



ALTAI C1N SERIES
WIFI AP/CPE

**WEB-ADMIN
CONFIGURATION
MANUAL**

Version 1.3
Date: January, 2016

Copyright © 2015 Altai Technologies Limited
ALL RIGHTS RESERVED.

Altai Technologies Limited

Unit 209, 2/Floor,
East Wing, Building 17
Hong Kong Science Park,
Sha Tin, New Territories,
Hong Kong

Telephone: +852 3758 6000

Fax: +852 2607 4021

Web: www.altaittechnologies.com

Customer Support Centre:

Email: support@altaittechnologies.com

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. If it is not installed and used in accordance with the instructions, harmful interference to radio communications may be caused.

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.

Warning

The user is advised to keep away from the base-station and antenna with at least 45cm when the base-station is in operation.

Please install a lightning arrestor to protect the base station from lightning dissipation during rainstorms. Lightning arrestors are mounted outside the structure and must be grounded by means of a ground wire to the nearest ground rod or item that is grounded.

Disclaimer

All specifications are subject to changes without prior notice. Altai Technologies assumes no responsibilities for any inaccuracies in this document or for any obligation to update information in this document. This document is provided for information purposes only. Altai Technologies reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Contents

| | |
|--|-------------------------------------|
| CONTENTS..... | 4 |
| MANUAL CONVENTIONS..... | 7 |
| 1. INTRODUCTION..... | 8 |
| 2. C1N SERIES MODEL AND FIRMWARE VERSION..... | 8 |
| 3. GETTING STARTED | 8 |
| 3.1. SETUP LOCAL AREA CONNECTION ON YOUR PC..... | 8 |
| 3.2. CHECK ACCESS..... | 11 |
| 3.3. CONFIGURATION WITH WEB-ADMIN..... | 11 |
| 3.4. PERMANENT SECONDARY IP | 13 |
| 3.5. INTERFACE INTRODUCTION | 14 |
| 3.6. LOGOUT FROM C1N SERIES WEB PAGE..... | 14 |
| 3.7. REBOOT C1N SERIES AP/CPE | 14 |
| 4. SYSTEM STATUS..... | 15 |
| 4.1. SYSTEM..... | ERROR! BOOKMARK NOT DEFINED. |
| 4.2. INTERFACE | 16 |
| 4.2.1. <i>Radio Interface Status</i> | 17 |
| 4.2.1.1. Radio0 Interface Status-AP Mode | 17 |
| 4.2.1.1.1. Status | 17 |
| 4.2.1.1.2. Statistic..... | 18 |
| 4.2.1.1.3. Channel Usage | 18 |
| 4.2.1.1.4. WLAN | 20 |
| 4.2.1.1.5. Association List..... | 21 |
| 4.2.1.2. Radio0 Interface Status-Station Mode | 23 |
| 4.2.1.2.1. Status | 23 |
| 4.2.1.2.2. Statistic..... | 24 |
| 4.2.1.2.3. Channel usage | 24 |
| 4.2.1.2.4. STA Info | 24 |
| 4.2.1.2.5. AP Info..... | 25 |
| 4.2.1.3. Radio0 Interface Status-Repeater Mode..... | 25 |
| 4.2.1.3.1. Status | 26 |
| 4.2.1.3.2. Statistic..... | 26 |
| 4.2.1.3.3. Channel usage | 26 |
| 4.2.1.3.4. STA Info | 27 |
| 4.2.1.3.5. AP Info..... | 27 |
| 4.2.1.3.6. WLAN | 27 |
| 4.2.1.3.7. Association List..... | 27 |
| 4.2.1.4. Radio0 Interface Status-Bridge Mode (for C1an and C1xan)..... | 28 |
| 4.2.2. <i>Ethernet Interface</i> | 28 |
| 4.2.2.1. Status | 28 |
| 4.2.2.2. Statistic..... | 29 |
| 4.3. HISTORICAL STATISTICS..... | 30 |
| 4.3.1. <i>System Statistics</i> | 30 |
| 4.3.2. <i>Ethernet Statistics</i> | 31 |
| 4.3.3. <i>Radio Statistics</i> | 33 |
| 4.3.4. <i>Logs</i> | 38 |
| 4.3.4.1. System Log | 38 |
| 4.3.4.2. Panic Log | 39 |
| 4.3.4.3. Alarm Log | 40 |
| 5. SYSTEM CONFIGURATION | 40 |
| 5.1. C1N SERIES AP/CPE BASIC CONFIGURATION PROCEDURES | 40 |
| 5.2. BASIC SYSTEM CONFIGURATION | 42 |
| 5.3. NETWORK CONFIGURATION..... | 43 |

| | | |
|--------------|--|------------|
| 5.3.1. | GENERAL NETWORK CONFIGURATION | 43 |
| 5.3.2. | VLAN | 50 |
| 5.3.3. | DHCP SERVER..... | 51 |
| 5.3.4. | PORT FORWARDING..... | 53 |
| 5.3.5. | SAFE MODE | 55 |
| 5.4. | WIRELESS | 56 |
| 5.4.1. | RADIO0 CONFIGURATION..... | 57 |
| 5.4.1.1. | RADIO0 CONFIGURATION – AP MODE | 57 |
| 5.4.1.1.1. | GENERAL CONFIGURATION | 57 |
| 5.4.1.1.2. | WLAN CONFIGURATION | 59 |
| 5.4.1.1.2.1. | WLAN X (0-15) GENERAL CONFIGURATION | 61 |
| 5.4.1.1.2.2. | WLAN X (0-15) SECURITY..... | 63 |
| 5.4.1.1.2.3. | WLAN X (0-15) ROGUE STATION LIST..... | 72 |
| 5.4.1.1.2.4. | WLAN X (0-15) QoS..... | 73 |
| 5.4.1.1.2.5. | WLAN X (0-15) BANDWIDTH CONTROL..... | 74 |
| 5.4.1.1.3. | ADVANCED CONFIGURATION..... | 76 |
| 5.4.1.1.4. | QoS CONFIGURATION | 80 |
| 5.4.1.1.5. | WEP KEY SETTING..... | 82 |
| 5.4.1.2. | RADIO0 CONFIGURATION – STATION MODE | 82 |
| 5.4.1.2.1. | GENERAL CONFIGURATION | 82 |
| 5.4.1.2.2. | STATION CONFIGURATION | 84 |
| 5.4.1.2.2.1. | WLAN 0 GENERAL CONFIGURATION | 84 |
| 5.4.1.2.2.2. | WLAN 0 SECURITY | 87 |
| 5.4.1.2.2.3. | WLAN 0 QoS | 87 |
| 5.4.1.3. | RADIO0 CONFIGURATION – REPEATER MODE | 88 |
| 5.4.1.3.1. | GENERAL CONFIGURATION | 88 |
| 5.4.1.3.2. | WLAN CONFIGURATION | 89 |
| 5.4.1.3.2.1. | REPEATER CONFIGURATION | 91 |
| 5.4.1.3.2.2. | WLAN CONFIGURATION | 91 |
| 5.4.1.4. | RADIO0 CONFIGURATION – BRIDGE MODE(FOR C1AN AND C1XAN) | 92 |
| 5.4.1.4.1. | GENERAL CONFIGURATION | 92 |
| 5.4.1.4.2. | STATIC BRIDGE SETTING | 94 |
| 5.4.1.4.2.1. | BRIDGE GENERAL SETTING..... | 94 |
| 5.4.1.4.2.2. | BRIDGE SECURITY SETTING..... | 95 |
| 5.4.1.4.2.3. | QoS SETTING..... | 96 |
| 5.5. | THIN AP CONFIGURATION..... | 96 |
| 6. | ADMINISTRATION CONFIGURATION | 99 |
| 6.1. | USER ADMIN | 99 |
| 6.2. | WEB ADMIN | 100 |
| 6.3. | SNMP SETTING..... | 101 |
| 6.3.1. | TRAP HOST SETTING | 102 |
| 6.4. | CERTIFICATE MANAGEMENT | 102 |
| 6.5. | FIRMWARE UPDATE | 103 |
| 6.6. | RESTORE FACTORY DEFAULT..... | 106 |
| 6.6.1. | RESET BACK TO FACTORY DEFAULT VIA WEB GUI..... | 106 |
| 6.6.2. | RESET BACK TO FACTORY DEFAULT VIA RESET BUTTON | 107 |
| 6.7. | BACKUP/RESTORE | 108 |
| 6.8. | CUSTOMIZATION | 109 |
| 6.9. | LICENSE | 112 |
| 7. | TOOLS..... | 112 |
| 7.1. | CHANNEL SCAN..... | 112 |
| 7.1.1. | OVERVIEW INFO..... | 113 |
| 7.1.2. | AP LIST INFO | 114 |
| 7.2. | DIAGNOSIS..... | 115 |

| | | |
|-----------|-------------------------------------|------------|
| 12.1.1. | <i>Ping to Host</i> | 115 |
| 12.1.2. | <i>Traceroute to Host</i> | 116 |
| 7.3. | WATCHDOG | 117 |
| 7.3.1. | SCHEDULE REBOOT | 117 |
| 7.3.2. | PING WATCHDOG..... | 119 |
| 8. | C1N SERIES INFORMATION | 119 |

Manual Conventions

| | |
|---------------|--|
| Bold | Bold type within paragraph text indicates commands, files names, directory names, paths, output, or returned values. |
| <i>Italic</i> | Within commands, italics indicate a variable that the user must specify. Titles of manuals or other published documents are also set in italics. |
| <u> </u> | Underline means that you have to pay attention to the words. |
| Courier | The courier font indicates output or display. |
| [] | Within commands, items enclosed in square brackets are optional parameters or values that the user can choose to specify or omit. |
| { } | Within commands, item enclosed in braces are options which the user must choose from. |
| | Within commands, the vertical bar separates options. |
| ... | An ellipsis indicates a repetition of preceding parameter. |
| > | The right angle bracket separates successive menu selection. |

NOTE: This message denotes neutral or positive information that calls out important points to the text. A note provides information that applies only in special cases.



Caution: Cautions call special attention to hazards that can cause system damage or data corruption, to a lesser degree than warnings.



Warnings: Warnings call special attention to hazards that can cause system damage, data corruption, personal injury, or death.

1. Introduction

This manual is to summarize how to perform basic configuration for the Altai C1n Series AP/CPE through web-admin interface. C1n Series AP/CPE includes 4 product models: C1n, C1xn, C1an and C1xan. They are all single-band WiFi AP/CPE: C1n and C1xn work at 2.4GHz band, C1an and C1xan work at 5GHz band.

2. C1n Series Model and Firmware Version

This manual is applicable for the following models, hardware and firmware versions:

| Product name | Model No. | Hardware Version | Firmware Version |
|--------------|------------|------------------|------------------|
| C1n | WA1011N-G | Above V1.1 | 1.2.6.x |
| C1an | WA1011N-A | Above V1.1 | 1.2.6.x |
| C1xn | WA1011N-GX | Above V1.1 | 1.2.6.x |
| C1xan | WA1011N-AX | Above V1.1 | 1.2.6.x |

Table 2-1 C1n Series Model

3. Getting Started

3.1. Setup Local Area Connection on Your PC

C1n Series AP/CPE can be connected to your PC in wired mode or in wireless mode. In the following, wired mode will be introduced. This is because the configurations are similar in wireless mode, except SSID has to be configured in both C1n Series AP/CPE and PC.

C1n Series AP/CPE can be connected to your PC directly or by a switch or a hub.

Start Network Configuration on your PC.

For **Windows XP** user,

1. Click the "**Start**" menu and choose "**Control Panel**".
2. Click "**Network Connections**".

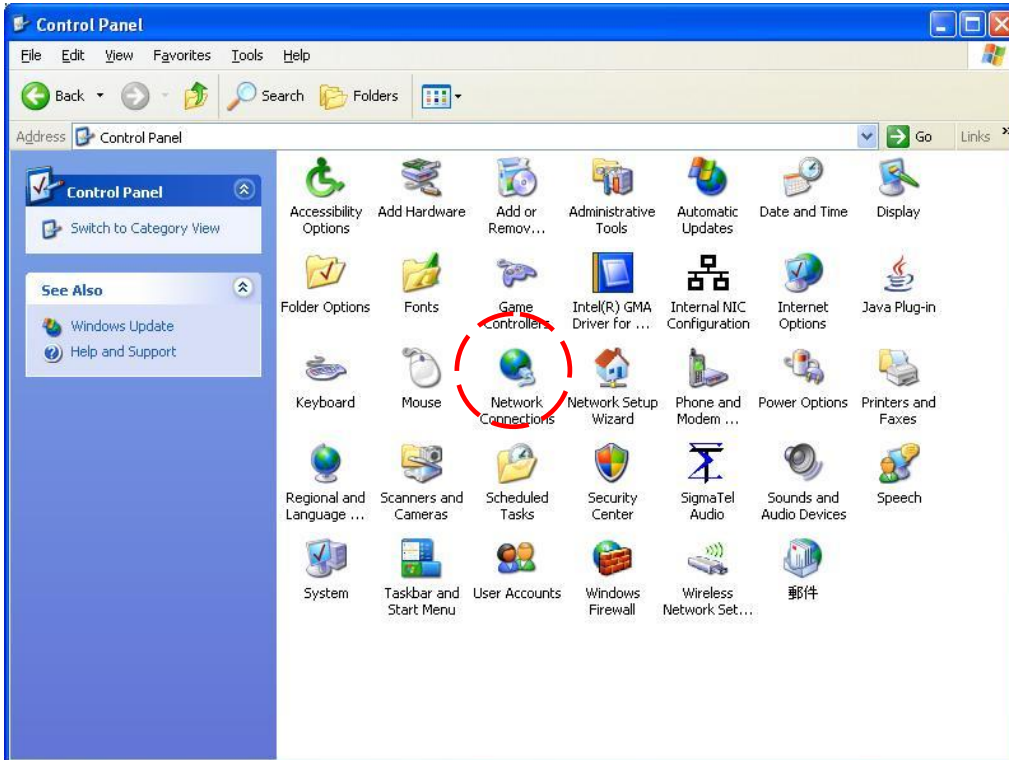


Figure 3-1 Control Panel in Windows XP

3. Right-click the "Local Area Connection" and select "Properties".

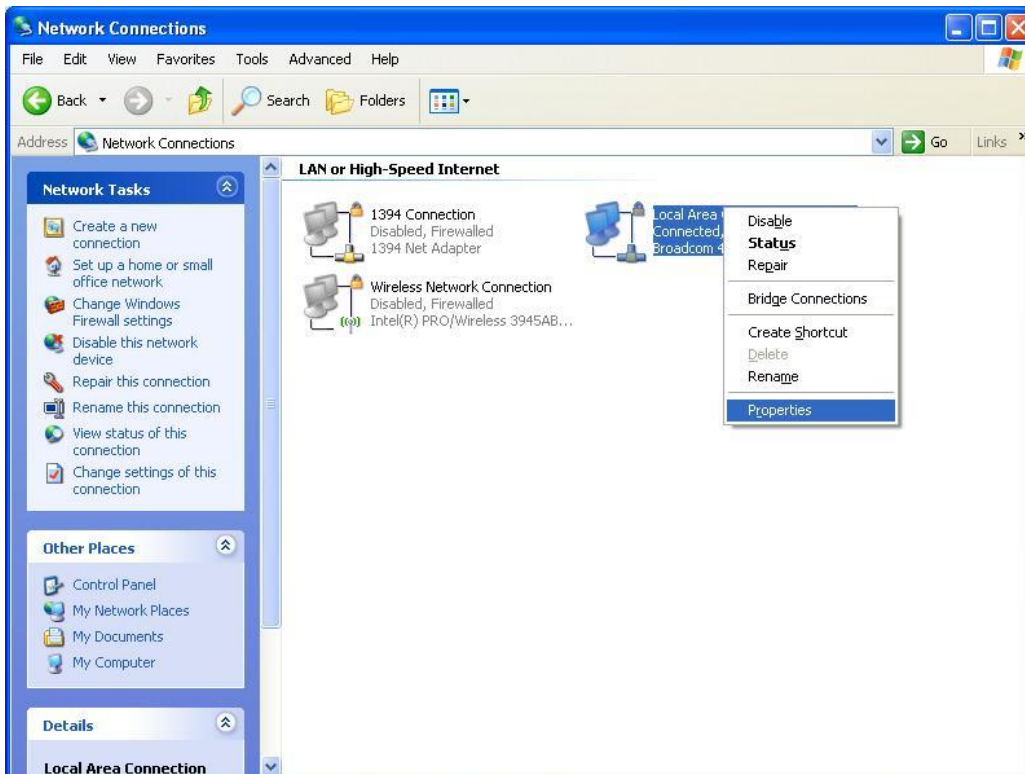


Figure 3-2 Network Connection in Windows XP

- After clicking "**Properties**", you will see the diagram as below.

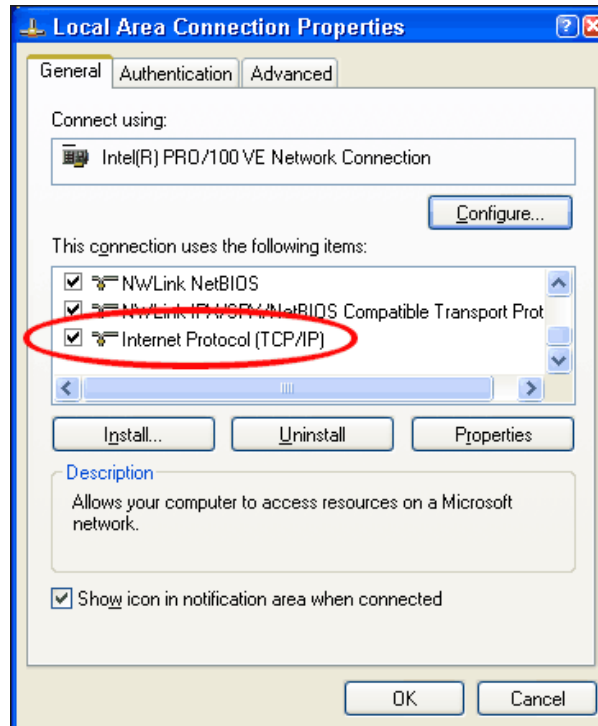


Figure 3-3 Local Area Connection Properties in Windows XP

- Mark the "**Internet Protocol (TCP/IP)**" and click "**Properties**".
- Type in an "**IP address**", for example, 192.168.1.2, which is under the same subnet as the Default IP Address of C1n Series AP/CPE (192.168.1.222).
- Using the default "**Subnet mask**" (default: 255.255.255.0) setting in the first time.
- Keep the "**Default gateway**" as "Blank".
- Keep the "**Preferred DNS server**" and "**Alternate DNS server**" as "**Blank**" also.
- Click "**OK**" when you finish setting and close the Window.

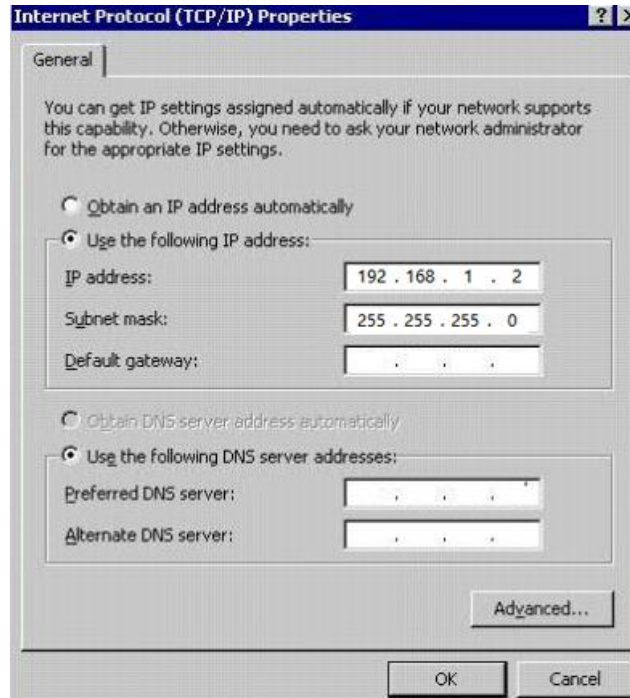


Figure 3-4 Internet Protocol (TCP/IP) Properties in Windows XP

3.2. Check Access

“ping” utility of Command Prompt is a handy tool to check the access to the C1n Series AP/CPE.

1. Go to the Command Prompt by typing “cmd” in “Run”.
2. Type command:

```
ping 192.168.1.222
```

The C1n Series AP/CPE shall respond to your ping request if C1n Series AP/CPE and your PC have a correct connection.

NOTE: Using the same PC to ping different C1n Series AP/CPE may cause ping failure. This is because C1n Series AP/CPE has the same default IP address **but different MAC addresses**. You need to type command “arp -d” in Command Prompt to clear ARP table on PC before each ping.

3.3. Configuration with Web-Admin

The C1n Series AP/CPE can be accessed through a Web Browser, for example, Internet Explorer (IE).

1. Open an IE session and type the IP address of the C1n Series AP/CPE. Example: http://192.168.1.222 or https://192.168.1.222, where 192.168.1.222 is the C1n Series 's IP address. The **default IP Address** is **192.168.1.222**.

- 2 A window will pop up, as shown in figure 3-5. Enter the user name and password in the corresponding fields, which are the same as for the CLI. The **default User Name** and **Password** are shown in Table 3-1. They are **case sensitive**.
- 3 Other level account "**guest**" for only view is shown in Table3-1 also. With this view only account, the user only can view the configuration of C1n but no change right.

| Firmware version | Default User Name | Default Password |
|------------------|-------------------|------------------|
| 1.2.6.x | admin | admin |
| 1.2.6.x | guest | guest |

Table 3-1 C1n Series default User Name and Password

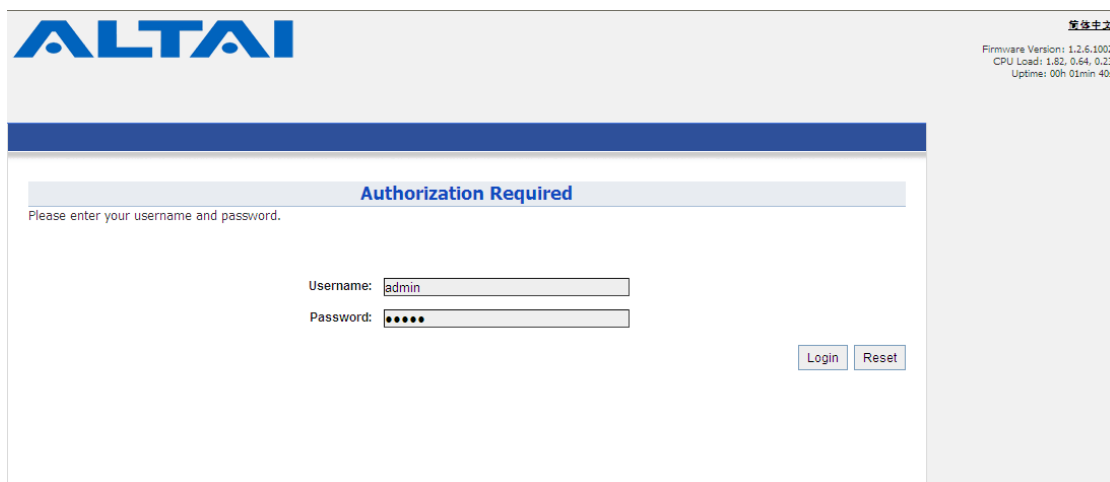


Figure 3-5 C1n Series AP/CPE web login page

- 4 A home page in IE appears, as shown in Figure 3-6. A **Menu Bar** is located on the top of the IE window. Different functions can be accessed through the menu bar.

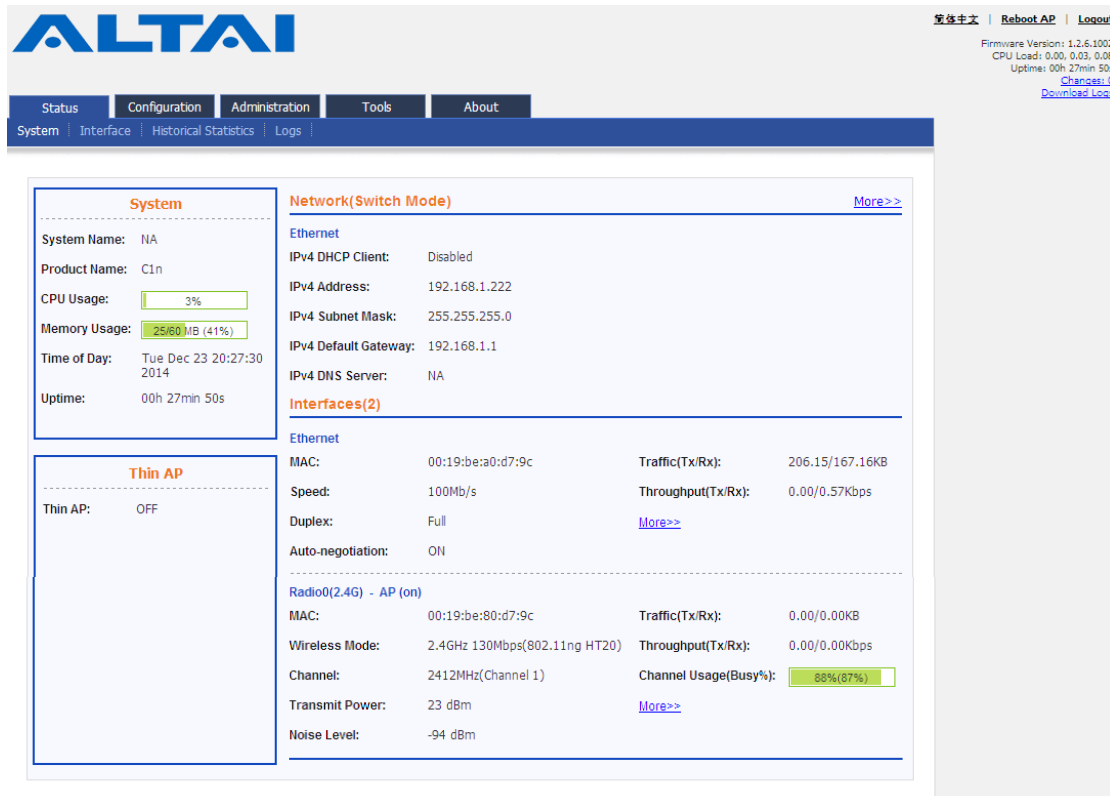


Figure 3-6 Web-admin home Page

3.4. Permanent Secondary IP

C1n Series supports a secondary IP address, which uses the last byte of the Ethernet MAC address as the last byte of the IP address.

Example:

Device Ethernet MAC address: 00:19:BE:20:03:6E

Factory Default Dynamic Secondary IP Address: 192.168.99.110 (6E (HEX) -> 110 (DEC))

The secondary IP shall use IP address from 192.168.99.5 to 192.168.99.254. The other IP addresses are reserved. If the last byte of the MAC address matches the reserved IP addresses, the supported device shall follow the following MAC to IP address mapping.

| Ethernet MAC address | Reserved Purpose | Replaced MAC byte | Secondary IP 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 | A3 | 192.168.99.163 |

| | | | |
|-------------------|-----------------------|----|----------------|
| | computer | | |
| 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:

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

Factory Default Secondary IP Address: 192.168.99.175 (FF (HEX)->AF(HEX)->175 (DEC))

3.5. Interface Introduction

C1n Series web interface is separated to 5 levels: Level 1 menu, Level 2 menu, Interface selection, Level 3 menu and Configuration options

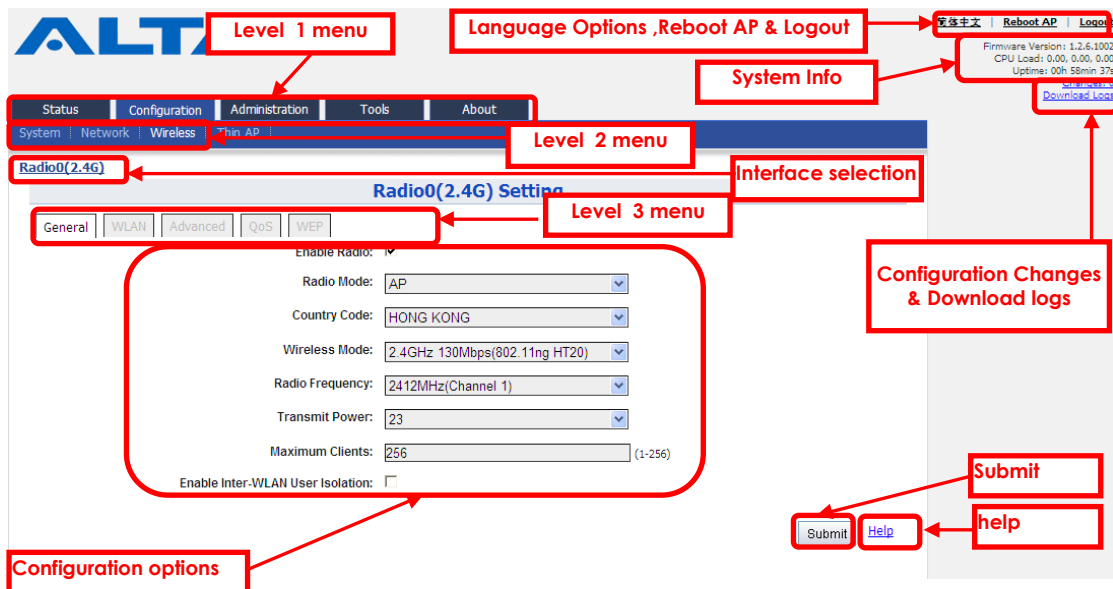


Figure 3-7 C1n Series Webpage

3.6. Logout from C1n Series Web Page

On the top right corner of C1n Series AP/CPE web interface, click "Logout" button to logout from C1n Series. On the other side, you can directly close C1n Series AP/CPE webpage to logout from C1n Series.



Figure 3-8 Logout

3.7. Reboot C1n Series AP/CPE

On the top right corner of C1n Series AP/CPE Web interface, click "Reboot AP" button then select "Perform reboot" to reboot C1n Series AP/CPE.

4. System Status

C1n Status function gives System information, interface information, Historical Statistics information and Log information.

4.1. System

User may check C1n basic information and real time status via **Status** → **System**.

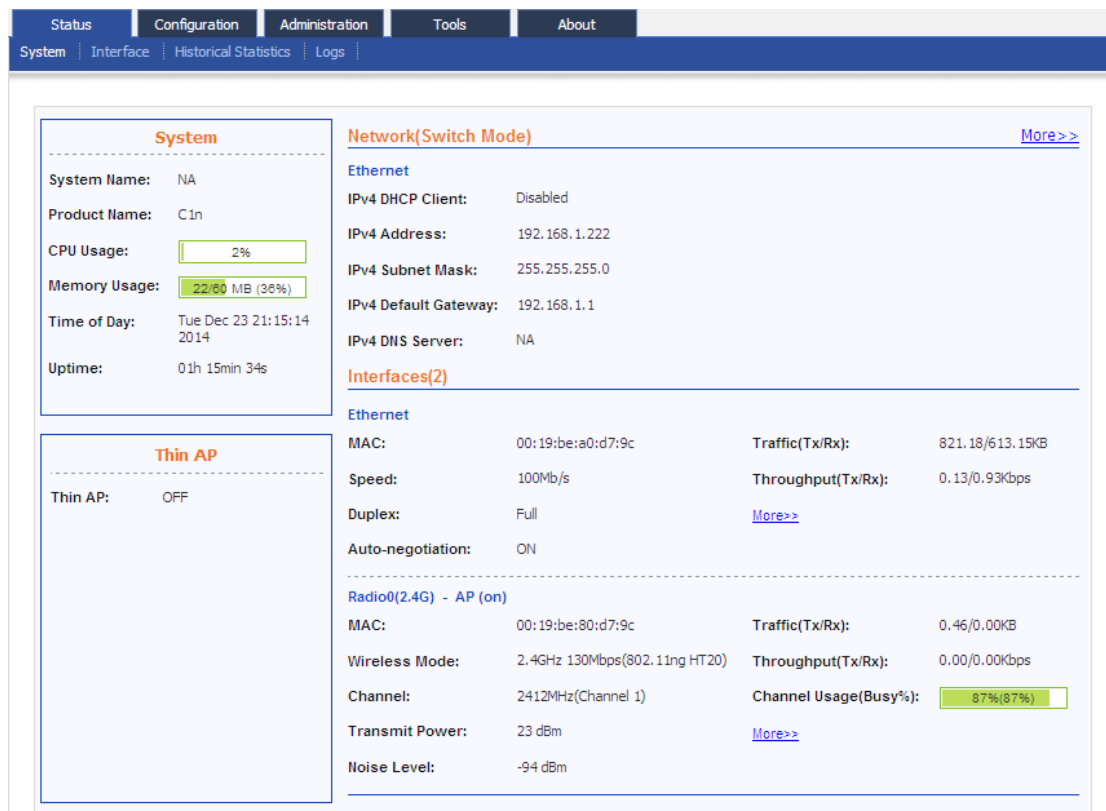


Figure 4-1 System Information

Following information can be found from "System" function:

1) System

System Name: System name for C1n Series AP/CPE, it can be customized by customer.

Product Name: C1n Series AP/CPE Product name.

CPU Usage: C1n Series AP/CPE CPU Usage (%).

Memory Usage: C1n Series AP/CPE memory Usage "used/all" MB (%).

Time of Day: system time.

Uptime: Operation time from last time reboot.

2) Thin AP

Show the status of thin AP function (On/Off).

When the thin AP function is On, We'll see more information about AC:

AC IP Address: shows the AC IP address.

AC Association Status: shows the status of thin AP associate to AC.

AC IP Address(DHCP Option 43): shows the AC IP acquired from DHCP Option 43.

AC IP Address(DHCP Option 60): shows the AC IP acquired from DHCP Option 60.

AC Online Time: shows the AC online time.

3) Network (Switch/Gateway)

It shows the status and information of network. It is switch mode as default.

IPv4 DHCP Client: Whether C1n Series AP/CPE was configured as IPv4 DHCP client.

IPv4 Address: current IPv4 address

IPv4 Subnet Mask: IPv4 subnet mask

IPv4 Default Gateway Address: IPv4 gateway address

IPv4 DNS Server: IPv4 DNS Server

4) Interfaces (2)

- Ethernet

It shows the status and information of Ethernet including Mac address, Traffic (Tx/Rx), Speed, Throughput (Tx/Rx), Duplex and Auto-negotiation. If click the "**More>>**", more detail information will be shown.

- Radio0 (2.4G) (for C1n & C1xn)

It shows Radio0 interface information including Operation Mode, Mac address, Traffic (Tx/Rx), Wireless Mode, Throughput (Tx/Rx), Channel, Channel Usage(Busy%), Transmit Power and Noise Level. If click the "**More>>**", more detail information will be shown. As default, the 2.4G radio is on.

- Radio0 (5G) (for C1an & C1xan)

It shows Radio0 interface information including Operation Mode, Mac address, Traffic (Tx/Rx), Wireless Mode, Throughput (Tx/Rx), Channel, Channel Usage(Busy%), Transmit Power and Noise Level. If click the "**More>>**", more detail information will be shown. As default, the 5G radio is off.

4.2. Interface

User may check the interface information of Radio0 and Ethernet via

Status→**Interface**.

