** -> **Control Panel**, and then "**Control Panel**" window appears. Click on "**Network Connections**", and then "**Network Connections**" window appears.
  - Click right on "**Local Area Connection**", and select **Properties**.

The following setup uses a Windows 7 PC, user OS may vary

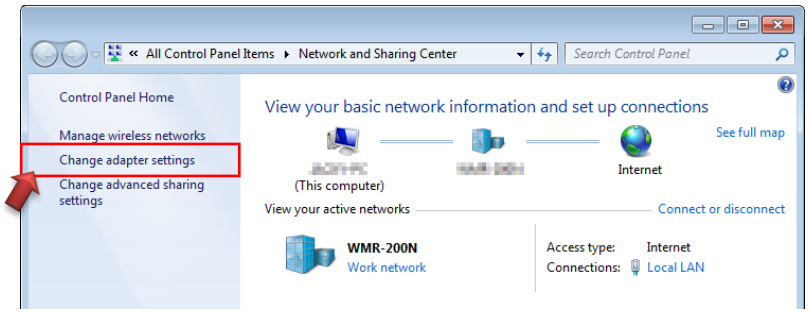
Please PC link to Device used cat5/6 Ethernet cable.



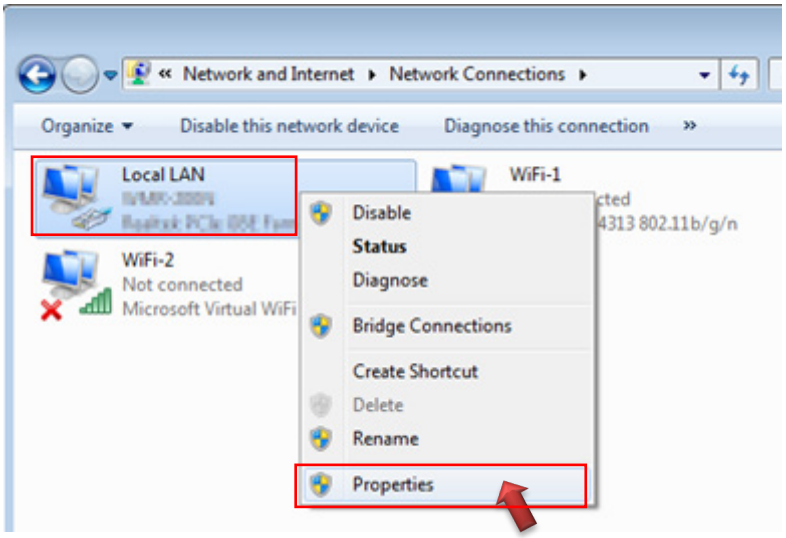
Step 1: Please click on the computer icon in the bottom right window, and click **"Open Network and Sharing Center"**



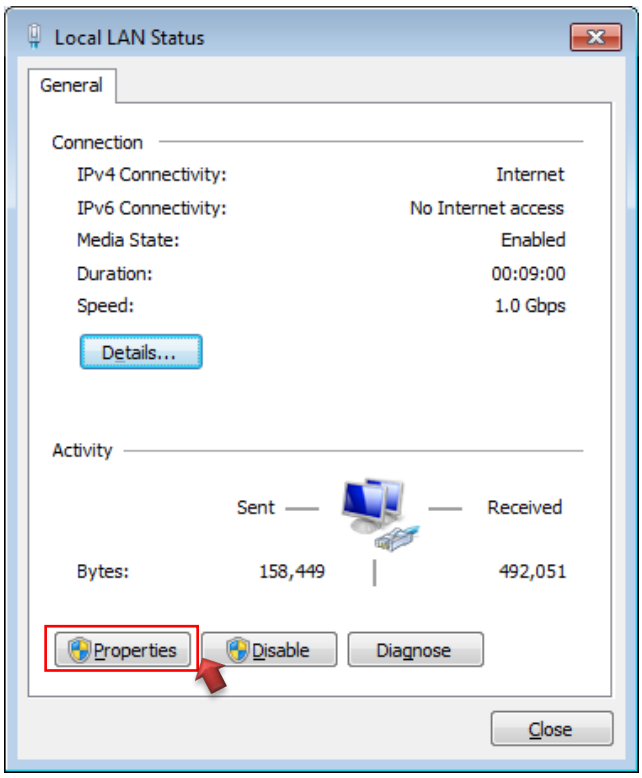
Step 2: In the Network and Sharing Center page, Please click on the left side of **"Change adapter setting"** button



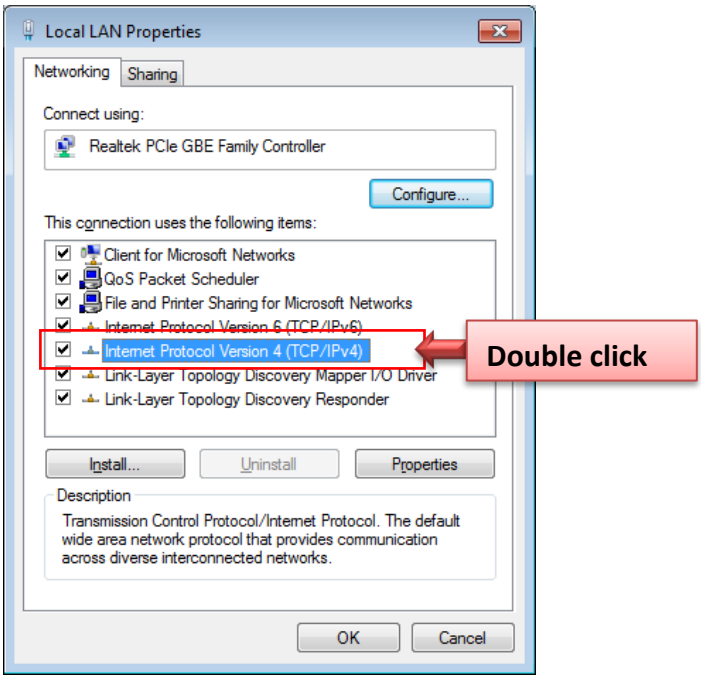
Step 3: In **"Change adapter setting"** Page. Please find Local LAN and Click the right button on the mouse and Click **"Properties"**



Step 4: In **"Properties"** page, please Click **"Properties"** button to TCP/IP setting



Step 5: In Properties page to setting IP address, please find **"Internet Protocol Version 4 (TCP/IPv4)"** and double click or click **"Install"** button.



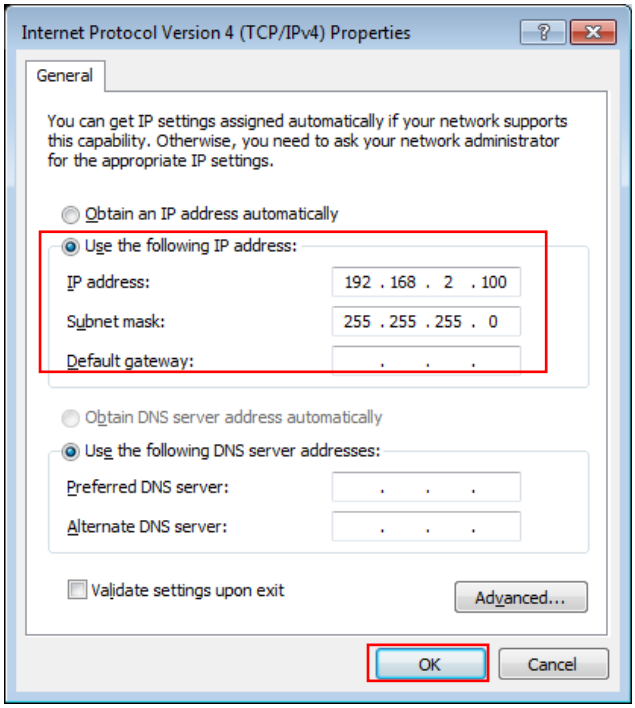
Step 6 :

Select **"Use the following IP address"**, and fix in IP Address : 192.168.2.#

ex. The # is any number by 1 to 253

Subnet mask : 255.255.255.0

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



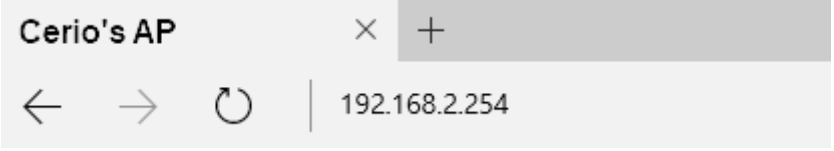
Please Open Web Browser

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

1.3 Login Web Page

➢ Launch Web Browser

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



➢ **System Login**

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

2. Software Setting

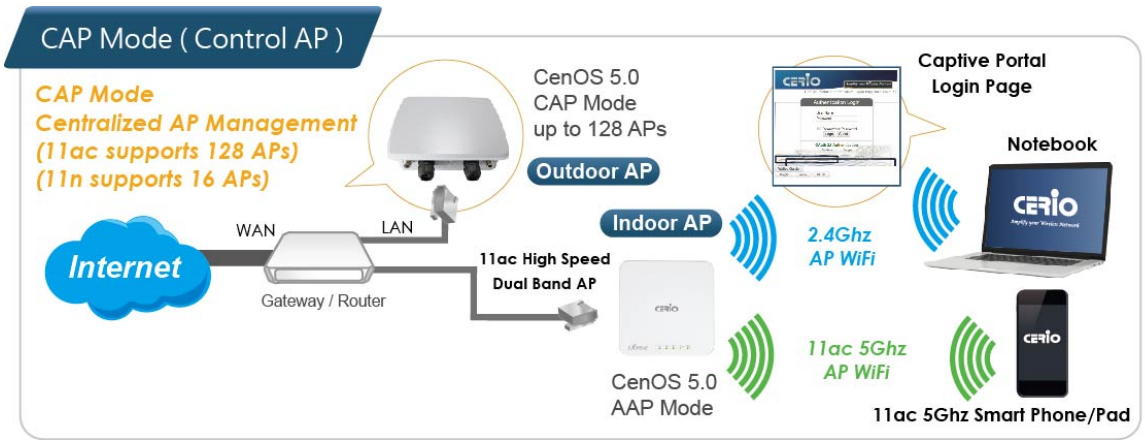
2.1 Operating Mode Introduction

Notice

Not all CenOS 5.0 devices support all five operation modes. Please reference the proper AP model's data sheet to see which operation modes are supported.

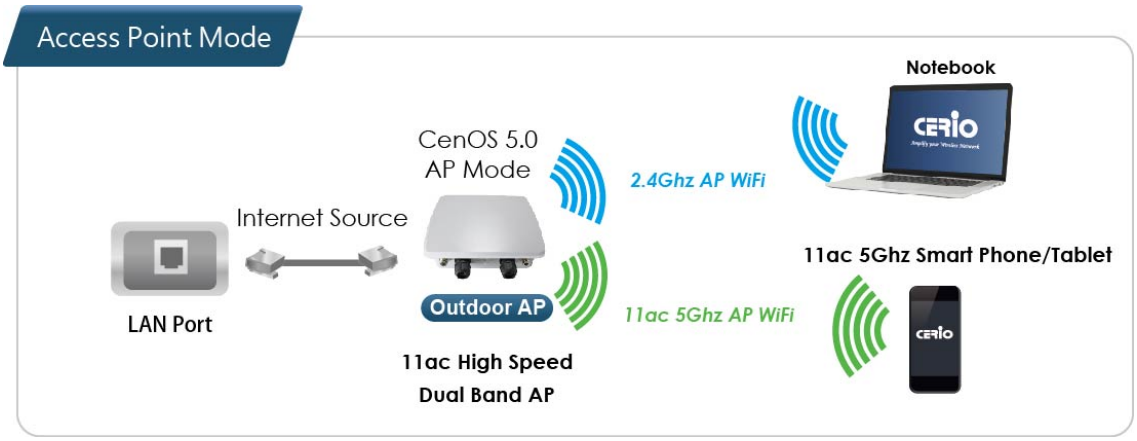
CAP mode (Centralizes Access Point)

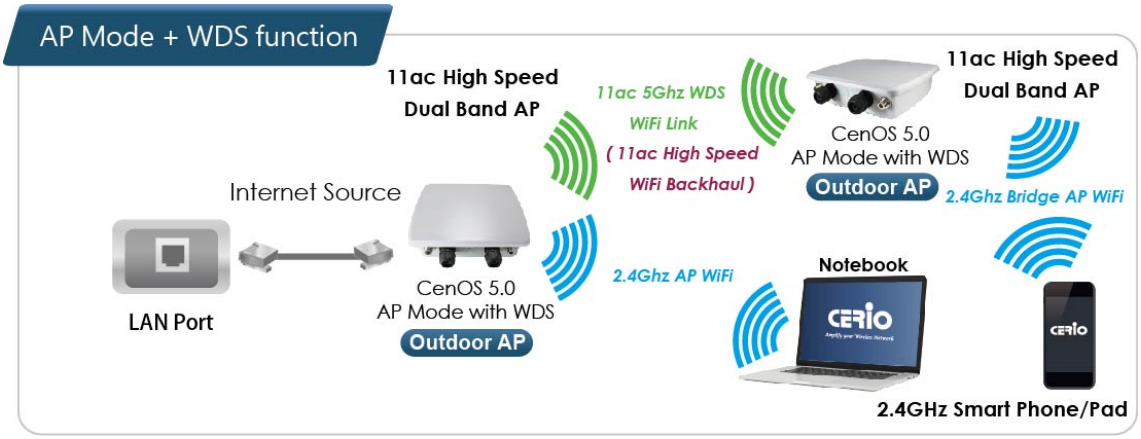
- Control Management of CenOS5.0 APs
  - **11ac devices** support management of up to **128 AP devices**
  - **11n devices** support management of up to **16 AP devices**
- AP Management support 802.1Q VLAN infrastructure
- Centralized setting Access Point function and firmware upgrade.
- APs Group management for concept.

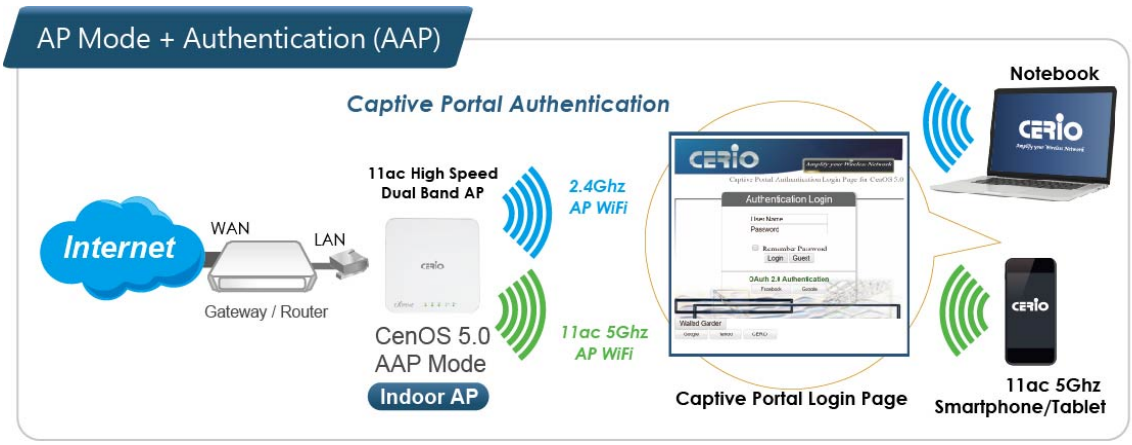


Access Point Mode (Supports AP+WDS Mode)

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





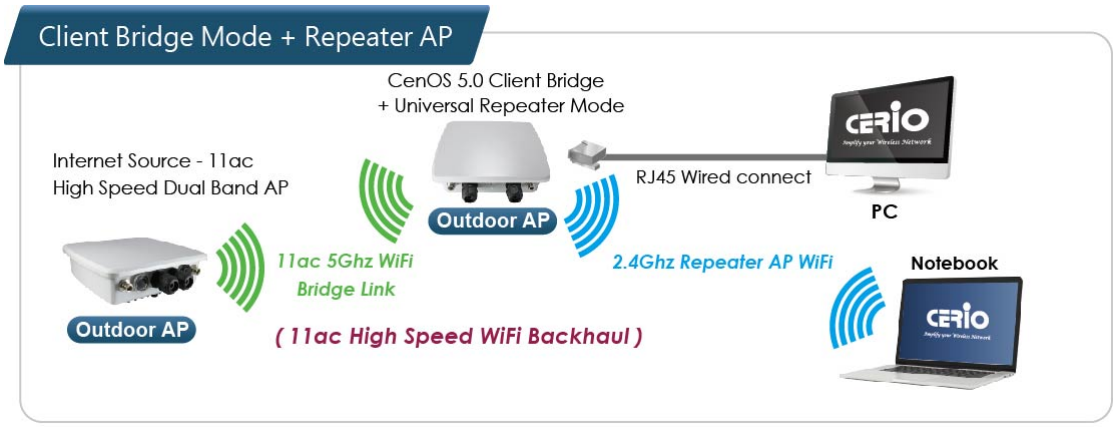


Client Bridge + Repeater Mode

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

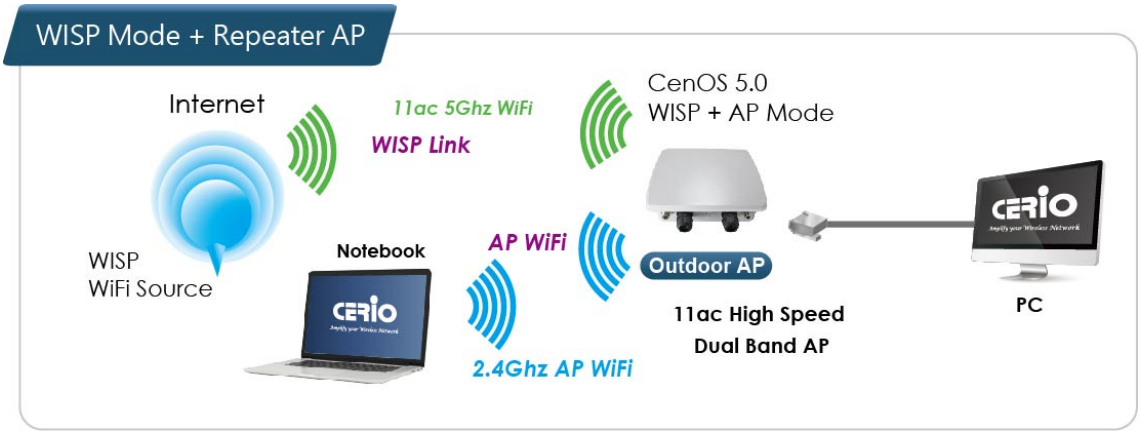
Notice

Relevant to dual-band devices ONLY: If client bridge uses the 5Ghz band, then the Repeater AP can only use the 2.4Ghz band.



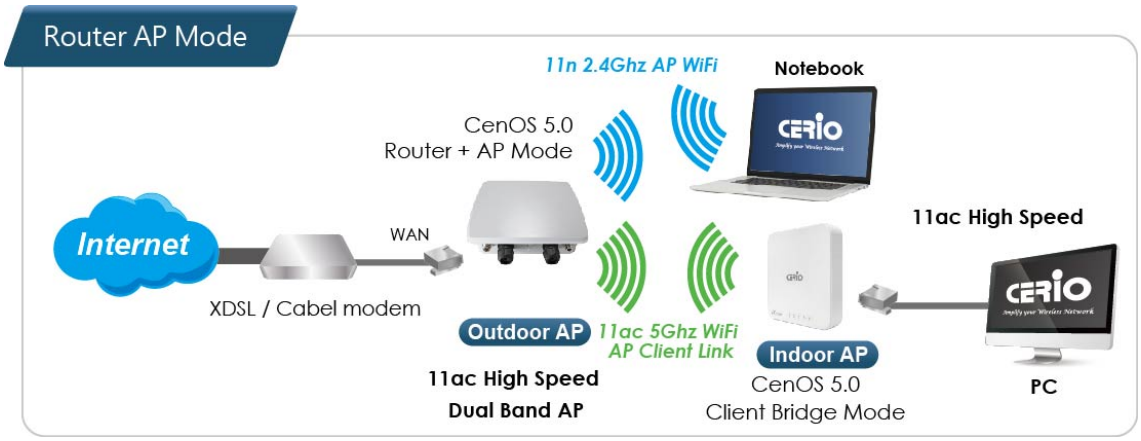
WISP + Repeater AP Mode

- It can be used as an WISP/Outdoor Customer Premises Equipment (CPE) to receive wireless signals over last mile application, helping WISPs deliver wireless broadband Internet service to residents and business customers
- In the WISP (CPE) mode, the CenOS 5.0 AP is a gateway enabled with NAT and DHCP Server functions. The wired clients connected to DT-300N are in different subnet from those connected to Main Base Station, and, in WISP (CPE) mode, it does not accept wireless association from wireless clients.



Router AP Mode

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



3. Access Point mode

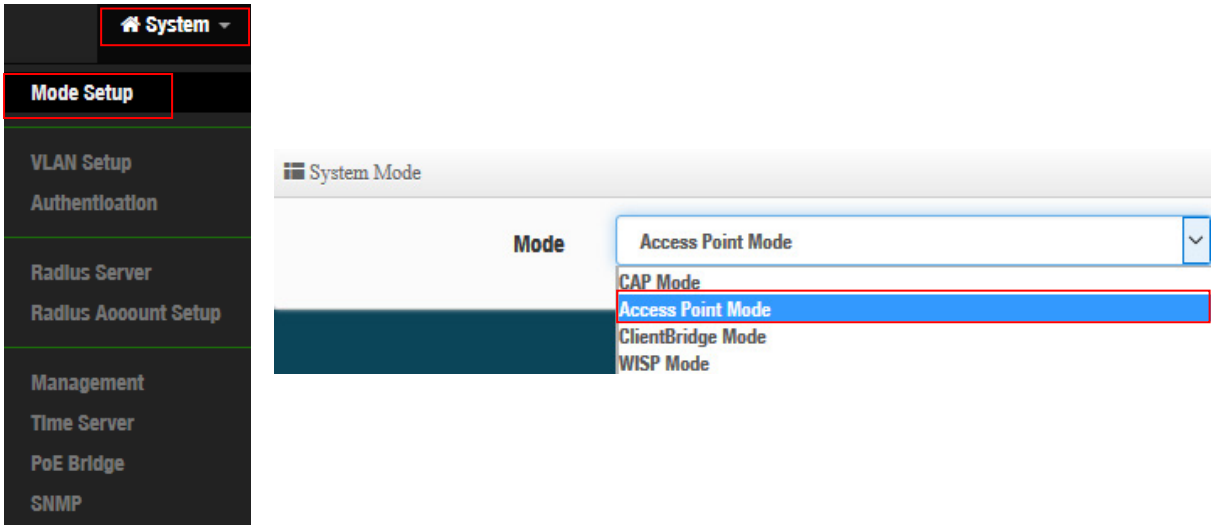
When AP mode is chosen, the system can be configured as an Access Point. This section provides detailed explanation for users to configure in the AP mode with help of illustrations. In the AP mode, functions listed in the table below are also available from the Web-based GUI interface.

3.1 Select AP Mode

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

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

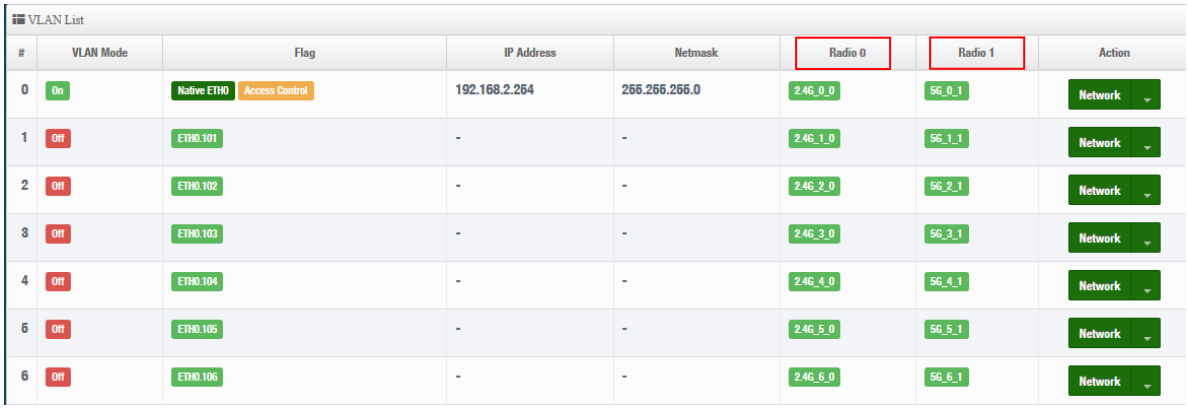
Please click on **System -> Mode Setup** and follow the below setting.



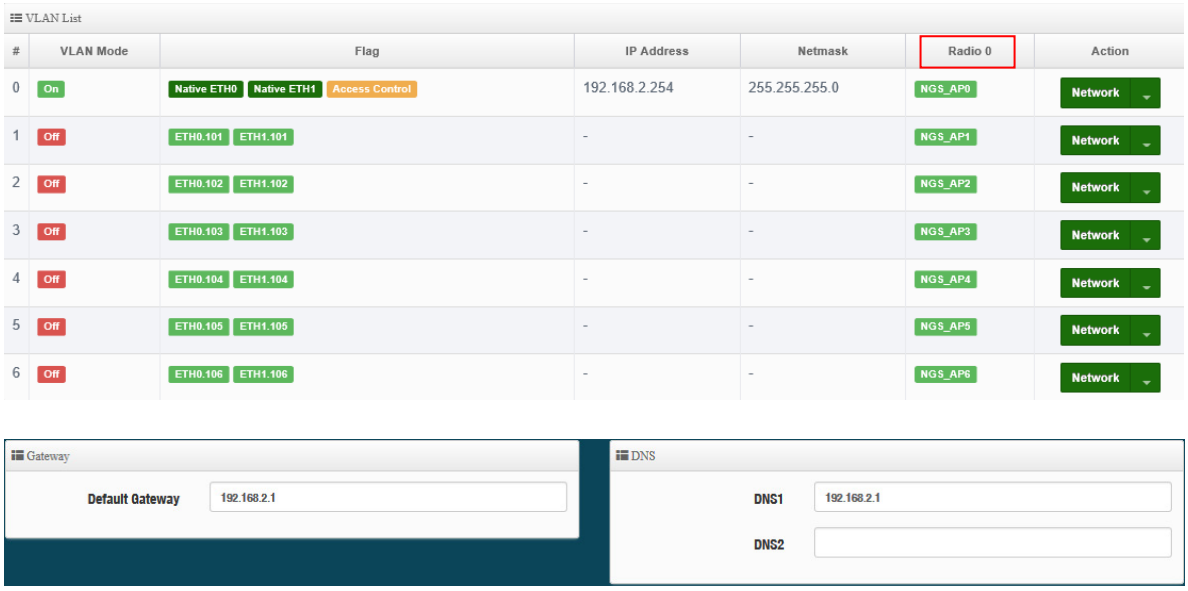
3.2 VLAN Setup

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

Notice 11ac models include dual band radios, support 16 VLANs and up to 32 SSIDs (16 SSIDs per frequency band)



Notice 11n models support 7 VLANs and up to 7 SSIDs

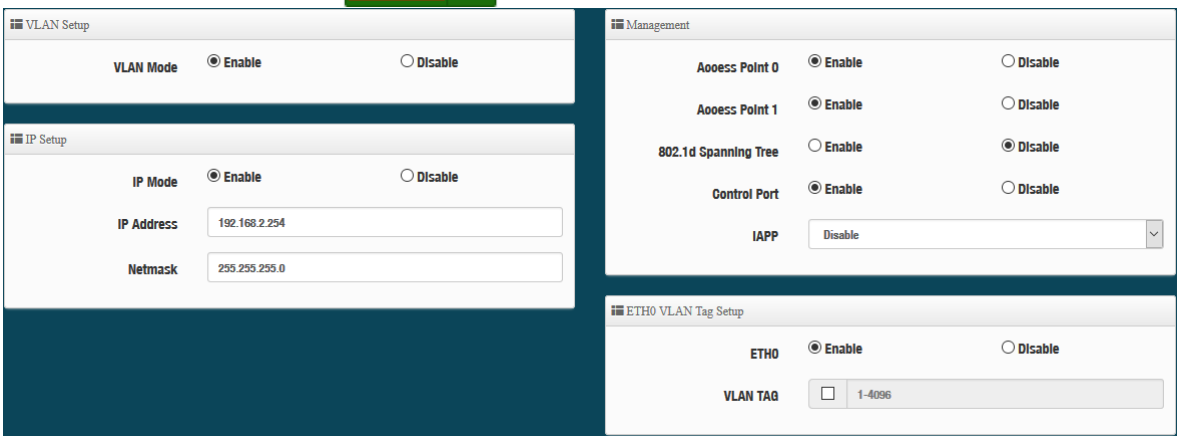


- **VLAN Mode**：Display on/off for the VLAN network.
- **Flag**：Display master VLAN and VLAN Tag No. information.
- **IP Address**：Display IP Address for VLAN Network.

- **NetMask**：Display IP netmask.
- **Radio 0**：Display radio 2.4G or 5GHz SSID name depending on AP model.
- **Radio 1**：Display radio 5G SSID name for 11ac AP models.
- **Action**：The button can set VLAN network functions and radio functions.

3.2.1 Network Button

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



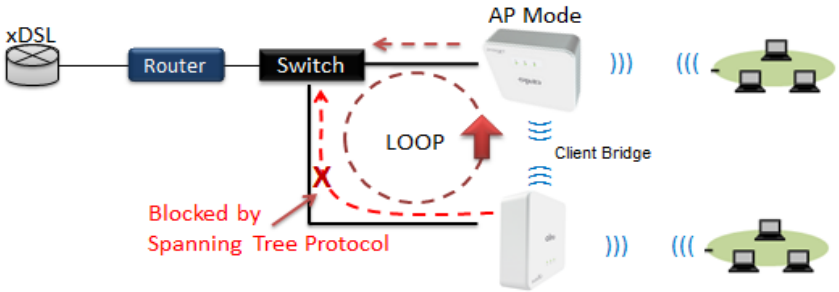
- **VLAN Mode**：Administrator can select Enable or disable for the VLAN Network.

Notice The VLAN list at least one must is enable.

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

Management

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



Client Bridge + Repeater AP

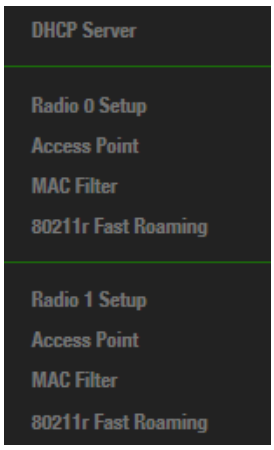
- **Control Port**：Administrator can select one of the VLAN as managed AP.
- **IAPP**：Administrator can select radio 2.4G or 5G for IAPP roaming.*(the IAPP condition must use WPA2-PSK Wi-Fi security and AES algorithm)*

3.2.2 Network Pull-down menu

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

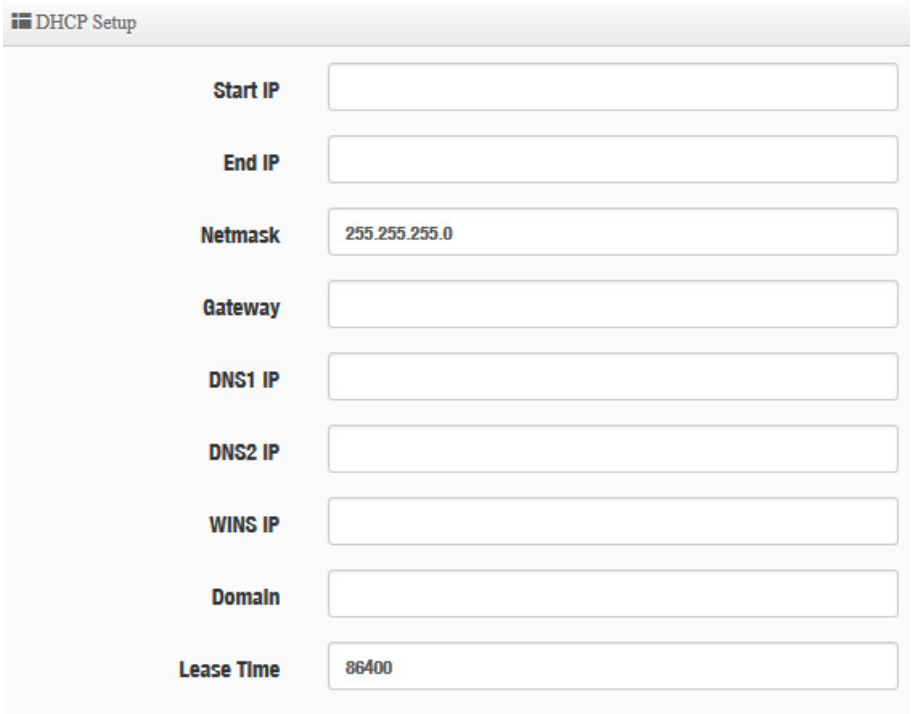
Please click the

pull-down button.



DHCP Server

Administrator can select enable / disable the function

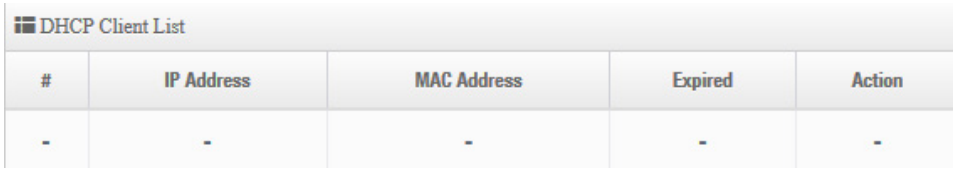


- **Start IP :** Set Start IP for DHCP Service.
- **End IP :** Set End IP for DHCP Service.
- **Netmask: Set IP Netmask, the default is 255.255.255.0**
- **Gateway: Set Gateway IP for DHCP Service.**

- **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.



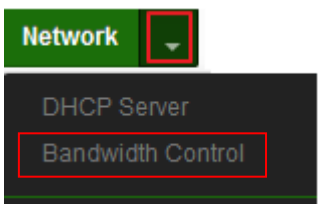
Static Lease IP Setup

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

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

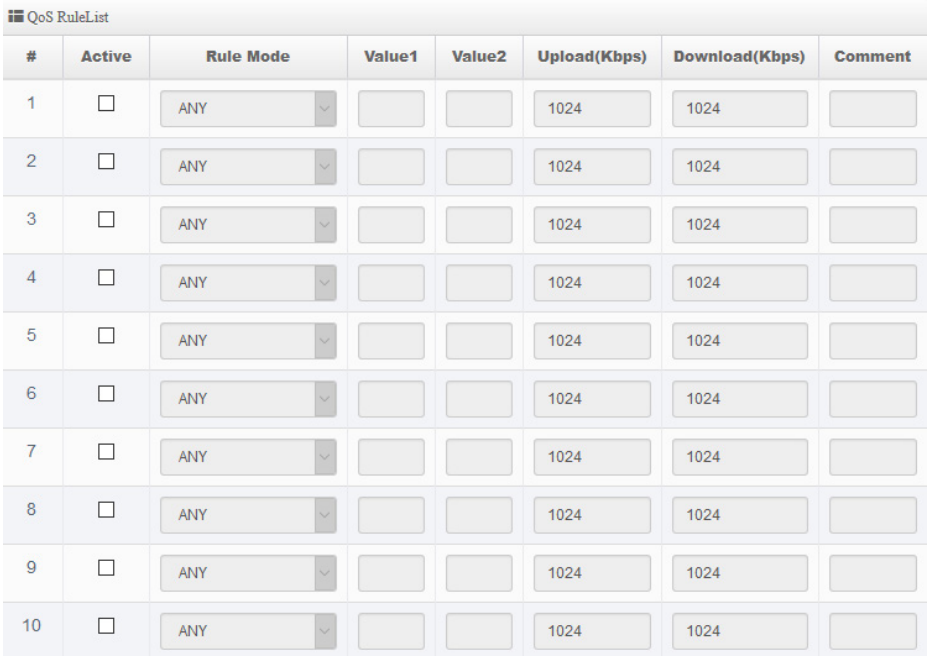
Bandwidth Control

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.



➢ **Mode:** Administrator can select Enable or Disable for the bandwidth control.

- Administrator can set total bandwidth used limit in VLAN.

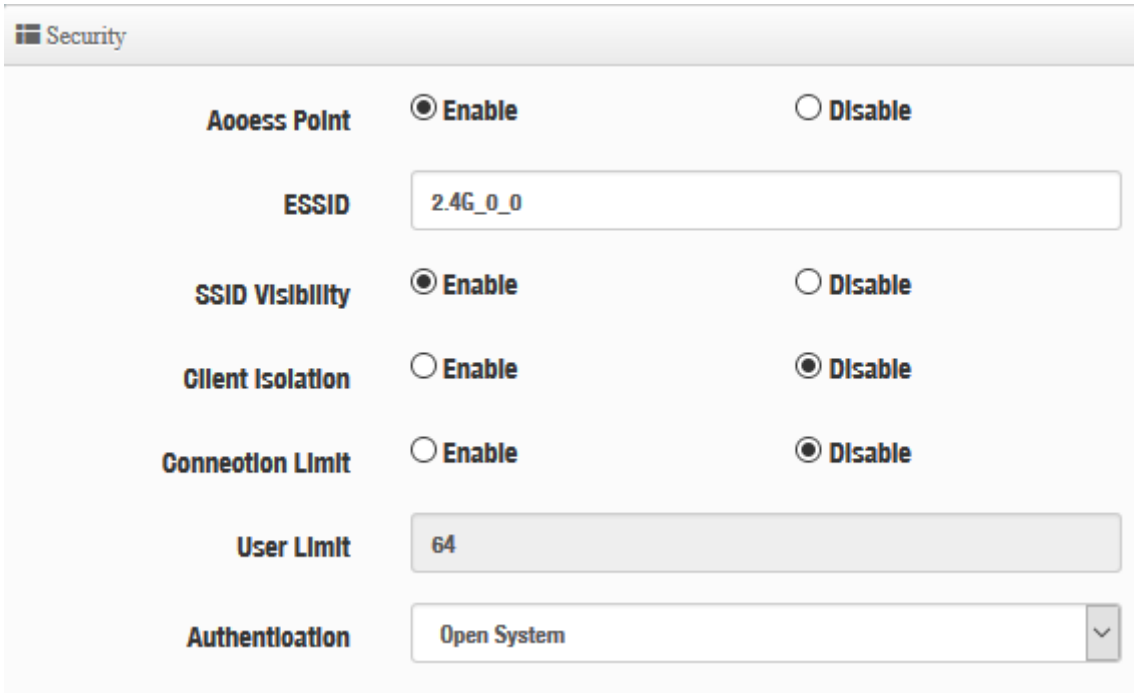


- **QoS Rule List:** Administrator can set bandwidth limit by IP/MASK, IP Range, Port(Service), SIP, RTP/RTSP, WEB protocol , each VLAN can set 10 bandwidth management rule.

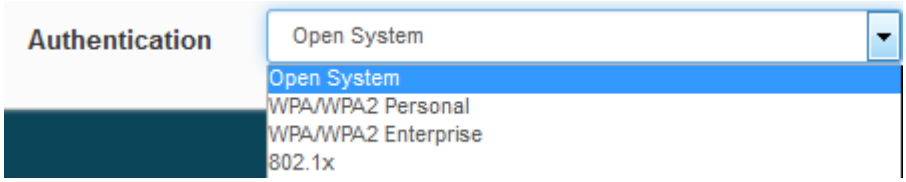
➢ **Airtime Fairness:** This feature can balance Tx/Rx traffic. When administrator enable then system can calculate traffic will try to balance Tx/Rx.

