Altai C1n Super WiFi CPE/AP Configuration Manual

For Firmware Version 1.0.0.x

Version 1.0

Date: 16-Aug-2012

Altai Technologies Limited
Unit 209, 2nd Floor,
No.10 Science Park West Avenue, Phase 2,
Hong Kong Science Park,
Shatin, New Territories,
Hong Kong

Telephone: +852 3758 6000
Fax: +852 2607 4021
Web: www.altaitechnologies.com

Customer Support Centre:
Email: support@altaitechnologies.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 and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

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

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

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

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator and your body.

Important Note

For product available in the USA/Canada market, only channel 1-11 can be operated. Selection of other channels is not possible.

Disclaimer

All specifications are subject to change 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.

Table of Contents

Table of Figures

Manual Conventions

Bold	Bold type within paragraph text indicates commands, files names, directory names, paths, output, or returned values.
Italic	Within commands, italics indicate a variable that the user must specify. Titles of manuals or other published documents are also set in italics.
_____	Underline means that the words you have to pay attention.
`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 from which the user must choose.
|	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 configuration for the ALTAI C1n Super WiFi CPE/AP through web-admin interface.

2 C1N MODEL AND FIRMWARE VERSION

This manual is applicable for the following models and firmware version:

Product name : **C1n Super WiFi CPE/AP**
Model number: **WA1011N-G**
Firmware version: **v1.0.0.x**

3 GETTING START

3.1 SETUP LOCAL AREA CONNECTION ON YOUR PC

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

- RJ-45 Ethernet Cable Straight Cable has to be used if C1n Super WiFi CPE/AP and your PC are connected by a switch or a hub.
- RJ-45 Ethernet Cable Crossover Cable has to be used if C1n Super WiFi CPE/AP and your PC are connected directly.

Please kindly refer to the Altai C1n Super WiFi CPE/AP Installation Guide.

Start Network Configuration on your PC.

For Windows XP user,

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

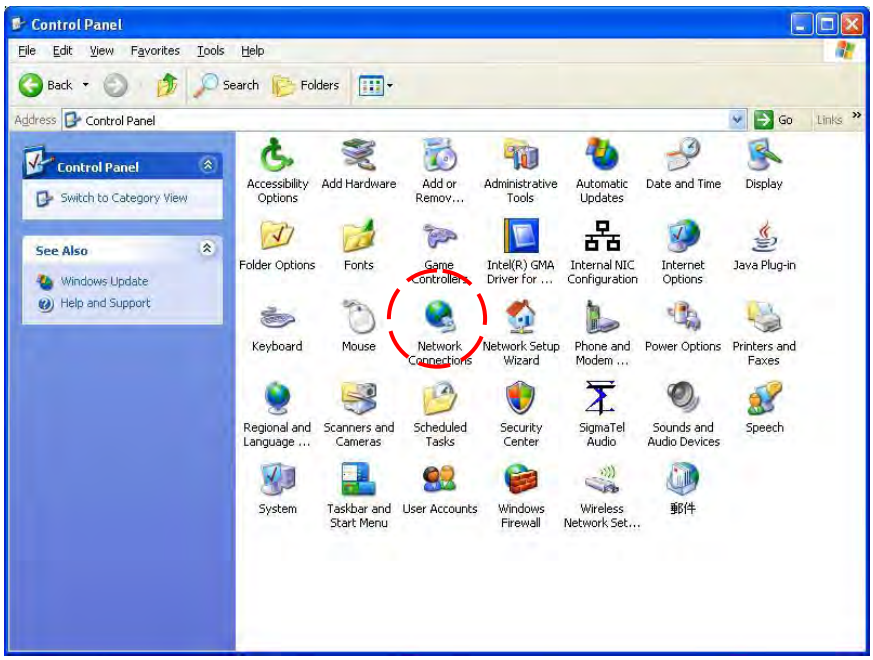


Figure 1 Control Panel in Windows XP

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

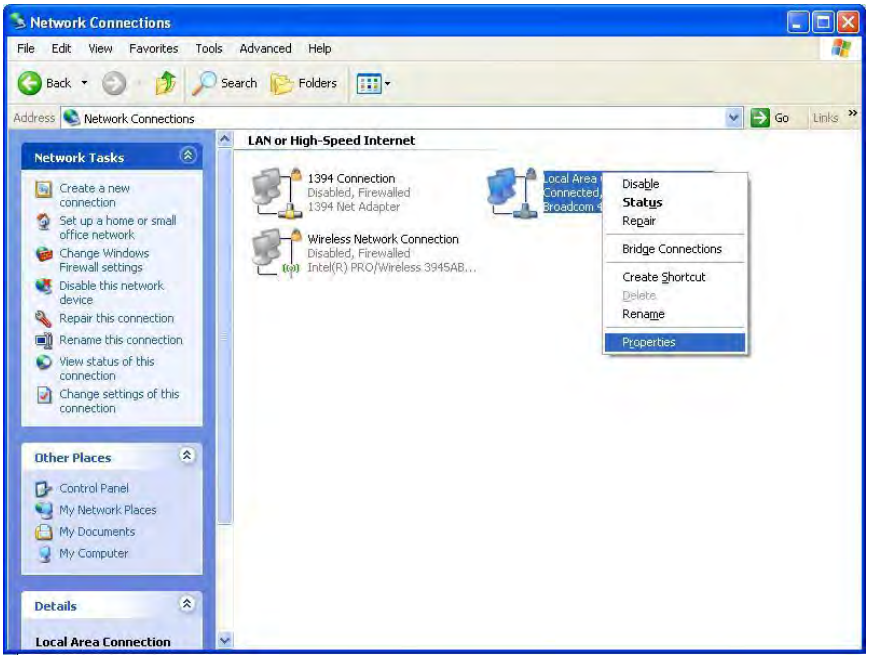


Figure 2 Network Connections in Windows XP

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

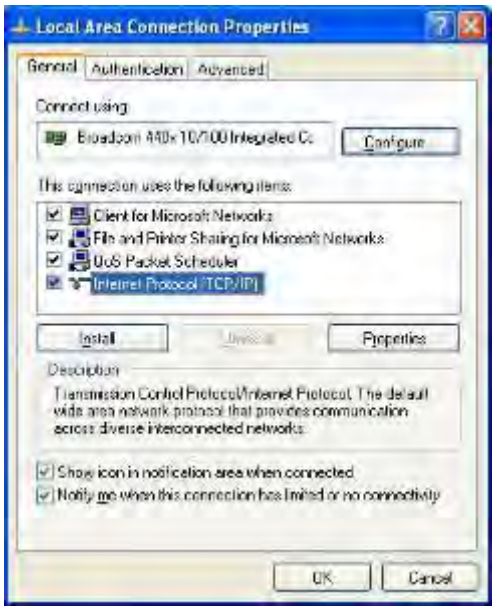


Figure 3 Local Area Connection Properties in Windows XP

5. Marking the "Internet Protocol (TCP/IP)" and click the "**Properties**".
6. Type in an "**IP address**", for example, 192.168.1.2, which is under the same subnet as the Default IP address of C1n Super WiFi CPE/AP (192.168.1.20).
7. Using the default "**Subnet mask**" (default: 255.255.255.0) setting at the first time.
8. Keep the "**Default gateway**" as "Blank".
9. Keep the "**Preferred DNS server**" and "**Alternate DNS server**" as "Blank" also.

10. Click "**OK**" when you finish setting and close the Window.

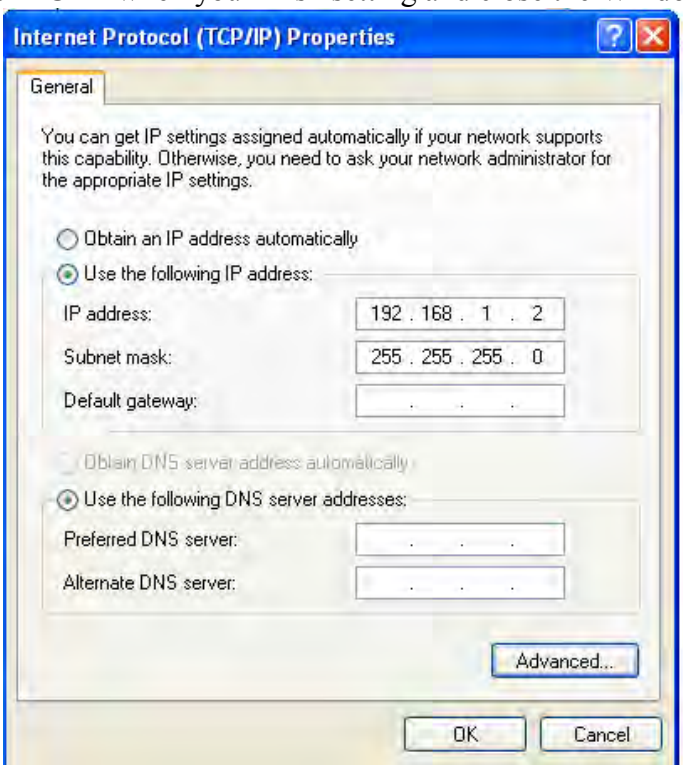


Figure 4 Internet Protocol (TCP/IP) Properties in Windows XP

3.2 CHECK ACCESS

"`ping`" utility of DOS mode is a handy tool to check the access to the C1n Super WiFi CPE/AP.

1. Go to DOS mode by typing "cmd" in "**Run**".
2. Type command:

   ```
   ping 192.168.1.20
   ```

   The C1n Super WiFi CPE/AP shall respond to your ping request if it has a correct connection with your PC.

NOTE: Using the same PC to ping different C1n Super WiFi CPE/AP may cause ping failure. This is because the C1n Super WiFi CPE/AP have the same default IP address but different MAC addresses. You need to type a command "`arp -d`" in DOS mode to clear ARP table on PC before each ping.

4 CONFIGURATION WITH WEB-ADMIN

4.1 WEB BROWSER CONNECTION

The C1n 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 Super WiFi CPE/AP. Example: http://192.168.1.20, where 192.168.1.20 is the C1n's IP address. The **C1n default IP Address** is **192.168.1.20**. Note: the release version 1.0.0.16 only supports **http format URL link.**

2. A window will pop up, as shown in Figure 5. Enter the user name and password in the corresponding fields. The **default User Name** and **Password** are shown in Table 1. They are **case sensitive**.

	Default User Name	Default Password
From version 1.0. onwards	***altai***	***wag***

Table 1 Default User Name and Password for logging in C1n Super WiFi CPE/AP

Figure 5 Enter User Name and Password

3. A **Menu Bar** is located on the left hand side of the IE window. Different configurations can be chosen through the menu bar.

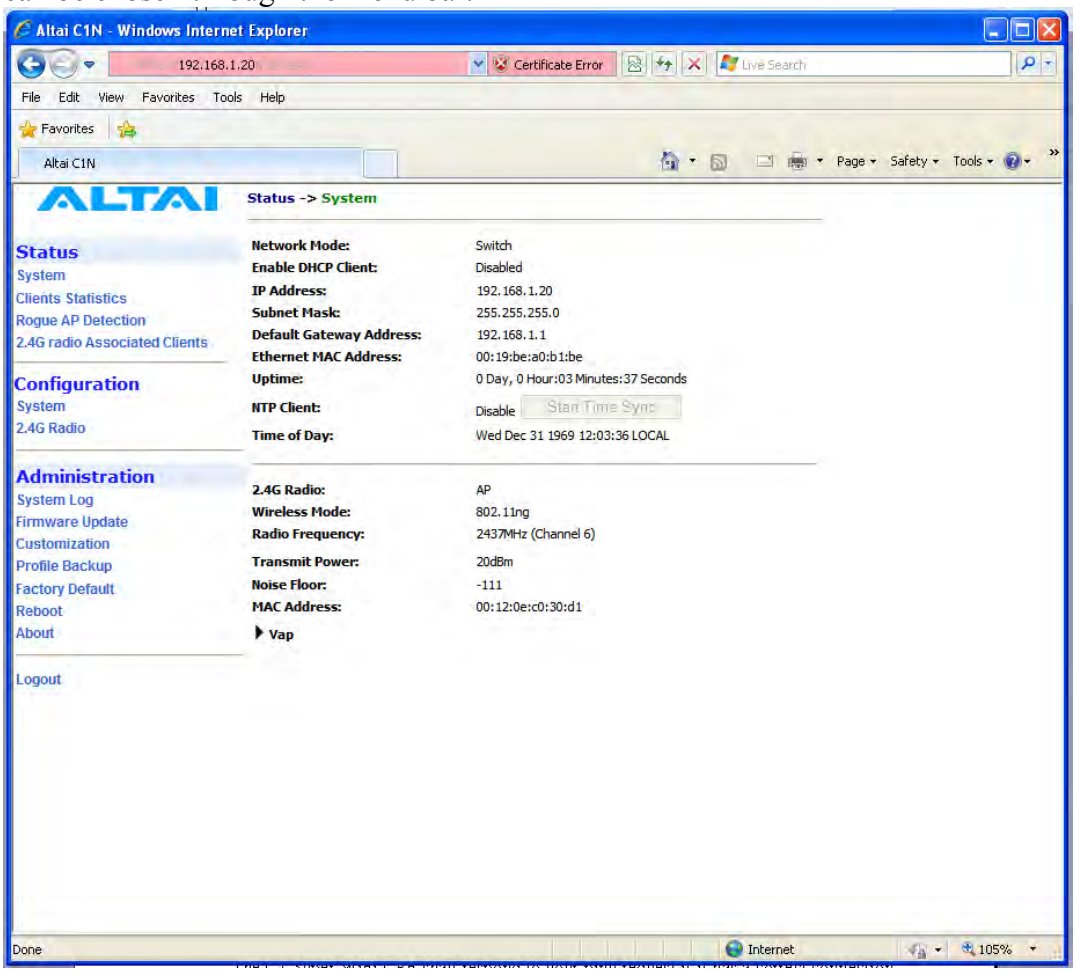


Figure 6 Web-admin Login Page

4.2 CHECKING THE C1N VERSIONS

The running version can be checked by selecting **About** under **Administration** in the menu bar. In Figure 7 Version of C1n Super WiFi CPE, it shows:

Firmware Version: v1.2.0.0

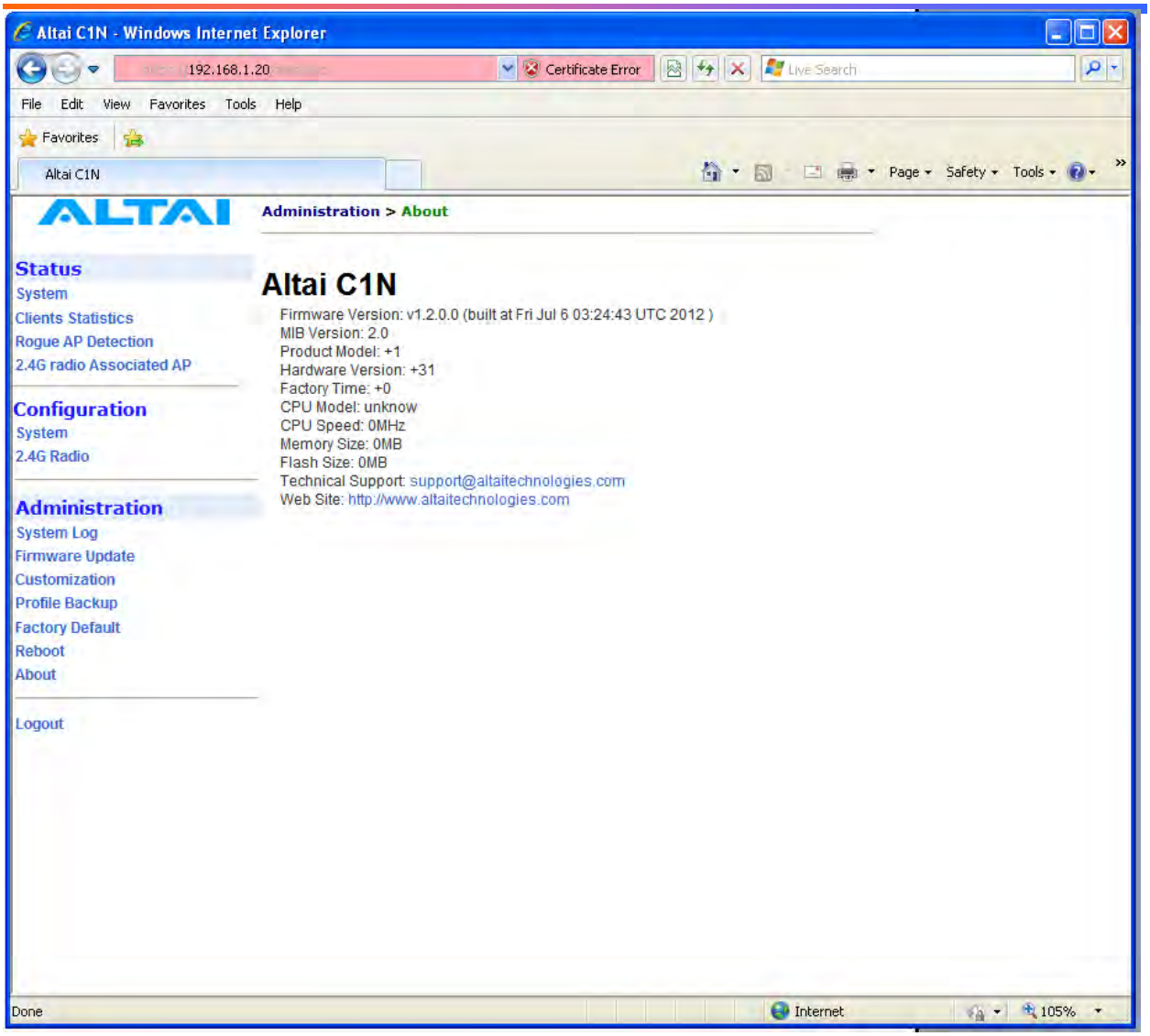


Figure 7 Version of C1n Super WiFi CPE/AP

4.3 SETUP – USER NAME, PASSWORD AND SYSTEM NAME

The ***Password*** and ***System Name*** can be configured by selecting **System** under **Configuration** in the menu bar, as shown in Figure 8 System Configuration

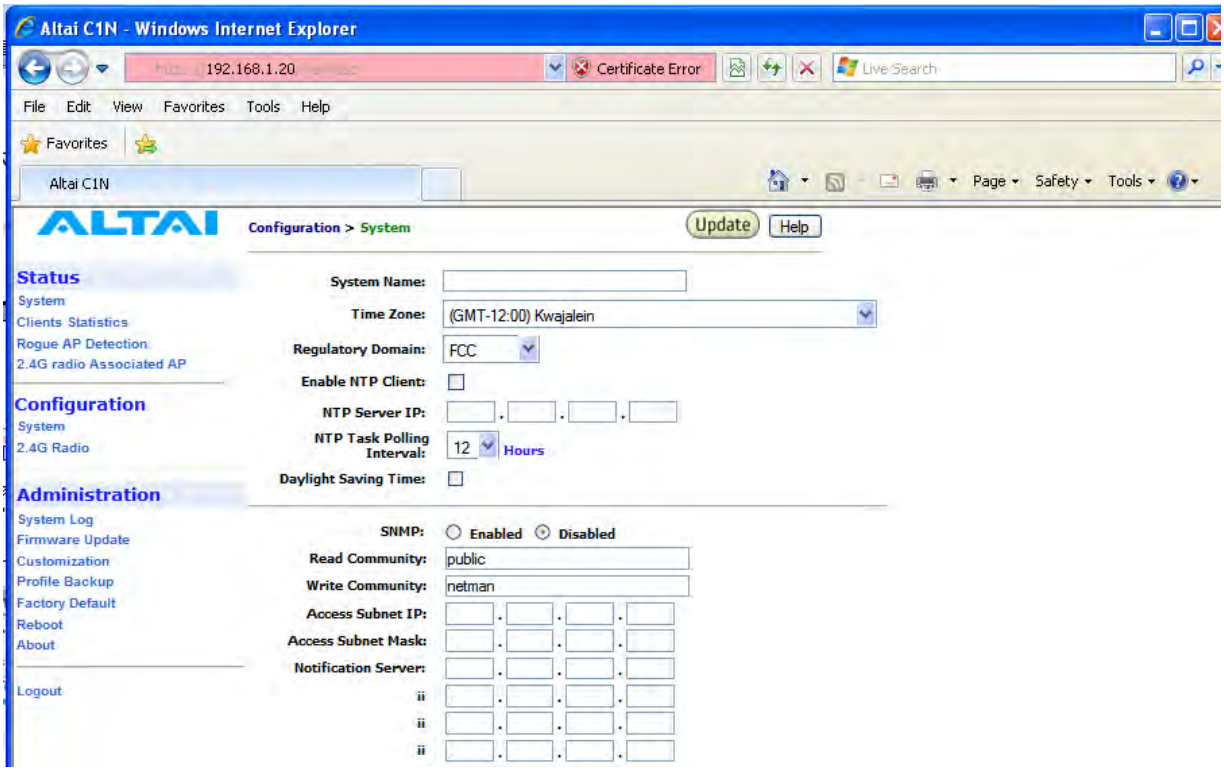


Figure 8 System Configuration

The ***User Name*** and ***Password*** for login are mentioned in Section 4.1, but only password can be changed by entering a new string in the field of ***Password***. Note: it is need to **re-enter to confirm** the password. Please press ***Change Password*** button to store the new password.

The ***System Name*** is the name of the C1n Super WiFi CPE/AP.

NOTE: Click the ***Update*** icon to store the changed settings.