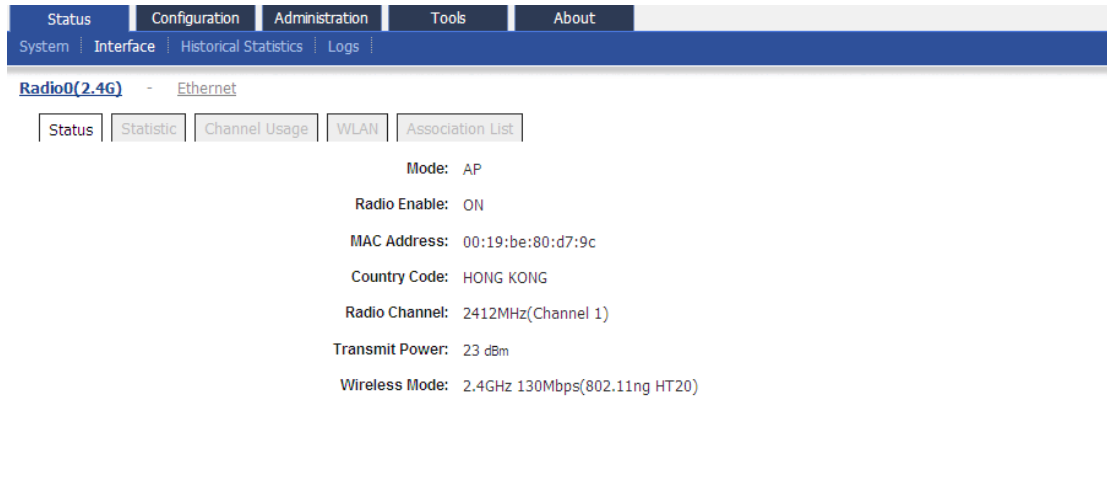


Figure 4-2 Interface Status

4.2.1. Radio Interface Status

User may obtain the information about Radio0 interface via **Status** → **Interface** → **Radio0(2.4G or 5G)**. The information is shown with the corresponding radio mode (AP/Station/Repeater), C1an and C1xn also have Bridge mode.

4.2.1.1. Radio0 Interface Status-AP Mode

When Radio0 work at AP mode, interface information includes following 5 parts: Status, Statistic, Channel Usage, WLAN and Association List.

4.2.1.1.1. Status

User may obtain the current status of Radio0 interface via **Status** → **Interface** → **Radio0** → **Status**. The parameters include Radio mode, Radio Enable, MAC Address, Country Code, Radio Channel, Transmit Power, and Wireless Mode.



Figure 4-3 Radio0 Interface Status

Mode: Operation mode (AP)

Radio Enable: Radio0 status (ON/OFF)

MAC Address: Radio0 MAC address.

Country Code: The default country code is HONG KONG.

Radio Channel: Radio0 current channel

Transmit Power : Radio0 transmit power

Wireless Mode : Radio0 wireless mode

4.2.1.1.2. Statistic

User may collect Radio0 statistical information via **Status**→**Interface**→**Radio0**→**Statistic**. The statistic includes Radio0 Tx and Rx Packets, Tx and Rx Packet Rate, Tx and Rx total traffic, and Tx and Rx Throughput.

| | TX | RX |
|---------------|----------|----------|
| Packets | 0.00K | 0.00K |
| Packet Rate | 0.00Kpps | 0.00Kpps |
| Total Traffic | 0.00KB | 0.00KB |
| Throughput | 0.00Kbps | 0.00Kbps |

Figure 4-4 Radio0 Statistic Information

Packets : Radio0 received and sent packets.

Packet Rate : Radio0 packet rate.

Total Traffic : Radio0 received and sent total traffic.

Throughput : Radio0 throughput.

4.2.1.1.3. Channel Usage

User may obtain the Radio0 channel usage information via **Status**→**Interface**→**Radio0**→**Channel Usage**. The Radio0 channel usage information includes Tx% (Avg), Rx% (Avg), Busy% (Avg), Noise Floor(dBm), CTL0, CTL1, EXT0, EXT1, Interference Mitigation Offset (0~50dB) , Traffic Distribution, Nearby AP List and Auto Refresh Interval.

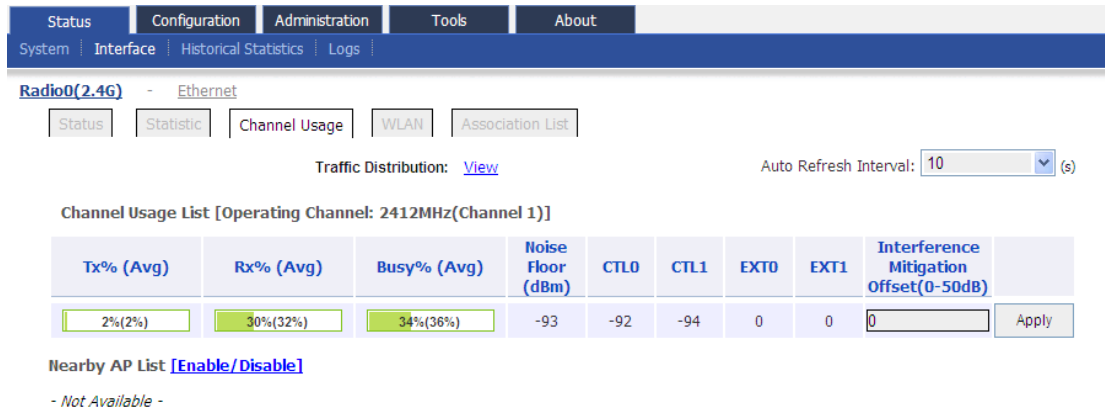


Figure 4-5 Radio0 Channel Usage information

Tx% (Avg): Average transmit frames percentage of operating channel.

Rx% (Avg): Average receive frames percentage of operating channel.

Busy% (Avg): Average busy state percentage of operating channel.

Noise Floor (dBm): Noise floor of operating channel.

CTL0: Chain 0 Noise Floor of the Control Channel (i.e. the center channel for HT20 case).

CTL1: Chain 1 Noise Floor of the Control Channel (i.e. the center channel for HT20 case).

EXT0: Chain 0 Noise Floor of the Extension Channel (i.e. the 2nd channel of the HT40 case).

EXT1: Chain 1 Noise Floor of the Extension Channel (i.e. the 2nd channel of the HT40 case).

Interference Mitigation Offset(0-50dB): This option will mask all noise / valid signal below "0-50" dB.

Traffic Distribution: Shows the distribution of control frame, data frame, management frame, etc. This information can be used to analyse device's performance. Click '**reset statistics**' can reset the #TX, TxBytes, TxBytes%, #Rx, RxBytes and RxBytes% data. Click '**Refresh**' button can refresh the #TX, TxBytes, TxBytes%, #Rx, RxBytes, RxBytes% data. Click '**close**' button at the bottom can close the 'Traffic Distribution Statistics' webpage.

| Traffic Distribution Statistics | | | | | | |
|--|-----|---------|----------|------|---------|----------|
| Traffic Distribution reset statistics Refresh | | | | | | |
| Rate | #Tx | TxBytes | TxBytes% | #Rx | RxBytes | RxBytes% |
| Control Frame | 0 | 0 | 0% | 0 | 0 | 0% |
| Data Frame | 0 | 0 | 0% | 0 | 0 | 0% |
| Management Frame | 660 | 204600 | 100% | 1938 | 150567 | 100% |
| 1M | 0 | 0 | 0% | 0 | 0 | 0% |
| 2M | 0 | 0 | 0% | 0 | 0 | 0% |
| 5.5M | 0 | 0 | 0% | 0 | 0 | 0% |
| 11M | 0 | 0 | 0% | 0 | 0 | 0% |
| 6M | 660 | 204600 | 100% | 978 | 76557 | 100% |
| 9M | 0 | 0 | 0% | 0 | 0 | 0% |
| 12M | 0 | 0 | 0% | 0 | 0 | 0% |
| 18M | 0 | 0 | 0% | 0 | 0 | 0% |
| 24M | 0 | 0 | 0% | 0 | 0 | 0% |
| 36M | 0 | 0 | 0% | 0 | 0 | 0% |
| 48M | 0 | 0 | 0% | 0 | 0 | 0% |
| 54M | 0 | 0 | 0% | 0 | 0 | 0% |
| MCS0 | 0 | 0 | 0% | 0 | 0 | 0% |
| MCS1 | 0 | 0 | 0% | 0 | 0 | 0% |
| MCS2 | 0 | 0 | 0% | 0 | 0 | 0% |
| MCS3 | 0 | 0 | 0% | 0 | 0 | 0% |
| MCS4 | 0 | 0 | 0% | 0 | 0 | 0% |
| MCS5 | 0 | 0 | 0% | 0 | 0 | 0% |
| MCS6 | 0 | 0 | 0% | 0 | 0 | 0% |
| MCS7 | 0 | 0 | 0% | 0 | 0 | 0% |
| MCS8 | 0 | 0 | 0% | 0 | 0 | 0% |
| MCS9 | 0 | 0 | 0% | 0 | 0 | 0% |
| MCS10 | 0 | 0 | 0% | 0 | 0 | 0% |
| MCS11 | 0 | 0 | 0% | 0 | 0 | 0% |
| MCS12 | 0 | 0 | 0% | 0 | 0 | 0% |
| MCS13 | 0 | 0 | 0% | 0 | 0 | 0% |
| MCS14 | 0 | 0 | 0% | 0 | 0 | 0% |
| MCS15 | 0 | 0 | 0% | 0 | 0 | 0% |
| MCS16 | 0 | 0 | 0% | 0 | 0 | 0% |
| MCS17 | 0 | 0 | 0% | 0 | 0 | 0% |
| MCS18 | 0 | 0 | 0% | 0 | 0 | 0% |
| MCS19 | 0 | 0 | 0% | 0 | 0 | 0% |
| MCS20 | 0 | 0 | 0% | 0 | 0 | 0% |
| MCS21 | 0 | 0 | 0% | 0 | 0 | 0% |
| MCS22 | 0 | 0 | 0% | 0 | 0 | 0% |
| MCS23 | 0 | 0 | 0% | 0 | 0 | 0% |
| Total | 660 | 204600 | - | 978 | 76557 | - |

Figure 4-6 Traffic Distribution Statistics

Nearby AP List: When the function is enabled, user can obtain the nearby AP information.

Auto Refresh Interval: Select the refresh interval of this webpage.

4.2.1.1.4. WLAN

User may collect Radio0 wireless network information via **Status**→**Interface**→**Radio0**→**WLAN**. The information includes Device ID, WLAN ID, SSID, MAC Address, Auth Mode, Unicast Cipher, Multicast Cipher, Num of Station, Throughput (TX/RX), Traffic (Tx/Rx) and State.

| Device ID | WLAN ID | SSID | MAC Address | Auth Mode | Unicast Cipher | Multicast Cipher | Num of Station | Throughput (Tx/Rx) | Traffic(Tx/Rx) | State |
|-----------|---------|---------------------|-------------------|-----------|----------------|------------------|----------------|--------------------|----------------|---------|
| radio0 | 0 | Superwifi Network 0 | 00:19:be:80:d7:9c | open | none | none | 0 | 0.00Kbps/0.00Kbps | 0.00KB/0.00KB | Enabled |

Figure 4-7 Radio0 WLAN Information

Device Id: Radio interface ID

WLAN: Wireless network number

SSID: SSID of WLAN, default SSID is Superwifi Network x (x is from 0 to 15)

MAC Address: wireless network MAC address (BSSID)

Auth Mode: Authentication mode for each wireless network

Unicast Cipher: Unicast cipher mode for each wireless network

Multicast Cipher: Multicast cipher mode for each wireless network

Num of Station: Number of associated client of each wireless network

Throughput (TX/RX): Actual throughput of each wireless network

Traffic (Tx/Rx): Download and Upload packets of each wireless network

State: Wireless network state

4.2.1.1.5. Association List

User may collect the associated clients' information via **Status**→**Interface**→**Radio0**→**Association List**. The information includes Total Client Association, Client Association Histogram, STA ID, MAC Address, IP Address, WLAN ID, Sector, SNR(dB), Throughput STA (Tx/Rx), Traffic STA (Tx/Rx), and Data Rate STA (Tx/Rx).

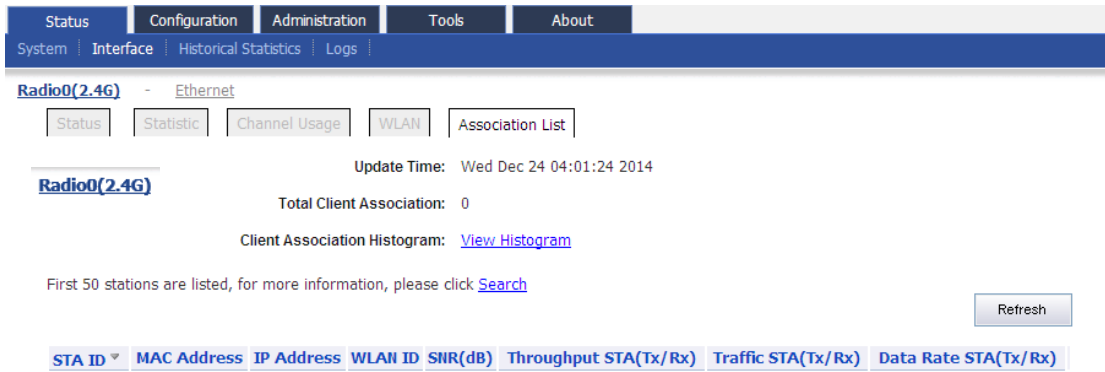


Figure 4-8 Radio0 Association List

Total Client Association: Total number of associated clients in Radio0

Client Association Histogram: Association client history records

STA ID: Wireless client's ID

MAC Address: Wireless client's MAC address

IP Address: Wireless client's IP address


WLAN ID: WLAN ID that wireless clients associated

SNR: Wireless client's SNR (Uplink)

Throughput STA (Tx/Rx): Wireless client's actual throughput (kbps)

Traffic STA (Tx/Rx): Wireless client's download and upload traffic (Bytes)

Data Rate STA (Tx/Rx): Wireless client's download and upload rate (Mbps)

Click this icon , below prompt will pop up. If choice 'OK', the associated client will be disconnected and added into rogue station list.

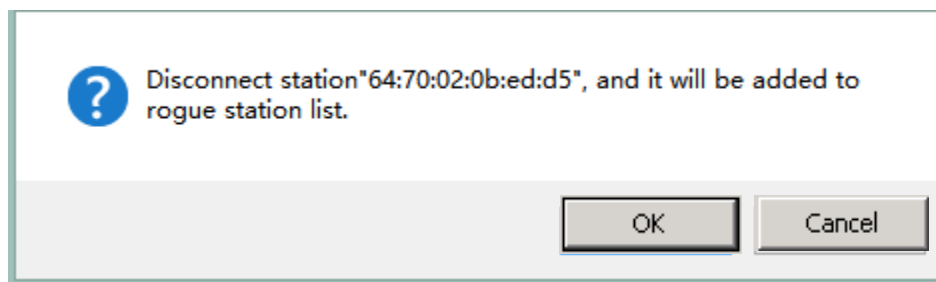


Figure 4-9 Add Client to Rogue Station List

Click the "View Histograms" user can see "SNR Histogram" and "Tx/Rx Rate Histogram".

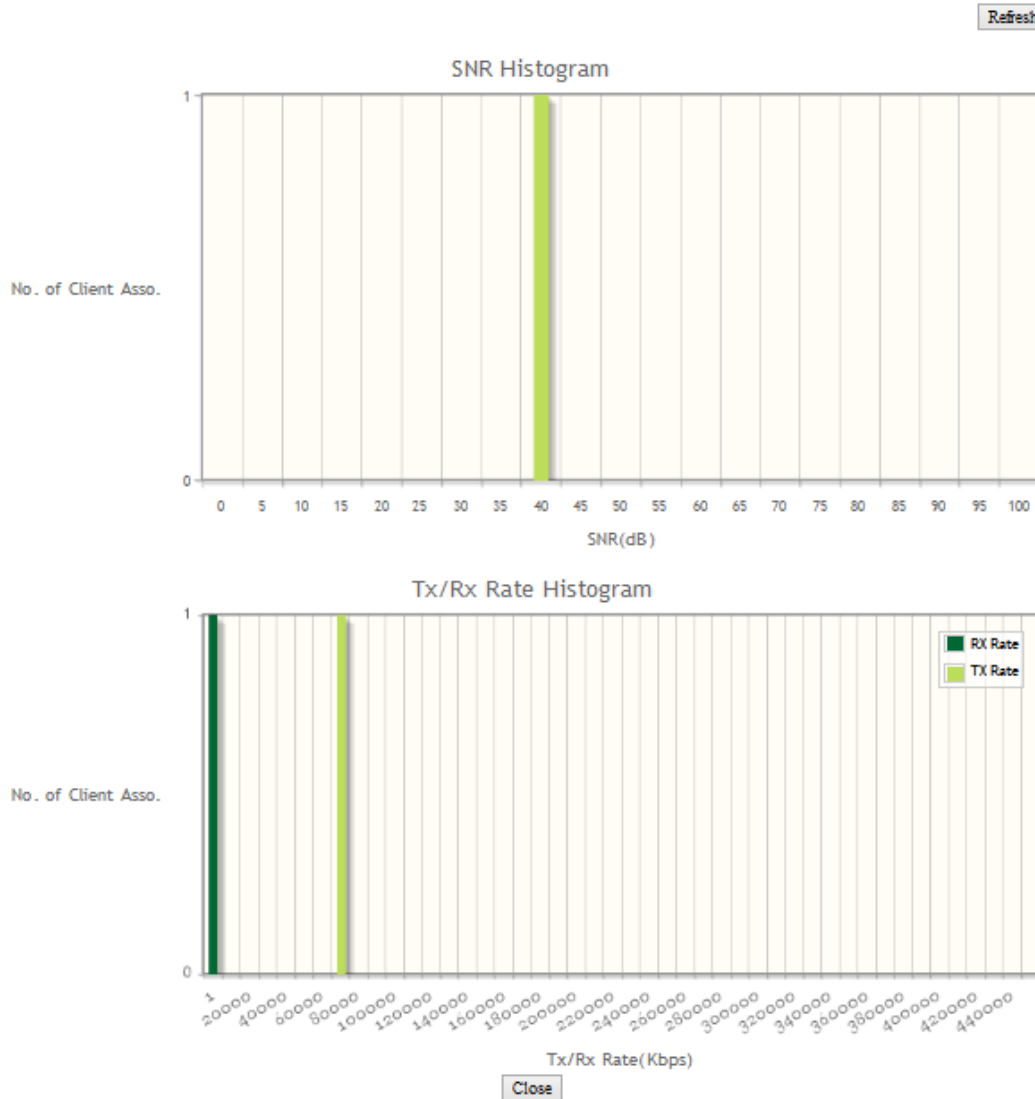


Figure 4-10 Radio0 Histogram Page

SNR Histogram: Shows No. of Client Associated and Client's SNR information.

Tx/Rx Rate Histogram: Shows No. of Client Associated and Client's Tx/Rx Rate information.

4.2.1.2. Radio0 Interface Status-Station Mode

When Radio0 work mode is configured to Station, C1n Series AP/CPE will be operated as a workstation, user need to associate Radio0 to a remote AP. At Station mode, Radio0 interface information includes: Status, Statistic, Channel Usage, STA Info, and AP Info.

4.2.1.2.1. Status

Please refer to section 4.2.1.1.1 for more details about radio status.

Radio0(2.4G) - Ethernet

Status | Statistic | Channel Usage | WLAN | Association List

Mode: AP

Radio Enable: ON

MAC Address: 00:19:be:80:d7:9c

Country Code: HONG KONG

Radio Channel: 2412MHz(Channel 1)

Transmit Power: 23 dBm

Wireless Mode: 2.4GHz 130Mbps(802.11ng HT20)

Figure 4-11 Radio0 station mode status

4.2.1.2.2. Statistic

Please refer to section 4.2.1.1.2 for more details about radio statistic.

Radio0(2.4G) - Ethernet

Status | Statistic | Channel Usage | WLAN | Association List

| | TX | RX |
|---------------|----------|----------|
| Packets | 0.00K | 0.00K |
| Packet Rate | 0.00Kpps | 0.00Kpps |
| Total Traffic | 0.00KB | 0.00KB |
| Throughput | 0.00Kbps | 0.00Kbps |

Figure 4-12 Radio0 station mode statistic

4.2.1.2.3. Channel usage

Please refer to 4.2.1.1.3 section for more details about channel usage.

Radio0(2.4G) - Ethernet

Status | Statistic | Channel Usage | WLAN | Association List

Traffic Distribution: View Auto Refresh Interval: 10 (s)

Channel Usage List [Operating Channel: 2412MHz(Channel 1)]

| Tx% (Avg) | Rx% (Avg) | Busy% (Avg) | Noise Floor (dBm) | CTL0 | CTL1 | EXT0 | EXT1 | Interference Mitigation Offset(0-50dB) |
|-----------|-----------|-------------|-------------------|------|------|------|------|--|
| 2%(2%) | 30%(32%) | 34%(36%) | -93 | -92 | -94 | 0 | 0 | 0 |

Nearby AP List Enable/Disable

- Not Available -

Figure 4-13 Radio0 station mode channel usage

4.2.1.2.4. STA Info

User may obtain the station information via **Status** → **Interface** → **Radio0** → **STA Info**. The information includes MAC Address, Auth Mode, Unicast Cipher, Multicast Cipher, and State.

| MAC Address | Auth Mode | Unicast Cipher | Multicast Cipher | State |
|-------------------|-----------|----------------|------------------|----------|
| 00:19:be:80:d7:9c | open | none | none | Disabled |

Figure 4-14 Radio0 station mode STA info

MAC Address: Radio0 MAC address.

Auth Mode: Authentication mode configured on C1n Series AP/CPE, the configuration is required to match with the remote AP.

Unicast Cipher: Unicast cipher mode configured on C1n Series AP/CPE, the configuration is required to match with the remote AP.

State: Radio0 current state.

4.2.1.2.5. AP Info

User may obtain the associated AP information via **Status** → **Interface** → **Radio0** → **AP Info**. The information includes MAC Address, SSID, SNR (dB), Channel, Max Data Rate, Throughput AP (Tx/Rx), Data Rate AP (Tx/Rx), and Connected Status.

| AP MAC Address | SSID | SNR(dB) | Channel | Max DataRate | Throughput AP (Tx/Rx) | Data Rate AP (Tx/Rx) | Connected Status |
|----------------|-----------|---------|---------|--------------|-----------------------|----------------------|------------------|
| NA | Network 0 | - | NA | NA | 0.00Kbps/0.00Kbps | 0Mbps/0Mbps | Not Connected |

Figure 4-15 Radio0 station mode AP info

AP MAC Address: MAC address of remote AP.

SSID: SSID information of remote AP.

SNR(dB): Remote AP SNR (Downlink).

Channel: Operating channel of remote AP.

Max DataRate: Maximum data transfer rate between station and remote AP.

Throughput AP(Tx/Rx): Actual throughput between station and remote AP.

Data Rate AP: Actual data transfer rate between station and remote AP.

Connected Status: Whether Radio0 is connected to remote AP.

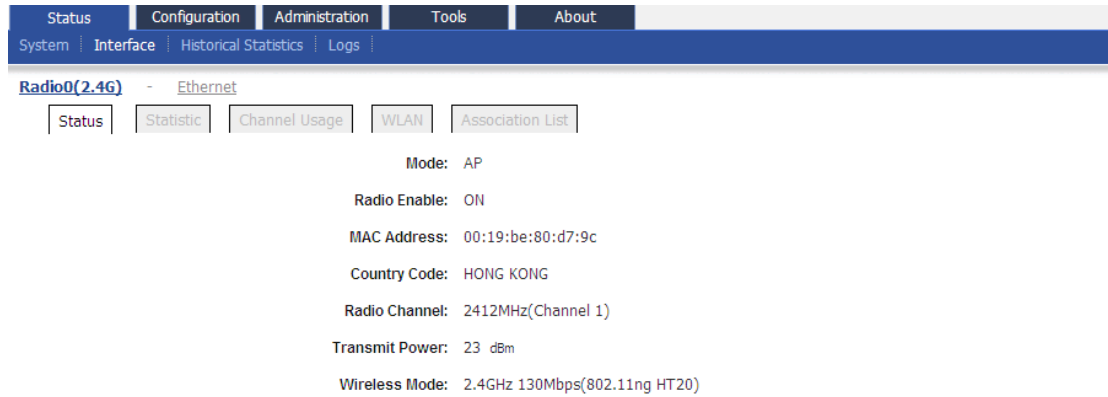
4.2.1.3. Radio0 Interface Status-Repeater Mode

When Radio0's work mode is configured to Repeater, C1n Series AP/CPE will be

operated as a wireless repeater, you need to associate it to a remote AP, then Radio0 forwards the remote AP's wireless signal. At Repeater mode, Radio0 interface information includes: Status, Statistic, Channel Usage, STA Info, AP Info, WLAN, and Association List.

4.2.1.3.1. Status

Please refer to section 4.2.1.1.1 for more details about status.

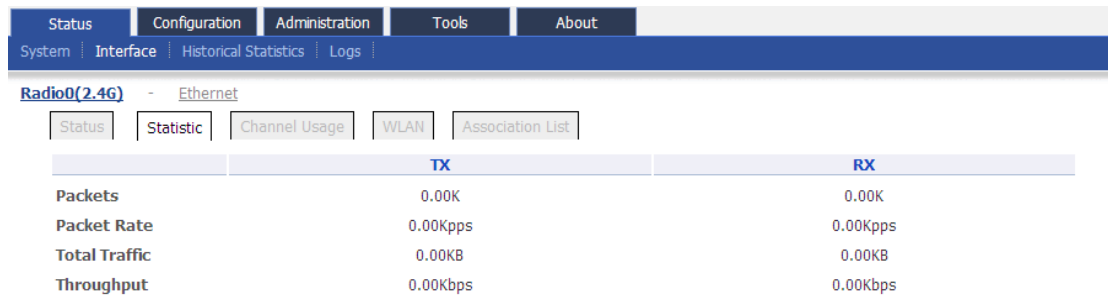


Mode: AP
 Radio Enable: ON
 MAC Address: 00:19:be:80:d7:9c
 Country Code: HONG KONG
 Radio Channel: 2412MHz(Channel 1)
 Transmit Power: 23 dBm
 Wireless Mode: 2.4GHz 130Mbps(802.11ng HT20)

Figure 4-16 Radio0 repeater mode status

4.2.1.3.2. Statistic

Please refer to section 4.2.1.1.2 for more details about radio statistic.

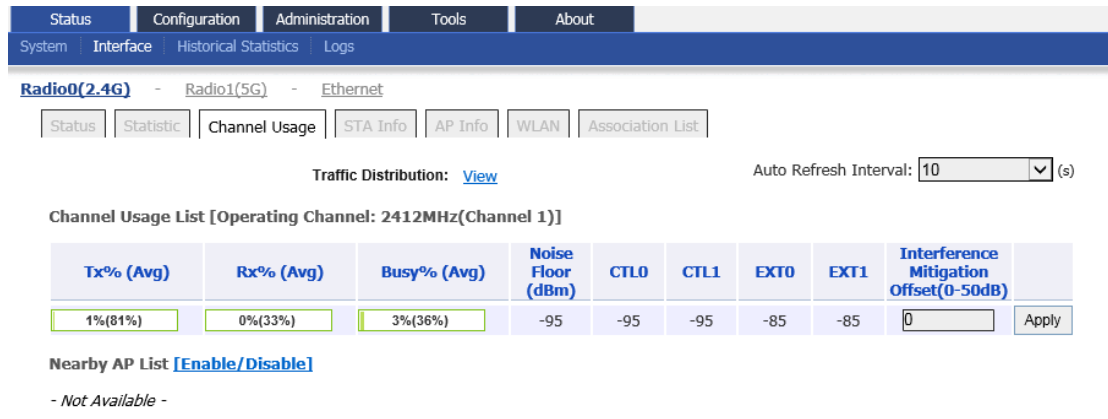


| | TX | RX |
|---------------|----------|----------|
| Packets | 0.00K | 0.00K |
| Packet Rate | 0.00Kpps | 0.00Kpps |
| Total Traffic | 0.00KB | 0.00KB |
| Throughput | 0.00Kbps | 0.00Kbps |

Figure 4-17 Radio0 repeater mode statistic

4.2.1.3.3. Channel usage

Please refer to section 4.2.1.1.3 for more details about channel usage.



| Tx% (Avg) | Rx% (Avg) | Busy% (Avg) | Noise Floor (dBm) | CTL0 | CTL1 | EXT0 | EXT1 | Interference Mitigation Offset(0-50dB) |
|-----------|-----------|-------------|-------------------|------|------|------|------|--|
| 1%(81%) | 0%(33%) | 3%(36%) | -95 | -95 | -95 | -85 | -85 | 0 |

Nearby AP List [\[Enable/Disable\]](#)
 - Not Available -

Figure 4-18 Radio0 repeater mode channel usage

4.2.1.3.4. STA Info

Please refer to section 4.2.1.2.4 for more details about STA info.

| MAC Address | Auth Mode | Unicast Cipher | Multicast Cipher | State |
|-------------------|-----------|----------------|------------------|----------|
| 00:19:be:80:d7:9c | open | none | none | Disabled |

Figure 4-19 Radio0 repeater mode STA info

4.2.1.3.5. AP Info

Please refer to section 4.2.1.2.5 for more details about AP info.

| AP MAC Address | SSID | SNR(dB) | Channel | Max DataRate | Throughput AP (Tx/Rx) | Data Rate AP (Tx/Rx) | Connected Status |
|----------------|-----------|---------|---------|--------------|-----------------------|----------------------|------------------|
| NA | Network 0 | | NA | NA | 0.00Kbps/0.00Kbps | 0Mbps/0Mbps | Not Connected |

Figure 4-20 Radio0 repeater mode AP info

4.2.1.3.6. WLAN

Please refer to section 4.2.1.1.4 for more details about WLAN.

| Device ID | WLAN ID | SSID | MAC Address | Auth Mode | Unicast Cipher | Multicast Cipher | Num of Station | Throughput (Tx/Rx) | Traffic(Tx/Rx) | State |
|-----------|---------|-----------------------------|-------------------|-----------|----------------|------------------|----------------|--------------------|----------------|---------|
| radio0 | 0 | Supervi fi Netwo rk 0 | 00:19:be:80:d7:9c | open | none | none | 0 | 0.00Kbps/0.00Kbps | 0.00KB/0.00KB | Enabled |

Figure 4-21 Radio0 repeater mode WLAN

4.2.1.3.7. Association List

Please refer to section 4.2.1.1.5 for more details about association list.

Update Time: Wed Dec 24 04:01:24 2014

Total Client Association: 0

Client Association Histogram: [View Histogram](#)

First 50 stations are listed, for more information, please click [Search](#)

| STA ID | MAC Address | IP Address | WLAN ID | SNR(dB) | Throughput STA(Tx/Rx) | Traffic STA(Tx/Rx) | Data Rate STA(Tx/Rx) |
|--------|-------------|------------|---------|---------|-----------------------|--------------------|----------------------|
|--------|-------------|------------|---------|---------|-----------------------|--------------------|----------------------|

Figure 4-22 Radio0 repeater mode association list

4.2.1.4. Radio0 Interface Status-Bridge Mode (for C1an and C1xan)

When Radio0(5G) work mode is configured to Bridge, C1an/C1xan will be operated as a wireless Bridge. 5G interface information shows the Status:

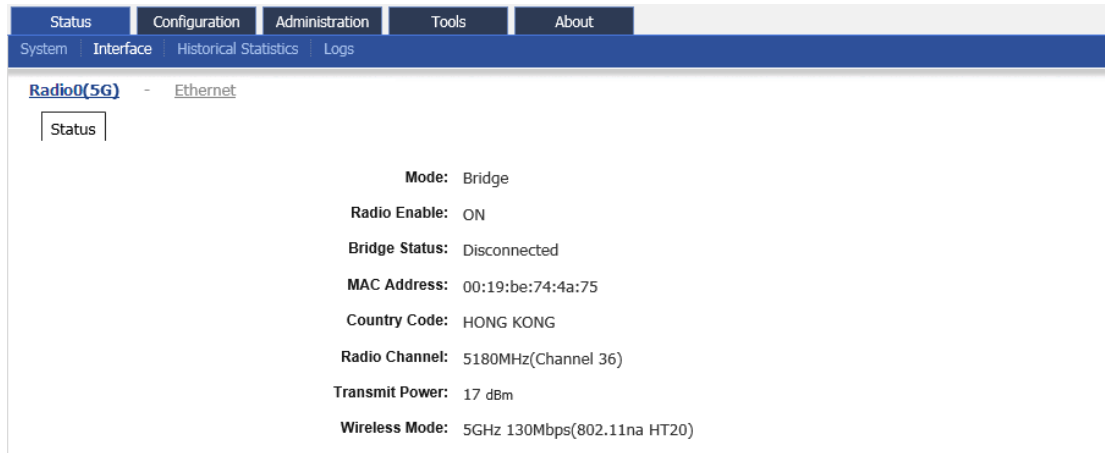


Figure 4-23 5G Radio bridge mode status

Mode: Operation mode, here is Bridge

Radio Enable: Radio0 (5G) status (ON/OFF)

Bridge Status: The status of bridging link to remote bridge

MAC Address: Radio0(5G) MAC address.

Country Code: Country Code information of Radio0(5G).

Radio Channel: Radio0(5G)operating channel

Transmit Power: Radio0(5G)current transmit power

Wireless Mode: Radio0(5G) wireless mode

4.2.2. Ethernet Interface

User may obtain Ethernet interface information via **Status**→**Interface**→**Ethernet**. The information includes Status and Statistic.

4.2.2.1. Status

User may obtain Ethernet interface status via **Status**→**Interface**→**Ethernet**→**Status**. The

parameters include Ethernet MAC Address, Speed, Duplex, Auto-negotiation, and Link Detected.

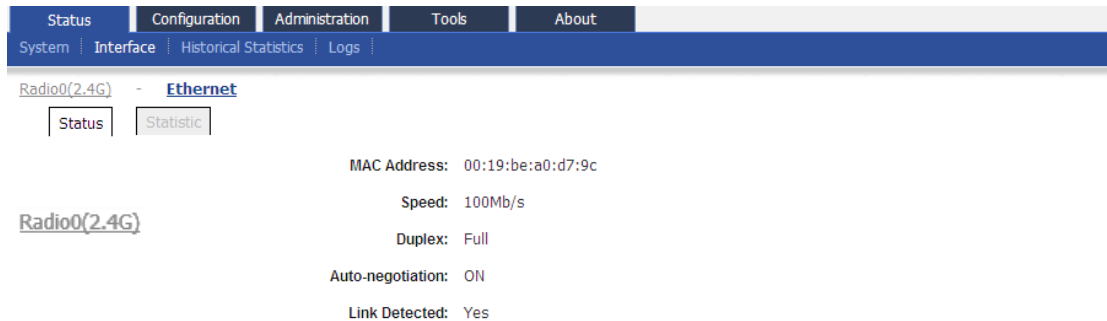


Figure 4-24 Ethernet Interface State

MAC Address: C1n Series AP/CPE Ethernet MAC address

Speed: Ethernet speed

Duplex: Ethernet duplex mode (Full/Half)

Auto-negotiation: Ethernet auto-negotiation mode ON or OFF, by default it is "ON".

Link Detected: Whether Ethernet does link detection, by default it is "yes".

4.2.2.2. Statistic

User may obtain Ethernet statistic information via **Status** → **Interface** → **Ethernet** → **Statistic**. The parameters include Ethernet Tx & Rx Packets, Packet Rate, Total Traffic, and Throughput.

| | TX | RX |
|---------------|----------|----------|
| Packets | 17.14K | 2.48M |
| Packet Rate | 0.00Kpps | 0.00Kpps |
| Total Traffic | 4.70MB | 2.45GB |
| Throughput | 9.74Kbps | 2.04Kbps |

Figure 4-25 Ethernet Interface Statistic

Packets: Ethernet transmitted and received packets

Packet Rate: Ethernet interface packet rate

Total Traffic: Ethernet transmitted and received total traffic.

