Industrial WiFi CPE/AP

CPE-2458-AC-S-I

Configuration Manual

Beijing Nodes Network Limited

2019 年

Table of contents

ALL RIGHTS RESERVED.
Beijing Nodes Network Limited
Telephone: 010-5165 2232
Fax: 010-5165 4922
Web: www.nodes.com.cn

Radio Frequency Interference Requirements

This device complies with Part 15 of FCC Rules.

Operation is subject to the following conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.
3. This device should not be co-located or operating in conjunction with any other antenna or transmitter.

Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules; these limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

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

FCC Caution: To assure continued compliance, (example – use only shielded interface cables when connecting to computer or peripheral devices). Any changes or modifications not expressly approved by the party responsible for compliance could void the user’s authority to operate this equipment.

1. Introduction

This guide covers the initial configuration of CPE 2458-AC-S-I via Web Administration Interface (Web UI). Web Administration Interface is the built-in and user-friendly graphic interface on all CPE products. It allows you to configure, monitor, and manage the devices using web browser. Mozilla Firefox, Google Chrome, and Internet Explorer 8+ are recommended.

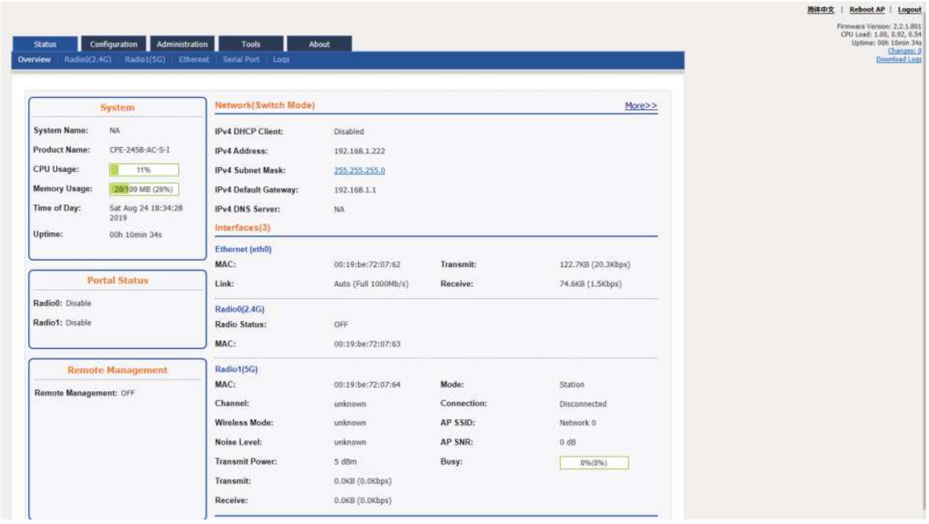
This guide is applicable with firmware version 2.2.1.801 or above for hardware platforms with the following models:

Table 1 – CPE/AP products

Product Name	Industrial WiFi CPE/AP
Model Number	CPE 2458-AC-S-I

2. Web Administration Interface (Web UI)

Figure 1 - AP Status Overview



Firmware Version: 2.2.1.801
CPU Load: 1.00, 0.92, 0.54
Uptime: 00h 10min 34s
Changes: 0
Download Logs

System

System Name: NA
Product Name: CPE-2458-AC-S-I
CPU Usage: 11%
Memory Usage: 28/109 MB (26%)
Time of Day: Sat Aug 24 18:34:28 2019
Uptime: 00h 10min 34s

Portal Status

Radio0: Disable
Radio1: Disable

Remote Management

Remote Management: OFF

Network(Switch Mode)

IPv4 DHCP Client: Disabled
IPv4 Address: 192.168.1.222
IPv4 Subnet Mask: 255.255.255.0
IPv4 Default Gateway: 192.168.1.1
IPv4 DNS Server: NA

Interfaces(3)

Ethernet (eth0)

MAC:	00:19:be:72:07:62	Transmit:	122.7KB (20.3Kbps)
Link:	Auto (Full 1000Mb/s)	Receive:	74.6KB (1.5Kbps)

Radio0(2.4G)

Radio Status:	OFF
MAC:	00:19:be:72:07:63

Radio1(5G)

MAC:	00:19:be:72:07:64	Mode:	Station
Channel:	unknown	Connection:	Disconnected
Wireless Mode:	unknown	AP SSID:	Network 0
Noise Level:	unknown	AP SNR:	0 dB
Transmit Power:	5 dBm	Busy:	0%(0%)
Transmit:	0.0KB (0.0Kbps)		
Receive:	0.0KB (0.0Kbps)		

Web Administration Interface (Web UI) consists of:

Primary Tabs:

Configuration

Administration

Tools

About

Links:

簡体中文/English – swap Web UI language between simplified Chinese and English.

Reboot AP – reboot AP.

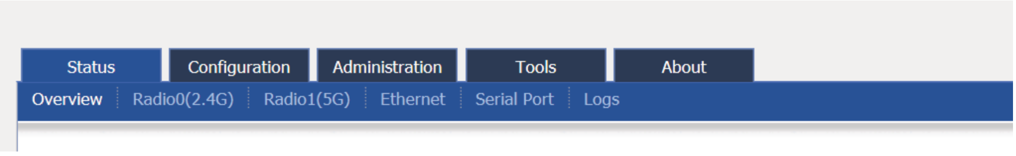
Logout – log out from Web UI.

Change: 0 – list out all unsaved configuration changes.

Download Logs – download the system log from AP.

2.1. Status

Figure 2 – Secondary tabs under Status tab



Status tab collects the information about AP's system status, interfaces status, and system logs. The following tabs can be found under status tab:

Overview – display vital information on the device's status. Information includes system status, thin AP status, network status, and interfaces status.

Radio0 (2.4G) – display 2.4G radio's information including radio settings, radio transmission and reception statistics, and connection information.

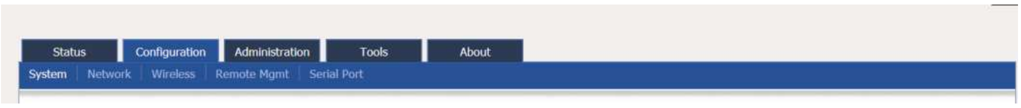
Radio1 (5G) – display 5G radio's information including radio settings, radio transmission and reception statistics, and connection information.

Ethernet - shows the current status of Ethernet interfaces. The information includes Port, MAC Address, Auto-negotiation, Speed, Duplex, Link Detected, instant throughput of uplink and downlink and traffic of of uplink and downlink.

Logs - display log files for system information, association activity, and alarm event.

2.2. Configuration

Figure 3 – Secondary tabs under Configuration tab



Configuration tab contains various configuration attributes about the device. The following tabs can be found under configuration tab:

System – the configuration attributes about system information, logging, Network Time Protocol (NTP), and web setting can be found in this tab.

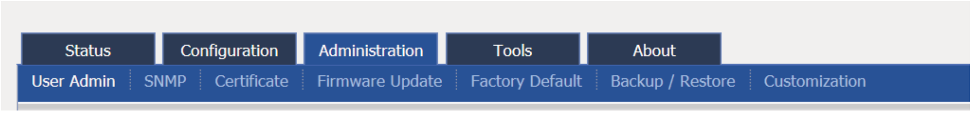
Network – the configuration attributes about IP address, interface assignment, VLAN, built-in DHCP server, port forward, and safe mode can be found under this tab

Wireless – the configuration attributes about both 2.4G radio and 5G radio can be found under this tab

Thin AP - the configuration attributes about thin AP mode can be found under this tab

2.3. Administration

Figure 4 – Secondary tabs under Administration tab



Administration tab contains various configuration attributes for managing the device. The following tabs can be found under configuration tab:

User Admin – collects the configuration attributes about user administration of the device

SNMP – collects the configuration attributes about Simple Network Management Protocol (SNMP)

Certificate – upload certification file and key file for HTTPS connection of the device

Firmware Update – update the firmware of the device

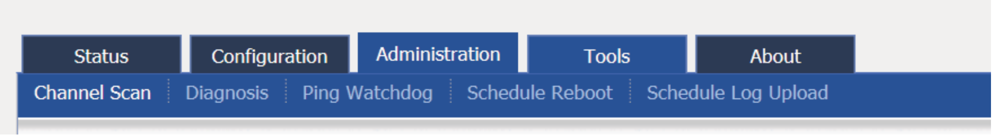
Factory Default – perform factory reset for the device

Backup/Restore – backup the current configuration from the device or restore the desire configuration to the device

Customization – upload customized configuration as factory default settings for the device

2.4. Tools

Figure 5 – Secondary tabs under Tools tab



Administration tab collects various tools for deployment and troubleshooting. The following tabs can be found under Tools tab:

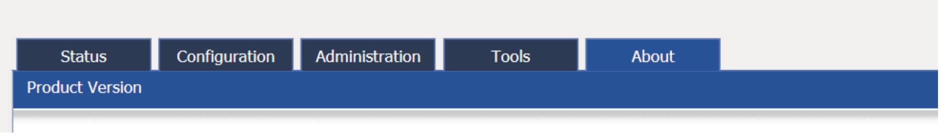
Channel Scan - collect the information of all WiFi channel on 2.4GHz frequency and 5GHz frequency in the surrounding area. The information includes noise floor, percentage of channel busy, and the number of BSS in particular radio channels.

Diagnosis – provide tools for testing the reachability, route, and packet capture for troubleshooting

Watchdog – provide various timers used to detect and recover from system malfunctions

2.5. About

Figure 6 – Secondary tabs under About tab



About tab collects the information about product information, hardware, firmware and company information.

3. Getting Started

This chapter covers the procedures for logging into / out CPE Series Products Web Administration Interface (Web UI) via Ethernet, and restarting the device via Web UI.

3.1. Preparing the Administrator Computer

1. On your Windows XP or Windows 7 computer, open the Network Connections (or Change adapter settings) control panel according to how the Start menu is set up:

   On **Windows XP**, click **Start** > **Control Panel** > **Network Connections**.

   On **Windows 7**, click **Start** > **Control Panel** > **Network and Internet**

> **Network and Sharing Center** > **Change adapter settings**.

2. Right-click the icon for **Local Area Connection**, and then click **Properties**.
3. When the Local Area Connection Properties dialog box appears, select **Internet Protocol (TCP/IP)** (or **Internet Protocol Version 4 (TCP/IPv4)**) from the scrolling list, and then click **Properties**. The Internet Protocol (TCP/IP) Properties dialog box appears.
4. Write down all of the currently active network settings. You will need this information later when you restore your computer to its current network configuration.
5. Configure the IP address settings with the values listed in
6. Table 2.

Table 2 - Configure administrative computer's IP address settings

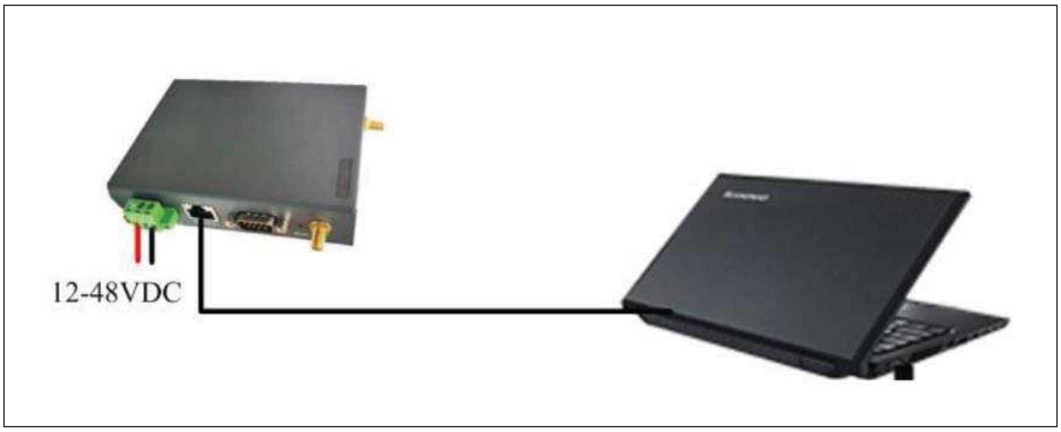
IP Address	*Any address in the 192.168.1.x, except 192.168.1.222 and 192.168.1.255* *Example: 192.168.1.2*
Subnet Mask	*255.255.255.0*
Default Gateway	Blank
DNS	Blank

7. Click **OK** to save the changes and close the TCP/IP Properties dialog box.
8. Click **OK** again to close the Local Area Connection Properties dialog box.

3.2. Connecting Access Point

1. Provide 12-48v dc power supply for CPE .
2. Connect your laptop to Ethernet port of the CPE using Ethernet cable.

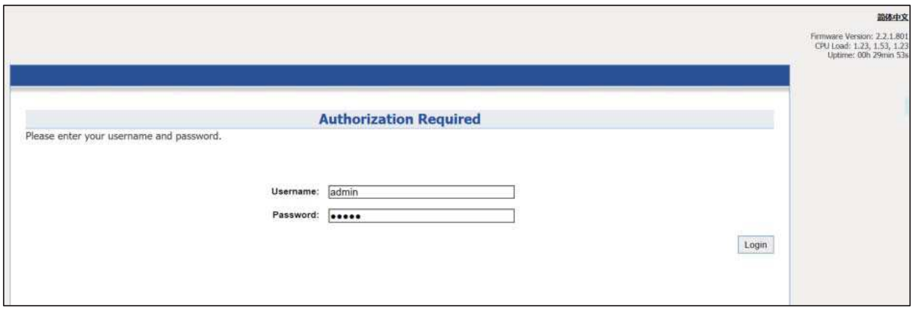
Figure8 – Connect to AP



3.3. Login the AP (via Ethernet)

1. Open a Web browser from the computer.
2. Type http://192.168.1.222 in the address bar or location bar (see
3. Figure 7).
4. Type *admin* (default username) in **Username**
5. Type *admin* (default password) in **Password**
6. Click **Login**

Figure 7 – CPE Series Product's Login Page



简体中文

Firmware Version: 2.2.1.801
CPU Load: 1.23, 1.53, 1.23
Uptime: 00h 29min 53s

Authorization Required

Please enter your username and password.

Username: admin
Password: •••••

Secondary IP Address of CPE Series Products

The default IP address of CPE is *192.168.1.222/24*. CPE series products support a fixed IP address on the Ethernet connection called Secondary IP Address. This secondary IP address is *192.168.99.x/24* where x denotes as the decimal value of the last byte of the Ethernet MAC address on the access point.

Example 1:

Device Ethernet MAC address: 00:19:BE:20:03:**8C**

Secondary IP Address of this device:

192.168.99.**140** (**8C** (HEX) → **140** (DEC))

The secondary IP address uses IP range from *192.168.99.5/24* to *192.168.99.254/24*. The rest of IP addresses are reserved. If the last byte of a MAC address matches any of the reserved IP addresses, the supported device shall follow the MAC to IP address mapping shown in Table 3:

Table 3 - CPE Series Product Secondary IP Address

Ethernet MAC address	Reserved Purpose	Replaced MAC byte	SecondaryIP address
XX:XX:XX:XX:XX:00	Invalid IP	A0	192.168.99.160
XX:XX:XX:XX:XX:01	For gateway	A1	192.168.99.161
XX:XX:XX:XX:XX:02	For operator computer	A2	192.168.99.162
XX:XX:XX:XX:XX:03	For operator computer	CPE	192.168.99.163
XX:XX:XX:XX:XX:04	For operator computer	A4	192.168.99.164
XX:XX:XX:XX:XX:FF	Invalid IP	AF	192.168.99.175

Example 2

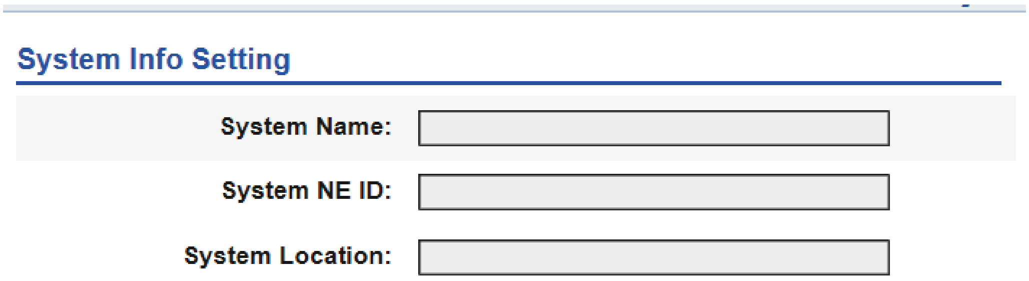
Device Ethernet MAC address: 00:19:BE:20:03:**FF**

Secondary IP Address of this device:

192.168.99.**175** (**FF** (HEX) → **AF** (HEX) → **175** (DEC))

3.4. System Info Setting

Figure 8 – System Info Setting



System Info Setting

System Name:

System NE ID:

System Location:

1. Click **Configuration** > **System**
2. Type in a string up to 255 characters in **System Name;** this entry is optional
3. Type in a string up to 64 characters in **System NE ID;** this entry is optional
4. Type in a string up to 255 characters in **System Location;** this entry is optional
5. Select **Power Save PoE** checkbox if CPE is powered by a PoE switch that is compliant with 802.3af only.
6. Click **Submit**

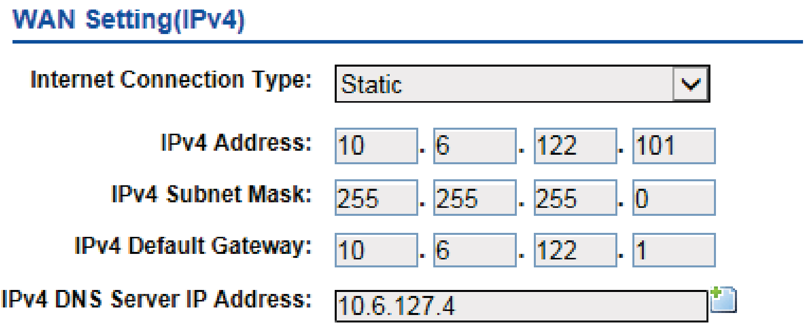
Note:

− In 802.3af power safe mode, CPE will operate in 2x3 MIMO with maximum transmission power 24 dBm.

3.5. Assign an IP Address to CPE Device

3.5.1Assign Static IPv4 IP Address

Figure 9 – IPv4 WAN Setting (Static IP Address)



WAN Setting(IPv4)

Internet Connection Type: Static

IPv4 Address: 10 . 6 . 122 . 101

IPv4 Subnet Mask: 255 . 255 . 255 . 0

IPv4 Default Gateway: 10 . 6 . 122 . 1

IPv4 DNS Server IP Address: 10.6.127.4

1. Go to **Configuration** > **Network** > **General** > **WAN Settings (IPv4)**
2. Select *Static* on **Internet Connection Type**
3. Enter valid IP Address on **IPv4 Address**; *192.168.1.222* is the default setting
4. Enter valid IP subnet mask on **IPv4 Subnet Mask**; 255.255.255.0 is default setting
5. Enter valid IP address of default gateway on **IPv4 Default Gateway**
6. Enter valid IP address of DNS server on **IPv4 DNS Server Address**

Note:

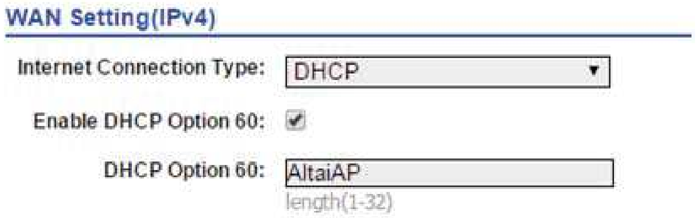
− Click ⊞ for adding more DNS;

− Click ☒ to remove existing DNS server entry

7. Click **Submit**

3.5.2Assign IPv4 IP Address from DHCP server

Figure 10 – IPv4 WAN Setting (DHCP Client)



WAN Setting(IPv4)

Internet Connection Type: DHCP ▾

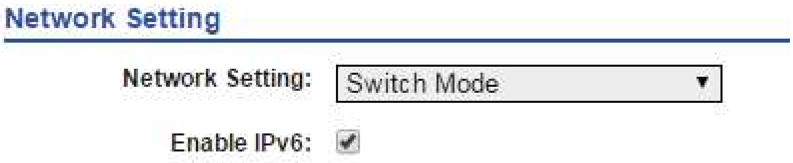
Enable DHCP Option 60: ☑

DHCP Option 60: AltaiAP
length(1-32)

1. Go to **Configuration** > **Network** > **General** > **WAN Settings (IPv4)**
2. Select *DHCP* on **Internet Connection Type**
3. Click **Enable DHCP Option 60** checkbox to specify vendor class identifier. This entry is optional.
4. Enter a string between 1 and 32 characters long on **DHCP Option 60**. This entry is optional.
5. Click **Submit**

3.5.3Assign Static IPv6 IP Address

Figure 11 – Enable IPv6 option



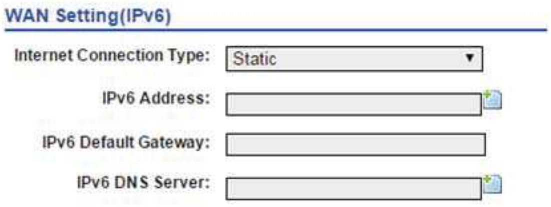
Network Setting

Network Setting: Switch Mode ▾

Enable IPv6: ☑

1. Go to **Configuration** > **Network** > **General** > **Network Setting**
2. Click **Enable IPv6** checkbox

Figure 12 – IPv6 WAN Setting



WAN Setting(IPv6)

Internet Connection Type: Static ▾

IPv6 Address:

IPv6 Default Gateway:

IPv6 DNS Server:

3. Go to **Configuration** > **Network** > **General** > **WAN Setting (IPv6)**
4. Select *Static* on **Internet Connection Type**
5. Enter valid IP Address on **IPv6 Address**
6. Enter valid IP subnet mask on **IPv6 Subnet Mask**
7. Enter valid IP address of default gateway on **IPv6 Default Gateway**

8. Enter valid IP address of DNS server on **IPv6 DNS Server Address**

Note:

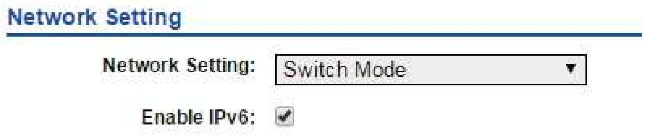
– Click ➕ for adding more IPv6 Address and IPv6 DNS Server;

– Click ✖ to remove existing IPv6 Address and IPv6 DNS Server entry

9. Click **Submit**

3.5.4Assign IPv6 IP Address from DHCP server

Figure 13 – Enable IPv6 option



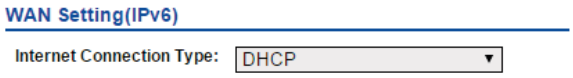
Network Setting

Network Setting: Switch Mode ▾

Enable IPv6: ☑

1. Go to **Configuration** > **Network** > **General** > **Network Setting**
2. Click **Enable IPv6** checkbox

Figure 14 – IPv6 WAN Setting



WAN Setting(IPv6)

Internet Connection Type: DHCP ▾

3. Go to **Configuration** > **Network** > **General** > **WAN Setting (IPv6)**
4. Select *DHCP* on **Internet Connection Type**
5. Click **Submit**

3.6. Apply Submitted Configurations on the CPE Device

1. Click **Save & Apply** from the top on the right.

4. Radios Settings

CPE products have both a high capacity 2.4 GHzradio and a 5 GHz radio. It can play as different role in your network. This chapter shows the typical deployment scenarios and configuration procedures.

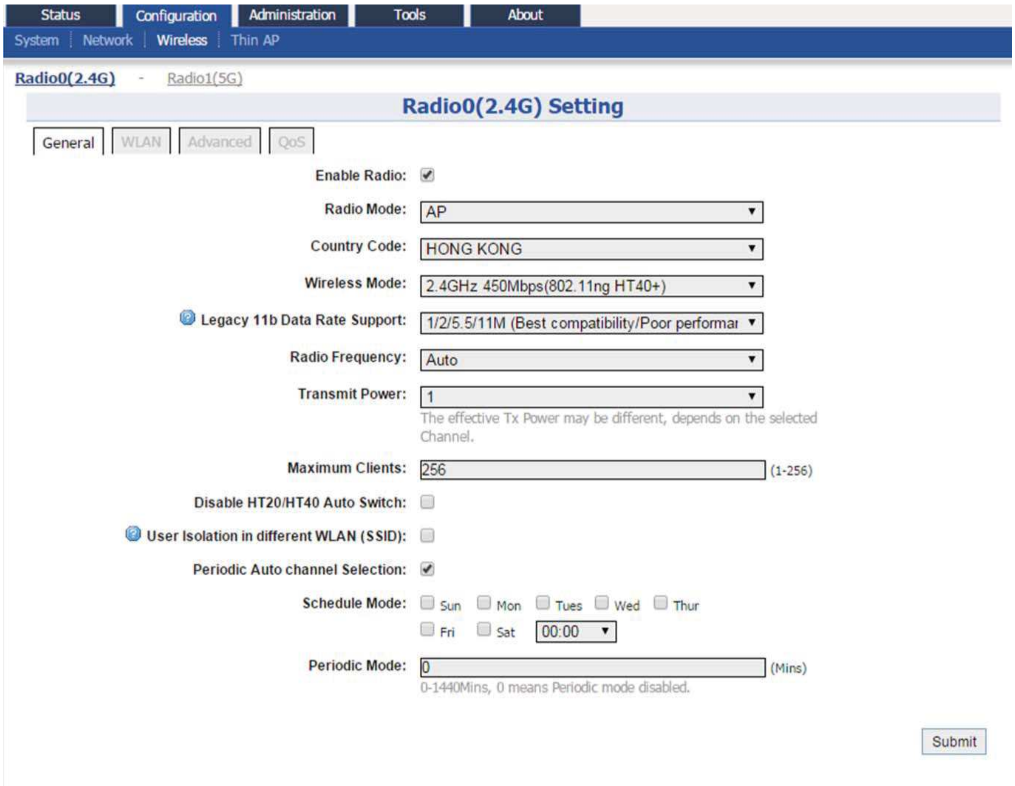
4.1. Access Point Mode

Access Point (AP) allows wireless devices to connect to a wired network using 802.11 a/b/g/n/ac standards. Wireless clients connect the AP to join the network, such as laptops, smart phones etc.

4.1.1Radio0 – 2.4G

4.1.1.1 Configure General Wireless Setting

Figure 15 – 2.4G Radio General Setting



Radio0(2.4G) Setting

Enable Radio: ☑

Radio Mode: AP

Country Code: HONG KONG

Wireless Mode: 2.4GHz 450Mbps(802.11ng HT40+)

Legacy 11b Data Rate Support: 1/2/5.5/11M (Best compatibility/Poor performar

Radio Frequency: Auto

Transmit Power: 1
The effective Tx Power may be different, depends on the selected Channel.

Maximum Clients: 256 (1-256)

Disable HT20/HT40 Auto Switch: □

User Isolation in different WLAN (SSID): □

Periodic Auto channel Selection: ☑

Schedule Mode: □ Sun □ Mon □ Tues □ Wed □ Thur □ Fri □ Sat 00:00

Periodic Mode: 0 (Mins)
0-1440Mins, 0 means Periodic mode disabled.

1. Go to **Configuration** > **Wireless** > **Radio0 (2.4G)** > **General**
2. Select **Enable Radio** checkbox to enable radio interface
3. Select *AP* on **Radio Mode**
4. Select the correct country code on **Country Code**; this option ensures that the CPE device uses only the radio channels allowed in your country or region
5. Select suitable wireless mode on **Wireless Mode**; the options include:

2.4G 11Mbps (802.11 b)

2.4G 54Mbps (802.11 bg)

2.4G 54Mbps (802.11 g-only)

*2.4G 216.7Mbps (802.11 ng HT20); **Default Setting***

2.4G 216.7Mbps (802.11 n-only HT20)

2.4G 450Mbps (802.11 ng HT40+)

2.4G 450Mbps (802.11 n-only HT40+)

2.4G 450Mbps (802.11 ng HT40-)

2.4G 450Mbps (802.11 n-only HT40-)

6. Select suitable option on **Legacy 11b Data Rate Support** for legacy client compatibility. In order to enhance the spectrum efficiency, low data rates (1/2/5.5/11M) should be eliminated. This entry is optional. Options include:

1/2/5.5/11M (Best compatibility /Poor performance)	All legacy clients will be supported
5.5/11M (Good compatibility /Good performance)	Clients only capable of 1/2Mbps will not be supported
Disable All (Poor compatibility/ Best performance)	Clients only capable of 802.11b standard will not be supported

Note:

– *2.4G 11Mbps (802.11 b)* is not applicable.

7. Select suitable operating channel on **Radio Frequency**;

Note:

– *You should select the suitable operating channel based on the on-site channel scan result.*

8. Select suitable transmission power on **Transmission Power**;

Note:

– *You should follow the regulation from local Communications Authority*

9. Enter the maximum associated client between 1 and 256 on **Maximum Client** that the radio interface serves. *256* is the default setting. This entry is optional.

10. Select **Disable HT20/HT40 Auto Switch** checkbox that CPE device will NOT switch the channel width between 20 MHz and 40 MHz automatically. This entry is optional and only available for the following wireless modes:

2.4G 450Mbps (802.11 ng HT40+)

2.4G 450Mbps (802.11 n-only HT40+)

2.4G 450Mbps (802.11 ng HT40-)

2.4G 450Mbps (802.11 n-only HT40-)

11. Select **Enable Inter-WLAN User Isolation** checkbox that CPE device block the users' communication across different SSID on the same AP directly. This entry is optional.

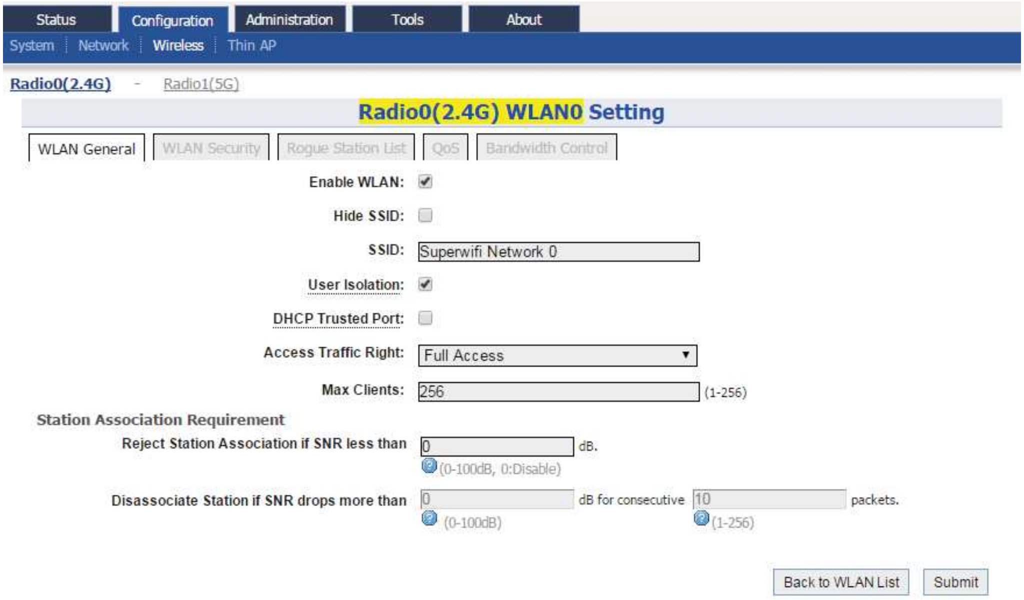
12. Select **Periodic Auto Channel Section** checkbox to enable scheduled channel selection task on the radio interface. This entry is optional and only available if *auto* is selected on **Radio Frequency**. The available schedule modes are:

Schedule Mode	Select exact time and day(s) for selecting radio frequency for the interface
Periodic Mode	Select a countdown timer (minute) for selecting radio frequency for the interface; *0* denotes disable.

13. Click **Submit**

4.1.1.2 Configure WLAN # General Setting

Figure 16 – 2.4G WLAN # General Setting



Radio0(2.4G) WLAN0 Setting

Enable WLAN: ☑

Hide SSID: □

SSID: Superwifi Network 0

User Isolation: ☑

DHCP Trusted Port: □

Access Traffic Right: Full Access ▼

Max Clients: 256 (1-256)

Station Association Requirement

Reject Station Association if SNR less than 0 dB. (0-100dB, 0:Disable)

Disassociate Station if SNR drops more than 0 dB for consecutive 10 packets. (0-100dB) (1-256)

1. Go to **Configuration** > **Wireless** > **Radio0 (2.4G)** > **WLAN #** > More…
2. Select **Enable WLAN** checkbox to enable WLAN
3. Select **Hide SSID** checkbox to hide SSID name from its beacon frame. This entry is optional.

4. Enter a unique name for the particular WLAN on **SSID**.

Note:

- *If you want to configure the same SSID on two different WLANs; their security setting MUST be different from each other.*

5. Select **User Isolation** checkbox to block user communication within the same SSID in the AP directly. This entry is optional.
6. Deselect the **DHCP Trust Port** checkbox to prevent illegal DHCP servers offering IP address to DHCP clients via this WLAN. This entry is optional.
7. Specify the suitable privilege of associated clients on **Access Traffic Right**; the options include

Full Access	Associated client can access Internet and manage AP
AP Management Only	Associated client can manage AP only, but not able to access the Internet
AP Management Disable	Associated client can access the Internet, but not able to manage AP

8. Enter the maximum associated clients between *1* and *256* on **Max Clients** for this WLAN. *256* is the default setting.

Note:

- **Max Clients** in WLAN 0 – 15 MUST be smaller than or equal to (≥) the **Max Clients** setting on Radio General Setting

9. Enter an additional requirement on Signal Strength to Noise Ratio (SNR) for associated clients under **Station Association Requirement**. These entries are optional. Network ad may fill up the following fields:

Reject Station Association if SNR less than *X* dB	*X* denote the minimum SNR level which allow clients to associate; You can select any integer between *0*dB and *100*dB; *0* denotes as disable; *0* is default setting

Disassociate Station if SNR drops more than *Y* dB for consecutive *Z* packets	*Y* denotes the SNR tolerance; *Z* denotes the number of consecutive packets their SNR are below the difference of *X* - *Y*.

Notes:

– Example for Station Association Requirement with the following settings:

Reject Station Association if SNR less than 30 dB (X = 30);

Disassociate Station if SNR drops more than 20 dB for consecutive 10 packets (Y = 20; Z = 10)

Consequence:

AP accepts the clients to associate if the SNR of packets from the clients is high than (>) 30dB;

AP kicks out the associated client if the SNR of 10 consecutive packets is below (<) 10 dB (30 dB – 20 dB)

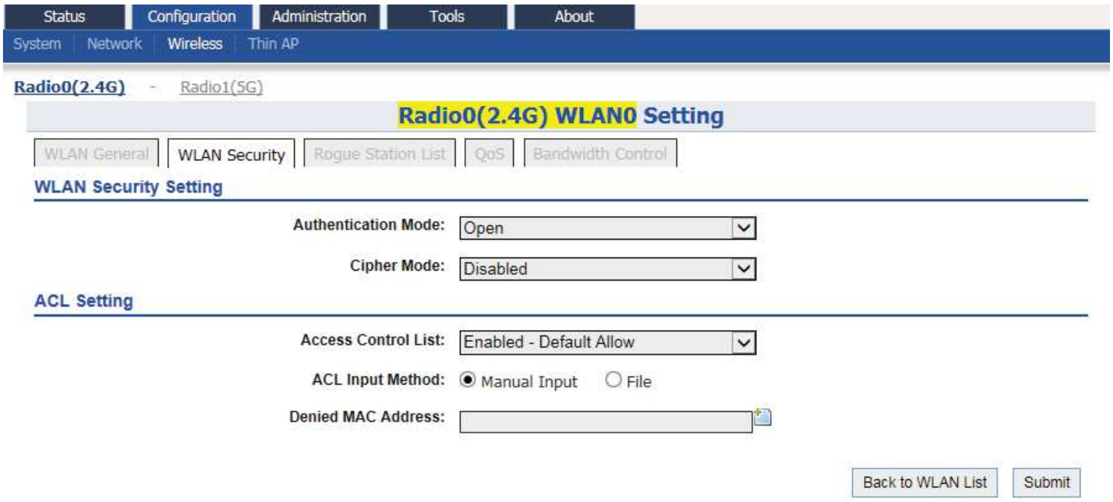
10. Click **Submit**

4.1.1.3 Configure WLAN # Security Setting

Configure WLAN as Open Network

This setting is typically only used in a guest network. No security measure is enforced.

Figure 17 – 2.4G WLAN # Security Setting: Open Network



Radio0(2.4G) WLAN0 Setting

WLAN Security Setting

Authentication Mode: Open

Cipher Mode: Disabled

ACL Setting

Access Control List: Enabled - Default Allow

ACL Input Method: ● Manual Input ○ File

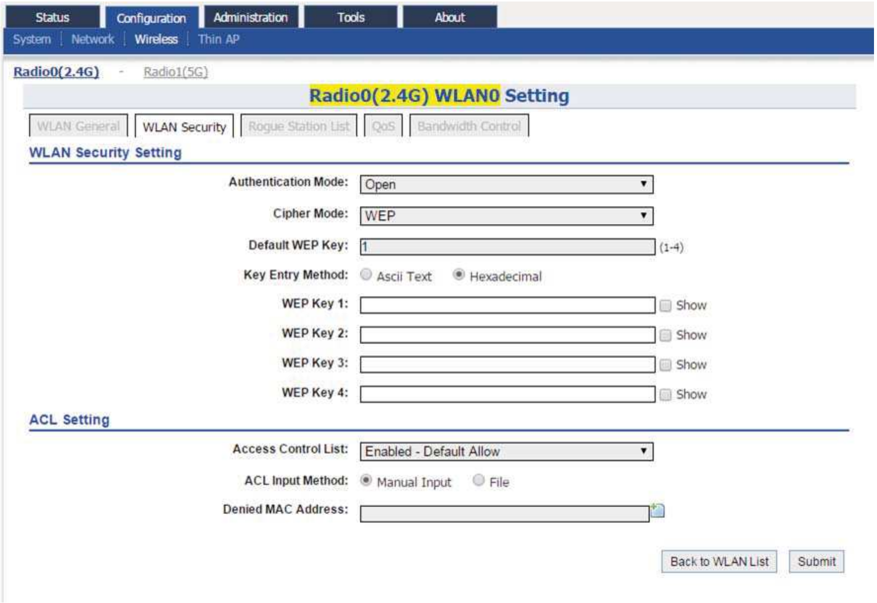
Denied MAC Address:

1. Go to **Configuration** > **Wireless** > **Radio0(2.4G)** > **WLAN** > **WLAN #** > **WLAN Security**
2. Select Open on **Authentication Mode**
3. Select *Disabled* on **Cipher Mode**
4. Click **Submit**

4.1.1.4 Configure WLAN as Open network with WEP encryption

This setting provides minimal security as it allows all requesting devices to join a given network.

Figure 18 – 2.4G WLAN # Security Setting: Open Network with WEP



Radio0(2.4G) WLAN0 Setting

WLAN Security Setting

Authentication Mode: Open

Cipher Mode: WEP

Default WEP Key: 1 (1-4)

Key Entry Method: ○ Ascii Text ● Hexadecimal

WEP Key 1: □ Show

WEP Key 2: □ Show

WEP Key 3: □ Show

WEP Key 4: □ Show

ACL Setting

Access Control List: Enabled - Default Allow

ACL Input Method: ● Manual Input ○ File

Denied MAC Address:

1. Go to **Configuration** > **Wireless** > **Radio0(2.4G)** > **WLAN** > **WLAN #** > **WLAN Security**
2. Select Open on **Authentication Mode**
3. Select *WEP* on **Cipher Mode**
4. Select key number *1 – 4* on **Default WEP Key**
5. Select suitable key type in **Key Entry Mode**; the options include:

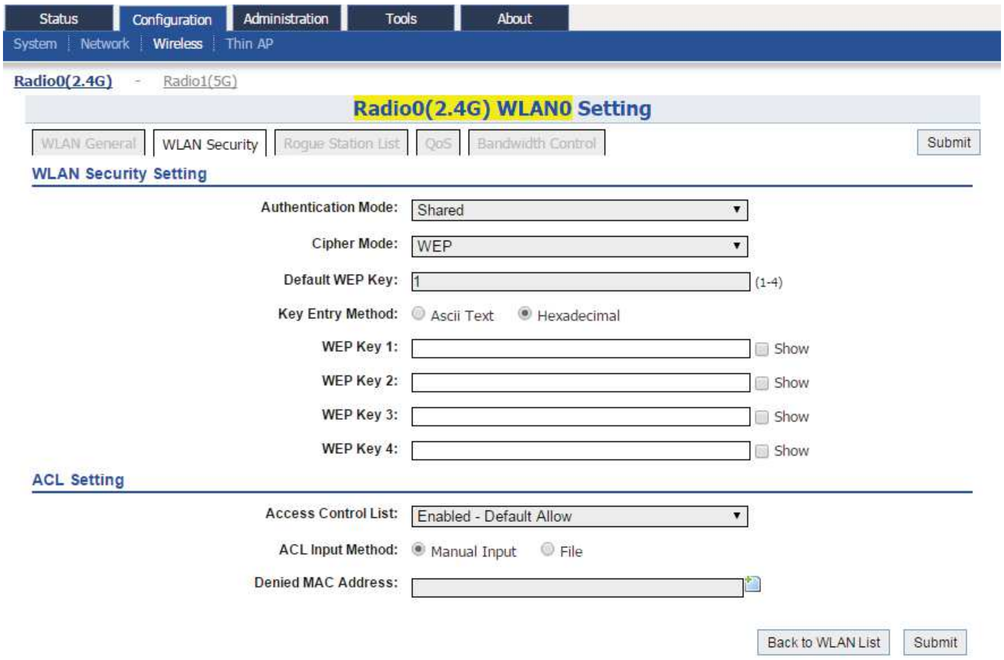
Ascii Text	key is encoded as ASCII characters (0–9, a–z, A–Z)
Hexadecimal	key is encoded as Hexadecimal characters (0–9, A–F)

6. Enter up to four keys in WEP Key 1, WEP Key 2, WEP Key 3 and WEP Key 4 respectively. You can type either up to 5 Ascii characters or up to 10 Hexadecimal characters as WEP Key.
7. Click **Submit**

4.1.1.4.1 Configure WLAN as Open network with Shared Key Authentication

Shared Key authentication is one of the authentication methods with WEP encryption. It verifies that station has knowledge of a shared secret.

Figure 19 – 2.4G WLAN # Security Setting: Shared Key Authentication



Radio0(2.4G) WLAN0 Setting

WLAN Security Setting

Authentication Mode: Shared

Cipher Mode: WEP

Default WEP Key: 1 (1-4)

Key Entry Method: ○ Ascii Text ● Hexadecimal

WEP Key 1: □ Show

WEP Key 2: □ Show

WEP Key 3: □ Show

WEP Key 4: □ Show

ACL Setting

Access Control List: Enabled - Default Allow

ACL Input Method: ● Manual Input ○ File

Denied MAC Address:

1. Go to **Configuration** > **Wireless** > **Radio0(2.4G)** > **WLAN** > **WLAN #** > **WLAN Security**
2. Select Open on **Authentication Mode**
3. Select *WEP* on **Cipher Mode**
4. Select key number *1 – 4* on **Default WEP Key**
5. Select suitable key type in **Key Entry Mode**; the options include:

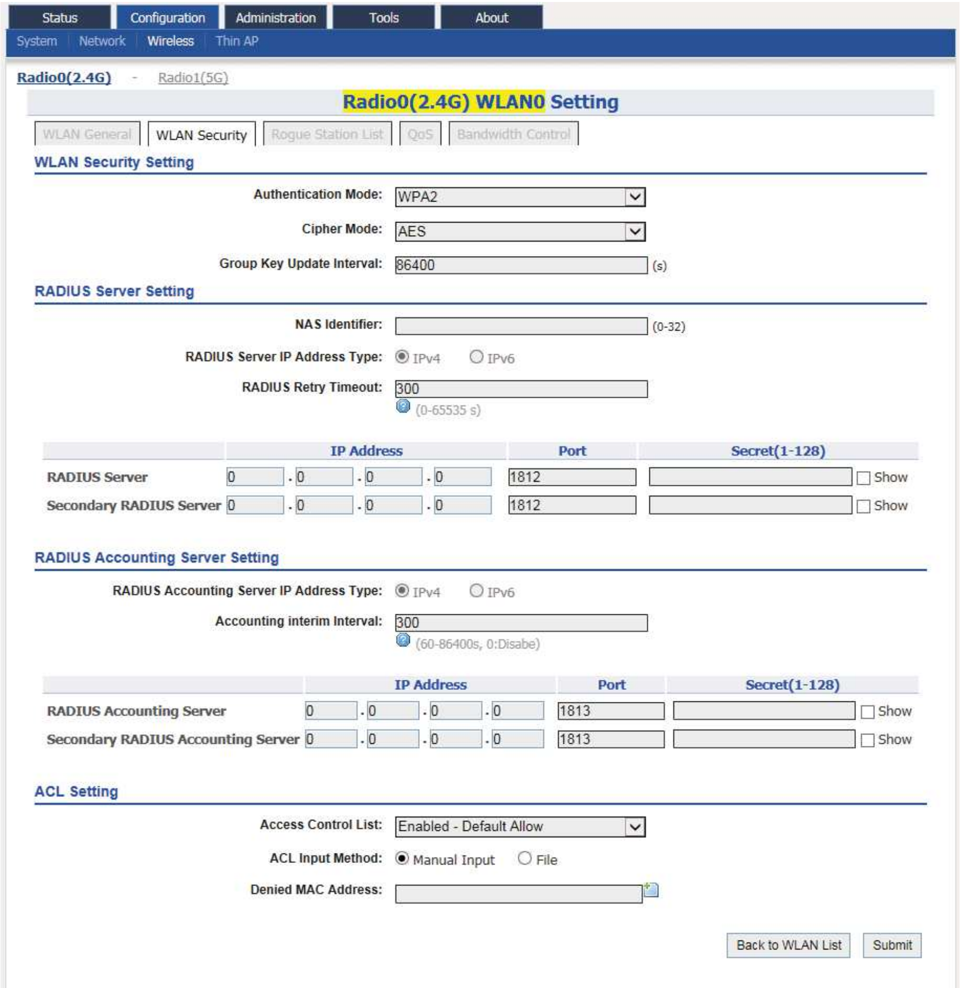
Ascii Text	key is encoded as ASCII characters (0–9, a–z, A–Z)
Hexadecimal	key is encoded as Hexadecimal characters (0–9, A–F)

6. Enter up to four keys in WEP Key 1, WEP Key 2, WEP Key 3 and WEP Key 4 respectively. You can type either up to 5 Ascii characters or up to 10 Hexadecimal characters as WEP Key.
7. Click **Submit**

4.1.1.4.2 Configure WLAN with WPA / WPA2 / WPA-auto Authentication

WPA (Wi-Fi Protected Access) or WPA2 provides enhanced security over WEP, and allows client authentication based on an external authentication server such as a RADIUS server, for corporate networks. WPA-auto is a mixed security mode which supports multiple implementations of the WPA standard, such as WPA and WPA2.

Figure 20 - 2.4G WLAN # Security Setting: WPA / WPA2 / WPA-auto Authentication



Radio0(2.4G) WLAN0 Setting

WLAN Security Setting

Authentication Mode: WPA2

Cipher Mode: AES

Group Key Update Interval: 86400 (s)

RADIUS Server Setting

NAS Identifier: (0-32)

RADIUS Server IP Address Type: ● IPv4 ○ IPv6

RADIUS Retry Timeout: 300 (0-65535 s)

	IP Address	Port	Secret(1-128)
RADIUS Server	0 . 0 . 0 . 0	1812	□ Show
Secondary RADIUS Server	0 . 0 . 0 . 0	1812	□ Show

RADIUS Accounting Server Setting

RADIUS Accounting Server IP Address Type: ● IPv4 ○ IPv6

Accounting interim Interval: 300 (60-86400s, 0:Disabe)

	IP Address	Port	Secret(1-128)
RADIUS Accounting Server	0 . 0 . 0 . 0	1813	□ Show
Secondary RADIUS Accounting Server	0 . 0 . 0 . 0	1813	□ Show

ACL Setting

Access Control List: Enabled - Default Allow

ACL Input Method: ● Manual Input ○ File

Denied MAC Address:

1. Go to **Configuration** > **Wireless** > **Radio0(2.4G)** > **WLAN** > **WLAN #** > **WLAN Security**
2. Select *WPA* / *WPA2* / *WPA-auto* on **Authentication Mode**
3. Select suitable encryption mode on **Cipher Mode**

If Authentication Mode is *WPA:*

TKIP + AES	This algorithm automatically selects TKIP or AES based on the client's capabilities
TKIP	This algorithm provides greater compatibility with older client devices, but is not supported by the 802.11n standard.

AES	This algorithm provides enhanced security over TKIP, and is the only encryption algorithm supported by the 802.11i standard.

If Authentication Mode is *WPA2*:

AES	This algorithm provides enhanced security over TKIP, and is the only encryption algorithm supported by the 802.11i standard.

If Authentication Mode is *WPA-auto*:

TKIP + AES	This algorithm automatically selects TKIP or AES based on the client's capabilities

Note:

- TKIP is not supported by 802.11n standard. If selected TKIP, the 802.11n's devices will be limited to 802.11g transfer rate, i.e. up to 54 Mbps

4. Enter suitable identification on **NAS identifier**. Remote RADIUS server uses this ID to identify its clients. This entry is available for WPA and WPA2 only.
5. Enter transmission timeout interval between *0* and *86400*s on **RADIUS Retry Timeout**. *300* is default setting. This entry is optional.
6. Enter IP address of remote RADIUS server for authentication in **IP Address of RADIUS Server**
7. Enter service port of remote RADIUS server in **Port of RADIUS Server**. *1812* is default setting.
8. Enter suitable secrets in **Secret of RADIUS Server**. It is used along with the MD5 hashing algorithm to obfuscate passwords. This secret MUST be as the same as that in RADIUS server.
9. Repeat step 6-8 if the backup RADIUS server is available. It is optional.
10. Enter interval between each interim update in seconds on **Accounting interim Interval**. *300* is default setting. This entry is optional.
11. Enter IP address of remote RADIUS Accounting Server on **IP Address of RADIUS Accounting Server**. This entry is optional.
12. Enter service port of remote RADIUS server in **Port of RADIUS Accounting Server**. *1813* is default setting. This entry is optional.

13. Enter suitable secrets in **Secret of RADIUS Accounting Server**. It is used along with the MD5 hashing algorithm to obfuscate passwords. This secret MUST be as the same as that in RADIUS server. This entry is optional.

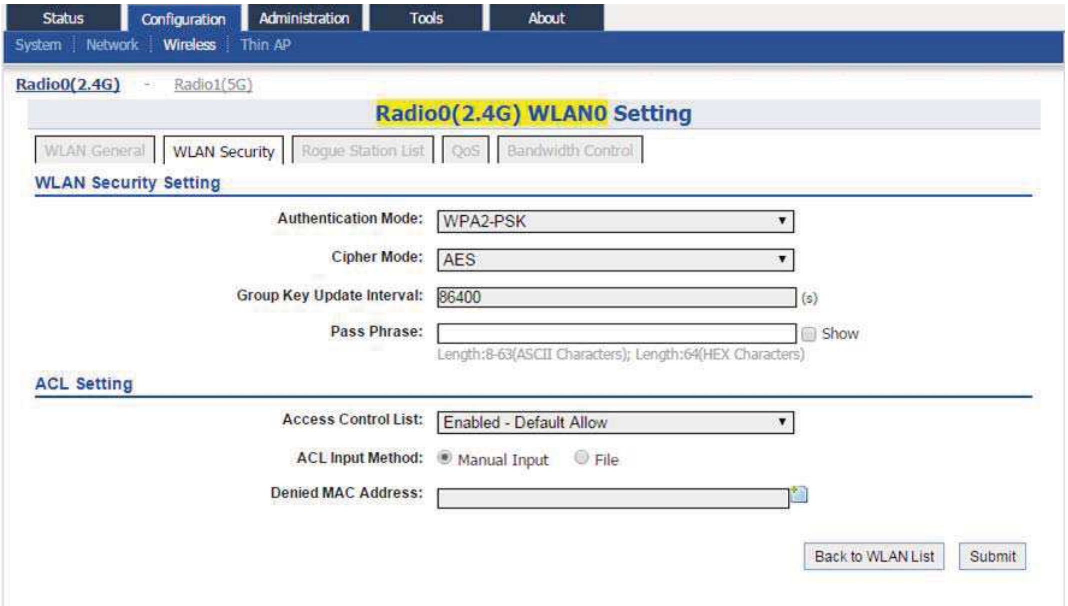
14. Repeat step 11-13 if the backup RADIUS Accounting server is available. It is optional.