4.4 NTP CONFIGURATION

NTP is a network time protocol for the AP to synchronize the system time. There is no NTP server IP address by default. If NTP is needed, IP address of the NTP server must be added and C1n will synchronize with the NTP server. This measure is useful to maintain the network and make sure all APs using the same system time by setting the same NTP server.

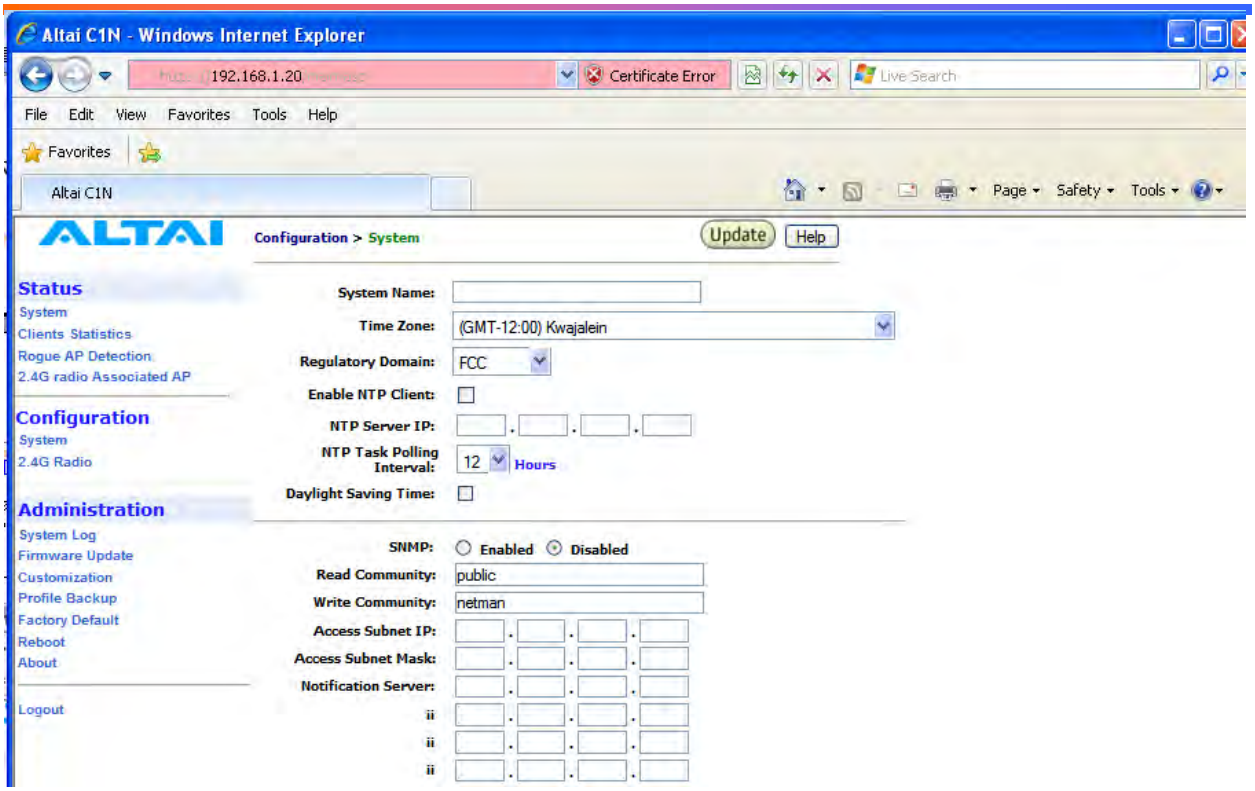


Figure 9 NTP Configuration

NOTE: Click the ***Update*** icon to store the changed settings.

4.5 SNMP CONFIGURATION

In the SNMP Manager, the administrator can change the **Read Community** and **Write Community**. **Access Subnet IP** and **Access Subnet Mask** can be configured to specify the C1n's SNMP Manger. **Notification Server** IP addresses can be added for SNMP control. They are parameters used for SNMP control between Altai C1n and AWMS system.

By enabling SNMP Manager ACL mode, the C1n will only be managed by the AWMS which IP is located in the ACL list with correct Read Community, Write Community and SNMP IP address.

It also supports SNMP Manager Access Control List which allows user to configure a list of allowed SNMP manager IPs for managing the C1n. When the SNMP manger ACL mode is enabled, only SNMP request generated from the any of configured SNMP manger on the ACL will be handled.

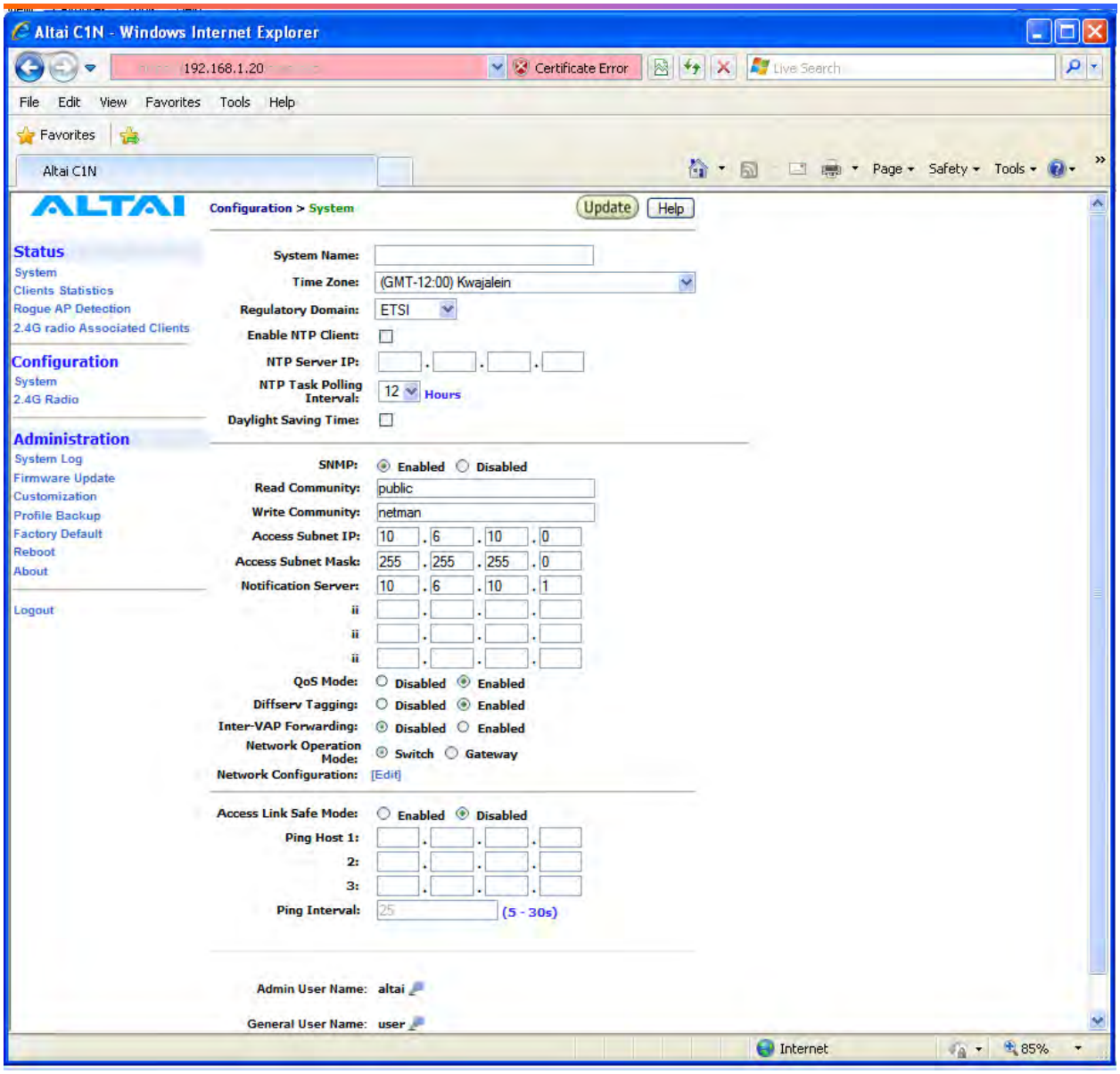


Figure 10 SNMP Configuration

NOTE: Click the ***Update*** icon to store the changed settings.

4.6 TELNET

Administrator can login to the C1n Super WiFi CPE/AP by telnet command in Command Prompt via Ethernet or WiFi. For example, to telnet C1n with IP address of 192.168.1.20; telnet command is "***telnet 192.168.1.20 2223***".

NOTE: The telnet port number is limited at ***2223***.

4.7 NETWORK OPERATION MODE

The default setting for the Network Operation Mode is ***Switch Mode***. If the C1n Super WiFi CPE/AP is set to ***Switch Mode***, it acts as a switch and routes traffic between the DS and wireless clients accordingly. When it is in ***Gateway*** mode, it acts as a gateway and the ***Local IP Address***

and ***Local IP Address Mask*** information must be entered to specify the C1n local interface for serving the wireless client.

In ***Switch*** mode, VLAN mode is by default disabled and clients in different SSID under the same C1n can communicate with each other. However, if VLAN is enabled, each SSID can be edited with a specific VLAN tag value. Only clients with same VLAN tag in same or different SSID can communicate. Moreover, in this mode, DHCPS, NAT and PPPoE configuration have no effort.

However, in ***Gateway*** mode, the DHCPS, NAT and PPPoE configurations can be configured but the VLAN has no effort.

In ***Switch*** mode,

- VLAN can be configured
- DHCPS, NAT and PPPoE are disabled

In ***Gateway*** mode

- VLAN is disabled
- DHCPS, NAT and PPPoE can be configured

4.8 SWITCH MODE

4.8.1 Static IP address

In *IP Assignation***, there are two kinds of working mode for C1n CPE/AP:** *Static IP address* **and** *DHCP Client*. By default, C1n CPE/AP is set to ***DHCP Client*** under ***switch*** mode. In ***Switch*** mode, by clicking ***Network Configuration*** in the System page, users can configure the ***IP Address***, ***Subnet Mask*** and ***Gateway Address***, as shown in Figure 11 , Figure 12 and Figure 12.

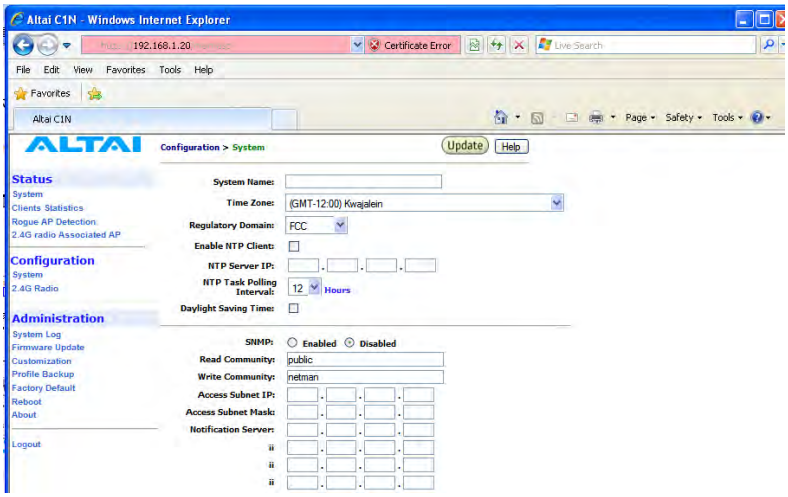


Figure 11 The IP address here is the Ethernet interface of the C1n

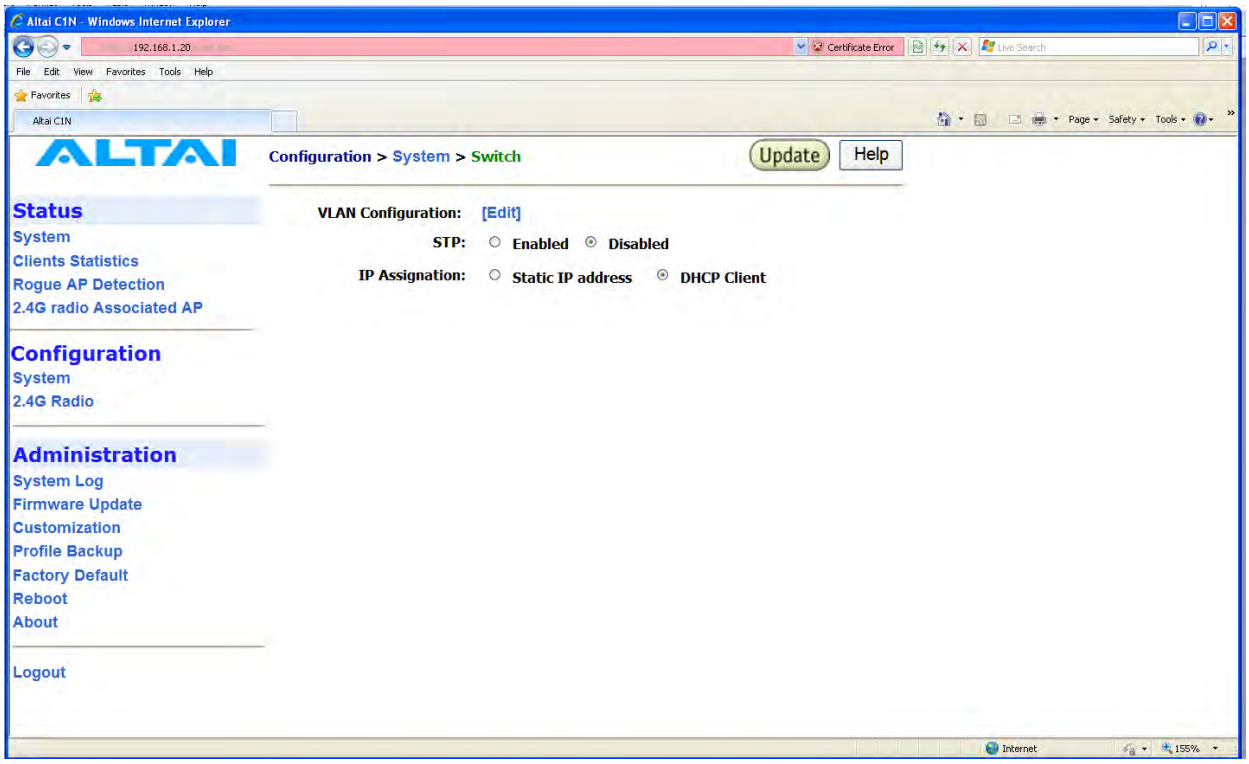


Figure 12 DHCP client under Switch mode

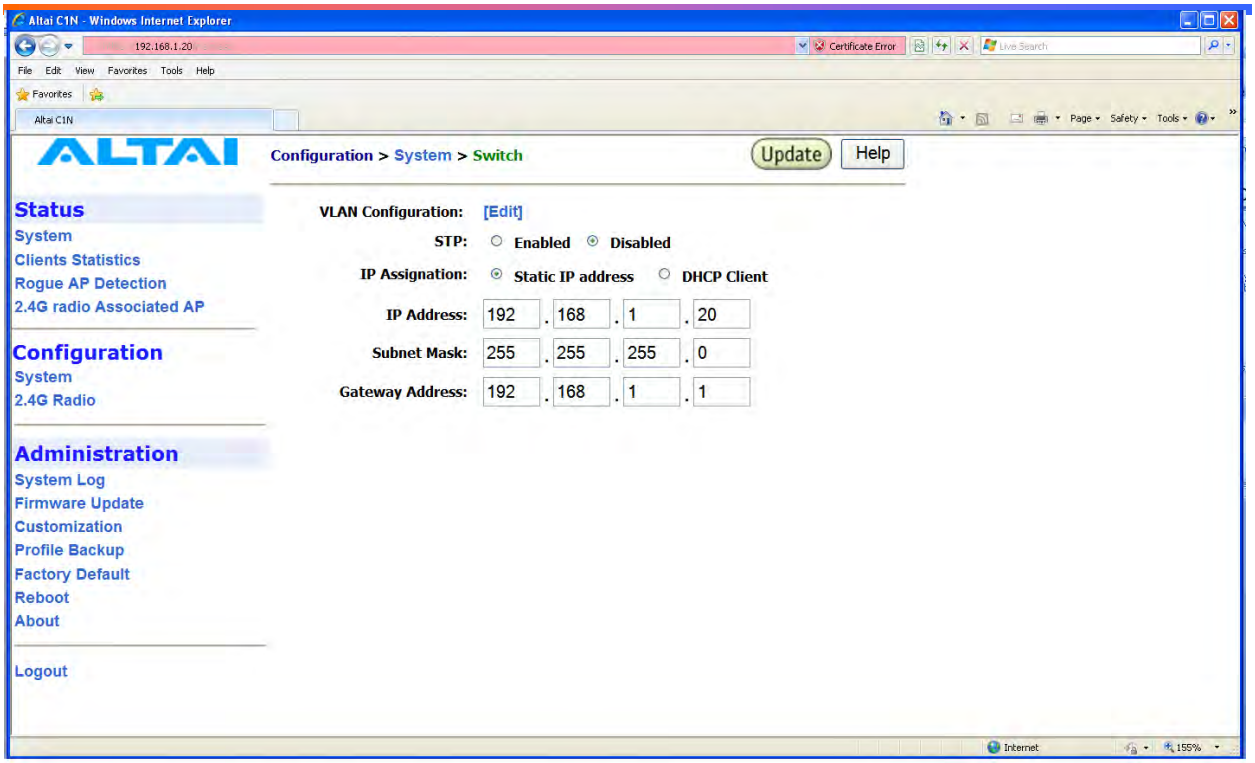


Figure 13 Static IP under switch mode

4.8.2 VLAN Configuration

Default setting of ***VLAN*** is "***Disabled***". By clicking "***Enabled***", VLAN can be enabled. C1n supports VLAN to VAP mappings to provide network security.

Management VLAN is used to configure the management VLAN of C1n. C1n can only be accessed through the specified management VLAN when VLAN is enabled. It will be ignored when VLAN is disabled.

Native VLAN Tagging control is used to control the untagged packet when VLAN is enabled. All the packets without VLAN tags should be sent to the VLAN with Native VLAN Tag ID. The default setting of Native VLAN Tagging is "***Disabled***". Native VLAN Tagging can be enabled when VLAN is enabled.

NOTE: VLAN could only be modified when C1n works under ***AP mode***.

4.8.3 DHCP Client

By default, DHCP Client is ***enabled***; the C1n CPE/AP will acquire a dynamic IP address from a DHCP server.

Without enabling DHCP Client, the ***IP Address***, ***Subnet Mask*** and the ***Gateway Address*** should be configured by the user.

NOTE: By enabling DHCP client, IP address of C1n CPE/AP is hard to predict after rebooting the C1n. Administrator can use default IP address '192.168.1.20' to access the web-admin to maintain C1n.

4.8.4 Static IP address

By enabling **Static IP address** and clicking the icon ***Update***, the C1n CPE/AP will be fixed an IP address by administrator after rebooting.

The ***IP Address***, ***Subnet Mask*** and the ***Gateway Address*** should be configured by the user, **unless** the user prefers using the DHCP client setting.

4.8.5 DNS Auto Update

By setting DNS Auto Update to ***Enabled*** and clicking the icon ***Update***, the C1n Super WiFi CPE/AP will acquire a DNS Server IP address via the DHCP Server after **rebooting**. User need not to set a DNS Server IP Address manually.

Without enabling the C1n as a DHCP Client, the ***DNS IP Address*** and ***DNS Domain Name*** should be configured by the user.

NOTE: DNS Auto Update can only be enabled when DHCP client is enabled. If the DNS Auto Update is enabled, it must be used in conjugation with either the DHCP Client or the PPPoE Mode being enabled. If both the DHCP Client and the PPPoE Mode are disabled then the DNS Auto Update must also be set to ***Disabled***.

4.9 GATEWAY MODE

In ***Gateway*** mode, by clicking ***Network Configuration*** in the System page, users can configure the WAN and LAN settings.