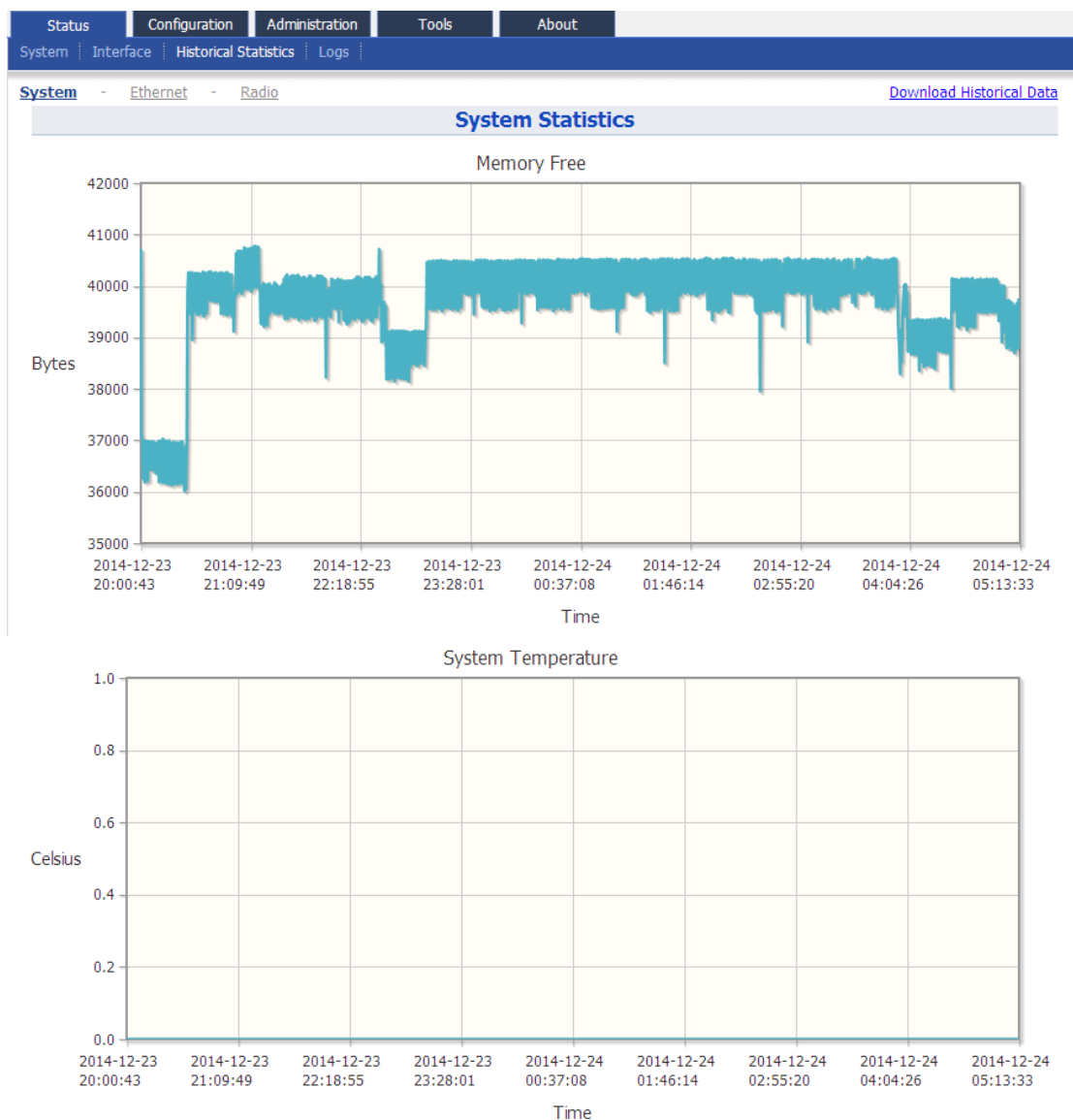
Throughput: Ethernet interface throughput

4.3. Historical Statistics

C1n Series AP/CPE can offer historical statistics of system, Ethernet and radio. These information can give helps to troubleshooting. We can also download the historical statistics information.

4.3.1. System Statistics

User may check system statistics via **Status**→**Historical Statistics**→**System**. It includes Memory free, and CPU Usage statistics.



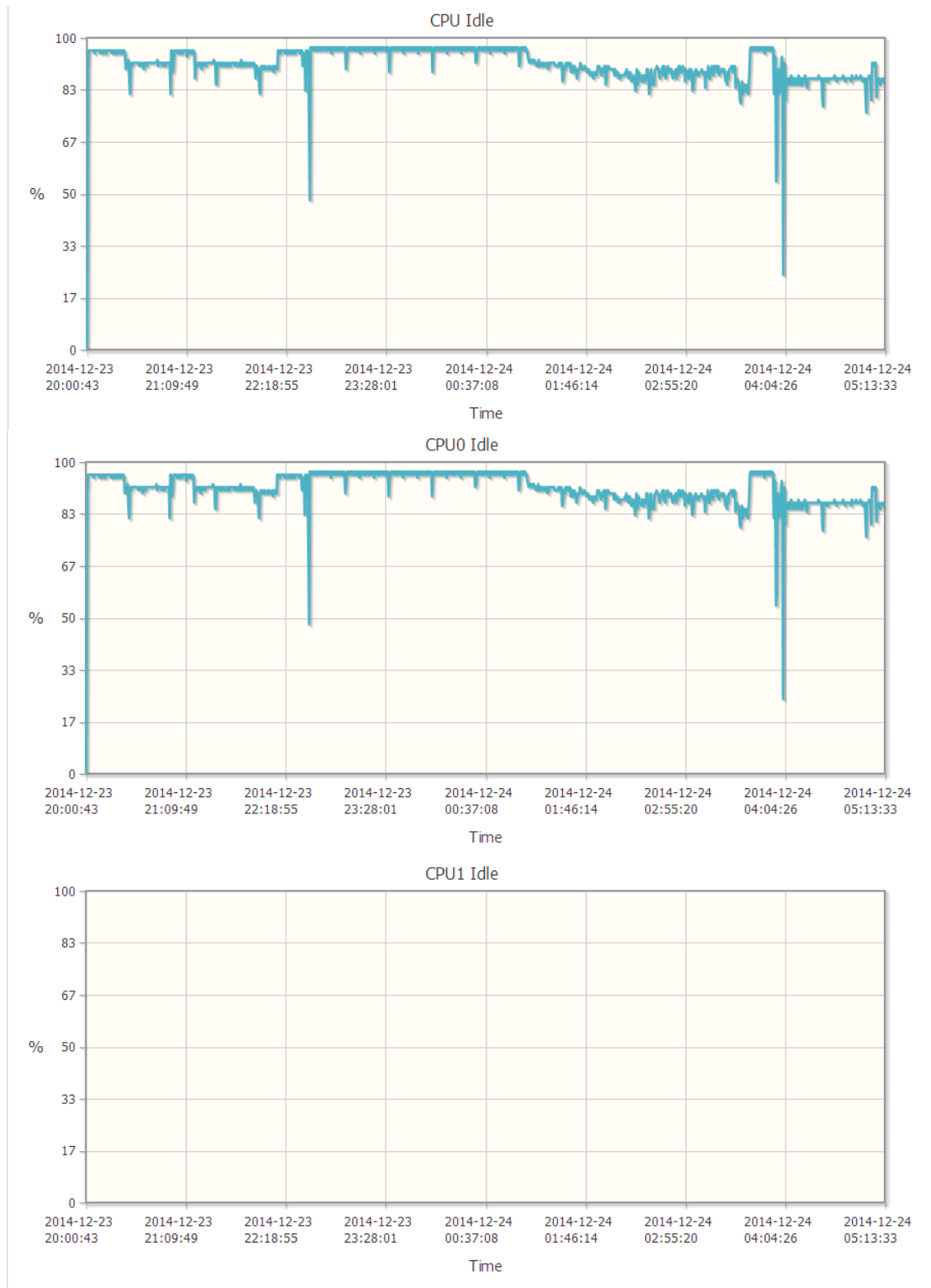
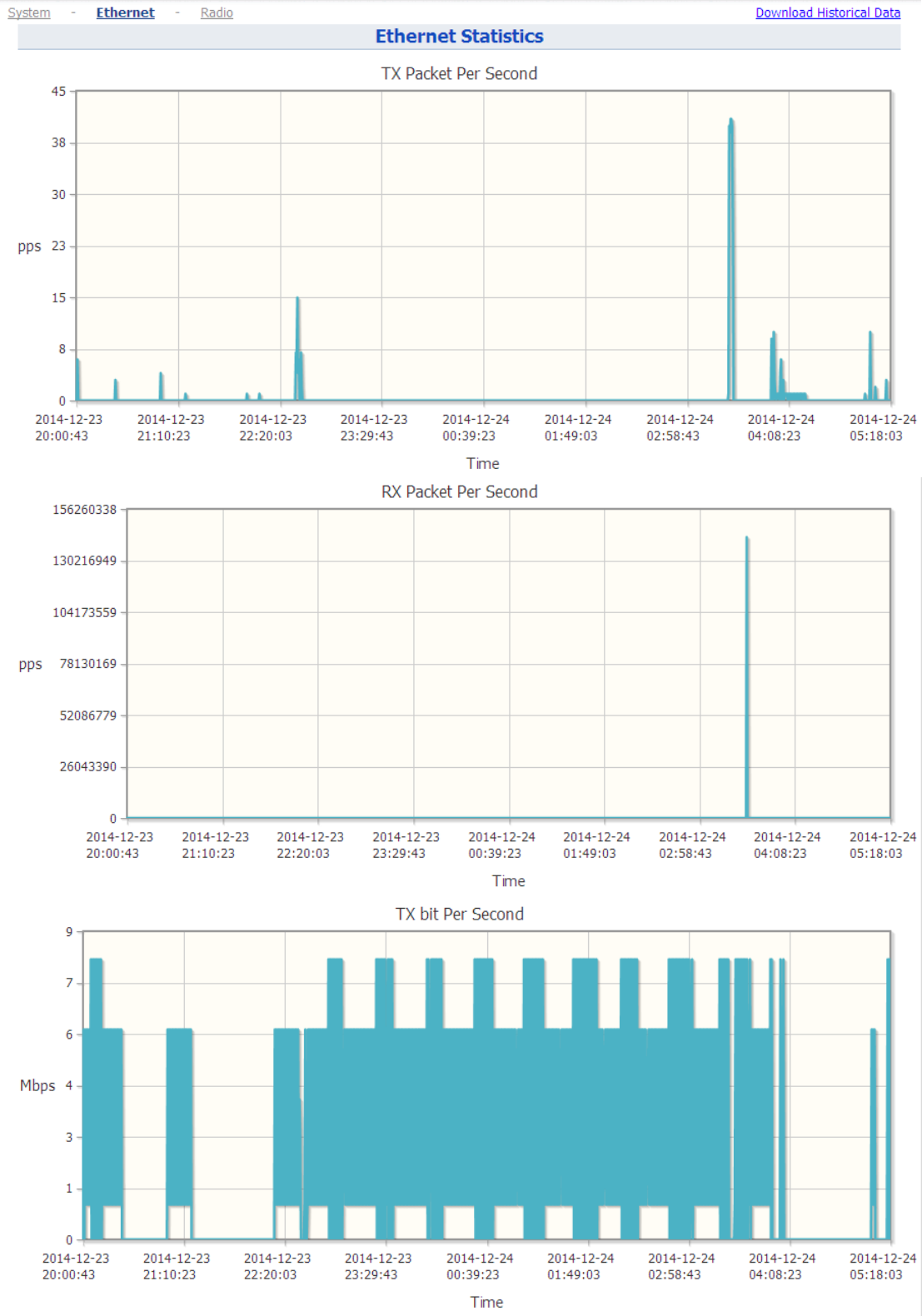


Figure 4-26 System historical

4.3.2. Ethernet Statistics

User may check Ethernet statistics via **Status** → **Historical Statistics** → **Ethernet**.



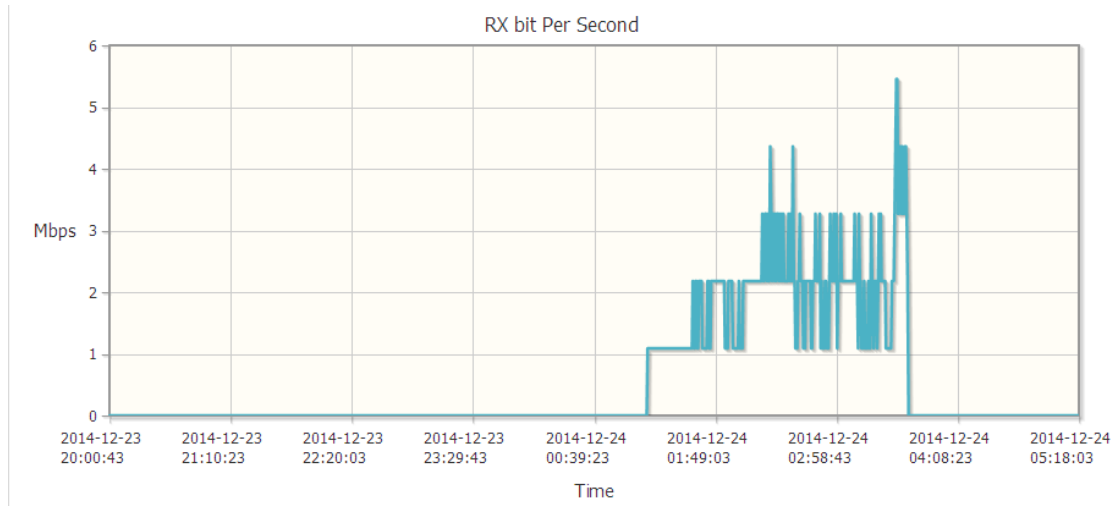


Figure 4-27 Ethernet Historical statistic

4.3.3. Radio Statistics

User may check radios statistics via **Status** → **Historical Statistics** → **Radio** → **Radio0**.

It includes "Throughput", "Busy%", "Tx Usage", "Rx Usage" and "Noise Floor". Select an item from the drop-down menu and click the **Show** button will show detail information.

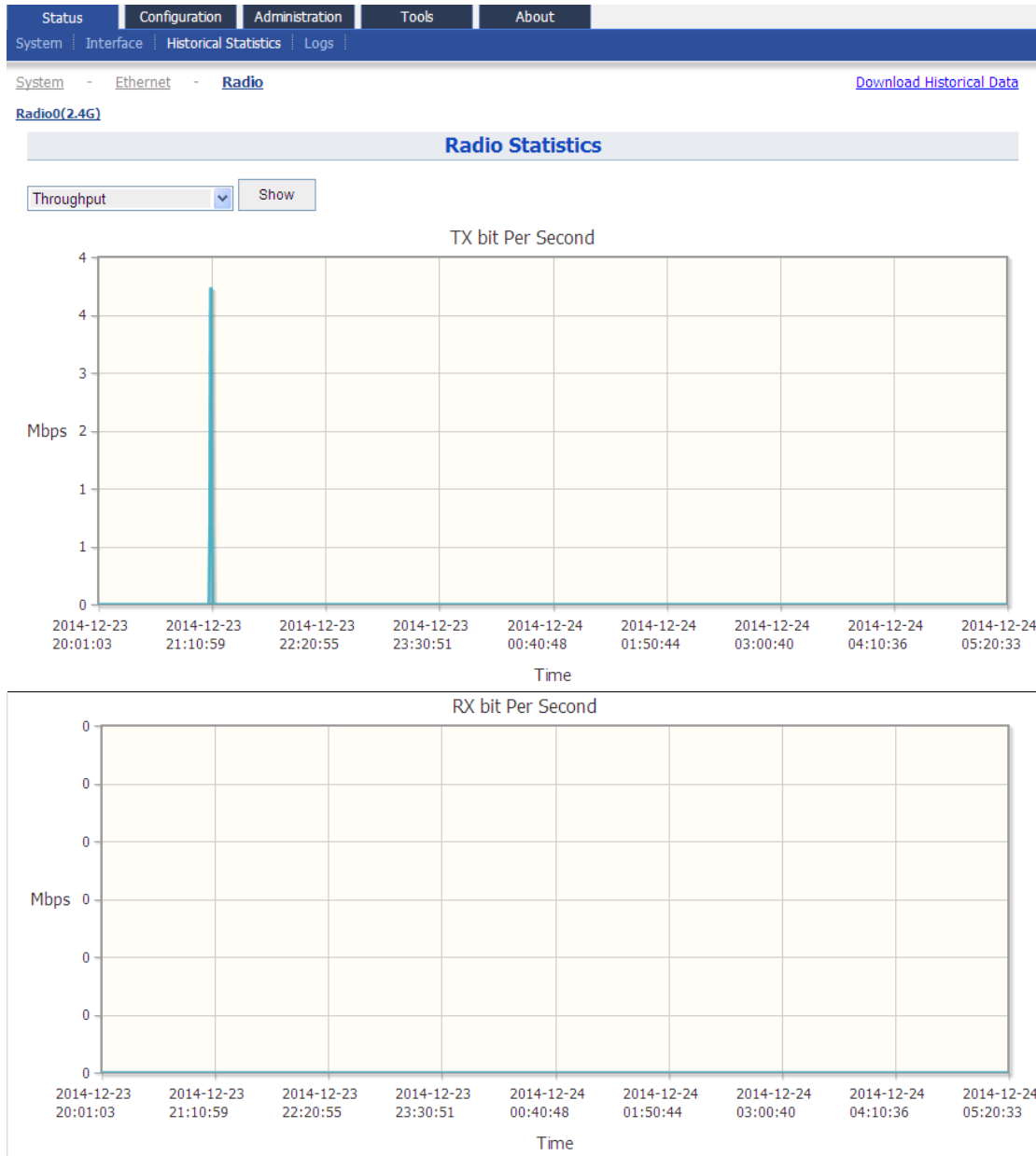


Figure 4-28 Radio0 Historical statistic

1) Radio Historical Statistics - Throughput

Select the "throughput" then click the **Show** button to check the Tx/Rx bit Per Second histogram.

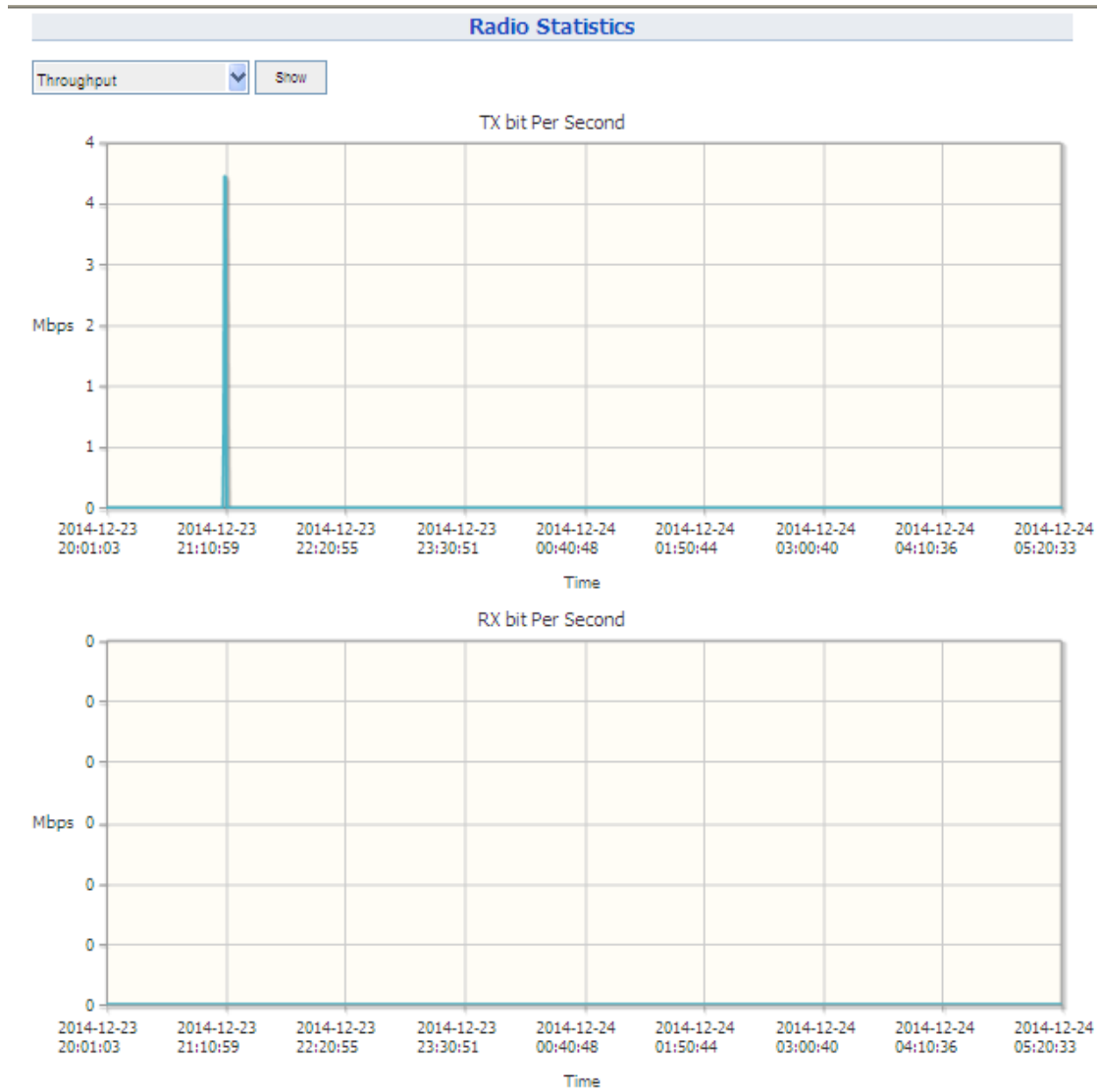


Figure 4-29 Throughput Historical Statistic

2) Radio Historical Statistics - Busy%

Select the "Busy%" then click the **Show** button to check the Radio system busy percentage histogram.

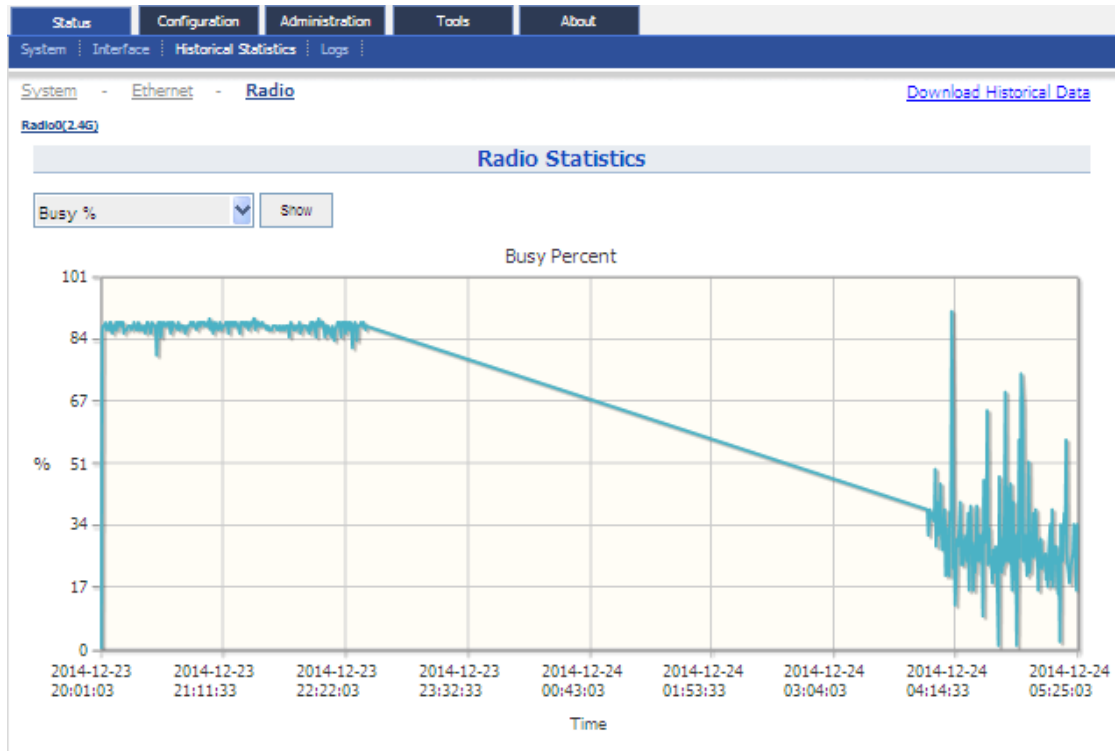


Figure 4-30 Busy% Historical Statistic

3) Radio Historical Statistics - Tx Usage / Rx Usage

Select the "Tx Usage / Rx Usage" then click the **Show** button to check the Tx/Rx usage percentage histogram.

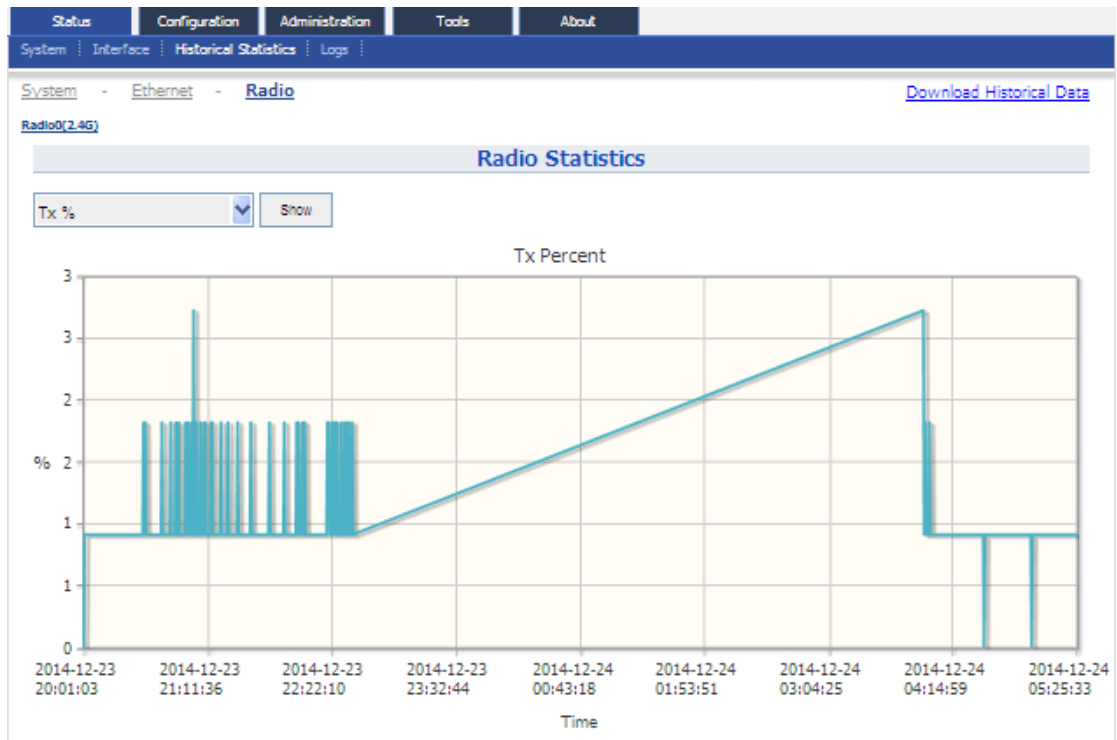


Figure 4-31 Tx Usage Historical Statistic

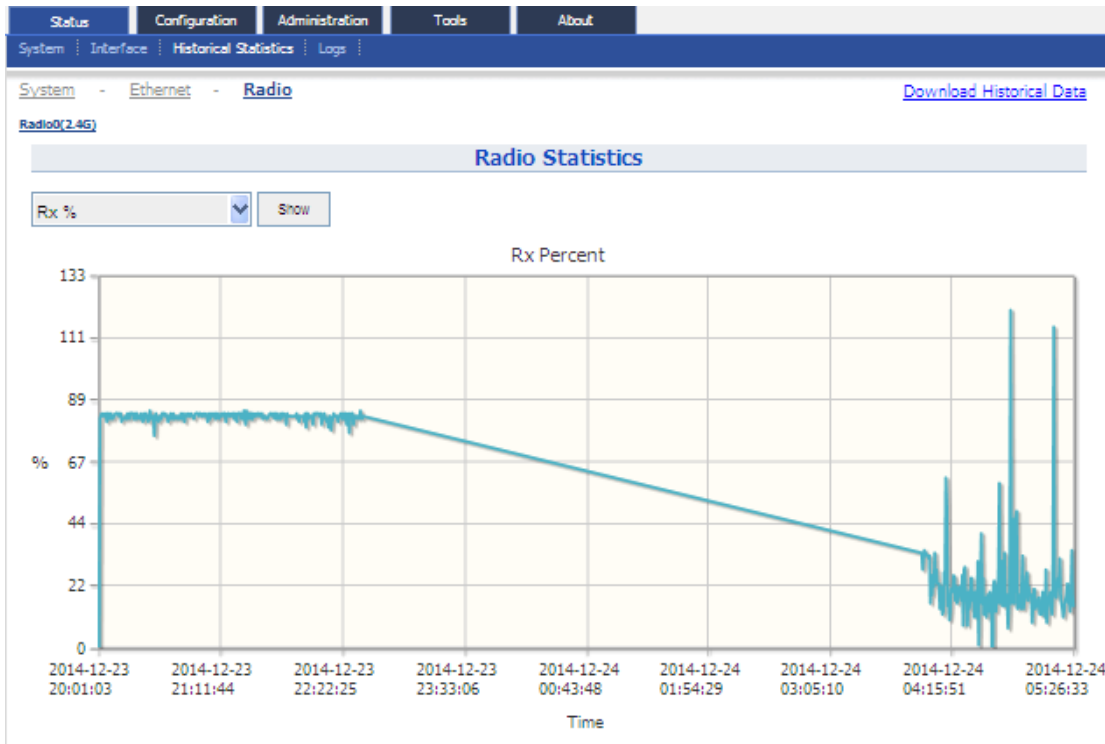


Figure 4-32 Rx Usage Historical Statistic

4) Radio Historical Statistics - Noise Floor

Select the "Noise Floor" then click the **Show** button to check the noise floor histogram.

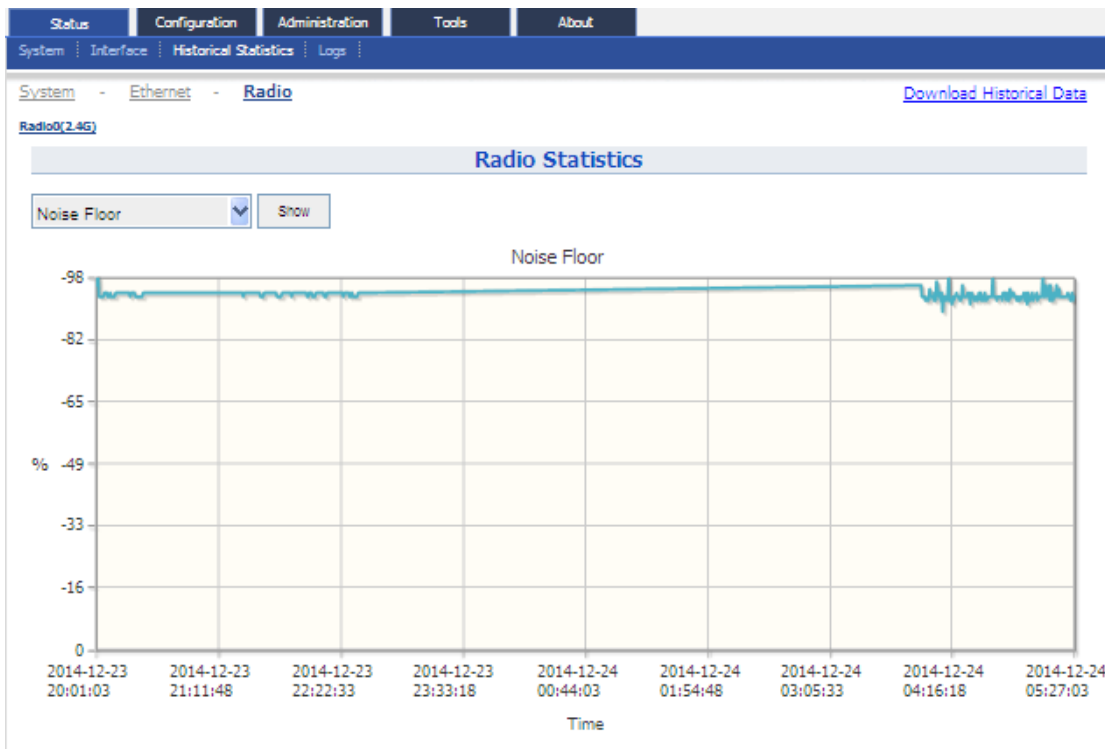


Figure 4-33 Noise Floor Historical Statistic

4.3.4.Logs

In order to realize easier monitoring and diagnosis, C1n Series AP/CPE provides log function. Selecting **Status** -> **Logs**, you will find 3 sub-items below: SysLog, Panic Log, and Alarm Logs.

4.3.4.1. System Log

The system log gives C1n Series AP/CPE system information like: software, hardware, system configuration, and self-checking result. User may check system log via **Status** -> **Log** -> **SysLog**.

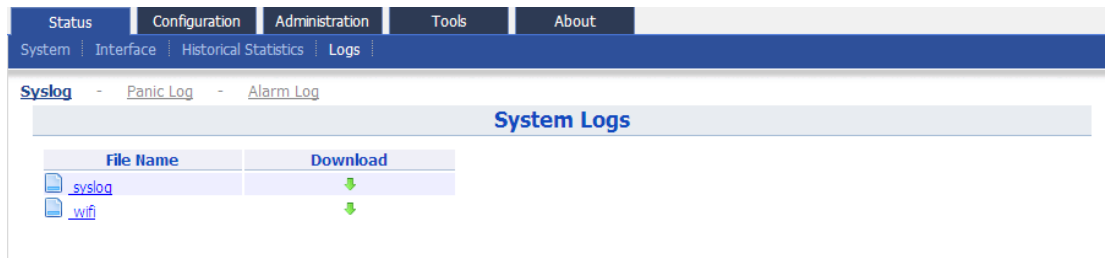


Figure 4-11 System Log

File Name: The name of log files, you can click it to open the log file.

Download: Download log file. Please click the green downward arrow to download the log file.

Click "syslog" under the **File Name**, and you will find the log page below:

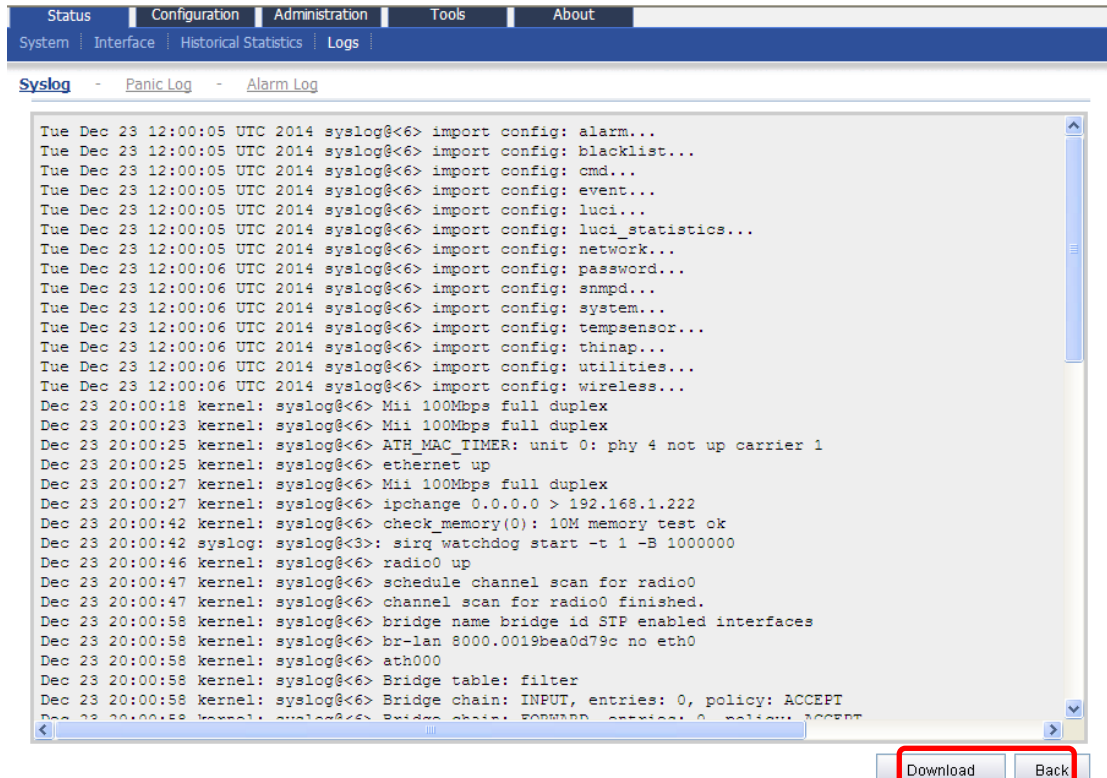


Figure 4-34 System Log “Download and Back” Button

Please click **Download** to download the system log file and click **Back** at the end of log to come back the previous page.

