



Configuration Guide Version 1.2

Altai A8n (ac) Series Super WiFi Base Station

Altai Technologies Ltd. All rights reserved



Copyright © 2015 Altai Technologies Limited

ALL RIGHTS RESERVED.

Altai Technologies Limited

Unit 209, 2/F, Lakeside 2, 10 Science Park West Avenue, Hong Kong Science Park, Shatin, New Territories, Hong Kong

Telephone: +852 3758 6000 Fax: +852 2607 4021 Web: <u>www.altaitechnologies.com</u>

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 A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference at his own expense.

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 apart 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 for 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.

A8n (ac) product series require professional installation. The installer shall be responsible for ensuring that the proper 5GHz antenna is employed so that the limits in FCC Part 15.247 are not exceeded. The installer is responsible for ensuring that the 5GHz radio is used exclusively for fixed, point-to-point operations.

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

1.	INTR	ODUCTION	1		
2.	2. GETTING STARTED				
	2.1.	Preparing the Administrator Computer	2		
	2.2.	CONNECT TO YOUR ALTAL ACCESS POINT.	3		
	23		4		
	2.3.		Λ		
	2. 4 . 2 E	SECONDART IT ADDRESS OF AON (AC) SERIEST RODOCTS	4		
	2.5.		5		
	2.6.		6		
	2.7.	REBOOT AP VIA WEB UI	6		
3.	SUM	IMARY OF BASIC CONFIGURATION TASKS	7		
	3.1.	CONFIGURE AS ACCESS POINT (AP)	7		
	3.2.	CONFIGURE AS STATION (CPE/STA) (5G RADIO ONLY)	9		
	3.3.	CONFIGURE AS REPEATER	. 11		
_					
4.	CON	FIGURE YOUR ACCESS POINT	. 13		
	4.1.	BASIC CONFIGURATIONS	. 14		
	4.1.1	. Synchronize AP's system clock with NTP server	. 14		
	412	Assian Internet Connection Type for AP (IPv4) – Static / DCHP	15		
	113	Configure Radio Interface as Access Point (AP)	16		
	7.1.3 Po	dio 0 - 2 A GHz Padio	16		
	110	Radio General Configuration	.10		
		WI AN List	10		
		WLAN 0.15 General Configuration	20		
		WI AN 0-15 Security Configuration			
		Configure WI AN as Open network	22		
		Configure WI AN as Open network with WEP encryption	23		
		Configure WI AN with Shared Key Authentication	24		
		Configure WI AN with WPA / WPA2 / WPA-auto Authentication	25		
		Configure WI AN with WPA-PSK / WPA2-PSK / WPA-auto-PSK Authentication	27		
		Configure WI AN with WAPI Authentication.	28		
		Configure WI AN with WAPI-PSK Authentication			
	Ra	idio 1 – 5GHz Radio			
		Radio General Configuration	31		
		WLAN List	33		
		WLAN 0 - 15 General Configuration	33		
		WLAN 0 - 15 Security Configuration	33		
	4.1.4	. Confiaure Radio Interface as Station (STA/CPE)	. 34		
	Ra	idio 0 – 2.4GHz Radio	34		
	Ra	idio 1 – 5GHz Radio	34		
		Radio General Configuration	34		
		Station Configuration	36		
		Station Security Configuration	37		
		Configure Station to associate Open network	38		
		Configure Station to associate Open network with WEP encryption	38		
		Configure Station to associate network with Shared Key authentication	39		
		Configure Station to associate network with WPA / WPA2 authentication	39		
		Configure Station to associate network with WPA-PSK / WPA2-PSK authentication	40		
	4.1.5	5. Configure Radio Interface as Repeater	. 42		
	Ra	idio 0 – 2.4GHz Radio	42		



Radio 1 – 5GHz Radio	42
Radio General Configuration	42
Repeater WLAN Configuration	43
4.2. Advance Configurations	44
4.2.1. Assign a unique identification on AP for network management	44
4.2.2. Configure syslog settings	44
4.2.3. Configure historical statistics settings	45
4.2.4. Configure refresh interval of on-screen information on Web UI	46
4.2.5. Configure http and https port number	46
4.2.6. Configure AP as IP Gateway	47
4.2.7. Enable Spanning Tree Protocol (STP)	48
4.2.8. Configure the operating mode on Ethernet interface	48
4.2.9. VLAN	49
Enable VLAN	49
4.2.10. DHCP	51
Enable DHCP server	51
4.2.11. Port Forward	52
Enable port forward on A8n (ac) device	52
4.2.12. Safe Mode	53
Enable safe mode on A8n (ac) device	53
4.2.13. Advanced Settings on Radio Interface	54
Advanced Settings	55
Configure AMPDU and AMSDU on radio interface	55
Configure the number of transmit radio chains and receive radio chains	55
Configure Delivery Traffic Indication Message (DTIM) time	55
Modify protect mechanism on hidden node problem of Wi-Fi network	
Change distance setting on A8n (ac)	
Enable IGMP Snooping	
Enable multicast traffic	58
Enable Nearby AP List on A8n (ac)	58
AirFi Settings	58
Data Rate Setting	59
4.2.14. Quality of Service on Radio Interface	59
Modify the QoS setting on Radio	59
Modify the QoS setting in WLAN 0 – 15	60
4.2.15. Bandwidth Control on WLAN	60
Enable bandwidth control for the WLAN on WLAN 0 – 15	61
How to enable bandwidth control per station on WLAN 0 – 15	61
5. MANAGE YOUR ACCESS POINT	62
5.1. User Admin	62
5.1.1. Local authentication	62
Modify admin account's password	62
Modify guest account's password	62
5.1.2. RADIUS authentication	63
Enable RADIUS authentication in A8n (ac) products	63
5.2. SNMP	64
5.2.1. Enable SNMP in A8n (ac) products	64
5.3. Certificate	65
5.3.1. Upload the customized certification for HTTPS connection on A8n (ac) proc 65	ducts
5.4. Firmware Update	66



	5.4.1. Update A8n (ac) device's firmware	66
ŗ	5.5. Factory Default	67
	5.5.1. Restore A8n (ac) device's settings with default settings	67
ŗ	5.6. BACKUP/RESTORE	67
	5.6.1. Backun A8n (ac) device's settings	67
	5.6.2 Restore A8n (ac) device's settings with configuration file	68
	$\mathbf{F}_{\mathbf{z}} = \mathbf{C}_{\mathbf{z}} $	60
	5.7. CUSTOMIZATION	00
	5.7.1. Create customized conjiguration file for A8n (ac) products	68
6.	MONITOR YOUR ACCESS POINT	70
(6.1. LED COLORS AND WHAT THEY MEAN	70
	6.1.1. A8n (ac) series	70
(6.2. Status > Overview	71
	6.2.1. System status	71
	6.2.2 Thin AP	72
	6.2.2 Notworks	72
	Switch Mode	/2 72
	Switch Mode	.72
		./5 72
	WAN	./3
		./3
	6.2.4. Interfaces	74
	Ethernet (ethu)	.74
	Radiou (2.46)	. 75
		. 75
(6.3. STATUS > RADIOU(2.4G)	76
	6.3.1. Status > Radio0(2.4G) > Status	76
	Radio Settings	.77
	Channel Usage List	.77
	Nearby AP List	.77
	Tx/Rx Statistics	.77
	6.3.2. Status > Radio0(2.4G) > Association List	78
	WAN	.78
	Station List	. 78
	Rogue Station List	.78
(6.4. Status > Radio1(5G)	79
	6.4.1. Status > Radio1(5G) > Status	79
	Radio Settings	.79
	Channel Usage List	.79
	Nearby AP List	.80
	Tx/Rx Statistics	.80
	6.4.2. Status > Radio1(5G) > Association List	80
	WAN	.80
	Station List	. 80
	Rogue Station List	.81
(6.5. STATUS > ETHERNET	82
	6.5.1. Status > Ethernet > Status	82
f	6.6. Status > Logs	82
_ `		
7.	EMBEDDED TOOLS FOR DEPLOYMENT / OPERATION / TROUBLESHOOTING	83
-	7.1. Channel Scan	83
	7.1.1. Perform channel scan on 2.4G radio	84
	7.1.2. Perform channel scan on 5G radio	84
-	7.2. IPERF	84



8. 0	COLLEC	CT DEVICE'S PRODUCT INFORMATION	91
	Enab	le ping watchdog	90
2	7.4.2.	Ping Watchdog	. 90
	Enab	le periodic log upload	88
	Enab	le periodic reboot	88
	7.4.1.	Schedule Reboot	. 88
7.4	. W	/атсноод	. 88
	How	to perform packet capture on A8n (ac)'s interface	87
	7.3.4.	Tcpdump	. 87
	How	to perform traceroute test	87
2	7.3.3.	Traceroute Test	. 86
2	7.3.2.	Perform ping test	. 86
2	7.3.1.	Ping Test	. 86
7.3	. D	IAGNOSIS	. 86
2	7.2.2.	Enable iPerf UDP Server	. 85
	7.2.1.	Enable iPerf TCP Server	. 85



1.Introduction

This guide covers the initial configuration of Altai A8n (ac) Series Super WiFi Base Station via Web Administration Interface (Web UI). Web Administration Interface (Web UI) is the built-in and user-friendly graphic interface on all Altai A8n (ac) Series products. It allows you to configure, monitor, and manage the devices using web browser. Mozilla Firefox, Google Chrome, and Internet Explorer 8+ are recommended.

This guide is applicable with firmware version 2.0.1.6 or above for hardware platforms with the following models:

Product Name	A8n (ac)	A8-Ein (ac)	A8in (ac)	
Model Number	WA8011NAC-X	WA8011NAC	WA8011NAC-H	
Table 1 App (ap) Series products				

Table 1 – A8n (ac) Series products

1



2.Getting Started

This chapter covers the procedures for logging into / out A8n (ac) Series Products Web Administration Interface (Web UI) via Ethernet, and restarting the device via Web UI.

2.1. Preparing the Administrator Computer

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

On Windows XP, click Start > Control Panel > Network Connections. On Windows 7, click Start > Control Panel > Network and Internet > Network and Sharing Center > Change adapter settings.

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

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

5. Configure the IP address settings with the values listed in Table 2.

Table 2 - Configure administrative computer's IP address settings

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



2.2. Connect to Your Altai Access Point

- 1. Connect your laptop to **Data In** port on the PoE Injector provided in the Altai's package using Ethernet cable
- 2. Connect the Ethernet port of AP to **Data & Power Out** port on the PoE Injector provided in the Altai's package using Ethernet cable.
- 3. Connect the power cord to the power port on the PoE Injector. Connect the other end of the power cord to a power outlet.



- Figure 2 A8n-Ein (ac)/ A8in (ac) Connection Diagram
- 4. Verify the AP's Power LED is steady green after a minute



2.3. Login the AP (via Ethernet)

- 1. Verify the AP's Power LED is steady green
- 2. Open a Web browser from the computer.
- 3. Type http://192.168.1.222 in the address bar or location bar (see Figure 3).
- 4. Type admin (default username) in Username
- 5. Type admin (default password) in Password

6.	Click	Login

🗛 A3c WiFi Access Point / Br 🗙 🚺		Min unterditeteringnose Month Intel		
← → C 🗋 192.168.1.222/cg	i-bin/luci			¶☆] =
	AITA			菌体中文
		•		Firmware Version: 2.0.0.504 CPU Load: 0.53, 0.57, 0.27 Uptime: 00h 05min 18s
		Authorization Required		
	Please enter your username and password.			
		Username:		
		Password:		
			Login Reset	

Figure 3 – A8n (ac) Series Product's Login Page

2.4. Secondary IP Address of A8n (ac) Series Products

The default IP address of A8n (ac) series products is 192.168.1.222/24. A8n (ac) series products support a fixed IP address on the Ethernet connection called Secondary IP Address. This secondary IP address is 192.168.99.x/24 where x denotes as the decimal value of the last byte of the Ethernet MAC address on the access point.

Example 1:

Device Ethernet MAC address: 00:19:BE:20:03:**8C** Secondary IP Address of this device:

192.168.99.140 (8C (HEX) → 140 (DEC))

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



Ethernet MAC	Reserved Purpose	Replaced MAC	Secondary IP
address		byte	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	A2	192.168.99.162
	computer		
XX:XX:XX:XX:XX:03	For operator	A3	192.168.99.163
	computer		
XX:XX:XX:XX:XX:04	For operator	A4	192.168.99.164
	computer		
XX:XX:XX:XX:XX:FF	Invalid IP	AF	192.168.99.175

Table 3 – A8n (ac) Series Product Secondary IP Address

Example 2

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

Secondary IP Address of this device:

192.168.99.175 (FF (HEX) → AF (HEX) → 175 (DEC))

2.5. Interface Guide

Status Configuration Administ view Radio0(2.4G) Radio1(5G) Eth	ration Tools nemet Logs	About			CPU Load Uptime
System	Network(Switch M	lode)		<u>More>></u>	
System Name: NA	Ethernet				
Droduct Name: A9 Ein	IPv4 DHCP Client:	Disabled			
CPILLIsage: 4%	IPv4 Address:	10.6.122.98			
Memory Lisage: 161/476 MB (33%)	IPv4 Subnet Mask:	255.255.255.0			
Time of Day: Wed Jup 24 10:12:50	IPv4 Default Gateway	: 10.6.122.1			
2015 2015	IPv4 DNS Server:	10.6.127.4			
Uptime: 00h 53min 01s	Interfaces(3)				
	Ethernet (eth0)				
This an	MAC:	00:19:be:20:03:c3	Transmit:	2.46MB (0.00Kbps)	
THIN AP	Link:	Auto (Full 1000Mb/s)	Receive:	431.08KB (0.00Kbps)	
Thin AP: OFF	Radio0(2.4G)				
	MAC:	00:19:be:00:1b:70	Mode:	AP	
	Channel:	2447MHz(Channel 8)	WLANs:	1	
	Wireless Mode:	2.4GHz 144Mbps(802.11ng HT20)	Clients:	0	
	Noise Level:	-97/-97/-97/-97(dBm)	Busy:	24%(18%)	
	Transmit Power:	1 dBm		15%(19%)	
	Transmit:	326 68KB (22 57Khps)		21%(16%)	
	Receive:	2.08MB (0.00Kbps)		12.0(10.0)	
	Radio1(5G)	2.00MD (0.00K0p5)			
	MAC:	00:19:be:28:01:4f	Mode:	AP	
	Channel:	5500MHz(Channel 100)	WLANs:	10	
	Wireless Mode:	5GHz 866.7Mbps(802.11ac HT80)	Clients:	0	
	Noise Level:	-103 dBm	Busy:	1%(2%)	
	Transmit Power:	5 dBm			
	Transmit:	0.00KB (0.00Kbps)			
	Receive:	0.00KB (0.00Khps)			

Figure 4 – AP Status Overview

Web Administration Interface (Web UI) consists of five primary tabs: **Status** Tab - show system status information, including system status, interfaces status, and system logs.



Configuration Tab – allow the configuration of device operation parameters, including system setting, network settings, and wireless LAN settings.

Administration Tab – allow the management of device, including user administration, certification, SNMP, firmware update, factory reset, configuration backup / restore, and customization.

Tools Tab – provide tools for radio planning, diagnosis, and device's maintenance.

About Tab – show product information, including hardware version, firmware version.

Also, Web UI has a quick tools bar on its top-right hand corner in all pages. It provides some quick tools and basic information. They are chosen language, device reboot, system logs download, and configuration application ...etc.

2.6. Logout from Web UI

1. Click Logout on top-right hand corner of Web UI



Figure 5 – Logout from Web UI

2. Click OK

2.7. Reboot AP via Web UI

- 1. Click Reboot AP on top-right hand corner of Web UI
- 2. Click Perform reboot



6



3. Summary of Basic Configuration Tasks

This chapter summarizes the quick setup procedures for configuring A8n (ac) Series products to operate in different roles in your network, including Access Point (AP), Station (CPE/STA), and Repeater.

3.1. Configure as Access Point (AP)

- 1. Go to Configuration > Network > General > WAN Settings
- 2. Select suitable internet connection type (DHCP / Static)

WAN Setting(IPv4)	

Internet Connection Type:	Static 🗸
IPv4 Address:	10 . 6 . 122 . 101
IPv4 Subnet Mask:	255 . 255 . 255 . 0
IPv4 Default Gateway:	10 . 6 . 122 . 1
IPv4 DNS Server IP Address:	10.6.127.4

Figure 7 – WAN Setting (IPv4)

- 3. Configure IP Address on the device (static internet connection only)
- 4. Click **Submit**
- 5. For 2.4G Radio: Go to Configuration > Wireless > Radio0(2.4G) > General

For 5G Radio: Go to Configuration > Wireless > Radio1(5G) > General

R	adio0(2.4G) Setting		
Advanced QoS WEP			
Enable Radio:	•		
Radio Mode:	AP	۲	
Country Code:	HONG KONG	۲	
Wireless Mode:	2.4GHz 450Mbps(802.11ng HT40+)	•	
Radio Frequency:	Auto	۲	
Transmit Power:	23	۲	
Maximum Clients:	256		(1-256)

Figure 8 – 2.4G Radio General Setting of AP

- 6. Select AP in Operating Mode
- 7. Select suitable **Country Code** that matches your device's installation location.
- Select suitable Wireless Mode
 802.11 ng HT20 is recommended option on 2.4G radio;
 802.11 ac HT80 is recommended option on 5G radio
- 9. Select the suitable Radio Frequency.
- 10. Select the suitable Transmission Power.
- 11. Click Submit



- 12.For 2.4G Radio: Go to Configuration > Wireless > Radio0(2.4G) > WLAN
 - For 5G Radio: Go to Configuration > Wireless > Radio1(5G) > WLAN

Status	Configuration	Administra	tion	Tools	About					
System Netwo	ork Wireless Thir	n AP								
adio0(2.46) - Radio1(5G)										
Radio0(2.4G) Setting										
General WLAN Advanced QoS WEP										
WLAN Con	figuration									
Enable WLAN	SSID	Max Clients	Isolation	Auth Mode	Access Traffic Right	WLAN Uplink/Downlink Control	Station Uplink/Downlink Control	Detail		
I 0	Superwifi Networ Hide SSID	256		<u>open</u>	Full Access	0		More		
	Superwifi Networ Hide SSID	256		open	Full Access	0	0 0	More		
□ 2	Superwifi Networ	256		open	Full Access	0	0 0	More		

Figure 9 – Radio 2.4G WLAN List

- 13. Provide unique **SSID** on each enabled WLAN
- 14. Click **Submit**
- 15.For 2.4G Radio: Go to Configuration > Wireless > Radio0(2.4G) > WLAN > WLAN 0-15 > WLAN Security

For 5G Radio: Go to Configuration > Wireless > Radio1(5G) > WLAN > WLAN 0-15 > WLAN Security

dio0(2.4G) - Radio1(5G	<u>.)</u>			
	Radio	00(2.4G) WLANO Settin	9	
WLAN General WLAN Sec	urity Rogue Station List	QoS Bandwidth Control		
WLAN Security Setting				
	Authentication Mode:	Open	\sim	
	Cipher Mode:	Disabled	~	
ACL Setting				
	Access Control List:	Enabled - Default Allow	~	
	ACL Input Method:	Manual Input O File		
	Denied MAC Address:		<u>1</u>	

Figure 10 - Radio 2.4G WLAN0 Security Setting

- 16.Setup suitable settings of WLAN Security on each operating WLAN
- 17. Click **Submit**
- 18. Save and apply the settings



3.2. Configure as Station (CPE/STA) (5G radio

only)

- 1. Go to Configuration > Network > General > WAN Settings
- 2. Select your ISP's internet connection type (DHCP / Static)
- 3. Configure IP Address on the device (for static internet connection type only)
- 4. Click Submit
- 5. Go to Configuration > Wireless > Radio1(5G) > General

ALTAI	
Status Configuration Administration Tools About System Network Wireless Thin AP	
Radio0(2.4G) - Radio1(5G)	
Radio1(5G) Setting	
General WLAN Advanced QoS	
Enable Radio: 😿	
Radio Mode: Station	
Country Code: HONG KONG	
Dynamic Radio Frequency Selection(DFS):	
Transmit Power: 5	
	Submit

Figure 11–5G Radio General Setting of Station

- 6. Select Station as **Operating Mode** on 5G radio the device.
- 7. Select suitable **Country Code** that matches your device's installation location.
- 8. Select the suitable Transmission Power.
- 9. Click Submit
- 10. Go to Configuration > Wireless > Radio1(5G) > Station > More...