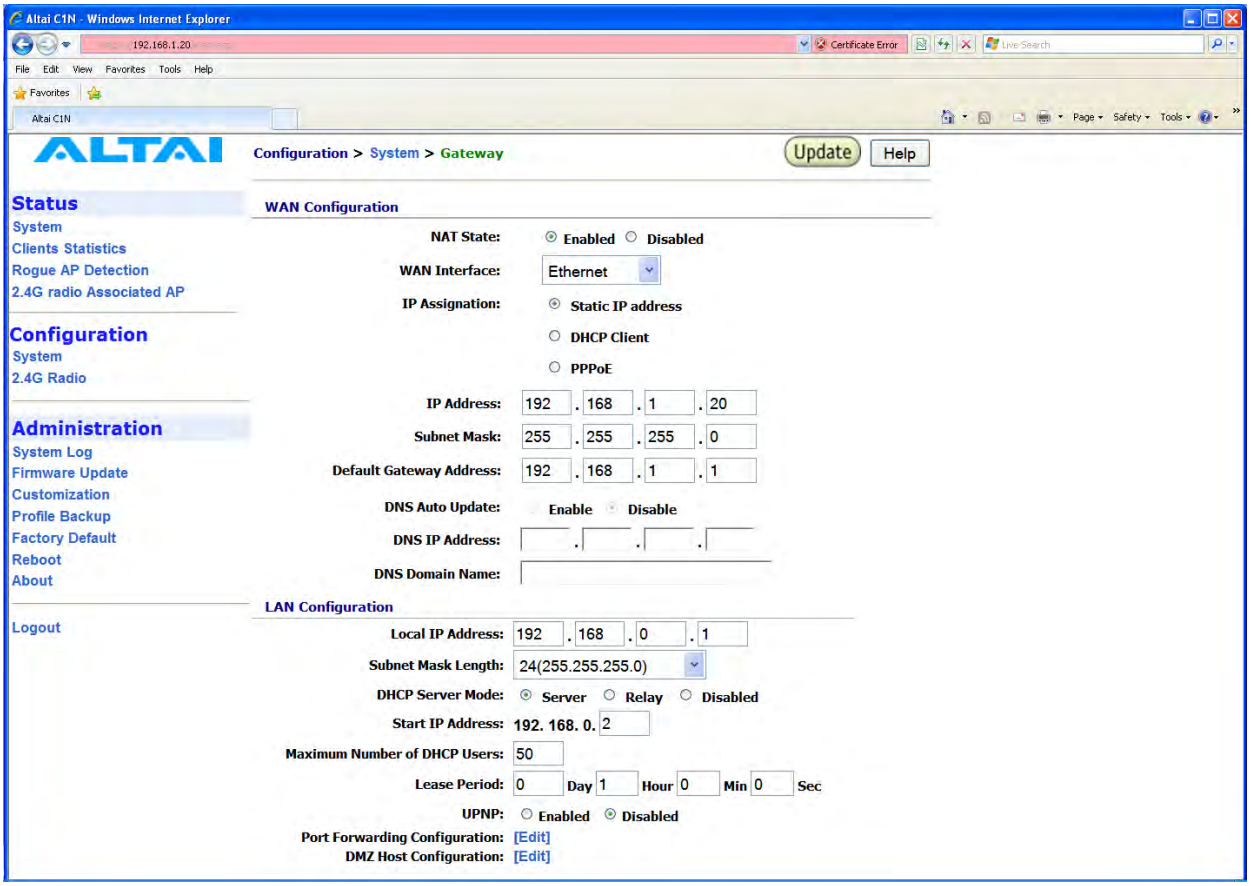


Figure 14 Network Configurations under Gateway mode

4.9.1 WAN Configuration

NAT is set to “Enabled” as default.

The settings for Static IP address and DHCP Client are similar to those in switch mode. Please refer to the previous section for details.

4.9.1.1 WAN Interface

Default setting is "Ethernet". This control is used to specify the WAN interface. The **Ethernet interface** or **5G bridge interfaces** can be used as the WAN interface when **VAP0** works on the **AP mode**. Use the pull down menu to select either one. The **2.4G Radio Client interface** is used as the WAN interface when **VAP0** works on the **Station mode**.

4.9.1.2 PPPoE Configuration

If PPPoE is chosen, a PPPoE login will be attempted for the ***PPPoE Username***, ***PPPoE Password*** and ***PPPoE Service Name***, see Figure 15.

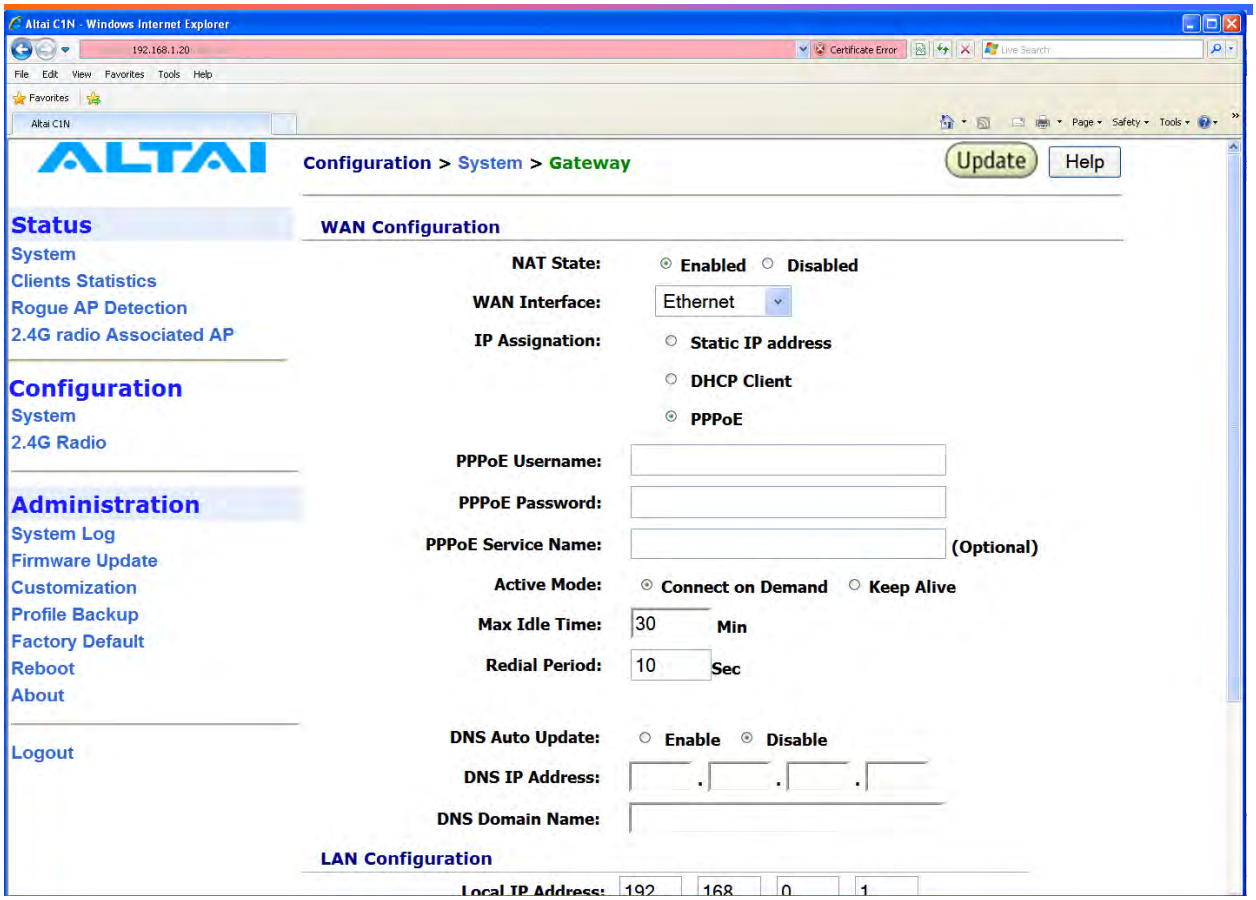


Figure 15 PPPoE Configuration

NOTE: The DNS Auto Update should be set to ***Disable*** when using PPPoE. User need to configure the DNS server IP address manually.

PPPoE ***Active Mode***, ***Max Idle Time*** and ***Redial Period*** can be configured.

When "***Connect on Demand***" is selected, PPPoE will establish the connection with the remote access concentrator only when hosts in the local subnet need to access the internet. If the parameter is set "***Keep Alive***", PPPoE will establish the connection with the remote access concentrator upon boot-up.

Default setting of ***Max Idle Time*** is ***30*** minutes. Only when PPPoE works under **Connect on Demand** mode, it will be disconnected if PPPoE connection has been idle for the Max Idle Time.

When last attempt failed, C1n CPE/AP will attempt to establish the PPPoE connection at ***Redial Period***.

4.9.2 LAN Configuration

In ***Gateway*** Mode, the C1n can be a DHCP server, a DHCP relay or none of them.

When the DHCP Server Mode sets to ***Server***, the C1n will act as a DHCP server and use the settings specified in the field ***Start IP Address***, ***Maximum Number of DHCP Users*** and ***DNS*** to serve the wireless clients.

1. Configure the ***Local IP Address*** and ***Subnet Mask Length***. Local IP Address is the gateway IP address for the client who associates C1n CPE/AP. Only the clients under the same subnet of local IP address can get IP address from C1n Super WiFi CPE/AP.
2. Configure the ***Start IP Address, Maximum Number of DHCP Users***, and ***DNS,*** see Figure 16.
3. Reboot the C1n

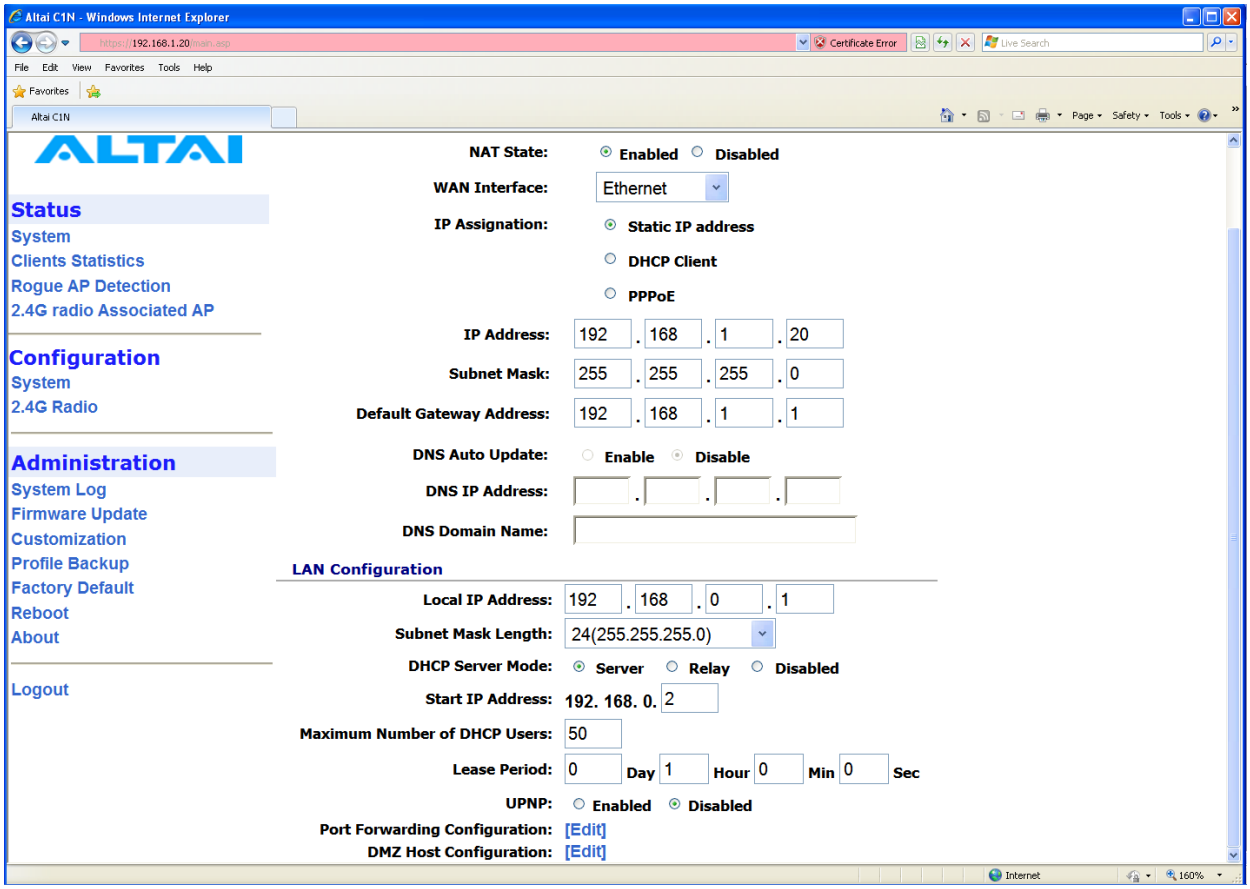


Figure 16 Configure DHCP Server

When the DHCP Server Mode sets to ***Relay***, the C1n will redirect all DHCP requests from the wireless clients to a backend DHCP server with IP address specified by the Relay Server IP Address.

1. Configure the ***Relay Server IP Address***, see Figure 17.
2. Reboot the C1n

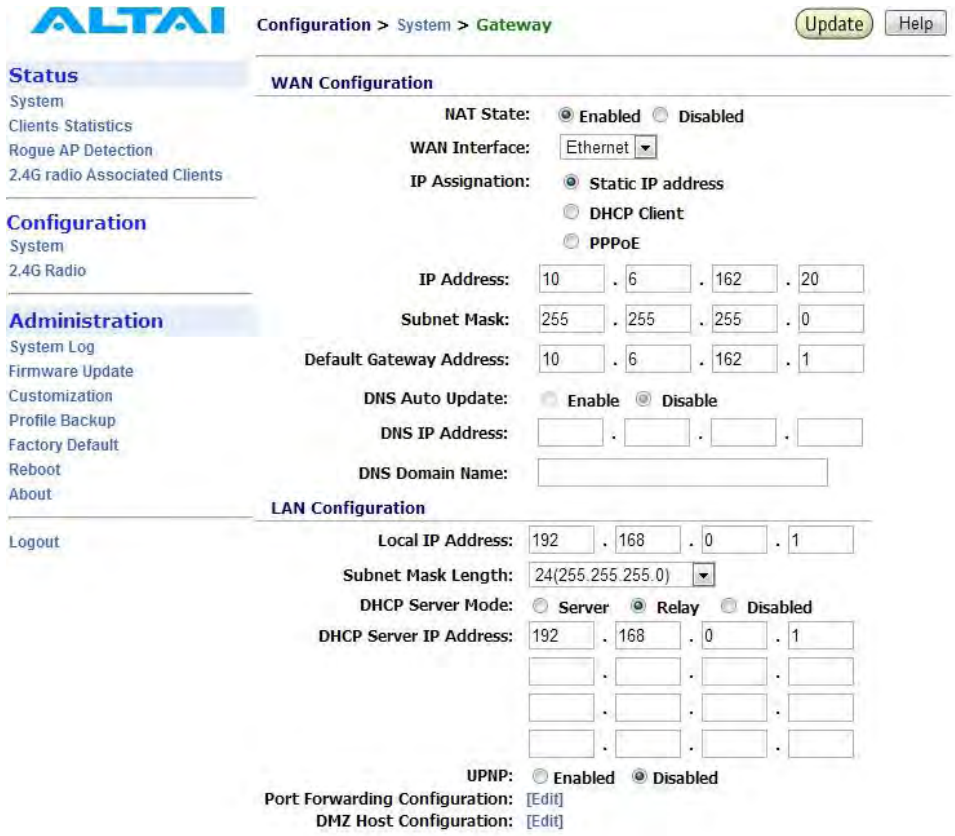


Figure 17 Configure DHCP Relay Server

When the DHCP Server Mode sets to ***Disabled***, the C1n will neither be a DHCP server nor a DHCP Relay and hence the wireless clients CANNOT get IP addresses from the C1n CPE/AP to access the Internet. Instead, each wireless client should set a fixed static IP address which is in the same network domain as the C1n.

4.9.3 Port Forwarding Configuration

In Gateway mode, the user can configure the Port Forwarding. Port Forwarding is the technique to forward a private port to public port. The external user can reach a port on a private IP address from the outside via C1n. This allows the remote computers to connect a specific computer with a private LAN.

1. Configure the ***Private IP, Private Port, Type and Public Port***, see Figure 18.
2. Choose ***Enable***
3. Reboot the C1n

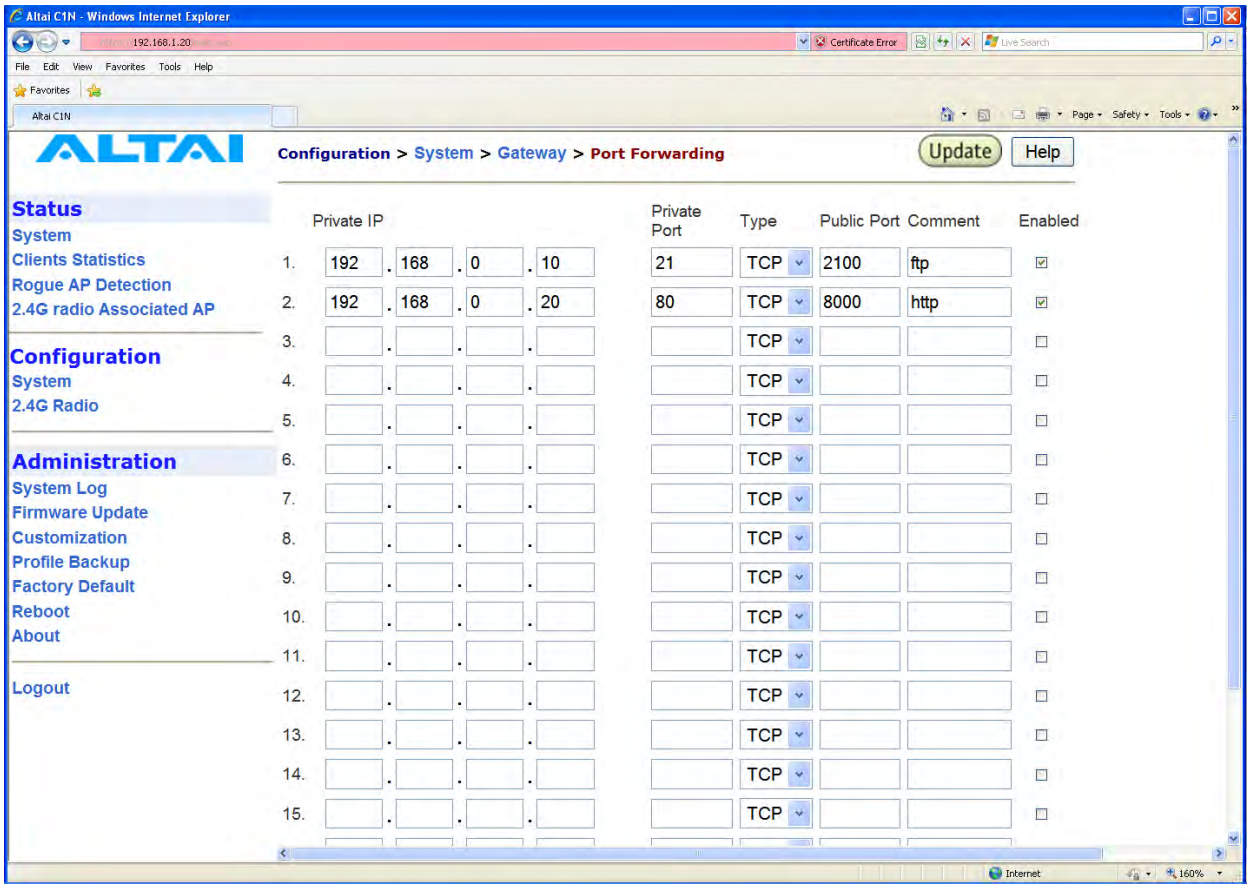


Figure 18 Configure Port Forwarding

4.9.4 DMZ Configuration

Demilitarized Zone is a physical or logical sub network that contains and exposes services to external network. By enable DMZ zone, external user can only access client with IP configured in DMZ IP. DMZ feature could be configured only under ***gateway*** mode and DMZ IP should be under ***LAN IP subnet***.

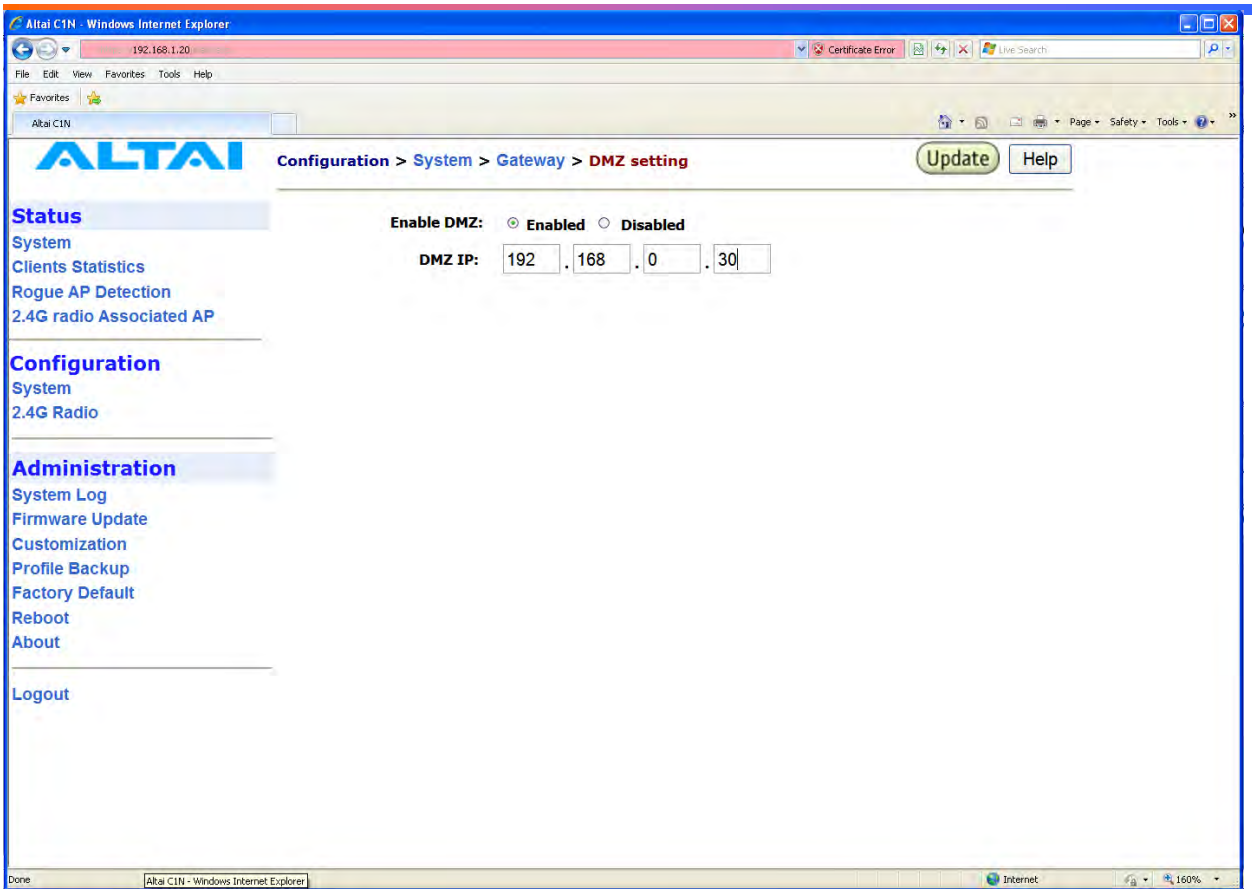


Figure 19 DMZ Configuration

4.10 ACCESS LINK SAFE MODE/ BACKHAUL LINK SELF-HEALING

Access Link 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 "C1n Safe Mode XXX", where "XXX" is the MAC address of the 2.4GHz radio in hexadecimal. This action can protect the client from connecting to a AP which has no backhaul to the Internet end. Default Access Link Safe Mode is ***Disabled***. Press the icon ***Enabled***, C1n CPE will work under Access Link Safe Mode.