4.3.4.2. Panic Log

Panic Log is a self-generated log when the system finished finds some internal errors and need to reboot itself.

User may check the panic log via **Status**→**Log**→**Panic Log**.

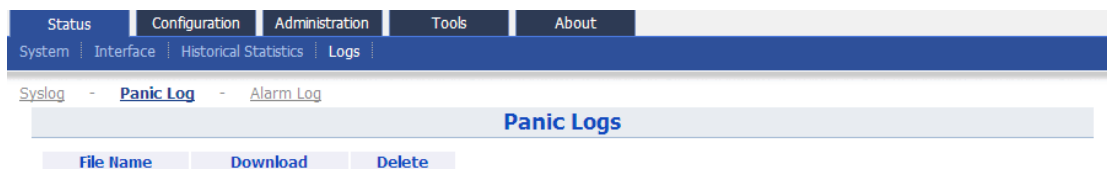


Figure 4-35 Panic Logs

File Name: The name of Panic log files, you can click it to open the log file.

Download: Download Panic log file. Please click the green downward arrow to download the log file.

Delete: Delete Panic log file.

4.3.4.3. Alarm Log

User may check the alarm log via **Status**→**Log**→**Alarm Log**.

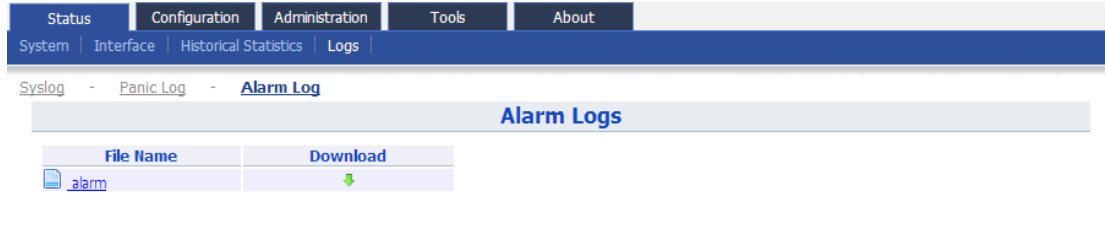


Figure 4-36 Alarm Logs

File Name: The name of log files, you can click it to open the log file.

Download: Download log file. Please click the green downward arrow to download the log file.

5. System Configuration

5.1. C1n Series AP/CPE basic Configuration Procedures

1. Users need to click **Submit** button to store the changed settings.

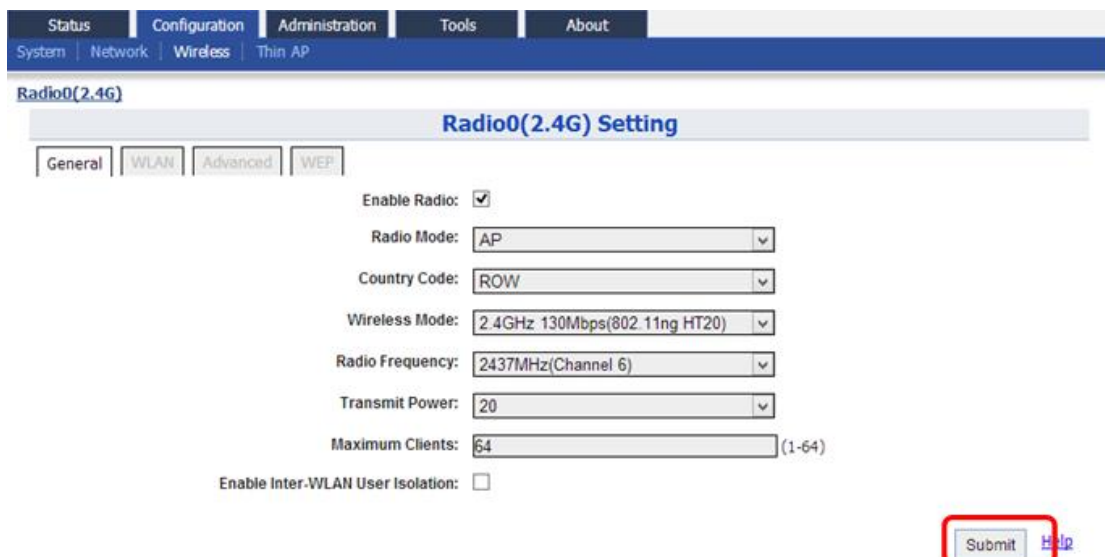


Figure 5-1 Submit Change

2. On the top right corner, there is an **Unsaved Changes** link; User may click it to check submitted items.



Figure 5-2 Unsaved Change

3. Please click **Unsaved Changes** link to review the pending configuration detail information.

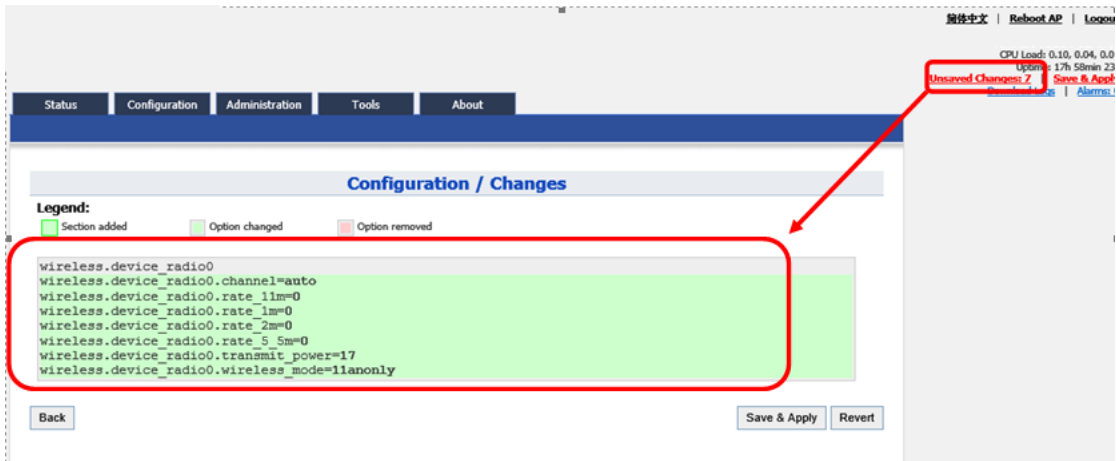


Figure 5-3 Unsaved Change Detail

4. Click **Save&Apply** link to apply all submitted changes:

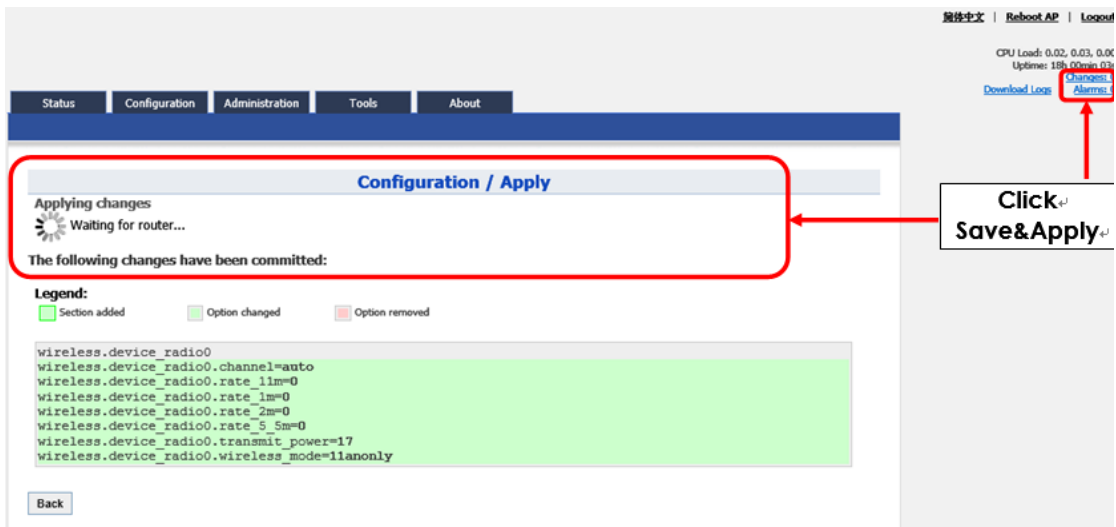


Figure 5-4 Save and Apply Changes

5. You will find "The following changes have been committed"

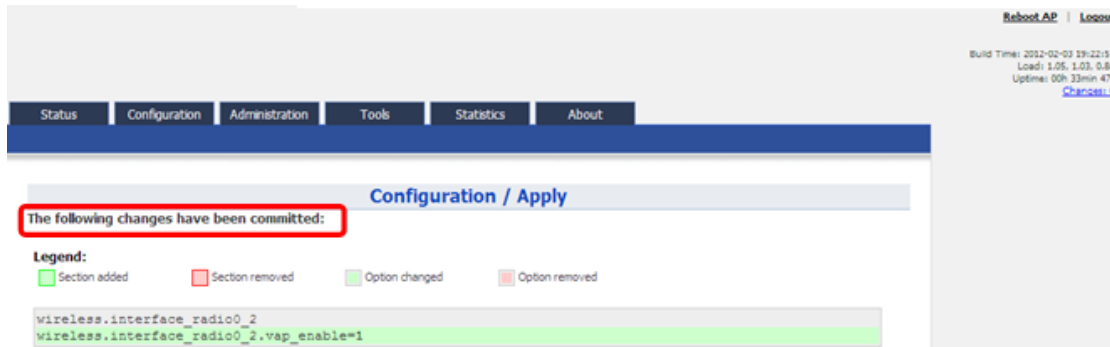


Figure 5-5 Changes have been committed

- The whole committing changes progress, it is no need to reboot C1n Series AP/CPE.

5.2. Basic System Configuration

User may specify the basic system parameters via **Configuration** → **System**. The parameters include System Info Setting, Network Time Protocol (NTP) Setting, and Historical Statistics Collection Setting.

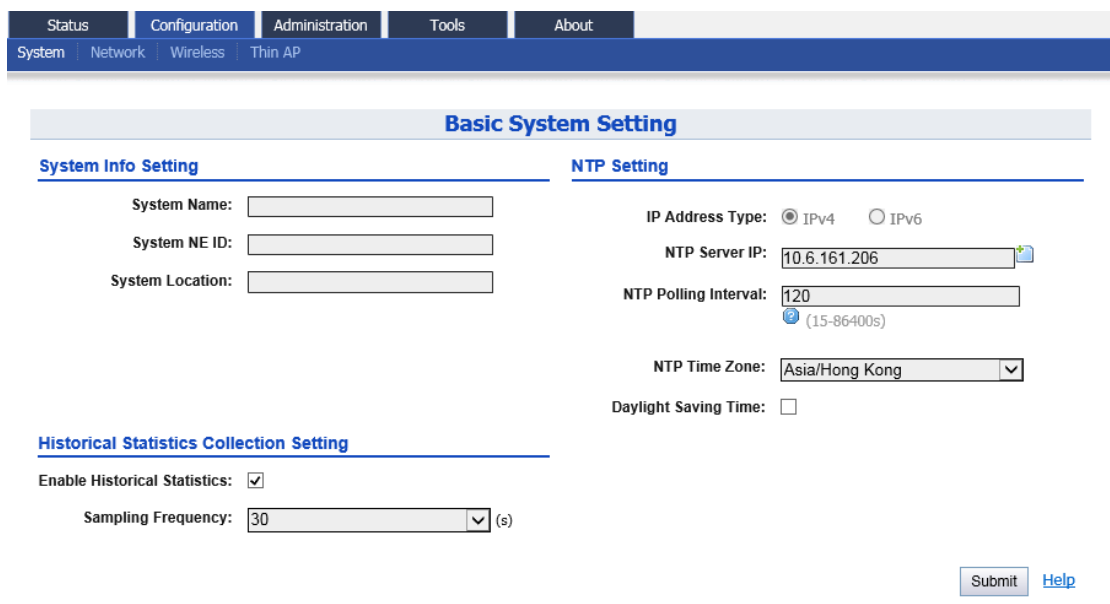


Figure 5-6 NTP Setting

“System Info Setting” is used to set network management information.

System Name: Set system name of the device, the system name can be up to 255 characters long.

System NE ID: Set system NE ID, the system NE ID can be up to 64 characters long.

System Location: Set system location, the system location can be up to 255 characters long.

“NTP Setting” is used to set NTP (network time protocol) information. NTP is a network time protocol for the C1n Series AP/CPE to synchronize the system time. If NTP is

needed, IP address of the NTP server must be added and C1n Series AP/CPE will synchronize with the NTP server. It is useful to maintain the network and make sure all APs are using the same system time by setting the same NTP server.

IP Address Type: IPv4 or IPv6. (Please note that IPv6 is available only if enabling IPv6 in Network setting web page).

NTP Server IP: NTP server IP address, please click “” to add new NTP server IP address.

NTP Polling Interval: By default, it is 600s

NTP Time Zone: Time Zone setting, by default it is Asia/Hong Kong.


Daylight Saving Time: By default, it is not selected.

“Historical Statistics Collection Setting” is used to set Historical Statistics function and the sampling frequency.

Enable Historical Statistics: Enable or Disable Historical Statistic function.

Sampling Frequency: Specify sampling frequency of statistics ; the default setting is 30 seconds per sample.

Procedures:

1. Select **Configuration** -> **System**, to go to system setting page.
2. Type in the system information if necessary.
3. Assign NTP IP address in **NTP Server IP**. Click “” to add NTP server if necessary.
4. Set polling interval in **NTP Polling Interval** from 15s to 86400s. The default setting is 600s.
5. Choose suitable time zone in **NTP Time Zone**
6. Enable day light saving time in **Daylight Saving Time** if necessary
7. Enable Historical Statistics function and select sampling frequency if necessary
8. Click **Submit**
9. Click **Save&Apply** to commit changes.

5.3. Network Configuration

User may configure the network via **Configuration** -> **Network**. The configuration includes General Network Setting, VLAN, DHCP, Port Forward, and Safe Mode.

5.3.1. General Network Configuration

User may configure the network via **Configuration** -> **Network** -> **General**. The parameters include Network Setting, WAN Setting (IPv4 and IPv6), STP Setting, WLAN/LAN Interface Assignment, LAN Setting, and Ethernet Setting.

The screenshot shows the 'General Network Setting' page. The 'Network Setting' section has 'Network Setting' set to 'Switch Mode' and 'Enable IPv6' unchecked. The 'WAN/LAN Interface Assignment' section has 'Ethernet' set to 'WAN' and 'Radio0(2.4G)' set to 'LAN', with 'Enable NAT Mode' checked. The 'WAN Setting (IPv4)' section has 'Internet Connection Type' set to 'Static', 'IPv4 Address' as 10.8.101.222, 'IPv4 Subnet Mask' as 255.255.255.0, and 'IPv4 Default Gateway' as 192.168.1.1. The 'LAN Setting (IPv4)' section has 'LAN IP Address' as 192.168.88.1 and 'LAN IP Address Mask' as 255.255.255.0. The 'WAN Setting (IPv6)' section has 'Internet Connection Type' set to 'Static'. The 'Ethernet Setting' section has 'Ethernet Mode' set to 'auto'. The 'STP Setting' section has 'Enable STP Mode' unchecked. There are 'Submit' and 'Help' buttons at the bottom right.

Figure 5-7 Network Setting

1) Network Setting

C1n can act as Layer 2 switch or Layer 3 gateway.

This screenshot is identical to Figure 5-7, but a red rectangular box highlights the 'Network Setting' section, which includes the 'Network Setting' dropdown menu (set to 'Switch Mode') and the 'Enable IPv6' checkbox (unchecked).

Figure 5-8 Network Setting

Network Setting: The operating mode of C1n, it can be configured as either Switch mode or Gateway mode. If configuring as Switch mode, C1n acts as a switch. It inter-exchanges the packets between Ethernet and WLAN(s); if configuring as Gateway mode, C1n acts as an IP gateway. NAT and DHCP server are available only in Gateway mode. By default, Switch mode is configured.

Enable IPv6: C1n is able to work with both IPv4 network and IPv6 network. Please enable it if AP is connected to IPv6 network; otherwise disable this option. By default, it is disabled.

Configure C1n as switch:

In switch mode, C1n works as a switch to deliver data between Ethernet interface and wireless interfaces.

- 1 Select **Configuration**->**Network**->**General** to go to configuration page.
- 2 Select "Switch Mode" in **Network Setting**.
- 3 Click **Submit**.
- 4 Click **Save&Apply** to apply changes.

Configure C1n as gateway:

In Gateway mode, C1n acts as a gateway. By default, Ethernet is assigned as WAN interface; while Radio interfaces (2.4G or 5G) are assigned as LAN interface. The LAN IP information, i.e. LAN IP address and LAN IP address mask, must be specified in gateway mode. C1n use LAN IP address communicate with the clients inside LAN; C1n use WAN IP address (the IP address under WAN Setting) to communicate with the outside network.

- 1 Select **Configuration**->**Network**->**General** to go to configuration page.
- 2 Select "Gateway Mode" in **Network Setting**.
- 3 Click **Submit**.
- 4 Click **Save&Apply** to apply changes.



Warnings: When the C1n acts as gateway, VLAN function is not available.

2) WLAN Setting (IPv4)

The screenshot shows the 'General Network Setting' page. The 'Network Setting' dropdown is set to 'Switch Mode'. The 'WAN Setting (IPv4)' section is highlighted with a red box and contains the following settings: Internet Connection Type: Static; IPv4 Address: 10.6.161.222; IPv4 Subnet Mask: 255.255.255.0; IPv4 Default Gateway: 192.168.1.1; IPv4 DNS Server IP Address: (empty). The 'LAN Setting (IPv4)' section shows LAN IP Address: 192.168.98.1 and LAN IP Address Mask: 255.255.255.0. The 'Ethernet Setting' section shows Ethernet Mode: auto.

Figure 5-9 WLAN Setting (IPv4)

Internet Connection Type: Static IP or DHCP client

IPv4 Address: If C1n uses static IP , please give it a fixed IP

IPv4 Subnet Mask: If C1n uses static IP , please give it a subnet mask

IPv4 Default Gateway: If C1n uses static IP, please give it a Gateway address

IPv4 DNS Server: If C1n uses static IP, please set DNS IP address

There are 2 internet connection types: Static or DHCP, in both Switch mode and Gateway mode.

Configure C1n with static IPv4 IP address:

User configures C1n IP address, subnet mask, gateway address, and DNS server IP address manually:

- 1 Select **Configuration**->**Network**->**General**
- 2 Select "Static" in **Internet Connection Type**.
- 3 Set IP address in **IP Address**.
- 4 Set IP address mask in **Subnet Mask**.
- 5 Set gateway's IP address mask in **Default Gateway Address**.
- 6 Set DNS server's IP address mask in **DNS Server IP Address**.
- 7 Click **Submit**
- 8 Click **Save&Apply** to apply

Configure C1n to obtain IPv4 address from DHCP server:

C1n obtains IP configuration from DHCP server automatically:

- 1 Select **Configuration**->**Network**->**General**
- 2 Select "DHCP" in **Internet Connection Type**.
- 3 Click **Submit**
- 4 Click **Save&Apply** to apply

3) WLAN Setting (IPv6)

The screenshot shows the 'General Network Setting' page. The 'WAN Setting(IPv6)' section is highlighted with a red box. It contains the following fields:

- Internet Connection Type: Static
- IPv6 Address: [Input field]
- IPv6 Default Gateway: [Input field]
- IPv6 DNS Server: [Input field]

Figure 5-10 WLAN Setting (Ipv6)

Internet Connection Type: Static IP or DHCP client

IPv6 Address: If C1n uses static IP , please give it a fixed IP

IPv6 Default Gateway: If C1n uses static IP, please give it a Gateway address

IPv6 DNS Server: If C1n uses static IP, please set DNS IP address

The WAN Setting(IPv6) configure procedure is similar to WAN Setting(IPv4)

4) STP Setting

The screenshot shows the 'General Network Setting' page. The 'STP Setting' section is highlighted with a red box. It contains the following field:

- Enable STP Mode:

Figure 5-11 STP Setting

Enable STP Mode: Enable or disable the STP service.

5) WAN/LAN Interface Assignment

The screenshot displays the 'General Network Setting' page in the ALTAI web-admin interface. The page is divided into several sections:

- Network Setting:** Network Setting is set to 'Switch Mode'. 'Enable IPv6' is checked.
- WAN Setting (IPv4):** Internet Connection Type is 'DHCP'. 'Enable DHCP Option 60' is unchecked.
- WAN Setting (IPv6):** Internet Connection Type is 'DHCP'.
- STP Setting:** 'Enable STP Mode' is unchecked.
- WAN/LAN Interface Assignment (highlighted):** 'Ethernet' is set to 'WAN'. 'Radio0(2.4G)' is set to 'LAN'. 'Enable NAT Mode' is checked.
- LAN Setting (IPv4):** LAN IP Address is 192.168.98.1. LAN IP Address Mask is 255.255.255.0.
- Ethernet Setting:** Ethernet Mode is 'auto'.

Buttons for 'Submit' and 'Help' are located at the bottom right of the configuration area.

Figure 5-12 WAN/LAN Interface Assignment

Ethernet/Radio0: Specify Ethernet, Radio0 as either LAN interface or WAN interface, it is only available in gateway mode.

Enable NAT Mode: If NAT Mode is set as "disable", the AP will not perform any network address translations on all traffics. The traffics that passed from the wireless clients to the DS (Ethernet) port or wireless bridge (802.11a radio) is not modified. If NAT Mode is set as "enable", the AP will perform network address translations on all traffic. AP translates IP address between the wireless client subnet and the DS subnet for the traffics that passed from the wireless clients to the DS (Ethernet) port or wireless bridge (802.11a radio). This option is only available in gateway mode.

6) LAN Setting (IPv4)

The screenshot shows the 'General Network Setting' page. The 'LAN Setting (IPv4)' section is highlighted with a red box. It contains the following fields:

- LAN IP Address: 192 . 168 . 98 . 1
- LAN IP Address Mask: 255 . 255 . 255 . 0

Other visible settings include:

- Network Setting: Switch Mode
- Enable IPv6:
- WAN Setting (IPv4): Internet Connection Type: DHCP
- WAN Setting (IPv6): Internet Connection Type: DHCP
- STP Setting: Enable STP Mode:
- WAN/LAN Interface Assignment: Ethernet: WAN, LAN; Radio0(2.4G): WAN, LAN; Enable NAT Mode:
- Ethernet Setting: Ethernet Mode: auto

Figure 5-13 LAN Setting (IPv4)

LAN IP Address: IP address of local area network. it is only available in gateway mode.

LAN IP Address Mask: IP address mask of local area network. it is only available in gateway mode.

7) Ethernet Setting

The screenshot shows the 'General Network Setting' page. The 'Ethernet Setting' section is highlighted with a red box. It contains the following field:

- Ethernet Mode: auto

Other visible settings include:

- Network Setting: Switch Mode
- Enable IPv6:
- WAN Setting (IPv4): Internet Connection Type: DHCP
- WAN Setting (IPv6): Internet Connection Type: DHCP
- STP Setting: Enable STP Mode:
- WAN/LAN Interface Assignment: Ethernet: WAN, LAN; Radio0(2.4G): WAN, LAN; Enable NAT Mode:
- LAN Setting (IPv4): LAN IP Address: 192 . 168 . 98 . 1; LAN IP Address Mask: 255 . 255 . 255 . 0

Figure 5-14 Ethernet Setting

Ethernet Mode: Detection mode of Ethernet link operation; the default setting is "auto".

Ethernet Duplex: AP Ethernet link operation mode; option includes 10 Mbps (Full duplex/Half duplex), and 100 Mbps (Full duplex/Half duplex). This option is only available if Ethernet mode is set as "manual".

Configure C1n with Ethernet auto-negotiation:

C1n performs auto-negotiation to select transmission parameters in Ethernet port, such as speed, duplex mode.

- 1 Select **Configuration**->**Network**->**General**
- 2 Select "auto" in **Ethernet Mode**.
- 3 Click **Submit**
- 4 Click **Save&Apply** to apply

Configure C1n without Ethernet auto-negotiation:

User configures the speed and duplex mode of Ethernet port manually. The option includes 100Mbps (Full/Half), and 10Mbps (Full/Half).

1. Select **Configuration**->**Network**->**General**
2. Select "manual" in **Ethernet Mode**.
3. Select suitable speed and duplex mode in **Ethernet Duplex**.
4. Click **Submit**
5. Click **Save&Apply** to apply

5.3.2. VLAN

User may configure VLAN setting via **Configuration** ->**Network** ->**VLAN**.

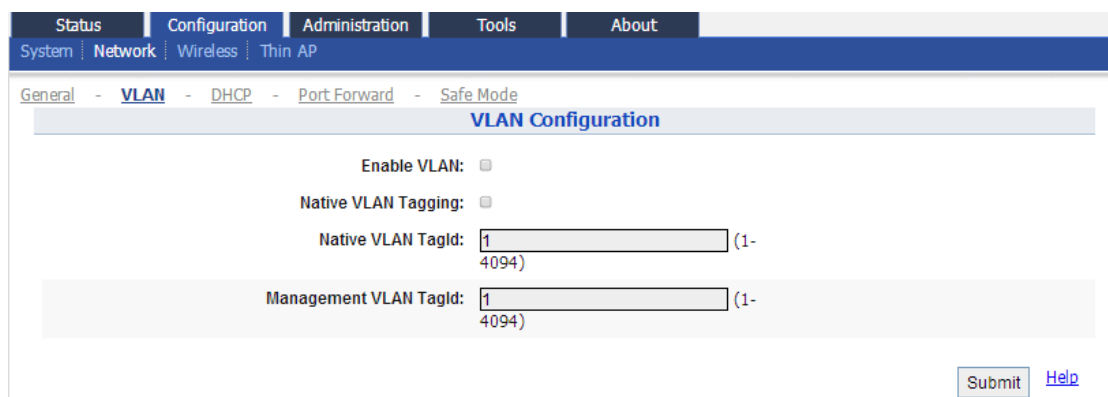


Figure 5-15 VLAN Setting

Enable VLAN: Enable or Disable VLAN function. By default, C1n Series CPE/AP VLAN setting is disabled.

Native VLAN Tagging: Enable or Disable Native VLAN Tagging; if enabled, C1n tags the incoming frame, which is untagged, with native VLAN id before forwarding the frame. By default, it is "disable".

Native VLAN TagId: Specify Native VLAN ID.

Management VLAN TagId: Specify Management VLAN ID.

Configure C1n with VLAN:

1. Select **Configuration** → **Network** → **VLAN**
2. Check **Enable VLAN**.
3. Check **Native VLAN Tagging** if necessary.
4. Specify Native VALN ID in **Native VLAN TagId** if necessary.
5. Specify Management VALN ID in **Management VLAN TagId**.
6. Specify VALN ID for each WLAN.
7. Click **Submit**
8. Click **Save&Apply** to apply

To specify VLAN ID for each WLAN, please refer to section **WLAN configuration** for more detail.

5.3.3. DHCP Server

DHCP Server function is available in Gateway Mode only. User may enable and configure DHCP server via **Configuration** → **Network** → **DHCP**. There are two options, Disable and Server Mode. If DHCP Server is set as "Server Mode", C1n acts as a DHCP server of LAN interface. It distributes network configuration parameters to all associated clients, such as IP address, gateway's IP address ...etc. User may specify the address pool setting by click the icon "🔍" under "Detail" column.

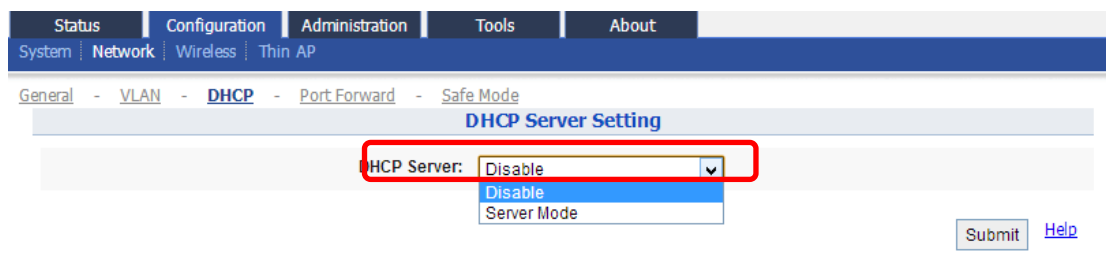


Figure 5-8 DHCP Server Setting drop-down Menu

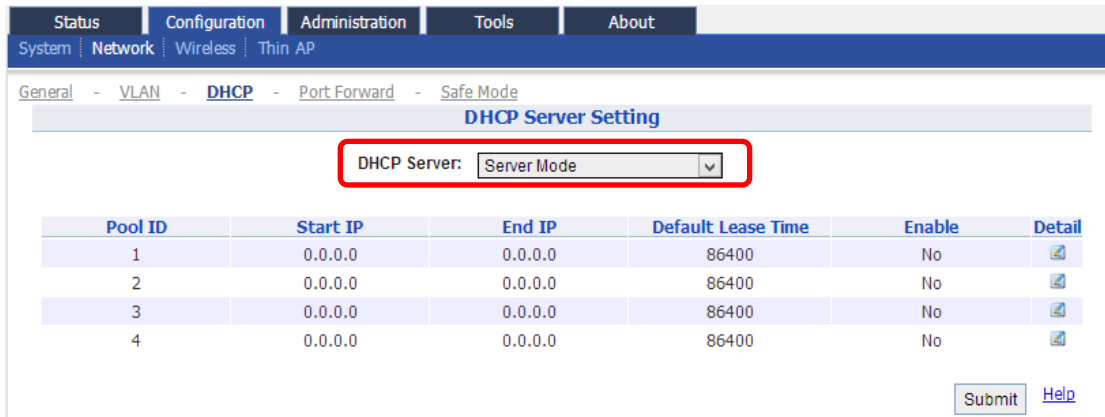


Figure 5-9 DHCP Server Mode Setting

If the DHCP Server Mode is set to Server, then the C1n Series CPE/AP will act as a DHCP server for allocation of IP address to the wireless client associated. The following procedures show the allocation of the IP address, subnets mask, gateway and DNS information. And edit the Pool ID 1.

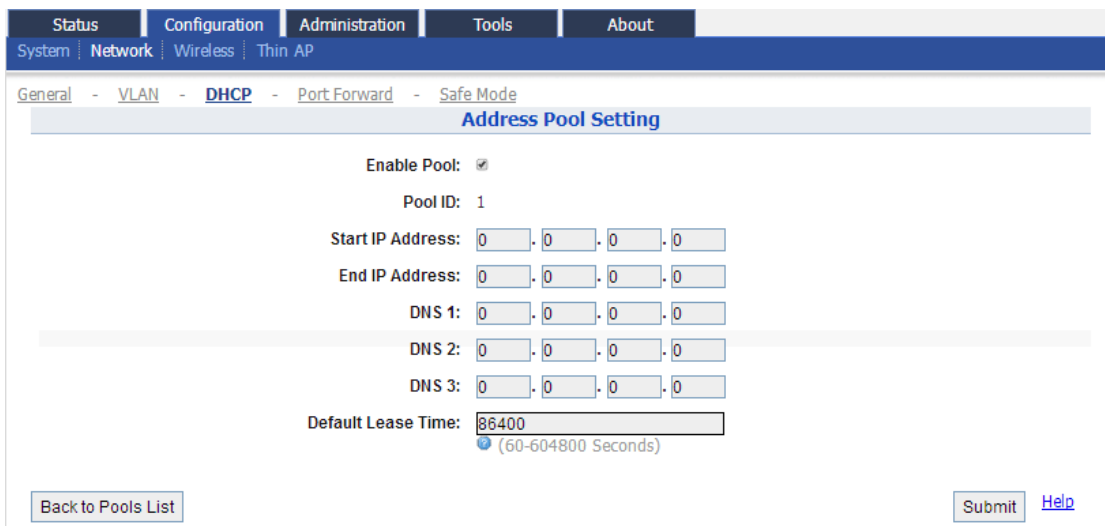


Figure 5-10 DHCP Server - Address Pool Setting

Enable Pool: Enable or Disable Pool

Pool ID: ID of the IP Pool


Start IP Address: Start IP address of the Pool

End IP Address: End IP address of the Pool


DNS1, 2, 3: DNS IP address of the Pool

Default Lease Time: Time to release the IP address to the clients

Configure C1n as DHCP server:

1. Select **Configuration** -> **Network** -> **DHCP**
2. Select "Server Mode" in **DHCP Server**.
3. Click **Submit**
4. Click the icon "" under "Detail" column.
5. Check **Enable Pool**
6. Provide IP address range for leasing by filling IP addresses in both **Start IP Address** and **End IP Address** respectively.
7. Set at least one DNS server's IP address in **DNS1**, **DNS 2**, or **DNS 3**.
8. Configure lease time in **Default Lease Time** from 60 s to 60480s. The default value is 86400s.
9. Click **Submit**
10. Click **Save&Apply** to apply

5.3.4. Port Forwarding

The Port forwarding service is only available at gateway mode. User may enable and configure port forward via **Configuration** -> **Network** -> **Port Forwarding**. The function is used to permit communications by external hosts with services provided within a private local area network. User may specify the port forward setting by click the icon "" under "Detail" column.

| ID | Local IP | Local Port | Type | Global Port | Enable | Detail |
|----|----------|------------|-----------|-------------|--------|--------|
| 1 | 0.0.0.0 | 0 | TCP & UDP | 0 | No | |
| 2 | 0.0.0.0 | 0 | TCP & UDP | 0 | No | |
| 3 | 0.0.0.0 | 0 | TCP & UDP | 0 | No | |
| 4 | 0.0.0.0 | 0 | TCP & UDP | 0 | No | |
| 5 | 0.0.0.0 | 0 | TCP & UDP | 0 | No | |
| 6 | 0.0.0.0 | 0 | TCP & UDP | 0 | No | |
| 7 | 0.0.0.0 | 0 | TCP & UDP | 0 | No | |
| 8 | 0.0.0.0 | 0 | TCP & UDP | 0 | No | |
| 9 | 0.0.0.0 | 0 | TCP & UDP | 0 | No | |
| 10 | 0.0.0.0 | 0 | TCP & UDP | 0 | No | |
| 11 | 0.0.0.0 | 0 | TCP & UDP | 0 | No | |
| 12 | 0.0.0.0 | 0 | TCP & UDP | 0 | No | |
| 13 | 0.0.0.0 | 0 | TCP & UDP | 0 | No | |
| 14 | 0.0.0.0 | 0 | TCP & UDP | 0 | No | |
| 15 | 0.0.0.0 | 0 | TCP & UDP | 0 | No | |
| 16 | 0.0.0.0 | 0 | TCP & UDP | 0 | No | |
| 17 | 0.0.0.0 | 0 | TCP & UDP | 0 | No | |
| 18 | 0.0.0.0 | 0 | TCP & UDP | 0 | No | |
| 19 | 0.0.0.0 | 0 | TCP & UDP | 0 | No | |
| 20 | 0.0.0.0 | 0 | TCP & UDP | 0 | No | |

Figure 5-11 Port Forwarding

Port Forward Setting

Enable:

ID: 1

Local IP Address: . . .