Radio 0/1 Access Point

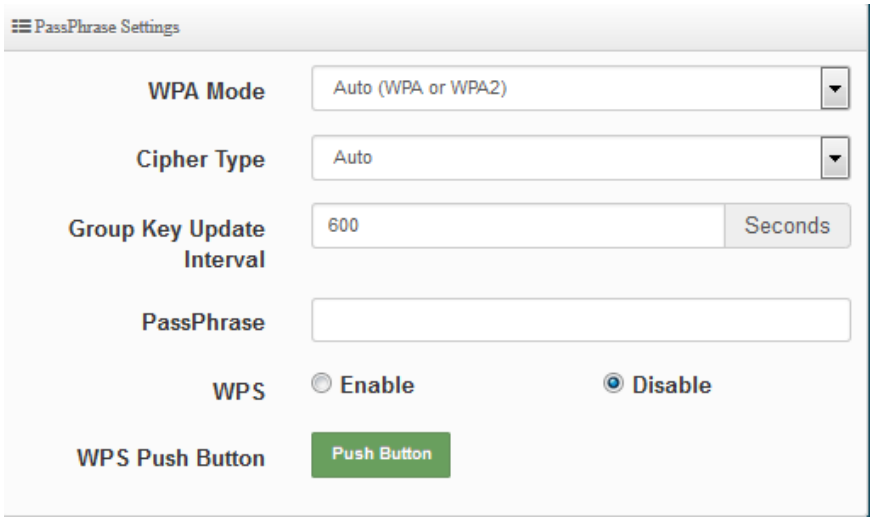
Administrator can Enable or Disable radio 0/1 (2.4/5G) Wi-Fi. If radio 0/1 (2.4/5G) are enabled, administrators can set the SSID and security for the 2.4/5G access point.



- **Access Point:** Administrator can Enable or Disable the radio 0/1 (2.4G/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.
- **Authentication:** Select the desired security type from the drop-down list; the options are WPA-PSK, WPA2-PSK, WPA/WPA2-Enterprise and WEP 802.1X.



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



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

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

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

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

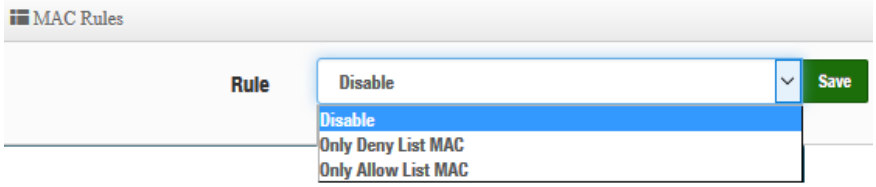
- ● **802.1X security:** When 802.1x Authentication is enabled, please refer to the following Dynamic WEP and RADIUS settings to complete the configuration.

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

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

MAC Filter

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

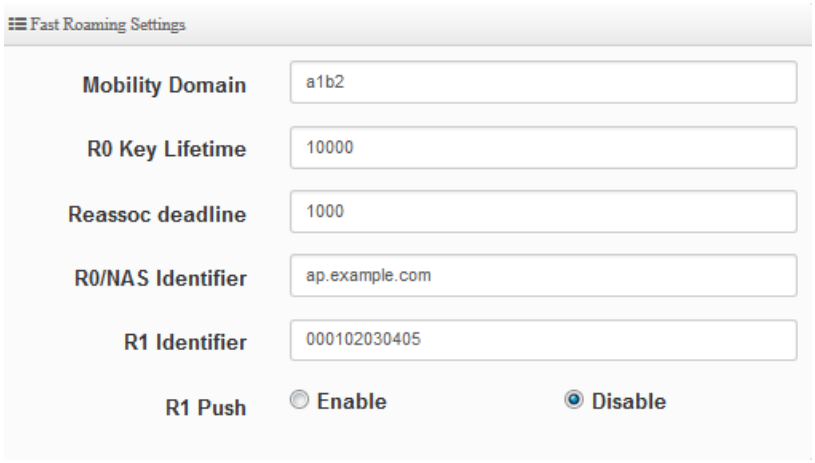


- ➢ **Disable**：Disable MAC Filter function.
- ➢ **Only Deny List MAC**：Administrator can add wireless users MAC address in MAC list. The access point will deny connection in MAC address list.
- ➢ **Only Allow List MAC**：Administrator can add wireless users MAC address in MAC list. The access point will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

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

802.11r/802.11k Fast Roaming

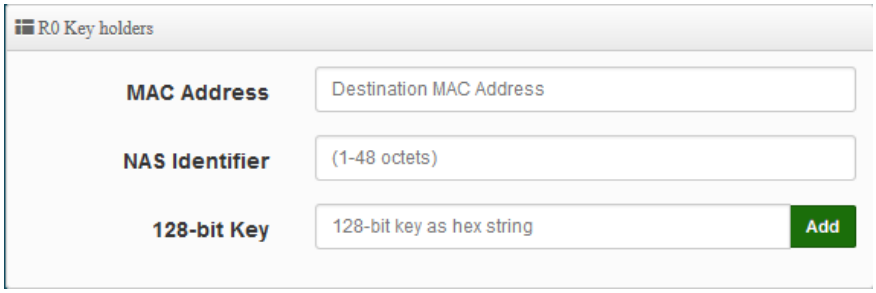
The dual band Access Point supports 802.11r/802.11k function for 2.4G and 5G radio. 802.11r, which is the IEEE standard for fast roaming, introduces a new concept of roaming where the initial handshake with the new AP is done even before the client roams to the target AP.



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

R0 Key Address:

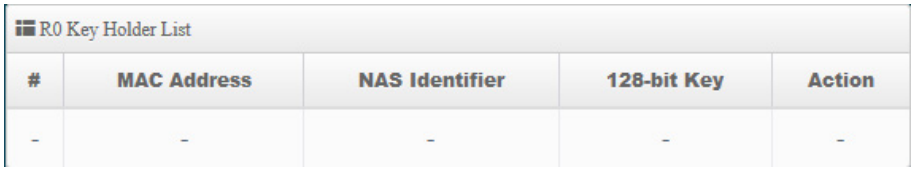
To enable roaming between multiple AP devices, AP1 must key in the MAC Address of AP2, and AP2 must key in the MAC Address of AP1. The NAS Identifier and 128-bit Key should be identical in both AP settings. This will enable device roaming between the two Access Points.



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

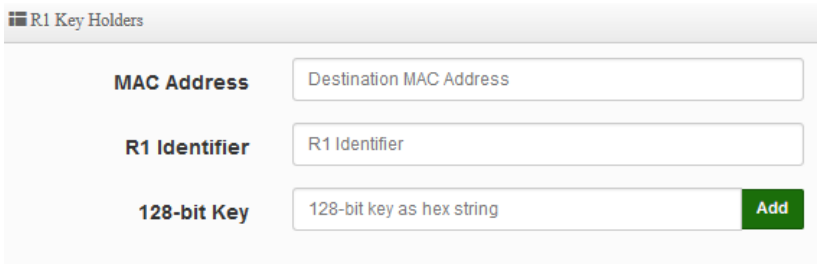
R0 Key Holder List:

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



R1 Key Holder List:

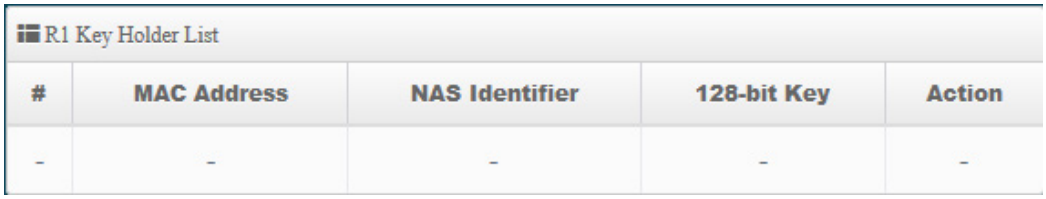
Enter a unified set of R1 Key Holder identification certification.



- **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.

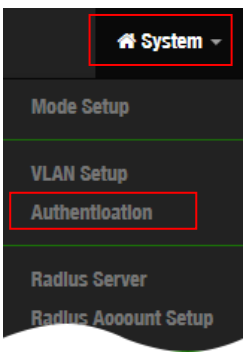


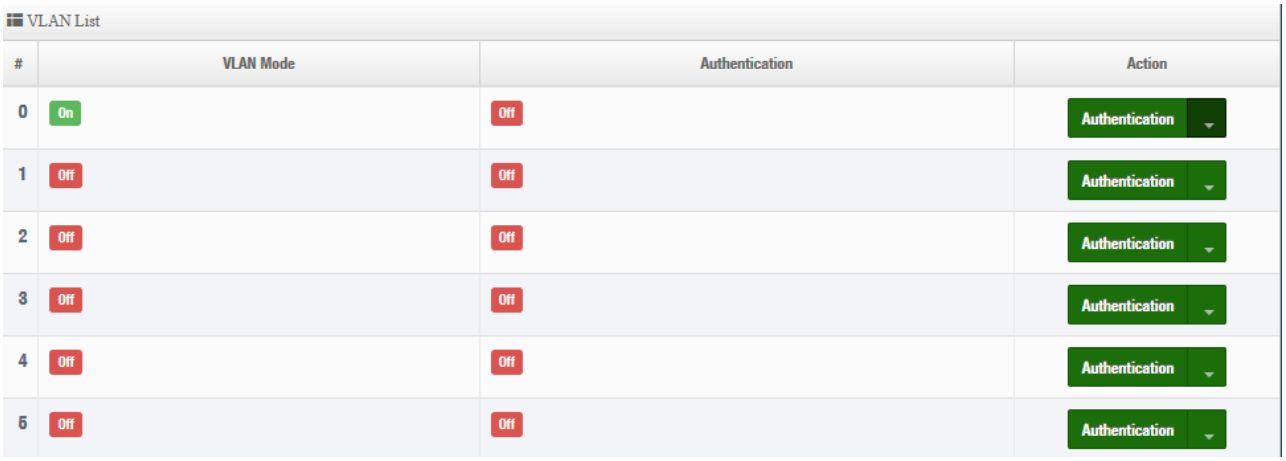
Click "**Save"** button to save your changes. Then click **Reboot** button to activate your changes.

3.3 Authentication

The function is for Web Authentication. It supports authentication for local users / RADIUS Server / OAuth2.0 and Guest. The system supports up to **16 VLANs for 11ac models** and up to **7 VLANs for 11n** models with web authentication.

Please click on **System -> Authentication**

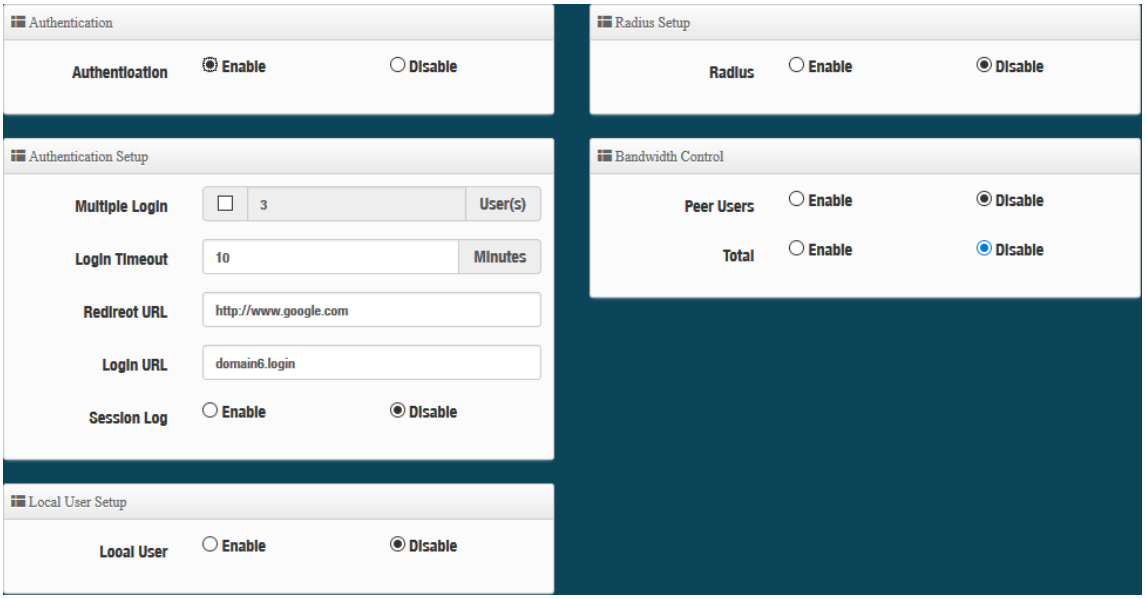




- **#**：Display **16 VLANs for 11ac models** or **7 VLANs for 11n models**.
- **VLAN Mode**：Displays VLAN on/off status.
- **Authentication**：Displays VLAN# whether enable or disable web authentication.
- **Action**：The function has 2 buttons (Authentication and Dropdown)

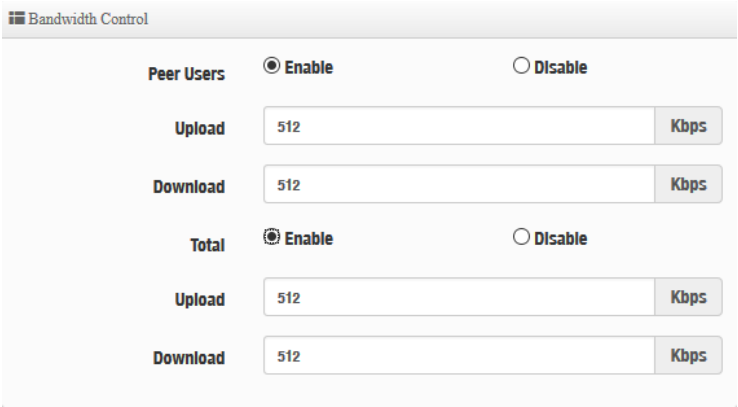
Authentication Button:

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



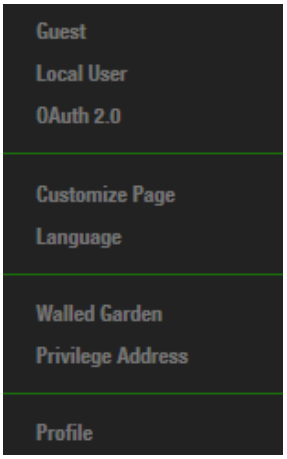
- **Authentication**：Administrator can enable or disable authentication function.
- **Multiple Login**：Administrator can set one account to multiple users simultaneously login and the users can set limit.(0 = not limited)
- **Login Timeout**：After account login for some time no traffic, system will automatic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

- **Redirect URL**：After the success of the login, system will redirect to URL. Administrator can enter web site URL.
- **Login URL**：Administrator can set URL for login page.
- **Session Log**：If network have Syslog server. Administrator can to system➔management setting IP address for syslog server and enable the function. Account session log will copy to syslog server.
- **Local User**：Administrator can enable authentication for local user. Create user account can to reference **"3.3.2 Local User".**
- **RADIUS**：Authentication support remote RADIUS Server. Administrator can enter security information for remote RADIUS Server.
- **Bandwidth Control**：Administrator can be control traffic by Users or total.



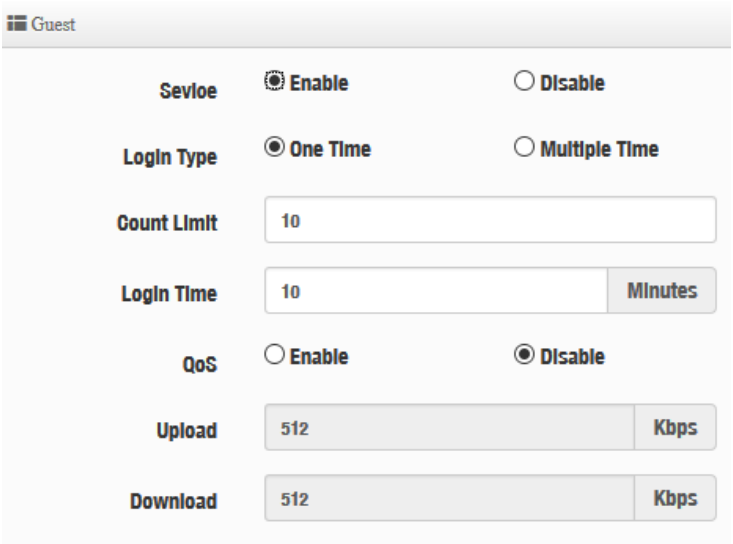
Authentication Dropdown Button

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



3.3.1 Guest

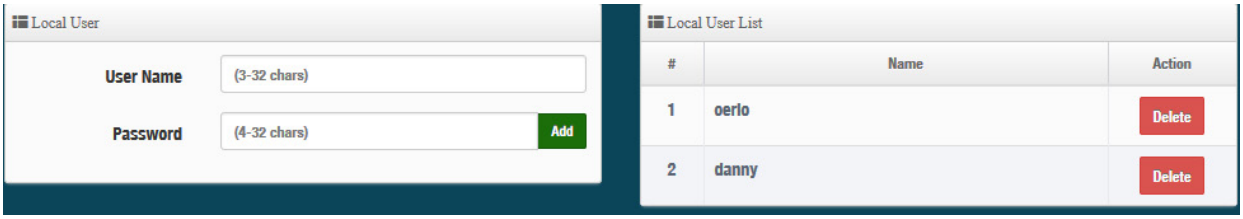
Administrator can enable or disable guest authentication. If enabled, the administrator can set guest Count Limit / login time and type and flow control.



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

3.3.2 Local User

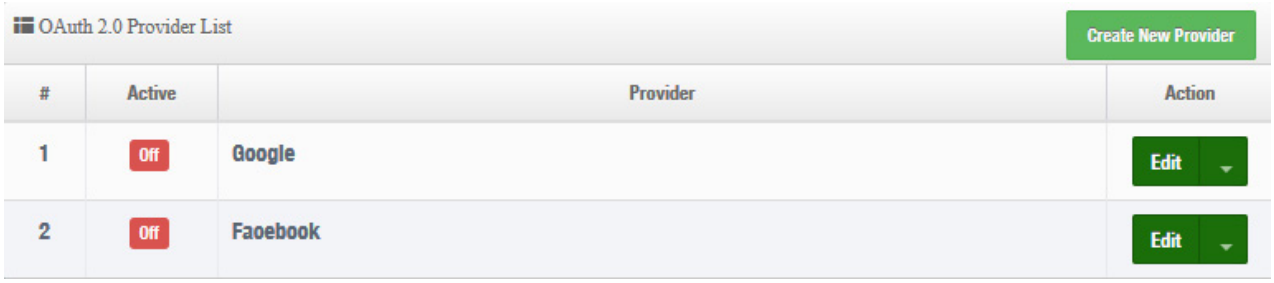
Administrator can create local user account for web login.



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

3.3.3 OAuth2.0

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



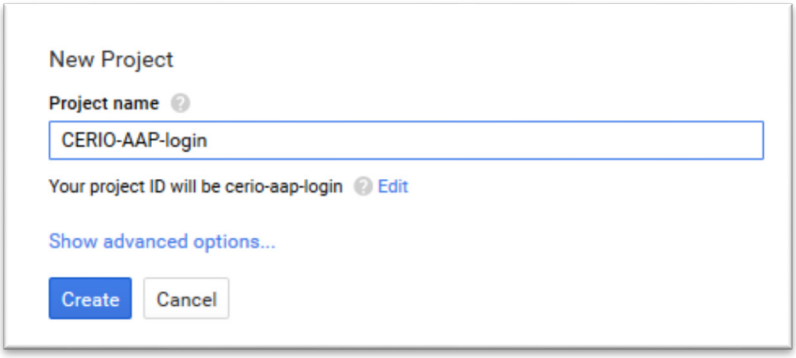
- **#**：Display items.
- **Active**：Display on/off status for the authentication.
- **Provider**：Display authentication server. The system default use authentication server for Google and Facebook

※ Sample for Google OAuth2.0 setup

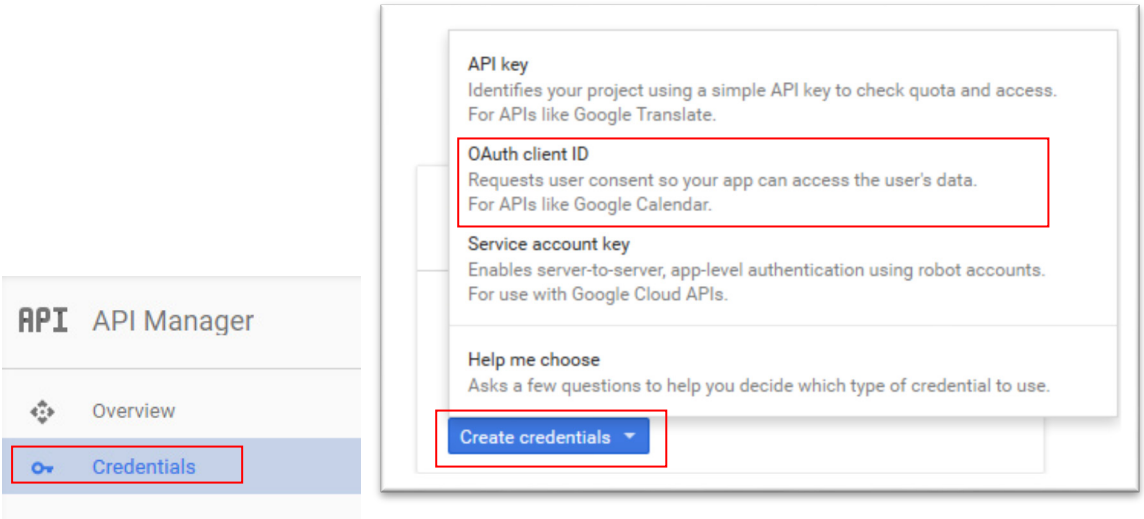
Please complete the application on the Google website to receive an account ID and password, follow the steps below.

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

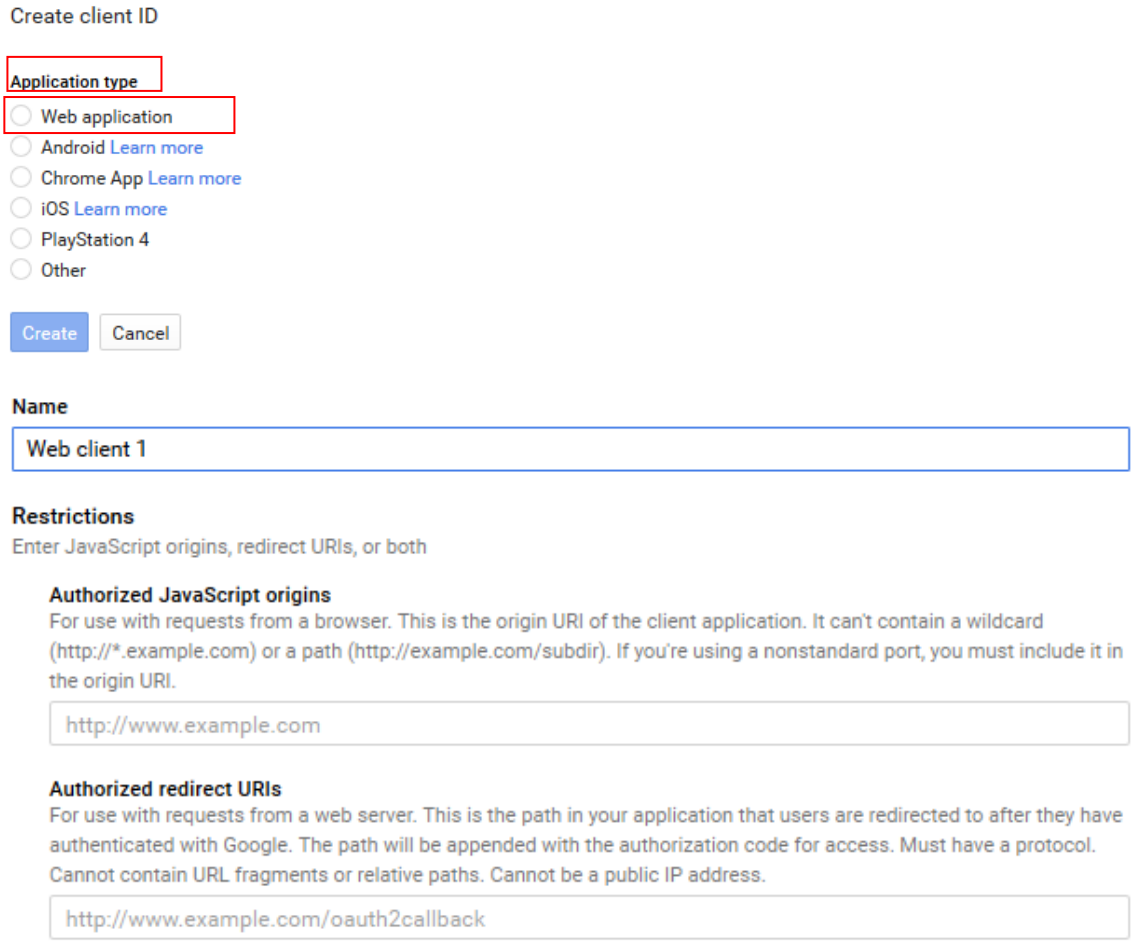
(Reference https://developers.google.com/identity/protocols/OAuth2)



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



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



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

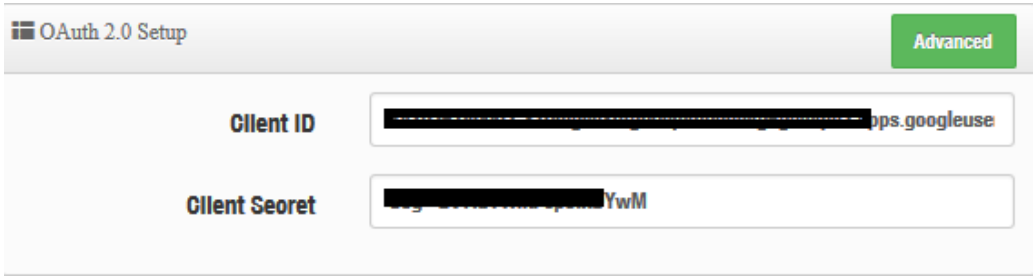
Administrator must set login URL in the device function. After complete set of login URL go to the **"Restrictions"** function in web page. Follow the steps below to set login URLs

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

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

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

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.

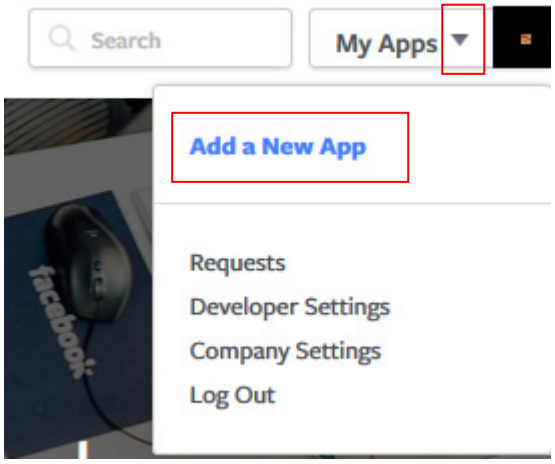


Save and reboot the AP system, complete the setup.

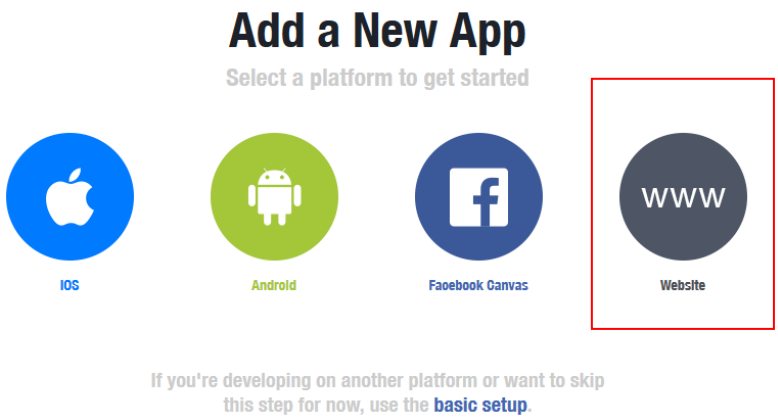
※ Sample for Facebook OAuth2.0 setup

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

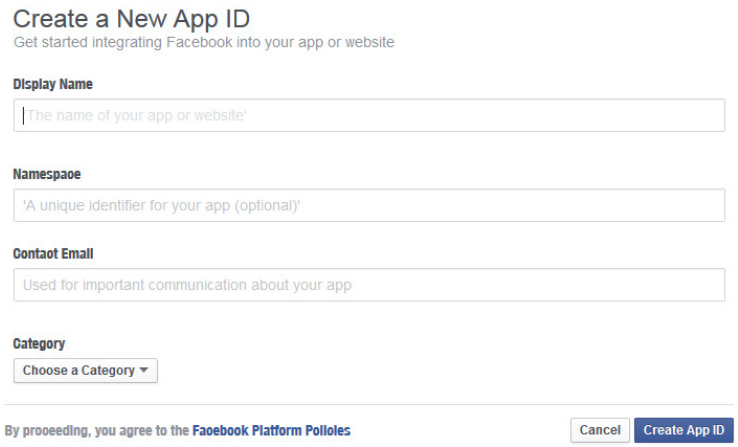
Step.1 Please to Facebook developer's page and add a New App



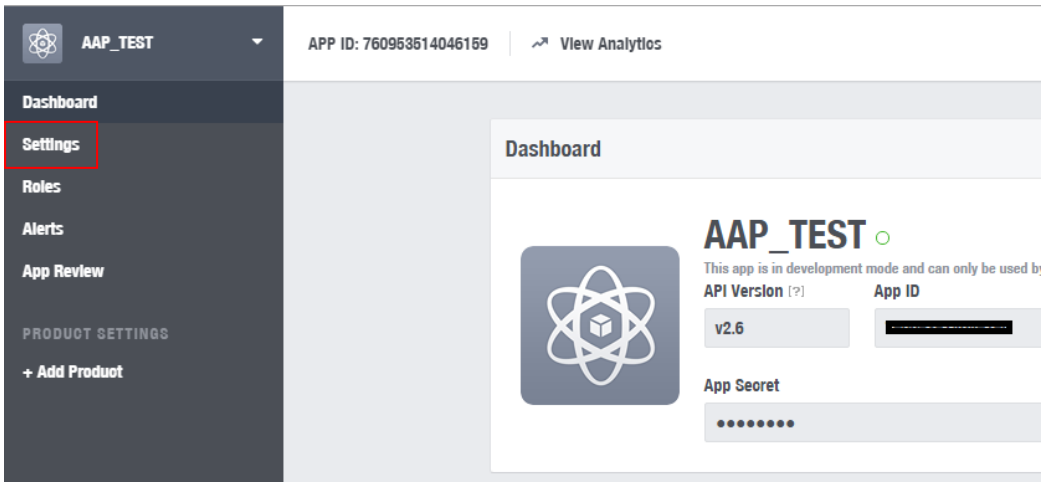
Step.2 Select WWW function



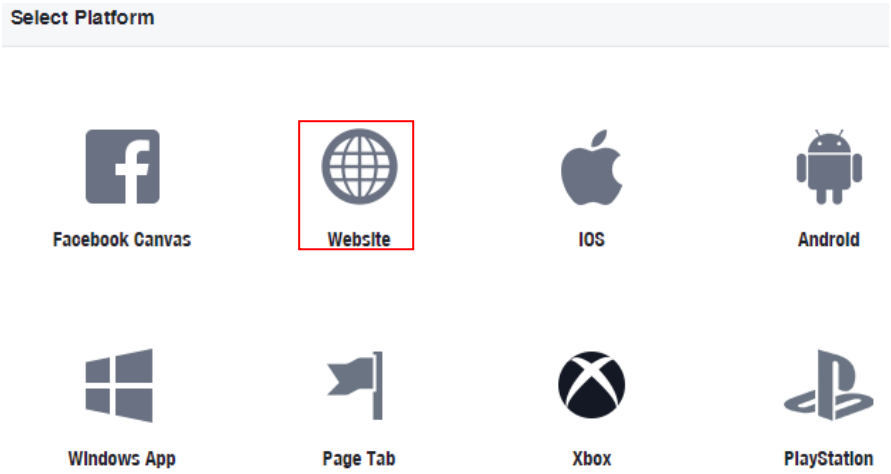
Step.3 Administrator must set www for your information.



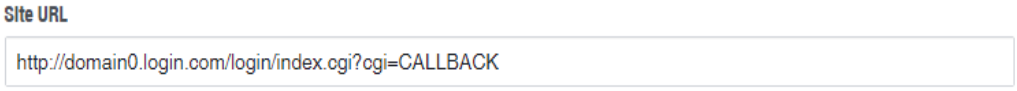
Step.4 Please click **"Setting"** and add Platform



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

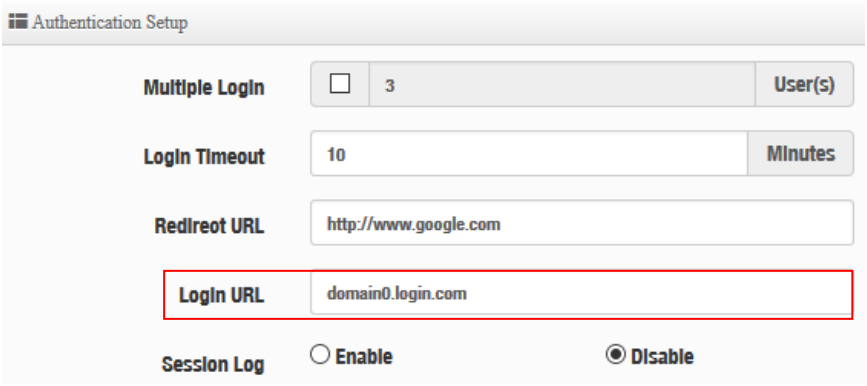


Step.6 Enter URL is **http://domain0.login.com/login/index.cgi?cgi=CALLBACK**



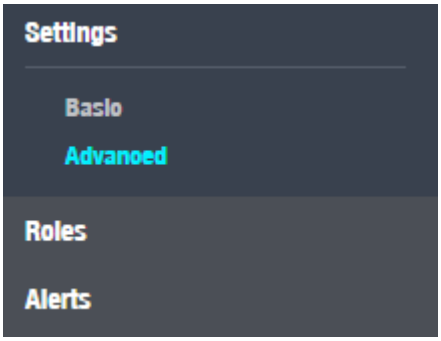
Administrator must set login URL in the device function. After complete set of login URL go to the "**Facebook** Site URL" function in web page. Follow the steps below to set login URLs

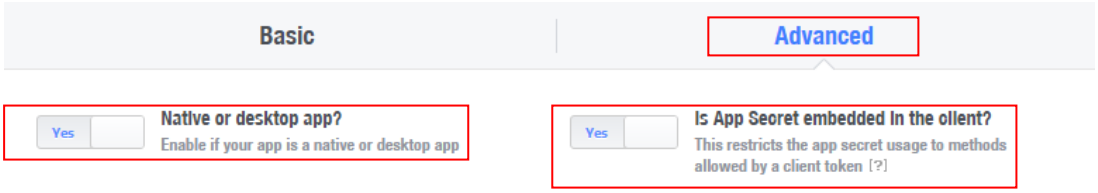
- Setup login URL in the device. Please Click **system➔Authentication** and enable the function.
- The **"Authentication Setup"** page to set Login URL



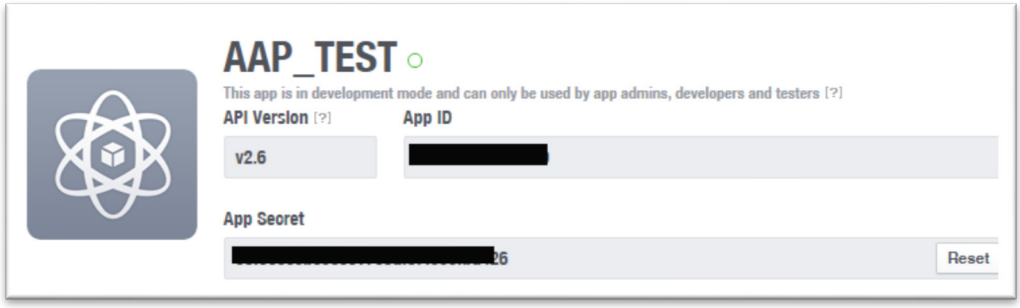
After complete set of login URL go to the "**Facebook** Site URL" function in web page. Copy and paste the login URL from the system display into the "Site URL" page on the Facebook website.

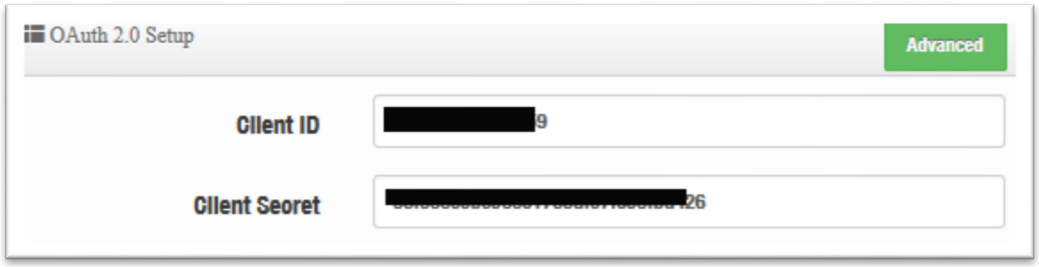
Step.7 Click Advanced function to enable the **"Native or desktop app?"** and **"Is App Secret embedded in the client? "**





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.



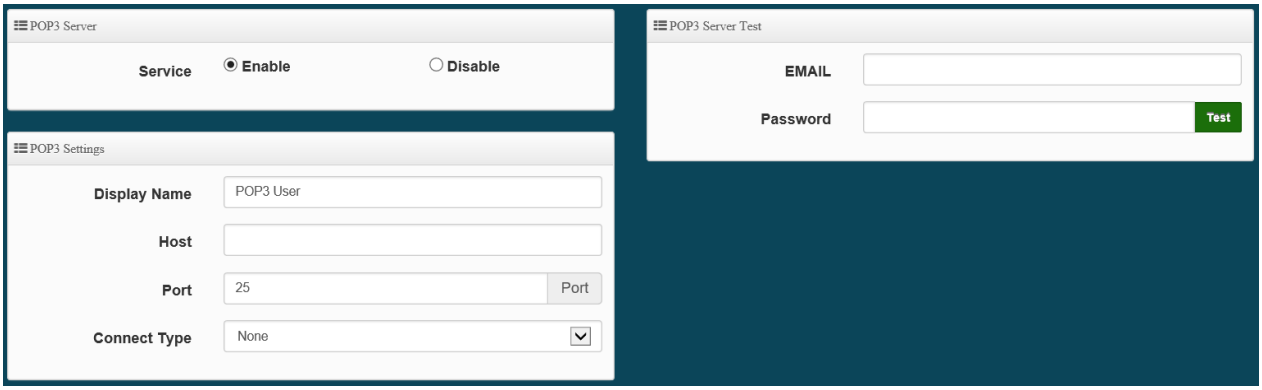


Notice

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.

3.3.4 POP3 Server

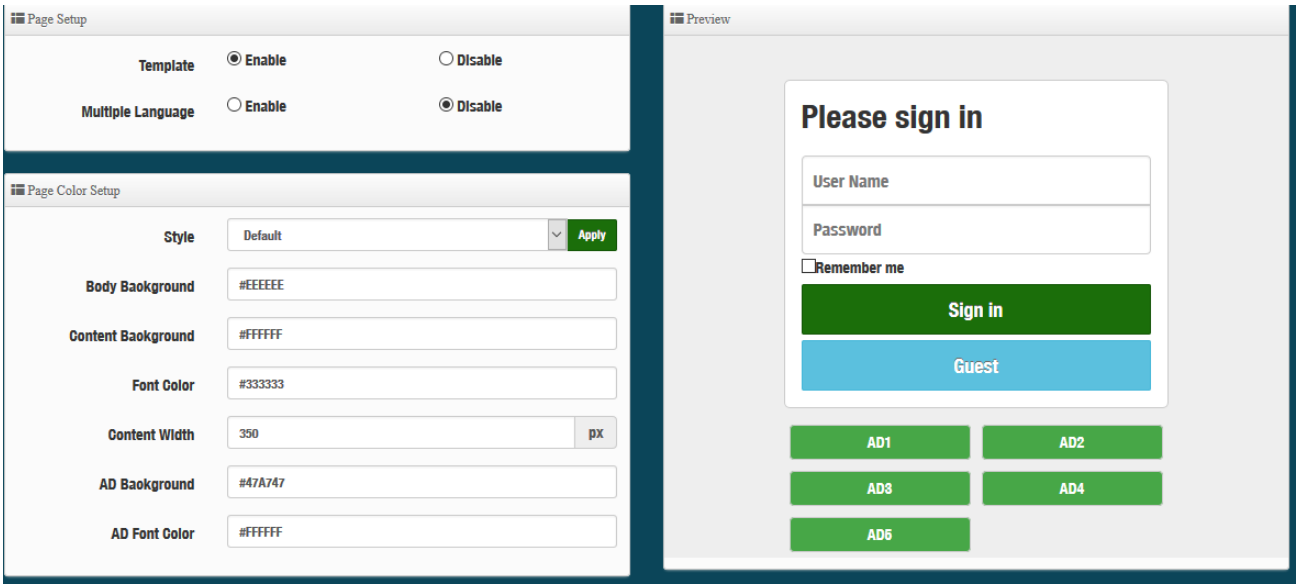
The purpose of this integrated function is to allow clients to link a POP3 server for receiving emails from a remote server.