In the case where **multiple physical backhauls** are available, the ***Backhaul Link Self-Healing*** feature will switch to other backhaul if the current one goes down. For example, when default backhaul is set to 5GHz Radio, once the 5GHz Bridge link is broken down, C1n Super WiFi CPE/AP will try Ethernet end as its new backhaul. Default setting is ***Disabled***. After enabled the Backhaul Link Self-Healing, Default Backhaul Link can be configured.

Three **different *Ping Host*** can be added to the list **for monitoring the connectivity**. If either Access Link Safe Mode or Backhaul Link Self-Healing is enabled, the AP will ping those specified hosts periodically at the ***Ping Interval*** configured.

4.11 SETUP – 2.4GHZ RADIO PARAMETER

The ***Radio Operation Mode, 2.4GHz Radio***, ***Wireless Mode***, ***Auto Channel Selection, Radio Frequency*** (Channel), ***Transmit Power***, ***Channel Bandwidth, Advanced Settings*** and ***VAP*** can be configured by selecting **2.4GHz Radio** under **Configuration** in the menu bar, as shown in Figure 20.

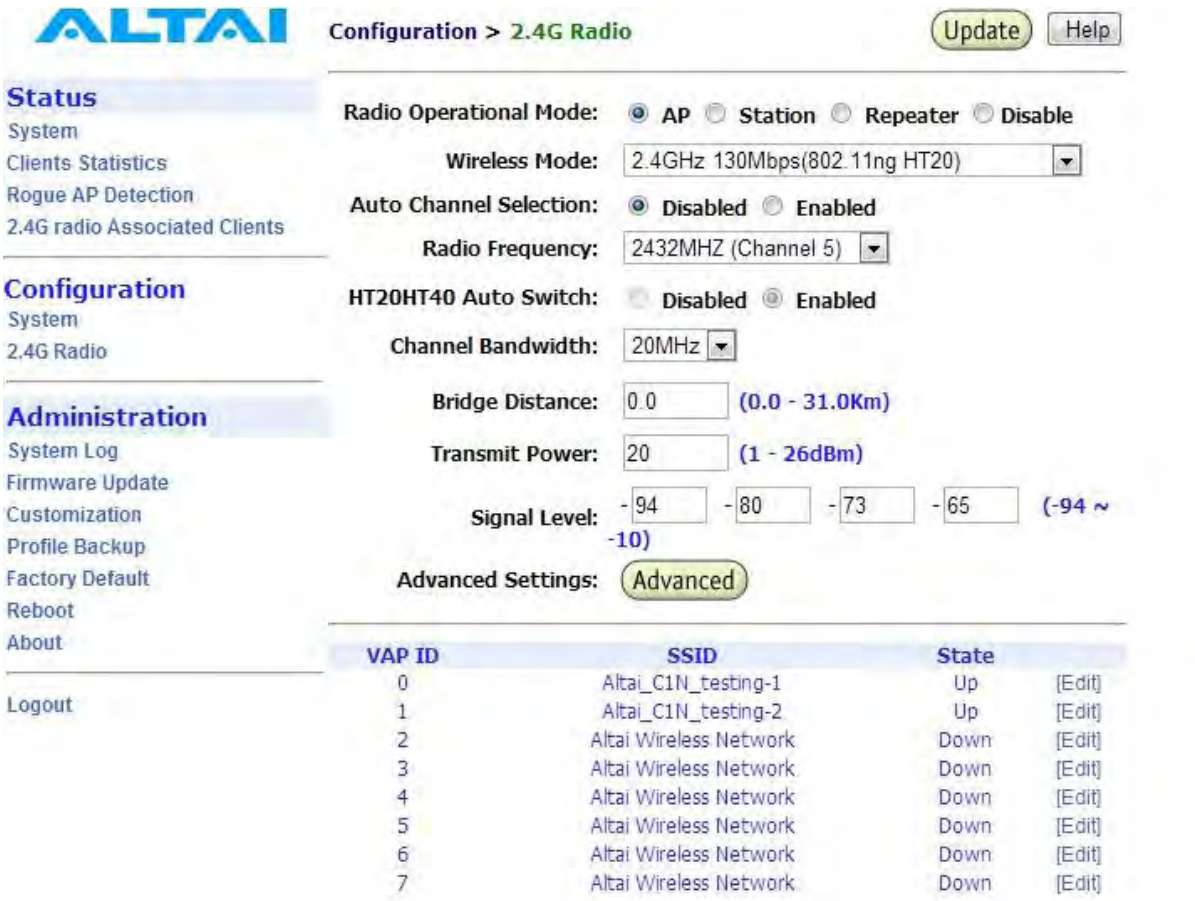


Figure 20 2.4GHz Radio Parameter Configuration

The 2.4GHz Radio can be enabled or disabled by selecting ***2.4GHz Radio***.

Under Station, C1n will follow the master AP channel. Under AP mode, the Auto Channel Selection is disabled by default; the C1n is fixed on Channel 6. When ***Enabled*** of Auto Channel Selection is chosen, C1n Super WiFi CPE/AP can scan all available radio channels which are assigned to the regulatory domain. The "cleanest" channel is then selected as the operating channel.

NOTE: After changing frequency channel, it takes around 3 minutes for C1n to optimize its 2.4GHz radio performance.

4.11.1 Service Set IDentifier (SSID) and Virtual Access Point (VAP)

In order for the C1n CPE/AP and mobile clients to communicate, they must all be configured to use the same SSID for communication both at the VAP and clients ends. SSID broadcast can be enabled or disabled by selecting ***Suppress SSID***. ***Suppress SSID*** is used to prevent unauthorized users scanning for SSID while still allowing users who know the correct SSID to connect.

NOTE: Suppress SSID can be enabled only when C1n works under ***AP mode***.

4.11.2 Wireless Mode and Radio Frequency

Altai C1n Super WiFi CPE/AP can offer 2.4GHz radio access, the following tables list the operation mode and available frequency under the particularly wireless mode. Default setting of AP mode radio is working on 2.4GHz 300Mbps (802.11ng HT40) and default channel is channel 3 (2422MHz).

2.4GHz Radio Mode	Data Rate	Channels	Radio Frequency
802.11b	11Mbps	1,2,3,4,5,6,7,8,9,10,11	2412MHz-2462MHz
802.11b/g	54Mbps	1,2,3,4,5,6,7,8,9,10,11	2412MHz-2462MHz
802.11ng HT20	130Mbps	1,2,3,4,5,6,7,8,9,10,11	2412MHz-2462MHz
802.11ng HT40	300Mbps	3,4,5,6,7,8,9	2422MHz-2452MHz

Table 2 2.4GHz Radio Frequency

4.11.3 Transmit Power

The value of the ***Transmit Power*** depends on both the gain of the 2.4GHz antenna and the maximum value of the Effective Isotropic Radiated Power (***Max EIRP***) allowed by the country in which C1n is used. The ***Transmit Power*** should be configured within the given range as shown in Figure 20

NOTE: Click the ***Update*** icon to store the changed settings.

4.11.4 Channel Bandwidth

There are two kinds of **Channel Bandwidth, 20MHz** and **10MHz.**

4.11.5 Bridge Distance

This feature is used to specify the **Bridge distance** value in ***kilometers*** using slider or enter the value manually. The value could be modified between **0** and **5**.Changing the distance value will change the ACK Timeout to the appropriate value of the distance in order to make C1n getting best performance at that distance.

4.11.6 LED signal

There are 6 LEDs at the back of C1n, the 4 LEDs in the right side are used for signal strength indication in CPE mode or AP mode. These 4 LEDs altogether can 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

Table 3 LED indicate method

The LED Signal indicator range could be configured from web page. The 4 signal level input should be in ascending order form left to right. The value range of these 4 signal level is -94~-10dBm. The default setting of LED signal threshold is -94, -80, -73 and -65. The 8 displayed signal levels are classified as:

Signal level	Signal range	SS1	SS2	SS3	SS4
1(Weakest)	-94 to -88	Blink	off	off	Off
2	-87 to -81	On	Off	Off	Off
3	-80 to -77	On	Blink	Off	Off
4	-76 to -73	On	On	Off	Off
5	-72 to -69	On	On	Blink	Off
6	-68 to -65	On	On	On	Off
7	-65 to -60	On	On	On	Blink
8	-60 to -55	On	On	On	On

Table 4 LED signal level

4.11.7 Advanced Radio Setting

More radio parameters can be verified and altered by selecting the ***Advanced*** icon in the field of ***Advanced Setting***. The parameters are shown in Figure 21.

Data Rate: Default setting is "best". When the "best" data rate is chosen, the C1n AP attempts to deliver unicast data frames at the highest possible "optimal" data rate that allows for reliable data transmission. If there are obstacles or interferences, the AP automatically steps down to a lower optimal data rate. Furthermore, the optimal data rate is adjusted periodically by the AP, based on past performance of the data transmissions at different data rates.

Fragment Threshold: It means the size of each frame. If it is set to 256 bytes and the size of data block is 1024 bytes, the data block will be divided to four frames to send.

RTS/CTS Threshold: RTS is a flow control mechanism to prevent collision between 802.11b and 802.11g mobile stations to send data to the access point in the same time. CTS is another flow control mechanism to prevent collision when two mobile stations, who do not know the existence of each other, send data to the access point in the same time. RTS and CTS are used for point-to-multipoint bridge application and they are enabled when the threshold set to 2346.

Beacon Interval: Default setting is 100 ms. The C1n AP transmits beacons for each supported BSS, with each BSS using the same beacon interval. The beacon interval is a value between 25 and 1000 ms. The following table showed is the best suggested interval worked with the current operated APs. Note that it is not suggested to change the parameters in Advanced Radio Settings unless you are experienced administrators.

Number of active VAPs	Auto Beacon Interval (ms)
1	100
2	200
3	300
4	400

Table 5 Beacon Interval Table

DTIM: Default setting is 1. The DTIM interval, also known as the data beacon rate, denotes the frequency at which AP beacon will include a DTIM. This frequency is measured in the number of beacon intervals, and is a value between 1 and 255.

Multicast Rate: This option allows Multicast packets to be sent in higher rates (up to the 54 Mbps) than commonly used (1 Mbps at IEEE 802.11b mode, 6 Mbps at IEEE 802.11g/a mode). This is ALTAI's C1n proprietary feature thus it may be incompatible with the devices from other vendors. Both C1n based devices the sender (Station) and the receiver (Access Point) must have the same Multicast Rate configured in order to achieve better multicast packet throughput performance

Short Preamble: Default setting is "Enabled". Short preamble usage is only available for 802.11b. If this option is set to "Enabled", both short and long preamble are used. Only long preambles are used when Short Preamble is set to ‘Disabled’.

Protection Mode: Default setting is "None". C1n turns off CTS protection under protection mode disabled. C1n will turns on CTS protection when Protection Mode is set to ‘always’. If Protection Mode is set to "Auto", the C1n dynamically turns on and off CTS protection depending on whether there are any 802.11b STAs associated/any traffic from associated 802.11b STAs.

Short Slot Time: Default setting is "disable". In 802.11g mode, if this feature is enabled, the C1n advertises and uses 9 us slot times until the first client associates that cannot support 9 us. Then, C1n advertises and uses 20 us slot times until all the stations that cannot support 9 us have timed out. If it is disabled, the C1n only uses long slot times. In 802.11b mode only long slot times are used.

QoS: Default setting is "Enabled". If QoS Mode is set to "Disabled", all traffic has equal priority and equal chance of being delivered in a timely manner. When congestion occurs, all traffic has an equal chance of being dropped. If QoS Mode is set to "Enabled", the QoS implementation is based on WMM, which is a subset of the 802.11e draft. It prioritizes traffic between the AP/Bridge and wireless client device/peer bridge device, on a per VAP basis. This control enables QoS for 2.4GHz radios.

Figure 21 Advanced 2.4GHz Radio Setting

4.11.8 Bandwidth Control

Under 2.4GHz Radio ***Advance*** setting, administer can enable '***Traffic shaping***'. This feature provides radio level bandwidth control in both UL & DL. This feature is disabled by default. By enable 'Traffic Shaping', user can define value of Incoming Traffic Limit, Incoming Traffic Burst, Outgoing Traffic Limit and Outgoing Traffic Burst.

Incoming Traffic Limit: Default value is 512Kbit/s. It can specify the maximum bandwidth value for traffic passing from wireless interface to Ethernet interface.

Incoming Traffic Burst: Default value is 0Kbytes. It can specify the data volume to which incoming Traffic Limit will not be effective afterwards data connection is initiated.

Outgoing Traffic Limit: Default value is 512Kbit/s. It can specify the maximum bandwidth value for traffic passing from Ethernet interface to wireless interface.

Outgoing Traffic Burst: Default value is 0Kbytes. It can specify the data volume to which outgoing Traffic Limit will not be effective afterwards data connection is initiated.

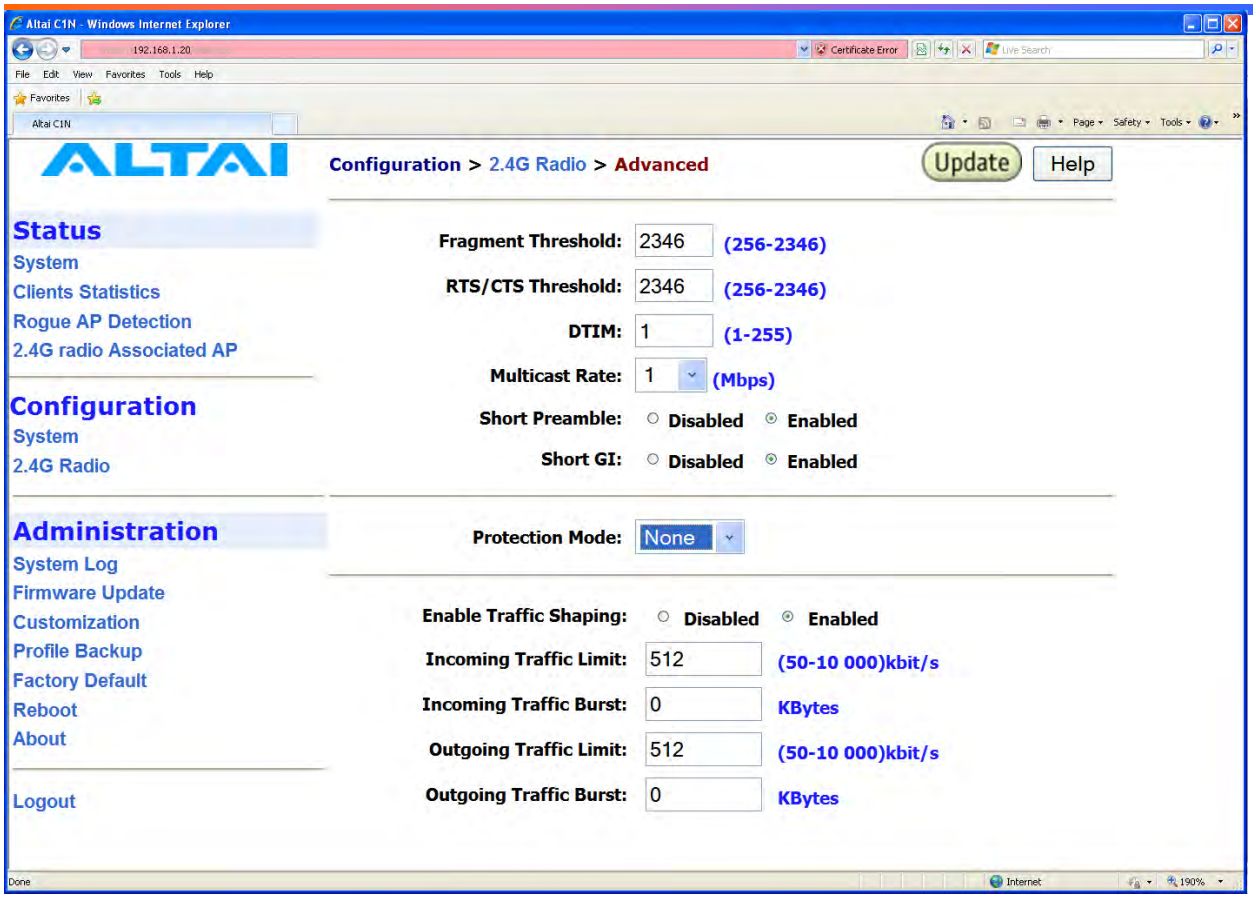


Figure 22 Bandwidth Control Configuration

4.11.9 Station Mode

Under VAP web-site interface, **AP** mode and **Station** mode can be chosen. By default, C1n is set to ***Station***, and backhaul link can be established through associating the Station VAP with the remote APs. That means Station VAP works as backhaul link, clients can connect with C1n by Ethernet end. The Security configuration should match to the remote SSID security type and pass phase.

There are three different station modes: **NAT mode**, **WDS mode** and **MAC address translation mode (MAT mode).**

When station works in **NAT mode**, C1n works in ***Gateway*** mode **and** the ***Station*** mode VAP is enabled. Repeater works in **WDS mode** when ***WDS*** is enabled **and** C1n works in ***Station*** mode. The **MAT mode** can be enabled when C1n runs in ***Switch*** mode and ***WDS*** is disabled.

Station Mode	System Mode	VAP0 working mode	WDS status
NAT mode	***Gateway*** mode	***Station*** mode	***Disabled***
WDS mode	***Switch*** mode	***Station*** mode	***Enabled***
MAT mode	***Switch*** mode	***Station*** mode	***Disabled***

Table 6 Repeater Mode Setting Method

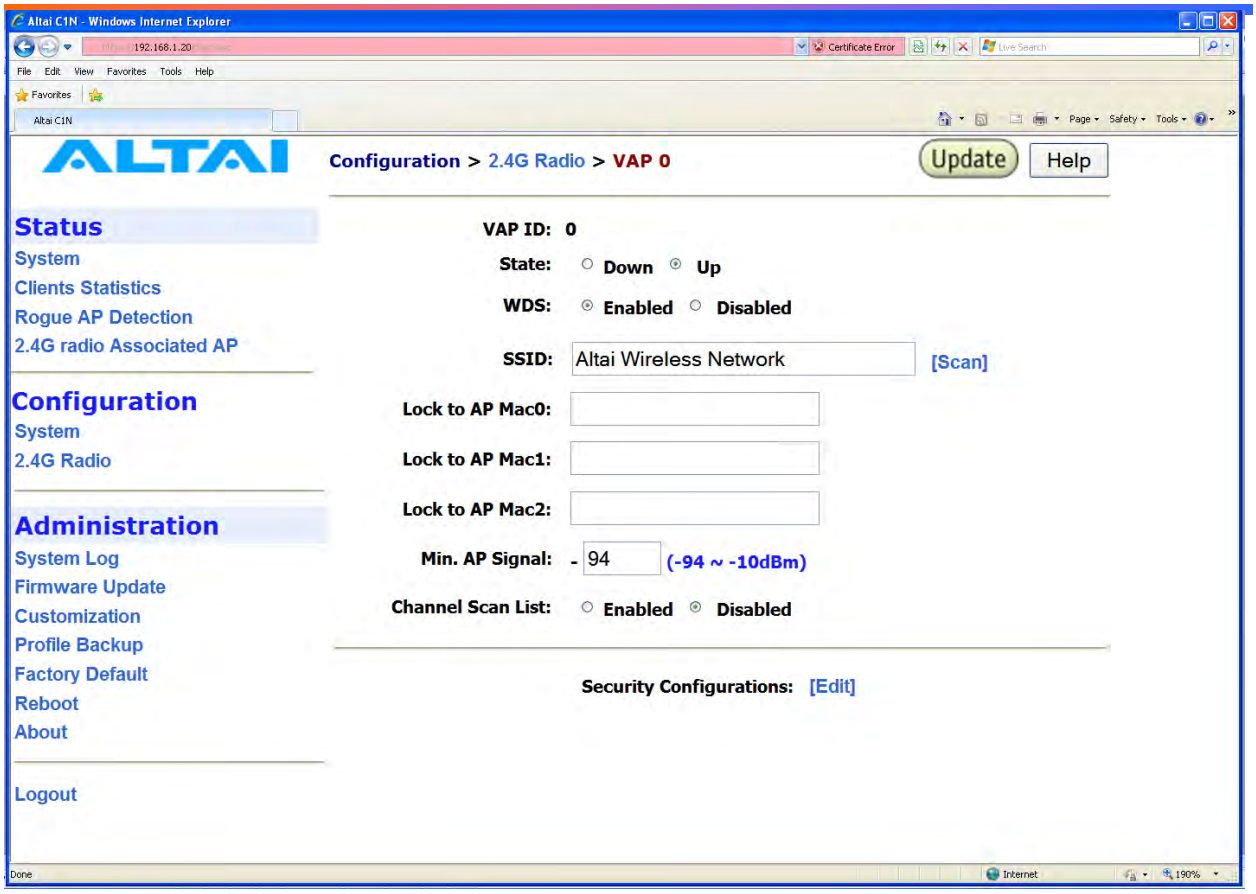


Figure 23 Station Mode Configuration

4.11.10 2.4G Radio Channel Scanning and Channel Scan List

Under Station Mode, C1n will automatically scans neighboring AP SSID by clicking ***Scan*** icon. Channel scanning result is list on the web-page, as shown in Figure 24 2.4G Radio Channel Scanning. The channel scan results includes: ***SSID***, ***MAC address***, ***Security***, ***Signal Strength*** and ***Channel***. Administrator can choose the appropriate SSID as C1n station mode wireless backhaul.