15. Click **Submit**

4.1.1.4.3 Configure WLAN with WPA-PSK / WPA2-PSK / WPA-auto-PSK Authentication

Use of WPA or WPA2 provides enhanced security over WEP, and allows client authentication based on either a pre-shared key (PSK), for home or small office networks. WPA-auto-PSK is a mixed security mode which supports multiple implementations of the WPA standard, such as WPA-PSK and WPA2-PSK.

Figure 21 - 2.4G WLAN # Security Setting: WPA-PSK / WPA2-PSK / WPA-auto-PSK Authentication



Radio0(2.4G) WLAN0 Setting

WLAN Security Setting

Authentication Mode: WPA2-PSK

Cipher Mode: AES

Group Key Update Interval: 86400 (s)

Pass Phrase: □ Show

Length:8-63(ASCII Characters); Length:64(HEX Characters)

ACL Setting

Access Control List: Enabled - Default Allow

ACL Input Method: ● Manual Input ○ File

Denied MAC Address:

1. Go to **Configuration** > **Wireless** > **Radio0(2.4G)** > **WLAN** > **WLAN #** > **WLAN Security**

2. Select *WPA-PSK* / *WPA2-PSK* / *WPA-auto-PSK* on **Authentication Mode**

3. Select suitable encryption mode on **Cipher Mode**

If Authentication Mode is *WPA:*

TKIP + AES	This algorithm automatically selects TKIP or AES based on the client's capabilities
TKIP	This algorithm provides greater compatibility with older client devices, but is not supported by the 802.11n standard.

AES	This algorithm provides enhanced security over TKIP, and is the only encryption algorithm supported by the 802.11i standard.

If Authentication Mode is *WPA2*:

AES	This algorithm provides enhanced security over TKIP, and is the only encryption algorithm supported by the 802.11i standard.

If Authentication Mode is *WPA-auto*:

TKIP + AES	This algorithm automatically selects TKIP or AES based on the client's capabilities

Note:

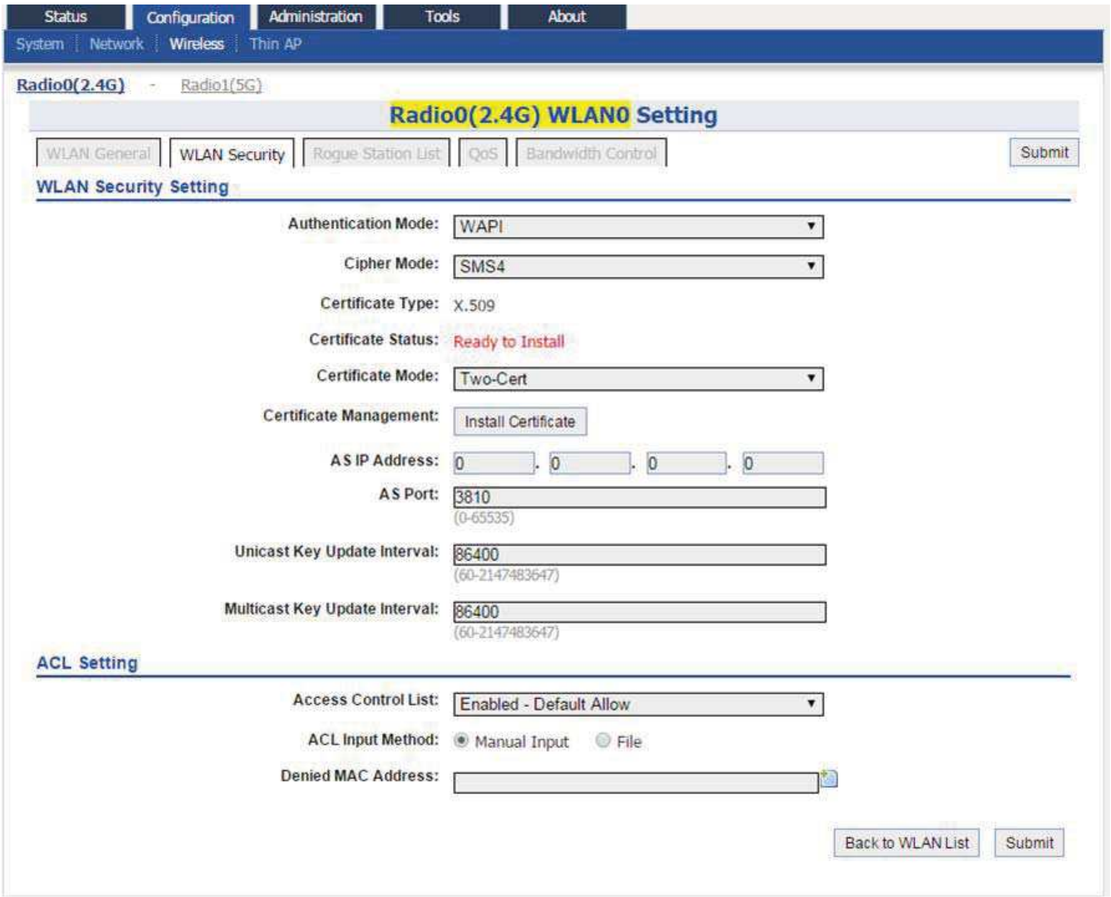
- *TKIP is not supported by 802.11n standard. If selected TKIP, the 802.11n's devices will be limited to 802.11g transfer rate, i.e. up to 54 Mbps*

4. Enter interval time in second in **Group Key Update Interval**. *86400* is default setting. This entry is optional.
5. Enter an ASCII string between 8 and 63 characters long or a HEX string with 64 characters long on **Pass Phrase** that users will use to connect to the wireless network.
6. Click **Submit**

4.1.1.4.4 Configure WLAN with WAPI Authentication

WLAN Authentication and Privacy Infrastructure (WAPI) is a Chinese National Standard for Wireless LANs (GB 15629.11-2003).

Figure 22 - 2.4G WLAN # Security Setting: WAPI Authentication



Radio0(2.4G) WLAN0 Setting

WLAN Security Setting

Authentication Mode: WAPI
Cipher Mode: SMS4
Certificate Type: X.509
Certificate Status: Ready to Install
Certificate Mode: Two-Cert
Certificate Management: Install Certificate
AS IP Address: 0 . 0 . 0 . 0
AS Port: 3810 (0-65535)
Unicast Key Update Interval: 86400 (60-2147483647)
Multicast Key Update Interval: 86400 (60-2147483647)

ACL Setting

Access Control List: Enabled - Default Allow
ACL Input Method: ● Manual Input ○ File
Denied MAC Address:

1. Go to **Configuration** > **Wireless** > **Radio0(2.4G)** > **WLAN** > **WLAN #** > **WLAN Security**
2. Select *WAPI* on **Authentication Mode**
3. Select *SMS4* in **Cipher Mode**

4. Select suitable option in **Certificate Mode**; the options includes:

Two-Cert	Wi-Fi client is verified by the certification from authentication server (AS) and Access Point (AP)
Three-Cert	Wi-Fi client is verified by the certification from authentication server (AS), access point (AP), and certificate authority (CA)

5. Click **Install Certificate**; a window for installing certificate is shown on Figure 23 and Figure 24.

Figure 23 - Two-Cert Mode Certification Installation

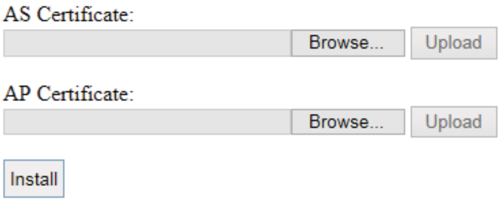
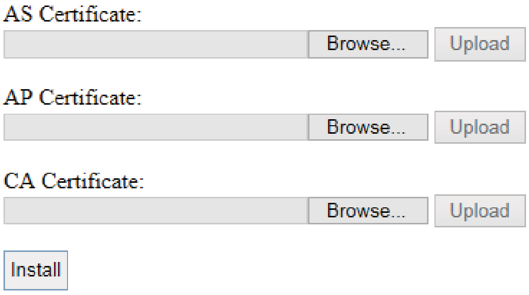


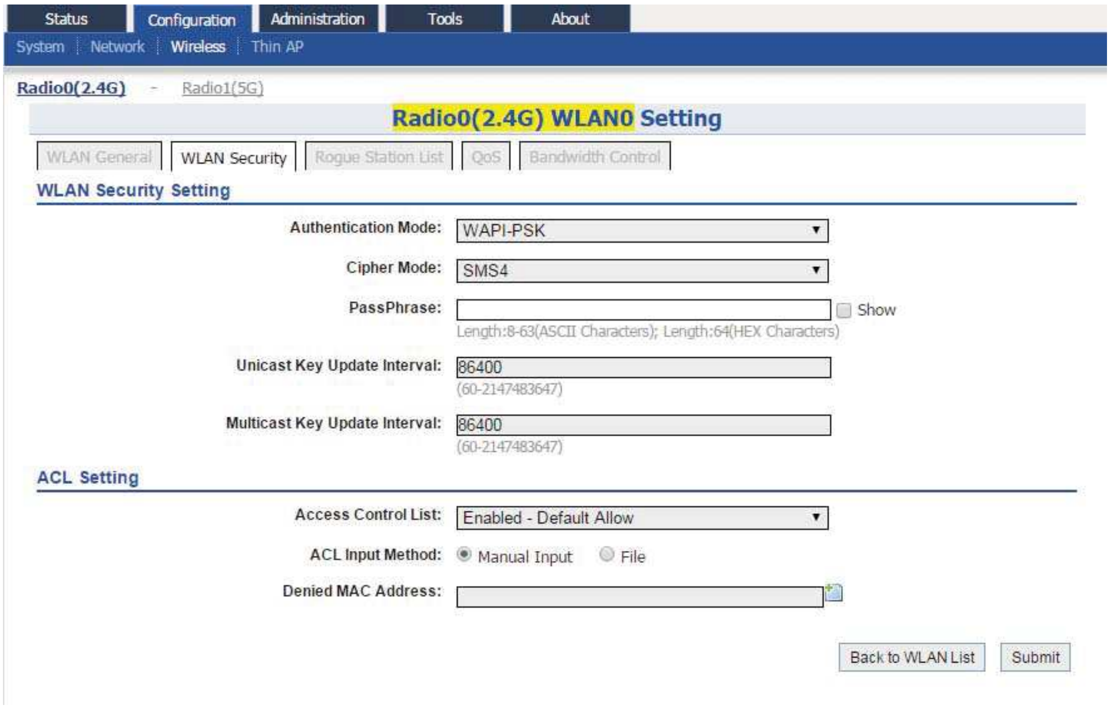
Figure 24 - Three-Cert Mode Certification Installation



6. Click **Browse** to select suitable certifications
7. Click **Upload** to upload the selected certifications to CPE
8. Click **Install** to install certifications
9. Enter IP address of AS server on **AS IP Address**
10. Enter service port of AS server in **AS Port**
11. Enter interval time between 60 and 2147483647s in **Unicast Key Update Interval**; *86400* is default setting. This entry is optional.
12. Enter interval time between 60 and 2147483647s in **Multicast Key Update Interval**; *86400* is default setting. This entry is optional.
13. Click **Submit**

4.1.1.4.5 Configure WLAN with WAPI-PSK Authentication

Figure 25 - 2.4G WLAN # Security Setting: WAPI-PSK Authentication



Authentication Mode: WAPI-PSK

Cipher Mode: SMS4

PassPhrase: □ Show
Length:8-63(ASCII Characters); Length:64(HEX Characters)

Unicast Key Update Interval: 86400
(60-2147483647)

Multicast Key Update Interval: 86400
(60-2147483647)

Access Control List: Enabled - Default Allow

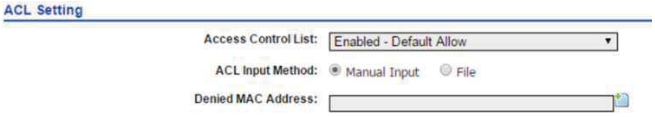
ACL Input Method: ● Manual Input ○ File

Denied MAC Address:

1. Go to **Configuration** > **Wireless** > **Radio0(2.4G)** > **WLAN** > **WLAN #** > **WLAN Security**
2. Select *WAPI* on **Authentication Mode**
3. Select *SMS4* in **Cipher Mode**
4. Enter in an ASCII string between 8 and 63 characters or a HEX string with 64 characters long in **Pass Phrase** that users will use to connect to the wireless network.
5. Enter interval time between 60 and 2147483647s in **Unicast Key Update Interval**; *86400* is default setting. This entry is optional.
6. Enter interval time between 60 and 2147483647s in **Multicast Key Update Interval**; *86400* is default setting. This entry is optional.
7. Click **Submit**

4.1.1.5 Step 4: Configure ACL Setting

Figure 26 – 2.4G WLAN # ACL Setting



ACL Setting

Access Control List: Enabled - Default Allow

ACL Input Method: ● Manual Input ○ File

Denied MAC Address:

1. Go to **Configuration** > **Wireless** > **Radio0(2.4G)** > **WLAN** > **WLAN #** > **ACL Setting**
2. Select appropriate option on **Access Control List**; options include

Disable	ACL is disabled
Enabled – Default Allow	ACL is enabled. The MAC addresses which are specified in the ACL will consider as Deny. Every wireless client can associate to the AP unless its MAC address is on the list
Enabled – Default Deny	ACL is enabled. The MAC addresses which are specified in the ACL will consider as Allow. Every wireless client CANNOT associate to the AP unless its MAC address is on the list

3. Select *Manual Input* on **ACL Input Method** if network administrator prefers input the entry one by one manually

   Or select File on **ACL Input Method** if network administrator prefers upload a MAC address list (.txt file)
4. Enter MAC address entry one by one or upload the corresponding file to CPE; it is optional
5. Click **Submit**

Note:

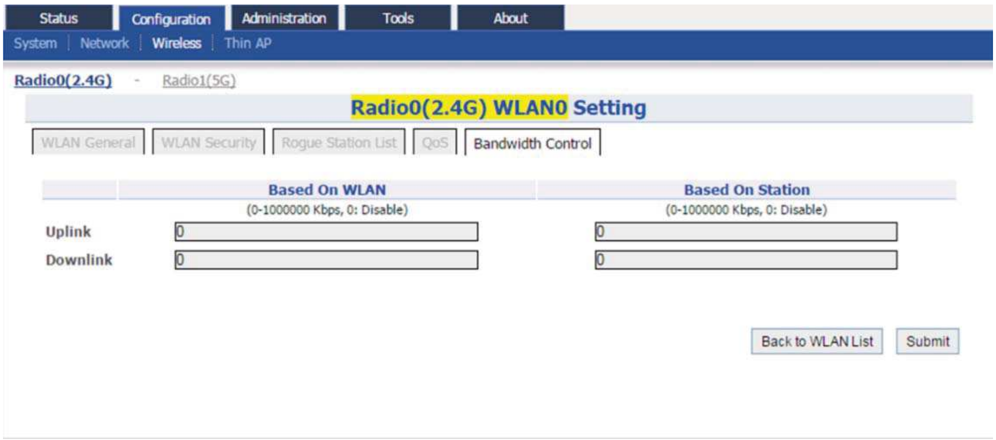
- *Network Administrator shall select Disable or Enabled – Default Allow if no ACL entry will be input on CPE*

4.1.1.6 Step 5: Configure WLAN # QoS

Please refer to Quality of Service (QoS) on page 129

4.1.1.7 Step 6: Configure WLAN # Bandwidth Control

Figure 27 – 2.4G WLAN # Bandwidth Control



Radio0(2.4G) WLAN0 Setting

	Based On WLAN (0-1000000 Kbps, 0: Disable)	Based On Station (0-1000000 Kbps, 0: Disable)
Uplink	0	0
Downlink	0	0

1. Go to **Configuration** > **Wireless** > **Radio0(2.4G)** > **WLAN** > **WLAN #** > **Bandwidth Control**
2. Specify the uplink and downlink limitation under **Based on WLAN** for the particular WLAN

   Or specify the uplink and downlink limitation under **Based on Station** for each associated station. *0* is default value and denotes as disable
3. Click **Submit**

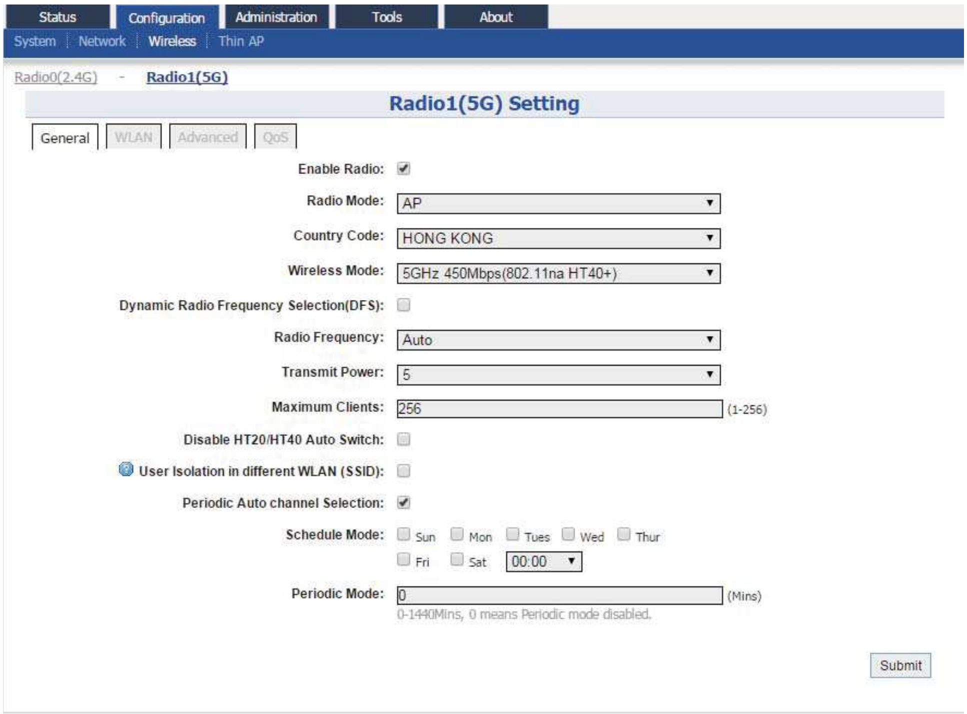
4.1.1.8 Step 7: Apply Submitted Configurations on the CPE Device

1. Click **Save & Apply** from the top on the right.

4.1.2Radio1 – 5G

4.1.2.1 Step 1: Configure General Wireless Setting

Figure 28 - Radio1 (5G) General Setting



Radio1(5G) Setting

Enable Radio: ☑

Radio Mode: AP

Country Code: HONG KONG

Wireless Mode: 5GHz 450Mbps(802.11na HT40+)

Dynamic Radio Frequency Selection(DFS): □

Radio Frequency: Auto

Transmit Power: 5

Maximum Clients: 256 (1-256)

Disable HT20/HT40 Auto Switch: □

User Isolation in different WLAN (SSID): □

Periodic Auto channel Selection: ☑

Schedule Mode: □ Sun □ Mon □ Tues □ Wed □ Thur □ Fri □ Sat 00:00

Periodic Mode: 0 (Mins)
0-1440Mins, 0 means Periodic mode disabled.

1. Go to **Configuration** > **Wireless** > **Radio1(5G)** > **General**
2. Select **Enable Radio** checkbox to enable radio interface
3. Select *AP* in **Radio Mode**
4. Select the correct country code on **Country Code**; this option ensures that the CPE device uses only the radio channels allowed in your country or region
5. Select suitable wireless mode on **Wireless Mode**; the options include:

5G 54Mbps (802.11 a)

5G 216.7Mbps (802.11 na HT20)

5G 216.7Mbps (802.11 n-only HT20)

5G 450Mbps (802.11 n-only HT40+)

5G 450Mbps (802.11 na HT40+)

5G 450Mbps (802.11 na HT40-)

5G 450Mbps (802.11 n-only HT40-)

5G 289Mbps (802.11 ac HT20)

5G 600Mbps (802.11 ac HT40+)

5G 600Mbps (802.11 ac HT40-)

*5G 1.3Gbps (802.11 ac HT80); **Default Setting***

6. Select **Dynamic Radio Frequency Selection (DFS)** checkbox to enable automatic channel selection that selects the least congested channel where radar is not detected during booting up.

Note:

- **Radio Frequency** is set as *auto* automatically if DFS is enabled

---

7. Select suitable operating channel on **Radio Frequency**;

Note:

- *You should select the suitable operating channel based on the on-site channel scan result.*

---

8. Select suitable transmission power on **Transmission Power**;

Note:

- *You should follow the regulation from local Communications Authority*

---

9. Enter the maximum associated client between 1 and 256 on **Maximum Client** that the radio interface serves. *256* is the default setting. This entry is optional.

10. Select **Disable HT20/HT40 Auto Switch** checkbox that CPE device will NOT switch the channel width between 20 MHz and 40 MHz automatically. This entry is optional and only available for the following wireless modes:

5G 450Mbps (802.11 n-only HT40+)

5G 450Mbps (802.11 na HT40+)

5G 450Mbps (802.11 na HT40-)

5G 450Mbps (802.11 n-only HT40-)

11. Select **Enable Inter-WLAN User Isolation** checkbox that CPE device block the users' communication across different SSID in the AP directly. This entry is optional.

12. Select **Periodic Auto Channel Section** checkbox to enable scheduled channel selection task on the radio interface. This entry is optional and only available if *auto* is selected on **Radio Frequency**. The available schedule modes are:

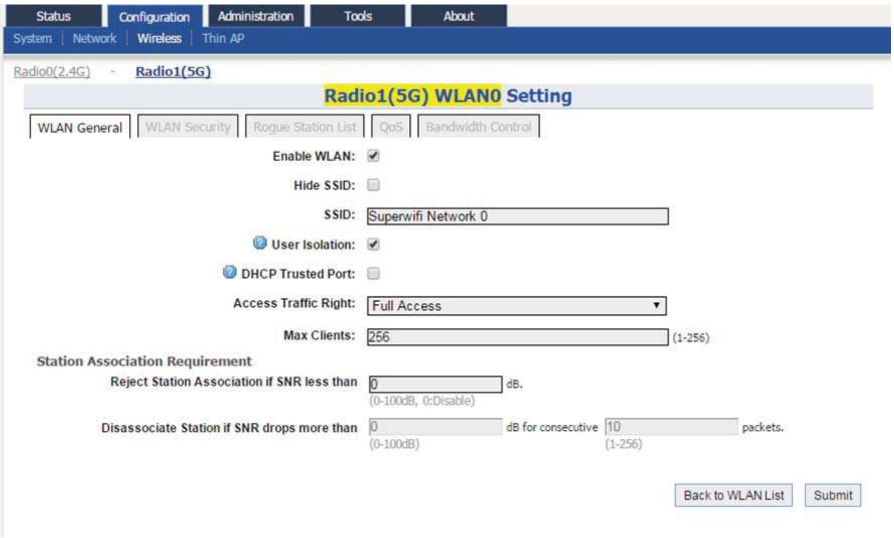
Schedule Mode Select exact time and day(s) for selecting radio frequency for the interface

Periodic Mode Select a countdown timer (minute) for selecting radio frequency for the interface; *0* denotes disable.

13. Click **Submit**

4.1.2.2 Step 2: Configure WLAN # General Setting

Figure 29 – 5G WLAN # General Setting



Radio1(5G) WLAN0 Setting

Enable WLAN: ☑

Hide SSID: □

SSID: Superwifi Network 0

User Isolation: ☑

DHCP Trusted Port: □

Access Traffic Right: Full Access

Max Clients: 256 (1-256)

Station Association Requirement

Reject Station Association if SNR less than 0 dB. (0-100dB, 0:Disable)

Disassociate Station if SNR drops more than 0 dB for consecutive 10 packets. (0-100dB) (1-256)

1. Go to **Configuration** > **Wireless** > **Radio1 (5G)** > **WLAN #** > More…

2. Select **Enable WLAN** checkbox to enable WLAN

3. Select **Hide SSID** checkbox to hide SSID name from its beacon frame. This entry is optional.

4. Enter a unique name for the particular WLAN on **SSID**.

Note:

– If you want to configure the same SSID on two different WLAN; their security setting MUST be different from each other.

5. Select **User Isolation** checkbox to block user communication within the same SSID in the AP directly. This entry is optional.

6. Deselect the **DHCP Trust Port** checkbox to prevent illegal DHCP servers offering IP address to DHCP clients via this WLAN. This entry is optional.

7. Specify the suitable privilege of associated clients on **Access Traffic Right**; the options include

Full Access	Associated client can access Internet and manage AP
AP Management Only	Associated client can manage AP only, but not able to access the Internet
AP Management Disable	Associated client can access the Internet, but not able to manage AP

8. Specify the maximum associated clients between *1* and *256* on **Max Clients** for this WLAN. *256* is the default setting.

Note:

- **Max Clients** in WLAN 0 – 15 MUST be smaller than or equal to (≥) the **Max Clients** setting on Radio General Setting

9. Specify an additional requirement on Signal Strength to Noise Ratio (SNR) for associated clients under **Station Association Requirement**. This requirement is optional. You may fill up the following fields:

Reject Station Association if SNR less than X dB	*X* denote the minimum SNR level which allow clients to associate; You can select any integer between *0*dB and *100*dB; *0* denotes as disable; *0* is default setting
Disassociate Station if SNR drops more than Y dB for consecutive Z packets	Y denotes the SNR tolerance; Z denotes the number of consecutive packets their SNR are below the difference of X - Y.

Notes:

- Example for Station Association Requirement with the following settings:

Reject Station Association if SNR less than *30* dB (X = 30); Disassociate Station if SNR drops more than *20* dB for consecutive *10* packets (Y = 20; Z = 10)

Consequence:

AP accepts the clients to associate if the SNR of packets from the clients is high than (>) 30dB;

AP kicks out the associated client if the SNR of 10 consecutive packets is below (<) 10 dB (30 dB – 20 dB)

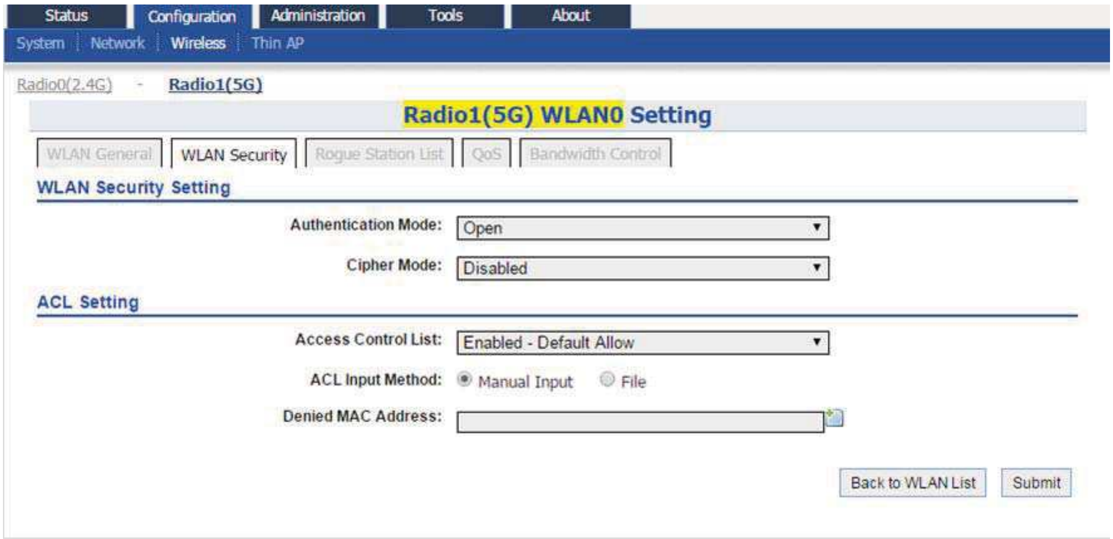
10. Click **Submit**

4.1.2.3 Step 3: Configure WLAN # Security Setting

4.1.2.3.1 Configure WLAN as Open Network

This setting is typically only used in a guest network. No security measure is enforced.

Figure 30 – 5G WLAN # Security Setting: Open Network



Authentication Mode: Open

Cipher Mode: Disabled

Access Control List: Enabled - Default Allow

ACL Input Method: ● Manual Input ○ File

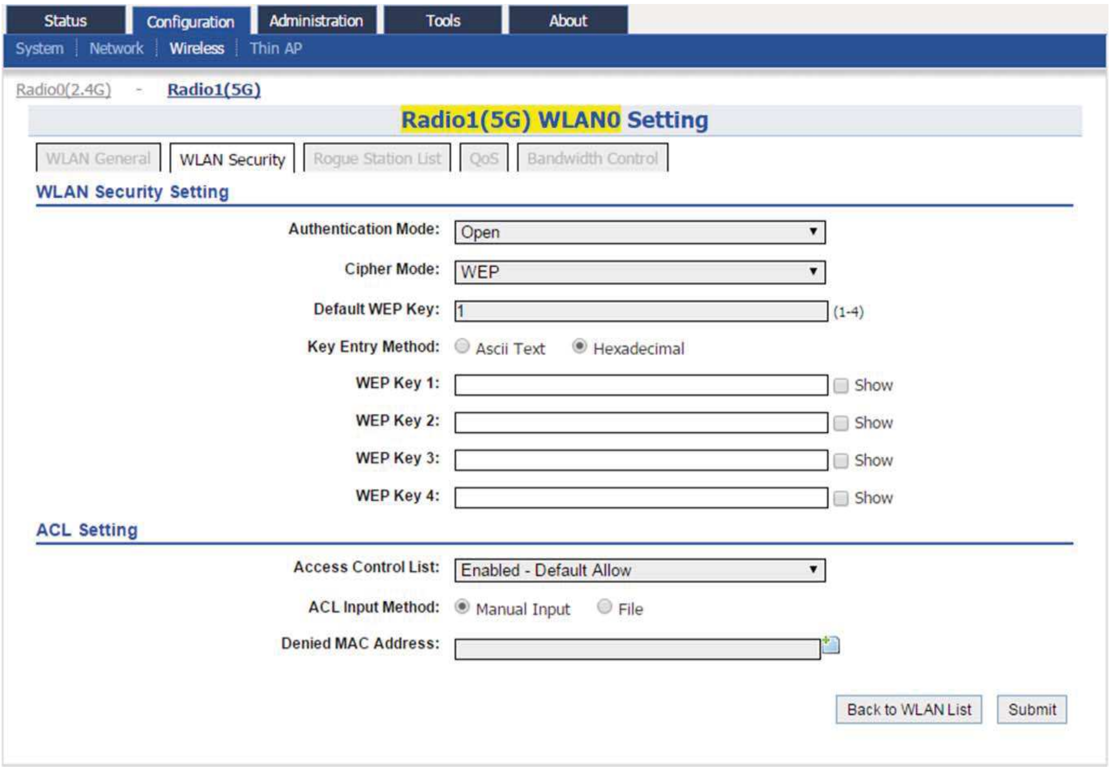
Denied MAC Address:

1. Go to **Configuration** > **Wireless** > **Radio1(5G)** > **WLAN** > **WLAN #** > **WLAN Security**
2. Select Open on **Authentication Mode**
3. Select *Disabled* on **Cipher Mode**
4. Click **Submit**

4.1.2.3.2 Configure WLAN as Open network with WEP encryption

This setting provides minimal security as it allows all requesting devices to join a given network.

Figure 31 – 5G WLAN # Security Setting: Open Network with WEP



Radio1(5G) WLAN0 Setting

WLAN Security Setting

Authentication Mode: Open

Cipher Mode: WEP

Default WEP Key: 1 (1-4)

Key Entry Method: ○ Ascii Text ● Hexadecimal

WEP Key 1: □ Show

WEP Key 2: □ Show

WEP Key 3: □ Show

WEP Key 4: □ Show

ACL Setting

Access Control List: Enabled - Default Allow

ACL Input Method: ● Manual Input ○ File

Denied MAC Address:

1. Go to **Configuration** > **Wireless** > **Radio1(5G)** > **WLAN** > **WLAN #** > **WLAN Security**
2. Select Open on **Authentication Mode**
3. Select *WEP* on **Cipher Mode**
4. Select key number *1 – 4* on **Default WEP Key**
5. Select suitable key type in **Key Entry Mode**; the options include:

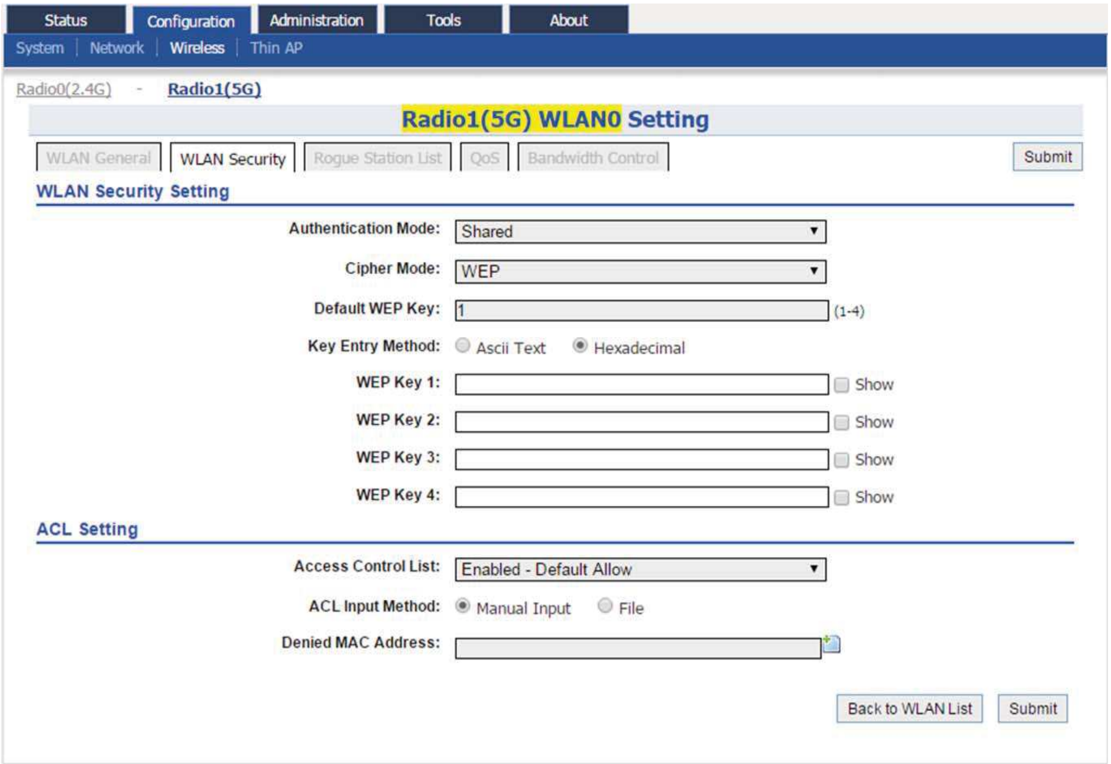
Ascii Text	key is encoded as ASCII characters (0–9, a–z, A–Z)
Hexadecimal	key is encoded as Hexadecimal characters (0–9, A–F)

6. Enter up to four keys in WEP Key 1, WEP Key 2, WEP Key 3 and WEP Key 4 respectively. You can type either up to 5 Ascii characters or up to 10 Hexadecimal characters as WEP Key.
7. Click **Submit**

4.1.2.3.3 Configure WLAN as Open network with Shared Key Authentication

Shared Key authentication is one of the authentication methods with WEP encryption. It verifies that station has knowledge of a shared secret.

Figure 32 – 5G WLAN # Security Setting: Shared Key Authentication



Radio1(5G) WLAN0 Setting

WLAN Security Setting

Authentication Mode: Shared

Cipher Mode: WEP

Default WEP Key: 1 (1-4)

Key Entry Method: ○ Ascii Text ● Hexadecimal

WEP Key 1: □ Show

WEP Key 2: □ Show

WEP Key 3: □ Show

WEP Key 4: □ Show

ACL Setting

Access Control List: Enabled - Default Allow

ACL Input Method: ● Manual Input ○ File

Denied MAC Address:

1. Go to **Configuration** > **Wireless** > **Radio1(5G)** > **WLAN** > **WLAN #** > **WLAN Security**
2. Select *Shared* on **Authentication Mode**
3. Select *WEP* on **Cipher Mode**
4. Select key number *1 – 4* on **Default WEP Key**
5. Select suitable key type in **Key Entry Mode**; the options include:

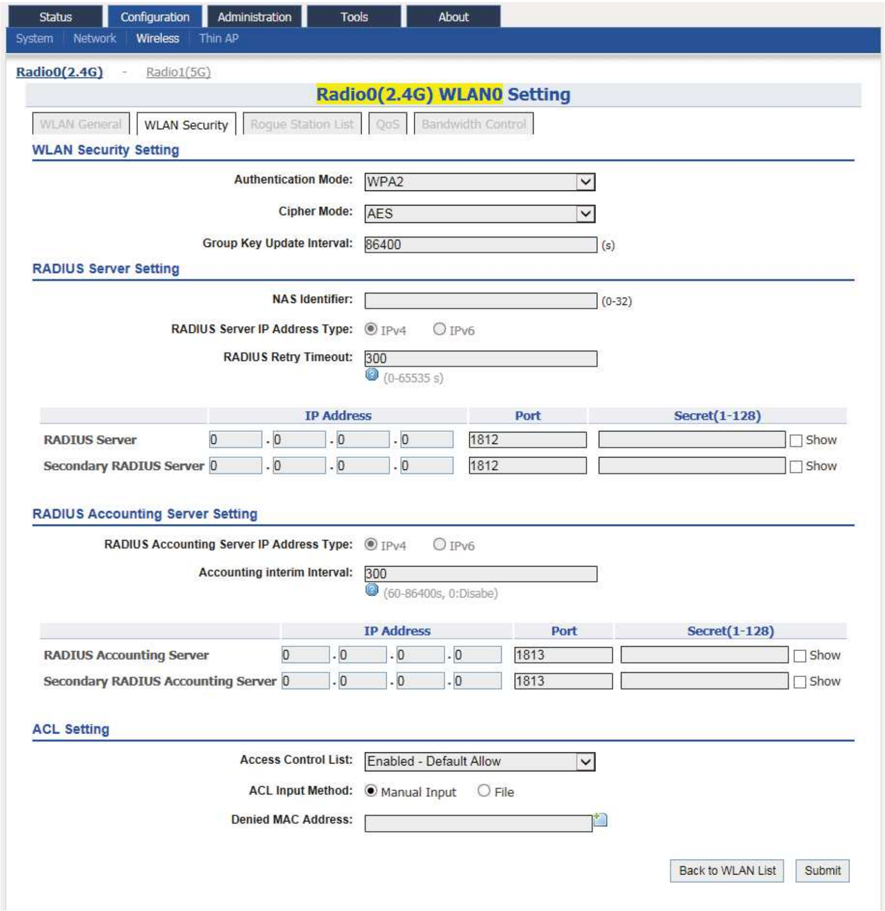
Ascii Text	key is encoded as ASCII characters (0–9, a–z, A–Z)
Hexadecimal	key is encoded as Hexadecimal characters (0–9, A–F)

6. Enter up to four keys in WEP Key 1, WEP Key 2, WEP Key 3 and WEP Key 4 respectively. You can type either up to 5 ASCII characters or up to 10 Hexadecimal characters as WEP Key.
7. Click **Submit**

4.1.2.3.4 Configure WLAN with WPA / WPA2 / WPA-auto Authentication

WPA (Wi-Fi Protected Access) or WPA2 provides enhanced security over WEP, and allows client authentication based on an external authentication server such as a RADIUS server, for corporate networks. WPA-auto is a mixed security mode which supports multiple implementations of the WPA standard, such as WPA and WPA2.

Figure 33 - 5G WLAN # Security Setting: WPA / WPA2 / WPA-auto Authentication



Radio0(2.4G) WLAN0 Setting

WLAN Security Setting

Authentication Mode: WPA2

Cipher Mode: AES

Group Key Update Interval: 86400 (s)

RADIUS Server Setting

NAS Identifier: (0-32)

RADIUS Server IP Address Type: ● IPv4 ○ IPv6

RADIUS Retry Timeout: 300 (0-65535 s)

	IP Address	Port	Secret(1-128)
RADIUS Server	0 . 0 . 0 . 0	1812	□ Show
Secondary RADIUS Server	0 . 0 . 0 . 0	1812	□ Show

RADIUS Accounting Server Setting

RADIUS Accounting Server IP Address Type: ● IPv4 ○ IPv6

Accounting interim Interval: 300 (60-86400s, 0:Disabe)

	IP Address	Port	Secret(1-128)
RADIUS Accounting Server	0 . 0 . 0 . 0	1813	□ Show
Secondary RADIUS Accounting Server	0 . 0 . 0 . 0	1813	□ Show

ACL Setting

Access Control List: Enabled - Default Allow

ACL Input Method: ● Manual Input ○ File

Denied MAC Address:

1. Go to **Configuration** > **Wireless** > **Radio1(5G)** > **WLAN** > **WLAN #** > **WLAN Security**
2. Select *WPA* / *WPA2* / *WPA-auto* on **Authentication Mode**
3. Select suitable encryption mode on **Cipher Mode**
4. If Authentication Mode is *WPA:*

TKIP + AES	This algorithm automatically selects TKIP or AES based on the client's capabilities
TKIP	This algorithm provides greater compatibility with older client

	devices, but is not supported by the 802.11n standard.
AES	This algorithm provides enhanced security over TKIP, and is the only encryption algorithm supported by the 802.11i standard.

If Authentication Mode is *WPA2*:

AES	This algorithm provides enhanced security over TKIP, and is the only encryption algorithm supported by the 802.11i standard.

If Authentication Mode is *WPA-auto*:

TKIP + AES	This algorithm automatically selects TKIP or AES based on the client's capabilities

Note:

－ TKIP is not supported by 802.11n standard. If selected TKIP, the 802.11n's devices will be limited to 802.11g transfer rate, i.e. up to 54 Mbps

5. Enter suitable identification on **NAS identifier**. Remote RADIUS server uses this ID to identify its clients. This entry is available for WPA and WPA2 only.
6. Enter transmission timeout interval between *0* and *86400*s on **RADIUS Retry Timeout**. *300* is default setting. This entry is optional.
7. Enter IP address of remote RADIUS server for authentication in **IP Address of RADIUS Server**
8. Enter service port of remote RADIUS server in **Port of RADIUS Server**. *1812* is default setting.
9. Enter suitable secrets in **Secret of RADIUS Server**. It is used along with the MD5 hashing algorithm to obfuscate passwords. This secret MUST be as the same as that in RADIUS server.
10. Repeat step 6-8 if the backup RADIUS server is available. It is optional.
11. Enter interval between each interim update in seconds on **Accounting interim Interval**. *300* is default setting. This entry is optional.
12. Enter IP address of remote RADIUS Accounting Server on **IP Address of RADIUS Accounting Server**. This entry is optional.
13. Enter service port of remote RADIUS server in **Port of RADIUS Accounting Server**. *1813* is default setting. This entry is optional.

14. Enter suitable secrets in **Secret of RADIUS Accounting Server**. It is used along with the MD5 hashing algorithm to obfuscate passwords. This secret MUST be as the same as that in RADIUS server. This entry is optional.

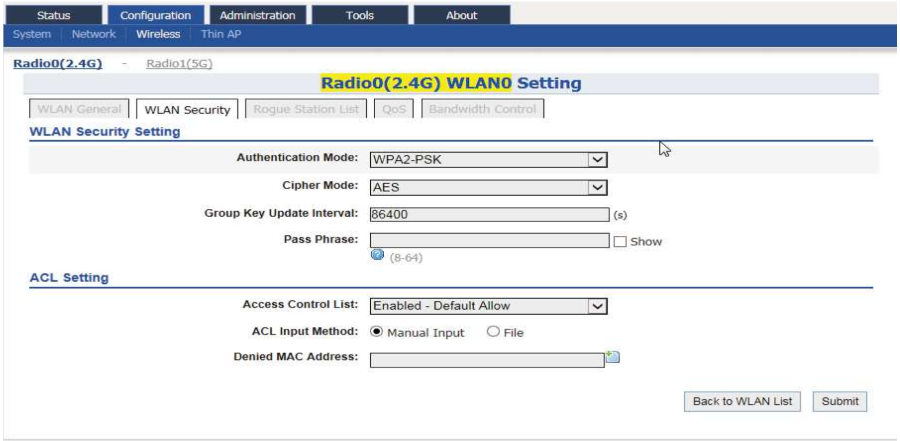
15. Repeat step 11-13 if the backup RADIUS Accounting server is available. It is optional.

16. Click **Submit**

Configure WLAN with WPA-PSK / WPA2-PSK / WPA-auto-PSK Authentication

Use of WPA or WPA2 provides enhanced security over WEP, and allows client authentication based on either a pre-shared key (PSK), for home or small office networks. WPA-auto-PSK is a mixed security mode which supports multiple implementations of the WPA standard, such as WPA-PSK and WPA2-PSK.

Figure 34 - 5G WLAN # Security Setting: WPA-PSK / WPA2-PSK / WPA-auto-PSK Authentication



Radio0(2.4G) WLAN0 Setting

WLAN Security Setting

Authentication Mode: WPA2-PSK

Cipher Mode: AES

Group Key Update Interval: 86400 (s)

Pass Phrase: □ Show (8-64)

ACL Setting

Access Control List: Enabled - Default Allow

ACL Input Method: ● Manual Input ○ File

Denied MAC Address:

1. Go to **Configuration** > **Wireless** > **Radio1(5G)** > **WLAN** > **WLAN #** > **WLAN Security**

2. Select *WPA-PSK* / *WPA2-PSK* / *WPA-auto-PSK* on **Authentication Mode**

3. Select suitable encryption mode on **Cipher Mode**

If Authentication Mode is *WPA:*

TKIP + AES	This algorithm automatically selects TKIP or AES based on the client's capabilities
TKIP	This algorithm provides greater compatibility with older client devices, but is not supported by the 802.11n standard.
AES	This algorithm provides enhanced security over TKIP, and is

	the only encryption algorithm supported by the 802.11i standard.

If Authentication Mode is *WPA2*:

AES	This algorithm provides enhanced security over TKIP, and is the only encryption algorithm supported by the 802.11i standard.

If Authentication Mode is *WPA-auto*:

TKIP + AES	This algorithm automatically selects TKIP or AES based on the client's capabilities

Note:

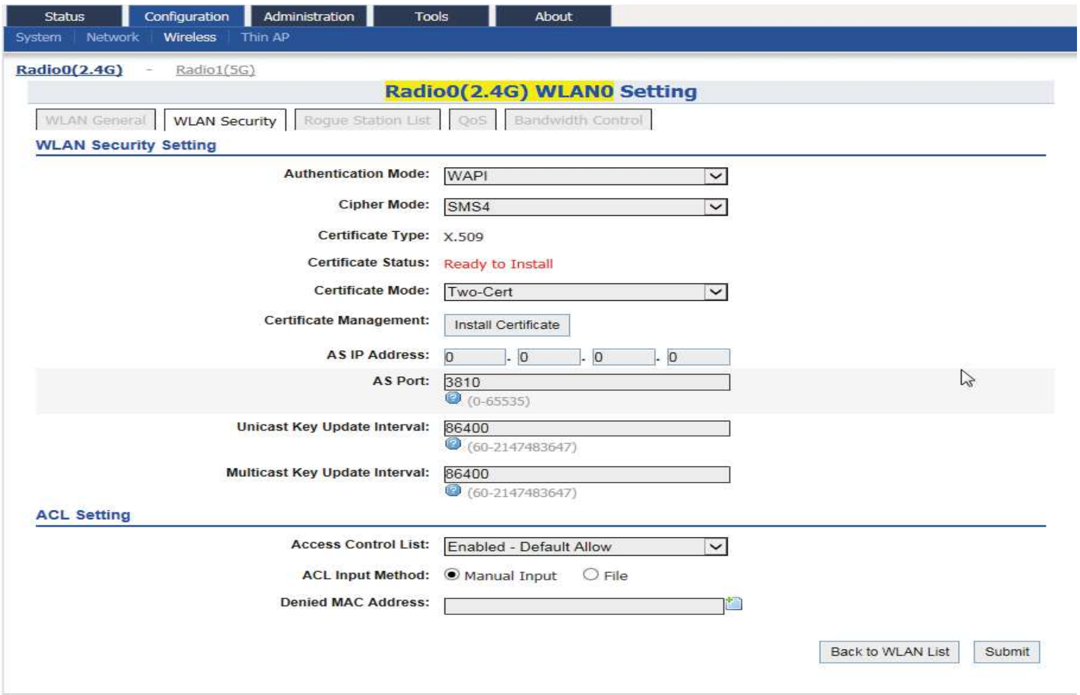
- *TKIP is not supported by 802.11n standard. If selected TKIP, the 802.11n's devices will be limited to 802.11g transfer rate, i.e. up to 54 Mbps*

4. Enter interval time in second in **Group Key Update Interval**. *86400* is default setting. This entry is optional.
5. Enter an ASCII string between 8 and 63 characters long or a HEX string with 64 characters long on **Pass Phrase** that users will use to connect to the wireless network.
6. Click **Submit**

4.1.2.3.5 Configure WLAN with WAPI Authentication

WLAN Authentication and Privacy Infrastructure (WAPI) is a Chinese National Standard for Wireless LANs (GB 15629.11-2003).