- **POP3 Server**：Click “Enable” or “Disable” to activate this function
- **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

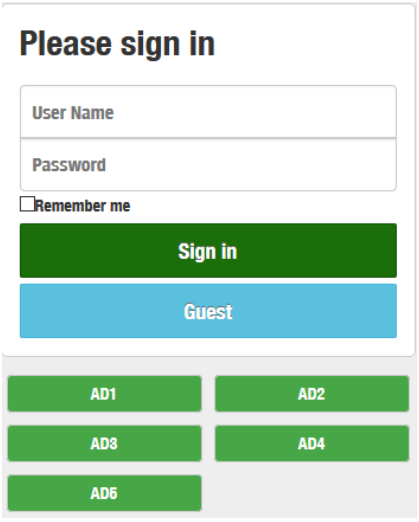
3.3.5 Customize Page

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

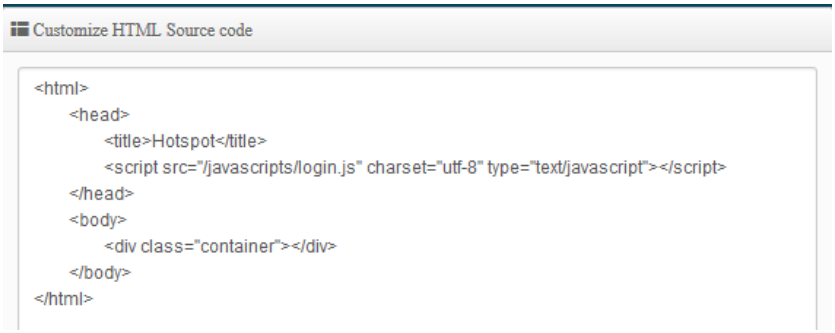


Page Setup

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



  - Select disable to active HTML Source code window for customization



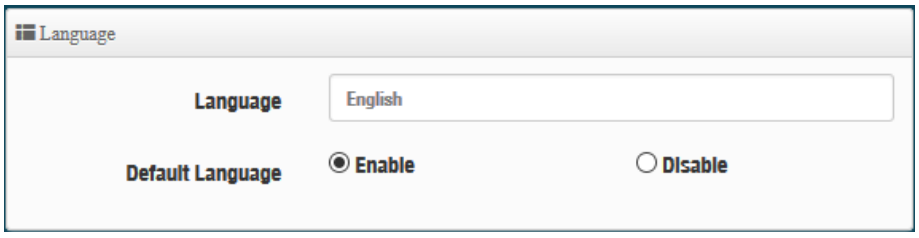
Sample: See sample login page below that is customized by html coding *(sample login page html code templates are available on Cerio website)*

The following function uses the enabled Template

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

3.3.6 Language

Administrator can create other language for login page.



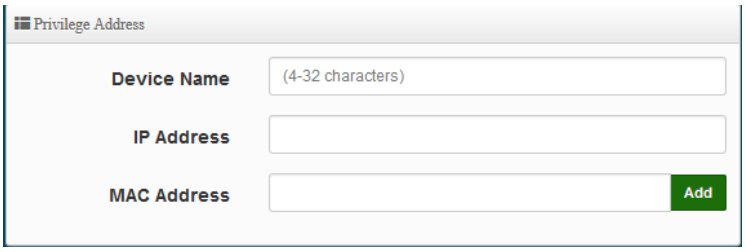
3.3.7 Walled Garden

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.

3.3.8 Privilege Address

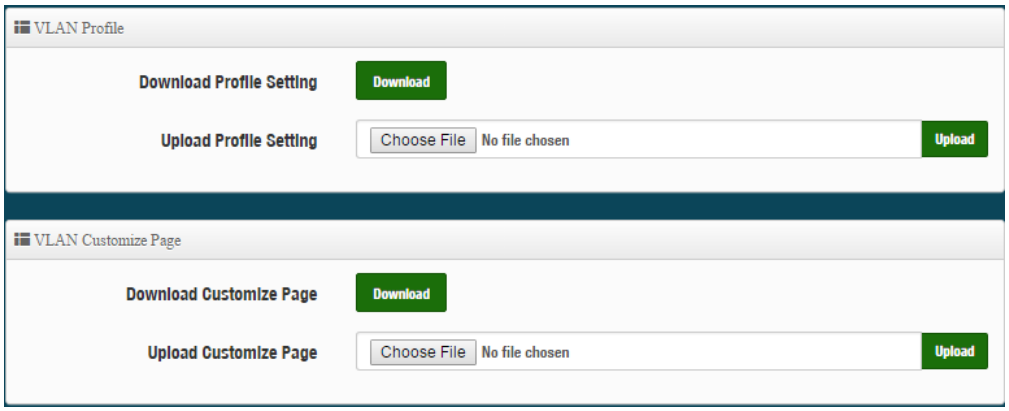
This function provides local device can access Internet without authentication. If there are some workstations belonging NGS Access Point that need to access to network without authentication, enter the IP or MAC address of these workstations in this list.



- **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.

3.3.9 Profile

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



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

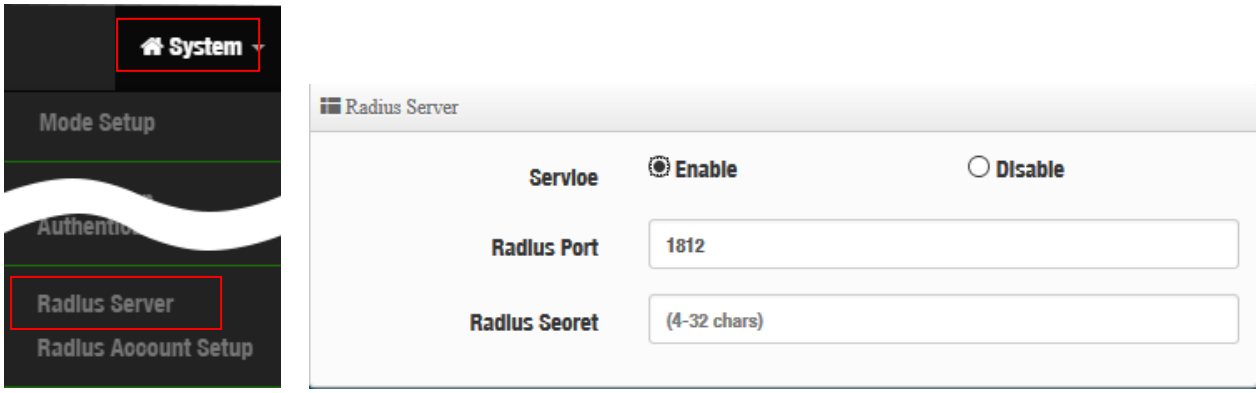
3.4 RADIUS Server

Notice

Only 11ac devices support built-in RADIUS Server. All other 11n models do not support this function.

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

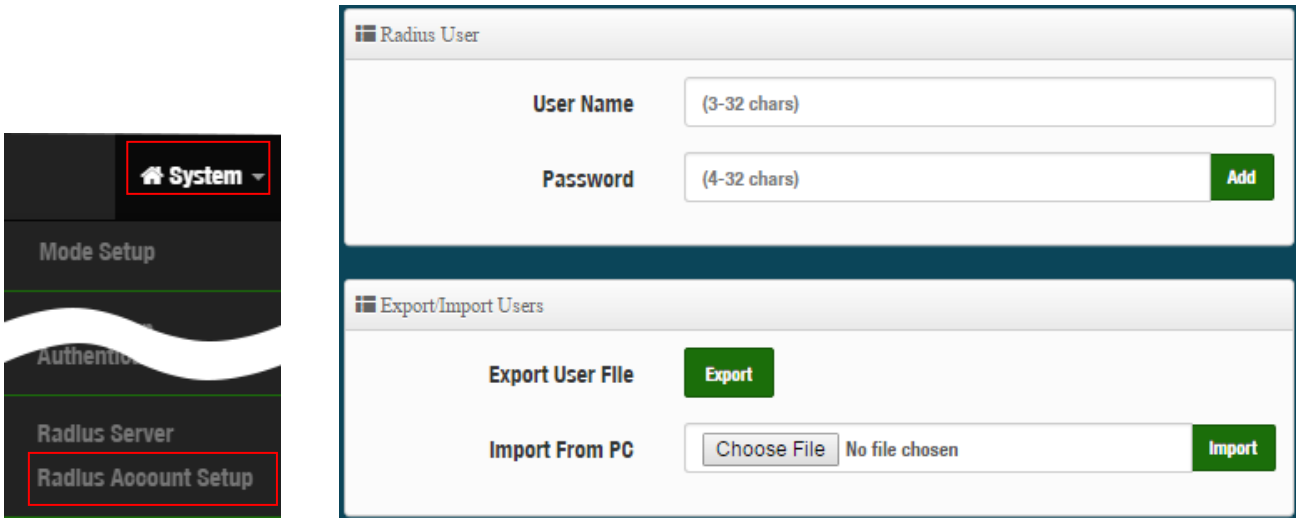
Please click on **System** ➔ **RADIUS Server**



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

3.5 Radius Account Setup

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



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

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

3.6 Wireless Basic Setup

Notice

The following displays dual band device user interfaces. Single band 11n devices will only include Radio 0 settings in the software interface

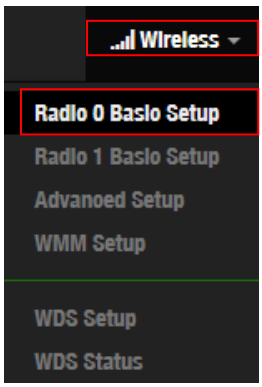
Note:

1. If the product used is dual band then Radio 0 is 2.4G / Radio 1 is 5G
2. If the product used is pure 2.4G then only Radio 0 (2.4G)
3. If the product used is pure 5G then only Radio 0 (5G)

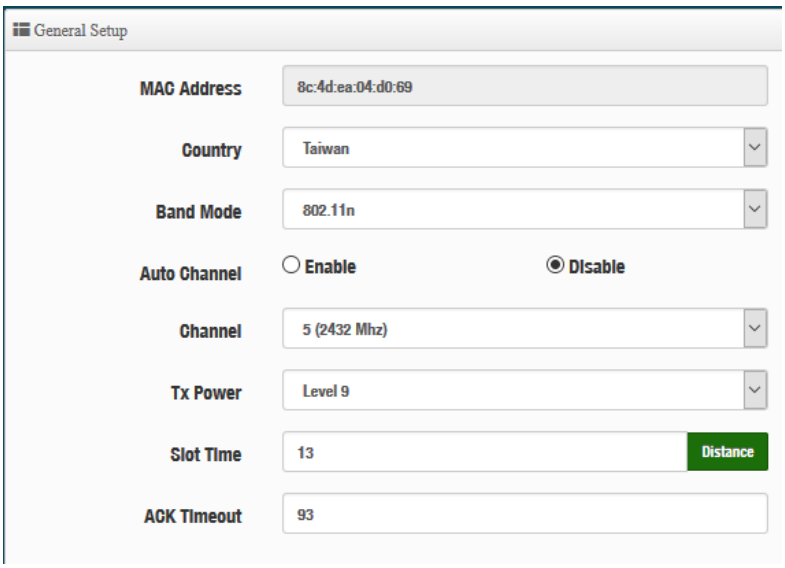
Wi-Fi band mode please according to the product data sheet

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

3.6.1 Radio 0 Basic Setup (2.4G)



General setup



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

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

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

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

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

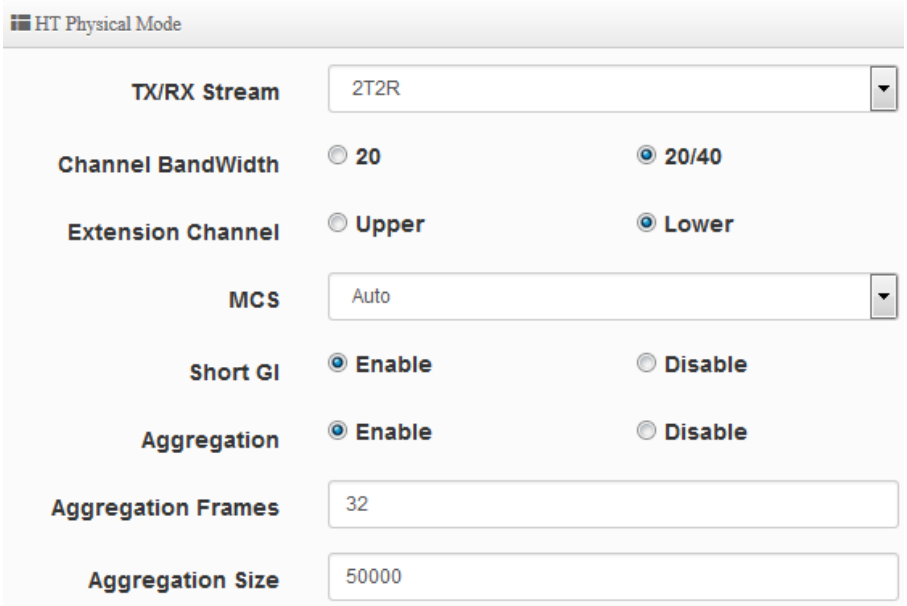
ACK Timeout is adjustable due to the fact that distance between two radio links may vary in different deployment. ACK Timeout makes significant influence in performance of long distance radio link. If ACK Timeout is set too short, transmitter will start to “Resend” packet before ACK is received, and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

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

Notice

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

HT Physical Mode



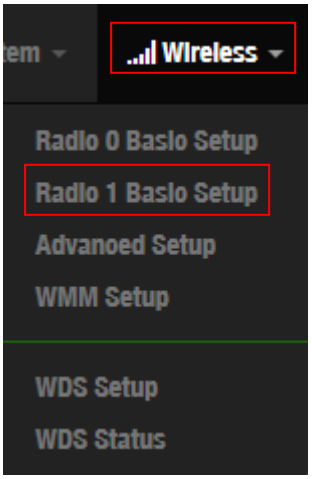
- **TX/RX Stream:** The CenOS 5.0 AP utilizes 2 antenna and supports 2TX/2RX streams. Administrator can select 1 or 2 TX/RX. The default is 2TX/2RX.
- **Channel Bandwidth:** The "**20/40**” MHz option is usually best. The other option is available for special circumstances.

Notice

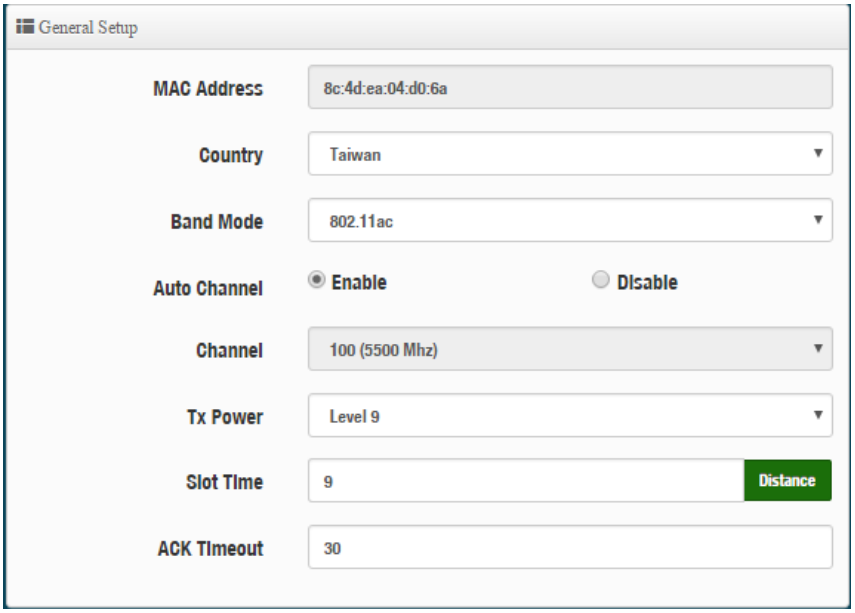
If select 20/40 mode then max Data rate limit is 300Mbps in wave1 chip, if device use wave2 chip then max data rate is 400Mbps.

- **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:** The Aggregation Frames is in the range of **2~64**, default is **32**. It determines the number of frames combined on the new larger frame.
- **Aggregation Size:** The Aggregation Size is in the range of **1024~65535**, default is **50000**. It determines the size (in Bytes) of the larger frame.

3.6.2 Radio 1 Basic Setup (5G)



General Setup



- **MAC Address:** Display 2.4G WiFi MAC address.
- **Country:** Administrator can select country: US or EU or Taiwan.
- **Band Mode:** Administrator can select 5G Band for 802.11a/n or 802.11ac. The default is 802.11ac
- **Auto Channel:** Administrator can Enable or Disable the function. If select disabled function the WiFi channel can be manually fixed.
- **Channel:** Supports US and EU country 5G Channel standards.
- **Tx Power:** Administrator can control the WiFi Tx output power. The power Max. Level 9.
- **Slot Time:** Slot time is in the range of **9~1489** and set in unit of ***microsecond***. The default value is **9** microsecond.

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

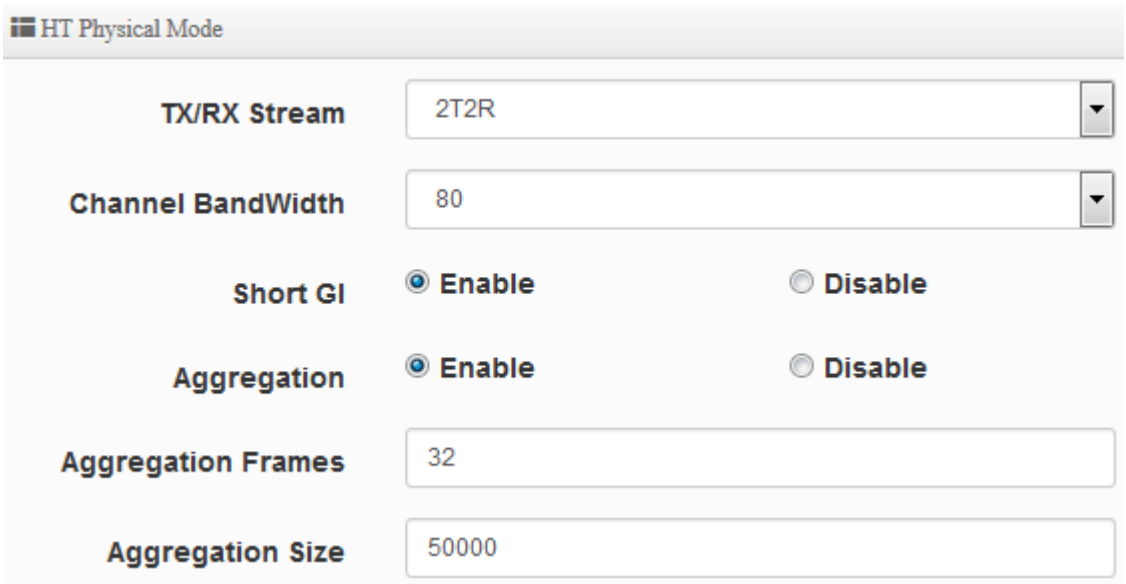
All data transmission in 802.11b/g request an “Acknowledgement” (ACK) send by receiving radio. The transmitter will resend the original packet if correspondent ACK failed to arrive within specific time interval, also refer to as “ACK Timeout”.

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

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

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

HT Physical Mode



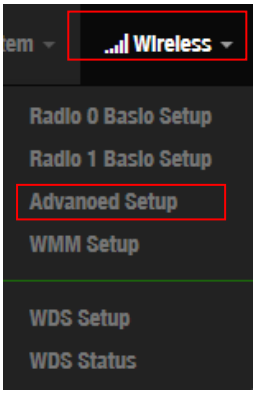
- **TX/RX Stream:** The CenOS 5.0 AP utilizes 2 antennas and supports 2TX/2RX streams. Administrator can select 1 or 2 TX/RX. The default is 2TX/2RX.
- **Channel Bandwidth:** The "**20/40 and 802.11ac 80**” MHz option is usually the best. The other option is available for special circumstances.
- **Shout 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.

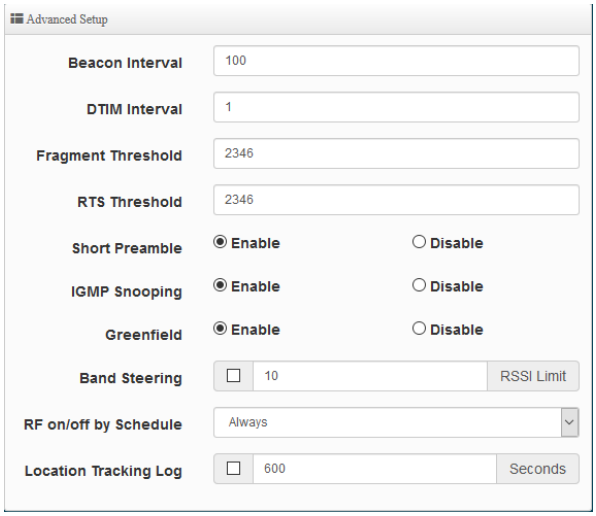
- **Aggregation:** By default, it's "**Enable**". Select "Disable" to deactivate Aggregation.
  A part of the 802.11n standard (or draft-standard). It allows sending multiple frames per single access to the medium by combining frames together into one larger frame. It creates the larger frame by combining 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.
- **Aggregation Frames:** The Aggregation Frames is in the range of **2~64**, default is **32**. It determines the number of frames combined on the new larger frame.
- **Aggregation Size:** The Aggregation Size is in the range of **1024~65535**, default is **50000**. It determines the size (in Bytes) of the larger frame.

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

3.6.3 Advanced Setup

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





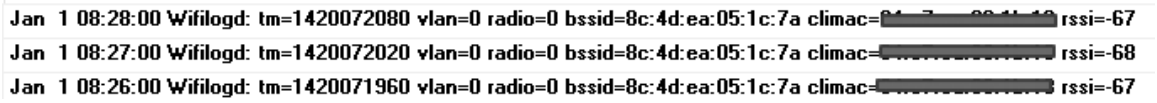
- **Beacon Interval:** Beacon Interval is in the range of **40~3500** and set in unit of *millisecond*. The default value is **100** msec.
  Access Point (AP) in IEEE 802.11 will send out a special approximated 50-byte frame, called "Beacon". Beacon is broadcast to all the stations, provides the basic 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 Steering (Dual Band Models ONLY):** Band Steering detects clients capable of 5 GHz operation and steers them to that frequency which leaves the more crowded 2.4 GHz band available for legacy clients. This helps improve end user experience by reducing channel utilization, especially in high density environments. The default RSSI Limit :10
- **RF on/off by schedule:** Wi-Fi(RF) signal on/off by schedule. Administrator can set time schedule in "system➔Time Schedule" function.
- **Location Tracking Log:** This function can provide the distance (RSSI calculation) information of the wireless user and the local wireless base station to the remote database for analysis.

  Client information as follow



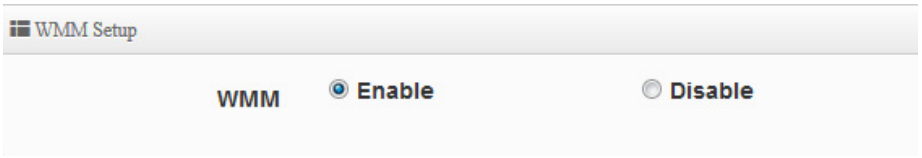
3.6.4 WMM Setup

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

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

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

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



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

WMM Parmameters of Access Point

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

WMM Parmameters of Station

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

✓ **AC Type**：

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

✓ **CWmin**：

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

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

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

✓ **TxOP Limit**：Transmission Opportunity is an interval of time when a WME AP has the right to initiate transmissions onto the wireless medium (WM). This value specifies (in milliseconds) the Transmission Opportunity (TXOP) for AP; that is, the interval of time when the WMM AP has the right to initiate transmissions on the wireless network. ◦

✓ **ACM bit**：Admission Control Mandatory, ACM only takes effect on AC_VI and AC_VO. When you do not click Checkbox, it means that the ACM is controlled by the connecting AP. If you click Checkbox, it means that the Client is in charge ◦

✓ **No ACK policy bit**：Acknowledgment Policy, WMM defines two ACK policies: **Normal ACK** and **No ACK**. Click "**Checkbox**" indicates "**No ACK**"

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

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

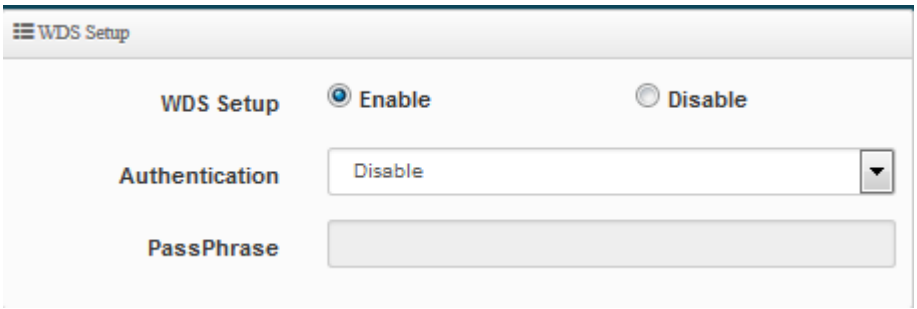
When the Normal ACK policy is used, the recipient acknowledges each received uncast packet. ◦

3.6.5 WDS Setup

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

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

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



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

WDS Client Setup

Radio 0(2.4G)		Radio 1(5G)	
Enable	MAC Address	Enable	MAC Address
☐		☐	
☐		☐	
☐		☐	
☐		☐	
☐		☐	
☐		☐	
☐		☐	
☐		☐	

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

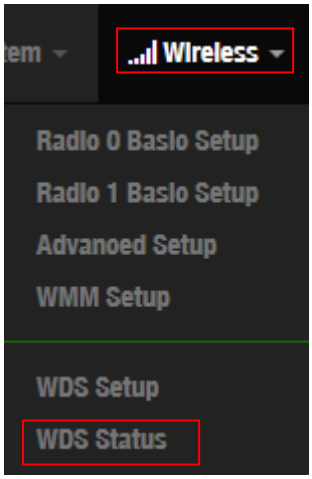
VLAN Setup

	Radio 0			Radio 1		
VLAN#	Native	TAG	TAG ID	Native	TAG	TAG ID
VLAN 0	◉	☐		◉	☐	
VLAN 1	○	☐	101	○	☐	101
VLAN 2	○	☐	102	○	☐	102
VLAN 3	○	☐	103	○	☐	103
VLAN 4	○	☐	104	○	☐	104
VLAN 5	○	☐	105	○	☐	105
VLAN 6	○	☐	106	○	☐	106
VLAN 7	○	☐	107	○	☐	107

3.6.6 WDS Status

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

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



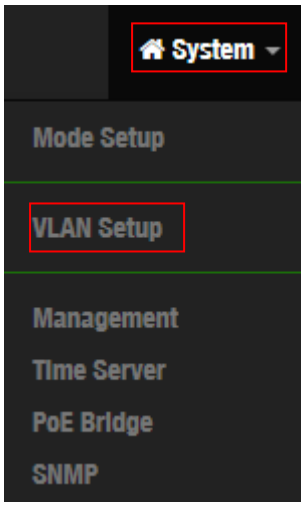
4. CAP Mode

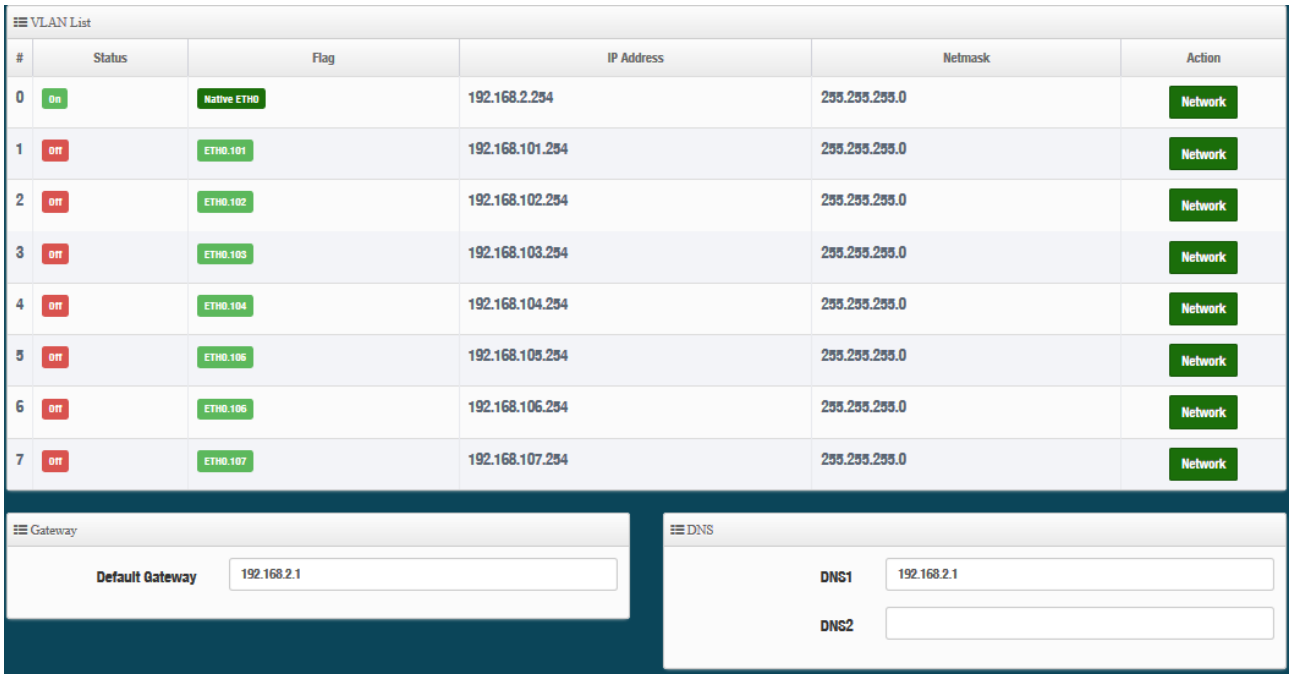
The CAP mode itself isn't Access Point. This mode is primarily to control all the managed AP.

4.1 System VLAN Setup

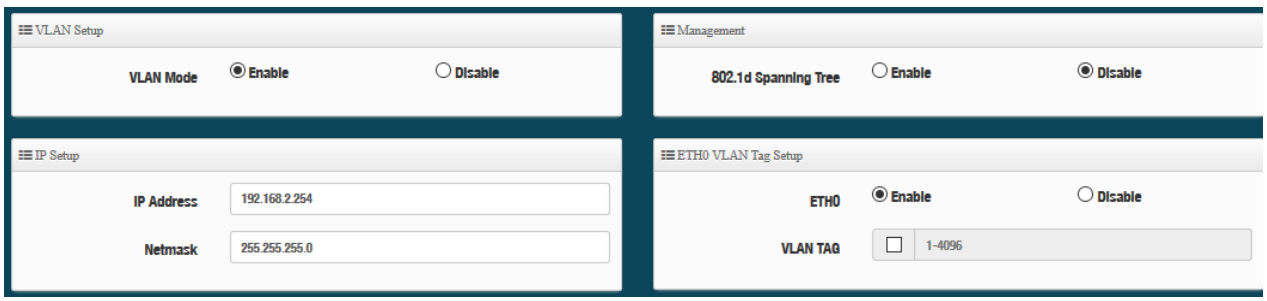
Setup Control AP of LAN or VLAN IP Address, Gateway, DNS and Ethernet Tag etc.

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





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

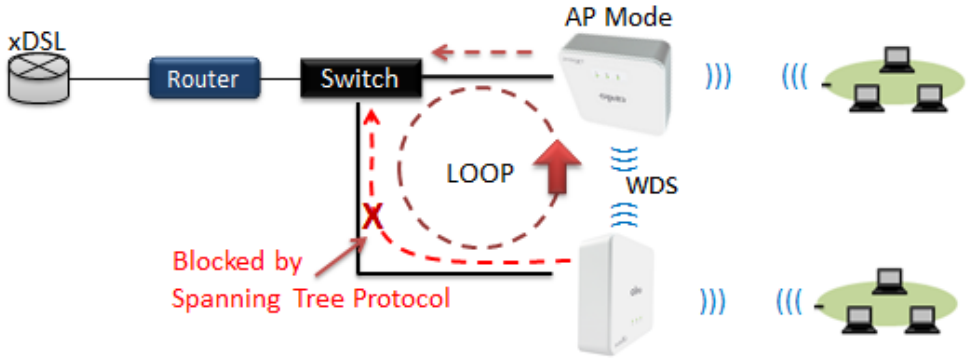


- **VLAN Mode**：Administrator can Enable or disable the VLAN function.

Notice

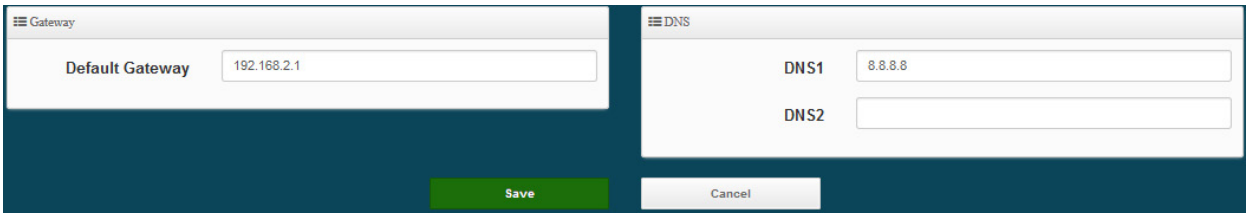
There must always be at least one VLAN enabled. If the administrator disables all the VLANs, he/she will not be able to login to the manager page. The administrator must then reset to default.

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



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

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

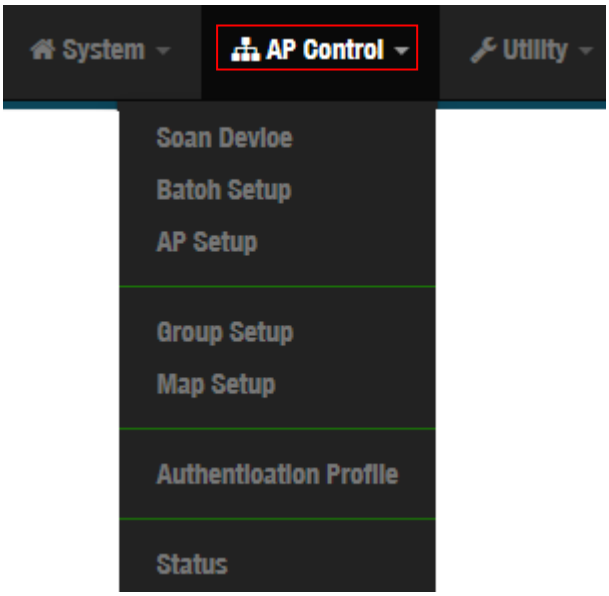


- **Gateway:** The default Gateway IP Address is 192.168.2.1, Please check your Gateway IP and change.
- **DNS**: Check either "**No Default DNS Server**" or "**Specify DNS Server IP**" button as desired to set up the system DNS.
  - ✓ **Primary**: The IP address of the primary DNS server.
  - ✓ **Secondary**: The IP address of the secondary DNS server.

4.2 AP Control

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

Please click **“AP Control”** to enter AP Management settings

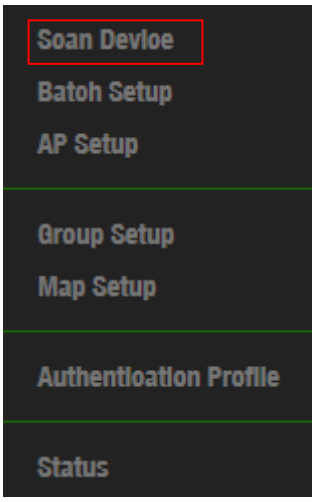


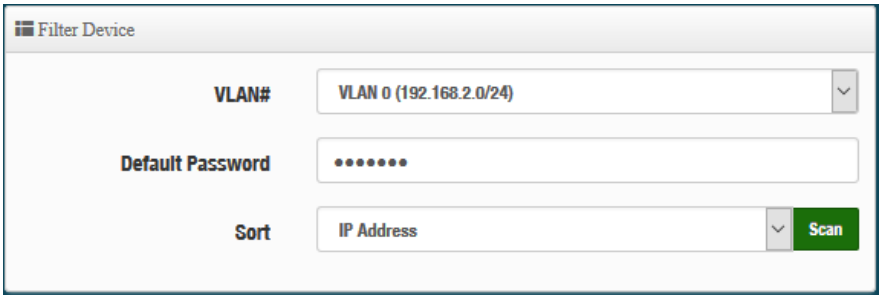
 # Centralized Management APs operating Instructions:

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

4.2.1 Scan Device

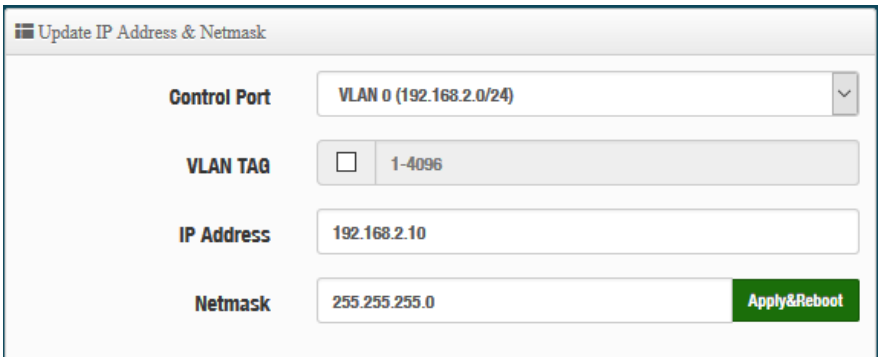
This management page can discover all managed APs in the network. Administrator can set IP address / Password and VLAN tag for managed APs. After the setup is complete, Administrator must import all managed APs to databases.





