Wireless LAN Controller Software User Guide

Table of Contents

目录

Chapter 1 Product Introduction

1.1 Product Description

Wireless controller transfers such features as wireless network and security handling to central WLAN switch for centralized management of all fit APs and wireless users. Featuring sophisticated RF management, link security backup, mandatory STA roaming and load balancing etc., this product is easy to upgrade and extend. By perfectly integrating with original network without changing its architecture, this product remarkably simplifies network deployment and management, and helps to save investment for users.

The AC series of wireless controllers independently developed by our company are operator-oriented novel high-speed wireless controllers. Thanks to the industry-leading multi-core processor architecture design, our products offer excellent data processing capacity and multi-service scalability, featuring high management AP capacity, strong processing performance, and diverse functional characteristics.

1.2 Product Features

The principal product features of the wireless controller are as follows:

1. High-performance and multi-form
2. Support network-wide seamless roaming
3. Support flexible networking based on distributed/centralized data forwarding architecture
4. Operation-level wireless user access control and management
5. AP location-based user access control
6. Intelligent load balancing technology
7. Highly reliable backup

Note: Please use IE8 browser to configure web management interface. User configuration is subject to actual product configuration page.

Chapter 2 Login Device Management

2.1 Introduction to WEB Management Login Interface

Wireless controller product is designed with built-in WEB Server; user could log into device via WEB management terminal (PC) for intuitive management and maintenance of device using the built-in WEB Server in a WEB-based manner.

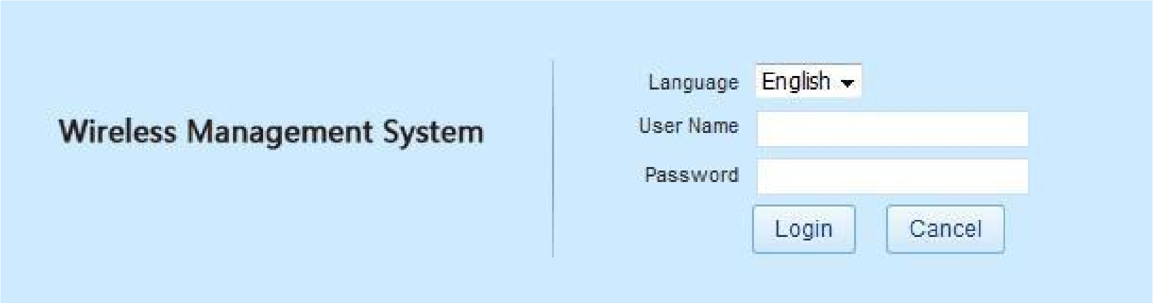
Wireless controller and WEB management terminal (PC) must be provided with corresponding network configuration so as to assure the normal login via WEB management.

Note:

1. The WEB Server of wireless controller is enabled by default; all front-panel network interfaces of factory default belong to default vlan with address 192.168.1.1. The network interface of web management terminal (PC) is connected with any interface on front panel; PC network card is configured as segment 192.168.1.X so as to manage wireless controller via WEB. Enter http://192.168.1.1 into the browser address field of WEB management terminal (PC), when the browser displays the WEB management login page, where user could enter the user name and password to log into Web management page for configuration.
2. For frame-type wireless controller, the web management terminal (PC) manages device through METH interface of master control board; the default address of management interface is 10.0.0.1; if the web management terminal (PC) is configured with segment 10.0.0.X, the frame-type wireless controller management page could be accessed in a way similar to the one mentioned above.

2.2 WEB Management Login

When user enters http://192.168.1.1 (the network between WEB management terminal and wireless controller must be unblocked) into browser address field of management PC, the browser shows WEB management login page (as shown in Fig. 2-1). Enter [user name] and [password] in login page ("admin" and "admin" by default), click on <login> button, and go to main interface of WEB management configuration upon successful login.


Wireless Management System

Language: English

User Name:

Password:

Fig. 2-1 WEB Management Login

The parameter description of WEB login interface is as shown in Table 2-1.

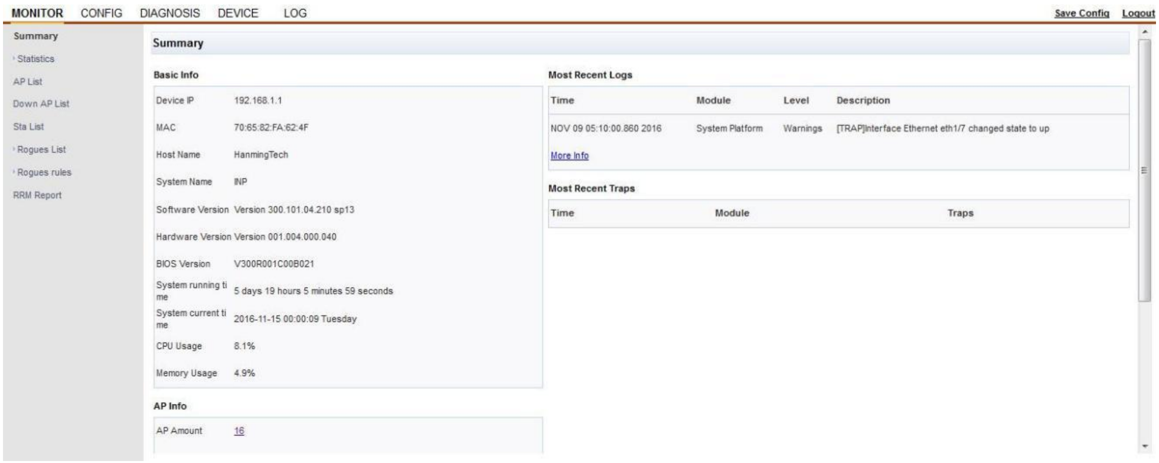
Configuration Item	**Description**
User Name	User account for system login
Password	The password for user account

Table 2-1 WEB Login Interface Parameter Description

Chapter 3 Network State

3.1 Function Description of Network State

This chapter describes the summary information of AC wireless control system, system statistics information, online status of AP, online status of STA, Rogues list information, Rogues rule information, and RRM report etc. Through the function query stated in this chapter, user could make a clear and quick understanding of system profile, multiple functions' statistical information, the online and offline status of AP, the online and offline status of STA, and the illegal and friendly AP\STA information in Rogues, and view RRM report information etc. [Network state] function comprises eight submenus, i.e. [Summary], [Statistics], [AP list], [Down AP list], [Terminal list], [Rogues list], [Rogues rule], and [RRM report], as shown in Fig. 3-1.



Summary

Basic Info

Device IP	192.168.1.1
MAC	70:65:82:FA:62:4F
Host Name	HanmingTech
System Name	INP
Software Version	Version 300.101.04.210 sp13
Hardware Version	Version 001.004.000.040
BIOS Version	V300R001C00B021
System running time	5 days 19 hours 5 minutes 59 seconds
System current time	2016-11-15 00:00:09 Tuesday
CPU Usage	8.1%
Memory Usage	4.9%

AP Info

AP Amount	16

Most Recent Logs

Time	Module	Level	Description
NOV 09 05:10:00.860 2016	System Platform	Warnings	[TRAP]Interface Ethernet eth1/7 changed state to up

More Info

Most Recent Traps

Time	Module	Traps

Fig. 3-1 Network State Management Page

3.2 Overview

[Summary] information page, as shown in Fig. 3-1, shows user the basic information of AC, the online/offline access information of Fit-AP and STA, the latest Log information, and the latest Trap information. The <more> button in the page links up with corresponding configuration page and AP/terminal information page.

The parameter description of summary page is as shown in Table 3-1.

The parameter description of summary page is as shown in Table 3-1.

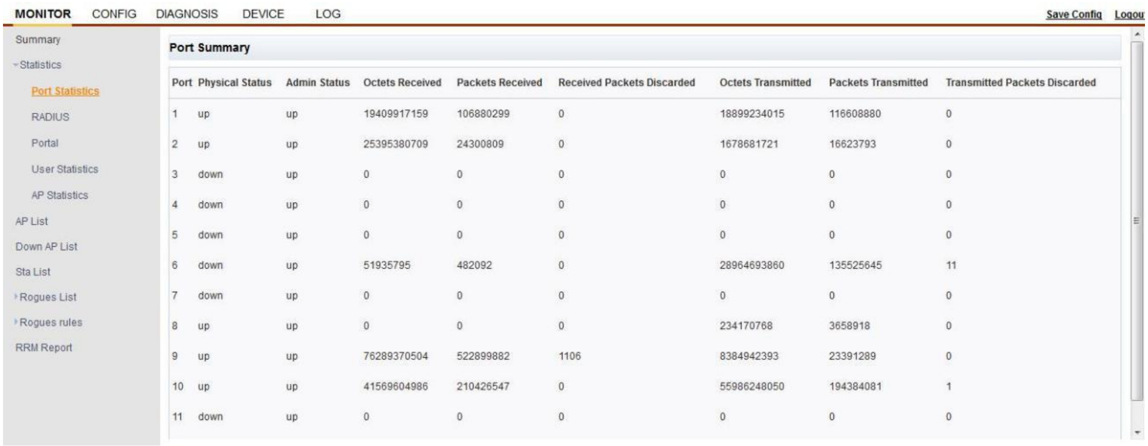
Parameter Item	**Description**
General Information	Show some general information of AC
AP Count	The total number of online and offline APs on this wireless controller AC, of which the value changes from time to time; AP count = Total online APs + Total offline APs; the counting is restarted after the rebooting of wireless controller device.
Total Online APs	The total number of online APs on this wireless controller AC, of which the value changes from time to time
Total Offline APs	The total number of offline APs on this wireless controller AC, of which the value changes from time to time
STA Count	The total number of online and offline STAs on this wireless controller AC, of which the value changes from time to time; STA count = Total online STAs + Total offline STAs; the counting is restarted after the rebooting of wireless controller device.
Total Online STAs	The total number of online STAs on this wireless controller AC, of which the value changes from time to time
Total Offline STAs	The total number of offline STAs on this wireless controller AC, of which the value changes from time to time
The Latest Log Information	Show the latest Log information in [log alarm] > [log message]
The Latest Trap Information	Show the latest Trap information in [device management] > [SNMP] > [Trap log]
More	View more latest Log/Trap information

Table 3-1 Summary Page Parameter Description

3.3 Statistics

[Statistics] shows the statistical information on port, RADIUS, Portal, user and AP performance.

[Port statistics] shows the statistical information on each port of wireless controller as shown in Fig. 3-2.

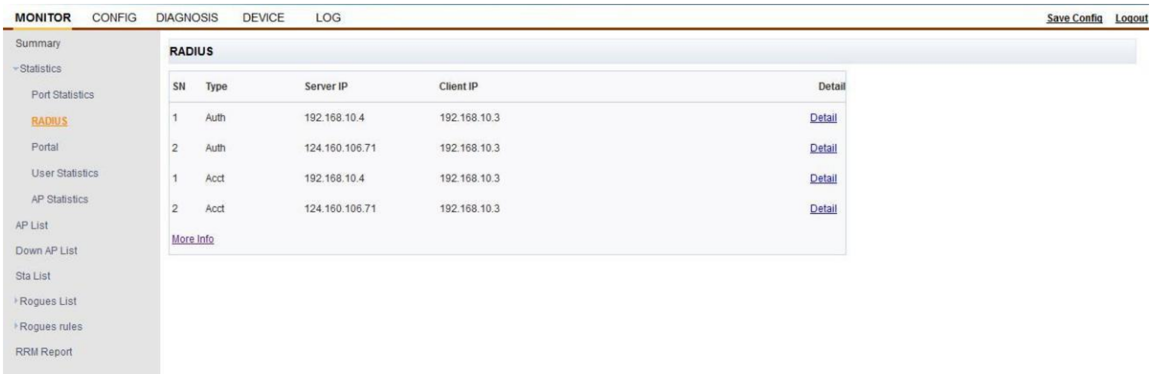


Port Summary

Port	Physical Status	Admin Status	Octets Received	Packets Received	Received Packets Discarded	Octets Transmitted	Packets Transmitted	Transmitted Packets Discarded
1	up	up	19409917159	106880299	0	18899234015	116608880	0
2	up	up	25395380709	24300809	0	1678681721	16623793	0
3	down	up	0	0	0	0	0	0
4	down	up	0	0	0	0	0	0
5	down	up	0	0	0	0	0	0
6	down	up	51935795	482092	0	28964693860	135525645	11
7	down	up	0	0	0	0	0	0
8	up	up	0	0	0	234170768	3658918	0
9	up	up	76289370504	522899882	1106	8384942393	23391289	0
10	up	up	41569604986	210426547	0	55986248050	194384081	1
11	down	up	0	0	0	0	0	0

Fig. 3-2 Port Statistics Information

[RADIUS statistics] shows the RADIUS authentication billing configuration information as shown in Fig. 3-3.

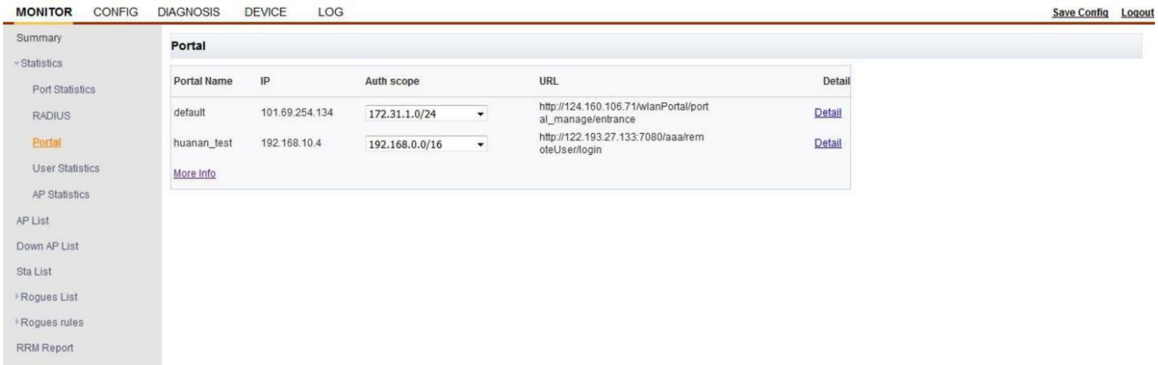


RADIUS

SN	Type	Server IP	Client IP	Detail
1	Auth	192.168.10.4	192.168.10.3	Detail
2	Auth	124.160.106.71	192.168.10.3	Detail
1	Acct	192.168.10.4	192.168.10.3	Detail
2	Acct	124.160.106.71	192.168.10.3	Detail

Fig.3-3 RADIUS Configuration Information

[Portal statistics] shows Portal configuration information as shown in Fig. 3-4.

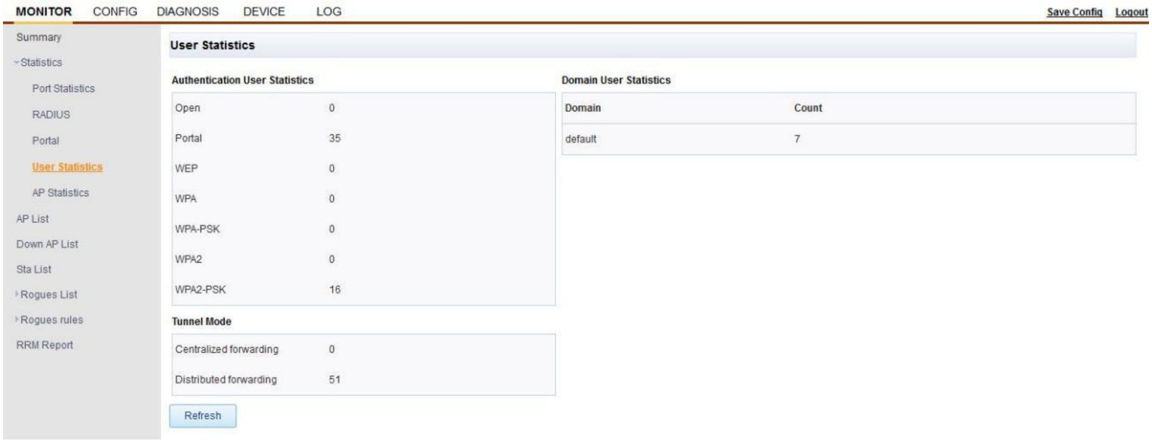


Portal

Portal Name	IP	Auth scope	URL	Detail
default	101.69.254.134	172.31.1.0/24	http://124.160.106.71/wlanPortal/portal_manage/entrance	Detail
huanan_test	192.168.10.4	192.168.0.0/16	http://122.193.27.133:7080/aaa/remoteUser/login	Detail

Fig. 3.4 Portal Configuration Information

[User statistics] shows the statistical information on user of wireless controller as shown in Fig. 3-5.



User Statistics

Authentication User Statistics

Open	0
Portal	35
WEP	0
WPA	0
WPA-PSK	0
WPA2	0
WPA2-PSK	16

Tunnel Mode

Centralized forwarding	0
Distributed forwarding	51

Domain User Statistics

Domain	Count
default	7

Fig. 3.5 User Statistics Information

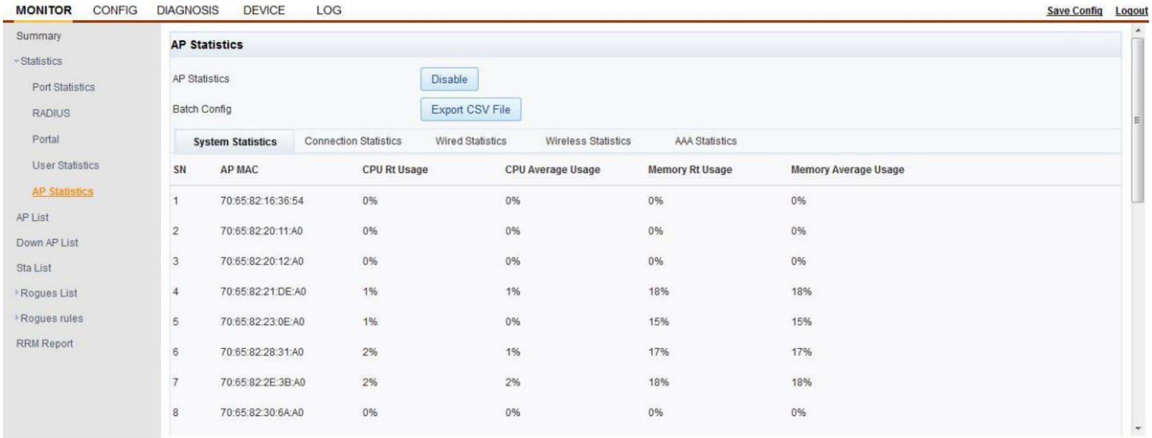
The user statistics information parameter description is as shown in Table 3-2.

Parameter Item	**Description**
Authenticated User Statistics	Show the authenticated user statistics in various encryption modes
Open	The number of terminal users connected to fit AP in a password-less fashion
Portal	The number of portal-authenticated terminal users, including the associated unauthenticated users
WEP	The number of WEP-encrypted terminal users
WPA	The number of WPA-encrypted terminal users
WPA-PSK	The number of WPA-PSK-encrypted terminal users
WPA2	The number of WPA2-encrypted terminal users
WPA2-PSK	The number of WPA2-PSK-encrypted terminal users
Distributed Forwarding	The number of users with distributed forwarding
Default Domain	The number of default domain-authenticated users

Table 3-2 User Statistics Information Parameter Description

[AP performance statistics] shows the statistical information on performance of all APs managed by wireless controller.

[System statistics] shows the statistical information on system performance of each AP as shown in Fig. 3-6.



AP Statistics

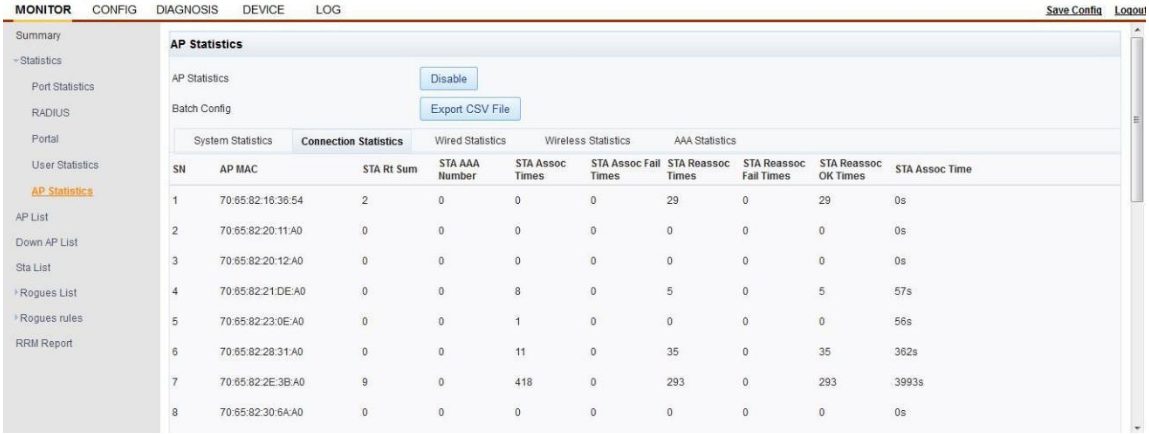
AP Statistics: Disable

Batch Config: Export CSV File

SN	AP MAC	CPU Rt Usage	CPU Average Usage	Memory Rt Usage	Memory Average Usage
1	70:65:82:16:36:54	0%	0%	0%	0%
2	70:65:82:20:11:A0	0%	0%	0%	0%
3	70:65:82:20:12:A0	0%	0%	0%	0%
4	70:65:82:21:DE:A0	1%	1%	18%	18%
5	70:65:82:23:0E:A0	1%	0%	15%	15%
6	70:65:82:28:31:A0	2%	1%	17%	17%
7	70:65:82:2E:3B:A0	2%	2%	18%	18%
8	70:65:82:30:6A:A0	0%	0%	0%	0%

Fig. 3-6 Statistical Information on FIT AP System

[Connection statistics] shows statistical information on associated terminal as shown in Fig. 3-7.



AP Statistics

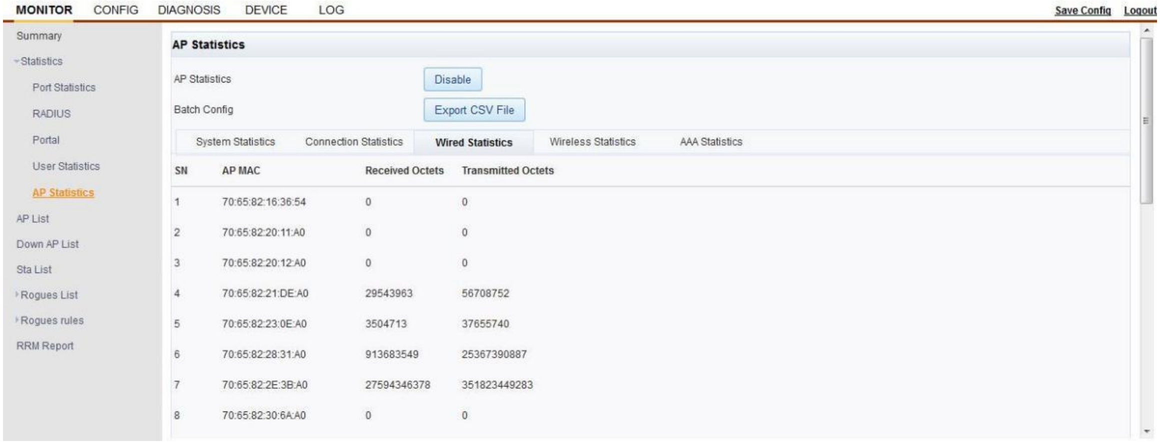
AP Statistics: Disable

Batch Config: Export CSV File

SN	AP MAC	STA Rt Sum	STA AAA Number	STA Assoc Times	STA Assoc Fail Times	STA Reassoc Times	STA Reassoc Fail Times	STA Reassoc OK Times	STA Assoc Time
1	70:65:82:16:36:54	2	0	0	0	29	0	29	0s
2	70:65:82:20:11:A0	0	0	0	0	0	0	0	0s
3	70:65:82:20:12:A0	0	0	0	0	0	0	0	0s
4	70:65:82:21:DE:A0	0	0	8	0	5	0	5	57s
5	70:65:82:23:0E:A0	0	0	1	0	0	0	0	56s
6	70:65:82:28:31:A0	0	0	11	0	35	0	35	362s
7	70:65:82:2E:3B:A0	9	0	418	0	293	0	293	3993s
8	70:65:82:30:6A:A0	0	0	0	0	0	0	0	0s

Fig. 3-7 Statistical Information on FIT AP Associated Terminal

[Wired statistics] shows the information on wired statistics of fit AP as shown in Fig. 3-8.



AP Statistics

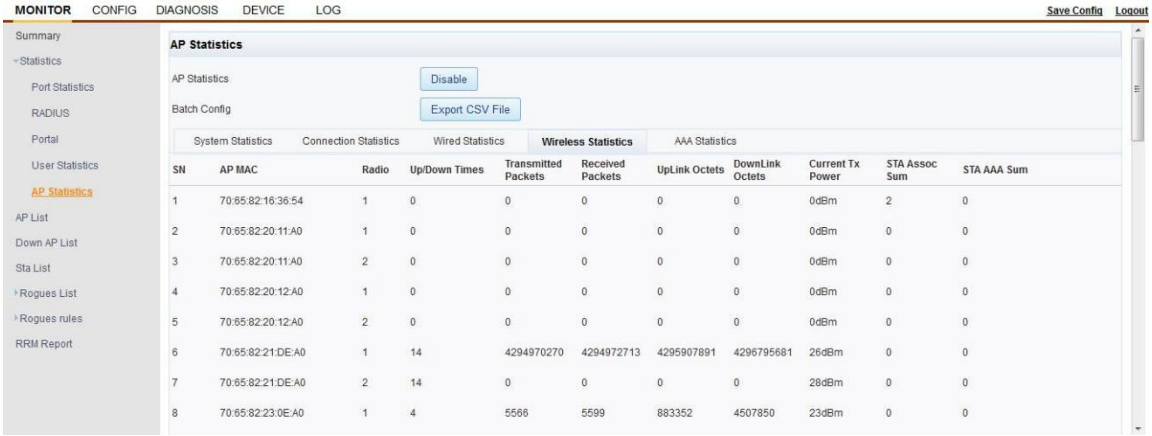
AP Statistics: Disable

Batch Config: Export CSV File

SN	AP MAC	Received Octets	Transmitted Octets
1	70:65:82:16:36:54	0	0
2	70:65:82:20:11:A0	0	0
3	70:65:82:20:12:A0	0	0
4	70:65:82:21:DE:A0	29543963	56708752
5	70:65:82:23:0E:A0	3504713	37655740
6	70:65:82:28:31:A0	913683549	25367390887
7	70:65:82:2E:3B:A0	27594346378	351823449283
8	70:65:82:30:6A:A0	0	0

Fig. 3-8 Statistical Information on Wired Terminal of FIT AP

[Wireless statistics] shows the statistical information on wireless terminal of fit AP as shown in Fig. 3-9.



AP Statistics

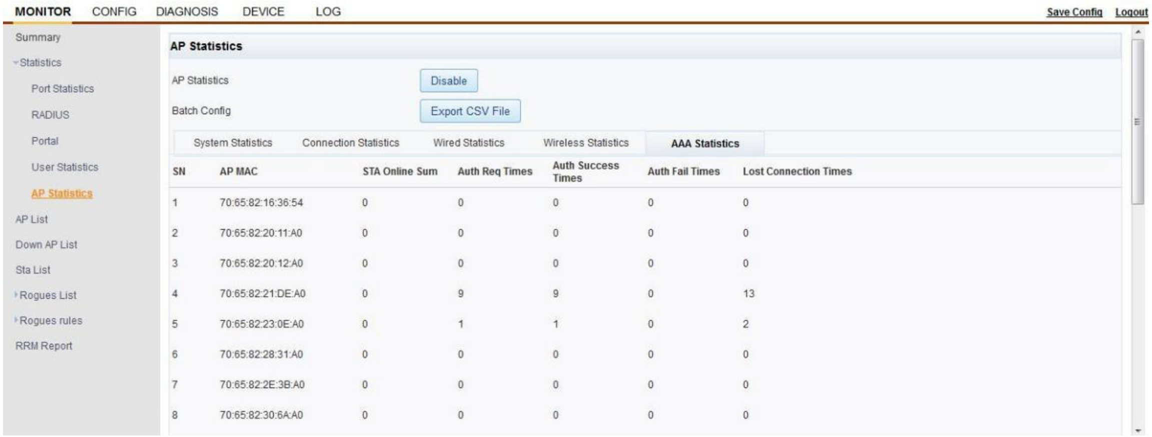
AP Statistics: Disable

Batch Config: Export CSV File

SN	AP MAC	Radio	Up/Down Times	Transmitted Packets	Received Packets	UpLink Octets	DownLink Octets	Current Tx Power	STA Assoc Sum	STA AAA Sum
1	70:65:82:16:36:54	1	0	0	0	0	0	0dBm	2	0
2	70:65:82:20:11:A0	1	0	0	0	0	0	0dBm	0	0
3	70:65:82:20:11:A0	2	0	0	0	0	0	0dBm	0	0
4	70:65:82:20:12:A0	1	0	0	0	0	0	0dBm	0	0
5	70:65:82:20:12:A0	2	0	0	0	0	0	0dBm	0	0
6	70:65:82:21:DE:A0	1	14	4294970270	4294972713	4295907891	4296795681	26dBm	0	0
7	70:65:82:21:DE:A0	2	14	0	0	0	0	28dBm	0	0
8	70:65:82:23:0E:A0	1	4	5566	5599	883352	4507850	23dBm	0	0

Fig.3 -9 Statistical Information on Wireless Terminal of FIT AP

[Authentication statistics] shows the statistical information on authenticated terminal of fit AP as shown in Fig. 3-10.



AP Statistics

AP Statistics: Disable

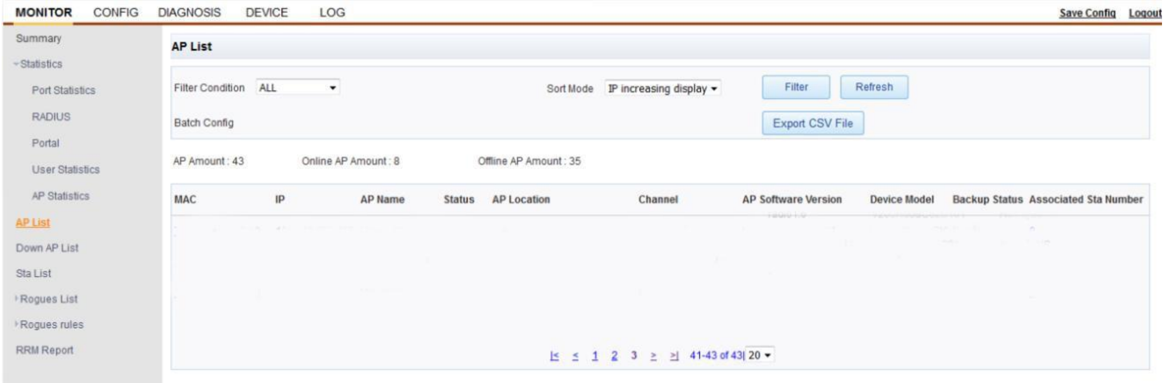
Batch Config: Export CSV File

SN	AP MAC	STA Online Sum	Auth Req Times	Auth Success Times	Auth Fail Times	Lost Connection Times
1	70:65:82:16:36:54	0	0	0	0	0
2	70:65:82:20:11:A0	0	0	0	0	0
3	70:65:82:20:12:A0	0	0	0	0	0
4	70:65:82:21:DE:A0	0	9	9	0	13
5	70:65:82:23:0E:A0	0	1	1	0	2
6	70:65:82:28:31:A0	0	0	0	0	0
7	70:65:82:2E:3B:A0	0	0	0	0	0
8	70:65:82:30:6A:A0	0	0	0	0	0

Fig. 3-10 Statistical Information on Authenticated Terminal of FIT AP

3.4 AP List

[AP list] shows the real-time statistical information of AP on current AC wireless controller, principally including all APs ever connected to AC, the current online state of AP, the number of STAs associated with online AP, the MAC address of AP, IP address, software version and device model etc. as shown in Fig. 3-11.



AP List

Filter Condition: ALL

Sort Mode: IP increasing display

Batch Config

AP Amount : 43 Online AP Amount : 8 Offline AP Amount : 35

MAC	IP	AP Name	Status	AP Location	Channel	AP Software Version	Device Model	Backup Status	Associated Sta Number

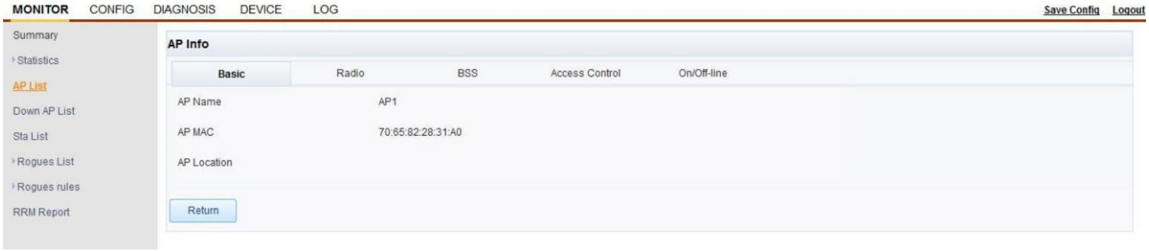
Fig. 3.11 AP List Information

The AP list page parameter description is as shown in Table 3-3.

Parameter Item	**Description**
Filter Criteria	Filter the massive data records in AP list using different values as criteria; click on <filter> button, when only AP lists meeting filter criteria are displayed and filtering
Arrangement Mode	User could sort AP list information in “IP ascending order” or “IP descending order”
Refresh	Manually refresh AP list data information
Export CSV File	Export all information in AP list in CSV file
AP Count	Total number of online and offline APs on this wireless controller AC
Online AP Count	The total number of online APs on this wireless controller AC, of which the value changes from time to time
Offline AP Count	The total number of offline APs on this wireless controller AC, of which the value changes from time to time
MAC Address	The actual MAC address information of AP; statistics mac address link is used to view the [detailed information] of AP
IP Address	Actual IP address information of AP
AP Name	The AP name parameter information reported by AP to AC
State	Current online/offline state of AP
AP Deployment Location	The information entered by user for this AP’s “deployment location” during AP deployment
AP Software Version	AP’s actual software version information reported to AC when AP goes online
Device Model	AP’s device model & type information reported to AC when AP goes online
Backup State	AC’s main/standby state; “master” is displayed when AP is on main AC; “standby” is displayed when AP is on standby AC
Number of Terminals	The number of STAs associated with this AP; click on this value to open [terminal list] page for viewing the details of terminal

Table 3-3 AP List Page Parameter Description

The detailed information of AP is as shown in Fig. 3-12.



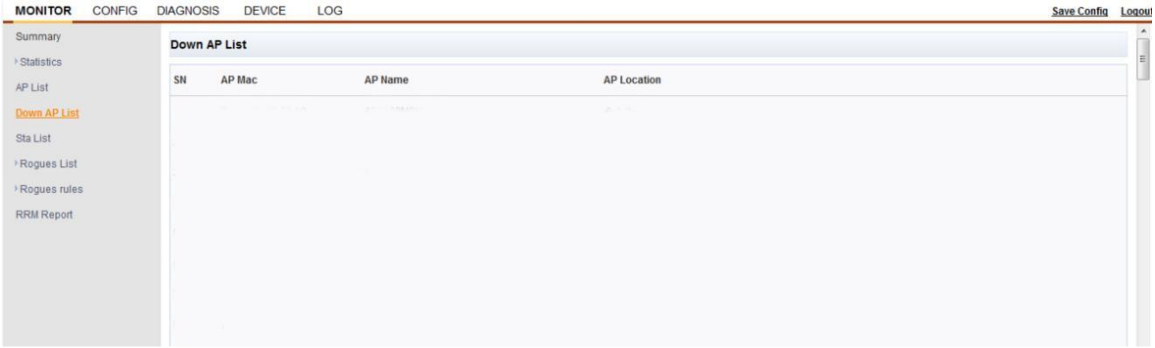
AP Info

AP Name	AP1
AP MAC	70:65:82:28:31:A0
AP Location	

Fig. 3-12 Detailed Information of AP

3.5 Down AP List

[Down AP list] shows the information about the AP that got connected to AC and did not go online after AC restart, including AP Mac, AP name, and AP deployment location etc. as shown in Fig. 3-13.



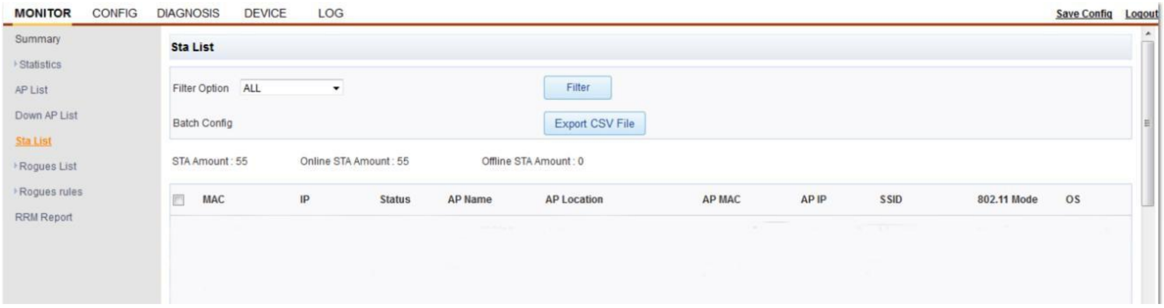
Down AP List

SN	AP Mac	AP Name	AP Location

Fig. 3-13 Down AP List Information

3.6 Terminal List

[Terminal list] page shows the information about terminals in wireless controller system, including STA count, the number of online STAs, and the number of offline STAs as shown in Fig. 3-14. User could search for eligible STAs based on different filter criteria, including AP’s IP, AP’s MAC, STA’s MAC, operating system, and slot.



Sta List

Filter Option ALL

Batch Config

STA Amount : 55 Online STA Amount : 55 Offline STA Amount : 0

□	MAC	IP	Status	AP Name	AP Location	AP MAC	AP IP	SSID	802.11 Mode	OS

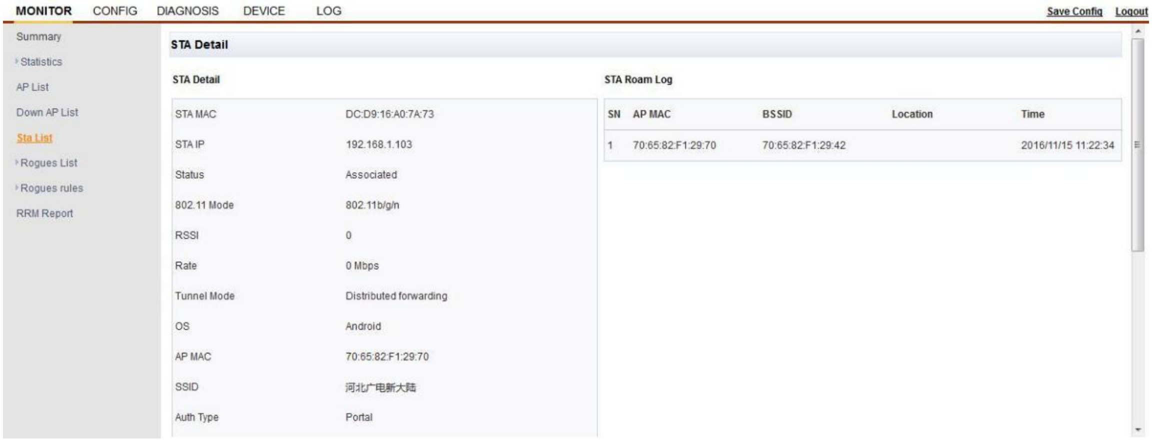
Fig. 3-14 Terminal List Information

The terminal list page parameter description is as shown in Table 3-4.

Parameter Item	**Description**
Filter Criteria	Filter the massive data records in terminal using different values as criteria; click on <filter> button, when the terminal list only displays the terminal information meeting filter criteria
Export CSV File	Export all terminal information in CSV file
STA Count	Total number of online and offline APs on this wireless controller AC
Total Online STAs	The total number of online STAs on this wireless controller AC, of which the value changes from time to time
Total Offline STAs	The total number of offline STAs on this wireless controller AC, of which the value changes from time to time
MAC Address	The actual MAC address information of STA; click on link to view [STA details], including the roaming record of STA
IP Address	The IP address of STA
State	The registered states of STA in AC include “associated”, “unassociated” and “licensed”. The “licensed” state is indicated when STA is associated with AC through portal authentication; the “associated” state is indicated when STA is associated with AC through non-portal authentication; “unassociated” state is indicated when STA is off-line
AP Name	The AP name associated with this STA
AP MAC Address	The AP MAC address associated with this STA
AP IP Address	The AP IP address associated with this STA
SSID	The SSID information associated with STA
802.11 Work Mode	The 802.11 work mode of RF where this AP’s SSID is located
Operating System	The type of operating system of STA

Table 3-4 Terminal List Page Parameter Description

The detailed information of STA is as shown in Fig. 3-15.