100(2.4G) - Radio1(56) Radiot	(5C)-WI AND Setting	
WEAR Converse	acum Cors	(56), Trento Setting	Subm
Coneral Setting	even at 11 store1	Rooming Setting	
WI AN Made		Freshin Desmiser	0
WLAN MODE.	station	Enable Roaming.	
Lock AP Mac:		Scan SNR threshold:	[36 (a treatil)
Remote \$SID:	Network 0	[Scan]	(0-10000)
Preferred AP0 Mac:		Roaming SNR bireshold:	(0-100dB)
Preferred AP1 Mac:		Max Scan Interval:	60
Dreferred AD2 Mac-			(1-3600s)
Protonou AP 2 mac.		Min Scan Interval:	10
			(1-605)
		Scan SNR Fluctuation	Б
		Threshold:	(0-10dB)
		Wireless Mode Weighting:	
		Bgscan Channel:	5180MHz(Channel 36) 5200MHz(Channel 40) 5220MHz(Channel 44) 5240MHz(Channel 48)

Figure 12 – 5G Radio WLAN Setting of Station

- 11. Scan and select the suitable SSID your ISP provides
- 12. Click **Submit**
- 13.Go to Configuration > Wireless > Radio1(5G) > Station > WLAN Security



- 14. Setup suitable settings of WLAN Security that your ISP provides
- 15. Click **Submit**
- 16.Save and apply the settings



3.3. Configure as Repeater

- 1. Go to Configuration > Network > General > WAN Settings
- 2. Select suitable internet connection type (DHCP / Static)
- 3. Configure IP Address on the device (for static internet connection type only)
- 4. Click Submit
- 5. Go to Configuration > Wireless > Radio1(5G) > General

Status Configuration Administration	īools	About			
System Network Wireless Thin AP					
Radio((30)	Radio	1(5G) Sett	ing		
General WLAN Advanced					
Enable Radio	: 💌				
Radio Mode	Repea	ter		•	
Country Code	HONG	KONG		•	
Transmit Powe	: 5 The effe Channe	ective Tx Power ma	ay be different, depend	▼ ds on the selected	
Maximum Clients	512			(1-512)	
User Isolation in different WLAN (SSID	:				
					Submit

Figure 13 – 5G Radio General Setting of Repeater

- 6. Select Repeater as **Operating Mode** on 5G radio the device.
- 7. Select suitable **Country Code** that matches your device's installation location.
- 8. Select the suitable Transmission Power
- 9. Click **Submit**



10. Go to Configuration > Wireless > Radio1(5G) > WLAN 0-15 > More...

0(2.4G)	- Radio1(5G)									
				Radio1	(5G) Setting					
General	WLAN Advanced	1								Su
ation Co	onfiguration									
	WLAN ID		Remote	SSID	Auth Mo	de			Detail	
	15	Netwo	ork U		open			-	<u>vore</u>	
LAN Cor	nfiguration									
						WL	AN	Sta	tion	
Enable WLAN	SSID	Max Clients	Isolation	Auth Mode	Access Traffic Right	Uplink/D	ownlink	Uplink/I	Downlink	Detai
	Rupopulfi Notword					Con	troi	Cor	itrol	
Ø 0	Hide SSID	512	1	<u>open</u>	Full Access 🔻	0	0	0	0	More
	Superwifi Network	E40			E-II A				D	
□ 1	Hide SSID	512		<u>open</u>	Full Access	0	U	U	U	More
2	Superwifi Networ	512	1	open	Full Access		0	0	0	More
- 2	Hide SSID	512		open	T dir/icecoo		<u> </u>		2	Morea
3	Superwifi Networ	512	s.	open	Full Access	0	0	0	0	More
	Hide SSID									
4	Superwifi Networ	512		open	Full Access	0	0	0	0	More
	Hide SSID									
5	Hide SSID	512	•	open	Full Access	0	0	0	0	More
	Superwifi Networ	540			F # A			0		
06	Hide SSID	512		open	Full Access		U	0	<u>v</u>	More
7	Superwifi Networ	512		open	Full Access		0	0	0	More
	Hide SSID		_	September 1						
8	Superwifi Networ	512		open	Full Access 🔻	0	0	0	0	More
	Hide SSID									
9	Superwifi Networ Hide SSID	512	*	<u>open</u>	Full Access 🔹	0	0	0	0	More
	Supervifi Network									
10	Hide SSID	512	1	open	Full Access 🔻	0	0	0	0	More
	Superwifi Networ	E12			Full Assess				0	
- 11	Hide SSID	512	•	<u>open</u>	Full Access	1	v	U	U.	More
12	Superwifi Networ	512	•	open	Full Access		0	0	0	More
	Hide SSID		_	open.		لـــــــــــــــــــــــــــــــــــــ		<u> </u>	<u> </u>	<u></u>
13	Superwifi Networ	512		open	Full Access	0	0	0	0	More
	Hide SSID									
14	Superwifi Networ	512	•	open	Full Access 🔹	0	0	0	0	More

Figure 14 – 2.4G Radio WLAN List

- 11.Scan and select the suitable SSID from remote AP that your device associate with on WLAN 15
- 12.Setup suitable settings of **WLAN Security** that matches the remote AP
- 13. Click Submit
- 14. Provide unique SSID on each operating WLAN
- 15. Setup suitable settings of WLAN Security on each operating WLAN
- 16. Click **Submit**
- 17. Save and apply the settings



4. Configure Your Access Point

This chapter covers the AP configurations including network configuration, wireless configuration, VLAN ... etc.

Notes:

- Click **Submit** to submit the modified configuration into temporary memory
- Click **Save & Apply** (top-right hand corner) to apply the modified configuration
- Click **Unsaved Change** (top-right hand corner) to review all modified configuration in temporary memory

Hints:

- You should click **Submit** to submit all changes on the same configuration page.
- You may click **Save & Apply** to apply all submitted change at the end of configuration



4.1. Basic Configurations

This section covers the basic configuration on A8n (ac) Series products.

4.1.1. Synchronize AP's system clock with NTP

server

NTP Setting	
IP Address Type:	● IPv4 O IPv6
NTP Server IP:	0.pool.ntp.org
NTP Polling Interval:	600 @ (15-86400s)
NTP Time Zone:	Asia/Hong Kong
Daylight Saving Time:	
Figure	15 – NTP Setting

- 1. Go to **Configuration** > **System**
- 2. Change the following settings:

NTP Server IP – Type in either the domain name / IP address of NTP server which you want to synchronize with.

NTP Polling Interval – Type in the interval in second between each synchronization request from the AP to NTP server. The default setting is 600 seconds

NTP Time Zone – Select the appropriate time zone. The default setting is Asia/Hong Kong

Daylight Saving Time – Select the checkbox if your place has daylight saving time

- 3. Click **Submit**
- 4. Click Save & Apply

Note:

- IP Address Type is changed by AP automatically based on whether IPv6 is enabled or not
- If providing NTP server's domain name in **NTP Server IP**, you must provide valid DNS server information (see 4.1.2 on page 15 for more detail). Otherwise, NTP setting cannot take effect.



4.1.2. Assign Internet Connection Type for AP (IPv4)

– Static / DCHP

WAN Setting(IPv4)	
Internet Connection Type:	Static 🗸
IPv4 Address:	10 . 6 . 122 . 101
IPv4 Subnet Mask:	255 . 255 . 255 . 0
IPv4 Default Gateway:	10 . 6 . 122 . 1
IPv4 DNS Server IP Address:	10.6.127.4

Figure 16 – WAN Settings (IPv4)

- 1. Go to Configuration > Network > General > WAN Settings
- 2. Change the following settings:

Internet Connection Type – configure AP either as a client with fixed IP address or DCHP client;

- Static Stand for Static IP addressing; AP will not update its IP address automatically
- DHCP Client Require an IP address from DCHP server on the network; AP renews its IP address periodically

IPv4 Address –Type in an IP address for AP (Static Internet Connection Type only)

IPv4 Subnet Mask – Type in a subnet mask for AP (Static Internet Connection Type only)

IPv4 Default Gateway – Type in an IP address of default gateway for AP (Static Internet Connection Type only)

IPv4 DNS Server – Type in IP address of one or more DNS server for AP (Static Internet Connection Type only).

Note:

- Click 🛄 for adding more DNS;
- Click 📧 to remove existing DNS server entry
- 3. Click **Submit**
- 4. Click Save & Apply



4.1.3. Configure Radio Interface as Access Point (AP)

Radio 0 – 2.4GHz Radio

Radio General Configuration

ALTAI			
Status Configuration Administration To System Network Wireless Thin AP	ois adout		
Radio0(2.4G) - Radio1(5G)			
F	Radio0(2.4G) Setting		
General WLAN Advanced QoS			Submit
Enable Radio:			
Radio Mode:	AP	•	
Country Code:	HONG KONG	v	
Wireless Mode:	2.4GHz 144Mbps(802.11ng HT20)	•	
Legacy 11b Data Rate Support:	1/2/5.5/11M (Best compatibility/Poor perf	ormar 🔻	
Radio Frequency:	Auto	•	
Transmit Power:	27	•	
Maximum Clients:	512	(1-512)	
User Isolation in different WLAN (SSID):		``````````````````````````````````	
Periodic Auto channel Selection:			
Schedule Mode:	Sun Mon Tues Wed Thur		
	□ Fri □ Sat 00:00 ▼		
Periodic Mode:	0	(Mins)	
Brees Ontertaction	0-1440Mins, 0 means Periodic mode disabled.		
Range Opumization:	Auto	•	
Sector Power Control:	S		
Sector	State	Secto	r Power
0	🖲 On 🔍 Off	25	•
1	On Off	25	•
2	● On ○ Off	25	•
3		20	×
			Submit

Figure 17 – Radio0 (2.4G) General Settings of AP

- 1. Go to Configuration > Wireless > Radio0(2.4G) > General;
- 2. Select **Enable Radio** checkbox to enable radio interface
- 3. Select AP in Radio Mode
- Change the following settings: Country Code – Select an option that matches your device's installation location; Hong Kong is the default setting.



Note:

- Country code enforces regulatory restrictions on radio frequencies and maximum transmission power that the AP can operate in.

Wireless Mode - Select suitable Wi-Fi operating mode for the AP;

2.4G 11Mbps (802.11 b) 2.4G 54Mbps (802.11 bg) 2.4G 54Mbps (802.11 g-only) 2.4G 144Mbps (802.11 ng HT20); Default Setting 2.4G 144Mbps (802.11 n-only HT20) 2.4G 300Mbps (802.11 ng HT40+) 2.4G 300Mbps (802.11 n-only HT40+) 2.4G 300Mbps (802.11 ng HT40-) 2.4G 300Mbps (802.11 n-only HT40-)

Legacy 11b Data Rate Support [Optional] – Select a suitable option for the legacy client compatibility. In order to enhance the spectrum efficiency, low data rates (1/2/5.5/11M) should be eliminated. The options include:

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

Note:

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

Radio Frequency – Choose the operating channel for the radio interface; AP selects the channel with the least amount of interference if Auto is selected. An optional feature **Periodic Auto channel Selection** will be shown if Auto is selected. 2412MHz (Channel 1) is the default setting

Note:

- Select the radio frequency based on the result of channel scan is recommended

Transmission Power – Select the total transmission power for the radio interface.

Maximum Client – Specify the maximum associated client between 1 and 512 that the radio interface serves. 512 is the default setting.



Disable HT20/HT40 Auto Switch [Optional] – If select the checkbox, AP will NOT switch the channel width between 20 MHz and 40 MHz automatically. This option is only available if any wireless mode with HT40+/- is selected.

User Isolation in different WLAN (SSID) [Optional] - Select the checkbox to block the users' communication across different SSID in the AP directly.

Periodic Auto Channel Section [Optional] – Select the checkbox to enable a scheduled channel selection task on the radio interface.

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

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

Range Optimization [Optional] – Select a coverage range for optimization. 'Auto' is the default value.

Sector Power Control [Optional] – Select the checkbox to enable a feature to assign a transmitting power for each sector.

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



WLAN List

	Status	Configuration	Administra	tion	Tools	About					
/ste		Padio1(5C)	in ap								
	100(2.40)	<u>Radio1(54)</u>			Radio0	(2.4G) Setting					
	General	WLAN Advanced	d QoS	WEP							
M	LAN Con	figuration									
	Enable WLAN	SSID	Max Clients	Isolation	Auth Mode	Access Traffic Right	WL Uplink/E Con	AN Downlink trol	Static Uplink/Do Contr	on wnlink ol	Detail
	V 0	Superwifi Networ Hide SSID	256		open	Full Access	0	0		0	More
		Superwifi Networ Hide SSID	256		open	Full Access	0	0	0	0	More
	2	Superwifi Networ Hide SSID	256		open	Full Access	0	0	0	0	More
	3	Superwifi Networ Hide SSID	256		open	Full Access	0	0	0	0	More
	4	Superwifi Networ Hide SSID	256		<u>open</u>	Full Access	0	0	0	0	More
	5	Superwifi Networ Hide SSID	256	\checkmark	<u>open</u>	Full Access	0	0	0	0	More
	6	Superwifi Networ Hide SSID	256		<u>open</u>	Full Access	0	0	0	0	More
	7	Superwifi Networ Hide SSID	256		<u>open</u>	Full Access	0	0	0	0	More
	8	Superwifi Networ Hide SSID	256		<u>open</u>	Full Access	0	0	0	0	More
	9	Superwifi Networ Hide SSID	256		open	Full Access	0	0	0	0	More
	10	Superwifi Networ Hide SSID	256		open	Full Access	0	0	0	0	More
	□ 11	Superwifi Networ Hide SSID	256		open	Full Access	0	0	0	0	More
	12	Superwifi Networ Hide SSID	256		open	Full Access	0	0	0	0	More
	□ 13	Superwifi Networ Hide SSID	256	\checkmark	<u>open</u>	Full Access	0	0	0	0	More
	14	Superwifi Networ Hide SSID	256		<u>open</u>	Full Access	0	0	0	0	More
	□ 15	Superwifi Networ Hide SSID	256		<u>open</u>	Full Access	0	0	0	0	More
											Submit

Figure 18 – WLAN List of Radio0(2.4G) of AP

- 1. Go to Configuration > Wireless > Radio0(2.4G) > WLAN
- 2. Select **Enable WLAN** checkbox to enable the WLAN 0 15 individually;

Note:

- A8n (ac) products support up to 16 WLANs on its Radio0

- 3. Click **Submit**
- 4. Click Save & Apply



WLAN 0-15 General Configuration

Status	Configuration	Administration	Tools	About				
System Netwo	rk Wireless 7	Thin Ap						
<u>Radio0(2.4G)</u>	- <u>Radio1(5G</u>	D)						
		R	adio0(2.4	4G) WLAN) Setting			
WLAN Gene	ral WLAN Sec	urity Rogue Station	QoS	Bandwidth Co	ontrol			
		Enable W	AN: 💌					
		Hide \$	SID:					
		s	SID: Superv	vifi Network 0				
		User Isola	tion: 🕑					
		OHCP Trusted	Port: 🗌					
		Access Traffic R	ight: Full A	ccess		T		
		Max Clie	ents: 512			(1-512)		
Station Ass	ociation Requir	rement						
	Reject Station As	ssociation if SNR less	than 0 (0-100d	B, 0:Disable)	dB.			
[)isassociate Stati	on if SNR drops more	than 0 (0-100d	В)	dB for consecutive 10 (1-256	5)	packets.	
						Back to \	WLAN List	Submit

Figure 19 – WLAN Detail Settings of WLAN 0 of AP

- 1. Go to Configuration > Wireless > Radio0(2.4G) > WLAN 0-15 > More...
- 2. Change the following settings:

Hide SSID [Optional] – Select the checkbox to hide SSID name from its beacon frame

SSID – Provide a unique name for the particular WLAN

Note:

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

User Isolation [Optional] – Select the checkbox to block user communication within the same SSID in the AP directly.

DHCP Trust Port [Optional] - Deselect the checkbox to prevent illegal DHCP servers offering IP address to DHCP clients via this WLAN.

Access Traffic Right – Specify the privilege of associated clients;

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

Max Clients - Specify the maximum associated clients between 1 and 512 on this WLAN. 512 is the default setting.