Figure 35 - 5G WLAN # Security Setting: WAPI Authentication



Radio0(2.4G) WLAN0 Setting

WLAN Security Setting

Authentication Mode: WAPI

Cipher Mode: SMS4

Certificate Type: X.509

Certificate Status: Ready to Install

Certificate Mode: Two-Cert

Certificate Management: Install Certificate

AS IP Address: 0 . 0 . 0 . 0

AS Port: 3810 (0-65535)

Unicast Key Update Interval: 86400 (60-2147483647)

Multicast Key Update Interval: 86400 (60-2147483647)

ACL Setting

Access Control List: Enabled - Default Allow

ACL Input Method: ● Manual Input ○ File

Denied MAC Address:

1. Go to **Configuration** > **Wireless** > **Radio1(5G)** > **WLAN** > **WLAN #** > **WLAN Security**
2. Select *WAPI* on **Authentication Mode**
3. Select *SMS4* in **Cipher Mode**
4. Select suitable option in **Certificate Mode**; the options includes:

Two-Cert	Wi-Fi client is verified by the certification from authentication server (AS) and Access Point (AP)
Three-Cert	Wi-Fi client is verified by the certification from authentication server (AS), access point (AP), and certificate authority (CA)

5. Click **Install Certificate**; a window for installing certificate is shown on

6. Figure 36 and Figure 37.

Figure 36 - Two-Cert Mode Certification Installation

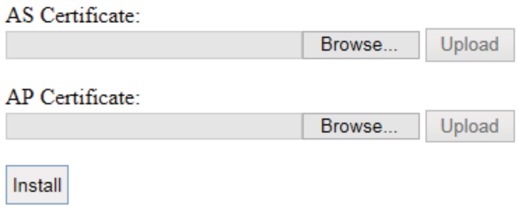
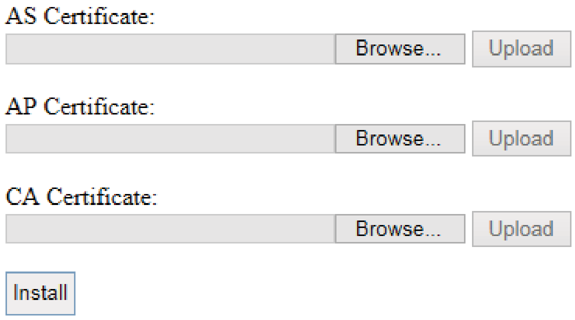


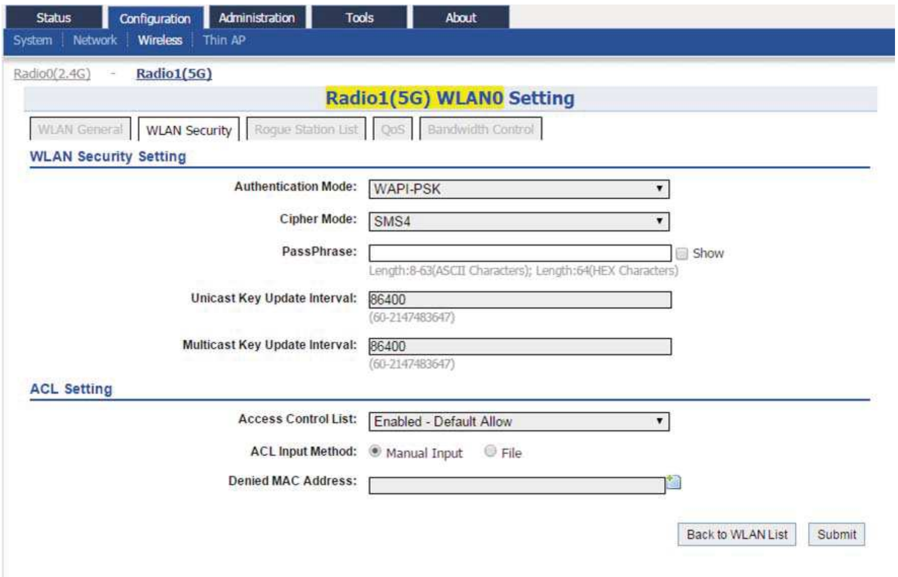
Figure 37 - Three-Cert Mode Certification Installation



7. Click **Browse** to select suitable certifications
8. Click **Upload** to upload the selected certifications to CPE
9. Click **Install** to install certifications
10. Enter IP address of AS server on **AS IP Address**
11. Enter service port of AS server in **AS Port**
12. Enter interval time between 60 and 2147483647s in **Unicast Key Update Interval**; *86400* is default setting. This entry is optional.
13. Enter interval time between 60 and 2147483647s in **Multicast Key Update Interval**; *86400* is default setting. This entry is optional.
14. Click **Submit**

Configure WLAN with WAPI-PSK Authentication

Figure 38 - 5G WLAN # Security Setting: WAPI-PSK Authentication



Radio1(5G) WLAN0 Setting

WLAN Security Setting

Authentication Mode: WAPI-PSK

Cipher Mode: SMS4

PassPhrase: □ Show
Length:8-63(ASCII Characters); Length:64(HEX Characters)

Unicast Key Update Interval: 86400
(60-2147483647)

Multicast Key Update Interval: 86400
(60-2147483647)

ACL Setting

Access Control List: Enabled - Default Allow

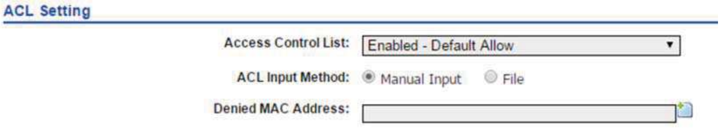
ACL Input Method: ● Manual Input ○ File

Denied MAC Address:

1. Go to **Configuration** > **Wireless** > **Radio1(5G)** > **WLAN** > **WLAN #** > **WLAN Security**
2. Select *WAPI* on **Authentication Mode**
3. Select *SMS4* in **Cipher Mode**
4. Enter in an ASCII string between 8 and 63 characters or a HEX string with 64 characters long in **Pass Phrase** that users will use to connect to the wireless network.
5. Enter interval time between 60 and 2147483647s in **Unicast Key Update Interval**; *86400* is default setting. This entry is optional.
6. Enter interval time between 60 and 2147483647s in **Multicast Key Update Interval**; *86400* is default setting. This entry is optional.
7. Click **Submit**

4.1.2.4 Step 4: Configure ACL Setting

Figure 39 - 5G WLAN #ACL Setting



ACL Setting

Access Control List: Enabled - Default Allow

ACL Input Method: ● Manual Input ○ File

Denied MAC Address:

1. Go to **Configuration** > **Wireless** > **Radio0(2.4G)** > **WLAN** > **WLAN #** > **ACL Setting**
2. Select appropriate option on **Access Control List**; options include

Disable	ACL is disabled

Enabled – Default Allow	ACL is enabled. The MAC addresses which are specified in the ACL will consider as Deny. Every wireless client can associate to the AP unless its MAC address is on the list
Enabled – Default Deny	ACL is enabled. The MAC addresses which are specified in the ACL will consider as Allow. Every wireless client CANNOT associate to the AP unless its MAC address is on the list

3. Select *Manual Input* on **ACL Input Method** if network administrator prefers input the entry one by one manually

Or select File on **ACL Input Method** if network administrator prefers upload a MAC address list (.txt file)

4. Enter MAC address entry one by one or upload the corresponding file to CPE; it is optional
5. Click **Submit**

Note:

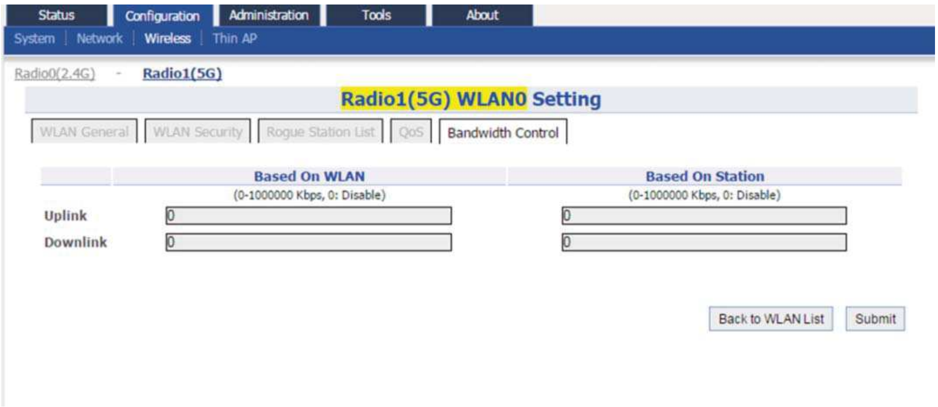
- *Network Administrator shall select Disable or Enabled – Default Allow if no ACL entry will be input on CPE*

4.1.2.5 Step 5: Configure WLAN # QoS

Please refer to Quality of Service (QoS) on page 129

4.1.2.6 Step 6: Configure WLAN # Bandwidth Control

Figure 40 – 5G WLAN # Bandwidth Control



	Based On WLAN (0-1000000 Kbps, 0: Disable)	Based On Station (0-1000000 Kbps, 0: Disable)
Uplink	0	0
Downlink	0	0

1. Go to **Configuration** > **Wireless** > **Radio1(5G)** > **WLAN** > **WLAN #** > **Bandwidth Control**
2. Specify the uplink and downlink limitation under **Based on WLAN** for the particular WLAN

   Or specify the uplink and downlink limitation under **Based on Station** for each associated station. *0* is default value and denotes as disable
3. Click **Submit**

4.1.2.7 Step 7: Apply Submitted Configurations on the CPE Device

1. Click **Save & Apply** from the top on the right.

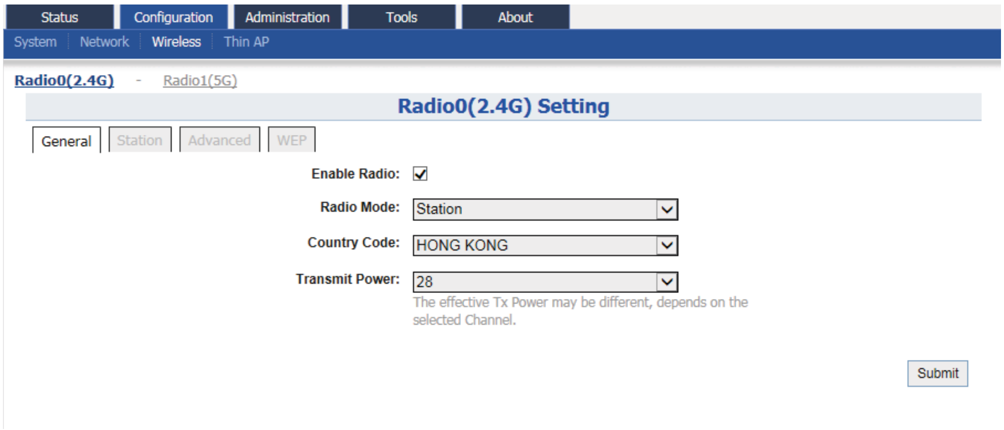
4.2. Station / CPE Mode

Station / CPE acts as a terminal and associated equipment located at a subscriber's premises and connected with a carrier's telecommunication channel at the demarcation point.

4.2.1Radio0 – 2.4G

4.2.1.1 Step 1: Configure General Wireless Setting

Figure 41 – 2.4G General Setting



Radio0(2.4G) Setting

Enable Radio: ☑

Radio Mode: Station

Country Code: HONG KONG

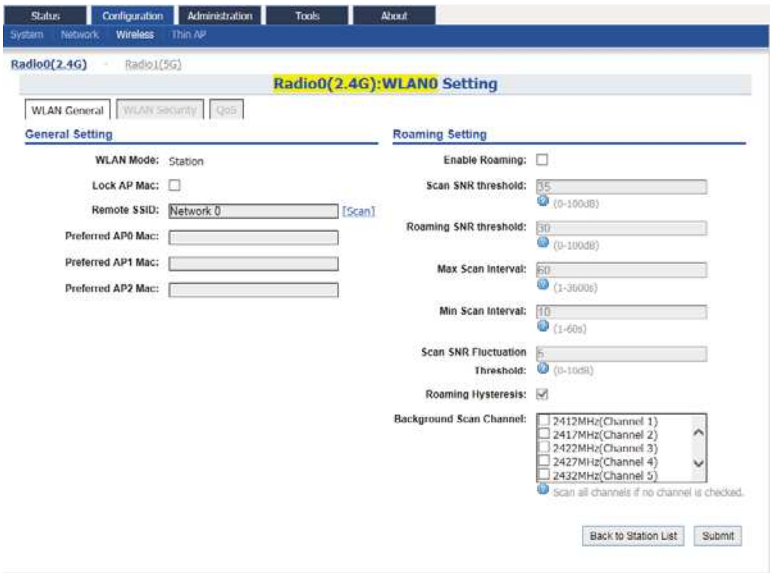
Transmit Power: 28

The effective Tx Power may be different, depends on the selected Channel.

1. Go to **Configuration** > **Wireless** > **Radio0(2.4G)** > **General**
2. Select **Enable Radio** checkbox to enable radio interface
3. Select *Station* in **Radio Mode**
4. Select maximum transmission power on **Transmission Power**
5. Click **Submit**

4.2.1.2 Step 2: Configure WLAN 0 General Setting

Figure 42 – 2.4G WLAN 0 General Setting



Radio0(2.4G):WLAN0 Setting

General Setting

WLAN Mode: Station

Lock AP Mac: □

Remote SSID: Network 0

Preferred AP0 Mac:

Preferred AP1 Mac:

Preferred AP2 Mac:

Roaming Setting

Enable Roaming: □

Scan SNR threshold: 35 (0-100dB)

Roaming SNR threshold: 30 (0-100dB)

Max Scan Interval: 60 (1-3600s)

Min Scan Interval: 10 (1-60s)

Scan SNR Fluctuation Threshold: 5 (0-10dB)

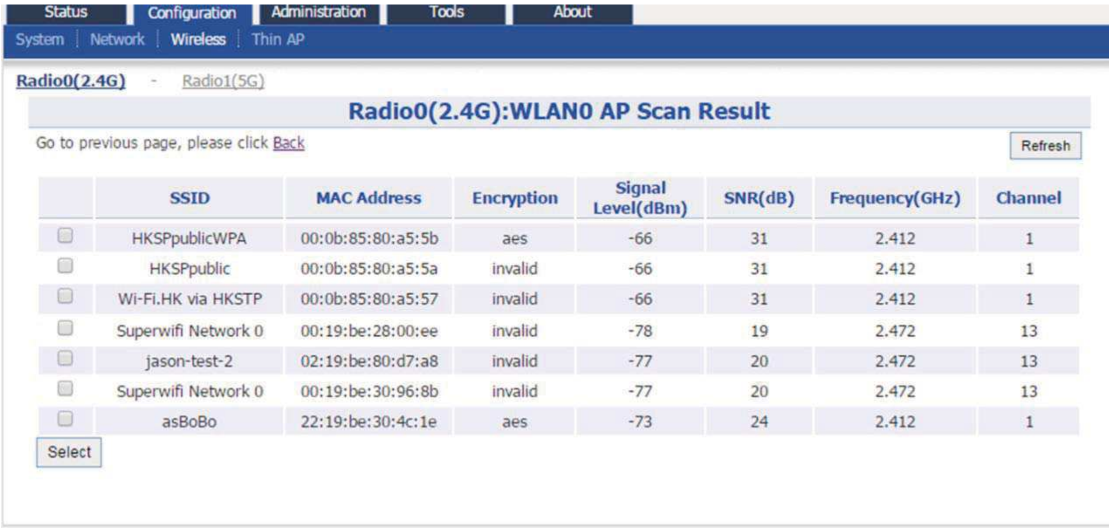
Roaming Hysteresis: ☑

Background Scan Channel:
□ 2412MHz(Channel 1)
□ 2417MHz(Channel 2)
□ 2422MHz(Channel 3)
□ 2427MHz(Channel 4)
□ 2432MHz(Channel 5)

Scan all channels if no channel is checked.

1. Go to **Configuration** > **Wireless** > **Radio0(2.4G)** > **Station** > **WLAN0** > **More…**
2. Select **Lock AP Mac** checkbox to force station that associate the AP with MAC address in **Remote AP MAC** only. This entry is optional.
3. Enter the desired SSID on **Remote SSID** that station is going to associate or click **[Scan]** to look for the surrounding SSID.

Figure 43 – 2.4G WLAN 0 AP scan result



Radio0(2.4G):WLAN0 AP Scan Result

Go to previous page, please click Back

	SSID	MAC Address	Encryption	Signal Level(dBm)	SNR(dB)	Frequency(GHz)	Channel
□	HKSPpublicWPA	00:0b:85:80:a5:5b	aes	-66	31	2.412	1
□	HKSPpublic	00:0b:85:80:a5:5a	invalid	-66	31	2.412	1
□	Wi-Fi.HK via HKSTP	00:0b:85:80:a5:57	invalid	-66	31	2.412	1
□	Superwifi Network 0	00:19:be:28:00:ee	invalid	-78	19	2.472	13
□	jason-test-2	02:19:be:80:d7:a8	invalid	-77	20	2.472	13
□	Superwifi Network 0	00:19:be:30:96:8b	invalid	-77	20	2.472	13
□	asBoBo	22:19:be:30:4c:1e	aes	-73	24	2.412	1

4. Select any one SSID checkbox shown on AP Scan Result, and then click **Select**.

5. Enter up to three preferred AP MAC addresses on **Preferred AP0 / AP1 / AP2 Mac** that station associates them preferentially. **Preferred AP0** is the highest priority. These entries are optional.

6. Select **Enable Roaming** checkbox to enable roaming on station. This entry is optional.

7. Enter SNR value from *0*dB to *100*dB on **Scan SNR Threshold** that station performs channel scanning if the SNR of received signal from serving AP is less than (<) this threshold; *35* is default setting.

8. Enter SNR value from *0*dB to *100*dB on **Roaming SNR Threshold** that station triggers roaming from the serving AP to other AP if the SNR of received signal from serving AP is less than (<) this threshold; *30* is default setting.

Note:

- **Scan SNR Threshold** MUST be higher than (>) **Roaming SNR Threshold**

9. Specify the duration from 1s to 3600s on **Max Scan Interval** for channel scanning; *60*s is default setting. CPE device conducts at least one scanning within this interval.

10. Specify the duration from *1*s to *60*s on **Min Scan Interval** for channel scanning; *10*s is default setting. No more than one scanning will be conducted within this interval. This parameter is to prevent too often channel scanning from affecting the data transmission.

Note:

- **Max Scan Interval** MUST be higher than (>)**Min Scan Interval**

11. Enter SNR value from *0*dB to *10*dB on **Scan SNR Fluctuation Threshold.** CPE device perform channel scan when the fluctuation of received signal level from a serving AP is larger than (>) this value. *5*dB is default setting.

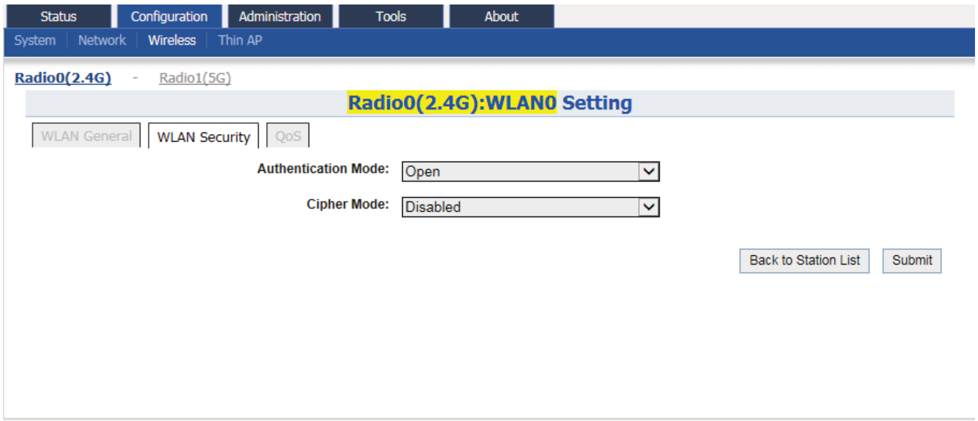
12. Select **Roaming Hysteresis** checkbox to prevent CPE jumping between two APs due to the received signal level fluctuation. It is known as Ping-Pong effect. This entry is optional.

13. Select desired channel(s) on **Background Scan Channel**. CPE scan the selected channel if the channel scan for roaming is triggered. If no any channels are checked in a list, all channels are scanned. This entry is optional.

14. Click **Submit**

4.2.1.3 Step 3: Configure WLAN 0 Security Setting

Figure 44 – WLAN0 Security Setting

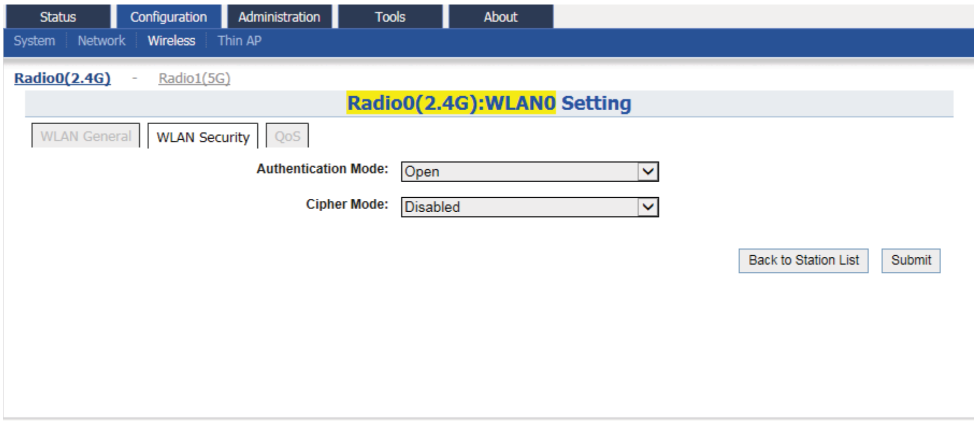


Radio0(2.4G):WLAN0 Setting

Authentication Mode: Open

Cipher Mode: Disabled

Figure 45 – WLAN 0 Security Setting – Associating Open Network



Radio0(2.4G):WLAN0 Setting

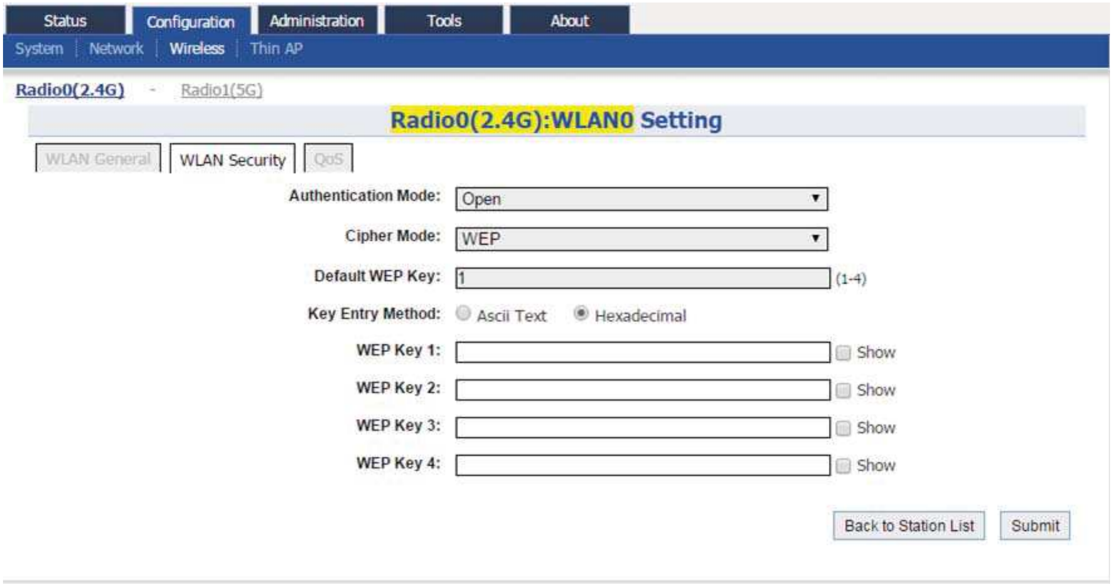
Authentication Mode: Open

Cipher Mode: Disabled

1. Go to **Configuration** > **Wireless** > **Radio0(2.4G)** > **Station** > **WLAN0** > **WLAN Security**
2. Select *Open* in **Authentication Mode**
3. Select *Disabled* in **Cipher Mode**
4. Click **Submit**

Configure to associate Open WLAN with WEP encryption

Figure 46 – 2.4G WLAN 0 Security Setting: Open Network with WEP



Radio0(2.4G):WLAN0 Setting

Authentication Mode: Open

Cipher Mode: WEP

Default WEP Key: 1 (1-4)

Key Entry Method: ○ Ascii Text ● Hexadecimal

WEP Key 1: □ Show

WEP Key 2: □ Show

WEP Key 3: □ Show

WEP Key 4: □ Show

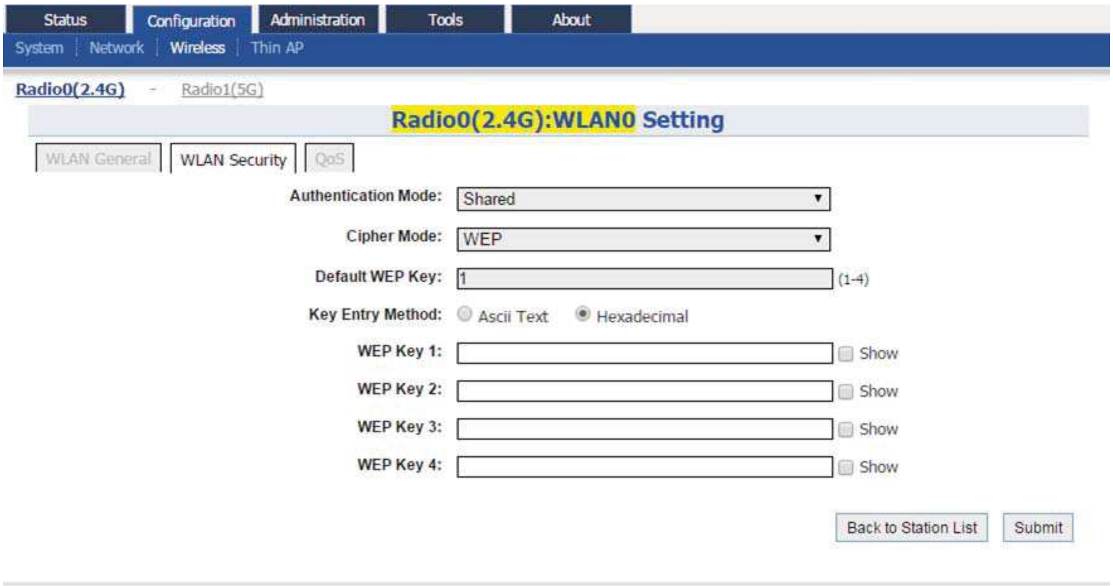
1. Go to **Configuration** > **Wireless** > **Radio0(2.4G)** > **WLAN0** > **WLAN Security**
2. Select Open on **Authentication Mode**
3. Select *WEP* on **Cipher Mode**
4. Select key number *1 – 4* on **Default WEP Key**
5. Select suitable key type in **Key Entry Mode**; the options include:

Ascii Text	key is encoded as ASCII characters (0–9, a–z, A–Z)
Hexadecimal	key is encoded as Hexadecimal characters (0–9, A–F)

6. Enter up to four keys in WEP Key 1, WEP Key 2, WEP Key 3 and WEP Key 4 respectively. You can type either up to 5 Ascii characters or up to 10 Hexadecimal characters as WEP Key.
7. Click **Submit**

Configure to associate WLAN with Shared Key authentication

Figure 47 – WLAN 0 Security Setting – Associating WLAN with Shared Key authentication



Radio0(2.4G):WLAN0 Setting

Authentication Mode: Shared

Cipher Mode: WEP

Default WEP Key: 1 (1-4)

Key Entry Method: ○ Ascii Text ● Hexadecimal

WEP Key 1: □ Show

WEP Key 2: □ Show

WEP Key 3: □ Show

WEP Key 4: □ Show

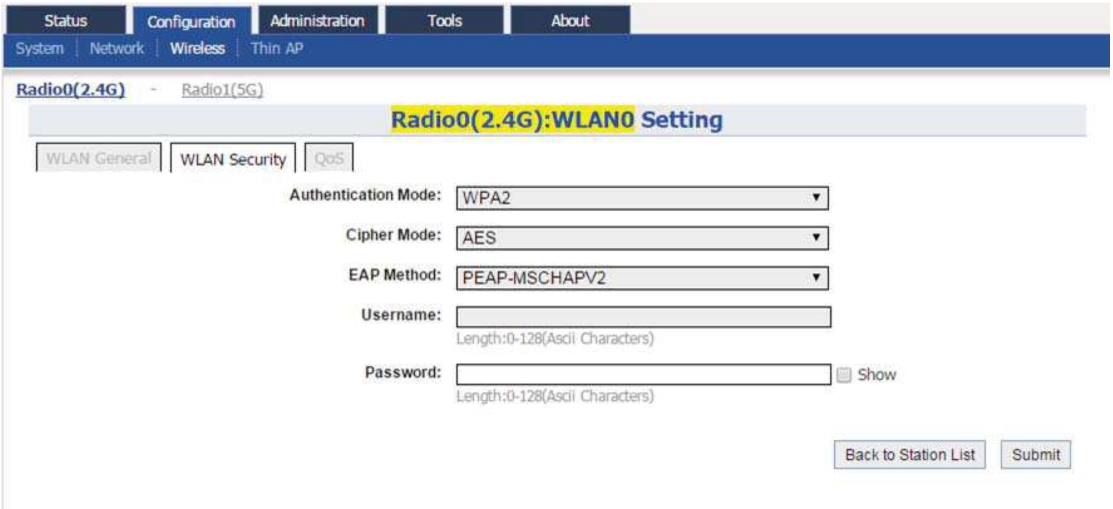
1. Go to **Configuration** > **Wireless** > **Radio0(2.4G)** > **WLAN0** > **WLAN Security**
2. Select Open on **Authentication Mode**
3. Select *WEP* on **Cipher Mode**
4. Select key number *1 – 4* on **Default WEP Key**
5. Select suitable key type in **Key Entry Mode**; the options include:

Ascii Text	key is encoded as ASCII characters (0–9, a–z, A–Z)
Hexadecimal	key is encoded as Hexadecimal characters (0–9, A–F)

6. Enter up to four keys in WEP Key 1, WEP Key 2, WEP Key 3 and WEP Key 4 respectively. You can type either up to 5 Ascii characters or up to 10 Hexadecimal characters as WEP Key.
7. Click **Submit**

Configure to associate WLAN with WPA / WPA2 authentication

Figure 48 - WLAN 0 Security Setting – Associating WLAN with WPA / WPA2 authentication



Radio0(2.4G):WLAN0 Setting

Authentication Mode: WPA2

Cipher Mode: AES

EAP Method: PEAP-MSCHAPV2

Username:
Length:0-128(Ascii Characters)

Password: □ Show
Length:0-128(Ascii Characters)

1. Go to **Configuration** > **Wireless** > **Radio0(2.4G)** > **Station** > **WLAN0** > **WLAN Security**
2. Select *WPA* / *WPA2* in **Authentication Mode**
3. Select suitable encryption mode in **Cipher Mode** as the followings:

If Authentication Mode is *WPA:*

TKIP + AES	This algorithm automatically selects TKIP or AES based on the client's capabilities
TKIP	This algorithm provides greater compatibility with older client devices, but is not supported by the 802.11n standard.
AES	This algorithm provides enhanced security over TKIP, and is the only encryption algorithm supported by the 802.11i standard.

If Authentication Mode is *WPA2*:

AES	This algorithm provides enhanced security over TKIP, and is the only encryption algorithm supported by the 802.11i standard.

If Authentication Mode is *WPA-auto*:

TKIP + AES	This algorithm automatically selects TKIP or AES based on the client's capabilities

4. Select suitable EAP method mode in **EAP Method**; the options include:

PEAP-MSCHAPV2

TTLS-MSCHAPV2

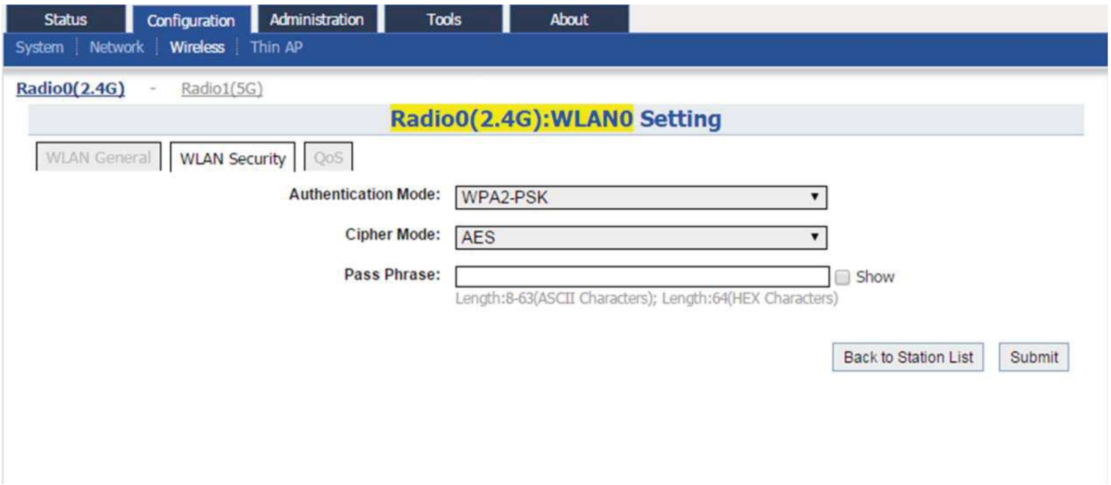
TTPS-PAP

TTLS-CHAP

5. Enter correct username in **Username** for authentication**.**
6. Enter correct password in **Password** for authentication**.**
7. Click **Submit**

Configure to associate network with WPA-PSK / WPA2-PSK authentication

Figure 49 - WLAN 0 Security Setting – Associating WLAN with WPA-PSK / WPA2-PSK authentication



Authentication Mode: WPA2-PSK

Cipher Mode: AES

Pass Phrase:

Length:8-63(ASCII Characters); Length:64(HEX Characters)

1. Go to **Configuration** > **Wireless** > **Radio0(2.4G)** > **Station** > **WLAN0** > **WLAN Security**
2. Select *WPA-PSK* / *WPA2-PSK* in **Authentication Mode**
3. Select suitable encryption mode in **Cipher Mode** as the followings:

If Authentication Mode is *WPA:*

TKIP	This algorithm automatically selects TKIP or AES based on

+ *AES*	the client’s capabilities
TKIP	This algorithm provides greater compatibility with older client devices, but is not supported by the 802.11n standard.
AES	This algorithm provides enhanced security over TKIP, and is the only encryption algorithm supported by the 802.11i standard.

If Authentication Mode is *WPA2*:

AES	This algorithm provides enhanced security over TKIP, and is the only encryption algorithm supported by the 802.11i standard.

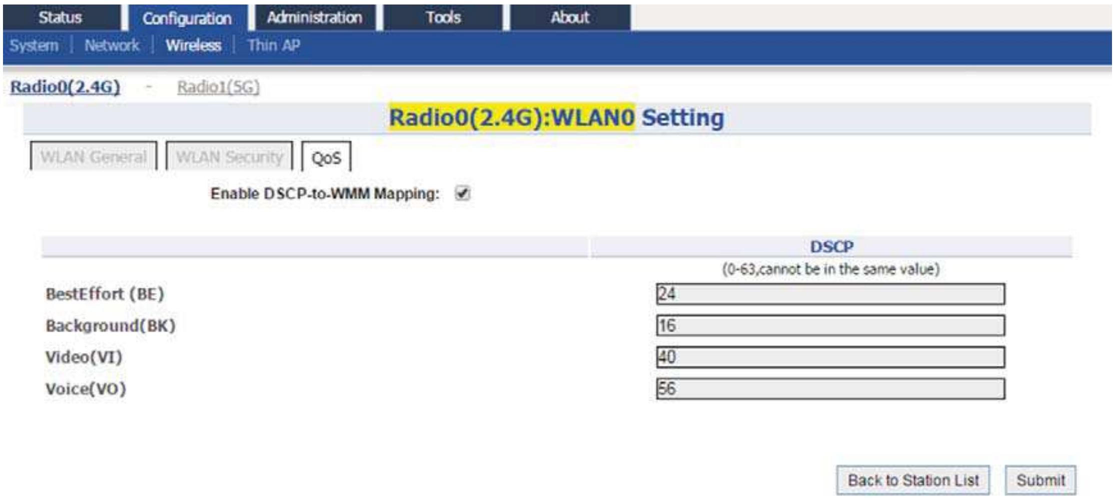
If Authentication Mode is *WPA-auto*:

TKIP + *AES*	This algorithm automatically selects TKIP or AES based on the client’s capabilities

4. Enter an ASCII string between 8 and 63 characters long or a HEX string with 64 characters long on **Pass Phrase** that matches with remote AP
5. Click **Submit**

4.2.1.4 Step 4: Configure WLAN 0 QoS

Figure 50 – 2.4G WLAN 0 QoS



Radio0(2.4G):WLAN0 Setting

Enable DSCP-to-WMM Mapping: ☑

	DSCP (0-63,cannot be in the same value)
BestEffort (BE)	24
Background(BK)	16
Video(VI)	40
Voice(VO)	56

1. Go to **Configuration** > **Wireless** > **Radio0(2.4G)** > **Station** > **WLAN0** > **QoS**
2. Select **Enable DSCP-to-WMM Mapping** checkbox that CPE provides different QoS to the incoming packet with the corresponding DSCP value
3. Enter DSCP value on **Best Effort (BE)**, **Background (BK)**, **Video (VI)**, and **Voice (VO)**; these entry is optional
4. Click **Submit**

Note:

– CPE classify the packet without DSCP marking as Best Effort (BE) traffic

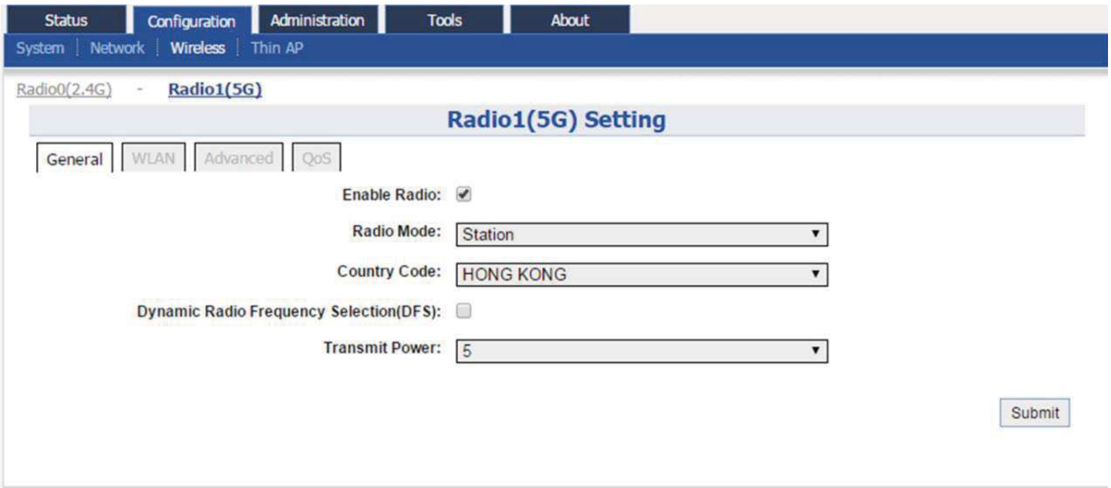
4.2.1.5 Step 5: Apply Submitted Configurations on the CPE Device

1. Click **Save & Apply** from the top on the right.

4.2.2Radio1 – 5G

4.2.2.1 Configure General Wireless Setting

Figure 51 - 5G General Setting



Enable Radio: ☑

Radio Mode: Station

Country Code: HONG KONG

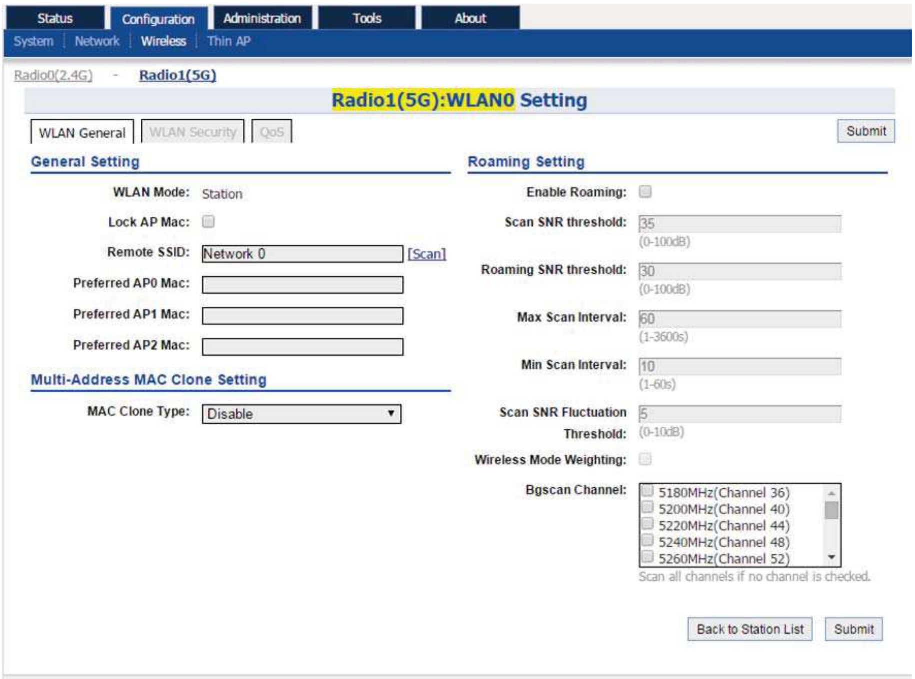
Dynamic Radio Frequency Selection(DFS): □

Transmit Power: 5

1. Go to **Configuration** > **Wireless** > **Radio1(5G)** > **General**
2. Select **Enable Radio** checkbox to enable radio interface
3. Select *Station* in **Radio Mode**
4. Select **Dynamic Radio Frequency Selection (DFS)** checkbox to enable automatic channel selection that selects the least congested channel where radar is not detected during booting up.
5. Select maximum transmission power on **Transmission Power**
6. Click **Submit**

4.2.2.2 Configure WLAN 0 General Setting

Figure 52 - WLAN 0 General Setting



Radio1(5G):WLAN0 Setting

General Setting

WLAN Mode: Station

Lock AP Mac: □

Remote SSID: Network 0 [Scan]

Preferred AP0 Mac:

Preferred AP1 Mac:

Preferred AP2 Mac:

Multi-Address MAC Clone Setting

MAC Clone Type: Disable

Roaming Setting

Enable Roaming: □

Scan SNR threshold: 35 (0-100dB)

Roaming SNR threshold: 30 (0-100dB)

Max Scan Interval: 60 (1-3600s)

Min Scan Interval: 10 (1-60s)

Scan SNR Fluctuation Threshold: 5 (0-10dB)

Wireless Mode Weighting: □

Bgscan Channel:
□ 5180MHz(Channel 36)
□ 5200MHz(Channel 40)
□ 5220MHz(Channel 44)
□ 5240MHz(Channel 48)
□ 5260MHz(Channel 52)

Scan all channels if no channel is checked.

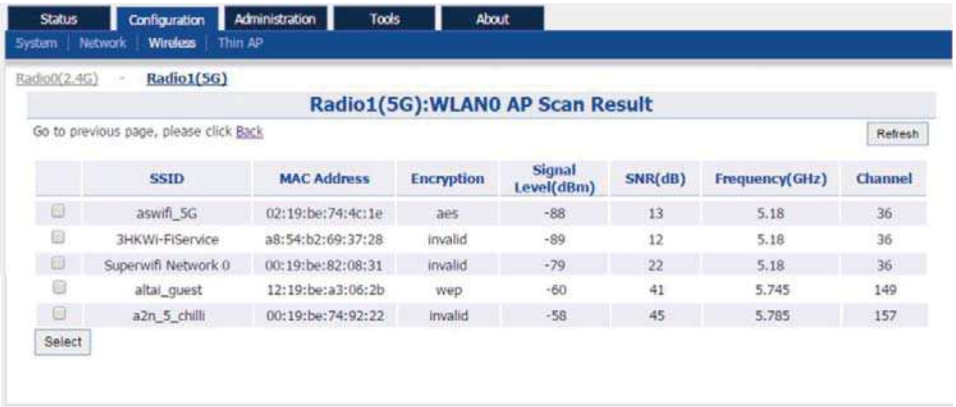
1. Go to **Configuration** > **Wireless** > **Radio1(5G)** > **WLAN0** > **More…**

2. Select **Lock AP Mac** checkbox to force station that associate the AP with MAC address in **Remote AP MAC** only. This entry is optional.

3. Enter the desired SSID on **Remote SSID** that station is going to associate or click **[Scan]** to look for the surrounding SSID.

4. Select any one SSID checkbox shown on AP Scan Result, and then click Select.

Figure 53 - AP scan result


Status
Configuration
Administration
Tools
About
System | Network | Wireless | Thin AP
Radio0(2.4G) - Radio1(5G)
Refresh
Select

Radio1(5G):WLAN0 AP Scan Result

Go to previous page, please click Back

	SSID	MAC Address	Encryption	Signal Level(dBm)	SNR(dB)	Frequency(GHz)	Channel
□	aswifi_5G	02:19:be:74:4c:1e	aes	-88	13	5.18	36
□	3HKWi-FiService	a8:54:b2:69:37:28	invalid	-89	12	5.18	36
□	Superwifi Network 0	00:19:be:82:08:31	invalid	-79	22	5.18	36
□	altai_guest	12:19:be:a3:06:2b	wep	-60	41	5.745	149
□	a2n_5_chilli	00:19:be:74:92:22	invalid	-58	45	5.785	157

5. Enter up to three preferred AP MAC addresses on **Preferred AP0** / **AP1** / **AP2 Mac** that station associates them preferentially. **Preferred AP0** is the highest priority. These entries are optional.

6. Select **Enable Roaming** checkbox to enable roaming on station. This entry is optional.

7. Enter SNR value from *0*dB to *100*dB on **Scan SNR Threshold** that station performs channel scanning if the SNR of received signal from serving AP is less than (<) this threshold; *35* is default setting.

8. Enter SNR value from *0*dB to *100*dB on **Roaming SNR Threshold** that station triggers roaming from the serving AP to other AP if the SNR of received signal from serving AP is less than (<) this threshold; *30* is default setting.

Note:

- **Scan SNR Threshold** MUST be higher than (>) **Roaming SNR Threshold**

9. Specify the duration from 1s to 3600s on **Max Scan Interval** for channel scanning; 60s is default setting. CPE device conducts at least one scanning within this interval.

10. Specify the duration from *1*s to *60*s on **Min Scan Interval** for channel scanning; *10*s is default setting. No more than one scanning will be conducted within this interval. This parameter is to prevent too often channel scanning from affecting the data transmission.

Note:

- **Max Scan Interval** MUST be higher than (>)**Min Scan Interval**

11. Enter SNR value from 0dB to 10dB on **Scan SNR Fluctuation Threshold**. CPE device perform channel scan when the fluctuation of received signal level from a serving AP is larger than (>) this value. 5dB is default setting.

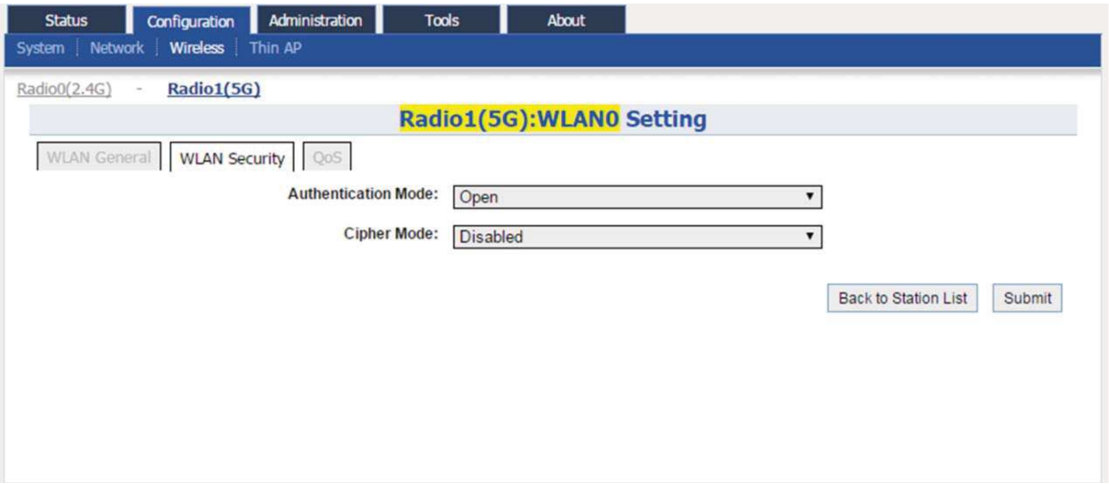
12. Select **Roaming Hysteresis** checkbox to prevent CPE jumping between two APs due to the received signal level fluctuation. It is known as Ping-Pong effect. This entry is optional.

13. Select desired channel(s) on **Background Scan Channel**. CPE scan the selected channel if the channel scan for roaming is triggered. If no any channels are checked in a list, all channels are scanned. This entry is optional.