STA Detail

STA Detail

STA MAC	DC:D9:16:A0:7A:73
STA IP	192.168.1.103
Status	Associated
802.11 Mode	802.11b/g/n
RSSI	0
Rate	0 Mbps
Tunnel Mode	Distributed forwarding
OS	Android
AP MAC	70:65:82:F1:29:70
SSID	河北广电新大陆
Auth Type	Portal

STA Roam Log

SN	AP MAC	BSSID	Location	Time
1	70:65:82:F1:29:70	70:65:82:F1:29:42		2016/11/15 11:22:34

Fig. 3-15 Detailed Information of STA

Chapter 4 RRM

4.1 RRM Function Description

WLAN Radio Resource Management (WLAN RRM) is a real-time intelligent RF management solution that offers a systematized real-time intelligent RF management approach so that wireless network could efficiently adapt to changes in wireless environment and maintain the optimal state of radio frequency resources through “acquisition (AP collects RF environment information in real time) -> analysis (AC performs analysis & evaluation of data acquired by AP) -> decision-making (AC performs coordinated management of channel assignment and transmitting power based on analysis result) -> execution (AP executes AC-set configuration for RF resources optimization)”.

4.2 Basic Workflow of RRM

The RRM workflow is as follows:

1. The same group name shall be assigned to all ACs throughout the system so that AP could authenticate whether the detected APs are the members from the same system.

2. AP periodically sends neighbor message and shares its own information, including the AC to which it is connected (IP+PORT) and its group name; these advertisements could be received by APs with the same group name.

3. AP receives the detected neighbor message based on its own group name, and uploads the information to the connected AC.

4. After learning about the ACs contained in this group, AC shares with the entire group the RF environment information it acquired, and elects a Group Leader.

5. The Group Leader ultimately acquires the RF environment information of every AP within the group, and then performs automatic channel adjustment with purpose of optimal AP configuration parameters, in which case the automatic power adjustment algorithm (blind spot detection coverage and fault self-healing are based on individual ACs) could run.

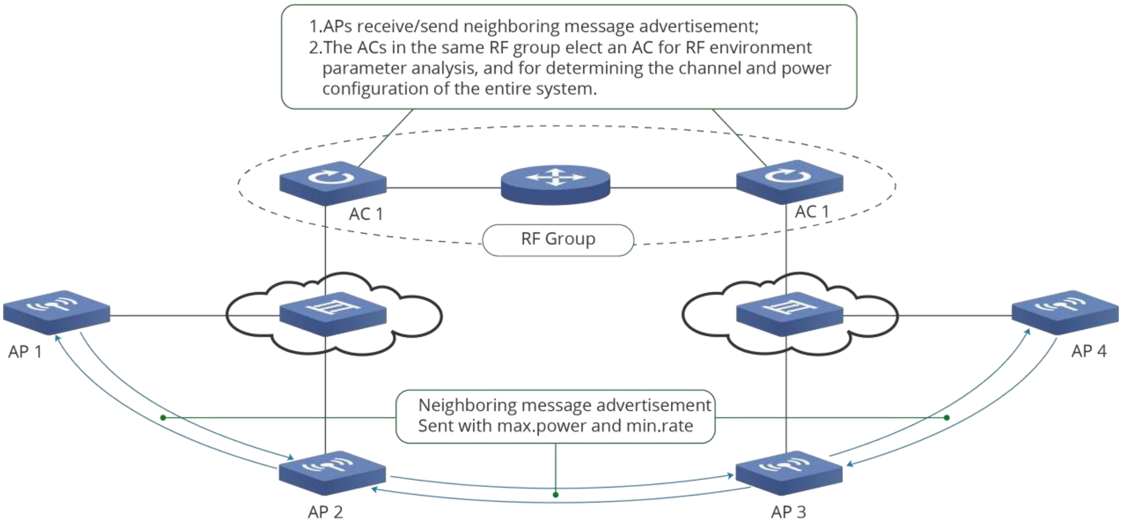
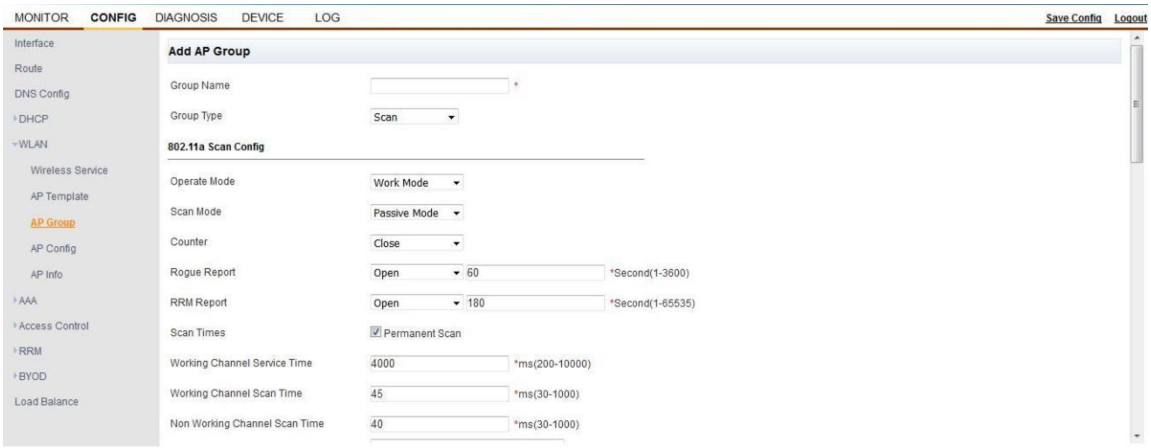

1.APs receive/send neighboring message advertisement;
2.The ACs in the same RF group elect an AC for RF environment parameter analysis, and for determining the channel and power configuration of the entire system.
AC 1
AC 1
RF Group
AP 1
AP 4
Neighboring message advertisement
Sent with max.power and min.rate
AP 2
AP 3

Fig. 4-1 RRM Workflow

4.3 Create Scan Group

To enable RRM, it’s essential to create a scan group in AP group as shown in Fig. 4-2.



Add AP Group

Group Name		*
Group Type	Scan	

802.11a Scan Config

Operate Mode	Work Mode	
Scan Mode	Passive Mode	
Counter	Close	
Rogue Report	Open 60	*Second(1-3600)
RRM Report	Open 180	*Second(1-65535)
Scan Times	☑ Permanent Scan	
Working Channel Service Time	4000	*ms(200-10000)
Working Channel Scan Time	45	*ms(30-1000)
Non Working Channel Scan Time	40	*ms(30-1000)

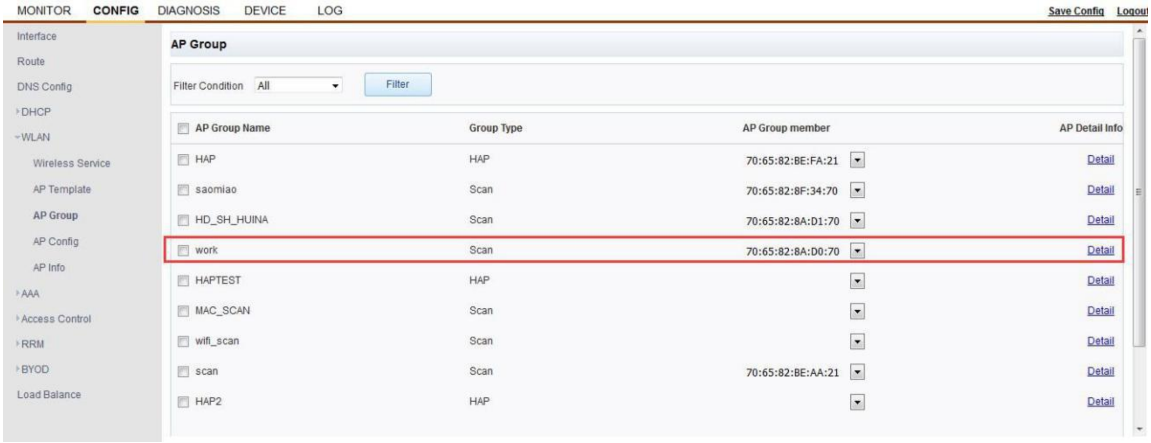
Fig. 4-2 Scan Group Addition Page

The parameter description of scan group is as shown in Table 4-1.

Parameter Item	**Description**
Group name	The name of AP group
Type	The type of AP group, including mirror image upgrade, backup, HAP, and scan; “scan” is selected when creating a scan group
802.11a Scan Configuration	5.8G RF scan configuration
Operating Mode	Include “work mode” and “detection mode”. AP functions properly in work mode; AP only does scanning without offering normal service in detection mode. Work mode is selected by default
Scan Mode	Include “passive mode” and “active mode”. In passive mode, AP monitors the message sending & receiving condition at null interface, identifies the AP and Ad hoc networks at null interface based on beacon frame and its parameters, and further identifies the STAs under each AP; in active mode, AP monitors null interface message, initiatively sends broadcast probe, and perform detection based on problem response
Rogue Countering	Enable/disable AP's Rogue countering function within group. The function is disabled by default
Rogue Reporting	Enable/disable AP's reporting of Rogue AP or STA information; “[network state] > [Rogues list]” has no information unless Rogue reporting is enabled. Rogues reporting is enabled by default
RRM Reporting	Enable/disable RRM reporting; “[network state] > [RRM report]” has no information unless RRM reporting is enabled. RRM reporting is enabled by default
Number of Scans	Define the number of scans; “permanent scanning” is enabled by default; the number of scans could be set when “permanent scanning” is disabled. A scan cycle is finished when AP completely scans all channels required to be scanned
Regular Scan	When “the number of scans” is not set to “permanent scanning”, regular scan could be enabled, in which case user could manually set the interval of regular scan and "scan now”
Working cChannel Service Time	The duration of message sending & receiving service offered by AP in working channel during scanning
Scan Time in Working Channel	The scanning time in AP's working channel
Scan Time in non-working Channel	Scanning time in user-designated channel set (except working channel)
Channel Set	User-designated collection of channels for scanning
Neighboring OUI	The first 6 bits of BSSID adjacent to AP used to obtain neighboring AP information
802.11b Scan Configuration	2.4G RF scan configuration, of which the parameter description is the same as above

Table 4-1 Scan Group Parameter Description

Scan group page is as shown in Fig. 4-3.



AP Group

Filter Condition: All

☐ AP Group Name	Group Type	AP Group member	AP Detail Info
☐ HAP	HAP	70:65:82:BE:FA:21	Detail
☐ saomiao	Scan	70:65:82:8F:34:70	Detail
☐ HD_SH_HUINA	Scan	70:65:82:8A:D1:70	Detail
☐ work	Scan	70:65:82:8A:D0:70	Detail
☐ HAPTEST	HAP		Detail
☐ MAC_SCAN	Scan		Detail
☐ wifi_scan	Scan		Detail
☐ scan	Scan	70:65:82:BE:AA:21	Detail
☐ HAP2	HAP		Detail

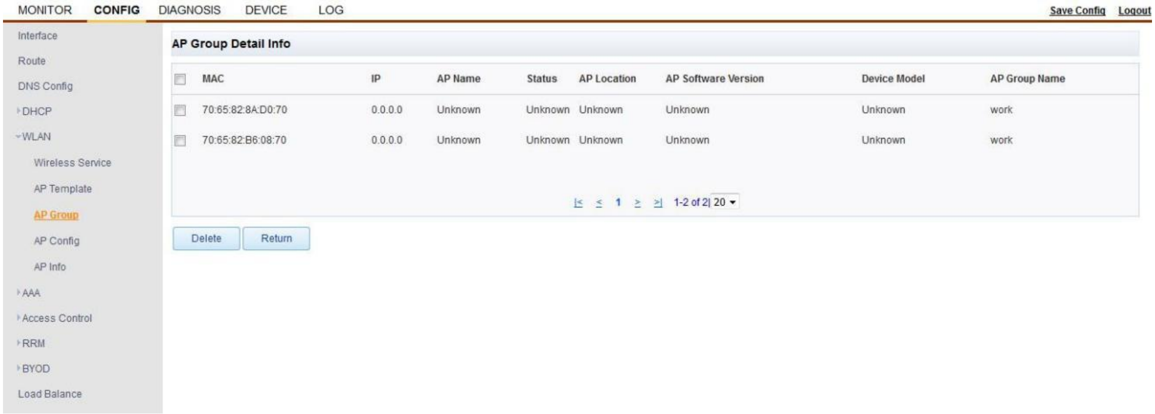
Fig. 4-3 Scan Group Information

The parameter description of scan group is as shown in Table 4-2.

Parameter Item	**Description**
Filter Criteria	Filter AP group by group type
Detailed Information	View the detailed information of this AP group
Create	Create different types of AP groups
Edit	Edit the information of chosen AP group
Delete	Delete AP group

Table 4-2 Scan Group Parameter Description

The detailed information of scan group is as shown in Fig. 4-4.



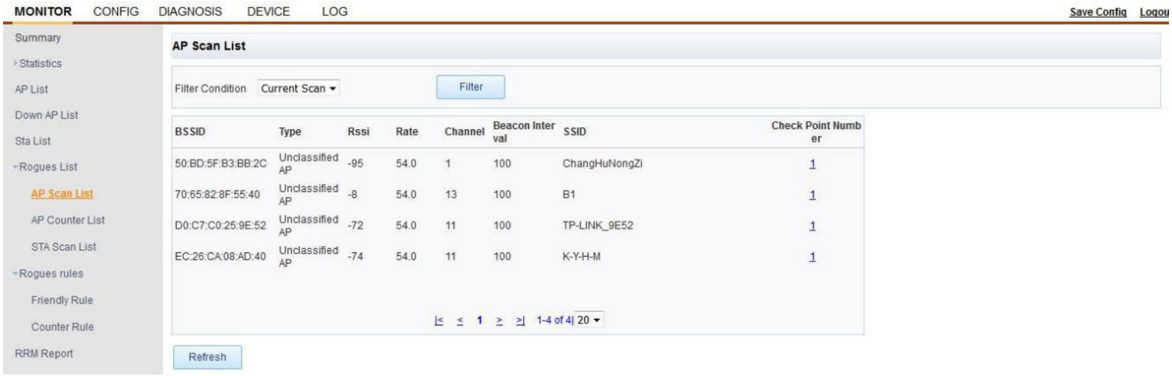
AP Group Detail Info

☐ MAC	IP	AP Name	Status	AP Location	AP Software Version	Device Model	AP Group Name
☐ 70:65:82:8A:D0:70	0.0.0.0	Unknown	Unknown	Unknown	Unknown	Unknown	work
☐ 70:65:82:B6:08:70	0.0.0.0	Unknown	Unknown	Unknown	Unknown	Unknown	work

Fig. 4-4 Detailed Information of Scan Group

4.4 Rogues List

[AP scan list] shows all AP information scanned in the current environment, including AP's BSSID, type, Rssi, rate, channel, Beacon interval, SSID, and the number of detection points as shown in Fig. 4-5.



AP Scan List

Filter Condition: Current Scan ▾ Filter

BSSID	Type	Rssi	Rate	Channel	Beacon Interval	SSID	Check Point Number
50:BD:5F:B3:BB:2C	Unclassified AP	-95	54.0	1	100	ChangHuNongZi	1
70:65:82:8F:55:40	Unclassified AP	-8	54.0	13	100	B1	1
D0:C7:C0:25:9E:52	Unclassified AP	-72	54.0	11	100	TP-LINK_9E52	1
EC:26:CA:08:AD:40	Unclassified AP	-74	54.0	11	100	K-Y-H-M	1

|< < 1 > >| 1-4 of 4| 20 ▾

Refresh

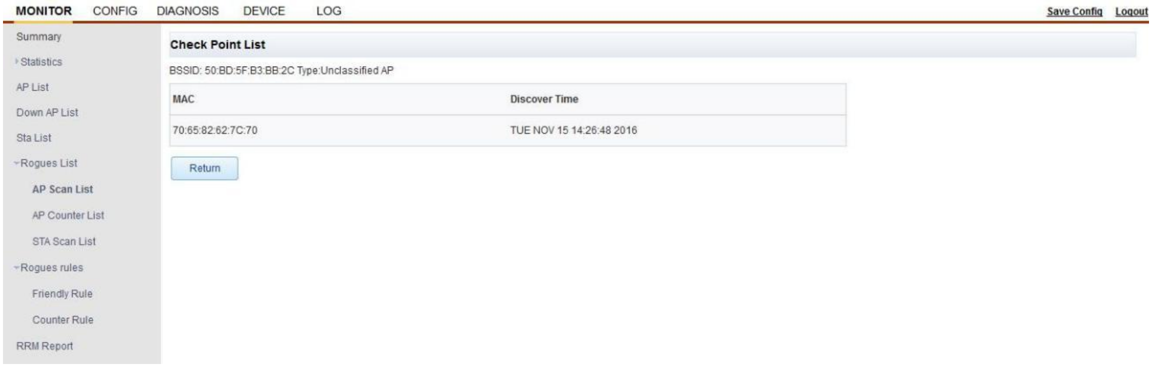
Fig. 4-5 AP Scan List Information

The parameter description of AP scan list is as shown in Table 4-3.

Parameter Item	Description
Filter Criteria	Filter AP information by type
Number of Detection Points	Click on<the number of detection points> link to open [the list of detection points]
Refresh	Refresh current list information

Table 4-3 AP Scan List Parameter Description

The detection point list is as shown in Fig. 4-6.



Check Point List

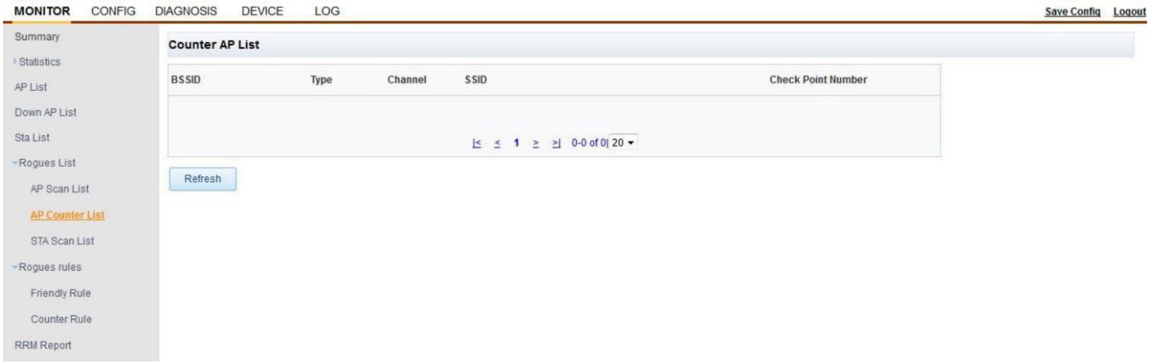
BSSID: 50:BD:5F:B3:BB:2C Type:Unclassified AP

MAC	Discover Time
70:65:82:62:7C:70	TUE NOV 15 14:26:48 2016

Return

Fig. 4-6 List of Detection Points

[AP counter list] shows the AP counter rule-compliant surrounding AP information on condition that counter rules are established in "[Rogues rule] > [list of AP rules]" as shown in Fig. 4-7.

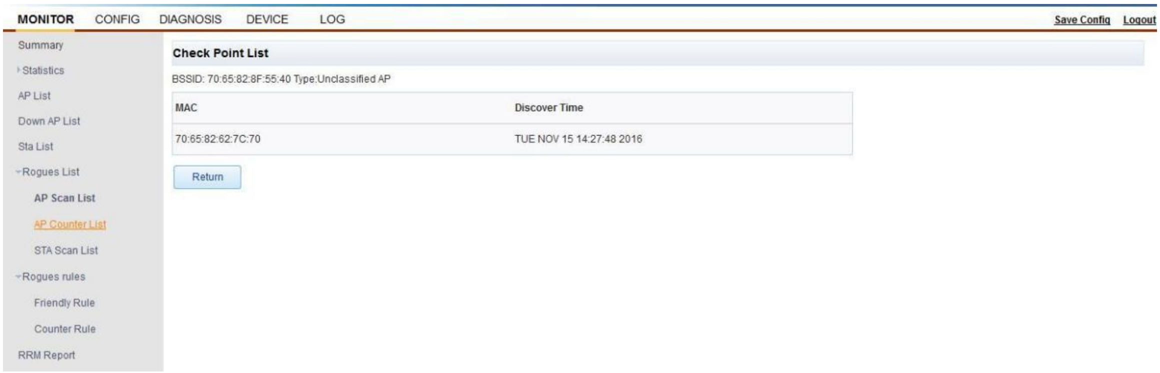


Counter AP List

BSSID	Type	Channel	SSID	Check Point Number

Fig. 4-7 AP Counter List

Click on<the number of detection points> to open [the list of detection points] as shown in Fig. 4-8.



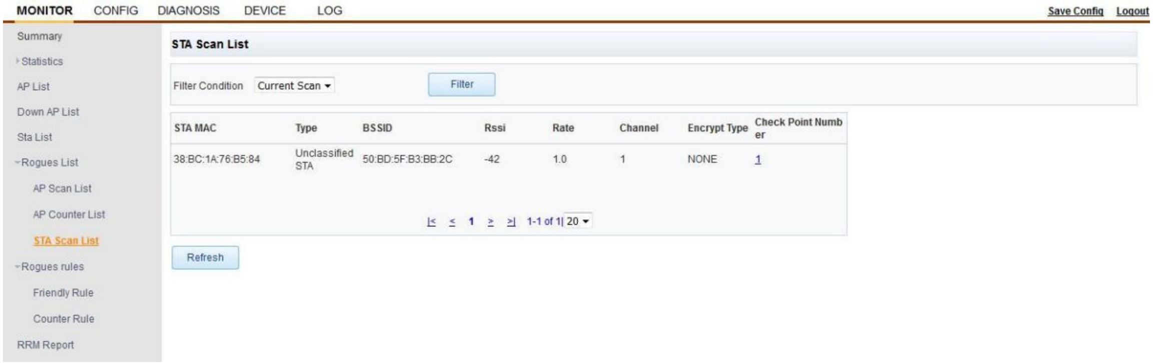
Check Point List

BSSID: 70:65:82:8F:55:40 Type:Unclassified AP

MAC	Discover Time
70:65:82:62:7C:70	TUE NOV 15 14:27:48 2016

Fig. 4.8 Information about the List of Detection Points

[STA scan list] shows all STA information scanned in the current environment as shown in Fig. 4-9.



STA Scan List

Filter Condition: Current Scan

STA MAC	Type	BSSID	Rssi	Rate	Channel	Encrypt Type	Check Point Number
38:BC:1A:76:B5:84	Unclassified STA	50:BD:5F:B3:BB:2C	-42	1.0	1	NONE	1

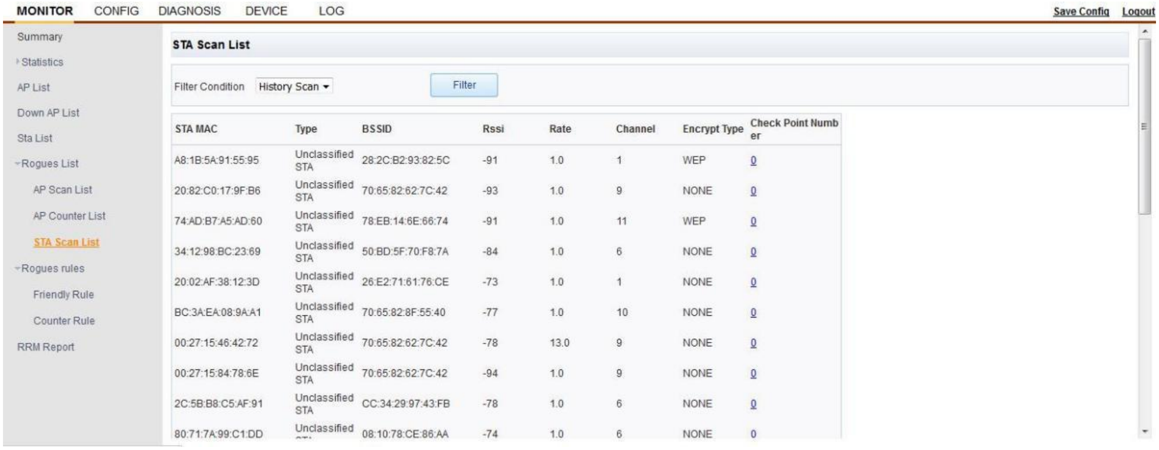
Fig. 4.9 STA Scan List Information

The parameter description of STA scan list is as shown in Table 4-4.

Parameter Item	Description
Filter Criteria	Filter STA list information based on "current scan", "historical scan" and "Rogue type". If the STA in [current scan] result is not scanned by any ap within 5 min., it will get aged and enter [historical scan] list
Number of Detection Points	Click on the STA detection point to open [list of detection points] REF _Ref369096519 \h * MERGEFORMAT as shown in Fig. 4-11.
Refresh	Manually refresh STA scan list information

Table 4-4 STA Scan List Parameter Description

STA historical scan information is as shown in Fig. 4-10.



STA Scan List

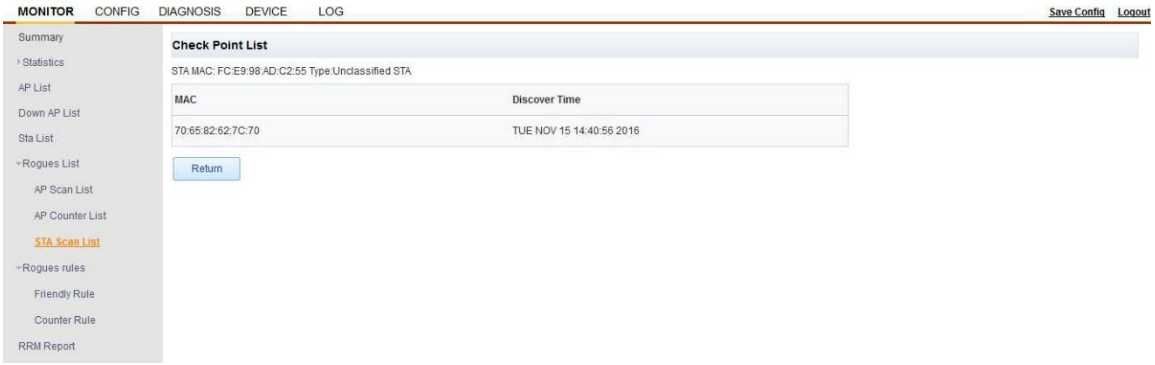
Filter Condition: History Scan

Filter

STA MAC	Type	BSSID	Rssi	Rate	Channel	Encrypt Type	Check Point Number
A8:1B:5A:91:55:95	Unclassified STA	28:2C:B2:93:82:5C	-91	1.0	1	WEP	0
20:82:C0:17:9F:B6	Unclassified STA	70:65:82:62:7C:42	-93	1.0	9	NONE	0
74:AD:B7:A5:AD:60	Unclassified STA	78:EB:14:6E:66:74	-91	1.0	11	WEP	0
34:12:98:BC:23:69	Unclassified STA	50:BD:5F:70:F8:7A	-84	1.0	6	NONE	0
20:02:AF:38:12:3D	Unclassified STA	26:E2:71:61:76:CE	-73	1.0	1	NONE	0
BC:3A:EA:08:9A:A1	Unclassified STA	70:65:82:8F:55:40	-77	1.0	10	NONE	0
00:27:15:46:42:72	Unclassified STA	70:65:82:62:7C:42	-78	13.0	9	NONE	0
00:27:15:84:78:6E	Unclassified STA	70:65:82:62:7C:42	-94	1.0	9	NONE	0
2C:5B:B8:C5:AF:91	Unclassified STA	CC:34:29:97:43:FB	-78	1.0	6	NONE	0
80:71:7A:99:C1:DD	Unclassified	08:10:78:CE:86:AA	-74	1.0	6	NONE	0

Fig. 4.10 STA Historical Scan Information

The detection point list information of STA is as shown in Fig. 4-11.



Check Point List

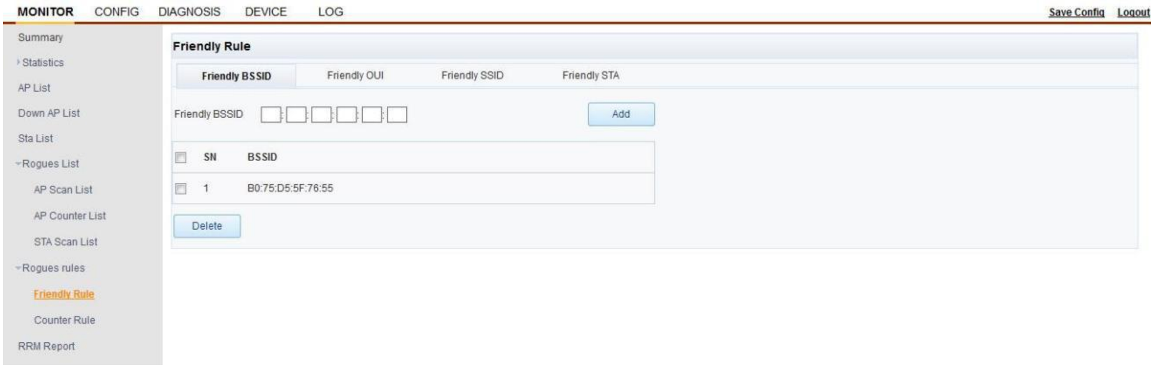
STA MAC: FC:E9:98:AD:C2:55 Type:Unclassified STA

MAC	Discover Time
70:65:82:62:7C:70	TUE NOV 15 14:40:56 2016

Fig. 4.11 Information about the List of Detection Points

4.5 Rogues Rules

[Friendly rule] sets up the conditions for friendly AP and STA. The set friendly AP is indicated as “friendly AP” in [Rogue type] under [AP scan list]; the set friendly STA is displayed as “friendly STA” in [Rogue type] under [STA scan list] as shown in Fig. 4-12.



SN	BSSID
1	B0:75:D5:5F:76:55

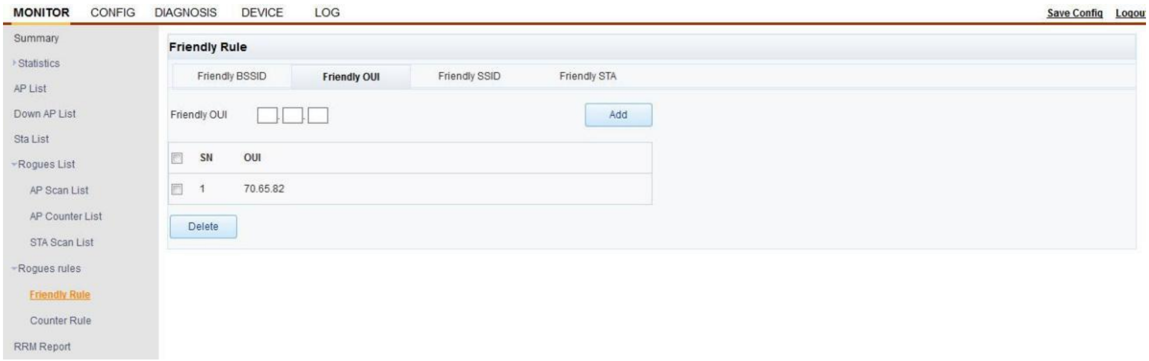
Fig. 4-12 Friendly Rule Information

The parameter description of friendly rule is as shown in Table 4-5.

Parameter Item	Description
Friendly BSSID List	Add friendly BSSID information, and the friendly AP will be indicated as “friendly AP” in [Rogue type] under [AP scan list]
Friendly OUI List	Add the first 6 bits of AP’s BSSID as OUI identification AP; this field must be used with friendly SSID so as to identify friendly AP information
Friendly SSID List	Add friendly SSID; this field must be used with allowable OUI so as to identify the friendly AP information
Friendly STA List	Add friendly STA, and the friendly STA will be indicated as “friendly STA” in [Rogue type] under [STA scan list]
Delete	Delete added friendly rule

Table 4-5 Friendly Rule Parameter Description

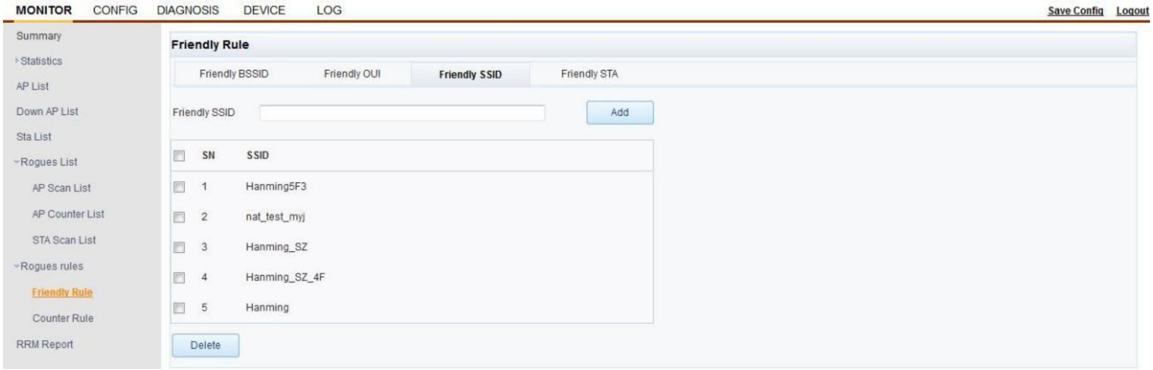
Friendly OUI list setup is as shown in Fig. 4-13.



SN	OUI
1	70.65.82

Fig. 4-13 Friendly OUI List Information

Friendly SSID list setup is as shown in Fig. 4.14.

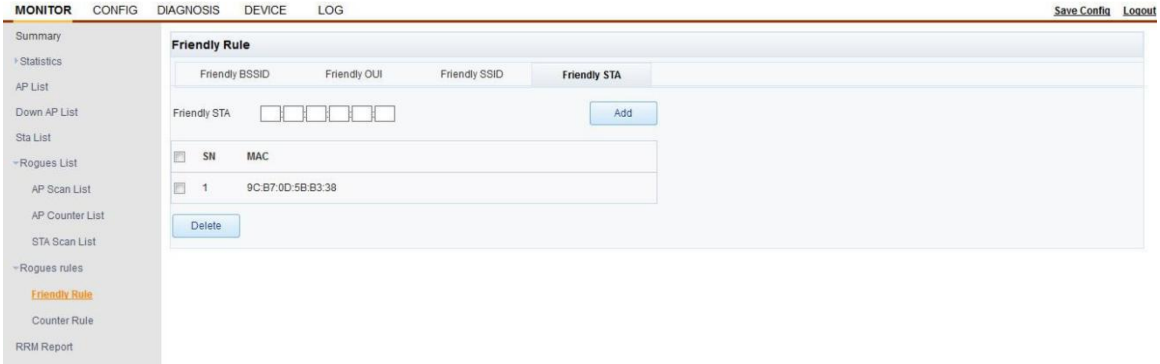


Friendly SSID

□	SN	SSID
□	1	Hanming5F3
□	2	nat_test_myj
□	3	Hanming_SZ
□	4	Hanming_SZ_4F
□	5	Hanming

Fig. 4.14 Friendly SSID List Information

Friendly STA list setup is as shown in Fig. 4-15.

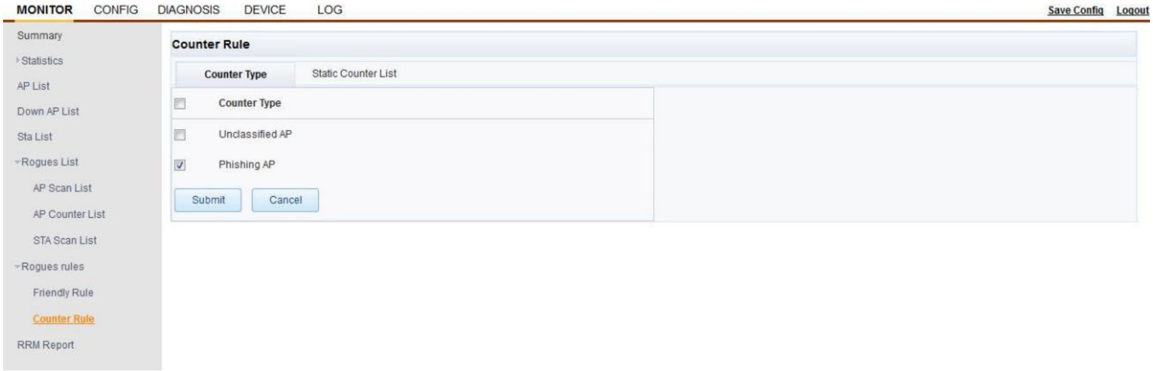


Friendly STA

□	SN	MAC
□	1	9C:B7:0D:5B:B3:38

Fig. 4-15 Friendly STA List Information

[Counter rules] sets up the rules of AP and STA to be countered as shown in Fig. 4-16.



□	Counter Type
□	Unclassified AP
☑	Phishing AP

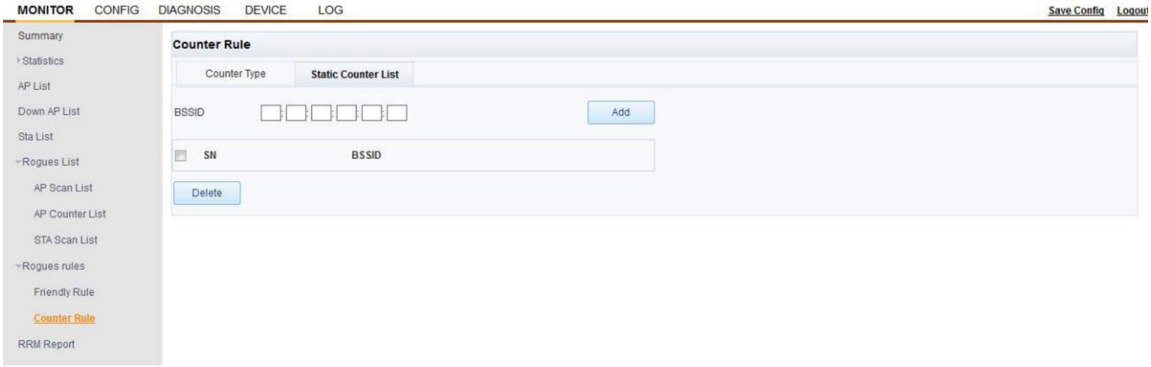
Fig. 4.16 Counter Rule Setup

The parameter description of counter rule is as shown in Table 4-6.

Parameter Item	Description
Counter Type	Select the AP type to be countered, including “unclassified AP” and “phishing AP”
Static Counter List	Manually add the BSSID to be countered, and it will be displayed in [AP counter list]

Table 4-6 Counter Rule Parameter Description

Static counter list is as shown in Fig. 4-17.



Counter Rule

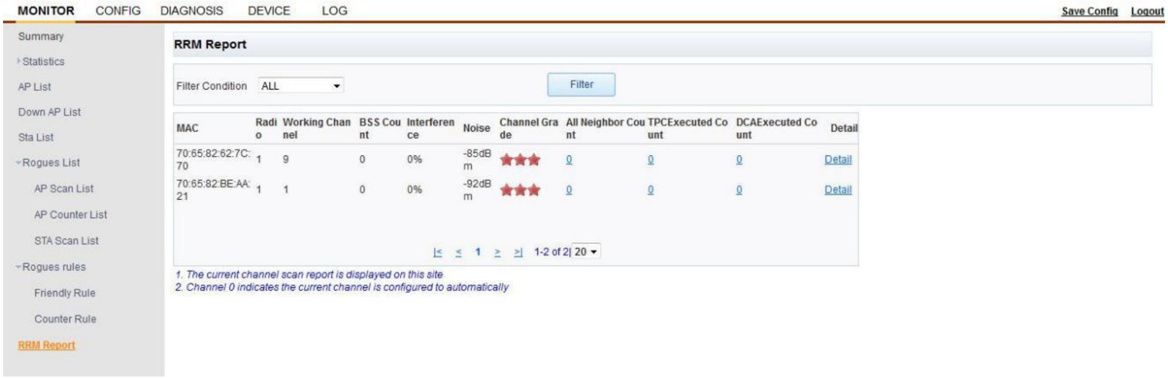
BSSID □:□:□:□:□:□

□ SN	BSSID

Fig. 4-17 Static Counter List

4.6 RRM Report

[RRM report] shows channel scan report information, including each AP’s RF, working channel, BSS count, interference, noise, neighboring AP count, and power regulation frequency etc. as shown in Fig. 4-18.