Note:

- Max Clients in WLAN 0 – 15 MUST be smaller than or equal to (\geq) the Max Clients setting in 0 Radio General Configuration



Station Association Requirement [Optional] – Specify and additional requirement on Signal Strength to Noise Ratio (SNR) for associated clients.

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

Notes:

- Example for Station Association Requirement with the following settings:

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

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

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

- 3. Click **Submit**
- 4. Click Save & Apply



WLAN 0-15 Security Configuration

Status	Configuration	Administration	Tools	About				
System Netwo	rk Wireless	Thin AP						
Radio0(2.4G)	- <u>Radio1(5</u>	<u>G)</u>						
			Radio0(2.	4G) WLAN	0 Setting			
WLAN Gene	ral WLAN Se	curity Rogue Stat	tion List QoS	Bandwidth C	ontrol			
WLAN Secu	rity Setting							
		Authentication	n Mode: Open		~	·		
		Ciphe	r Mode: Disab	led	~	1		
ACL Setting	I							
		Access Cont	rol List: Enabl	ed - Default Allo	w 🗸	ŕ		
		ACL Input I	Method: 💿 Mar	nual Input	File			
		Denied MAC A	ddress:			1		
							Back to WI AN List	Submit
							Dack to WEAN LIST	Submit

Figure 20 – WLAN Security Setting for WLAN 0 of AP

Configure WLAN as Open network

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

Status	Configuration	Administration	Tools	About				
System Netwo	rk Wireless 1	- Thin Ap						
Radio0(2.4G)	- <u>Radio1(50</u>	<u>5)</u>						
			Radio0(2.4	4G) WLAN	0 Setting			
WLAN Gene	ral WLAN Sec	urity Rogue Sta	tion List QoS	Bandwidth C	Control			
WLAN Secu	rity Setting							
		Authenticatio	n Mode: Open		•	~		
		Ciphe	er Mode: Disabl	ed		~		
ACL Setting	I							
		Access Cont	rol List: Enable	ed - Default Allo	w	~		
		ACL Input	Method: 💿 Man	ual Input	File			
		Denied MAC A	ddress:					
							Back to WLAN List	Submit

Figure 21 – Open network of AP

- 1. Go to Configuration > Wireless > Radio0(2.4G) > WLAN > WLAN 0-15 > WLAN Security
- 2. Select Open in Authentication Mode
- 3. Select Disabled in Cipher Mode
- 4. Click **Submit**
- 5. Click Save & Apply



Configure WLAN as Open network with WEP encryption

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

Status Configuration Administration Too	vis About
System Network Wireless Thin AP	
Radio0(2.4G) - Radio1(5G)	
Radio	00(2.4G) WLAN0 Setting
WLAN General WLAN Security Rogue Station List	QoS Bandwidth Control
WLAN Security Setting	
Authentication Mode:	Open v
Cipher Mode:	WEP •
Default WEP Key:	1 (1-4)
Key Entry Method:	O Ascii Text
WEP Key 1:	Show
WEP Key 2:	Show
WEP Key 3:	Show
WEP Key 4:	Show
ACL Setting	
Access Control List:	Enabled - Default Allow
ACL Input Method:	Manual Input
Denied MAC Address:	
	j==
	Back to WLAN List Submit

Figure 22 – Open network with WEP encryption of AP

- 1. Go to Configuration > Wireless > Radio0(2.4G) > WLAN > WLAN 0-15 > WLAN Security
- 2. Select Open in Authentication Mode
- 3. Select WEP in Cipher Mode
- 4. Select key number 1 4 in Default WEP Key
- 5. Select Key Entry Method

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

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



Configure WLAN with Shared Key Authentication

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

Status Configuration Administration Too	ols About
System Network Wireless Thin AP	
Radio0(2.4G) - Radio1(5G)	
Radio	o <mark>0(2.4G) WLAN0</mark> Setting
WLAN General WLAN Security Rogue Station List	QoS Bandwidth Control
WLAN Security Setting	
Authentication Mode:	Shared v
Cipher Mode:	WEP
Default WEP Key:	1 (1-4)
Key Entry Method:	
WED Key 1	
WEP Rey 2:	Show
WEP Key 3:	Show
WEP Key 4:	Show
ACL Setting	
Access Control List:	Enabled - Default Allow
ACL Input Method:	Manual Input Gile
Denied MAC Address:	
	Back to WLAN List Submit

Figure 23 – Shared Key Authentication of AP

- Go to Configuration > Wireless > Radio0(2.4G) > WLAN > WLAN 0-15 > WLAN Security
- 2. Select Shared in Authentication Mode
- 3. Select WEP in Cipher Mode
- 4. Select key number 1 4 in **Default WEP Key**
- 5. Select **Key Entry Method** Ascii Text key is encoded as ASCII characters (0–9, a–z, A–Z) Hexadecimal key is encoded as Hexadecimal characters (0–9, A–F)
- Type in up to four keys in WEP Key 1, WEP Key 2, WEP Key 3 and WEP Key 4 respectively. You can type either up to 5 Ascii characters or up to 10 Hexadecimal characters as WEP Key
- 7. Click **Submit**
- 8. Click Save & Apply



Configure WLAN with WPA / WPA2 / WPA-auto Authentication

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

Status Configuration Admini	stration To	ols Ab	out		
rstem Network Wireless Thin AP					
adio0(2.4G) - Radio1(5G)					
	Radi	00(2.4G) W	<mark>/LANO</mark> Setti	ng	
WLAN General WLAN Security	Roque Station List	QoS Band	width Control		
WLAN Security Setting	2	11 - 11			
	hantication Mode				
Au	nenucation mode:	WPA2		\checkmark	
	Cipher Mode:	AES		\checkmark	
Group Ke	y Update Interval:	86400		(s)	
RADIUS Server Setting					
	NAS Identifier:			(0-32)	
RADIUS Server	IP Address Type:	IPv4 ()	IPv6		
PADI	IIS Potry Timoout:	200	11 40		
(AD)	os keuy mileout.	(0-65535 s)			
	IP Addr	ess	Port		Secret(1-128)
RADIUS Server 0	.0.0	. 0	1812		Show
Secondary RADIUS Server 0	.00	- 0	1812		Show
RADIUS Accounting Server Setting	3				
RADIUS Accounting Server	IP Address Type:	● IPv4 O	IPv6		
Accountin	ıg interim Interval:	300			
		🦉 (60-86400s, ():Disabe)		
		IP Address		Port	Secret(1-128)
RADIUS Accounting Server	0.0	.0.	0 1813		Show
Secondary RADIUS Accounting Se	rver 0 . 0	.0.	0 1813		Show
ACL Setting					
Ac	cess Control List:	Enabled - Defa	ult Allow	~	
	CL Input Methods		0.5%		
-	ACL Input Method:	Manual Input O File			
Den	ied MAC Address:				
					Back to WLAN List Submit

Figure 24 – WPA2 setting of AP

- Go to Configuration > Wireless > Radio0(2.4G) > WLAN > WLAN 0-15 > WLAN Security
- 2. Select WPA / WPA2 / WPA-auto in Authentication Mode
- 3. Select suitable encryption mode in **Cipher Mode** as the followings: If Authentication Mode is WPA:

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

TKIP - This algorithm provides greater compatibility with older client devices, but is not supported by the 802.11n standard.

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

If Authentication Mode is WPA2:

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



If Authentication Mode is WPA-auto:

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

Note:

- TKIP is not supported by 802.11n standard. If selected TKIP, the 802.11n's devices will be limited to 802.11g transfer rate, i.e. up to 54 Mbps
- 4. Provide suitable identification in **NAS identifier**. Remote RADIUS server use this ID to identify its clients [WPA or WPA2 only]
- 5. Provide transmission timeout interval between 0 and 86400s in **RADIUS Retry Timeout** [Optional]. 300 is default setting.
- 6. Provide IP address of remote RADIUS server for authentication in IP Address of RADIUS Server
- 7. Provide service port of remote RADIUS server in **Port of RADIUS Server**. 1812 is default setting.
- 8. Provide suitable secrets in **Secret of RADIUS Server**. It is used along with the MD5 hashing algorithm to obfuscate passwords. This secret MUST be as the same as that in RADIUS server.
- 9. Repeat step 7-9 if the backup RADIUS server is available.
- 10. RADIUS Accounting Server Setting is optional; you may select if the WLAN requires accounting service from remote RADIUS server. You can change the following settings:

Accounting interim Interval - indicates the number of seconds between each interim update in seconds; 300 is default setting.

IP Address - IP address of remote RADIUS Accounting Server **Port** - Service port of remote RADIUS server for accounting service. *1813* is default setting.

Secret - Password MUST be as the same as that in RADIUS server

11.Click **Submit**

12. Click Save & Apply



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

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

Status Configuration Administration Too	ols About
System Network Wireless Thin AP	
Radio0(2.4G) - Radio1(5G)	
Radi	o0(2.4G) WLAN0 Setting
WLAN General WLAN Security Rogue Station List	QoS Bandwidth Control
WLAN Security Setting	
Authentication Mode:	WPA2-PSK
Cipher Mode:	AES
Group Key Update Interval:	86400 (s)
Pass Phrase:	Show
	(8-64)
ACL Setting	
Access Control List:	Enabled - Default Allow
ACL Input Method:	Manual Input O File
Denied MAC Address:	<u> </u>
	Back to WLAN List Submit

Figure 25 – WPA2-PSK Setting of AP

- 1. Go to Configuration > Wireless > Radio0(2.4G) > WLAN > WLAN 0-15 > WLAN Security
- 2. Select WPA-PSK / WPA2-PSK / WPA-auto-PSK in Authentication Mode
- 3. Select suitable encryption mode in **Cipher Mode** as the followings: If Authentication Mode is WPA-PSK:

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

TKIP - This algorithm provides greater compatibility with older client devices, but is not supported by the 802.11n standard.

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

If Authentication Mode is WPA2-PSK:

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

If Authentication Mode is WPA-auto-PSK:

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

Note:

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



- 4. Provide time in second in **Group Key Update Interval** [Optional]. 86400 is default setting.
- 5. Type in a string between 8 and 64 characters long in **Pass Phrase** that users will use to connect to the wireless network.
- 6. Click **Submit**
- 7. Click Save & Apply

Configure WLAN with WAPI Authentication

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

Status Configuration Administration Too	ols About				
ystem Network Wireless Thin AP					
adio0(2.4G) - Radio1(5G)					
Radi	o0(2.4G) WLAN0 Setting				
WLAN General WLAN Security Roque Station List	QoS Bandwidth Control				
WLAN Security Setting					
Authoritation Mode: Luco					
Authentication mode.	WAPI				
Cipher Mode:	SMS4				
Certificate Type:	X.509				
Certificate Status:	Ready to Install				
Certificate Mode:	Two-Cert				
Certificate Management:					
continente munagement.	Install Certificate				
AS IP Address:					
AS Port:	3810				
	(0-65535)				
Unicast Key Update Interval:	86400				
	• (60-214/48364/)				
Multicast Key Update Interval:	86400				
ACL Setting	(00 210 1000 //)				
Access Control List:					
Access Control List.					
ACL Input Method:	Manual Input O File				
Denied MAC Address:	<u> </u>				
	Back to WLAN List Submit				

Figure 26 – WAPI Settings of AP

- 1. Go to Configuration > Wireless > Radio0(2.4G) > WLAN > WLAN 0-15 > WLAN Security
- 2. Select WAPI in Authentication Mode
- 3. Select SMS4 in Cipher Mode
- 4. Select suitable option in **Certificate Mode**:
- Two-Cert Wi-Fi client is verified by the certification from authentication server (AS) and Access Point (AP) Three-Cert - Wi-Fi client is verified by the certification from authentication server (AS), access point (AP), and certificate authority (CA)
- 5. Click **Install Certificate**; a window for installing certificate is shown (see Figure 27 and Figure 28)




AS Certificat	te:		
Choose file	No file chosen		Upload
AP Certificat	te:		
Choose file	No file chosen		Upload
Install			
Figure 27 – Two	-Cert Mode Ce	ertification	Installation
AS Certificat	te:		
Choose file	No file chosen		Upload
AP Certificat	te:		
Choose file	No file chosen		Upload
CA Certifica	te:		
Choose file	No file chosen		Upload
Install			

Figure 28 - Three-Cert Mode Certification Installation

- 6. Click Browse to select suitable certifications
- 7. Click Upload to upload the selected certifications to A8n (ac)
- 8. Click Install to install certifications
- 9. Type IP address of AS server in AS IP Address
- 10. Type service port of AS server in AS Port
- 11. Enter interval time between 60 and 2147483647s in **Unicast Key Update Interval** [Optional]; 86400 is default setting
- 12. Enter interval time between 60 and 2147483647s in **Multicast Key Update Interval** [Optional]; 86400 is default setting
- 13. Click **Submit**
- 14. Click Save & Apply



Configure WLAN with WAPI-PSK Authentication

Radio0(2.4G) WLAN0 Setting								
WLAN Security Rogue Station List	QoS Bandwidth Control							
etting								
Authentication Mode:	WAPI-PSK	~						
Cipher Mode:	SMS4	\checkmark						
PassPhrase:	(9.54)	Sho	w					
Unicast Key Update Interval:	86400 (60-2147483647)							
Multicast Key Update Interval:	86400 (60-2147483647) 							
Access Control List:	Enabled - Default Allow	$\overline{}$						
ACL Input Method:	Manual Input O File							
Denied MAC Address:		<u> </u>						
			Back to W					

Figure 29 – WAPI-PSK Setting of AP

- Go to Configuration > Wireless > Radio0(2.4G) > WLAN > WLAN 0-15 > WLAN Security
- 2. Select WAPI in Authentication Mode
- 3. Select SMS4 in Cipher Mode
- 4. Type in a string between 8 and 64 characters long in **Pass Phrase** that users will use to connect to the wireless network.
- 5. Enter interval time between 60 and 2147483647s in **Unicast Key Update Interval** [Optional]; 86400 is default setting
- 6. Enter interval time between 60 and 2147483647s in **Multicast Key Update Interval** [Optional]; 86400 is default setting
- 7. Click Submit
- 8. Click Save & Apply



Radio 1 – 5GHz Radio

Status Configuration Administration Too	ls About
System Network Wireless Thin AP	
Radio0(2.4G) - Radio1(5G)	
	Radio1(5G) Setting
General WLAN Advanced QoS	
Enable Radio:	
Radio Mode:	AP 🔻
Country Code:	HONG KONG
Wireless Mode:	5GHz 866.7Mbps(802.11ac HT80)
Dynamic Radio Frequency Selection(DFS):	
Radio Frequency:	Auto
Transmit Power:	5
	The effective Tx Power may be different, depends on the selected Channel.
Maximum Clients:	512 (1-512)
User Isolation in different WLAN (SSID):	
Periodic Auto channel Selection:	
Schedule Mode:	Sun Mon Tues Wed Thur
	Fri Sat 00:00 •
Periodic Mode:	0 (Mins)
	0-1440Mins, 0 means Periodic mode disabled.
	Submit

Figure 30 – Radio1 (5G) General Setting of AP

Radio General Configuration

- 1. Go to Configuration > Wireless > Radio1(5G) > General
- 2. Select Enable Radio checkbox to enable radio interface
- 3. Select AP in **Radio Mode**
- 4. You can change the following settings:

Country Code – Select an option that matches your device's installation location; *Hong Kong* is the default setting.

Note:

 Country code sets the regulatory domain for the radio frequencies and maximum transmission power that AP can use

Wireless Mode – Select suitable Wi-Fi operating mode for the AP:

5G 54Mbps (802.11 a) 5G 144Mbps (802.11 na HT20); Default Setting 5G 144Mbps (802.11 n-only HT20) 5G 300Mbps (802.11 n-only HT40+) 5G 300Mbps (802.11 na HT40+) 5G 300Mbps (802.11 na HT40-) 5G 300Mbps (802.11 n-only HT40-) 5G 173Mbps (802.11 ac HT20) 5G 400Mbps (802.11 ac HT40+)



5G 400Mbps (802.11 ac HT40-) 5G 866.7Mbps (802.11 ac HT80)

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

Note:

- Radio Frequency is set as auto if DFS is enabled

Radio Frequency – Choose the operating channel for the radio interface; AP selects the channel with the least amount of interference if *Auto* is selected. 5180*MHz* (*Channel* 36) is the default setting

Transmission Power – Select the total transmission power for the radio interface.

Maximum Client [Optional] – Specify the maximum associated client between 1 and 512 that the radio interface serves. 512 is the default setting.

Disable HT20/HT40 Auto Switch [Optional] – If select the checkbox, AP will NOT switch the channel width between 20 MHz and 40 MHz automatically. This option is only available if any wireless mode with 802.11n-only/na HT40+/- is selected.

User Isolation in different WLAN (SSID): [Optional] - Select the checkbox to block the users' communication across different SSID in the AP directly.

Periodic Auto channel Section [Optional] – Select the checkbox to enable scheduled channel selection task on the radio interface:

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

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

5. Click **Submit**

6. Click Save & Apply



W	LAN	List
---	-----	------

Status System Ne	Configuration	Administrat n AP	ion Ti	pols	About						CPU Load: 1.11, 1.08, 1 Uptime: 03h 13min (<u>Changes</u> <u>Download Le</u>
Radio0(2.4G)	- <u>Radio1(5G)</u>										
Ceneral	WLAN Advanced	Oos		Radio1	(5G) Setting					Submit	
WLAN C	onfiguration										
Enable WLAN	SSID	Max Clients	Isolation	Auth Mode	Access Traffic Right	Wi Uplink/i Coi	LAN Downlink htrol	Stal Uplink/D Con	tion)ownlink trol	Detail	
≥ 0	Superwifi Networ Hide SSID	512	۲	open	Full Access V	0	0	0	0	More	
□ 1	Superwifi Networ Hide SSID	512	۲	open	Full Access	0	0	0	0	More	
2	Superwifi Networ Hide SSID	512		open	Full Access 🔻	0	0	0	0	More	
3	Superwifi Networ Hide SSID	512	۲	open	Full Access	0	0	0	0	More	
4	Superwifi Networ Hide SSID	512	۲	open	Full Access 🔻	0	0	0	0	More	
5	Superwifi Networ Hide SSID	512	۲	<u>open</u>	Full Access	0	0	0	0	More	
6	Superwifi Networ Hide SSID	512	۲	open	Full Access V	0	0	0	0	More	
7	Superwifi Networ Hide SSID	512	e	open	Full Access	0	0	0	0	More	
8	Superwifi Networ Hide SSID	512		open	Full Access 🔻	0	0	0	0	More	
9	Superwifi Networ Hide SSID	512	e	open	Full Access	0	0	0	0	More	
10	Superwifi Networ Hide SSID	512		open	Full Access 🔻	0	0	0	0	More	
11	Superwifi Networ	512	۲	open	Full Access 🔻	0	0	0	0	More	
12	Superwifi Networ Hide SSID	512		open	Full Access 🔻	0	0	0	0	More	
13	Superwifi Networ Hide SSID	512		open	Full Access 🔻	0	0	0	0	More	
14	Superwifi Networ Hide SSID	512		open	Full Access	0	0	0	0	More	
□ 15	Superwifi Networ Hide SSID	512	ø	open	Full Access V	0	0	0	0	More	
										Submit	

Figure 31 – WLAN list on Radio1(5G) of AP

- 1. Go to Configuration > Wireless > Radio1(5G) > WLAN
- 2. Please refer to WLAN List on page 19 for more detail.