- **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)

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

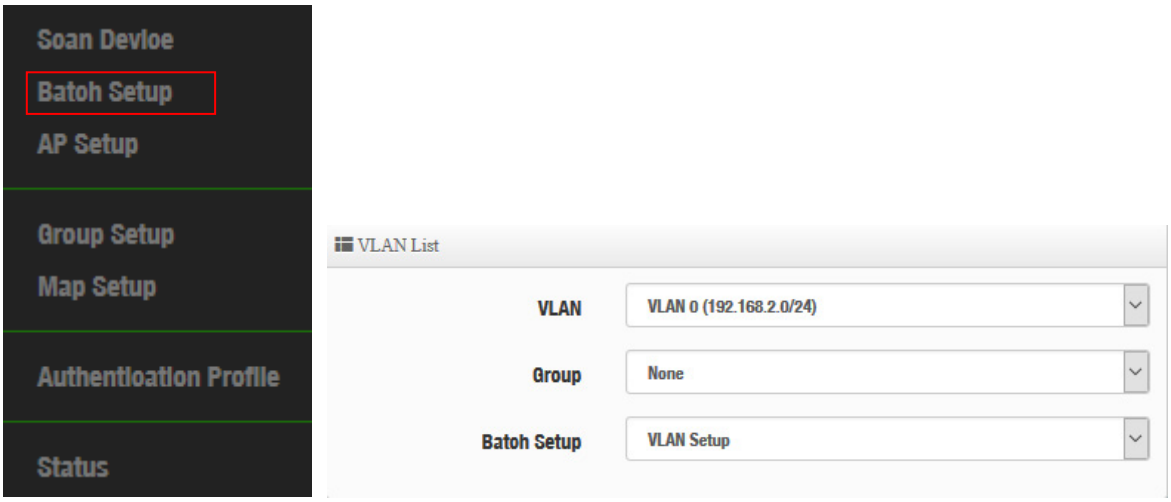


- **Control Port**：Administrator can change VLAN network for managed APs.
- **VLAN TAG**：Administrator can set VLAN TAG ID for managed APs.
- **IP Address**：Administrator can set IP address for managed APs, the IP address is auto-incrementally.
- **NetMask**：Administrator can set NetMask for managed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

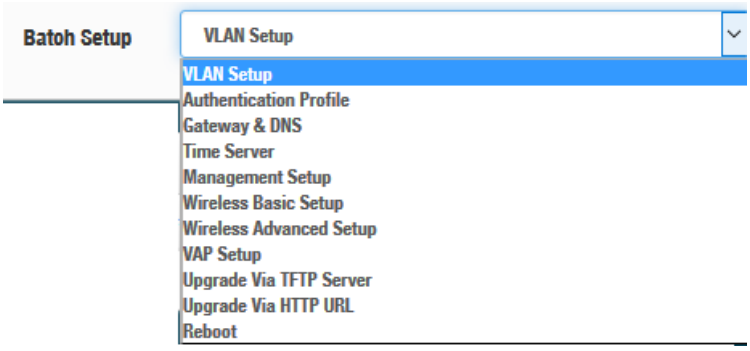
When the setting managed APs is completed, please click Apply & Reboot button to complete the setup process.

4.2.2 Batch Setup

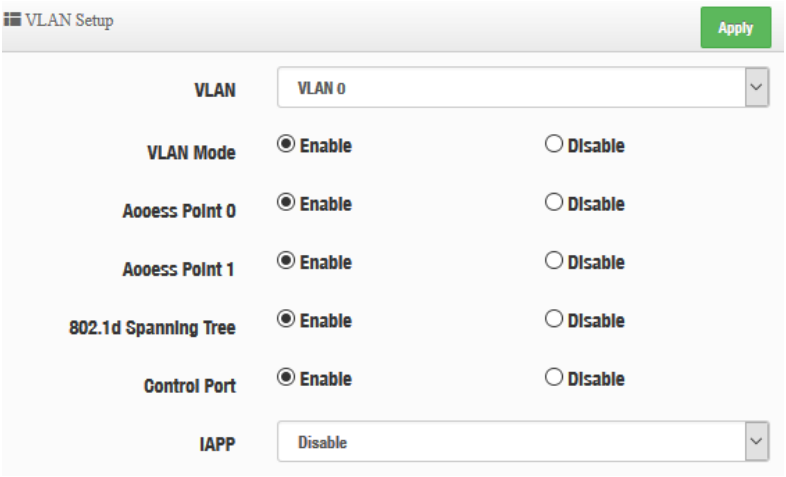
The AP control function supports centralized configuration of managed APs. Administrator can change VLAN network / Group and batch setup for managed APs.



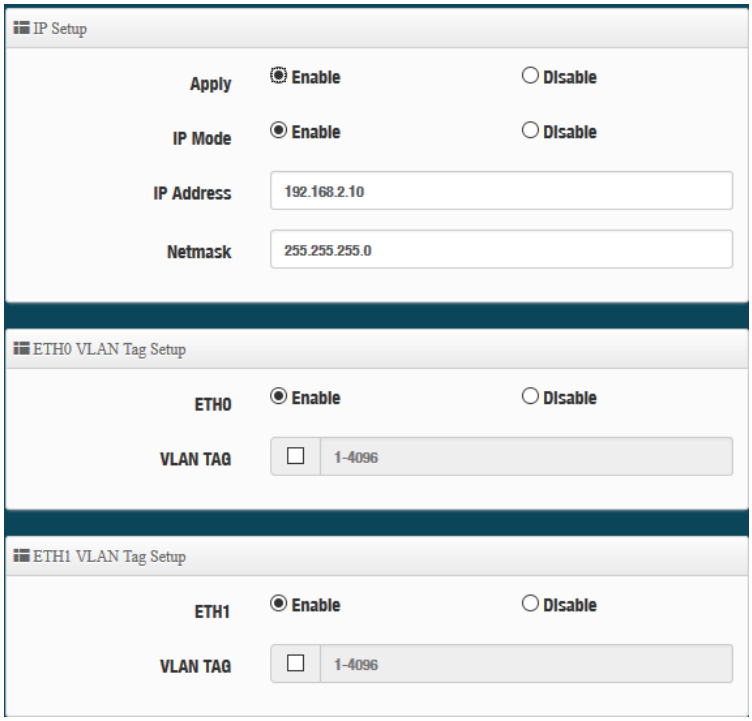
- **LAN**：When VLAN Tag function is enabled (please refer to 4.1 System VLAN Setup), administrator can change VLAN tag for managed APs.
- **Group**：When AP Groups are created (please refer to 4.2.4 Group setup), Administrators can select and change group settings of managed APs.
- **Batch Setup**：Administrator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



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



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

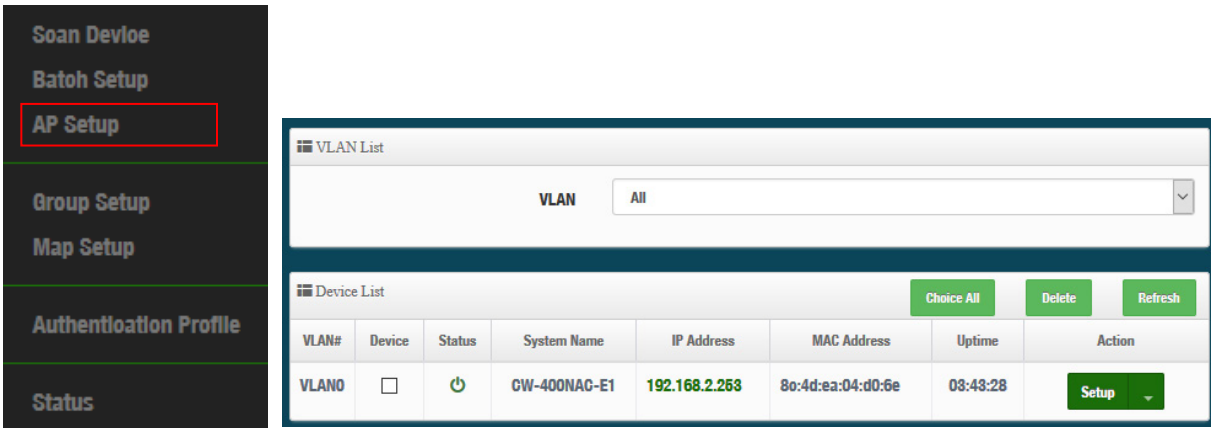


- ✓ **IP Setup**：Administrator can set IP address and Netmask of the managed APs.
- ✓ **ETH0/1 VLAN Tag Setup**：Administrator can set VLAN Tag or disable VLAN function of the managed APs.

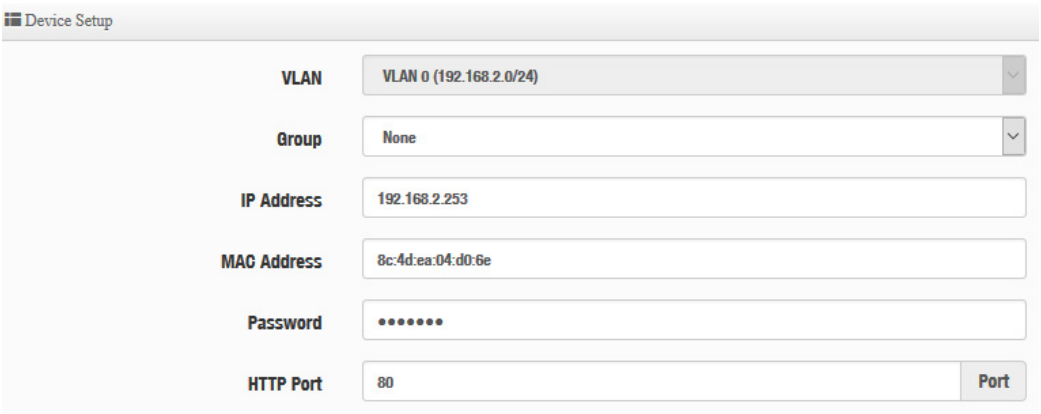
- **Authentication Profile**：After creating Profiles, See: “4.2.6 Authentication Profile” users can conveniently apply Authentication profiles
- **Gateway & DNS:** Setting Gateway and DNS for managed APs.
- **Time Server:** Setting System Time for managed APs. (Please refer to 5.2 Configure Time Server)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

4.2.3 AP Setup

Administrator can monitor statuses and modify managed APs information.

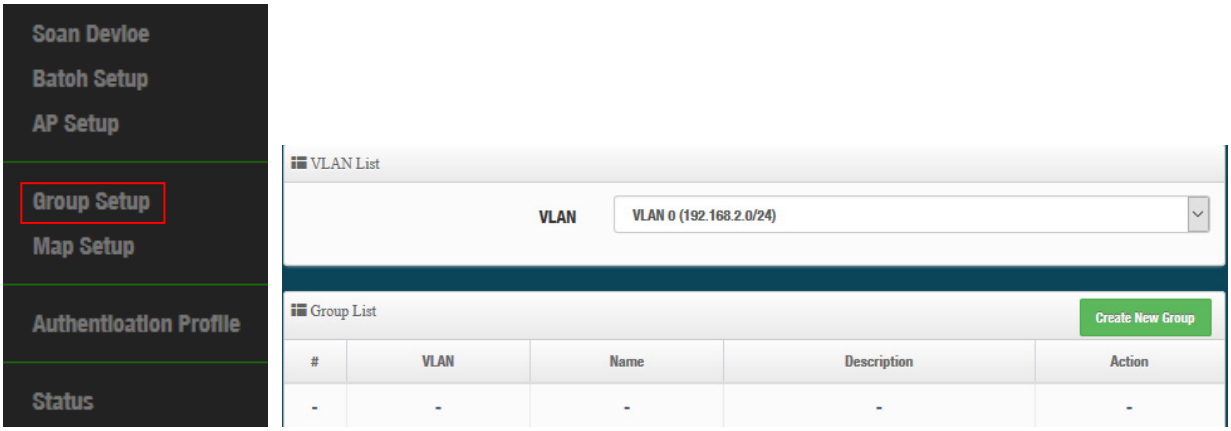


- **VLAN**：Select desired VLAN for AP setup
- **Setup**：Administrator can modify IP addresses, system login passwords, and web login port for managed APs. If administrator has change AP devices, administrator can modify MAC address of the new managed AP.

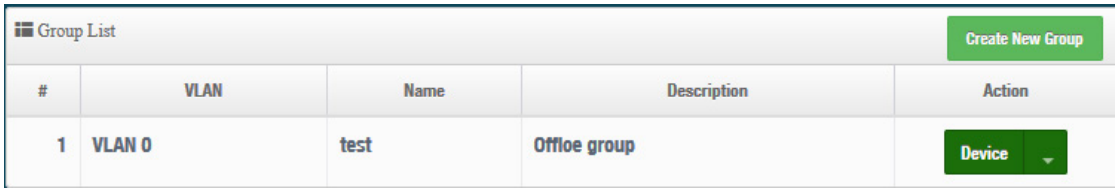


4.2.4 Group Setup

Administrator can create Groups within the same VLAN.



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

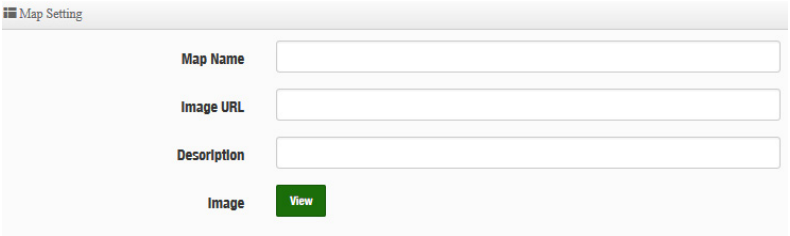


✓ **Device button**：Administrator can select managed APs and import them into the Group.

4.2.5 Map Setup

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

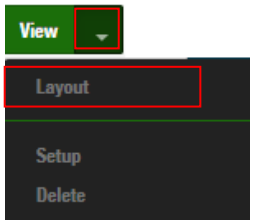
- **Create New Map**：Click the button to create map.



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

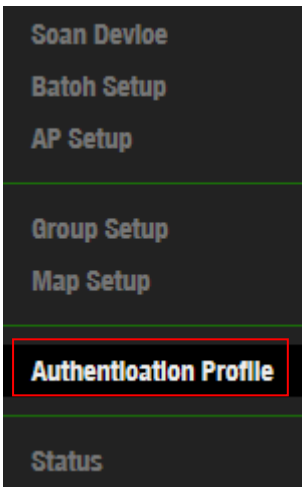
After the Map URL setup confirmation, please reboot the system.

: 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.

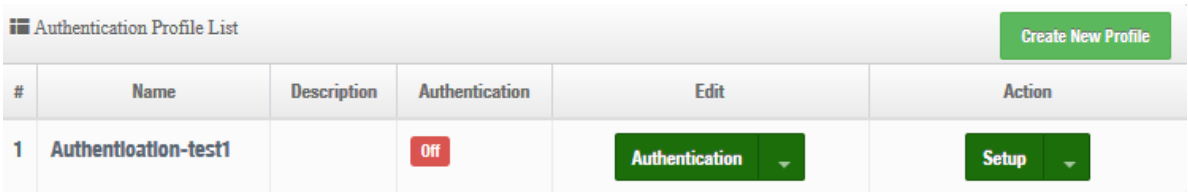


View：Once complete, administrators can click the “View” button to monitor AP statuses and locations.

4.2.6 Authentication Profile



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



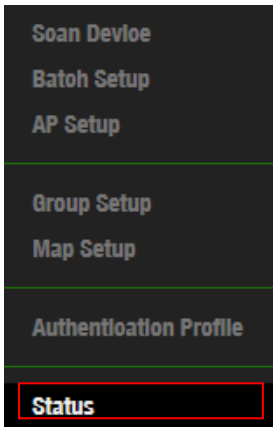
- **Create New Profile**：Administrator can create authentication profile.
- **Edit**：

Click the Authentication button to Enable or Disable authentication function. For more details, refer to **"3.3 Authentication".**

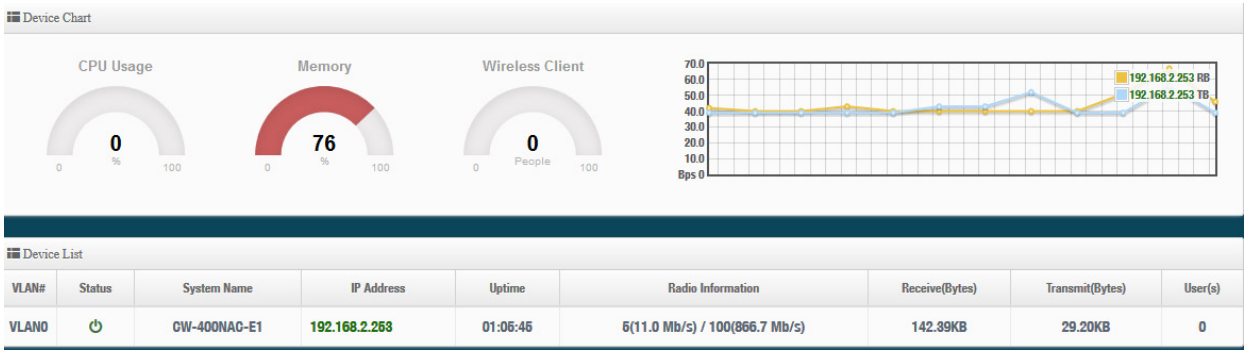
Click Dropdown to set authentication functions. Refer to **"3.3 Authentication"** dropdown functions.
- **Action:**

The button can modify or delete for the authentication profile.

4.2.7 Status



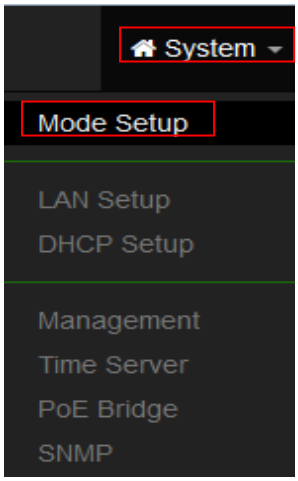
Administrator can monitor Tx/Rx flow information, show online users and check system CPU / Memory information and on/off line for the managed APs. The information data display support graphical interface.

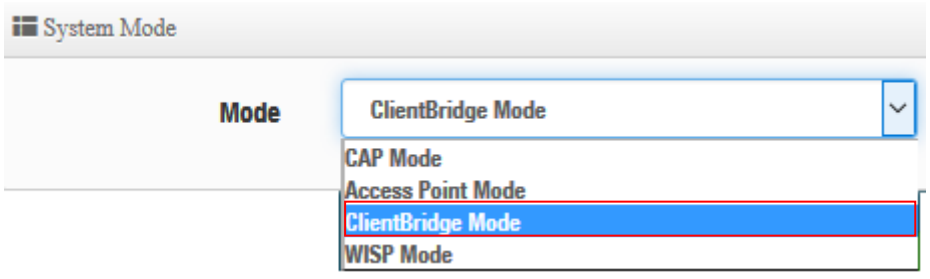


5. Client Bridge Mode

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

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



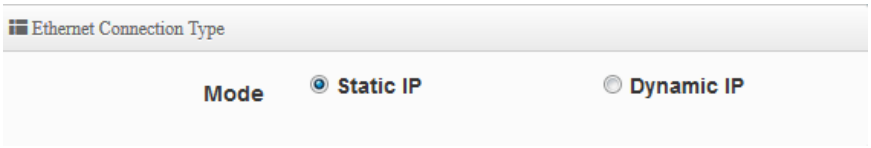


Notice

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

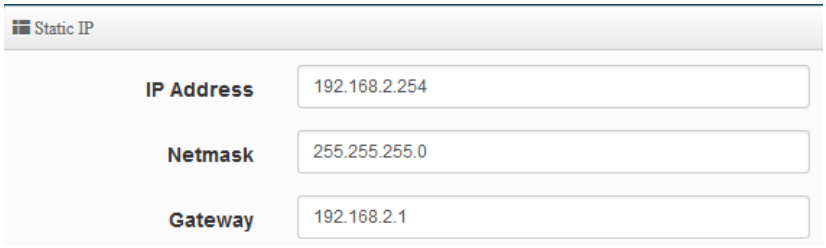
5.1 Configure LAN Setup

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



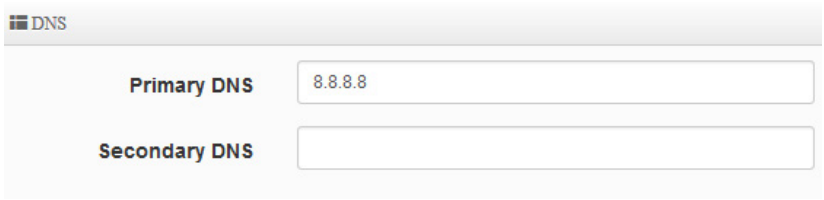
Mode: Administrator can select the IP used Static or Dynamic IP address.

- **Static IP:**



- **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.

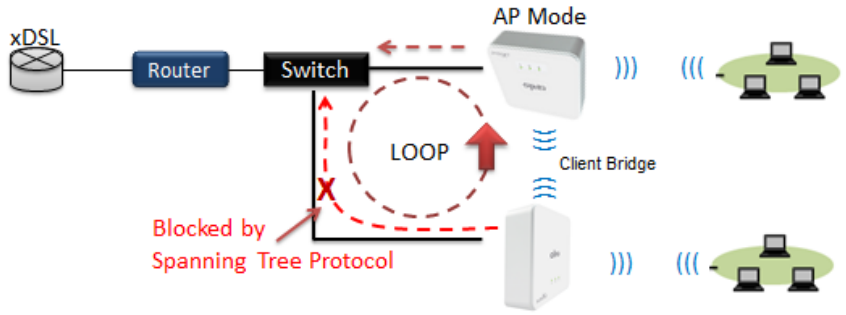
- **DNS**: Enter IP address of domain name service.



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

- **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.

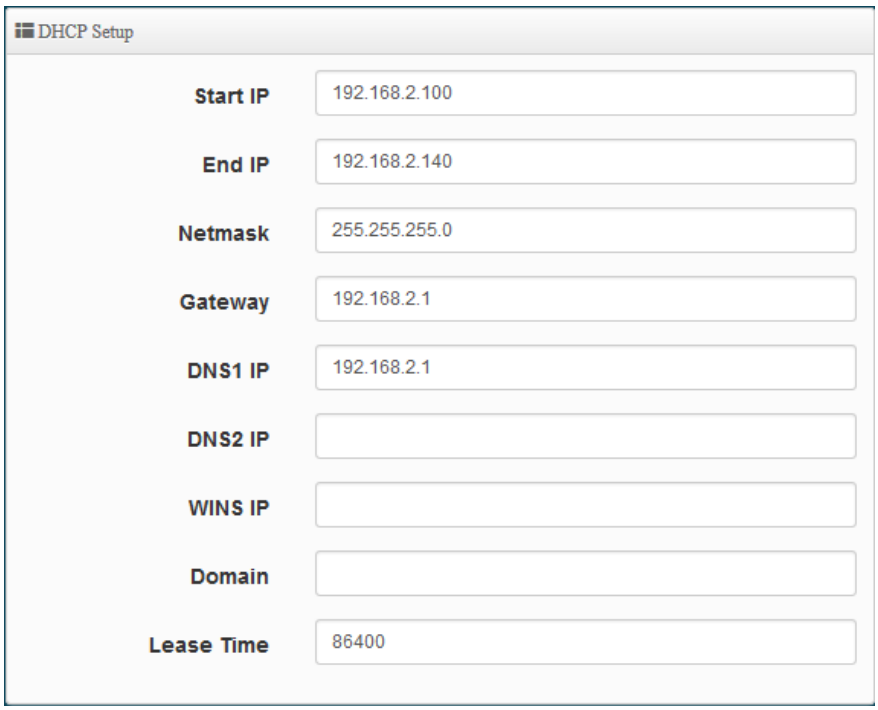


Client Bridge + Repeater AP

- **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.

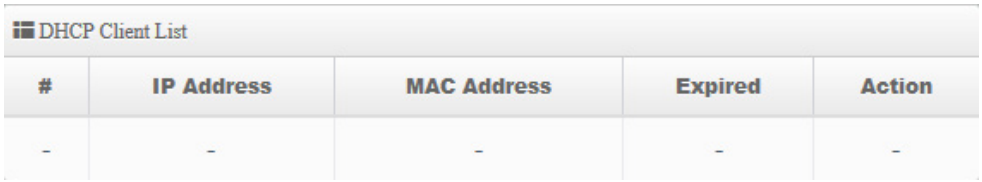
5.2 Configure DHCP Setup

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



- **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.



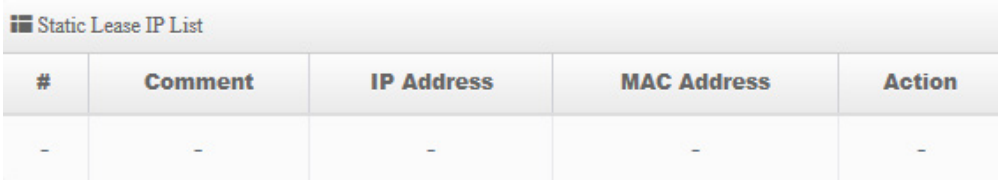
- **IP Address:** Display users used IP address.
- **MAC Address:** Display MAC Address of users used device.
- **Expired:** Display Lease expiration time of IP address.

- **Action:** Kicked user button.

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

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

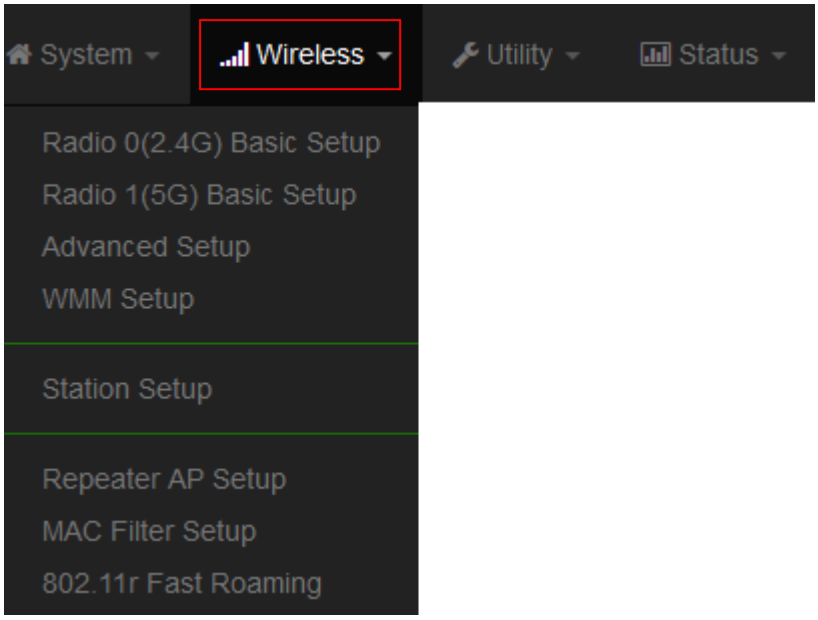
Static Lease IP List: Display users list of static IP address.



5.3 Wireless General Setup

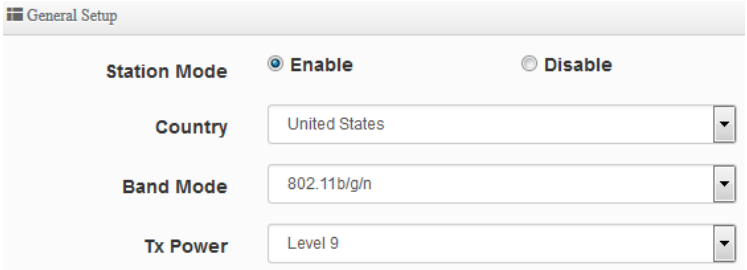
Notice The following instructions cover dual band access point. 11n devices will not support Radio 1

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



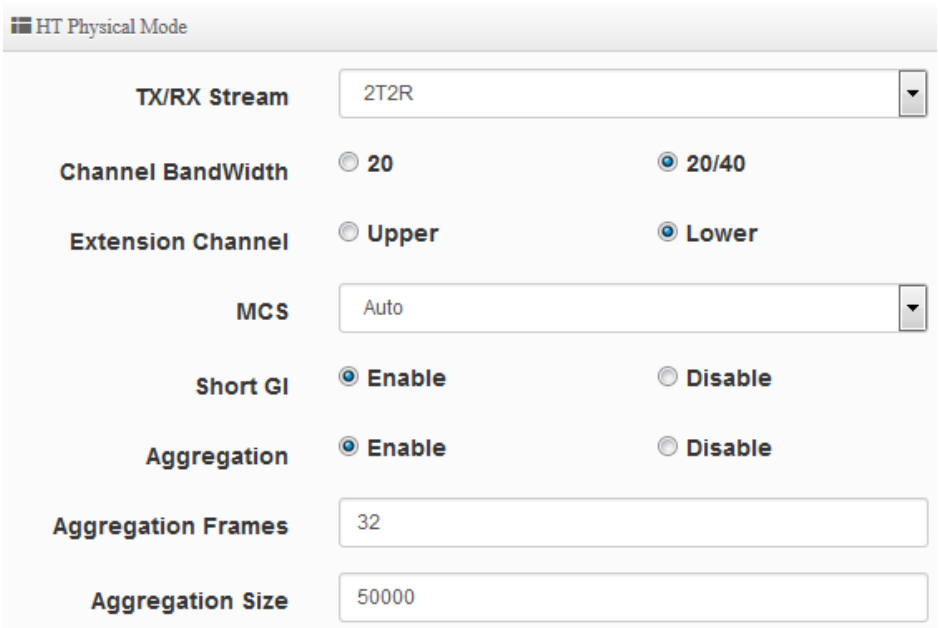
5.3.1 Radio 0(2.4G) Basic Setup

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



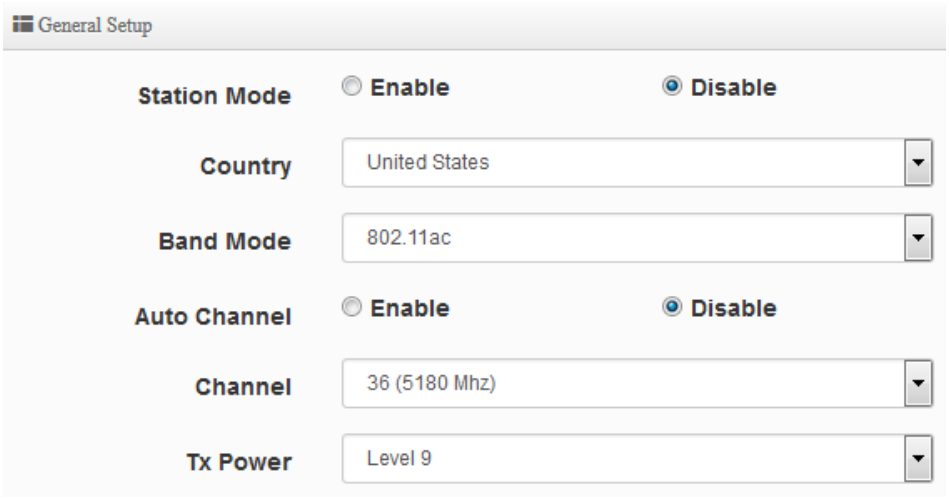
- **Station Mode:** Administrator can Enable or Disable the radio.
- **Country:** Administrator can select country used channel by US and EU.
- **Band Mode:** Select an appropriate wireless band; bands available are **801.11 b/g/n mixed mode.**
- **Tx Power:** Administrator can adjust the output power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

HT Physical Mode



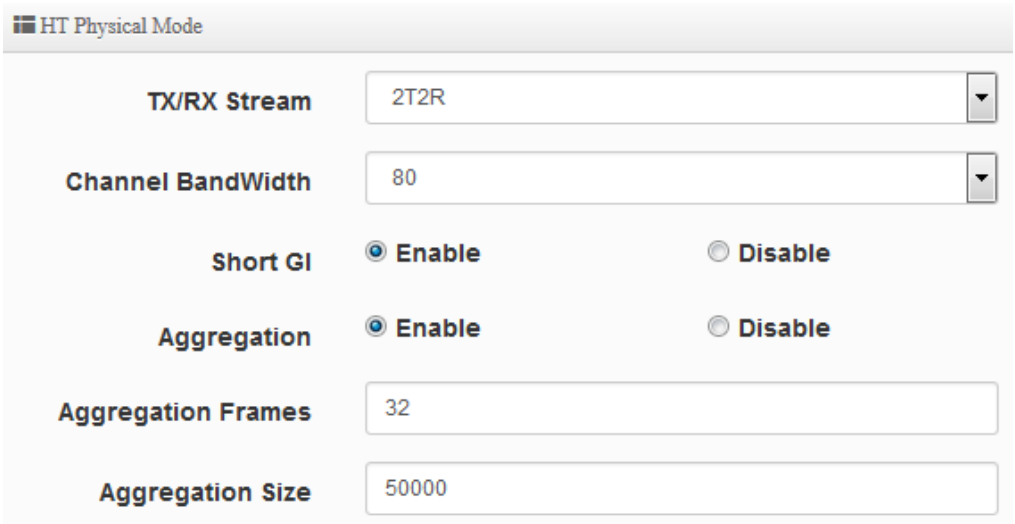
- **TX/RX Stream:** CenOS 5.0 APs utilizes 2 antennas, supporting 2TX/2RX streams. Administrator can select 1 or 2 TX/RX. The default is 2TX/2RX.
- **Channel Bandwidth:** The "**20/40**" MHz option is usually best. The other option is available for special circumstances.
- **Extension Channel:** Set channel select of Upper or Lower, the Upper support 1 to 7 range CH and Lower support 5 to 11 range CH.
- **MCS:** This parameter represents transmission rate. By default (Auto) the fastest possible transmission rate will be selected. You have the option of selecting the speed if necessary.
- **Shout GI:** Short Guard Interval, by default, it's "Enable". it's can increase throughput. However, it can also increase error rate in some installations, due to increased sensitivity to radio-frequency reflections. Select the option that works best for your installation.
- **Aggregation:** By default, it's "**Enable**". To "Disable" to deactivated Aggregation.
  A part of the 802.11n standard (or draft-standard). It allows sending multiple frames per single access to the medium by combining frames together into one larger frame.
  It creates the larger frame by combining smaller frames with the same physical source and destination end points and traffic class (i.e. QoS) into one large frame with a common MAC header.
- **Aggregation Frames:** The Aggregation Frames is in the range of **2~64**, the default is **32**. It determines the number of frames combined on the new larger frame.
- **Aggregation Size:** The Aggregation Size is in the range of **1024~65535**, the default is **50000**. It determines the size (in Bytes) of the larger frame.

5.3.2 Radio 1(5G) Basic Setup



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

HT Physical Mode

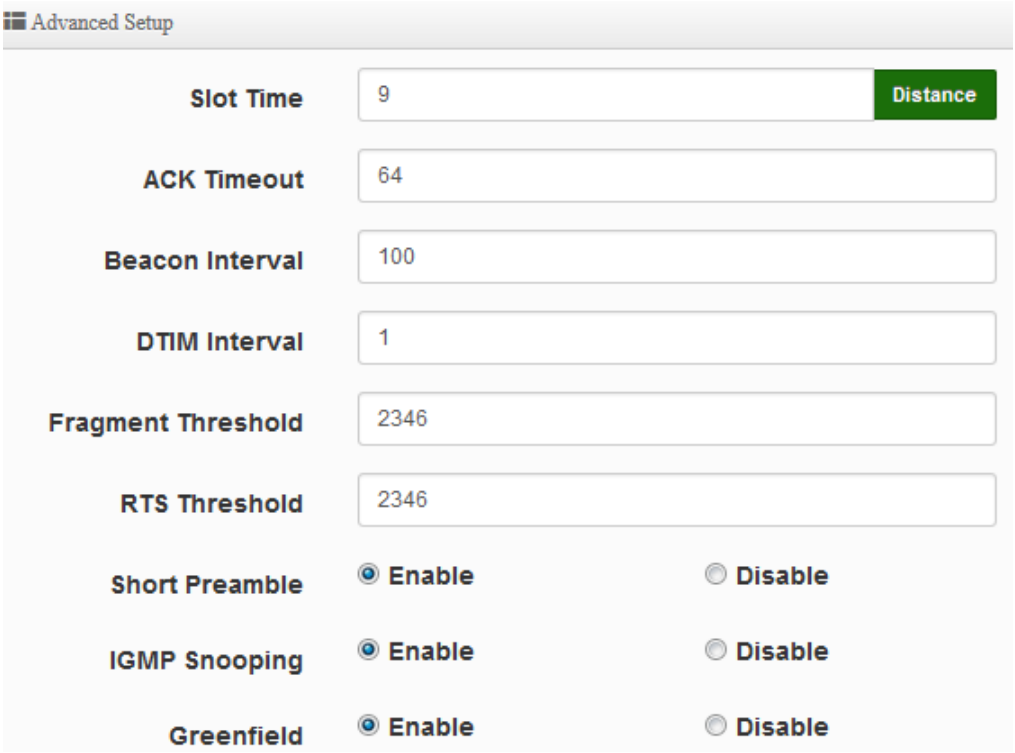


- **TX/RX Stream:** CenOS 5.0 APs utilizes 2 antenna and supports 2TX/2RX streams. Administrator can select 1 or 2 TX/RX. The default is 2TX/2RX.
- **Channel Bandwidth:** The "**20/40 and 802.11ac 80**" MHz option is usually best. The other option is available for special circumstances.

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

5.3.3 Advanced Setup

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



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

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

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

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

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

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

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

- **Beacon Interval:** Beacon Interval is in the range of **40~3500** and set in unit of *millisecond*. The default value is **100** msec.

  Access Point (AP) in IEEE 802.11 will send out a special approximated 50-byte frame, called "Beacon". Beacon is broadcast to all the stations, provides the basic information of AP such as SSID, channel, encryption keys, signal strength, time stamp, support data rate.

  All the radio stations received beacon recognizes the existence of such AP, and may proceed next actions if the information from AP matches the requirement. Beacon is sent on a periodic basis, the time interval can be adjusted.

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

- **DTIM Interval:** The DTIM interval is in the range of **1~255**. The default is **1**.
  DTIM is defined as *Delivery Traffic Indication Message*. It is used to notify the wireless stations, which support power saving mode, when to wake up to receive multicast frame. DTIM is necessary and critical in wireless environment as a mechanism to fulfill power-saving synchronization.
  A DTIM interval is a count of the number of beacon frames that must occur before the access point sends the buffered multicast frames. For instance, if DTIM Interval is set to 3, then the Wi-Fi clients will expect to receive a multicast frame after receiving three Beacon frame. The higher DTIM interval will help power saving and possibly decrease wireless throughput in multicast applications.
- **Fragmentation Threshold:** Fragmentation Threshold is one more parameter which is given in all stations and Access points. Fine tuning Fragmentation Threshold parameter can result in good throughput but not using it properly can results in low throughput. In simple words it does the same thing which MTU do in Ethernet. Both are different parameters but the work done is same, it fragments the data packets.
  Fragmentation threshold will be used when we have more data packet size to be transmitted and we have less fragment threshold value. 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, it's "***Enable***". To ***Disable*** is to use Long 128-bit Preamble Synchronization field.
  The preamble is used to signal "here is a train of data coming" to the receiver. The short preamble provides 72-bit Synchronization field to improve WLAN transmission efficiency with less overhead.
- **IGMP Snooping:** the process of listening to Internet Group Management Protocol (IGMP) network traffic. The feature allows a network switch to listen in on the IGMP conversation between hosts and routers. By listening to these conversations the switch maintains a map of which links need which IP multicast streams. Multicasts may be filtered from the links which do not need them and thus controls which ports receive specific multicast traffic.