RRM Report

Filter Condition ALL

MAC	Radio	Working Channel	BSS Count	Interference	Noise	Channel Grade	All Neighbor Count	TPCExecuted Count	DCAExecuted Count	Detail
70:65:82:62:7C:70	1	9	0	0%	-85dBm	★★★	0	0	0	Detail
70:65:82:BE:AA:21	1	1	0	0%	-92dBm	★★★	0	0	0	Detail

1-2 of 2| 20

1. The current channel scan report is displayed on this site
2. Channel 0 indicates the current channel is configured to automatically

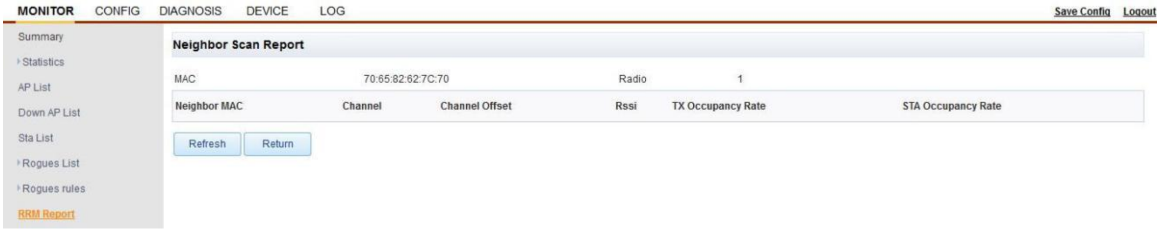
Fig. 4.18 RRM Report Information

The parameter description of RRM report is as shown in Table 4-7.

Parameter item	Description
Filter Criteria	Channel scan report could be screened by AP's MAC address and channel rating
Neighboring AP Count	Show the neighboring AP information of each AP; click on the numbers to open [neighboring AP scan report]
Power regulation Frequency	View the automatic power regulation cycles on condition that "[WLAN Radio Resource Management] > [automatic power regulation]" is enabled; wireless controller automatically regulates power at the set interval based on surrounding wireless signal intensity
Channel regulation Fequency	View the automatic channel regulation cycles on condition that "[WLAN Radio Resource Management] > [automatic channel regulation]" is enabled; wireless controller automatically regulates channel at the set interval based on surrounding wireless signal intensity
Detailed Information	Click on [detailed information] link to view detailed report on channel scan as shown in Fig. 424; click on the "+7" beside AP working channel to view the historical record of the latest 7 scans at this channel

Table 4-7 RRM Report Parameter Description

The neighboring AP scan report is as shown in Fig. 4-19.



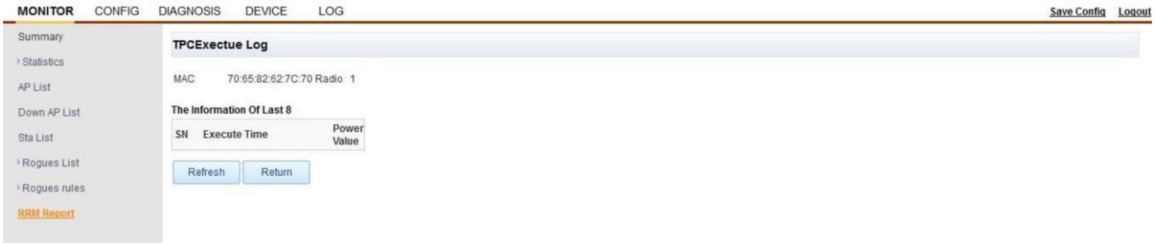
Neighbor Scan Report

MAC 70:65:82:62:7C:70 Radio 1

Neighbor MAC	Channel	Channel Offset	Rssi	TX Occupancy Rate	STA Occupancy Rate

Fig. 4-19 Neighboring AP Scan Report

Automatic power regulation operation record is as shown in Fig. 4-20.



TPCExectue Log

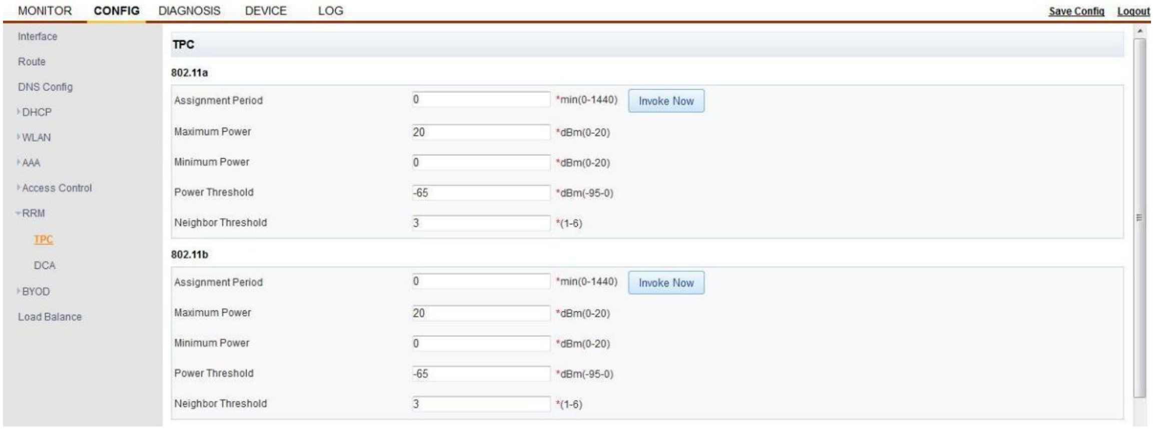
MAC 70:65:82:62:7C:70 Radio 1

The Information Of Last 8

SN	Execute Time	Power Value

Fig. 4-20 Automatic Power Regulation Operation Record

The automatic power regulation setup is as shown in Fig. 4-21.



TPC

802.11a

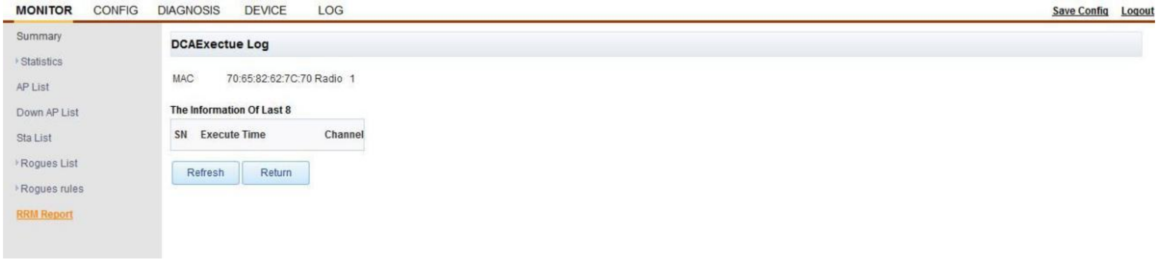
Assignment Period	0	*min(0-1440)
Maximum Power	20	*dBm(0-20)
Minimum Power	0	*dBm(0-20)
Power Threshold	-65	*dBm(-95-0)
Neighbor Threshold	3	*(1-6)

802.11b

Assignment Period	0	*min(0-1440)
Maximum Power	20	*dBm(0-20)
Minimum Power	0	*dBm(0-20)
Power Threshold	-65	*dBm(-95-0)
Neighbor Threshold	3	*(1-6)

Fig. 4-21 Automatic Power Regulation Setup

Automatic power channel operation record is as shown in Fig. 4-22.



DCAExectue Log

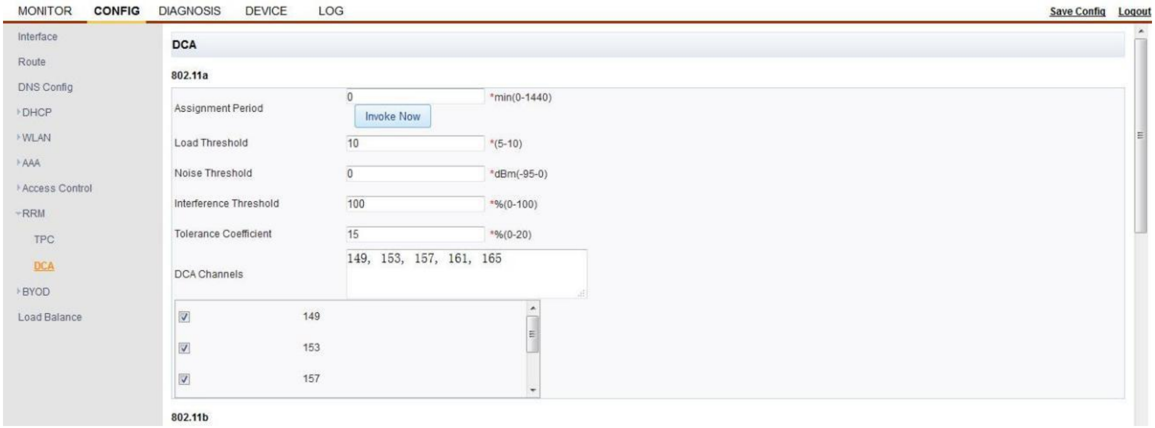
MAC 70:65:82:62:7C:70 Radio 1

The Information Of Last 8

SN	Execute Time	Channel

Fig. 4-22 Automatic Channel Regulation Operation Record

The automatic channel regulation setup is as shown in Fig. 4-23.



DCA

802.11a

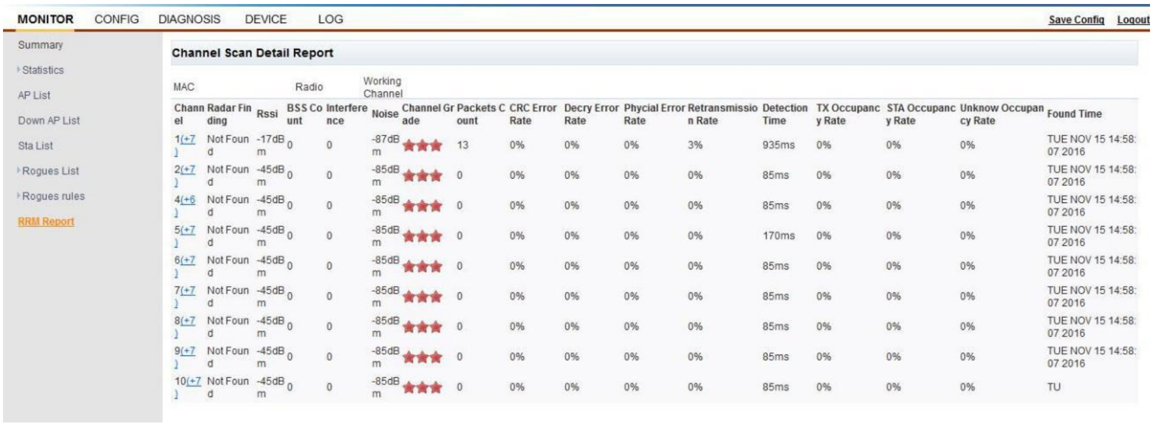
Assignment Period	0	*min(0-1440)
Load Threshold	10	*(5-10)
Noise Threshold	0	*dBm(-95-0)
Interference Threshold	100	*%(0-100)
Tolerance Coefficient	15	*%(0-20)
DCA Channels	149, 153, 157, 161, 165	

☑ 149
☑ 153
☑ 157

802.11b

Fig. 4-23 Automatic Channel Regulation Setup

The detailed report on channel scan is as shown in Fig. 4-24.



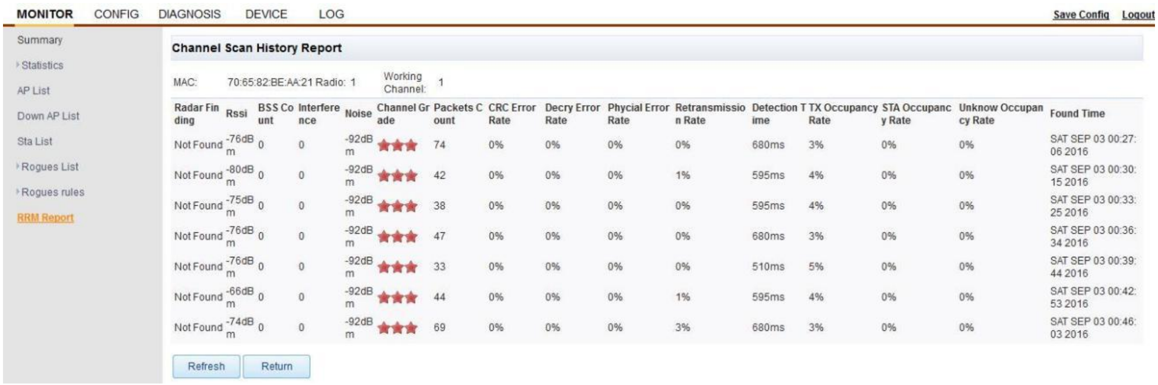
Channel Scan Detail Report

MAC Radio Working Channel

Channel	Radar Finding	Rssi	BSS Count	Interference	Noise	Channel Grade	Packets Count	CRC Error Rate	Decry Error Rate	Phycial Error Rate	Retransmission Rate	Detection Time	TX Occupancy Rate	STA Occupancy Rate	Unknow Occupancy Rate	Found Time
1(+7)	Not Found	-17dBm	0	0	-87dBm	★★★	13	0%	0%	0%	3%	935ms	0%	0%	0%	TUE NOV 15 14:58:07 2016
2(+7)	Not Found	-45dBm	0	0	-85dBm	★★★	0	0%	0%	0%	0%	85ms	0%	0%	0%	TUE NOV 15 14:58:07 2016
4(+6)	Not Found	-45dBm	0	0	-85dBm	★★★	0	0%	0%	0%	0%	85ms	0%	0%	0%	TUE NOV 15 14:58:07 2016
5(+7)	Not Found	-45dBm	0	0	-85dBm	★★★	0	0%	0%	0%	0%	170ms	0%	0%	0%	TUE NOV 15 14:58:07 2016
6(+7)	Not Found	-45dBm	0	0	-85dBm	★★★	0	0%	0%	0%	0%	85ms	0%	0%	0%	TUE NOV 15 14:58:07 2016
7(+7)	Not Found	-45dBm	0	0	-85dBm	★★★	0	0%	0%	0%	0%	85ms	0%	0%	0%	TUE NOV 15 14:58:07 2016
8(+7)	Not Found	-45dBm	0	0	-85dBm	★★★	0	0%	0%	0%	0%	85ms	0%	0%	0%	TUE NOV 15 14:58:07 2016
9(+7)	Not Found	-45dBm	0	0	-85dBm	★★★	0	0%	0%	0%	0%	85ms	0%	0%	0%	TUE NOV 15 14:58:07 2016
10(+7)	Not Found	-45dBm	0	0	-85dBm	★★★	0	0%	0%	0%	0%	85ms	0%	0%	0%	TU

Fig. 4-24 Detailed Report on Channel Scan

The historical report on channel scan is as shown in Fig. 4-25.



Channel Scan History Report

MAC: 70:65:82:BE:AA:21 Radio: 1 Working Channel: 1

Radar Finding	Rssi	BSS Count	Interference	Noise	Channel Grade	Packets Count	CRC Error Rate	Decry Error Rate	Phycial Error Rate	Retransmission Rate	Detection Time	TX Occupancy Rate	STA Occupancy Rate	Unknow Occupancy Rate	Found Time
Not Found	-76dBm	0	0	-92dBm	★★★	74	0%	0%	0%	0%	680ms	3%	0%	0%	SAT SEP 03 00:27:06 2016
Not Found	-80dBm	0	0	-92dBm	★★★	42	0%	0%	0%	1%	595ms	4%	0%	0%	SAT SEP 03 00:30:15 2016
Not Found	-75dBm	0	0	-92dBm	★★★	38	0%	0%	0%	0%	595ms	4%	0%	0%	SAT SEP 03 00:33:25 2016
Not Found	-76dBm	0	0	-92dBm	★★★	47	0%	0%	0%	0%	680ms	3%	0%	0%	SAT SEP 03 00:36:34 2016
Not Found	-76dBm	0	0	-92dBm	★★★	33	0%	0%	0%	0%	510ms	5%	0%	0%	SAT SEP 03 00:39:44 2016
Not Found	-66dBm	0	0	-92dBm	★★★	44	0%	0%	0%	1%	595ms	4%	0%	0%	SAT SEP 03 00:42:53 2016
Not Found	-74dBm	0	0	-92dBm	★★★	69	0%	0%	0%	3%	680ms	3%	0%	0%	SAT SEP 03 00:46:03 2016

Fig. 4-25 Historical Report on Channel Scan

Chapter 5 BYOD

5.1 BYOD Function Description

BYOD (Bring Your Own Device) is the acronym of “bring your own device”; the devices include PC, mobile phone, and tablet etc. Log into company's mail box and online office system without the constraints of time, place, device, personnel and network environment - BYOD shows us a perfect future office scene. Many corporates began to seek the possibility of allowing employees to use their own intelligent devices with internal applications of enterprises. By doing so, the enterprises are intended to address employees' pursuit of new technologies and individualization, while improving their work efficiency and minimizing the cost and investment in mobile terminals.

5.2 Device Identification

Device identification is the prior condition for BYOD, and DHCP's Option 60 could distinguish various terminal types at present; DHCP Option 60 could distinguish terminals down to the level of operating systems like IOS, Windows, Linux, and Android etc. [Device identification configuration] shows BYOD device identification information; since wireless controller incorporates some operating system identification information, user could define identification information as needed as shown in Fig. 5.1.

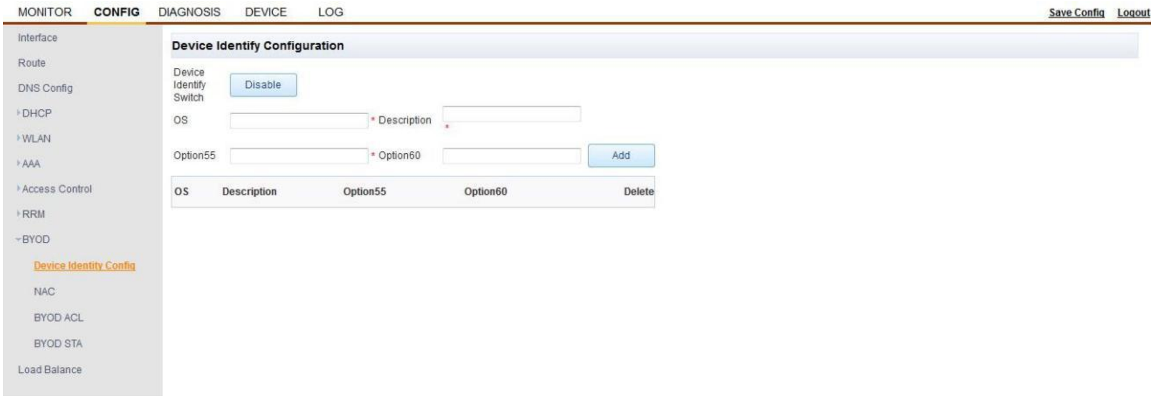


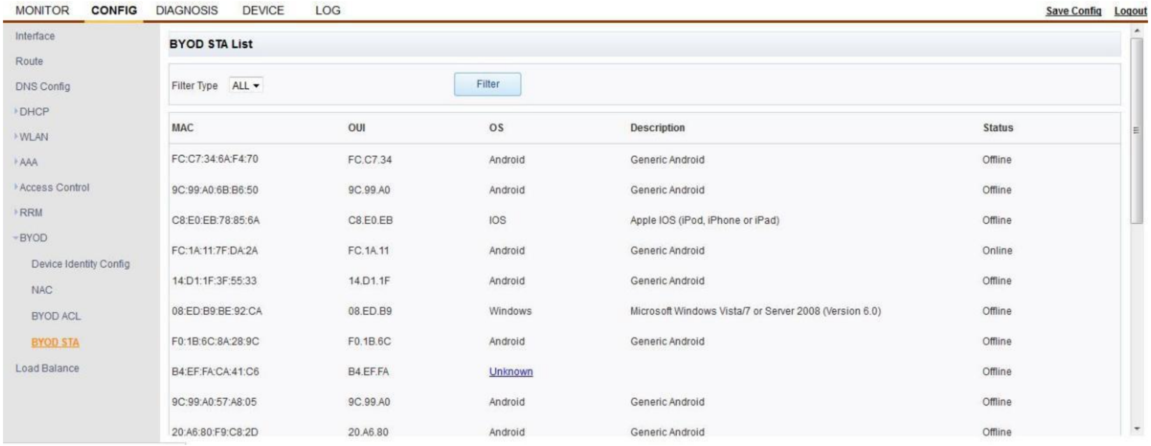
Fig. 5.1 Device Identification Configuration Information

The parameter description of device identification is as shown in Table 5-1.

Parameter Item	**Description**
Device Identification on/off	Device identification on/off is realized through “enable” / ”disable”. [BYOD client] information can only be viewed in enabled state
Operating System	The operating system of device to be identified when device identification is added
Description	Give a brief description of the device to be identified when device identification is added
Option55	Strictly speaking, it can't be used to distinguish device information, but segmentation (e.g. iPhone and iPad etc.) is possible since the request table information varies with device
Option60	Used to obtain manufacturer field, and distinguish down to operating system level (Windows, IOS)
Delete	Delete user-defined device identification information

Table 5-1 Device Identification Parameter Description

[BYOD client] shows identified client information as shown in Fig. 5-2.



BYOD STA List

Filter Type ALL

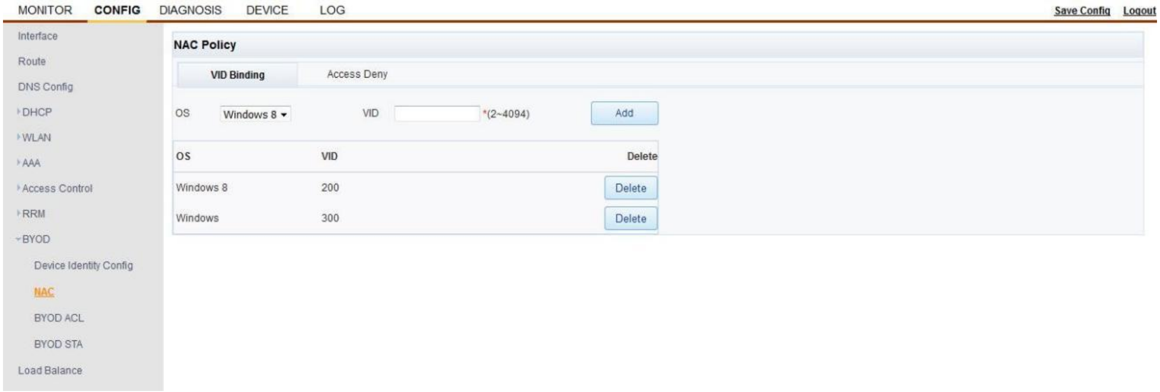
MAC	OUI	OS	Description	Status
FC:C7:34:6A:F4:70	FC.C7.34	Android	Generic Android	Offline
9C:99:A0:6B:B6:50	9C.99.A0	Android	Generic Android	Offline
C8:E0:EB:78:85:6A	C8.E0.EB	IOS	Apple IOS (iPod, iPhone or iPad)	Offline
FC:1A:11:7F:DA:2A	FC.1A.11	Android	Generic Android	Online
14:D1:1F:3F:55:33	14.D1.1F	Android	Generic Android	Offline
08:ED:B9:BE:92:CA	08.ED.B9	Windows	Microsoft Windows Vista/7 or Server 2008 (Version 6.0)	Offline
F0:1B:6C:8A:28:9C	F0.1B.6C	Android	Generic Android	Offline
B4:EF:FA:CA:41:C6	B4.EF.FA	Unknown		Offline
9C:99:A0:57:A8:05	9C.99.A0	Android	Generic Android	Offline
20:A6:80:F9:C8:2D	20.A6.80	Android	Generic Android	Offline

Fig. 5-2 BYOD Client List

5.3 NAC Policy

NAC (Network Access Control) policy enables the access control for different devices through policy setup.

[VID binding] Realize a centralized networking environment; the devices with different operating systems involve different bound service VIDs after being identified by wireless controller. This function has no effect on distributed networking as shown in Fig. 5-3.



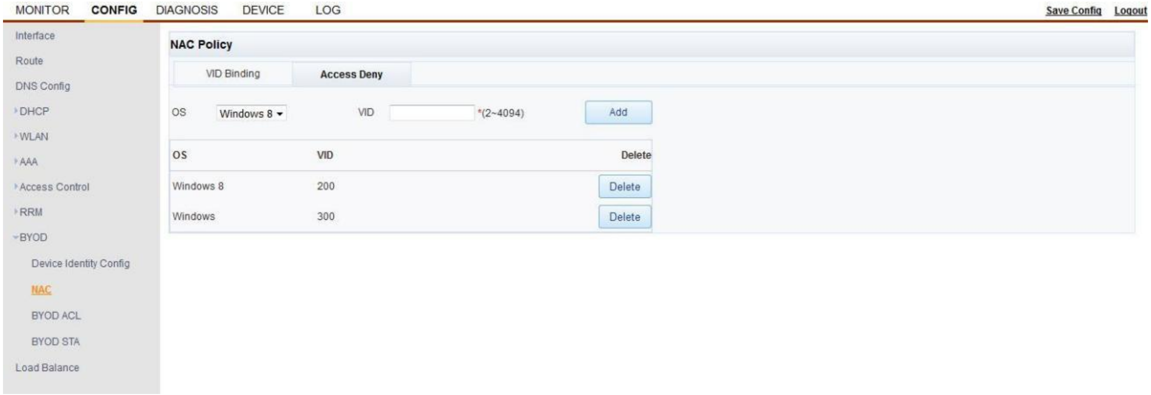
NAC Policy

OS Windows 8 VID *(2~4094)

OS	VID	Delete
Windows 8	200	Delete
Windows	300	Delete

Fig. 5-3 VID Binding Setup

[Access rejection] shows the device operating system that rejects the access; the device with operating system rejecting the access can't be connected to fit AP as shown in Fig. 5-4.



NAC Policy

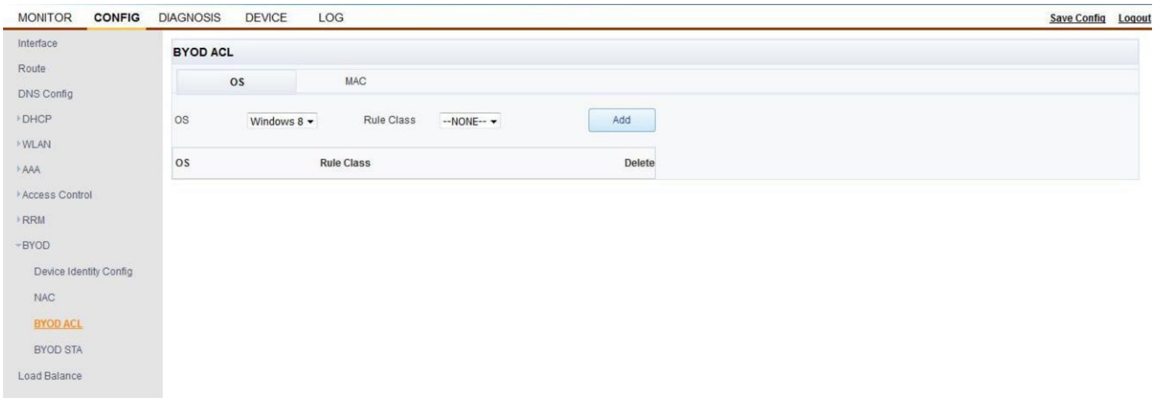
OS Windows 8 VID *(2~4094)

OS	VID	Delete
Windows 8	200	Delete
Windows	300	Delete

Fig.5-4 Access Rejection Setup

5.4 BYOD ACL

[BYOD ACL] shows BYOD-identified device access control policy as shown in Fig.5-5.



OS: Windows 8
Rule Class: --NONE--

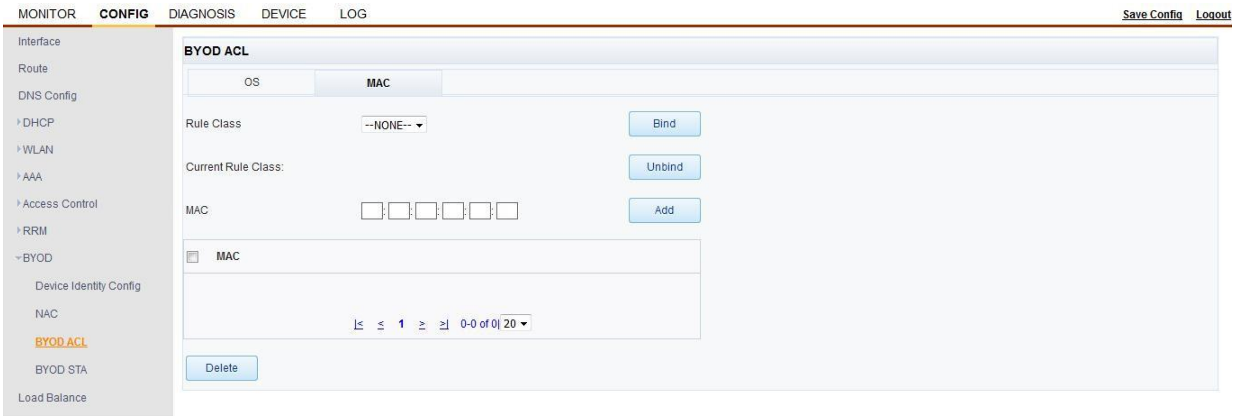
Fig. 5-5 BYOD ACL Policy Setup

The parameter description of BYOD ACL is as shown in Table 5-2.

Parameter Item	Description
Operating System	Choose some identified operating systems of wireless associated system
MAC Address	Set byod acl rule corresponding to terminal
Policy Set	Add byod-type policy set in "[access control] > [wireless access control]". Then, the BYOD ACL page could reference policy rules in that policy set

Table 5-2 BYOD ACL Parameter Description

The addition of BYOD ACL rule to MAC address is as shown in Fig. 5-6.



Rule Class: --NONE--
Current Rule Class:
MAC: □:□:□:□:□:□

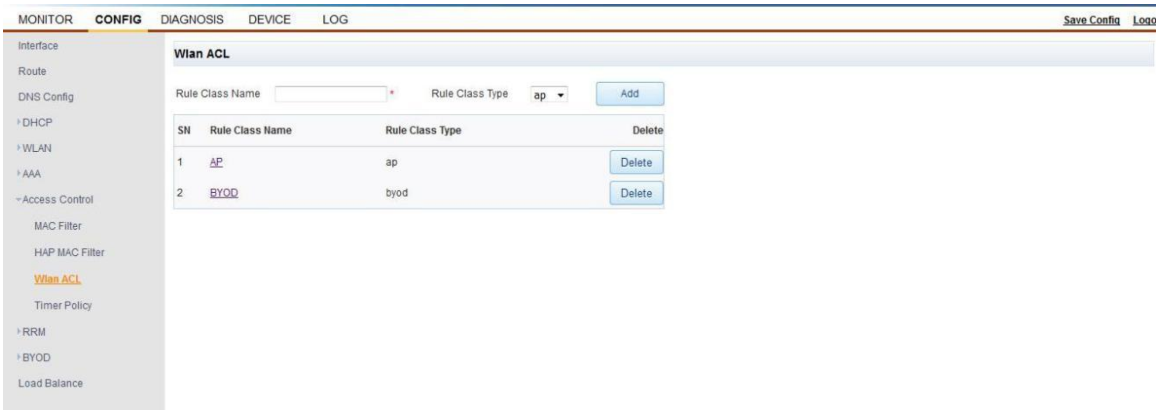
Fig. 5-6 Addition of BYOD ACL Rule to MAC Address

The parameter description for addition of BYOD ACL rule to MAC address is as shown in Table 5-3.

Parameter Item	**Description**
Binding	Bind existing policy set; this BYOD policy set is added in "[access control] > [wireless access control]"
Unbind	Release the bound policy set
Add	Add terminal MAC address
Delete	Delete MAC address

Table 5-3 Parameter Description for Addition of BYOD ACL Rule to MAC Address

The addition of byod policy set information is as shown in Fig. 5-7.



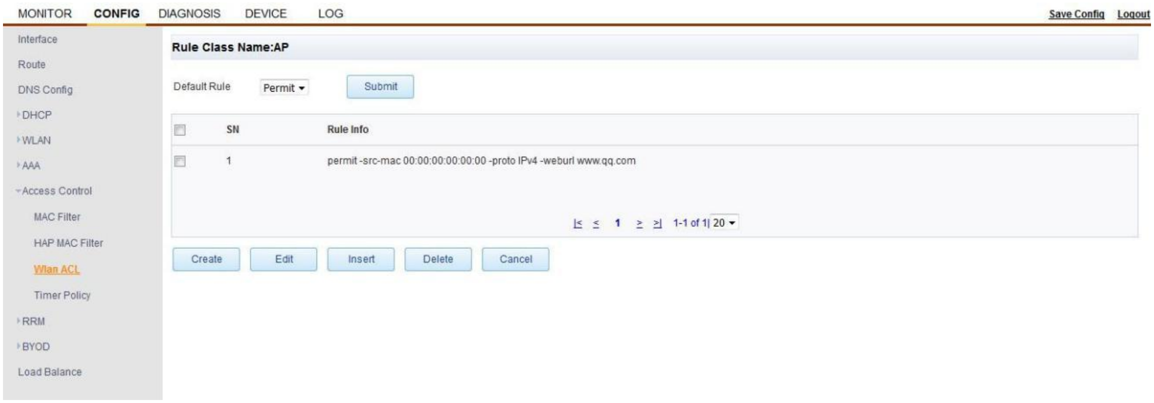
Wlan ACL

Rule Class Name: * Rule Class Type: ap

SN	Rule Class Name	Rule Class Type	Delete
1	AP	ap	Delete
2	BYOD	byod	Delete

Fig. 5-7 BYOD Policy Set Addition Information

Click on existing policy set link to create, edit, delete and insert the policy set as shown in Fig. 5-8.



Rule Class Name:AP

Default Rule: Permit

□	SN	Rule Info
□	1	permit -src-mac 00:00:00:00:00:00 -proto IPv4 -weburl www.qq.com

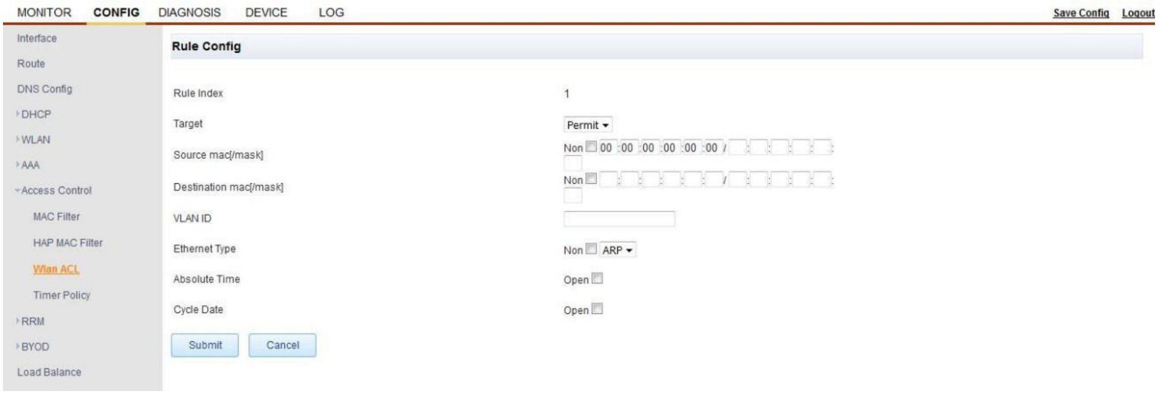
Fig. 5-8 Policy Set Operation List

The parameter description of BYOD policy set is as shown in Table 5-4.

Parameter Item	Description
Create	Create a new policy rule in sequence
Edit	Edit existing policy
Insert	Insert a new policy rule in a specified location
Delete	Delete existing policy rules separately or collectively
Cancel	Return to policy set page

Table 5-4 BYOD Policy Set Parameter Description

The BYOD policy addition page is as shown in Fig. 5-9.



Rule Config

Rule Index 1

Target Permit

Source mac[/mask] Non □ 00 :00 :00 :00 :00 :00 /

Destination mac[/mask] Non □

VLAN ID

Ethernet Type Non □ ARP

Absolute Time Open □

Cycle Date Open □

Fig. 5-9 BYOD Policy Addition Page

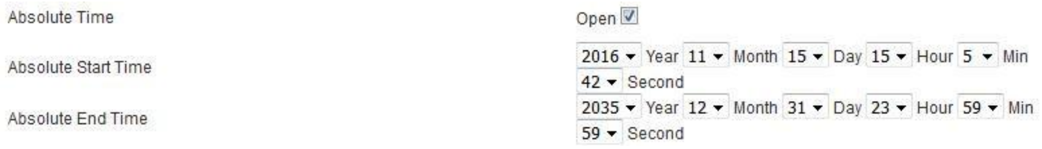
The parameter description of BYOD policy rule addition is as shown in Table 5-5.

Parameter Item	Description
Policy Index	This index is in ascending order and can't be modified during policy creation; this index could be edited (1 by default) during policy insertion
Purpose	Choose from [permit] and [disable] to indicate the purpose of this access control rule
Source IP Address [/mask]	Set the source IP address and subnet mask of rule

Destination IP Address [/mask]	Set the destination IP address and subnet mask of rule
Source IP Segment	Set the source IP address segment of rule
Destination IP Segment	Set the destination IP address segment of rule
IP Protocol	Set up the IP protocols for rule, including TCP, UDP, SCTP, DCCP, ICMP and ALL; where the first four protocols are selected, the source port number and destination port number corresponding to protocol could be set up
Absolute Time	Set the absolute starting and ending time of rule
Cycle Time	Set the rule cycle time, including daily cycle, monthly cycle and weekly cycle
NOT	Negate the set information

Table 5-5 Parameter description of BYOD policy rule addition

The setup of absolute time is as shown in Fig. 5-10.



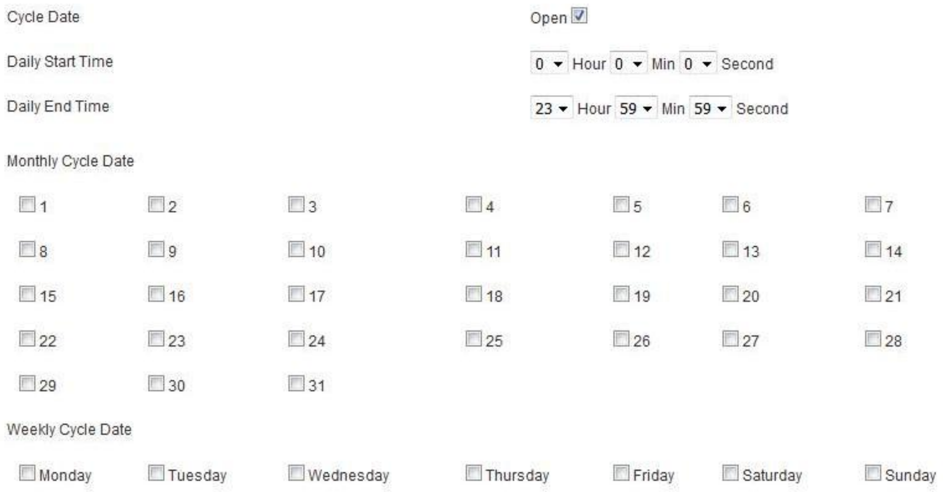
Absolute Time: Open ☑

Absolute Start Time: 2016 Year 11 Month 15 Day 15 Hour 5 Min 42 Second

Absolute End Time: 2035 Year 12 Month 31 Day 23 Hour 59 Min 59 Second

Fig. 5-10 Absolute Time Setup

The setup of cycle time is as shown in Fig. 5-11.