14. Click **Submit**

4.2.2.3 Configure WLAN 0 Security Setting

Figure 54 - WLAN0 Security Setting

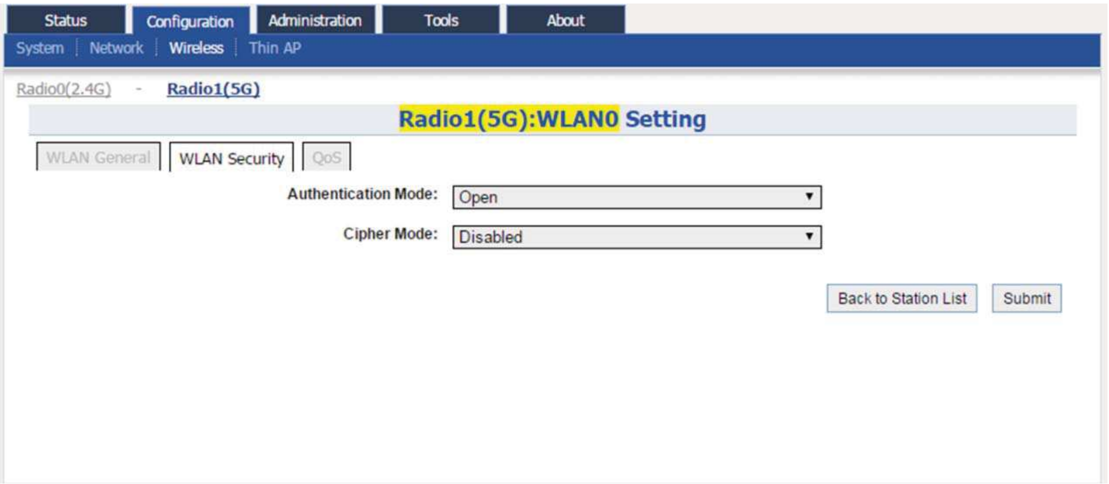


Authentication Mode: Open

Cipher Mode: Disabled

Configure to associate Open WLAN

Figure 55 - WLAN 0 Security Setting – Associating Open Network



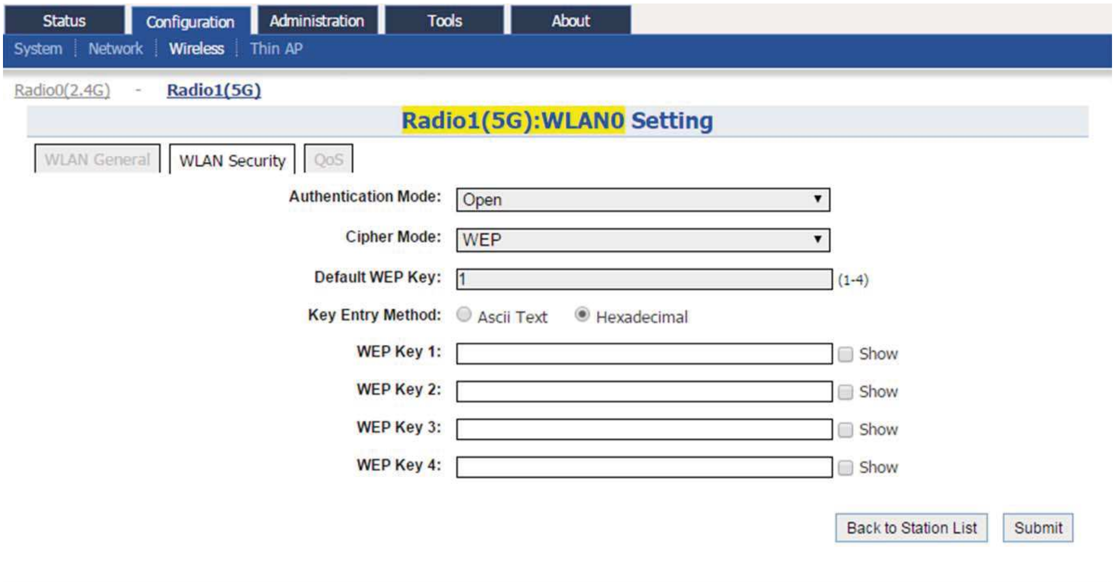
Authentication Mode: Open

Cipher Mode: Disabled

1. Go to **Configuration** > **Wireless** > **Radio1(5G)** > **WLAN0** > **WLAN Security**
2. Select *Open* in **Authentication Mode**
3. Select *Disabled* in **Cipher Mode**
4. Click **Submit**

Configure to associate Open WLAN with WEP encryption

Figure 56 – WLAN0 Security Setting – Associating Open Network with WEP encryption



Authentication Mode: Open

Cipher Mode: WEP

Default WEP Key: 1 (1-4)

Key Entry Method: ○ Ascii Text ● Hexadecimal

WEP Key 1: □ Show

WEP Key 2: □ Show

WEP Key 3: □ Show

WEP Key 4: □ Show

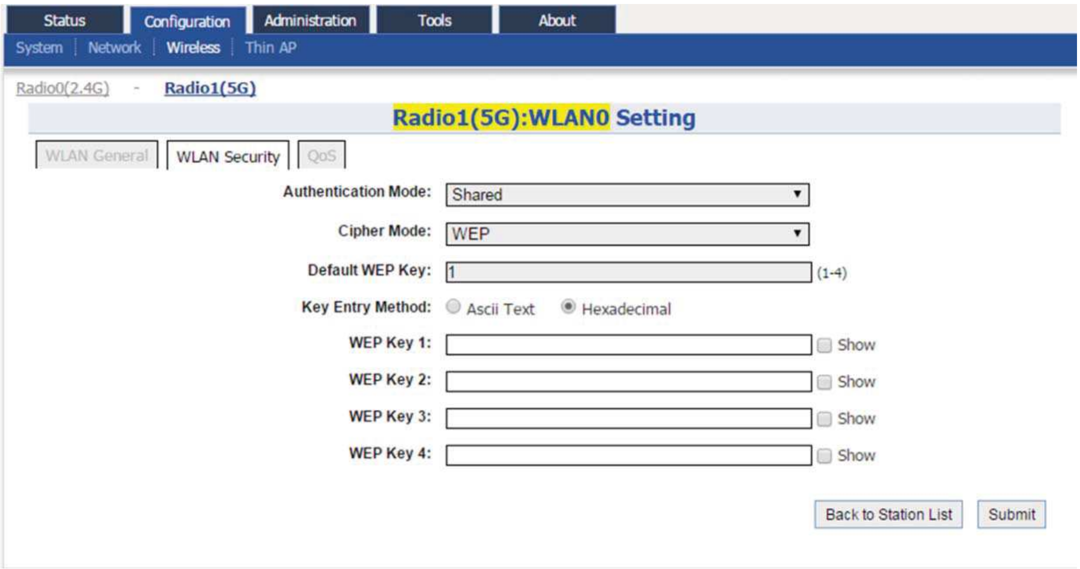
1. Go to **Configuration** > **Wireless** > **Radio1(5G) > WLAN0 > WLAN Security**
2. Select Open on **Authentication Mode**
3. Select *WEP* on **Cipher Mode**
4. Select key number *1 – 4* on **Default WEP Key**
5. Select suitable key type in **Key Entry Mode**; the options include:

Ascii Text	key is encoded as ASCII characters (0–9, a–z, A–Z)
Hexadecimal	key is encoded as Hexadecimal characters (0–9, A–F)

6. Enter up to four keys in WEP Key 1, WEP Key 2, WEP Key 3 and WEP Key 4 respectively. You can type either up to 5 Ascii characters or up to 10 Hexadecimal characters as WEP Key.
7. Click **Submit**

Configure to associate WLAN with Shared Key authentication

Figure 57 - WLAN 0 Security Setting – Associating WLAN with Shared Key authentication



Authentication Mode: Shared

Cipher Mode: WEP

Default WEP Key: 1 (1-4)

Key Entry Method: ○ Ascii Text ● Hexadecimal

WEP Key 1: □ Show

WEP Key 2: □ Show

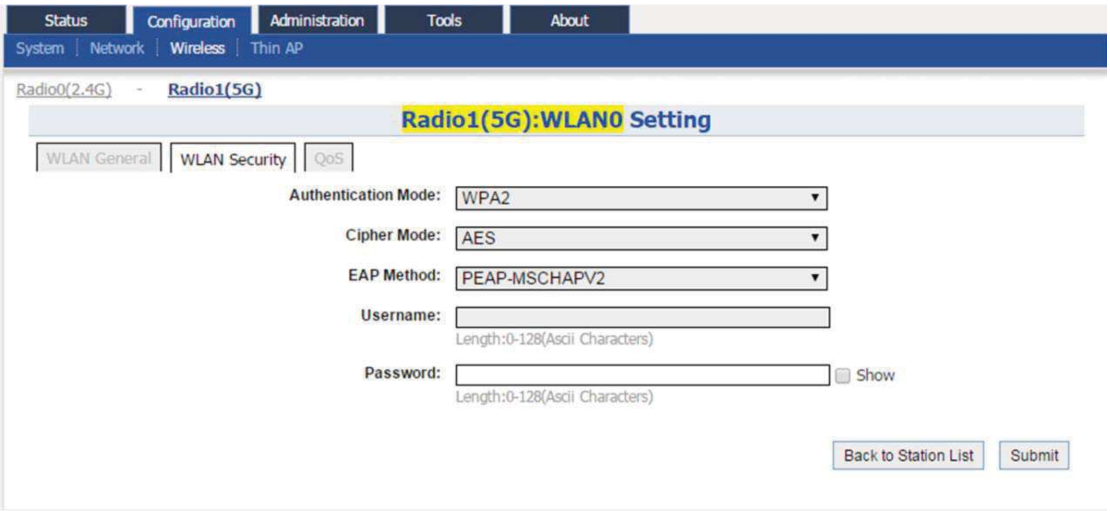
WEP Key 3: □ Show

WEP Key 4: □ Show

1. Go to **Configuration** > **Wireless** > **Radio1(5G)** > **WLAN0** > **WLAN Security**
2. Select *Shared* in **Authentication Mode**
3. Select *WEP* in **Cipher Mode**
4. Select key number *1 – 4* in **Default WEP Key**
5. Click **Submit**

Configure to associate WLAN with WPA / WPA2 authentication

Figure 58 - WLAN 0 Security Setting – Associating WLAN with WPA / WPA2 authentication



Authentication Mode: WPA2

Cipher Mode: AES

EAP Method: PEAP-MSCHAPV2

Username:
Length:0-128(Ascii Characters)

Password: □ Show
Length:0-128(Ascii Characters)

1. Go to **Configuration** > **Wireless** > **Radio1(5G)** > **WLAN0** > **WLAN Security**
2. Select *WPA* / *WPA2* in **Authentication Mode**
3. Select suitable encryption mode in **Cipher Mode** as the followings:
4. If Authentication Mode is *WPA:*

TKIP + AES	This algorithm automatically selects TKIP or AES based on the client's capabilities
TKIP	This algorithm provides greater compatibility with older client devices, but is not supported by the 802.11n standard.
AES	This algorithm provides enhanced security over TKIP, and is the only encryption algorithm supported by the 802.11i standard.

If Authentication Mode is *WPA2*:

AES	This algorithm provides enhanced security over TKIP, and is the only encryption algorithm supported by the 802.11i standard.

If Authentication Mode is *WPA-auto*:

TKIP + AES	This algorithm automatically selects TKIP or AES based on the client's capabilities

5. Select suitable EAP method mode in **EAP Method**; the options include:

PEAP-MSCHAPV2

TTLS-MSCHAPV2

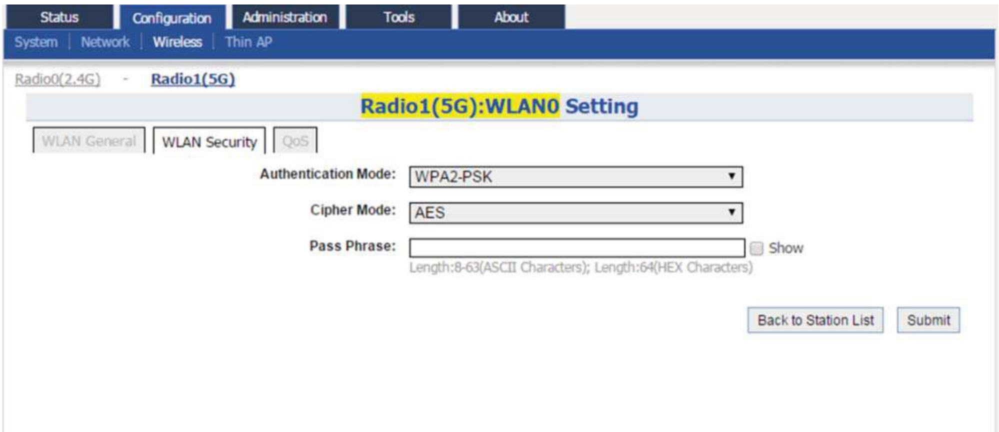
TTPS-PAP

TTLS-CHAP

6. Enter correct username in **Username** for authentication**.**
7. Enter correct password in **Password** for authentication**.**
8. Click **Submit**

Configure to associate WLAN with WPA-PSK / WPA2-PSK authentication

Figure 59 - WLAN 0 Security Setting – Associating WLAN with WPA-PSK / WPA2-PSK authentication



Radio1(5G):WLAN0 Setting

Authentication Mode: WPA2-PSK

Cipher Mode: AES

Pass Phrase: □ Show

Length:8-63(ASCII Characters); Length:64(HEX Characters)

1. Go to **Configuration** > **Wireless** > **Radio1(5G)** > **WLAN0** > **WLAN Security**
2. Select *WPA-PSK* / *WPA2-PSK* in **Authentication Mode**
3. Select suitable encryption mode in **Cipher Mode** as the followings:

If Authentication Mode is *WPA:*

TKIP + AES	This algorithm automatically selects TKIP or AES based on the client's capabilities
TKIP	This algorithm provides greater compatibility with older client devices, but is not supported by the 802.11n standard.
AES	This algorithm provides enhanced security over TKIP, and is the only encryption algorithm supported by the 802.11i standard.

If Authentication Mode is *WPA2*:

AES	This algorithm provides enhanced security over TKIP, and is the only encryption algorithm supported by the 802.11i standard.

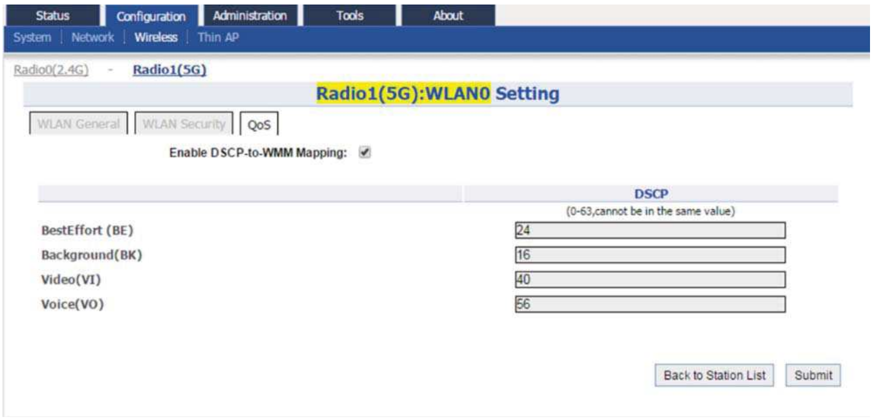
If Authentication Mode is *WPA-auto*:

TKIP + AES	This algorithm automatically selects TKIP or AES based on the client's capabilities

4. Enter an ASCII string between 8 and 63 characters long or a HEX string with 64 characters long on **Pass Phrase** that matches with remote AP
5. Click **Submit**

4.2.2.4 Configure WLAN 0 QoS

Figure 60 – 5G WLAN 0 QoS



Radio1(5G):WLAN0 Setting

Enable DSCP-to-WMM Mapping: ☑

	DSCP (0-63,cannot be in the same value)
BestEffort (BE)	24
Background(BK)	16
Video(VI)	40
Voice(VO)	56

1. Go to **Configuration** > **Wireless** > **Radio1(5G)** > **WLAN0** > **QoS**
2. Select **Enable DSCP-to-WMM Mapping** checkbox that CPE provides different QoS to the incoming packet with the corresponding DSCP value
3. Enter DSCP value on **Best Effort (BE)**, **Background (BK)**, **Video (VI)**, and **Voice (VO)**; these entry is optional
4. Click **Submit**

Note:

– CPE classify the packet without DSCP marking as Best Effort (BE) traffic

4.2.2.5 Apply Submitted Configurations on the CPE Device

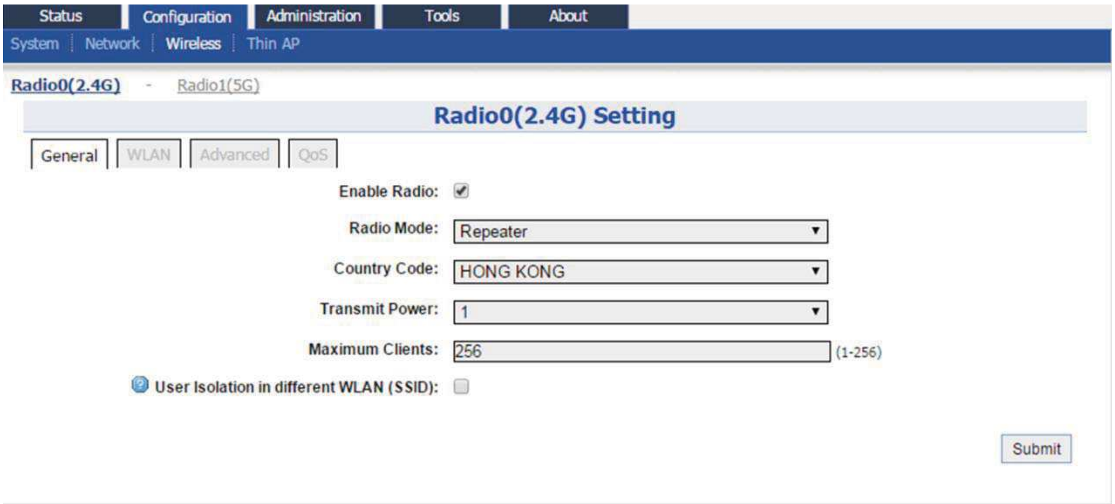
1. Click **Save & Apply** from the top on the right.

4.3. Repeater Mode

4.3.1Radio0 – 2.4G

4.3.1.1 Configure General Wireless Setting

Figure 61 - 2.4G General Setting



Enable Radio: ☑

Radio Mode: Repeater

Country Code: HONG KONG

Transmit Power: 1

Maximum Clients: 256 (1-256)

User Isolation in different WLAN (SSID): □

1. Go to **Configuration** > **Wireless** > **Radio0(2.4G)** > **General**
2. Select **Enable Radio** checkbox to enable radio interface
3. Select *Repeater* in **Radio Mode**
4. Select the correct country code on **Country Code**; this option ensures that the CPE device uses only the radio channels allowed in your country or region
5. Select suitable transmission power on **Transmission Power**;

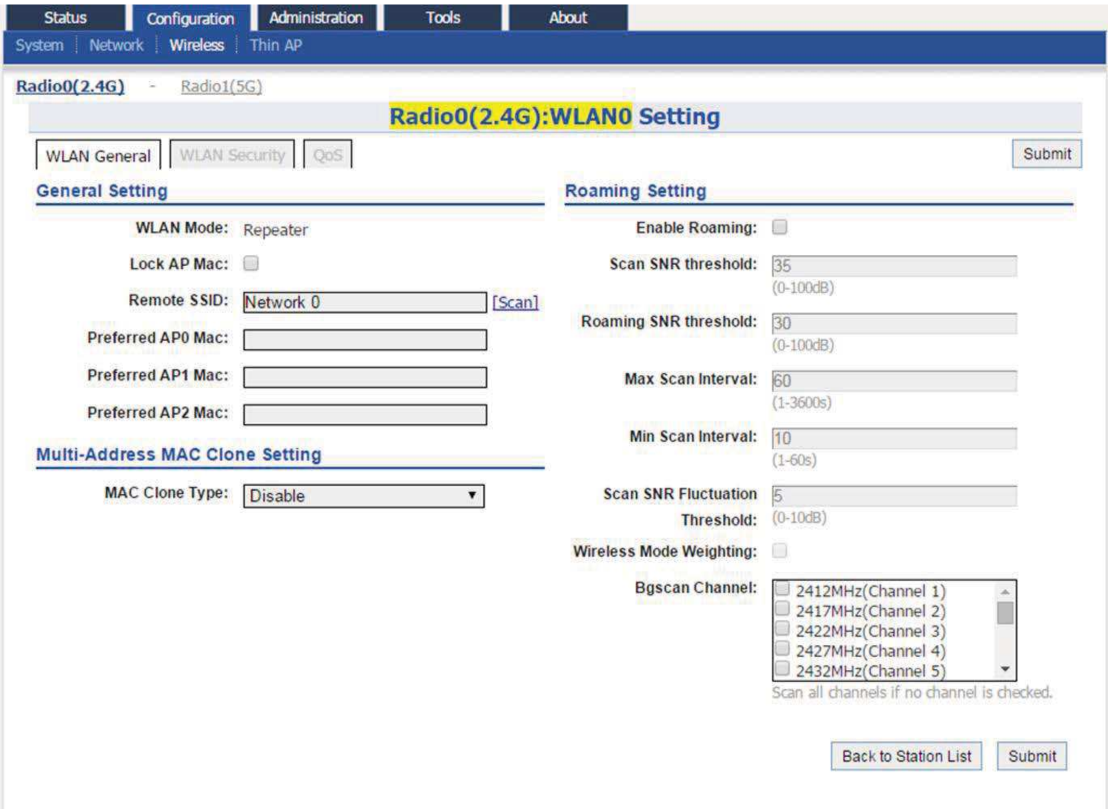
Note:

– *You should follow the regulation from local Communications Authority*

6. Enter the maximum associated client between 1 and 256 on **Maximum Client** that the radio interface serves. *256* is the default setting. This entry is optional.
7. Select **Enable Inter-WLAN User Isolation** checkbox that CPE device block the users' communication across different SSID in the AP directly. This entry is optional.
8. Click **Submit**

4.3.1.2 Configure WLAN 15 General Setting (Station / CPE)

Figure 62 – 2.4G WLAN15 General Setting



Radio0(2.4G):WLAN0 Setting

General Setting

WLAN Mode: Repeater

Lock AP Mac: □

Remote SSID: Network 0 [Scan]

Preferred AP0 Mac:

Preferred AP1 Mac:

Preferred AP2 Mac:

Multi-Address MAC Clone Setting

MAC Clone Type: Disable

Roaming Setting

Enable Roaming: □

Scan SNR threshold: 35 (0-100dB)

Roaming SNR threshold: 30 (0-100dB)

Max Scan Interval: 60 (1-3600s)

Min Scan Interval: 10 (1-60s)

Scan SNR Fluctuation Threshold: 5 (0-10dB)

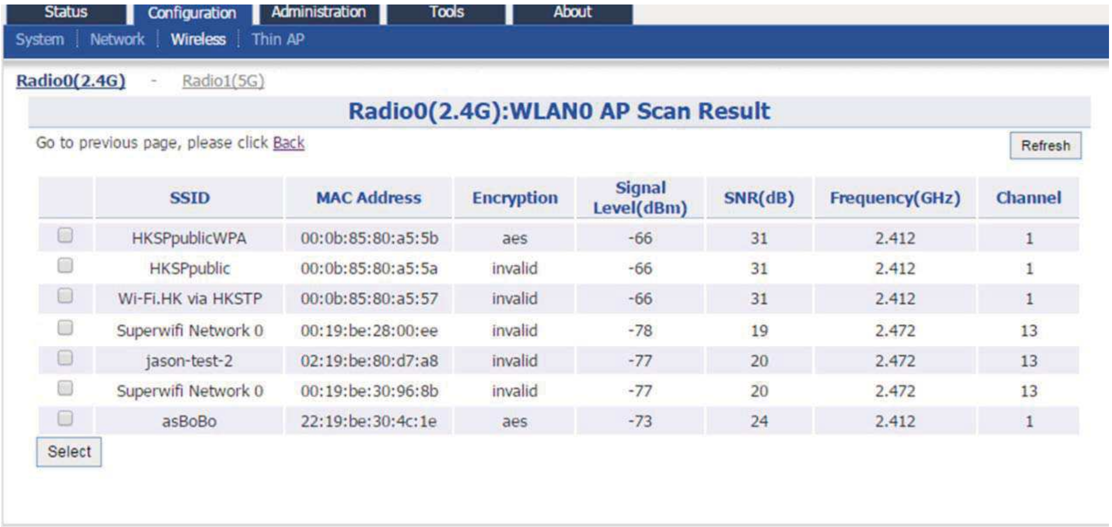
Wireless Mode Weighting: □

Bgscan Channel:
□ 2412MHz(Channel 1)
□ 2417MHz(Channel 2)
□ 2422MHz(Channel 3)
□ 2427MHz(Channel 4)
□ 2432MHz(Channel 5)

Scan all channels if no channel is checked.

1. Go to **Configuration** > **Wireless** > **Radio0 (2.4G)** > **Station Configuration** > **WLAN 15** > More…
2. Select **Lock AP Mac** checkbox to force station that associate the AP with MAC address in **Remote AP MAC** only. This entry is optional.
3. Enter the desired SSID on **Remote SSID** that station is going to associate or click **[Scan]** to look for the surrounding SSID.

Figure 63 - 2.4G WLAN 0 AP scan result



Radio0(2.4G):WLAN0 AP Scan Result

Go to previous page, please click Back

	SSID	MAC Address	Encryption	Signal Level(dBm)	SNR(dB)	Frequency(GHz)	Channel
□	HKSPpublicWPA	00:0b:85:80:a5:5b	aes	-66	31	2.412	1
□	HKSPpublic	00:0b:85:80:a5:5a	invalid	-66	31	2.412	1
□	Wi-Fi.HK via HKSTP	00:0b:85:80:a5:57	invalid	-66	31	2.412	1
□	Superwifi Network 0	00:19:be:28:00:ee	invalid	-78	19	2.472	13
□	jason-test-2	02:19:be:80:d7:a8	invalid	-77	20	2.472	13
□	Superwifi Network 0	00:19:be:30:96:8b	invalid	-77	20	2.472	13
□	asBoBo	22:19:be:30:4c:1e	aes	-73	24	2.412	1

4. Select any one SSID checkbox shown on AP Scan Result, and then click Select.

5. Enter up to three preferred AP MAC addresses on **Preferred AP0 / AP1 / AP2 Mac** that station associates them preferentially. **Preferred AP0** is the highest priority. These entries are optional.

6. Select **Enable Roaming** checkbox to enable roaming on station. This entry is optional.

7. Enter SNR value from *0*dB to *100*dB on **Scan SNR Threshold** that station performs channel scanning if the SNR of received signal from serving AP is less than (<) this threshold; *35* is default setting.

8. Enter SNR value from *0*dB to *100*dB on **Roaming SNR Threshold** that station triggers roaming from the serving AP to other AP if the SNR of received signal from serving AP is less than (<) this threshold; *30* is default setting.

Note:

- **Scan SNR Threshold** MUST be higher than (>) **Roaming SNR Threshold**

9. Specify the duration from 1s to 3600s on **Max Scan Interval** for channel scanning; 60s is default setting. CPE device conducts at least one scanning within this interval.

10. Specify the duration from *1*s to *60*s on **Min Scan Interval** for channel scanning; *10*s is default setting. No more than one scanning will be conducted within this interval. This parameter is to prevent too often channel scanning from affecting the data transmission.

Note:

- **Max Scan Interval** MUST be higher than (>)**Min Scan Interval**

11. Enter SNR value from *0*dB to *10*dB on **Scan SNR Fluctuation Threshold.** CPE device perform channel scan when the fluctuation of received signal level from a serving AP is larger than (>) this value. *5*dB is default setting.

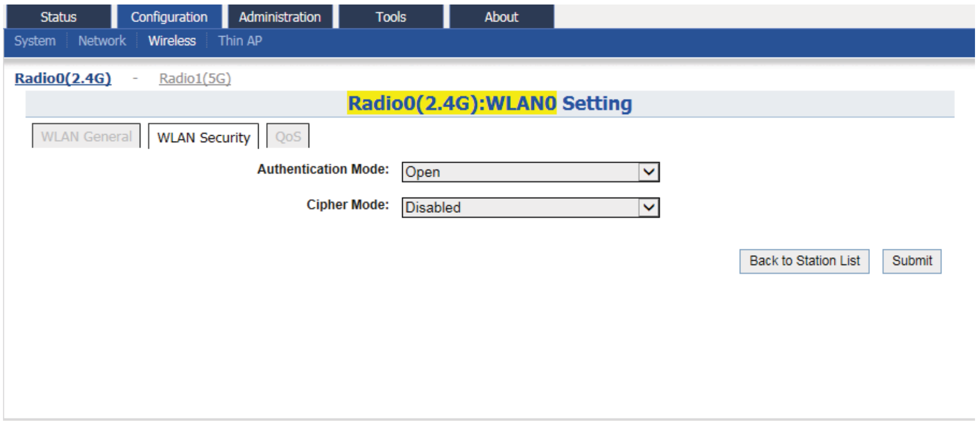
12. Select **Roaming Hysteresis** checkbox to prevent CPE jumping between two APs due to the received signal level fluctuation. It is known as Ping-Pong effect. This entry is optional.

13. Select desired channel(s) on **Background Scan Channel**. CPE scan the selected channel if the channel scan for roaming is triggered. If no any channels are checked in a list, all channels are scanned. This entry is optional.

14. Click **Submit**

4.3.1.3 Configure WLAN15 Security Setting

Figure 64 – WLAN15 Security Setting

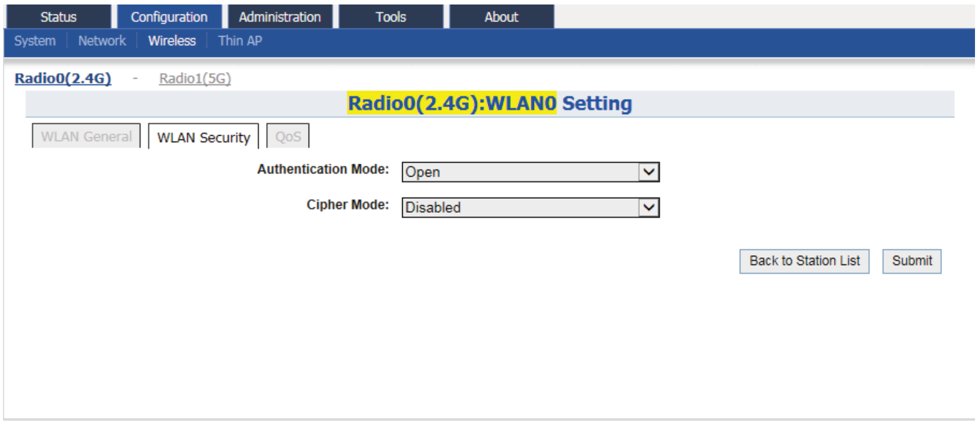


Authentication Mode: Open

Cipher Mode: Disabled

Configure to associate Open WLAN

Figure 65 - WLAN15 Security Setting – Associating Open Network



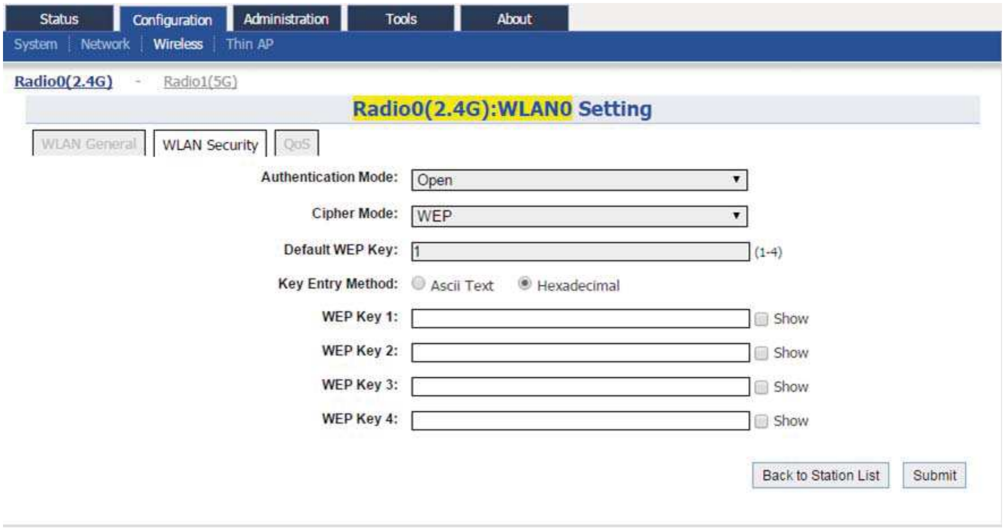
Authentication Mode: Open

Cipher Mode: Disabled

1. Go to **Configuration** > **Wireless** > **Radio0(2.4G)** > **Station Configuration** > **WLAN15** > **WLAN Security**
2. Select *Open* in **Authentication Mode**
3. Select *Disabled* in **Cipher Mode**
4. Click **Submit**

Configure to associate Open WLAN with WEP encryption

Figure 66 - 2.4G WLAN15 Security Setting: Open Network with WEP



Radio0(2.4G):WLAN0 Setting

Authentication Mode: Open

Cipher Mode: WEP

Default WEP Key: 1 (1-4)

Key Entry Method: ○ Ascii Text ● Hexadecimal

WEP Key 1: □ Show

WEP Key 2: □ Show

WEP Key 3: □ Show

WEP Key 4: □ Show

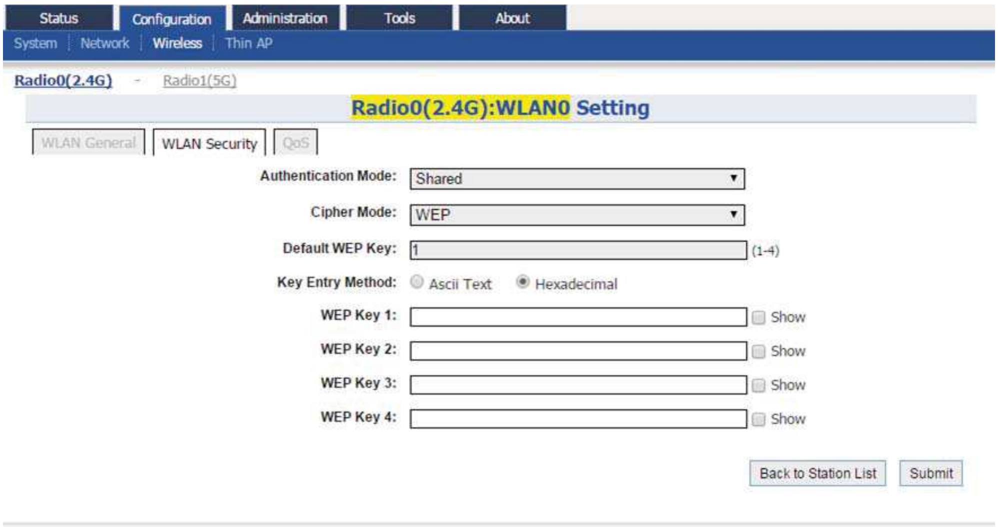
1. Go to **Configuration** > **Wireless** > **Radio0(2.4G)** > **Station Configuration** > **WLAN15** > **WLAN Security**
2. Select Open on **Authentication Mode**
3. Select *WEP* on **Cipher Mode**
4. Select key number *1 – 4* on **Default WEP Key**
5. Select suitable key type in **Key Entry Mode**; the options include:

Ascii Text	key is encoded as ASCII characters (0–9, a–z, A–Z)
Hexadecimal	key is encoded as Hexadecimal characters (0–9, A–F)

6. Enter up to four keys in WEP Key 1, WEP Key 2, WEP Key 3 and WEP Key 4 respectively. You can type either up to 5 Ascii characters or up to 10 Hexadecimal characters as WEP Key.
7. Click **Submit**

Configure to associate WLAN with Shared Key authentication

Figure 67 – WLAN15 Security Setting – Associating WLAN with Shared Key authentication



Radio0(2.4G):WLAN0 Setting

Authentication Mode: Shared

Cipher Mode: WEP

Default WEP Key: 1 (1-4)

Key Entry Method: ○ Ascii Text ● Hexadecimal

WEP Key 1: □ Show

WEP Key 2: □ Show

WEP Key 3: □ Show

WEP Key 4: □ Show

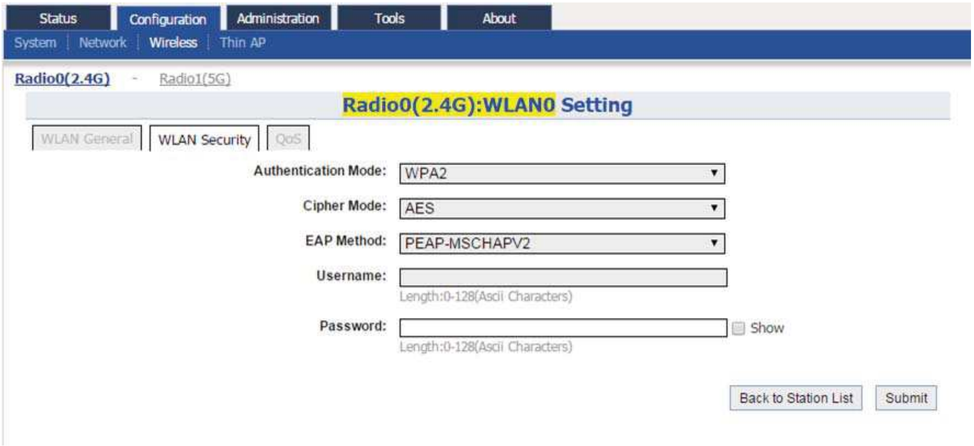
1. Go to **Configuration** > **Wireless** > **Radio0(2.4G)** > **Station Configuration** > **WLAN15** > **WLAN Security**
2. Select *Shared* on **Authentication Mode**
3. Select *WEP* on **Cipher Mode**
4. Select key number *1 – 4* on **Default WEP Key**
5. Select suitable key type in **Key Entry Mode**; the options include:

Ascii Text	key is encoded as ASCII characters (0–9, a–z, A–Z)
Hexadecimal	key is encoded as Hexadecimal characters (0–9, A–F)

6. Enter up to four keys in WEP Key 1, WEP Key 2, WEP Key 3 and WEP Key 4 respectively. You can type either up to 5 Ascii characters or up to 10 Hexadecimal characters as WEP Key.
7. Click **Submit**

Configure to associate WLAN with WPA / WPA2 authentication

Figure 68 – WLAN15 Security Setting – Associating WLAN with WPA / WPA2 authentication



Radio0(2.4G):WLAN0 Setting

Authentication Mode: WPA2

Cipher Mode: AES

EAP Method: PEAP-MSCHAPV2

Username:

Length:0-128(Ascii Characters)

Password:

Length:0-128(Ascii Characters)

1. Go to **Configuration** > **Wireless** > **Radio0(2.4G)** > **Station Configuration** > **WLAN15** > **WLAN Security**
2. Select *WPA* / *WPA2* in **Authentication Mode**
3. Select suitable encryption mode in **Cipher Mode** as the followings:

If Authentication Mode is *WPA:*

TKIP + AES	This algorithm automatically selects TKIP or AES based on the client's capabilities
TKIP	This algorithm provides greater compatibility with older client devices, but is not supported by the 802.11n standard.
AES	This algorithm provides enhanced security over TKIP, and is the only encryption algorithm supported by the 802.11i standard.

If Authentication Mode is *WPA2*:

AES	This algorithm provides enhanced security over TKIP, and is the only encryption algorithm supported by the 802.11i standard.

If Authentication Mode is *WPA-auto*:

TKIP + AES	This algorithm automatically selects TKIP or AES based on the client's capabilities

4. Select suitable EAP method mode in **EAP Method**; the options include:

PEAP-MSCHAPV2

TTLS-MSCHAPV2

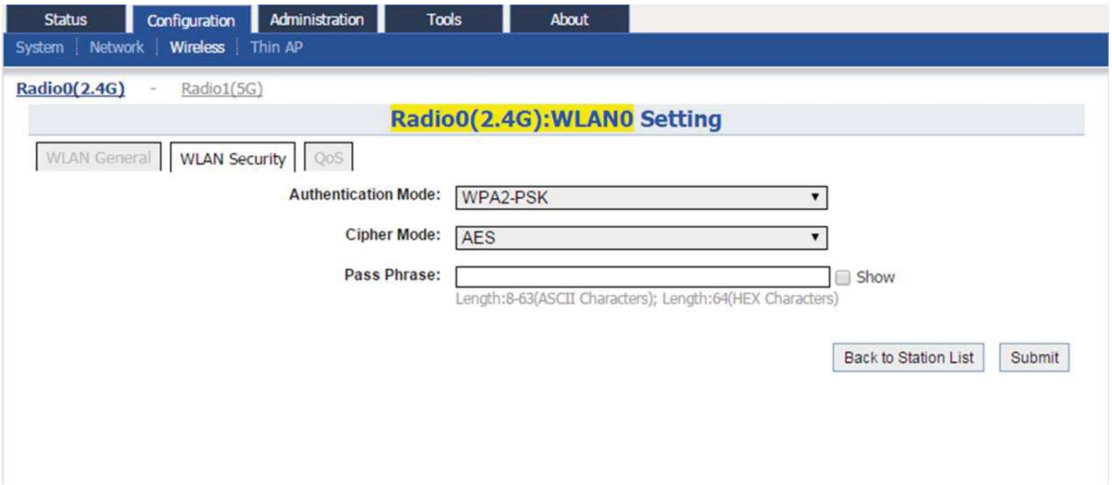
TTPS-PAP

TTLS-CHAP

5. Enter correct username in **Username** for authentication**.**
6. Enter correct password in **Password** for authentication**.**
7. Click **Submit**

Configure to associate network with WPA-PSK / WPA2-PSK authentication

Figure 69 – WLAN15 Security Setting – Associating WLAN with WPA-PSK / WPA2-PSK authentication



Authentication Mode: WPA2-PSK

Cipher Mode: AES

Pass Phrase: □ Show

Length:8-63(ASCII Characters); Length:64(HEX Characters)

1. Go to **Configuration** > **Wireless** > **Radio0(2.4G)** > **Station Configuration** > **WLAN15** > **WLAN Security**
2. Select *WPA-PSK* / *WPA2-PSK* in **Authentication Mode**
3. Select suitable encryption mode in **Cipher Mode** as the followings:

If Authentication Mode is *WPA:*

TKIP + AES	This algorithm automatically selects TKIP or AES based on the client's capabilities
TKIP	This algorithm provides greater compatibility with older client

	devices, but is not supported by the 802.11n standard.
AES	This algorithm provides enhanced security over TKIP, and is the only encryption algorithm supported by the 802.11i standard.

If Authentication Mode is *WPA2*:

AES	This algorithm provides enhanced security over TKIP, and is the only encryption algorithm supported by the 802.11i standard.

If Authentication Mode is *WPA-auto*:

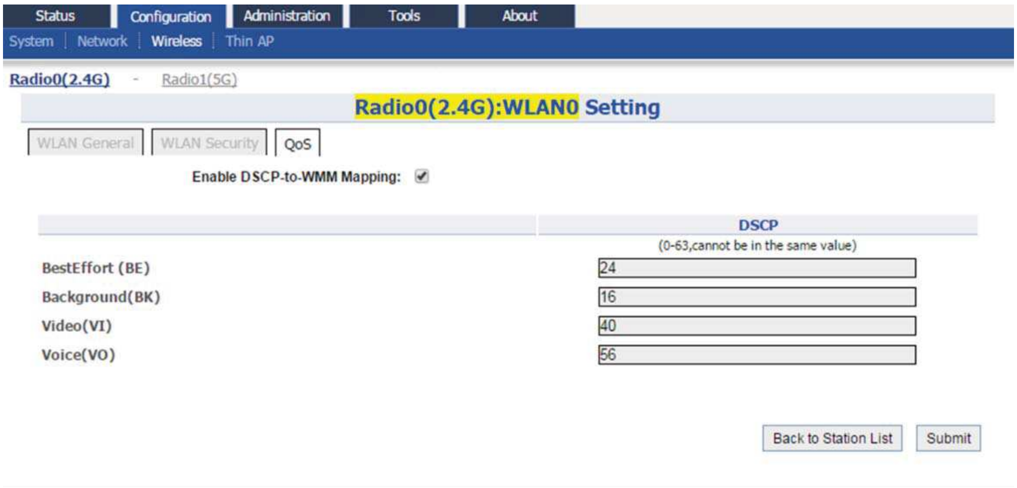
TKIP + *AES*	This algorithm automatically selects TKIP or AES based on the client's capabilities

4. Enter an ASCII string between 8 and 63 characters long or a HEX string with 64 characters long on **Pass Phrase** that matches with remote AP

5. Click **Submit**

4.3.1.4 Configure WLAN15 QoS

Figure 70 – 2.4G WLAN15 QoS



Radio0(2.4G):WLAN0 Setting

Enable DSCP-to-WMM Mapping: ☑

	DSCP (0-63,cannot be in the same value)
BestEffort (BE)	24
Background(BK)	16
Video(VI)	40
Voice(VO)	56

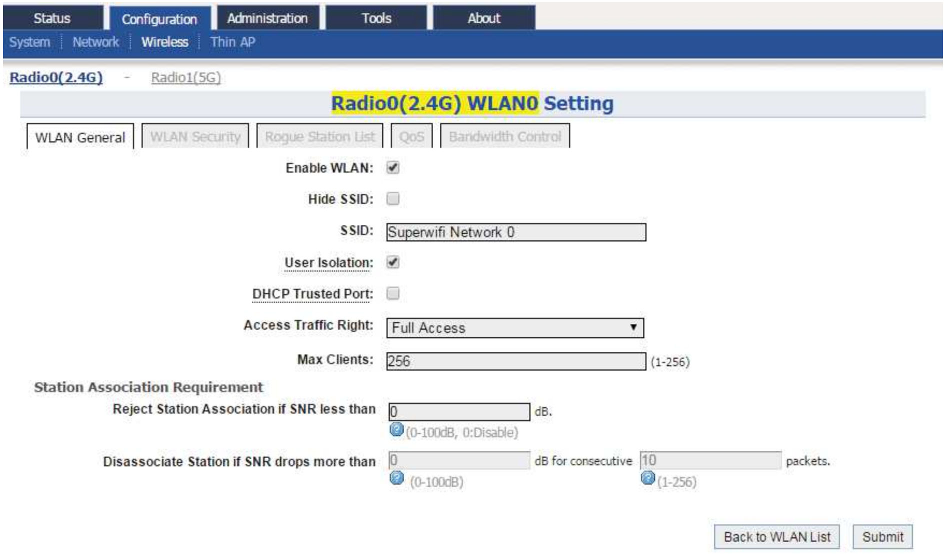
1. Go to **Configuration** > **Wireless** > **Radio0(2.4G)** > **Station** > **WLAN15** > **QoS**
2. Select **Enable DSCP-to-WMM Mapping** checkbox that CPE provides different QoS to the incoming packet with the corresponding DSCP value
3. Enter DSCP value on **Best Effort (BE)**, **Background (BK)**, **Video (VI)**, and **Voice (VO)**; these entry is optional
4. Click **Submit**

Note:

- CPE classify the packet without DSCP marking as Best Effort (BE) traffic

4.3.1.5 Configure WLAN # General Setting

Figure 71 - WLAN # General Setting



Radio0(2.4G) WLAN0 Setting

Enable WLAN: ☑

Hide SSID: □

SSID: Superwifi Network 0

User Isolation: ☑

DHCP Trusted Port: □

Access Traffic Right: Full Access

Max Clients: 256 (1-256)

Station Association Requirement

Reject Station Association if SNR less than 0 dB. (0-100dB, 0:Disable)

Disassociate Station if SNR drops more than 0 dB for consecutive 10 packets. (0-100dB) (1-256)

1. Go to **Configuration** > **Wireless** > **Radio0 (2.4G)** > **WLAN Configuration** > **WLAN #** > More…
2. Select **Enable WLAN** checkbox to enable WLAN
3. Select **Hide SSID** checkbox to hide SSID name from its beacon frame. This entry is optional.
4. Enter a unique name for the particular WLAN on **SSID**.

Note:

- If you want to configure the same SSID on two different WLAN; their security setting MUST be different from each other.

5. Select **User Isolation** checkbox to block user communication within the same SSID in the AP directly. This entry is optional.
6. Deselect the **DHCP Trust Port** checkbox to prevent illegal DHCP servers offering IP address to DHCP clients via this WLAN. This entry is optional.
7. Specify the suitable privilege of associated clients on **Access Traffic Right**; the options include

Full Access - Associated client can access Internet and manage AP

AP Management Only - Associated client can manage AP only, but not able to access the Internet

AP Management Disable - Associated client can access the Internet, but not able to manage AP

8. Specify the maximum associated clients between *1* and *256* on **Max Clients** for this WLAN. *256* is the default setting.

Note:

- **Max Clients** in WLAN 0 – 15 MUST be smaller than or equal to (≥) the **Max Clients** setting on Radio General Setting

9. Specify an additional requirement on Signal Strength to Noise Ratio (SNR) for associated clients under **Station Association Requirement**. This requirement is optional. You may fill up the following fields:

Reject Station Association if SNR less than X dB	*X* denote the minimum SNR level which allow clients to associate; You can select any integer between *0*dB and *100*dB; *0* denotes as disable; *0* is default setting
Disassociate Station if SNR drops more than Y dB for consecutive Z packets	Y denotes the SNR tolerance; Z denotes the number of consecutive packets their SNR are below the difference of X - Y.

Notes:

- Example for Station Association Requirement with the following settings:

Reject Station Association if SNR less than *30* dB (X = 30); Disassociate Station if SNR drops more than *20* dB for consecutive *10* packets (Y = 20; Z = 10)

Consequence:

AP accepts the clients to associate if the SNR of packets from the clients is high than (>) 30dB;

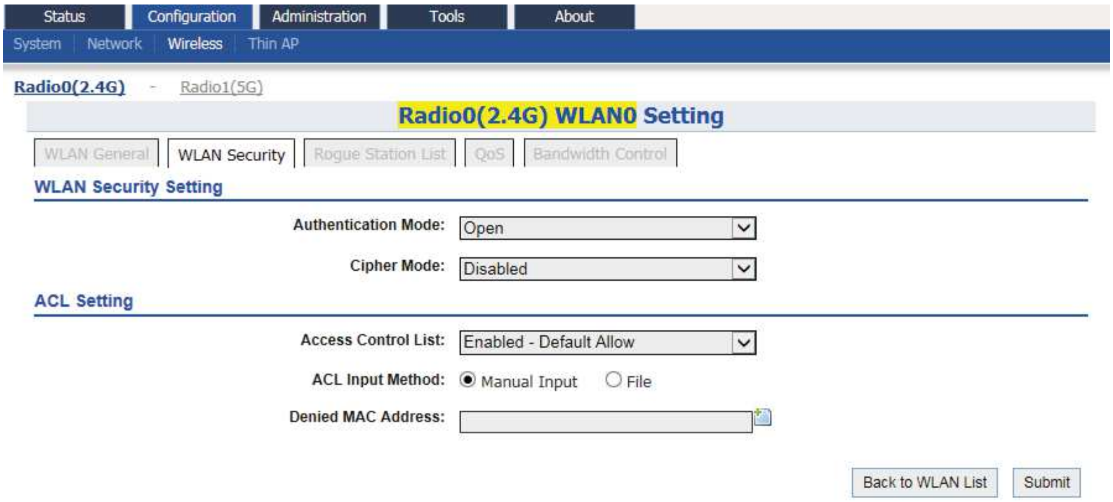
AP kicks out the associated client if the SNR of 10 consecutive packets is below (<) 10 dB (30 dB – 20 dB)

10. Click **Submit**

4.3.1.6 Configure WLAN # Security Setting

Configure WLAN as Open Network

Figure 72 - WLAN # General Setting



WLAN Security Setting

Authentication Mode: Open

Cipher Mode: Disabled

ACL Setting

Access Control List: Enabled - Default Allow

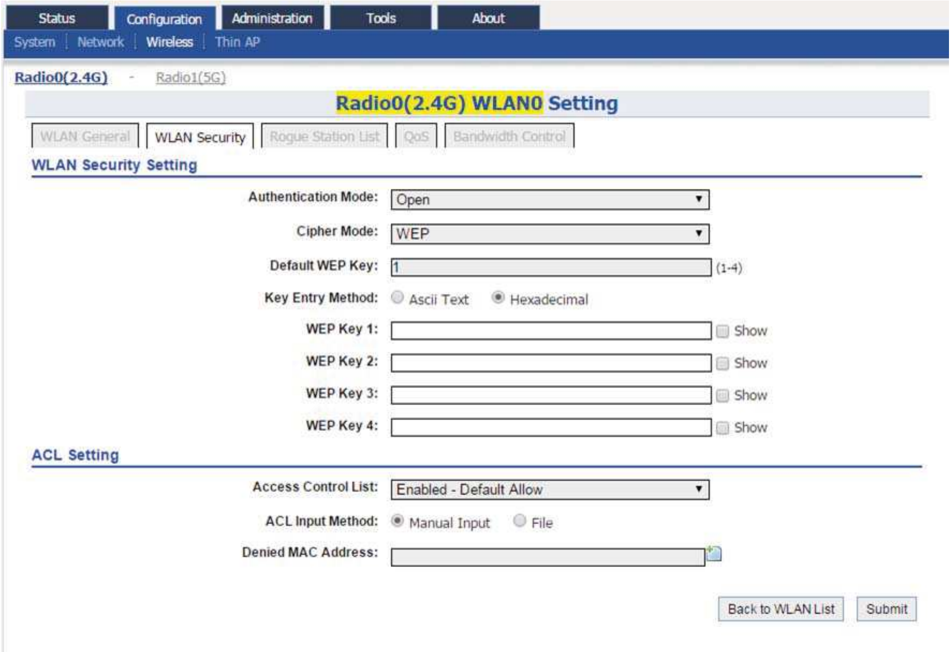
ACL Input Method: ● Manual Input ○ File

Denied MAC Address:

1. Go to **Configuration** > **Wireless** > **Radio0(2.4G)** > **WLAN** > **WLAN #** > **WLAN Security**
2. Select Open on **Authentication Mode**
3. Select *Disabled* on **Cipher Mode**
4. Click **Submit**

Configure WLAN as Open network with WEP encryption

Figure 73 – WLAN # Security Setting: Open Network with WEP



Radio0(2.4G) WLAN0 Setting

WLAN Security Setting

Authentication Mode: Open

Cipher Mode: WEP

Default WEP Key: 1 (1-4)

Key Entry Method: ○ Ascii Text ● Hexadecimal

WEP Key 1: □ Show

WEP Key 2: □ Show

WEP Key 3: □ Show

WEP Key 4: □ Show

ACL Setting

Access Control List: Enabled - Default Allow

ACL Input Method: ● Manual Input ○ File

Denied MAC Address:

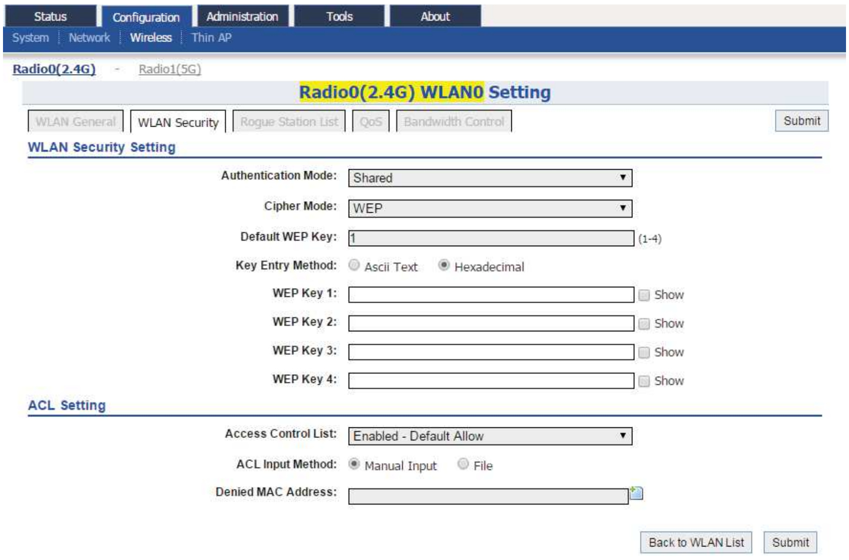
1. Go to **Configuration** > **Wireless** > **Radio0(2.4G)** > **WLAN** > **WLAN #** > **WLAN Security**
2. Select Open on **Authentication Mode**
3. Select *WEP* on **Cipher Mode**
4. Select key number *1 – 4* on **Default WEP Key**
5. Select suitable key type in **Key Entry Mode**; the options include:

Ascii Text	key is encoded as ASCII characters (0–9, a–z, A–Z)
Hexadecimal	key is encoded as Hexadecimal characters (0–9, A–F)

6. Enter up to four keys in WEP Key 1, WEP Key 2, WEP Key 3 and WEP Key 4 respectively. You can type either up to 5 Ascii characters or up to 10 Hexadecimal characters as WEP Key.
7. Click **Submit**

Configure WLAN as Open network with Shared Key Authentication

Figure 74 – WLAN # Security Setting: Shared Key Authentication



Radio0(2.4G) WLAN0 Setting

WLAN Security Setting

Authentication Mode: Shared

Cipher Mode: WEP

Default WEP Key: 1 (1-4)

Key Entry Method: ○ Ascii Text ● Hexadecimal

WEP Key 1: □ Show

WEP Key 2: □ Show

WEP Key 3: □ Show

WEP Key 4: □ Show

ACL Setting

Access Control List: Enabled - Default Allow

ACL Input Method: ● Manual Input ○ File

Denied MAC Address:

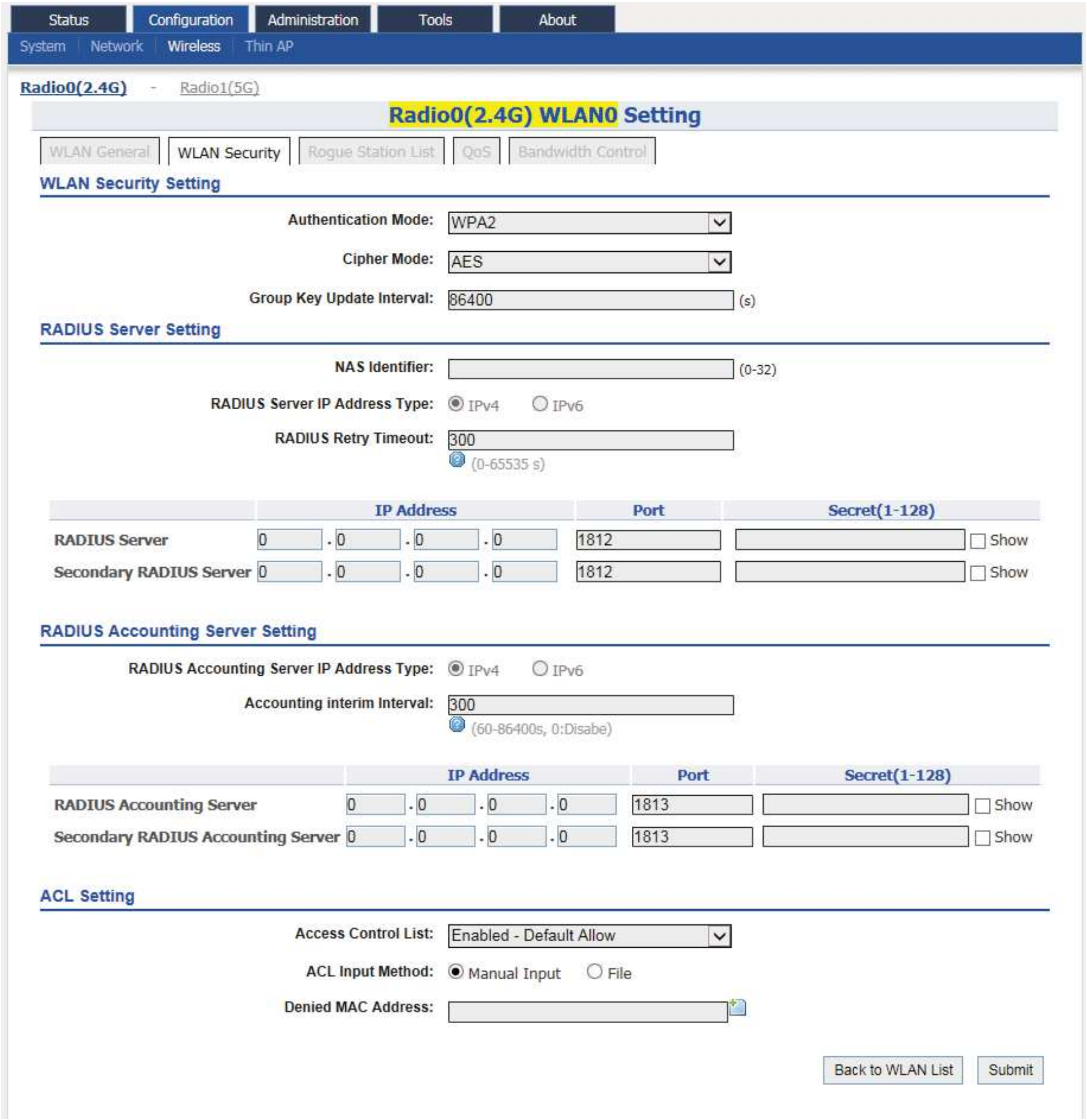
1. Go to **Configuration** > **Wireless** > **Radio0(2.4G)** > **WLAN** > **WLAN #** > **WLAN Security**
2. Select Open on **Authentication Mode**
3. Select *WEP* on **Cipher Mode**
4. Select key number *1 – 4* on **Default WEP Key**
5. Select suitable key type in **Key Entry Mode**; the options include:

Ascii Text	key is encoded as ASCII characters (0–9, a–z, A–Z)
Hexadecimal	key is encoded as Hexadecimal characters (0–9, A–F)

6. Enter up to four keys in WEP Key 1, WEP Key 2, WEP Key 3 and WEP Key 4 respectively. You can type either up to 5 Ascii characters or up to 10 Hexadecimal characters as WEP Key.
7. Click **Submit**

Configure WLAN with WPA / WPA2 / WPA-auto Authentication

Figure 75 - WLAN # Security Setting: WPA / WPA2 / WPA-auto Authentication



Radio0(2.4G) WLAN0 Setting

WLAN Security Setting

Authentication Mode: WPA2

Cipher Mode: AES

Group Key Update Interval: 86400 (s)

RADIUS Server Setting

NAS Identifier: (0-32)

RADIUS Server IP Address Type: ● IPv4 ○ IPv6

RADIUS Retry Timeout: 300 (0-65535 s)

	IP Address	Port	Secret(1-128)
RADIUS Server	0 . 0 . 0 . 0	1812	□ Show
Secondary RADIUS Server	0 . 0 . 0 . 0	1812	□ Show

RADIUS Accounting Server Setting

RADIUS Accounting Server IP Address Type: ● IPv4 ○ IPv6

Accounting interim Interval: 300 (60-86400s, 0:Disabe)

	IP Address	Port	Secret(1-128)
RADIUS Accounting Server	0 . 0 . 0 . 0	1813	□ Show
Secondary RADIUS Accounting Server	0 . 0 . 0 . 0	1813	□ Show

ACL Setting

Access Control List: Enabled - Default Allow

ACL Input Method: ● Manual Input ○ File

Denied MAC Address:

1. Go to **Configuration** > **Wireless** > **Radio0(2.4G)** > **WLAN** > **WLAN #** > **WLAN Security**
2. Select *WPA* / *WPA2* / *WPA-auto* on **Authentication Mode**
3. Select suitable encryption mode on **Cipher Mode**

If Authentication Mode is *WPA:*

TKIP + AES	This algorithm automatically selects TKIP or AES based on the client's capabilities
TKIP	This algorithm provides greater compatibility with older client

	devices, but is not supported by the 802.11n standard.
AES	This algorithm provides enhanced security over TKIP, and is the only encryption algorithm supported by the 802.11i standard.