Local Port:

Protocol Type:

Global Port:

Description:

[Help](#)

Figure 5-12 Port Forwarding Setting

Enable: Whether the particular port forwarding entry is active or not; all the port forwarding entries are saved in system configuration file. Only the enabled entries take effect.

Local IP Address: Specify the host, which is connected to the internal network, is accessible from the external network.


Local Port: Specify the port number of the application running on the host, which is connected to the internal network, is accessible from the external network.

Protocol Type: Specify Transport Layer protocol that the application uses . The options are "TCP&UDP", "TCP", and "UDP".

Global Port: Specify the listen port on WAN interface of C1n; C1n accepts and forwards the traffic from the external network via global port to the particular host.

Description: Additional information about the port forwarding entry.

Enable port forwarding in C1n:

1. Select **Configuration** -> **Network** -> **Port Forwarding**
2. Click the icon "" under "Detail" column.
3. Check **Enable**
4. Specify host's IP address in **Local IP Address**
5. Specify host's port in **Local Port**
6. Specify Transport Layer protocol in **Protocol Type**
7. Specify C1n listen port in **Global Port**
8. Type in a port forward entry's description in **Description** if necessary
9. Click **Submit**
10. Click **Save&Apply** to apply

5.3.5. Safe Mode

User may configure Safe mode via **Configuration** -> **Network** -> **Safe Mode**. Safe Mode is 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 in hexadecimal. This action can protect 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. By default, Safe Mode is disabled.

The screenshot shows the web-admin interface for the C1n Series. The top navigation bar includes 'Status', 'Configuration', 'Administration', 'Tools', and 'About'. Under 'Configuration', there are sub-menus for 'System', 'Network', 'Wireless', and 'Thin AP'. The 'Network' sub-menu is expanded, showing 'General', 'VLAN', 'DHCP', 'Port Forward', and 'Safe Mode'. The 'Safe Mode' sub-menu is selected, leading to the 'Safe Mode Setting' page. This page contains the following settings:

- Enable Safe Mode:** A checkbox that is currently unchecked.
- Ping Host 1:** An input field with the value '0'.
- Ping Host 2:** An input field with the value '0'.
- Ping Host 3:** An input field with the value '0'.
- Ping Interval:** An input field with the value '10' and a range of '(3-30s)'.

At the bottom right of the form, there is a 'Submit' button and a 'Help' link.

Figure 5-13 Safe Mode Setting

Enable Safe Mode: Enable or disable safe mode. By default, it is disabled.

Ping Host 1, 2, 3: Three ping hosts can be specified. AP will ping these hosts periodically at the ping interval configured through its current backhaul link.

Ping Interval: Specify the ping interval of safe mode from 3s to 30s. Default setting is 10 seconds.

Enable safe mode in C1n:

- 1 Select **Configuration** → **Network** → **Safe Mode**
- 2 Click **Enable Safe Mode**.
- 3 Specify at least one server's IP address in **Ping Host 1**, **Ping Host 2**, or **Ping Host 3**
- 4 Specify the ping interval time in **Ping Interval**.
- 5 Click **Submit**
- 6 Click **Save&Apply** to apply

5.4. Wireless

User may configure wireless network via **Configuration** → **Wireless**. C1n and C1an only have 2.4GHz Radio, C1an and C1xan only have 5GHz Radio.

The screenshot shows the 'Radio0(2.4G) Setting' page in the web-admin interface. The 'Radio0(2.4G)' tab is highlighted with a red box. The page contains the following settings:

- Enable Radio:**
- Radio Mode:** AP
- Country Code:** HONG KONG
- Wireless Mode:** 2.4GHz 130Mbps(802.11ng HT20)
- Radio Frequency:** 2412MHz(Channel 1)
- Transmit Power:** 29
- Maximum Clients:** 200 (1-256)
- Enable Inter-WLAN User Isolation:**

Buttons for 'Submit' and 'Help' are located at the bottom right of the configuration area.

Figure 5-22 Radio Setting

5.4.1. Radio0 Configuration

User may configure wireless network on radio0 via **Configuration** -> **Wireless** -> **Radio0**. The content is related with Radio Mode, C1n and C1xn have AP/Station/Repeater mode, C1an and C1xan have AP/Station/Repeater/Bridge mode.

5.4.1.1. Radio0 Configuration – AP Mode

5.4.1.1.1. General Configuration

User may set Radio0 general configuration via **Configuration** -> **Wireless** -> **Radio0** -> **General**.

The screenshot shows the 'Radio0(2.4G) Setting' page. At the top, there are navigation tabs: Status, Configuration, Administration, Tools, and About. Below these are sub-tabs: System, Network, Wireless, and Thin AP. The main content area is titled 'Radio0(2.4G) Setting' and has sub-tabs: General, WLAN, Advanced, QoS, and WEP. The 'General' tab is selected. The settings are as follows:

- Enable Radio:
- Radio Mode: AP
- Country Code: HONG KONG
- Wireless Mode: 2.4GHz 130Mbps(802.11ng HT20)
- Radio Frequency: 2412MHz(Channel 1)
- Transmit Power: 29
- Maximum Clients: 200 (1-256)
- Enable Inter-WLAN User Isolation:

At the bottom right, there are 'Submit' and 'Help' buttons.

Figure 5-23 Radio Parameters

Enable Radio: Enable or disable radio0, by default it is enabled.

Radio Mode: Operation mode of radio0, It can be configured as AP, Station, Repeater or Bridge.

Country Code: Specify country that C1n locates. This setting is related about radio regulatory domain, such as maximum transmission power, available operating frequency channel ... etc. Hong Kong is default setting.

Wireless Mode: Specify wireless mode of C1n; User may configure the WLAN standard and channel bandwidth via this option.

Radio Frequency: Specify the operating frequency channel. User may select "auto" or fix a frequency channel manually. If "auto" is selected, C1n selects the best channel automatically.

Transmit Power: Specify the transmission power (dBm) of radio0.

Maximum Clients: Specify the maximum number of users C1n serves. The value should less than 256.

Enable Inter-WLAN User Isolation: Allow or block inter-WLAN user communication. If enabled, clients cannot communicate to each other directly when they associated into different WLAN. By default, it is "disable".

Disable HT20/HT40 Auto Switch: C1n may change the channel bandwidth between 20 MHz and 40 MHz automatically during operating time. This option disables such change if user enables this function. This option is available if **Wireless Mode** is configured as HT40.

Periodic Auto channel Selection: Specify how often C1n selects the operating channel for WLAN. If enabled, user may specify channel selection time by either schedule or periodic. This option is available if **Radio Frequency** is configured as "auto"

Dynamic Radio Frequency Selection (DFS): This configuration item can only have in C1an and C1xan. DFS is a mechanism to allow unlicensed devices to use the 5 GHz frequency bands already allocated to radar systems without causing interference to those radars. When enabled, AP monitors radar during CAC period. Provided that no radar is detected during CAC period, a communication link is established on the selected channel. CAC period is 10 minutes between 5.6GHz and 5.65GHz; while CAC period is 60 seconds outside 5.6GHz and 5.65GHz.

Remark: The Radio Frequency must be set to "Auto".

Configure radio0 as AP:

- 1 Select **Configuration** → **Wireless** → **Radio0** → **General**
- 2 Check **Enable Radio**.
- 3 Select to "AP" in **Radio Mode**
- 4 Select your country code in **Country Code**
- 5 Select desire wireless mode in **Wireless Mode**
- 6 Select operating channel in **Radio Frequency**
- 7 Set maximum transmit power in **Transmit Power**
- 8 Set the maximum number of users Radio0 serves in **Maximum Clients**
- 9 Check **Enable Inter-WLAN User Isolation** if necessary.
- 10 Check **Periodic Auto channel Selection** if necessary; please specify channel selection time by either schedule or periodic if **Periodic Auto channel Selection** is enabled.
- 11 Click **Submit**
- 12 Click **Save&Apply** to apply

5.4.1.1.2. WLAN Configuration

C1n Series AP/CPE radio0 supports maximum 16 WLANs, and they can be configured separately. User may configure each individual WLAN via **Configuration** → **Wireless** → **Radio0** → **WLAN**.

Status Configuration Administration Tools About

System Network Wireless Thin AP

Radio0(2.4G)

Radio0(2.4G) Setting

General WLAN Advanced QoS WEP

WLAN Configuration

| WLAN | SSID | Max Clients | Isolation | VLAN Pass-Through/ID | Auth Mode | Access Traffic Right | WLAN Uplink/Downlink Control | | | | Station Uplink/Downlink Control | Detail | |
|-----------------------------|---|-------------|--------------------------|--|-----------|----------------------|------------------------------|---|---|---|---------------------------------|--------|---------|
| <input type="checkbox"/> 0 | ircao-local <input type="checkbox"/> Hide SSID | 128 | <input type="checkbox"/> | 1 <input type="checkbox"/> Pass through | open | Full Access | 0 | 0 | 0 | 0 | 0 | 0 | More... |
| <input type="checkbox"/> 1 | ircao-tunnel <input type="checkbox"/> Hide SSID | 75 | <input type="checkbox"/> | 355 <input type="checkbox"/> Pass through | open | Full Access | 0 | 0 | 0 | 0 | 0 | 0 | More... |
| <input type="checkbox"/> 2 | ircao-tunnel2 <input type="checkbox"/> Hide SSID | 32 | <input type="checkbox"/> | 366 <input type="checkbox"/> Pass through | open | Full Access | 0 | 0 | 0 | 0 | 0 | 0 | More... |
| <input type="checkbox"/> 3 | ircao-tunnel3 <input type="checkbox"/> Hide SSID | 32 | <input type="checkbox"/> | 330 <input type="checkbox"/> Pass through | open | Full Access | 0 | 0 | 0 | 0 | 0 | 0 | More... |
| <input type="checkbox"/> 4 | Superwifi Network <input type="checkbox"/> Hide SSID | 256 | <input type="checkbox"/> | 1 <input type="checkbox"/> Pass through | open | Full Access | 0 | 0 | 0 | 0 | 0 | 0 | More... |
| <input type="checkbox"/> 5 | Superwifi Network <input type="checkbox"/> Hide SSID | 256 | <input type="checkbox"/> | 1 <input type="checkbox"/> Pass through | open | Full Access | 0 | 0 | 0 | 0 | 0 | 0 | More... |
| <input type="checkbox"/> 6 | Superwifi Network <input type="checkbox"/> Hide SSID | 256 | <input type="checkbox"/> | 1 <input type="checkbox"/> Pass through | open | Full Access | 0 | 0 | 0 | 0 | 0 | 0 | More... |
| <input type="checkbox"/> 7 | Superwifi Network <input type="checkbox"/> Hide SSID | 256 | <input type="checkbox"/> | 1 <input type="checkbox"/> Pass through | open | Full Access | 0 | 0 | 0 | 0 | 0 | 0 | More... |
| <input type="checkbox"/> 8 | Superwifi Network <input type="checkbox"/> Hide SSID | 256 | <input type="checkbox"/> | 1 <input type="checkbox"/> Pass through | open | Full Access | 0 | 0 | 0 | 0 | 0 | 0 | More... |
| <input type="checkbox"/> 9 | Superwifi Network <input type="checkbox"/> Hide SSID | 256 | <input type="checkbox"/> | 1 <input type="checkbox"/> Pass through | open | Full Access | 0 | 0 | 0 | 0 | 0 | 0 | More... |
| <input type="checkbox"/> 10 | Superwifi Network <input type="checkbox"/> Hide SSID | 256 | <input type="checkbox"/> | 1 <input type="checkbox"/> Pass through | open | Full Access | 0 | 0 | 0 | 0 | 0 | 0 | More... |
| <input type="checkbox"/> 11 | Superwifi Network <input type="checkbox"/> Hide SSID | 256 | <input type="checkbox"/> | 1 <input type="checkbox"/> Pass through | open | Full Access | 0 | 0 | 0 | 0 | 0 | 0 | More... |
| <input type="checkbox"/> 12 | Superwifi Network <input type="checkbox"/> Hide SSID | 256 | <input type="checkbox"/> | 1 <input type="checkbox"/> Pass through | open | Full Access | 0 | 0 | 0 | 0 | 0 | 0 | More... |
| <input type="checkbox"/> 13 | Superwifi Network <input type="checkbox"/> Hide SSID | 256 | <input type="checkbox"/> | 1 <input type="checkbox"/> Pass through | open | Full Access | 0 | 0 | 0 | 0 | 0 | 0 | More... |
| <input type="checkbox"/> 14 | Superwifi Network <input type="checkbox"/> Hide SSID | 256 | <input type="checkbox"/> | 1 <input type="checkbox"/> Pass through | open | Full Access | 0 | 0 | 0 | 0 | 0 | 0 | More... |
| <input type="checkbox"/> 15 | Superwifi Network <input type="checkbox"/> Hide SSID | 256 | <input type="checkbox"/> | 1 <input type="checkbox"/> Pass through | open | Full Access | 0 | 0 | 0 | 0 | 0 | 0 | More... |

Figure 5-24 Radio0 WLAN Setting

Enable WLAN: Enable or Disable WLAN from 0-15.

SSID: Specify SSID of each WLAN; it supports up to 32 characters. The default SSID is Superwifi Network X, where X is WLAN number.

Max Clients: Specify maximum associated clients of each WLAN. This value must be smaller than or equal to the value of **Maximum Clients** in General setting. The default value is 256.

Isolation: Allow or block intra-WLAN user communication. If enabled, clients cannot communicate to each other directly in the same WLAN. By default, it is enabled.

VLAN Pass-Through/ID: Specify the VLAN ID of WLAN or configure the WLAN that acts as VLAN truck port. This option is available if user enables VLAN. If user specifies a VLAN ID, A2 tags all incoming packets from the radio with VLAN ID, and then forwards

them out. If user specifies a WLAN as VLAN pass through, C1n does not modify the incoming packets that are tagged. Also, C1n tags the packets, which are not tagged, with native VLAN ID if Native VLAN Tagging is enabled.

Auth Mode: Specify security of particular WLAN; wireless client may be authenticated during association.

Access Traffic Right: Specify AP management privilege of associated client; there are 3 options: "Full Access", "AP Management Only", and "AP Management Disable".

"Full Access": Associated client can act as normal user and access AP for configuration.

"AP Management Only": Associated client can access AP for configuration only.

"AP Management Disable": Associated client can act as normal user but cannot access AP.

WLAN Uplink/Downlink Control: Bandwidth control for WLAN; user may limit the maximum speed of uplink and downlink for particular WLAN respectively. The value is in term of kbps. "0" means disable. By default, it is disabled.

Station Uplink/Downlink Control: Bandwidth control for each associated client in particular WLAN; user may limit the maximum speed of uplink and downlink for each associated client in particular WLAN respectively. The value is in term of kbps. "0" means disable. By default, it is disabled.

5.4.1.1.2.1. WLAN X (0-15) General Configuration

C1n Series AP/CPE radio0 supports maximum 16 WLANs, and they can be configured separately. User may have detail configuration of each WLAN via

Configuration → **Wireless** → **Radio0** → **WLAN**, then click "More..." of each WLAN.

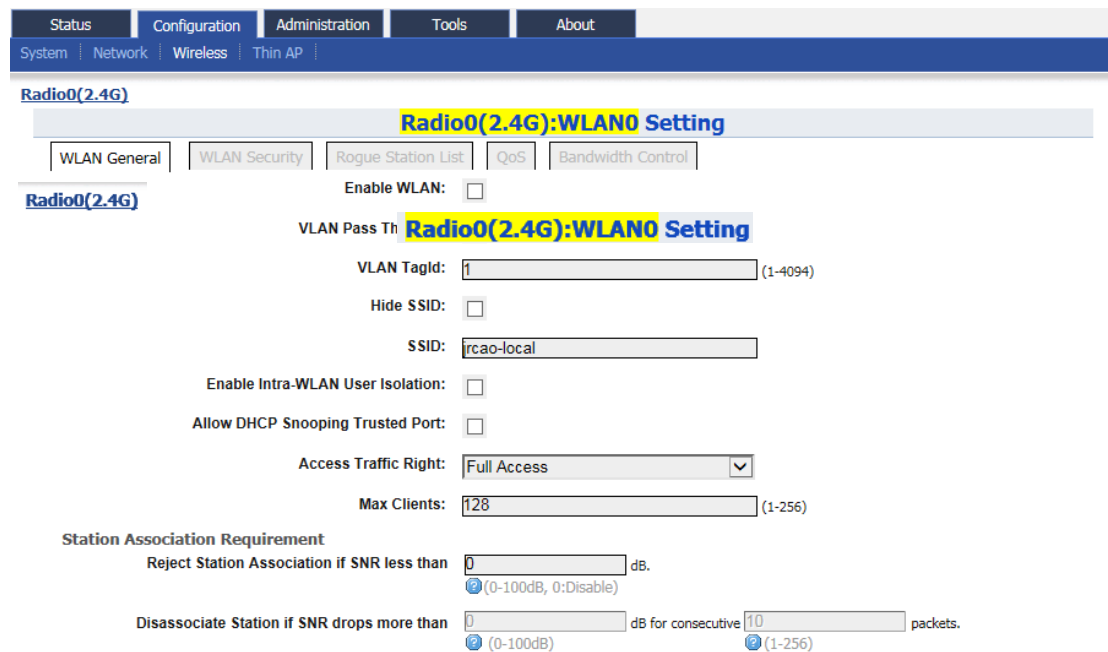


Figure 5-25 WLAN General Setting

Enable WLAN: Enable or disable this WLAN.

VLAN Pass Through: Configure the WLAN that acts as VLAN trunk port. This option is available if user enables VLAN. If user specifies a WLAN as VLAN pass through, C1n does not modify the incoming packets that are tagged. Also, C1n tags the packets, which are not tagged, with native VLAN ID if Native VLAN Tagging is enabled.

VLAN TagId: Specify the VLAN ID of WLAN; this option is available if user enables VLAN. If user specifies a VLAN ID, C1n tags all incoming packets from the radio with VLAN ID, and then forwards them out.

Hide SSID: Specify whether C1n broadcasts this SSID or not. If checked, C1n will not broadcast such SSID.

SSID: Specify SSID of each WLAN; it supports up to 32 characters. The default SSID is Superwifi Network X, where X is WLAN number.

Enable Intra-WLAN User Isolation: Allow or block intra-WLAN user communication. If enabled, clients cannot communicate to each other directly in the same WLAN. By default, it is enabled. By default, it is enabled.

Allow DHCP Snooping Trusted Port: DHCP snooping prevents illegal DHCP servers from offering IP address on untrusted wireless port.

Access Traffic Right: Specify AP management privilege of associated client; there are 3 options: "Full Access", "AP Management Only", and "AP Management Disable".

Max Clients: Specify maximum associated clients of each WLAN. The default value is 256.

Station Association Requirement

Reject Station Association if SNR less than X: Set the minimum signal value X(SNR) for client can associate to this WLAN. When a client's SNR lower than X, This client can't associate to this WLAN, The range is 0~100dB, and 0 means disable.

Disassociate Station if SNR drops more than Y dB for consecutive Z packets: Set the signal threshold value Y(SNR) and the packet threshold value Z. When a client's SNR is lower than Y and loose Z packets consecutively, this client will be disassociated from Radio0.

Back to WLAN List: Go back to previous page

Configure a WLAN in Radio0:

1. Select **Configuration** → **Wireless** → **Radio0** → **WLAN** to click "**More...**" behind the WLAN, and then select **WLAN General**.
2. Check **Enable WLAN**.
3. Enable VLAN pass through in **VLAN Pass Through** or set VLAN ID in **VLAN TagId** if necessary.
4. Specify whether Radio0 broadcasts this SSID.
5. Specify SSID in **SSID**.
6. Enable **Intra-WLAN User Isolation** if necessary.
7. Select WLAN's Access Traffic Right.
8. Set the maximum number of users this WLAN serves in **Max Clients**.
9. Set the values in **Reject Station Association if SNR less than X**, **Disassociate Station if SNR drops more than Y**, and **for consecutive Z packets** if necessary.

10. Click **Submit**
11. Click **Save&Apply** to apply

5.4.1.1.2.2. WLAN X (0-15) Security

C1n supports different wireless security scheme to prevent unauthorized access. User may enable the wireless security with different combination of authentication scheme and cipher scheme. The default security setting is Open without cipher scheme, i.e. no security and data encryption. User may specify the wireless security via **Configuration**→**Wireless**→**Radio0**→**WLAN** to select "**More...**" behind the WLAN, and then select **WLAN Security** to access to security configuration page.

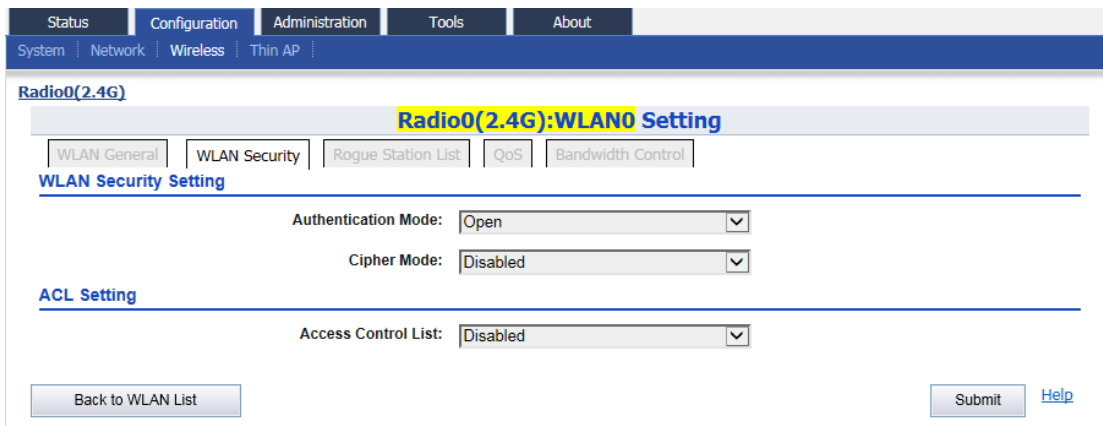


Figure 5-26 WLAN Security Setting

1) Open

If a WLAN opens to the public without any authentication, user may configure authentication mode of that WLAN as "Open". User may enable the cipher mode when authentication mode is set as "Open". The option of cipher mode is "WEP" only.

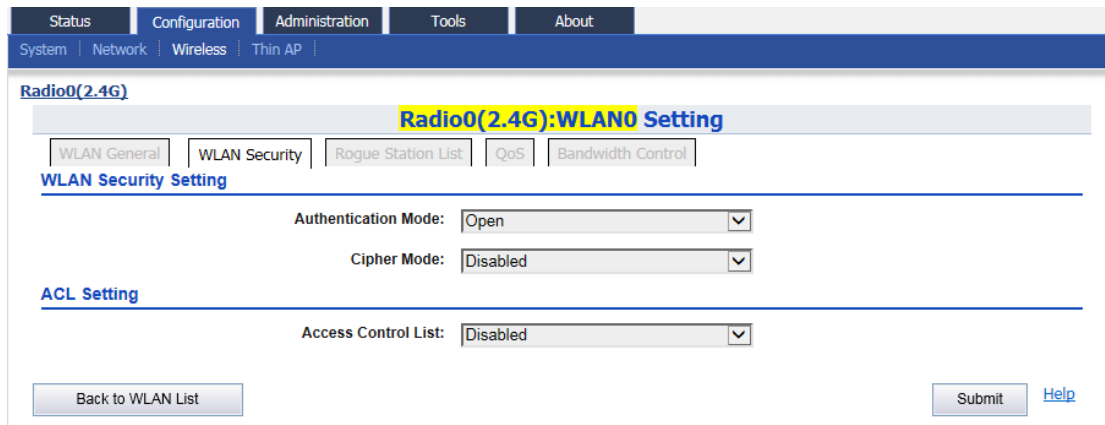


Figure 5-27 Open & No Security

Configure an open WLAN without data encryption:

1. Select **Configuration** -> **Wireless** -> **Radio0** -> **WLAN** to edit "**More...**" behind the WLAN, and then select **WLAN Security** to access to security configuration page.
2. Select "Open" in **Authentication Mode**
3. Select "Disabled" in **Cipher Mode**
4. Click **Submit**
5. Click **Save&Apply** to apply

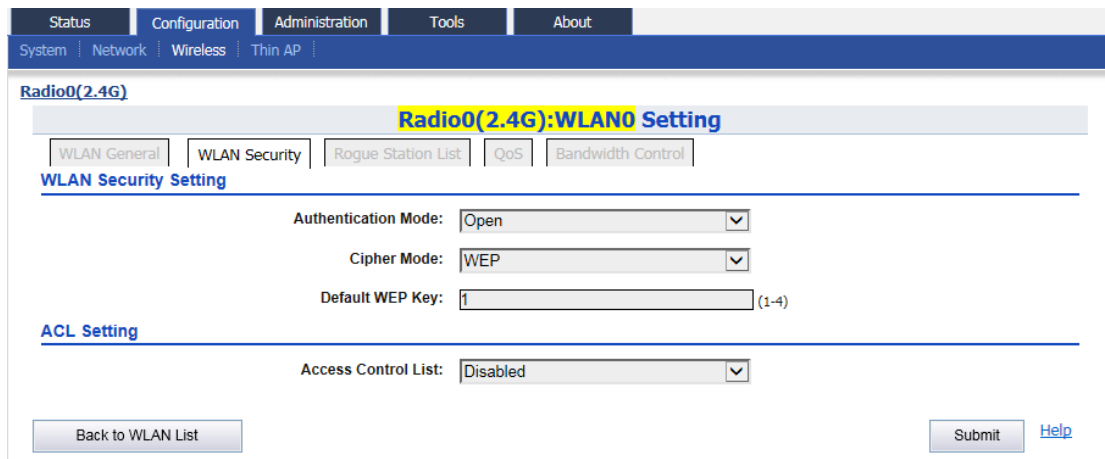


Figure 5-14 Open & WEP Setting

Configure an open WLAN with WEP encryption:

1. Select **Configuration** -> **Wireless** -> **Radio0** -> **WLAN** to edit "**More...**" behind the WLAN, and then select **WLAN Security** to access to security configuration page.
2. Select "Open" in **Authentication Mode**
3. Select "WEP" in **Cipher Mode**
4. Set the Key number (1-4) in **Default WEP Key**
5. Click **Submit**

- Click **Save&Apply** to apply

To specify the WEP key, please refer to section WEP Key Setting for more details.

2) Shared Key Mode

Shared Key authentication is one of the authentication methods with WEP encryption. Wireless clients must be passed through the authentication procedure before association. WEP is the only chiper scheme for shared key authentication.

The screenshot shows the configuration interface for Radio0(2.4G). The main title is 'Radio0(2.4G):WLAN0 Setting'. Underneath, there are tabs for 'WLAN General', 'WLAN Security', 'Rogue Station List', 'QoS', and 'Bandwidth Control'. The 'WLAN Security Setting' section is active, showing 'Authentication Mode' as 'Shared', 'Cipher Mode' as 'WEP', and 'Default WEP Key' as '1'. Below this is the 'ACL Setting' section with 'Access Control List' set to 'Disabled'. At the bottom, there are buttons for 'Back to WLAN List', 'Submit', and a 'Help' link.

Figure 5-29 Shared Key

Configure an WLAN with Shared Key authentication:

- Select **Configuration** -> **Wireless** -> **Radio0**-> **WLAN** to edit "**More...**" behind the WLAN, and then select **WLAN Security** to access to security configuration page.
- Select "Shared" in **Authentication Mode**
- Select "WEP" in **Cipher Mode**
- Set the Key number (1-4) in **Default WEP Key**
- Click **Submit**
- Click **Save&Apply** to apply

To specify the WEP key, please refer to section 2.4G WEP Key Setting for more details.

3) WPA/WPA2/WPA-auto

WPA is a security technology that improves on the authentication and encryption features of WEP. WPA provides stronger encryption than WEP by introducing two standard technologies: Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES). TKIP generates a new 128-bit key for each packet and

thus prevents the types of attacks that compromised WEP; while AES provide stronger data protection than TKIP. WPA2 is a security standard that aims to replace WPA. AES is the only option in cipher mode in WPA2 security. If AP is configured with WPA-auto authentication, it supports clients using either WPA or WPA2 authentication, AES+TKIP is the only option in cipher mode in WPA-auto security.

WPA-Enterprise (WPA) or WPA2-Enterprise (WPA2) is designed for enterprise networks and requires a RADIUS authentication server. This requires a more complicated setup, but provides additional security.

The screenshot shows the configuration interface for Radio0(2.4G) with the following sections:

- Radio0(2.4G) WLAN Security Setting:**
 - Authentication Mode: WPA
 - Cipher Mode: AES+TKIP
 - 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 | 10 . 6 . 161 . 80 | 1812 | <input type="checkbox"/> Show |
| Secondary RADIUS Server | 0 . 0 . 0 . 0 | 0 | <input type="checkbox"/> 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 | <input type="checkbox"/> Show |
| Secondary RADIUS Accounting Server | 0 . 0 . 0 . 0 | 1813 | <input type="checkbox"/> Show |
- ACL Setting:**
 - Access Control List: Disabled

Buttons: Back to WLAN List, Submit, Help

Figure 5-30 WPA/WPA2/WPA-auto

WLAN Security Setting

Authentication Mode: WPA, WPA2 or WPA-auto.

Cipher Mode: Specify data encryption scheme; there are 3 options: "TKIP", "AES", and "TKIP + AES". AES is the only option in cipher mode in WPA2 security. TKIP causes bad performance on 802.11n network.

Group Key Update Interval: Specify the interval for updating group key; the default value is 86400s.

RADIUS Server Setting

NAS Identifier: Specify network access server's ID; RADIUS server uses NAS ID to identify its client.

RADIUS Server IP Address Type: Specify RADIUS sever locates in either IPv4 network or IPv6 network; IPv6 option is available if user configures IPv6 network in general network setting.

RADIUS Retry Timeout: Specify timeout for each connection request that C1n issues to RADIUS Server.

Radius Server: Specify Radius server's IP address

Radius Port: Specify Radius server's service port; the default setting is 1812

Radius Secret: Specify Radius secret; it is used along with the MD5 hashing algorithm to obfuscate passwords. This setting MUST be as the same as that in RADIUS server

Secondary Radius Server: Specify Secondary Radius server's IP address

Secondary Radius Port: Specify Secondary Radius server's port

Secondary Radius Secret: Specify Secondary Radius server's secret

show: Specify Whether shows the accounting radius server's secret information.

RADIUS Accounting Server Setting

RADIUS Server IP Address Type: Specify RADIUS sever locates in either IPv4 network or IPv6 network; IPv6 option is available if user configures IPv6 network in general network setting.

Accounting Interim Interval: Specify accounting interim interval value. The range is 60-86400s, 0 means disable.

Radius Accounting Server: Specify accounting Radius server's IP address

Radius Accounting Port: Specify accounting Radius server's service port; the default setting is 1813

Radius Accounting Secret: Specify Radius secret; it is used along with the MD5 hashing algorithm to obfuscate passwords. This setting MUST be as the same as that in accounting RADIUS server

Secondary Accounting Radius Server: Specify Secondary accounting Radius server's IP address

Secondary Accounting Radius Port: Specify Secondary accounting Radius server's port

Secondary Accounting Radius Secret: Specify Secondary accounting Radius server's secret

showt: Specify Whether shows the accounting radius server's secret information.

Configure a WLAN with either WPA/WPA2/WPA-auto security:

1. Select **Configuration**→**Wireless**→**Radio0**→**WLAN** to edit “More...” behind the WLAN, and then select **WLAN Security** to access to security configuration page.
2. Select “WPA”, “WPA2” or “WPA-auto” in **Authentication Mode**.
3. Select suitable cipher mode in **Cipher Mode**. If **Authentication Mode** is set as “WPA2”, “AES” is the only option. If **Authentication Mode** is set as “WPA-auto”, “AES+TKIP” is the only option.
4. Specify update time of group key in **Group Key Update Interval**. The default value is 86400s
5. Specify network access server's ID in **NAS Identifier** if necessary.
6. Specify connection timeout in **RADIUS Retry Timeout**. The default value is 300s
7. Set Radius server IP address in **Radius Server**
8. Set Radius server port in **Radius Port**
9. Set Radius secret in **Radius Secret**
10. Set Secondary Radius server IP address in **Secondary Radius Server** if necessary
11. set Secondary Radius server port in **Secondary Radius Port** if necessary
12. set Secondary Radius server secret in **Secondary Radius Secret** if necessary
13. Specify accounting interim interval in **Accounting interim interval**. The default value is 300s
14. Set Radius accounting server IP address in **Radius Accounting Server**
15. Set Radius accounting server port in **Radius Accounting Port**
16. Set Radius accounting secret in **Radius Accounting Secret**
17. Set Secondary Radius accounting server IP address in **Secondary Radius Accounting Server** if necessary
18. set Secondary Radius accounting server port in **Secondary Radius Accounting Port** if necessary
19. set Secondary Radius accounting server secret in **Secondary Radius Accounting Secret** if necessary
20. Click **Submit**
21. Click **Save&Apply** to apply

NOTE: TKIP causes bad performance on 802.11n network.

4) WPA-PSK/WPA2-PSK/WPA-PSK-auto

WPA-Personal (WPA-PSK) or WPA2-Personal (WPA2-PSK) is designed for home and small office networks and doesn't require an authentication server. Each wireless network device authenticates with the access point using the same 256-bit key generated from a password or passphrase. Similar to WPA-Enterprise (WPA) or WPA2-Enterprise (WPA2), WPA-Personal (WPA-PSK) support both TKIP and AES as cipher mode; WPA2-Personal (WPA2-PSK) support AES as cipher mode only. If AP is configured with WPA-PSK-auto authentication, it supports clients using either WPA-PSK or WPA2-PSK authentication, AES+TKIP is the only option in cipher mode in WPA-auto security.

The screenshot shows the web-admin interface for Radio0(2.4G) with the following settings:

- Radio0(2.4G):WLAN0 Setting**
 - WLAN General | **WLAN Security** | Rogue Station List | QoS | Bandwidth Control
- WLAN Security Setting**
 - Authentication Mode: WPA-PSK
 - Cipher Mode: AES+TKIP
 - Group Key Update Interval: 86400 (s)
 - Pass Phrase: (8-64) [Show]
- ACL Setting**
 - Access Control List: Disabled

Buttons: Back to WLAN List, Submit, Help

Figure 5-31 WPA-PSK/WPA2-PSK/WPA-PSK-auto

Authentication Mode: WPA-PSK, WPA2-PSK or WPA-PSK-auto.

Cipher Mode: Specify data encryption scheme; there are 3 options: "TKIP", "AES", and "TKIP + AES". AES is the only option in cipher mode in WPA2 security. TKIP causes bad performance on 802.11n network.

Group Key Update Interval: Specify the interval for updating group key; the default value is 86400s.

Pass Phrase: Specify the passphrase for authentication; the length of passphrase is from 8 to 64 characters.