Cycle Date: Open ☑

Daily Start Time: 0 Hour 0 Min 0 Second

Daily End Time: 23 Hour 59 Min 59 Second

Monthly Cycle Date

□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7
□ 8	□ 9	□ 10	□ 11	□ 12	□ 13	□ 14
□ 15	□ 16	□ 17	□ 18	□ 19	□ 20	□ 21
□ 22	□ 23	□ 24	□ 25	□ 26	□ 27	□ 28
□ 29	□ 30	□ 31				

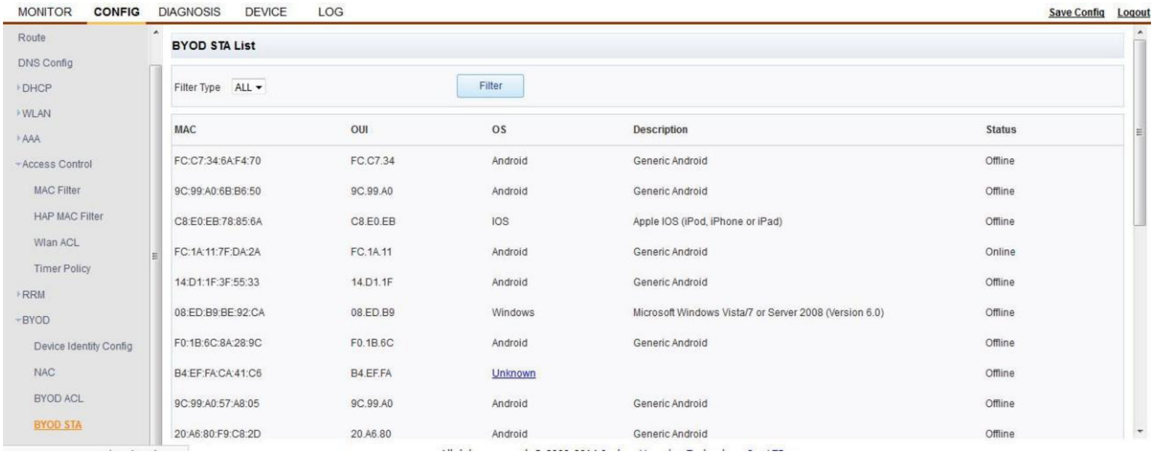
Weekly Cycle Date

□ Monday □ Tuesday □ Wednesday □ Thursday □ Friday □ Saturday □ Sunday

Fig. 5.11 Cycle Time Setup

5.5 BYOD Client

[BYOD client] shows client terminal information identified by wireless controller as shown in Fig. 5-12.



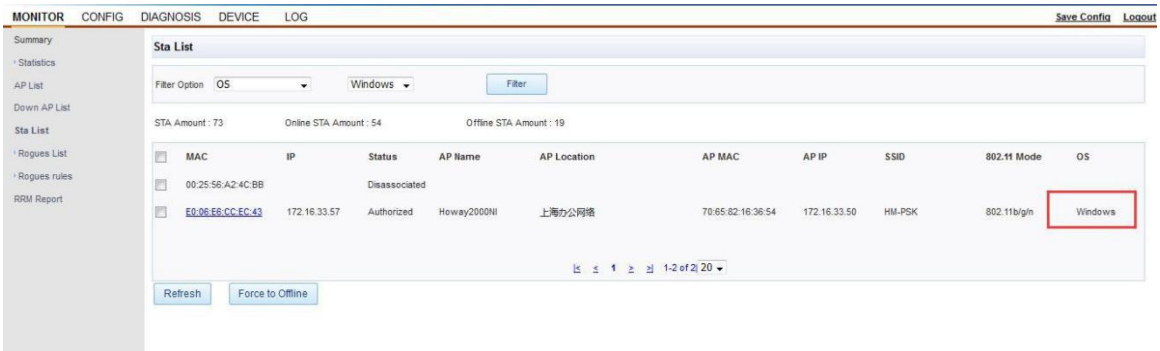
BYOD STA List

Filter Type: ALL

MAC	OUI	OS	Description	Status
FC:C7:34:6A:F4:70	FC.C7.34	Android	Generic Android	Offline
9C:99:A0:6B:B6:50	9C.99.A0	Android	Generic Android	Offline
C8:E0:EB:78:85:6A	C8.E0.EB	IOS	Apple IOS (iPod, iPhone or iPad)	Offline
FC:1A:11:7F:DA:2A	FC.1A.11	Android	Generic Android	Online
14:D1:1F:3F:55:33	14.D1.1F	Android	Generic Android	Offline
08:ED:B9:BE:92:CA	08.ED.B9	Windows	Microsoft Windows Vista/7 or Server 2008 (Version 6.0)	Offline
F0:1B:6C:8A:28:9C	F0.1B.6C	Android	Generic Android	Offline
B4:EF:FA:CA:41:C6	B4.EF.FA	Unknown		Offline
9C:99:A0:57:A8:05	9C.99.A0	Android	Generic Android	Offline
20:A6:80:F9:C8:2D	20.A6.80	Android	Generic Android	Offline

Fig. 5-12 BYOD Client List

The identified operating systems in terminal list are as shown in Fig. 5-13.



Sta List

Filter Option: OS, Windows

STA Amount : 73 Online STA Amount : 54 Offline STA Amount : 19

☐	MAC	IP	Status	AP Name	AP Location	AP MAC	AP IP	SSID	802.11 Mode	OS
☐	00:25:56:A2:4C:BB		Disassociated							
☐	E0:06:E6:CC:EC:43	172.16.33.57	Authorized	Howay2000NI	上海办公网络	70:65:82:16:36:54	172.16.33.50	HM-PSK	802.11b/g/n	Windows

1-2 of 2 20

Fig. 5-13 Terminal List

Chapter 6 WLAN ACL

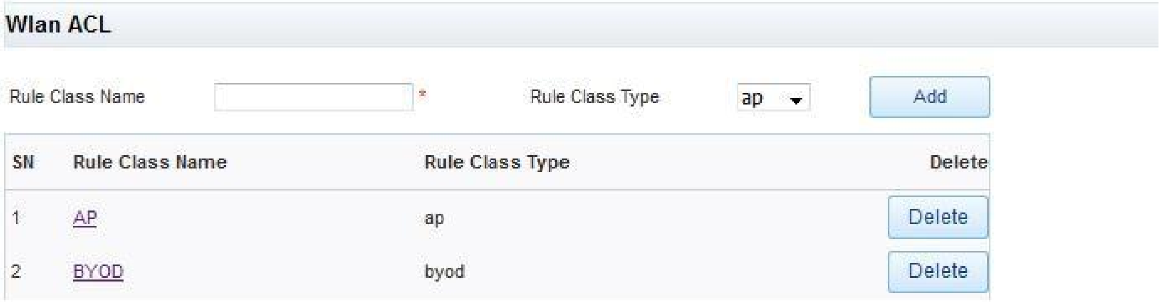
6.1 WLAN ACL Description

Wireless controller distributes set WLAN ACL rule to AP to realize the access control of wireless terminal.

6.2 Configure WLAN ACL Rule

Add WLAN ACL Policy Set

Add WLAN ACL rule with AP policy set in [wireless access control] page as shown in Fig. 6-1.



Wlan ACL

Rule Class Name: *

Rule Class Type: ap

SN	Rule Class Name	Rule Class Type	Delete
1	AP	ap	Delete
2	BYOD	byod	Delete

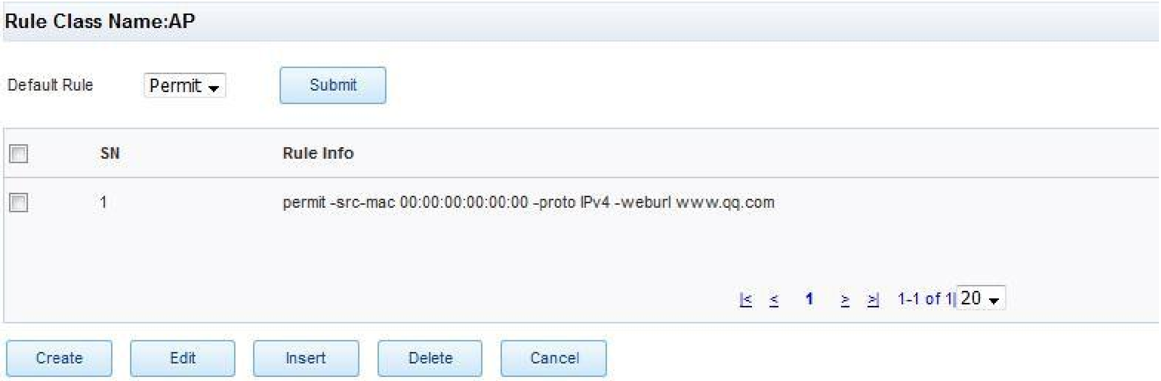
Fig. 6-1 Wireless Access Control Page

The parameter description of wireless access control is as shown in Table 6-1.

Parameter Item	Description
Add	Add [AP] or [BYOD] type wireless access policy set
Name of Policy Set	Click on [AP] policy set to open policy set configuration page
Delete	Delete policy set

Table 6-1 Wireless Access Control Parameter Description

Policy set configuration information is as shown in Fig. 6-2.



Rule Class Name:AP

Default Rule: Permit

☐	SN	Rule Info
☐	1	permit -src-mac 00:00:00:00:00:00 -proto IPv4 -weburl www.qq.com

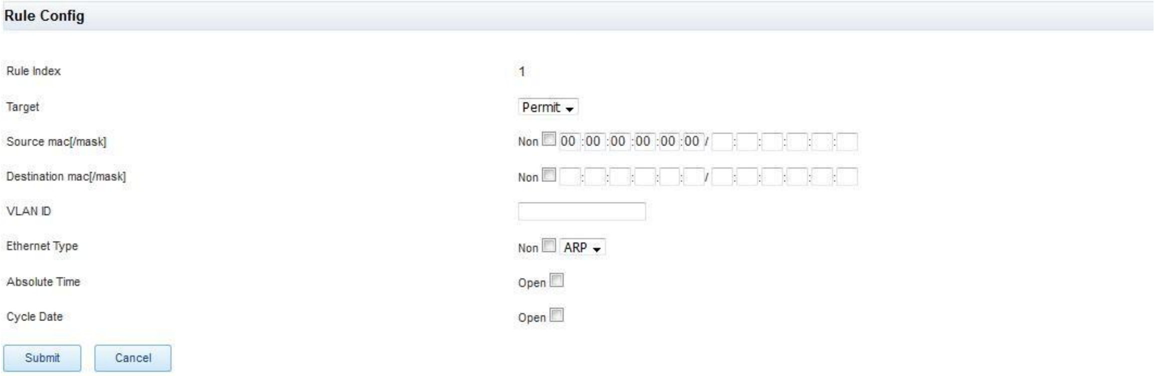
1-1 of 1 20

Fig. 6.2 Policy Set Configuration Information

The parameter description of policy set configuration is as shown in Table 6-2.

Parameter Item	**Description**
Default Policy	Set the default policy of this policy set; it's [disabled] by default
Create	Create a new policy rule in sequence
Edit	Edit existing policy
Insert	Insert a new policy rule in a specified location
Delete	Delete existing policy rules separately or collectively
Cancel	Return to policy set page

Table 6-2 Policy Set Configuration Parameter Description



Rule Config

Rule Index	1
Target	Permit
Source mac[/mask]	Non □ 00 :00 :00 :00 :00 :00 / : : : : :
Destination mac[/mask]	Non □ : : : : : / : : : : :
VLAN ID	
Ethernet Type	Non □ ARP
Absolute Time	Open □
Cycle Date	Open □

Create policy configuration information as shown in Fig. 6-3.

Fig. 6-3 Create policy configuration information

The policy configuration parameter description is as shown in Table 6-3.

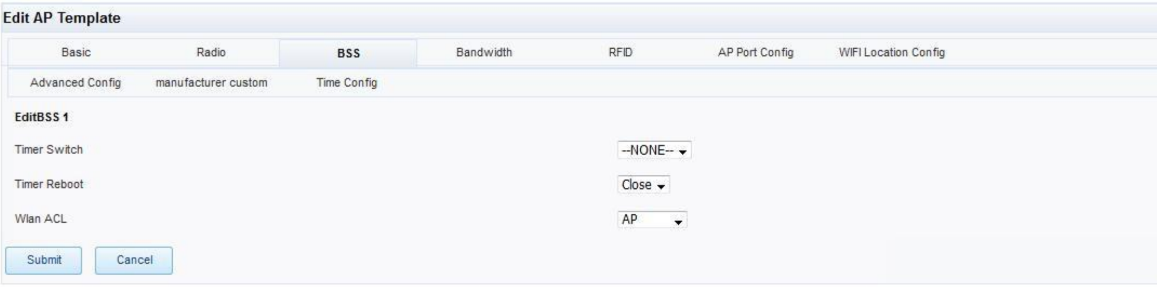
Parameter item	**Description**
Policy Index	This index is in ascending order and can't be modified during policy creation; this index could be edited (1 by default) during policy insertion
Purpose	Choose from [permit] and [disable] to indicate the purpose of this access control rule
Source MAC Address	Set the source MAC address and mask of policy

Destination MAC Address	Set the destination MAC address and mask of policy
VLAN ID	Set the VLAN ID of policy
Ethernet Type	Choose from [IPv4] and [ARP]
Source IP Address [/mask]	The source IP address and subnet mask of rule can't be set up unless the type of Ethernet is set to [IPv4]
Destination IP Address [/mask]	The destination IP address and subnet mask of rule can't be set up unless the type of Ethernet is set to [IPv4]
Source IP Segment	Set the source IP address segment of rule when the type of Ethernet is set to [IPv4]
Destination IP Segment	Set the destination IP address segment of rule when the type of Ethernet is set to [IPv4]
IP Service Type	Set the IP service type (TOS) within the value range 1~7
IP Protocol	Set up the IP protocols for rule, including TCP, UDP, SCTP, DCCP, ICMP and ALL; where the first four protocols are selected, the source port number and destination port number corresponding to protocol could be set up
Absolute Time	Set the absolute starting and ending time of rule
Cycle Time	Set the rule cycle time, including daily cycle, monthly cycle and weekly cycle

Table 6-3 Policy Cconfiguration Parameter Description

6.3 WLAN ACL Distribution

Bind the configured WLAN ACL policy set to AP template, and distribute the template to AP so that AP could have WLAN ACL function as shown in Fig. 6-4.



EditBSS 1

Timer Switch --NONE--

Timer Reboot Close

Wlan ACL AP

Fig. 6-4 AP Template Bound with WLAN ACL Policy Set

Note:

1. User could set up wireless access control policies depending on BSS.

2. Wireless controller distributes the modified WLAN ACL policy set timely to AP, making it unnecessary to distribute AP template again.

Chapter 7 HAP

7.1 HAP Description

Outbound service is not possible in the case of AC and fit AP networking unless AP is online (sta is accessible). Once AP goes off line, it will not transmit RF; in other words, offline AP can't continue to provide service even if it can transmit RF; that is to say, new users can't get connected while all the connected users go off line. In the case of HAP (Hybrid Access Point), the AP and AC link break should not affect local forwarding of user data; when AP and AC link returns to normal, AP's getting the IP address assigned by AC shall not affect user's network operation.

The typical application scenario of HAP is as shown in Fig. 7-1.

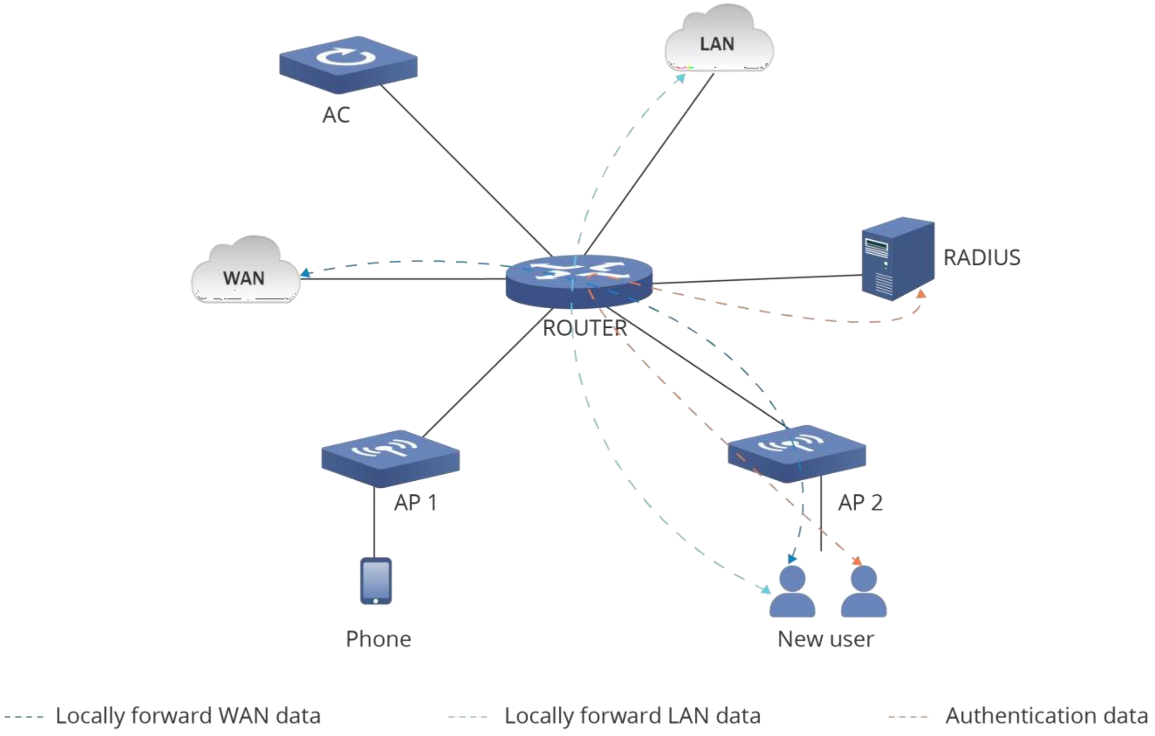


Fig. 7-1 Typical Application Scenario of HAP

Connected mode and independent mode:

In connected mode, the CAPWAP control channel from HAP to wireless controller functions properly, which means WAN link is effective.

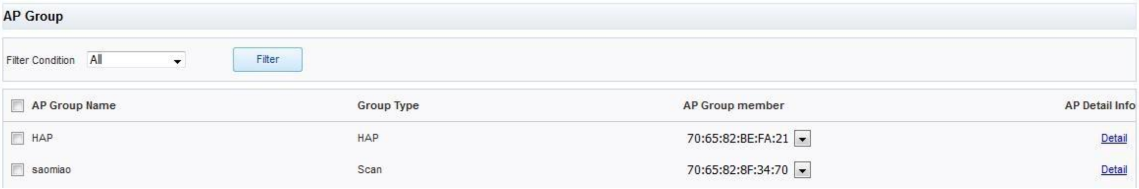
In independent mode, there is no normal control message interaction between HAP wireless AP and wireless controller.

As shown in Fig. 7-1, when AP goes from connected mode to independent mode, the distributed users originally connected on HAP could access LAN and WAN. In the meantime, all centralized users connected with HAP go offline.

The connection with any new user is impossible if the terminal users on HAP are centralized. In the case of open and shared WPA-PSK or WPA2-PSK authentication mode of distributed forwarding, new wireless clients could be authenticated without the help of other devices so that HAP could complete the new user authentication; in the case of wpa/wpa2 authentication, AC could enable it to support new user access through radius service configuration.

7.2 HAP Group

HAP group is configured in [AP group] page as shown in Fig. 7-2.



AP Group

Filter Condition All ▾ Filter

□ AP Group Name	Group Type	AP Group member	AP Detail Info
□ HAP	HAP	70:65:82:BE:FA:21 ▾	Detail
□ saomiao	Scan	70:65:82:8F:34:70 ▾	Detail

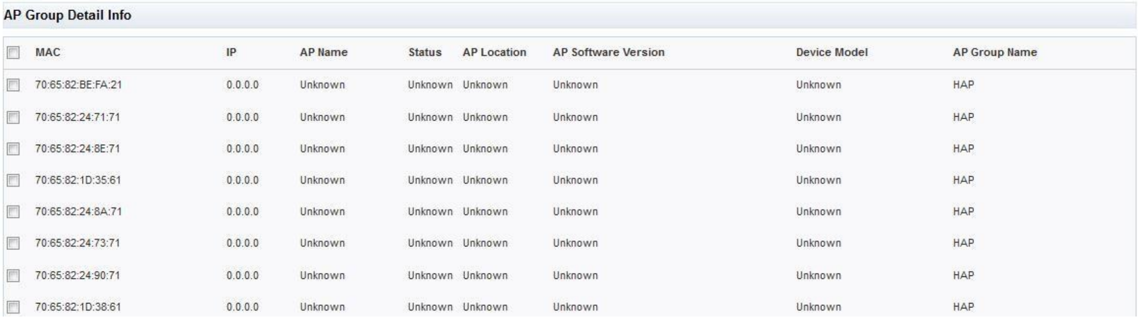
Fig. 7-2 AP Configuration Information

The parameter description of HAP is as shown in Table 7-1.

Parameter Item	**Description**
Filter Criteria	AP group information could be filtered by group type
AP Group Member	The information about members of AP group could be viewed through drop-down button
Detailed Information	The [detailed information on HAP group] could also be viewed by clicking on detailed information link
Create	Create new AP group
Edit	Edit the designated AP group information
Delete	Delete designated AP group

Table 7-1 HAP Group Parameter Description

The detailed information on HAP group is as shown in Fig. 7-3.



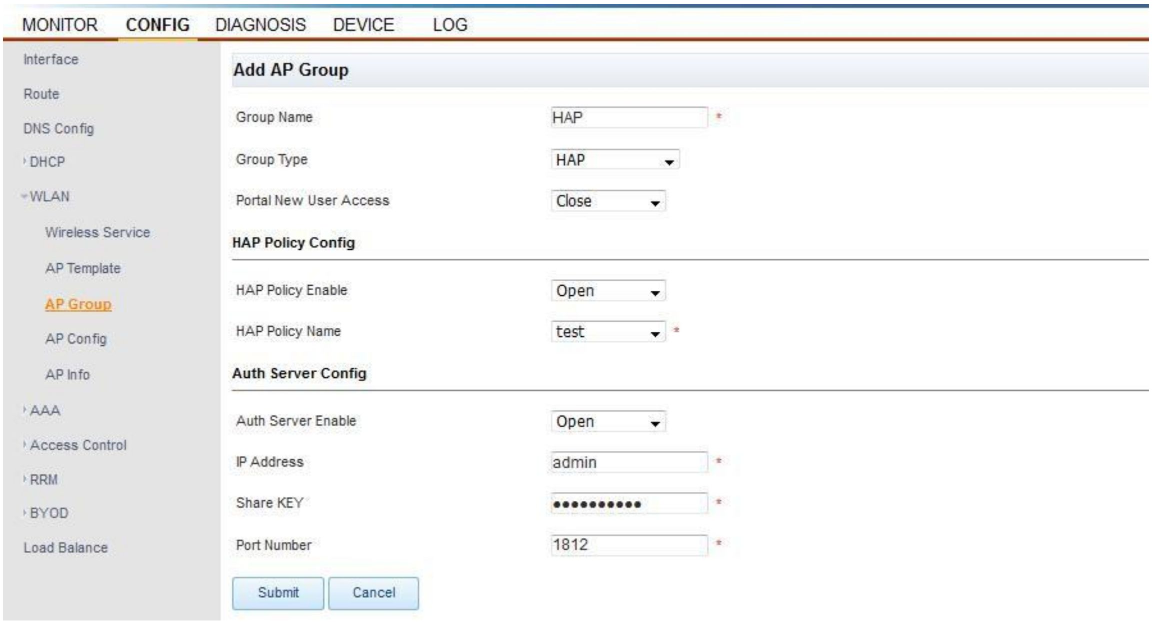
AP Group Detail Info

□ MAC	IP	AP Name	Status	AP Location	AP Software Version	Device Model	AP Group Name
□ 70:65:82:BE:FA:21	0.0.0.0	Unknown	Unknown	Unknown	Unknown	Unknown	HAP
□ 70:65:82:24:71:71	0.0.0.0	Unknown	Unknown	Unknown	Unknown	Unknown	HAP
□ 70:65:82:24:8E:71	0.0.0.0	Unknown	Unknown	Unknown	Unknown	Unknown	HAP
□ 70:65:82:1D:35:61	0.0.0.0	Unknown	Unknown	Unknown	Unknown	Unknown	HAP
□ 70:65:82:24:8A:71	0.0.0.0	Unknown	Unknown	Unknown	Unknown	Unknown	HAP
□ 70:65:82:24:73:71	0.0.0.0	Unknown	Unknown	Unknown	Unknown	Unknown	HAP
□ 70:65:82:24:90:71	0.0.0.0	Unknown	Unknown	Unknown	Unknown	Unknown	HAP
□ 70:65:82:1D:38:61	0.0.0.0	Unknown	Unknown	Unknown	Unknown	Unknown	HAP

Fig. 7-3 Detailed information on HAP group

7.3 Create HAP Group

HAP group in the page as shown in Fig. 7-4.



Add AP Group

Group Name	HAP *
Group Type	HAP
Portal New User Access	Close

HAP Policy Config

HAP Policy Enable	Open
HAP Policy Name	test *

Auth Server Config

Auth Server Enable	Open
IP Address	admin *
Share KEY	●●●●●●●●●●● *
Port Number	1812 *

Fig. 7-4 HAP Group Creation Page

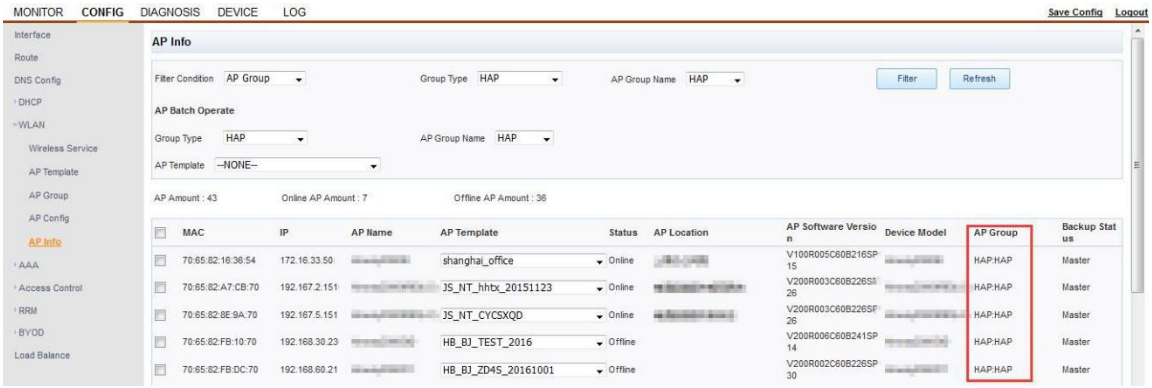
The parameter description of HAP is as shown in Table 7-2.

Parameter Item	**Description**
Group Name	HAP group name that must be unique
Type	There are several types of AP groups, and HAP group shall be selected in this case
Portal New User Access	Determine whether portal new user access on/off is allowable in HAP mode
HAP Rule Configuration	HAP rule configuration is set up in “[access control] > [HAP filter configuration]” page
Authentication Server Configuration	Set up the authentication server configuration information in HAP mode

Table 7-2 HAP Group Parameter Description

7.4 Addition to HAP

"[WLAN configuration] > [AP information]" adds AP into HAP group as shown in Fig. 7-5.



AP Info

Filter Condition: AP Group | Group Type: HAP | AP Group Name: HAP

AP Batch Operate

Group Type: HAP | AP Group Name: HAP

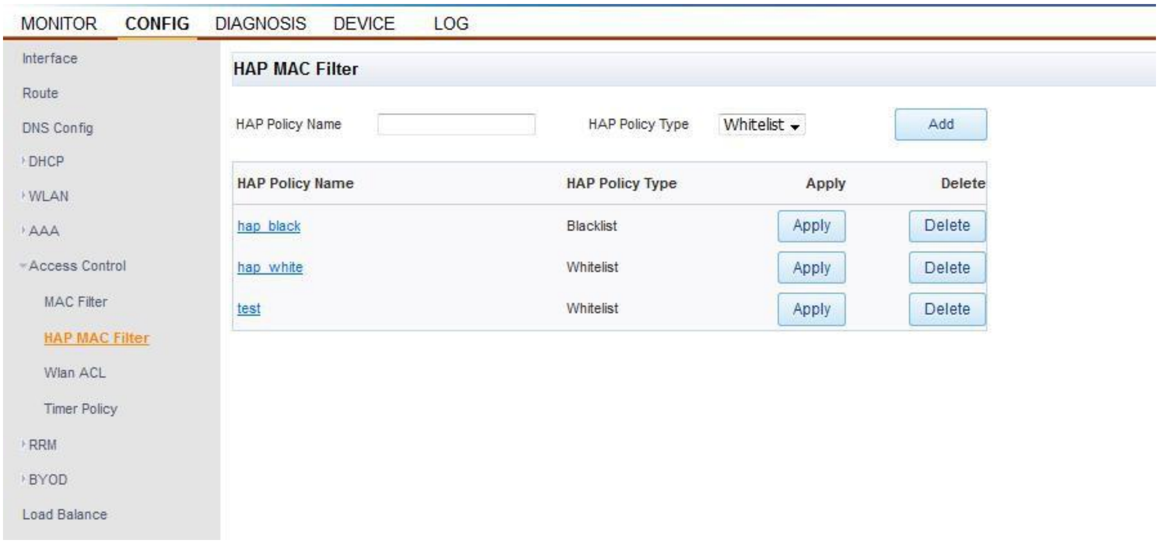
AP Template: --NONE--

AP Amount : 43 | Online AP Amount : 7 | Offline AP Amount : 36

☐	MAC	IP	AP Name	AP Template	Status	AP Location	AP Software Version	Device Model	AP Group	Backup Status
☐	70:65:82:16:36:54	172.16.33.50	[redacted]	shanghai_office	Online	[redacted]	V100R005C60B216SP15	[redacted]	HAP:HAP	Master
☐	70:65:82:A7:CB:70	192.167.2.151	[redacted]	JS_NT_hhtx_20151123	Online	[redacted]	V200R003C60B226SP26	[redacted]	HAP:HAP	Master
☐	70:65:82:8E:9A:70	192.167.5.151	[redacted]	JS_NT_CYCSXQD	Online	[redacted]	V200R003C60B226SP26	[redacted]	HAP:HAP	Master
☐	70:65:82:FB:10:70	192.168.30.23	[redacted]	HB_BJ_TEST_2016	Offline		V200R006C60B241SP14	[redacted]	HAP:HAP	Master
☐	70:65:82:FB:DC:70	192.168.60.21	[redacted]	HB_BJ_ZD4S_20161001	Offline		V200R002C60B226SP30	[redacted]	HAP:HAP	Master

Fig. 7-5 Add AP into HAP Group

HAP filter configuration is as shown in Fig. 7-6.



HAP MAC Filter

HAP Policy Name: | HAP Policy Type: Whitelist

HAP Policy Name	HAP Policy Type	Apply	Delete
hap_black	Blacklist	Apply	Delete
hap_white	Whitelist	Apply	Delete
test	Whitelist	Apply	Delete

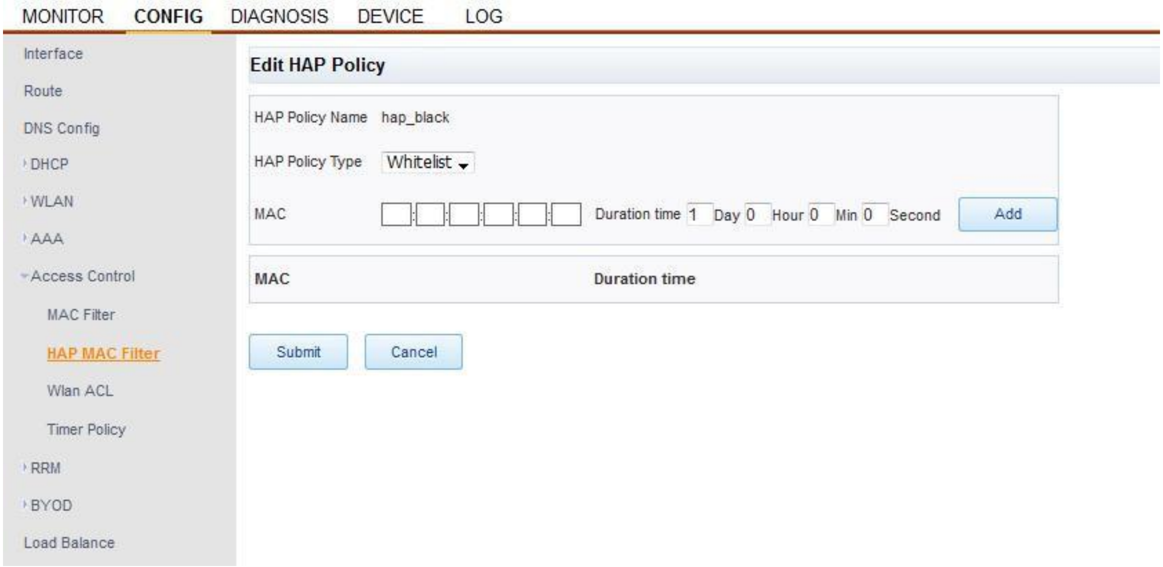
Fig. 7-6 HAP Filter Configuration

The HAP filter configuration parameter description is as shown in Table 7-3.

Parameter Item	Description
Add	Add different types of HAP rules
HAP Rule Name	Click on name link to [edit HAP rule]
Application	Apply HAP rule
Delete	Delete HAP rule

Table 7-3 HAP Filter Configuration Parameter Description

Edit HAP rule as shown in Fig. 7-7.



Edit HAP Policy

HAP Policy Name hap_black

HAP Policy Type Whitelist

MAC □:□:□:□:□:□ Duration time 1 Day 0 Hour 0 Min 0 Second

MAC	Duration time

Fig. 7-7 Edit HAP Rule

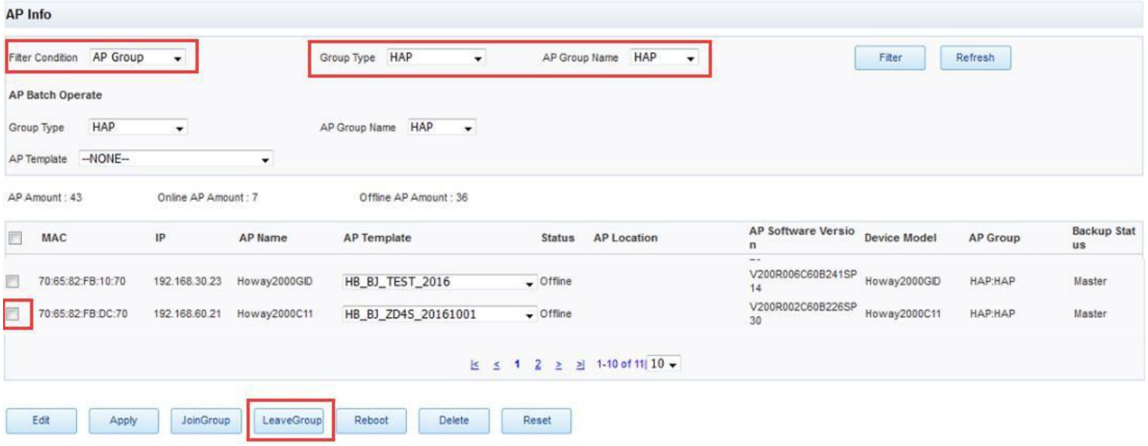
The parameter description of HAP rule edition is as shown in Table 7-4.

Parameter Item	Description
HAP Rule Type	The rule types include [white list] and [blacklist]
Add	Add terminal MAC addresses of different rules
Delete	Delete the added terminal MAC address

Table 7-4 HAP Rule Edition Parameter Description

7.5 Exit from HAP Group

User could choose the AP that are to exit from HAP group, set the type to “HAP”, select the name of group from which the AP will exit, and click on <exit from group>button as shown in Fig. 7-8, then AP will exit from the designated HAP group.



AP Info

Filter Condition AP Group

Group Type HAP AP Group Name HAP

AP Batch Operate

Group Type HAP AP Group Name HAP

AP Template --NONE--

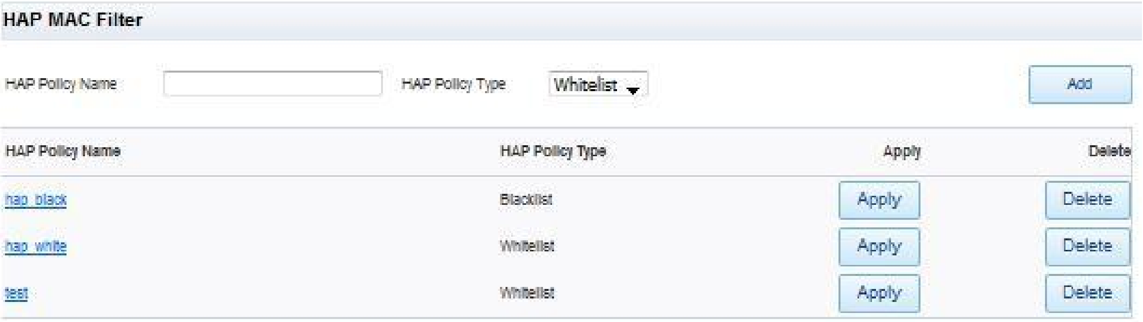
AP Amount : 43 Online AP Amount : 7 Offline AP Amount : 36

□	MAC	IP	AP Name	AP Template	Status	AP Location	AP Software Version	Device Model	AP Group	Backup Status
□	70:65:82:FB:10:70	192.168.30.23	Howay2000GID	HB_BJ_TEST_2016	Offline		V200R006C60B241SP14	Howay2000GID	HAP:HAP	Master
□	70:65:82:FB:DC:70	192.168.60.21	Howay2000C11	HB_BJ_ZD4S_20161001	Offline		V200R002C60B226SP30	Howay2000C11	HAP:HAP	Master

Fig. 7-8 Exit from HAP Group

7.6 HAP Filter Configuration

[HAP filter configuration] sets up the filtering rules for terminal in independent AP mode as shown in Fig. 7-9.



HAP MAC Filter

HAP Policy Name | HAP Policy Type: Whitelist | Add

HAP Policy Name	HAP Policy Type	Apply	Delete
hap_black	Blacklist	Apply	Delete
hap_white	Whitelist	Apply	Delete
test	Whitelist	Apply	Delete

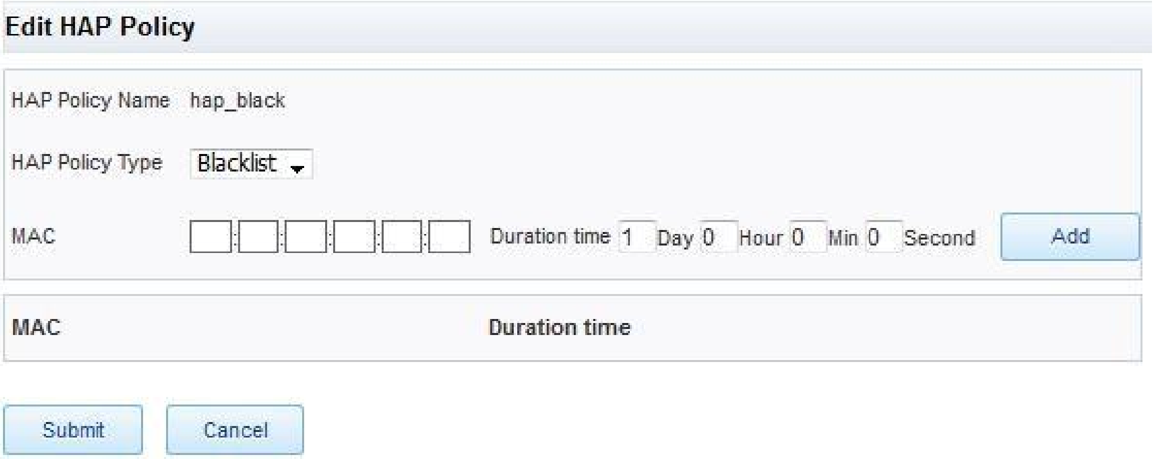
Fig. 7-9 HAP Filter Configuration

The HAP filter configuration parameter description is as shown in Table 7-5.

Parameter Item	Description
HAP Rule Type	The rule types include [white list] and [blacklist]
Add	Add different HAP rules
Application	Issue HAP rule configuration information to AP
Rule Name	Click on rule name to open [edit HAP rule] page
Delete	Delete the added terminal MAC address

Table 7-5 HAP Filter Configuration Parameter Description

Edit HAP rule as shown in Fig. 7-10.



Edit HAP Policy

HAP Policy Name hap_black

HAP Policy Type: Blacklist

MAC □:□:□:□:□:□ Duration time 1 Day 0 Hour 0 Min 0 Second Add

MAC	Duration time

Fig. 7-10 Edit HAP Rule

The parameter description of HAP rule edition is as shown in Table 7-6.