If Authentication Mode is *WPA2*:

AES	This algorithm provides enhanced security over TKIP, and is the only encryption algorithm supported by the 802.11i standard.

If Authentication Mode is *WPA-auto*:

TKIP + AES	This algorithm automatically selects TKIP or AES based on the client's capabilities

Note:

－ TKIP is not supported by 802.11n standard. If selected TKIP, the 802.11n's devices will be limited to 802.11g transfer rate, i.e. up to 54 Mbps

4. Enter suitable identification on **NAS identifier**. Remote RADIUS server uses this ID to identify its clients. This entry is available for WPA and WPA2 only.
5. Enter transmission timeout interval between *0* and *86400*s on **RADIUS Retry Timeout**. *300* is default setting. This entry is optional.
6. Enter IP address of remote RADIUS server for authentication in **IP Address of RADIUS Server**
7. Enter service port of remote RADIUS server in **Port of RADIUS Server**. *1812* is default setting.
8. Enter suitable secrets in **Secret of RADIUS Server**. It is used along with the MD5 hashing algorithm to obfuscate passwords. This secret MUST be as the same as that in RADIUS server.
9. Repeat step 6-8 if the backup RADIUS server is available. It is optional.
10. Enter interval between each interim update in seconds on **Accounting interim Interval**. *300* is default setting. This entry is optional.
11. Enter IP address of remote RADIUS Accounting Server on **IP Address of RADIUS Accounting Server**. This entry is optional.
12. Enter service port of remote RADIUS server in **Port of RADIUS Accounting Server**. *1813* is default setting. This entry is optional.

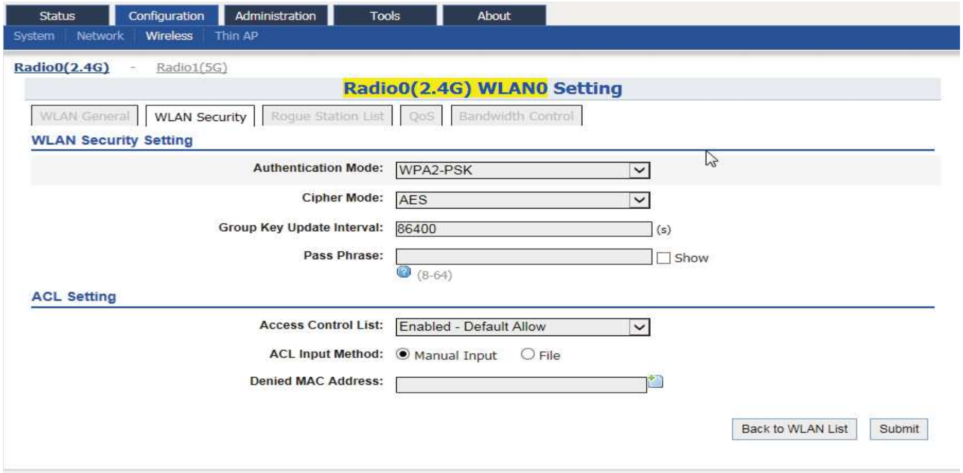
13. Enter suitable secrets in **Secret of RADIUS Accounting Server**. It is used along with the MD5 hashing algorithm to obfuscate passwords. This secret MUST be as the same as that in RADIUS server. This entry is optional.

14. Repeat step 11-13 if the backup RADIUS Accounting server is available. It is optional.

15. Click **Submit**

Configure WLAN with WPA-PSK / WPA2-PSK / WPA-auto-PSK Authentication

Figure 76 - WLAN # Security Setting: WPA-PSK / WPA2-PSK / WPA-auto-PSK Authentication



Radio0(2.4G) WLAN0 Setting

WLAN Security Setting

Authentication Mode: WPA2-PSK

Cipher Mode: AES

Group Key Update Interval: 86400 (s)

Pass Phrase: □ Show (8-64)

ACL Setting

Access Control List: Enabled - Default Allow

ACL Input Method: ● Manual Input ○ File

Denied MAC Address:

1. Go to **Configuration** > **Wireless** > **Radio0(2.4G)** > **WLAN** > **WLAN #** > **WLAN Security**

2. Select *WPA-PSK / WPA2-PSK / WPA-auto-PSK* on **Authentication Mode**

3. Select suitable encryption mode on **Cipher Mode**

If Authentication Mode is *WPA:*

TKIP + AES	This algorithm automatically selects TKIP or AES based on the client's capabilities
TKIP	This algorithm provides greater compatibility with older client devices, but is not supported by the 802.11n standard.
AES	This algorithm provides enhanced security over TKIP, and is the only encryption algorithm supported by the 802.11i standard.

If Authentication Mode is *WPA2*:

AES	This algorithm provides enhanced security over TKIP, and is the only encryption algorithm supported by the 802.11i standard.

If Authentication Mode is *WPA-auto*:

TKIP + AES	This algorithm automatically selects TKIP or AES based on the client's capabilities

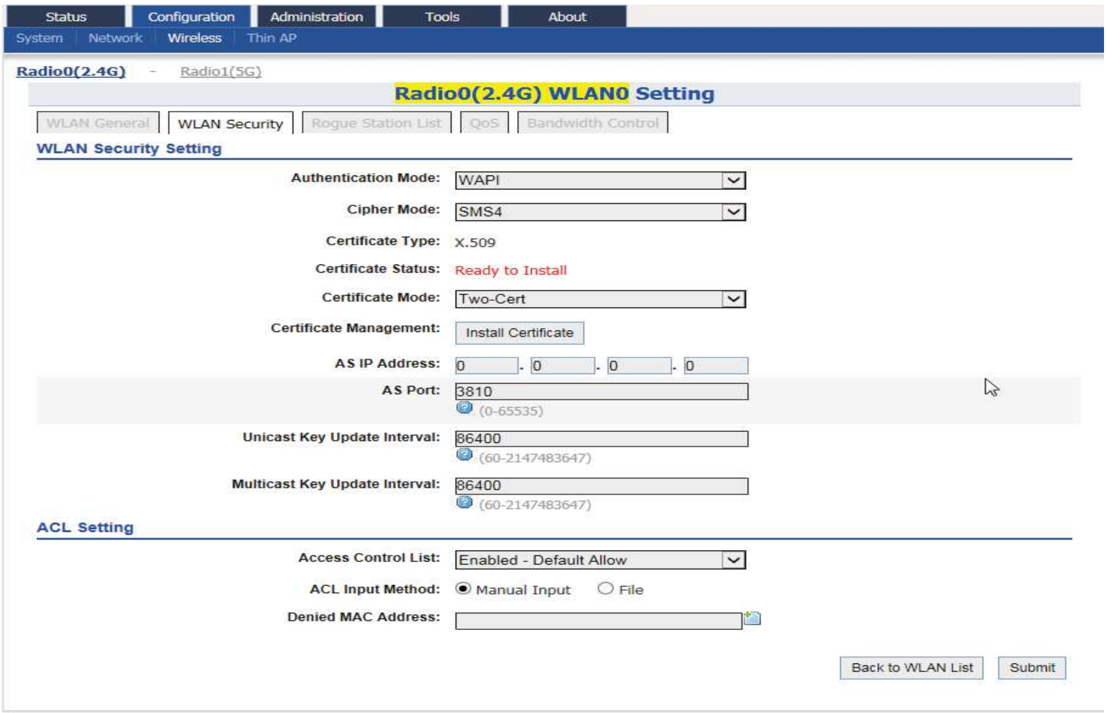
Note:

- TKIP is not supported by 802.11n standard. If selected TKIP, the 802.11n's devices will be limited to 802.11g transfer rate, i.e. up to 54 Mbps

4. Enter interval time in second in **Group Key Update Interval**. *86400* is default setting. This entry is optional.
5. Enter a string between 8 and 64 characters long in **Pass Phrase** that users will use to connect to the wireless network.
6. Click **Submit**

Configure WLAN with WAPI Authentication

Figure 77 - WLAN # Security Setting: WAPI Authentication



Radio0(2.4G) WLAN0 Setting

WLAN Security Setting

Authentication Mode: WAPI

Cipher Mode: SMS4

Certificate Type: X.509

Certificate Status: Ready to Install

Certificate Mode: Two-Cert

Certificate Management: Install Certificate

AS IP Address: 0 . 0 . 0 . 0

AS Port: 3810 (0-65535)

Unicast Key Update Interval: 86400 (60-2147483647)

Multicast Key Update Interval: 86400 (60-2147483647)

ACL Setting

Access Control List: Enabled - Default Allow

ACL Input Method: ● Manual Input ○ File

Denied MAC Address:

1. Go to **Configuration** > **Wireless** > **Radio0(2.4G)** > **WLAN** > **WLAN #** > **WLAN Security**
2. Select *WAPI* on **Authentication Mode**
3. Select *SMS4* in **Cipher Mode**
4. Select suitable option in **Certificate Mode**; the options includes:

Two-Cert	Wi-Fi client is verified by the certification from authentication server (AS) and Access Point (AP)
Three-Cert	Wi-Fi client is verified by the certification from authentication server (AS), access point (AP), and certificate authority (CA)

5. Click **Install Certificate**; a window for installing certificate is shown on Figure 78 and Figure 79.

Figure 78 - Two-Cert Mode Certification Installation

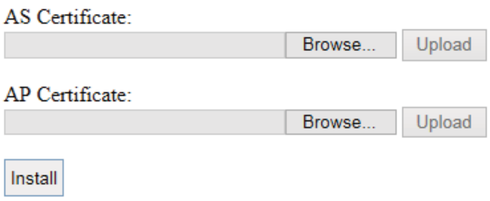
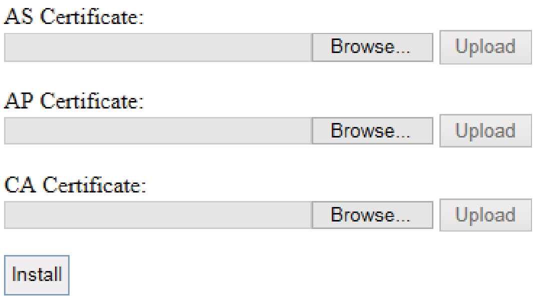


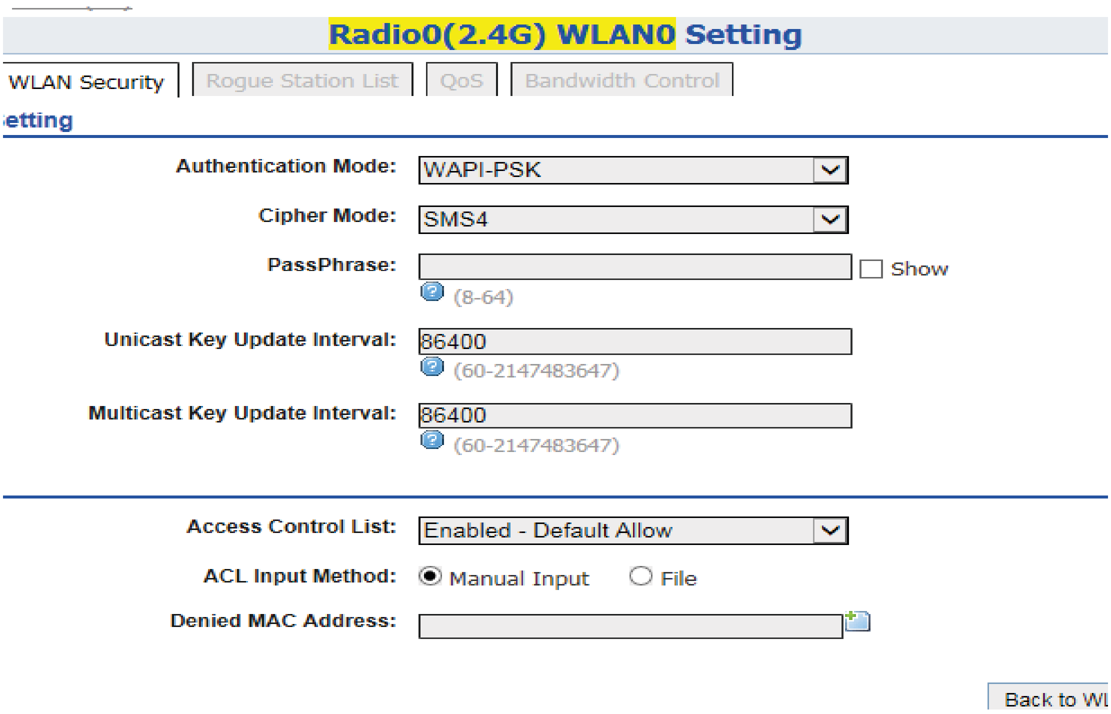
Figure 79 - Three-Cert Mode Certification Installation



6. Click **Browse** to select suitable certifications
7. Click **Upload** to upload the selected certifications to CPE
8. Click **Install** to install certifications
9. Enter IP address of AS server on **AS IP Address**
10. Enter service port of AS server in **AS Port**
11. Enter interval time between 60 and 2147483647s in **Unicast Key Update Interval**; *86400* is default setting. This entry is optional.
12. Enter interval time between 60 and 2147483647s in **Multicast Key Update Interval**; *86400* is default setting. This entry is optional.
13. Click **Submit**

Configure WLAN with WAPI-PSK Authentication

Figure 80 - WLAN # Security Setting: WAPI-PSK Authentication



Authentication Mode: WAPI-PSK

Cipher Mode: SMS4

PassPhrase: □ Show (8-64)

Unicast Key Update Interval: 86400 (60-2147483647)

Multicast Key Update Interval: 86400 (60-2147483647)

Access Control List: Enabled - Default Allow

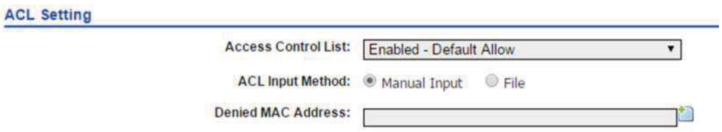
ACL Input Method: ● Manual Input ○ File

Denied MAC Address:

1. Go to **Configuration** > **Wireless** > **Radio0(2.4G)** > **WLAN** > **WLAN #** > **WLAN Security**
2. Select *WAPI* on **Authentication Mode**
3. Select *SMS4* in **Cipher Mode**
4. Enter in a string between 8 and 64 characters long in **Pass Phrase** that users will use to connect to the wireless network.
5. Enter interval time between 60 and 2147483647s in **Unicast Key Update Interval**; *86400* is default setting. This entry is optional.
6. Enter interval time between 60 and 2147483647s in **Multicast Key Update Interval**; *86400* is default setting. This entry is optional.
7. Click **Submit**

4.3.1.7 Configure ACL Setting

Figure 81 – 5G WLAN #ACL Setting



ACL Setting

Access Control List: Enabled - Default Allow

ACL Input Method: ● Manual Input ○ File

Denied MAC Address:

1. Go to **Configuration** > **Wireless** > **Radio0(2.4G)** > **WLAN** > **WLAN #** > **ACL Setting**
2. Select appropriate option on **Access Control List**; options include

Disable	ACL is disabled
Enabled – Default Allow	ACL is enabled. The MAC addresses which are specified in the ACL will consider as Deny. Every wireless client can associate to the AP unless its MAC address is on the list
Enabled – Default Deny	ACL is enabled. The MAC addresses which are specified in the ACL will consider as Allow. Every wireless client CANNOT associate to the AP unless its MAC address is on the list

3. Select *Manual Input* on **ACL Input Method** if network administrator prefers input the entry one by one manually

Or select File on **ACL Input Method** if network administrator prefers upload a MAC address list (.txt file)

4. Enter MAC address entry one by one or upload the corresponding file to CPE; it is optional
5. Click **Submit**

Note:

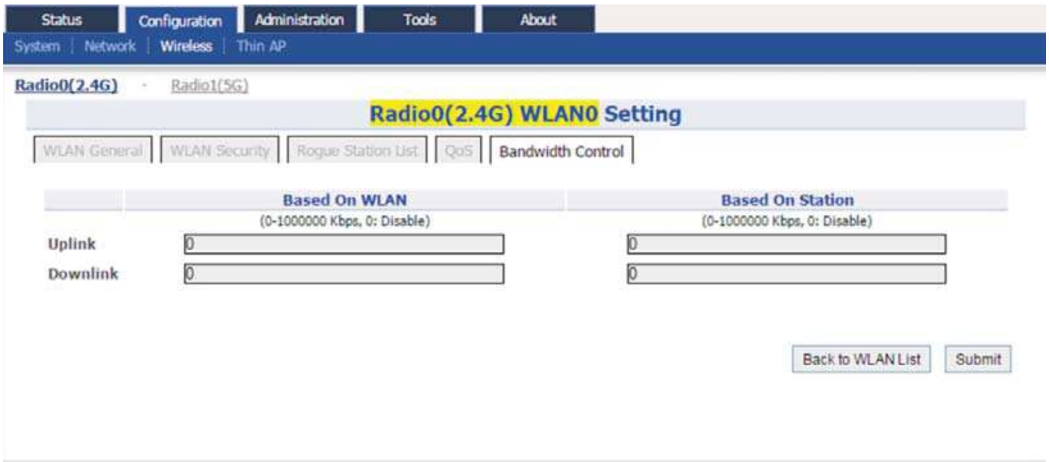
- *Network Administrator shall select Disable or Enabled – Default Allow if no ACL entry will be input on CPE*

4.3.1.8 Configure WLAN # QoS

Please refer to Quality of Service (QoS) on page 129

4.3.1.9 Configure WLAN # Bandwidth Control

Figure 82 – 2.4G WLAN # Bandwidth Control



	Based On WLAN (0-1000000 Kbps, 0: Disable)	Based On Station (0-1000000 Kbps, 0: Disable)
Uplink	0	0
Downlink	0	0

1. Go to **Configuration** > **Wireless** > **Radio0(2.4G)** > **WLAN** > **WLAN #** > **Bandwidth Control**
2. Specify the uplink and downlink limitation under **Based on WLAN** for the particular WLAN

   Or specify the uplink and downlink limitation under **Based on Station** for each associated station. *0* is default value and denotes as disable
3. Click **Submit**

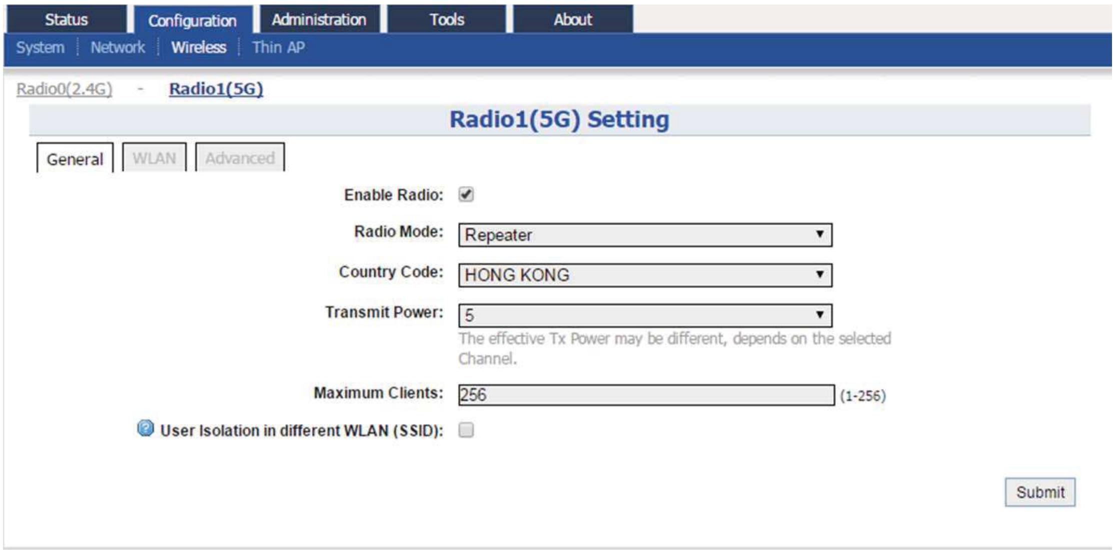
4.3.1.10 Apply Submitted Configurations on the CPE Device

1. Click **Save & Apply** from the top on the right.

4.3.2Radio1 – 5G

4.3.2.1 Configure General Wireless Setting

Figure 83 – 5G General Setting



Radio1(5G) Setting

Enable Radio: ☑

Radio Mode: Repeater

Country Code: HONG KONG

Transmit Power: 5

The effective Tx Power may be different, depends on the selected Channel.

Maximum Clients: 256 (1-256)

User Isolation in different WLAN (SSID): □

1. Go to **Configuration** > **Wireless** > **Radio1(5G)** > **General**
2. Select **Enable Radio** checkbox to enable radio interface
3. Select *Repeater* in **Radio Mode**
4. Select the correct country code on **Country Code**; this option ensures that the CPE device uses only the radio channels allowed in your country or region
5. Select suitable transmission power on **Transmission Power**;

Note:

– You should follow the regulation from local Communications Authority

6. Enter the maximum associated client between 1 and 256 on **Maximum Client** that the radio interface serves. *256* is the default setting. This entry is optional.
7. Select **Enable Inter-WLAN User Isolation** checkbox that CPE device block the users' communication across different SSID in the AP directly. This entry is optional.
8. Click **Submit**

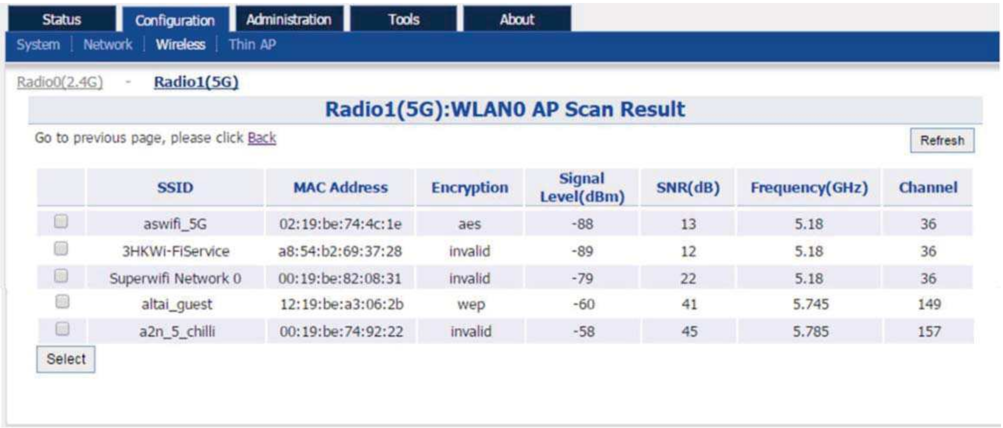
4.3.2.2 Configure WLAN 15 General Setting (Station / CPE)

1. Go to **Configuration** > **Wireless** > **Radio1 (5G)** > **WLAN 15** > More…

2. Select **Lock AP Mac** checkbox to force station that associate the AP with MAC address in **Remote AP MAC** only. This entry is optional.

3. Enter the desired SSID on **Remote SSID** that station is going to associate or click **[Scan]** to look for the surrounding SSID.

Figure 84 – 5G AP scan result



Radio1(5G):WLAN0 AP Scan Result

Go to previous page, please click Back

	SSID	MAC Address	Encryption	Signal Level(dBm)	SNR(dB)	Frequency(GHz)	Channel
□	aswifi_5G	02:19:be:74:4c:1e	aes	-88	13	5.18	36
□	3HKWi-FiService	a8:54:b2:69:37:28	invalid	-89	12	5.18	36
□	Superwifi Network 0	00:19:be:82:08:31	invalid	-79	22	5.18	36
□	altai_guest	12:19:be:a3:06:2b	wep	-60	41	5.745	149
□	a2n_5_chilli	00:19:be:74:92:22	invalid	-58	45	5.785	157

4. Select any one SSID checkbox shown on AP Scan Result, and then click Select.

5. Enter up to three preferred AP MAC addresses on **Preferred AP0 / AP1 / AP2 Mac** that station associates them preferentially. **Preferred AP0** is the highest priority. These entries are optional.

6. Select **Enable Roaming** checkbox to enable roaming on station. This entry is optional.

7. Enter SNR value from *0*dB to *100*dB on **Scan SNR Threshold** that station performs channel scanning if the SNR of received signal from serving AP is less than (<) this threshold; *35* is default setting.

8. Enter SNR value from *0*dB to *100*dB on **Roaming SNR Threshold** that station triggers roaming from the serving AP to other AP if the SNR of received signal from serving AP is less than (<) this threshold; *30* is default setting.

Note:

– **Scan SNR Threshold** MUST be higher than (>) **Roaming SNR Threshold**

9. Specify the duration from 1s to 3600s on **Max Scan Interval** for channel scanning; 60s is default setting. CPE device conducts at least one scanning within this interval.

10. Specify the duration from *1*s to *60*s on **Min Scan Interval** for channel scanning; *10*s is default setting. No more than one scanning will be conducted within this interval. This parameter is to prevent too often channel scanning from affecting the data transmission.

Note:

- **Max Scan Interval** MUST be higher than (>)**Min Scan Interval**

11. Enter SNR value from *0*dB to *10*dB on **Scan SNR Fluctuation Threshold.** CPE device perform channel scan when the fluctuation of received signal level from a serving AP is larger than (>) this value. *5*dB is default setting.

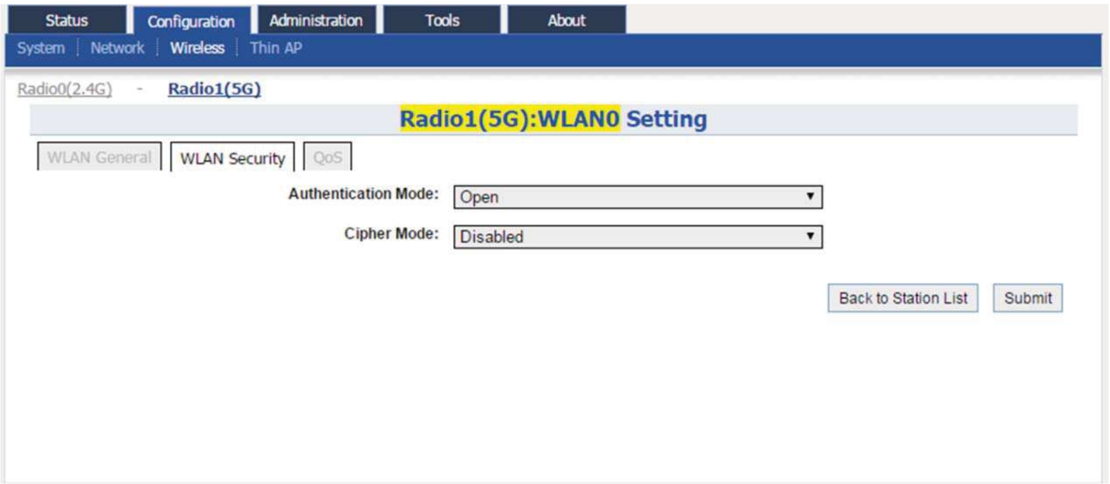
12. Select **Roaming Hysteresis** checkbox to prevent CPE jumping between two APs due to the received signal level fluctuation. It is known as Ping-Pong effect. This entry is optional.

13. Select desired channel(s) on **Background Scan Channel**. CPE scan the selected channel if the channel scan for roaming is triggered. If no any channels are checked in a list, all channels are scanned. This entry is optional.

14. Click **Submit**

4.3.2.3 Configure WLAN15 Security Setting

Figure 85 – WLAN15 Security Setting



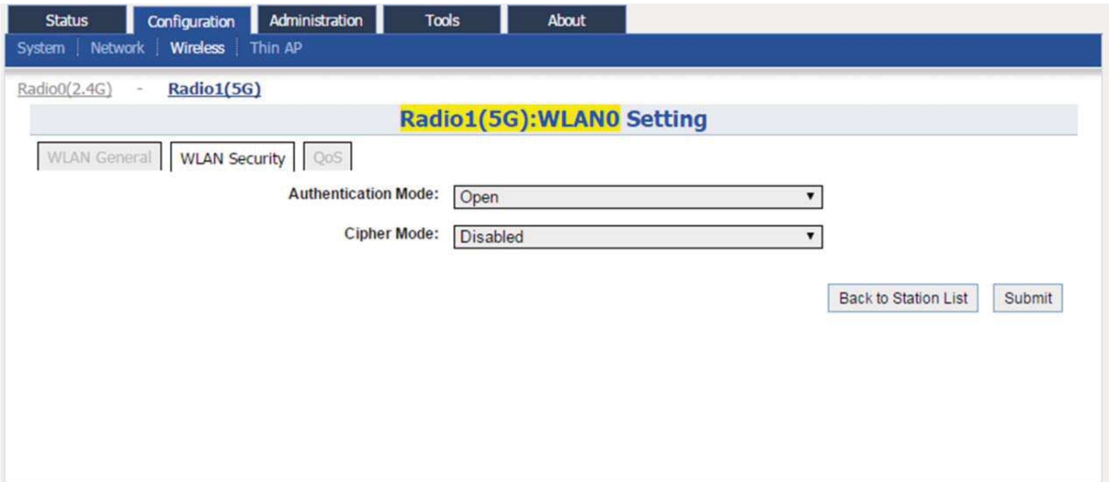
Radio1(5G):WLAN0 Setting

Authentication Mode: Open

Cipher Mode: Disabled

Configure to associate Open WLAN

Figure 86 - WLAN15 Security Setting – Associating Open Network



Radio1(5G):WLAN0 Setting

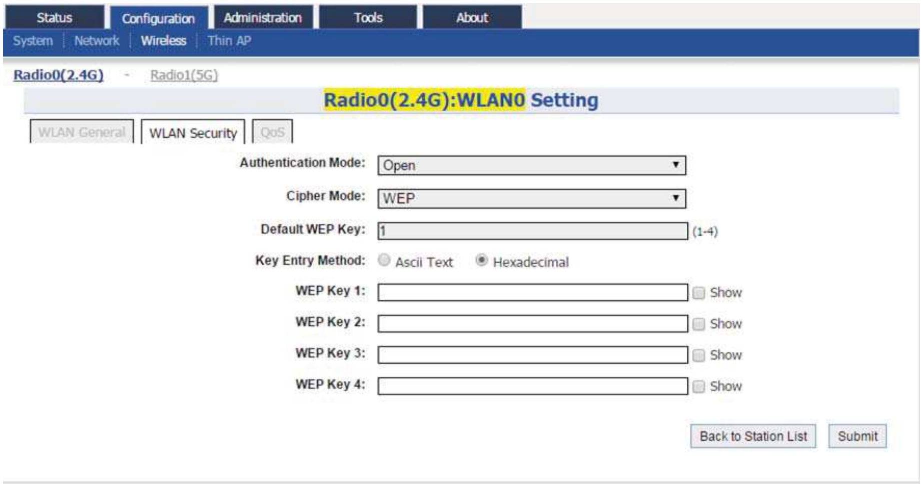
Authentication Mode: Open

Cipher Mode: Disabled

1. Go to **Configuration** > **Wireless** > **Radio1(5G)** > **Repeater** > **WLAN15** > **WLAN Security**
2. Select *Open* in **Authentication Mode**
3. Select *Disabled* in **Cipher Mode**
4. Click **Submit**

Configure to associate Open WLAN with WEP encryption

Figure 87 – WLAN15 Security Setting – Associating Open Network with WEP encryption



Radio0(2.4G):WLAN0 Setting

Authentication Mode: Open

Cipher Mode: WEP

Default WEP Key: 1 (1-4)

Key Entry Method: ○ Ascii Text ● Hexadecimal

WEP Key 1: □ Show

WEP Key 2: □ Show

WEP Key 3: □ Show

WEP Key 4: □ Show

1. Go to **Configuration** > **Wireless** > **Radio1(5G) > WLAN0 > WLAN Security**
2. Select Open on **Authentication Mode**
3. Select *WEP* on **Cipher Mode**
4. Select key number *1 – 4* on **Default WEP Key**
5. Select suitable key type in **Key Entry Mode**; the options include:

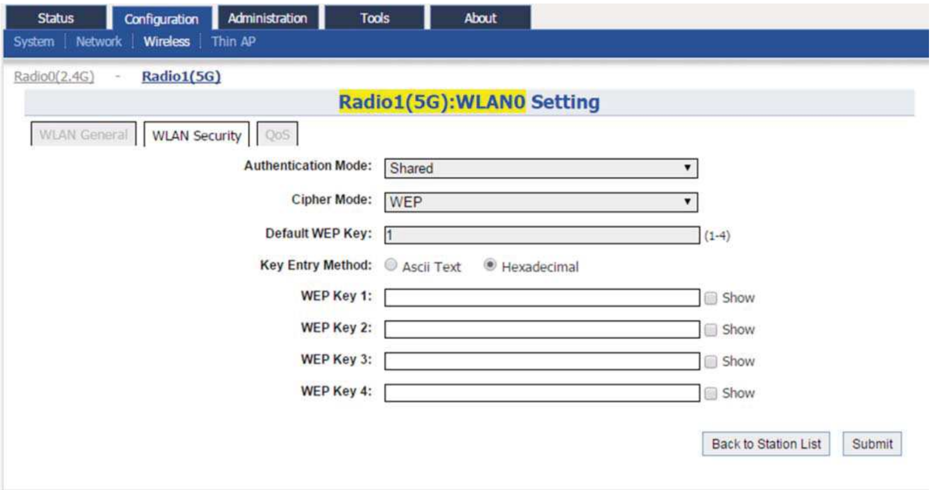
Ascii Text key is encoded as ASCII characters (0–9, a–z, A–Z)

Hexadecimal key is encoded as Hexadecimal characters (0–9, A–F)

6. Enter up to four keys in WEP Key 1, WEP Key 2, WEP Key 3 and WEP Key 4 respectively. You can type either up to 5 Ascii characters or up to 10 Hexadecimal characters as WEP Key.
7. Click **Submit**

Configure to associate WLAN with Shared Key authentication

Figure 88 – WLAN15 Security Setting – Associating WLAN with Shared Key authentication



Radio1(5G):WLAN0 Setting

Authentication Mode: Shared

Cipher Mode: WEP

Default WEP Key: 1 (1-4)

Key Entry Method: ○ Ascii Text ● Hexadecimal

WEP Key 1: □ Show

WEP Key 2: □ Show

WEP Key 3: □ Show

WEP Key 4: □ Show

1. Go to **Configuration** > **Wireless** > **Radio1(5G) > WLAN0 > WLAN Security**
2. Select *Shared* on **Authentication Mode**
3. Select *WEP* on **Cipher Mode**
4. Select key number *1 – 4* on **Default WEP Key**
5. Select suitable key type in **Key Entry Mode**; the options include:

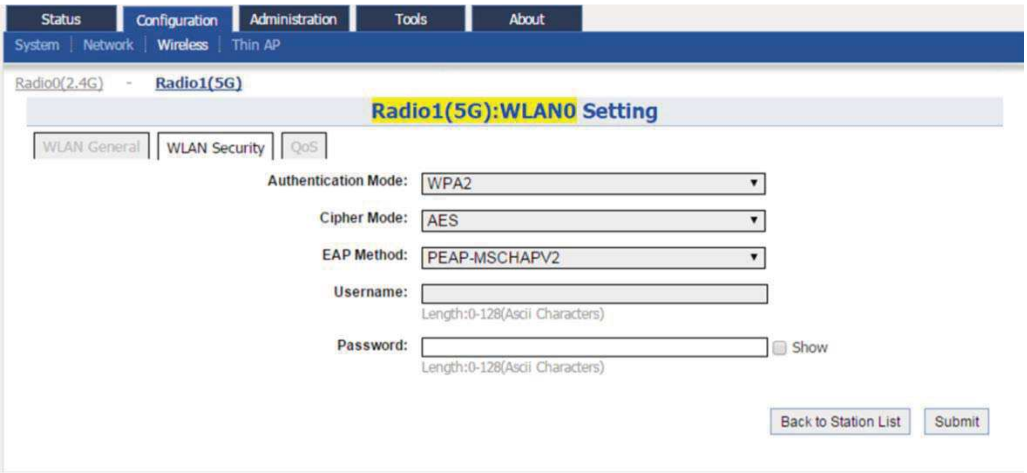
Ascii Text key is encoded as ASCII characters (0–9, a–z, A–Z)

Hexadecimal key is encoded as Hexadecimal characters (0–9, A–F)

6. Enter up to four keys in WEP Key 1, WEP Key 2, WEP Key 3 and WEP Key 4 respectively. You can type either up to 5 Ascii characters or up to 10 Hexadecimal characters as WEP Key.
7. Click **Submit**

Configure to associate WLAN with WPA / WPA2 authentication

Figure 89 - WLAN15 Security Setting – Associating WLAN with WPA / WPA2 authentication



Authentication Mode: WPA2
Cipher Mode: AES
EAP Method: PEAP-MSCHAPV2
Username:
Length:0-128(Ascii Characters)
Password: □ Show
Length:0-128(Ascii Characters)

1. Go to **Configuration** > **Wireless** > **Radio1(5G)** > **Station** > **WLAN0** > **WLAN Security**
2. Select *WPA* / *WPA2* in **Authentication Mode**
3. Select suitable encryption mode in **Cipher Mode** as the followings:

If Authentication Mode is *WPA:*

TKIP + AES	This algorithm automatically selects TKIP or AES based on the client's capabilities
TKIP	This algorithm provides greater compatibility with older client devices, but is not supported by the 802.11n standard.
AES	This algorithm provides enhanced security over TKIP, and is the only encryption algorithm supported by the 802.11i standard.

If Authentication Mode is *WPA2*:

AES	This algorithm provides enhanced security over TKIP, and is the only encryption algorithm supported by the 802.11i standard.

If Authentication Mode is *WPA-auto*:

TKIP + AES	This algorithm automatically selects TKIP or AES based on the client's capabilities

4. Select suitable EAP method mode in **EAP Method**; the options include:

PEAP-MSCHAPV2

TTLS-MSCHAPV2

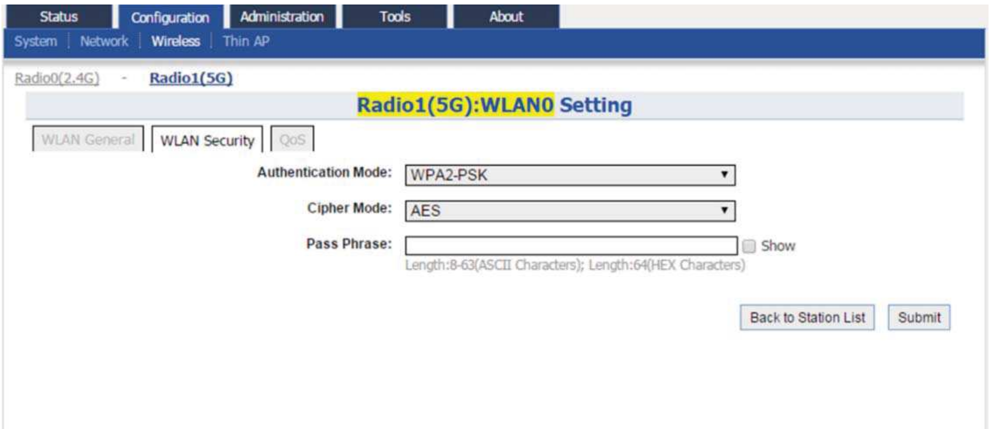
TTPS-PAP

TTLS-CHAP

5. Enter correct username in **Username** for authentication**.**
6. Enter correct password in **Password** for authentication**.**
7. Click **Submit**

Configure to associate network with WPA-PSK / WPA2-PSK authentication

Figure 90 - WLAN15 Security Setting – Associating WLAN with WPA-PSK / WPA2-PSK authentication



Radio1(5G):WLAN0 Setting

Authentication Mode: WPA2-PSK

Cipher Mode: AES

Pass Phrase:

Length:8-63(ASCII Characters); Length:64(HEX Characters)

1. Go to **Configuration** > **Wireless** > **Radio1(5G)** > **Repeater** > **WLAN15** > **WLAN Security**
2. Select *WPA-PSK* / *WPA2-PSK* in **Authentication Mode**
3. Select suitable encryption mode in **Cipher Mode** as the followings:

If Authentication Mode is *WPA:*

TKIP + AES	This algorithm automatically selects TKIP or AES based on the client's capabilities

TKIP	This algorithm provides greater compatibility with older client devices, but is not supported by the 802.11n standard.
AES	This algorithm provides enhanced security over TKIP, and is the only encryption algorithm supported by the 802.11i standard.

If Authentication Mode is *WPA2*:

AES	This algorithm provides enhanced security over TKIP, and is the only encryption algorithm supported by the 802.11i standard.

If Authentication Mode is *WPA-auto*:

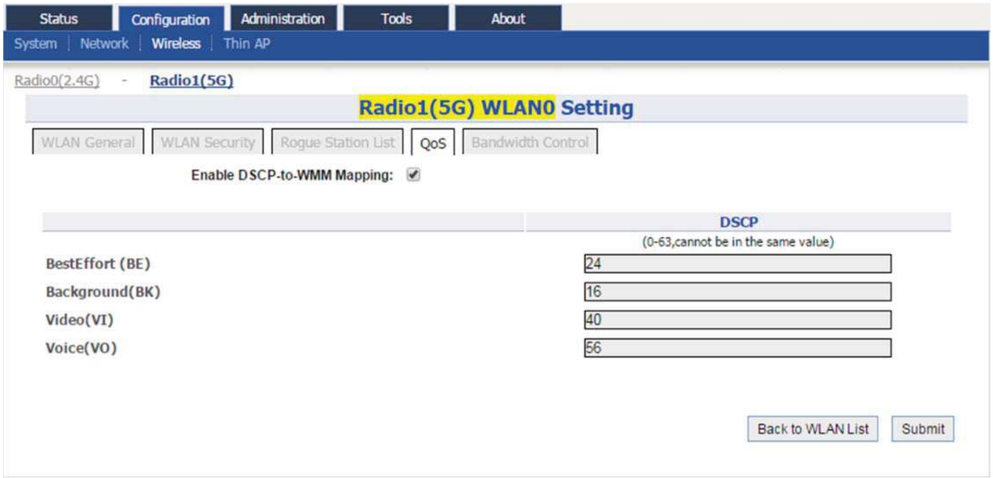
TKIP + AES	This algorithm automatically selects TKIP or AES based on the client's capabilities

4. Enter an ASCII string between 8 and 63 characters long or a HEX string with 64 characters long on **Pass Phrase** that matches with remote AP

5. Click **Submit**

4.3.2.4 Configure WLAN15 QoS

Figure 91 – 5G WLAN # QoS



Radio1(5G) WLAN0 Setting

Enable DSCP-to-WMM Mapping: ☑

	DSCP (0-63,cannot be in the same value)
BestEffort (BE)	24
Background(BK)	16
Video(VI)	40
Voice(VO)	56

1. Go to **Configuration** > **Wireless** > **Radio1(5G)** > **WLAN** > **WLAN #** > **QoS**

2. Select **Enable DSCP-to-WMM Mapping** checkbox that CPE provides different QoS to the incoming packet with the corresponding DSCP value

3. Enter DSCP value on **Best Effort (BE)**, **Background (BK)**, **Video (VI)**, and **Voice (VO)**; these entry is optional

4. Click **Submit**

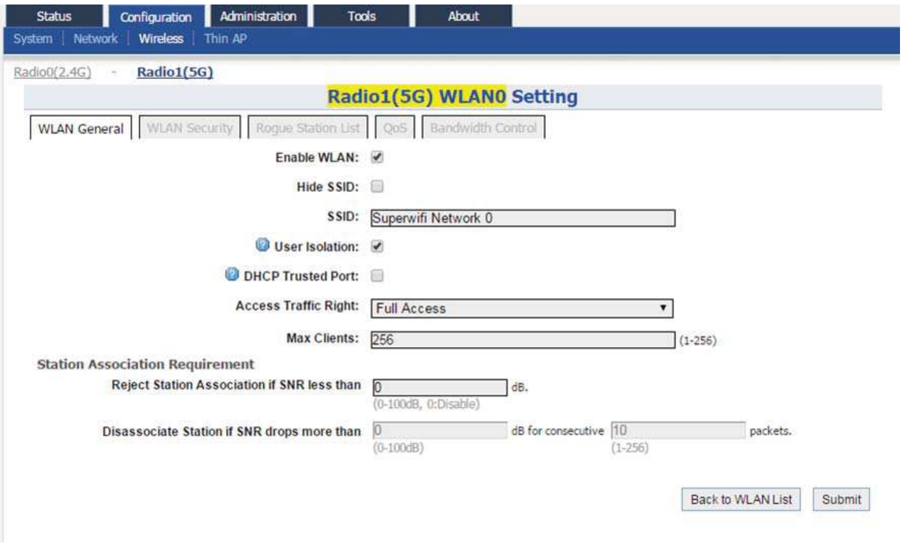
Note:

– CPE classify the packet without DSCP marking as Best Effort (BE) traffic

---

4.3.2.5 Configure WLAN # General Setting

Figure 92 - 5G WLAN # General Setting



Radio1(5G) WLAN0 Setting

Enable WLAN: ☑

Hide SSID: □

SSID: Superwifi Network 0

User Isolation: ☑

DHCP Trusted Port: □

Access Traffic Right: Full Access

Max Clients: 256 (1-256)

Station Association Requirement

Reject Station Association if SNR less than 0 dB. (0-100dB, 0:Disable)

Disassociate Station if SNR drops more than 0 (0-100dB) dB for consecutive 10 (1-256) packets.

1. Go to **Configuration** > **Wireless** > **Radio1 (5G)** > **WLAN #** > More…

2. Select **Enable WLAN** checkbox to enable WLAN

3. Select **Hide SSID** checkbox to hide SSID name from its beacon frame. This entry is optional.

4. Enter a unique name for the particular WLAN on **SSID**.

Note:

– If you want to configure the same SSID on two different WLAN; their security setting MUST be different from each other.

---

5. Select **User Isolation** checkbox to block user communication within the same SSID in the AP directly. This entry is optional.