Configure a WLAN with WPA-PSK/WPA2-PSK/WPA-PSK-auto security:

1. Select **Configuration** → **Wireless** → **Radio0** → **WLAN** to edit "**More...**" behind the WLAN, and then select **WLAN Security** to access to security configuration page.
2. Select "WPA-PSK", "WPA2-PSK", or "WPA-PSK-auto" in **Authentication Mode**

3. Select suitable cipher mode in **Cipher Mode**. If **Authentication Mode** is set as "WPA2", "AES" is the only option. If **Authentication Mode** is set as "WPA-PSK-auto", "AES+TKIP" is the only option.
4. Specify update time of group key in **Group Key Update Interval**. The default value is 86400s.
5. Set the passphrase in **Pass Phrase**. Special characters are supported, e.g. @, #...etc.
6. Click **Submit**
7. Click **Save&Apply** to apply

5) ACL Configurations

C1n Series AP/CPE supports Access Control List (ACL), it bases on MAC address filtering. There are 3 modes in the Access Control List (ACL). They are "Disabled", "Enabled-Default Allow" and "Enabled-Default Deny".

"Disable" - means the function of ACL is disabled.

"Enabled-Default Allow" - The function of ACL is enabled. The MAC addresses which are specified in the ACL will consider as Allow. That means no one can access to the base station, unless the computer which has an MAC address matches one of the entries of the ACL with its ACL Type is Allow.

"Enabled-Default Deny" - The function of ACL is enabled. The MAC addresses which are specified in the ACL will consider as Deny. Every computer can access to the base station, unless the computer which has an MAC address matches one of the entries of the ACL with its ACL Type is Deny.

The screenshot shows the configuration interface for Radio0(2.4G) WLAN Security Setting. The 'WLAN Security Setting' section includes 'Authentication Mode' (Open) and 'Cipher Mode' (Disabled). The 'ACL Setting' section includes 'Access Control List' (Enabled - Default Allow), 'ACL Input Method' (Manual Input), and a list of 'Denied MAC Address' entries: '8c:70:5a:e0:2e:11' and '68:7f:74:b8:f0:d5'. Buttons for 'Back to WLAN List', 'Submit', and 'Help' are visible at the bottom.

Figure 5-32 ACL-Default Allow

The screenshot shows the configuration page for Radio0(2.4G) under the 'Radio0(2.4G):WLAN0 Setting' tab. The 'WLAN Security Setting' section has 'Authentication Mode' set to 'Open' and 'Cipher Mode' set to 'Disabled'. The 'ACL Setting' section has 'Access Control List' set to 'Enabled - Default Deny' and 'ACL Input Method' set to 'Manual Input'. The 'Allowed MAC Address' field contains two entries: '8c:70:5a:e0:2e:11' and '68:7f:74:b8:f0:d5'. There are 'Back to WLAN List' and 'Submit' buttons at the bottom.

Figure 5-33 ACL-Default Deny

This screenshot is similar to Figure 5-33 but with 'ACL Input Method' set to 'File'. The 'MAC Address File' field now has an 'Upload File...' button and the text '(Not upload yet)'. The 'Access Control List' remains 'Enabled - Default Deny'. The 'Back to WLAN List' and 'Submit' buttons are still present.

Figure 5-34 ACL-ACL Input Method

Access Control List: Specify the modes of ACL; the options are “Disabled”, “Enabled-Default Allow”, and “Enable-Default Deny”.

ACL Input Method: Specify the source of ACL; user may manual input the list or upload the list from text file.

Denied MAC Address: Specify the MAC addresses in the list will be blocked; this option is available if **Access Control List** is configured as “Enabled-Default Allow”

Allowed MAC Address: Specify the MAC addresses in the list can access only; this option is available if **Access Control List** is configured as “Enable-Default Deny”.

Disable ACL function in WLAN:

1. Select **Configuration** → **Wireless** → **Radio0** → **WLAN** to edit “More...” behind the WLAN, and then select **WLAN Security** to access to security configuration page
2. Select “Disable” in **Access Control List**
3. Click **Submit**

4. Click **Save&Apply** to apply

Enable ACL function with “Enabled-Default Allow” in WLAN:

1. Select **Configuration**→**Wireless**→**Radio0**→**WLAN** to edit “**More...**” behind the WLAN, and then select **WLAN Security** to access to security configuration page
2. Select “Enabled-Default Allow” in **Access Control List**
3. Select suitable input method in **ACL Input Method**
4. Input MAC address in **Denied MAC Address** or upload a text file by pressing “Upload File”
5. Click **Submit**
6. Click **Save&Apply** to apply

Enable ACL function with “Enabled-Default Deny” in WLAN:

1. Select **Configuration**→**Wireless**→**Radio0**→**WLAN** to edit “**More...**” behind the WLAN, and then select **WLAN Security** to access to security configuration page
2. Select “Enable-Default Deny” in **Access Control List**
3. Select suitable input method in **ACL Input Method**
4. Input MAC address in **Allowed MAC Address** or upload a text file by pressing “Upload File”
5. Click **Submit**
6. Click **Save&Apply** to apply

5.4.1.1.2.3. WLAN X (0-15) Rogue Station List

Rogue station stands for the devices that can potentially disrupt wireless networks and can sometimes cause irrevocable damage to the network owners. C1n Series AP/CPE supports Rogue Station List to prevent potential damages from rogue station; User may input the rogue station's MAC address into rogue station list, then this station cannot associate to WLAN. User may manage the rogue station via **Configuration**→**Wireless**→**Radio0**→**Rogue Station List**.



Figure 5-35 Rogue Station List

Rogue Station: Specify MAC address of rogue station.

Add a rogue station into rogue station list:

1. Select **Configuration** → **Wireless** → **Radio0** → **WLAN** to edit “[More...](#)” behind the WLAN, and then select **Rogue Station List** to access rogue station list configuration page
2. Set the rogue station's MAC address in **Rogue Station**.
3. Click “+” for adding a new entry if necessary.
4. Click **Submit**
5. Click **Save&Apply** to apply

Remove a rogue station into rogue station list:

1. Select **Configuration** → **Wireless** → **radio0** → **WLAN** to edit “[More...](#)” behind the WLAN, and then select **Rogue Station List** to access rogue station list configuration page
2. Clear the MAC address in **Rogue Station** or click “✖” of particular MAC address.
3. Click **Submit**
4. Click **Save&Apply** to apply

5.4.1.1.2.4. WLAN X (0-15) QoS

C1n supports QoS (DSCP-to-WMM Mapping) setting of each WLAN, User can specify the DSCP value that Correspondence to BestEffort (BE), Background(BK), Video(VI) and Voice(VO). User may manage the QoS via **Configuration** → **Wireless** → **Radio0** → **QoS** to access to WLAN X (0-15) QoS configuration page.

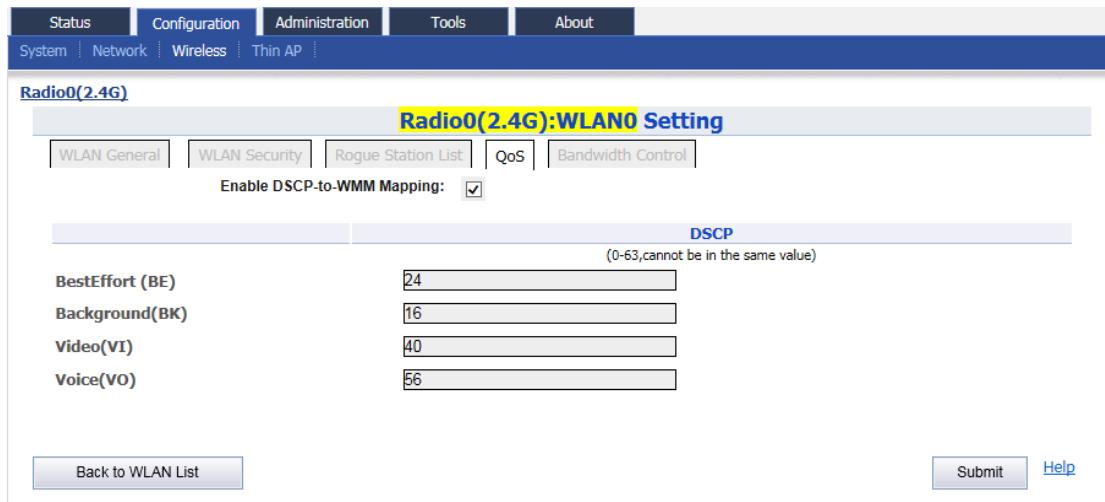


Figure 5-36 WLAN QoS

Enable DSCP-to-WMM Mapping: Enable or Disable DSCP to WMM mapping function.

Configure QoS based on a WLAN:

1. Select **Configuration** → **Wireless** → **radio0** → **WLAN** to edit “[More...](#)” behind the WLAN, and then select **QoS** to access Bandwidth Control configuration page
2. Set the DSCP value under “DSCP” that Correspondence to BestEffort (BE), Background(BK), Video(VI) and Voice(VO).
3. Click **Submit**
4. Click **Save&Apply** to apply

5.4.1.1.2.5. WLAN X (0-15) Bandwidth Control

C1n supports different bandwidth control setting of each WLAN. User specifies the maximum speed (kbps) of bandwidth based on WLAN or based on station. Bandwidth control based on WLAN specifies limit the maximum speed of uplink and downlink for particular WLAN. All wireless clients share the limited bandwidth in this WLAN. Bandwidth control based on station specifies limit the maximum speed of uplink and downlink for each associated wireless client. Wireless client cannot exceed the limitation even it is the only client in WLAN. User may manage the rogue station via **Configuration** → **Wireless** → **Radio0** → **Bandwidth Control** to access to Bandwidth Control configuration page.

The screenshot shows the 'Radio0(2.4G):WLAN0 Setting' page. At the top, there are navigation tabs: Status, Configuration, Administration, Tools, and About. Below these are sub-tabs: System, Network, Wireless, and Thin AP. The main content area is titled 'Radio0(2.4G):WLAN0 Setting' and contains several sub-sections: 'WLAN General', 'WLAN Security', 'Rogue Station List', 'QoS', and 'Bandwidth Control'. The 'Bandwidth Control' section is active and shows two columns: 'Based On WLAN' and 'Based On Station'. Each column has 'Uplink' and 'Downlink' settings, both currently set to '0'. Below the settings are buttons for 'Back to WLAN List', 'Submit', and 'Help'.

Figure 5-37 WLAN Bandwidth Control

Uplink: Specify the maximum bandwidth of uplink (from wireless clients to C1n); the range is from 0-1000000Kbps. "0" means disable. The default setting is "0".

Downlink: Specify the maximum bandwidth of downlink (from C1n to wireless clients); the range is from 0-1000000Kbps. "0" means disable. The default setting is "0".

Configure bandwidth limitation based on a WLAN:

1. Select **Configuration** → **Wireless** → **radio0** → **WLAN** to edit "**More...**" behind the WLAN, and then select **Bandwidth Control** to access Bandwidth Control configuration page
2. Set uplink bandwidth limitation (Kbps) for uplink in **Uplink** under "based on WLAN"
3. Set uplink bandwidth limitation (Kbps) for downlink in **Downlink** under "based on WLAN"
4. Click **Submit**
5. Click **Save&Apply** to apply

Configure bandwidth limitation based on a station:

1. Select **Configuration** -> **Wireless** -> **radio0** -> **WLAN** to edit "**More...**" behind the WLAN, and then select **BandwidthControl** to access Bandwidth Control configuration page
2. Set uplink bandwidth limitation (Kbps) for uplink in **Uplink** under "based on Station"
3. Set uplink bandwidth limitation (Kbps) for downlink in **Downlink** under "based on Station"
4. Click **Submit**
5. Click **Save&Apply** to apply

5.4.1.1.3. Advanced Configuration

C1n provides more WLAN parameters in radio's advance page. User may alter C1n radio performance by changing the advance parameters. Please note that inappropriate configuration may bring negative impact on the network performance. It is not suggested to change the parameters in Advanced Radio Settings unless you are experienced administrators. **Default setting is recommended.**

Note: The Advanced Configuration for Radio0 in AP mode, Station mode, Repeater mode, Bridge mode are the same, And the configuration will not be introduced in later chapter.

Status | Configuration | Administration | Tools | About

System | Network | Wireless | Thin AP

Radio0(2.4G)

Radio0(2.4G) Setting

General | WLAN | Advanced | QoS | WEP

Advanced Setting

AMPDU:

AMPDU Limit: (1-64)

AMSDU:

Max Tx Streams:

Max Rx Streams:

Beacon Interval Auto:

Beacon Interval: (40-3500)

DTIM: (1-255)

Fragmentation Threshold: (256-2346)

Protection Mode:

Data Rate Setting

Data Rate: (Mbps)

Data Rate Setting:

1Mbps: Enable Disable

2Mbps: Enable Disable

5.5Mbps: Enable Disable

11Mbps: Enable Disable

6Mbps: Enable Disable

9Mbps: Enable Disable

12Mbps: Enable Disable

18Mbps: Enable Disable

24Mbps: Enable Disable

36Mbps: Enable Disable

Protection Rate:

RTS/CTS Threshold: (0-2347)

Distance: (0-50km)

IGMP Snooping:

Multicast Traffic:

U-APSD:

Enable Nearby AP List: [\[Nearby AP List\]](#)

48Mbps: Enable Disable

54Mbps: Enable Disable

Multicast Data Rate: (Mbps)

AirFi Setting

AirFi Mode:

AirFi Level:

[Help](#)

Figure 5-38 Radio Advanced Setting

Advanced Setting

AMPDU: Enable or Disable IEEE802.11n aggregation of MAC protocol data unit; if enabled, C1n pushes aggregated MPDU (MAC protocol data units) into a single PDU (physical protocol data unit). This option may improve the throughput of 802.11n network. By default, it is enabled.

AMPDU Limit: Specify the maximum number of data frames that C1n pushes into a single PDU. The range is from 1 to 64. The default setting is 64.

AMSDU: Enable or Disable IEEE802.11n aggregation of MAC service data unit; if enabled, C1n pushes aggregated MSDU (MAC service data units) into a single MPDU. This option may improve the throughput of 802.11n network. By default, it is enabled.

Max Tx/Rx Streams: Specify the maximum number of transmission streams and receiving streams in 802.11n MIMO. The default value is 2 for both transmission and receiving stream.

Beacon Interval Auto: Radio0 adjusts the beacon interval itself in order to reduce the beacon frame overhead in wireless network.

Beacon Interval: Specify interval of beacon transmissions of each supported BSS. Each BSS share this setting. 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.

DTIM: Specify the interval between two DTIM; this message is generated to inform the associated clients about the presence of buffered multicast/broadcast data on the access point. The unit is in term of second. The range is from 1 to 255. The default value is 1.

Fragmentation Threshold: Specify the frame size of each frame. Frames that are smaller than the specified fragmentation threshold value will not be fragmented; otherwise, the frames will be fragmented into smaller packets and transmitted a piece at a time instead of all at once. The unit is in term of Byte. The range is from 256 to 2346 bytes. The default setting is 2346 bytes. It is recommended to use the default value or only minor reductions of this default value.

Protection Mode: Specify the protect mechanism on hidden node problem of Wi-Fi network. This mechanism can decrease the rate of data collision wireless stations. When the protection mode is enabled, the throughput of the AP will be a little lower due to many of frame traffic should be transmitted.

There are 3 options: "None", "CTS-only" and "RTS-CTS".

"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.

Protection Rate: Specify the transmission rate of protection frame, i.e. CTS frame and RTS frame.

RTS/CTS Threshold: 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 this default value. The value range is from 0 to 2347.

Distance: Specify the estimate distance of target area (round to the nearest km). C1n adjusts the round-trip time latency according to this value. The range is from 1 to 50km. The default value is 2km.

IGMP Snooping: Enable or Disable IGMP snooping; by default, it is enabled. AP is a Layer 2 device when it is configured as Switch mode. However, IGMP Snooping implementation on AP is a little bit different than that of standard Layer 2 Switch. Each Virtual AP (WLAN) port is similar to a Layer 2 switch port. With IGMP Snooping enabled in the AP, clients associated to a WLAN will only receive multicast packets if there is at least one client joined the multicast group in that VAP. Unlike ordinary IGMP Snooping implementation, where Layer 2 switch converts multicast to unicast and delivers them to devices registered with the multicast group, AP should simply send out the multicast packets from the WLAN which has at least one client joined the multicast group. This is done because the wireless media is a broadcast media. It does not need to be sent multiple times when there are more than one registered clients.

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

The IGMP snooping forwarding table (port and multicast MAC address mapping table) should support aging mechanism to age out the entry which has no multicast traffic for a period of time.

Multicast Traffic: Enable or Disable that AP processes multicast traffic in WLANs. If enabled, AP process multicast traffic in all WLANs; otherwise; AP drops the multicast traffic.

U-APSD: UAPSD is an acronym for Unscheduled Automatic Power Save Delivery, a feature of Wi-Fi devices that allows them to save power.

Enable Nearby AP List: Enable or disable the radio scan nearby AP function, When it's enabled, radio0 will scan nearby AP and display the nearby AP list in

Status → **Interface** → **Radio0** → **Channel Usage** page.

[Data Rate Setting](#)

Data Rate: Specify which data rate that AP will or will not serve. 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.

Multicast Traffic Data Rate Setting: Specify the data rate of multicast packet; C1n allows multicast packets to be sent in higher rates rather than commonly used (1 Mbps at IEEE 802.11b mode, 6 Mbps at IEEE 802.11g/a mode). This is Altai's proprietary feature; it may be incompatible with the devices from other vendors. If the sender and receiver, which are Altai's products, have the same setting, they can achieve better multicast packet throughput performance.

AirFi Setting

AirFi Mode: Enable or Disable AirFi function; AirFi technology is the latest advanced software control wireless algorithm developed by Altai for optimizing network throughput capacity performance. Using the Altai AirFi control algorithm can optimize the wireless bandwidth for the high speed clients as well as the low speed clients (i.e. 11b and 11g clients), and as a result the system throughput can be improved substantially.

AirFi Level: There are four options for AirFi level: Level I, Level II, Level III and Custom. AirFi level I is recommended. When select "Custom", user can configure **AirFi Level**

Custom value.

5.4.1.1.4. QoS Configuration

User may specify the Radio0 QoS setting via **Configuration** → **Wireless** → **Radio0** → **QoS**.

Radio0(2.4G) Setting

General | WLAN | Advanced | **QoS** | WEP

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 | <input type="checkbox"/> |
| Background(BK) | 5 | 10 | 7 | 0 | <input type="checkbox"/> |
| Video(VI) | 3 | 4 | 1 | 3008 | <input type="checkbox"/> |
| Voice(VO) | 2 | 3 | 1 | 1504 | <input type="checkbox"/> |

Submit Help

Figure 5-39 Radio0 QoS Parameters

Optimization Mode: Specify QoS/WMM parameters of Radio0. There are 4 modes, “Default”, “Optimized for throughput”, “Optimized for capacity”, and “Manual Configuration” .

“Default” is a set of QoS/WMM parameters as default configuration.

“Optimized for throughput” is a set of QoS/WMM parameters that can achieve the highest throughput for a single user.

“Optimized for capacity” is a set of QoS/WMM parameters that that can achieve highest system throughput for multiple users, e.g. > 30 users.

When select “Manual Configuration”, User can set Radio(AP-side) WMM Parameters.

CWMIN, CWMAX, AIFS, TXOP, NOACK: Specify the value that correspond to BestEffort (BE), Background(BK), Video(VI) and Voice(VO).

Configure Radio0 QoS Setting:

1. Select **Configuration**→**Wireless**→**Radio0**→**QoS**
2. Select **Optimization Mode** to Specify QoS/WMM parameters of Radio0.
3. When select “Manual Configuration” Specify the Radio(AP-side) WMM Parameters under **CWMIN, CWMAX, AIFS, TXOP and NOACK**.
4. Click **Submit**
5. Click **Save&Apply** to apply

5.4.1.1.5. WEP Key Setting

User may specify the WEP key for wireless security in WEP key setting via **Configuration**
→ **Wireless** → **Radio0** → **WEP**.

Figure 5-40 Radio0 WEP Key

Key Entry Method: Specify the character coding scheme of WEP key; AP interprets WEP key either as ASCII characters or HEX characters.

WEP Key 1, 2, 3, 4: Specify the WEP key; the key is up to 26 HEX characters or 13 ASCII characters.

Configure WEP Key for wireless security:

Pre-condition: Please specify the WLAN's security as Open with WEP or shared key.

1. Select **Configuration** → **Wireless** → **Radio0(2.4G)** → **WEP**
2. Select suitable key format in **Key Entry Method**
3. Input key phrase in **WEP Key 1, 2, 3, 4**
4. Click **Submit**
5. Click **Save&Apply** to apply

Note: The WEP Key Setting for Radio0 in AP mode, Station mode, Repeater mode, Bridge mode are the same, And the configuration will not be introduced in later chapter.

5.4.1.2. Radio0 Configuration – Station Mode

5.4.1.2.1. General Configuration

C1n can work as CPE/Station. When C1n is set to "station" mode, the backhaul link must be established through associating with the remote APs. User may configure C1n as station in Radio's general page via **Configuration**→**Wireless**→**Radio0**.

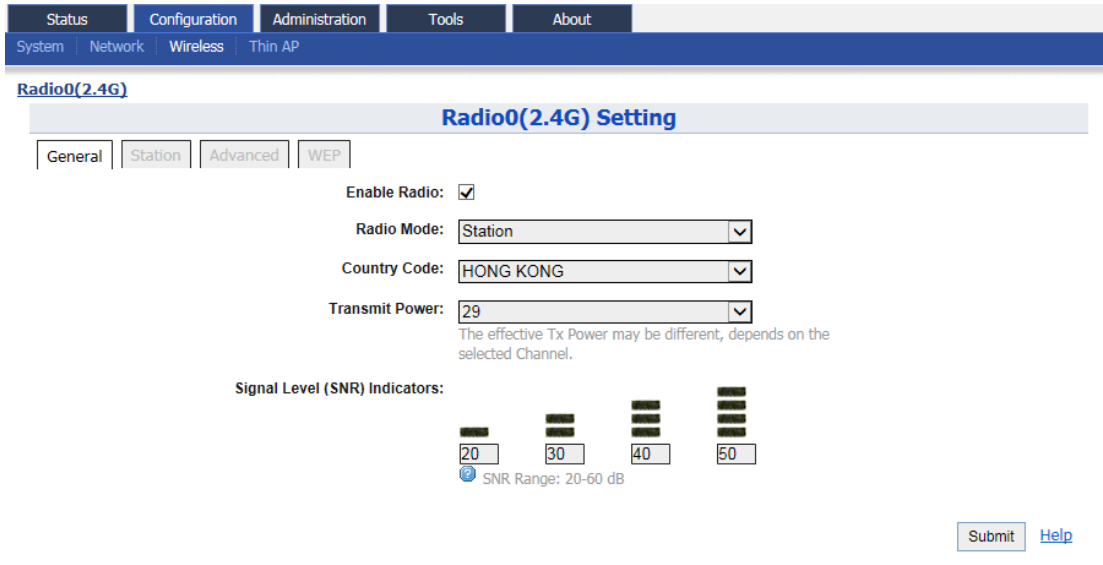


Figure 5-15 Radio0 Station Setting

Signal Level (SNR) Indicators: There are 6 LEDs at the back of the C1n, 4 LEDs are used for signal strength indication in Station mode for association with another AP. The 4 LEDs altogether shall display 8 levels of signal strength, in the following manner.

| Signal level | PWR | LAN | SS1 | SS2 | SS3 | SS4 |
|--------------|-----|-----|-------|-------|-------|-------|
| 1 (Weakest) | | | Blink | Off | Off | Off |
| 2 | | | On | Off | Off | Off |
| 3 | | | On | Blink | Off | Off |
| 4 | | | On | On | Off | Off |
| 5 | | | On | On | Blink | Off |
| 6 | | | On | On | On | Off |
| 7 | | | On | On | On | Blink |
| 8 | | | On | On | On | On |

Configure C1n as CPE / Station:

1. Select **Configuration**→**Wireless**→**Radio0**
2. Check the **Enable Radio** option
3. Select the "Station" in **Radio Mode**
4. Set the corresponding country code in **Country Code**; HONG KONG is default setting.
5. Set desired transmission power in **Transmit Power**; the effective transmission power is depended on the remote AP.

6. Set the desired SNR value in **Signal Level (SNR) Indicators**.
7. Click **Submit**
8. Click **Save&Apply** to apply

5.4.1.2.2. Station Configuration

User may provide the remote AP's information and configure the corresponding security setting via **Configuration**→**Wireless**→**Radio0**→**Station**. For more detail setting, please click the "More..." under the "Detail".

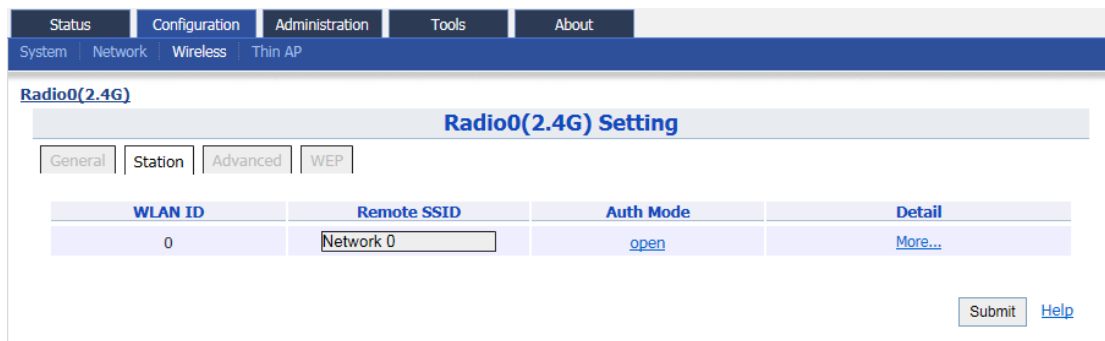


Figure 5-16 Radio0 Station Setting

WLAN ID: WLAN number. It must be "0".

Remote SSID: Specify the SSID of access point that C1n is going to associate; User may click the "More..." for more detail station settings.

Auth Mode: Specify the wireless security setting that the remote AP uses; User may click "open" for configuring. This setting must be configured correctly; otherwise, C1n cannot associate the remote AP. Also, user may click the "More..." for more detail station settings.

5.4.1.2.2.1. WLAN 0 General Configuration

User may provide the remote AP's details via **Configuration**→**Wireless**→**Radio0**→**Station** to click "More..." behind the WLAN0, and then select **WLAN General**.

Figure 5-17 Radio0 WLAN0 Setting

General Setting

WLAN Mode: The operating mode of C1n; Here is "Station".

Lock AP Mac: When C1n Radio0 lock to a remote AP Mac, Radio0 will not roaming among remote APs. User should input the MAC of remote AP in **Remote AP Mac**.

Remote SSID: Specify the SSID of access point that C1n is going to associate; the SSID should be up to 32 characters. User may select "[Scan]" to look for the surrounding SSID.

Preferred AP0, AP1, AP2 Mac: Specify the AP that C1n should associate them preferentially. User may specify up to 3 AP's MAC addresses in the order of priority.

MAC Clone Setting

Enable MAC Clone: Enable or Disable MAC Clone function, when it's enabled, Radio0 will use the cloned MAC associate remote AP. This feature supports one laptop/PC only.

MAC Clone Type: either input manually or cloned from connection laptop/PC directly.

Roaming Setting

Enable Roaming: When enabled, station performs channel scanning and roams to other AP with better SNR based on specified scanning & roaming parameters; otherwise, it never performs channel scanning and associates with the other AP if the current connection is broken.

Scan SNR threshold: Station performs channel scanning if the SNR of received signal from associated AP is worse than this threshold, (0-100dB, default value is 35).

Scan SNR Threshold must be larger (>) than Roaming SNR Threshold.

Roaming SNR threshold: Station triggers the roaming if the SNR of received signal from associated AP is less than this threshold. (0-100dB, default value is 30).

Max Scan Interval: Specify the maximum duration for channel scanning. (1-3600s, default value is 60s).

Min Scan Interval: Specify the minimum duration for channel scanning. (1-60s, default value is 10s)

Scan SNR Fluctuation Threshold: When the SNR of remote AP change in value exceeds the threshold setting here within **Min Scan Interval**, Radio0 will start background scan.

Wireless Mode Weighting: When enabled, station will be more stickier to current associated AP.

Bgscan Channel: Specify the particular channel for scan. Radio0 will scan all channels if no channel is checked.

Configure C1n to associate with specified remote AP:

1. Select **Configuration** → **Wireless** → **Radio0** → **Station** to click "More..." behind the WLAN0.
2. Check **Lock AP Mac** if necessary. User should also input the MAC of remote AP in **Remote AP Mac**.
3. Set remote AP's SSID in **Remote SSID** or click **[Scan]** to find remote AP in the surrounding area.
4. Set up to 3 preferential MAC addresses of remote AP in **Preferred AP0/AP1/AP2 MAC** if necessary.
5. Check the **Enable MAC Clone** if necessary, user should also select **MAC Clone Type**.
6. Check the **Enable Roaming** if roaming is needed.
7. Set varies value about roaming: **Scan SNR threshold**, **Roaming SNR threshold**, **Max Scan Interval**, **Min Scan Interval**, **Scan SNR Fluctuation Threshold**, **Wireless Mode Weighting**, **Roaming Hysteresis Level**, and **Bgscan Channel**.

8. Click **Submit**
9. Click **Save&Apply** to apply

5.4.1.2.2.2. WLAN 0 Security

User may configure the wireless security that as the same as the setting in remote AP. For the detail of wireless security in C1n, please refer to section **WLAN X(0-15) Security** for more details.

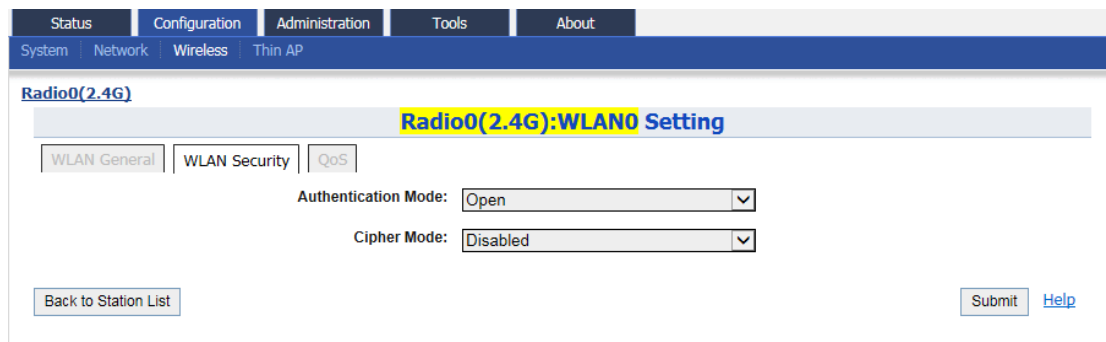


Figure 5-18 Radio0:WLAN0 Security Setting

Configure WPA / WPA2 as wireless security in Station mode (for example):

1. Select **Configuration** → **Wireless** → **Radio0** → **Station** to click “More...” then select **WLAN Security**
2. Select “WPA” or “WPA2” in **Authentication Mode**
3. Select the desired cipher mode in **Cipher Mode**
4. Select the desired EAP mode in **EAP Mode**
5. Set username and password in **Username** and **Password** respectively
6. Click **Submit**
7. Click **Save&Apply** to apply

NOTE: The security setting Must be as the same as the remote AP; otherwise, C1n cannot connect to remote AP.

5.4.1.2.2.3. WLAN 0 QoS

The WLAN QoS configuration in Station mode is as the same as that in AP mode. For the detail of WLAN QoS configuration in Station mode, please refer to section **WLAN X(0-15) QoS** for more details.

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

Figure 5-45 Radio0:WLAN0 QoS Setting

5.4.1.3. Radio0 Configuration – Repeater Mode

5.4.1.3.1. General Configuration

C1n can act as wireless relay base station if it is configured as “Repeater” mode. It relays the data between remote base station and wireless clients. Unlike “AP” mode, C1n support up to 15 WLANs in “Repeater” Mode since C1n uses 1 WLAN to associate with remote AP for setting up a wireless backhaul link.

Figure 5-46 Radio0 Repeater Mode Setting

Enable Radio: Enable or disable radio0, by default it is enabled.

Radio Mode: Operation mode of C1n Series AP/CPE

Country Code: Specify country that C1n locates. This setting is related about radio regulatory domain, such as maximum transmission power, available operating frequency channel ... etc. Hong Kong is default setting.

Transmit Power: Specify the maximum transmission power (dBm) of C1n for radio0.

Maximum Clients: Specify the maximum number of users C1n serves.

Enable Inter-WLAN User Isolation: Allow or block inter-WLAN user communication. If enabled, clients cannot communicate to each other directly when they associated into different WLAN. By default, it is "disable".

Signal Level (SNR) Indicators: There are 6 LEDs at the back of the C1n, 4 LEDs are used for signal strength indication in Station mode for association with another AP. The 4 LEDs altogether shall display 8 levels of signal strength, in the following manner.

| Signal level | PWR | LAN | SS1 | SS2 | SS3 | SS4 |
|--------------|-----|-----|-------|-------|-------|-------|
| 1 (Weakest) | | | Blink | Off | Off | Off |
| 2 | | | On | Off | Off | Off |
| 3 | | | On | Blink | Off | Off |
| 4 | | | On | On | Off | Off |
| 5 | | | On | On | Blink | Off |
| 6 | | | On | On | On | Off |
| 7 | | | On | On | On | Blink |
| 8 | | | On | On | On | On |

Configure C1n as wireless relay station (i.e. "Repeater" Mode):

1. Select **Configuration** → **Wireless** → **Radio0**
2. Enable radio by clicking **Enable Radio**
3. Select "Repeater" in **Radio Mode**
4. Select your country code in **Country Code**
5. Set maximum transmit power in **Transmit Power**
6. Set the maximum number of users A2 serves in **Maximum Clients**
7. Check **Enable Inter-WLAN User Isolation** if necessary.
8. Set the desired SNR value in **Signal Level (SNR) Indicators**.
9. Click **Submit**
10. Click **Save&Apply** to apply

5.4.1.3.2. WLAN Configuration

C1n Series AP/CPE radio0 supports maximum 15 WLANs (SSIDs) and associate 1 remote AP simultaneously. User may configure wireless network via **Configuration** → **Wireless** → **Radio0** → **WLAN**.