Parameter Item	**Description**
HAP Rule Type	The rule types include [white list] and [blacklist], and user could modify HAP rule type
Add	Add HAP rules for different terminal MACs

Table 7-6 HAP Rule Edition Parameter Description

Chapter 8 Interface Configuration

8.1 Interface Configuration Function Description

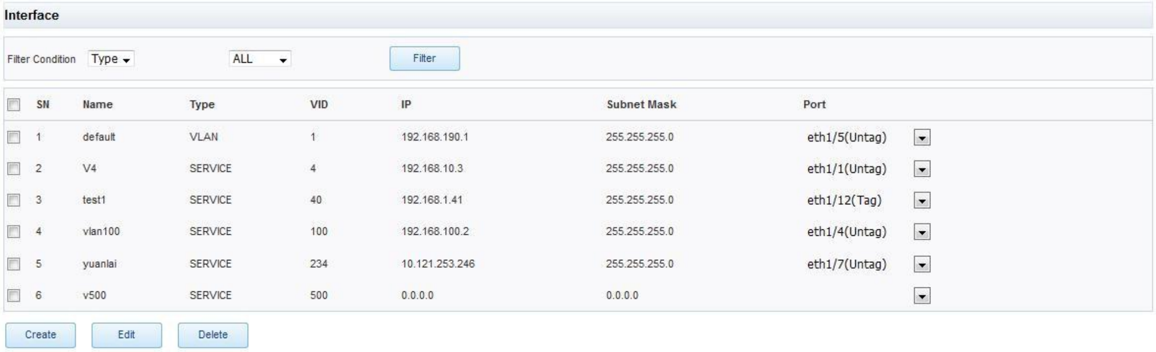
Interface configuration principally deals with device VLAN configuration, three-level interface address configuration, and the binding of VLAN and physical port, thereby enabling basic network communication interface configuration. AC wireless control system divides traditional VLAN into 3 interface types, i.e. VLAN, SERVICE and CAPWAP by service function type based on unique WLAN service features.

VLAN interface configuration is described as follows, and is principally used for AC management, and could also be used as an interface communicating with other devices, thus being equivalent with network device vlan using standard 802.1q protocol.

The created SERVICE interface could keep UP state without the involvement of any port, manage AP and Radius client’s vlan interface, and connect with Router and switch to constitute unified uplink interface.

when AC serves as gateway, the IP address of this interface is taken as STAgateway.

The interface configuration page is as shown in Fig. 8-1.


Interface

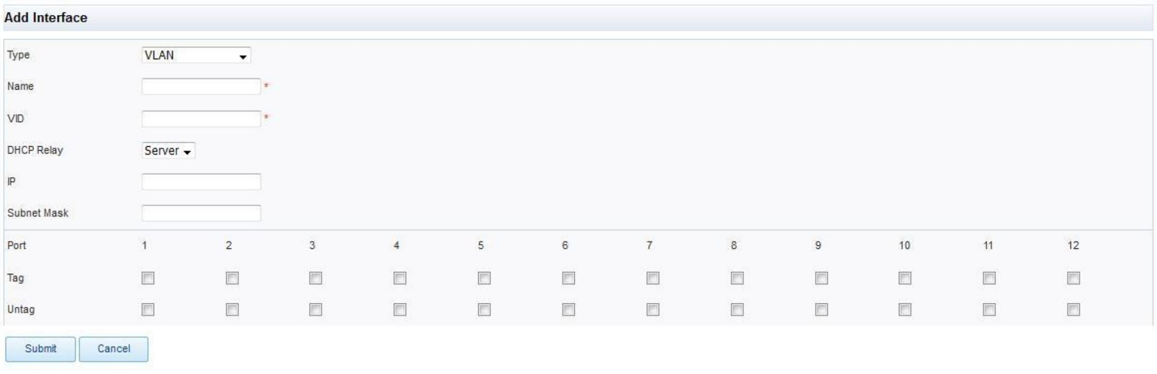
Filter Condition: Type, ALL

□	SN	Name	Type	VID	IP	Subnet Mask	Port
□	1	default	VLAN	1	192.168.190.1	255.255.255.0	eth1/5(Untag)
□	2	V4	SERVICE	4	192.168.10.3	255.255.255.0	eth1/1(Untag)
□	3	test1	SERVICE	40	192.168.1.41	255.255.255.0	eth1/12(Tag)
□	4	vlan100	SERVICE	100	192.168.100.2	255.255.255.0	eth1/4(Untag)
□	5	yuanlai	SERVICE	234	10.121.253.246	255.255.255.0	eth1/7(Untag)
□	6	v500	SERVICE	500	0.0.0.0	0.0.0.0	

Fig. 8-1 Interface Configuration Page

8.2 Create Interface Configuration

User could click on <create> button in the page as shown in Fig. 8-1 to open the [add interface] page as shown in Fig. 8-2.



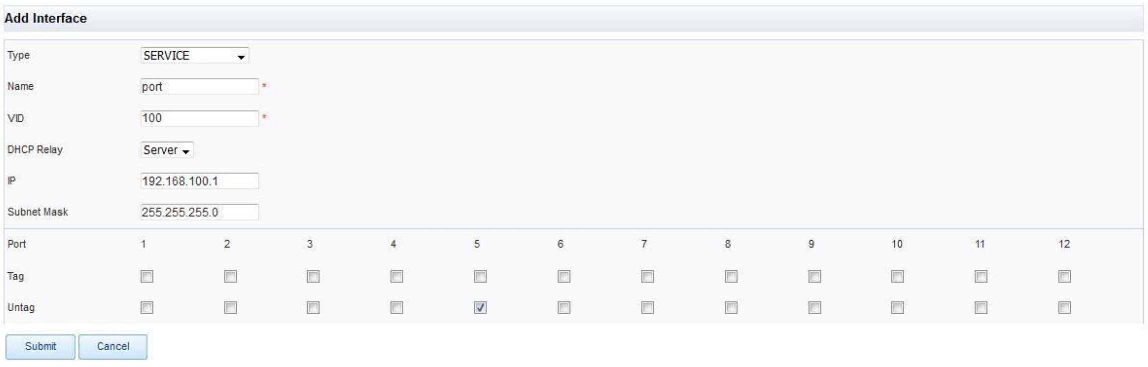
Add Interface

Type: VLAN
Name: *
VID: *
DHCP Relay: Server
IP:
Subnet Mask:

Port	1	2	3	4	5	6	7	8	9	10	11	12
Tag	□	□	□	□	□	□	□	□	□	□	□	□
Untag	□	□	□	□	□	□	□	□	□	□	□	□

Fig. 8-2 Add Interface Page

User could select “VLAN”, “SERVICE” and “CAPWAP” in [interface type] drop-down list based on actual networking requirements. Properly enter [interface name], [interface VID], [IP address] and [subnet mask], assign port to interface as needed as shown in Fig. 8-3, and click on “OK” to finish the creation.



Add Interface

Type: SERVICE
Name: port *
VID: 100 *
DHCP Relay: Server
IP: 192.168.100.1
Subnet Mask: 255.255.255.0

Port	1	2	3	4	5	6	7	8	9	10	11	12
Tag	□	□	□	□	□	□	□	□	□	□	□	□
Untag	□	□	□	□	☑	□	□	□	□	□	□	□

Fig. 8-3 Interface Addition Example

The page parameter description is as shown in Table 8-1.

Configuration Item	**Description**
Interface Type	The service types of VLAN, including “VLAN”, “SERVICE” and “CAPWAP”
Interface Name	VLAN interface description

Interface VID	Set the VLAN ID to be created
DHCP Relay	The types of DHCP Relay, including “Server” (default) and “Agent”
IP Address	Set the interface IP address of VLAN
Subnet Mask	Set the subnet mask of interface
Tagged Port	Port members send this VLAN message with tag
Untagged Port	Port members send this VLAN message without tag

Table 8-1 Interface Configuration Page Creation Parameter Description

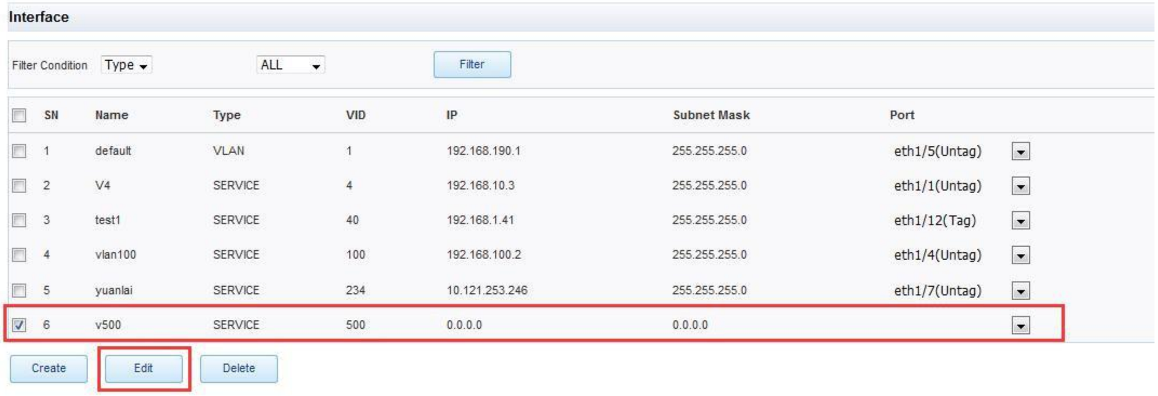
Note:

1. [Interface name] and [interface VID] can't be null; [interface name] could contain letters, numbers and underscores, and must begin with a letter; [interface VID] numbers should be within the range “1-4094”.
2. The interface added without setting IP address is two-level VLAN interface, and the interface added with IP address is three-level VLAN interface.

The binding principle of port: An “untagged port” belongs only to one VLAN, while a “tagged port” could subordinate to several VLANs.

8.3 Edit Interface Configuration

As shown in Fig. 8-4, select the created interface and click on <edit> to open interface edition page.



Interface

Filter Condition: Type ▾ ALL ▾ [Filter]

☐	SN	Name	Type	VID	IP	Subnet Mask	Port
☐	1	default	VLAN	1	192.168.190.1	255.255.255.0	eth1/5(Untag) ▾
☐	2	V4	SERVICE	4	192.168.10.3	255.255.255.0	eth1/1(Untag) ▾
☐	3	test1	SERVICE	40	192.168.1.41	255.255.255.0	eth1/12(Tag) ▾
☐	4	vlan100	SERVICE	100	192.168.100.2	255.255.255.0	eth1/4(Untag) ▾
☐	5	yuanlai	SERVICE	234	10.121.253.246	255.255.255.0	eth1/7(Untag) ▾
☑	6	v500	SERVICE	500	0.0.0.0	0.0.0.0	▾

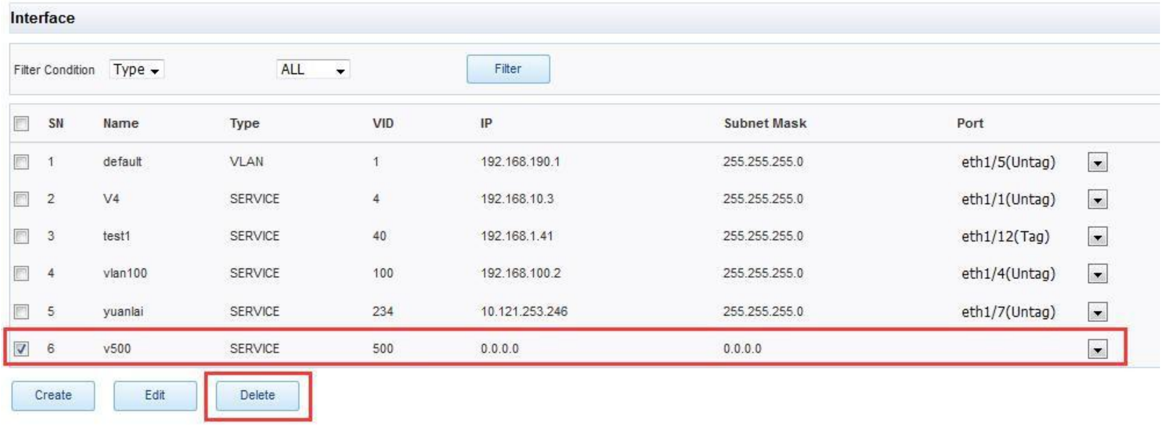
Fig. 8-4 Edit interface Configuration

Note:

1. Only the “DHCP Relay” type, “IP address”, “subnet mask” and “port” could be modified in edition page.
2. Only one interface configuration data could be edited a time.

8.4 Delete Interface Configuration

Select the created interface in the page as shown in Fig. 8-5, and click on <delete> to successfully delete the interface configuration.



Interface

Filter Condition: Type, ALL

□	SN	Name	Type	VID	IP	Subnet Mask	Port
□	1	default	VLAN	1	192.168.190.1	255.255.255.0	eth1/5(Untag)
□	2	V4	SERVICE	4	192.168.10.3	255.255.255.0	eth1/1(Untag)
□	3	test1	SERVICE	40	192.168.1.41	255.255.255.0	eth1/12(Tag)
□	4	vlan100	SERVICE	100	192.168.100.2	255.255.255.0	eth1/4(Untag)
□	5	yuanlai	SERVICE	234	10.121.253.246	255.255.255.0	eth1/7(Untag)
☑	6	v500	SERVICE	500	0.0.0.0	0.0.0.0	

Fig. 8-5 Delete Interface Configuration

Note:

1. A number of interface configuration data could be collectively deleted every time.
2. Default VLAN is the default VLAN with a VID of 1, which mustn't be manually deleted or created.

8.5 Search Criteria

Interface configuration data could be subjected to filtered query based on filter criteria "interface type", "interface name" and "VID". Please refer to Table 8-2 for filter criteria parameter description.

Configuration Item	Description
Interface Type	There are four parameters available, i.e. "ALL", "VLAN", "SERVICE" and "CAPWAP"
Interface Name	The set VLAN interface description
VID	The created VLAN ID

Table 8-2 Search Criteria Parameter Description

Chapter 9 DHCP Configuration

9.1 DHCP Function Overview

DHCP (Dynamic Host Configuration Protocol) employs client/server communication mode, where the client applies to server for configuration, and the server replies with the IP address assigned to client and other corresponding configuration information for the dynamic configuration of IP address and other information.

The process of dynamically obtaining IP address is as follows (Fig. 9-1).

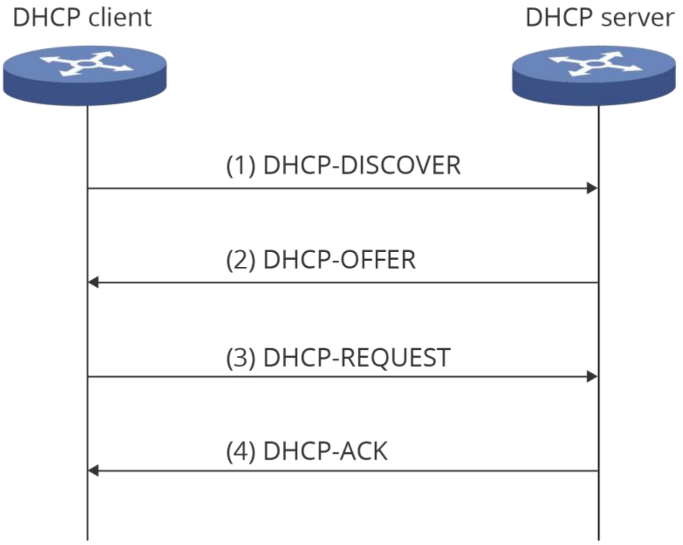


Fig. 9-1 DHCP Interaction Process

DHCP client principally gets IP address from DHCP server dynamically through the following four stages:

1) Discovery stage, in which DHCP client seeks DHCP server. The client sends DHCP-DISCOVER message through broadcasting.

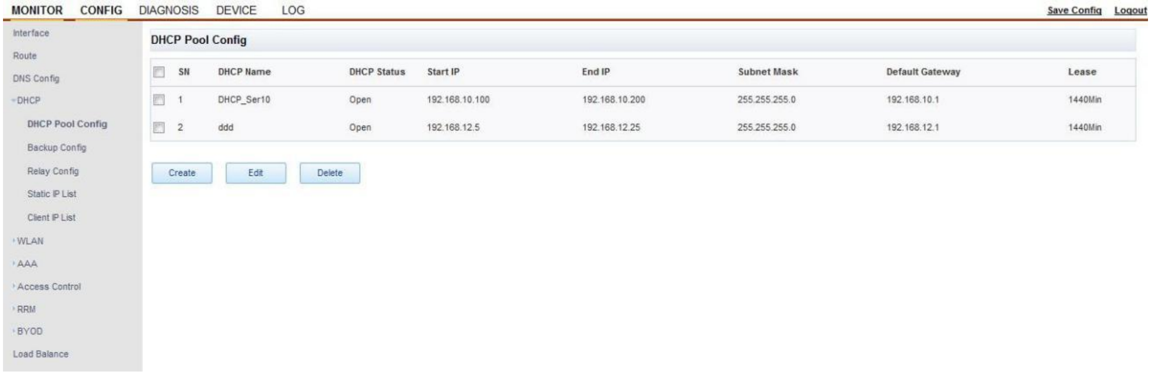
2) Offer stage, in which DHCP server offers IP address. Upon receipt of DHCP-DISCOVER message from client, DHCP server chooses an IP address based on the priority of IP address allocation, and sends it together with other parameters to client through DHCP-OFFER message. The method for sending DHCP-OFFER message is dependent on flag field in DHCP-DISCOVER message.

3) Selection stage, in which DHCP client selects the IP address. Where several DHCP servers send the client DHCP-OFFER message, the client only accepts the first received DHCP-OFFER message, and sends DHCP-REQUEST message through broadcasting, which contains the IP address assigned by DHCP server in DHCP-OFFER message.

4) Confirmation stage, in which the DHCP server acknowledges IP address. Once DHCP server receives the DHCP-REQUEST message from DHCP client, only the servers selected by DHCP client are allowed to perform the following operations: If the allocation of address to this client is acknowledged, DHCP-ACK message is returned; otherwise, DHCP-NAK message is returned to indicate that the address can't be assigned to the client.

9.2 Configure DHCP

Click on “[network configuration] > [DHCP configuration]” to open DHCP configuration page, which is composed of five parts, i.e. address pool configuration, hot standby configuration, Relay configuration, static IP and client list as shown in Fig. 9-2.



DHCP Pool Config

□	SN	DHCP Name	DHCP Status	Start IP	End IP	Subnet Mask	Default Gateway	Lease
□	1	DHCP_Ser10	Open	192.168.10.100	192.168.10.200	255.255.255.0	192.168.10.1	1440Min
□	2	ddd	Open	192.168.12.5	192.168.12.25	255.255.255.0	192.168.12.1	1440Min

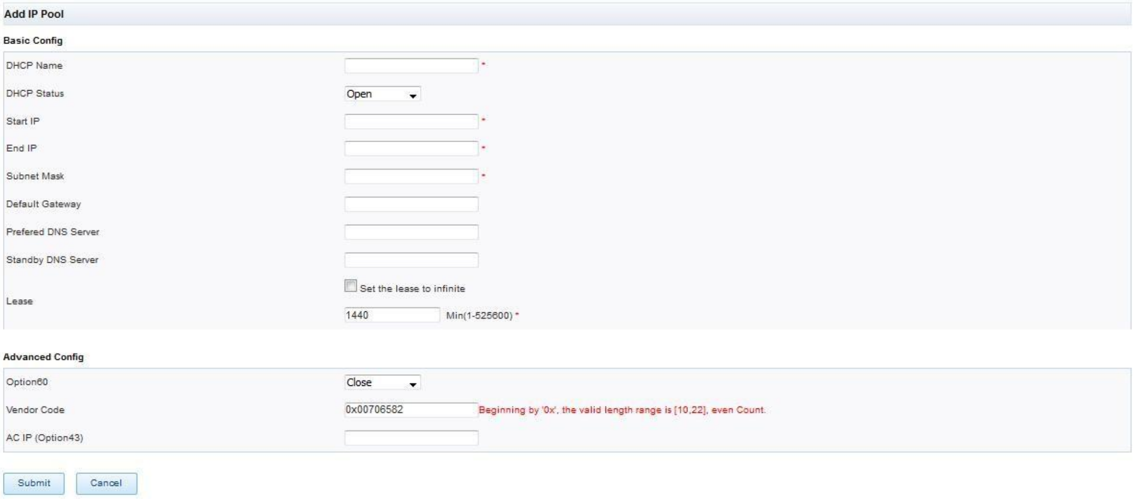
Fig. 9-2 DHCP Configuration Page

DHCP service is enabled by default; user could add a number of address pools to DHCP list; DHCP address allocation is associated through the gateway configuration and interface address in DHCP configuration; DHCP client gets corresponding address from the DHCP address pool under corresponding interface address VLAN.

DHCP hot backup feature configuration is set up globally; where AC wireless controller is subjected to capwap hot standby, DHCP hot standby function is used; please refer to Chapter 19 for details of dual CAPWAP hot standby function.

9.2.1 Create DHCP Address Pool

Click on <create> in DHCP list page as shown in Fig. 9-2 to open [add DHCP] page; as shown in Fig. 9-3, user could enter [DHCP name], [DHCP state], [starting IP address], [ending IP address], [subnet mask], [default gateway], [preferred DNS server], [standby DNS server], [manufacturer code], [lease time], [AC IP (Option43)] and [Option60] in this page as needed, and click on <OK> to finish the creation.



Add IP Pool

Basic Config

DHCP Name	*
DHCP Status	Open
Start IP	*
End IP	*
Subnet Mask	*
Default Gateway	
Prefered DNS Server	
Standby DNS Server	
Lease	□ Set the lease to infinite 1440 Min(1-525600) *

Advanced Config

Option60	Close
Vendor Code	0x00706582 Beginning by '0x', the valid length range is [10,22], even Count.
AC IP (Option43)	

Fig. 9-3 Create DHCP Page

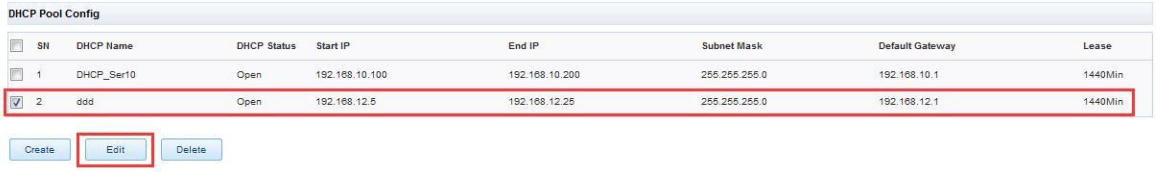
Please refer to Table 9-1 for DHCP configuration parameter description.

Configuration Item	**Description**
DHCP Name	The created DHCP address pool name
DHCP State	Determine whether or not to enable this DHCP address pool rule (enable/disable)
Starting IP Address	The starting address assigned to client
Ending IP Address	The ending address assigned to client
Subnet Mask	The subnet mask of address assigned to client
Default Gateway	The gateway IP address assigned to DHCP client; the data has to be forwarded through gateway when DHCP client is used to access servers or host outside this network segment
Preferred DNS Server	The main DNS server IP address assigned to DHCP client; DHCP server shall allocate IP address to client and designate the DNS server address so that DHCP client could access a host at Internet through domain name
Alternate DNS Server	The alternate DNS server IP address assigned to DHCP client
Lease Time	Set the valid lease period of dynamically allocated IP address in DHCP address pool
Option60	Option60 is principally used for client to report its own manufacturer and configuration information; DHCP server determines whether the client is legal based on the reported manufacturer information; address is assigned to legal client but not to illegal client
Manufacturer Code	
AC IP (option43)	AC IP (Option43) informs AP of the address of wireless controller, and is principally used for AP device in WLAN to get AC IP through option43 attribute issued by dhcp server after getting an address from dhcp server, and then seek AC for registration based on AC IP

Table 9-1 Parameter Description of Add DHCP Configuration Addition

9.2.2 Modify DHCP Address Pool

In the page as shown in Fig. 9-4, user could select the DHCP address pool record to be modified, and click on <edit> to open the address pool configuration page for the modification of corresponding parameters.



DHCP Pool Config

□	SN	DHCP Name	DHCP Status	Start IP	End IP	Subnet Mask	Default Gateway	Lease
□	1	DHCP_Ser10	Open	192.168.10.100	192.168.10.200	255.255.255.0	192.168.10.1	1440Min
☑	2	ddd	Open	192.168.12.5	192.168.12.25	255.255.255.0	192.168.12.1	1440Min

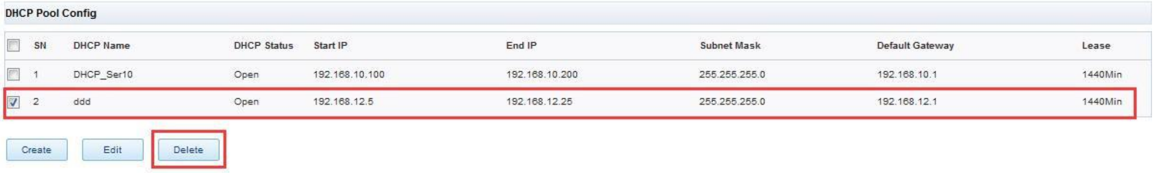
Fig. 9-4 Edit DHCP Configuration

Note:

1. Only the parameters of [DHCP state], [default gateway], [DNS server] and [advanced configuration] could be modified in edition page.
2. Only one address pool configuration data could be edited every time.

9.2.3 Delete DHCP Address Pool

In the page as shown in Fig. 9-5, user could select the DHCP address pool record to be deleted and click on <delete> button.



DHCP Pool Config

□	SN	DHCP Name	DHCP Status	Start IP	End IP	Subnet Mask	Default Gateway	Lease
□	1	DHCP_Ser10	Open	192.168.10.100	192.168.10.200	255.255.255.0	192.168.10.1	1440Min
☑	2	ddd	Open	192.168.12.5	192.168.12.25	255.255.255.0	192.168.12.1	1440Min

Fig. 9-5 Delete DHCP Address Pool Configuration

Note: A number of DHCP configuration data could be collectively deleted by user every time.

9.3 Hot Standby Configuration

DHCP hot standby configuration (Fig. 9-6) is used for switching DHCP address pool upon AC switching during AC active-standby networking so as to ensure DHCP could offer normal service during AC rearrangement. For configuration it's essential to designate local AC IP address and peer AC IP address.

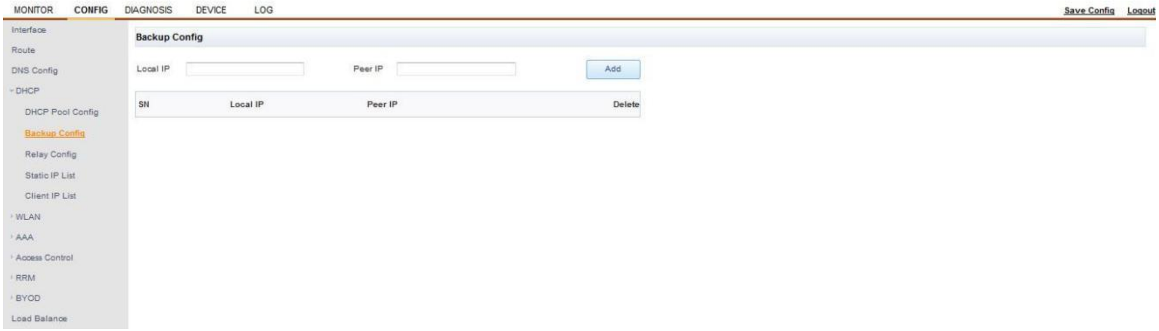


Fig. 9-6 DHCP Hot Standby Configuration

9.4 Relay Configuration

AC supports DHCP Relay, which is also known as DHCP relay agent. If DHCP client and DHCP server share the same physical segment, the client could correctly obtain the dynamically allocated ip address. If they are not in the same physical segment, DHCP Relay Agent is needed. DHCP Relay agent makes it not necessary to arrange DHCP server in each physical segment; it could transfer message to DHCP servers in different physical subnets, and transfer server message back to DHCP clients in different physical subnets. Please refer to Fig. 9-7.

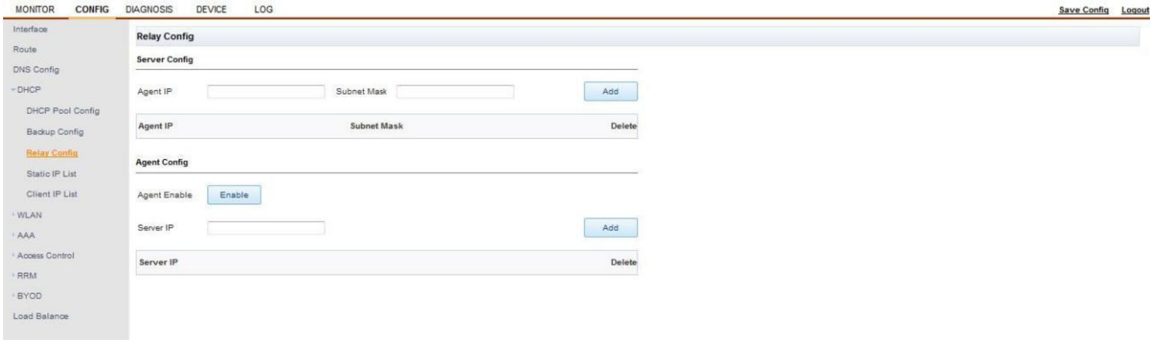


Fig. 9-7 DHCP Relay Configuration

9.5 Static IP List

DHCP supports static IP and MAC address binding for automatic assignment of fixed IP address to client as shown in Fig. 9-8. User could click on <create> button to add client's MAC address and bind it with the IP address to be assigned. When this client automatically gets address, the static IP address assigned by administrator is sent to the client.

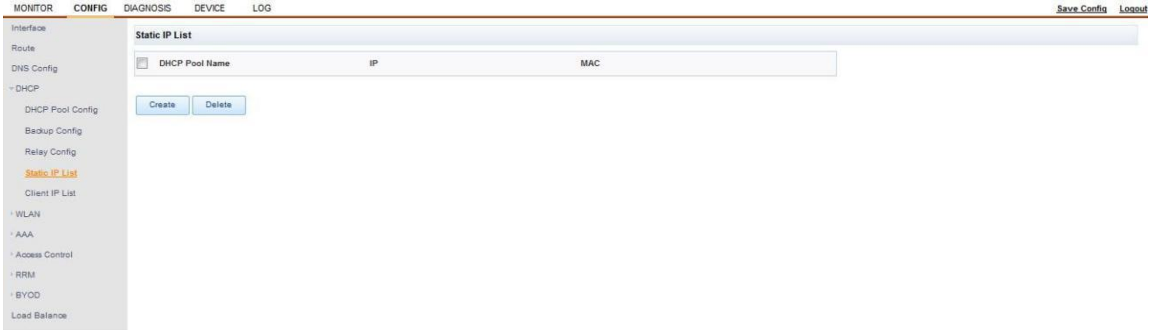


Fig. 9-8 Static IP List

9.6 Client List

DHCP client list shows the information about address assigned by DHCP server to client as shown in Fig. 9-9. User could search by "address pool name" or click on <refresh> button to refresh the page in real time so as to view the latest list information.

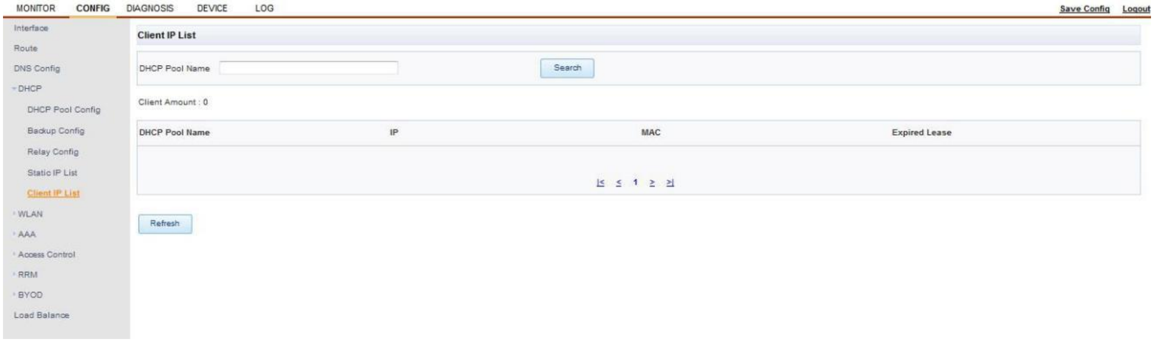


Fig. 9-9 Client List

Chapter 10 Routing Configuration

10.1 Routing Function Description

Router is essential for route selection at Internet; router selects an appropriate route (through a certain network) based on the destination address of received message, and transmits the message to next router. The last router in the path delivers message to the destination host.

10.1.1 Route List

Route list is the key to message forwarding by router. Every router maintains a route list, where each route item indicates the router interface through which the message is delivered to a certain subnet or host, the next hop of the path, or the delivery to destination host in a directly connected network without passing through other routers.
The routes in route list could normally be divided into the following three categories by source:
1)The routes discovered by link layer protocol (also known as interface route or directly connected route).
2)Static routes manually configured by network administrator.
3)Routes discovered by dynamic route protocol.

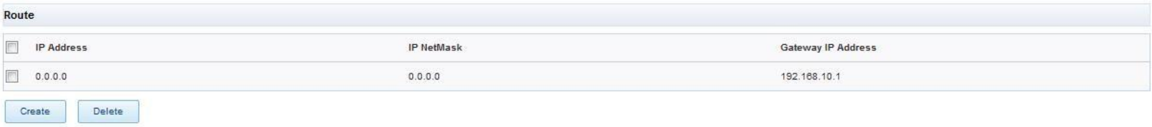
Route list contains the following critical items:
1) IP address: Used to identify the destination host or destination network of IP datagram.
2) Network mask: Used with destination address to identify the network segment where destination host or router is located.
3)Gateway address: Namely the next hop address, i.e. the IP address of next router that is closer to destination network.

10.1.2 Static Route

Static route refers to the routing information manually configured by user or network administrator. When network topology structure or link state changes, network administrator has to manually modify related static route information in route list. Static route is normally applicable for simple network environment, where network administrator could have a clear understanding of network topology structure for correct setup of routing information.

10.2 Static Route Configuration

User could perform routing configuration in "[network configuration] > [configuration page]" page as shown in Fig. 10-1.



Route

□	IP Address	IP NetMask	Gateway IP Address
□	0.0.0.0	0.0.0.0	192.168.10.1

Fig. 10-1 Routing Configuration Page

10.2.1 Create Static Route

User could create static route data by clicking on the <create> button as shown in Fig. 10.1. Enter [IP address], [subnet mask] and [gateway address] parameters in the page as shown in Fig. 10-2.

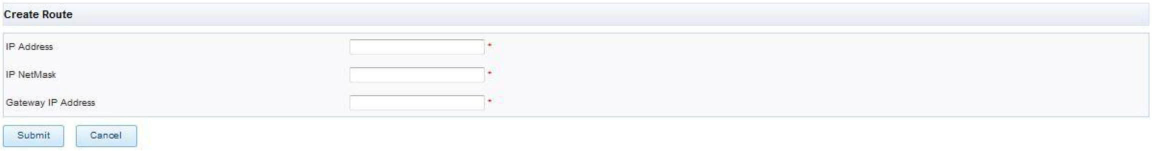


Fig. 10-2 Create Routing Configuration

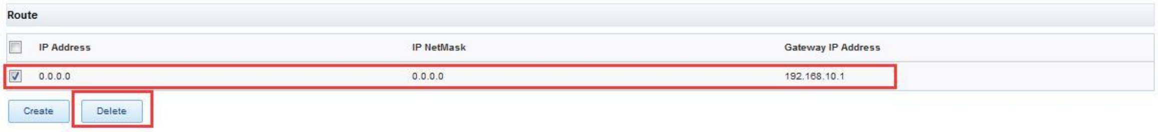
The parameter description of routing configuration page is as shown in Table 10-1.

Configuration Item	Description
IP Address	Used to identify the destination host or destination network of IP datagram
Subnet Mask	Used with destination address to identify the network segment where destination host or router is located
Gateway Address	Next hop address of route

Table 10-1 Routing Configuration Creation Parameter Description

10.2.2 Delete Static Route

User could delete existing static route data by clicking on the <delete> button as shown in Fig. 10-3.



□	IP Address	IP NetMask	Gateway IP Address
☑	0.0.0.0	0.0.0.0	192.168.10.1

Fig. 10-3 Delete Static Route

Note: A number of routing configuration data could be collectively deleted by user every time.

Chapter 11 WLAN Configuration

11.1 WLAN Service Description

WLAN (Wireless Local Area Network) technology is a focus of current communication field; as compared with wired network, wireless local area network is characterized by easier startup and implementation and low maintenance cost; a local area network covering the entire building or area could be established normally by arranging one or more AP devices. WLAN system, however, is not a completely wireless system as its server and backbone network are arranged in fixed network, although users could access the network wirelessly.

With WLAN solution, network operators and enterprises could provide users with wireless local area network service in the following aspects: Use devices with wireless local area network features to establish a wireless network, via which users could visit fixed networks or the Internet.

1) Wireless users could access traditional 802.3 LAN.

2) Securely access WLAN using different authentication and encryption methods.

3)Provide wireless users with secure network access and seamless roaming in mobile area.

11.1.1 User Access Process

To get connected with AP, users have to pass through the active/passive scanning, authentication and association. The flow chart is as shown in Fig. 11-1.

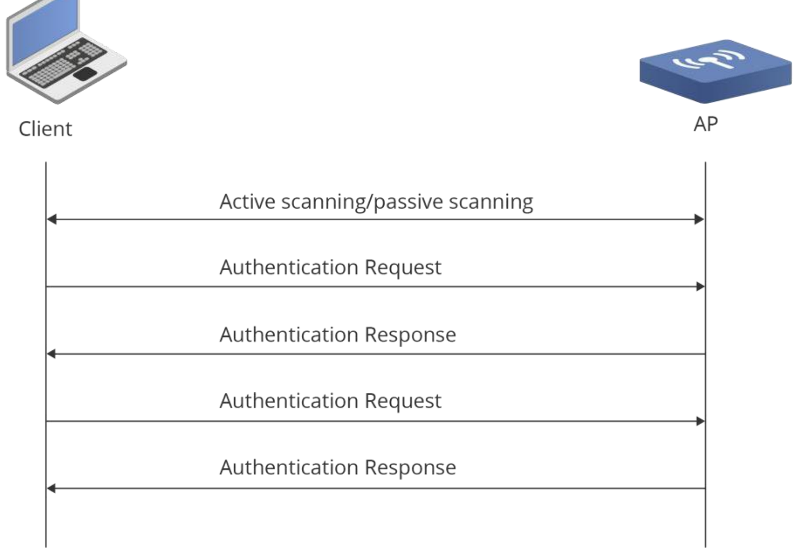


Fig. 11-1 User Access Process

1) Wireless scanning

(1) Active scanning

User could actively seek network by scanning surrounding wireless networks through "active scanning". Active scanning is divided into two categories by SSID:

① Client sends Probe Request (SSID is null): User predefines a channel list, and the client broadcasts probe request frame (Probe Request) in channels therein. Upon receipt of the probe request frame, AP gives probe response frame. The client makes association with the AP with the strongest signal. This method could be used for wireless client to determine if there is any wireless service available through active scanning.

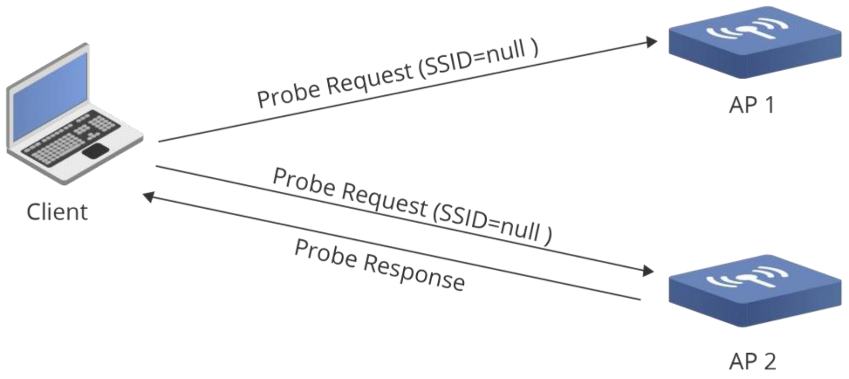


Fig. 11-2 Active Scanning Process (SSID is NULL in Probe Request)

② Client sends Probe Request (which carries designated SSID): In such a case, the client only unicasts probe request frame due to the SSID carried; the corresponding AP makes response to the request received. This method could be used for wireless client to get connected to designated wireless network through active scanning.