WLAN 0 - 15 General Configuration

- 1. Go to Configuration > Wireless > Radio1(5G) > WLAN 0-15 > More...
- 2. Please refer to WLAN 0-15 General Configuration on page 20 for more detail.

WLAN 0 - 15 Security Configuration

- Go to Configuration > Wireless > Radio1(5G) > WLAN > WLAN 0-15 > WLAN Security
- Please refer to the following chapters for more detail: Configure WLAN as Open network (see Configure WLAN as Open network on page 22)

Configure WLAN as Open network with WEP encryption (see Configure WLAN as Open network with WEP encryption on page 23)



Configure WLAN with Shared Key Authentication (see Configure WLAN with Shared Key Authentication on page 24)

Configure WLAN with WPA / WPA2 / WPA-auto Authentication (see Configure WLAN with WPA / WPA2 / WPA-auto Authentication on page 25)

Configure WLAN as with WPA-PSK / WPA2-PSK / WPA-auto-PSK Authentication (see Configure WLAN with WPA-PSK / WPA2-PSK / WPA-auto-PSK Authentication on page 27)

Configure WLAN with WAPI Authentication (see Configure WLAN with WAPI Authentication on page 28)

Configure WLAN with WAPI-PSK Authentication (see Configure WLAN with WAPI-PSK Authentication on page 30)

4.1.4. Configure Radio Interface as Station (STA/CPE)

Radio 0 – 2.4GHz Radio

Station radio mode is not available in Radio 0(2.4G) interface.

Radio 1 – 5GHz Radio

Status Configuration Administration Tor System Network Wireless Thin AP	Status Configuration Administration Tools About System Network Wireless Thin AP						
Radio0(2.4G) - Radio1(5G) General WUAN Advanced QoS WEP	Radio1(5G) Setting						
Enable Radio Radio Mode: Country Code: Dynamic Radio Frequency Selection(DF 5): Transmit Power:	Station HONG KONG 17 Submit						
		L ₈					

Figure 32 – Radio 1 General Setting of Station

Radio General Configuration

- 1. Go to Configuration > Wireless > Radio1(5G) > General
- 2. Select Enable Radio checkbox to enable radio interface
- 3. Select Station in Radio Mode
- 4. Change the following settings:



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

- Radio Frequency is set as auto if DFS is enabled

Transmission Power – Select the total transmission power for the radio interface.

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



Station Configuration

Status Configuration System Network Wireless Radioo(2.4G) - Radio1(50	Administration Tools Thin AP 2) Radio 1	About (5G) Setting		驚法主文 Reboot.A2 Loscout Firmmens Venior 2.3.0.54 (2011.sch 0.06, 0.04, 0.00 Uptime: PH 0.25min 65 Unsaved Chances: Z Save & Acely Download Lose
General Station Advar	nced WEP			
WLAN ID	Remote SSID	Auth Mode	Detail More	
			Submit	
	₹.			
Status Configuration System Network Wireless Radio0(2.4G) - Radio1(5G	Administration Tools Then AP) Radio1(5G)	About :WLANO Setting		董年文 Reboot AP Loosed Firmware Version 2.0.056 U Load 013 0.068, 0.01 U Load 013 0.068, 0.01 Unsaved Changes Z Save & Ageby Download Loga
WLAN General WLAN Sec	urity QoS			
General Setting		Roaming Setting		
WLAN Mode: s	itation	Enable Roaming:	D.C.	
Remote SSID:	Johnark 0	Scan SNR ureshold:	(0-100dB)	
Preferred AP0 Mac:		Roaming SNR threshold:	30	
Preferred AP1 Mac:		Max Scan Interval	• (0-100dB)	
Preferred AP2 Mac:		mux soun fillerval.	(1-3600s)	
		Min Scan Interval:	10 (1-60s)	
		Scan SNR Fluctuation	5	
		Threshold:	(0-10dB)	
		Roaming Hysteresis:		<u>∫</u> _g
		Background scan channel:	State	
			Back to Station List Submit	

Figure 33 - Station Setting

- 1. Go to Configuration > Wireless > Radio1(5G) > Station > <u>More...</u>
- 2. Change the following settings:

Lock AP Mac [Optional] – Select to force station that associate the AP with MAC address in **Remote AP MAC** only

Remote SSID – Enter the SSID that station is going to associate. You may use **[Scan]** to look for the surrounding SSID.

Status	Configurat	tion Administration	Tools	About			
System Ne	etwork Wirele	ss ⊨ Thin AP					
<u>Radio0(2.4G</u>	<u>)</u> - <u>Radio</u>	<u>1(56)</u> Ra	dio1(5G)·W		an Rocult		
Go to prev	vious page, plea	ise click <u>Back</u>	ulo1(50).W	LANG AF SC	an Result		Refresh
	SSID	MAC Address	Encryption	Signal Level(dBm)	SNR(dB)	Frequency(GHz)	Channel
	myAX-A3c-5	00:19:be:a3:07:47	aes	-84	19	5.745	149
Select							





Preferred AP0 / AP1 / AP2 Mac [Optional] – Enter up to three AP MAC addresses that station associates them preferentially. AP0 is the highest priority.

Roaming Setting [Optional]

Enable Roaming - Select to enable roaming on station

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

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

Note:

 Scan SNR Threshold MUST be larger than (>)Roaming SNR Threshold

Max Scan Interval - Specify the maximum duration from 1s to 3600s for channel scanning; 60s is default setting.

Min Scan Interval - Specify the minimum duration from 1s to 60s for channel scanning; 10s is default setting

Scan SNR Fluctuation Threshold – Enter SNR from 0dB to 10dB; the current AP's signal fluctuation (compared with previous scan result) is higher than (>) this threshold, the station will do scanning. 5dB is default setting.

Roaming Hysteresis – Select to enable that station will be stickier to current associated AP.

Scan Channel List – Select the particular channel for scan

- 3. Click **Submit**
- 4. Click **Save & Apply**

Station Security Configuration

Satus Configuration Administration Tools About	養性中文 Reboot AP Logout Firmware Version: 2.0.0.504 CPU Load: 0.05, 0.04, 0.00 Uptime: 040 Primi 595 Unsaved Changes: 2 Save & Apply Download Loge
System Network Wireles Thin AP Radio0(2.4G) - Radio1(5G) Radio1(5G):WLANO Setting WLAN General WLAN Security QOS Authentication Mode: Open Cipher Mode: Disabled Back to Station List Submit	
3	ý.

Figure 35 – Security Settings of Station



Configure Station to associate Open network

- Go to Configuration > Wireless > Radio1(5G) > Station > WLAN Security
- 2. Select Open in Authentication Mode
- 3. Select Disabled in Cipher Mode
- 4. Click Submit
- 5. Click Save & Apply

Configure Station to associate Open network with WEP encryption

Status Configuration Administration To	vis About
System Network Wireless Thin AP	
Radio0(2.4G) - Radio1(5G)	
Rad	io1(5G):WLAN0 Setting
WLAN General WLAN Security QoS	
Authentication Mode:	Open T
Cipher Mode:	WEP v
Default WEP Key:	1 (1-4)
Key Entry Method:	O Ascii Text
WEP Key 1:	Show
WEP Key 2:	Show
WEP Key 3:	Show
WEP Key 4:	Show
	Desists Obstan List Outwith
	Back to Station List Submit

Figure 36 – Open network with WEP of Station

- Go to Configuration > Wireless > Radio1(5G) > Station > WLAN Security
- 2. Select Open in Authentication Mode
- 3. Select WEP in Cipher Mode
- 4. Select key number 1 4 in Default WEP Key
- 5. Select Key Entry Method

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

- Type in up to four keys in WEP Key 1, WEP Key 2, WEP Key 3 and WEP Key 4 respectively. You can type either up to 5 Ascii characters or up to 10 Hexadecimal characters as WEP Key
- 7. Click **Submit**
- 8. Click Save & Apply



	Configure Station to	associate network	with Shared Ke	v authentication
--	----------------------	-------------------	----------------	------------------

Status	Configuration	Administration	Tools	About			
System Netwo	rk Wireless						
Radio0(2.4G)	- <u>Radio1(5G</u>)					
			Radio1(5	<mark>G):WLANO</mark>	Setting		
WLAN Gene	ral WLAN Sec	curity QoS					
		Authentication	Mode: Shared	ł		T	
		Cipher	Mode: WEP			•	
		Default WE	P Key: 1			(1-4)	
		Key Entry M	Method: 🔘 Ascii	Text 🖲 Hexa	decimal		
		WEP	Key 1:			Show	
		WEP	Key 2:			Show	
		WEP	Key 3:			Show	
		WEP	Key 4:			Show	
						Back to Station List	Submit

Figure 37 - Shared Key Authentication of Station

- Go to Configuration > Wireless > Radio1(5G) > Station > WLAN Security
- 2. Select Shared in Authentication Mode
- 3. Select WEP in Cipher Mode
- 4. Select key number 1 4 in **Default WEP Key**
- 5. Select **Key Entry Method** Ascii Text key is encoded as ASCII characters (0–9, a–z, A–Z) Hexadecimal key is encoded as Hexadecimal characters (0–9, A–F)
- 6. Type in up to four keys in **WEP Key 1**, **WEP Key 2**, **WEP Key 3** and **WEP Key 4** respectively. You can type either up to 5 Ascii characters or up to 10 Hexadecimal characters as WEP Key
- 7. Click **Submit**
- 8. Click Save & Apply

Configure Station to associate network with WPA / WPA2 authentication

aomenication			
Status Configuration Administration To	ols About		
System Network Wireless Thin AP			
Radio0(2.4G) - Radio1(5G)			
Rad	lio1(5G):WLAN0 Sett	ting	
WLAN General WLAN Security QoS			
Authentication Mode:	WPA2	T	
Cipher Mode:	AES	¥	
EAP Method:	PEAP-MSCHAPV2	¥	
Username:	Length:0-128(Ascii Characters)		
Password:	Lendth:0-128(Ascii Characters)	Show	
		Back to Station List	Submit

Figure 38 – WPA2 Authentication of Station



- Go to Configuration > Wireless > Radio1(5G) > Station > WLAN Security
- 2. Select WPA / WPA2 in Authentication Mode
- Select suitable encryption mode in Cipher Mode as the followings: If Authentication Mode is WPA: *TKIP* + AES - This algorithm automatically selects TKIP or AES based on the client's capabilities *TKIP* - This algorithm provides greater compatibility with older client devices, but is not supported by the 802.11n standard. *AES* - This algorithm provides enhanced security over TKIP, and is the only encryption algorithm supported by the 802.11i standard. If Authentication Mode is WPA2: *AES* - This algorithm provides enhanced security over TKIP, and is the only encryption algorithm supported by the 802.11i standard.
 Select suitable EAP method mode in EAP Method:
- Select suitable EAP method mode in EAP Method: PEAP-MSCHAPV2 TTLS-MSCHAPV2 TTPS-PAP TTLS-CHAP
- 5. Provide username in **Username** for authentication.
- 6. Provide password in **Password** for authentication.
- 7. Click **Submit**
- 8. Click Save & Apply

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

domentication		
Status Configuration Administration To	ools About	
System Network Wireless Thin AP		
Radio0(2.4G) - Radio1(5G)		
Rac	lio1(5G):WLAN0	Setting
WLAN General WLAN Security QoS		
Authentication Mode:	WPA2-PSK	T
Cipher Mode:	AES	Ŧ
Pass Phrase:	Length:8-63(ASCII Charad	Errs); Length:64(HEX Characters)
		Back to Station List Submit

Figure 39 – WPA2-PSK Authentication of Station

- Go to Configuration > Wireless > Radio1(5G) > Station > WLAN Security
- 2. Select WPA-PSK / WPA2-PSK in Authentication Mode
- Select suitable encryption mode in Cipher Mode as the followings: If Authentication Mode is WPA: TKIP + AES - This algorithm automatically selects TKIP or AES based on the client's capabilities



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

If Authentication Mode is WPA2:

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

- 4. Type a string between 8 and 64 characters long in **Pass Phrase** that matches with remote AP
- 5. Click **Submit**
- 6. Click Save & Apply



4.1.5. Configure Radio Interface as Repeater

Radio 0 – 2.4GHz Radio

Repeater radio mode is not available in Radio 0(2.4G) interface.

Radio 1 – 5GHz Radio

Radio General Configuration

Status Configuration Administration To	als About
System Network Wireless Thin AP	
Radio0(2.4G) - Radio1(5G)	
	Radio1(5G) Setting
General WLAN Advanced	
Enable Radio:	
Radio Mode:	Repeater •
Country Code:	HONG KONG
Transmit Power:	5 The effective Tx Power may be different, depends on the selected Channel.
Maximum Clients:	512 (1-512)
User Isolation in different WLAN (SSID):	
	Submit

Figure 40 – Radio 1 General Setting of Repeater

- 1. Go to Configuration > Wireless > Radio1(5G) > General;
- 2. Select Enable Radio checkbox to enable radio interface
- 3. Select Repeater in **Radio Mode**
- 4. Change the following settings:

Country Code – Select an option that matches your device's installation location; *Hong Kong* is the default setting.

Note:

- Country code sets the regulatory domain for maximum transmission power that Repeater can use

Transmission Power – Select the total transmission power for the radio interface.

Maximum Client – Specify the maximum associated client between 1 and 512 that the radio interface serves. 512 is the default setting. Enable Inter-WLAN User Isolation - Select the checkbox to block the users' communication across different SSID in the AP directly.

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



Repeater WLAN Configuration

Status	Configuration	Administrati	on Ti	xols	About				Download Loc
dio0(2.4G)	- <u>Radio1(5G)</u>	T AF							
		7		Radio1	(5G) Setting				
General Station Co	WLAN Advanced							Submit	
	WLAN ID		Remote	SSID	Auth Mod	e	Detail		
	15	Netwo	ork 0		open		More		
WLAN Co	nfiguration								
Enable WLAN	SSID	Max Clients	Isolation	Auth Mode	Access Traffic Right	WLAN Uplink/Downli Control	Station nk Uplink/Downlin Control	c Detail	
Ø 0	Superwifi Networ Hide SSID	512		<u>open</u>	Full Access 🔹	0		More	
1	Superwifi Networ Hide SSID	512	•	open	Full Access 🔹	0	0 0	More	
2	Superwifi Networ Hide SSID	512		<u>open</u>	Full Access 🔻	0		More	
3	Superwifi Networ Hide SSID	512	•	open	Full Access 🔹	0	0 0	More	
4	Superwifi Networ Hide SSID	512	•	<u>open</u>	Full Access 🔹	0		More	
5	Superwifi Networ Hide SSID	512	•	open	Full Access 🔹	0 0	0 0	More	
6	Superwifi Networ Hide SSID	512	•	<u>open</u>	Full Access 🔻	0		More	
7	Superwifi Networ Hide SSID	512	•	open	Full Access •	0 0	0 0	More	
8	Superwifi Networ Hide SSID	512	•	<u>open</u>	Full Access 🔻	0		More	
9	Superwifi Networ Hide SSID	512	•	open	Full Access •	0 0	0 0	More	
10	Superwifi Networ Hide SSID	512		open	Full Access 🔻	0		More	
□ 11	Superwifi Networ Hide SSID	512		open	Full Access 🔻	0 0		More	
12	Superwifi Networ Hide SSID	512		open	Full Access 🔻			More	
13	Superwifi Networ Hide SSID	512	ø	open	Full Access 🔻	0		More	
14	Superwifi Networ Hide SSID	512		<u>open</u>	Full Access 🔻			More	

Figure 41 – WLAN List of Repeater

- Go to Configuration > Wireless > Radio1(5G) > WLAN > WLAN Configuration > WLAN 0-14 > More... for extending WLAN service form remote SSID.
- 2. Please refer to 4.1.3 on page 16 for WLAN Configuration.

Submit



4.2. Advance Configurations

4.2.1. Assign a unique identification on AP for network management

If your network contains many AP, consider assigning a unique system info setting for each of them to facilitate network management.