User can select one of choices on the list for C1n association. By enable '***Channel Scan List***', C1n will scan the surrounding AP working in the predefined channel list in '***Selecting Channel***' only.

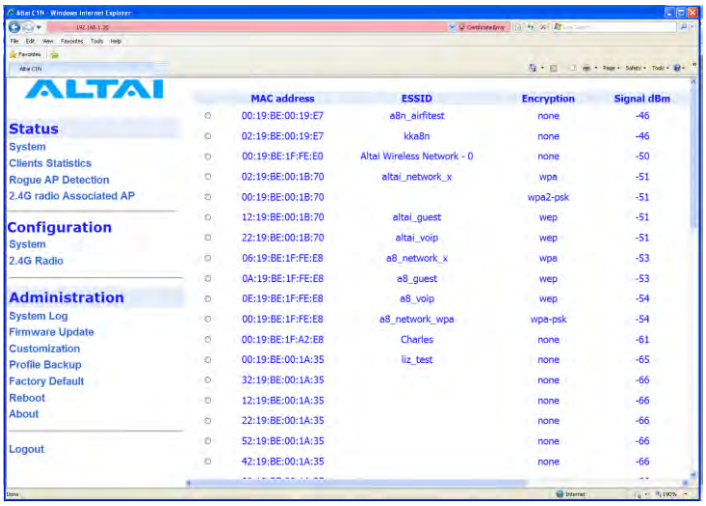


Figure 24 2.4G Radio Channel Scanning

4.11.11 Lock to AP MAC and Min. AP Signal

The "***Lock to AP Mac***" function is used to allow the CPE to maintain connection to a particular AP with a specific MAC under ***Station*** mode. With AP lock on, the CPE will lock to the defined MAC address and no roam between several Access Points with the same SSID. The MAC address will be automatically filled in when user chooses the preferred SSID from scanning list.

Min AP signal can be configured under station mode VAP. C1n measure the signal strength of remote SSID. Station mode VAP can only associate to remote SSID with higher signal strength than min AP signal threshold. Default Min.ap signal Strength value is "-94". The value can be set from **-94** to **-10**.

The MAC address of the preferred AP can be inputted, if the AP is found and the signal strength is higher than the min.ap signal strength, the C1n will connect to the AP. If the C1n received signal is lower than the min.ap signal strength and does not have the Lock MAC address set, it will connect to another AP with same broadcast SSID.

4.11.12 AP Mode

By clicking ***AP***, user can switch C1n from Station mode to AP mode. When C1n works under AP mode, C1n is as an access point. Clients can associate to C1n with wired backhaul. Under AP mode there are 4 VAP, each of the VAPs can be set to different SSID, security and encryption.

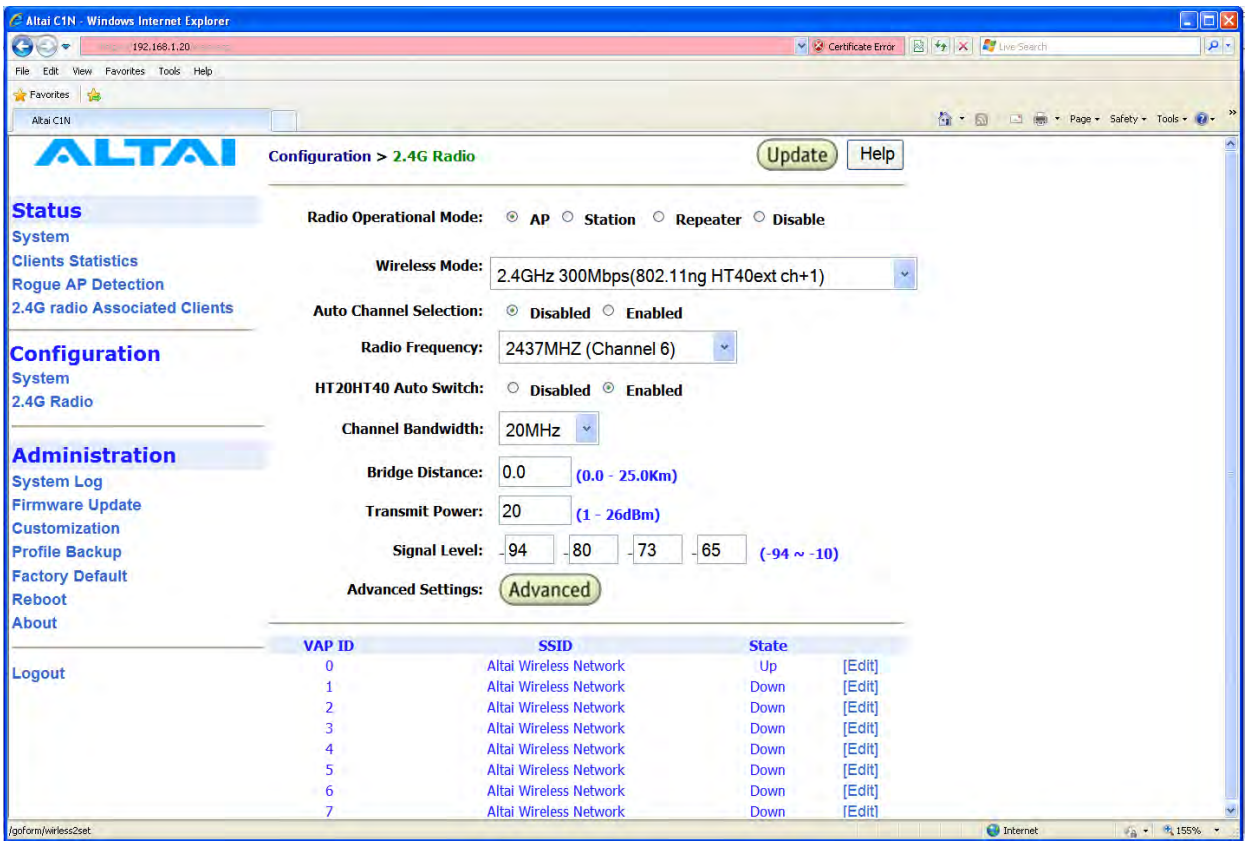


Figure 25 AP mode Setting

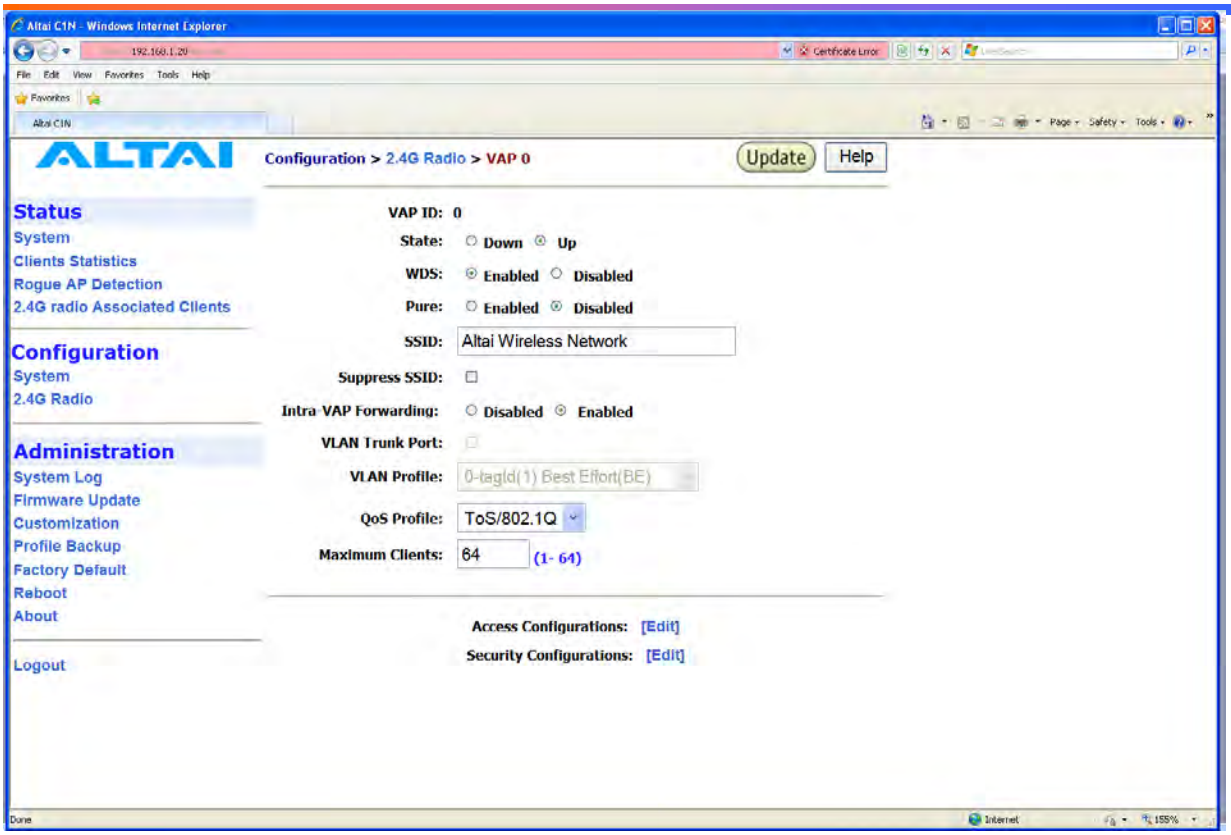


Figure 26 AP mode VAP Setting

4.11.13 VLAN Tag

VLAN can be enabled by adding different ***VLAN Tag*** ID. The traffic will pass through the specific VLAN switch port when VLAN is enabled.

Each VAP setting (including SSID) can be altered by selecting ***Edit***. The setting of each VAP is shown in **Error! Reference source not found.**. The ***default SSID*** for each ***VAP ID*** is ***Altai Wireless Network***. ***VLAN Tag*** can also be set here.

NOTE: **VLAN Tag** can be enabled only when C1n works under ***AP mode***.

4.11.14 Access Control List (ACL)

By selecting ***Access Configurations,*** a window, as shown in Figure 27 ACL, is brought up for choosing the ACL mode, adding ***MAC Address*** with ***ACL Type*** (***Allow*** or ***Deny***).

There are three modes in the Access Control List (ACL). They are ***Disabled***, ***Enabled-Allow*** and ***Strict-Deny***:

1. ***Disabled***
   - The function of ACL is **disabled**.
2. ***Enabled–Allow***
   - The function of ACL is **enabled**.
   - The MAC addresses which are specified in the ACL will consider as Allow.
   - i.e. **No** 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 ***Allow***.
3. ***Enabled–Deny***
   - The function of ACL is **enabled**.
   - The MAC addresses which are specified in the ACL will consider as Deny.
   - i.e. **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***.

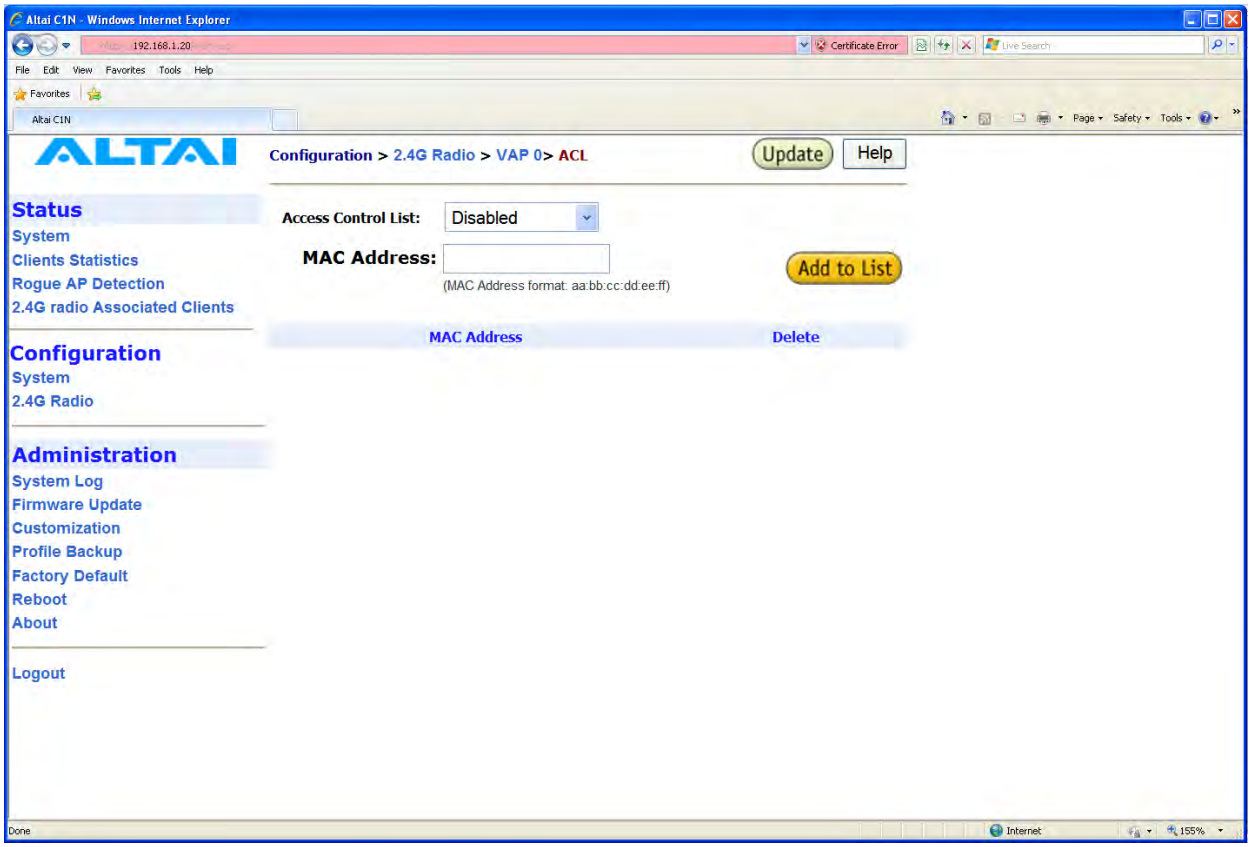


Figure 27 ACL

4.11.15 Encryption and Authentication

By selecting ***Security Configurations,*** a window, as shown in Figure 28, is brought up for choosing the ***Authentication Mode*** and ***Cipher Mode***.

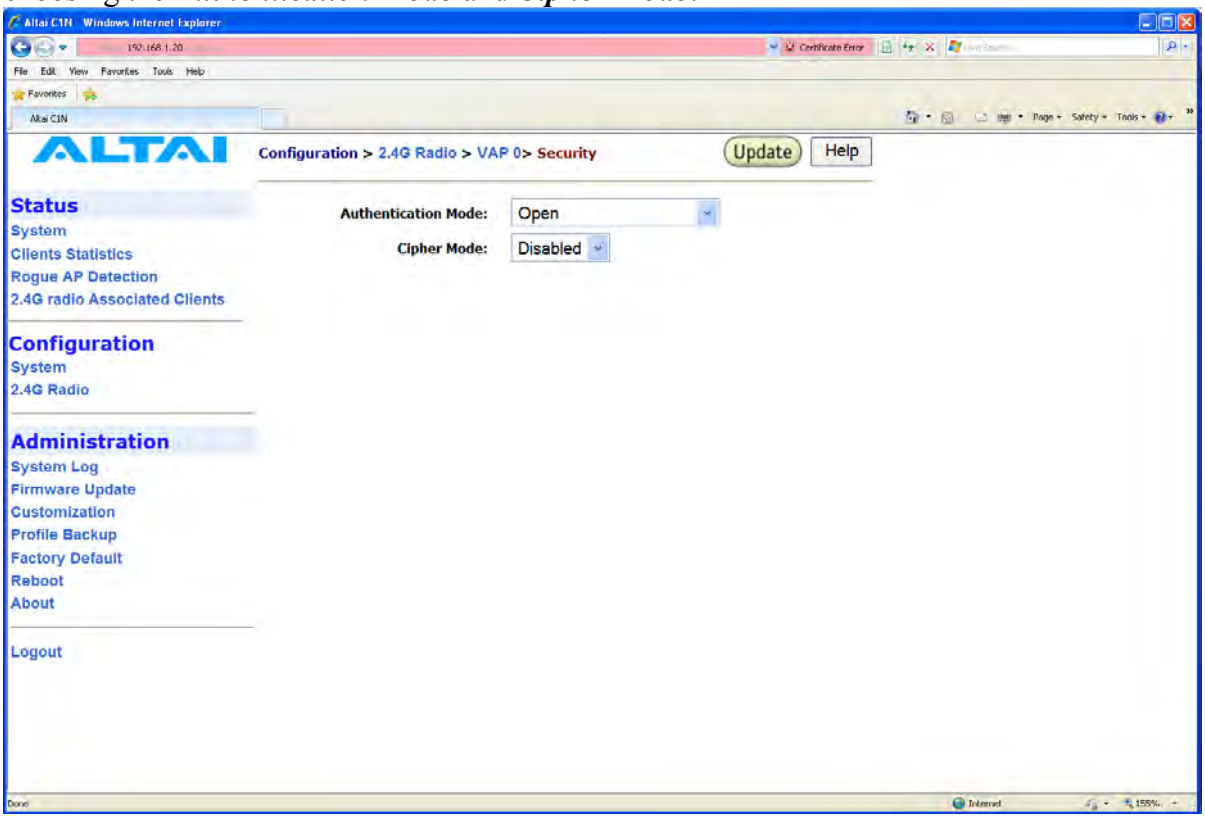


Figure 28 2.4GHz Radio Security Configuration

After selecting ***Open*** or ***Shared-Key*** for Authentication Mode, ***WEP*** for Cipher Mode, the WEP key settings can be defined as shown in Figure 29.

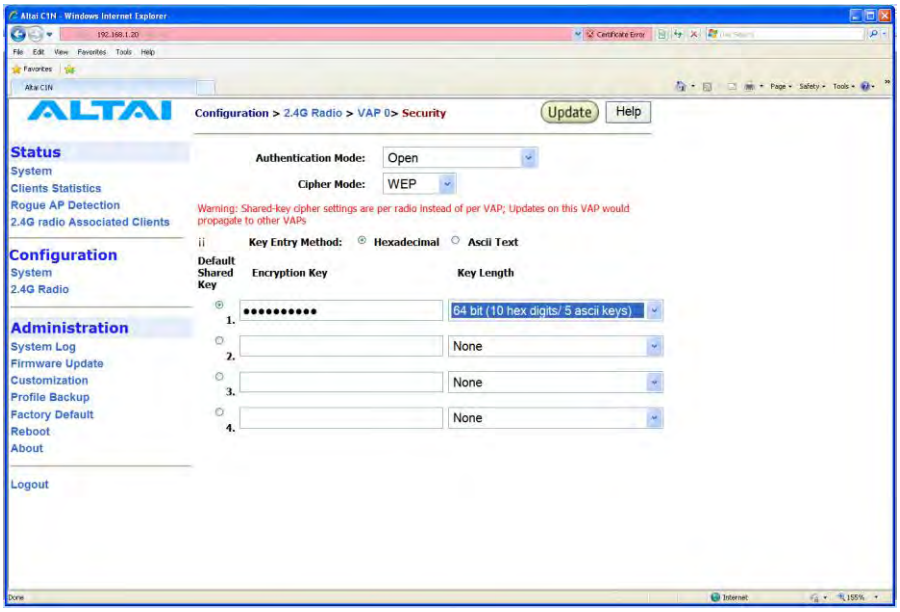


Figure 29 WEP Key Settings

WPA/WPA2 or WPA-PSK/WPA2-PSK can be enabled by selecting ***WPA/WPA2 or WPA-PSK/WPA2-PSK*** for Authentication Mode. The ***AES*** and ***TKIP*** are the two available options for Cipher Mode. The related settings are shown in Figure 28, Figure 32 and Figure 32 respectively.

NOTE: Click the ***Update*** icon to store the WEP or WPA settings.