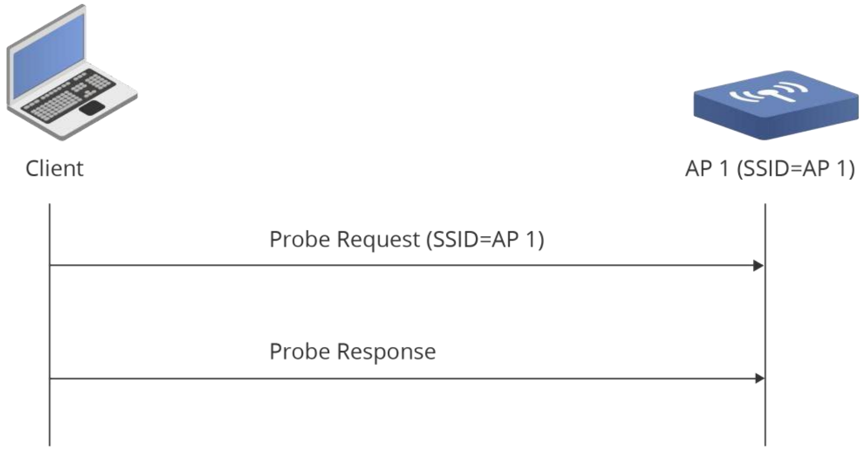


Fig. 11-3 Active Scanning Process (Probe Request Carries Designated SSID)

(2) Passive scanning

Passive scanning means the client finds network by listening to the Beacon frame sent regularly by AP. User predefines a channel list for scan, and listens to beacon in each channel. Passive scanning requires AP to periodically send Beacon frame. Passive scanning could be used when user need to save power. General VoIP terminal normally employs passive scanning.

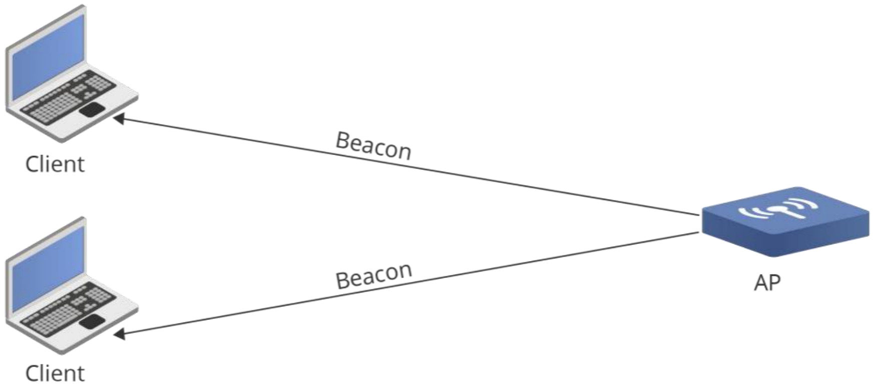


Fig. 11-4 Passive Scanning

2) Authentication process

To avoid illegal user access, the authentication must be established between user and AC; there are two authentication mechanisms. Authentication is the prior condition for association stage.

- Open system authentication
- Shared key authentication

3) Association process

To access wireless network through AP, user has to get associated with certain AP. User could send association request frame to AP after selecting wireless network through designated SSID and passing AP authentication. AP adds user information to database and makes association response to user. User could only get associated with one AP a time, and the association is always initiated by user.

4) Other related processes

① Deauthentication

Deauthentication is used to interrupt established authentication relation. AC sends deauthentication frame to remove user from wireless system. A variety of factors may trigger deauthentication, e.g.

- Receipt of association or disassociation frame from non-authenticated user.
- Receipt of data frame from non-authenticated user.
- Receipt of PS-Poll frame from non-authenticated user.
- User’s valid timer expires or user port is not a secure port.

② Disassociation

User sends disassociation frame to AP so as to terminate the association. A variety of factors may trigger disassociation, e.g.

- Receipt of authenticated unassociated user’s data frame.
- Receipt of authenticated unassociated user’s PS-Poll frame.

Disassociation frame could be either broadcast frame or unicast frame.

③ Reassociation

When roaming from an AP area/BSS area to another AP area/BSS area, the client could use reassociation. AP sends reassociation request to AC. AC notifies original AP to delete this user information from database, notifies destination AP to add user information to database, and sends frame to announce the successful reassociation with user.

Where the client temporarily gets out of AP’s coverage, reassociation must be conducted if it gets connected again.

11.2 CAPWAP Protocol Overview

CAPWAP (Controlling and Provisioning of Wireless Access Point) protocol defines the way of communication between wireless access point (AP) and wireless controller (AC), and provides a general encapsulation and transport mechanism for interconnection between AP and AC as shown in Fig. 11-5.

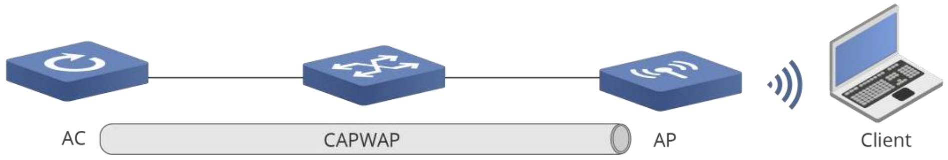


Fig. 11-5 CAPWAP Diagram

CAPWAP runs in AP and AC simultaneously to assure the security of AC-AP communication in WLAN system. The AP-AC communication is established based on standard UDP client/server side model.

CAPWAP offers data tunnel for encapsulating the data packets sent to AC. These data packets could be 802.11 protocol-compliant data packets.

In addition, CAPWAP supports the remote AP configuration and WLAN management service etc. of AC.

11.3 WLAN Canonical Topology

Both two-level networking and three-level networking is available between AC and AP. The networking is flexible and diverse.

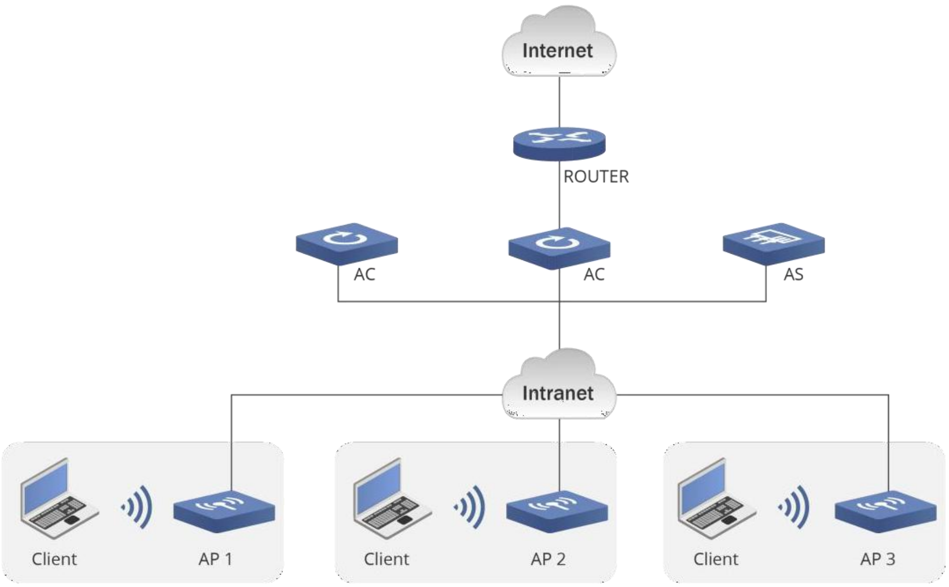
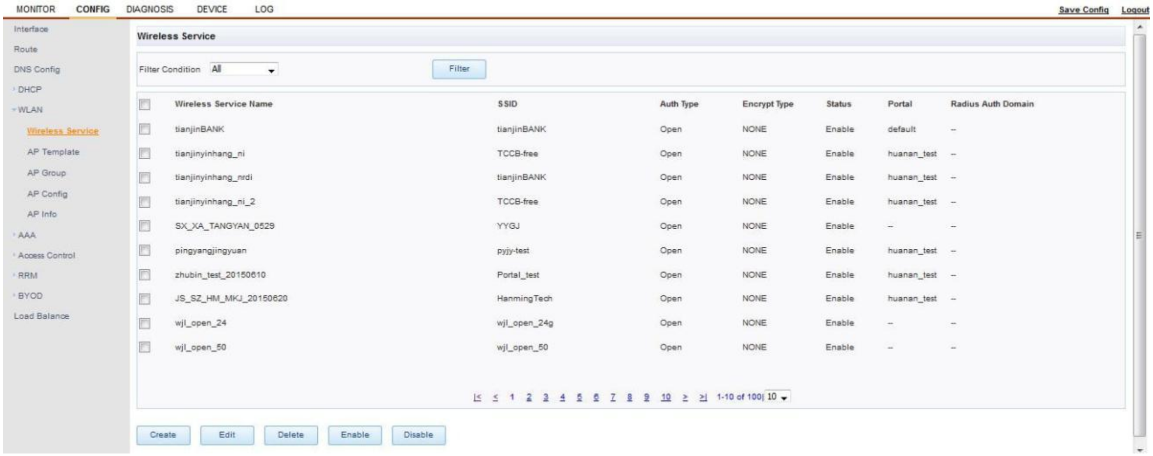


Fig. 11-6 Canonical Topology Networking Diagram of WLAN

11.4 WLAN Configuration

[WLAN configuration] is divided into five submenus, i.e. [wireless service configuration], [AP template], [AP group], [AP configuration] and [AP information] as shown in Fig. 11-7.



Wireless Service

Filter Condition: All

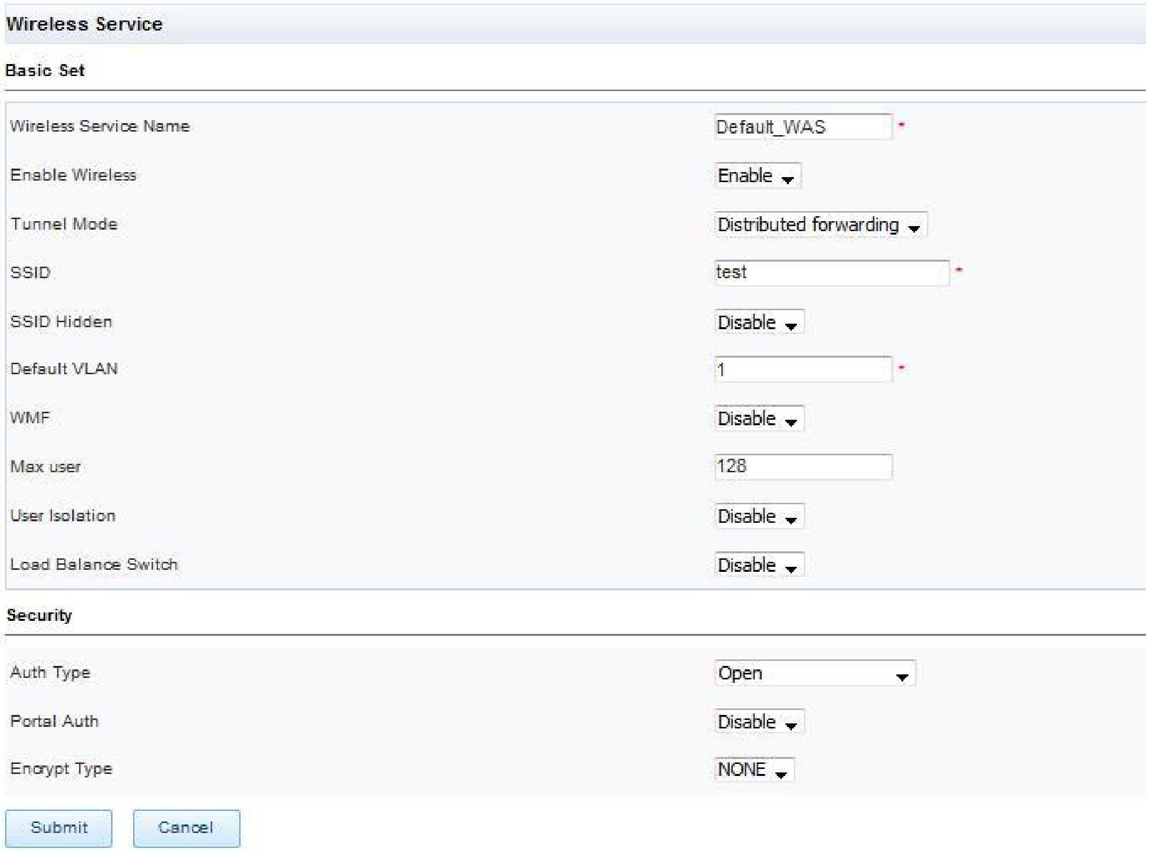
☐	Wireless Service Name	SSID	Auth Type	Encrypt Type	Status	Portal	Radius Auth Domain
☐	tianjinBANK	tianjinBANK	Open	NONE	Enable	default	--
☐	tianjinyinhang_ni	TCCB-free	Open	NONE	Enable	huanan_test	--
☐	tianjinyinhang_nrdi	tianjinBANK	Open	NONE	Enable	huanan_test	--
☐	tianjinyinhang_ni_2	TCCB-free	Open	NONE	Enable	huanan_test	--
☐	SX_XA_TANGYAN_0529	YYGJ	Open	NONE	Enable	--	--
☐	pingyangjingyuan	pyjy-test	Open	NONE	Enable	huanan_test	--
☐	zhubin_test_20150610	Portal_test	Open	NONE	Enable	huanan_test	--
☐	JS_SZ_HM_MKJ_20150620	HanmingTech	Open	NONE	Enable	huanan_test	--
☐	wjl_open_24	wjl_open_24g	Open	NONE	Enable	--	--
☐	wjl_open_50	wjl_open_50	Open	NONE	Enable	--	--

|< < 1 2 3 4 5 6 7 8 9 10 > >| 1-10 of 100| 10

Fig. 11-7 WLAN Configuration Page

11.4.1 Wireless Service Configuration

1) Create Wireless Service Configuration
User could click on <create> button to add wireless service configuration in the wireless service configuration page as shown in Fig. 11-7; in the page as shown in Fig. 11-8, user could configure wireless service parameters, and click on <OK> therein.



Wireless Service

Basic Set

Wireless Service Name	Default_WAS *
Enable Wireless	Enable
Tunnel Mode	Distributed forwarding
SSID	test *
SSID Hidden	Disable
Default VLAN	1 *
WMF	Disable
Max user	128
User Isolation	Disable
Load Balance Switch	Disable

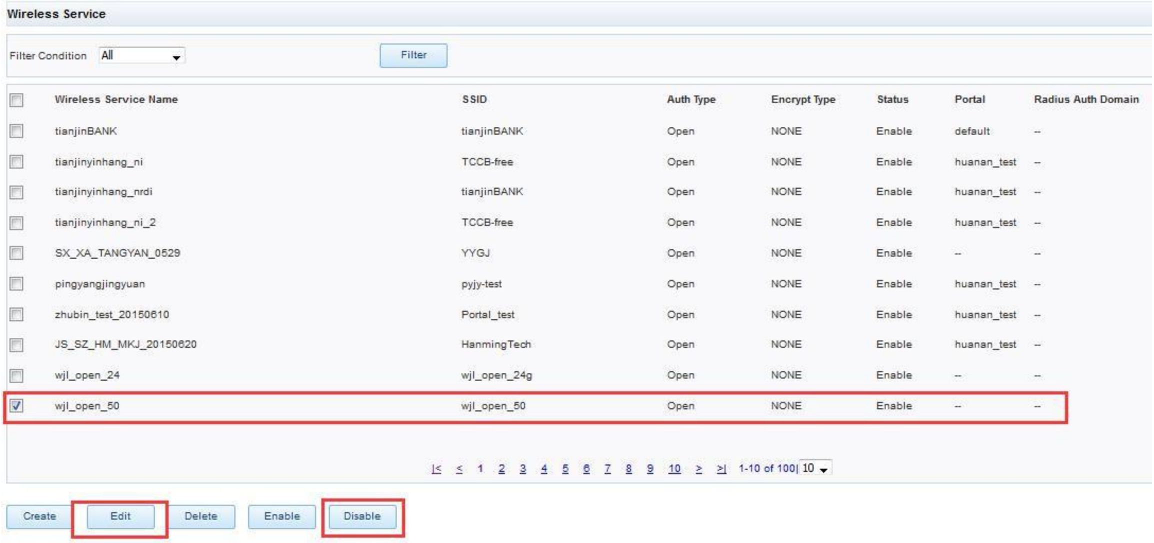
Security

Auth Type	Open
Portal Auth	Disable
Encrypt Type	NONE

Fig. 11-8 Wireless Service Configuration

2) Edit Wireless Service Configuration

<Disable> wireless service template before <editing> it. As shown in Fig. 11-9, select a wireless service, <disable>the wireless service, re-select the wireless service and click on <edit> to get into [wireless access service configuration] page; in the page as shown in Fig. 11-9, user could edit & modify the wireless service template, and click on <OK> button at bottom of page upon completion of edition. Select the modified wireless service upon completion of addition, and click on <enable> button to bring it into effect.

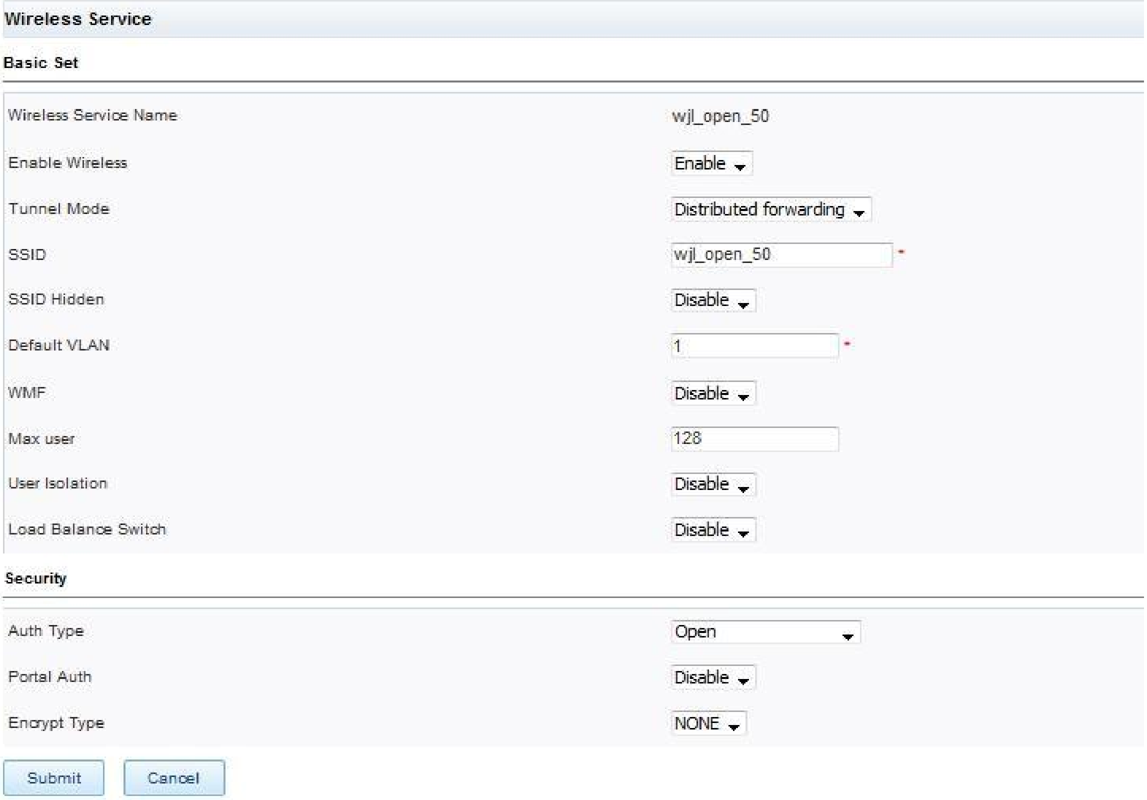


Wireless Service

Filter Condition: All

☐	Wireless Service Name	SSID	Auth Type	Encrypt Type	Status	Portal	Radius Auth Domain
☐	tianjinBANK	tianjinBANK	Open	NONE	Enable	default	--
☐	tianjinyinhang_ni	TCCB-free	Open	NONE	Enable	huanan_test	--
☐	tianjinyinhang_nrdi	tianjinBANK	Open	NONE	Enable	huanan_test	--
☐	tianjinyinhang_ni_2	TCCB-free	Open	NONE	Enable	huanan_test	--
☐	SX_XA_TANGYAN_0529	YYGJ	Open	NONE	Enable	--	--
☐	pingyangjingyuan	pyjy-test	Open	NONE	Enable	huanan_test	--
☐	zhubin_test_20150610	Portal_test	Open	NONE	Enable	huanan_test	--
☐	JS_SZ_HM_MKJ_20150620	HanmingTech	Open	NONE	Enable	huanan_test	--
☐	wjl_open_24	wjl_open_24g	Open	NONE	Enable	--	--
☑	wjl_open_50	wjl_open_50	Open	NONE	Enable	--	--

Fig. 11-9 Disable Wireless Service



Wireless Service

Basic Set

Wireless Service Name	wjl_open_50
Enable Wireless	Enable
Tunnel Mode	Distributed forwarding
SSID	wjl_open_50 *
SSID Hidden	Disable
Default VLAN	1 *
WMF	Disable
Max user	128
User Isolation	Disable
Load Balance Switch	Disable

Security

Auth Type	Open
Portal Auth	Disable
Encrypt Type	NONE

Fig. 11-10 Edit Wireless Service

3) Delete Wireless Service Configuration

Select the name of wireless service to be deleted in the page as shown in Fig. 11-9, disable it, and click on "delete" at bottom of the page to delete a wireless service.

4) Enable/disable wireless service

User could select a wireless service in the page as shown in Fig. 11-10, and click on "enable" or "disable" to enable or disable it.

Note:

User must disable the wireless service before modifying or deleting its configuration data.

Enable the modified wireless service, when the configuration modified takes effect.

Wireless service configuration parameter description is as shown in Table 11-1.

Configuration Item	**Description**
Wireless Service Name	Used to identify the description of wireless access service name
Enable Wireless Network	Wireless service on/off (ON or OFF)
Tunnel Mode	Specify the tunnel mode for wireless access service data; the tunnel mode is divided into distributed forwarding
SSID	The character string for identification of a virtual wireless AP
Hide SSID	When "hide SSID" is enabled, STA can't scan the SSID name of AP; when "hide SSID" is turned off, STA could scan the SSID name of AP. A method for preventing illegal STA access
Default VLAN	This is VLAN ID of service VLAN; this is the VID of STA data message; "0" is untagged VID; "1-4094" are VIDs with tag
Enable WMF	Wireless multicast on/off; when "on" is selected, wireless multicast is enabled in BSS; when "off" is selected, this function is disabled
Max. Number of Users Associated	Used to configure the max. number of users that could be connected to this SSID (128 by default); user could select the max. number within 1-128
User Isolation	Select "enable" to enable isolation mode, or select "disable" to disable the SSID isolation mode; users associated with this SSID could communicate with each other
Load Balancing on/off	Turn on/off load balancing function switch (off by default). When "enable" is selected, the [load balancing mode] option appears below
Load Balancing Mode	The option that appears after enabling load balancing includes two modes, i.e. "number of users" and "traffic". "The number of users" means load balancing is performed based on the number of users at each AP; "traffic" means load balancing is performed based on data traffic at each AP
Authentication Mode	Provide options for this SSID wireless connection security mode, and enhance wireless security by configuring different authentication methods of SSID; user could choose from the six authentication methods, i.e. Open, Shared, WPA, WPA2, WPA-PSK and WPA2-PSK, as needed
Portal Authentication	When the authentication mode "Open" is enabled, "Portal authentication" configuration is active. "Portal authentication" involves two states: On and off

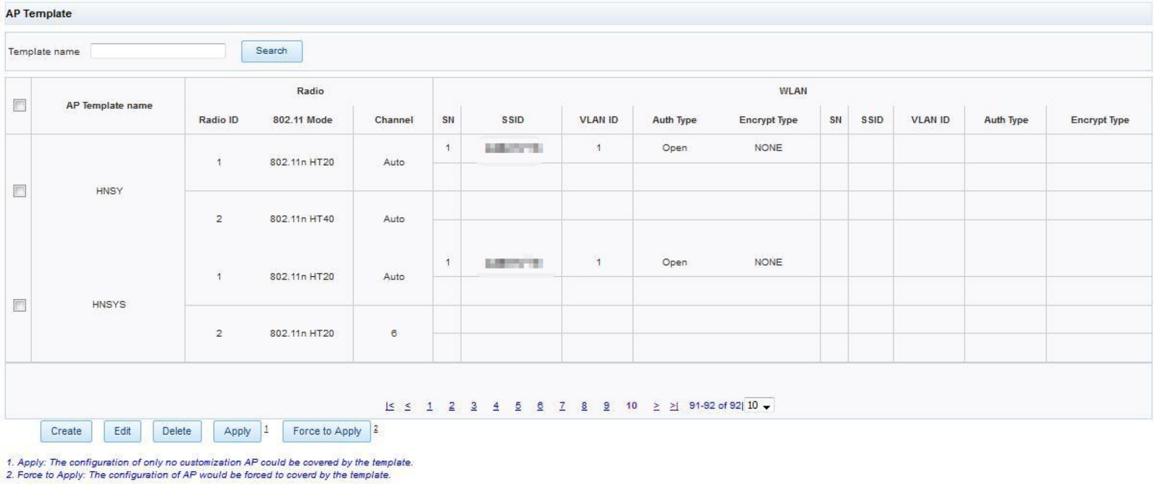
Portal Server Name	This item is configurable when "portal authentication" is enabled; the user-authenticated portal server under this ess could be designated
White List Set	This item is configurable when "portal authentication" is enabled; the white list set accessible to user before portal authentication under this ess is designated
Encryption Type	Enable the encryption type of this SSID: When "authentication method" is "Open", the encryption types include "not used" and "WEP"When "authentication method" is "Shared", the encryption type is "WEP" When "authentication method" is "WPA"/"WPA2"/"WPA-PSK"/"WPA2-PSK", the encryption types include "TKIP" and "AES"
WEP Encryption Type	When "encryption type" is "WEP", "WEP encryption type" is active and configurable. "WEP encryption" types include "WEP64" and "WEP128"
WEP Key	The length of WEP key varies depending on "WEP encryption type": When 64-bit key is selected, it's necessary to enter 10 hexadecimal number characters or 5 ASCII characters; when 128-bit key is selected, it's necessary to enter 26 hexadecimal number characters or 13 ASCII characters. User could set four keys, i.e. WEP key 1, WEP key 2, WEP key 3 and WEP key 4, and then select corresponding key based on key index
Current WEP Key Number	Namely the key index that corresponds to the key selection in wireless network
PSK Key Phrase	When authentication method is set to "WPA-PSK"/"WPA2-PSK", the "PSK key phrase" is active and configurable; user could configure PSK key here as needed
GTK Dynamic Refresh	When the authentication method is set to "WPA"/"WAP2"/"WPA-PSK"/"WPA2-PSK", GTK could be configured, and it's off by default
GTK Refresh Period	The default value is 24 hours
Radius Authentication Domain	This option appears when WPA/WPA2 or portal authentication is enabled, and is used to manually specify the domain for authentication; it's disabled by default. MAC non-sense authentication is enabled when portal authentication is selected and this option is used
Pre-association Authentication	This option appears only when WPA2 authentication is selected, and is enabled by default. Terminal roaming rate could be improved by enabling this function

Table 11 -1 Wireless Service Configuration Parameter Description

Note: GTK is used for encryption of multicast message at AP side, and decryption of AP multicast message at STA side. GTK is subjected to unified management at AC based on ESS; all STAs share the same GTK under ESS; when a user turns into non-authorized user from an authorized user, he/she could do malicious act on broadcast message and thereby bringing about potential safety hazard for 802.11 network since he/she has got GTK. To avoid such risk, we employ a timed GTK refresh mechanism, where GTK is refreshed at regular intervals to assure the key timeliness and improve network security.

11.4.2 AP Template Configuration

[Network configuration] > [WLAN configuration] > [AP template]; as shown in Fig. 11-11, [AP template] page is principally used to inquire about, add, edit, delete, apply and mandatorily apply AP template.



AP Template

Template name [ ] Search

☐	AP Template name	Radio			WLAN									
		Radio ID	802.11 Mode	Channel	SN	SSID	VLAN ID	Auth Type	Encrypt Type	SN	SSID	VLAN ID	Auth Type	Encrypt Type
☐	HNSY	1	802.11n HT20	Auto	1	[redacted]	1	Open	NONE					
		2	802.11n HT40	Auto										
☐	HNSYS	1	802.11n HT20	Auto	1	[redacted]	1	Open	NONE					
		2	802.11n HT20	6										

|< < 1 2 3 4 5 6 7 8 9 10 > >| 91-92 of 92| 10

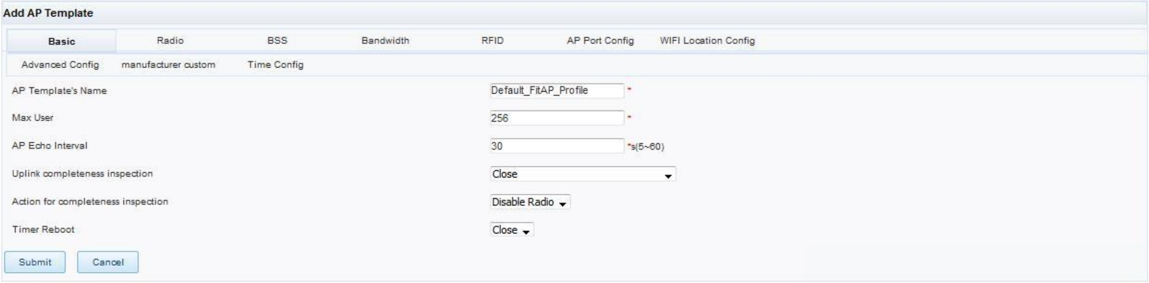
Create Edit Delete Apply [1] Force to Apply [2]

1. Apply: The configuration of only no customization AP could be covered by the template.
2. Force to Apply: The configuration of AP would be forced to coverd by the template.

Fig. 11-11 AP Template Page

1) Create AP Template

Click on <create> at bottom of the page as shown in Fig. 11-11 to open [add AP template] page; as shown in Fig. 11-12, [add AP template] page is composed of ten parts: Basic configuration, RF configuration, BSS configuration, bandwidth configuration, RFID configuration, AP port configuration, advanced configuration, manufacturer-defined configuration, and time settings.



Add AP Template

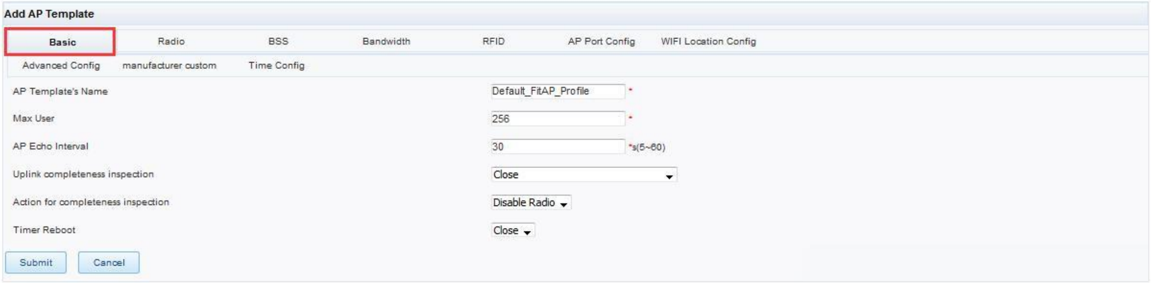
AP Template's Name: Default_FitAP_Profile *
Max User: 256 *
AP Echo Interval: 30 *s(5~60)
Uplink completeness inspection: Close
Action for completeness inspection: Disable Radio
Timer Reboot: Close

Submit Cancel

Fig. 11-12 AP Template Addition Page

- Basic Configuration

In [basic configuration] page, user could set [AP template name]/[max. number of access users]/[AP keep-alive time]/[uplink integrity inspection]/[uplink integrity inspection action]/[timed reboot] as shown in Fig. 11-13.



Add AP Template

AP Template's Name: Default_FitAP_Profile *
Max User: 256 *
AP Echo Interval: 30 *s(5~60)
Uplink completeness inspection: Close
Action for completeness inspection: Disable Radio
Timer Reboot: Close

Submit Cancel

Fig. 11-13 Basic Configuration Page

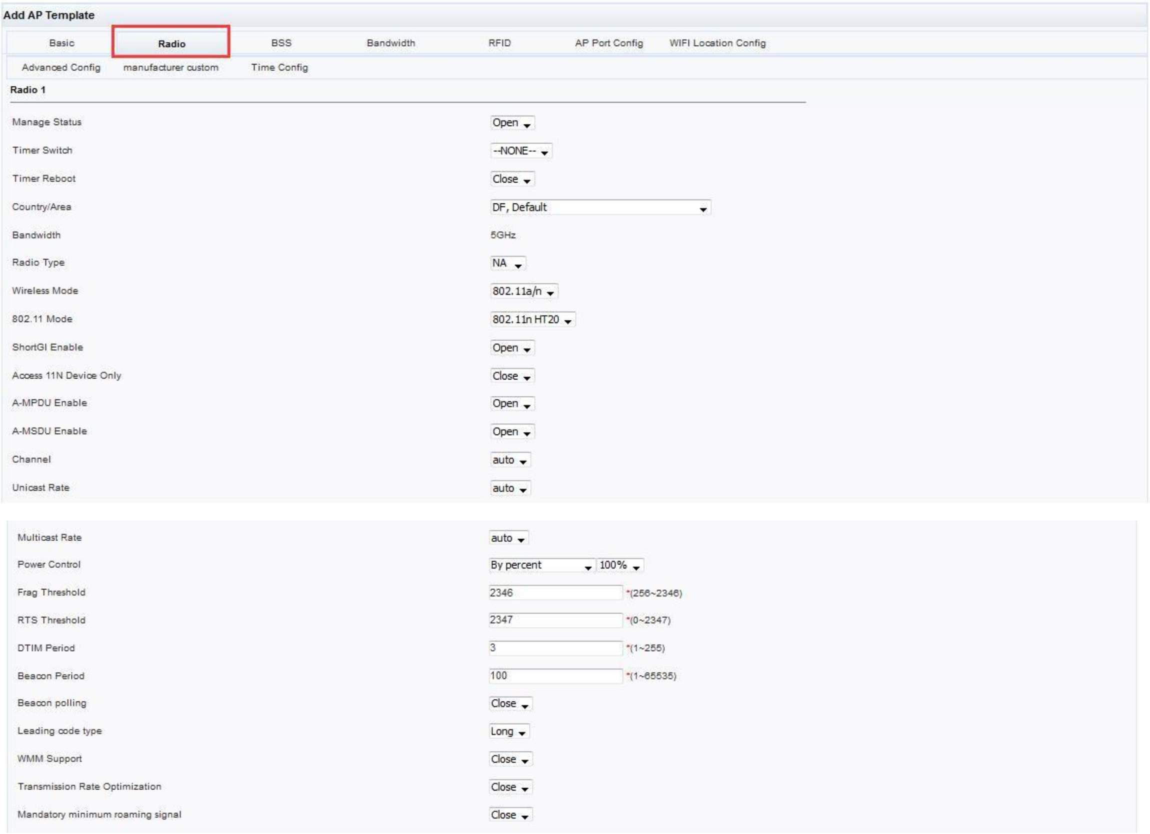
The basic configuration page configuration parameter description is as shown in Table 11-2 Basic configuration page Parameter description.

Configuration Item	**Description**
AP Template Name	Used to identify the name of added AP template
Max. Number of Access Users	The number of users accessible to the AP running this template (128 by default); "0" means the number of access users is not limited
AP Keep-alive Time	The heartbeat interaction interval between AP and C (30s by default)
Uplink Integrity Inspection	Turn on or off uplink integrity inspection (off by default)
Link Integrity Inspection Action	Turn off RF or restart AP when physical uplink is disconnected [Turn off RF or restart AP when the CAPWAP link between AC and AP is disconnected
Timed Reboot	The timed reboot of AP; see Section 12.4

Table 11 -2 Basic Configuration Page Parameter Description

• RF Configuration

The [RF configuration] page as shown in Fig. 11-14 offers the RF configuration for AP template. Wireless controller (AC) currently supports the configuration of RF card parameters for 2 radios.



Radio 1

Manage Status	Open
Timer Switch	--NONE--
Timer Reboot	Close
Country/Area	DF, Default
Bandwidth	5GHz
Radio Type	NA
Wireless Mode	802.11a/n
802.11 Mode	802.11n HT20
ShortGI Enable	Open
Access 11N Device Only	Close
A-MPDU Enable	Open
A-MSDU Enable	Open
Channel	auto
Unicast Rate	auto
Multicast Rate	auto
Power Control	By percent 100%
Frag Threshold	2346 *(256~2346)
RTS Threshold	2347 *(0~2347)
DTIM Period	3 *(1~255)
Beacon Period	100 *(1~65535)
Beacon polling	Close
Leading code type	Long
WMM Support	Close
Transmission Rate Optimization	Close
Mandatory minimum roaming signal	Close

Fig. 11-14 RF Configuration Page

Please refer to Table 11-3 for details of RF configuration page parameters.

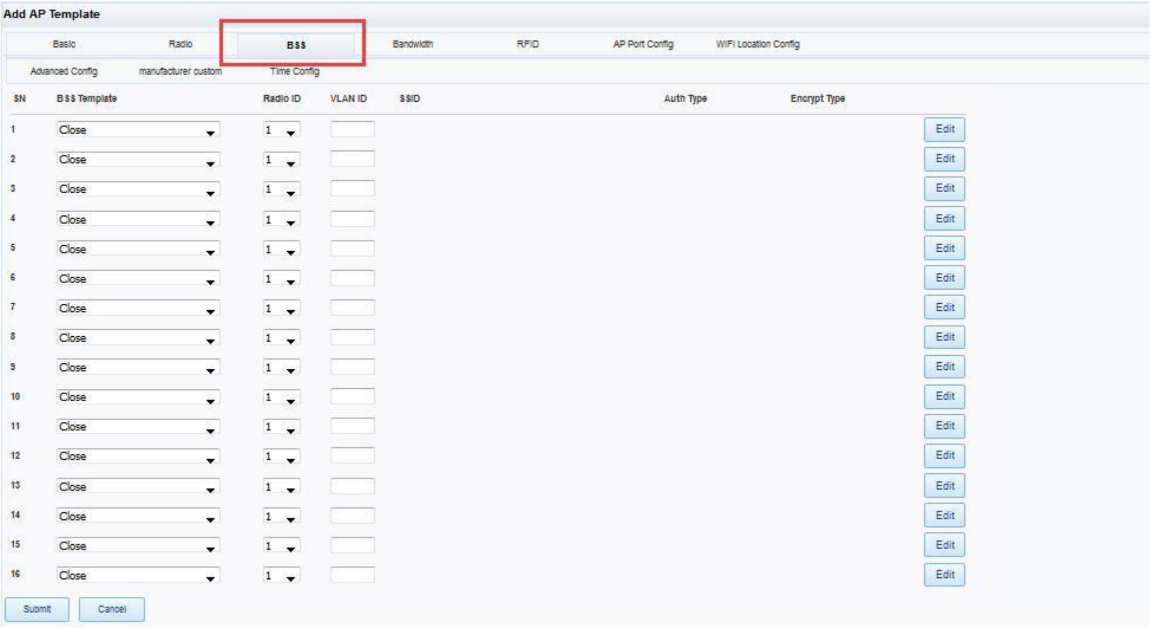
Configuration Item	Description
Management state	RF configuration enable switch (ON/OFF)
Timed on/off	Set up timed on/off of RF; see Section 12.3 for details
Time Period	The time period for timed on/off of RF; see Section 12.3 for details
Timed Reboot	Timed reboot of AP RF
Country/Region	Issue appropriate country code ("DF, default" by default); other options include "CN, China", "US, the United States", "GB, the UK", "FR, France", and "DE, Germany"
Frequency Band	[The two parameter values, i.e. 5.8GHz and 2.4GHz are in one-to-one correspondence to Radio type
Radio Type	The parameters available include "B", "G", "BG", "NBG", "A" and "AN"
Wireless Working Mode	Used to configure different network connection rates and working modes of fit AP
802.11n Working Mode	802.11n involves two bandwidth modes: HT (High Throughput) 20 and HT40; HT20 means "20M bandwidth". Working modes "802.11n HT20" and "802.11n HT40"
Determine Whether or Not to Enable ShortGI	[GI, Guard Interval. GI is between wireless data blocks, and is 800us in length, while the Short GI is 400us in length; Short GI helps to improve the rate by 10%
Only 11n Device Access Allowed	When this option is enabled, only 11n device is accessible; when this option is disabled, the type of access device is not limited
A-MPDU on/off	[A-MPDU technology helps to reduce frame transmission cost and improve system throughput
A-MSDU on/off	[A-MSDU technology helps to reduce message transmission cost, minimize response frames, and improve message transfer efficiency
Channel	Choose different channels based on the frequency band where AP functions
Unicast Rate	Set the message rate of AP unicast frame; default is recommended
Multicast Rate	Set the message rate of AP multicast frame; default is recommended
Power Regulation	[Used to configure the wireless signal emission power of AP. The output power is directly proportional to the coverage of device's wireless signal, the power consumption, and the interference with neighboring devices. The default output power is 20dbm, and the output power could be manually reduced or increased

Fragmentation Threshold	Used to configure the wireless packet division of AP; in case of large data packets at MAC layer, error and retransmission may frequently occur in an environment with interference, where the error rate and transmission quality could be improved by dividing big packets into small ones; its setup range is 256-2346, and it can only be set to an even number. Default value is recommended
RTS Threshold	Used to configure AP's wireless packet RTS (Request To Send) for resolving network conflict. Conflict may occur when two sites send data to AP simultaneously, and is likely to result in data loss. RTS threshold is used to solve this problem. When the data packet to be transmitted is beyond RTS threshold, the RTS mechanism is activated, when the site sends an RTS to AP so as to inform AP of data transmission. Upon receipt of the application, AP sends CTS to other sites and requires them to put off the transmission. In the meantime, AP notifies the RTS site to transmit data. This threshold could be set within 0-2346, and the default value is recommended
DTIM Interval	This value means delivery traffic indication message interval. DTIM is a backward counter used to notify client of next window that listens to broadcast and multicast information. When wireless AP buffers the broadcast or multicast information sent to client, it sends next DTIM and DTIM interval to arouse the client for receiving the information. The effective value range is 1-255. Default value is recommended
Beacon Interval	Beacon means the message sent by wireless AP periodically for synchronous connection with the wireless terminal on the wireless AP. The effective range of beacon is 1-65535, and the default value is recommended
Beacon Polling	Enable/disable the beacon level polling in multi-BSS mode
Preamble Type	Preamble is the first domain (followed by frame head and data volume domain) of communication protocol data unit (PPDU), and is principally used to determine the time point when data message is transmitted and received between wireless terminal and wireless AP, i.e. synchronization. Moreover, the preamble notifies other wireless terminals to avoid conflict. 802.11G standard supports "long" (128 bits) and "short" (56 bits) preambles. 802.11B only supports "short" (56 bits) preamble. Short preamble helps to improve the overall utilization of wireless channel, and achieve high prioritized transfer bandwidth. However, long preamble is recommended for environments with dense interference. This configuration item offers two options, i.e. "long" and "short"
WMM Support	A wireless QoS protocol used to ensure high priority messages could be transmitted preferentially, thereby assuring the better quality of voice and video applications in wireless network
Transmission Rate Optimization	Enable/disable transmission rate optimization mode; fragmentation function (the critical value is 2346) must be disabled when this mode is enabled

Table 11-3 RF Configuration Page Parameter Description

• BSS Configuration

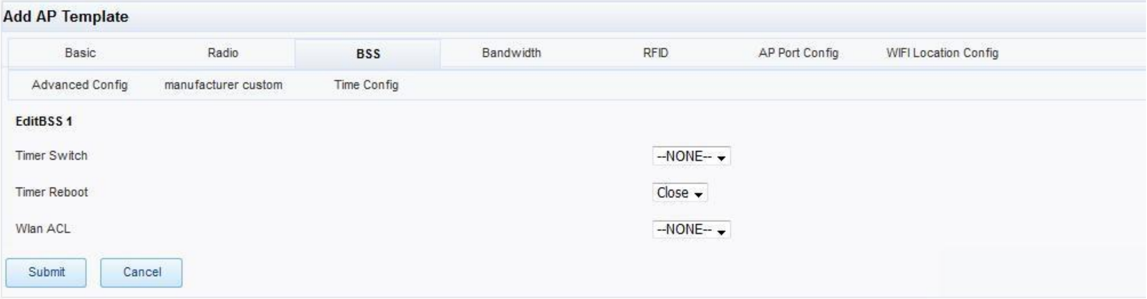
[BSS configuration] enables fit AP template to select wireless service template; user could select corresponding wireless service template in drop-down list of [BSS template], select [Radio ID], and click on <application> at page bottom to finish BSS configuration and the addition of entire fit AP template; user could manually modify VID without using wireless service as shown in Fig. 11-15. One AP template could associate and configure up to 16 BSS templates; <edit> button could be used to configure the bandwidth limitation of each BSS as shown in Fig. 11-16.