6. Deselect the **DHCP Trust Port** checkbox to prevent illegal DHCP servers offering IP address to DHCP clients via this WLAN. This entry is optional.

7. Specify the suitable privilege of associated clients on **Access Traffic Right**; the options include

Full Access - Associated client can access Internet and manage AP

AP Management Only - Associated client can manage AP only, but not able to access the Internet

AP Management Disable - Associated client can access the Internet, but not able to manage AP

8. Specify the maximum associated clients between *1* and *256* on **Max Clients** for this WLAN. *256* is the default setting.

Note:

- **Max Clients** in WLAN 0 – 15 MUST be smaller than or equal to (≥) the **Max Clients** setting on Radio General Setting

9. Specify an additional requirement on Signal Strength to Noise Ratio (SNR) for associated clients under **Station Association Requirement**. This requirement is optional. You may fill up the following fields:

Reject Station Association if SNR less than X dB	*X* denote the minimum SNR level which allow clients to associate; You can select any integer between *0*dB and *100*dB; *0* denotes as disable; *0* is default setting
Disassociate Station if SNR drops more than Y dB for consecutive Z packets	Y denotes the SNR tolerance; Z denotes the number of consecutive packets their SNR are below the difference of X - Y.

Notes:

- Example for Station Association Requirement with the following settings:

Reject Station Association if SNR less than *30* dB (X = 30); Disassociate Station if SNR drops more than *20* dB for consecutive *10* packets (Y = 20; Z = 10)

Consequence:

AP accepts the clients to associate if the SNR of packets from the clients is high than (>) 30dB;

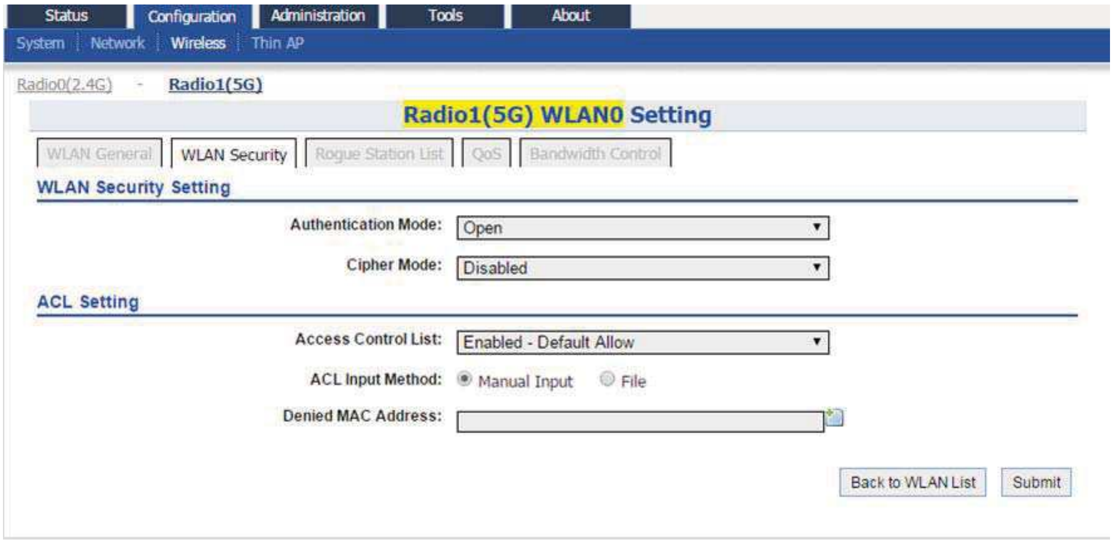
AP kicks out the associated client if the SNR of 10 consecutive packets is below (<) 10 dB (30 dB – 20 dB)

10. Click **Submit**

4.3.2.6 Configure WLAN # Security Setting

Configure WLAN as Open Network

Figure 93 - 5G WLAN # Security Setting: Open Network



Radio1(5G) WLAN0 Setting

WLAN Security Setting

Authentication Mode: Open

Cipher Mode: Disabled

ACL Setting

Access Control List: Enabled - Default Allow

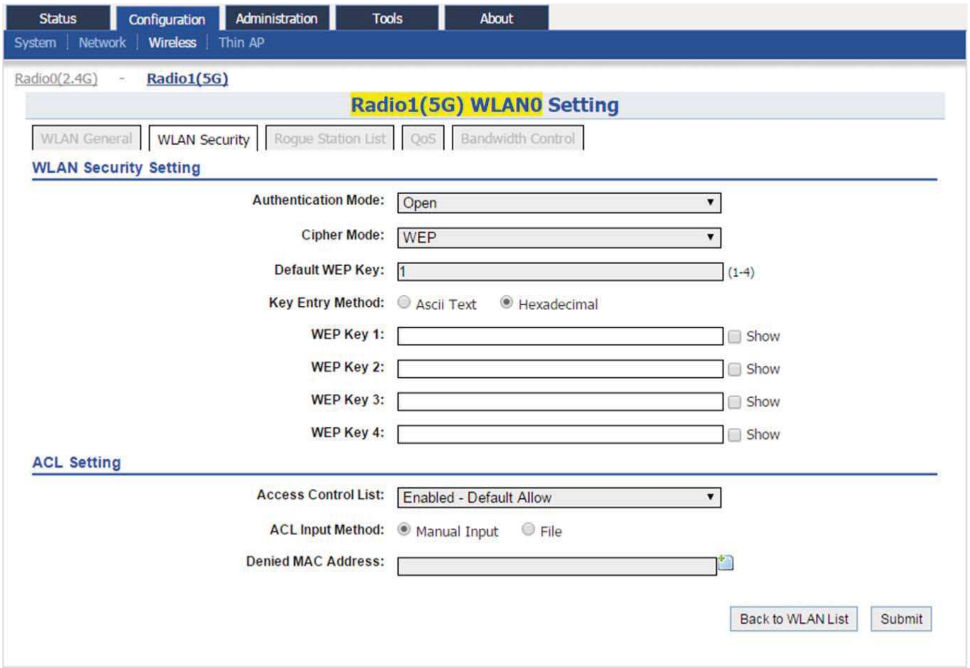
ACL Input Method: ● Manual Input ○ File

Denied MAC Address:

5. Go to **Configuration** > **Wireless** > **Radio1(5G)** > **WLAN** > **WLAN #** > **WLAN Security**
6. Select Open on **Authentication Mode**
7. Select *Disabled* on **Cipher Mode**
8. Click **Submit**

Configure WLAN as Open network with WEP encryption

Figure 94 - WLAN # Security Setting: Open Network with WEP



Radio1(5G) WLAN0 Setting

WLAN Security Setting

Authentication Mode: Open

Cipher Mode: WEP

Default WEP Key: 1 (1-4)

Key Entry Method: ○ Ascii Text ● Hexadecimal

WEP Key 1: □ Show

WEP Key 2: □ Show

WEP Key 3: □ Show

WEP Key 4: □ Show

ACL Setting

Access Control List: Enabled - Default Allow

ACL Input Method: ● Manual Input ○ File

Denied MAC Address:

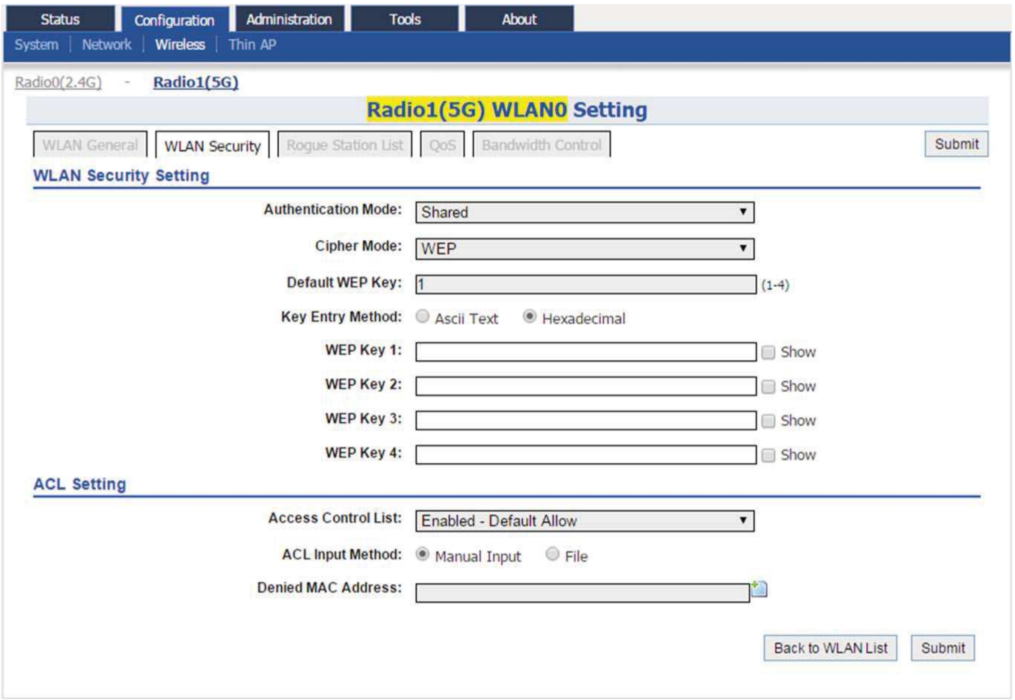
1. Go to **Configuration** > **Wireless** > **Radio1(5G)** > **WLAN** > **WLAN #** > **WLAN Security**
2. Select Open on **Authentication Mode**
3. Select *WEP* on **Cipher Mode**
4. Select key number *1 – 4* on **Default WEP Key**
5. Select suitable key type in **Key Entry Mode**; the options include:

Ascii Text	key is encoded as ASCII characters (0–9, a–z, A–Z)
Hexadecimal	key is encoded as Hexadecimal characters (0–9, A–F)

6. Enter up to four keys in WEP Key 1, WEP Key 2, WEP Key 3 and WEP Key 4 respectively. You can type either up to 5 Ascii characters or up to 10 Hexadecimal characters as WEP Key.
7. Click **Submit**

Configure WLAN as Open network with Shared Key Authentication

Figure 95 - 5G WLAN # Security Setting: Shared Key Authentication



Radio1(5G) WLAN0 Setting

WLAN Security Setting

Authentication Mode: Shared

Cipher Mode: WEP

Default WEP Key: 1 (1-4)

Key Entry Method: ○ Ascii Text ● Hexadecimal

WEP Key 1: □ Show

WEP Key 2: □ Show

WEP Key 3: □ Show

WEP Key 4: □ Show

ACL Setting

Access Control List: Enabled - Default Allow

ACL Input Method: ● Manual Input ○ File

Denied MAC Address:

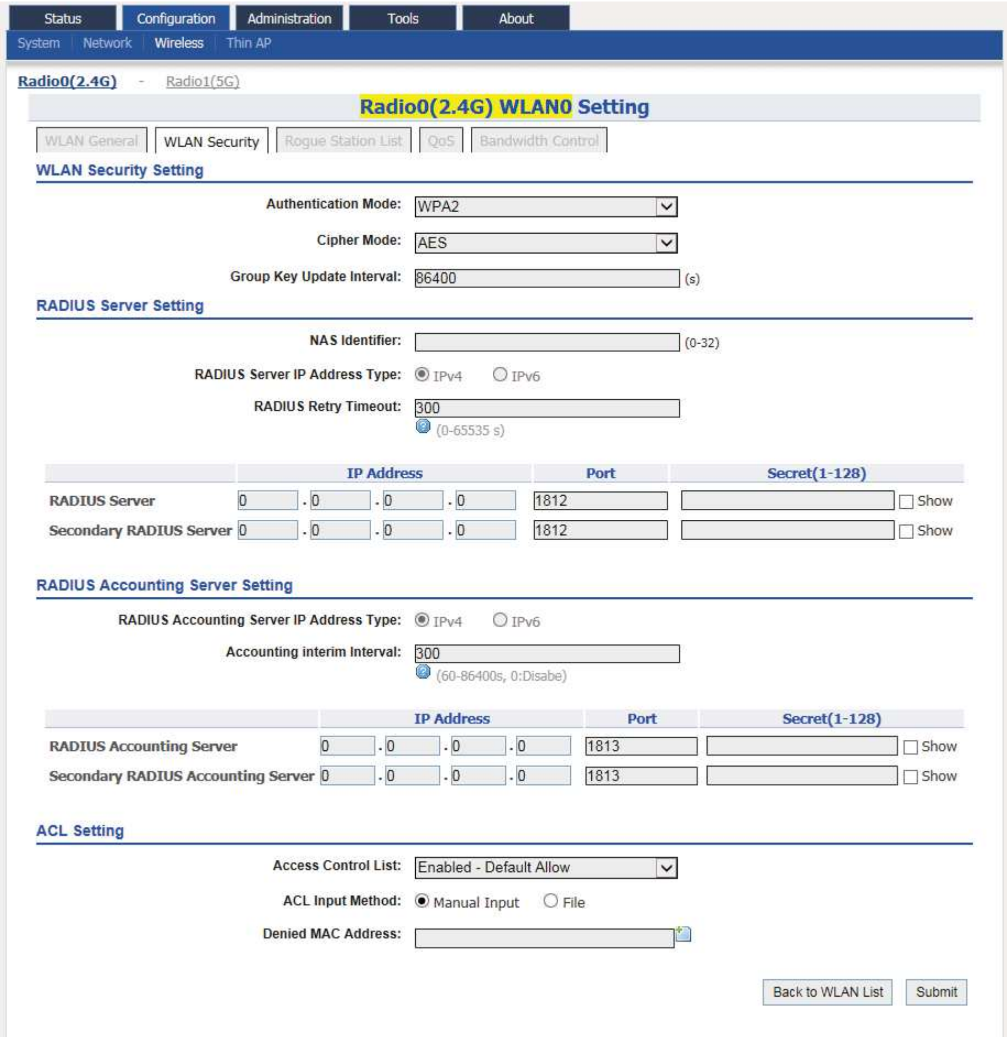
1. Go to **Configuration** > **Wireless** > **Radio1(5G)** > **WLAN** > **WLAN #** > **WLAN Security**
2. Select *Shared* on **Authentication Mode**
3. Select *WEP* on **Cipher Mode**
4. Select key number *1 – 4* on **Default WEP Key**
5. Select suitable key type in **Key Entry Mode**; the options include:

Ascii Text	key is encoded as ASCII characters (0–9, a–z, A–Z)
Hexadecimal	key is encoded as Hexadecimal characters (0–9, A–F)

6. Enter up to four keys in WEP Key 1, WEP Key 2, WEP Key 3 and WEP Key 4 respectively. You can type either up to 5 ASCII characters or up to 10 Hexadecimal characters as WEP Key.
7. Click **Submit**

Configure WLAN with WPA / WPA2 / WPA-auto Authentication

Figure 96 - 5G WLAN # Security Setting: WPA / WPA2 / WPA-auto Authentication



Radio0(2.4G) WLAN0 Setting

WLAN Security Setting

Authentication Mode: WPA2

Cipher Mode: AES

Group Key Update Interval: 86400 (s)

RADIUS Server Setting

NAS Identifier: (0-32)

RADIUS Server IP Address Type: ● IPv4 ○ IPv6

RADIUS Retry Timeout: 300 (0-65535 s)

	IP Address	Port	Secret(1-128)
RADIUS Server	0 . 0 . 0 . 0	1812	□ Show
Secondary RADIUS Server	0 . 0 . 0 . 0	1812	□ Show

RADIUS Accounting Server Setting

RADIUS Accounting Server IP Address Type: ● IPv4 ○ IPv6

Accounting interim Interval: 300 (60-86400s, 0:Disabe)

	IP Address	Port	Secret(1-128)
RADIUS Accounting Server	0 . 0 . 0 . 0	1813	□ Show
Secondary RADIUS Accounting Server	0 . 0 . 0 . 0	1813	□ Show

ACL Setting

Access Control List: Enabled - Default Allow

ACL Input Method: ● Manual Input ○ File

Denied MAC Address:

1. Go to **Configuration** > **Wireless** > **Radio1(5G)** > **WLAN** > **WLAN #** > **WLAN Security**
2. Select *WPA* / *WPA2* / *WPA-auto* on **Authentication Mode**
3. Select suitable encryption mode on **Cipher Mode**

If Authentication Mode is *WPA:*

TKIP + AES	This algorithm automatically selects TKIP or AES based on the client's capabilities
TKIP	This algorithm provides greater compatibility with older client devices, but is not supported by the 802.11n standard.
AES	This algorithm provides enhanced security over TKIP, and is

	the only encryption algorithm supported by the 802.11i standard.

If Authentication Mode is *WPA2*:

AES	This algorithm provides enhanced security over TKIP, and is the only encryption algorithm supported by the 802.11i standard.

If Authentication Mode is *WPA-auto*:

TKIP + AES	This algorithm automatically selects TKIP or AES based on the client's capabilities

Note:

- TKIP is not supported by 802.11n standard. If selected TKIP, the 802.11n's devices will be limited to 802.11g transfer rate, i.e. up to 54 Mbps

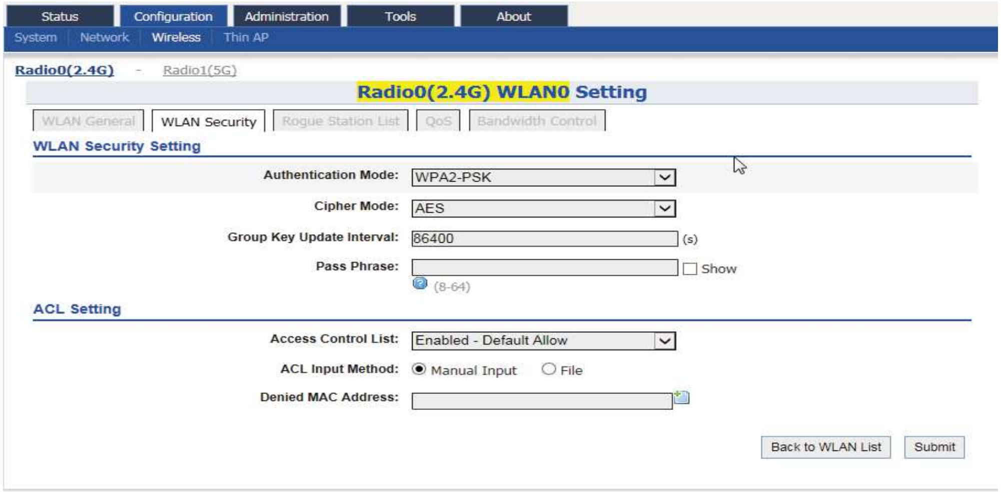
4. Enter suitable identification on **NAS identifier**. Remote RADIUS server uses this ID to identify its clients. This entry is available for WPA and WPA2 only.
5. Enter transmission timeout interval between *0* and *86400*s on **RADIUS Retry Timeout**. *300* is default setting. This entry is optional.
6. Enter IP address of remote RADIUS server for authentication in **IP Address of RADIUS Server**
7. Enter service port of remote RADIUS server in **Port of RADIUS Server**. *1812* is default setting.
8. Enter suitable secrets in **Secret of RADIUS Server**. It is used along with the MD5 hashing algorithm to obfuscate passwords. This secret MUST be as the same as that in RADIUS server.
9. Repeat step 6-8 if the backup RADIUS server is available. It is optional.
10. Enter interval between each interim update in seconds on **Accounting interim Interval**. *300* is default setting. This entry is optional.
11. Enter IP address of remote RADIUS Accounting Server on **IP Address of RADIUS Accounting Server**. This entry is optional.
12. Enter service port of remote RADIUS server in **Port of RADIUS Accounting Server**. *1813* is default setting. This entry is optional.
13. Enter suitable secrets in **Secret of RADIUS Accounting Server**. It is used along with the MD5 hashing algorithm to obfuscate passwords. This secret MUST be as the same as that in RADIUS server. This entry is optional.

14. Repeat step 11-13 if the backup RADIUS Accounting server is available. It is optional.

15. Click **Submit**

Configure WLAN with WPA-PSK / WPA2-PSK / WPA-auto-PSK Authentication

Figure 97 - 5G WLAN # Security Setting: WPA-PSK / WPA2-PSK / WPA-auto-PSK Authentication



Radio0(2.4G) WLAN0 Setting

WLAN Security Setting

Authentication Mode: WPA2-PSK

Cipher Mode: AES

Group Key Update Interval: 86400 (s)

Pass Phrase: □ Show
(8-64)

ACL Setting

Access Control List: Enabled - Default Allow

ACL Input Method: ● Manual Input ○ File

Denied MAC Address:

1. Go to **Configuration** > **Wireless** > **Radio1(5G)** > **WLAN** > **WLAN #** > **WLAN Security**

2. Select *WPA-PSK* / *WPA2-PSK* / *WPA-auto-PSK* on **Authentication Mode**

3. Select suitable encryption mode on **Cipher Mode**

If Authentication Mode is *WPA:*

TKIP + AES	This algorithm automatically selects TKIP or AES based on the client's capabilities
TKIP	This algorithm provides greater compatibility with older client devices, but is not supported by the 802.11n standard.
AES	This algorithm provides enhanced security over TKIP, and is the only encryption algorithm supported by the 802.11i standard.

If Authentication Mode is *WPA2*:

AES	This algorithm provides enhanced security over TKIP, and is

	the only encryption algorithm supported by the 802.11i standard.

If Authentication Mode is *WPA-auto*:

TKIP + AES	This algorithm automatically selects TKIP or AES based on the client's capabilities

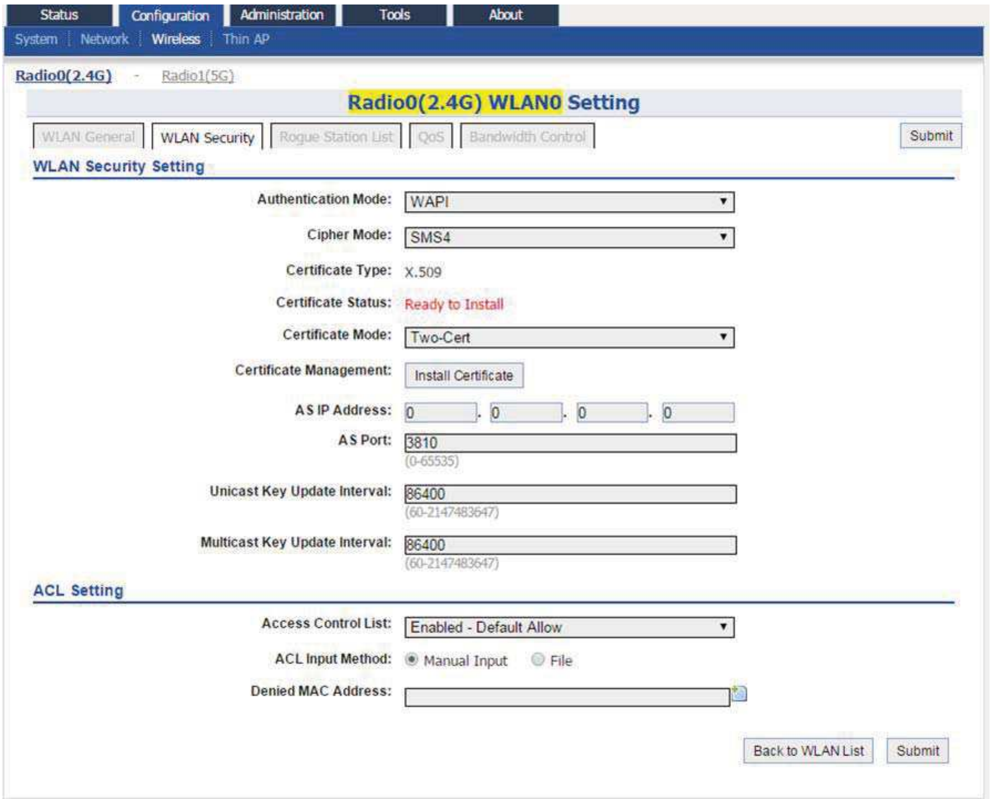
Note:

- TKIP is not supported by 802.11n standard. If selected TKIP, the 802.11n's devices will be limited to 802.11g transfer rate, i.e. up to 54 Mbps

4. Enter interval time in second in **Group Key Update Interval**. *86400* is default setting. This entry is optional.
5. Enter an ASCII string between 8 and 63 characters long or a HEX string with 64 characters long on **Pass Phrase** that users will use to connect to the wireless network.
6. Click **Submit**

Configure WLAN with WAPI Authentication

Figure 98 - 5G WLAN # Security Setting: WAPI Authentication



Radio0(2.4G) WLAN0 Setting

WLAN Security Setting

Authentication Mode: WAPI

Cipher Mode: SMS4

Certificate Type: X.509

Certificate Status: Ready to Install

Certificate Mode: Two-Cert

Certificate Management: Install Certificate

AS IP Address: 0 . 0 . 0 . 0

AS Port: 3810 (0-65535)

Unicast Key Update Interval: 86400 (60-2147483647)

Multicast Key Update Interval: 86400 (60-2147483647)

ACL Setting

Access Control List: Enabled - Default Allow

ACL Input Method: ● Manual Input ○ File

Denied MAC Address:

1. Go to **Configuration** > **Wireless** > **Radio1(5G)** > **WLAN** > **WLAN #** > **WLAN Security**
2. Select *WAPI* on **Authentication Mode**
3. Select *SMS4* in **Cipher Mode**
4. Select suitable option in **Certificate Mode**; the options includes:

Two-Cert – Wi-Fi client is verified by the certification from authentication server (AS) and Access Point (AP)

Three-Cert - Wi-Fi client is verified by the certification from authentication server (AS), access point (AP), and certificate authority (CA)

5. Click Install Certificate; a window for installing certificate is shown on Figure 99 and Figure 100.

Figure 99 - Two-Cert Mode Certification Installation

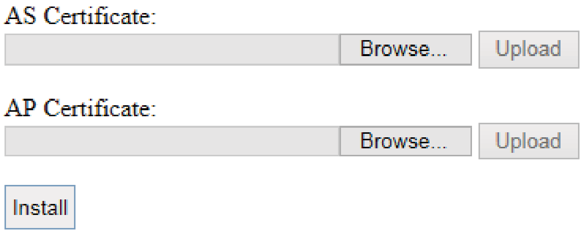
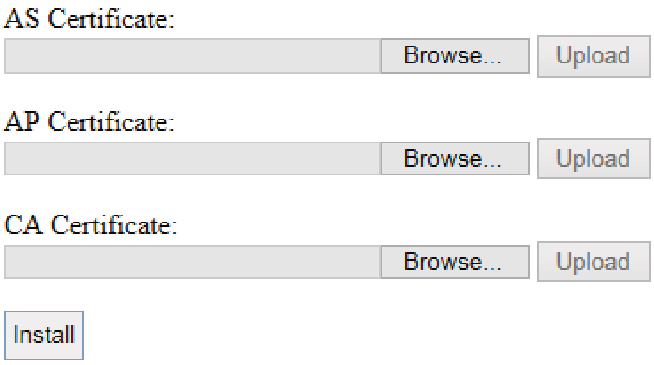


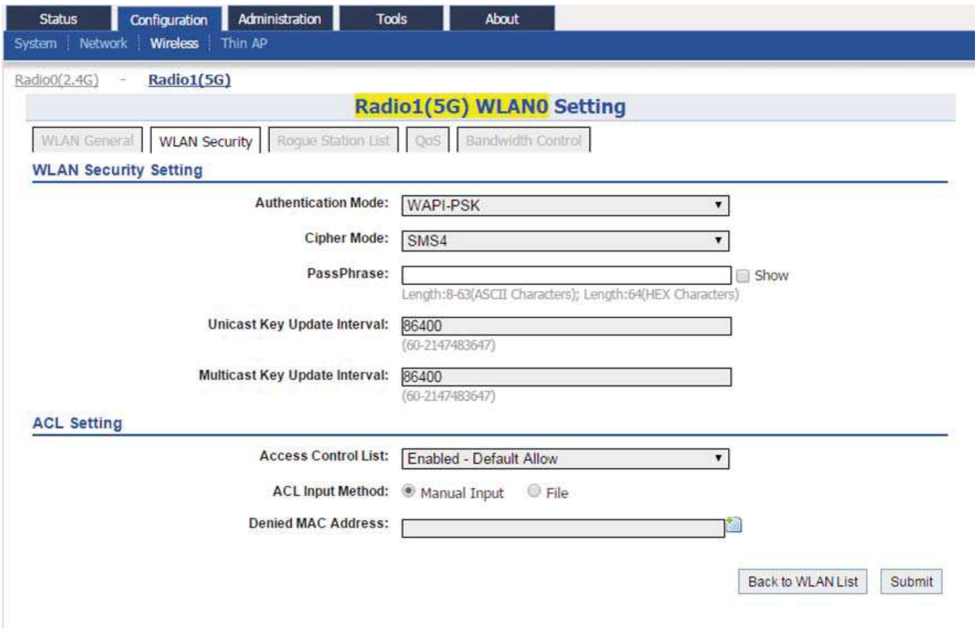
Figure 100 - Three-Cert Mode Certification Installation



6. Click **Browse** to select suitable certifications
7. Click **Upload** to upload the selected certifications to CPE
8. Click **Install** to install certifications
9. Enter IP address of AS server on **AS IP Address**
10. Enter service port of AS server in **AS Port**
11. Enter interval time between 60 and 2147483647s in **Unicast Key Update Interval**; *86400* is default setting. This entry is optional.
12. Enter interval time between 60 and 2147483647s in **Multicast Key Update Interval**; *86400* is default setting. This entry is optional.
13. Click **Submit**

Configure WLAN with WAPI-PSK Authentication

Figure 101 - 5G WLAN # Security Setting: WAPI-PSK Authentication



Radio1(5G) WLAN0 Setting

WLAN Security Setting

Authentication Mode: WAPI-PSK

Cipher Mode: SMS4

PassPhrase: □ Show
Length:8-63(ASCII Characters); Length:64(HEX Characters)

Unicast Key Update Interval: 86400
(60-2147483647)

Multicast Key Update Interval: 86400
(60-2147483647)

ACL Setting

Access Control List: Enabled - Default Allow

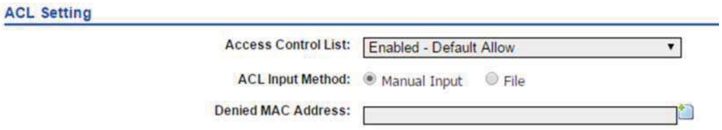
ACL Input Method: ● Manual Input ○ File

Denied MAC Address:

1. Go to **Configuration** > **Wireless** > **Radio1(5G)** > **WLAN** > **WLAN #** > **WLAN Security**
2. Select *WAPI* on **Authentication Mode**
3. Select *SMS4* in **Cipher Mode**
4. Enter in an ASCII string between 8 and 63 characters or a HEX string with 64 characters long in **Pass Phrase** that users will use to connect to the wireless network.
5. Enter interval time between 60 and 2147483647s in **Unicast Key Update Interval**; *86400* is default setting. This entry is optional.
6. Enter interval time between 60 and 2147483647s in **Multicast Key Update Interval**; *86400* is default setting. This entry is optional.
7. Click **Submit**

4.3.2.7 Configure ACL Setting

Figure 102 – 5G WLAN #ACL Setting



ACL Setting

Access Control List: Enabled - Default Allow ▾

ACL Input Method: ● Manual Input ○ File

Denied MAC Address:

1. Go to **Configuration** > **Wireless** > **Radio0(2.4G)** > **WLAN** > **WLAN #** > **ACL Setting**
2. Select appropriate option on **Access Control List**; options include

Disable	ACL is disabled
Enabled – Default Allow	ACL is enabled. The MAC addresses which are specified in the ACL will consider as Deny. Every wireless client can associate to the AP unless its MAC address is on the list
Enabled – Default Deny	ACL is enabled. The MAC addresses which are specified in the ACL will consider as Allow. Every wireless client CANNOT associate to the AP unless its MAC address is on the list

3. Select *Manual Input* on **ACL Input Method** if network administrator prefers input the entry one by one manually

Or select File on **ACL Input Method** if network administrator prefers upload a MAC address list (.txt file)

4. Enter MAC address entry one by one or upload the corresponding file to CPE; it is optional
5. Click **Submit**

Note:

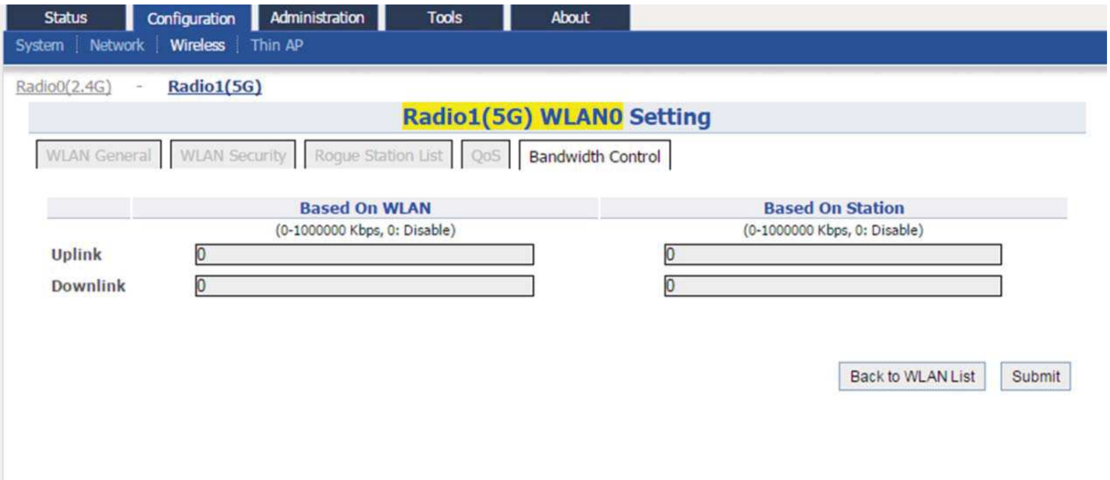
- *Network Administrator shall select Disable or Enabled – Default Allow if no ACL entry will be input on CPE*

4.3.2.8 Configure WLAN # QoS

Please refer to Quality of Service (QoS) on page 129

4.3.2.9 Configure WLAN # Bandwidth Control

Figure 103 – 5G WLAN # Bandwidth Control



Radio1(5G) WLAN0 Setting

	Based On WLAN (0-1000000 Kbps, 0: Disable)	Based On Station (0-1000000 Kbps, 0: Disable)
Uplink	0	0
Downlink	0	0

1. Go to **Configuration** > **Wireless** > **Radio1(5G)** > **WLAN** > **WLAN #** > **Bandwidth Control**
2. Specify the uplink and downlink limitation under **Based on WLAN** for the particular WLAN

   Or specify the uplink and downlink limitation under **Based on Station** for each associated station. *0* is default value and denotes as disable
3. Click **Submit**

4.3.2.10 Apply Submitted Configurations on the CPE Device

1. Click **Save & Apply** from the top on the right.

5. Advanced Radio Settings

Advanced radio settings are available on each radio interface; these settings include Frame Aggregation, Data Rate setting, Medium Access Protection Mechanism, Spatial Stream, and Throughput Optimization mechanism.

Caution:

– *Inappropriate configuration may bring negative impact on the network performance*

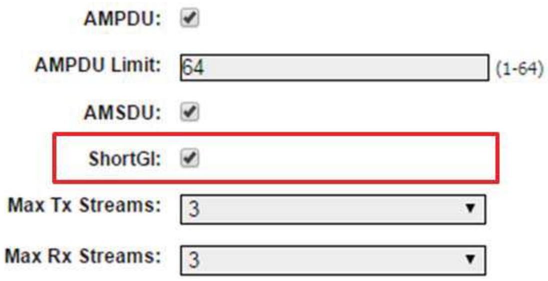
– *Only technically advanced users who have sufficient knowledge about WLAN technology should use the advanced wireless settings.*

– ***Default setting is recommended***

5.1. Short Guard Interval

Guard Intervals (GI) are used to ensure that distinct transmissions do not interfere with one another. The standard symbol guard interval used in 802.11 OFDM is 800ms. To increase data rate, 802.11n/ac added optional supports for a 400ms guard interval. It is known as Short Guard Interval. This provides an 11% increase in data rate.

Figure 104 - Short GI Setting



AMPDU: ☑

AMPDU Limit: 64 (1-64)

AMSDU: ☑

ShortGI: ☑

Max Tx Streams: 3

Max Rx Streams: 3

1. 2.4G Radio: Go to **Configuration** > **Wireless > Radio0(2.4G) > Advanced > Advanced Settings**

   5G Radio: Go to **Configuration** > **Wireless > Radio1(5G) > Advanced > Advanced Settings**

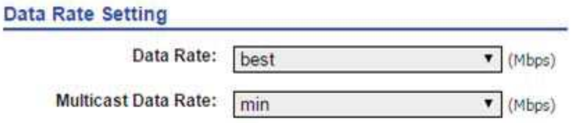
2. Click **ShortGI** checkbox
3. Click **Submit**
4. Click **Save & Apply** from the top on the right.

5.2. Data Rate Setting

The fact is that low data rate transmissions consume more air time than high data rates. It may affect the system performance. By disabling low data rates, AP rules out some remote clients with poor signal strength and hence low link data rate, preventing them from consuming too much air time and leaves the air time for higher data rates transmissions. In this way, overall system performance can be improved. The most common way we use it is to disable low data rates (e.g., 1M, 2M) when the AP performance is reported poor.

CPE has two (2) configurable parameters about data rate setting; they are **Data Rate** and **Multicast Data Rate**. **Data Rate** stands for the data rate setting for unicast data packet; while **Multicast Data Rate** stands for the data rate setting for multicast data packet.

Figure 105 – Data Rate Setting



Data Rate Setting

Data Rate: best (Mbps)

Multicast Data Rate: min (Mbps)

5.2.1 Configure Data Rate

1. 2.4G Radio: Go to **Configuration** > **Wireless > Radio0(2.4G) > Advanced > Data Rate Setting**

   5G Radio: Go to **Configuration** > **Wireless > Radio1(5G) > Advanced**

   > Data Rate Setting

2. Select appropriate data rate on **Data Rate**; *best* is default setting. This option lets CPE device to determine the best data rate for transferring data time by time. Otherwise, CPE uses the selected data rate for unicast packet transmission under any condition.
3. Click **Submit**
4. Click **Save & Apply** from the top on the right.

5.2.2Configure Multicast Rate

1. 2.4G Radio: Go to **Configuration** > **Wireless > Radio0(2.4G) > Advanced > Data Rate Setting**

   5G Radio: Go to **Configuration** > **Wireless > Radio1(5G) > Advanced**

   > Data Rate Setting

2. Select appropriate data rate on **Multicast Rate**; *min* is default setting. This option lets CPE device to use the minimum data rate for

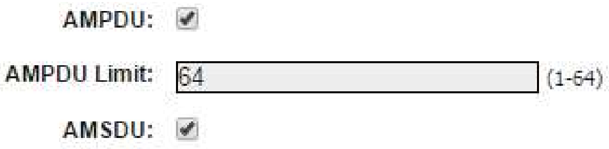
transferring multicast packets. Otherwise, CPE uses the selected data rate for multicast packet transmission under any condition.

3. Click **Submit**
4. Click **Save & Apply** from the top on the right.

5.3. Frame Aggregation

Frame aggregation allows the device to send multiple frames per single access to the medium by combining frames together into one larger frame.

Figure 106 – Frame Aggregation Configuration



AMPDU: ☑

AMPDU Limit: 64 (1-64)

AMSDU: ☑

1. 2.4G Radio: Go to **Configuration** > **Wireless > Radio0(2.4G) > Advanced > Advanced Settings**

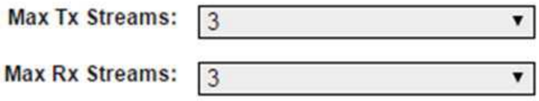
   5G Radio: Go to **Configuration** > **Wireless > Radio1(5G) > Advanced > Advanced Settings**

2. Click **AMPDU** checkbox to enable aggregation of MAC protocol data unit (MPDU)
3. Enter the maximum number of data frame between *1* and *64* on **AMPDU Limit** that CPE pushes MPDUs into single PPDU; *64* is default setting
4. Select **AMSDU** checkbox to enable aggregation of MAC service data unit; CPE pushes aggregated MSDU (MAC service data units) into a single MPDU
5. Click **Submit**
6. Click **Save & Apply** from the top on the right.

5.4. Spatial Streaming

With multiple-input and multiple-output (MIMO) technique, CPE can use one or more individual stream for data transmission and reception. In general, more available streams increase spatial efficiency.

Figure 107 – Spatial Streaming Configuration



Max Tx Streams: 3

Max Rx Streams: 3

1. 2.4G Interface: Go to **Configuration** > **Wireless > Radio0 > Advanced > Advanced Settings**

   5G Interface: Go to **Configuration** > **Wireless > Radio1 > Advanced > Advanced Settings**

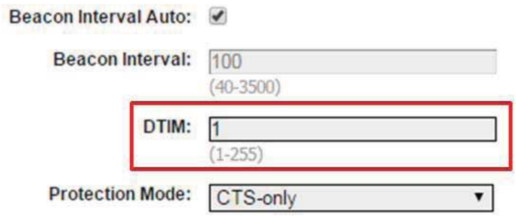
2. Select the maximum number of transmission between *1* and *3* on **Max Tx Streams**

3. Select the maximum number of transmission between *1* and *3* on **Max Rx Streams**
4. Click **Submit**
5. Click **Save & Apply** from the top on the right.

5.5. Delivery Traffic Indication Message (DTIM) time

According to the 802.11 standards, a Delivery Traffic Indication Map (DTIM) period value is a number that determines how often a beacon frame includes a Delivery Traffic Indication Message, and this number is included in each beacon frame. The 802.11 standards define a power-save mode for client devices. In power-save mode, a client device may choose to sleep for one or more beacon intervals waking for beacon frames that include DTIMs. When the DTIM period is 2, a client device in power-save mode will awaken to receive every other beacon frame. Upon entering power-save mode, a client device will transmit a notification to the access point, so that the access point will know how to handle unicast traffic destined for the client device.

Figure 108 – DTIM Setting



Beacon Interval Auto: ☑

Beacon Interval: 100 (40-3500)

DTIM: 1 (1-255)

Protection Mode: CTS-only

1. 2.4G Interface: Go to **Configuration** > **Wireless > Radio0 > Advanced > Advanced Settings**

   5G Interface: Go to **Configuration** > **Wireless > Radio1 > Advanced > Advanced Settings**
2. Specify the interval time between *1* and *255* in **DTIM.**
3. Click **Submit**
4. Click **Save & Apply** from the top on the right.

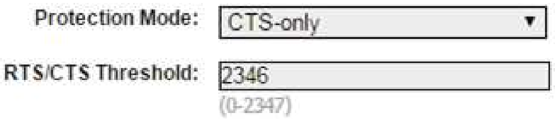
Note:

- The higher the DTIM period, the longer a client device may sleep and therefore the more power that particular client device may potentially save.

5.6. WiFi Protect mechanism [Hidden node problem]

In wireless networking, the hidden node problem or hidden terminal problem occurs when a node is visible from a wireless access point (AP), but not from other nodes communicating with that AP. This leads to difficulties in media access control sublayer. IEEE 802.11 uses 802.11 RTS/CTS acknowledgment and handshake packets to partly overcome the hidden node problem.

Figure 109 – Protection Mode Setting



Protection Mode: CTS-only

RTS/CTS Threshold: 2346 (0-2347)

1. 2.4G Interface: Go to **Configuration** > **Wireless > Radio0 > Advanced > Advanced Settings**

5G Interface: Go to **Configuration** > **Wireless > Radio1 > Advanced > Advanced Settings**

2. Select suitable mechanism on **Protection Mode**; options include:

None - no protect mechanism is used. It is the default setting.

CTS-only - also known as CTS-to-Self; AP issues a CTS frame to itself before sending data. All clients will not transmit during the time.

RTS-CTS - AP sends a RTS frame, waits for the clients CTS frame and then sends the data packet. It allow more robust operation, but at the expense of additional overheads.

3. Specify frame size in byte between *0* and *2347* bytes on **RTS/CTS Threshold**; *2346* is default setting.

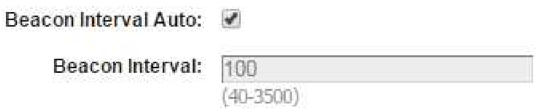
If a frame is smaller than the RTS/CTS threshold, it will be sent by the AP without modification. If a frame is larger than the RTS/CTS threshold, then two frames will be sent by the AP. The first frame is an RTS (request to send) frame. After the RTS frame is sent, the AP listens for the corresponding CTS from the target client. Upon reception of the CTS, the AP then sends the data frame. There are trade-offs when considering what value you should set for the RTS/CTS threshold. Smaller values will cause RTS to be sent more often, increasing overheads. However, the more often RTS packets are sent, the sooner the system can recover from collisions. It is recommended to use the default value or only minor reductions of the default setting.

4. Click **Submit**
5. Click **Save & Apply** from the top on the right.

5.7. Beacon interval of BSS

Beacon interval stands for the time interval of beacon transmissions of each supported BSS. The unit is in term of millisecond (ms). The beacon interval can be configured between 40 and 3500ms. The default setting is 100ms, i.e. 10 beacons per second.

Figure 110 – Beacon Interval Setting


Beacon Interval Auto: ☑

Beacon Interval: 100 (40-3500)

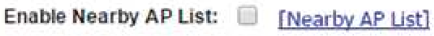
1. 2.4G Interface: Go to **Configuration** > **Wireless > Radio0 > Advanced > Advanced Settings**

   5G Interface: Go to **Configuration** > **Wireless > Radio1 > Advanced > Advanced Settings**

2. Select **Beacon Interval Auto** checkbox CPE tunes the interval of beacon transmissions of each supported BSS automatically. Enabling is default and recommended setting
3. Enter interval time between *40*ms and *3500*ms on **Beacon Interval**; this option is available if **Beacon Interval Auto** is NOT enabled. Each BSS share this setting.
4. Click **Submit**
5. Click **Save & Apply** from the top on the right.

5.8. Nearby AP List

Figure 111 – Nearby AP List Setting


Enable Nearby AP List: ☐ [Nearby AP List]

To configure nearby AP list, perform the followings:

1. 2.4G Interface: Go to **Configuration** > **Wireless > Radio0(2.4G) > Advanced > Advanced Settings**

5G Interface: Go to **Configuration** > **Wireless > Radio1(5G) > Advanced > Advanced Settings**

2. Select **Nearby AP List** checkbox to enable that CPE sniffs the surrounding AP periodically; The result list is shown on the corresponding radios' status information
3. Click **Submit**
4. Click **Save & Apply** from the top on the right.

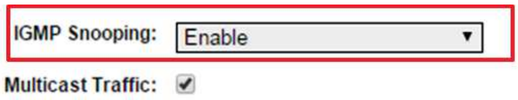
5.9. IGMP Snooping

CPE acts as a Layer 2 device when it is configured as Switch mode. However, IGMP Snooping implementation on CPE is a little bit different than that of standard Layer 2 Switch.

Typically, IGMP Snooping allows a switch to only forward multicast traffic to the links that have at least one client joined the multicast group. Unlike ordinary IGMP Snooping implementation, CPE converts multicast to unicast and delivers them to devices registered with the multicast group.

When IGMP Snooping is turned on, multicast packets should be dropped at the WLAN exit if there is no client from the WLAN who has joined the corresponding multicast group.

Figure 112 – IGMP Snooping Setting



IGMP Snooping: Enable

Multicast Traffic: ☑

1. 2.4G Interface: Go to **Configuration** > **Wireless > Radio0(2.4G) > Advanced > Advanced Settings**

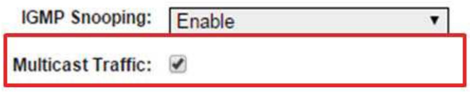
5G Interface: Go to **Configuration** > **Wireless > Radio1(5G) > Advanced > Advanced Settings**

2. Select **IGMP Snooping** checkbox to enable IGMP Snooping
3. Click **Submit**
4. Click **Save & Apply** from the top on the right.

5.10. Multicast Traffic

Network administrator allows CPE to process or discard the multicast traffic by configuring the multicast traffic option on Web UI.

Figure 113 – Multicast Traffic Setting



IGMP Snooping: Enable

Multicast Traffic: ☑

1. 2.4G Interface: Go to **Configuration** > **Wireless > Radio0(2.4G) > Advanced > Advanced Settings**

5G Interface: Go to **Configuration** > **Wireless > Radio1(5G) > Advanced > Advanced Settings**

2. Select Multicast Traffic checkbox to enable that CPE processes multicast traffic in WLANs
3. Click **Submit**
4. Click **Save & Apply** from the top on the right.

6. VLAN Configuration

VLAN is layer-2 network domain that may be partitioned to create multiple distinct broadcast domains, which are mutually isolated so that packets can only pass between them via one or more routers.

Note:

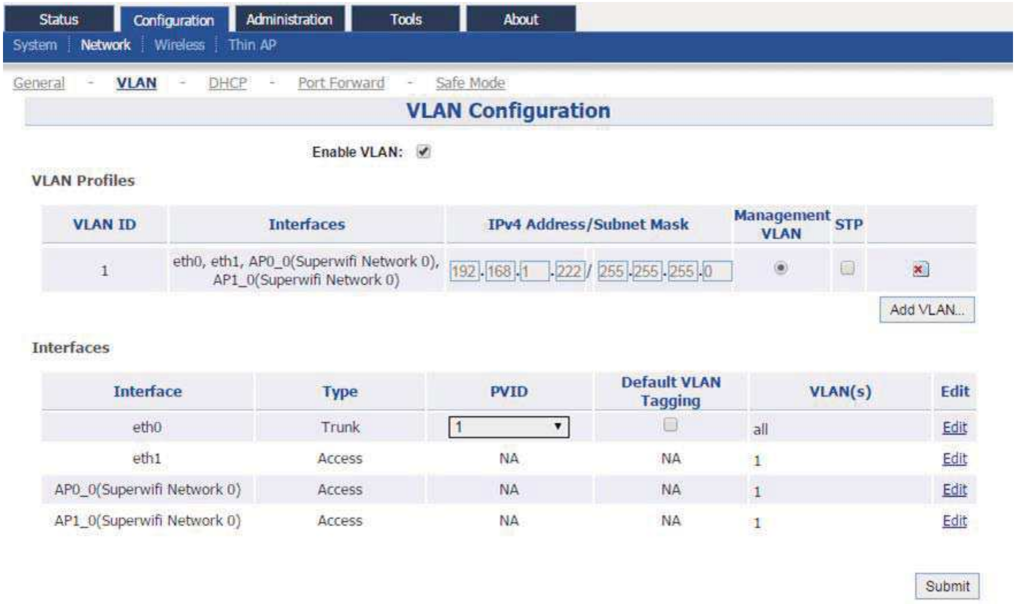
- *VLAN is applicable on Switch mode ONLY*

6.1 Configure Radio Settings

Please refer to Radios Setting on Page 17 to complete the radio settings

6.2 Enable VLAN

Figure 114 – VLAN Setting


Status
Configuration
Administration
Tools
About
System | Network | Wireless | Thin AP
General - VLAN - DHCP - Port Forward - Safe Mode

VLAN Configuration

Enable VLAN: ☑

VLAN Profiles

VLAN ID	Interfaces	IPv4 Address/Subnet Mask	Management VLAN	STP	
1	eth0, eth1, AP0_0(Superwifi Network 0), AP1_0(Superwifi Network 0)	192.168.1.222/ 255.255.255.0	●	□	☒

Add VLAN...