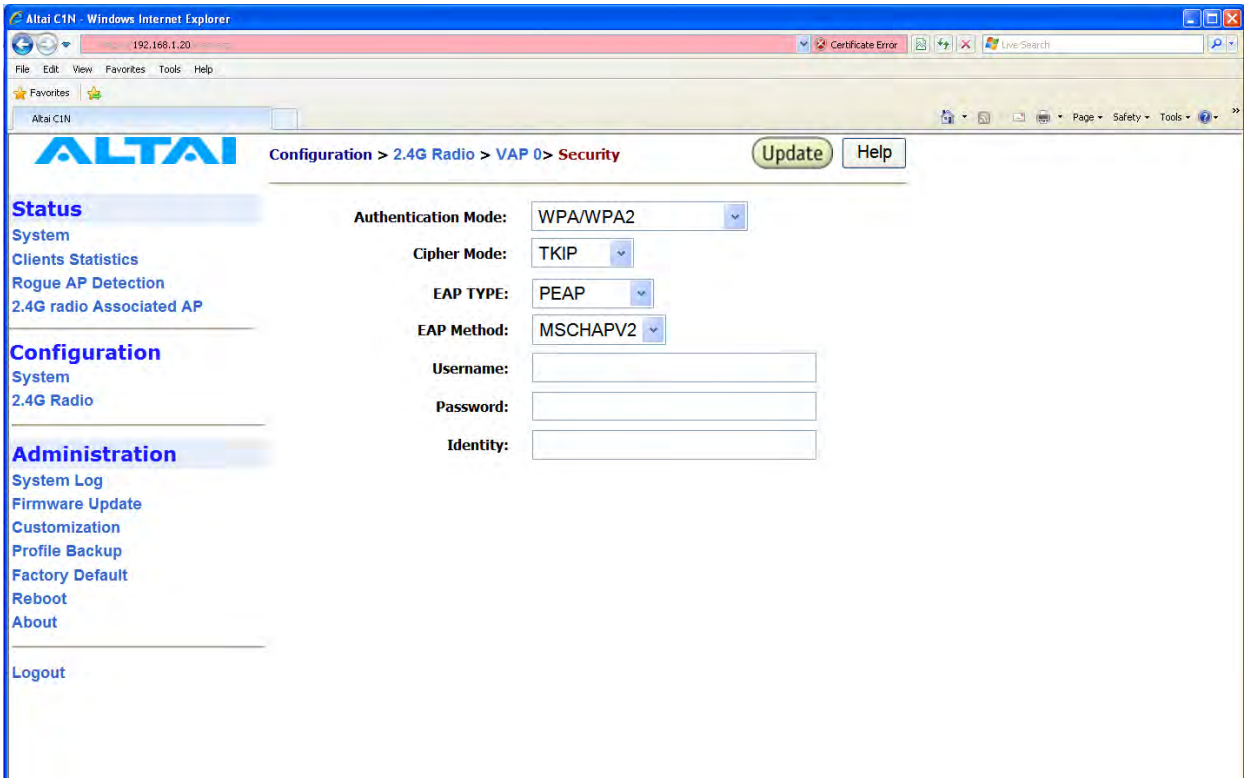


Figure 30 WPA-AES Settings

RADIUS server is used for authentication. C1n can store separate RADIUS server address for each VAP. It is only visible when the **Authentication** Mode is set to "***WPA***". The default setting of ***RADIUS server port*** is 1812. ***RADIUS secret*** shared password between the RADIUS server and C1n CPE/AP. A password up to 128 characters long can be added. The ***VLAN IP address*** and ***VLAN Subnet Mask*** configured on the VAP security web page will be used only when C1n runs in the following conditions.

1. C1n Super WiFi CPE/AP runs in **switch** mode and VLAN is **enabled**.
2. The VAP does **not** belong to **native VLAN**.
3. The authentication mode is **WPA**

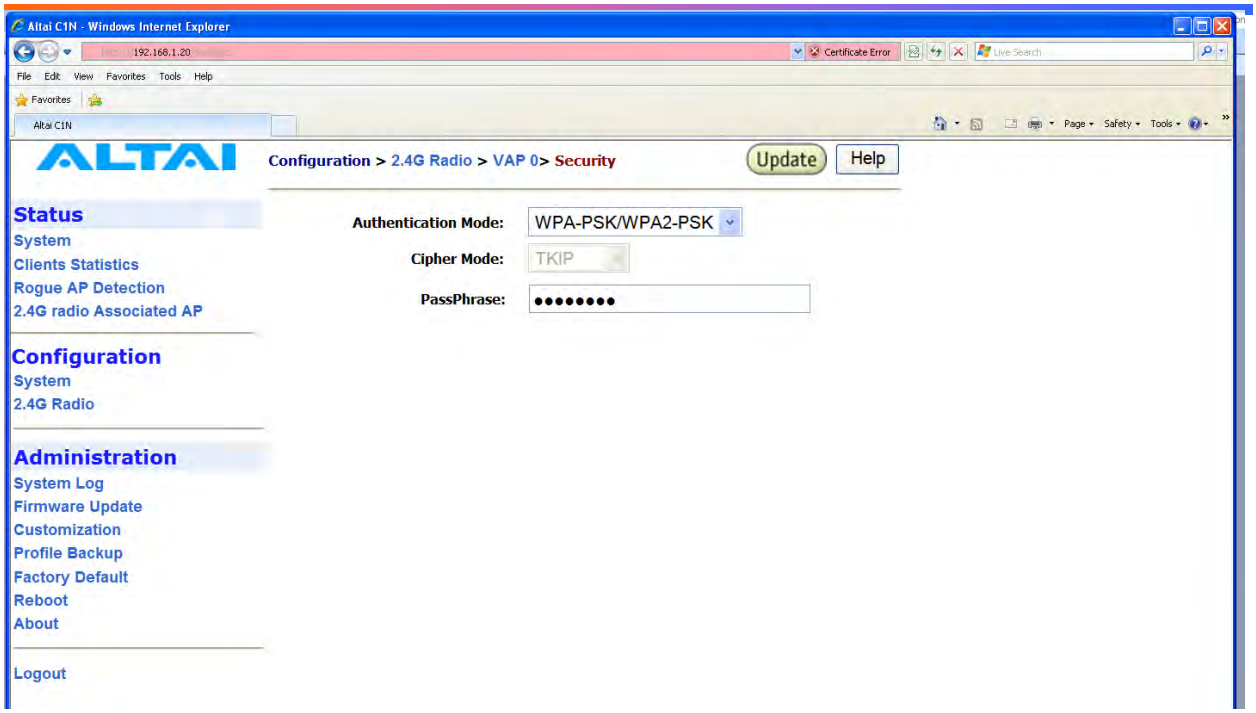


Figure 31 WPA-TKIP Settings

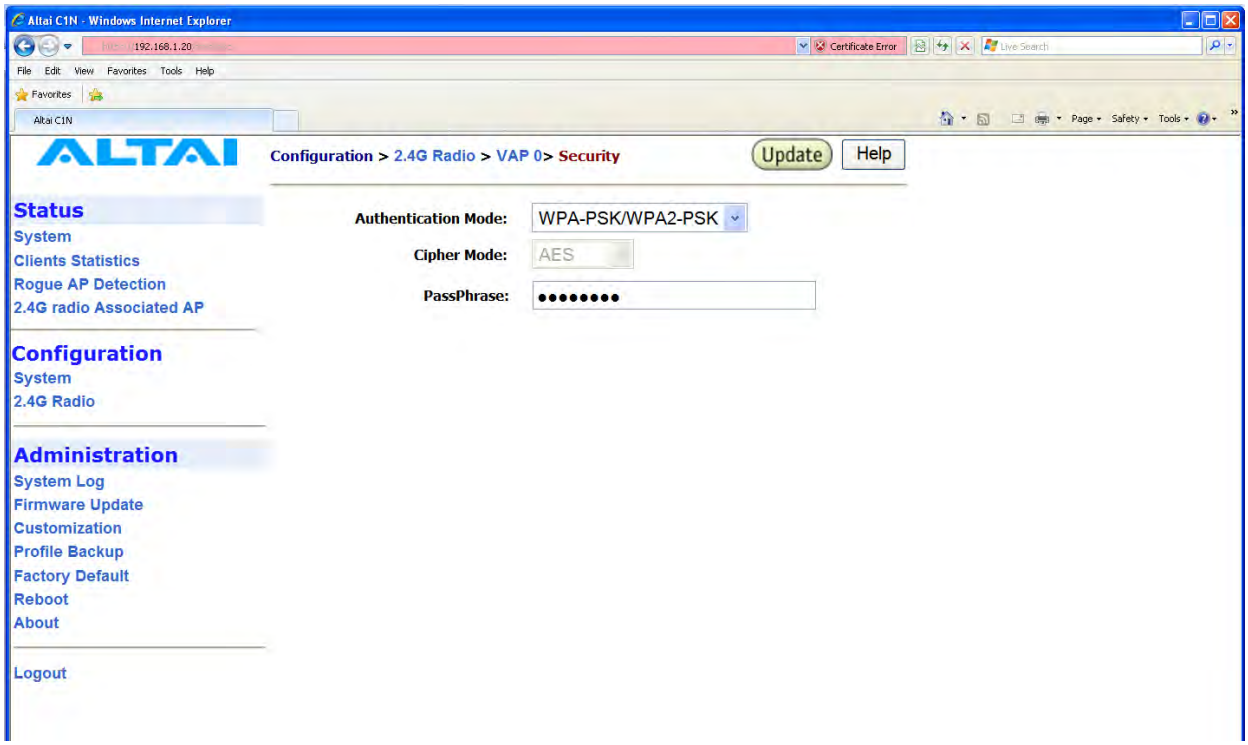


Figure 32 WPA-PSK Settings

4.12 SYSTEM LOG

C1n Super WiFi CPE/AP supports event logs for diagnostic purpose. The System Log can be chosen under the System Log in the menu bar. Administrator can classify system log by configuring digit of ***Kernel Log Level***. The following from lists Kernel log level which is presented by digits.

Digit	*Kernel Log Level*
0	KERNER_EMERG
1	KERNER_ALERT
2	KERNER_CRIT
3	KERNER_ERR
4	KERNER_WARNING
5	KERNER_NOTICE
6	KERNER_INFO
7	KERNER_DEBUG

Table 7 Kernel Log Level

System Log allows C1n sending system log messages into a System Log server instantaneously to the IP address of the System Log Server. Administrator could choose either Local System Log Server or Remote System Log Server. When ***System Log To Local*** is enabled, the system message is send to Local System Log Server and listed on the Web-Admin Interface. Click the **Browser** button will load the system messages stored in the AP buffer. By typing remote System Log server IP address in System Log to Remote IP field, C1n will send System messages to remote server.

NOTE: All event logs will be lost after A8 is rebooted.

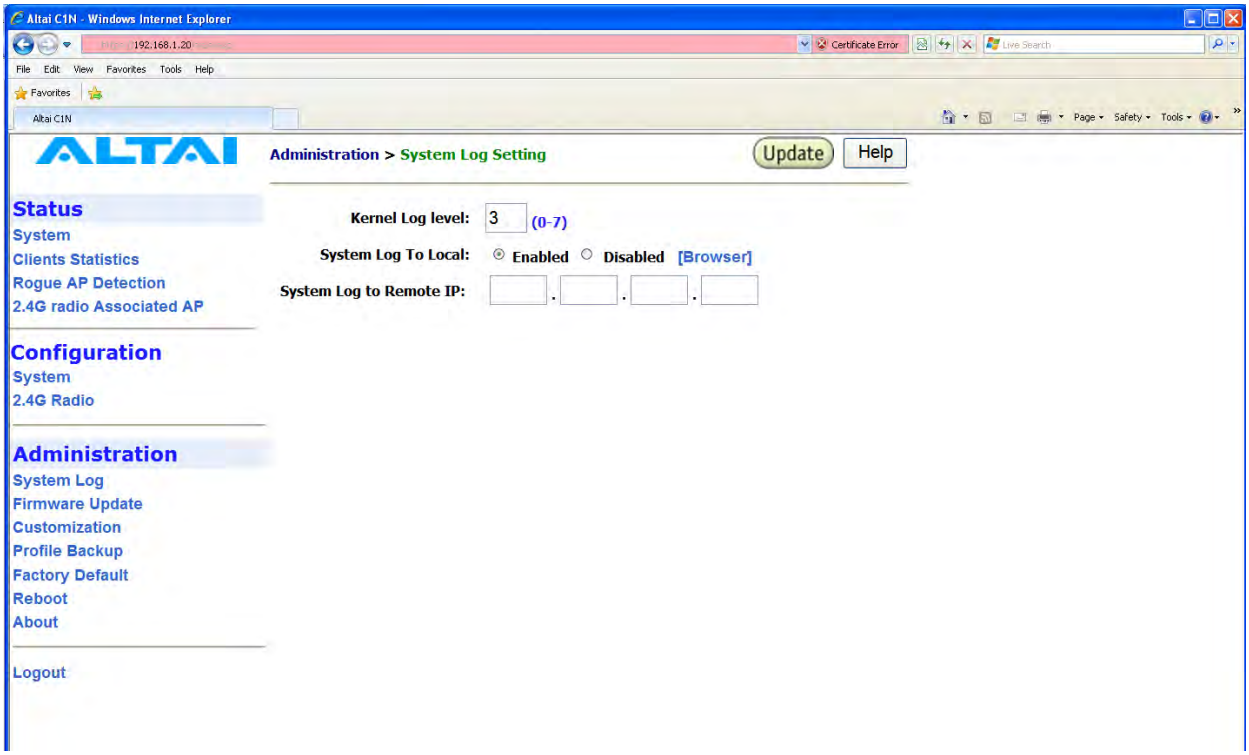


Figure 33 System Log Setting

4.13 REBOOT

System reboot of C1n CPE/AP can be chosen by selecting **Reboot** under **Administration** in the menu bar. It is required to select ***Reboot Device*** to confirm this action, as shown in Figure 34 Reboot Window.

When the C1n CPE/AP is rebooting, a message "**Please wait… Device is Rebooting**" is shown on the window, as shown in Figure 35 C1n is Rebooting. It will take about 20 seconds for C1n to boot up.

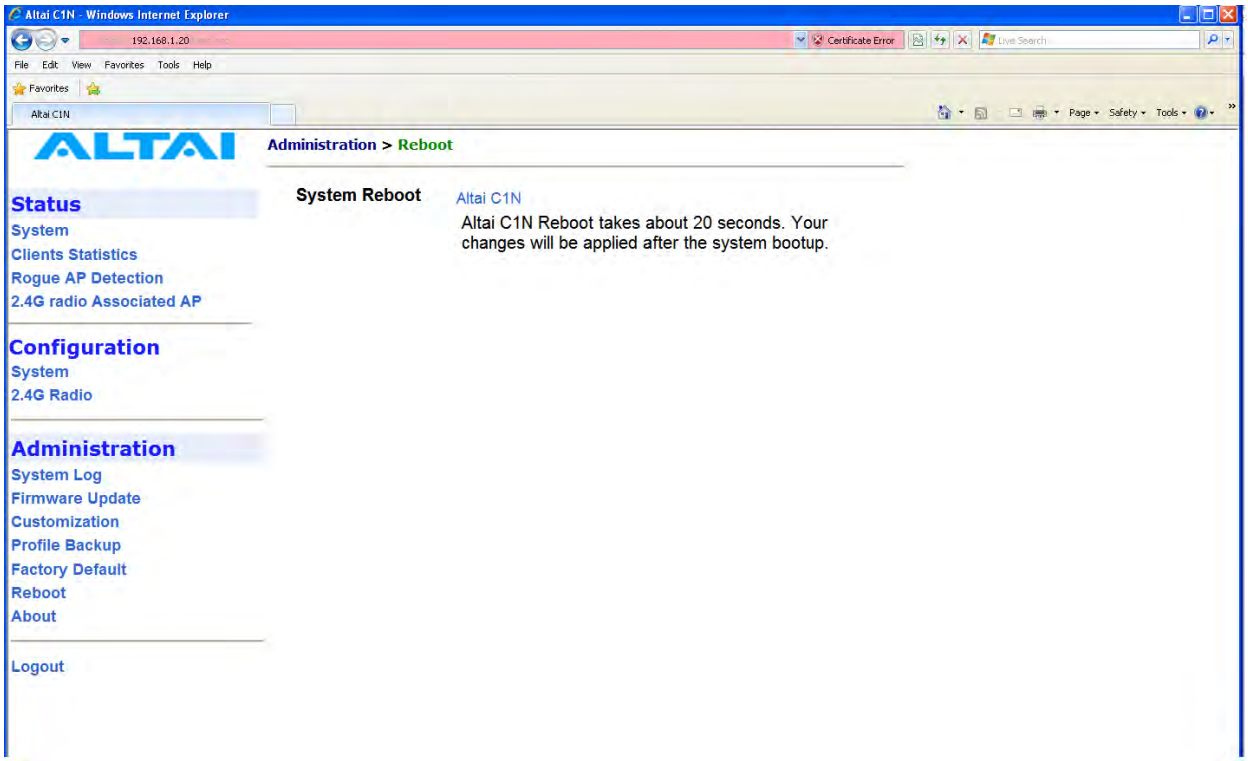


Figure 34 Reboot Window

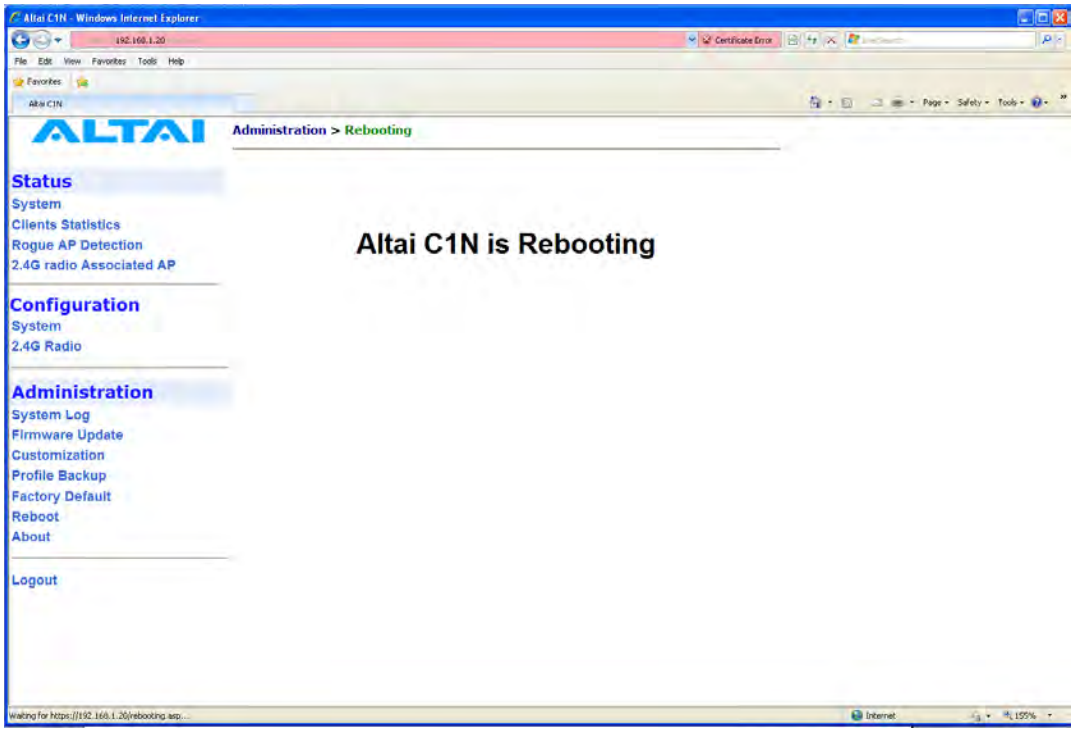


Figure 35 C1n is Rebooting

4.14 RESTORE CONFIGURATION TO DEFAULT SETTING

Restoring configuration to factory default can be achieved by hardware reset or software reset. For software reset, the choices of factory default can be chosen by selecting **Factory Default** under **Administrations** in the menu bar.

The default settings (**IP Address, Subnet Mask, Default Gateway Address and Remote Bridge Configurations are retained**) can be restored by selecting the icon ***Reset to Factory Default (address retained)*** or ***Reset to Factory Default***, as shown in Figure 36 Reset to Factory Default Setting in Web-admin. Please reboot the C1n CPE/AP afterwards.

Note: after resetting to factory default **without address retained**, please type <*http://192.168.1.20*> to open C1n CPE/AP web-admin.

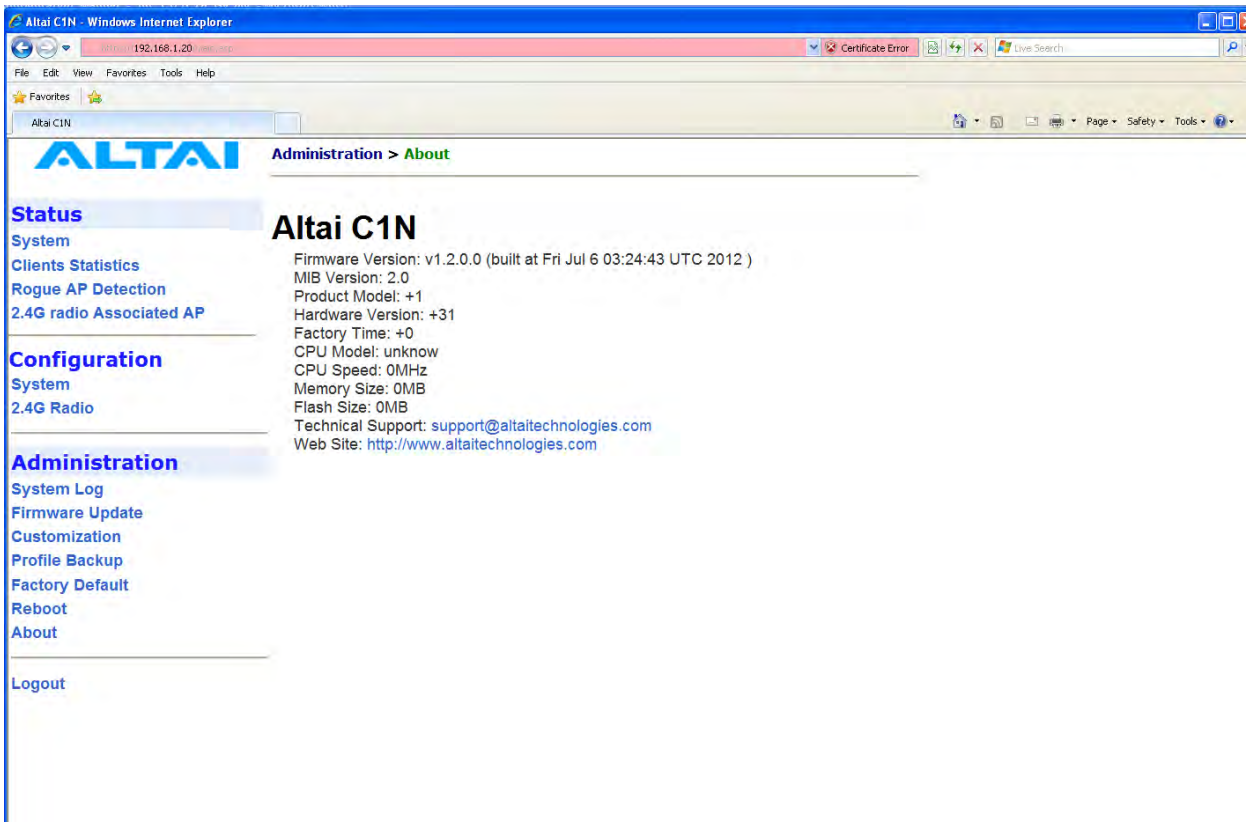


Figure 36 Reset to Factory Default Setting in Web-admin

For hardware reset, a reset button can be found next to the Ethernet port on C1n. First, make sure the C1n is already powered up. Then, press and hold the C1n reset button until the power LED turns off. **Hardware reset will reset the C1n to factory default without retaining IP address.**

5 PERFORMANCE MANAGEMENT MONITORING IN WEB-ADMIN

5.1 SYSTEM

The statistics can be monitored by selecting **System** under **Status** in the menu bar. All details are shown on the window, as shown in Figure .