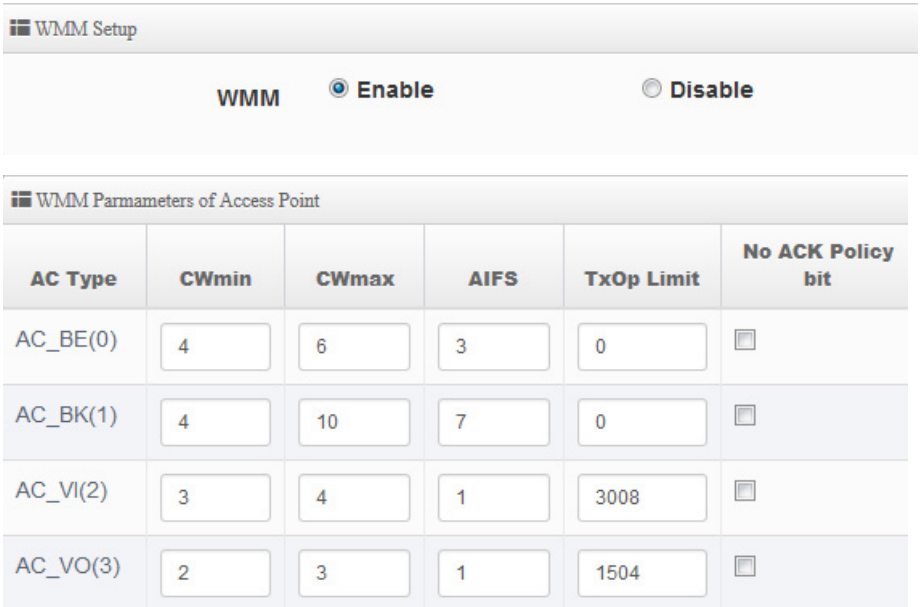
- **Greenfield:** In wireless WLAN technology, greenfield mode is a feature of major components of the 802.11n specification. The greenfield mode feature is designed to improve efficiency by eliminating support for 802.11b/g devices in an all draft-n network. In greenfield mode the network can be set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

5.3.4 WMM Setup

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

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

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



WMM Parmameters of Station

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

✓ **AC Type**：

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

✓ **CWmin**：

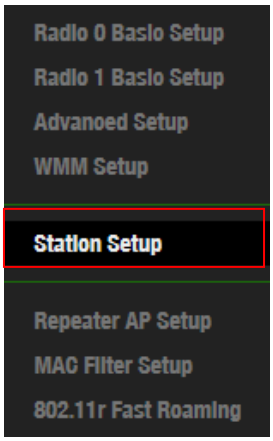
Minimum Contention Window. This parameter is input to the algorithm that determines the initial random backoff wait time ("window") for retry of a transmission. The value specified here in the Minimum Contention Window is the upper limit (in milliseconds) of a range from which the initial random backoff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

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

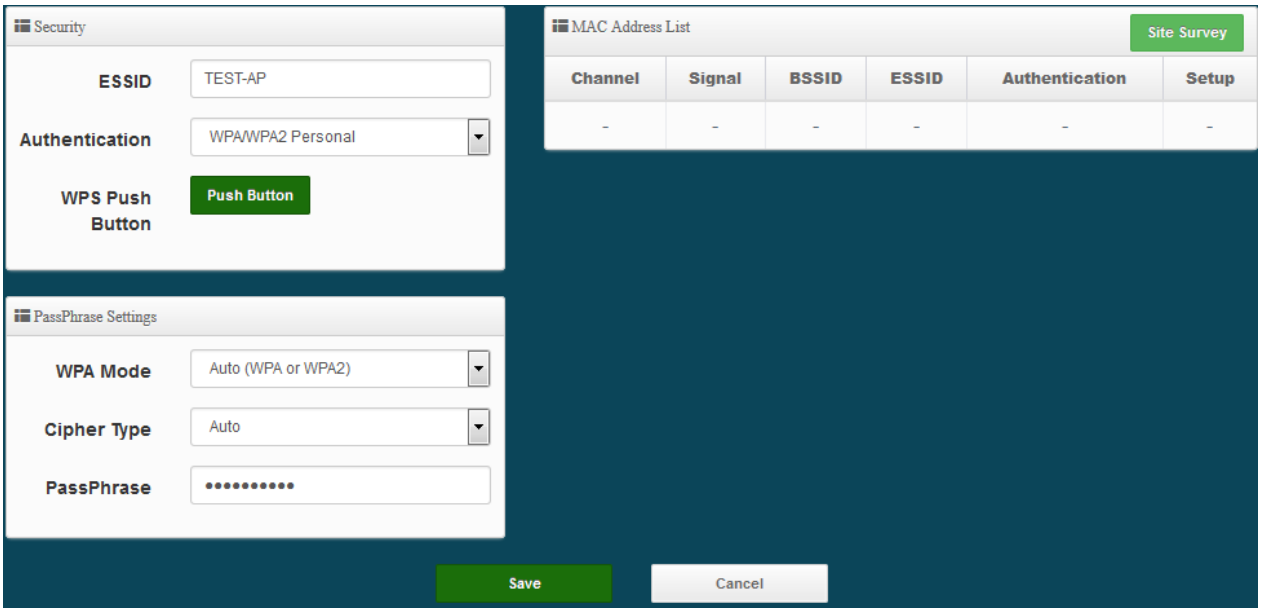
✓ **AIFS**：The Arbitration Inter-Frame Spacing Number specifies a wait time (in milliseconds) for data frames ◦

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

5.3.5 Station Setup



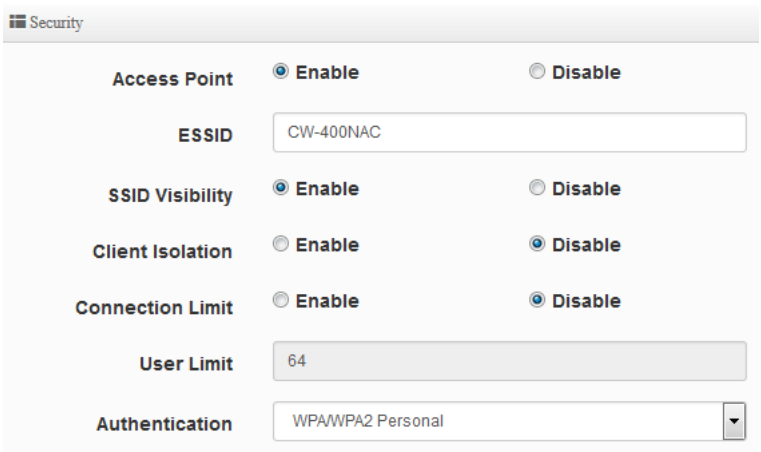
The functions setting functions include Client Bridge link to AP station. Administrator can used "site survey" function to Search for AP stations.



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

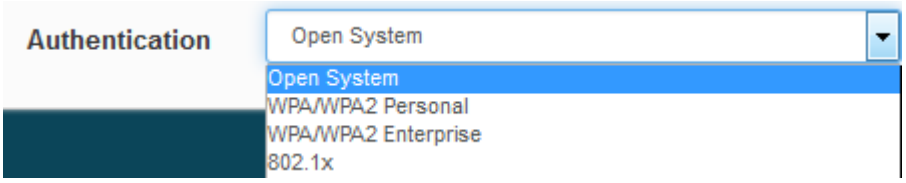
5.3.6 Repeater AP Setup

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

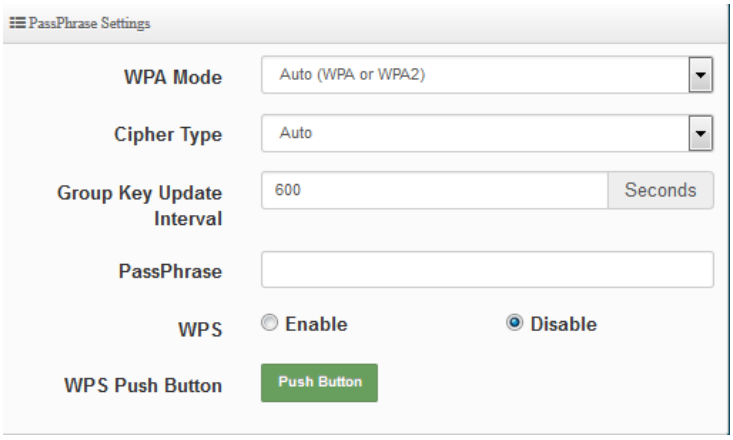


- **Access Point:** Administrator can Enable or Disable the Repeater AP function.
- **ESSID:** Enter the Repeater AP of ESSID name.
- **SSID Visibility:** The default it's Enable**.** When select Disable the SSID will not is discovered.
- **Client Isolation:** This function is Disabled by default. All 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.



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



✓ **WPA Mode:** Administrator can select security for Auto or only WPA or only WPA2.

✓ **Cipher Type:** Administrator can select use AES or TKIP with WPA / WPA2 encryption method.

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

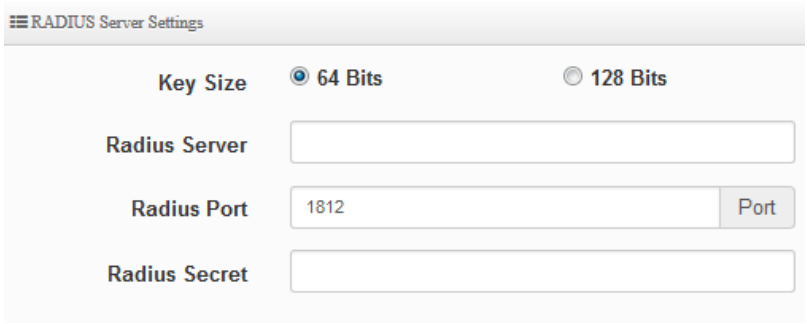
TKIP is short for "**Temporal Key Integrity Protocol**", TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with.

✓ **Group Key Update Interval**: This time interval for re-keying GTK (broadcast/multicast encryption keys) in seconds. Enter the time-length required; the default time is 600 seconds.

✓ **Pass Phrase:** Enter the ESSID pass phrase.

✓ **WPS:** Administrator can used WPS function link WiFi client, if select enable the function, administrator can click the WPS Push Button.

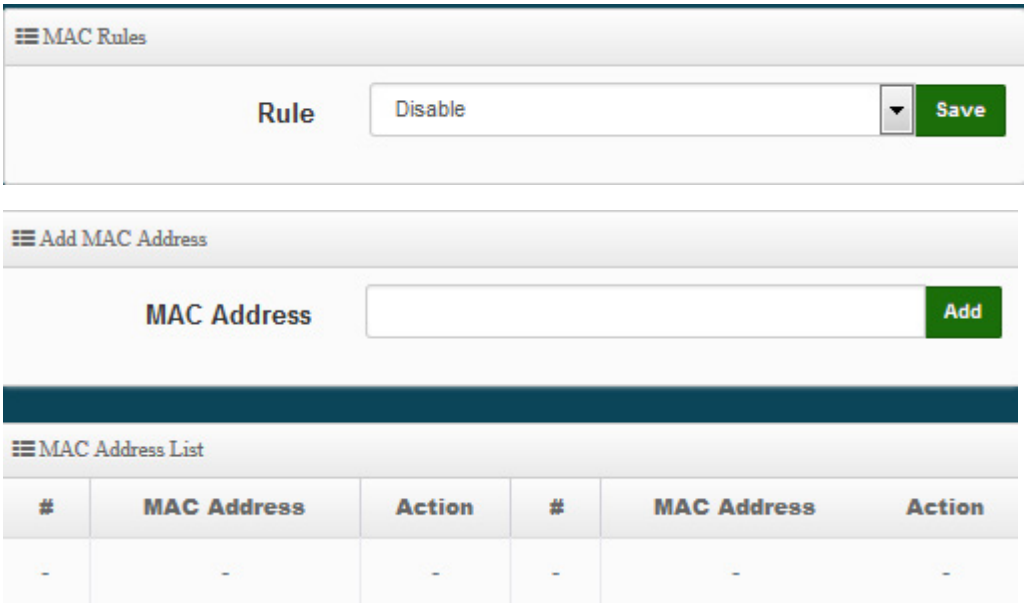
- **802.1X security:** When 802.1x Authentication is enabled, please refer to the following Dynamic WEP and RADIUS settings to complete the configuration.



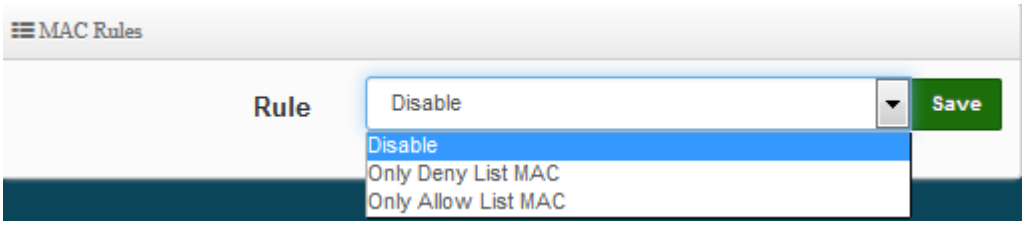
- ✓ **Key Size:** Check on the respected button to enable either 64bits or 128bits key length. The system will automatically generate WEP keys for encryption.
- ✓ **Radius Server:** Enter the IP address of the Authentication RADIUS server.
- ✓ **Radius Port:** The port number used by Authentication RADIUS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

5.3.7 MAC Filter

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



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

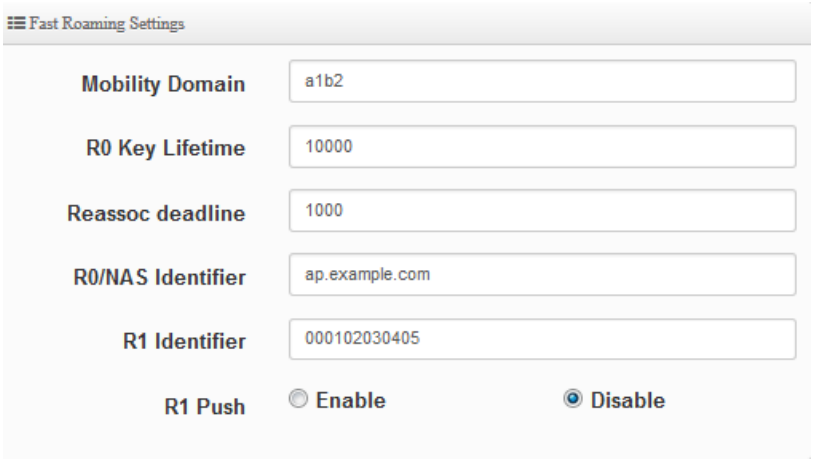


- **Only Allow List MAC**: Define certain wireless clients in the list which will have granted access to the Access Point while the access will be denied for all the remaining clients – Action Type is set to "**Only Allow List MAC**".
- **Only Deny List MAC**: Define certain wireless clients in the list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

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

5.3.8 802.11r/802.11k Fast Roaming

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

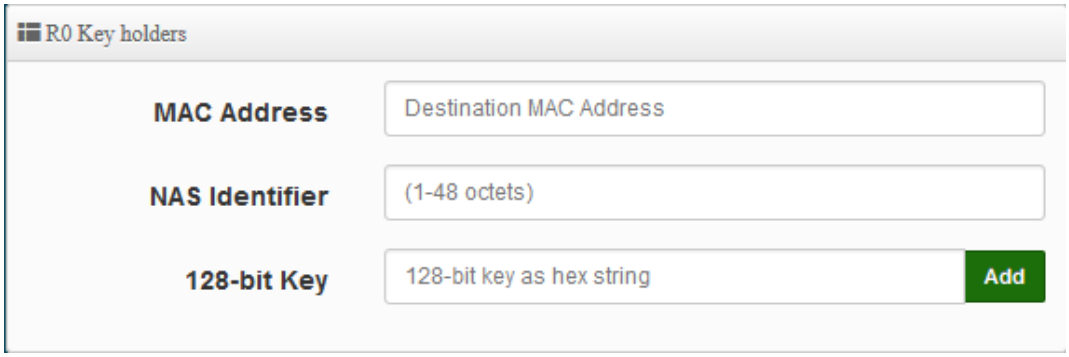


- **Mobility Domain:** MDID is used to indicate a group of APs (within an ESS, i.e., sharing the same SSID) between which a STA can use Fast BSS Transition. Please enter 2-octet identifier as a hex string.
- **R0 Key Lifetime:** Default lifetime of the PMK-RO in minutes, the default is 10000, administrator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

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

R0 Key Address:

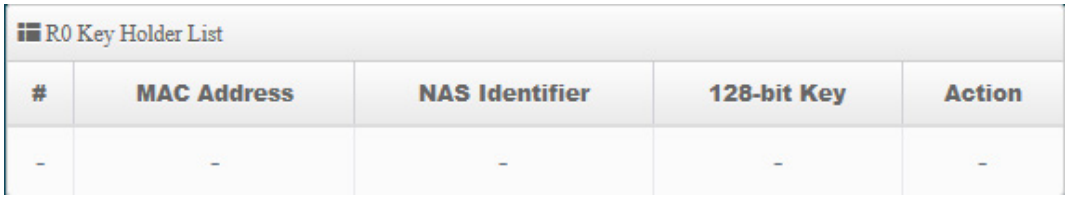
To enable roaming between multiple AP devices, AP1 must key in the MAC Address of AP2, and AP2 must key in the MAC Address of AP1. The NAS Identifier and 128-bit Key should be identical in both AP settings. This will enable device roaming between the two Access Points.



- **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.

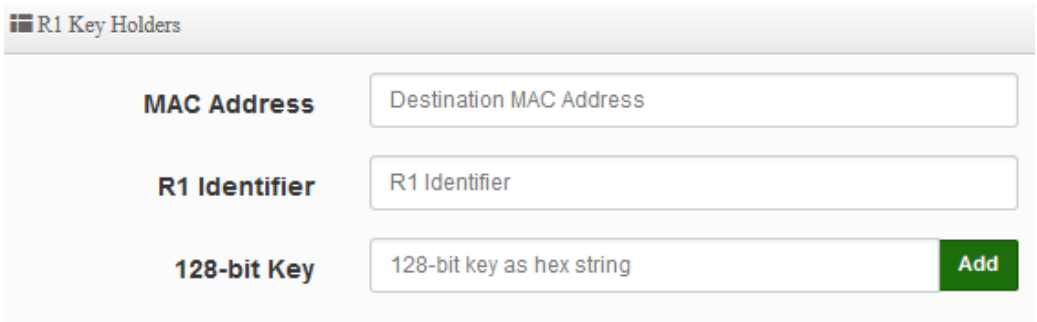
R0 Key Holder List:

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



R1 Key Holder List:

Enter a unified set of R1 Key Holder identification certification.



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

R1 Key Holder List:

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

R1 Key Holder List

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

6. WISP Mode

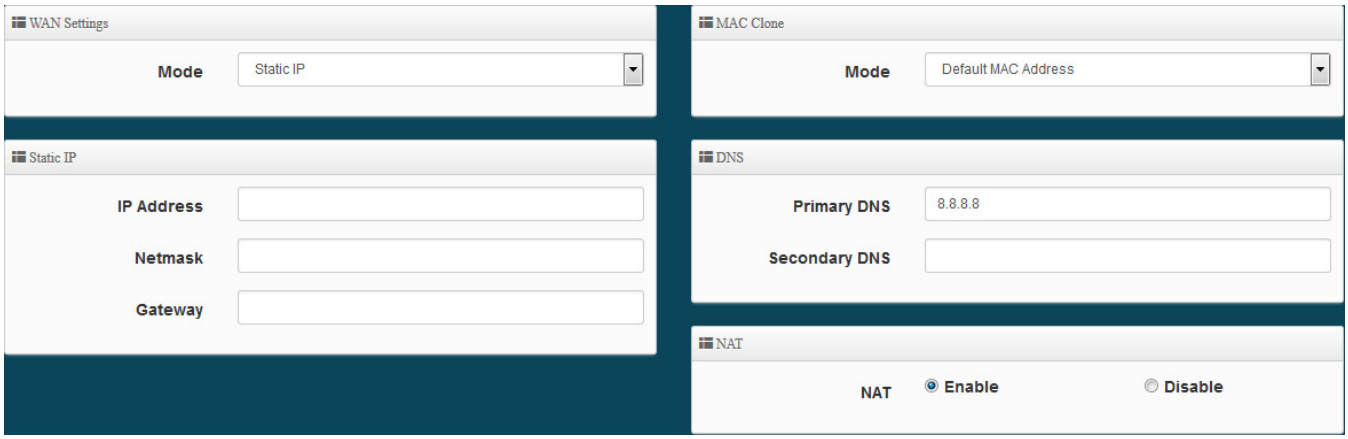
WISP Mode is a router function, if the Telecom company permits wireless connection to their WAN, administrators can change the CenOS 5.0 AP to WISP Mode to connect to the wifi network.
The WISP Mode support PPPoE / Static IP / Dynamic IP and PPTP for WAN, and support Repeater AP function.

Notice

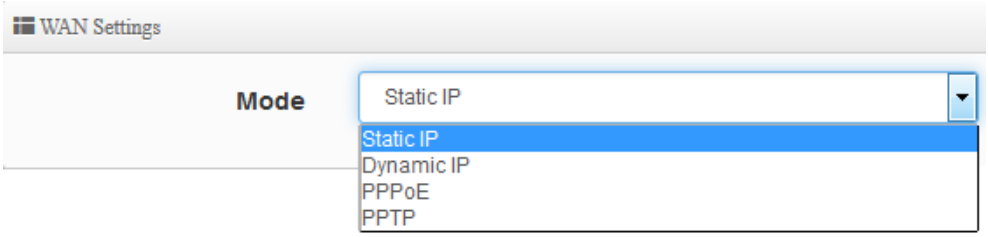
Relevant to Dual Band Devices Only: If wireless WAN used 2.4G radio connection to Telecom company station, the Repeater AP radio only used 5G radio. So wireless WAN used 5G radio connection to Telecom company station, the Repeater AP radio only used 2.4G radio.

6.1 Configure WAN Setup

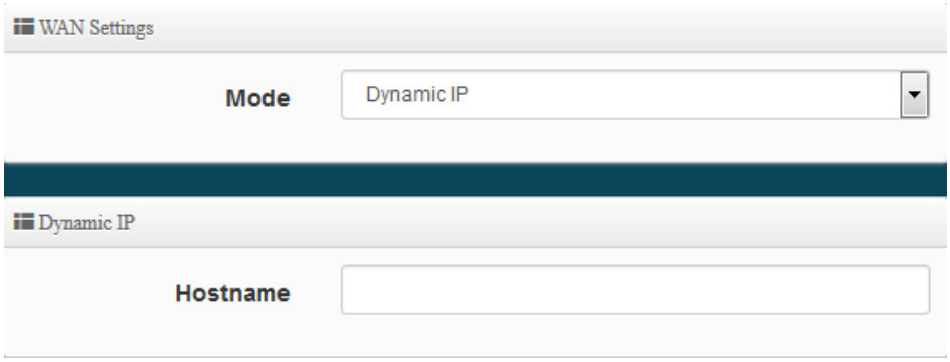
There are four connection types for the WAN port: **Static IP**, **Dynamic IP**, **PPPoE** and **PPTP**. Please click on **System -> WAN** and follow the below setting.



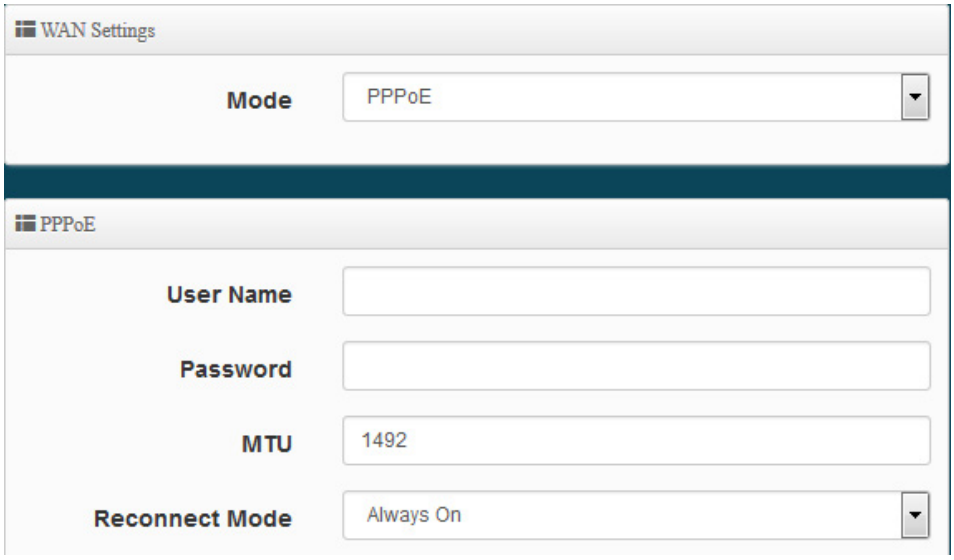
WAN Setting



- **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.



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

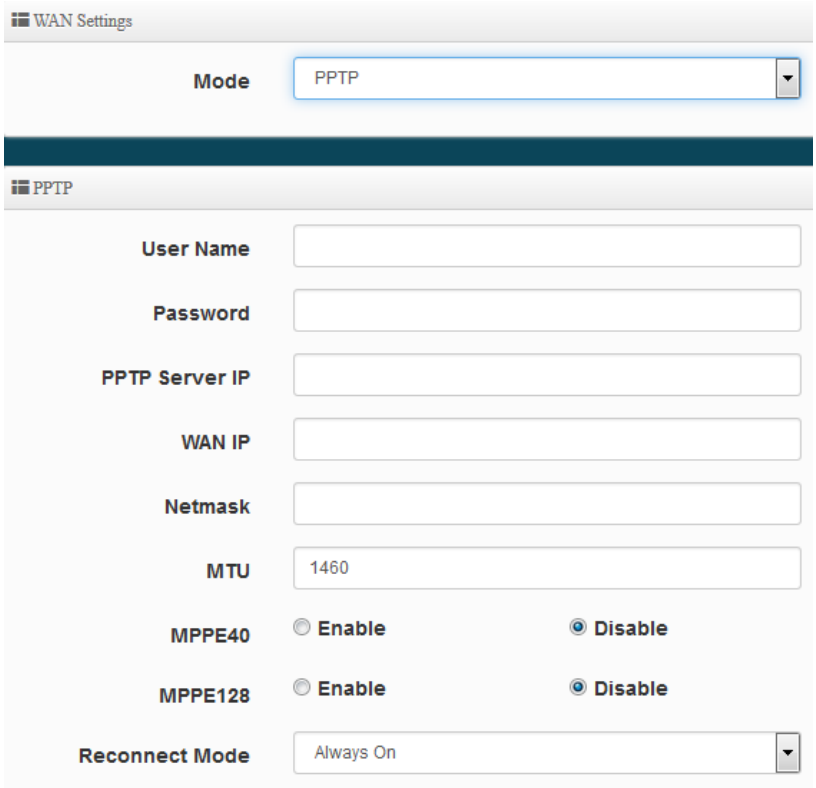


- **User Name :** Enter User Name for PPPoE connection
- **Password :** Enter Password for PPPoE connection
- **MTU:** By default, MTU is set to **1492** bytes. MTU stands for Maximum Transmission Unit. Consult with WISP for a correct MTU setting.
- **Reconnect Mode:** Administrator can select three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

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

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

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



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

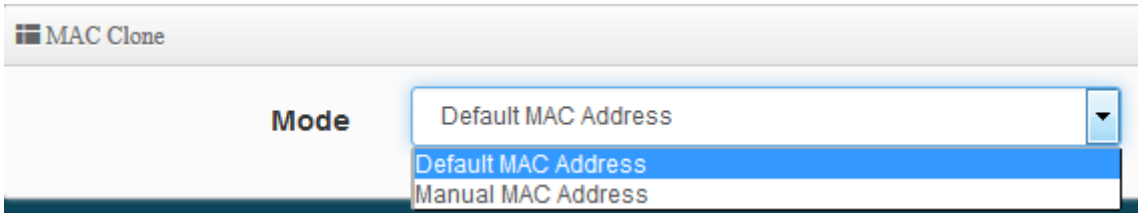
- **Netmask:** The Subnet mask of the WAN port.
- **MTU:** By default, it's **1460** bytes. MTU stands for Maximum Transmission Unit. Consult with WISP for a correct MTU setting.
- **MPPE40/128:** Microsoft Point-to-Point Encryption (MPPE) encrypts data in Point-to-Point Protocol (PPP)-based dial-up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

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

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

➢ MAC Clone

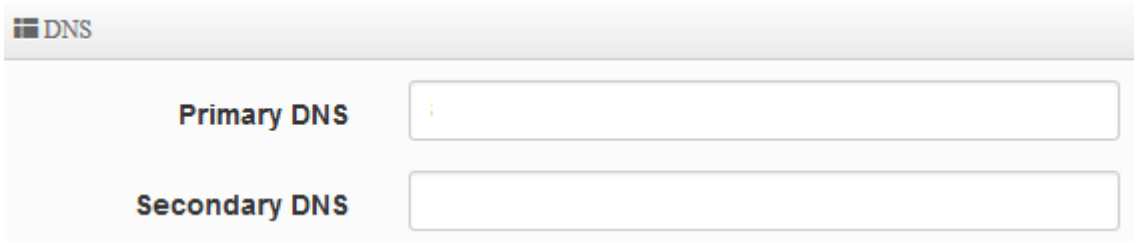
The MAC address is a 12-digit HEX code uniquely assigned to hardware as identification. Some ISPs require you to register a MAC address in order to access to Internet. If not, you could use default MAC or clone MAC from a PC.



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

➢ DNS

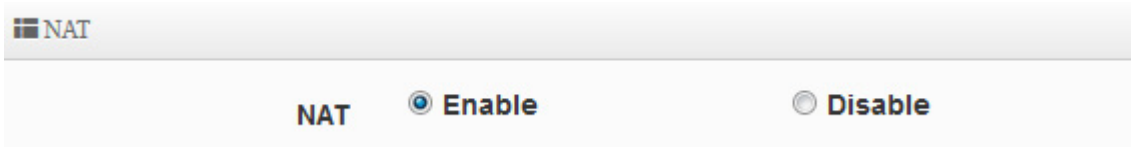
Check "No Default DNS Server" or "Specify DNS Server IP" radial button as desired to set up system DNS.



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

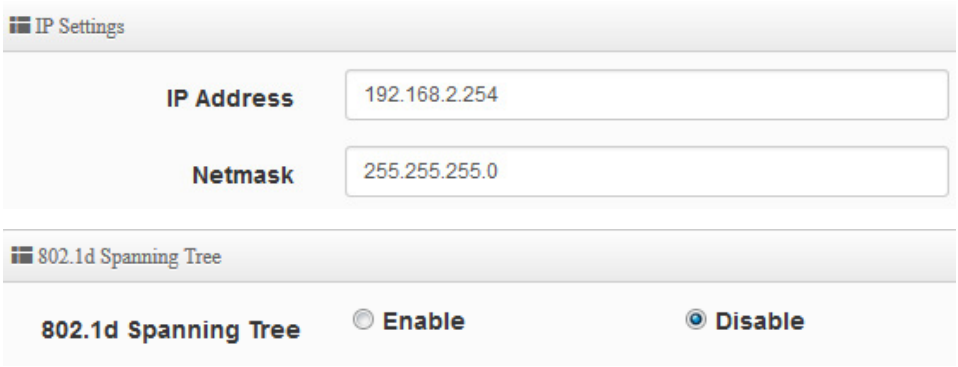
➢ **NAT**

The NAT support Enable and Disable Service



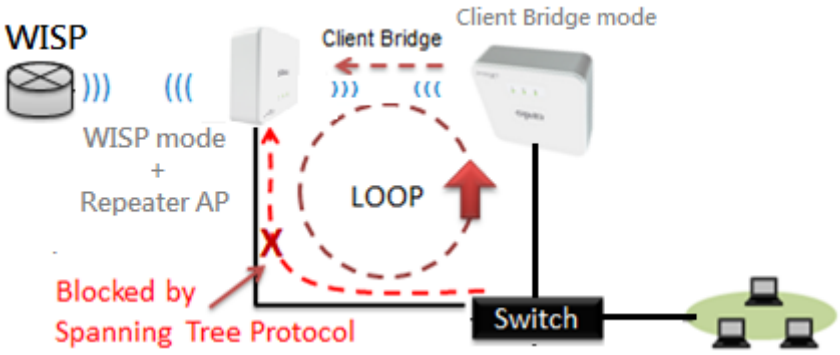
6.2 Configure LAN Setup

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



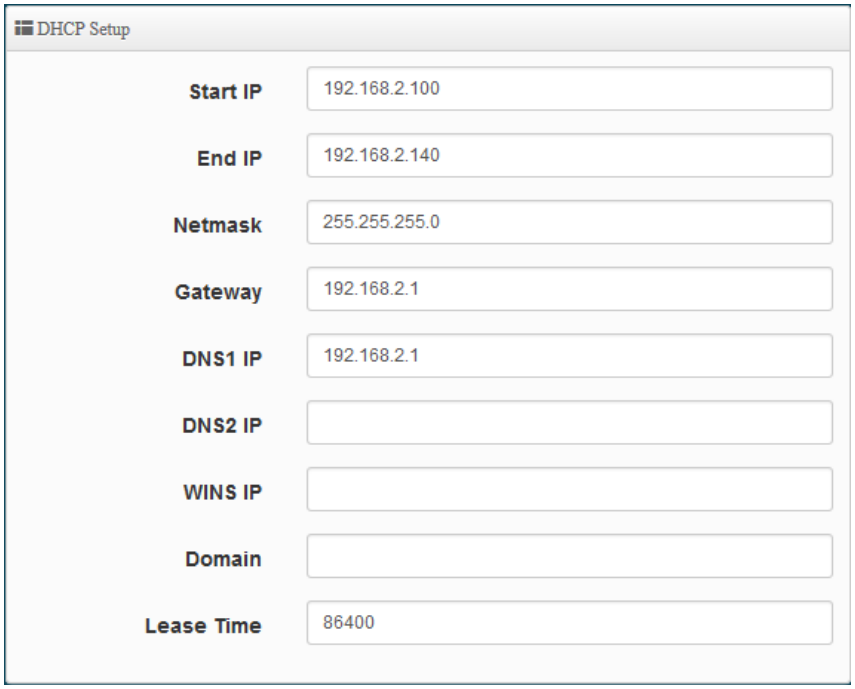
IP Setup: The administrator can manually setup the LAN IP address.

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



6.3 Configure DHCP Server

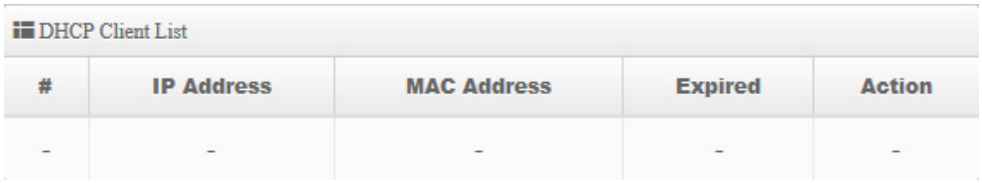
The DHCP Service function in the Client Bridge device can select a separate IP Address range within the same network segment of the source AP, and allocate those IP Addresses to connecting clients.



- **Start IP / End IP:** Specify the range of IP addresses to be used by the DHCP server when assigning IP address to clients.
- **Netmask:** The netmask default is 255.255.255.0.
- **Gateway:** Enter source gateway IP address.
- **DNS1:** Enter IP address of the first DNS server; this field is required.
- **DNS2:** Enter IP address of the second DNS server; this is optional.

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

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


DHCP Client List

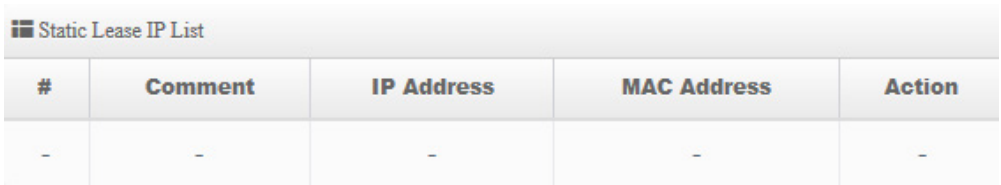
#	IP Address	MAC Address	Expired	Action
-	-	-	-	-

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

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

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

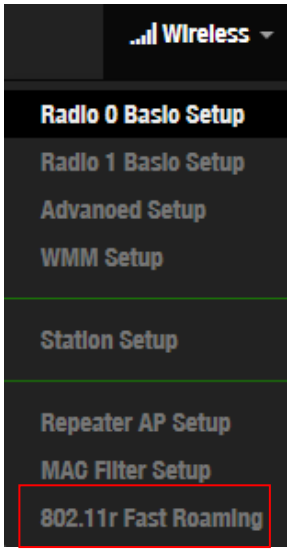
Static Lease IP List: Display users list of static IP address.


Static Lease IP List

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

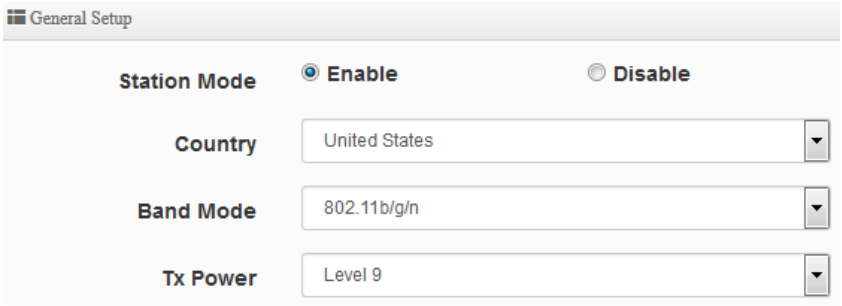
6.4 Wireless General Setup

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



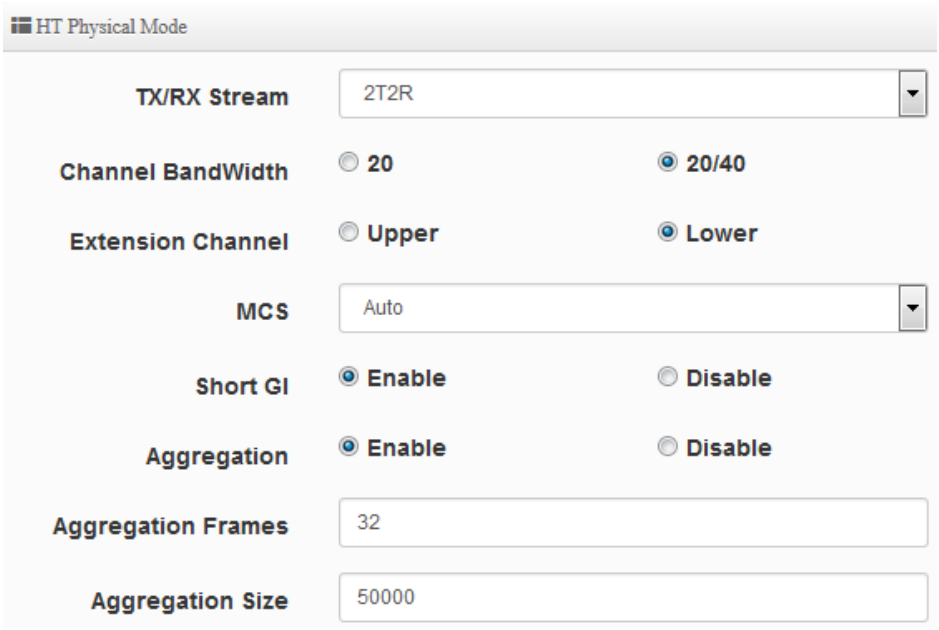
6.4.1 Radio 0(2.4G) Basic Setup

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



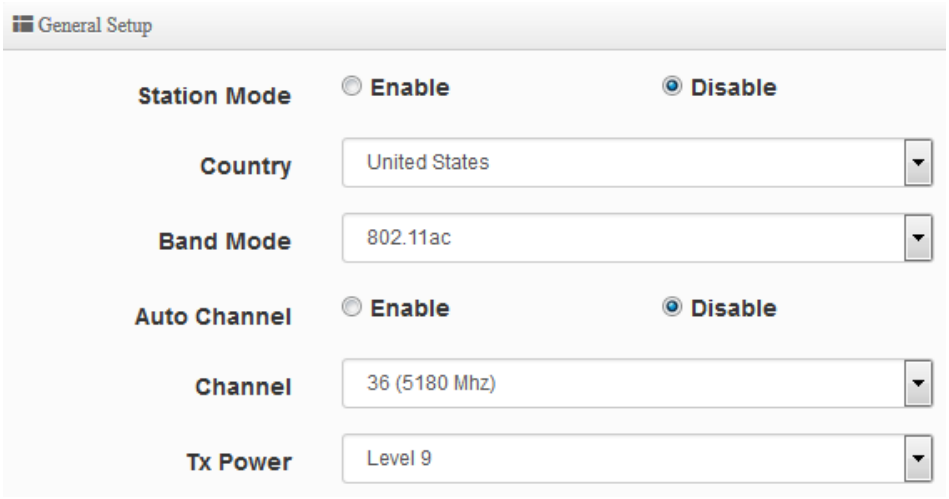
- **Station Mode:** Administrator can Enable or Disable the radio.
- **Country:** Administrator can select country used channel by US and EU.
- **Band Mode:** Select an appropriate wireless band; bands available are **801.11 b/g/n mixed mode.**
- **Tx Power:** Administrator can adjust the output power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

HT Physical Mode



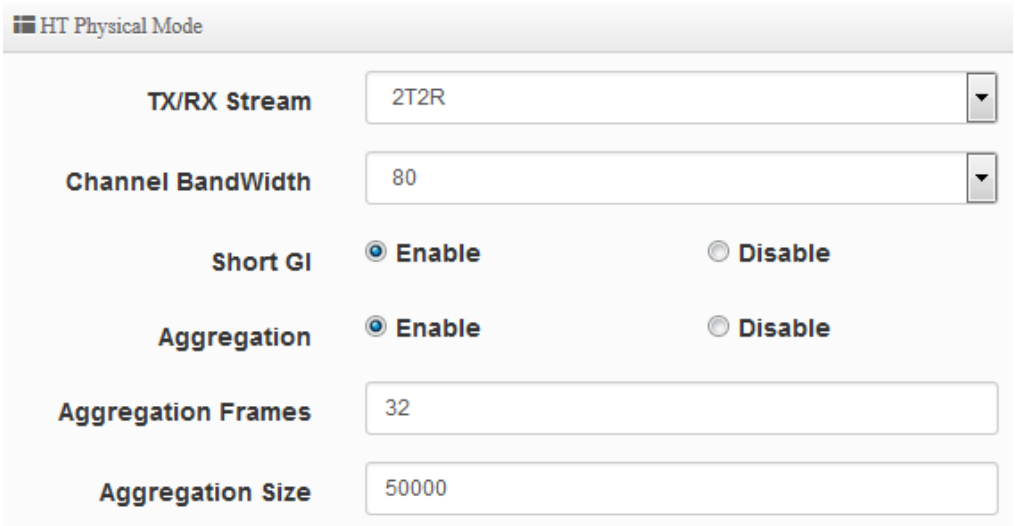
- **TX/RX Stream:** CenOS 5.0 APs utilizes 2 antennas, supporting 2TX/2RX streams. Administrator can select 1 or 2 TX/RX. The default is 2TX/2RX.
- **Channel Bandwidth:** The "**20/40**" MHz option is usually best. The other option is available for special circumstances.
- **Extension Channel:** Set channel select of Upper or Lower, the Upper support 1 to 7 range CH and Lower support 5 to 11 range CH.
- **MCS:** This parameter represents transmission rate. By default (Auto) the fastest possible transmission rate will be selected. You have the option of selecting the speed if necessary.
- **Shout GI:** Short Guard Interval, by default, it's "Enable". This can increase throughput. However, it can also increase error rate in some installations, due to increased sensitivity to radio-frequency reflections. Select the option that works best for your installation.
- **Aggregation:** By default, it's "**Enable**". To "Disable" to deactivated Aggregation.
  A part of the 802.11n standard (or draft-standard). It allows sending multiple frames per single access to the medium by combining frames together into one larger frame.
  It creates the larger frame by combining smaller frames with the same physical source and destination end points and traffic class (i.e. QoS) into one large frame with a common MAC header.
- **Aggregation Frames:** The Aggregation Frames is in the range of **2~64**, the default is **32**. It determines the number of frames combined on the new larger frame.
- **Aggregation Size:** The Aggregation Size is in the range of **1024~65535**, the default is **50000**. It determines the size (in Bytes) of the larger frame.