Interfaces

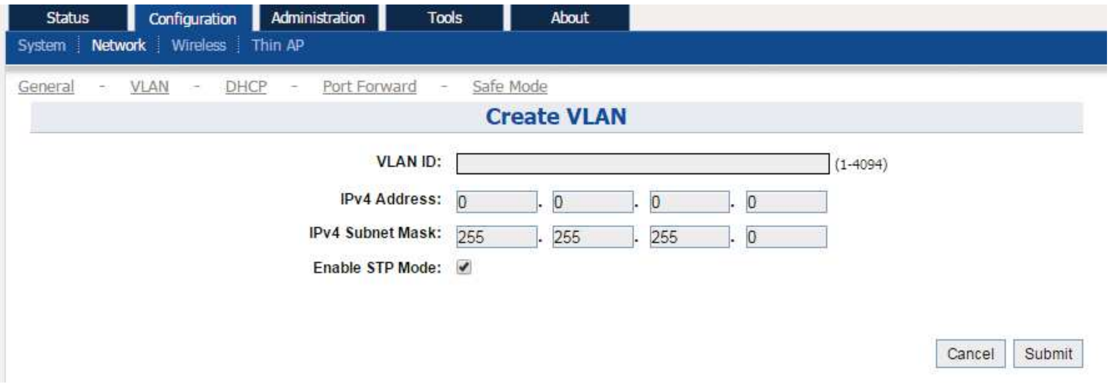
Interface	Type	PVID	Default VLAN Tagging	VLAN(s)	Edit
eth0	Trunk	1	□	all	Edit
eth1	Access	NA	NA	1	Edit
AP0_0(Superwifi Network 0)	Access	NA	NA	1	Edit
AP1_0(Superwifi Network 0)	Access	NA	NA	1	Edit

Submit

1. Go to **Configuration** > **Network** > **VLAN**
2. Click **Enable VLAN** checkbox to enable VLAN on CPE device
3. Click **Submit**

6.3 Create VLAN Profile

Figure 115 – VLAN Profile Setting



Create VLAN

VLAN ID: (1-4094)

IPv4 Address: 0 . 0 . 0 . 0

IPv4 Subnet Mask: 255 . 255 . 255 . 0

Enable STP Mode: ☑

1. Go to **Configuration** > **Network** > **VLAN** > **VLAN Profile**
2. Click **Add VLAN**
3. Enter an identification number between *1* and *4094* on **VLAN ID** that is an unique identification representing a VLAN
4. Enter valid IP Address on **IPv4 Address** of CPE device in the VLAN
5. Enter valid IP subnet mask on **IPv4 Subnet Mask** of the VLAN
6. Click **Enable STP Mode** checkbox to enable Spanning Tree Protocol (STP) on this VLAN profile
7. Click **Submit**

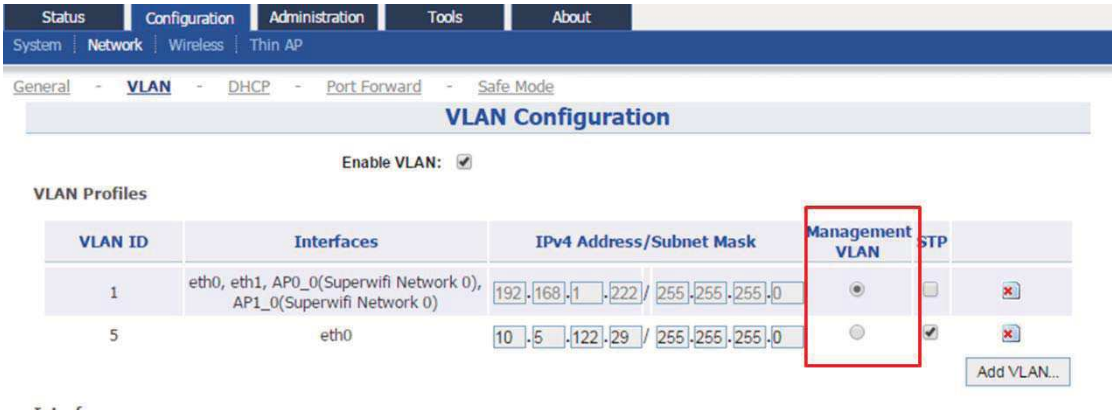
Note:

– *Click ☒ to remove the existing VLAN profile*

6.4 Specify Management VLAN Profile

Management VLAN stands for an IP network that can provide remote administration. Network administrator can access the Web UI via the management VLAN only if VLAN is enabled on CPE device.

Figure 116 – Management VLAN Setting


Status
Configuration
Administration
Tools
About
System | Network | Wireless | Thin AP
General - VLAN - DHCP - Port Forward - Safe Mode
Add VLAN...

VLAN Configuration

Enable VLAN: ☑

VLAN Profiles

VLAN ID	Interfaces	IPv4 Address/Subnet Mask	Management VLAN	STP	
1	eth0, eth1, AP0_0(Superwifi Network 0), AP1_0(Superwifi Network 0)	192.168.1.222/ 255.255.255.0	●	□	☒
5	eth0	10.5.122.29/ 255.255.255.0	○	☑	☒

1. Go to **Configuration** > **Network** > **VLAN** > **VLAN Profile**
2. Click **Management VLAN** checkbox on the row with appropriate VLAN ID
3. Click **Submit**

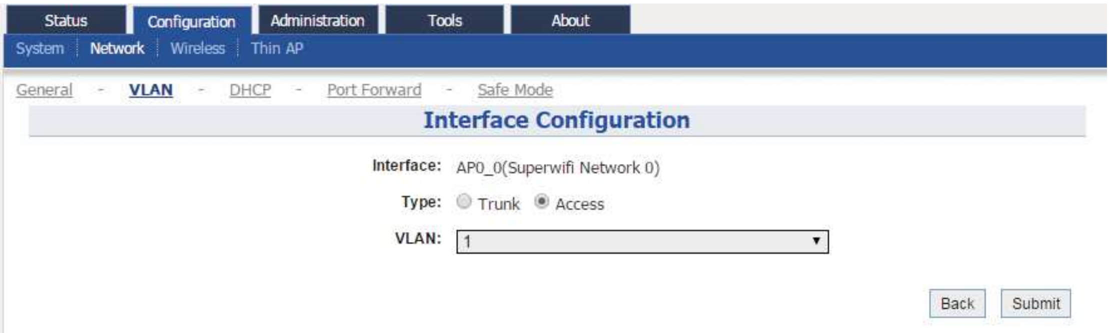
Note:

– *IP address of Management VLAN is same as IP address of WAN Setting*

6.5 Assign VLAN Profile on Interface as Access Port

Access port belongs to a single VLAN and does not provide any identifying marks on the frames that are passed between devices. Access port also carries traffic that comes from only the VLAN assigned to the port. Typically, interface that end-user device connects to is assigned as access port.

Figure 117 – VLAN Profile Assignment


Status
Configuration
Administration
Tools
About
System | Network | Wireless | Thin AP
General - VLAN - DHCP - Port Forward - Safe Mode
Back
Submit

Interface Configuration

Interface: AP0_0(Superwifi Network 0)

Type: ○ Trunk ● Access

VLAN: 1

1. Go to **Configuration** > **Network** > **VLAN** > **Interfaces**
2. Click Edit on the row with appropriate interface
3. Select **Access** checkbox

4. Select appropriate VLAN ID on **VLAN** that indicate which VLAN the interface belongs to
5. Click **Submit**

6.6 Assign VLAN Profile on Interface as Trunk Port

1. Go to **Configuration** > **Network** > **VLAN** > **Interfaces**
2. Click Edit on the row with appropriate interface
3. Select **Trunk** checkbox
4. Select appropriate VLAN ID on **PVID** as default VLAN ID of the interface
5. Click **Default VLAN Tagging** checkbox that CPE tags all incoming untagged packet with PVID before forwarding them. This entry is optional
6. Click **VLAN Pass Through** checkbox that CPE does not modify the VLAN tag on incoming packets before forwarding them. This entry is optional
7. Select appropriate VLAN ID(s) on the **VLAN(s)** list that interface forwards the packet with selected VLAN ID(s). Unlike **VLAN Pass Trough**, the interface only forwards the packets to selected VLAN.
8. Click **Submit**

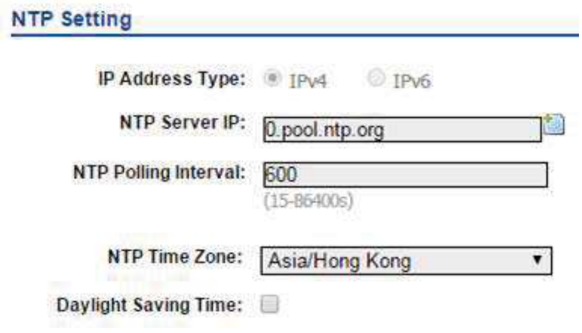
6.7 Apply Submitted VLAN Configurations on the CPE Device

1. Click **Save & Apply** from the top on the right.

7. Network Time Protocol (NTP) Settings

For successful and proper communication between various elements in a network, time synchronization between the elements and across the network is critical. Network Time Protocol (NTP), a networking protocol for clock synchronization, is required to obtain the precise time from a server and to regulate the local time in each network element. The NTP server on CPE devices is set to *0.pool.ntp.org* by default.

Figure 118 – NTP Setting



NTP Setting

IP Address Type: ● IPv4 ○ IPv6

NTP Server IP: 0.pool.ntp.org

NTP Polling Interval: 600 (15-86400s)

NTP Time Zone: Asia/Hong Kong ▼

Daylight Saving Time: □

1. Go to **Configuration** > **System** > **NTP Setting**
2. Enter either the domain name / IP address of NTP server which you want to synchronize with on **NTP Server IP**.

Note:

- Click ➕ for adding more NTP Server entry;
- Click ❌ to remove existing NTP server entry

3. Enter suitable polling interval between *15*s and *86400*s on **NTP Polling Interval** that specifies the interval between each synchronization request from the CPE device to NTP server(s). *600*s is default setting.
4. Select appropriate time zone on **NTP Time Zone**; *Asia/Hong Kong* is default setting
5. Click **Daylight Saving Time** checkbox if your place has daylight saving time
6. Click **Submit**
7. Click **Save & Apply** from the top on the right.

Note:

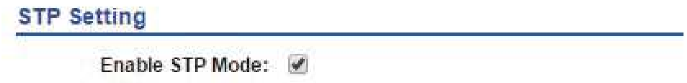
- ***IP Address Type** is changed by AP automatically based on whether **IPv6** is enabled or not*

– *If providing NTP server's domain name in* ***NTP Server IP****, you must provide valid DNS server information (Refer to* Assign an IP Address to CPE Device *on page 14 for more detail)*

8. STP

Spanning Tree Protocol (STP) is a network protocol that ensures a loop-free topology for any bridged Ethernet local area network.

Figure 119 – STP Setting


STP Setting

Enable STP Mode: ☑

1. Go to **Configuration** > **Network > General > STP Setting**
2. Select **Enable STP Mode** checkbox to enable spanning tree protocol on CPE device
3. Click **Submit**
4. Click **Save & Apply** from the top on the right.

9. Safe Mode

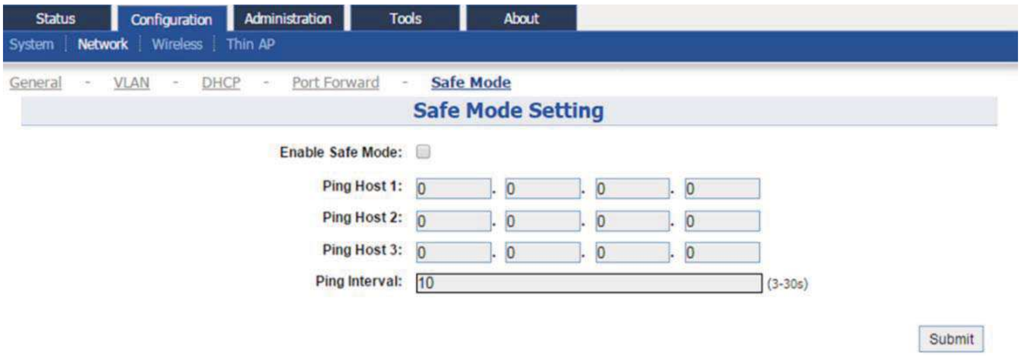
Safe Mode is used for detecting the backhaul link integrity. If the AP loses its backhaul connectivity, it forces the clients to re-associate with another AP by changing its SSID to a default Safe Mode_X, where X is the MAC address of the radio interface in hexadecimal.

This mechanism protects the client from connecting to the AP which has no backhaul to the Internet end. Total duration for AP from losing backhaul link to safe mode is 3 x ping interval seconds.

Note:

– CPE device recovers itself from safe mode if it detects the backhaul link had been recovered

Figure 120 – Safe Mode Setting


Status
Configuration
Administration
Tools
About
System | Network | Wireless | Thin AP
General - VLAN - DHCP - Port Forward - Safe Mode
Submit

Safe Mode Setting

Enable Safe Mode: □

Ping Host 1: 0 . 0 . 0 . 0

Ping Host 2: 0 . 0 . 0 . 0

Ping Host 3: 0 . 0 . 0 . 0

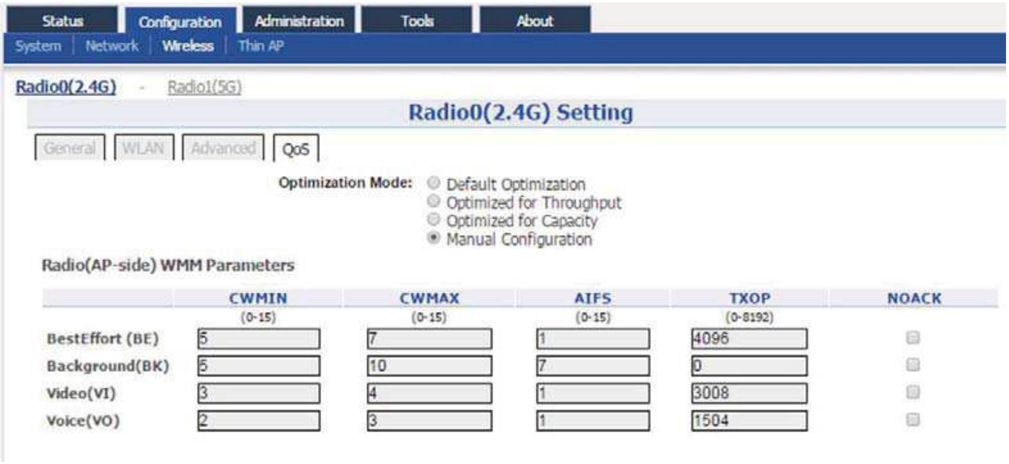
Ping Interval: 10 (3-30s)

1. Go to **Configuration** > **Network** > **Safe Mode**
2. Click **Enable Safe Mode** checkbox
3. Enter at least one IP address of remote host in **Ping Host 1 / Ping Host 2 / Ping Host 3**
4. Enter interval time between *3*s and *30*s in **Ping Interval**
5. Click **Submit**
6. Click **Save & Apply** from the top on the right

10. Quality of Service (QoS)

CPE supports Wireless Multimedia Extensions (WME), also known as Wi-Fi Multimedia (WMM), based on the IEEE 802.11e standard. It provides Quality of Service (QoS) feature on WiFi network. Network administrator can select the suitable per-defined profile or specify WMM parameters to maintain the network’s QoS.

Figure 121 – Quality of Service (WMM)



Radio0(2.4G) Setting

Optimization Mode: ○ Default Optimization ○ Optimized for Throughput ○ Optimized for Capacity ● Manual Configuration

Radio(AP-side) WMM Parameters

	CWMIN (0-15)	CWMAX (0-15)	AIFS (0-15)	TXOP (0-8192)	NOACK
BestEffort (BE)	5	7	1	4096	□
Background(BK)	5	10	7	0	□
Video(VI)	3	4	1	3008	□
Voice(VO)	2	3	1	1504	□

1. 2.4G Interface: Go to **Configuration** > **Wireless > Radio0(2.4G) > QoS**

5G Interface: Go to **Configuration** > **Wireless > Radio1(5G) > QoS**

2. Select suitable profile on **Optimization Mode**; options include:

Default Optimization – a set of QoS/WMM parameters for most scenarios; default setting

Optimized for Throughput – a set of QoS/WMM parameters for single user Wi-Fi network; Wi-Fi network achieves the highest throughput for a single user.

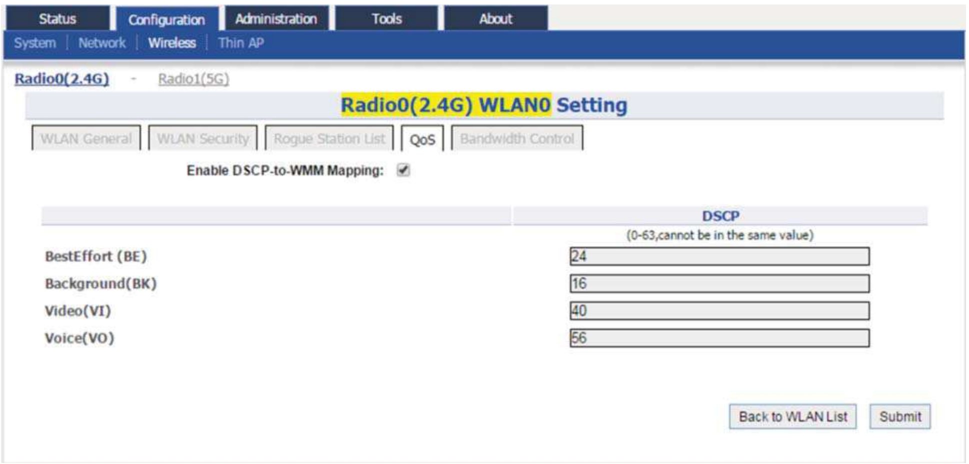
Optimized for Capacity – a set of QoS/WMM parameters for multi-user (>20) Wi-Fi network; Wi-Fi network can achieve highest system throughput for multiple users

Manual Configuration - Specify QoS/WMM parameters manually

3. Click **Submit**
4. Click **Save & Apply** from the top on the right

Except WMM settings on each CPE's radio interface, CPE also provide DSCP-to-WMM mapping on each individual SSID. Network administrator specifies different DSCP value on the four WMM access categories; they are Best Effort (BE), Background (BK), Video (VI), and Voice (VO).

Figure 122 – 2.4G WLAN # QoS



Radio0(2.4G) WLAN0 Setting

Enable DSCP-to-WMM Mapping: ☑

	DSCP (0-63,cannot be in the same value)
BestEffort (BE)	24
Background(BK)	16
Video(VI)	40
Voice(VO)	56

1. 2.4G Interface: Go to **Configuration** > **Wireless > Radio0(2.4G) > WLAN** > **WLAN # > QoS**

   5G Interface: Go to **Configuration** > **Wireless > Radio1(5G) > WLAN** > **WLAN # > QoS**

2. Select **Enable DSCP-to-WMM Mapping** checkbox that CPE provides different QoS to the incoming packet with the corresponding DSCP value
3. Enter DSCP value on **Best Effort (BE)**, **Background (BK)**, **Video (VI)**, and **Voice (VO)**; these entry is optional
4. Click **Submit**
5. Click **Save & Apply** from the top on the right

Note:

– CPE classify the packet without DSCP marking as Best Effort (BE) traffic

11. IP Gateway

To provide the flexibility on network deployment, CPE device can act as IP gateway on the network. IP Gateway is a network element that connects to two or more IP network physically, no matter via wire medium or wireless medium.

Note:

– *Interfaces under the same group work as switch interfaces. E.g. Ethernet 0 and WLAN 0 of Radio 1 are assigned as WAN, they forward packet between them based on MAC address.*

11.1. IP Gateway

➢ Step 1: Configure WAN IP Setting

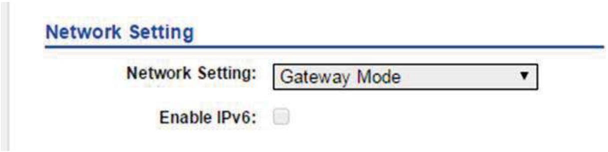
Refer to Assign an IP Address to CPE Device on page 14 for more detail

➢ Step 2: Configure Radio Settings

Please refer to Radios Setting on Page 17 to complete the radio settings

➢ Step 3: Enable Gateway Mode

Figure 123 – Network Setting



Network Setting

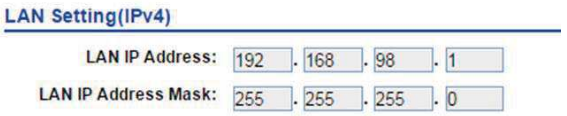
Network Setting: Gateway Mode ▼

Enable IPv6: □

1. Go to **Configuration** > **Network** > **Network Setting**
2. Select *Gateway Mode* on **Network Setting**
3. Click **Submit**

➢ Step 4: Configure LAN IP Setting

Figure 124 – LAN Setting (IPv4)



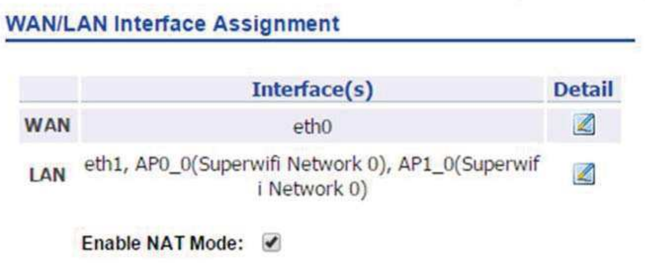
LAN Setting(IPv4)

LAN IP Address: 192 . 168 . 98 . 1

LAN IP Address Mask: 255 . 255 . 255 . 0

1. Go to **Configuration** > **Network** > **LAN Setting (IPv4)**
2. Enter valid IP Address on **LAN IP Address**; *192.168.98.1* is the default setting
3. Enter valid IP subnet mask on **LAN IP Subnet Mask**; 255.255.255.0 is default setting
4. Click **Submit**

Figure 125 – WAN/LAN Interface Assignment



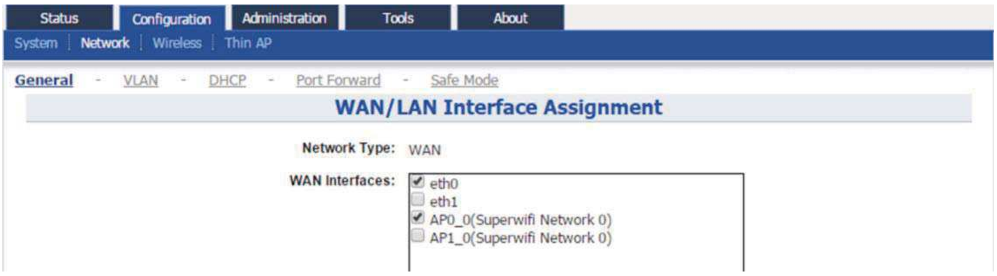
WAN/LAN Interface Assignment

	Interface(s)	Detail
WAN	eth0	✎
LAN	eth1, AP0_0(Superwifi Network 0), AP1_0(Superwifi Network 0)	✎

Enable NAT Mode: ☑

- Step 5: Assign Interface(s) as WAN Interface

Figure 126 – WAN Interface Assignment



WAN/LAN Interface Assignment

Network Type: WAN

WAN Interfaces:
☑ eth0
□ eth1
☑ AP0_0(Superwifi Network 0)
□ AP1_0(Superwifi Network 0)

1. Go to **Configuration** > **Network** > **WAN/LAN Interface Assignment**
2. Click ✎ at the end of **WAN** row
3. Select appropriate interface(s) on **WAN Interfaces** list that acts as WAN interface.
4. Click **Submit**

- Step 6: Assign Interface(s) as LAN Interface

1. Go to **Configuration** > **Network** > **WAN/LAN Interface Assignment**
2. Click ✎ at the end of **LAN** row
3. Select appropriate interface(s) on **LAN Interfaces** list that acts as WAN interface.
4. Click **Submit**

- Step 7: NAT Setting

1. Go to **Configuration** > **Network** > **WAN/LAN Interface Assignment**
2. Click Enable NAT Mode checkbox if NAT is required. This entry is optional
3. Click **Submit**

- Step 8: Apply Submitted Configurations on the CPE Device

1. Click **Save & Apply** from the top on the right.

11.2. DHCP Server

CPE series products have built-in DHCP server; it can dynamically distribute network configuration parameters to the connected end devices on all LAN interfaces.

Note:

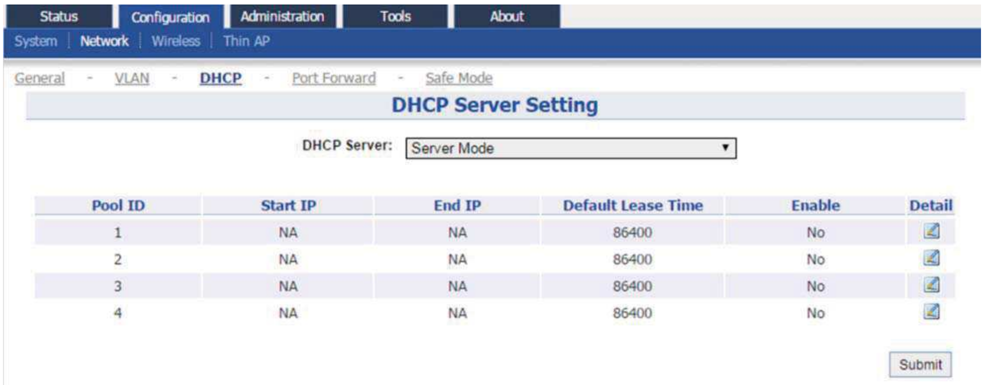
– *DHCP Server is applicable on Gateway mode ONLY*

➢ Step 1: Configure as Gateway Mode

Refer to IP Gateway on page 132 for more detail

➢ Step 2: Enable DHCP Server

Figure 127 – DHCP Server Setting


Status
Configuration
Administration
Tools
About
System | Network | Wireless | Thin AP
General - VLAN - DHCP - Port Forward - Safe Mode
Submit

DHCP Server Setting

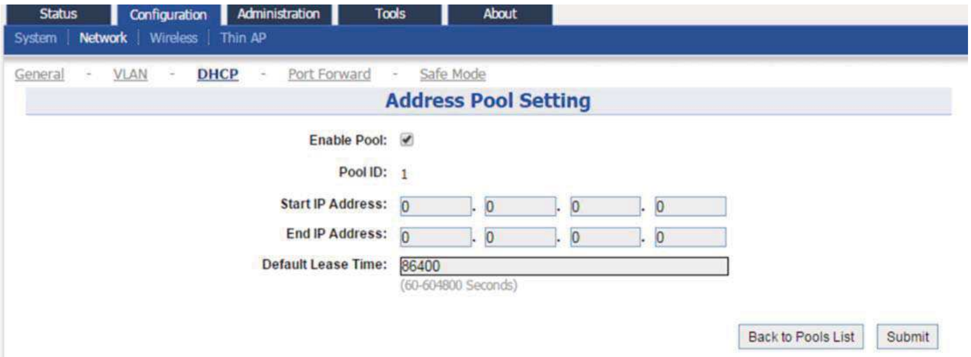
DHCP Server: Server Mode

Pool ID	Start IP	End IP	Default Lease Time	Enable	Detail
1	NA	NA	86400	No	✎
2	NA	NA	86400	No	✎
3	NA	NA	86400	No	✎
4	NA	NA	86400	No	✎

1. Go to **Configuration** > **Network** > **DHCP**
2. Select *Server Mode* on **DHCP Server**
3. Click **Submit**

➢ Step 3: Assign IP Address Range for Leasing on DHCP Server

Figure 128 – Address Pool Setting


Status
Configuration
Administration
Tools
About
System | Network | Wireless | Thin AP
General - VLAN - DHCP - Port Forward - Safe Mode
Back to Pools List
Submit

Address Pool Setting

Enable Pool: ☑

Pool ID: 1

Start IP Address: 0 . 0 . 0 . 0

End IP Address: 0 . 0 . 0 . 0

Default Lease Time: 86400
(60-604800 Seconds)

1. Go to **Configuration** > **Network** > **DHCP**
2. Click ✎ on any **Pool ID**
3. Click **Enable Pool** checkbox
4. Enter the first valid IP address on **Start IP Address**
5. Enter the last valid IP address on **End IP Address**
6. Enter lease time between *60*s and *604800*s on **Default Lease Time**; *86400*s is default setting.
7. Click **Submit**

Note:

– *All IP address for leasing MUST be within the LAN IP subnet (Refer to* Step 4: Configure LAN IP Setting *on page 132 for more detail)*

- Step 4: Apply Submitted Configurations on the CPE Device

1. Click **Save & Apply** from the top on the right.

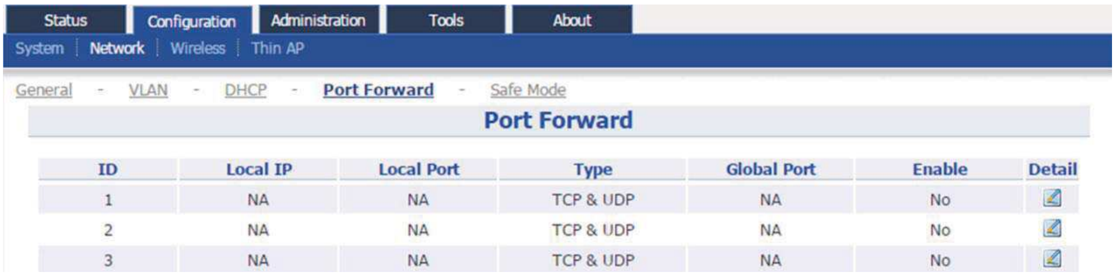
11.3. Port Forward

Port forward is an application of Network Address Translation (NAT) that redirects a communication request between WAN interface(s) and LAN interface(s) while the packets are traversing CPE device in gateway mode. This technique is most commonly used to make services on a host residing on LAN interface(s) available to hosts on WAN interface(s), by remapping the destination IP address and port number of the communication to a host on LAN side.

- Step 1: Configure as Gateway Mode

Refer to IP Gateway on page 132 for more detail

Figure 129 – Port Forward List

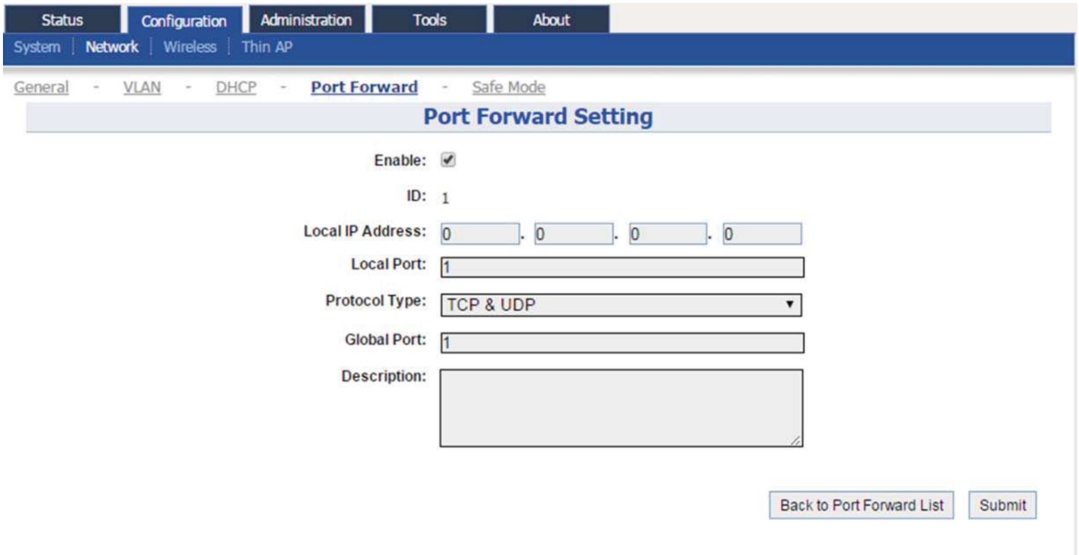


Port Forward

ID	Local IP	Local Port	Type	Global Port	Enable	Detail
1	NA	NA	TCP & UDP	NA	No	✎
2	NA	NA	TCP & UDP	NA	No	✎
3	NA	NA	TCP & UDP	NA	No	✎

- Step 2: Configure Port Forwarding

Figure 130 – Port Forward Setting


Status
Configuration
Administration
Tools
About
System | Network | Wireless | Thin AP
General - VLAN - DHCP - Port Forward - Safe Mode

Port Forward Setting

Enable:	☑
ID:	1
Local IP Address:	0 . 0 . 0 . 0
Local Port:	1
Protocol Type:	TCP & UDP ▾
Global Port:	1
Description:	

Back to Port Forward List | Submit

1. Go to **Configuration** > **Network** > **Port Forward**
2. Click 📝 on any **ID**
3. Click **Enable** checkbox to enable port forward profile
4. Enter the host’s IP address on **Local IP Address** that provides service to hosts on WAN interface(s)
5. Enter the service listening port of the host on **Local Port** that provides service to hosts on WAN interface(s)
6. Select suitable protocol(s) on **Protocol Type**. Options include

   TCP & UDP

   TCP

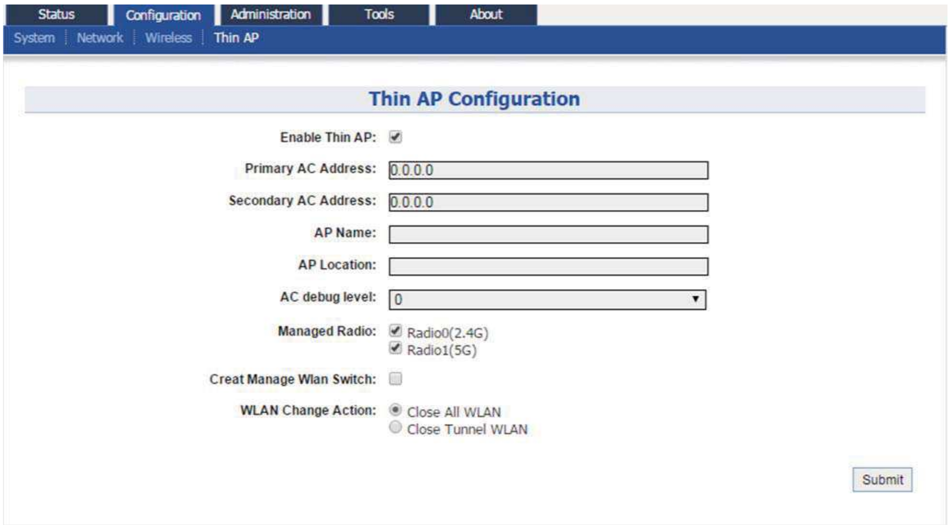
   UDP
7. Enter the listening port at WAN side on **Global Port**
8. Enter any description on **Description** about this port forward profile. This entry is optional.
9. Click **Submit**

➢ Step 3: Apply Submitted Configurations on the CPE Device

1. Click **Save & Apply** from the top on the right.

12. Thin AP

Figure 131 – Thin AP Setting



Thin AP Configuration

Enable Thin AP: ☑

Primary AC Address: 0.0.0.0

Secondary AC Address: 0.0.0.0

AP Name:

AP Location:

AC debug level: 0

Managed Radio: ☑ Radio0(2.4G) ☑ Radio1(5G)

Creat Manage Wlan Switch: □

WLAN Change Action: ● Close All WLAN ○ Close Tunnel WLAN

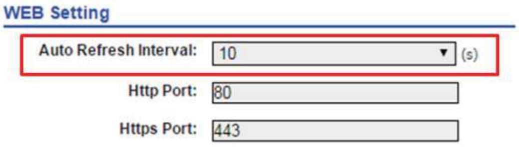
Thin AP stands for AP simply passes wireless network traffic to the switch, performing few complex tasks locally. All encryption, authentication, and policy settings generally occur on a central switch or controller, to which multiple thin access points are connected, rather than on the AP itself. Access controller or equivalent platform is required if thin AP is enabled

1. Go to **Configuration** > **Thin AP**
2. Select **Enable Thin AP** checkbox to enable thin AP mode
3. Enter valid IP Address / domain name of primary AC on **Primary AC Address**; CPE can also acquire AC's IP address from DHCP Server by DHCP options (DHCP option 60 or option 43) when it is configured as DHCP client**.**
4. Enter valid IP Address / domain name of secondary AC on **Secondary AC Address**; this entry is optional.
5. Enter name of AP on **AP Name**; this entry is optional
6. Enter information of AP's location on **AP Location**; this entry is optional
7. Select desired debug level from 0 to 10 on **AC debug level**;
8. Select Radio0(2.4G) and/or Radio1(5G) checkbox on **Managed Radio** that AC manages the selected radio interface(s)
9. Select **Creat Manage Wlan Switch** checkbox if a WLAN for AP management is required. Network administrator can manage AP via this WLAN even CPE disconnects from AC
10. Select *Close All WLAN* or *Close Tunnel WLAN* on **WLAN Change Action**. When CPE disconnects from AC, it disables either all WLAN or tunnel WLAN.
11. Click **Submit**
12. Click **Save & Apply**

13. Web UI Administration

13.1. Auto Refreshment

Figure 132 – Auto Refreshment Setting



WEB Setting

Auto Refresh Interval: 10 (s)

Http Port: 80

Https Port: 443

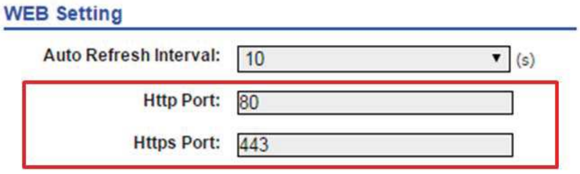
1. Click **Configuration** > **System** > **WEB Setting**
2. Select appropriate refresh interval on **Auto Refresh Interval** that Web UI refreshes itself automatically. Options include:

Disable	Refresh manually
5s	Refresh every 5 seconds
10s	Refresh every 10 seconds (Default Setting)
20s	Refresh every 20 seconds
30s	Refresh every 30 seconds
40s	Refresh every 40 seconds

3. Click **Submit**
4. Click **Save & Apply** from the top on the right

13.2. Web UI Port Configuration

Figure 133 – HTTP / HTTPS Port Setting



WEB Setting

Auto Refresh Interval: 10 (s)

Http Port: 80

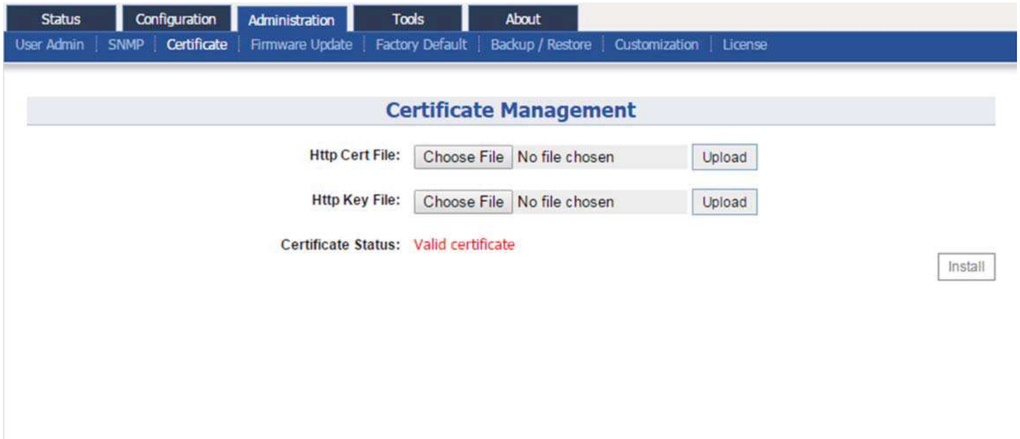
Https Port: 443

1. Click **Configuration** > **System** > **WEB Setting**
2. Enter suitable port number on **HTTP Port** for HTTP connection; *80* is default setting
3. Enter suitable port number on **HTTPS Port** for HTTPS connection; *433* is default setting
4. Click **Submit**
5. Click **Save & Apply** from the top on the right

13.3. HTTPS Certification

CPE devices support both HTTP and HTTPS connection for their web UI. Certificate management allows network administrator to upload their own certifications for HTTPS connection.

Figure 134 – Certificate Management



Certificate Management

Http Cert File: No file chosen

Http Key File: No file chosen

Certificate Status: Valid certificate

1. Go to **Administration** > **Certificate**
2. Click **Browse** on **Http Cert File** and select suitable certification file for HTTPS connection
3. Click **Upload** on **Http Cert File** to upload certification
4. Click **Browse** on **Http Key File** and select suitable certification file for HTTPS connection
5. Click **Upload** on **Http Key File** to upload certification
6. Click **Install**

Note:

- The existing certification file and key file will be overwritten for executing installation each time

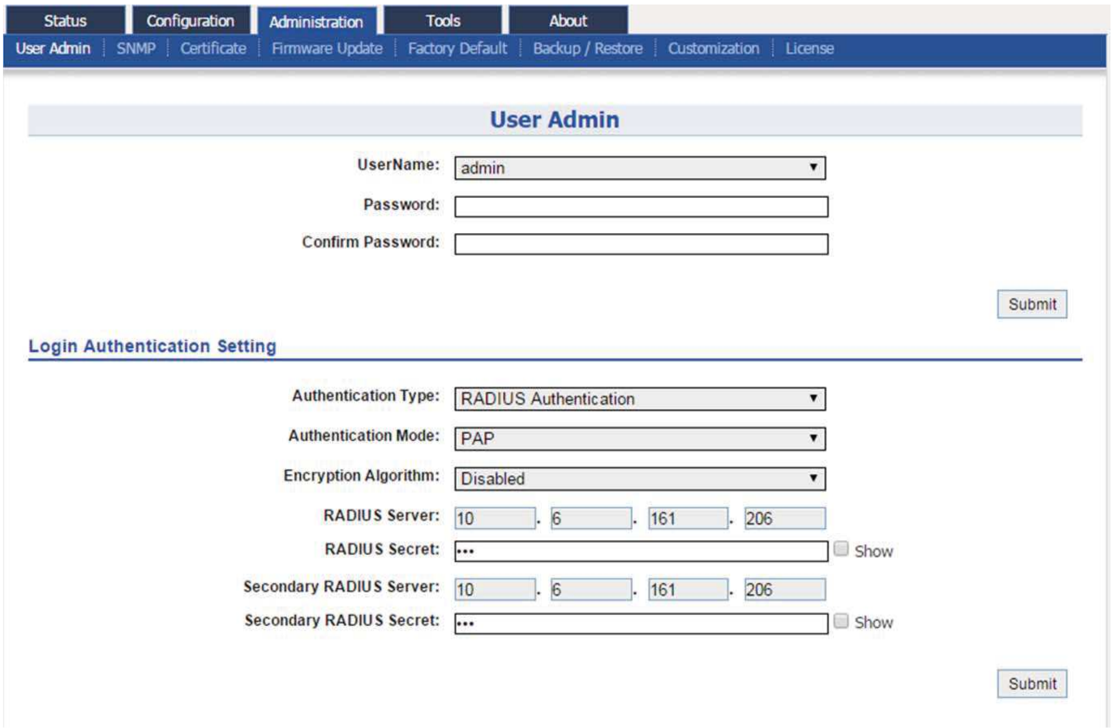
13.4. User Administration

CPE device allows network administrator to manage user account and privilege for accessing Web UI via local authentication and/or RADIUS authentication. Table 4 describes the authentication setting on CPE device.

Table 4 - Authentication setting on CPE device

Authentication	Description
Local (Default)	Support 3-level User Login (root/admin/guest)
RADIUS	Authenticate user through RADIUS; if no response returned from RADIUS server, AP fallbacks to local authentication
RADIUS + Local	Login AP with local user login or RADIUS user login

Figure 135 – User Admin Setting



UserName: admin
Password:
Confirm Password:

Login Authentication Setting

Authentication Type: RADIUS Authentication
Authentication Mode: PAP
Encryption Algorithm: Disabled
RADIUS Server: 10 . 6 . 161 . 206
RADIUS Secret: ••• □ Show
Secondary RADIUS Server: 10 . 6 . 161 . 206
Secondary RADIUS Secret: ••• □ Show

13.4.1 Local authentication

13.4.1.1 Modify admin account’s password

1. Go to **Administration** > **User Admin**
2. Select *admin* in **UserName**
3. Type a new password in **Password**
4. Type a new password again in **Confirm Password**
5. Click **Submit**

13.4.1.2 Modify guest account's password

1. Go to **Administration** > **User Admin**
2. Select *guest* in **UserName**
3. Type a new password in **Password**
4. Type a new password again in **Confirm Password**
5. Click **Submit**

Note:

- Please login as admin for modifying password

13.4.2 RADIUS authentication

1. Go to **Administration** > **User Admin > Login Authentication Setting**
2. Select *RADIUS authentication* or *RADIUS + Local authentication* in **Authentication Type**
3. Select suitable authentication in **Authentication Mode;** options include:

PAP

EAP

4. Select suitable encryption in **Encryption Algorithm;** options include:

For authentication Mode is *PAP:*

Disable

For authentication Mode is E*AP:*

PEAP-GTC

PEAP-MS-CHAP-V2

TTLS-PAP

TTLS-CHAP

TTLS-MS-CHAP

TTLS-MS-CHAP-V2

5. Enter IP address of remote RADIUS server in **RADIUS Server**
6. Enter suitable secrets in **Secret** of **RADIUS Secret.**
7. Left **Secondary RADIUS Server** blank if no backup RADIUS server is available

8. Left **Secondary RADIUS Secret** blank if no backup RADIUS server is available
9. Click **Submit**
10. Click **OK**

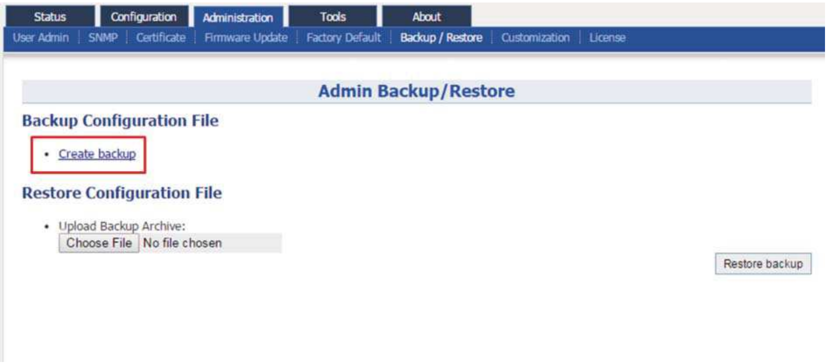
14. Device Configuration & Firmware Management

14.1. Backup & Restore Device Configuration

Network administrator backups / restores CPE device’s settings via web UI.

Backup Device Configuration

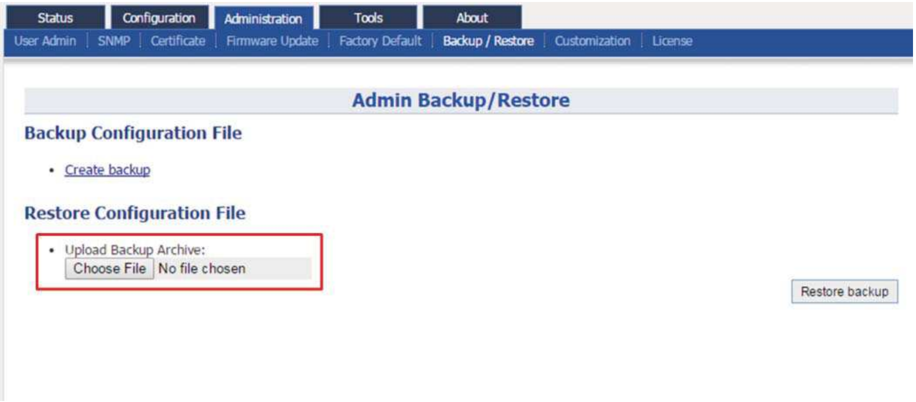
Figure 136 – Backup configuration



1. Go to **Administration** > **Backup/Restore > Backup Configuration File**
2. Click Create backup and save configuration file

Restore Device Configuration

Figure 137 – Restore configuration

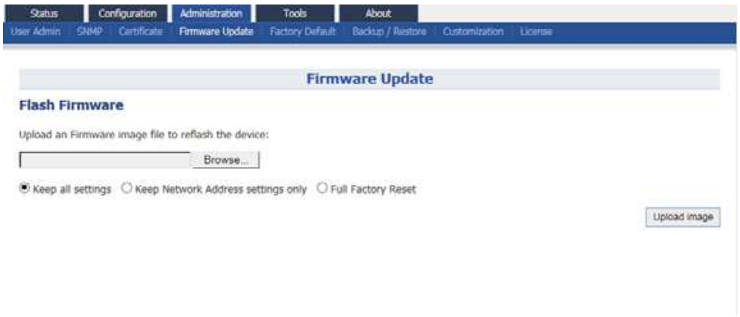


1. Go to **Administration** > **Backup/Restore > Restore Configuration File**
2. Click **Browse**, then select suitable configuration file (.tar.gz)
3. Click **Restore backup**

14.2. Firmware Update

Network administrator updates (upgrades or downgrades) CPE device’s firmware via web UI.

Figure 138 – Firmware Update



Firmware Update

Flash Firmware

Upload an Firmware image file to reflash the device:

● Keep all settings ○ Keep Network Address settings only ○ Full Factory Reset

1. Go to **Administration** > **Firmware Update**
2. Click **Browse**, then select suitable firmware image file (.bin)
3. Select the suitable options under the Browse button; options include

Keep all settings - Device keeps all operating setting after updating firmware

Keep Network Address settings only - Device keeps IP address, subnet mask only after updating firmware; the other settings will be restored as default settings

Full Factory Reset - Device restores all setting as default settings after updating firmware

4. Click **Upload Image**
5. If uploaded firmware image is valid, click **Proceed** to continue; otherwise, error message will be shown
6. Wait unit CPE completes updating firmware
7. Login with correct username and password, then check the firmware version on **About** > **Product Version**

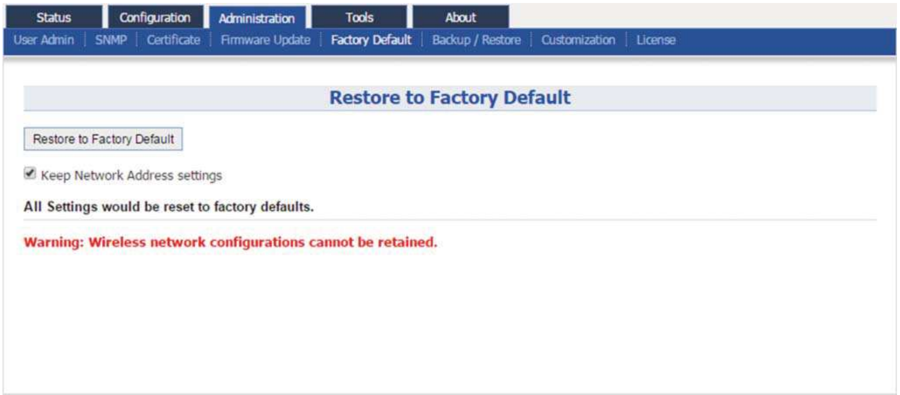
Caution:

- **Do not interrupt the process of firmware update. Please maintain network connection and power supply during updating firmware; otherwise CPE may not function.**

14.3. Factory Default

Network administrator restores CPE device's settings as default settings via web UI.

Figure 139 – Restore to Factory Default



Restore to Factory Default

Restore to Factory Default

☑ Keep Network Address settings

All Settings would be reset to factory defaults.

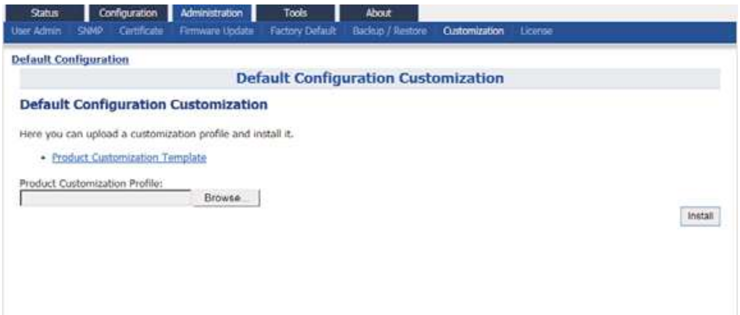
Warning: Wireless network configurations cannot be retained.

1. Go to **Administration** > **Factory Default**
2. Select **Keep Network Address settings** checkbox for keeping IP address and subnet mask settings; otherwise, deselect the checkbox
3. Click **Restore to Factory Default**

14.4. Factory Default Configuration Customization

Network administrator may create customized settings as factory default settings for CPE products. Once the customized configuration file is imported, CPE products restore with the customized settings as default settings rather than the original default settings.

Figure 140 – Default Configuration Customization



Default Configuration Customization

Default Configuration Customization

Here you can upload a customization profile and install it.

- Product Customization Template

Product Customization Profile: Browse...