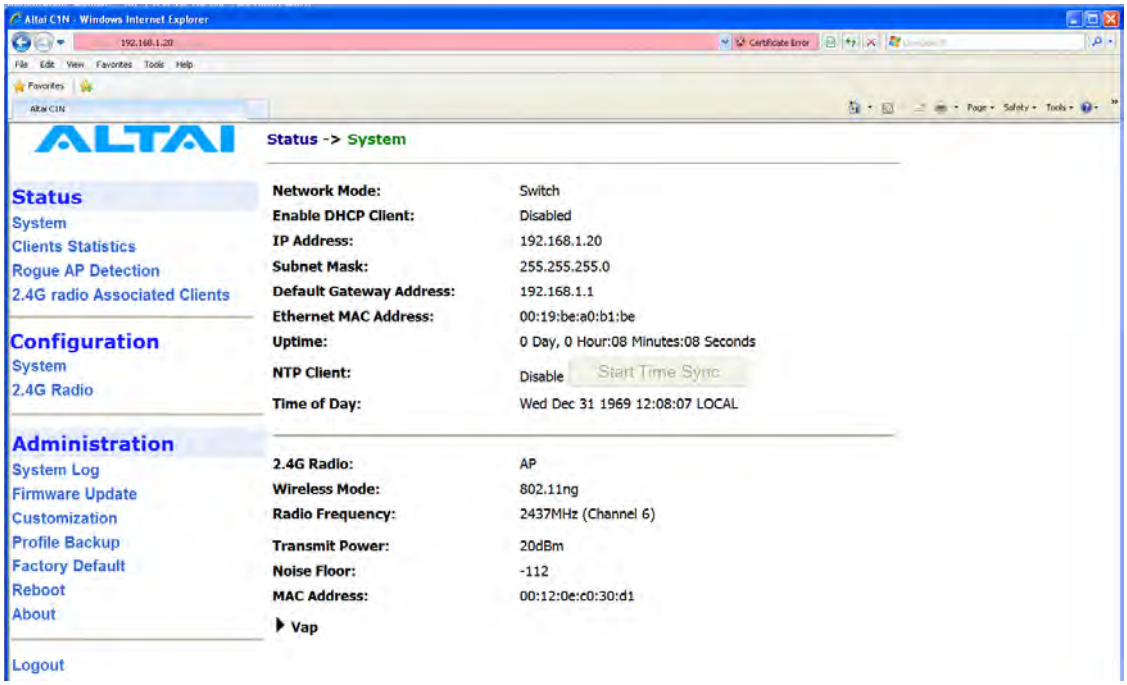


Figure 37 Details of the system

When C1n works as a Access Point, the status of each VAP can be shown by clicking ***Vap*** under the field of ***2.4GHz Radio***, as shown in Figure .

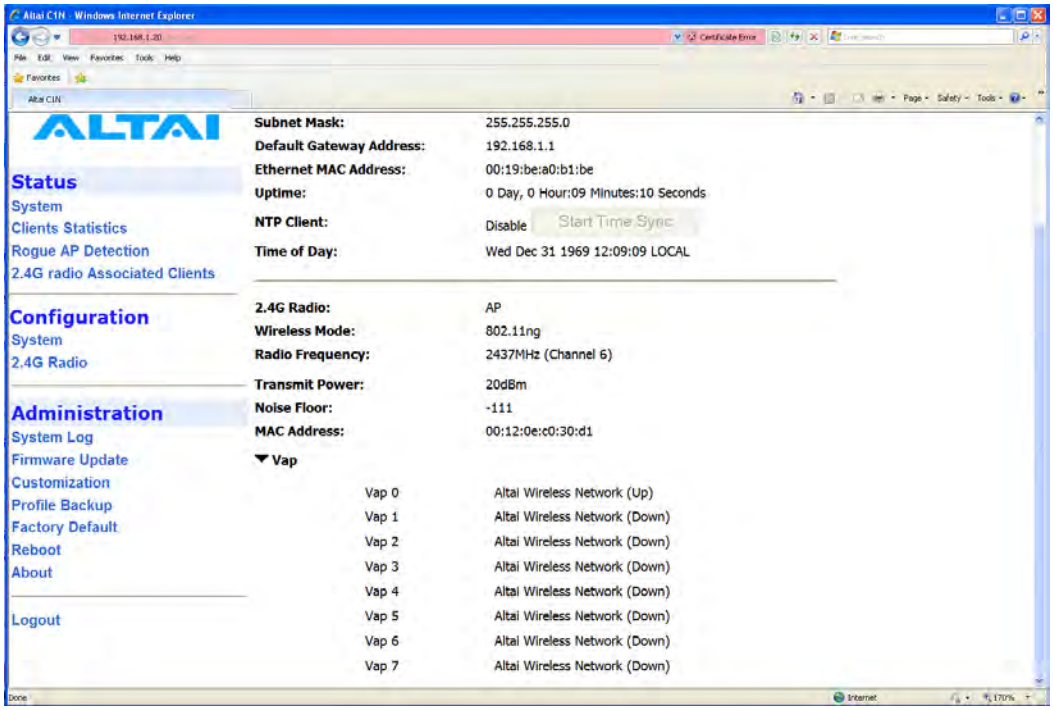


Figure 38 Statuses of the Vaps

5.2 2.4GHz Statistics

The 2.4GHz radio statistics can be monitored by selecting **2.4GHz Statistics** under the field of **Status** in the menu bar, as shown in Figure .

The Address Lease Table shows the ***Client MAC Address***, ***Client IP Address*** of each end user.

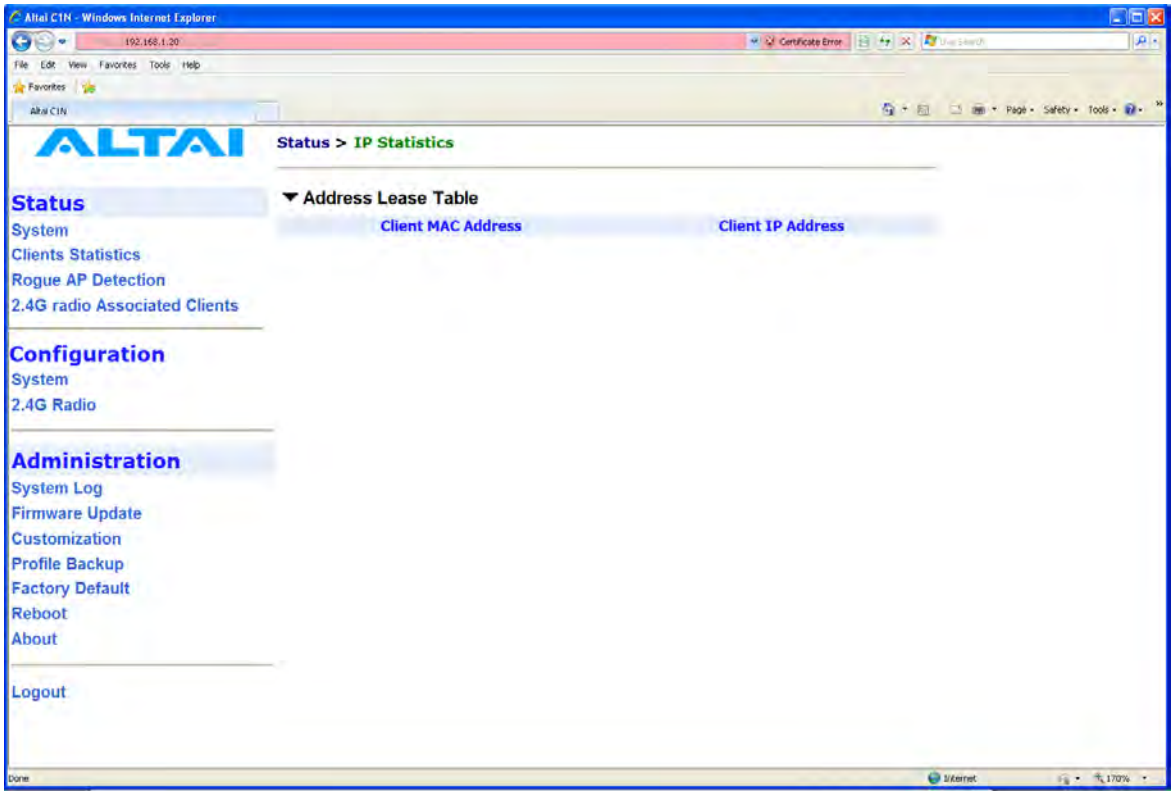


Figure 39 2.4GHz Radio Statistics Menu

5.3 2.4GHz Association Client

The 2.4GHz radio association can be monitored by selecting **2.4GHz Association Client** under the field of **Status** in the menu bar. The 2.4GHz Association Table shows the ***ID***, ***Mac Address***, ***RSSI***, and ***VAP*** of each station as shown in Figure . A more detailed 2.4GHz Association Statistic of each station can be brought up by selecting the related ***Mac Address*** as shown in Figure 41.

Status	Description
ID	Station ID, a number randomly generated by C1n to represent a mobile client
Mac Address	Station Mac Address
RSSI	Receiver Signal Strength
VAP	Virtual Access Point ID Number that the mobile client associates to

Table 8 2.4GHz Client Association Status

NOTE: The association page would be refreshed for every 15 seconds

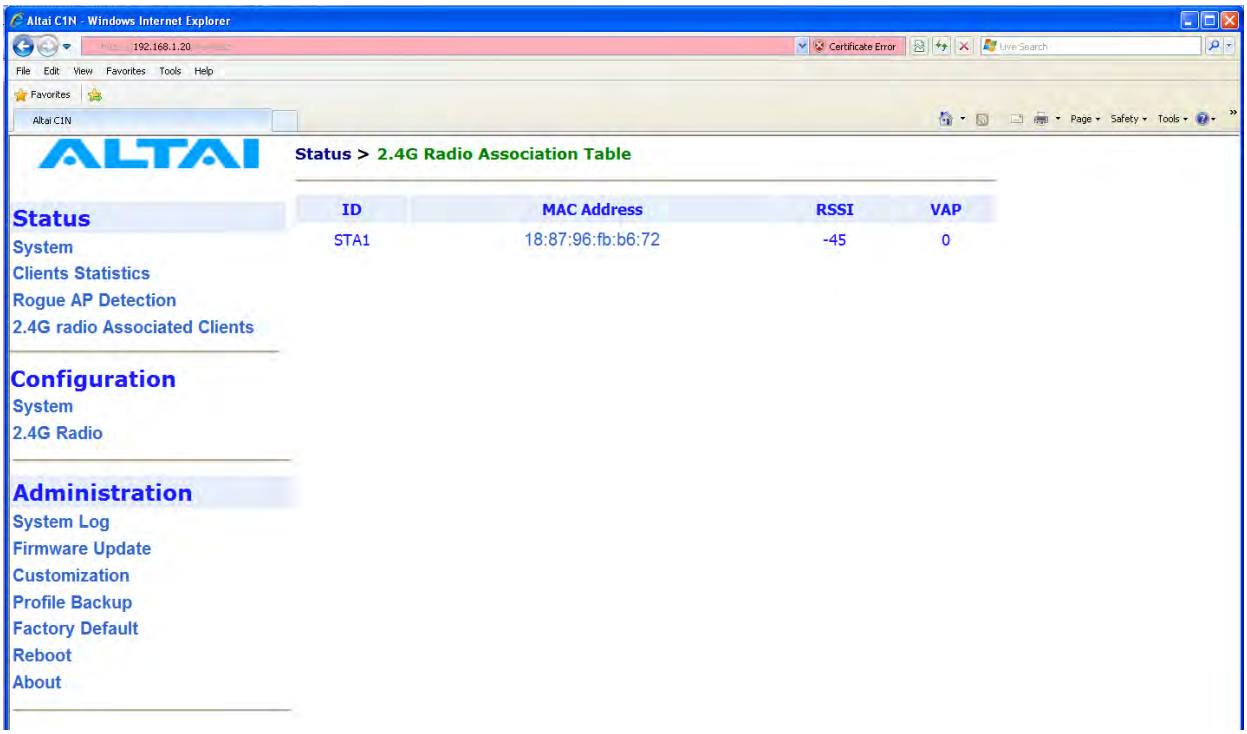


Figure 40 2.4GHz Association Table

Figure 41 2.4GHz Radio Statistics per MAC Address (data is cumulative)

5.4 2.4GHz Association AP

The 2.4GHz radio association can be monitored by selecting **2.4GHz Association Client** under the field of **Status** in the menu bar.

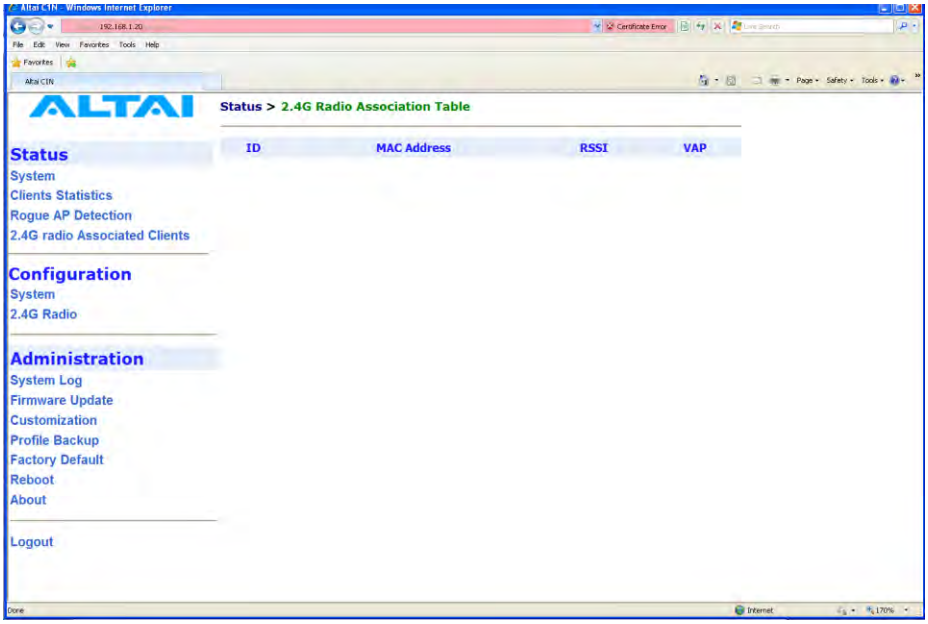


Figure 42 2.4G Radio Association AP List

6 SOFTWARE UPGRADE THROUGH WEB-ADMIN

The firmware can be upgraded by selecting **Firmware Update** under the field of **Administrations** in the menu bar respectively. Please note that the connection link should be maintained during file transfer to prevent interruption to the system.

6.1 FIRMWARE UPDATE THROUGH HTTP OR HTTPS

Follow the steps below to perform the Firmware Update with a firmware image file (.bin) in local directory through HTTP or HTTPS.

1. Click the ***Browse…*** bottom to bring up a file chooser dialog which you can specify the name and location of the firmware image you want to import.
2. Click the ***Update Firmware*** bottom to start uploading the new firmware from the local directory, see Figure .
3. If the firmware upgrade is successful, a window will appear as Figure 44 Successful Firmware Update - Web-admin. C1n Super WiFi CPE/AP will reboot automatically.
4. Type in URL with **http**://<*ip address of C1n*>, note 'http' can not link to the web admin of C1n under the new firmware version.
5. After the C1n reboots, check the firmware version by selecting **About** under the field of **Administrations** in the menu bar, as discussed in Section 4.2, to ensure the expected firmware is uploaded.
6. Select **Factory Default** under the field **Administrations** in the menu bar and click **Reset to Factory Default** (**address retained**) or **Reset to Factory Default** to make the default settings effective. Note: If press **Reset to Factory Default** with **address retained**, the IP address of C1n web-admin will not be changed after rebooting the AP. While **Reset to Factory Default** is chosen, IP address of C1n Super WiFi CPE/AP will be changed into **192.168.1.20** .
7. Click the icon ***REBOOT AP*** to reboot the C1n Super WiFi CPE/AP.

Warning: The C1n Access Point will not be working properly if there is some mistaken in the upgrade process. You are NOT advised to perform firmware upgrade if you have not received any training from ALTAI or its partners.

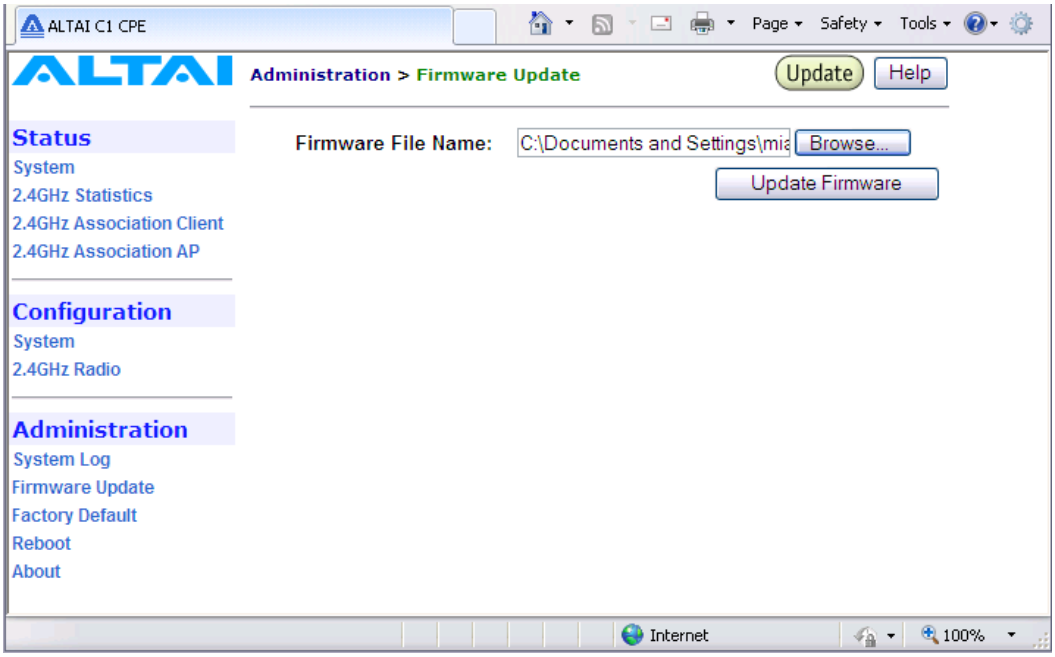


Figure 43 Upload the Firmware through HTTP

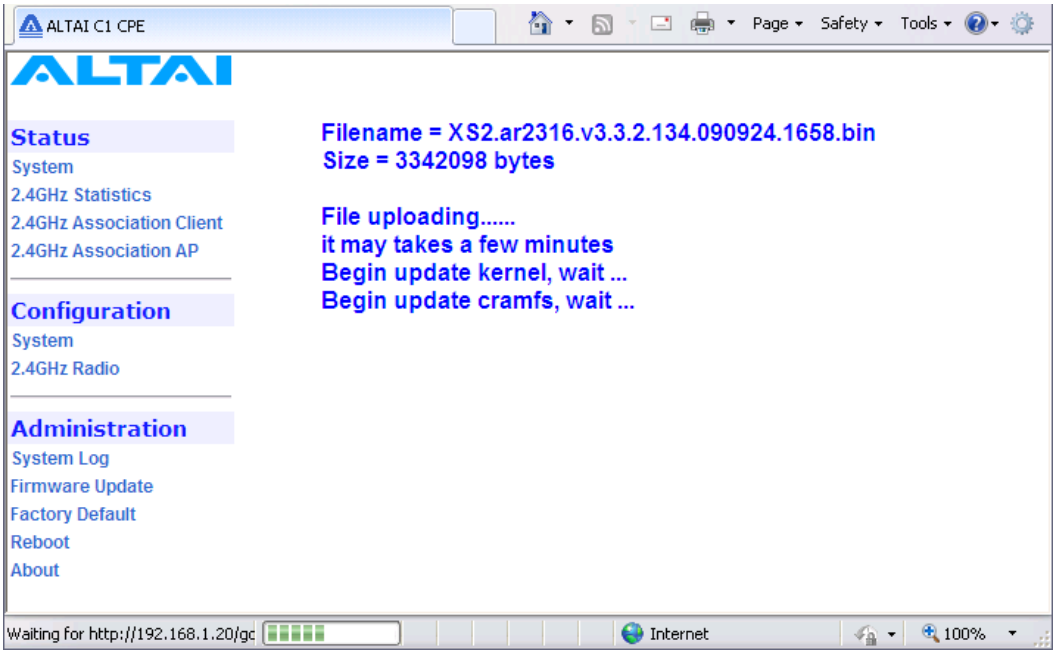


Figure 44 Successful Firmware Update - Web-admin

7 FREQUENCY ASK QUESTION

Q1) Before any configuration, why my computer cannot access to C1n web page?