ΔΙΤΔΙ	
Status Configuration Administration Tools	About
System Network Wireless Thin AP	
Basic Syst	rem Settina
System Info Setting	NTP Setting
System Name:	IP Address Type: IP 10/4 IP/6
System NE ID:	NTP Server IP: 0.pool.ntp.org
System Location:	NTP Polling Interval: 600
	(15-86400s)
	NTP Time Zone: Asia/Hong Kong 🔻
	Daylight Saving Time: 📄
Figure 42 – Unique Identification	n on AP for Network Management
 Click Configuration - system Type in a string up to 255 charac 	ters in System Name
3 Type in a string up to 64 characte	ers in System NE ID
4. Type in a string up to 255 charac	ters in System Location
5. Click Submit	
6. Click Save & Apply	
4.2.2. Configure syslog so	ettings
Logging Settings	WEB Setting
Enable Syslog: 🖉	Auto Reliesh interval:
Server IP Address: 0 . 0 . 0 . 0	
Severity: Informational V	
Enable Historical Statistics: 🕑	
Sampling Frequency: 30 V (s)	

Figure 43 – Syslog Setting

- 1. Click **Configuration** > **System**
- 2. Change the following settings:



Enable Syslog – Select the checkbox to enable system logging function

Server IP Address – Type in IP address of the remote syslog server that AP sends system logs instantaneously. 0.0.0.0 denote that AP saves the syslog in its local memory

Severity – Set severity level of log that AP stores / sends to remote syslog server:

- *Emergency* A "panic" condition usually affecting multiple apps/servers/sites. At this level it would usually notify all tech staff on call.
- Alert Should be corrected immediately, therefore notify staff who can fix the problem. An example would be the loss of a primary ISP connection.
- Critical Should be corrected immediately, but indicates failure in a secondary system, an example is a loss of a backup ISP connection.
- *Error* Non-urgent failures, these should be relayed to developers or admins; each item must be resolved within a given time.
- Warning Warning messages, not an error, but indicate that an error will occur if action is not taken, e.g. file system 85% full each item must be resolved within a given time.
- Notice Events that are unusual but not error conditions might be summarized in an email to developers or admins to spot potential problems - no immediate action required.
- Informational Normal operational messages may be harvested for reporting, measuring throughput, etc. no action required. (Default Setting)
- Debug Info useful to developers for debugging the application, not useful during operations.
- 3. Click **Submit**
- 4. Click Save & Apply

4.2.3. Configure historical statistics settings

			<u> </u>
Logging Settings		WEB Setting	
Enable Syslog:		Auto Refresh Interval:	10 v (s)
Server IP Address:	0.0.0.0		
Severity:	Informational •		
Enable Historical Statistics:	۲		
Sampling Frequency:	30 v (s)		

Figure 44 – Historical Statistic Setting

- 1. Click **Configuration** > **System**
- Change the following settings: Enable Historical Statistics - Select the checkbox to enable AP statistics function



Sampling Frequency - Set the sampling time of statistics:

- 1s1 second per sample5s5 seconds per sample
- 10s 10 seconds per sample
- 30s 30 seconds per sample (Default Setting)
- 3. Click **Submit**
- 4. Click Save & Apply

4.2.4. Configure refresh interval of on-screen

information on Web UI

Logging Settings		WEB Setting	
Enable Syslog:	•	Auto Refresh Interval:	10 ▼ (s)
Server IP Address:	0.0.0.0	Http Port:	80
Severity:	Informational •	Https Port:	443
Enable Historical Statistics:	۲		
Sampling Frequency:	30 v (s)		
1. Click Config	Figure 45 – Auto F Juration > System	Refresh Interval Set	ting

- 2. Change the following setting:
 - **Auto Refresh Interval** specify the interval in second that Web UI refreshes itself automatically:

	Joronnancany.
Disable	Refresh manually
5s	Refresh every 5 seconds

- 10s Refresh every 10 seconds (Default Setting)
- 20s Refresh every 20 seconds
- 30s Refresh every 30 seconds
- 40s Refresh every 40 seconds
- 3. Click **Submit**
- 4. Click Save & Apply

4.2.5. Configure http and https port number

Logging Settings		WEB Setting	
Enable Syslog:	•	Auto Refresh Interval:	10 v (s)
Server IP Address:	0.0.0.0	Http Port:	80
Severity:	Informational T	Https Port:	443
Enable Historical Statistics:	۷		
Sampling Frequency:	30 v (s)		
1. Click Config	guration > System		

- Change the following setting: Http Port – specify the http port number. Default is port 80. Https Port – specify the https port number. Default is port 443.
- 3. Click **Submit**
- 4. Click Save & Apply



4.2.6. Configure AP as IP Gateway

Status Configuration	Administration Tools	About		
System Network Wireless	Thin AP			
<u>General</u> - <u>VLAN</u> - <u>C</u>	<u> Port Forward</u> - <u>Safe Mo</u>	<u>ode</u>		
	General N	letwork Set	ting	
Network Setting		WAN/LAN	Interface Assignment	
Network Setting:	Gateway Mode		Interface(s)	Detail
Enable IPv6:		WAN	eth0	
		LAN	eth1	
		En	able NAT Mode: 🗹	
WAN Setting(IPv4)		LAN Settin	ıg(IPv4)	
Internet Connection Type:	Static 🗸	L	AN IP Address: 192 . 168 . 98	. 1
IPv4 Address:	10 . 6 . 122 . 101	LAN IP	Address Mask: 255 . 255 . 255	- 0
IPv4 Subnet Mask:	255 . 255 . 255 . 0			
IPv4 Default Gateway:	10 . 6 . 122 . 1			
IPv4 DNS Server IP Address:	10.6.127.4			

Figure 46 – Gateway Settings

- 1. Go to Configuration > Network > General
- 2. Select Gateway in Network Setting
- 3. Change the followings on WAN setting:

Internet Connection Type – Set AP as a client with fixed IP address or DCHP client:

Static Stand for Static IP addressing; AP will not update its IP address automatically

DHCP Client Require an IP address from DCHP server on the network; AP renews its IP address periodically

IPv4 Address – Type in an IP address for AP (Static Internet Connection Type only)

IPv4 Subnet Mask – Type in a subnet mask for AP (Static Internet Connection Type only)

IPv4 Default Gateway – Type in an IP address of default gateway for AP (Static Internet Connection Type only)

IPv4 DNS Server – Type in one or more DNS server for AP (Static Internet Connection Type only).

- Change the followings on LAN setting: LAN IP Address – Provide an IP address on LAN interface of device LAN IP Address Subnet Mask – Provide a subnet mask on LAN interface of device
- 5. Assign enabled interfaces into WAN group or LAN group in **WAN/LAN Interface Assignment**; all interfaces in the same group work as bridge
- 6. Select Enable NAT Mode to enable NAT in AP [Optional]
- 7. Click **Submit**
- 8. Click Save & Apply



4.2.7. Enable Spanning Tree Protocol (STP)

STP Setting	
Enable STP Mode:	7

Figure 47 – STP Setting

- 1. Go to Configuration > Network > General > STP Setting
- 2. Select Enable STP to enable spanning tree protocol on A8n (ac) device
- 3. Click Submit
- 4. Click Save & Apply

4.2.8. Configure the operating mode on Ethernet

interface

Etherne	t Setting			
	Mode		Speed	
eth0	Auto Detect	•	100Mbps/Full	•
	MTU:	1500 (576-6000	OBvtes)	

Figure 48 – Ethernet Setting

- 1. Go to Configuration > Network > General > Ethernet Setting
- 2. Change the following settings:

Mode – Select the operating mode on Ethernet 0:

AutoA8n (ac) device negotiates with connected device
automatically and selects the best optionManualNetwork administrator select speed and duplex mode
manually

Speed (Eth0) – Select the speed and duplex mode on Ethernet 0. It is only available if *Manual* is selected in **Mode**:

10Mbps/Half 10Mbps/Full 100Mbps/Half 100Mbps/Full

MTU – Select the Maximum transmission unit on Ethernet 0. Default is 1500 Bytes.

- 3. Click Submit
- 4. Click Save & Apply



4.2.9. VLAN

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

ΝI	$\sim t$	~·
IN	ΟI	е.

- VLAN can be enabled on Switch mode ONLY

neral - <u>VLAN</u> -	DHCP - Port Forward	- Safe Mode			
		VLAN Configurat	ion		
	Enable VLA	AN: 🗹			
VLAN Profiles					
VLAN ID	Interfaces	IPv4 Addres	ss/Subnet Mask	VLAN	STP
1	eth0, eth1	10 6 122 10	1/ 255.255.255.0	۲	X
					Add VLAN
Interfaces					
Interface	Туре	Default VLAN (PVID)	Default VLAN Tagging	I VL	AN(s) Edit
eth0	Trunk	1 🗸		all	Edit
eth1	Access	NA	NA	1	Edit

Figure 49 – VLAN Settings

Enable VLAN

- 1. Go to Configuration > Network > VLAN
- 2. Click **Submit**
- 3. Go to Configuration > Network > VLAN > VLAN Profiles

System	Netw	ork	Wirele	ss Thi	n AP			
<u>General</u>		VLAN		DHCP		Port Forward	- <u>Safe Mode</u>	
							Create VLAN	
						VLAN II	0: (1-4094)	
						IPv4 Addres	. 0 . 0 . 0	
						IPv4 Subnet Mas	·· 255 · 255 · 255 · 0	
						Enable STP Mod	a: 🗹	
							Cancel	Submit

Figure 50 – VLAN Setting – Create VLAN

- 4. Click Add VLAN to create new VLAN
- Change the following settings:
 VLAN ID Type in an identification number that represents a VLAN IPv4 Address – Type in IP address for the VLAN IPv4 Subnet Mask - Type in subnet mask for the VLAN Enable STP Mode – Select the checkbox to enable STP on VLAN
- 6. Click **Submit**
- 7. Select a desired VLAN as Management VLAN
- 8. Click **Submit**



Status Configuration Administration Too	ls About
System Network Wireless Thin AP	
General - VLAN - DHCP - Port Forward -	Safe Mode
In	terface Configuration
Interface:	eth0
Type:	Trunk O Access
Default VLAN (PVID):	×
Default VLAN Tagging:	
VLAN Pass Through:	
VLAN(s):	
	Back Submit

Figure 51 – VLAN Setting – Interface Configuration

- 9. Go to Configuration > Network > VLAN > Interfaces
- 10. Click Edit to assign VLAN profile on each interface respectively
- 11. Change the following settings:

Type – select type of VLAN connection link:

TrunkAble to carry multiple VLAN traffic. Typically trunk link is
used to connect switches to other switches or to routersAccessIt is part of only one VLAN; it is for end devices

If Access is selected on Type;

VLAN – assign the VLAN profile on the interface

If Trunk is selected on Type;

Default VLAN (PVID) - Stand for Port VLAN ID; select the default VLAN for the interface

Default VLAN Tagging – Select checkbox that AP tags the untagged packet with PVID

VLAN Pass Through - Select checkbox that AP does not modify the incoming packets that are tagged. Also, AP tags the packets, which are not tagged if **Default VLAN Tagging** is selected.

VLAN(s) – Assign one or more VLAN profile to the interface. Unlike VLAN Pass Trough, the interface only forwards the packets to selected VLAN.

12. Click **Submit**

13. Click Save & Apply



4.2.10. DHCP

A8n (ac) series products have built-in DHCP server; it can dynamically distribute network configuration parameters to the connected end devices on all LAN interfaces.

Note:

- DHCP server is available on Gateway mode ONLY

Status Configuratio	n Administration	Tools About			
System Network Wireless	Thin AP				
<u>General - VLAN - [</u>	OHCP - Port Forward	- <u>Safe Mode</u>			
		DHCP Server Se	etting		
	DHCP Serv	er: Server Mode	\checkmark		
Pool ID	Start IP	End IP	Default Lease Time	Enable	Detail
1	NA	NA	86400	No	
2	NA	NA	86400	No	
3	NA	NA	86400	No	2
4	NA	NA	86400	No	\swarrow
					Submit

Figure 52 – DHCP Server Setting

Enable DHCP server

- 1. Go to Configuration > Network > DHCP
- 2. Select Server Mode on **DHCP Server**
- 3. Click **Submit**
- 4. Click dunder **Detail** of each pool

Status Configuration Administration	Tools	About			
stem Network Wireless Thin AP					
eneral - VLAN - DHCP - Port Forw	ard - Safe	Mode			
	Addre	ss Pool Set	ting		
Enab	le Pool: 🗸				
1	Pool ID: 1				
Start IP A	ddress: 0	. 0 . 0	. 0		
End IP A	ddress: 0	. 0 . 0	. 0		
Default Leas	e Time: 86400	-604800 Seconds)			
	(00	00100000000000000			
				Back to Pools List	Submit

Figure 53 – DHCP Server – Address Pool Setting

- 5. Select Enable Pool check box
- 6. Type in IP address on Start IP Address
- 7. Type in IP address on End IP Address
- 8. Specify lease time between 60s and 604800s in **Default Lease Time**; 86400s is default setting
- 9. Click **Submit**
- 10. Click Save & Apply



4.2.11. Port Forward

Port forward allows remote computers from WAN to connect to a specific computer or service within a private local-area network (LAN).

Note:

- Port forward is available on Gateway mode ONLY

Status Co	nfiguration Administrat	ion Tools	About				
stem Network	- DHCR - Ro	t Forward - Caf	a Mada				
	<u>leral - VLAN - DHCP - Port Forward</u> - <u>sare Mode</u>						
	T OF C F OF MARK						
ID	Local IP	Local Port	Туре	Global Port	Enable	Deta	
1	NA	NA	TCP & UDP	NA	No	2	
2	NA	NA	TCP & UDP	NA	No	2	
3	NA	NA	TCP & UDP	NA	No		
4	NA	NA	TCP & UDP	NA	No	\swarrow	
5	NA	NA	TCP & UDP	NA	No	2	
6	NA	NA	TCP & UDP	NA	No	2	
7	NA	NA	TCP & UDP	NA	No	2	
8	NA	NA	TCP & UDP	NA	No	Z	
9	NA	NA	TCP & UDP	NA	No	2	
10	NA	NA	TCP & UDP	NA	No	2	
11	NA	NA	TCP & UDP	NA	No		
12	NA	NA	TCP & UDP	NA	No	2	
13	NA	NA	TCP & UDP	NA	No		
14	NA	NA	TCP & UDP	NA	No	2	
15	NA	NA	TCP & UDP	NA	No	2	
16	NA	NA	TCP & UDP	NA	No	2	
17	NA	NA	TCP & UDP	NA	No	2	
18	NA	NA	TCP & UDP	NA	No	2	
19	NA	NA	TCP & UDP	NA	No		
20	NA	NA	TCP & UDP	NA	No		
20	10		. a. a obi		110		
						Submit	
						2.56111	

Figure 54 – Port Forward List

Enable port forward on A8n (ac) device

1. Go to Configuration > Network > Port Forward

Status Configuration Administr	ation Tools	About		
System Network Wireless Thin AP				
<u>General</u> - <u>VLAN</u> - <u>DHCP</u> - PC	rt Forward - Safe	Mode		
	Port F	orward Sett	ing	
	Enable: 🗹			
	ID: 1			
Lo	ocal IP Address: 0	. 0 . 0	- 0	
	Local Port: 1			
	Protocol Type: TCP &	UDP	~	
	Global Port: 1			
	Description:		^	
			~	
	<		>	
				Bask to Bast Fooward List Submit
				Back to Port Forward List Submit

Figure 55 – Port Forward Setting

- 2. Click 🗹 under Detail
- 3. Select **Enable** checkbox
- 4. Type in target host's IP address in Local IP Address
- 5. Type in port number of target host in Local Port



- Select suitable protocol in Protocol Type: TCP & UDP TCP UDP
- 7. Type in port number of AP in Global Port
- 8. Type in description in **Description** [Optional]
- 9. Click **Submit**
- 10. Click Save & Apply

4.2.12. 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 interface 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.

Note:

- A8n (ac) recovers itself from safe mode if it detects the backhaul link is recovered

Status Configuration Administration Tool	s About
System Network Wireless Thin AP	
General - <u>VLAN</u> - <u>DHCP</u> - <u>Port Forward</u> -	Safe Mode
	Safe Mode Setting
Enable Safe Mode:	
Ping Host 1:	0
Ping Host 2:	0 . 0 . 0
Ping Host 3:	0 . 0 . 0
Ping Interval:	10 (3-30s)
	Submit



Enable safe mode on A8n (ac) device

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



4.2.13. Advanced Settings on Radio Interface

A8n (ac) provides advanced settings on each radio interface; these settings include data rate, AirFi, Tx/Rx Stream settings ... etc.

Caution:

- 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

ALT					
Status Configuration	Administration	Tools	About		
System Network Wireless	Thin AP				
Radio0(2.4G) - Radio1((<u>5G)</u>		_		
		Radio0(2.4	4G) Setting		
General WLAN Adva	anced QoS				Submit
Advanced Setting			Data Rate Setting		
AMPDU:	 Image: A start of the start of		Data Rate:	best	 (Mbps)
AMPDU Limit:	64	(1-64)	Multicast Data Rate:	min	 (Mbps)
AMSDU:	 Image: A start of the start of				
Max IX Sueams:	2	•			
Max Rx Streams:	2	•			
Beacon Interval Auto:	✓				
Beacon Interval:	(40-3500)				
DTIM:	1 (1-255)				
Protection Mode:	CTS-only	•			
RTS/CTS Threshold:	2346 (0-2347)				
Distance:	2 (0-50km)				
IGMP Snooping:	Enable	•			
Multicast Traffic:					
MTU:	1500 (576-2290Bytes)				
Enable Nearby AP List:	[Nearby AP List]				
AirFi Setting					
AirFi Mode:					
AirFi Level:	Level I	•			
					Submit

Figure 57 – Radio O's Advanced Settings



Advanced Settings

Configure AMPDU and AMSDU on radio interface

AMPDU: 🗸

AMPDU Limit: 64 (1-64)

AMSDU: 🗸

Figure 58 – AMPDU and AMSDU Setting

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

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

- 2. Select **AMPDU** checkbox to enable aggregation of MAC protocol unit
- 3. Type in the maximum number of data frame between 1 and 64 that A8n (ac) pushes them into single PPDU; 64 is default setting
- 4. Select **AMSDU** checkbox to enable aggregation of MAC service data unit; A8n (ac) pushes aggregated MSDU (MAC service data units) into a single MPDU
- 5. Click **Submit**
- 6. Click Save & Apply

Configure the number of transmit radio chains and receive radio chains

Max Tx Streams:	2	•
Max Rx Streams:	2	v

Figure 59 - transmit radio chains and receive radio chains setting

 2.4G Interface: Go to Configuration > Wireless > Radio0 > Advanced > Advanced Settings
 Contacting a Contacting > Wireless > Partial > Advanced >

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

- 2. Select the maximum number of transmission between 1 and 2 on **Max Tx Streams**
- 3. Select the maximum number of transmission between 1 and 2 on Max Rx Streams
- 4. Click **Submit**
- 5. Click **Save & Apply**

Configure beacon interval of BSS

Beacon Interval Auto: 🗹

Beacon Interval: 100

Figure 60 – Beacon Setting

 2.4G Interface: Go to Configuration > Wireless > Radio0 > Advanced > Advanced Settings 5G Interface: Go to Configuration > Wireless > Radio1 > Advanced > Advanced Settings



2. Change the following settings:

Beacon Interval Auto – Select checkbox that A8n (ac) tunes the interval of beacon transmissions of each supported BSS automatically

Beacon Interval – Available if **Beacon Interval Auto** is NOT selected; Specify the interval time between 40ms and 3500ms in **Beacon Interval.** Each BSS share this setting.