6.4.2 Radio 1(5G) Basic Setup



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

HT Physical Mode

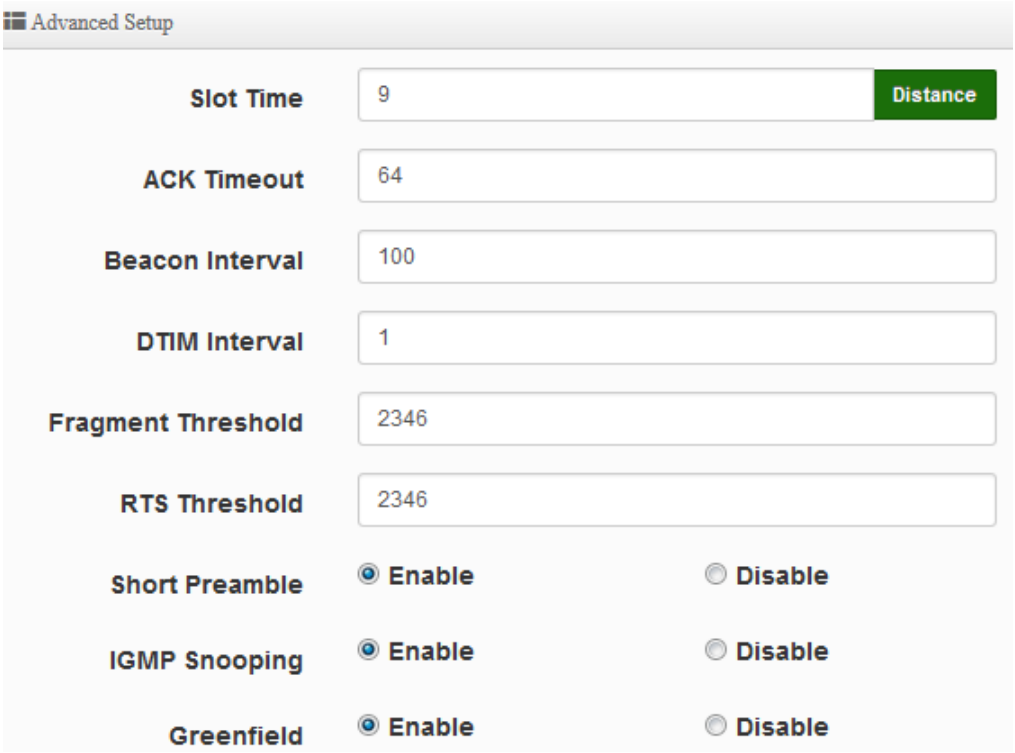


- **TX/RX Stream:** CenOS 5.0 APs utilizes 2 antenna and supports 2TX/2RX streams. Administrator can select 1 or 2 TX/RX. The default is 2TX/2RX.
- **Channel Bandwidth:** The "**20/40 and 802.11ac 80**" MHz option is usually best. The other option is available for special circumstances.

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

6.4.3 Advanced Setup

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



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

- **ACK Timeout:** ACK timeout is in the range of **1~372** and set in unit of ***microsecond***. The default value is **64** microsecond.
  All data transmission in 802.11b/g request an "Acknowledgement" (ACK) send by receiving radio. The transmitter will resend the original packet if correspondent ACK failed to arrive within specific time interval, also refer to as "ACK Timeout".

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

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

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

- **Beacon Interval:** Beacon Interval is in the range of **40~3500** and set in unit of *millisecond*. The default value is **100** msec.
  Access Point (AP) in IEEE 802.11 will send out a special approximated 50-byte frame, called

"Beacon". Beacon is broadcast to all the stations, provides the basic information of AP such as SSID, channel, encryption keys, signal strength, time stamp, support data rate.

All the radio stations received beacon recognizes the existence of such AP, and may proceed next actions if the information from AP matches the requirement. Beacon is sent on a periodic basis, the time interval can be adjusted.

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

- **DTIM Interval:** The DTIM interval is in the range of **1~255**. The default is **1**.

  DTIM is defined as *Delivery Traffic Indication Message*. It is used to notify the wireless stations, which support power saving mode, when to wake up to receive multicast frame. DTIM is necessary and critical in wireless environment as a mechanism to fulfill power-saving synchronization.

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

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

  Fragmentation threshold will be used when we have more data packet size to be transmitted and we have less fragment threshold value. 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, it's "***Enable***". To ***Disable*** is to use Long 128-bit Preamble Synchronization field.

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

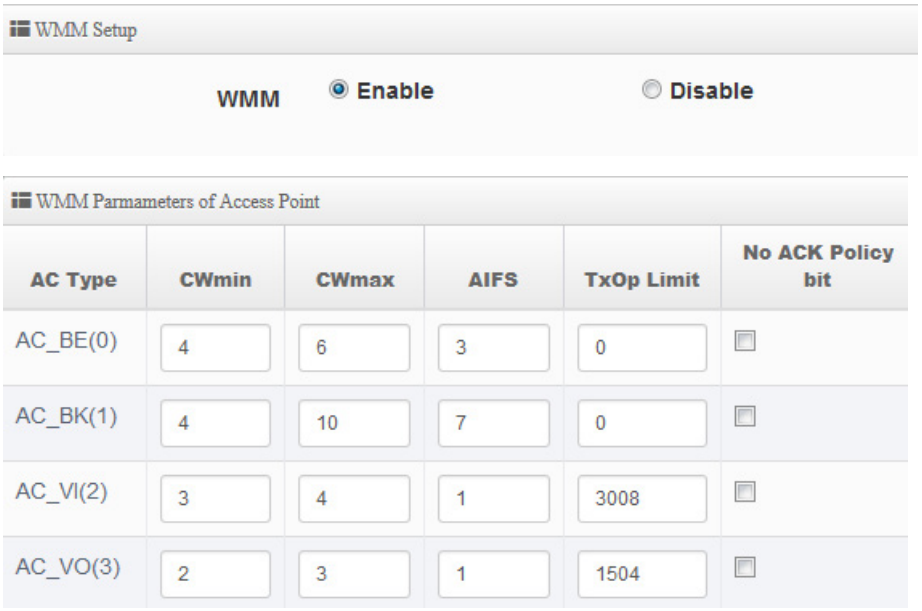
- **IGMP Snooping:** the process of listening to Internet Group Management Protocol (IGMP) network traffic. The feature allows a network switch to listen in on the IGMP conversation between hosts and routers. By listening to these conversations the switch maintains a map of which links need which IP multicast streams. Multicasts may be filtered from the links which do not need them and thus controls which ports receive specific multicast traffic.
- **Greenfield:** In wireless WLAN technology, greenfield mode is a feature of major components of the 802.11n specification. The greenfield mode feature is designed to improve efficiency by eliminating support for 802.11b/g devices in an all draft-n network. In greenfield mode the network can be set to ignore all earlier standards.

6.4.4 WMM Setup

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

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

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



WMM Parmameters of Station

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

✓ **AC Type**：

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

✓ **CWmin**：

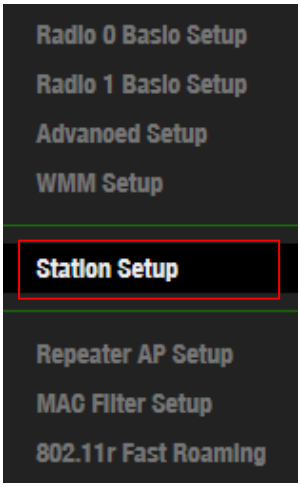
Minimum Contention Window. This parameter is input to the algorithm that determines the initial random backoff wait time ("window") for retry of a transmission. The value specified here in the Minimum Contention Window is the upper limit (in milliseconds) of a range from which the initial random backoff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

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

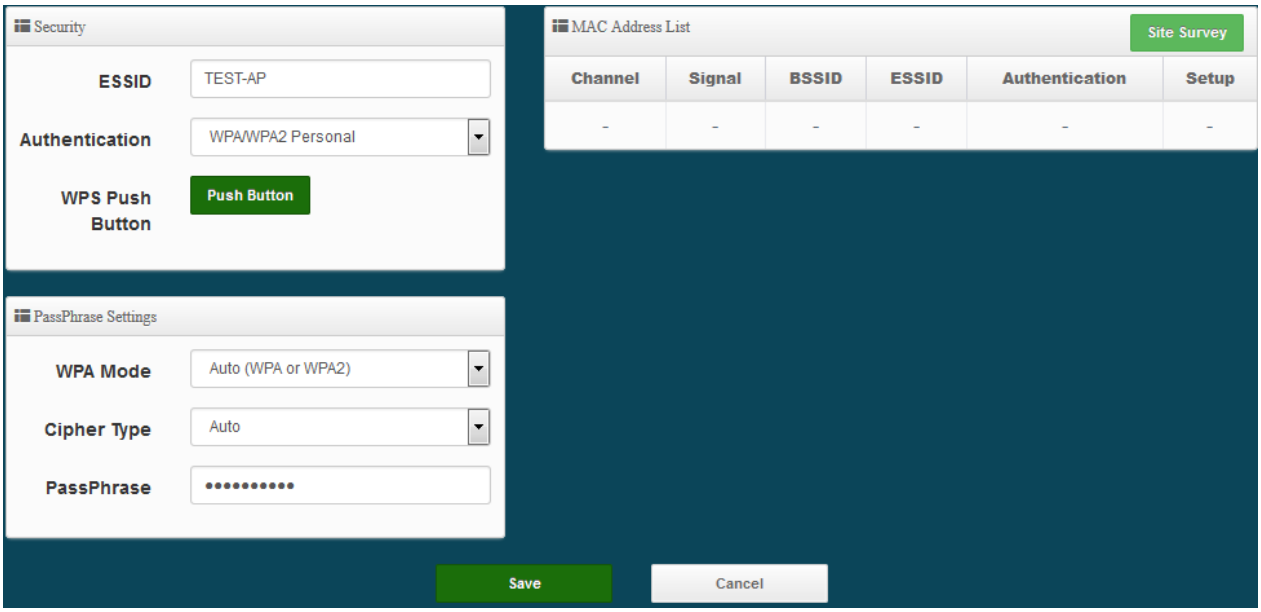
✓ **AIFS**：The Arbitration Inter-Frame Spacing Number specifies a wait time (in milliseconds) for data frames ◦

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

6.4.5 Station Setup



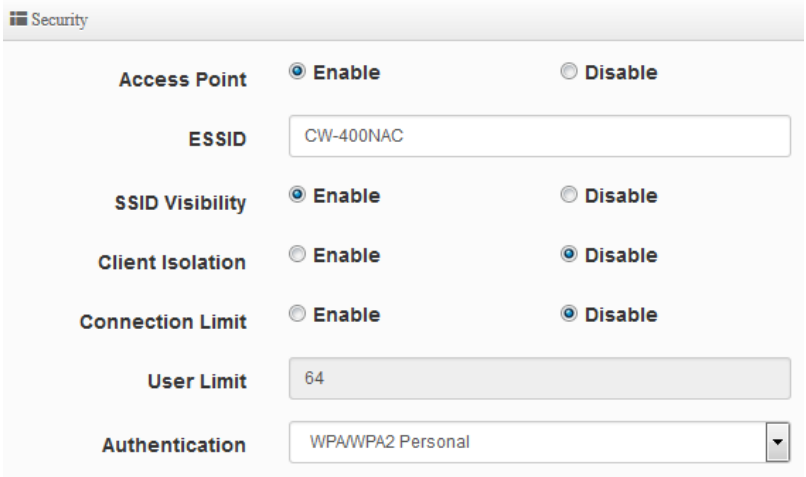
The functions setting functions include Client Bridge link to AP station. Administrator can used "site survey" function to Search for AP stations.



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

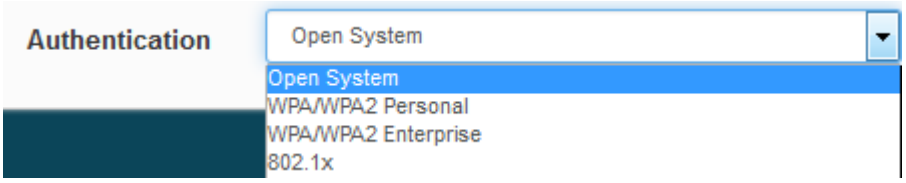
6.4.6 Repeater AP Setup

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

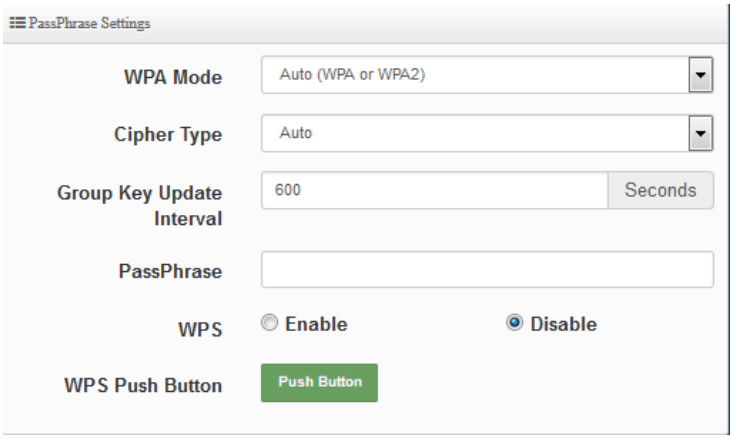


- **Access Point:** Administrator can Enable or Disable the Repeater AP function.
- **ESSID:** Enter the Repeater AP of ESSID name.
- **SSID Visibility:** The default it's Enable**.** When select Disable the SSID will not is discovered.
- **Client Isolation:** This function is Disabled by default. All 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.



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



✓ **WPA Mode:** Administrator can select security for Auto or only WPA or only WPA2.

✓ **Cipher Type:** Administrator can select use AES or TKIP with WPA / WPA2 encryption method.

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

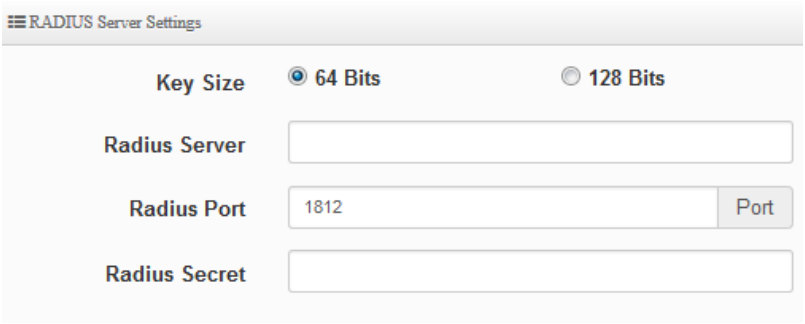
TKIP is short for "**Temporal Key Integrity Protocol**", TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with.

✓ **Group Key Update Interval**: This time interval for re-keying GTK (broadcast/multicast encryption keys) in seconds. Enter the time-length required; the default time is 600 seconds.

✓ **Pass Phrase:** Enter the ESSID pass phrase.

✓ **WPS:** Administrator can used WPS function link WiFi client, if select enable the function, administrator can click the WPS Push Button.

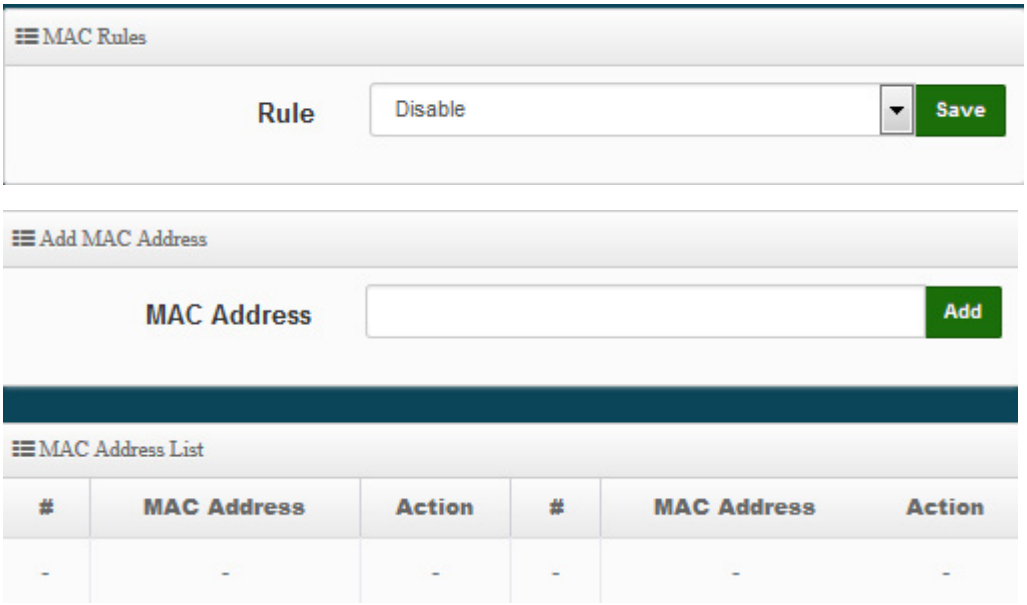
- **802.1X security:** When 802.1x Authentication is enabled, please refer to the following Dynamic WEP and RADIUS settings to complete the configuration.



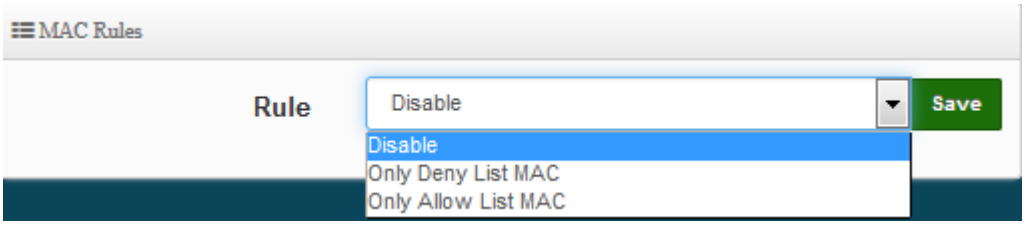
- ✓ **Key Size:** Check on the respected button to enable either 64bits or 128bits key length. The system will automatically generate WEP keys for encryption.
- ✓ **Radius Server:** Enter the IP address of the Authentication RADIUS server.
- ✓ **Radius Port:** The port number used by Authentication RADIUS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

6.4.7 MAC Filter

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



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

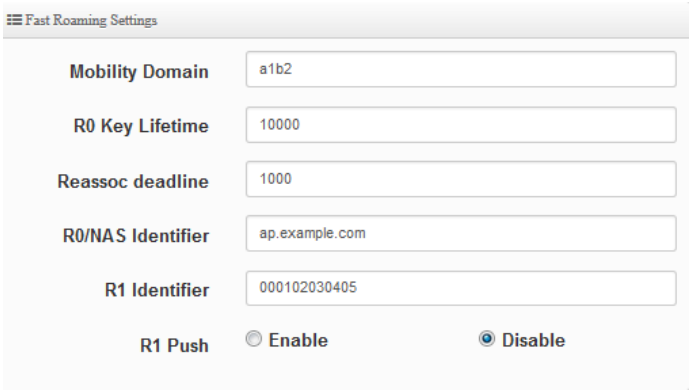


- **Only Allow List MAC**: Define certain wireless clients in the list which will have granted access to the Access Point while the access will be denied for all the remaining clients – Action Type is set to "**Only Allow List MAC**".
- **Only Deny List MAC**: Define certain wireless clients in the list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

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

6.4.8 802.11r/802.11k Fast Roaming

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

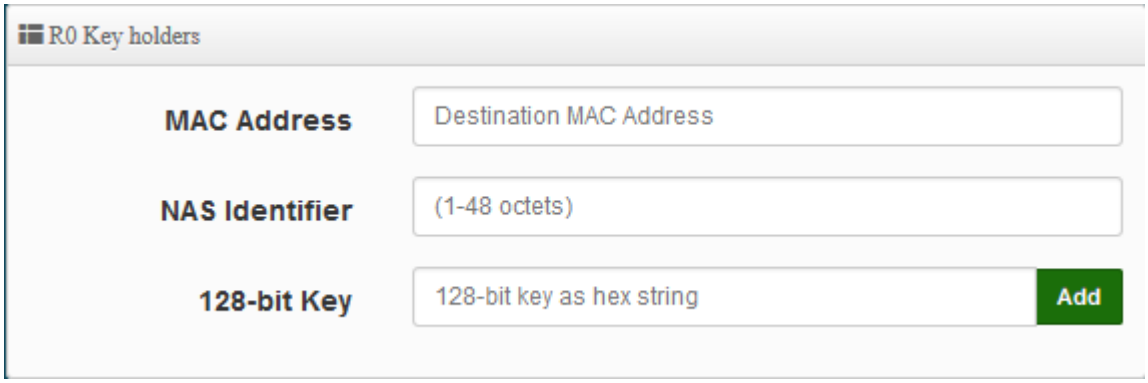


- **Mobility Domain:** MDID is used to indicate a group of APs (within an ESS, i.e., sharing the same SSID) between which a STA can use Fast BSS Transition. Please enter 2-octet identifier as a hex string.
- **R0 Key Lifetime:** Default lifetime of the PMK-RO in minutes, the default is 10000, administrator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

- **R1 Identifier:** PMK-R1 Key Holder identifier 6-octet identifier as a hex string.
- **R1 Push:** Administrator can select Enable or disable. If enable the function will automatically sent the R1 Key.

R0 Key Address:

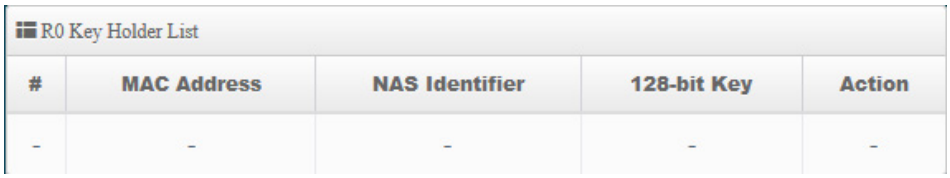
To enable roaming between multiple AP devices, AP1 must key in the MAC Address of AP2, and AP2 must key in the MAC Address of AP1. The NAS Identifier and 128-bit Key should be identical in both AP settings. This will enable device roaming between the two Access Points.



- **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.

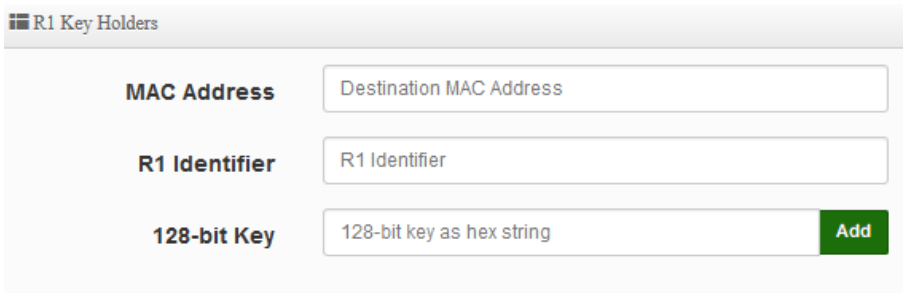
R0 Key Holder List:

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



R1 Key Holder List:

Enter a unified set of R1 Key Holder identification certification.



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

R1 Key Holder List:

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

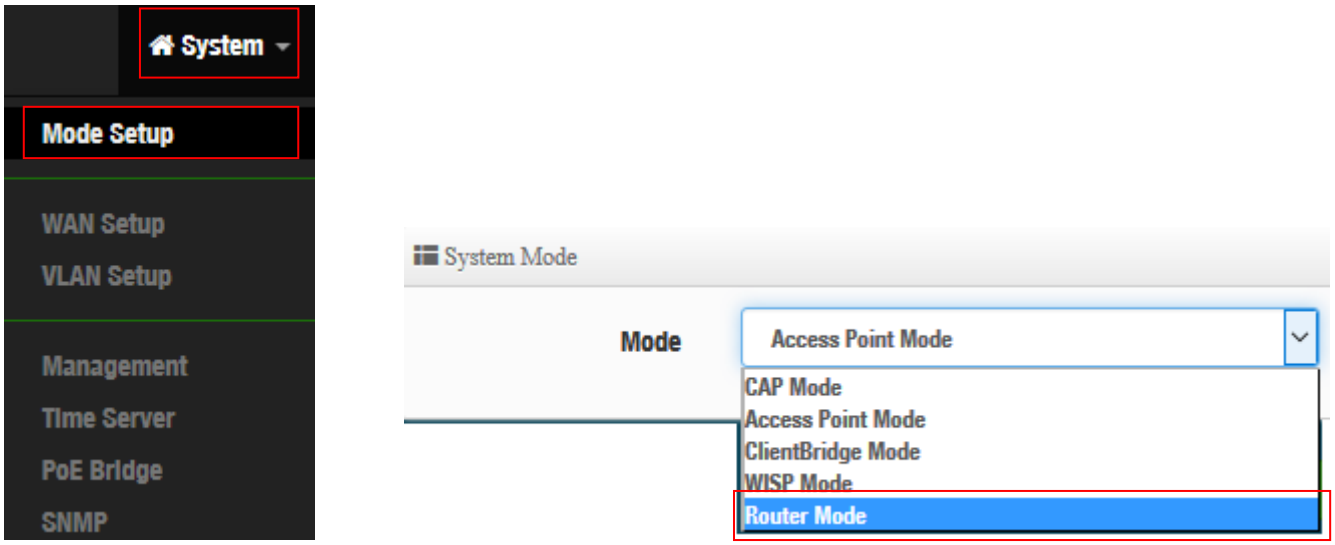
R1 Key Holder List

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

7. Router Mode

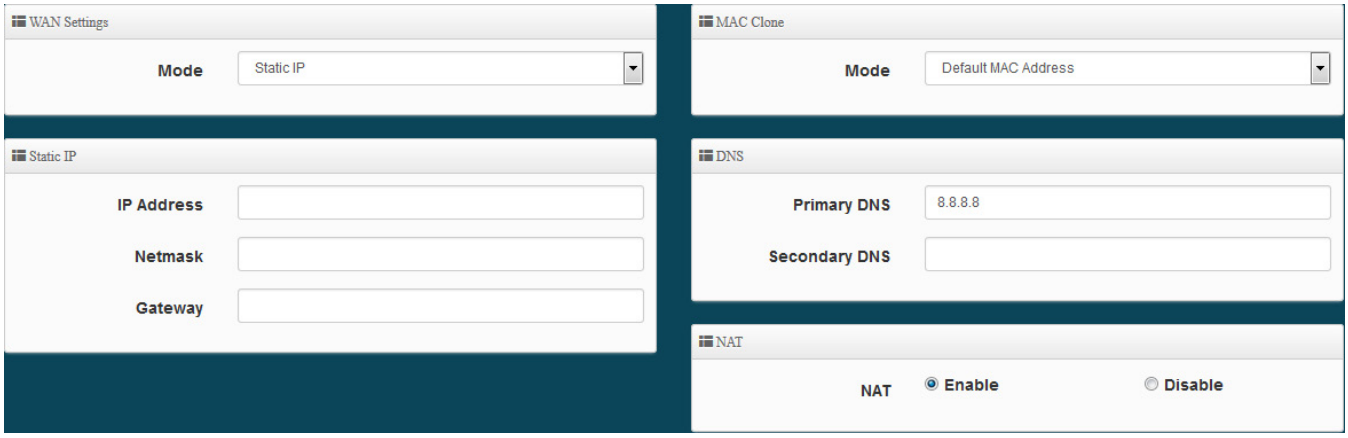
When Router AP mode is chosen, the system can be configured as an Router AP mode. This section provides detailed explanation for users to configure in the Router AP mode with help of illustrations. In the Router AP mode, functions listed in the table below are also available from the Web-based GUI interface.

Please click **"System"➔" Mode Setup"** to change Router Mode.

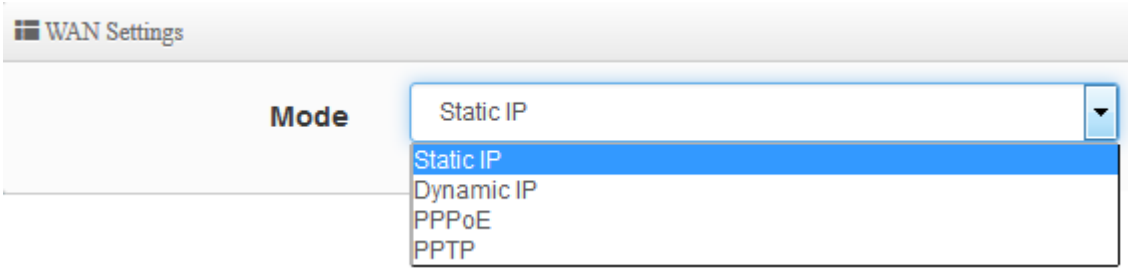


7.1 Configure WAN Setup

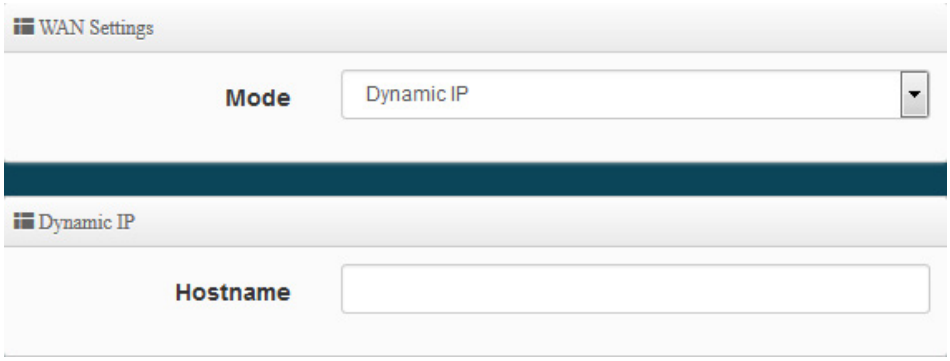
There are four connection types for the WAN port: **Static IP**, **Dynamic IP**, **PPPoE** and **PPTP**. Please click on **System -> WAN** and follow the below setting.



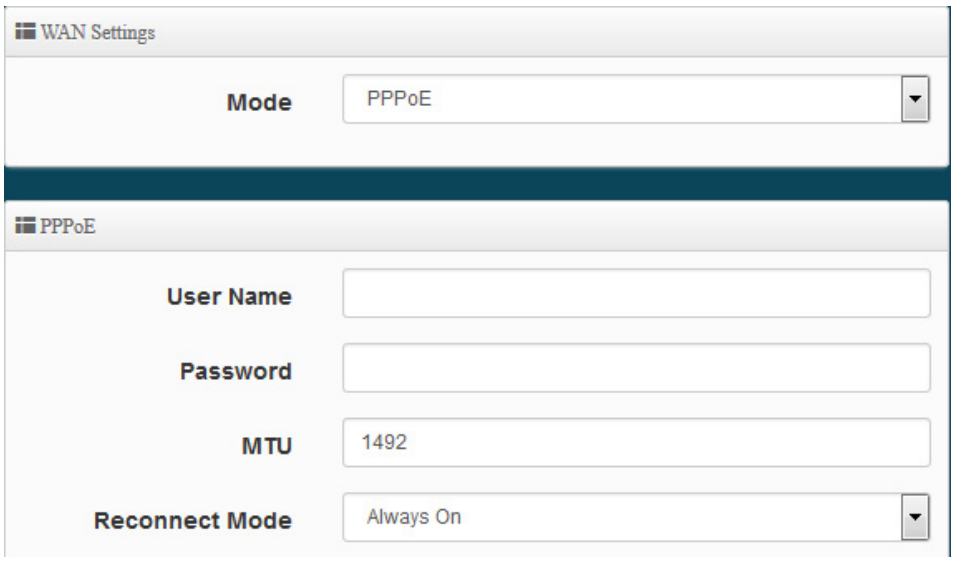
WAN Setting



- **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.



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

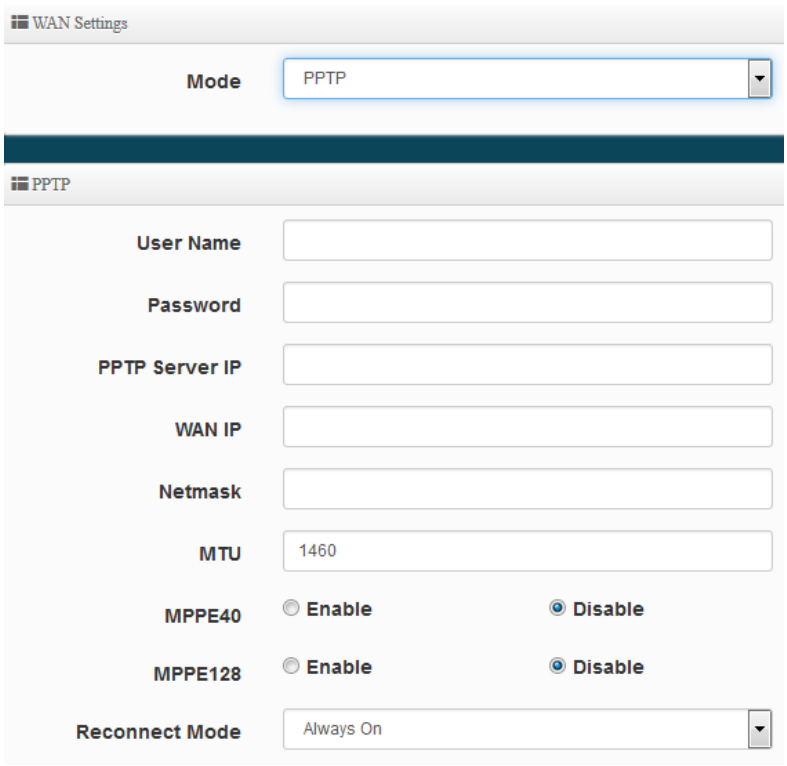


- **User Name :** Enter User Name for PPPoE connection
- **Password :** Enter Password for PPPoE connection
- **MTU:** By default, MTU is set to **1492** bytes. MTU stands for Maximum Transmission Unit. Consult with WISP for a correct MTU setting.
- **Reconnect Mode:** Administrator can select three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

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

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

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



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

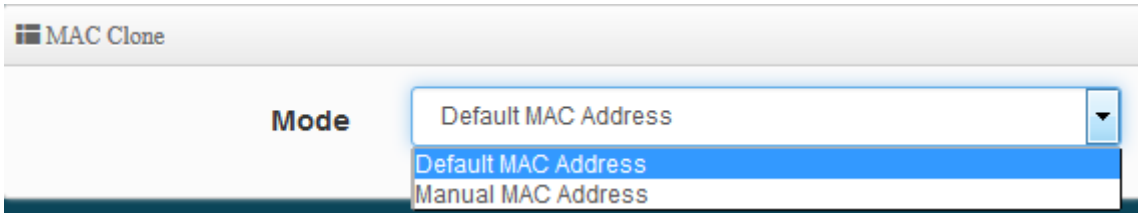
Notice

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

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

➢ MAC Clone

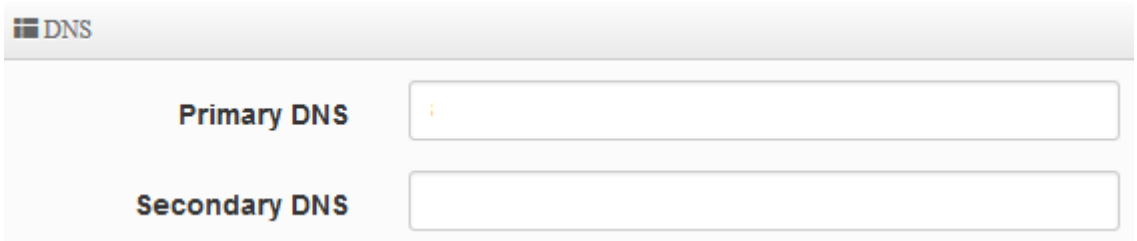
The MAC address is a 12-digit HEX code uniquely assigned to hardware as identification. Some ISPs require you to register a MAC address in order to access to Internet. If not, you could use default MAC or clone MAC from a PC.



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

➢ DNS

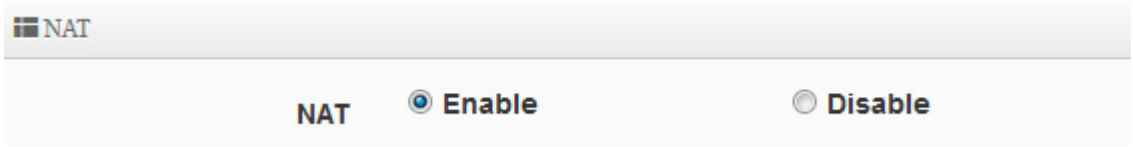
Check “No Default DNS Server” or “Specify DNS Server IP” radial button as desired to set up system DNS.