Radio0(2.4G) Setting

General | **WLAN** | Advanced | WEP

Station Configuration

| WLAN ID | Remote SSID | Auth Mode | Detail |
|---------|-------------|-----------|---------|
| 15 | Network 0 | open | More... |

WLAN Configuration

| Enable WLAN | SSID | Max Clients | Isolation | VLAN Pass-Through/ID | Auth Mode | Access Traffic Right | WLAN Uplink/Downlink Control | Station Uplink/Downlink Control | Detail |
|-----------------------------|---|-------------|--------------------------|--|-----------|----------------------|------------------------------|---------------------------------|---------|
| <input type="checkbox"/> 0 | ircao-local <input type="checkbox"/> Hide SSID | 128 | <input type="checkbox"/> | 1 <input type="checkbox"/> Pass through | open | Full Access | 0 0 | 0 0 | More... |
| <input type="checkbox"/> 1 | ircao-tunnel <input type="checkbox"/> Hide SSID | 75 | <input type="checkbox"/> | 355 <input type="checkbox"/> Pass through | open | Full Access | 0 0 | 0 0 | More... |
| <input type="checkbox"/> 2 | ircao-tunnel2 <input type="checkbox"/> Hide SSID | 32 | <input type="checkbox"/> | 366 <input type="checkbox"/> Pass through | open | Full Access | 0 0 | 0 0 | More... |
| <input type="checkbox"/> 3 | ircao-tunnel3 <input type="checkbox"/> Hide SSID | 32 | <input type="checkbox"/> | 330 <input type="checkbox"/> Pass through | open | Full Access | 0 0 | 0 0 | More... |
| <input type="checkbox"/> 4 | Superwifi Network <input type="checkbox"/> Hide SSID | 256 | <input type="checkbox"/> | 1 <input type="checkbox"/> Pass through | open | Full Access | 0 0 | 0 0 | More... |
| <input type="checkbox"/> 5 | Superwifi Network <input type="checkbox"/> Hide SSID | 256 | <input type="checkbox"/> | 1 <input type="checkbox"/> Pass through | open | Full Access | 0 0 | 0 0 | More... |
| <input type="checkbox"/> 6 | Superwifi Network <input type="checkbox"/> Hide SSID | 256 | <input type="checkbox"/> | 1 <input type="checkbox"/> Pass through | open | Full Access | 0 0 | 0 0 | More... |
| <input type="checkbox"/> 7 | Superwifi Network <input type="checkbox"/> Hide SSID | 256 | <input type="checkbox"/> | 1 <input type="checkbox"/> Pass through | open | Full Access | 0 0 | 0 0 | More... |
| <input type="checkbox"/> 8 | Superwifi Network <input type="checkbox"/> Hide SSID | 256 | <input type="checkbox"/> | 1 <input type="checkbox"/> Pass through | open | Full Access | 0 0 | 0 0 | More... |
| <input type="checkbox"/> 9 | Superwifi Network <input type="checkbox"/> Hide SSID | 256 | <input type="checkbox"/> | 1 <input type="checkbox"/> Pass through | open | Full Access | 0 0 | 0 0 | More... |
| <input type="checkbox"/> 10 | Superwifi Network <input type="checkbox"/> Hide SSID | 256 | <input type="checkbox"/> | 1 <input type="checkbox"/> Pass through | open | Full Access | 0 0 | 0 0 | More... |
| <input type="checkbox"/> 11 | Superwifi Network <input type="checkbox"/> Hide SSID | 256 | <input type="checkbox"/> | 1 <input type="checkbox"/> Pass through | open | Full Access | 0 0 | 0 0 | More... |
| <input type="checkbox"/> 12 | Superwifi Network <input type="checkbox"/> Hide SSID | 256 | <input type="checkbox"/> | 1 <input type="checkbox"/> Pass through | open | Full Access | 0 0 | 0 0 | More... |
| <input type="checkbox"/> 13 | Superwifi Network <input type="checkbox"/> Hide SSID | 256 | <input type="checkbox"/> | 1 <input type="checkbox"/> Pass through | open | Full Access | 0 0 | 0 0 | More... |
| <input type="checkbox"/> 14 | Superwifi Network <input type="checkbox"/> Hide SSID | 256 | <input type="checkbox"/> | 1 <input type="checkbox"/> Pass through | open | Full Access | 0 0 | 0 0 | More... |

Submit Help

Figure 5-47 Radio0 Repeater Mode WLAN Setting

5.4.1.3.2.1. Repeater Configuration

User may provide the remote AP's information and configure the corresponding security setting via **Configuration**→**Wireless**→**Radio0**→**WLAN**, then click the “More...” behind the WLAN 15 to access repeater setting page. The detail of repeater configuration is as the same as that in “Station” mode. Please refer to section **5.4.1.2 Radio0 Configuration- Station Mode** for more details.

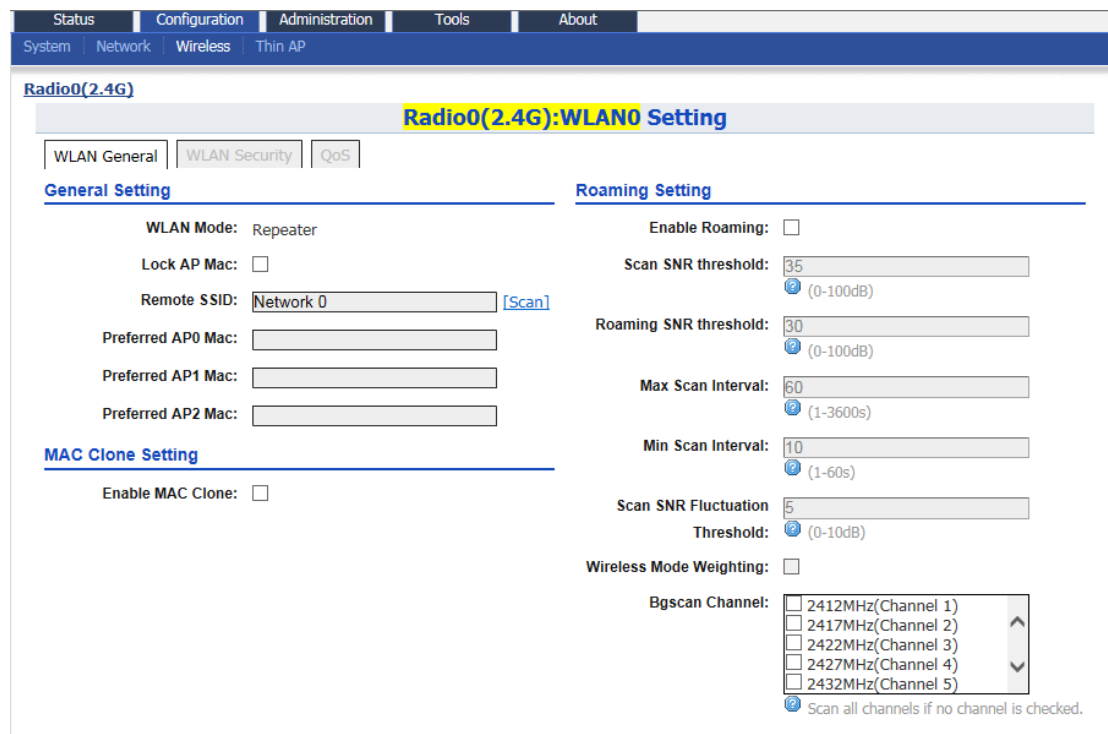


Figure 5-48 Repeater Mode - WLAN15 Setting

5.4.1.3.2.2. WLAN Configuration

Maximum 15 WLAN can be configured as access point in “Repeater” mode, the detail of repeater configuration is as the same as that in “AP” mode. User may specify the WLAN setting via **Configuration**→**Wireless**→**Radio0**→**WLAN** to click the “More...” behind the WLANs. Please refer to section **Radio0 General configuration- AP Mode** for more details.

Figure 5-49 Repeater Mode - WLAN0 Setting

5.4.1.4. Radio0 Configuration – Bridge Mode(for C1an and C1xn)

5.4.1.4.1. General Configuration

C1an and C1xn can work as wireless bridge under either 802.11a or 802.11na mode to build up a wireless backhaul link. User may configure Radio0 as bridge in Radio's general page via **Configuration**→**Wireless**→**Radio0**. This connection is a point-to-point connection. The setting of bridge devices **MUST** be the same in "Wireless Mode", "Radio Frequency", and "Security".

Figure 5-50 Bridge Mode

Enable Radio: Enable or disable Radio0.

Radio Mode: Operation mode of Radio0; It can be configured as AP, Station, Repeater and Bridge.

Country Code: Specify country that C1an locates. This setting is related about radio regulatory domain, such as maximum transmission power, available operating frequency channel ... etc. Hong Kong is default setting.

Wireless Mode: Specify wireless mode of C1an; User may configure the WLAN standard and channel bandwidth via this option. By default, it is 5GHz 130Mbps (802.11na HT20).

Radio Frequency: Specify the operating frequency channel.

Transmit Power: Specify the maximum transmission power (dBm) of C1an radio0.

Configure C1an radio0 as “Bridge” Mode:

- 1 Select **Configuration**->**Wireless**->**Radio0**->**General**
- 2 Check **Enable Radio** to enable radio0 if necessary.
- 3 Select to “Bridge” in **Radio Mode**
- 4 Select your country code in **Country Code**
- 5 Select desire wireless mode in **Wireless Mode**
- 6 Select operating channel in **Radio Frequency**
- 7 Set maximum transmit power in **Transmit Power**
- 8 Click **Submit**
- 9 Click **Save&Apply** to apply

5.4.1.4.2. Static Bridge Setting

User may provide the remote AP's information and configure the corresponding security setting via **Configuration**→**Wireless**→**Radio0**→**Static Bridge**. For more detail setting, please click the "More..." under "Detail".



Figure 5-51 5G bridge setting

Bridge ID: Bridge number.

Remote MAC Address: MAC address of the remote bridge peer.

Cipher Mode: Specify the data encryption mechanism; there are 3 options: "Disable", "WEP" and "AES". The default setting is "Disable".

5.4.1.4.2.1. Bridge General Setting

User may provide the details about remote bridge peer via **Configuration**→**Wireless**→**Radio0**→**Static Bridge** to click "More..."

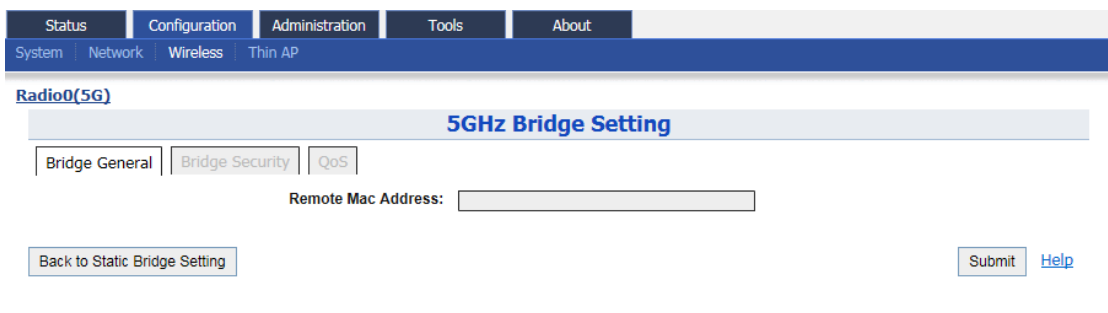


Figure 5-52 5G bridge setting

Remote MAC Address: Specify the MAC address of remote bridge peer.

5.4.1.4.2.2. Bridge Security Setting

User may specify the cipher mode in bridge link via **Configuration** → **Wireless** → **Radio0** → **Static Bridge**, to click the “More...” then select **Bridge Security**. It provides “Disable”, “WEP”, and “AES” as cipher mode. “WEP” means all data is transmitted with WEP encryption. The type of WEP encryption and key settings are determined by the entries in the WEP Key Table. AES provide stronger data protection than WEP. User is required to provide a 128-bit HEX pass phrase for data encryption.

The screenshot shows the web configuration interface for the 5GHz Bridge Security setting. The navigation menu includes Status, Configuration, Administration, Tools, and About. Under Configuration, there are links for System, Network, Wireless, and Thin AP. The main content area is titled "Radio0(5G) 5GHz Bridge Setting" and has three tabs: Bridge General, Bridge Security (selected), and QoS. The "Authentication Mode" is set to "Open". The "Cipher Mode" dropdown menu is set to "Disabled". There are "Back to Static Bridge Setting" and "Submit" buttons, along with a "Help" link.

Figure 5-53 5G bridge security setting-Open & No security

The screenshot shows the web configuration interface for the 5GHz Bridge Security setting. The navigation menu includes Status, Configuration, Administration, Tools, and About. Under Configuration, there are links for System, Network, Wireless, and Thin AP. The main content area is titled "Radio0(5G) 5GHz Bridge Setting" and has three tabs: Bridge General, Bridge Security (selected), and QoS. The "Authentication Mode" is set to "Open". The "Cipher Mode" dropdown menu is set to "WEP". The "Default WEP Key" is set to "1" with a "(1-4)" label. There are "Back to Static Bridge Setting" and "Submit" buttons, along with a "Help" link.

Figure 5-54 5G bridge security setting-Open & WEP

The screenshot shows the web configuration interface for the 5GHz Bridge Security setting. The navigation menu includes Status, Configuration, Administration, Tools, and About. Under Configuration, there are links for System, Network, Wireless, and Thin AP. The main content area is titled "Radio0(5G) 5GHz Bridge Setting" and has three tabs: Bridge General, Bridge Security (selected), and QoS. The "Authentication Mode" is set to "Open". The "Cipher Mode" dropdown menu is set to "AES". The "Pass Phrase" field is empty, with a "Show" checkbox and a "(128-Bits HEX Key)" label. There are "Back to Static Bridge Setting" and "Submit" buttons, along with a "Help" link.

Figure 5-55 5G bridge security setting-Open & AES

Cipher Mode: Specify the data encryption mechanism for bridge link. It provides 3 options: "Disable", "WEP" and "AES".

"Disable" - no encryption is used for data transmission over the bridge link.

"WEP" - WEP encryption is used for data transmission over the bridge link. The type of WEP encryption and key settings are determined by the entries in the WEP Key Table.

"AES" - AES encryption is used for packet encryption over the bridge link. A 128-bit HEX pass phrase is required.

Default WEP Key: Specify which WEP key is used; this option is available only if cipher mode is set as "WEP"

Pass Phrase: Specify a 128-Bits HEX key for AES; this option is available only if cipher mode is set as "AES"



Warning: The configuration of bridge security MUST be the same in both bridge peers; otherwise the bridge link cannot be established.

5.4.1.4.2.3. QoS Setting

The QoS configuration in Bridge mode is as the same as that in AP mode. For the detail of QoS configuration in Station mode, please refer to section **WLAN X(0-15) QoS** for more details.

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

Figure 5-56 5G bridge Qos setting

5.5. Thin AP Configuration

C1n Series AP/CPE support thin AP mode. In thin AP mode user need an Access Controller (AC) to control and manage all the APs.

In Thin AP mode:

AP will accept the wireless access controller's management;

AP Execute 802.11 PHY and MAC layer function;

AP will complete encryption/decryption of 802.11 packets;

AP will complete Radio interface statistics ...etc.

AC controls AP and gives the configuration information to AP;

AC controls user's access to a wireless network, user's data forwarding and data statistics;

AC response for user's roaming management and security control...etc.

User may configure Thin AP via **Configuration**→**Thin AP**.

Figure 5-57 Thin AP Configurations

Thin AP: Enable or disable Thin AP mode.

Primary AC Address: Specify the Primary AC's IP address or domain name. Thin AP can also acquire AC's IP address from DHCP Server by DHCP options (DHCP option60 or option 43) when it's configured to a DHCP client.

Secondary AC Address: Specify the Secondary AC's IP address.

AP Name: Specify the Thin AP's name if necessary.

AP Location: Specify the AP Location information if necessary.

AC debug level: Set AC debug level information (from 0-10).

Managed Radio: Specify the Radio0 can managed by AC.

Creat Manage Wlan Switch: Specify whether create manage WLAN on thin AP. If create a manage WLAN, When thin AP is disconnected to AC, User can also manage this thin AP through manage WLAN.

WLAN Change Action: When the thin AP is disconnected to AC, It can close all WLAN or Tunnel WLAN.

Configure the thin AP Mode:

- 1 Enable VLAN via **Configuration** ->**Network** ->**VLAN**
- 2 Select **Configuration**->**Thin AP**
- 3 Check **Enable Thin AP** to enable C1n thin AP mode.
- 4 Specify the primary AC IP address in **Primary AC Address**
- 5 Specify the Secondary AC IP address in **Secondary AC Address**
- 6 Specify the **AP Name** when it's needed
- 7 Specify the **AP Location** when it's needed
- 8 Select **AC debug level** when it's needed
- 9 Specify the **Managed Radio** of C1n
- 10 Check the **Create Manage Wlan Switch** if necessary
- 11 Select Close All WLAN or Close Tunnel WLAN When the thin AP is disconnected to AC
- 12 Click **Submit**
- 13 Click **Save&Apply** to apply

Notice: When C1n enables DHCP client, it supports DHCP Option 60 in both IPv4 and IPv6. Administrator can specifies a DHCP Option 60 string up to 32 characters.

The screenshot shows the 'General Network Setting' page. The 'DHCP Option 60' field is highlighted with a red box. The value 'AltaiAP' is entered in this field. Other settings include 'Network Setting' set to 'Switch Mode', 'WAN Setting (IPv4)' set to 'DHCP', and 'LAN Setting (IPv4)' with IP address '192.168.98.1' and mask '255.255.255.0'.

Figure 5-58 DHCP Option 60 setting

6. Administration Configuration

6.1. User Admin

C1n supports three authentication options (Local/RADIUS/RADIUS + Local) for logging in web GUI. When user use RADIUS/RADIUS + Local for logging in web GUI, C1n support maximum two RADIUS servers (one for backup).

User may modify the password of administrator account and select the mode of logging in web GUI via **Administration** → **User Admin**. The default username is "admin", and default password is "admin".

The screenshot shows the 'User Admin' page. The 'UserName' field is set to 'admin'. The 'Authentication Type' dropdown is set to 'Local Authentication'. There are fields for 'Password' and 'Confirm Password'.

Figure 6-1 User Admin

Authentication Type: Here can select Local Authentication, RADIUS Authentication or RADIUS + Local Authentication

Local Authentication: Support 3-level User Login (root/admin/guest)

RADIUS Authentication: Authenticate user through RADIUS; if no response returned from RADIUS server, AP fallbacks to local authentication

RADIUS +Local Authentication: Login AP with local user login or RADIUS user login

6.2. Web Admin

User may specify the refresh interval of C1n web page and enable or disable system log for diagnostic purpose via **Administration**→**User Admin**.

The screenshot shows the 'Web Administration' page with two tabs: 'WEB Setting' and 'System Log Setting'. Under 'WEB Setting', there is a dropdown menu for 'Auto Refresh Interval' set to '10' with '(s)' next to it. Under 'System Log Setting', there is a checked checkbox for 'Enable Syslog', a 'Server IP Address' field with four input boxes each containing '0', and a 'Severity' dropdown menu set to 'Informational'. At the bottom right, there are 'Submit' and 'Help' buttons.

Figure 6-2 WEB Administration

Auto Refresh Interval: Specify the refresh interval that C1n refresh its web page automatically. The default setting is 10s.

Enable Syslog: Enable or Disabled syslog function; Administrator can classify system log by configuring digit of Kernel Log Level. The following table lists Severity log level which is presented by digits.


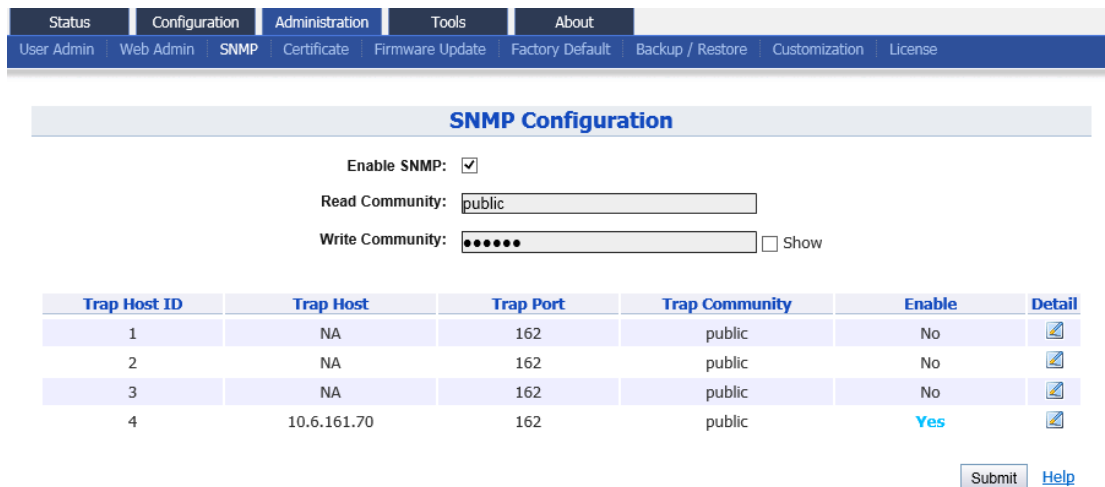
| Digit | Severity Level |
|--------------|-----------------------|
| 0 | Emergency |
| 1 | Alert |
| 2 | Critical |
| 3 | Error |
| 4 | Warning |
| 5 | Notice |
| 6 | Information |
| 7 | Debug |

Table 6- 1 Syslog severity

Server IP Address: Specify a remote syslog server that C1n sends the log messages; System Log allows C1n to send system log messages to a System Log server instantaneously. Administrator can choose either Local System Log Server or Remote System Log Server.

Syslog severity: Specify which severity level of log that C1n sends to remote syslog server. The severity options are listed in Table 6-1.

6.3. SNMP Setting

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. C1n supports SNMP protocol that user may use ALTAI Wireless Management System (AWMS) or a third party NMS to manage C1n Series AP/CPE. User may specify the SNMP setting via **Administration** → **SNMP**. Also user may click “







| 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 | 10.6.161.70 | 162 | public | Yes |  |

Figure 6-3 SNMP Configuration

Enable SNMP: Enable or Disable SNMP in C1n; if enabled, C1n communicates with AWMS or others NMS. By default, it is “Enabled”.

Read Community: Specify read community of SNMP protocol; the string of **Read Community** between NMS and C1n must be identical. If the community string is correct, C1n responds with the requested information from NMS; otherwise, C1n simply discards the request and does not respond. The default setting is “public”

Write Community: Specify write community of SNMP protocol; the string of **Write Community** between NMS and C1n must be identical. If the community string is correct, NMS can modify C1n configuration; C1n simply discards the request and does not respond. The default setting is “netman”.


Press  : To edit Trap Host

Enable SNMP function in C1n:

1. Select **Administration** → **SNMP**
2. Check **Enable SNMP** to enable SNMP protocol
3. Specify the string in both **Read Community** and **Write Community** that are identical in the NMS's setting.

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

6.3.1. Trap Host Setting

User may click "" to specify the SNMP manager if necessary.

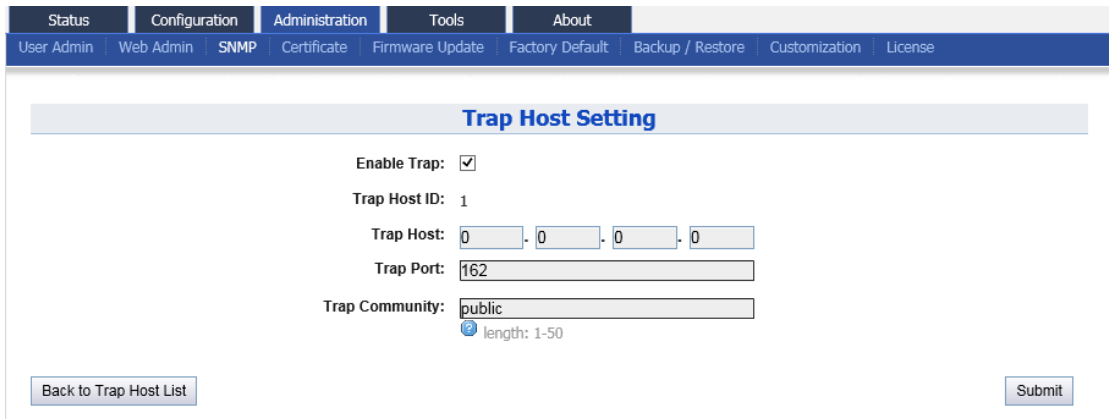


Figure 6-4 SNMP Trap Host

Enable Trap: Enable or Disable a particular trap host.


Trap Host ID: SNMP Trap host ID; C1n supports maximum 4 Trap Host.

Trap Host: Specify IP address of SNMP manager.

Trap Port: Specify the service port of SMNP Trap service, by default it is 162

Trap Community: Specify the string of trap community information.

Configure a trap host in C1n:

1. Select **Administration** → **SNMP**, then click ""
2. Check **Enable Trap**
3. Specify the IP address in **Trap Host**
4. Specify the port number of **Trap Port**
5. Specify the community string in **Trap Community** that is identical in the NMS's setting.
6. Click **Submit**
7. Click **Save&Apply** to apply

6.4. Certificate Management

C1n support HTTPS for its web portal, user may upload his SSL certification file and key file to C1n. User may manage SSL certification file and key file via **Administration** → **Certificate** to access Certification Management page.

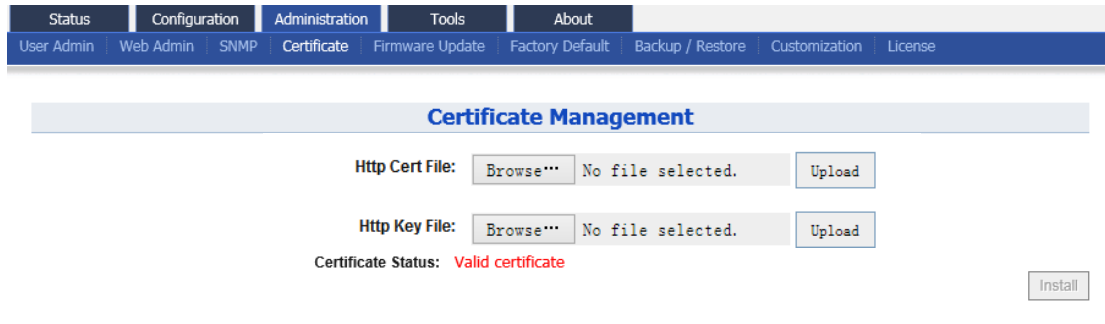


Figure 6-5 Certificate Management

Http Cert File: Specify user's certification file for HTTPS connection

Http Key File: Specify user's key file for HTTPS connection.

Configure C1n with customized SSL certification file and key file:

1. Select **Administration** → **Certificate**
2. Specify certificate file by clicking **Choose File** in **Http CertFile**, then click **Upload**
3. Specify key file by clicking **Choose File** in **Http Key File**, then click **Upload**.
4. Click **Submit**
5. Click **Save&Apply** to apply

6.5. Firmware Update

User upgrades or downgrades the C1n firmware via **Administration** → **Firmware Update** to access firmware update page. *It is highly recommended that please reboot once BEFORE performing firmware update.*

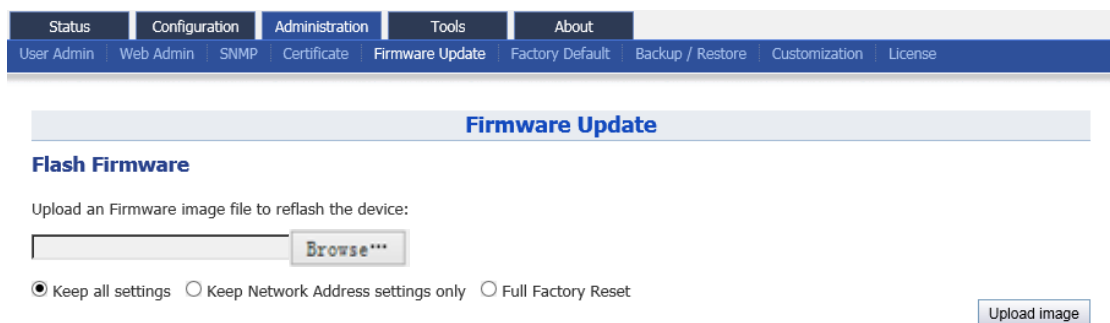


Figure 6-6 Firmware Upgrade



Caution: Do not interrupt the process of firmware update. Please maintain network connection and power supply. C1n Series AP/CPE will not function properly if interruption happened during firmware update.

Update the C1n firmware via web portal:

1. Select **Administration** -> **Firmware Update**
2. Specify the firmware image file (.bin)in local directory by clicking **Browse...**

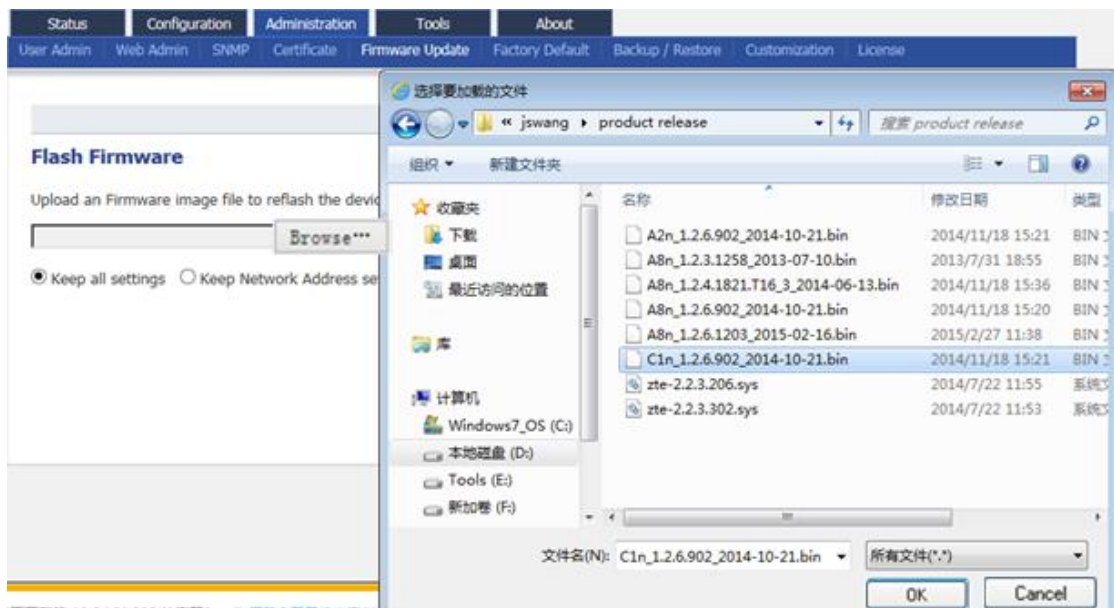


Figure 6-7 Select firmware file

3. Press **Upload image** to begin the update, the **keep all settings** allow user to keep the current configuration after update

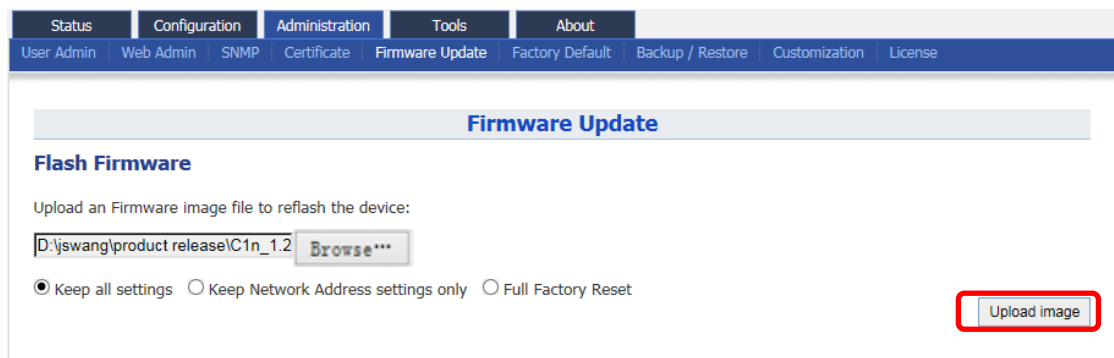


Figure 6-8 Press Upload Image to start firmware update

Keep all settings : All configuration will be kept after upgrading or downgrading.

Keep Network Address settings only : The configuration about the network settings like IP address and VLAN will be kept after upgrading or downgrading.

Full Factory Reset : All configuration will be lost and back to factory settings after upgrading or downgrading.

4. C1n will run the checksum on the firmware, once it validate the firmware, press **proceed** to continue.

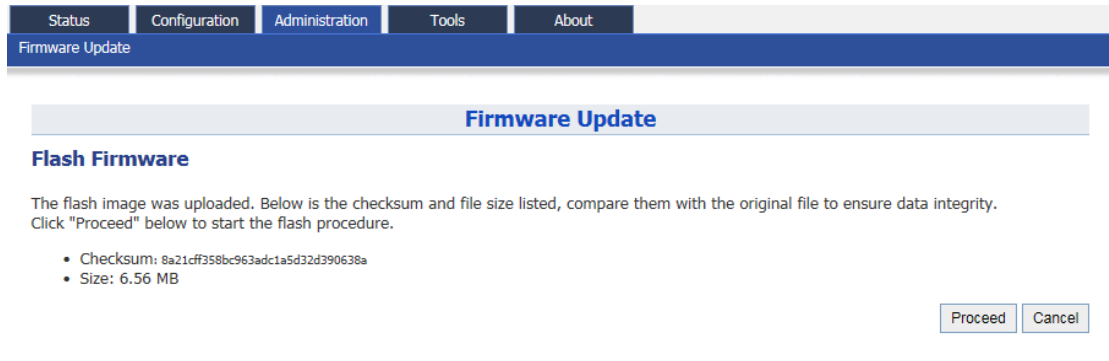


Figure 6-9 Press "Proceed"

5. You will find following upgrading status bar:

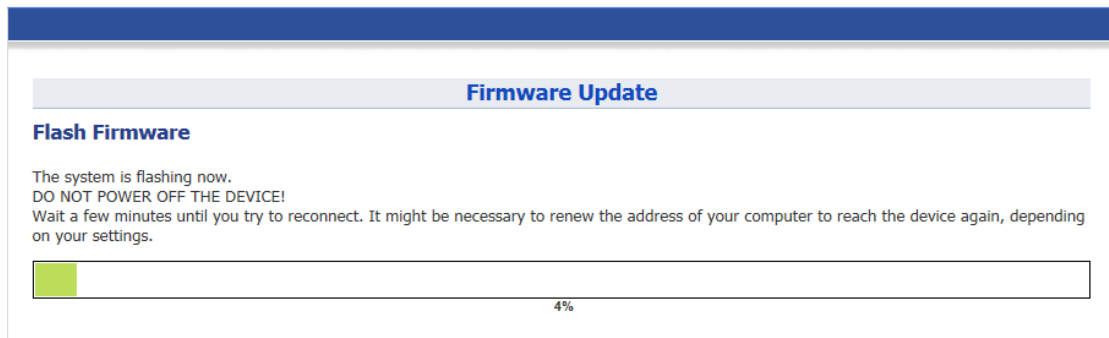


Figure 6-10 Progress of firmware update

6. C1n will reboot and load the Main page after firmware update.
7. Login with username and password, check the firmware version on the top right corner or go to the "About" page.



Figure 6-11 Information after firmware update

6.6. Restore Factory Default

There are 2 ways to reset the system back to factory default settings. User may reset the system via:

- Web portal;
- Hardware reset button

6.6.1. Reset back to factory default via web GUI

User can reset the C1n back to factory default settings via **Administration** → **Factory Default** to access Restore to Factory Default page. User may clear all the setting with or without restoring the current IP address.

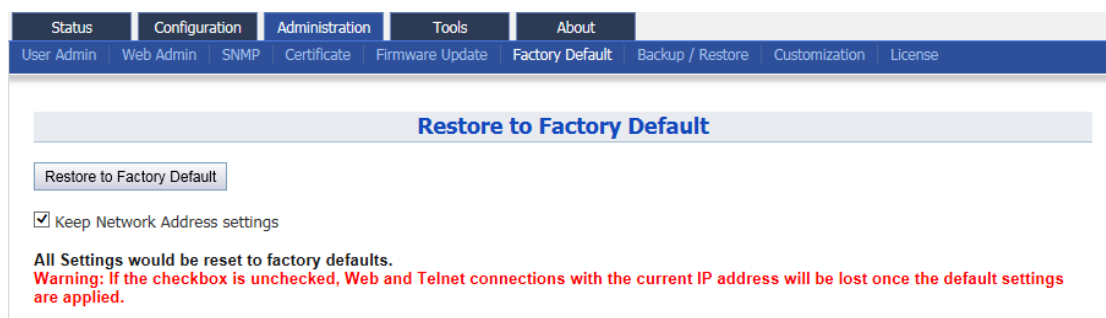


Figure 6-12 Restore to Factory Default

Restore C1n configuration to factory settings:

1. Select **Administration** → **Factory Default**

2. Check the option in **Keep Network Address Settings** if user wishes to retain the current IP address.
3. Press **Reset to Factory Default**

Once restore to factory default configuration, user can login to the C1n with the following information:

C1n Series default IP address: **192.168.1.222**

Username: **admin**

Password: **admin**

6.6.2. Reset back to factory default via reset button

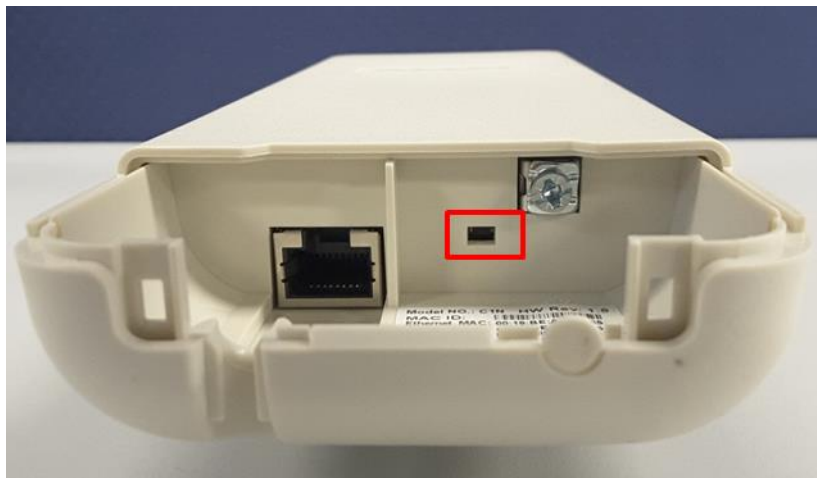


Figure 6-13 Reset Button

Hardware reset button have 2 functions:

- Soft-reboot [equivalent to UI: Reboot).
 - Press & Hold the reset button until you see four signal level LEDs blink once
 - Then release it immediately
- Reset to factory default [equivalent to UI: Reset factory (NOT retain network address)]
 - Press & Hold the reset button until you see four signal level LEDs blink once
 - Continue pressing the button until you see four signal level LEDs blink twice consecutively
 - Then release it immediately

6.7. Backup/Restore

C1n provides a Backup / Restore function that user backup or restore the configuration easily and quickly. User may backup or restore the C1n configuration via **Administration** → **Backup/Restore**.