- 3. Click **Submit**
- 4. Click Save & Apply

Configure Delivery Traffic Indication Message (DTIM) time

- 2.4G Interface: Go to Configuration > Wireless > Radio0 > Advanced > Advanced Settings 5G Interface: Go to Configuration > Wireless > Radio1 > Advanced > Advanced Settings
- 2. Specify the interval time between 1 and 255 in DTIM.
- 3. Click **Submit**
- 4. Click Save & Apply

Note:

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

Modify protect mechanism on hidden node problem of Wi-Fi network

Protection Mode:	CTS-only
RTS/CTS Threshold:	2346
	(0-2347)

Figure 61 – Protection Mechanism Setting

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

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

- Select suitable mechanism on Protection Mode; you can select: None - no protect mechanism is used. It is the default setting. CTS-only - also known as CTS-to-Self; AP issues a CTS frame to itself before sending data. All clients will not transmit during the time. RTS-CTS - AP sends a RTS frame, waits for the clients CTS frame and then sends the data packet. It allow more robust operation, but at the expense of additional overheads.
- 3. Specify frame size in byte between 0 and 2347 bytes on **RTS/CTS Threshold**; 2346 is default setting.

If a frame is smaller than the RTS/CTS threshold, it will be sent by the AP without modification. If a frame is larger than the RTS/CTS threshold, then two frames will be sent by the AP. The first frame is an RTS (request to send) frame. After the RTS frame is sent, the AP listens



for the corresponding CTS from the target client. Upon reception of the CTS, the AP then sends the data frame. There are trade-offs when considering what value you should set for the RTS/CTS threshold. Smaller values will cause RTS to be sent more often, increasing overheads. However, the more often RTS packets are sent, the sooner the system can recover from collisions. It is recommended to use the default value or only minor reductions of the default setting.

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

Change distance setting on A8n (ac)

Distance setting is the estimated distance of target area (round to the nearest km); A8n (ac) adjusts the round-trip time latency according to this setting.

- 2.4G Interface: Go to Configuration > Wireless > Radio0 > Advanced > Advanced Settings 5G Interface: Go to Configuration > Wireless > Radio1 > Advanced > Advanced Settings
- 2. Type in the estimate distance of target area between 1 and 50 km in **Distance**; 2 km is default setting.
- 3. Click **Submit**
- 4. Click Save & Apply

Enable IGMP Snooping

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 VAP 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 VAP 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 VAP 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.

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



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

- 2. Select **IGMP Snooping** checkbox to enable IGMP Snooping
- 3. Click **Submit**
- 4. Click Save & Apply

Enable multicast traffic

- 2.4G Interface: Go to Configuration > Wireless > Radio0 > Advanced > Advanced Settings 5G Interface: Go to Configuration > Wireless > Radio1 > Advanced > Advanced Settinas
- 2. Select **Multicast Traffic** checkbox that A8n (ac) process multicast traffic in all WLANs; otherwise; AP drops the multicast traffic.
- 3. Click **Submit**
- 4. Click Save & Apply

Enable Nearby AP List on A8n (ac)

- 2.4G Interface: Go to Configuration > Wireless > Radio0 > Advanced > Advanced Settings 5G Interface: Go to Configuration > Wireless > Radio1 > Advanced > Advanced Settings
- 2. Select **Nearby AP List** checkbox that A8n (ac) sniffs the surrounding AP periodically
- 3. Click **Submit**
- 4. Click Save & Apply

AirFi Settings

AirFi technology is an 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.





- Go to Configuration > Wireless > Radio0 > Advanced > Advanced Settings
- 2. Select AirFi checkbox to enable AirFi feature
- Select suitable level in AirFi Level
 Level I favor the fast (802.11n) client most
 Level I favor the fast (802.11n) client moderate
 Level III favor the fast (802.11n) client less
- 4. Click **Submit**
- 5. Click Save & Apply



Note:

- Level I is recommended

Data Rate Setting

Altai AP provides the capability to limit all clients to transmit data and multicast data in the certain data rate.

Data Rate Setting

	Data H	are octin	·9					
		D	ata Rate:	best		T	(Mbps)	
	М	ulticast Da	ata Rate:	min		۲	(Mbps)	
			Figure	63 – Dat	a Rate Setting)		
Note								
-	Data recom	rate: Imende	Best ed	and	Multicast	Data	Rate:	
								_

 2.4G Radio: Go to Configuration > Wireless > Radio0 > Advanced > Data Rate Settings

5G Radio: Go to Configuration > Wireless > Radio1 > Advanced > Data Rate Settings

- 2. Select a data rate on Data Rate; best is default setting
- 3. Select a data rate on Multicast Data Rate; min is default setting
- 4. Click Submit
- 5. Click Save & Apply

4.2.14. Quality of Service on Radio Interface

A8n (ac) provides QoS/WMM configuration on both radio interface and each WLAN.

Modify the QoS setting on Radio

Status	Configuration	Administration	Tools	About							
	Wireless T										
Radio0(2.4G) - Radio1(5G)											
Radio0(2.4G) Setting											
General WLAN Advanced QoS WEP											
Optimization Mode: Optimization Optimized for Throughput Optimized for Capacity Manual Configuration Radio(AP-side) WMM Parameters											
	C	WMIN	CWMAX	AIFS	ТХОР	NOACK					
BestEffort (Background Video(VI) Voice(VO)	Construction Construction 0:0-15) BestEffort (BE) B Background(BK) E Video(V1) S Voice(V0) 2 C C		(0-15) 7 10 4 3	(0-15) 1 7 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	(0-8192) 4096 0 3008 1504						
Submit											



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



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

 Select suitable configuration in Optimization Mode; you can select: Default Optimization – a set of QoS/WMM parameters for most scenarios; it is a default setting

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

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

Manual Configuration – Specify QoS/WMM parameters manually

- 3. Click Submit
- 4. Click Save & Apply

Modify the QoS setting in WLAN 0 – 15

Status Configuration Administration Tools About	
System Network Wireless Thin AP	
Radio0(2.4G) - Radio1(5G)	
Radio0(2.4G) WLANO Set	tting
WLAN General WLAN Security Rogue Station List QoS Bandwidth Control]
Enable DSCP-to-WMM Mapping: 🔽	
	DSCP
	(0-63,cannot be in the same value)
BestEffort (BE)	24
Background(BK)	16
Video(VI)	40
Voice(VO)	56
	Back to WLAN List Submit

Figure 65 – QoS Setting on WLAN 0-15

1. 2.4G WLAN 0-15: Go to Configuration > Wireless > Radio0 > WLAN 0-15 > QoS

5G WLAN 0-15: Go to Configuration > Wireless > Radio1 > WLAN 0-15 > QoS

- 2. Specify QoS/WMM parameters manually
- 3. Click Submit
- 4. Click Save & Apply

4.2.15. Bandwidth Control on WLAN

Status Configuration	Administration Tools	About			
vstem Network Wireless	Thin AP				
adio0(2.4G) - Radio1(5	<u>G)</u>				
	Radio0(2.4	4 <mark>G) WLANO</mark> S	Setting		
WLAN General WLAN Se	curity Rogue Station List QoS	Bandwidth Cont	rol		
	Based On	WLAN		Based On Station	
	(0-1000000 Kbp	is, 0: Disable)	(0-1000000 Kbps, 0: Disable)	
Uplink	0		0		
Downlink	0		0		
				Back to WLAN List	Submit

Figure 66 – Bandwidth Control Setting on WLAN 0-15



Enable bandwidth control for the WLAN on WLAN 0 – 15

- 2.4G WLAN 0-15: Go to Configuration > Wireless > Radio0 > WLAN 0-15 > Bandwidth Control 5G WLAN 0-15: Go to Configuration > Wireless > Radio1 > WLAN 0-15 > Bandwidth Control
- 2. Type in maximum throughput in kbps between 0 to 1000000 kbps on **Uplink** under **Based on WLAN**; 0 denotes disable, and is default setting
- 3. Type in maximum throughput in kbps between 0 to 1000000 kbps on **Downlink** under **Based on WLAN**; 0 denotes disable, and is default setting
- 4. Click **Submit**
- 5. Click Save & Apply

How to enable bandwidth control per station on WLAN 0 – 15

- 2.4G WLAN 0-15: Go to Configuration > Wireless > Radio0 > WLAN 0-15 > Bandwidth Control 5G WLAN 0-15: Go to Configuration > Wireless > Radio1 > WLAN 0-15 > Bandwidth Control
- Type in maximum throughput in kbps between 0 to 1000000 kbps on Uplink under Based on Station; 0 denotes disable, and is default setting
- Type in maximum throughput in kbps between 0 to 1000000 kbps on Downlink under Based on Station; 0 denotes disable, and is default setting
- 4. Click **Submit**
- 5. Click Save & Apply



5.Manage Your Access Point

5.1. User Admin

A8n (ac) device allows network administrator to manage user account and privilege for accessing Web UI via local authentication and/or RADIUS authentication.

Status Configuration Administration Too	ols About
	,
	User Admin
UserName:	admin
Password:	
Confirm Password:	
	Submit
Login Authentication Setting	
Authentication Type:	RADIUS+Local Authentication
Authentication Mode:	PAP
Encryption Algorithm:	Disabled
RADIUS Server:	10 . 6 . 161 . 206
RADIUS Secret:	••• Show
Secondary RADIUS Server:	
Secondary RADIUS Secret:	Show
	Submit

Figure 67 – User Admin

Table 4 describes the authentication setting of A8m (ac) device.

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

Table 4 - Different authentication type

5.1.1. Local authentication

Modify admin account's password

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

Modify guest account's password

- 1. Go to Administration > User Admin
- 2. Select guest in UserName



- 3. Type a new password in Password
- 4. Type a new password again in Confirm Password
- 5. Click **Submit**

Note:

- Please login as admin for modifying password

5.1.2. RADIUS authentication

Enable RADIUS authentication in A8n (ac) products

- 1. Go to Administration > User Admin > Login Authentication Setting
- 2. Select RADIUS authentication or RADIUS + Local authentication in Authentication Type
- Select suitable authentication in Authentication Mode; you can select:

PAP EAP

4. Select suitable encryption in **Encryption Algorithm**; you can select: For authentication Mode is *PAP*:

```
Disable
For authentication Mode is EAP:
PEAP-GTC
PEAP-MS-CHAP-V2
TTLS-PAP
TTLS-CHAP
TTLS-MS-CHAP
TTLS-MS-CHAP-V2
```

- 5. Provide IP address of remote RADIUS server in RADIUS Server
- 6. Provide suitable secrets in **Secret** of **RADIUS Secret**.
- 7. Left **Secondary RADIUS Server** blank if no backup RADIUS server is available
- 8. Left **Secondary RADIUS Secret** blank if no backup RADIUS server is available
- 9. Click Submit
- 10. Click OK (see Figure 68)



Figure 68 – Popup window for confirming the change of RADIUS authentication



5.2. SNMP

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

Sta	atus Co	nfiguration	Administration	Tools	About					
	dmin SNMP									
SNMP Configuration										
			Enable	SNMP:						
			Read Comm	nunity: public						
			Write Comm	nunity:			Show			
	Trap Host	ID	Trap Host	Trap	Port	Trap Community	1	Enable	Detail	
	1		NA	16	2	public		No	2	
	2		NA	16	2	public		No	2	
	3		NA	16	2	public		No	2	
	4		NA	16	2	public		No	2	
									Submit	

Figure 69 – SNMP Configuration

5.2.1. Enable SNMP in A8n (ac) products

- 1. Go to Administration > User Admin > SNMP
- 2. Select **Enable SNMP** checkbox to enable SNMP function
- 3. Type in suitable string in **Read Community**; the string of **Read Community** between Network Manage System (NMS) and A8n (ac) must be identical, otherwise, NMS cannot get information from A8n (ac). *public* is default setting.
- 4. Type in suitable string in **Write Community**; the string of **Write Community** between Network Manage System (NMS) and A8n (ac) must be identical, otherwise, NMS cannot modify A8n (ac)'s setting. *netman* is default setting.
- 5. Click **Submit**
- 6. Click Save & Apply

Note:

 A8n (ac) support up to four trap host at the same time. The information about trap hosts will be listed in the trap host table (see Figure 70)

Trap Host ID	Trap Host	Trap Port	Trap Community	Enable	Detail			
1	NA	162	public	No	2			
2	NA	162	public	No	\swarrow			
3	NA	162	public	No	2			
4	NA	162	public	No	\swarrow			
Figure 70 – Trap host table								


5.3. Certificate

A8n (ac) devices support both HTTP and HTTPS connection for their web UI. Certificate management allows network administrator to upload their own certifications for HTTPS connection.

Status Configuration Administration T User Admin SNMP Certificate Firmware Update Fact	ools About
	an pendare ; bechap ; receare ; customizariar ; becane
C	ertificate Management
Http Cert File:	Choose file No file chosen Upload
Http Key File:	Choose file No file chosen Upload
Certificate Status:	Valid certificate

Figure 71 – Certificate Management

5.3.1. Upload the customized certification for HTTPS

connection on A8n (ac) products

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

Note:

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



5.4. Firmware Update

Network administrator updates (upgrades or downgrades) A8n (ac) device's firmware via web UI.

Status Configuration Administration Tools About	
User Admin SNMP Certificate Firmware Update Factory Default Backup / Restore Customization License	
Firmware Update	
Flash Firmware	
Upload an Firmware image file to reflash the device:	
Choose file No file chosen	
${old one}$ Keep all settings ${igodol one}$ Keep Network Address settings only ${igodol one}$ Full Factory Reset	
	Upload image

Figure 72 – Firmware Update

5.4.1. Update A8n (ac) device's firmware

- 1. Go to Administration > Firmware Update
- 2. Click Choose file, then select suitable firmware image file (.bin)

3.	You may select:	
	Keeps all settings	Device keeps all operating setting after updating firmware
	Keep Network Address settings only	Device keeps IP address, subnet mask only after updating firmware; the other settings will be restored as default settings
	Full Factory Reset	Device restores all setting as default settings after updating firmware

4. Click Upload Image

- 5. If uploaded firmware image is valid, click **Proceed** to continue; otherwise, error message will be shown
- 6. Wait unit A8n (ac) completes updating firmware
- 7. Login with correct username and password, then check the firmware version on **About** > **Software Version**

Caution:

 Do not interrupt the process of firmware update. Please maintain network connection and power supply during updating firmware; otherwise A8n (ac) may not function.



5.5. Factory Default

Network administrator restores A8n (ac) device's settings as default settings via web UI.

Status	Configuration	Administration	Tools	About		
User Admin	SNMP Certificate	Firmware Update	Factory Default	Backup / Restore	Customization	License
			Restore t	o Factory De	fault	
Peetore tr	Eactory Default					
INSIDIE II	r actory Delduit					
Keep N	etwork Address setti	ngs				
All Setting	js would be reset t	o factory defaults.				
Warning:	Wireless network	configurations ca	annot be retain	ed.		
		5				



5.5.1. Restore A8n (ac) device's settings with default settings

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

Note:

- Please refer to 2.3 Login the AP (via Ethernet) on page 4 for logging in A8n (ac) after performing factory default

5.6. Backup/Restore

Network administrator backups / restores A8n (ac) device's settings via web UI.

Status Configuration Administration	Tools About	
User Admin SNMP Certificate Firmware Upd	ite Factory Default Backup / Restore	Customization License
	Admin Backup/Rest	ore
Backup Configuration File		
<u>Create backup</u>		
Restore Configuration File		
 Upload Backup Archive: 		
Choose file No file chosen		
		Restore backup

Figure 74 – Admin Backup / Restore

5.6.1. Backup A8n (ac) device's settings

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



5.6.2. Restore A8n (ac) device's settings with

configuration file

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

5.7. Customization

Network administrator may create customized settings as factory default settings for A8n (ac) products. Once the customized configuration file is imported, A8n (ac) products restore with the customized settings as default settings rather than the original default settings.



Figure 75 – Default Configuration Customization

5.7.1. Create customized configuration file for A8n

(ac) products

- 1. Go to Administration > Customization > Default Configuration Customization
- 2. Click <u>Product Customization Template</u> to download configuration template file (.tar.gz)
- 3. Use 7-zip software to open the template file, and edit the files in the factory_default.zip.
- Edit system, network, and wireless files with the desired settings; system
 Contain settings about SNMP, syslog ...etc
 Contain network settings about all interfaces, such as IP address, VLAN enabling, and STP ...etc.
 wireless
 Contain settings about radio interfaces, including radio enabling, WLAN settings ... etc
- 5. Save the modified files



- 6. Go to Administration > Customization > Default Configuration Customization
- 7. Click **Choose file**, then select the modified customization file
- 8. Click Install

Caution:

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

Note:

 Customization will take effect after reboot. Since improper customization may cause malfunction of A8n (ac), please contact Altai support team (<u>support@altaitechnologies.com</u>) for any queries.



6.Monitor Your Access Point

This chapter introduces various information / statistics from Web UI or LED indication that monitoring the device's status.

6.1. LED Colors and What They Mean

6.1.1. A8n (ac) series

LED	LED Status (Color)	Meaning	
Power LED	Off	Power off	
	Solid (Green)	Operating	
	Off	Link Down	
Ethernet LED	Solid (Green)	Link Up	
	Blinking (Green)	Activity	
 Remarks: All LED will be off once pressing down the reset button Pressing and holding the reset button until Power LED blinks once, the device reboots. Pressing and holding the reset button until Power LED blinks twice consecutively, the device restores the factory default setting. 			