Add AP Template

SN	BSS Template	Radio ID	VLAN ID	SSID	Auth Type	Encrypt Type	
1	Close	1					Edit
2	Close	1					Edit
3	Close	1					Edit
4	Close	1					Edit
5	Close	1					Edit
6	Close	1					Edit
7	Close	1					Edit
8	Close	1					Edit
9	Close	1					Edit
10	Close	1					Edit
11	Close	1					Edit
12	Close	1					Edit
13	Close	1					Edit
14	Close	1					Edit
15	Close	1					Edit
16	Close	1					Edit

Fig. 11-15 BSS Configuration Page



Add AP Template

EditBSS 1

Timer Switch: --NONE--

Timer Reboot: Close

Wlan ACL: --NONE--

Fig. 11-16 BSS Edition Information

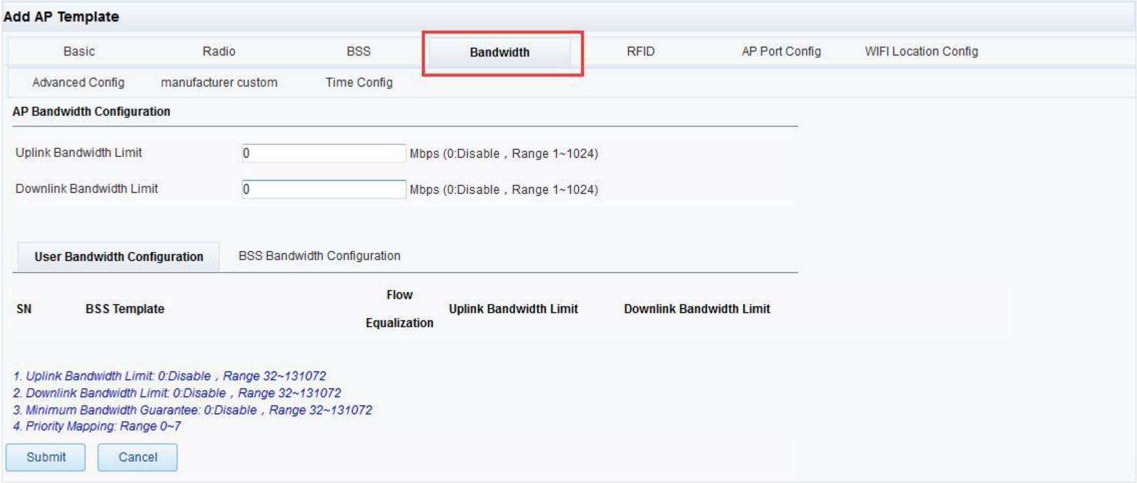
Configuration Item	Description
Timed Switch	Timed on/off of individual BSS'
Timed Reboot	Timed reboot of individual BSS'
Wireless Access Control	Set wireless access control for individual BSS'

Table 11-4 BSS Edition Page Parameter Description

Note: [In the case of AP with single frequency card, Radio 1 in [RF configuration] page is enabled, while Radio 2 is disabled.
The radio type of RF configuration must match with the RF card of actual AP, or AP template can't match with the type of AP RF card, which may result in AP template issue failure.

• Bandwidth Configuration

[Bandwidth configuration includes "AP total bandwidth configuration", "user bandwidth configuration" and "BSS bandwidth configuration" as shown in Fig. 11-17.



AP Bandwidth Configuration

Uplink Bandwidth Limit: 0 Mbps (0:Disable，Range 1~1024)

Downlink Bandwidth Limit: 0 Mbps (0:Disable，Range 1~1024)

User Bandwidth Configuration | BSS Bandwidth Configuration

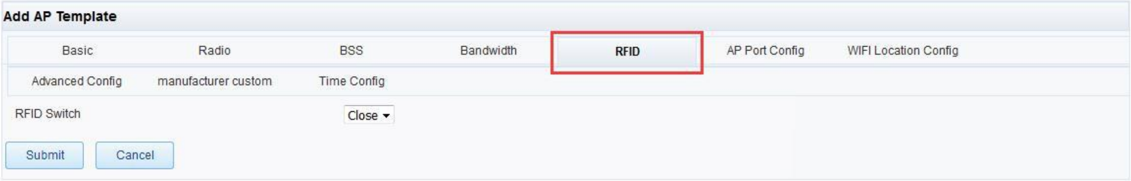
SN	BSS Template	Flow Equalization	Uplink Bandwidth Limit	Downlink Bandwidth Limit

1. Uplink Bandwidth Limit: 0:Disable，Range 32~131072
2. Downlink Bandwidth Limit: 0:Disable，Range 32~131072
3. Minimum Bandwidth Guarantee: 0:Disable，Range 32~131072
4. Priority Mapping: Range 0~7

Fig. 11-17 Bandwidth Configuration

• RFID Configuration

RF identification, i.e. RFID (Radio Frequency IDentification), also known as electronic tag or wireless RF identification, is a communication technology that identifies certain targets and reads/writes related data through radio signal, thereby making it not necessary to establish mechanical or optical contact between identification system and certain targets. RFID card reader works with AP hardware to indirectly realize the configuration management of RFID card reader by AC through the configuration management of AP by AC. RFID configuration page is as shown in Fig. 11-18.



RFID Switch: Close

Fig. 11-18 RFID Configuration Page

The RFID configuration parameter description is as shown in Table 11-5.

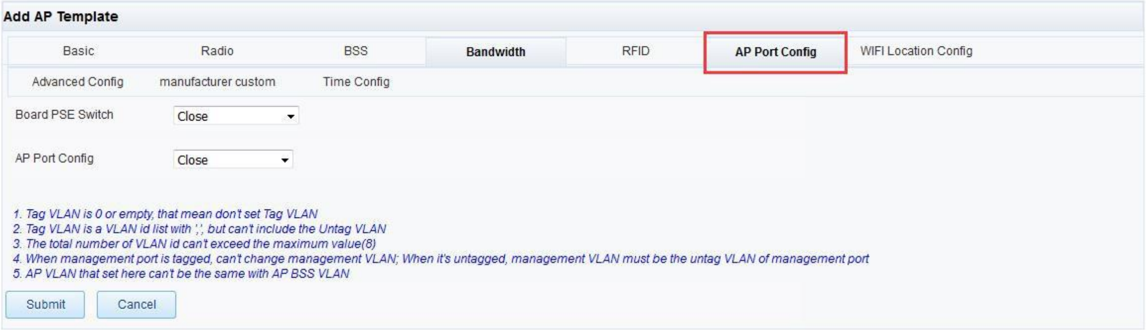
Configuration Item	**Description**
RFID Switch	Enable/disable RFID function (disabled by default)
Center Frequency	Center frequency of tag card
RFID Server	Server address of RFID
Server Port	The RFID server port for receiving information
Proxy Port	The source port for RFID card reader to send message

Table 11-5 RFID Configuration Parameter Description

Note: Where the AP is not designed with RFID, it's not necessary to open RFID function during the configuration of AP template.

- AP Port Configuration

User could subject the physical port of AP to PVID configuration through AP port configuration as shown in Fig. 11-19.



Board PSE Switch: Close

AP Port Config: Close

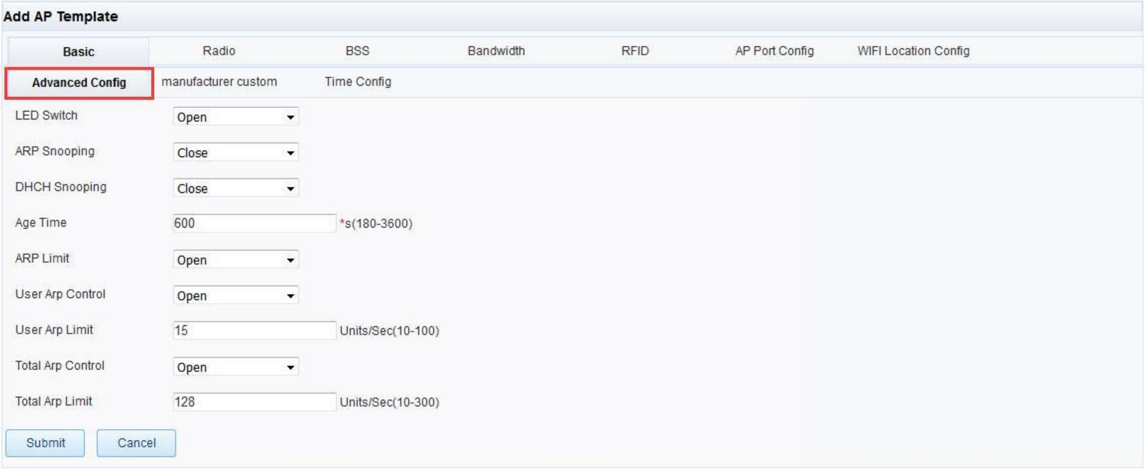
1. Tag VLAN is 0 or empty, that mean don't set Tag VLAN
2. Tag VLAN is a VLAN id list with ',', but can't include the Untag VLAN
3. The total number of VLAN id can't exceed the maximum value(8)
4. When management port is tagged, can't change management VLAN; When it's untagged, management VLAN must be the untag VLAN of management port
5. AP VLAN that set here can't be the same with AP BSS VLAN

Fig. 11-19 AP Port Configuration Page

- Advanced Configuration

Advanced configuration includes the configuration of "LED on/off", "ARP broadcast to unicast" and "DHCP broadcast to unicast".

The configuration is as shown in Fig. 11-20.



LED Switch: Open

ARP Snooping: Close

DHCH Snooping: Close

Age Time: 600 *s(180-3600)

ARP Limit: Open

User Arp Control: Open

User Arp Limit: 15 Units/Sec(10-100)

Total Arp Control: Open

Total Arp Limit: 128 Units/Sec(10-300)

Fig. 11-20 Advanced Configuration

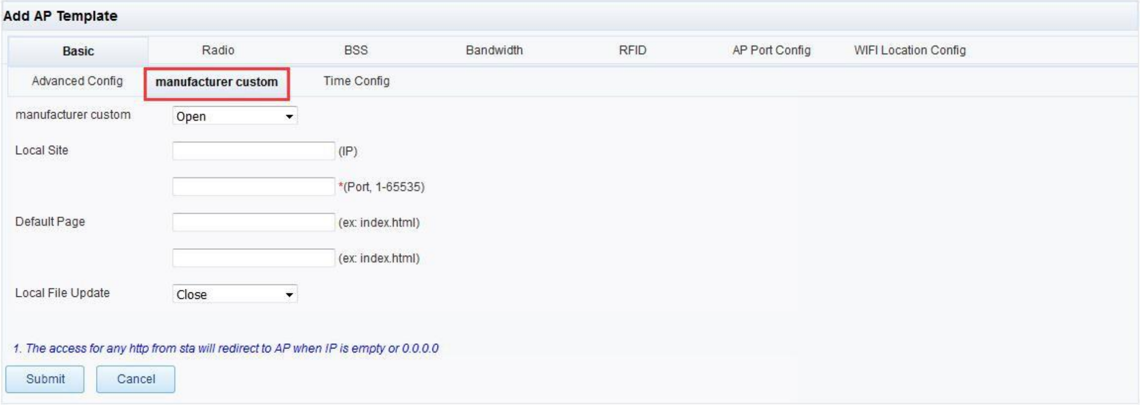
The advanced configuration parameter description is as shown in Table 11-6.

Configuration Item	**Description**
LED Switch	Control the on/off of AP's LED indicator lamp. When this option is enabled, AP's LED lamp is enabled; when the option is disabled, AP's LED lamp is disabled; the options is disabled by default
ARP Broadcast to Unicast	Convert the ARP broadcast message to be sent to STA into unicast message; disabled by default
DHCP Broadcast to Unicast	Convert the DHCP broadcast message to be sent to STA into unicast message; disabled by default
Aging Time	The timeout period of IP and MAC mapping relation learned by AP dynamically (600s by default)

Table 11-6 Advanced Configuration Parameter Description

- Manufacturer-defined Configuration

User is forced to visit local files; upon the association of STA with AP, the access to any external website is mandatorily redirected to AP's local designated webpage. The configuration is as shown in Fig. 11-21.



manufacturer custom: Open

Local Site: (IP)

*(Port, 1-65535)

Default Page: (ex: index.html)

(ex: index.html)

Local File Update: Close

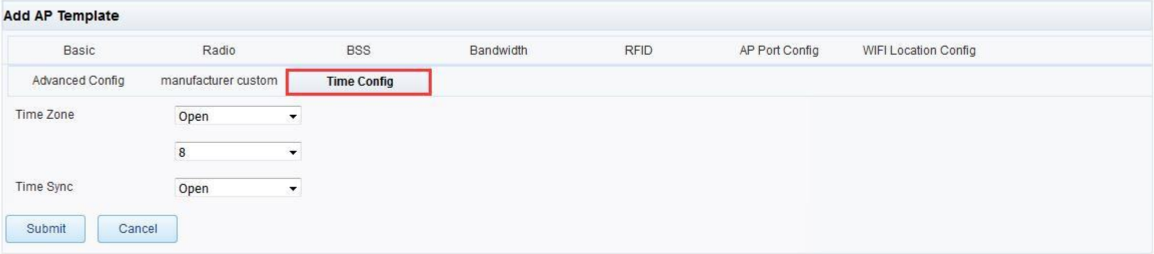
1. The access for any http from sta will redirect to AP when IP is empty or 0.0.0.0

Fig. 11-21 Manufacturer-defined Configuration

Note: The manufacturer-defined configuration is only supported by LTEFi device, and is not recommended for other types of APs.

- Time Settings

Set AP time zone, and issue the set time zone and the current time of AC to AP. The configuration is as shown in Fig. 11-22.



Time Zone: Open

8

Time Sync: Open

Fig. 11-22 Time Settings

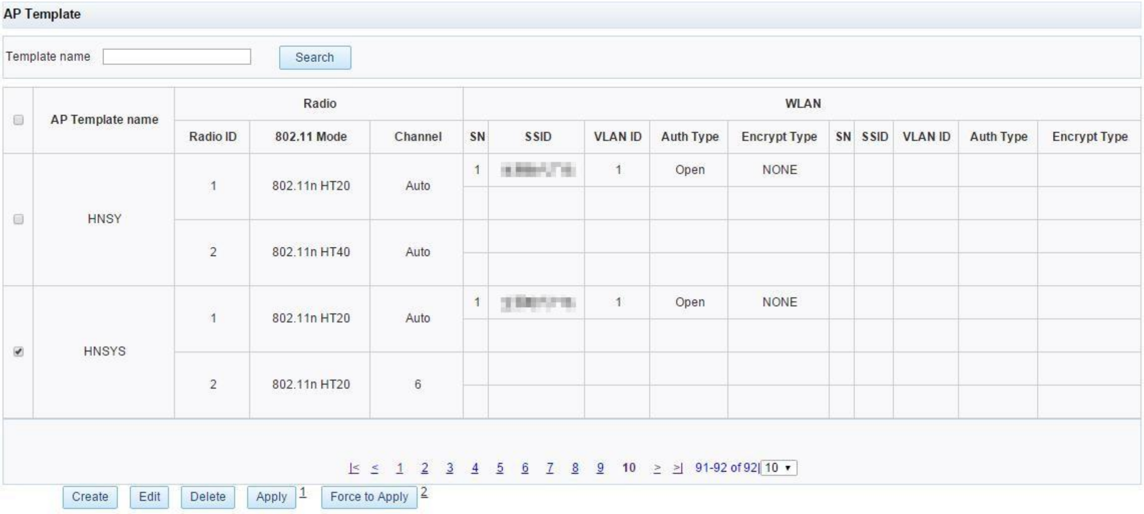
The time settings parameter description is as shown in Table 11-7.

Configuration Item	**Description**
Time Zone Settings	The time zone setup switch used to set up AP time zone (-12~12)
Time Synchronization	AP-AC time synchronization on/off; when this option is enabled, AP is automatically synchronized with AC's current time

Table 11-7 Time Settings Parameter Description

2) Edit AP Template

Select the name of fit AP template to be edited in Fig. 11-23, click on the <edit> button at bottom of page to open the [configure AP template] page, where user could edit the parameters of AP template.



AP Template

☐	AP Template name	Radio			WLAN									
		Radio ID	802.11 Mode	Channel	SN	SSID	VLAN ID	Auth Type	Encrypt Type	SN	SSID	VLAN ID	Auth Type	Encrypt Type
☐	HNSY	1	802.11n HT20	Auto	1	[redacted]	1	Open	NONE					
		2	802.11n HT40	Auto										
☑	HNSYS	1	802.11n HT20	Auto	1	[redacted]	1	Open	NONE					
		2	802.11n HT20	6										

Fig. 11-23 Edit AP Template

3) Delete AP Template

Select the name of fit AP template to be deleted in Fig. 11-23, and click on the <delete> button at page bottom to delete corresponding template.

4) Apply AP Template

After the modification of AP template, the <application> or <mandatory application> button could be used to issue the modified data to the AP running this template.

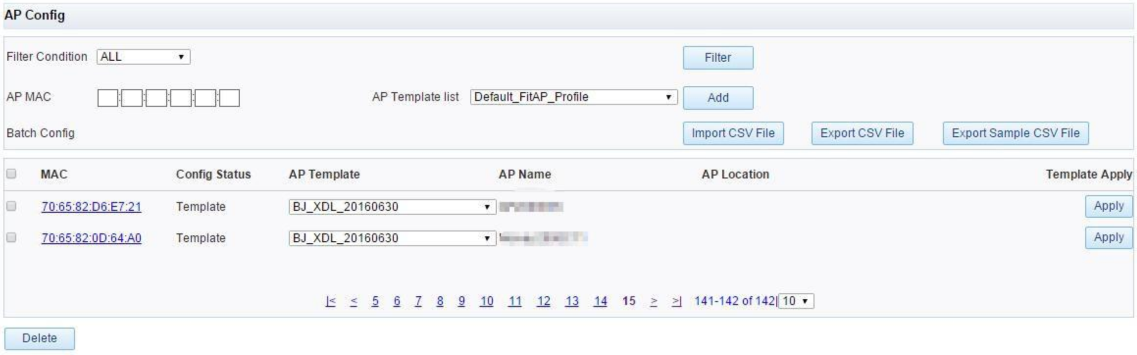
Note:

Application: Only cover the configuration of related non-customized AP.

Mandatory application: The mandatory application of template covers configuration of all related APs.

11.4.3 AP Configuration

[AP configuration] page records the information about binding of AP and template. When AP goes online, [AP configuration] is checked for AP-template correspondence information; if there is any, the template is automatically applied based on corresponding information without issuing template in [AP information] page. Upon the successful issue of matching template to the online AP in [AP information] page, the AP's MAC and the corresponding AP template binding information are automatically presented in [configuration page] page as shown in Fig. 11-24.



AP Config

Filter Condition: ALL

AP MAC: □:□:□:□:□:□

AP Template list: Default_FitAP_Profile

Batch Config

□	MAC	Config Status	AP Template	AP Name	AP Location	Template Apply
□	70:65:82:D6:E7:21	Template	BJ_XDL_20160630	[redacted]		Apply
□	70:65:82:0D:64:A0	Template	BJ_XDL_20160630	[redacted]		Apply

|< < 5 6 7 8 9 10 11 12 13 14 15 > >| 141-142 of 142| 10

Fig. 11-24 AP Configuration

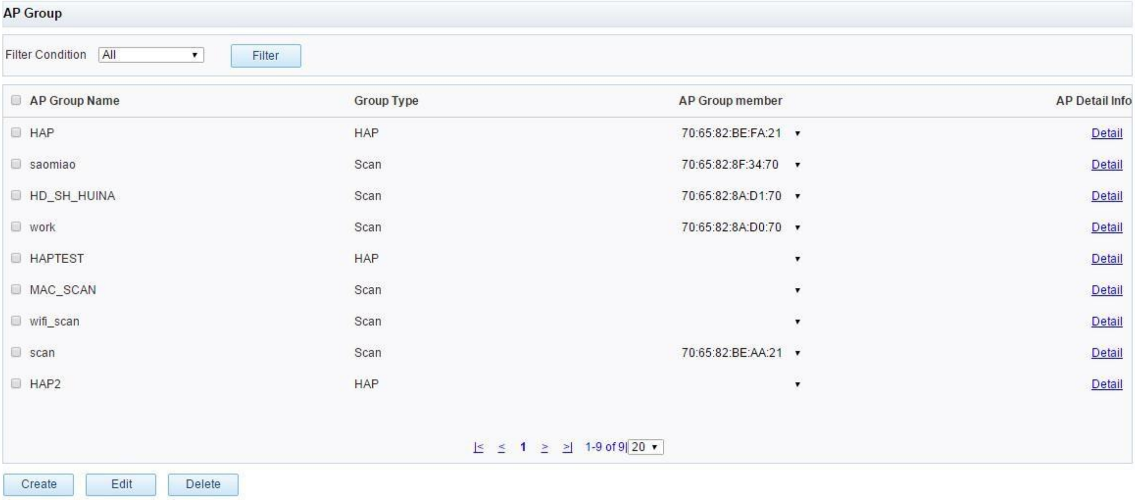
Configuration Item	Description
Filter Criteria	The template binding list could be filtered with [MAC address], [configuration state], [AP name], and [AP deployment location]
Add	Bind the AP with designated MAC to specified AP template
Import CSV File	Import the existing AP configuration list into wireless controller
Export CSV File	Export current AP configuration list in CSV file
Download Sample CSV	Download CSV file sample
Application	Apply single template binding
Delete	Delete the AP information of binding template

Table 11-8 AP Configuration Parameter Description

11.4.4 AP Group Configuration

AP group is principally used for AC to provide AP with configuration by group. AP groups include active-standby group, mirror image upgrade group, HAP group and scan group.

User could add/delete AP group, configure the purpose of AP group and add AP etc. as shown in Fig. 11-25. The normal configuration sequence of AP group: Create -> Configure purpose -> Add Ap.



AP Group

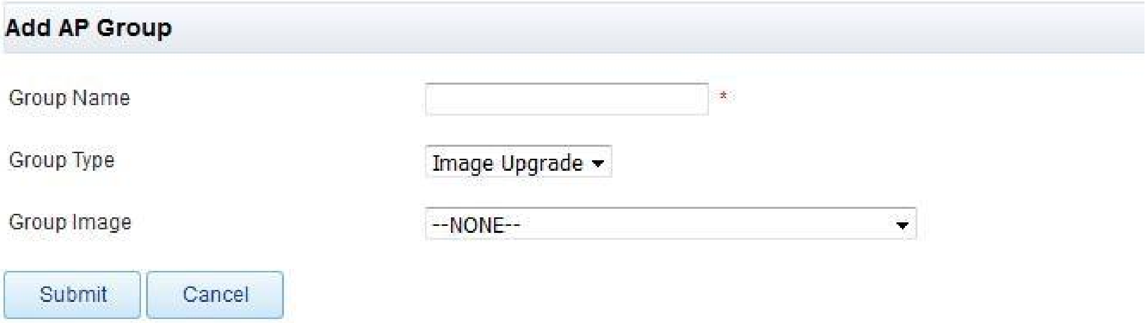
Filter Condition: All

□ AP Group Name	Group Type	AP Group member	AP Detail Info
□ HAP	HAP	70:65:82:BE:FA:21	Detail
□ saomiao	Scan	70:65:82:8F:34:70	Detail
□ HD_SH_HUINA	Scan	70:65:82:8A:D1:70	Detail
□ work	Scan	70:65:82:8A:D0:70	Detail
□ HAPTEST	HAP		Detail
□ MAC_SCAN	Scan		Detail
□ wifi_scan	Scan		Detail
□ scan	Scan	70:65:82:BE:AA:21	Detail
□ HAP2	HAP		Detail

Fig. 11-25 AP Group Configuration Page

- Create AP Mirror Image Upgrade Group

Click on <create> in the page as shown in Fig. 11-25 to open [add AP group] page, and select "mirror image upgrade" type in [type] drop-down list; as shown in Fig. 11-26, user could set the [group name] and [type], select [mirror image], and enable/disable [update on/off] in [add AP group] page.



Add AP Group

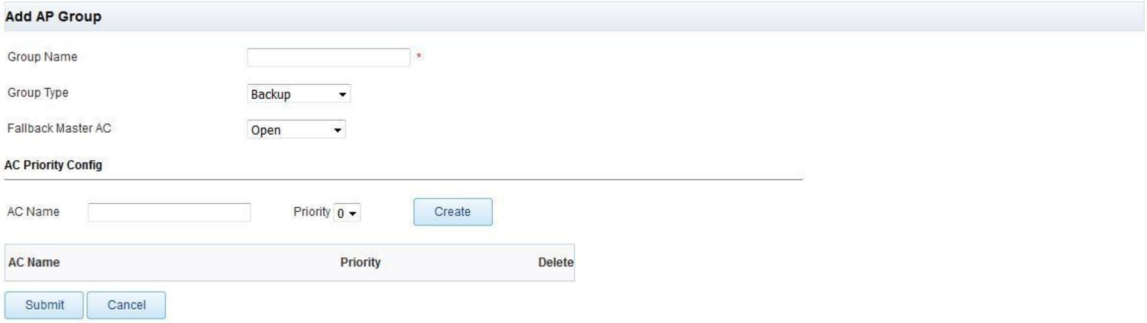
Group Name	*
Group Type	Image Upgrade
Group Image	--NONE--

Fig. 11-26 Add AP Mirror Image Upgrade Group

Note: "Mirror image" means to bind upgrade version file for this AP group; the mirror image name is automatically generated in [mirror image] drop-down box; user should configure FTP data in "[device management] > [AP upgrade] > [FTP server configuration]" page, and then obtain AP image file name through FTP in "[device management] > [AP upgrade] > [AP image management]" page or upload AP image to AC wireless controller through CAPWAP (CF card shall be inserted in the case of frame-type AC master control board). [Upgrade on/off] indicates whether AP automatic update is enabled by AP group. AP automatic update is subject to [update on/off] and the [automatic update] on/off in [AP image management]. The priority of [update on/off] in [AP group] is higher than that of [automatic update] on/off in [AP image management], which is to say, if the [update on/off] in [AP group] is configured as "enabled", the AP in [AP group] activates automatic update even if the [automatic update] feature in [AP image management] is set to "off". When AP is added to a certain AP group for mirror image upgrade, its automatic update feature in online stage is first dependent on the configuration of [mirror image] and [update on/off] in [AP group]; if this [AP group] is bound with image file while the [update on/off] is in "ON" state, the state of image bound with this [AP group] could be checked; if this image file's [automatic update] state is "ON" in [AP image management], this AP could be automatically updated when AP is online.

- Create AP Active-standby Group

Click on <create> in Fig. 11-25 to enter [add AP group] page, select "active-standby" in the drop-down list of [type] as shown in Fig. 11-27, and get into active-standby group edition page. AP active-standby group is principally used for AC to perform hot standby networking; the dual capwap hot standby features are described in detail in the sections below.


Add AP Group

Group Name *

Group Type: Backup

Fallback Master AC: Open

AC Priority Config

AC Name Priority: 0

Fig. 11-27 Add AP Active-standby Group

The parameter description is as shown in Table 11-9.

Configuration Item	Description
Group Name	The name of AP backup set must be consistent with the group name created in active-standby AC
Type	When AC employs dual CAPWAP link backup, the type of all AP groups created in active-standby AC is "backup"
Restore Main AC	Decide whether or not to restore the parameters of main AC when main AC returns to normal
AC Name	Consistent AC name in "[device management] > [basic configuration]" page
Priority	Make AP distinguish main AC from standby AC based on priority; if [AC priority configuration] is not configured, the priority is considered to be 0. The priority is divided into 8 levels (0-7); the bigger the number, the higher the priority; hence, the priority of [AC priority configuration] in main AC is higher than the priority configured in standby AC in the case of active-standby AC

Table 11-9 Parameter Description for the Creation of AP Backup Set

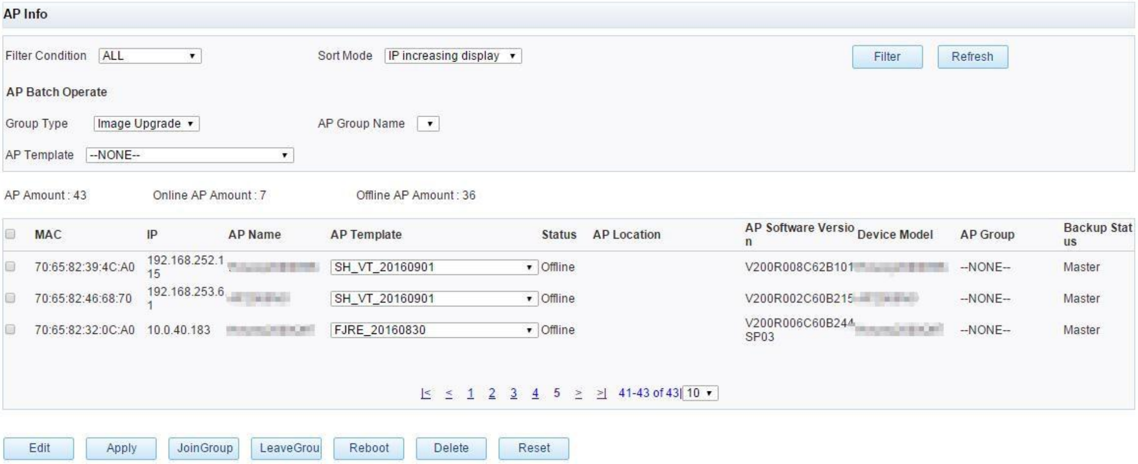
11.4.5 AP Information

As shown in Fig. 11-28, [AP configuration] page shows the information about all APs registered to AC classified by online/offline AP, IP address, AP name, deployment location, product type, MAC address and slot number, and offers AP filtration.

[AP configuration] enables addition to/quit from AP group.

In [AP configuration] page, user could <edit>, <apply template>, <restart> and <recover> online AP, and <delete> offline AP. <Edit> is used to modify AP's basic configuration, RF configuration, BSS configuration, access control and QoS configuration.

This chapter only offers operating instructions for the frequently used AP filter, template application, AP name and deployment location modification, AP restart and deletion, and AP recovery.



AP Info

Filter Condition: ALL ▾ Sort Mode: IP increasing display ▾

AP Batch Operate

Group Type: Image Upgrade ▾ AP Group Name: ▾

AP Template: --NONE-- ▾

AP Amount : 43 Online AP Amount : 7 Offline AP Amount : 36

□	MAC	IP	AP Name	AP Template	Status	AP Location	AP Software Version	Device Model	AP Group	Backup Status
□	70:65:82:39:4C:A0	192.168.252.115	[redacted]	SH_VT_20160901 ▾	Offline		V200R008C62B101	[redacted]	--NONE--	Master
□	70:65:82:46:68:70	192.168.253.61	[redacted]	SH_VT_20160901 ▾	Offline		V200R002C60B215	[redacted]	--NONE--	Master
□	70:65:82:32:0C:A0	10.0.40.183	[redacted]	FJRE_20160830 ▾	Offline		V200R006C60B244SP03	[redacted]	--NONE--	Master

Fig. 11-28 AP Configuration Page

1) AP Filter

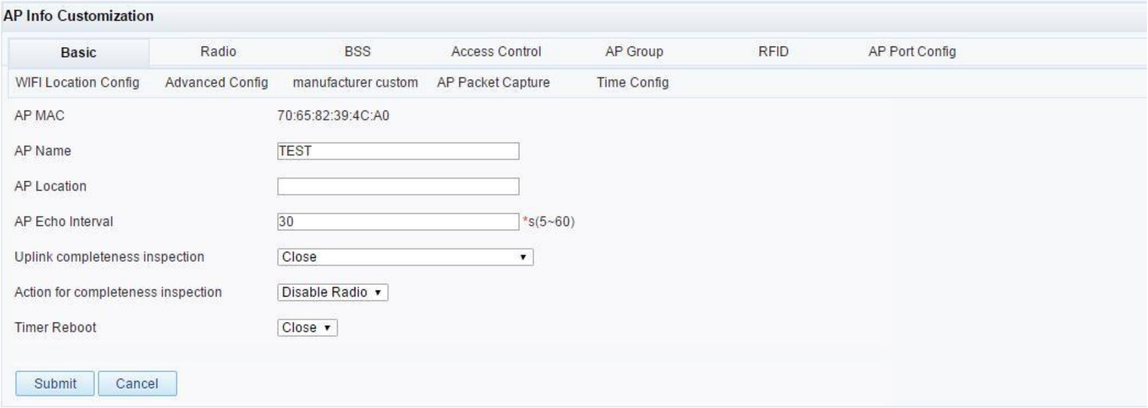
In "AP filter", user could find eligible APs based on different filter criteria, which include: All APs, online APs, offline APs, IP address, AP name, deployment location, device model, MAC address, AP group, and backup status.

2) Apply AP Template

Upon the successful registration of AP to AC, the AP configuration page automatically generates a record information about AP as shown in Fig. 11-28; if the AP is initially registered and not bound with [AP binding template] page, it's displayed as "unused" in [AP template] parameter of the [AP configuration] page, which is to say, the AC configures no data for the AP; in such a case, user could select desired [AP template] for AP based on existing AP template data, and click on <apply> button to issue centralized management configuration to the AP.

3) Modify AP Name and Deployment Location

By modifying AP name and AP deployment location through AP configuration edition, user could intuitively manage and identify AP devices in wireless controller interface so as to facilitate subsequent maintenance as shown in Fig.11-29.



AP Info Customization

AP MAC	70:65:82:39:4C:A0
AP Name	TEST
AP Location	
AP Echo Interval	30 *s(5~60)
Uplink completeness inspection	Close
Action for completeness inspection	Disable Radio
Timer Reboot	Close

Fig. 11-29 Modify AP Name and Deployment Location

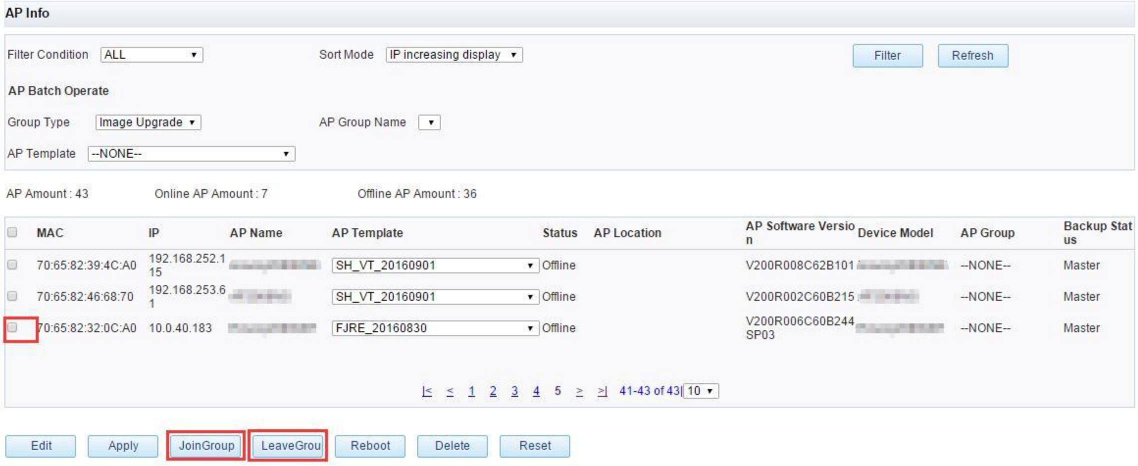
Please refer to Table 11-10 for page parameter description.

Configuration Item	**Description**
AP Name	Used to identify the name of added AP template
AP Deployment Location	Describe the deployment location of AP so that the administrator could identify the location of AP conveniently

Table 11-10 AP Name and Deployment Location Parameter Description

4) Join group/exit from group

User could add several online APs selected to group of "mirror image upgrade" or "active-standby" so as to realize batch mirror image upgrade of AP or online registration in active-standby AC. To exit from group, user could select the online AP and click on <exit from group> as shown in Fig. 11-30.