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

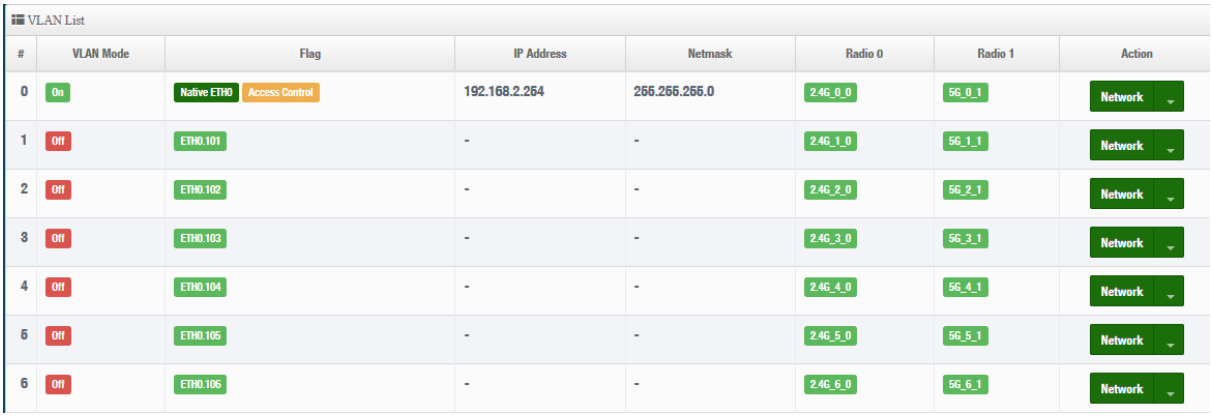
➢ NAT

The NAT support Enable and Disable Service



7.2 Configure LAN Setup

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

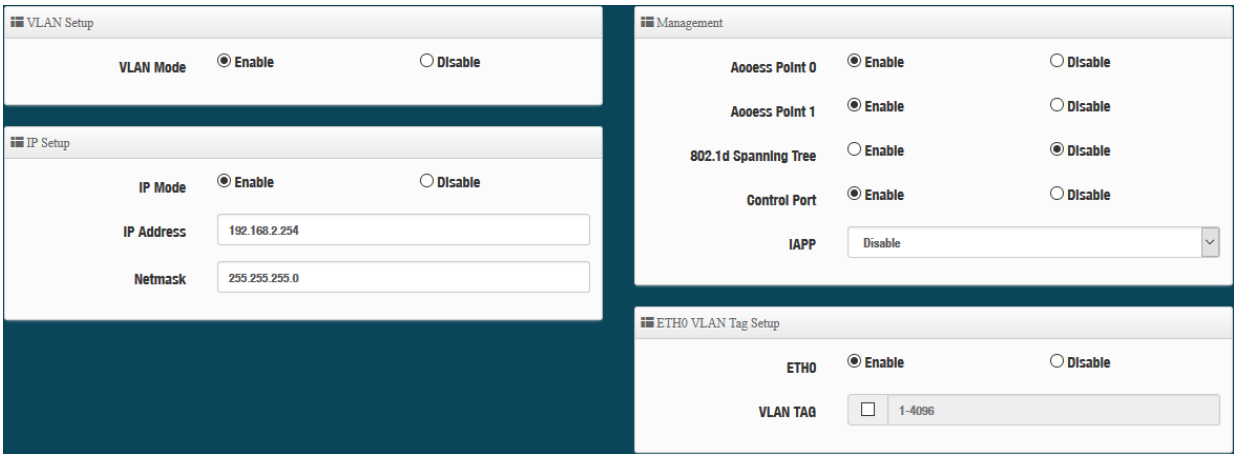


- **VLAN Mode**：Display on/off for the VLAN network.
- **Flag**：Display master VLAN and VLAN Tag No. information.
- **IP Address**：Display IP Address for VLAN Network.
- **NetMask**：Display IP netmask.
- **Radio 0**：Display radio 2.4G or 5GHz SSID name (Depending on 11ac or 11n model)
- **Radio 1**：Display radio 5G SSID name.
- **Action**：The button can set VLAN network functions and radio functions.

7.2.1 Network Button

Administrator can click

utton to set VLAN network functions.



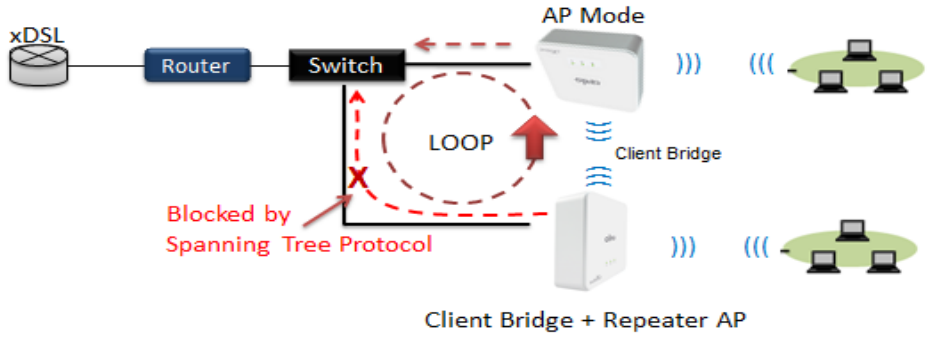
- **VLAN Mode**：Administrator can select Enable or disable for the VLAN Network.

Notice | At least one VLAN must always be enabled

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

Management

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



Client Bridge + Repeater AP

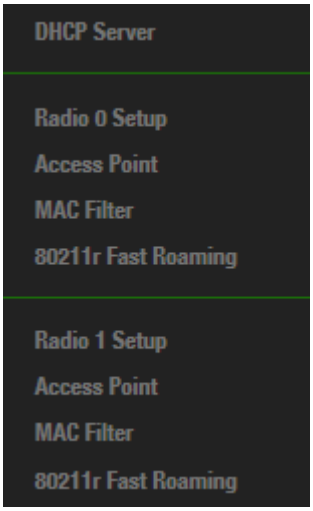
- **Control Port**：Administrator can select one of the VLAN as managed AP.
- **IAPP**：Administrator can select radio 2.4G or 5G for IAPP roaming.*(the IAPP condition must use WPA2-PSK Wi-Fi security and AES algorithm)*

7.2.2 Network Pull-down menu

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

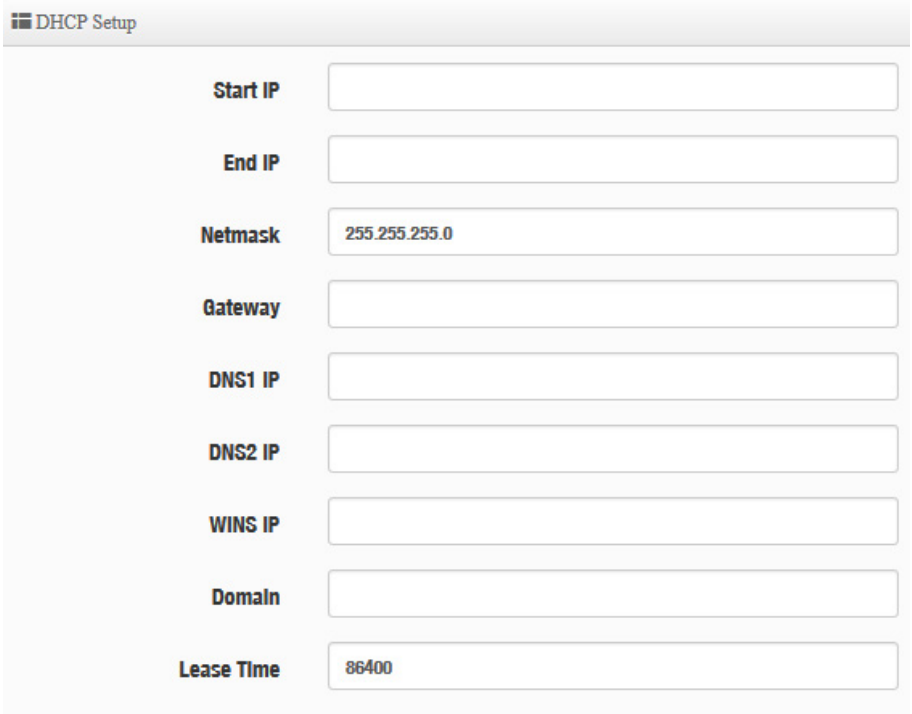
Please click

pull-down button.



DHCP Server

Administrator can select enable / disable the function

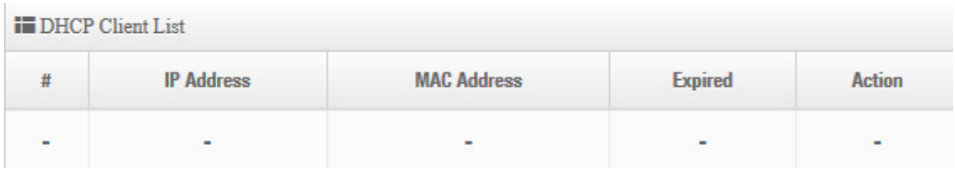


- **Start IP:** Set Start IP for DHCP Service.
- **End IP:** Set End IP for DHCP Service.
- **Netmask: Set IP Netmask, the default is 255.255.255.0**
- **Gateway: Set Gateway IP for DHCP Service.**

- **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.



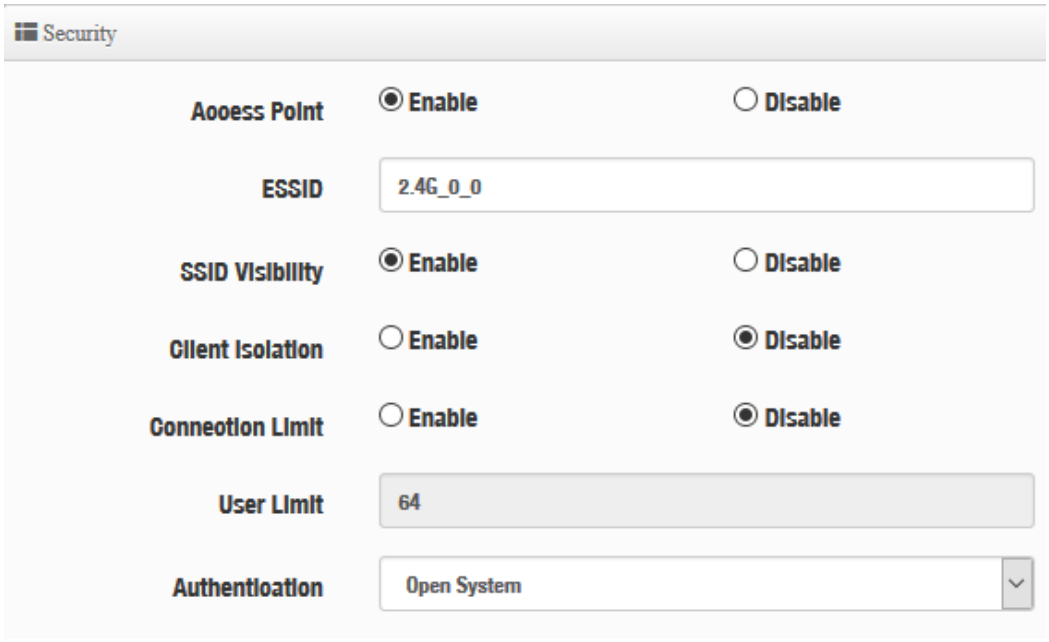
Static Lease IP Setup

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

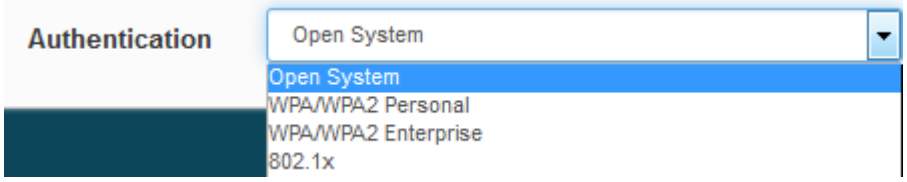
- **Comment:** Enter rule description.
- **IP Address:** Enter access point IP.
- **MAC Address:** Enter Client MAC Address of PC network.

Radio 0/1 Access Point

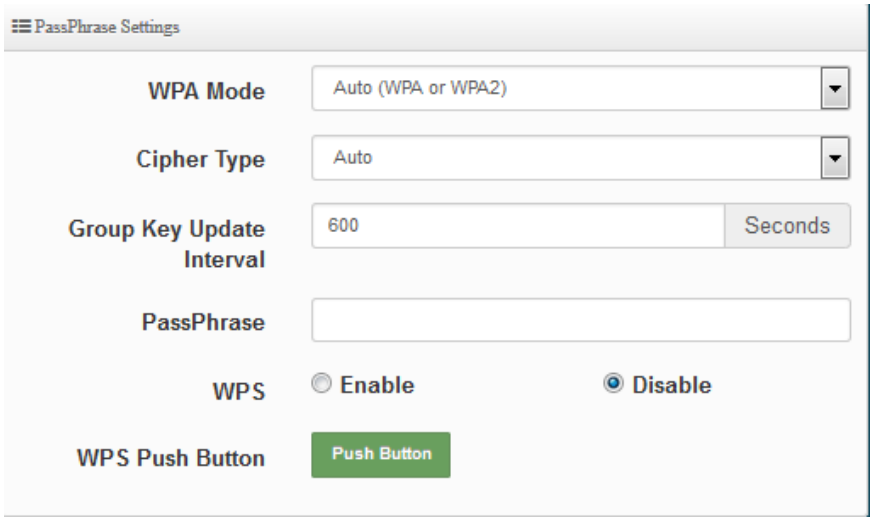
Administrator can Enable or Disable radio 0/1 (2.4/5G) Wi-Fi. If radio 0/1 (2.4/5G) are enabled, administrators can set the SSID and security for the 2.4/5G access point.



- **Access Point:** Administrator can Enable or Disable the radio 0/1 (2.4G or 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.
- **Authentication:** Select the desired security type from the drop-down list; the options are WPA-PSK, WPA2-PSK, WPA/WPA2-Enterprise and WEP 802.1X.



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



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

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

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

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

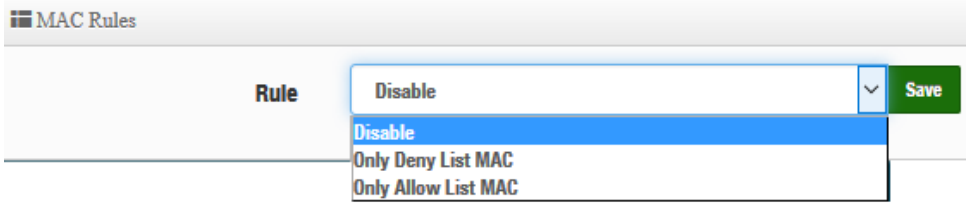
- ● **802.1X security:** When 802.1x Authentication is enabled, please refer to the following Dynamic WEP and RADIUS settings to complete the configuration.

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

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

MAC Filter

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

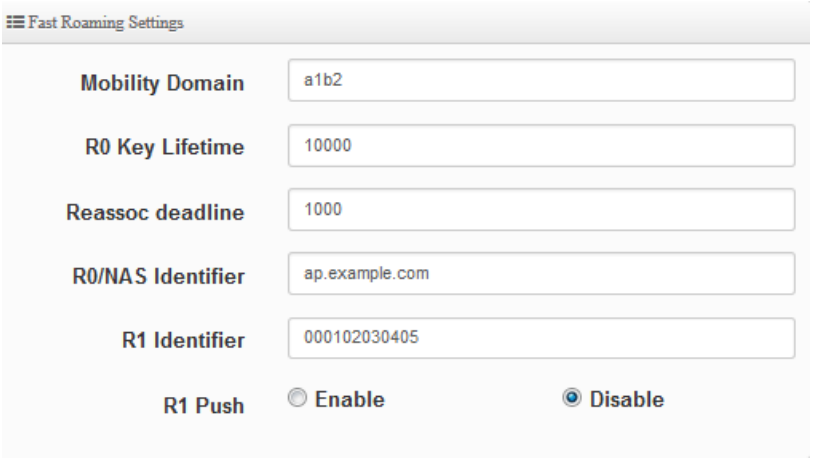


- ➢ **Disable**：Disable MAC Filter function.
- ➢ **Only Deny List MAC**：Administrator can add wireless users MAC address in MAC list. The access point will deny connection in MAC address list.
- ➢ **Only Allow List MAC**：Administrator can add wireless users MAC address in MAC list. The access point will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

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

802.11r/802.11k Fast Roaming

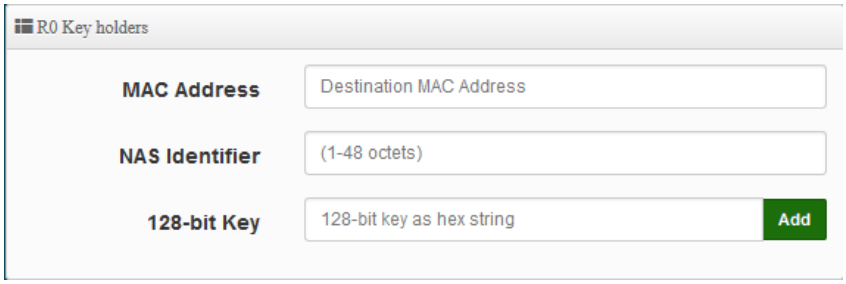
The dual band Access Point supports 802.11r/802.11k function for 2.4G and 5G radio. 802.11r, which is the IEEE standard for fast roaming, introduces a new concept of roaming where the initial handshake with the new AP is done even before the client roams to the target AP.



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

R0 Key Address:

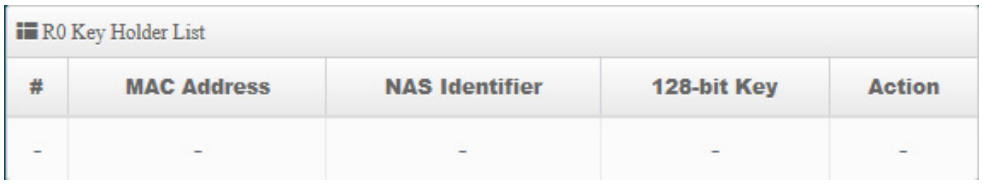
To enable roaming between multiple AP devices, AP1 must key in the MAC Address of AP2, and AP2 must key in the MAC Address of AP1. The NAS Identifier and 128-bit Key should be identical in both AP settings. This will enable device roaming between the two Access Points.



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

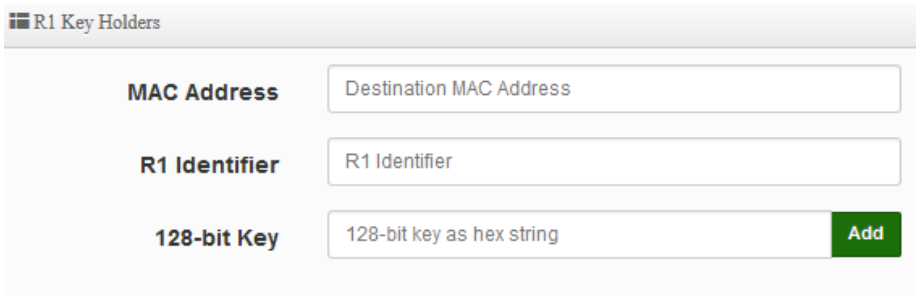
R0 Key Holder List:

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



R1 Key Holder List:

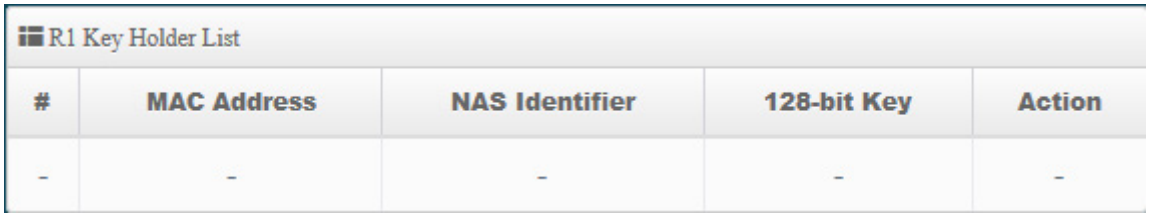
Enter a unified set of R1 Key Holder identification certification.



- **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.



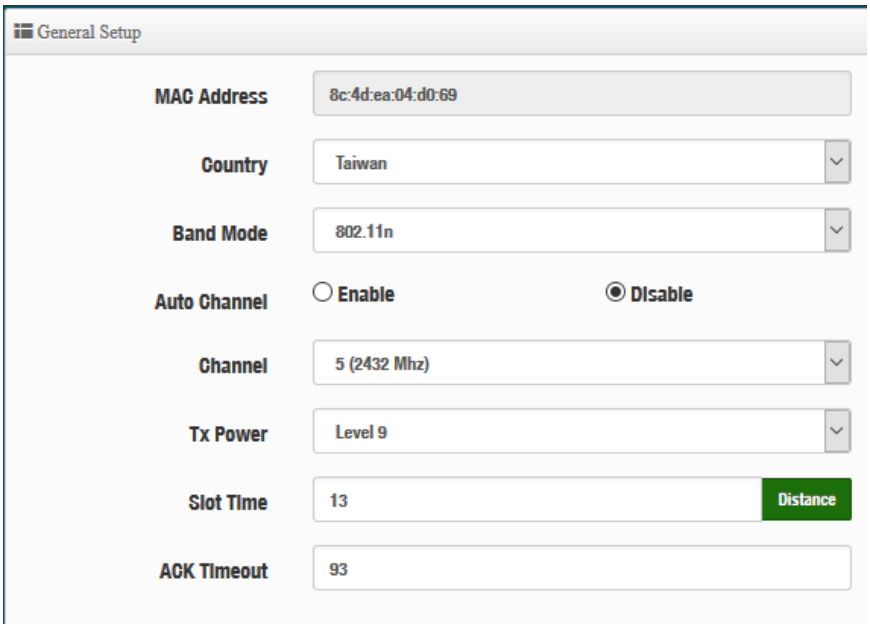
Click "**Save"** button to save your changes. Then click **Reboot** button to activate your changes.

7.3 Wireless Basic Setup

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

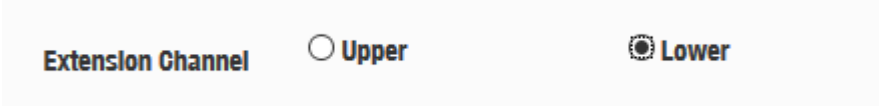
7.3.1 Radio 0 Basic Setup (2.4G)

General setup



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

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



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

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

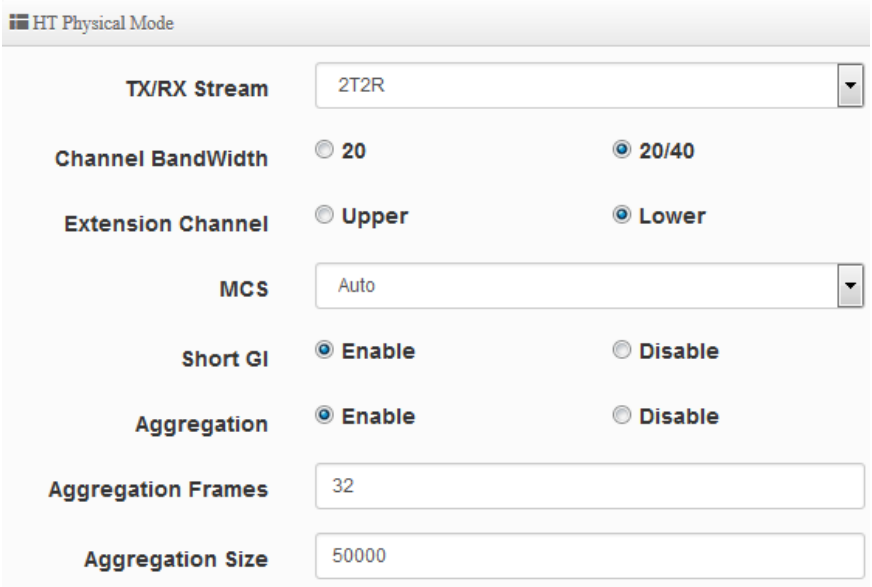
  All data transmission in 802.11b/g request an "Acknowledgement" (ACK) send by receiving radio. The transmitter will resend the original packet if correspondent ACK failed to arrive within specific time interval, also refer to as "ACK Timeout".

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

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

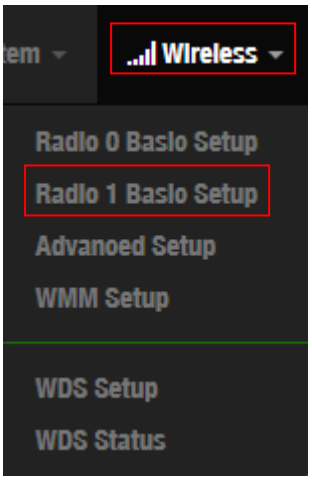
Notice	Slot Time and ACK Timeout settings are for long distance links. It is important to tweak settings to achieve the optimal result based on requirement.

HT Physical Mode

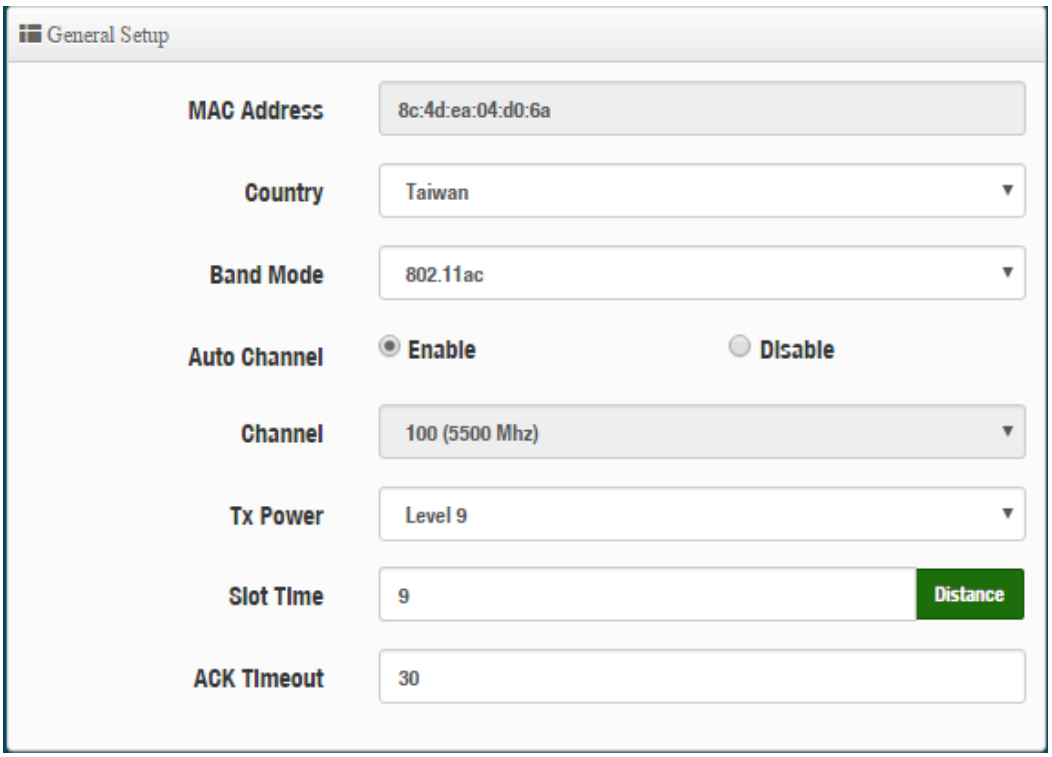


- **TX/RX Stream:** CenOS 5.0 APs utilizes 2 antenna and supports 2TX/2RX streams. Administrator can select 1 or 2 TX/RX. The default is 2TX/2RX.
- **Channel Bandwidth:** The "**20/40**" MHz option is usually best. The other option is available for special circumstances.
- **Extension Channel:** Sets channel select to Upper or Lower. The Upper supports 1 to 7 range CH and Lower supports 5 to 11 range CH.
- **MCS:** This parameter represents transmission rate. By default (Auto) the fastest possible transmission rate will be selected. You have the option of selecting the speed if necessary.
- **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:** The Aggregation Frames is in the range of **2~64**, default is **32**. It determines the number of frames combined on the new larger frame.
- **Aggregation Size:** The Aggregation Size is in the range of **1024~65535**, default is **50000**. It determines the size (in Bytes) of the larger frame.

7.3.2 Radio 1 Basic Setup (5G)



General Setup



- **MAC Address:** Display 2.4G WiFi MAC address.
- **Country:** Administrator can select country: US or EU or Taiwan.
- **Band Mode:** Administrator can select 5G Band for 802.11a/n or 802.11ac. The default is 802.11ac
- **Auto Channel:** Administrator can Enable or Disable the function. If select disabled function the WiFi channel can be manually fixed.
- **Channel:** Supports US and EU country 5G Channel standards.
- **Tx Power:** Administrator can control the WiFi Tx output power. The power Max. Level 9.
- **Slot Time:** Slot time is in the range of **9~1489** and set in unit of ***microsecond***. The default value is **9** microsecond.

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

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

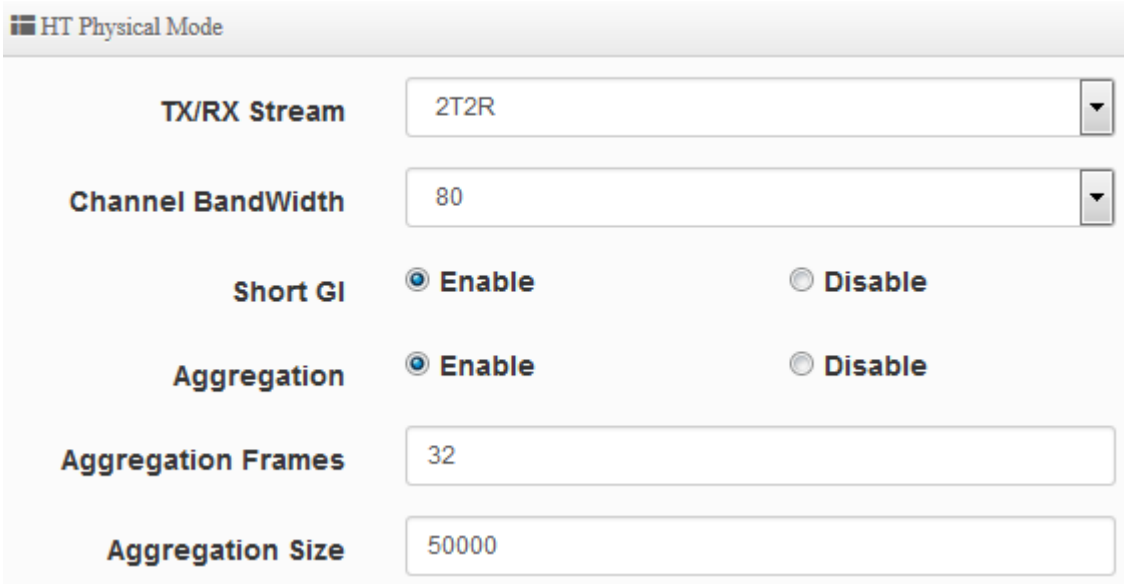
  All data transmission in 802.11b/g request an "Acknowledgement" (ACK) send by receiving radio. The transmitter will resend the original packet if correspondent ACK failed to arrive within specific time interval, also refer to as "ACK Timeout".

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

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

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

HT Physical Mode

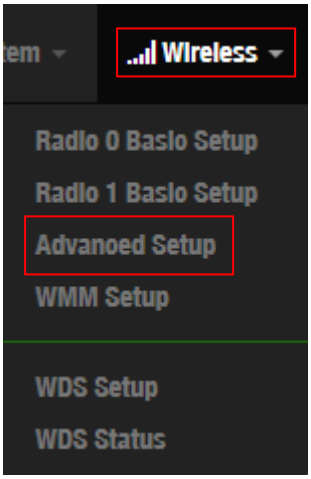


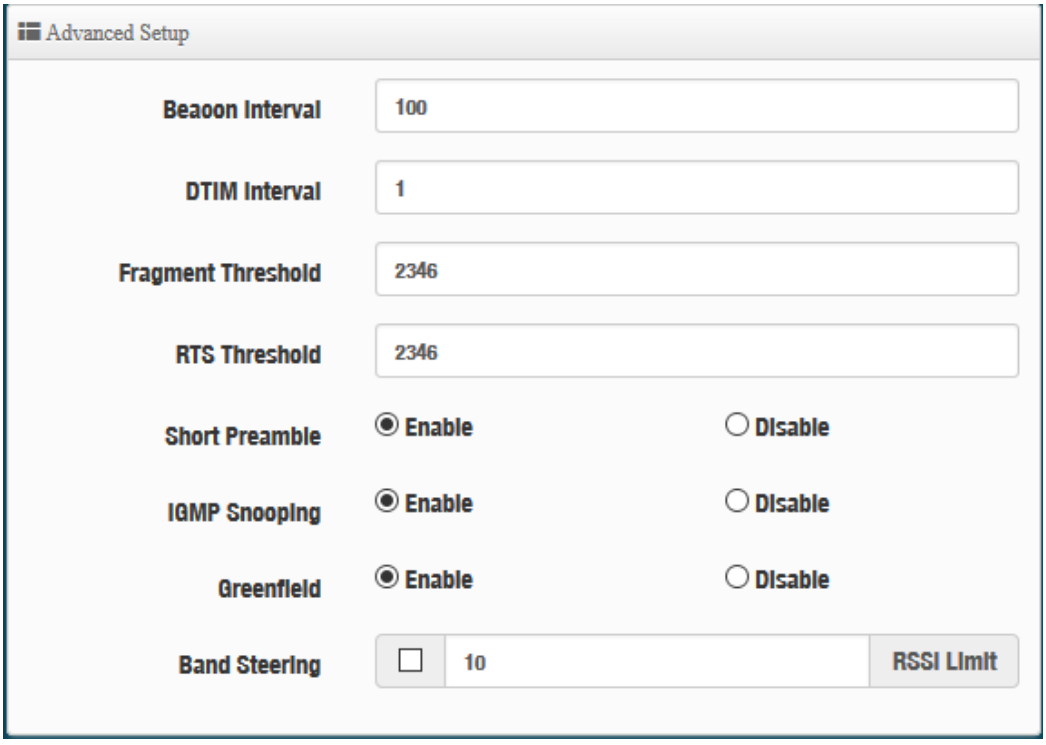
- **TX/RX Stream:** CenOS 5.0 APs utilizes 2 antennas and supports 2TX/2RX streams. Administrator can select 1 or 2 TX/RX. The default is 2TX/2RX.
- **Channel Bandwidth:** The "**20/40 and 802.11ac 80**" MHz option is usually the best. The other option is available for special circumstances.
- **Shout 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.
- **Aggregation Frames:** The Aggregation Frames is in the range of **2~64**, default is **32**. It determines the number of frames combined on the new larger frame.
- **Aggregation Size:** The Aggregation Size is in the range of **1024~65535**, default is **50000**. It determines the size (in Bytes) of the larger frame.

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

7.3.3 Advanced Setup

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





- **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 Steering: Dual band operation with Band Steering** detects clients capable of 5 GHz operation and steers them to that frequency which leaves the more crowded 2.4 GHz band available for legacy clients. This helps improve end user experience by reducing channel utilization, especially in high density environments. The default RSSI Limit :10

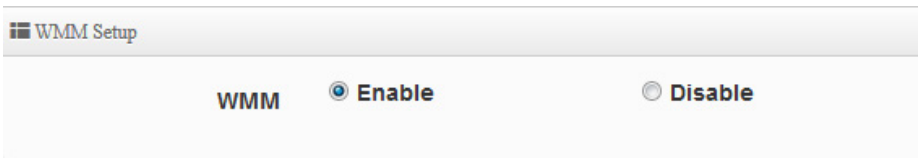
7.3.4 WMM Setup

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

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

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

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



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

WMM Parmameters of Access Point

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

WMM Parmameters of Station

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

✓ **AC Type**：

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

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

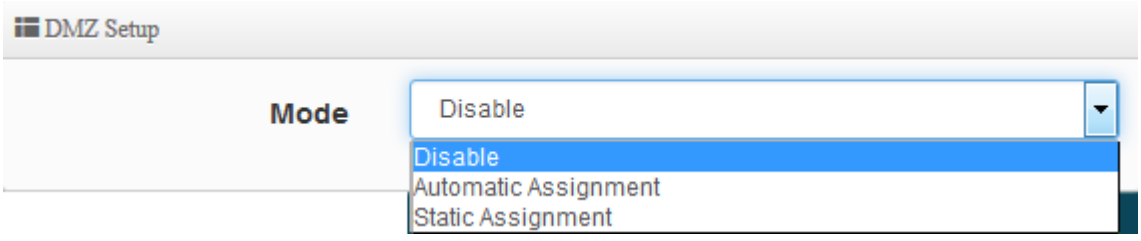
✓ **CWmax**: Maximum Contention Window. The value specified here in the Maximum Contention Window is the upper limit (in milliseconds) for the doubling of the random backoff value. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached. Once the Maximum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

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

8. Advanced Setup By WISP & Router Mode

8.1 DMZ

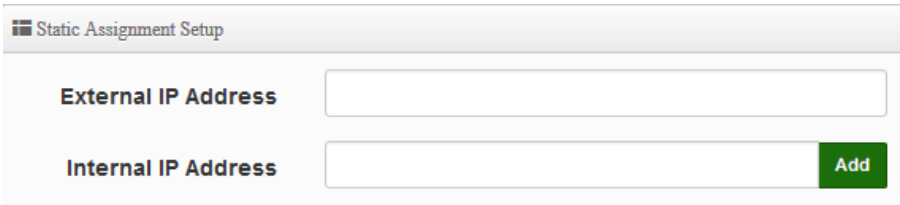
DMZ is commonly work with the NAT functionality as an alternative of Virtual Server(Port Forwarding) while wanting all ports of DMZ host visible to Internet users. Virtual Server rules have precedence over the DMZ rule. In order to use a range of ports available to access to different internal hosts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



➢ **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



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

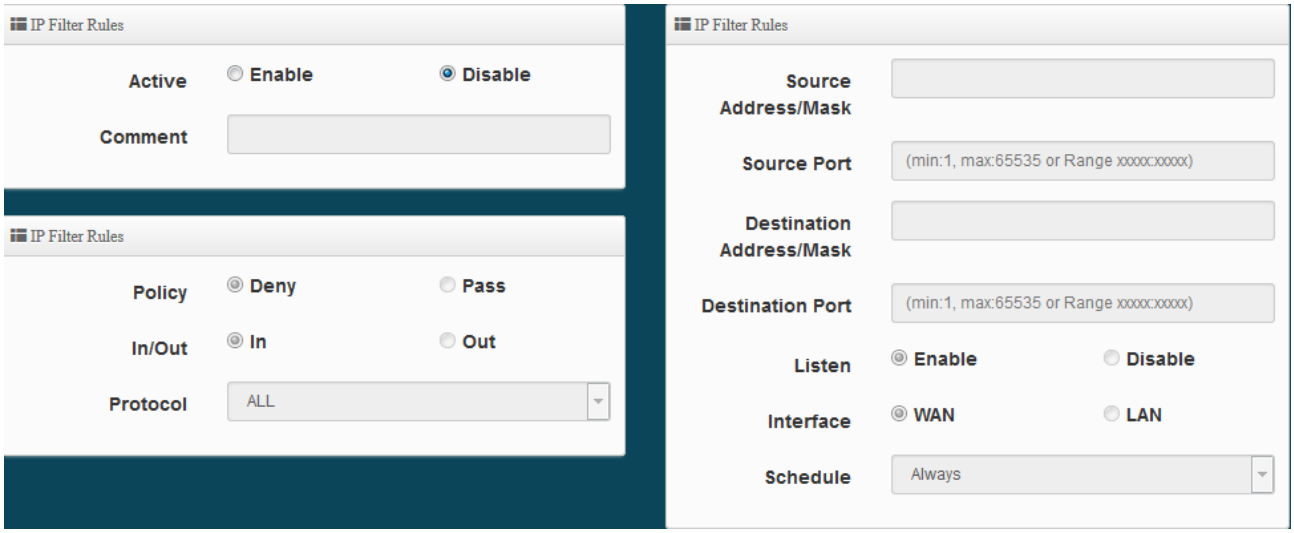
8.2 IP Filter

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

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.