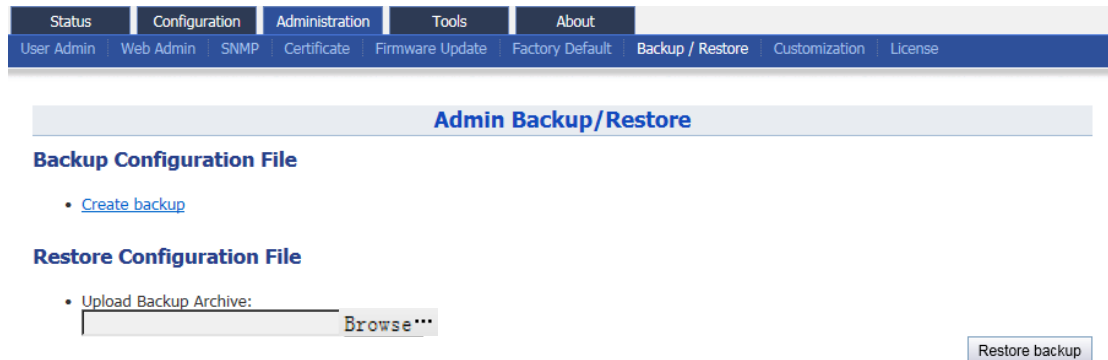


Figure 6-14 Backup/Restore

Backup C1n configuration:

1. Select **Administration** → **Backup/Restore**
2. Press **Create backup** and save it.

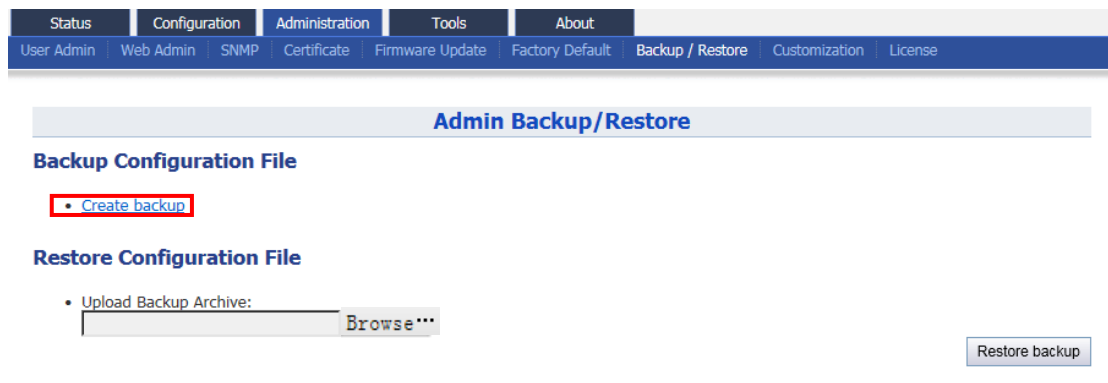


Figure 6-15 Backup

Restore C1n configuration from backup configuration file:

1. Select **Administration** → **Backup/Restore**

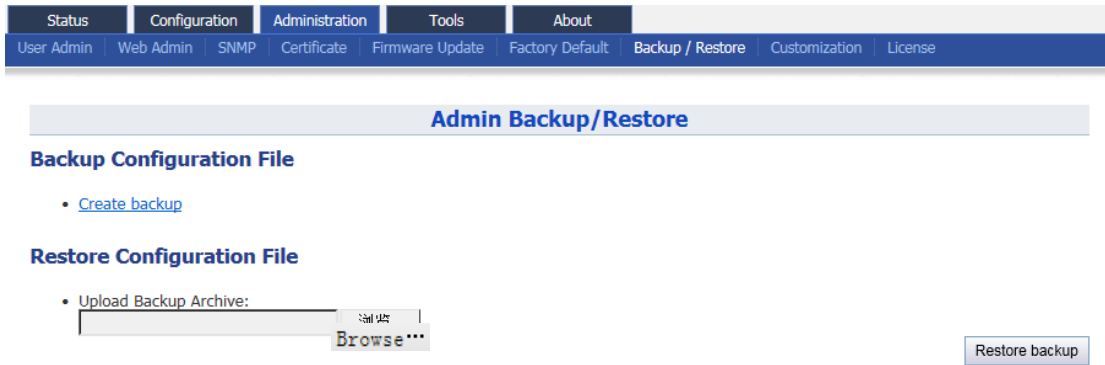


Figure 6-16 Restore Backup

- Specify the configuration in local directory by clicking **Browse...**

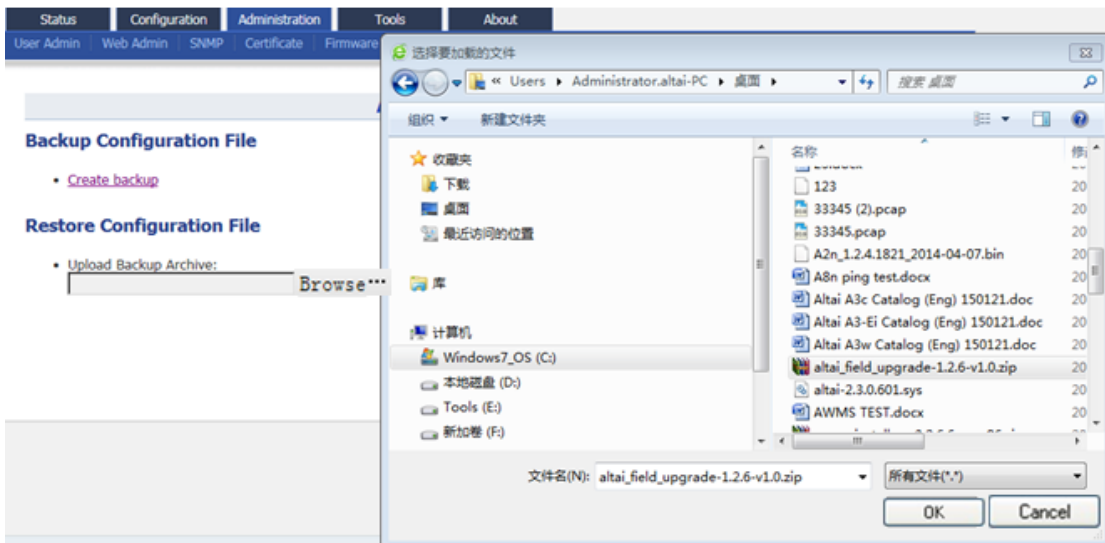


Figure 6-17 Select the backup file

- Click **Restore backup** to restore the configuration file.

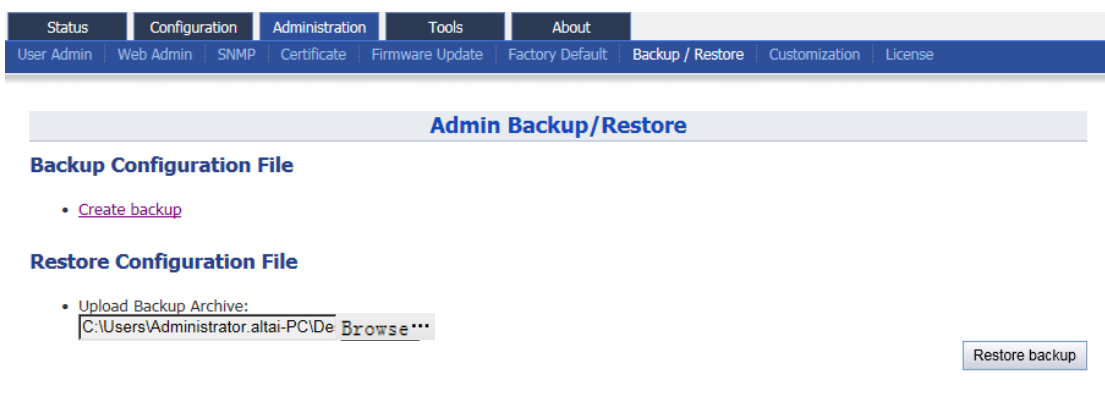


Figure 6-17 Press "Restore backup" to start restore

6.8. Customization

C1n supports factory restore customization; user may specify the desired configuration as factory default settings. User may manage configuration

customization via **Administration** → **Customization** to access Default Configuration Customization page. The important customize file are system, network, and wireless. They are used for customize the system, network, wireless default configuration information respectively.

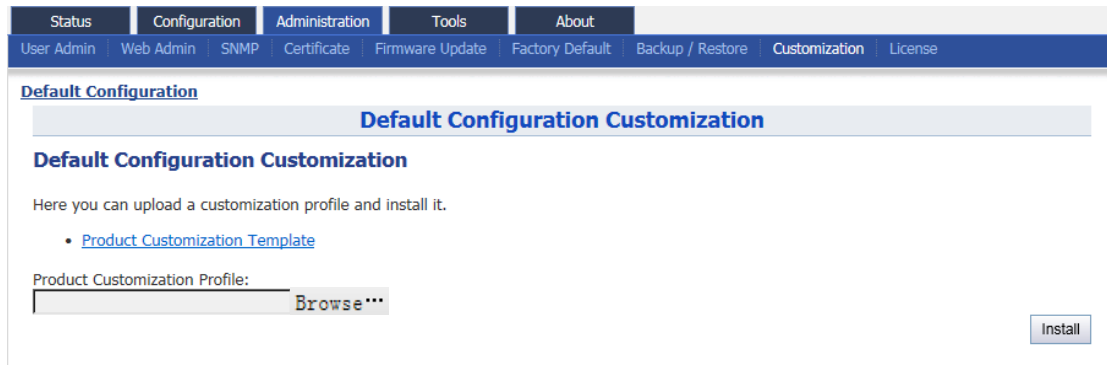


Figure 6- 18 Default Configuration Customization

Customize a configuration as desired default settings:

1. Download the template by clicking [Product Customization Template](#) and save it.

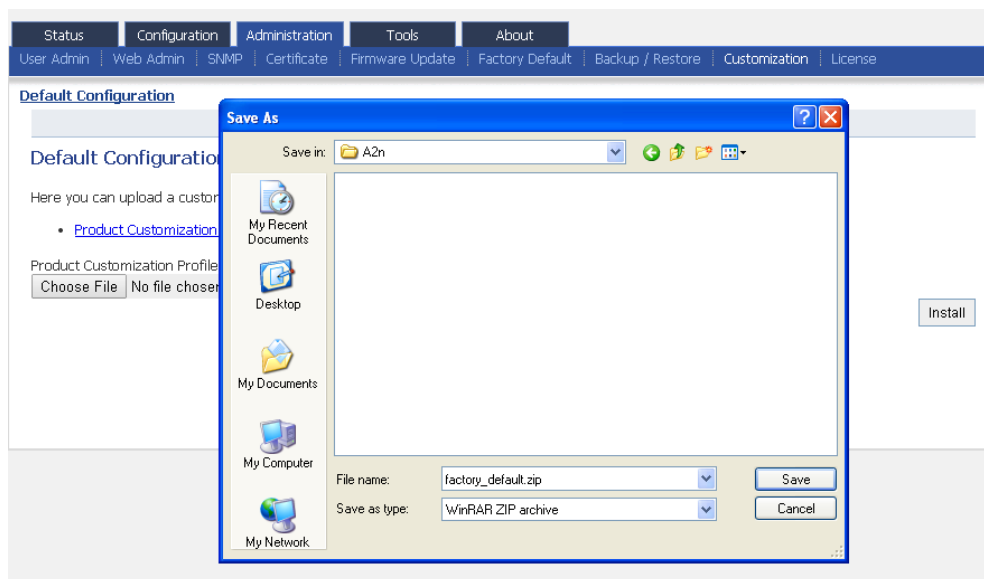


Figure 6- 19 Save the products custom templates to the specified directory

2. Use 7-zip software to open the template file, and edit the files in the factory_default.zip.



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.

3. Edit the desired setting in system, network, and wireless files.

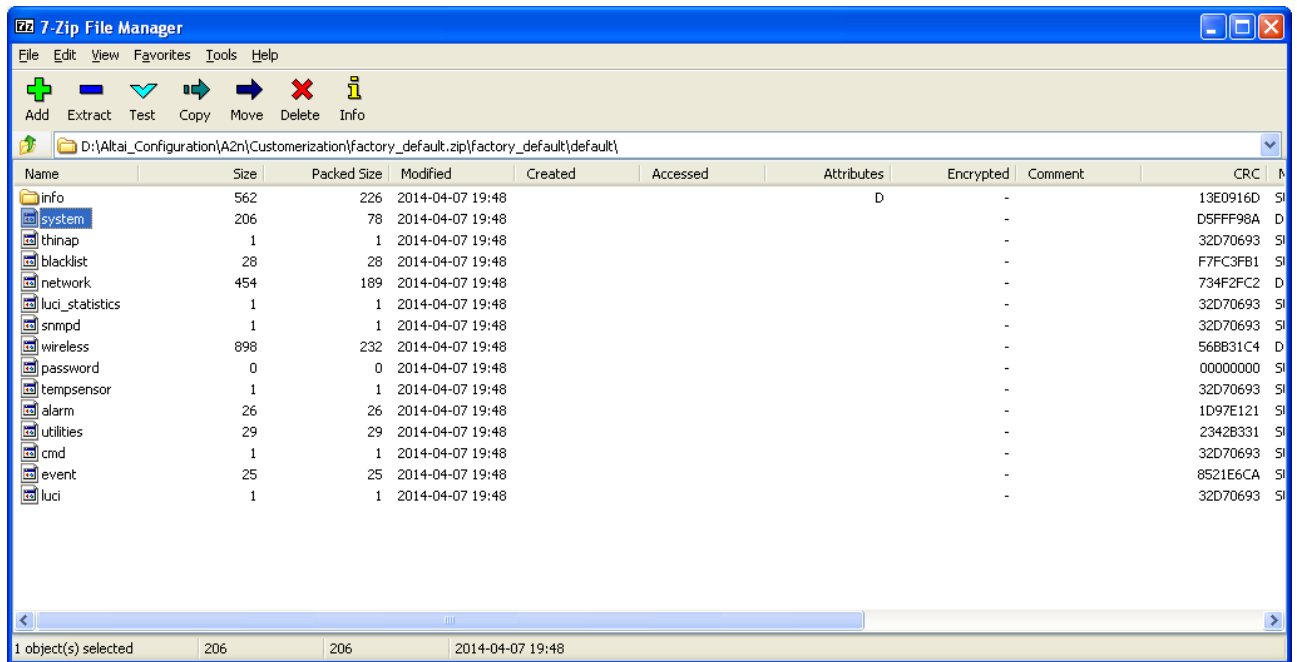


Figure 6- 20 files under "default"

4. Right click on the file and select "Edit the file to customize (open with notepad)", click the "Save" and exit after edit

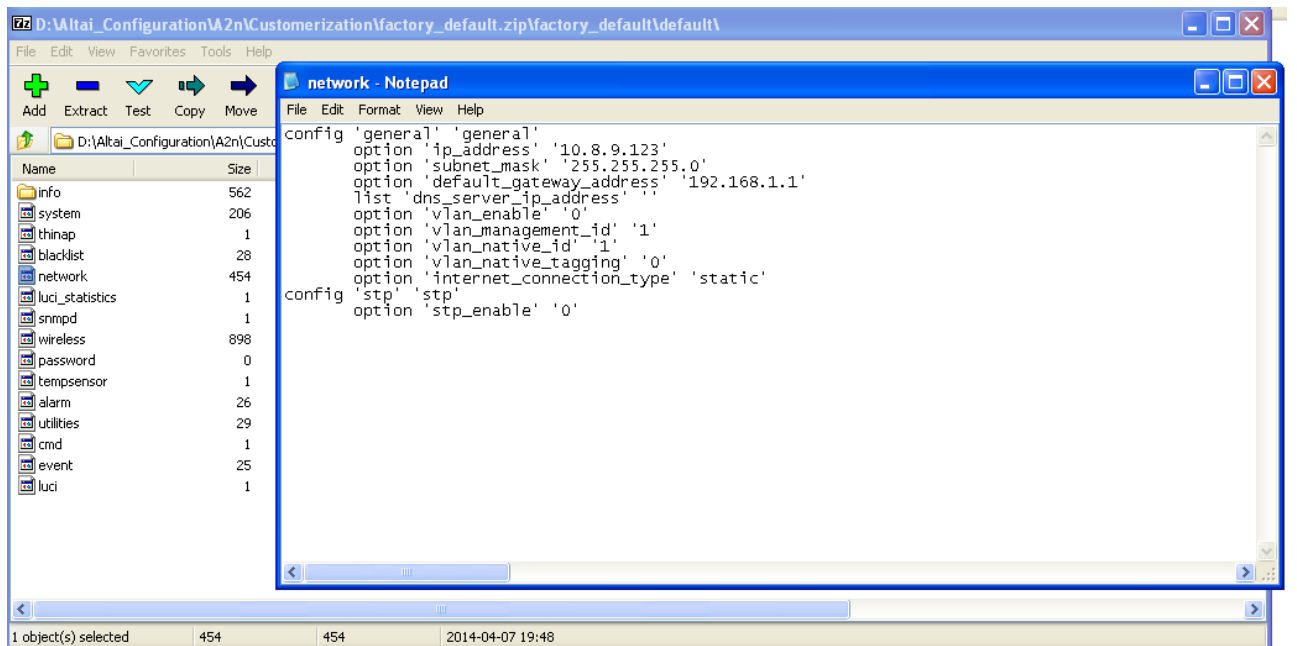


Figure 6- 21 Customized network settings

5. Access the Default Configuration Customization page via **Administration** → **Customization**.
6. Specify the customization file in local directory by clicking **Choose File**
7. Press **Install** button
8. Restore C1n to factory default after upload success.



Warning: Customization will take effect after reboot. Since improper customization may cause malfunction of C1n, please contact Altai support team for any queries.

6.9. License

C1n supports license management functions for defining Radio module operating mode. User may manage the customized license file via **Administration** → **License**.

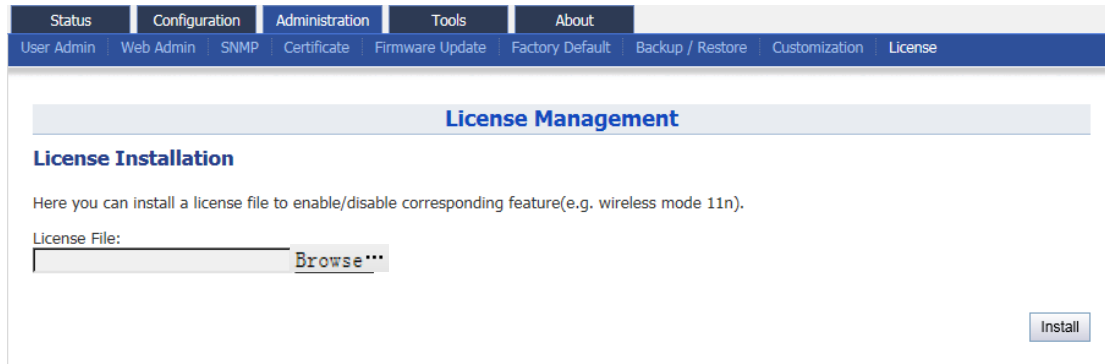


Figure 6- 22 C1n license management

Upload a license file to C1n:

1. Select **Administration** → **License**
2. Specify the license file in local directory by clicking **Browse...**
3. Press **Install** button

7. Tools

C1n provides useful tools for radio planning, diagnosis, and device's maintenance.

7.1. Channel Scan

C1n Series AP/CPE provides a channel scanning tool; user is able to know the status of 2.4GHz radio (C1n and C1xn) or 5GHz radio (C1an and C1xan) in the surrounding area. Throughout this tool, user may collect noise floor, percentage of channel busy, and the number of AP in particular radio channels. User may configure this Wi-Fi network based on such useful information. User may perform channel scan via **Tools** → **Channel Scan**.

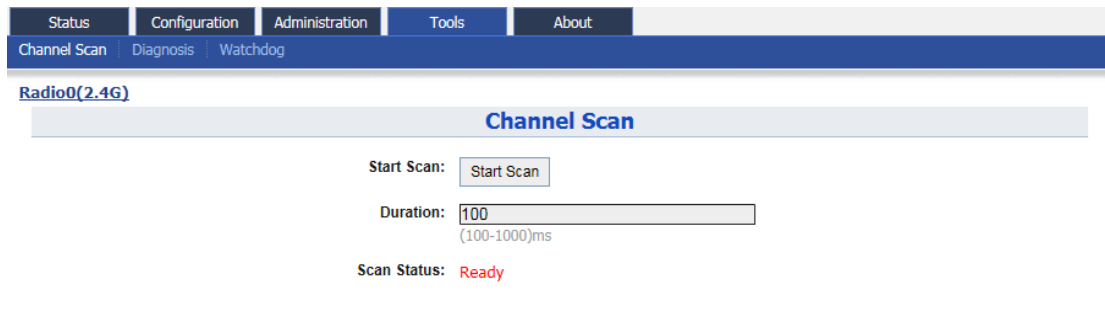


Figure 7-7-1 Channel Scan

Start Scan: Press **Start Scan** to start Radio0 channel scan.

Duration: Specify the channel scanning interval; the range is from 100ms to 1000ms. The default setting is 100ms.

Scan Status: Indicate the current status of 2.4GHz radio for channel scanning. It can be "Ready", "In Progress", and "Success".

"Ready" means that the radio can perform scanning.

"In Progress" means that the radio is scanning.

"Success" means the scanning is finished. User may review the result or scan the channel again.

Scan the channel status of radio0:

1. Select **Tools** → **Channel Scan** → **Radio0**
2. Specify the scanning duration in **Duration**
3. Press **Start Scan**
4. Wait until the scan status change to "Success". The scanning will take approximately 20 seconds

7.1.1. Overview Info

User may review the information about channel usage via **Tools** → **Channel Scan** → **Radio0** → **Overview**. The information includes "Noise Floor", "Busy %", and "no. of AP".

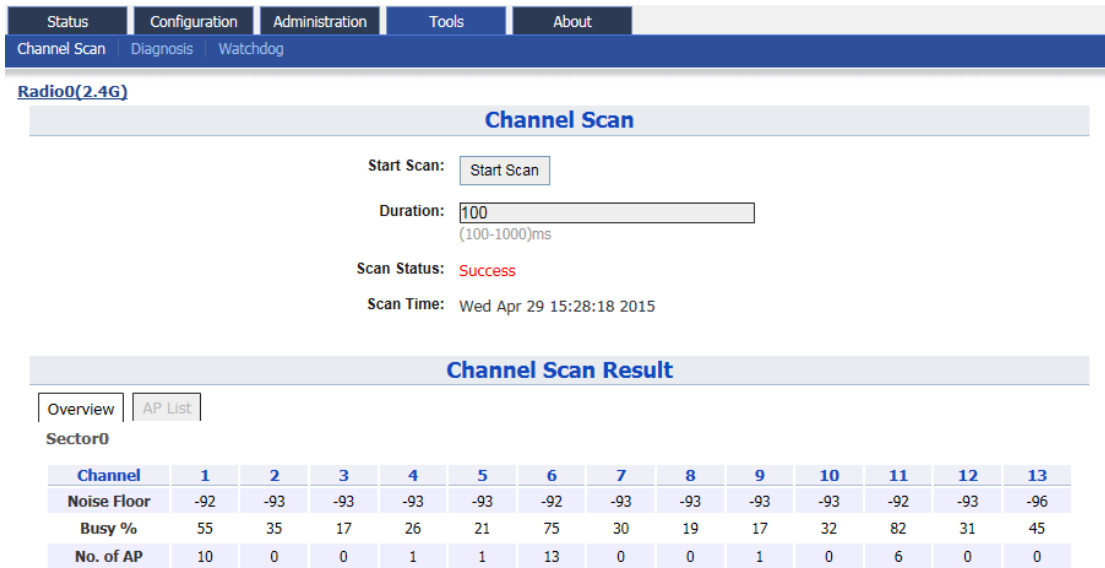


Figure 7-2 2.4G Channel Scan

Noise Floor(dBm): Noise floor of 2.4GHz channels.

Busy%: Busy state percentage of 2.4GHz channels.

No. of AP: The number of APs that are operating in the particular channel.

7.1.2. AP List Info

User may review view 2.4G AP List Info around C1n via **Tools** → **Channel Scan** → **Radio0** → **AP List**. It includes SSID, BSSID, Authentication Mode, Cipher, Channel, Date Rate and SNR.

The screenshot shows the web-admin interface for Radio0(2.4G). The top navigation bar includes Status, Configuration, Administration, Tools, and About. Below this, there are tabs for Channel Scan, Diagnosis, and Watchdog. The main content area is titled "Radio0(2.4G)" and contains a "Channel Scan" section. In this section, there is a "Start Scan" button, a "Duration" input field set to 100 (with a range of 100-1000)ms, a "Scan Status" indicator showing "Success", and a "Scan Time" of "Wed Apr 29 15:28:18 2015". Below the scan configuration is a "Channel Scan Result" section with two tabs: "Overview" and "AP List". The "AP List" tab is active, displaying a table of detected APs.

| SSID | BSSID | Auth Mode | Cipher | Channel | Rate(Kbps) | SNR(dB) |
|---------------------|-------------------|-----------|--------|---------|------------|---------|
| CITYUSRI | 00:23:89:34:8c:b0 | open | none | 11 | 54000 | 38 |
| CITYUSRI-WPA | 00:23:89:34:8c:b1 | wpa | tkip | 11 | 54000 | 38 |
| jason-test-open | 00:19:be:80:b2:19 | open | none | 11 | 130000 | 46 |
| CITYUCB | 00:23:89:75:0a:f2 | open | none | 11 | 54000 | 20 |
| CITYUCB | 00:23:89:34:8c:b2 | open | none | 11 | 54000 | 38 |
| CITYUSRI | 00:23:89:75:0a:f0 | open | none | 11 | 54000 | 19 |
| Superwifi Network 0 | 00:19:be:80:b2:0d | open | none | 1 | 130000 | 48 |
| CITYUSRI | 00:23:89:34:8c:90 | open | none | 1 | 54000 | 20 |
| Superwifi Network 0 | 00:19:be:00:50:0c | open | none | 1 | 130000 | 34 |
| Superwifi Network 0 | 00:19:be:a3:06:8e | open | none | 1 | 216700 | 39 |

Figure 7-3 2.4G AP List Info



Caution: During the process of channel scan, all WiFi clients associated to C1n Series AP/CPE via 2.4G or 5G channel will be drop for approximately 15-20 seconds. The operation for 5G Radio of C1an/C1xan be the same to 2.4G Radio.

7.2. Diagnosis

Press **Tools** -> **Diagnosis** to start the diagnosis.

12.1.1. Ping to Host

Press **Tools** -> **Diagnosis** -> **Ping** to start the ping.

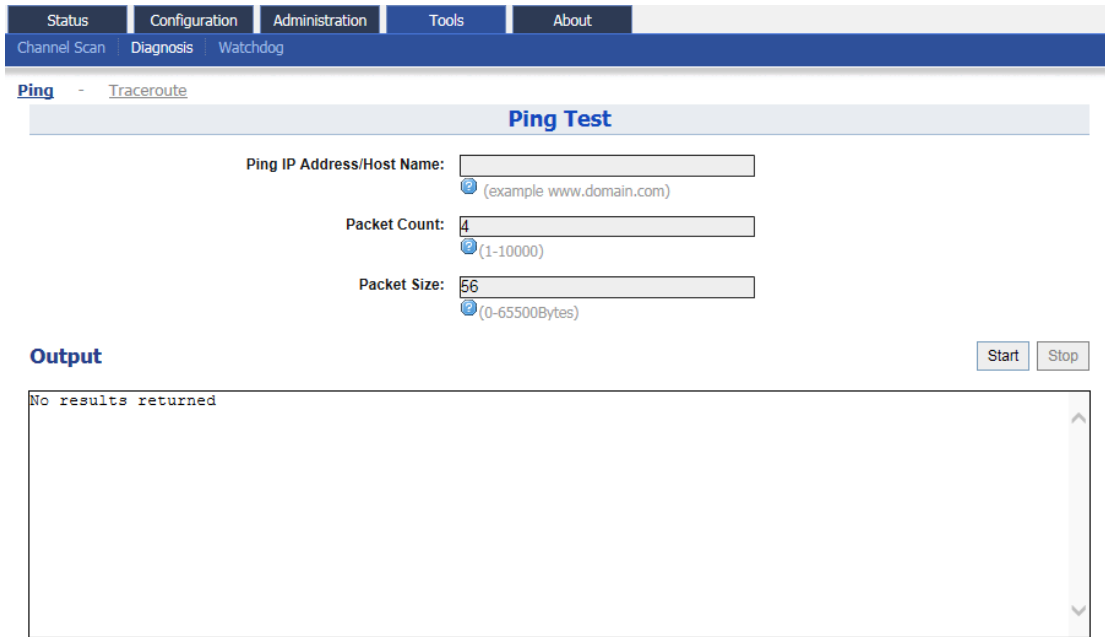


Figure 7-4 Ping to Host

Ping IP Address/Host Name: Type in the target IP address or target Host name.

Packet Count: The range for Packet count is 1-10000.

Packet Size: Type in the packet size for ping.

12.1.2. Traceroute to Host

Press **Tools** -> **Diagnosis** -> **Traceroute** to start the trace.

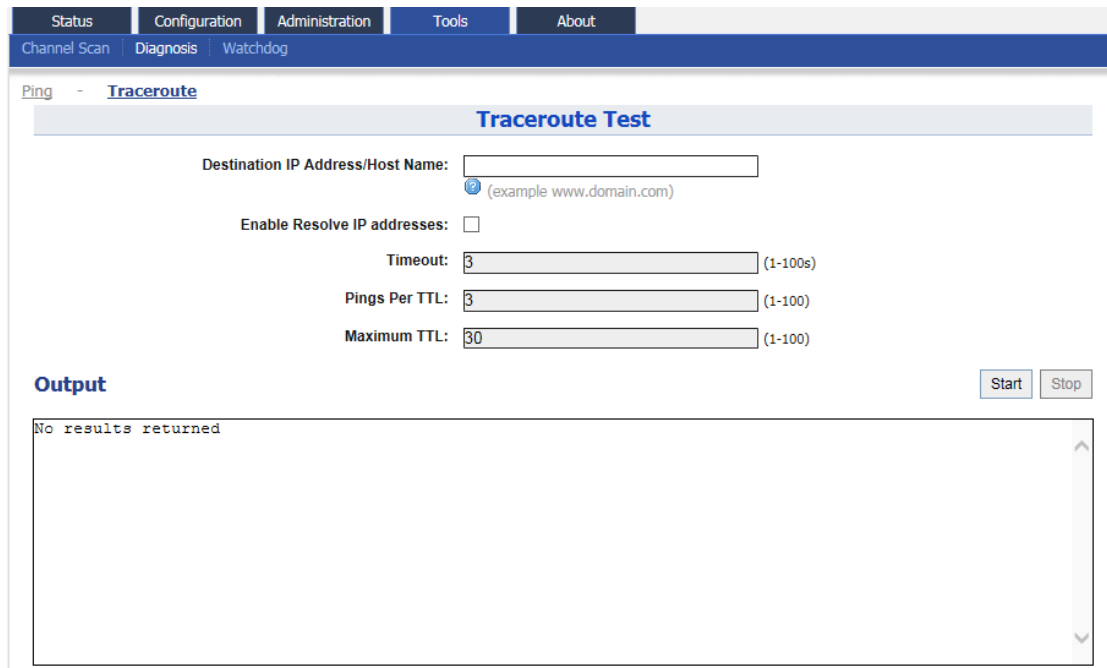


Figure 7-5 Traceroute

Destination IP Address/Host Name: Type in the target IP address or target Host name.

Enable Resolve IP Address: Enable or disable IP address resolve.

Timeout: Type in the timeout value.

Ping per TTL: Type in the TTL value for ping.

Maximum TTL: Type in the maximum TTL value for ping.

7.3. Watchdog

7.3.1. Schedule Reboot

Schedule reboot Watchdog is an electronic timer that is used to detect and recover from system malfunctions. That is timer for periodic reboot and Periodic upload log.

User may enable the watchdog via **Tools** -> **Watchdog**.

Figure 7-6 Watchdog Setting

Periodic Reboot: Enable or Disable the periodic reboot function, by default, it is disable.

Random Delay: Enable or disable a random delay on scheduled rebooting time; it prevents all APs reboot at the same time. If all APs reboot at the same time, the service may be suspended completely. By default, it is disabled.

Schedule Mode: Specify the reboot time.

Periodic Mode: Set the periodic time for rebooting, the max period is 30days.

Periodic Upload Log: Enable or Disable the periodic upload log function, by default, it is disable.

Random Delay: Enable or disable a random delay on scheduled upload time; if all APs are upload log at same time, it may cause network very busy. By default, it is disabled.

FTP Server User Name: Type in the FTP account user name.

FTP Server Password: Type in the FTP account password.

FTP Server IP Address: Type in the IP address of FTP server.

FTP Server Port: Type in the port number of FTP server.

Schedule Mode: Specify the time for uploading log file.

Periodic Mode: Set the periodic time for uploading the log, the max period is 30days.

7.3.2. Ping Watchdog

This feature allows devices to ping the target host periodically.

Figure 7-7 Ping watchdog

Enable Ping Watchdog: Enable or disable ping watchdog.

IP Address To Ping: Set the target IP address to ping.

Ping Interval: The default ping interval (time between ICMP echo requests are sent) is 300 seconds.

Startup Delay: Startup Delay specifies the initial time delay (in seconds) until the first ICMP echo requests are sent by Ping Watchdog. The default value is 300 seconds. 60 seconds is recommended value for the Startup Delay as the network interface and wireless connection initialization takes a considerable amount of time if the device is rebooted.

Failure Count to Reboot: Failure Count to Reboot Specify the number of ICMP echo response replies. If the specified number of ICMP echo response packets is not received continuously, Ping Watchdog will reboot the device. The default value is 3.

8. C1n Series Information

The “About” in the web layout shows the hardware, software version and information of company.



Figure 8-8-1 C1n Series "About"

Details of C1n Series AP/CPE Information:

Production Information: This shows the name, code, serial number, product mode information of C1n.

Hardware Version: Display the hardware version of C1n.

Software Version: Display the software version of firmware and MIB.

Company Information: Display information of Altai.