Table 5 – A8n (ac) series operation LED indicators

70



6.2. Status > Overview

Status Co rview Radio0(2.	onfiguration Adminis 4G) Radio1(5G) E	stration Tools	About		
S	ystem	Network(Switch M	lode)		<u>More>></u>
System Name: Product Name: CPU Usage: Memory Usage: Time of Day: Uptime:	NA A8-Ein 1% 171/476 MB (35%) Mon Jun 15 17:11:02 2015 00h 07min 10s	Ethernet IPv4 DHCP Client: IPv4 Address: IPv4 Subnet Mask: IPv4 Default Gateway IPv4 DNS Server: Interfaces(3)	Disabled 192.168.4.4 255.255.255.0 /: 192.168.4.1 NA		
T	hin AP	Ethernet (eth0) MAC: Link:	00:19:be:20:03:c3 Auto (Full 1000Mb/s)	Transmit: Receive:	206.41KB (0.00Kbps) 38.59KB (0.00Kbps)
THE AP.	UFF	Radio0(2.4G) Radio Status: OFF Radio1(5G) MAC: Channel: Wireless Mode: Noise Level: Transmit Power: Transmit:	00:19:be:28:01:55 5745MHz(Channel 149) 5GHz 866.7Mbps(802.11ac HT80) -105 dBm 28 dBm 0.00KB (0.00Kbps)	Mode: WLANs: Clients: Busy:	AP 2 0 0%(0%)

Figure 76 – A8n (ac) device's status overview

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

6.2.1. System status

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

System			
System Name:	NA		
Product Name:	A8-Ein		
CPU Usage:	1%		
Memory Usage:	171/476 MB (35%)		
Time of Day: Mon Jun 15 17:11:02 2015			
Uptime:	00h 07min 10s		

Figure 77 – System Status



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

Product Name – Device's product name

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

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

Time of Day – system time of device

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

6.2.2. Thin AP



Figure 78 – Thin AP Status

Thin AP - indicate status of thin AP feature

6.2.3. Networks

Networks provide basic information about Layer 3 status.

Switch Mode

Network(Switch Mode)				
Ethernet IPv4 DHCP Client:	Disabled	IPv6 DHCP Client:	Disabled	
IPv4 Address:	10.6.122.101	IPv6 Address:	NA	
IPv4 Subnet Mask:	255.255.255.0	IPv6 Default Gateway:	NA	
IPv4 Default Gateway:	10.6.122.1	IPv6 DNS Server:	NA	
IPv4 DNS Server:	10.6.127.4			

Figure 79 – Network Status in Switch Mode

IPv4 DHCP Client – indicate whether device's IP address is assigned by DHCP server or not

IPv4 Address – Current IPv4 address of device

IPv4 Subnet Mask - indicate the subnetwork device belongs to

IPv4 Default Gateway – indicate a node that helps device to another network.

IPv4 DNS Server - indicate a node that provides DNS service for the device

The following information is available if IPv6 option is enabled.

IPv6 DHCP Client – indicate whether device's IP address is assigned by IPv6 DHCP server or not

IPv6 Address - Current IPv6 address of device



IPv6 Default Gateway – indicate a node that helps device to another network.

IPv6 DNS Server - indicate a node that provides DNS service for the device

Gateway Mode

Network(Gateway Mode)			
WAN - eth0			
IPv4 DHCP Client:	Disabled		
IPv4 Address:	192.168.4.4		
IPv4 Subnet Mask:	255.255.255.0		
IPv4 Default Gateway:	192.168.4.1		
IPv4 DNS Server:	NA		
LAN -			
IP Address:	192.168.98.1	NAT:	Enabled
Subnet Mask:	255.255.255.0	DHCP Server:	Disabled

Figure 80 – Network Status in Gateway Mode

WAN

IPv4 DHCP Client – indicate whether device's IP address is assigned by DHCP server or not

IPv4 Address - Current IPv4 address of device on WAN

IPv4 Subnet Mask - indicate the subnetwork device belongs to

IPv4 Default Gateway – indicate a node that helps device to another network.

IPv4 DNS Server - indicate a node that provides DNS service for the device

LAN

IP Address - Current IP address of device on LAN

Subnet Mask – indicate the subnetwork device belongs to

NAT – indicate whether device performs network address translation (NAT) or not

DHCP Server - indicate whether built-in DHCP server is enabled or not



6.2.4. Interfaces

Interfaces provide the real time status of all interfaces on the A8n (ac) device.

Interfaces(3)			
Ethernet (eth0)			
MAC:	00:19:be:20:03:c3	Transmit:	2.94MB (0.00Kbps)
Link:	Auto (Full 1000Mb/s)	Receive:	980.07KB (0.00Kbps)
Radio0(2.4G)			
MAC:	00:19:be:00:1b:70	Mode:	AP
Channel:	2412MHz(Channel 1)	WLANs:	1
Wireless Mode:	2.4GHz 144Mbps(802.11ng HT20)	Clients:	0
Noise Level:	-97/-97/-97/dBm)	Busy:	NA
Transmit Power:	25 dBm		
Transmit:	0.00KB (0.00Kbps)		
Receive:	0.00KB (0.00Kbps)		
Radio1(5G)			
MAC:	00:19:be:28:01:55	Mode:	AP
Channel:	5745MHz(Channel 149)	WLANs:	2
Wireless Mode:	5GHz 866.7Mbps(802.11ac HT80)	Clients:	0
Noise Level:	-108 dBm	Busy:	NA
Transmit Power:	28 dBm		
Transmit:	0.00KB (0.00Kbps)		
Receive:	0.00KB (0.00Kbps)		

Figure 81 – Status of all available interfaces

Ethernet (eth0)

Ethernet (eth0)			
MAC:	00:19:be:20:03:c3	Transmit:	2.94MB (0.00Kbps)
Link:	Auto (Full 1000Mb/s)	Receive:	980.07KB (0.00Kbps)

Figure 82 – Ethernet 0 Status

MAC – MAC address of Ethernet 0 interface

Link – indicate the status and operating mode of Ethernet 0

Transmit – indicate the traffic and instant throughput of transmission on Ethernet 0

Receive – indicate the traffic and instant throughput of receive operation on Ethernet 0



Radio0 (2.4G)

Radio0(2.4G)			
MAC:	00:19:be:00:1b:70	Mode:	AP
Channel:	2412MHz(Channel 1)	WLANs:	1
Wireless Mode:	2.4GHz 144Mbps(802.11ng HT20)	Clients:	0
Noise Level:	-97/-97/-97/-97(dBm)	Busy:	NA
Transmit Power:	25 dBm		
Transmit:	0.00KB (0.00Kbps)		
Receive:	0.00KB (0.00Kbps)		

Figure 83 – Radio O Status

MAC – MAC address of Radio 0 interface

Channel – indicate operating frequency (channel) of Radio 0 **Wireless Mode** – indicate 802.11 standards that Radio 0 operates **Noise Level** – indicate the noise level in terms of dBm of operating channel

Transmission Power – indicate the total transmission power of Radio 0 **Transmit** – indicate the traffic and instant throughput of transmission on Radio 0

Receive – indicate the traffic and instant throughput of receive operation on Radio 0

Mode – indicate operating mode of Radio 1

WLANs - indicate the number of operating WLAN on Radio 0 (AP mode and Repeater Mode only)

Clients - indicate the number of clients that Radio 0 servers currently (AP mode and Repeater mode only)

Connection – indicate connection status between Radio 0 and remote AP (Station mode only)

AP SSID – indicate the SSID that station associates with (Station mode only)

AP SNR – indicate received SNR from remote AP (Station mode only) **Busy** – indicate busy of operating channel

Radio1 (5G)

Radio1(5G)			
MAC:	00:19:be:28:01:55	Mode:	AP
Channel:	5745MHz(Channel 149)	WLANs:	2
Wireless Mode:	5GHz 866.7Mbps(802.11ac HT80)	Clients:	0
Noise Level:	-108 dBm	Busy:	NA
Transmit Power:	28 dBm		
Transmit:	0.00KB (0.00Kbps)		
Receive:	0.00KB (0.00Kbps)		

Figure 84 – Radio 1 Status

MAC – MAC address of Radio 1 interface Channel – indicate operating frequency (channel) of Radio 1 Wireless Mode – indicate 802.11 standards that Radio 1 operates



Noise Level – indicate the noise level in terms of dBm of operating channel

Transmission Power – indicate the total transmission power of Radio 1 **Transmit** – indicate the traffic and instant throughput of transmission on Radio 1

Receive – indicate the traffic and instant throughput of receive operation on Radio 1

Mode - indicate operating mode of Radio 1

WLANs - indicate the number of operating WLAN on Radio 1 (AP mode and Repeater Mode only)

Clients - indicate the number of clients that Radio 1 servers currently (AP mode and Repeater mode only)

Connection – indicate connection status between Radio 0 and remote AP (Station mode only)

AP SSID – indicate the SSID that station associates with (Station mode only)

AP SNR – indicate received SNR from remote AP (Station mode only) **Busy** – indicate busy of operating channel

6.3. Status > Radio0(2.4G)

6.3.1. Status > Radio0(2.4G) > Status

Status		Con	nfigur	ation		Admi	nistra	ation		То	ols		Abo	ut										
erview (Radio	0(2.4	G) ∣	Rad	io1(50	G)	Ethe	rnet	Lo	gs														
atus	- <u>As</u>	soci	ation	List																				
											Sta	tus	Into	rma	ition				c 1					
Radio S	Settin	gs																Auto Re	efresh	Interv	al: 11)		•
Radio	Status				01	N										Мо	de				AP			
MAC A	ddres	s			00	:19:	be:00):1b:7	70							Co	untry	Code			HC	NG KOI	NG	
Radio (Chann	el			24	12M	Hz(C	hanne	el 1)							Tra	nsmit	Power	r		25	dBm		
Wireles	ss Moo	le			2.	4GHz	: 144	Mbps	(802	.11ng	HT20	0												
Channe	el Usa	ae I	ist	Ope	eratii	1a C	hanı	nel: :	2412	MHz	(Cha	nnel 1	ա											
Sou	rtor		St	ato		т	v0/_		D	v 0/_		Ruci	19/-	Noi	co Elo	or dD	m) T	atorfo	mnco	Mitia	ation	Offen	10-5	ode
Jet			30	aue			0			15		Dus		NO	07[07	/ 071		literre 0	rence	mug	auon			oub
	J		0	41			0			ŧ0		02			-97[-97	[-97]		<u> </u>					эріу	
-	1		0	n			1		4	12		77			-97[-97	/-97]		0				A	oply	
2	2		Q	n			0		4	¥1		57			-97[-97	/-97]		0				A	oply	
3	3		o	n			0		4	13		69			-97[-97	/-97]		0				A	oply	
Nearby		ist [Enal	hle/	Disa	ble]																		
- Not Av	ailable	3 -	Lina		Disa	bicj																		
HOL AI	-cincibite	·																						
Tx/Rx	Statis	tics	[Re	set]																				
Rate (Mhne	`	1		2		5	5		11		6	0		12		18	24	1	36		48		54
Tx	%	' _	100		0			0		0		0	0		0		0	0		0		0		0
Rx	%		61		0		3	39		0		0	0		0		0	0		0		0		0
						_																		
MCS Type	0	1	2	3	4	5	6	/	8	9	10	11	12	13	14	15	16	1/	18	19	20	21	22	2
Rx%	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
104.70		Ŭ	Ŭ	5	5			5	9	5	5	0	0	0	0	0	0		0	5	0	5	3	
	Fra	me	Тур	e				C	ontro	l Fra	me			м	anage	ment	Frame	9			Data	Fram	е	
		Tx9	6							0						0						0		

Figure 85 – Radio O Status (detail)



Radio Settings

Radio Status – indicate the current status of Radio 0 interface
MAC – MAC address of Radio 0 interface
Radio Channel - indicate operating frequency (channel) of Radio 0
Wireless Mode – indicate 802.11 standards that Radio 0 operates
Mode – indicate operating mode of Radio 0
Country Code – indicate country code setting of Radio 0
Transmission Power – indicate the total transmission power of Radio 0

Channel Usage List

Tx(%) – average transmit frames percentage of operating channel
Rx(%) – average receive frames percentage of operating channel
Busy (%) – average busy state percentage of operating channel
Noise Floor (dBm) – in ate noise floor of operating channel and noise floor of chain 0, chain 1, and chain 2 on the control channel; if operating with 40MHz bandwidth, it shows the noise floor of chain 0, chain 1, and channel as well.

Interference Mitigation Offset (0-50dB) – signal offset option that will mask all noise / valid signal below 0-50 dB; 0 denotes disabled

Nearby AP List

If Nearby AP List is enabled, device collects nearby AP information and builds Nearby AP List from all beacon frames received during operation. Information shows the SSID, BSSID, authentication mode, cipher mode, operating channel, data rate, and received SNR of collected APs.

Tx/Rx Statistics

This statistic shows traffic distribution about Radio 0 interface. The statistical data includes distribution in terms of data rate and frame type for all incoming and outgoing data frame via Radio 0 interface.



6.3.2. Status > Radio0(2.4G) > Association List

This information is available on AP mode and Repeater mode only.

Status	Configuration	Administration	Tools	About				
Overview Rac	lioo(2.4G) Radio1(5G) Ethernet	Logs					
itatus - 🥂	ssociation List							
			Asso	ciation List				
							Pofro	eh
WLAN							None.	311
WLAN II) SSID	MAC Addre	ss Auth Mo	de Cipher	#Clients	Throughput	Total Traffic	с
0	Superwifi Net work 0	00:19:be:00:1	b:70 open	invalid	1	TX: 12.74Kbps RX: 4.91Kbps	TX: 91.12KB RX: 38.93KB	3
				Total	1	TX: 12.74Kbps RX: 4.91Kbps	TX: 91.12KB RX: 38.93KB	3
Station List	t <mark>SNR Distributio</mark>	n						
STA ID ♥	MAC Address	IP Addres	ss SNR(dB)) RSSI(dBm)	Throughput	Traffic	Data Rate	
0-1	b4:ce:f6:df:56:10	10.6.122.1	05 44	-53	TX: 14.71Kbps RX: 33.47Kbps	5 TX: 41.48KB 5 RX: 84.48KB	TX: 130Mbps RX: 130Mbps	æ
					* Only first 50 st	ations are listed. <u>S</u>	earch Station here	ə
Rogue Stat	ion List							
	WLAN		MAC A	ddress		Unblo	c k	
			This section	contains no values ye	ŧ			
Add Un	DIOCK AII							

Figure 86 – Radio O Association List

WAN

It shows the current status of all operating WLAN on Radio 0 interface. The information includes WLAN ID, SSID, MAC Address, authentication mode, cipher mode, number of associated clients, instant throughput, and total traffic of each operating WLAN respectively.

Station List

It shows the real time status of first 50 associated stations. The status includes Station ID, MAC Address, IP address, SNR(dB) of uplink, RSSI (dBm) of uplink, instant throughput, cumulated traffic of uplink and downlink, and instant data rate of uplink and downlink for each associated station respectively.

Rogue Station List

It lists out the stations that can potentially disrupt wireless networks and can sometimes cause irrevocable damage to the network owners. Network administrator inputs the rogue station's MAC address manually or selects any station from the station List by clicking .



6.4. Status > Radio1(5G)

6.4.1. Status > Radio1(5G) > Status

Status	Cor	nfigurat	on	Ad	ministrat	ion		Tools			About											
erview R	ladio0(2.4	IG) I	ladio:	l (5 G)	Ether	net	Logs															
atus -	Associ	ation L	st																			
								S	tatu	s Ir	nfori	mati	on									
Radio Set	ttings														A	uto Re	fresh	Interv	al: 10			۲
Radio Sta	atus			ON										Mode	е				AP			
MAC Add	ress			00:1	9:be:28:	01:5	5							Cour	ntry C	ode			HOI	NG KOT	١G	
Radio Ch	annel			5745	MHz(Ch	anne	149)							Tran	smit P	ower			28 (dBm		
Wireless	Mode			5GH2	866.7N	lbps(802.11	ac HT	80)													
Tx (c% 0		F	8x% 0			Bus	y%		1	Noise -105	Floor -105/-	(dBm) 105])	Inte	erfere 0	nce N	litiga	tion O	ffset(0-50 ply	dB)
Tx ((% 0		F	8x% 0			Bus 1	γ%		1	Noise -105	Floor -105/-	[dBm] 105])	Inte	erfere 0	nce N	litiga	tion O	ffset(0-50 ply	dB)
Tx (Nearby A	0 P List [Enabl	F e/Di	0 sable	e]		Bus 1	y%		1	Noise -105	Floor -105/-	[dBm] 105]		Inte	erfere 0	nce N	litiga	tion O	ffset(0-50 ply	dB)
Nearby A - Not Avail	(%) 0 IP List [lable -	Enabl	F ≥/Di	0 sable	e]		Bus 1	y%		1	Noise -105	Floor -105/-	(dBm) 105]		Int	0	nce N	litiga	tion O	ffset(0-50 ply	dB)
Tx (Nearby A - Not Avail Tx/Rx St:	0 P List [lable -	Enable [Rese	F 2/Di t]	0 0 sabl	e]		Bus 1	y%		1	Noise -105	Floor -105/-	[dBm] 105]		Inte	0	nce M	litiga	tion O	ffset(0-50	dB)
Tx (Nearby A - Not Avail Tx/Rx St: Rate (Mt	o P List (lable - atistics bps)	Enable [Rese	F 2/Di 2]	0 sable	e] 5.5		Bus 1	y %	6	'	Noise -105	Floor -105/-	(dBm) 105]	18	Inte	o 24	nce M	litiga 36	tion O	ffset(ply	dB) 54
Tx (Nearby A - Not Avail Tx/Rx St Rate (Mt Tx%	0 P List [lable - atistics	Enable [Rese 1 0	F 2/Di t]	0 sable 2 0	e] 5.5 0		Bus 1 11 0	γ%	6 0		9 0	-105/-	(dBm) 105] 2	18 0	Inte	24 0	nce M	iitiga 36 0	tion O	48 0	0-50	dB) 54
Tx (Nearby A - Not Avail Tx/Rx Sta Rate (Mt Tx% Rx%	o P List (lable - atistics	Enable [Rese 1 0 0	F 2/Di t]	2 0 2 0 0 0	e] 5.5 0 0		Bus 1 1 1 1 0 0	y%	6 0		9 0 0	105/-	(dBm) 105] 2	18 0 0	Inte	24 0 0	nce N	36 0	tion O	48 0 0	0-50	54 0
Tx (Nearby A - Not Avail Tx/Rx Sta Rate (Mt Tx% Rx% MCS (0 P List [lable - atistics bps)	Enable [Rese 1 0 0	F 2/Di t]	0 sable 2 0 0	e] 5.5 0 0 5 6	7	Bus 11 0 0 8	y%	6 0 0 10	11	9 0 12	1 1 1 1 1 1 1 3	(dBm) 105] 2 14	18 0 15	Inte 16	24 0 0 17	18	36 0 0 19	20	48 0 21	0-50 ply	54 0 0 23
Tx •	0 0 P List [lable - atistics 0 0 1 20 21	Enable [Rese 1 0 0 2 49	F 2/Di 21 3 7	2 0 2 0 0 2 1	 5.5 0 0 5 6 2 0 	7	Bus 11 0 0 8 8	9 0	6 0 0 10 0	11 0	9 0 0 12 0	105/- 105/-	2 105] 14 0	18 0 0 15 0	Interview 16 0	24 0 0 17 0	18 0	36 0 0 19 0	20 0	48 0 0 21 0	0-500 ply 22 0	54 0 23 0
Tx (1) Nearby A - Not Avail Tx/Rx Str Rate (Mt Tx% Rx% MCS Tx% Rx% MCS Rx%	c% 0 0 I atistics 0 0 1 20 21 1.8 74	Enable [Rese 1 0 0 2 49 8	F 2/Di 3 7 0	2 0 2 0 0 4 1 0	5.5 0 0 5 2 0 0 0	7 0	Bus 11 0 0 8 0 0	9 0 0	6 0 0 10 0 0	11 0 0	9 0 0 12 0	Floor -105/- 1 ((() 0 0	2 105] 14 0	18 0 0 15 0	Inte 16 0	24 0 0 17 0	18 0	36 0 0 19 0	20 0 0	48 0 0 21 0	0-500 ply 22 0 0	54 0 23 0 0
Tx (1) Nearby A - Not Avail Tx/Rx St: Rx% MCS Tx% Rx% MCS Tx% Rx%	c% 0 AP List [1 atistics 1 bps) 1 20 21 18 74 Frame 1	Enabl [Rese 1 0 0 2 49 8 Type	F 2/Di t] 3 7 0	2 0 2 0 0 0 4 1 0	 5.5 0 0 5 6 2 0 0 	7 0 0 0	Bus 11 0 0 8 0 0	9 0 0	6 0 0 0 10 0 0	11 0	9 0 0 12 0 0	Floor -105/- 1 (((1 3 0 0 0 Man	2 2 105] 14 0 0 3gen	18 0 0 15 0 0	Into 16 0 0	24 0 0 0 17 0 0	18 0	36 0 0 19 0 0	20 0 0 Data	<pre>ffset(</pre>	0-50 ply 22 0 0 0	54 0 0 23 0 0