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

Example 1:

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

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

Example 2:

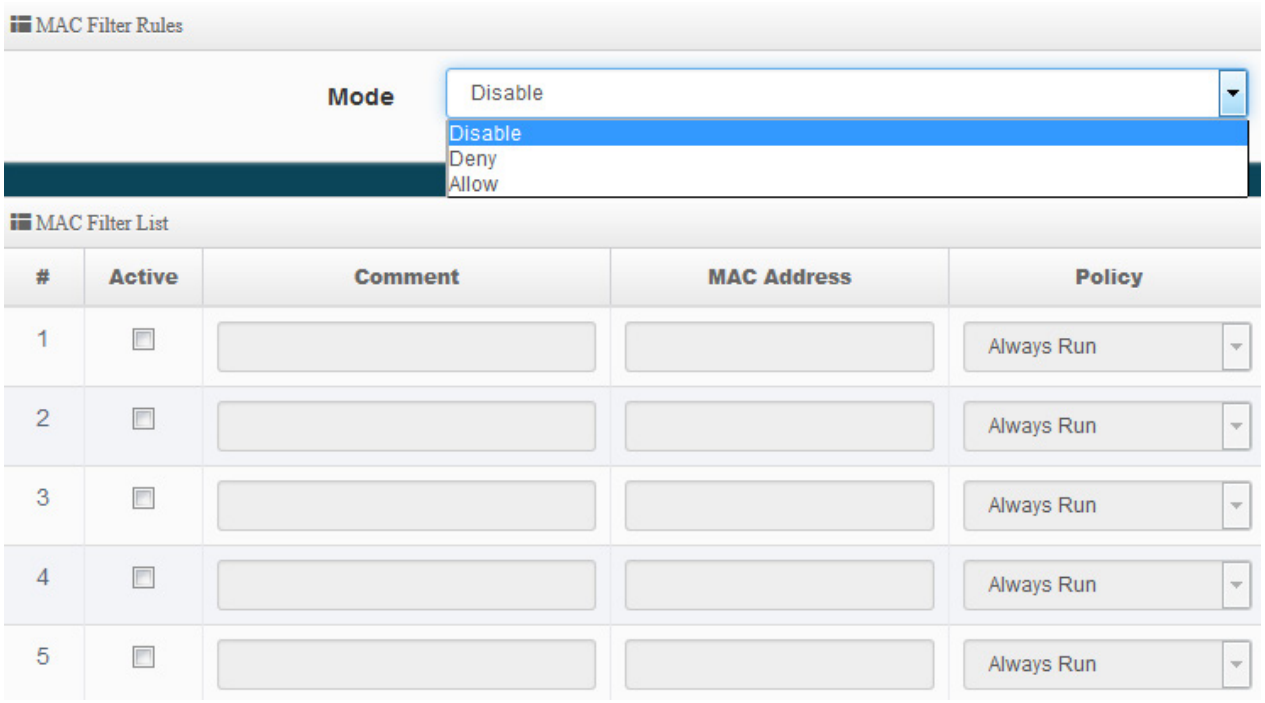
All Telnet access to the system from the IP addresses of subnet 192.168.2.x works with the rule 1 of Example 2. The rule 2 won't make any difference.

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

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

8.3 MAC Filter

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



- **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".**

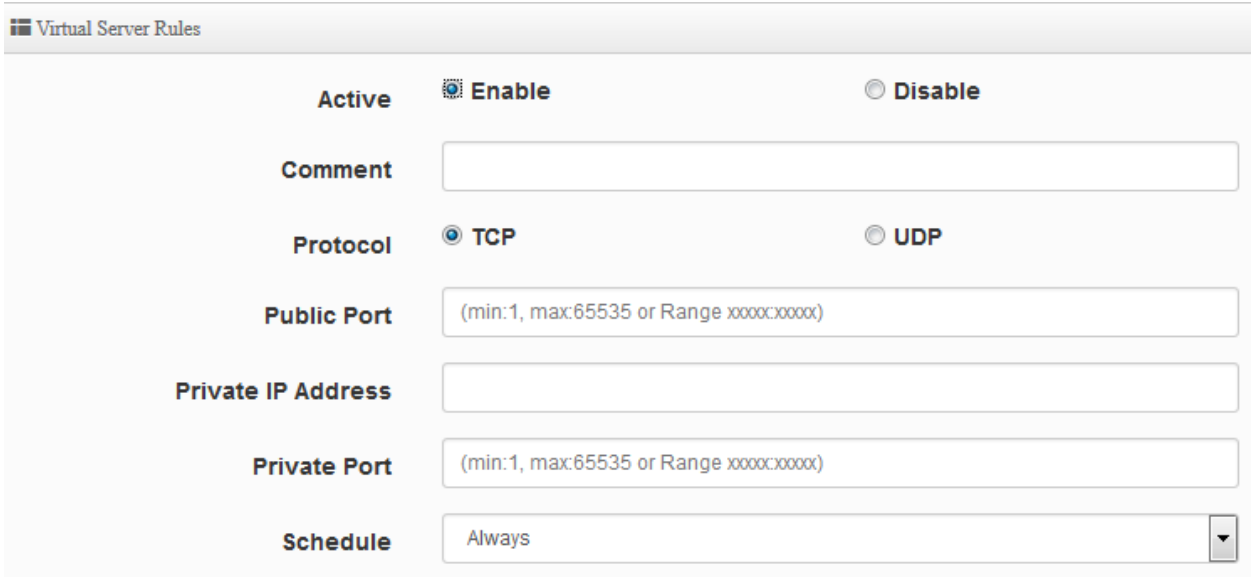
8.4 Virtual Server

The **"Virtual Server"** can also referred to as "Port Forward" as well and used interchangeably. Resources in the network can be exposed to the Internet users in a controlled manner including on-line gaming, video conferencing or others via Virtual Server setup. Don't repeat ports' usage to avoid confusion.
Suppose you want to assign ports 21-25 to one FTP, Telnet and SMTP server (A in the example), and port 80 to another (B in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

Virtual Server List

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

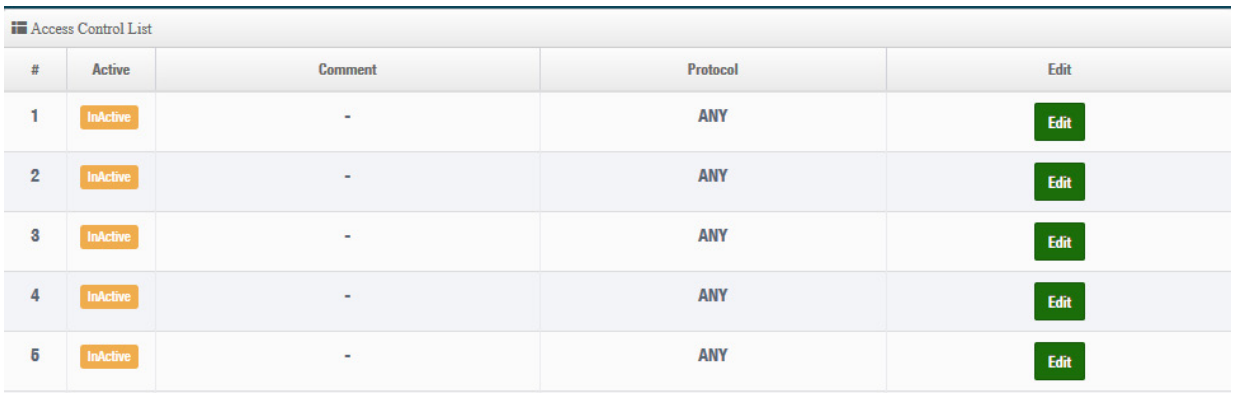
Please click **Edit** button to setting Virtual Server rules.



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

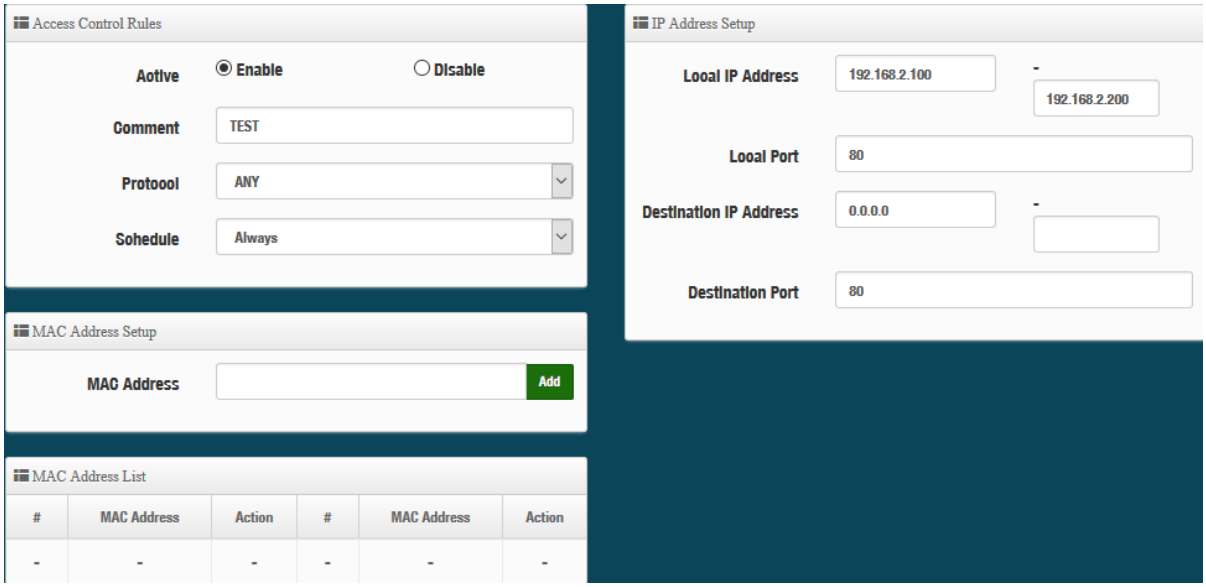
8.5 Access Control

The Access Control function administrator can to block or allow specific kinds of TCP/UDP/ICMP protocol, such as Internet access, designated services, and websites. The Access Control function can set 20 profiles. Please click on **Advance -> Access Control** and follow the below setting.



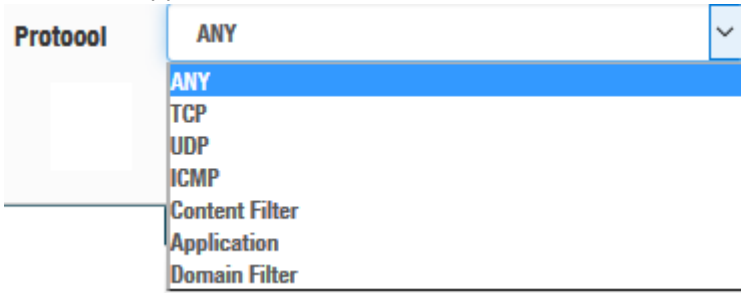
- **#**：Display access control list.
- **Active**：Display Active or InActive for the access control rule.
- **Comment:** Display information for the rule.

- **Protocol**：Display information for the protocol.
- **Edit**：Administrator can click the button to set Access Control rule.



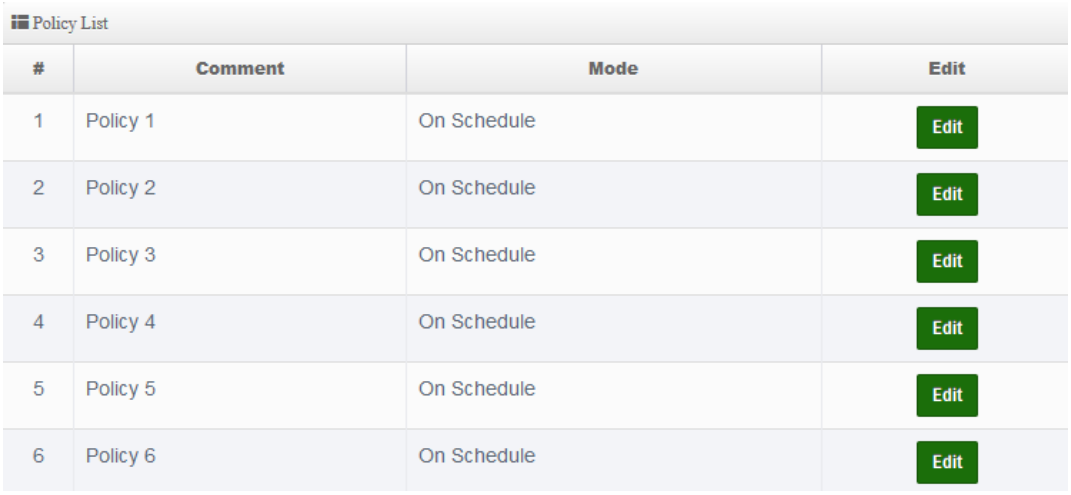
 # Access control rules：

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

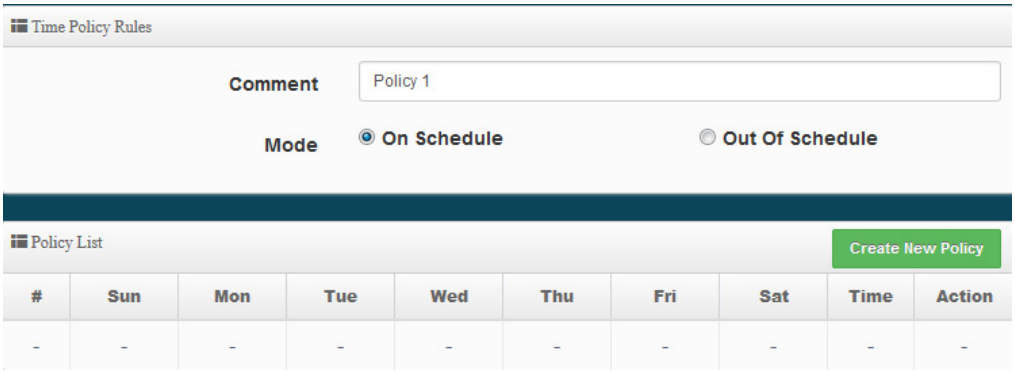


- ✓ **ANY:** Select **"Any"** is all deny Protocol, administrator can filter local IP / IP range go to destination IP / IP range and use protocol.
- ✓ **TCP:** Deny TCP Protocol, Administrator can set TCP protocol and assign IP / IP range.
- ✓ **UDP:** Deny UDP Protocol, Administrator can set UDP protocol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

8.6 Time Policy



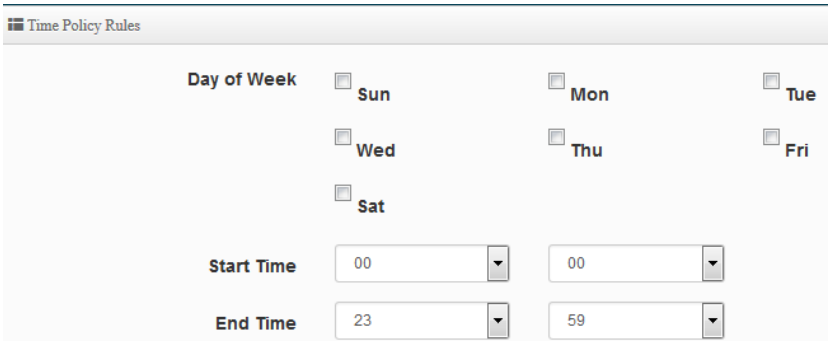
Please click **Edit** button to setting Time Policy rules.



- **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.



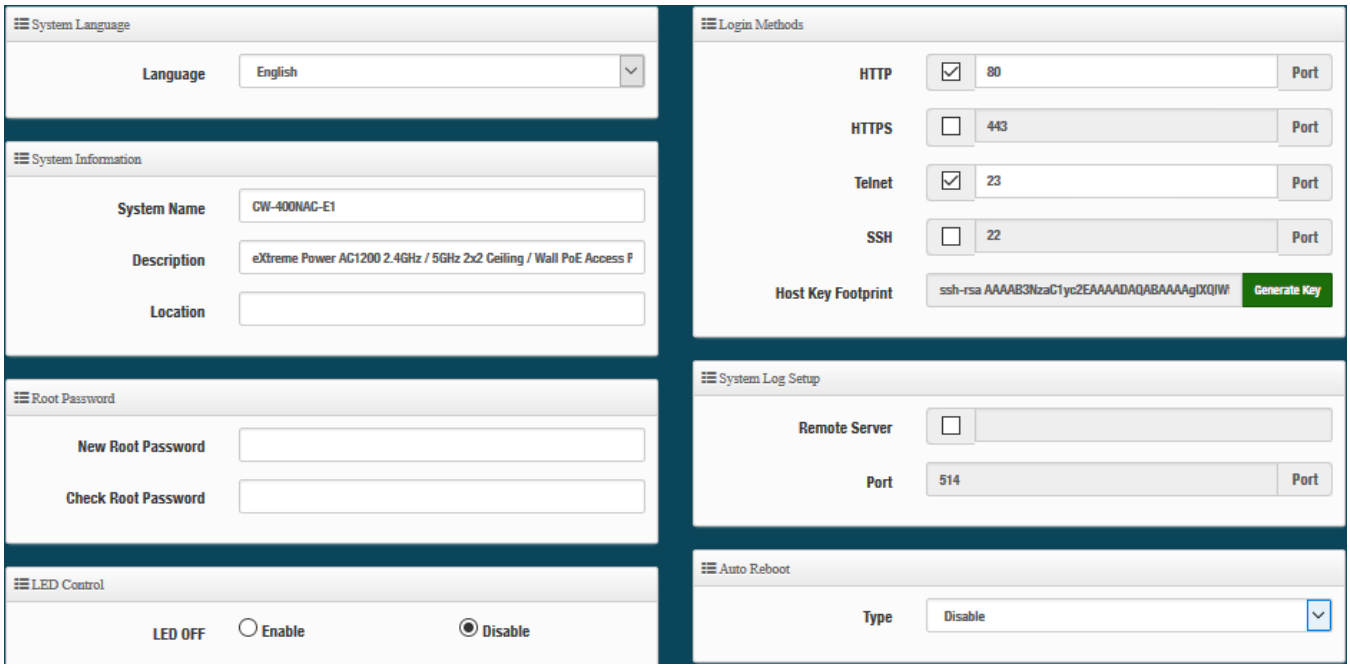
Click “Save” button to add schedule to policy. There are 10 schedule maximum allowed in the each time policy. All schedules can be edited or removed in the each time policy. Click **Reboot** button to activate your changes.

9. System Management

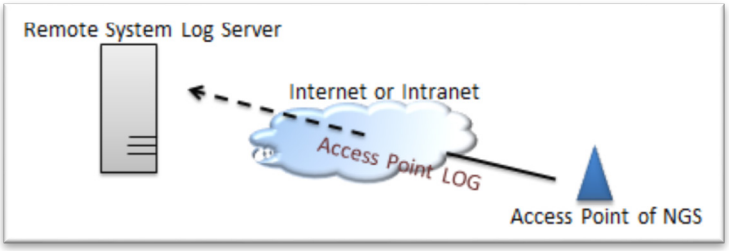
9.1 Configure system management

Administrators can specify geographical location of the system via instructions in this page and modify system login password and select use system login protocol by 80, 443, 23, 22 Port.

The management page adds LED control on/off and system auto reboot function.



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

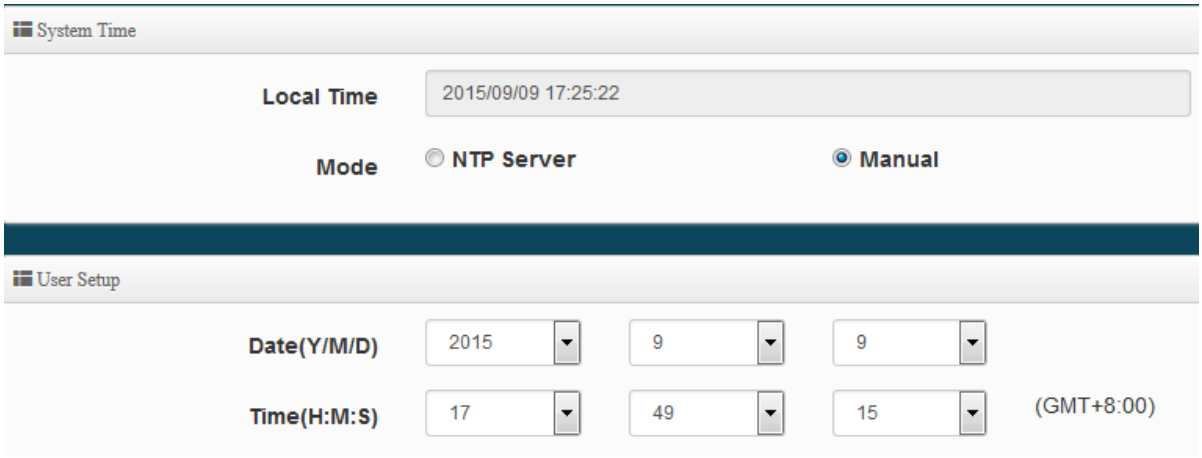


- **Auto Reboot:** The functions can Auto-reboot the system by Date/time management.
  - **Daily：** Setting time to system reboot.
  - **Weekly :** Setting frequency (ex. Weekly) and time of system reboot
  - **Monthly :** Setting Every month, fixed date and time to system reboot

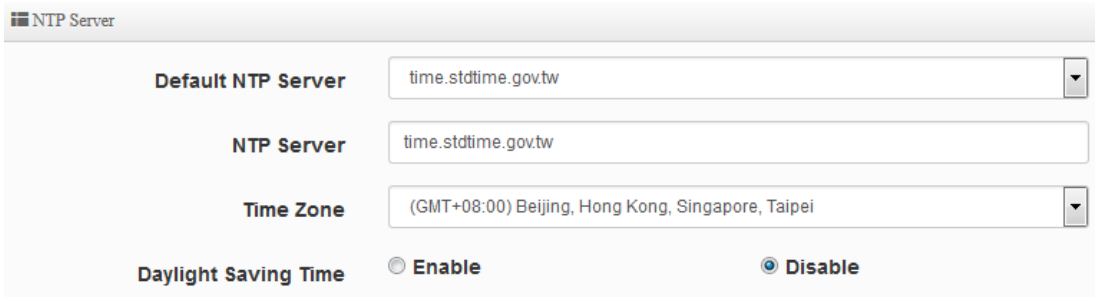
Click ***"Save"*** button to save your changes. And click ***"Reboot"*** button to activate your changes

9.2 Configure Time Server

Administrator can select manual or via a NTP server to modify system time for the right local time.
If select update the system time for manual, when administrator reboot system the system time will reply default.
If select update the system time for the NTP Server, system must set gateway and DNS server, the system can be connected internet.



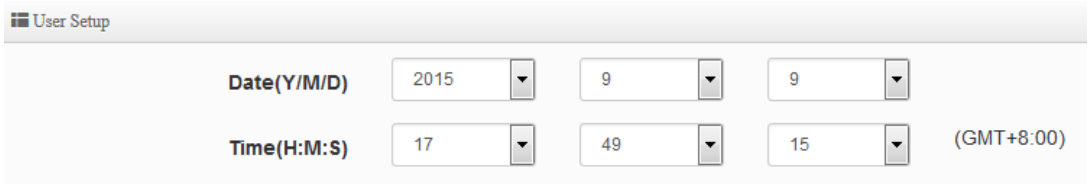
- **Mode:** Administrator can select NTP Server or Manual.
  - **NTP Server:** System can auto update the system time. Administrator needs setting as NTP Server.



- ✓ **Default NTP Server:** Administrator can select NTP Server.
- ✓ **NTP Server:** Administrator can setting as NTP Server.
- ✓ **Time Zone:** Administrator can select a desired time zone from the drop-down list.

- ✓ **Daylight saving Time:** Enable or disable Daylight saving.

- **Manual:** Administrator need to set the system time.



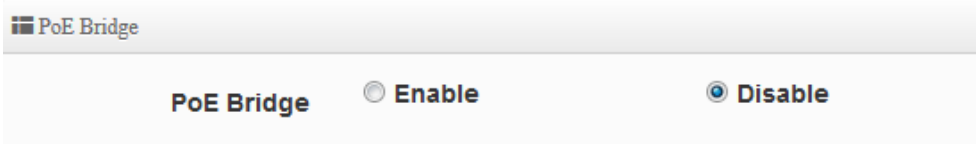
Click ***"Save"*** button to save your changes. And click ***"Reboot"*** button to activate your changes

9.3 Control PoE Bridge

Notice

Not all CenOS 5.0 devices support PoE Bridge Function. Please reference the proper AP model's data sheet to check if your device supports PoE Bridge.

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



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

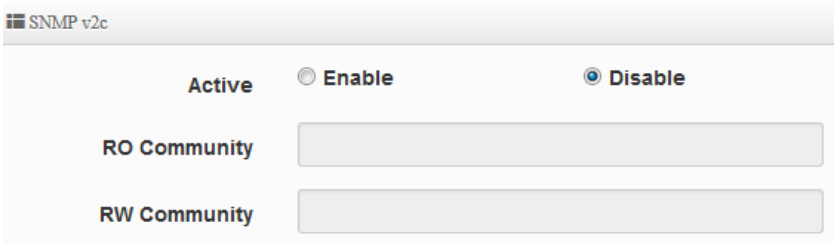
Click ***"Save"*** button to save your changes. And click ***"Reboot"*** button to activate your changes

9.4 Configure SNMP Setup

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

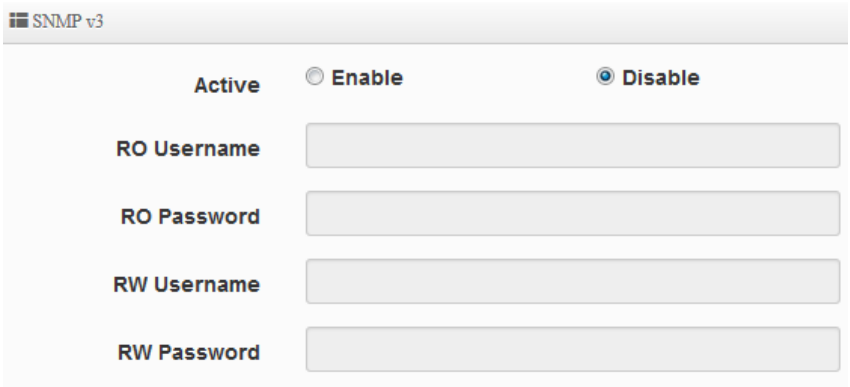
Please click on **System -> SNMP** and follow the below setting.

SNMP v2c function



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

SNMP v3 function



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

SNMP Trap

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

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

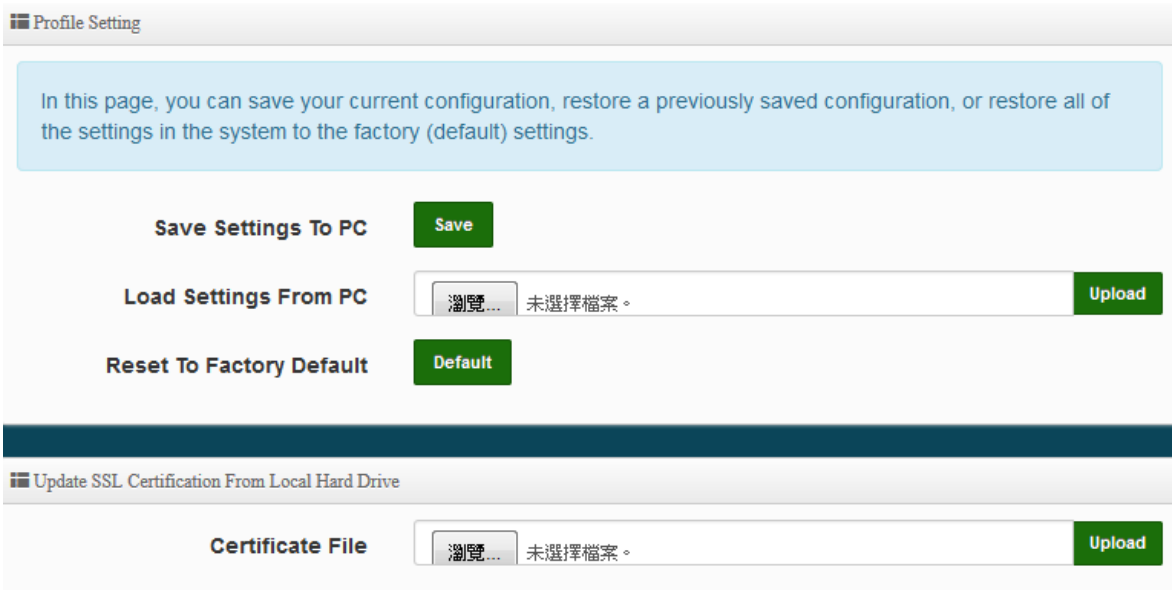
Click ***"Save"*** button to save your changes. And click ***"Reboot"*** button to activate your changes

10. Utilities

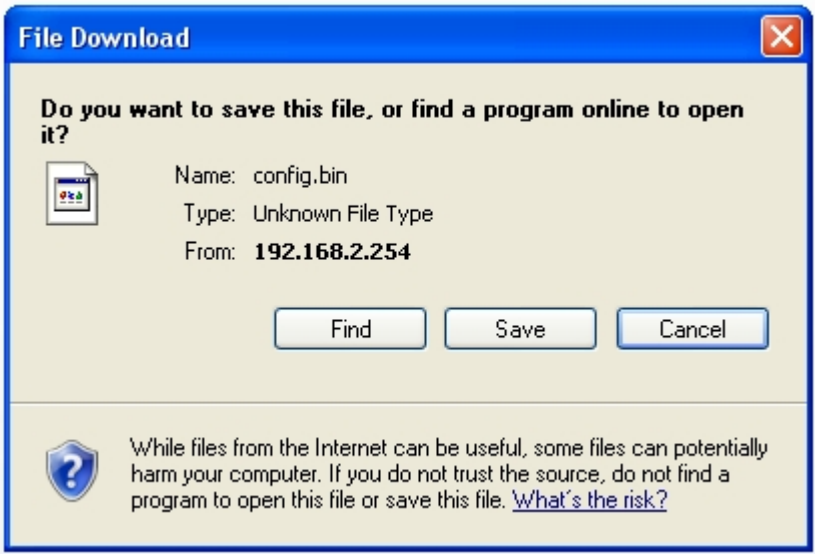
10.1 Profile Setting

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

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



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



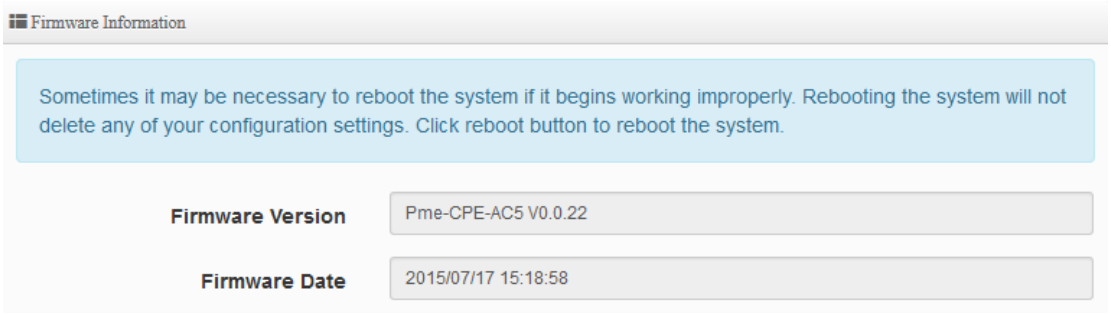
- **Load Settings from PC:** Click ***Browse*** button to locate a configuration file to restore, and then click ***Upload*** button to upload.
- **Reset To Factory Default:** Click ***Default*** button to reset back to the factory default settings and expect **Successful** loading message**.** Then,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

10.2 System Upgrade

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

Firmware Information:

Display the system firmware information.



Upgrade Via Local PC and TFTP Server:

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

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

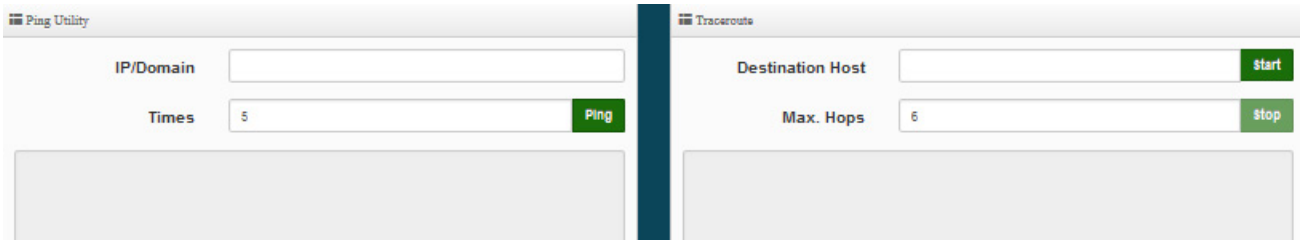
- **TFTP Server:** Enter IP address for TFTP Server.
- **File Name:** Enter file name.

Notice

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

10.3 Network Utility

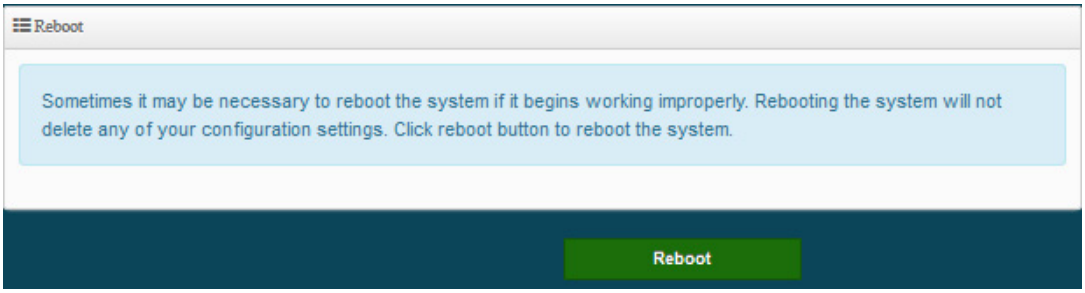
The administrator can diagnose network connectivity via the PING or TRACEROUTE utility. Please click on **Utilities** -> **Network Utility** and follow the below setting.



- **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.

10.4 Reboot

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

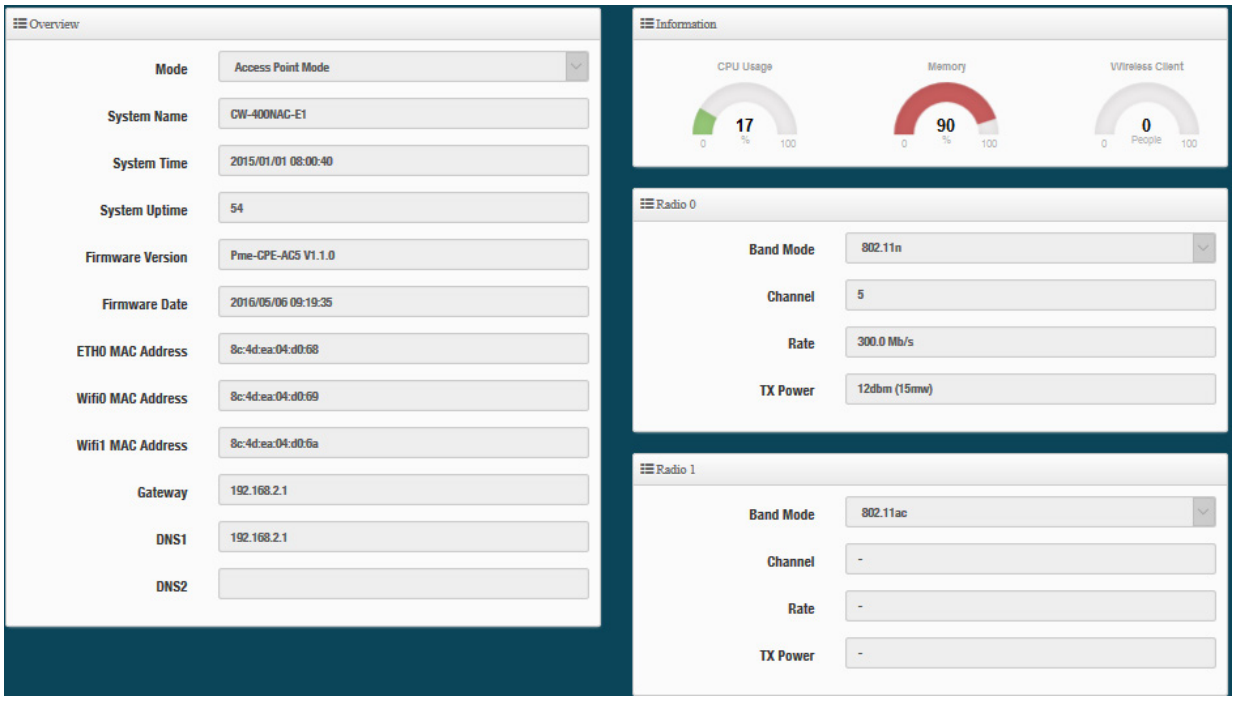


11. Status

11.1 Overview

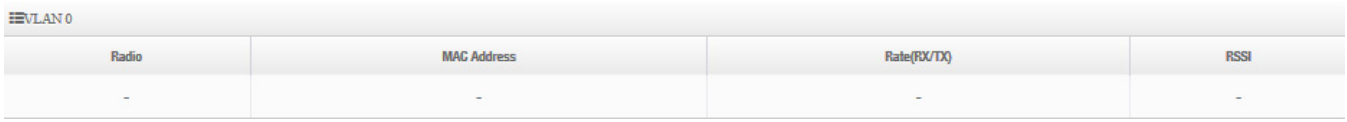
Detailed information on System, Network can be reviewed via this page.

If device use wave1 chip then 11n max data rate is 300Mbps, if device use wave2 chip then 11n max data rate is 400Mbps, product whether is wave1 or wave2 can refer to the product data sheet.



11.2 Wireless Client

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



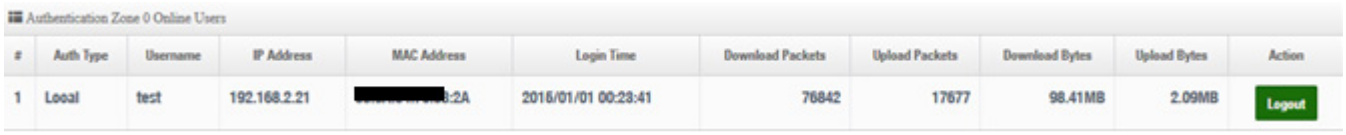
11.3 Online Users by Captive Portal

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

Authentication Zone Online Users

VLAN#	Authentication	User Count	Download Packets	Upload Packets	Download Bytes	Upload Bytes	Action
0	ON	1	76842	17677	98.41MB	2.09MB	Detail

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

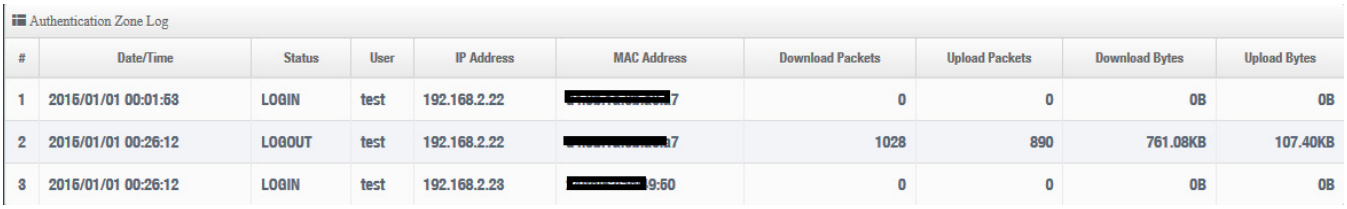

Authentication Zone 0 Online Users

#	Auth Type	Username	IP Address	MAC Address	Login Time	Download Packets	Upload Packets	Download Bytes	Upload Bytes	Action
1	Local	test	192.168.2.21	[redacted]:2A	2016/01/01 00:23:41	76842	17677	98.41MB	2.09MB	Logout

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

11.4 Authentication Log by Captive Portal

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



Authentication Zone Log

#	Date/Time	Status	User	IP Address	MAC Address	Download Packets	Upload Packets	Download Bytes	Upload Bytes
1	2016/01/01 00:01:53	LOGIN	test	192.168.2.22	[redacted]7	0	0	0B	0B
2	2016/01/01 00:26:12	LOGOUT	test	192.168.2.22	[redacted]7	1028	890	761.08KB	107.40KB
3	2016/01/01 00:26:12	LOGIN	test	192.168.2.23	[redacted]9:60	0	0	0B	0B

11.5 System Log

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

System Log

Refresh Clear

Time	Facility	Severity	Message
-	-	-	-

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

Appendix A. WEB GUI Valid Characters

Table B WEB GUI Valid Characters

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

Table B WEB GUI Valid Characters (continued)

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

Table B WEB GUI Valid Characters (continued)

Block	Field	Valid Characters

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