- Make sure C1n Power LED lights green
- Make sure C1n Ethernet LED lights green
- Make sure your computer LAN Connection IP address is configured as 192.168.1.2. The IP address of your LAN can be found in LAN connection status.

First, click **Start** -> **Control Panel** -> **Network Connections**. Double click on **Local Area Connection**. Under **General** tab, the **Status** should be displayed as *Connected*. If not, please check the network cable connection or replace the network cable.

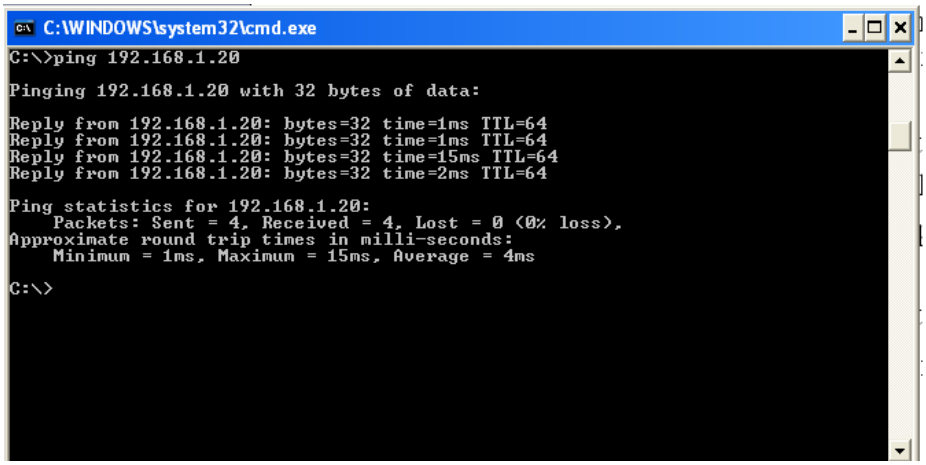
Then, click on **Support** tab. Address type should be *Manually Configured* and it shows the IP address.

- Make sure your computer can ping to C1n.

First, click **Start** -> **Accessories** -> **Command Prompt**.

Second, type *ping 192.168.1.20*

If the connection is successful, the result should be shown as the following:



If the ping result appears **request timed out**, please verify the network cable connection.

Q2) Why C1n CPE mode cannot associate to my AP?

- Verify the connection status by clicking on **2.4GHz associated AP**
- Make sure C1n is configured as **station mode**
- Verify the **SSID**, **authentication** and **cipher** mode are correctly configured.
- Make sure the AP side MAC address filter has included the C1n 2.4GHz radio MAC address or the filter is disabled.
- Verify the network cable between C1n and laptop is working properly.

Q3) Why my laptop cannot access to Internet through C1n CPE mode?

- Verify the connection status by clicking on **2.4GHz associated AP**
- Check if WDS is enabled on AP side. If WDS is not enabled and it is not used, WDS should be disabled on C1n. Otherwise, WDS should be enabled on AP side. Please notice that WDS has to be enabled for certain applications.
- Check if the C1n is associated to AP on AP connection client
- Check it the AP is already accessible to Internet.

8 GLOSSARY

802.1q IEEE 802.1Q was a project in the IEEE 802 standards process to develop a mechanism to allow multiple bridged networks to transparently share the same physical network link without leakage of information between networks (i.e. trunking). IEEE 802.1Q is also the name of the standard issued by this process, and in common usage the name of the encapsulation protocol used to implement this mechanism over Ethernet networks. This protocol allows for individual VLANs to communicate with one another with the use of a layer-3 (network) router.

802.11 802.11 refers to a family of specifications developed by the IEEE for wireless LAN technology. 802.11 specifies an over-the-air interface between a wireless client and a base station or between two wireless clients. The IEEE accepted the specification in 1997.

802.11a An extension to 802.11 that applies to wireless LANs and provides up to 54 Mbps in the 5GHz band. 802.11a uses an Orthogonal Frequency Division Multiplexing (OFDM) encoding scheme rather than Frequency Hopping Spread Spectrum (FHSS) or Direct Sequence Spread Spectrum.

802.11b Also referred to as 802.11 High Rate or Wi-Fi. It is an extension to 802.11 that applies to wireless LANS and provides 11 Mbps transmission (with a fallback to 5.5, 2 and 1 Mbps) in the 2.4 GHz band. 802.11b uses only DSSS. 802.11b was a 1999 ratification to the original 802.11 standard, allowing wireless functionality comparable to Ethernet.

802.11e A supplement to the IEEE 802.11 wireless LAN (WLAN) specification for enhancements to the 802.11 Medium Access Control (MAC) to improve and manage Quality of Service (QoS), provide Classes of Service (CoS), and enhanced security and authentication mechanisms.

802.11g The 802.11g specification is a standard for Wireless Local Area Networks (WLANs) that offers transmission over relatively short distances at up to 54 megabits per second (Mbps), compared with the 11 Mbps theoretical maximum with the earlier 802.11b standard. Networks employing 802.11g operate at radio frequencies between 2.400 GHz and 2.4835 GHz, the same band as 802.11b. But the 802.11g specification employs Orthogonal Frequency Division Multiplexing (OFDM), the modulation scheme used in 802.11a, to obtain higher data speed. Computers or terminals set up for 802.11g can fall back to speeds of 11 Mbps. This feature makes 802.11b and 802.11g devices compatible within a single network. Modification of an 802.11b access point to 802.11g compliance usually involves only a firmware upgrade.

802.11i A supplement to the IEEE 802.11 wireless LAN (WLAN) specification for enhanced security through the use of stronger encryption protocols such as the Temporal Key Integrity Protocol (TKIP) and AES Counter-Mode Cipher Block Chaining Message Authentication Code Protocol (AES-CCMP). These protocols provide replay protection, cryptographically keyed integrity checks, and key derivation based on the IEEE 802.1X port authentication standard.

ACL Access Control List: It is a table that tells a computer operating system which access rights each user has to a particular system object, such as a file directory or individual file.

ad-hoc mode An 802.11 networking framework in which devices or stations communicate directly with each other, without the use of an Access Point (AP). Ad-hoc mode is also referred to as peer-to-peer mode or an Independent Basic Service Set (IBSS). Ad-hoc mode is useful for establishing a network where wireless infrastructure does not exist or where services are not required.

antenna gain The measure of an antenna assembly performance relative to a theoretical antenna, called an isotropic radiator (radiator is another term for antenna). Certain antenna designs feature higher performance relative to vectors or frequencies.

AP Access Point: A hardware unit that acts as a communication hub by linking wireless mobile 802.11 stations such as PCs to a wired backbone network. A Trapeze Networks Mobility System has Mobility Point APs.

ASCII American Standard Code for Information Interchange: An 8-bit code for representing characters, consisting of 7 data bits plus 1 parity bit.

association The relationship established between mobile (wireless) stations and a wireless AP (AP) in which the stations receive services from the AP.

bandwidth The gap between the highest and lowest frequencies employed by network signals. More commonly, it refers to the rated throughput capacity of a network protocol or medium. The frequency range necessary to convey a signal measured in units of hertz (Hz).

broadcast A data frame or packet that is transmitted to every node on the local network segment (as defined by the broadcast domain). Broadcasts are known by their broadcast address, which is a destination network and host address with all the bits turned on.

channel Communication path wide enough to permit a single RF transmission. Multiple channels can be multiplexed over a single cable in certain environments.

dB decibels: Unit for measuring relative power ratios in terms of gain or loss. Units are expressed in terms of the logarithm to base 10 of a ratio and typically are expressed in watts. dB is not an absolute value, rather it is the measure of power lost or gained between two devices. Because antennas and other RF devices/systems commonly have power gains or losses on the orders of magnitude or even orders of four orders of magnitude, dB is a more easily used expression.

dBd decibels over Dipole: A relative gain measurement with respect to a half wave dipole (0 dBd = 2.14 dBi) using a standard dipole antenna as a reference.

dBi dBi referenced to an isotropic antenna, which theoretically is perfect in terms of symmetric patterns of radiation. Real world antennas do not perform with even nominal amounts of symmetry, but this effect generally is used to the advantage of the system designer.

dBm decibels per Milliwatt: 0 dBm is defined as 1 mw at 1 kHz of frequency at 600 ohms of impedance.

DHCP Dynamic Host Configuration Protocol: Provides a mechanism for allocating IP addresses dynamically so that addresses can be reused when hosts no longer need them.

DNS Domain Name Server: System used on the Internet for translating names of network nodes into addresses.

DSSS Direct Sequence Spread Spectrum: One of two types of spread spectrum radio technology used in wireless LAN (WLAN) transmissions. To increase a data signal's resistance to interference, the signal at the sending station is combined with a higher-rate bit sequence that spreads the user data in frequency by a factor equal to the spreading ratio.

EIRP Effective Isotropic Radiated Power: Term for the expression of the performance of an antenna in a given direction relative to the performance of a theoretical (isotropic) antenna and is expressed in watts or dBW. EIRP is the sum of the power sent to the antenna plus antenna gain.

encryption The conversion of information into a scrambled form that effectively disguises it to prevent unauthorized access. Every encryption scheme uses some well-defined algorithm, which is reversed at the receiving end by an opposite algorithm in a process known as decryption.

Ethernet Baseband LAN specification invented by Xerox Corporation and developed jointly by Xerox, Intel, and Digital Equipment Corporation. Ethernet networks use CSMA/CD and run over a variety of cable types at 10 Mbps. Ethernet is similar to the IEEE 802.3 series of standards.

FastRoaming™ The Trapeze Mobility System feature that quickly hands off a roaming user's credentials. Mobility Exchanges in a Trapeze Mobility Domain pass each other this vital user information to permit seamless roaming. This allows 802.1X and non-802.1X, MAC-authenticated devices, such as 802.11 phones, to roam quickly between Mobility Exchanges.

FCC Federal Communications Commission: U.S. government agency that supervises, licenses, and controls electronic and electromagnetic transmission standards. The FCC Rules in Title 47 of the Code of Federal Regulations govern telecommunications in the United States. Wireless LANs must comply with Part 15 of the FCC rules, which are written specifically for RF devices.

firmware Software instructions set permanently or semipermanently in ROM.

FHSS Frequency Hopping Spread Spectrum: One of two types of spread spectrum radio technology used in wireless LAN (WLAN) transmissions. The FHSS technique modulates the data signal with a narrowband carrier signal that “hops” in a predictable sequence from frequency to frequency as a function of time over a wide band of frequencies. Interference is reduced, because a narrowband interferer affects the spread spectrum signal only if both are transmitting at the same frequency at the same time. The transmission frequencies are determined by a spreading (hopping) code. The receiver must be set to the same hopping code and must listen to the incoming signal at the proper time and frequency to receive the signal.

FPGA Field Programmable Gate Array: An FPGA is a specially made digital semiconductor often used for prototyping. With an FPGA, a design engineer is able to program electrical connections on site for a specific application, without paying thousands of dollars to have the chip manufactured in mass quantities.

FTP File Transfer Protocol: Defined in RFC 959, it is a Application protocol that is part of the TCP/IP protocol stack, used for transferring files between network nodes.

gateway In the IP community, an older term referring to a routing device. Today, the term router is used to describe nodes that perform this function, and gateway refers to a special-purpose device that performs an application-layer conversion of information from one protocol stack to another.

handoff The process of transferring the handling of that cellular call to the new base station.

host address Logical address configured by an administrator or server on a device. Logically identifies this device on an internetwork.

https Hypertext Transfer Protocol over Secure Sockets Layer: An Internet protocol developed by Netscape to encrypt and decrypt network connections to web servers. Built into all secure browsers, HTTPS uses the Secure Sockets Layer (SSL) protocol as a sublayer under the regular HTTP application layer, and uses port 443 instead of HTTP Port 80 in its interactions with the lower layer, TCP/IP.

ICMP Internet Control Message Protocol: Defined in RFC 792, it is a Network layer Internet protocol that reports errors and provides other information relevant to IP packet processing.

IEEE Institute of Electrical and Electronic Engineers: An American professional society whose standards for the computer and electronics industry often become national or international standards. In particular, the IEEE 802 standards for LANs are widely followed.

infrastructure network In an infrastructure network, all communications are relayed through an AP (AP). Wireless devices can communicate with each other or with a wired network. The network is defined by the distance of mobile stations from the AP, but no restriction is placed on the distance between stations. Stations must request association with the AP to obtain network services, which the AP can grant or deny based on the contents of the association request. Like most corporate wireless LANs (WLANs), which must access a wired LAN for file servers and printers, Trapeze Networks Mobility System is an infrastructure network.

IP Internet Protocol: Defined in RFC 791, it is a Network Layer protocol that is part of the TCP/IP stack and allows connectionless service. IP furnishes an array of features for addressing, type-of-service specification, fragmentation and reassembly, and security.

IP address Often called an “Internet address”, this is an address uniquely identifying any device (host) on the Internet (or any TCP/IP network). Each address consists of four octets (32 bits), represented as decimal numbers separated by periods (a format known as “dotted-decimal”). Every address is made up of a network number, an optional subnetwork number, and a host number. The network and subnetwork numbers together are used for routing, while the host number addresses an individual host within the network or subnetwork. The network and subnetwork information is extracted from the IP address by using the subnet mask. There are five classes of IP addresses (A-E), which allocate different numbers of bits to the network, subnetwork, and host portions of the address.

LOS Line Of Sight: Refers to the fact that there must be a clear, unobstructed path between the transmitters and receivers. This is essential for our LMDS products and enhances general performance in every RF deployment as opposed to partial or completely obstructed data paths. The opposite to LOS is NLOS, or Non Line Of Sight.

MAC address Media Access Control address: A Data Link Layer hardware address that every port or device needs to connect to a LAN segment. These addresses are used by various devices in the network for accurate location of logical addresses. MAC addresses are defined by the IEEE standard, and their length is six characters, typically using the burned-in address (BIA) of the local LAN interface. Variously called “hardware address”, “physical address”, “burned-in address” or “MAC-layer address”.

MTU Maximum Transmission Unit: The largest packet size, measured in bytes, that an interface can handle.

NAT Network Address Translation: An algorithm instrumental in minimizing the requirement for globally unique IP addresses, permitting an organization whose addresses are not all globally unique to connect to the Internet, regardless, by translating those addresses into globally routable address space.

NLOS Non Line Of Sight. Also known as obstructed path or pathway.

noise Undesirable communications channel signals.

NTP Network Time Protocol: Protocol built on top of TCP that ensures accurate local time-keeping with reference to radio and atomic clocks located on the Internet. This protocol is capable of synchronizing distributed clocks within milliseconds over long time periods.

OFDM Orthogonal Frequency Division Multiplexing: A technique that splits a wide frequency band into a number of narrow frequency bands and sends data across the subchannels. The wireless networking standards 802.11a and 802.11g are based on OFDM.

open system authentication The sender and the recipient do not share a secret key. Each party generates its own key-pair and asks the receiver to accept the (usually randomly) generated key. Once accepted, this key is used for a short time only, then a new key is generated and agreed upon. So, it is a two-step authentication method, in which sender first sends its identity and in response of that it gets the authentication results.

ping Packet Internet Groper: ICMP echo message and its reply. Often used in IP networks to test the reach ability of a network device.

PoE Power over Ethernet: A technology, defined in the developing IEEE 802.3af standard, to deliver dc power over twisted-pair Ethernet data cables rather than power cords. The electrical current, which enters the data cable at the power-supply end and comes out at the device end, is kept separate from the data signal so neither interferes with the other.

Remote Bridge A bridge located on a network system separate from the host system.

RF Radio Frequency: Any frequency within the electromagnetic spectrum associated with radio wave propagation. When an RF current is supplied to an antenna, an electromagnetic field is created that then is able to propagate through space. Many wireless technologies are based on RF field propagation.

RFC Request For Comments: Document series used as the primary means for communicating information about the Internet. Some RFCs are designated by the IAB as Internet standards. Most RFCs document protocol specifications, such as Telnet and FTP, but some are humorous or historical. RFCs are available online from numerous sources.

shared key authentication Shared key authentication supports authentication of STAs as either a member of those who know a shared secret key or a member of those who do not. Shared key authentication accomplishes this with the use of the WEP privacy mechanism. Therefore, this authentication scheme is only available if the WEP option is implemented. The required secret, shared key is presumed to have been delivered to participating STAs via a secure channel that is independent of IEEE 802.11. During the shared key authentication exchange, both the challenge and the encrypted challenge are transmitted. This facilitates unauthorized discovery of the pseudorandom number (PRN) sequence for the key/IV pair used for the exchange. Implementations should therefore avoid using the same key/IV pair for subsequent frames.

SNMP Simple Network Management Protocol: SNMP forms part of the Internet Protocol suite, as defined by the Internet Engineering Task Force (IETF). It 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.

SNMP2 Simple Network Management Protocol Version 2: Version 2 of the popular network management protocol. SNMP2 supports centralized as well as distributed network management strategies, and includes improvements in the SMI, protocol operations, management architecture, and security.

SSID Service Set Identifier: A 32-character (maximum) unique identifier attached to the header of packets sent over a WLAN that acts as a password when a mobile device tries to connect to the Basic Service Set.

STP Spanning-Tree Protocol: Bridge protocol that uses the spanning-tree algorithm, enabling a learning bridge to dynamically work around loops in a network topology by creating a spanning tree. Bridges exchange BPDU messages with other bridges to detect loops, and then remove the loops by shutting down selected bridge interfaces. Refers to both the IEEE 802.1 Spanning-Tree Protocol standard and the earlier Digital Equipment Corporation Spanning-Tree Protocol upon which it is based. The IEEE version supports bridge domains and allows the bridge to construct a loop-free topology across an extended LAN. The IEEE version generally is preferred over the Digital version.

subnet mask A 32-bit address mask used in IP to identify the bits of an IP address that are used for the subnet address. Using a mask, the router does not need to examine all 32 bits, only those selected by the mask.

telnet The standard terminal emulation protocol within the TCP/IP protocol stack. Defined in RFC 854, it is a method of remote terminal connection, enabling users to log in to remote networks and use those resources as if they were locally connected.

throughput Rate of information arriving at, and possibly passing through, a particular point in a network system.

VAP Virtual Access Point: It is a logical entity that exists within a physical Access Point (AP). When a single physical AP supports multiple “Virtual APs”, each Virtual AP appears to stations (STAs) to be an independent physical AP, even though only a single physical AP is present.

VLAN Virtual LAN: Group of devices on one or more LANs that are configured (using management software) so that they can communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, they are extremely flexible.

VLAN tag It works by tagging each frame, i.e. an Ethernet header extension that enlarges the header from 14 to 18 bytes. The VLAN tag contains the VLAN ID and priority.

WDS can preserve the MAC address of client packets across links between accent points. WDS have to be enabled when repeater AP WDS is enabled.

WEP Wired Equivalent Privacy: A security protocol for wireless local area networks (WLANs) defined in the 802.11b standard. WEP is designed to provide the same level of security as that of a wired LAN. LANs are inherently more secure than WLANs because LANs are somewhat protected by the physicalities of their structure, having some or all part of the network inside a building that can be protected from unauthorized access. WLANs, which are over radio waves, do not have the same physical structure and therefore are more vulnerable to tampering. WEP aims to provide security by encrypting data over radio waves so that it is protected as it is transmitted from one end point to another. However, it has been found that WEP is not as secure as once believed. WEP is used at the two lowest layers of the OSI model - the data link and physical layers; it therefore does not offer end-to-end security.

Wi-Fi Wireless Fidelity: Wi-Fi is a label for devices conforming to the IEEE 802.11b standard for WLAN. The IEEE 802.11b standard has been published by the IEEE, which does not perform conformance testing. In order to establish such a conformance testing process, the Wi-Fi Alliance (formerly known as WECA) has been formed, which tests devices for conformance with the IEEE 802.11b standard and issues the Wi-Fi label for conforming devices.

WME Wireless Multimedia Extensions: Also known as Wi-Fi Multimedia (WMM), it is a Wi-Fi Alliance interpretability certification, based on the IEEE 802.11e draft standard. It provides basic Quality of service (QoS) features to IEEE 802.11 networks. WMM prioritizes traffic according to 4 AC (Access Categories) - voice, video, best effort and background. However, it does not provide guaranteed throughput. It is suitable for simple applications that require QoS, such as Wi-Fi Voice over IP (VoIP) phone.

WPA Wi-Fi Protected Access: WPA was created by the Wi-Fi Alliance in 2002, in part out of impatience with the slow-moving IEEE 802.11i standard. The industry consortium's consensus was that an alternative to WEP was needed quickly, and WPA was the result. To avoid multiple standards and conflicts later on, WPA was designed from the get-go to be compatible with IEEE 802.11i and was based on its early draft specifications.