Install

1. Go to **Administration** > **Customization > Default Configuration Customization**
2. Click Product Customization Template to download configuration template file (.tar.gz)
3. Use 7-zip software to open the template file, and edit the files in the factory_default.zip.
4. Edit system, network, and wireless files with the desired settings;

system	Contain settings about SNMP, syslog …etc
network	Contain network settings about all interfaces, such as IP address, VLAN enabling, and STP …etc.

wireless	Contain settings about radio interfaces, including radio enabling, WLAN settings … etc

5. Save the modified files
6. Go to **Administration** > **Customization > Default Configuration Customization**
7. Click **Browse**, then select the modified customization file
8. Click **Install**

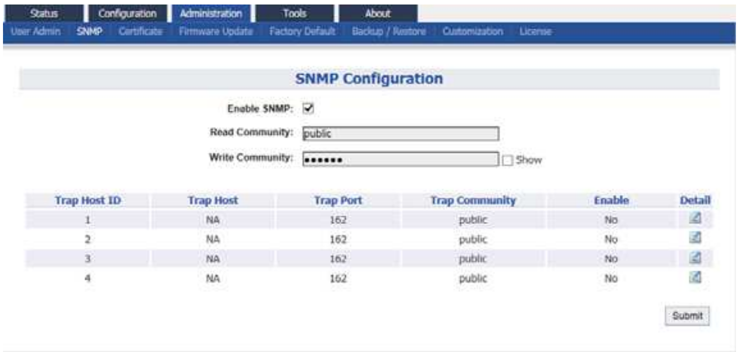
Caution:

- **Do not unzip the file during edit; otherwise, error may appear after uploading the customization file. 7-zip is recommended software to use in customization.**

15. SNMP

Simple Network Management Protocol (SNMP) is a Network management protocol used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.

Figure 141 – SNMP Setting



SNMP Configuration

Enable SNMP: ☑

Read Community: public

Write Community: •••••• □ Show

Trap Host ID	Trap Host	Trap Port	Trap Community	Enable	Detail
1	NA	162	public	No	📝
2	NA	162	public	No	📝
3	NA	162	public	No	📝
4	NA	162	public	No	📝

1. Go to **Administration** > **User Admin > SNMP**
2. Select **Enable SNMP** checkbox to enable SNMP function
3. Type in suitable string in **Read Community**; the string of **Read Community** between Network Manage System (NMS) and CPE must be identical, otherwise, NMS cannot get information from CPE. *public* is default setting.
4. Type in suitable string in **Write Community**; the string of **Write Community** between Network Manage System (NMS) and CPE must be identical, otherwise, NMS cannot modify CPE’s setting. *netman* is default setting.
5. Click **Submit**
6. Click **Save & Apply**

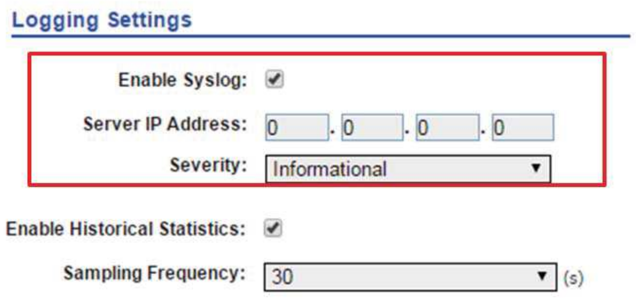
Note:

- CPE support up to four trap host at the same time. The information about trap hosts will be listed in the trap host table

16. Logging Configuration

16.1. System Logs

Figure 142 – Syslog Setting



Logging Settings

Enable Syslog: ☑

Server IP Address: 0 . 0 . 0 . 0

Severity: Informational

Enable Historical Statistics: ☑

Sampling Frequency: 30 (s)

1. Go to **Configuration** > **System** > **Logging Settings**
2. Select **Enable Syslog** checkbox to enable system logging function
3. Type in IP address of the remote syslog server that AP sends system logs instantaneously. *0.0.0.0 denote that AP saves the syslog in its local memory*
4. Specify severity level of log that AP stores / send to remote syslog server; options include:

Emergency - A "panic" condition usually affecting multiple apps/servers/sites. At this level it would usually notify all tech staff on call.

Alert - Should be corrected immediately, therefore notify staff who can fix the problem. An example would be the loss of a primary ISP connection.

Critical - Should be corrected immediately, but indicates failure in a secondary system, an example is a loss of a backup ISP connection

Error - Non-urgent failures, these should be relayed to developers or admins; each item must be resolved within a given time.

Warning - Warning messages, not an error, but indicate that an error will occur if action is not taken, e.g. file system 85% full - each item must be resolved within a given time.

Notice - Events that are unusual but not error conditions - might be summarized in an email to developers or admins to spot potential problems - no immediate action required.

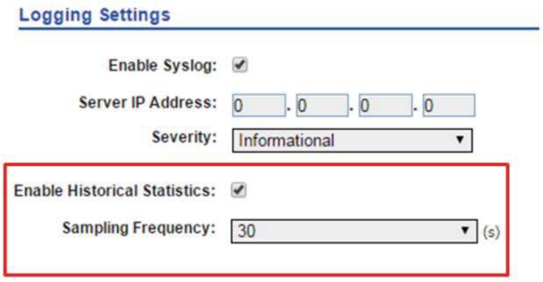
Informational - Normal operational messages - may be harvested for reporting, measuring throughput, etc. - no action required. (Default Setting)

Debug - Info useful to developers for debugging the application, not useful during operations.

5. Click **Submit**
6. Click **Save & Apply**

16.2. Historical Statistic

Figure 143 – Historical Statistics Setting



Logging Settings

Enable Syslog: ☑

Server IP Address: 0 . 0 . 0 . 0

Severity: Informational

Enable Historical Statistics: ☑

Sampling Frequency: 30 (s)

1. Go to **Configuration** > **System** > **Logging Settings**
2. Select **Enable Historical Statistics** checkbox to enable AP statistics function
3. Select the sampling time of statistics; options include:

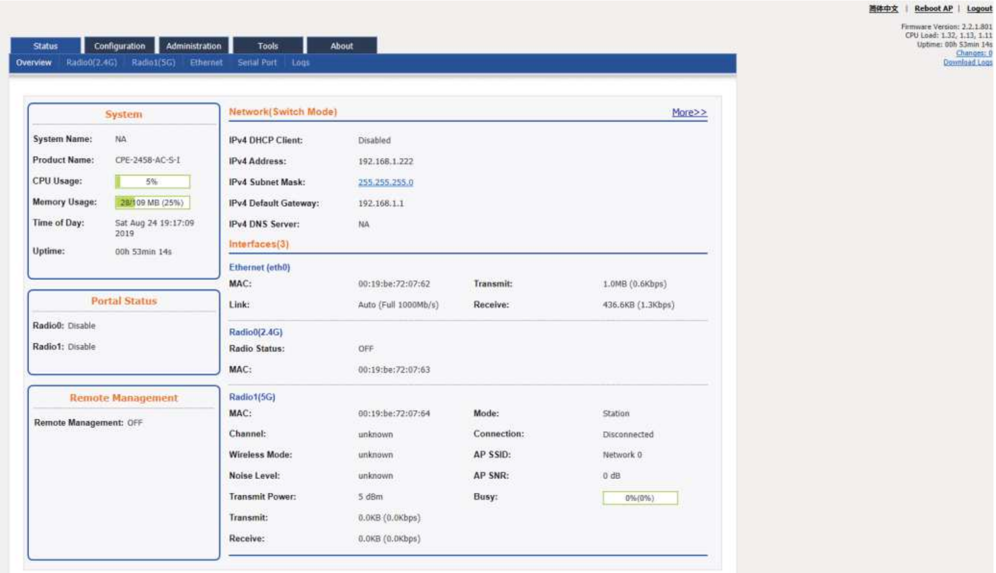
1s	1 second per sample
5s	5 second per sample
10s	10 second per sample
30s (Default Setting)	30 second per sample

4. Click **Submit**
5. Click **Save & Apply**

17. Monitor Your CPE Device

17.1. System Status Overview

Figure 144 – Status Overview



Firmware Version: 2.2.1.801
CPU Load: 1.32, 1.13, 1.11
Uptime: 00h 53min 14s
Changes: 0
Download Logs

System

System Name: NA
Product Name: CPE-2458-AC-S-I
CPU Usage: 5%
Memory Usage: 28/109 MB (25%)
Time of Day: Sat Aug 24 19:17:09 2019
Uptime: 00h 53min 14s

Portal Status

Radio0: Disable
Radio1: Disable

Remote Management

Remote Management: OFF

Network(Switch Mode)

IPv4 DHCP Client: Disabled
IPv4 Address: 192.168.1.222
IPv4 Subnet Mask: 255.255.255.0
IPv4 Default Gateway: 192.168.1.1
IPv4 DNS Server: NA

Interfaces(3)

Ethernet (eth0)

MAC:	00:19:be:72:07:62	Transmit:	1.0MB (0.6Kbps)
Link:	Auto (Full 1000Mb/s)	Receive:	436.6KB (1.3Kbps)

Radio0(2.4G)

Radio Status: OFF
MAC: 00:19:be:72:07:63

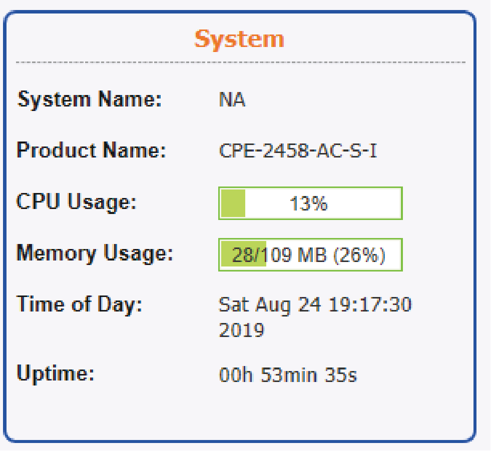
Radio1(5G)

MAC:	00:19:be:72:07:64	Mode:	Station
Channel:	unknown	Connection:	Disconnected
Wireless Mode:	unknown	AP SSID:	Network 0
Noise Level:	unknown	AP SNR:	0 dB
Transmit Power:	5 dBm	Busy:	0%(0%)
Transmit:	0.0KB (0.0Kbps)		
Receive:	0.0KB (0.0Kbps)		

Status overview provides the summary of vital information on the device's status. Information includes system status, thin AP status, network status, and interfaces status.

17.1.1 System Status

Figure 145 – System Status



System

System Name: NA
Product Name: CPE-2458-AC-S-I
CPU Usage: 13%
Memory Usage: 28/109 MB (26%)
Time of Day: Sat Aug 24 19:17:30 2019
Uptime: 00h 53min 35s

System status provides basic information and real time status of device.

System Name – Name represents the device in Wi-Fi network; it is customized by network administrator.

Product Name – Device's product name

CPU Usage – indicate that how many CPU resources the device is currently using

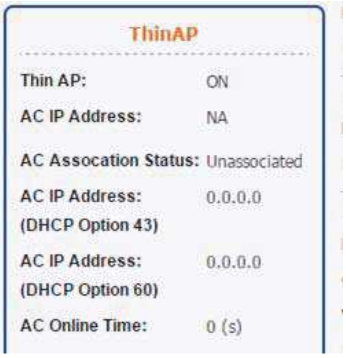
Memory Usage – indicate that how many memory resources the device is currently using

Time of Day – system time of device

Uptime – indicate operation time of device from last time boot up / reboot

17.1.2 Thin AP

Figure 146 – Thin AP Status



ThinAP

Thin AP: ON

AC IP Address: NA

AC Assocation Status: Unassociated

AC IP Address: (DHCP Option 43) 0.0.0.0

AC IP Address: (DHCP Option 60) 0.0.0.0

AC Online Time: 0 (s)

Thin AP - indicate status of thin AP feature

AC IP Address – indicate the controller's IP address that CPE connect

AC Association Status – indicate association status between controller and CPE

AC IP Address (DHCP Option 43) – indicate the controller's IP address that acquired from DHCP server with DHCP Option 43

AC IP Address (DHCP Option 60) – indicate the controller's IP address that acquired from DHCP server with DHCP Option 60

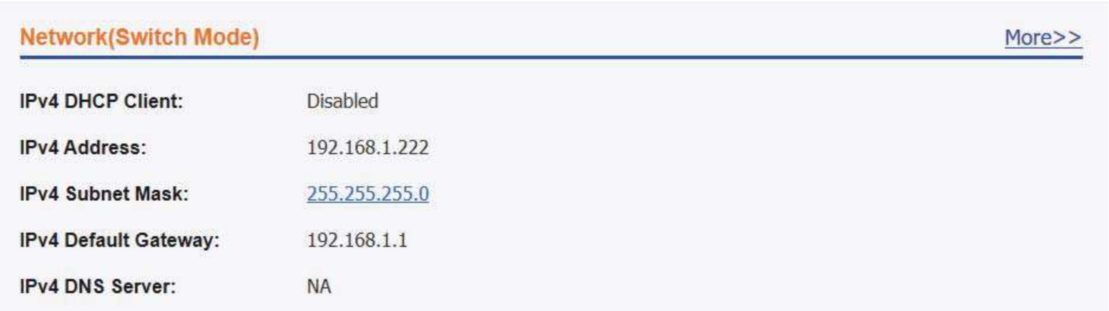
AC Online Time – indicate the AC online time

17.1.3 Networks

Networks provide basic information about Layer 3 status.

17.1.3.1 Switch Mode

Figure 147 – Network (Switch Mode)



Network(Switch Mode)

IPv4 DHCP Client: Disabled

IPv4 Address: 192.168.1.222

IPv4 Subnet Mask: 255.255.255.0

IPv4 Default Gateway: 192.168.1.1

IPv4 DNS Server: NA

IPv4 DHCP Client – indicate whether device's IP address is assigned by DHCP server or not

IPv4 Address – Current IPv4 address of device

IPv4 Subnet Mask – indicate the subnetwork device belongs to

IPv4 Default Gateway – indicate a node that helps device to another network.

IPv4 DNS Server - indicate a node that provides DNS service for the device

The following information is available if IPv6 option is enabled.

IPv6 DHCP Client – indicate whether device's IP address is assigned by IPv6 DHCP server or not

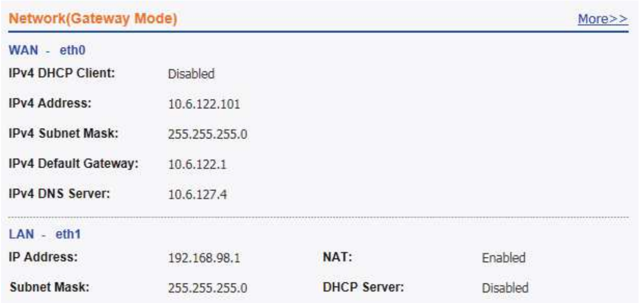
IPv6 Address – Current IPv6 address of device

IPv6 Default Gateway – indicate a node that helps device to another network.

IPv6 DNS Server - indicate a node that provides DNS service for the device

17.1.3.1 Gateway Mode

Figure 148 – Network (Gateway Mode)



Network(Gateway Mode)

WAN - eth0

IPv4 DHCP Client: Disabled

IPv4 Address: 10.6.122.101

IPv4 Subnet Mask: 255.255.255.0

IPv4 Default Gateway: 10.6.122.1

IPv4 DNS Server: 10.6.127.4

LAN - eth1

IP Address: 192.168.98.1 NAT: Enabled

Subnet Mask: 255.255.255.0 DHCP Server: Disabled

WAN Interface

IPv4 DHCP Client – indicate whether device's IP address is assigned by DHCP server or not

IPv4 Address – Current IPv4 address of device on WAN

IPv4 Subnet Mask – indicate the subnetwork device belongs to

IPv4 Default Gateway – indicate a node that helps device to another network.

IPv4 DNS Server - indicate a node that provides DNS service for the device

LAN Interface

IP Address - Current IP address of device on LAN

Subnet Mask – indicate the subnetwork device belongs to

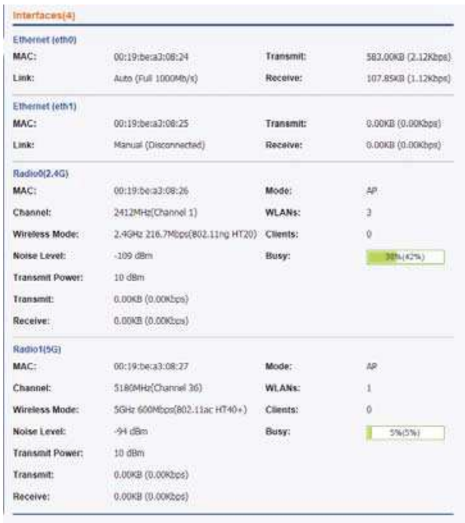
NAT – indicate whether device performs network address translation (NAT) or not

DHCP Server - indicate whether built-in DHCP server is enabled or not

17.1.4 Interfaces

Interfaces provide the real time status of all interfaces on the CPE device.

Figure 149 – Interfaces



Interfaces(4)

Ethernet (eth0)			
MAC:	00:19:be:a3:08:24	Transmit:	583.00KB (2.12Kbps)
Link:	Auto (Full 1000Mb/s)	Receive:	107.85KB (1.12Kbps)

Ethernet (eth1)			
MAC:	00:19:be:a3:08:25	Transmit:	0.00KB (0.00Kbps)
Link:	Manual (Disconnected)	Receive:	0.00KB (0.00Kbps)

Radio0(2.4G)			
MAC:	00:19:be:a3:08:26	Mode:	AP
Channel:	2412MHz(Channel 1)	WLANs:	3
Wireless Mode:	2.4GHz 216.7Mbps(802.11ng HT20)	Clients:	0
Noise Level:	-109 dBm	Busy:	38%(42%)
Transmit Power:	10 dBm		
Transmit:	0.00KB (0.00Kbps)		
Receive:	0.00KB (0.00Kbps)		

Radio1(5G)			
MAC:	00:19:be:a3:08:27	Mode:	AP
Channel:	5180MHz(Channel 36)	WLANs:	1
Wireless Mode:	5GHz 600Mbps(802.11ac HT40+)	Clients:	0
Noise Level:	-94 dBm	Busy:	5%(5%)
Transmit Power:	10 dBm		
Transmit:	0.00KB (0.00Kbps)		
Receive:	0.00KB (0.00Kbps)		

14.4.1.1 Ethernet (eth0) / Ethernet (eth1)

MAC – MAC address of Ethernet 0/1 interface

Link – indicate the status and operating mode of Ethernet 0/1

Transmit – indicate the traffic and instant throughput of transmission on Ethernet 0/1

Receive – indicate the traffic and instant throughput of receive operation on Ethernet 0 /1

Radio0 (2.4G) / Radio1 (5G)

MAC – MAC address of Radio 0 interface

Channel – indicate operating frequency (channel) of Radio 0/1

Wireless Mode – indicate 802.11 standards that Radio 0/1 operates

Noise Level – indicate the noise level in terms of dBm of operating channel

Transmission Power – indicate the total transmission power of Radio 0/1

Transmit – indicate the traffic and instant throughput of transmission on Radio 0/1

Receive – indicate the traffic and instant throughput of receive operation on Radio 0/1

Mode – indicate operating mode of Radio 0/1

WLANs - indicate the number of operating WLAN on Radio 0/1 (AP mode and Repeater Mode only)

Clients - indicate the number of clients that Radio 0/1 servers currently (AP mode and Repeater mode only)

Connection – indicate connection status between Radio 0/1 and remote AP (Station mode only)

AP SSID – indicate the SSID that station associates with (Station mode only)

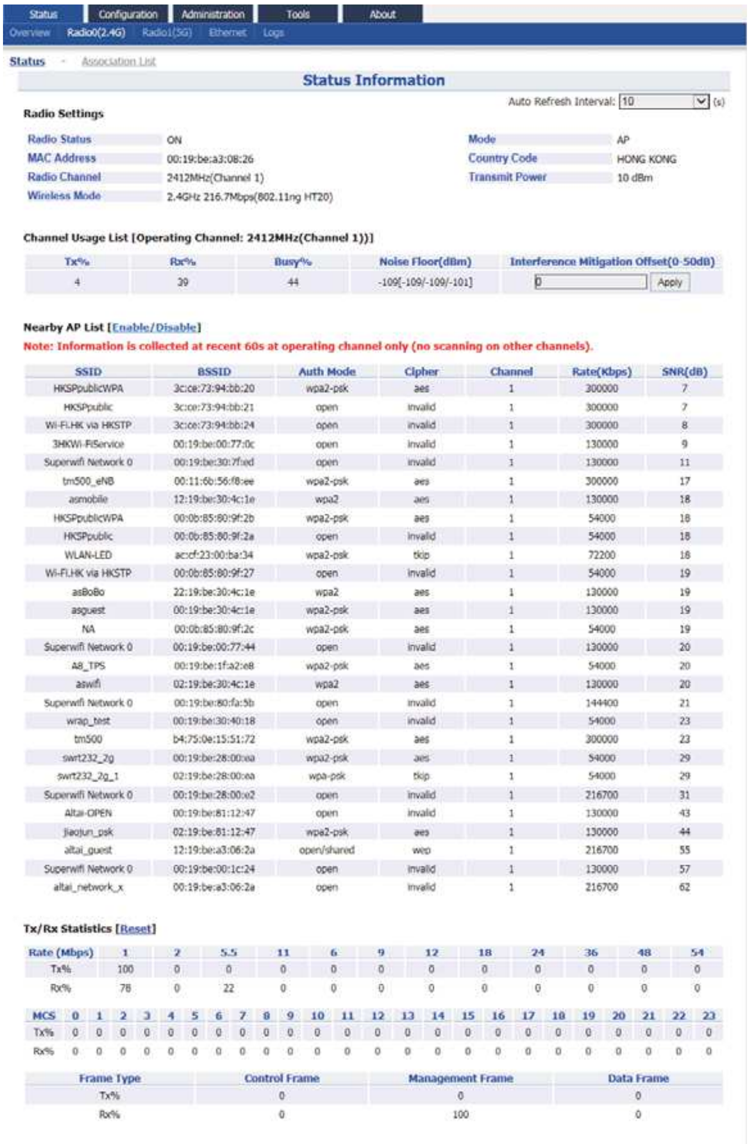
AP SNR – indicate received SNR from remote AP (Station mode only)

Busy – indicate busy of operating channel

17.2. Radio0 (2.4G) / Radio1 (5G) Status

17.2.1 Radio0 (2.4G) / Radio1 (5G) Status Information

Figure 150 – Radio0 (2.4G) Status Information



Status Information

Auto Refresh Interval: 10 (s)

Radio Settings

Radio Status	ON	Mode	AP
MAC Address	00:19:be:a3:08:26	Country Code	HONG KONG
Radio Channel	2412MHz(Channel 1)	Transmit Power	10 dBm
Wireless Mode	2.4GHz 216.7Mbps(802.11ng HT20)		

Channel Usage List [Operating Channel: 2412MHz(Channel 1))]

Tx%	Rx%	Busy%	Noise Floor(dBm)	Interference Mitigation Offset(0-50dB)
4	39	44	-109[-109/-109/-101]	0 Apply

Nearby AP List [Enable/Disable]

Note: Information is collected at recent 60s at operating channel only (no scanning on other channels).

SSID	BSSID	Auth Mode	Cipher	Channel	Rate(Kbps)	SNR(dB)
HKSPpublicWPA	3c:ce:73:94:bb:20	wpa2-psk	aes	1	300000	7
HKSPpublic	3c:ce:73:94:bb:21	open	invalid	1	300000	7
Wi-Fi.HK via HKSTP	3c:ce:73:94:bb:24	open	invalid	1	300000	8
3HKWi-FiService	00:19:be:00:77:0c	open	invalid	1	130000	9
Superwifi Network 0	00:19:be:30:7f:ed	open	invalid	1	130000	11
tm500_eNB	00:11:6b:56:f8:ee	wpa2-psk	aes	1	300000	17
asmobile	12:19:be:30:4c:1e	wpa2	aes	1	130000	18
HKSPpublicWPA	00:0b:85:80:9f:2b	wpa2-psk	aes	1	54000	18
HKSPpublic	00:0b:85:80:9f:2a	open	invalid	1	54000	18
WLAN-LED	ac:cf:23:00:ba:34	wpa2-psk	tkip	1	72200	18
Wi-Fi.HK via HKSTP	00:0b:85:80:9f:27	open	invalid	1	54000	19
asBoBo	22:19:be:30:4c:1e	wpa2	aes	1	130000	19
asguest	00:19:be:30:4c:1e	wpa2-psk	aes	1	130000	19
NA	00:0b:85:80:9f:2c	wpa2-psk	aes	1	54000	19
Superwifi Network 0	00:19:be:00:77:44	open	invalid	1	130000	20
A8_TPS	00:19:be:1f:a2:e8	wpa2-psk	aes	1	54000	20
aswifi	02:19:be:30:4c:1e	wpa2	aes	1	130000	20
Superwifi Network 0	00:19:be:80:fa:5b	open	invalid	1	144400	21
wrap_test	00:19:be:30:40:18	open	invalid	1	54000	23
tm500	b4:75:0e:15:51:72	wpa2-psk	aes	1	300000	23
swrt232_2g	00:19:be:28:00:ea	wpa2-psk	aes	1	54000	29
swrt232_2g_1	02:19:be:28:00:ea	wpa-psk	tkip	1	54000	29
Superwifi Network 0	00:19:be:28:00:e2	open	invalid	1	216700	31
Altai-OPEN	00:19:be:81:12:47	open	invalid	1	130000	43
jiaojun_psk	02:19:be:81:12:47	wpa2-psk	aes	1	130000	44
altai_guest	12:19:be:a3:06:2a	open/shared	wep	1	216700	55
Superwifi Network 0	00:19:be:00:1c:24	open	invalid	1	130000	57
altai_network_x	00:19:be:a3:06:2a	open	invalid	1	216700	62

Tx/Rx Statistics [Reset]

Rate (Mbps)	1	2	5.5	11	6	9	12	18	24	36	48	54
Tx%	100	0	0	0	0	0	0	0	0	0	0	0
Rx%	78	0	22	0	0	0	0	0	0	0	0	0

MCS	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Tx%	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Rx%	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Frame Type	Control Frame	Management Frame	Data Frame
Tx%	0	0	0
Rx%	0	100	0

17.2.1.1 Radio Settings

Radio Status – indicate the current status of Radio 0/1 interface

MAC – MAC address of Radio 0/1 interface

Radio Channel - indicate operating frequency (channel) of Radio 0/1

Wireless Mode – indicate 802.11 standards that Radio 0/1 operates

Mode – indicate operating mode of Radio 0/1

Country Code – indicate country code setting of Radio 0/1

Transmission Power – indicate the total transmission power of Radio 0/1

17.2.1.2 Channel Usage List

Tx(%) – average transmit frames percentage of operating channel

Rx(%) – average receive frames percentage of operating channel

Busy (%) – average busy state percentage of operating channel

Noise Floor (dBm) – indicate noise floor of operating channel and noise floor of chain 0, chain 1, and chain 2 on the control channel; if operating with 40MHz bandwidth, it shows the noise floor of chain 0, chain 1, and chain 2 on the extension channel as well.

Interference Mitigation Offset (0-50dB) – signal offset option that will mask all noise / valid signal below *0-50* dB; *0* denotes disabled

17.2.1.3 Nearby AP List

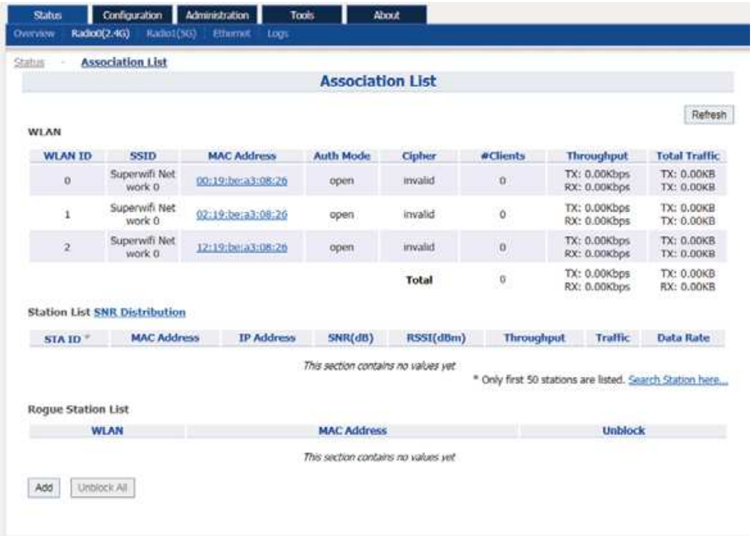
If Nearby AP List is enabled, device collects nearby AP information and builds Nearby AP List from all beacon frames received during operation. Information shows the SSID, BSSID, authentication mode, cipher mode, operating channel, data rate, and received SNR of collected APs.

17.2.1.4 Tx/Rx Statistics

This statistic shows traffic distribution about Radio 0/1 interface. The statistical data includes distribution in terms of data rate and frame type for all incoming and outgoing data frame via Radio 0/1 interface.

17.2.2 Radio0 (2.4G) / Radio1 (5G) Association List

Figure 151 – Radio0 (2.4G) Association List



Association List

WLAN

WLAN ID	SSID	MAC Address	Auth Mode	Cipher	#Clients	Throughput	Total Traffic
0	Superwifi Network 0	00:19:be:a3:08:26	open	invalid	0	TX: 0.00Kbps RX: 0.00Kbps	TX: 0.00KB TX: 0.00KB
1	Superwifi Network 0	02:19:be:a3:08:26	open	invalid	0	TX: 0.00Kbps RX: 0.00Kbps	TX: 0.00KB TX: 0.00KB
2	Superwifi Network 0	12:19:be:a3:08:26	open	invalid	0	TX: 0.00Kbps RX: 0.00Kbps	TX: 0.00KB TX: 0.00KB
				Total	0	TX: 0.00Kbps RX: 0.00Kbps	TX: 0.00KB RX: 0.00KB

Station List SNR Distribution

STA ID *	MAC Address	IP Address	SNR(dB)	RSSI(dBm)	Throughput	Traffic	Data Rate

This section contains no values yet

* Only first 50 stations are listed. Search Station here...

Rogue Station List

WLAN	MAC Address	Unblock

This section contains no values yet

Add Unblock All

17.2.2.1 WAN

It shows the current status of all operating WLAN on Radio 0/1 interface. The information includes WLAN ID, SSID, MAC Address, authentication mode, cipher mode, number of associated clients, instant throughput, and total traffic of each operating WLAN respectively.

17.2.2.2 Station List

It shows the real time status of first 50 associated stations. The status includes Station ID, MAC Address, IP address, SNR(dB) of uplink, RSSI (dBm) of uplink, instant throughput, cumulated traffic of uplink and downlink, and instant data rate of uplink and downlink for each associated station respectively.

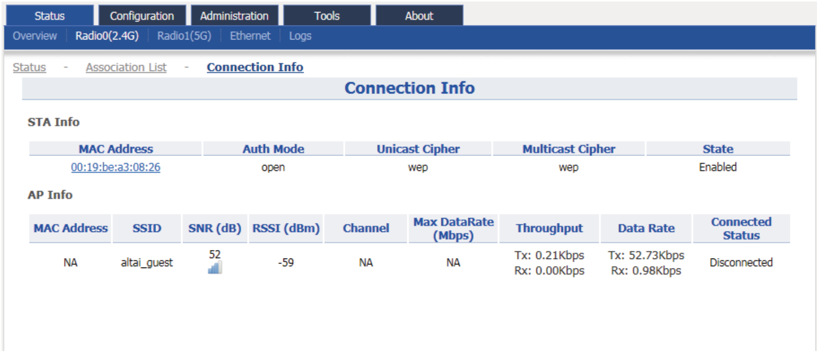
17.2.2.3 Rouge Station List

It lists out the stations that can potentially disrupt wireless networks and can sometimes cause irrevocable damage to the network owners. Network administrator inputs the rogue station’s MAC address manually or selects any station from the station List by clicking 👤.

17.2.3 Radio0 (2.4G) / Radio1 (5G) Connection Info

This information is available on Station mode and Repeater mode only.

Figure 152 – Radio0 (2.4G) Connection Info



Connection Info

STA Info

MAC Address	Auth Mode	Unicast Cipher	Multicast Cipher	State
00:19:be:a3:08:26	open	wep	wep	Enabled

AP Info

MAC Address	SSID	SNR (dB)	RSSI (dBm)	Channel	Max DataRate (Mbps)	Throughput	Data Rate	Connected Status
NA	altai_guest	52	-59	NA	NA	Tx: 0.21Kbps Rx: 0.00Kbps	Tx: 52.73Kbps Rx: 0.98Kbps	Disconnected

17.2.3.1 STA Info

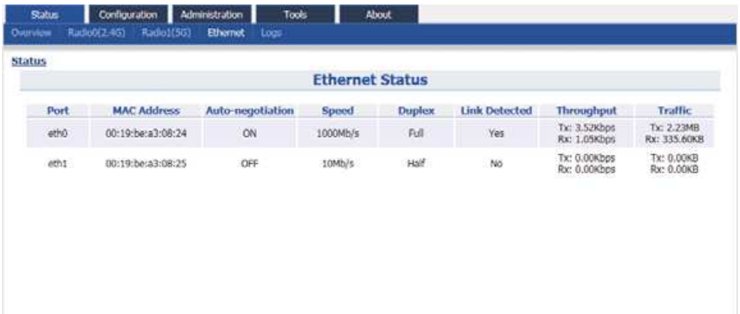
It shows station information on Radio 0. The information includes MAC Address, Authentication Mode, Unicast Cipher, Multicast Cipher, and State.

17.2.3.2 AP Info

It shows remote AP information on Radio 0. The information includes MAC Address, SSID, SNR (dB), RSSI (dBm), Channel, Max Data Rate, Throughput of uplink and downlink, Data Rate of uplink and downlink, and Connected Status.

17.3. Ethernet Status

Figure 153 – Ethernet Status



Ethernet Status

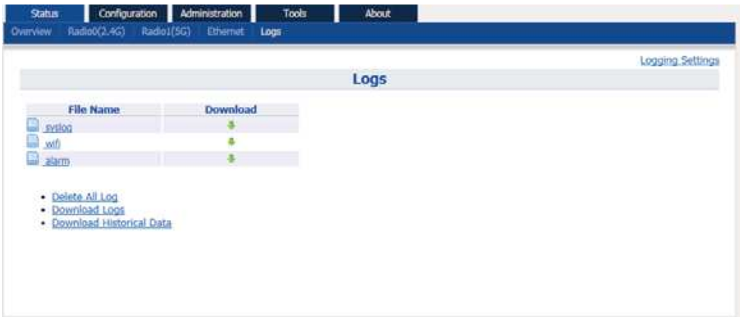
Port	MAC Address	Auto-negotiation	Speed	Duplex	Link Detected	Throughput	Traffic
eth0	00:19:be:a3:08:24	ON	1000Mb/s	Full	Yes	Tx: 3.52Kbps Rx: 1.05Kbps	Tx: 2.23MB Rx: 335.60KB
eth1	00:19:be:a3:08:25	OFF	10Mb/s	Half	No	Tx: 0.00Kbps Rx: 0.00Kbps	Tx: 0.00KB Rx: 0.00KB

It shows the current status of Ethernet interfaces. The information includes Port, MAC Address, Auto-negotiation, Speed, Duplex, Link Detected, instant throughput of uplink and downlink and traffic of of uplink and downlink on Ethernet 0 and Ethernet 1 respectively.

18. Tools for Deployment / Operation / Troubleshooting

18.1. System Logs

Figure 154 –Logs



Logs

File Name	Download
syslog	⬇
wifi	⬇
alarm	⬇

- Delete All Log
- Download Logs
- Download Historical Data

In order to realize easier monitoring and diagnosis, CPE products provide log function for system information, association activity, and alarm event.

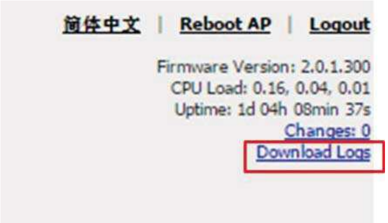
syslog – records the information about system information, such as software, hardware, system configuration, and self-checking result

wifi – records the information about association activity, such as association, dissociation, and roaming event

alarm – records the alert information of CPE device, such as radio down, too high CPU usage

Download system logs

Figure 155 – Download Logs



Firmware Version: 2.0.1.300
CPU Load: 0.16, 0.04, 0.01
Uptime: 1d 04h 08min 37s
Changes: 0
Download Logs

1. Click Download Logs from the top on the right

OR

1. Go to **Status** > **Logs**
2. Click Download Logs

18.2. Historical Statistic

Network administrator and engineer monitor collect the historical statistical data about system, interfaces, wireless condition, and wireless client information from CPE

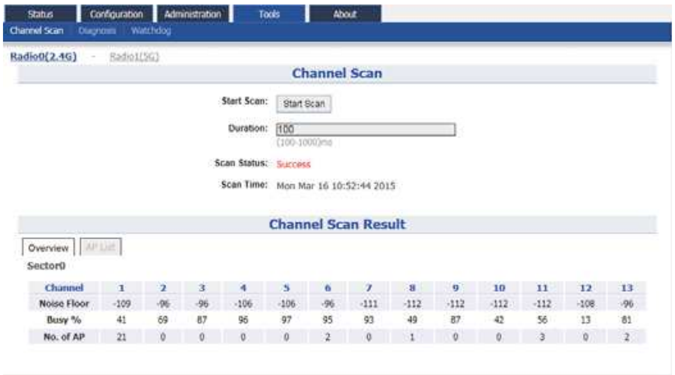
Download historical statistical data

1. Go to **Status** > **Logs**
2. Click Download Historical Data

18.3. Channel Scan

Network administrator and engineer collect the status of 2.4GHz radio and 5GHz radio in the surrounding area. Throughout this tool, network administrator and engineer collect noise floor, percentage of channel busy, and the number of BSS in particular radio channels.

Figure 156 – Channel Scan Result (Overview)



Channel Scan

Start Scan: Start Scan

Duration: 100 (100-1000)ms

Scan Status: Success

Scan Time: Mon Mar 16 10:52:44 2015

Channel Scan Result

Sector0

Channel	1	2	3	4	5	6	7	8	9	10	11	12	13
Noise Floor	-109	-96	-96	-106	-106	-96	-111	-112	-112	-112	-112	-108	-96
Busy %	41	69	87	96	97	95	93	49	87	42	56	13	81
No. of AP	21	0	0	0	0	2	0	1	0	0	3	0	2

CPE shows the channel scan result into Overview tab and AP List tab.

Overview Tab – displays general information from channel 1 to channel 11. Information includes noise floor, percentage of channel busy, and the number of BSS on each channel respectively.

AP List Tab - displays information scanned WLAN; information includes SSID, BSSID, authentication Mode, cipher, channel, rate in kbps, and received SNR (dB)

1. 2.4G Radio: Go to **Tools** > **Channel Scan > Radio0(2.4G)**

   5G Radio: Go to **Tools** > **Channel Scan > Radio1(5G)**
2. Enter scan interval from 100ms to 1000ms in **Duration**; this entry is optional
3. Click **Start Scan**
4. Wait until Scan Status is changed from *In Process* to *Success*; it will take for 20 seconds approximately

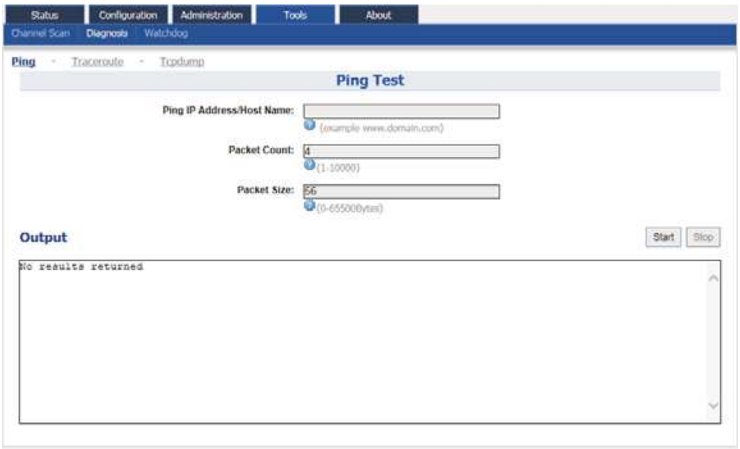
Note:

- Wi-Fi service will be interrupted during channel scan

18.4. Ping Test

Network administrator and engineer test the reachability of a host and measures the round-trip time between CPE and the host over an Internet Protocol (IP) network by using ping tool.

Figure 157 – Ping Test



Ping Test

Ping IP Address/Host Name:
(example www.domain.com)

Packet Count: 4
(1-10000)

Packet Size: 56
(0-65500Bytes)

Output

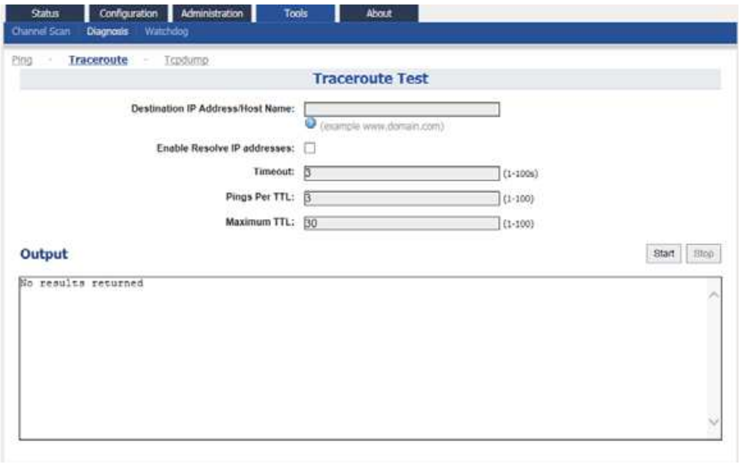
```
No results returned
```

1. Go to **Tools** > **Diagnosis** > **Ping**
2. Type target IP address / host name in **Ping IP Address/Host Name**
3. Specify how many ICMP (ping) packet that CPE sends to the target host in **Packet Count***; 4* is default setting. This entry is optional.
4. Specify the packet size of ICMP packet in **Packet Size**; *56* is default setting. This entry is optional.
5. Click **Start**
6. Click **Stop** to terminate ping test if necessary

18.5. Traceroute Test

Network administrator tests the route (path) and measuring transit delays of packets across an Internet Protocol (IP) network by using traceroute test.

Figure 158 – Tracerout Test



Traceroute Test

Destination IP Address/Host Name:
(example www.domain.com)

Enable Resolve IP addresses: □

Timeout: 3 (1-100s)

Pings Per TTL: 3 (1-100)

Maximum TTL: 30 (1-100)

Output

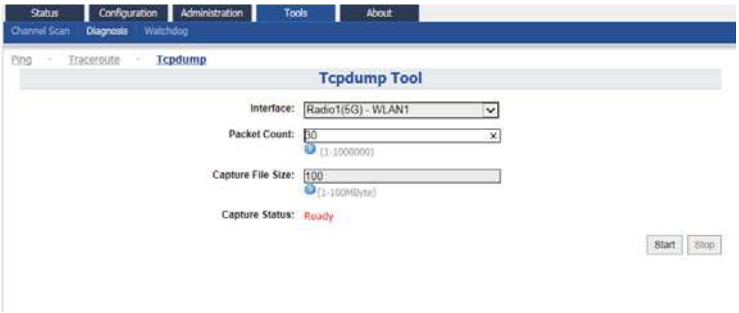
```
No results returned
```

1. Go to **Tools** > **Diagnosis** > **traceroute**
2. Type target IP address / host name in **Destination IP Address/Host Name**
3. Click **Enable Resolve IP addresses** checkbox to enable IP address to domain name translation; this entry is optional
4. Specify timeout interval between *1*s and *100*s in **Timeout** for traceroute test; this entry is optional
5. Specify TTL value between *1* and *100* in **Pings Per TTL**; *3* is default setting. This entry is optional
6. Specify TTL value between *1* and *100* in **Maximum TTL**; *30* is default setting. This entry is optional
7. Click **Start**
8. Click **Stop** to terminate ping test if necessary

18.6. Tcpdump

CPE provides a tool to capture packets that passing through a particular interface. It helps network administrator for troubleshooting.

Figure 159 – Tcpdump Tool



Tcpdump Tool

Interface: Radio1(5G) - WLAN1

Packet Count: 30 (1-1000000)

Capture File Size: 100 (1-100MByte)

Capture Status: Ready

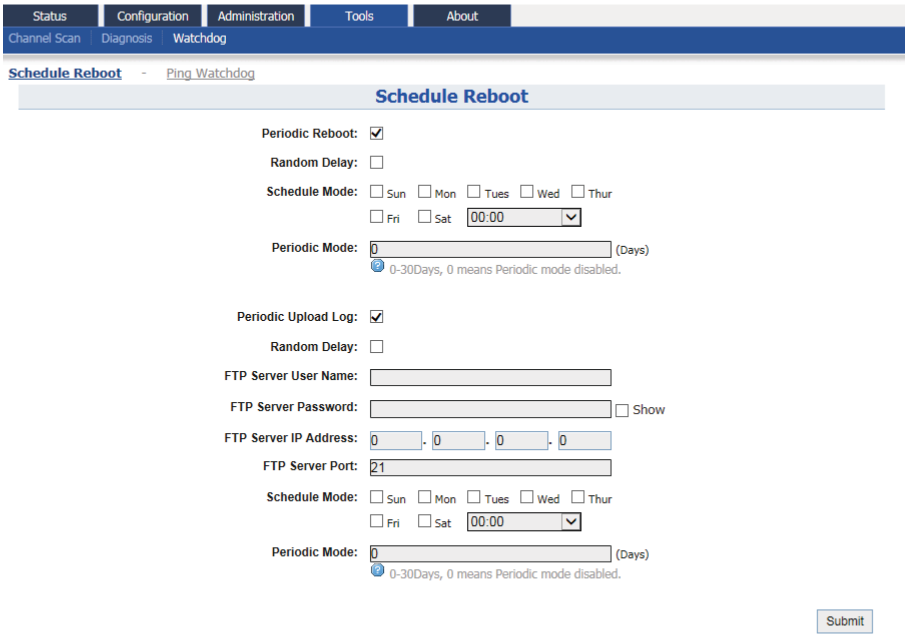
1. Go to **Tools** > **Diagnosis** > **Tcpdump**
2. Select suitable interface in **Interface**
3. Specify maximum number of packet in **Packet Count**; this entry is optional
4. Specify maximum file size in **Capture File Size**; this entry is optional
5. Click **Start**
6. Click **Stop** to terminate ping test if necessary
7. Download capture file after finished.

18.7. Watchdog

Watchdog is an electronic timer that is used to detect and recover from system malfunctions. That is timer for periodic reboot.

Schedule Reboot

Figure 160 – Schedule Reboot



Schedule Reboot

Periodic Reboot: ☑

Random Delay: □

Schedule Mode: □ Sun □ Mon □ Tues □ Wed □ Thur □ Fri □ Sat 00:00

Periodic Mode: 0 (Days)

0-30Days, 0 means Periodic mode disabled.

Periodic Upload Log: ☑

Random Delay: □

FTP Server User Name:

FTP Server Password: □ Show

FTP Server IP Address: 0 . 0 . 0 . 0

FTP Server Port: 21

Schedule Mode: □ Sun □ Mon □ Tues □ Wed □ Thur □ Fri □ Sat 00:00

Periodic Mode: 0 (Days)

0-30Days, 0 means Periodic mode disabled.

17.3.2.1 Periodic reboot

1. Go to **Tools** > **Watchdog** > **Schedule Reboot**
2. Select **Periodic Reboot** checkbox to enable reboot scheduler
3. Select **Radom Delay** checkbox to enable a random delay on scheduled rebooting time. It prevents all APs reboot at the same time; this entry is optional
4. Select exact time and day(s) in **Schedule Mode** for rebooting device;

   Or select a countdown timer (minute) in **Periodic Mode** for rebooting device
5. Click **Submit**
6. Click **Save & Apply**

17.3.2.2 Periodic log upload

1. Go to **Tools** > **Watchdog** > **Schedule Reboot**
2. Select **Periodic Upload Log** checkbox to enable upload log scheduler
3. Select **Radom Delay** checkbox to enable a random delay on scheduled rebooting time. It prevents all APs reboot at the same time

4. Enter username on **FTP Server User Name** for logging in remote FTP server
5. Enter password on **FTP Server Password** for logging in remote FTP server
6. Enter IP address of remote FTP server on **FTP Server IP Address**
7. Specify service port of remote FTP server on **FTP Server Port**; *21* is default setting
8. Select exact time and day(s) in **Schedule Mode** for uploading log to FTP server;

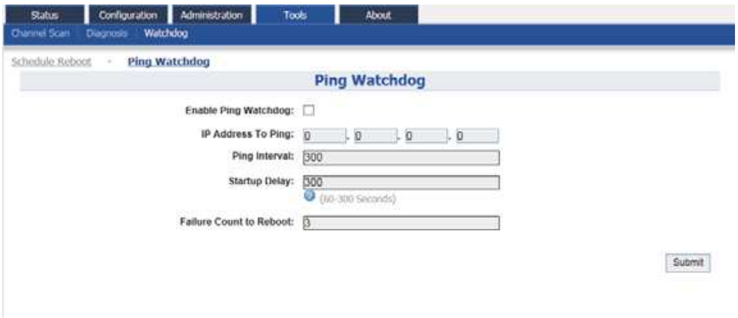
Or select a countdown timer (minute) in **Periodic Mode** for uploading log to FTP server

9. Click **Submit**
10. Click **Save & Apply**

Ping Watchdog

Ping watchdog is mechanism that CPE reboots itself if it fails to communicate (ping) to target host for serval time.

Figure 161 – Ping Watchdog



Ping Watchdog

Enable Ping Watchdog: □

IP Address To Ping: 0 . 0 . 0 . 0

Ping Interval: 300

Startup Delay: 300

(60-300 Seconds)

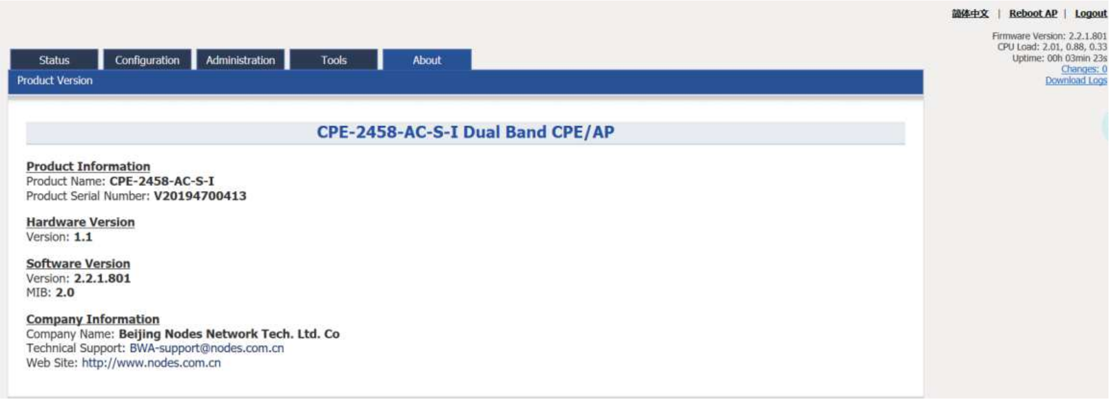
Failure Count to Reboot: 3

1. Go to **Tools** > **Watchdog** > **Ping watchdog**
2. Click **Enable Ping Watchdog** to enable this function
3. Type in IP address of target host in **IP Address To Ping**
4. Enter interval between each ICMP request in **Ping Interval**; *300* is default setting. This entry is optional.
5. Specify delay time of each ICMP request in **Startup Delay**; *300* is default setting. This entry is optional.
6. Specify fail tolerant in **Failure Count to Reboot**; *3* is default setting. This entry is optional.
7. Click **Submit**
8. Click **Save & Apply**

19. Product Information

CPE product shows the information about product information, hardware, software and company information in **About** tab.

Figure 162 - About



Firmware Version: 2.2.1.801
CPU Load: 2.01, 0.88, 0.33
Uptime: 00h 03min 23s

CPE-2458-AC-S-I Dual Band CPE/AP

Product Information
Product Name: **CPE-2458-AC-S-I**
Product Serial Number: **V20194700413**

Hardware Version
Version: **1.1**

Software Version
Version: **2.2.1.801**
MIB: **2.0**

Company Information
Company Name: **Beijing Nodes Network Tech. Ltd. Co**
Technical Support: BWA-support@nodes.com.cn
Web Site: http://www.nodes.com.cn

RF exposure statement:

The transmitter must not be colocated or operated in conjunction with any other antenna or transmitter. This equipment complies with the FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20cm between the radiator and any part of your body.

Antenna gain: 3dBi