Figure 87 – Radio 1 Status Information

Radio Settings

Radio Status – indicate the current status of Radio 1 interface MAC – MAC address of Radio 1 interface

Radio Channel - indicate operating frequency (channel) of Radio 1 Wireless Mode – indicate 802.11 standards that Radio 1 operates Mode – indicate operating mode of Radio 1

Country Code – indicate country code setting of Radio 1 Transmission Power – indicate the total transmission power of Radio 1

Channel Usage List

Tx(%) – average transmit frames percentage of operating channel
Rx(%) – average receive frames percentage of operating channel
Busy (%) – average busy state percentage of operating channel
Noise Floor (dBm) – indicate noise floor of operating channel and noise floor of chain 0, chain 1, and chain 2 on the control channel; if operating with 40MHz bandwidth, it shows the noise floor of chain 0, chain 1, and channel as well.

Interference Mitigation Offset (0-50dB) – signal offset option that will mask all noise / valid signal below 0-50 dB; 0 denotes disabled



Nearby AP List

If Nearby AP List is enabled, device collects nearby AP information and builds Nearby AP List from all beacon frames received during operation. Information shows the SSID, BSSID, authentication mode, cipher mode, operating channel, data rate, and received SNR of collected APs.

Tx/Rx Statistics

This statistic shows traffic distribution about Radio 1 interface. The statistical data includes distribution in terms of data rate and frame type for all incoming and outgoing data frame via Radio 1 interface.

6.4.2. Status > Radio1(5G) > Association List

Status	Configuration	Administration	Tools	About			
erview Rad	lio0(2.4G) Radio1(5G) Ethernet	Logs				
atus - A	ssociation List						
			Ass	ociation Lis	t		
							Defree
WLAN							Relies
WLAN II) SSID	MAC Addre	ess Auth I	Mode Ciphe	r #Clients	Throughput	Total Traffic
0	A8n (ac)	00:19:be:28:	01:55 op	en invalio	i 1	TX: 136.38Kbp RX: 15.82Kbp	os TX: 3.57MB s RX: 4.09MB
1	A8-Ein	02:19:be:28:	01:55 op	en invalio	i 0	TX: 0.00Kbps RX: 0.00Kbps	TX: 0.00KB RX: 0.00KB
				Tota	1	TX: 136.38Kbp RX: 15.82Kbp	os TX: 3.57MB s RX: 4.09MB
Station List	t SNR Distribution	D					
STA ID ♥	MAC Address	IP Addre	ss SNR(d	B) RSSI(d	3m) Through	nput Traffic	Data Rate
0-1	b4:ce:f6:df:56:10	10.6.122.1	105 14	-91	TX: 139.4 RX: 166.3	3Kbps TX: 3.56MB 1Kbps RX: 4.09MB	TX: 87.8Mbps RX: 13Mbps
					* Only first	50 stations are listed.	Search Station here
Rogue Stat	ion List						
	WLAN		MAC	Address		Unbl	ock
			This secti	on contains no val	ies vet		
					e		
Add	nblock All						

Figure 88 – Radio 1 Association List

WAN

It shows the current status of all operating WLAN on Radio 0 interface. The information includes WLAN ID, SSID, MAC Address, authentication mode, cipher mode, number of associated clients, instant throughput, and total traffic of each operating WLAN respectively.

Station List

It shows the real time status of first 50 associated stations. The status includes Station ID, MAC Address, IP address, SNR(dB) of uplink, RSSI (dBm) of uplink, instant throughput, cumulated traffic of uplink and downlink, and instant data rate of uplink and downlink for each associated station respectively.



Rogue Station List

It lists out the stations that can potentially disrupt wireless networks and can sometimes cause irrevocable damage to the network owners. Network administrator inputs the rogue station's MAC address manually or selects any station from the station List by clicking .



6.5. Status > Ethernet

Status Overview Rad	Configuration Adm lio0(2.4G) Radio1(5G)	inistration Tools Ethernet Logs	s Abo	ut			
<u>Status</u>			Ethernet	Status			
Port	MAC Address	Auto-negotiation	Speed	Duplex	Link Detected	Throughput	Traffic
eth0	00:19:be:20:03:c3	ON	1000Mb/s	Full	Yes	Tx: 0.00Kbps Rx: 0.00Kbps	Tx: 6.92MB Rx: 5.43MB

Figure 89 – Ethernet Status (detail)

6.5.1. Status > Ethernet > Status

It shows the current status of Ethernet interfaces. The information includes Port, MAC Address, Auto-negotiation, Speed, Duplex, Link Detected, instant throughput of uplink and downlink and traffic of of uplink and downlink on Ethernet 0 and Ethernet 1 respectively.

6.6. Status > Logs



Figure 90 – Status > Logs

In order to realize easier monitoring and diagnosis, A8n (ac) products provide log function for system information, association activity, and alarm event.

syslog – records the information about system information, such as software, hardware, system configuration, and self-checking result

wifi – records the information about association activity, such as association, dissociation, and roaming event

alarm – records the alert information of A8n (ac) device, such as radio down, too high CPU usage

Note:

 Syslog is one of the vital information for Altai's engineer for troubleshooting. It is highly recommended that syslog MUST be enabled



7.Embedded Tools for Deployment /

Operation / Troubleshooting

A8n (ac) products have various tools to help network administrator or engineer on deployment, operating, and troubleshooting. Tools include channel scan, ping ... etc.

7.1. Channel Scan

Network administrator and engineer collect the status of 2.4GHz radio and 5GHz radio in the surrounding area. Throughout this tool, network administrator and engineer collect noise floor, percentage of channel busy, and the number of BSS in particular radio channels.



Figure 91 – Chanel Scan Result (Overview)

A8n (ac) shows the channel scan result into Overview tab and AP List tab.

Overview Tab – displays general information from channel 1 to channel 11 at different sector. Information includes noise floor, percentage of channel busy, and the number of BSS on each channel respectively. **AP List Tab** - displays information scanned WLAN; information includes SSID, BSSID, authentication Mode, cipher, channel, rate in kbps, and received SNR (dB)



Sector X AP List Tab– displays information scanned WLAN in sector 0 – 4. X is the sector number. Information includes SSID, BSSID, authentication Mode, cipher, channel, rate in kbps, and received SNR (dB)

7.1.1. Perform channel scan on 2.4G radio

- 1. Go to Tools > Channel Scan > Radio 0 (2.4G)
- 2. [Optional] Provide channel scan interval from 100ms to 1000ms in **Duration**
- 3. Click Start Scan
- 4. Wait until Scan Status is changed from *In Process* to Success; it will take for 20 seconds approximately

Note:

- Wi-Fi service will be interrupted during channel scan

7.1.2. Perform channel scan on 5G radio

- 1. Go to Tools > Channel Scan > Radio 1 (5G)
- 2. [Optional] Provide channel scan interval from 100ms to 1000ms in **Duration**
- 3. Click Start Scan
- 4. Wait until Scan Status is changed from *In Process* to Success; it will take for 20 seconds approximately

Note:

- Wi-Fi service will be interrupted during channel scan

7.2. iPerf

A8n (ac) Series products embed iPerf server tool. Network Administrator / Engineer can test the throughput performance via Ethernet, Radio0, or Radio1 with this built-in tool.

Status Configuration Adm				
	inistration Tools	About		
nel Scan 🛛 i Perf 🛛 Diagnosis 🔤 Wal	tchdog			
	Deuf Comu			
	IPert Serve	er Configuration		
Server ID	Server Type	Server Port	Server Status	Deta
1	TCP	5001	OFF	2
2	UDP	5002	OFF	2
				Submit

Figure 92 – iPerf Server Configuration



7.2.1. Enable iPerf TCP Server

Status	Configuration	Administration	Tools	About
Channel Scan	iPerf Diagnosis	Watchdog		
			iPerf	f Server Setting
		Enable	Server:	
		Se	rver ID: 1	
		Serve	er Type: 🔍 UD	IDP Server
			Port: 5001	1
			(0-655)	535)
				Back to iPerf Server List Submit

Figure 93 – iPerf TCP Server Setting

- 1. Go to **Tools** > iPerf
- 2. Click d of either Sever ID 1 or Sever ID 2
- 3. Click Enable Server checkbox to enable iPerf TCP Server
- 4. Click **TCP Server** checkbox
- 5. Specify the listening port between 0 and 65535 on Port [Optional]
- 6. Click **Submit**
- 7. Click Save & Apply

7.2.2. Enable iPerf UDP Server

Status Configuration Administration To	ols About
Channel Scan iPerf Diagnosis Watchdog	
	iPerf Server Setting
Enable Server:	
Server ID:	2
Server Type:	UDP Server O TCP Server
Port:	5002
	(0-65335)
	Back to iPerf Server List Submit

Figure 94 – iPerf UDP Server Setting

- 1. Go to Tools > iPerf
- 2. Click dof either Sever ID 1 or Sever ID 2
- 3. Click Enable Server checkbox to enable iPerf UDP Server
- 4. Click **UDP Server** checkbox
- 5. Specify the listening port between 0 and 65535 on Port [Optional]
- 6. Click **Submit**
- 7. Click Save & Apply



7.3. Diagnosis

7.3.1. Ping Test

Network administrator and engineer test the reachability of a host and measures the round-trip time between A8n (ac) and the host over an Internet Protocol (IP) network by using ping tool.

Ig - <u>Traceroute</u> - <u>Tcpdump</u>	Dive Test
	Ping Test
Ping IP Address/Host Name:	 (example www.domain.com)
Packet Count:	4 ●(1-10000)
Packet Size:	66 (0-65500Bytes)
Dutput	Start
o results returned	

Figure 95 – Ping Test

7.3.2. Perform ping test

- 1. Go to Tools > Diagnosis > Ping
- 2. Type target IP address / host name in Ping IP Address/Host Name
- 3. [Optional] Specify how many ICMP (ping) packet that A8n (ac) sends to the target host in **Packet Count**; 4 is default setting
- 4. [Optional] Specify the packet size of ICMP packet in **Packet Size**; 56 is default setting
- 5. Click Start
- 6. Click **Stop** to terminate ping test if necessary

7.3.3. Traceroute Test

Network administrator tests the route (path) and measuring transit delays of packets across an Internet Protocol (IP) network by using traceroute test.



Status Configuration Administration To	ols About
nanner Scan Diagnosis Watchdog	
ing - Traceroute - Topdump	Traceroute Test
	Traceroute rest
Destination IP Address/Host Name:	(example www.domain.com)
Enable Resolve IP addresses:	
Timeout:	3 (1-100s)
Pings Per TTL:	3 (1-100)
Maximum TTL:	30 (1-100)
Output	Start Stop
No results returned	
	r

Figure 96 – Traceroute Test

How to perform traceroute test

- 1. Go to Tools > Diagnosis > traceroute
- 2. Type target IP address / host name in **Destination IP Address/Host** Name
- 3. [Optional] Click **Enable Resolve IP addresses** checkbox to enable IP address to domain name translation
- 4. [Optional] Specify timeout interval between 1s and 100s in **Timeout** for traceroute test
- 5. [Optional] Specify TTL value between 1 and 100 in **Pings Per TTL**; 3 is default setting
- 6. [Optional] Specify TTL value between 1 and 100 in Maximum TTL; 30 is default setting
- 7. Click Start
- 8. Click **Stop** to terminate ping test if necessary

7.3.4. Tcpdump

A8n (ac) provides a tool to capture packets that passing through a particular interface. It helps network administrator for troubleshooting.

Channel Scan Diagnosis Watchdog	
Ping - Traceroute - Tcpdump	
	Tcpdump Tool
Interface:	Radio1(5G) - WLAN1
Packet Count:	B0 × (1-1000000)
Capture File Size:	100 (1-100MByte)
Capture Status:	Ready
	Start Stop



How to perform packet capture on A8n (ac)'s interface

- 1. Go to Tools > Diagnosis > Tcpdump
- 2. Select suitable interface in Interface



- 3. [Optional] Specify maximum number of packet in **Packet Count**
- 4. [Optional] Specify maximum file size in Capture File Size
- 5. Click Start
- 6. Click **Stop** to terminate ping test if necessary
- 7. Download capture file after finished.

7.4. Watchdog

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

7.4.1. Schedule Reboot

Status Configuration Administration Too	ols About
Channel Scan Diagnosis Watchdog	
Schedule Reboot - Ping Watchdog	Schedule Rehoot
	Schedule Reboot
Periodic Reboot:	
Random Delay:	
Schedule Mode:	Sun Mon Tues Wed Thur
	🗌 Fri 🔲 Sat 00:00 🔽
Periodic Mode:	0(Days)
	0-30Days, 0 means Periodic mode disabled.
Deriodic Unload Log	
Periodic Opioad Log:	×
Random Delay:	
FTP Server User Name:	
FTP Server Password:	Show
FTP Server IP Address:	0 · 0 · D · D
FTP Server Port:	21
Schedule Mode:	Sun Mon Tues Wed Thur
	🗆 Fri 🔲 Sat 00:00 🔽
Periodic Mode:	0 (Davs)
	0-30Days, 0 means Periodic mode disabled.
	Submit

Figure 98 – Schedule Root

Enable periodic reboot

- 1. Go to Tools > Watchdog > Schedule Reboot
- 2. Click **Periodic Reboot** to enable reboot scheduler
- 3. You may change the following settings:

Radom Delay – Select the checkbox to enable a random delay on scheduled rebooting time. It prevents all APs reboot at the same time

Schedule ModeSelect exact time and day(s) for rebooting devicePeriodic ModeSelect a countdown timer (minute) for rebooting
device

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

Enable periodic log upload

- 1. Go to Tools > Watchdog > Schedule Reboot
- 2. Click Periodic Upload Log to enable upload log scheduler
- 3. You may change the following settings:



Radom Delay – Select the checkbox to enable a random delay on scheduled rebooting time. It prevents all APs reboot at the same time

FTP Server User Name – Type in username for logging in remote FTP server

FTP Server Password – Type in password for logging in remote FTP server

FTP Server IP Address - Type in IP address of remote FTP server

FTP Server Port - Specify service port of remote FTP server; 21 is default setting

Schedule ModeSelect exact time and day(s) for uploading logPeriodic ModeSelect a countdown timer (minute) for uploading log

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



7.4.2. Ping Watchdog

Ping watchdog is mechanism that A8n (ac) reboots itself if it fails to communicate (ping) to target host for serval time.

hedule Reboot - Ping Watchdog		
Ping Watchdog		
Enable Ping Watchdog:		
IP Address To Ping:	0.0.0.0	
Ping Interval:	300	
Startup Delay:	300 (60-300 Seconds)	
Failure Count to Reboot:	3	
	Submit	



Enable ping watchdog

- 1. Go to Tools > Watchdog > Ping watchdog
- 2. Click **Enable Ping Watchdog** to enable this function
- 3. Type in IP address of target host in IP Address To Ping
- 4. [Optional] Specify interval between each ICMP request in **Ping** Interval; 300 is default setting
- 5. [Optional] Specify delay time of each ICMP request in **Startup Delay**; 300 is default setting
- 6. [Optional] Specify fail tolerant in **Failure Count to Reboot**; 3 is default setting
- 7. Click **Submit**
- 8. Click Save & Apply



8. Collect Device's Product Information

A8n (ac) product shows the information about product information, hardware, software and company information in **About** tab.

ALTAI
Status Configuration Administration Tools About
Product Version
A8-Ein Super WIFI Base Station
Product Information Product Name: A8-Ein Product Code: SD.A8-EHN0-00 Product Serial Number: 1AN120200012 Product Serial Number: 1AN120200012 Product Model: WA8011N Housing: Ei Heater: supported Wireless Mode 11n: supported Hardware Version Version: 1.1 RF1 Version: 0.0 Software Version Version: 2.0.1103 FPGA: 0xcd MIB: 1.2
Radio Information(Radio0(2.4G)) Antenna Type: 15 Filters: 0/0/1/0/1/0
Company Information Company Name: Altai Technologies Limited Technical Support: support@altaitechnologies.com Web Site: http://www.altaitechnologies.com Company Address: Unit 209, 2/F, Lakeside 2, 10 Science Park West Avenue, HK Science Park, Shatin, Hong Kong