AP Info

Filter Condition: ALL   Sort Mode: IP increasing display

AP Batch Operate

Group Type: Image Upgrade   AP Group Name:

AP Template: --NONE--

AP Amount : 43   Online AP Amount : 7   Offline AP Amount : 36

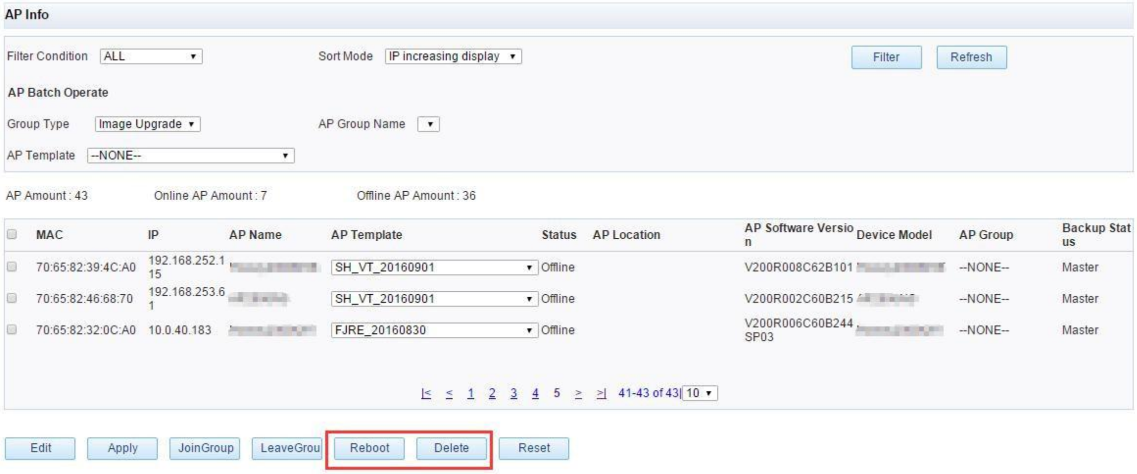
□	MAC	IP	AP Name	AP Template	Status	AP Location	AP Software Version	Device Model	AP Group	Backup Status
□	70:65:82:39:4C:A0	192.168.252.115	[redacted]	SH_VT_20160901	Offline		V200R008C62B101	[redacted]	--NONE--	Master
□	70:65:82:46:68:70	192.168.253.61	[redacted]	SH_VT_20160901	Offline		V200R002C60B215	[redacted]	--NONE--	Master
□	70:65:82:32:0C:A0	10.0.40.183	[redacted]	FJRE_20160830	Offline		V200R006C60B244SP03	[redacted]	--NONE--	Master

Fig. 11-30 "Join group/exit from group" Configuration Page

5) Restart and Delete AP

User could only <restart> online AP. Select the AP to be restarted in the [AP configuration] page, and click on <restart>, when the AC issues <restart> action command to the AP, and the AP would be restarted.

User could only <delete> offline AP. Select the offline AP to be deleted in the [AP configuration] page, and click on <delete> to delete the AP as shown in Fig. 11-31.



AP Info

Filter Condition ALL ▾ Sort Mode IP increasing display ▾ Filter Refresh

AP Batch Operate

Group Type Image Upgrade ▾ AP Group Name ▾

AP Template --NONE-- ▾

AP Amount : 43 Online AP Amount : 7 Offline AP Amount : 36

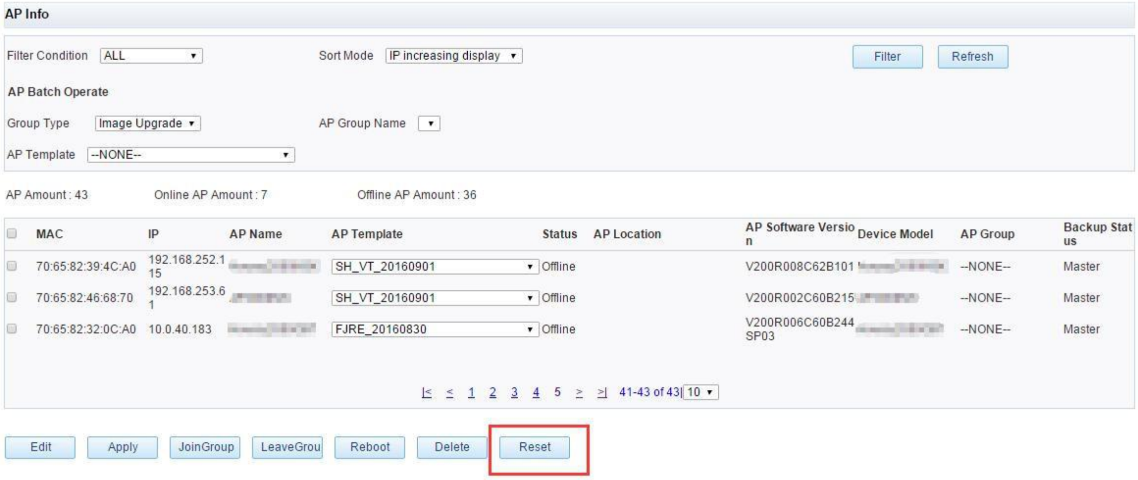
□	MAC	IP	AP Name	AP Template	Status	AP Location	AP Software Version	Device Model	AP Group	Backup Status
□	70:65:82:39:4C:A0	192.168.252.115	[redacted]	SH_VT_20160901 ▾	Offline		V200R008C62B101	[redacted]	--NONE--	Master
□	70:65:82:46:68:70	192.168.253.61	[redacted]	SH_VT_20160901 ▾	Offline		V200R002C60B215	[redacted]	--NONE--	Master
□	70:65:82:32:0C:A0	10.0.40.183	[redacted]	FJRE_20160830 ▾	Offline		V200R006C60B244SP03	[redacted]	--NONE--	Master

|< < 1 2 3 4 5 > >| 41-43 of 43 10 ▾

Fig. 11-31 Restart and Delete AP

6) AP Reset to Factory Default

Select the online AP and click on <restore factory default> to restore its factory default as shown in Fig. 11-32.



AP Info

Filter Condition ALL ▾ Sort Mode IP increasing display ▾ Filter Refresh

AP Batch Operate

Group Type Image Upgrade ▾ AP Group Name ▾

AP Template --NONE-- ▾

AP Amount : 43 Online AP Amount : 7 Offline AP Amount : 36

□	MAC	IP	AP Name	AP Template	Status	AP Location	AP Software Version	Device Model	AP Group	Backup Status
□	70:65:82:39:4C:A0	192.168.252.115	[redacted]	SH_VT_20160901 ▾	Offline		V200R008C62B101	[redacted]	--NONE--	Master
□	70:65:82:46:68:70	192.168.253.61	[redacted]	SH_VT_20160901 ▾	Offline		V200R002C60B215	[redacted]	--NONE--	Master
□	70:65:82:32:0C:A0	10.0.40.183	[redacted]	FJRE_20160830 ▾	Offline		V200R006C60B244SP03	[redacted]	--NONE--	Master

|< < 1 2 3 4 5 > >| 41-43 of 43 10 ▾

Fig. 11-32 AP Reset to Factory Default

Chapter 12 Timed Shutdown of AP RF

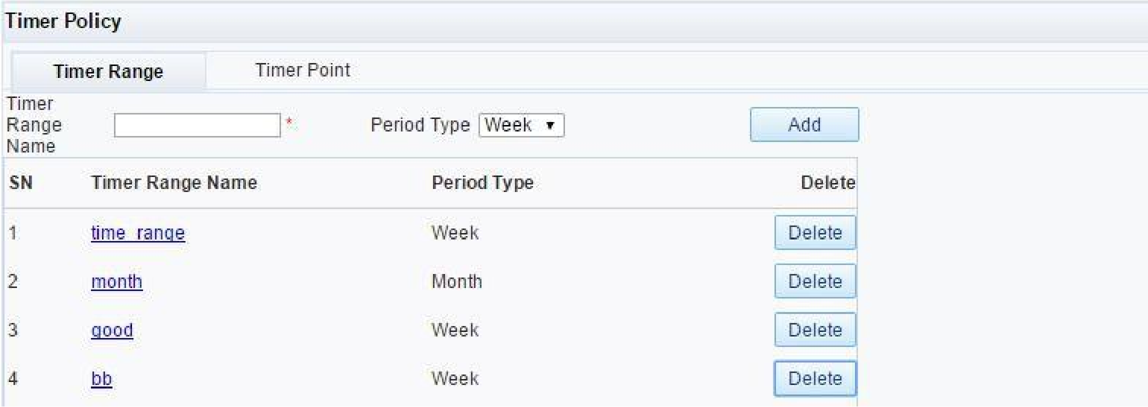
12.1 Description of Timed Shutdown of AP RF

In the case of traditional AP AC networking, AP could continuously offer wireless access service if it's configured with "wireless service" by AC; AP will not stop providing wireless service unless manual intervention (e.g. AC manually issues AP RF shutdown or bssid shutdown) is conducted. The timed shutdown of AP RF is based on the configured time period; AP RF or bssid is turned off or on at specified time point within designated time period.

12.2 Time Rule

Time rule is divided into time period rule and time point rule; time period rule is used for regular shutdown and activation of RF function; time point rule is principally used for regular restart of AP etc.

[Time period] rule setup; time period rule could be set up with week and month as shown in Fig. 12-1.



Period Type: Week

SN	Timer Range Name	Period Type	Delete
1	time_range	Week	Delete
2	month	Month	Delete
3	good	Week	Delete
4	bb	Week	Delete

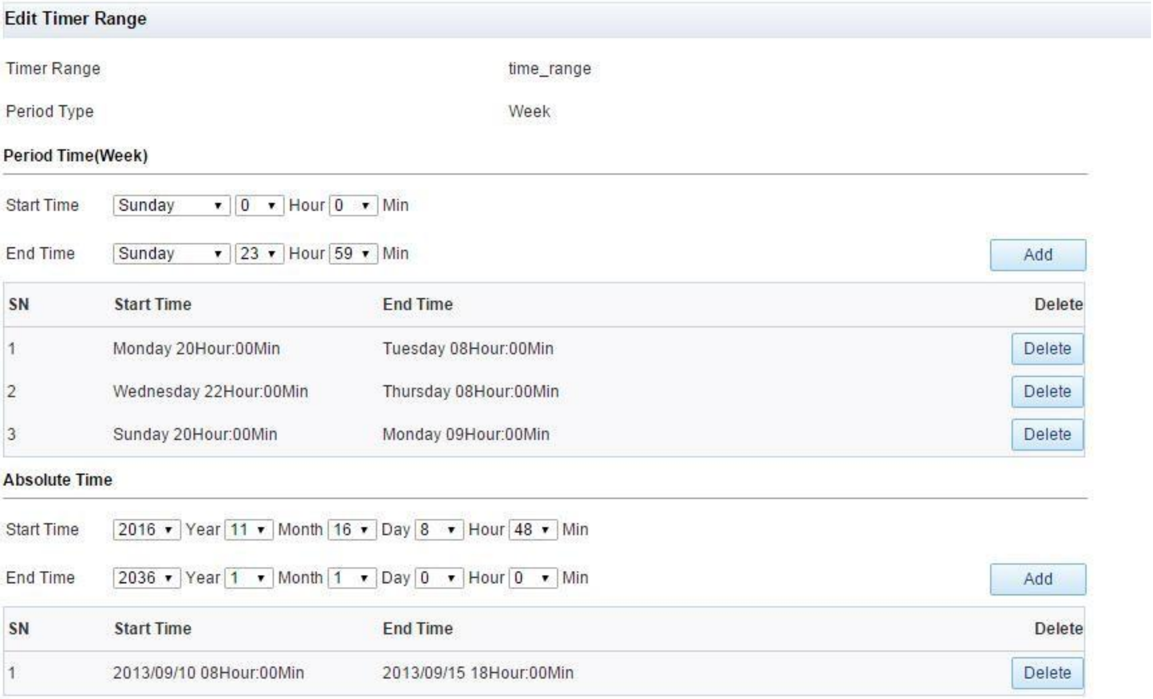
Fig. 12-1 Time Period Setup

The time period setup parameter description is as shown in Table 12-1.

Configuration Item	**Description**
Time Period Name	Time period name must be unique
Period Type	Time period types include [week] and [month]
Time Period name - Period Type [week]	Click on time period name link to open time period setup page
Time Period Name - Period Type !	Click on time period name link to open time period setup page
Delete	Delete time period rule

Table 12-1 Time Period Setup Parameter Description

The time period (week) setup information is as shown in Fig. 12-2.



Edit Timer Range

Timer Range	time_range
Period Type	Week

Period Time(Week)

Start Time: Sunday, 0 Hour, 0 Min

End Time: Sunday, 23 Hour, 59 Min

SN	Start Time	End Time	Delete
1	Monday 20Hour:00Min	Tuesday 08Hour:00Min	Delete
2	Wednesday 22Hour:00Min	Thursday 08Hour:00Min	Delete
3	Sunday 20Hour:00Min	Monday 09Hour:00Min	Delete

Absolute Time

Start Time: 2016 Year, 11 Month, 16 Day, 8 Hour, 48 Min

End Time: 2036 Year, 1 Month, 1 Day, 0 Hour, 0 Min

SN	Start Time	End Time	Delete
1	2013/09/10 08Hour:00Min	2013/09/15 18Hour:00Min	Delete

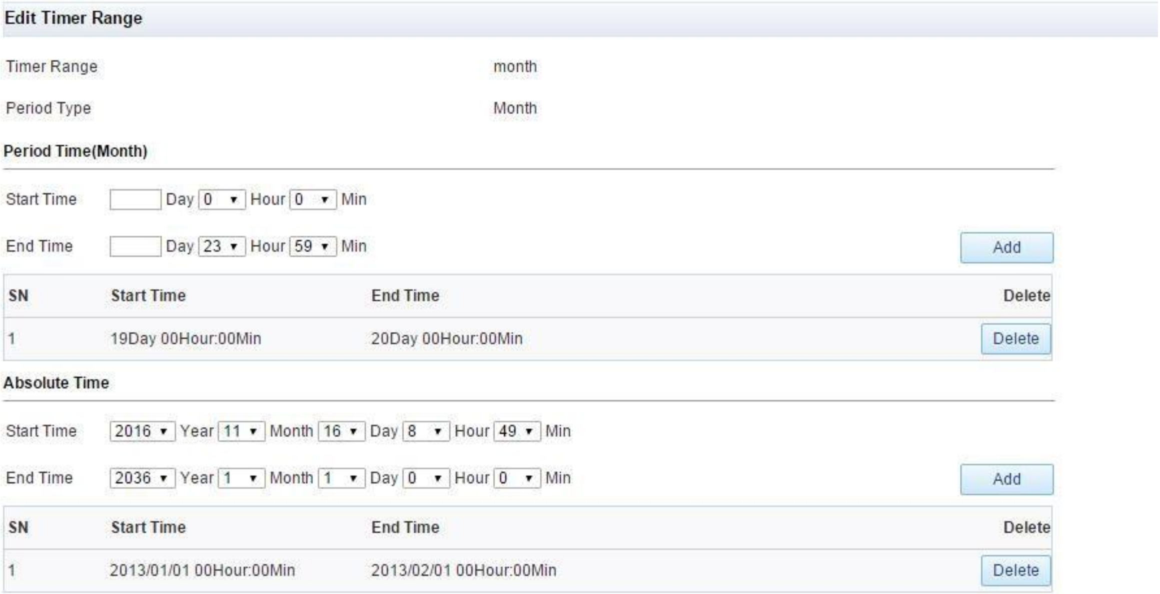
Fig. 12- 2 Time Period (week) Setup Information

The time period (week) setup parameter description is as shown in Table 12-2.

Configuration Item	Description
Add Period Time	Add the range of period time. Support "day cross"
Add Absolute Time	Add the absolute time of week rule
Delete	Delete period time rule or absolute time

Table 12- 2 Time Period (week) Parameter Specification

The time period (month) setup is as shown in Fig. 12-3.



Edit Timer Range

Timer Range	month
Period Type	Month

Period Time(Month)

Start Time [ ] Day 0 Hour 0 Min

End Time [ ] Day 23 Hour 59 Min

SN	Start Time	End Time	Delete
1	19Day 00Hour:00Min	20Day 00Hour:00Min	Delete

Absolute Time

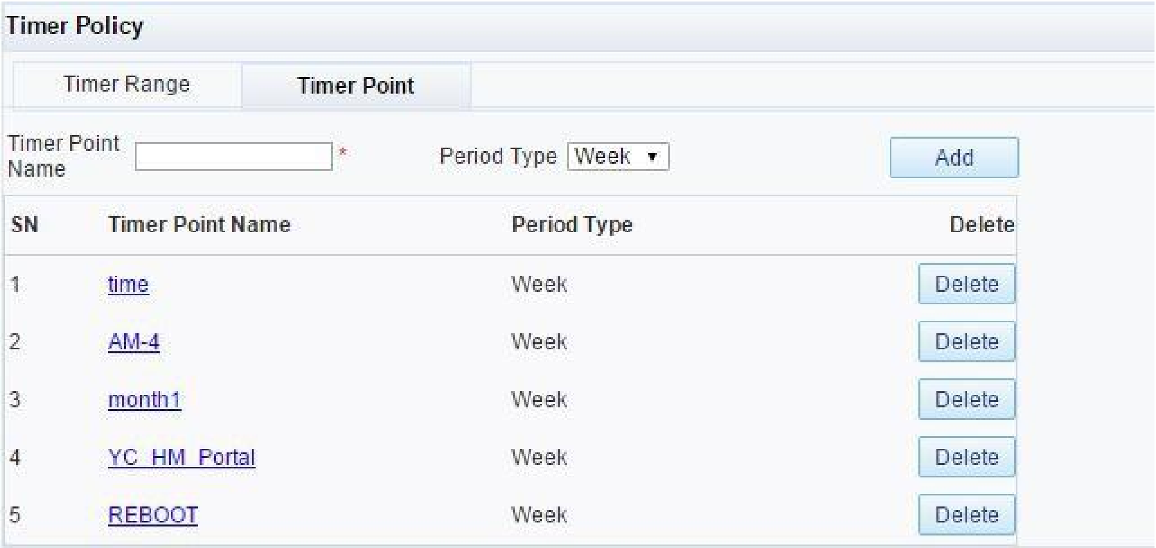
Start Time 2016 Year 11 Month 16 Day 8 Hour 49 Min

End Time 2036 Year 1 Month 1 Day 0 Hour 0 Min

SN	Start Time	End Time	Delete
1	2013/01/01 00Hour:00Min	2013/02/01 00Hour:00Min	Delete

Fig. 12-3 [Month] Period Type Time Period Setup

[Time point] rule setup; time point rule could be set up by [week] or [month] as shown in Fig. 12-4.



Timer Policy

Timer Point Name [ ] * Period Type Week

SN	Timer Point Name	Period Type	Delete
1	time	Week	Delete
2	AM-4	Week	Delete
3	month1	Week	Delete
4	YC_HM_Portal	Week	Delete
5	REBOOT	Week	Delete

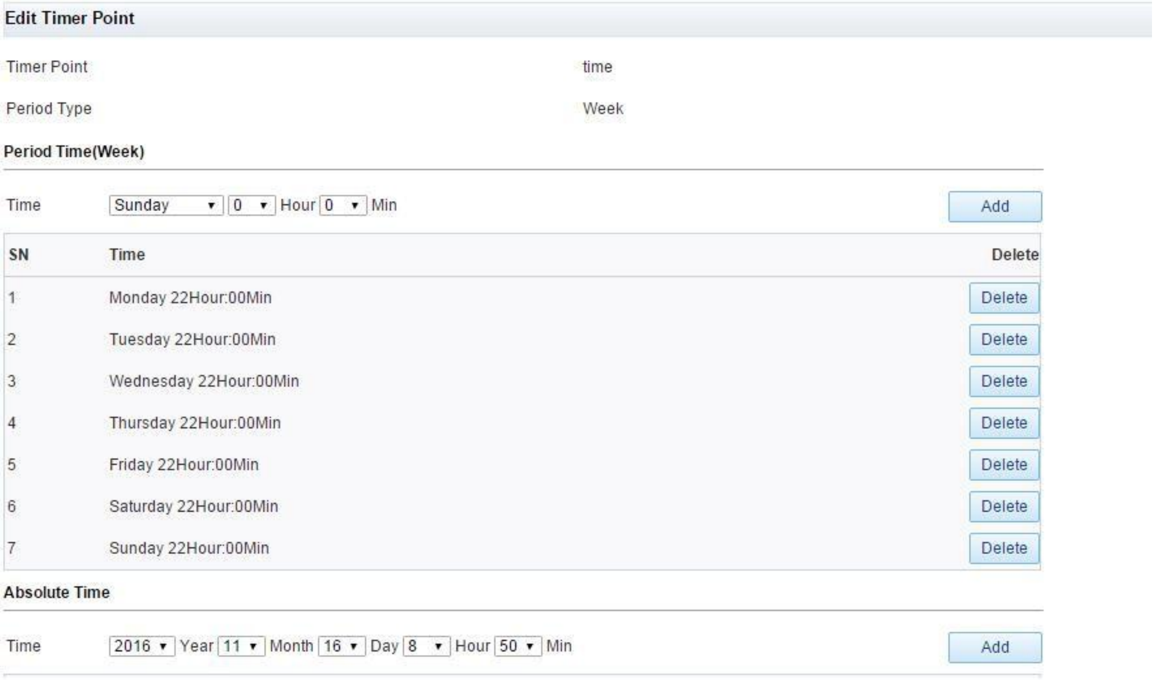
Fig. 12- 4 Time Point Rule Setup

Time point rule parameter description is as shown in Table 12-3.

Configuration Item	Description
Time Point Name	Time point name must be unique
Period Type	Time point types include [week] and [month]
Time Point Name - Period Type [week]	Click on time point name link to open time point setup page
Time Point Name - Period Type !	Click on time point name link to open time point setup page
Delete	Delete time period rule

Table 12- 3 Time Point Rule Parameter Description

The time point [week] setup is as shown in Fig. 12-5.



Edit Timer Point

Timer Point: time

Period Type: Week

Period Time(Week)

Time: Sunday ▾ 0 ▾ Hour 0 ▾ Min

SN	Time	Delete
1	Monday 22Hour:00Min	Delete
2	Tuesday 22Hour:00Min	Delete
3	Wednesday 22Hour:00Min	Delete
4	Thursday 22Hour:00Min	Delete
5	Friday 22Hour:00Min	Delete
6	Saturday 22Hour:00Min	Delete
7	Sunday 22Hour:00Min	Delete

Absolute Time

Time: 2016 ▾ Year 11 ▾ Month 16 ▾ Day 8 ▾ Hour 50 ▾ Min

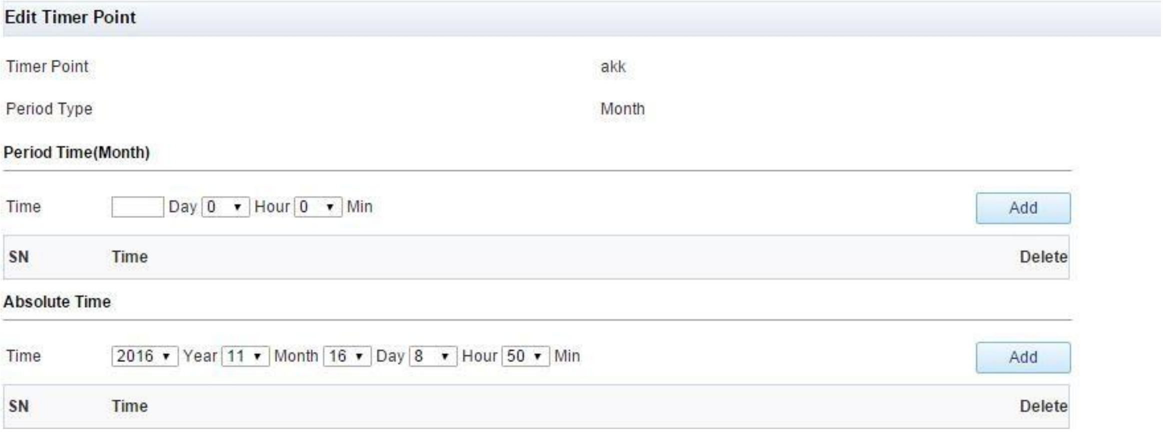
Fig. 12-5 Time Point Setup with Period Type [week]

The time point setup parameter description is as shown in Table 12-4.

Configuration Item	Description
Add	Add period time point or absolute time point
Delete	Delete period time point or absolute time point

Table 12-4 Time Point Setup Parameter Description

The time point setup is as shown in Fig. 12-6.



Edit Timer Point

Timer Point: akk

Period Type: Month

Period Time(Month)

Time [ ] Day [0 ▾] Hour [0 ▾] Min

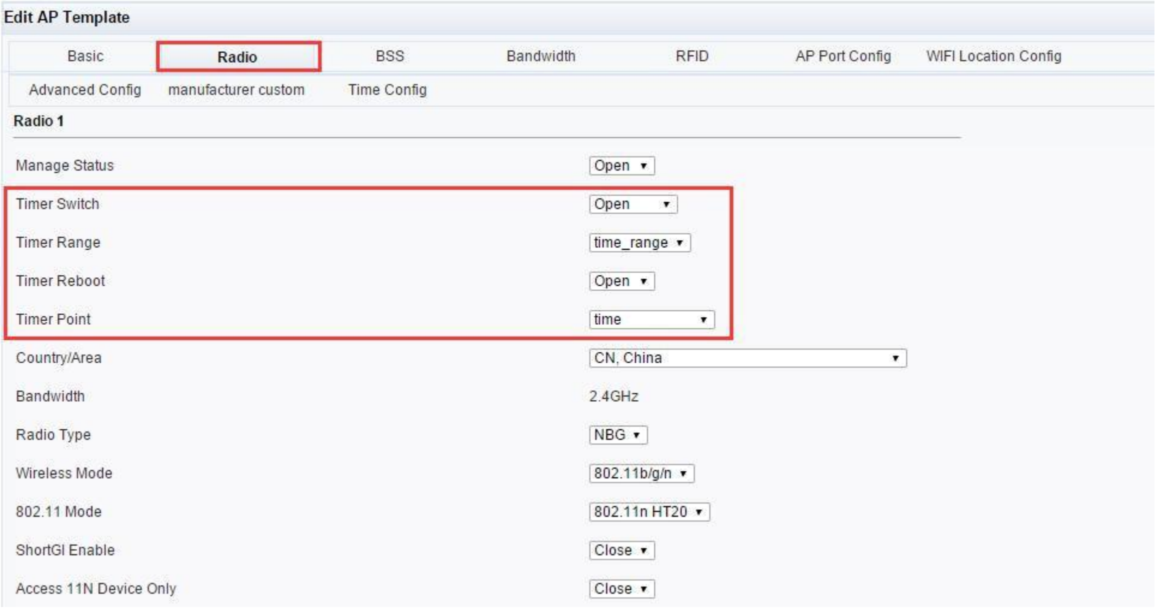
Absolute Time

Time [2016 ▾] Year [11 ▾] Month [16 ▾] Day [8 ▾] Hour [50 ▾] Min

Fig. 12-6 Time Point Setup with Period Type

12.3 Time Rule Bound with RF Configuration

Bind the set time rule with AP template RF configuration to enable the timed on/off or restart of single or dual RF as shown in Fig. 12-7.



Edit AP Template

Radio 1

Manage Status: Open ▾

Timer Switch: Open ▾

Timer Range: time_range ▾

Timer Reboot: Open ▾

Timer Point: time ▾

Country/Area: CN, China ▾

Bandwidth: 2.4GHz

Radio Type: NBG ▾

Wireless Mode: 802.11b/g/n ▾

802.11 Mode: 802.11n HT20 ▾

ShortGI Enable: Close ▾

Access 11N Device Only: Close ▾

Fig. 12- 7 Time Rule Bound with RF Configuration

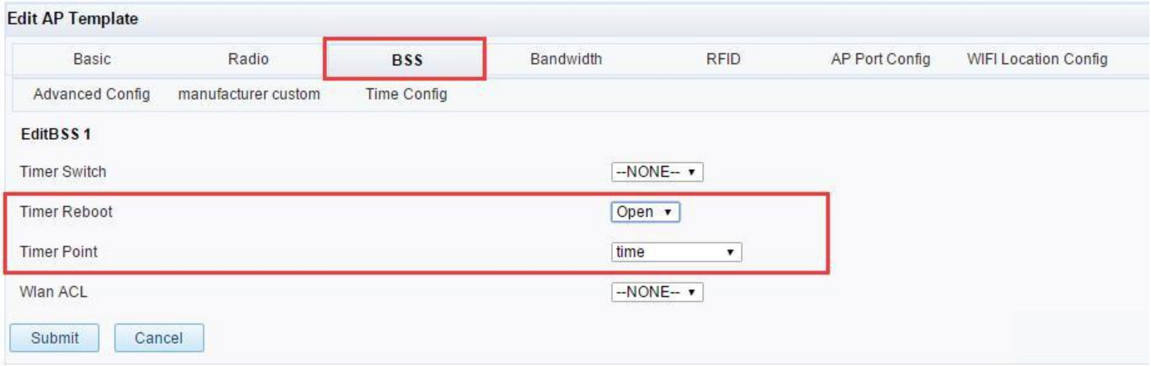
The parameter description for time rule bound with RF configuration is as shown in Table 12-5.

Configuration Item	Description
Timed on/off	The timed on/off of RF is realized by setting [unused], [ON] and [OFF]
Time Period	Select the time range for timed on/off of RF
Timed Restart	The timed restart of RF is realized by setting [unused], [ON] and [OFF]
Time Point	Select the time point for RF restart

Table 12-5 Parameter Description for Time Rule Bound with RF Configuration

12.4 Time Rule Bound with BSS Configuration

Bind the set time rule with BSS configuration of AP template and issue it to AP so that the AP's single or multiple wireless signals could be turned on/off or restarted within the set time as shown in Fig. 12-8.


Edit AP Template

EditBSS 1

Timer Switch: --NONE--

Timer Reboot: Open

Timer Point: time

Wlan ACL: --NONE--

Fig. 12- 8 Time Rule Bound with AP Template BSS Configuration

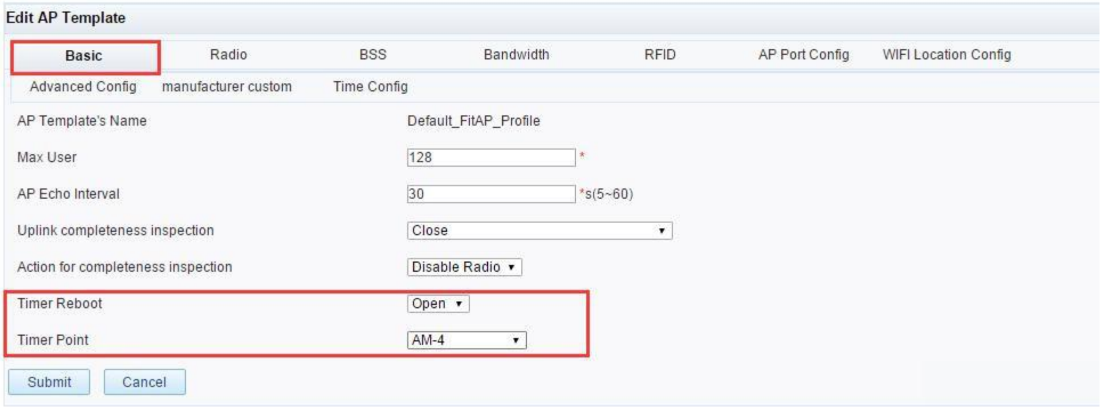
The parameter description for time rule bound with AP template BSS configuration is as shown in Table 12-6.

Configuration Item	Description
Timed on/off	The timed on/off of individual BSS' is realized by setting [unused], [ON] and [OFF]
Time Period	Select the time range for timed on/off of BSS
Timed Restart	The timed restart of individual BSS' is realized by setting [unused], [ON] and [OFF]
Time Point	Select the time point for restart of individual BSS'

Table 12-6 Parameter Description for Time Rule Bound with AP Template BSS Configuration

12.5 Timed Restart of AP

Bind the set time point rule with basic configuration item in AP template and issue it to AP for timed restart of AP as shown in Fig. 12-9.


Edit AP Template

AP Template's Name	Default_FitAP_Profile
Max User	128 *
AP Echo Interval	30 *s(5~60)
Uplink completeness inspection	Close
Action for completeness inspection	Disable Radio
Timer Reboot	Open
Timer Point	AM-4

Fig. 12-9 Timed Restart of AP

Chapter 13 AuthenticationConfiguration

13.1 WEB Authentication Description

Just as its name implies, "WEB authentication" means user is authenticated by logging into WEB page so as to access application system; it's one of the mainstream authentication methods employed by operators at present.

WEB authentication must be performed with Portal server (custom WEB page) and RADIUS server (user authentication and billing).

13.1.1 WEB Authentication System Structure

WEB-based authentication takes AC/SC as WLAN user for access to authentication point. Fig. 13-1 indicates WEB-based account number/password authentication system structure.

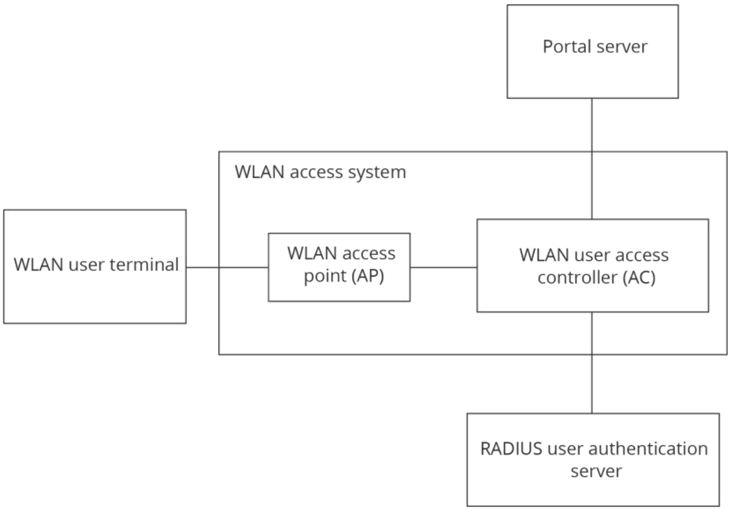


Fig. 13-1 WEB-based Account Number/Password Authentication System Structure

- WLAN User Terminal

WLAN user terminal must be provided with 802.11a/b/g/n-compliant wireless network card and WEB browser software.

- WLAN access point (AP)

AP is used for wireless access of WLAN user.

- WLAN user access controller (AC)

As the WLAN user access authentication point, AC checks if the connected user has passed authentication, and works with background WEB authentication server to authenticate WLAN user. As a service control point, it's used for service control during WLAN accessing, including mandatory PORTAL etc.

- Portal server

Push authentication page to WLAN user (support PC and mobile phone terminals).

- RADIUS user authentication server

RADIUS user authentication server performs WEB-based user authentication

13.1.2 Relation between Portal, Radius and Domain

The relation between Portal, Radius and domain is shown in Fig. 13-2. Domain-offered network resources are not accessible to unauthorized user, unless it turns into authenticated user through Portal authentication. Portal server is like a door of the domain; in order to become a domain authenticated user, the user has to pass the authentication at the portal pushed through Portal server.

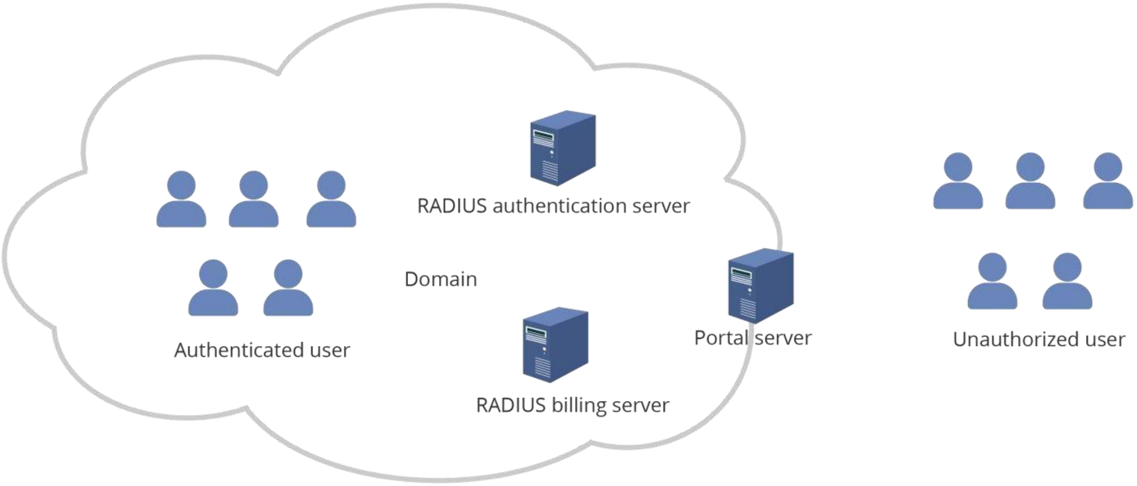
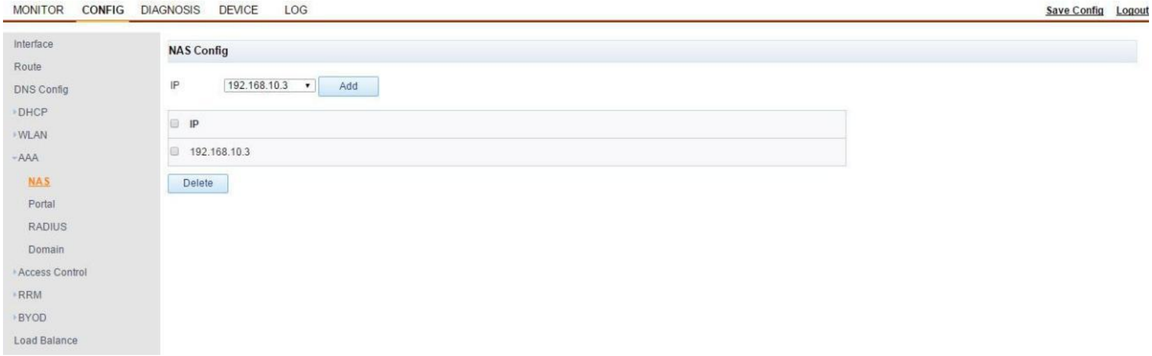


Fig. 13-2 Diagram of Relation between Portal, Radius and Domain

13.2 Authentication Configuration

[Authentication configuration] page is divided into four parts, i.e. [NAS configuration], [portal configuration], [Radius configuration] and [domain configuration] as shown in Fig. 13-3.



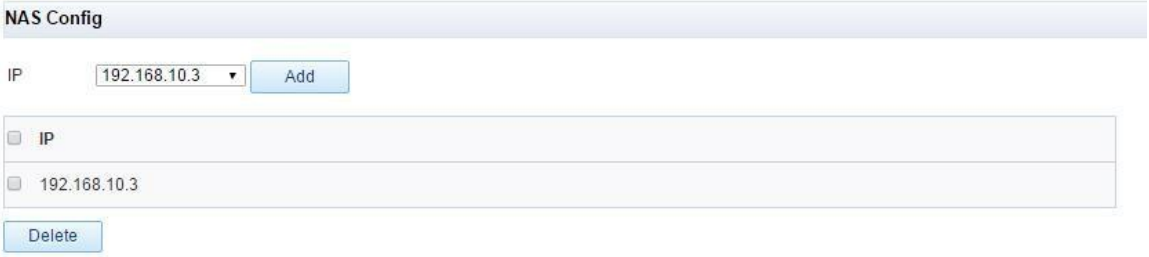
IP 192.168.10.3

□ IP
□ 192.168.10.3

Fig. 13-3 Authentication Configuration Page

13.2.1 NAS Configuration

NAS configuration is as shown in Fig. 13-4; NAS list contains all client ips that could be taken as portal server and radius server; only SERVICE interface address could be added to NAS list; up to 5 NAS entities could be configured, i.e. 5 NAS IPs.



IP 192.168.10.3

□ IP
□ 192.168.10.3

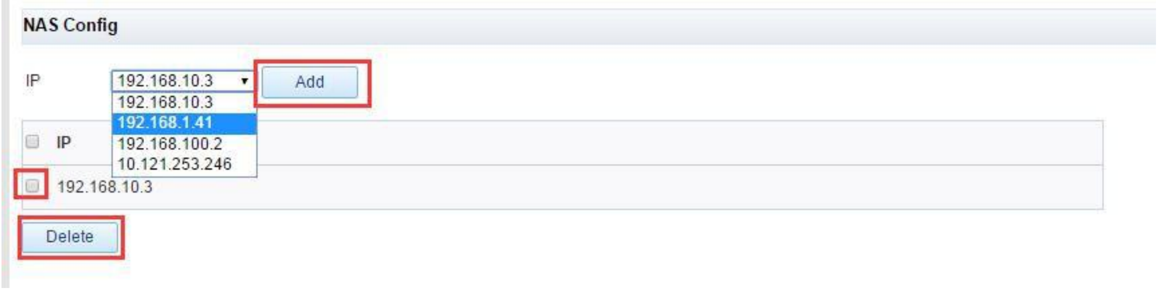
Fig. 13-4 NAS Configuration

Note: Slot could be chosen for frame-type AC page, and each slot could be configured with up to 5 NAS entities.

- Add/delete NAS IP

As shown in Fig. 13-5, the drop-down list of [IP address] shows all SERVICE interface addresses on this service board; user could choose a SERVICE interface address, and click on <add> to add SERVICE interface to NAS list as shown in Fig. 13-5.

To delete an added NAS IP, user could select the IP address record as shown in Fig. 8-5, and click on <delete> button to delete NAS IP address.



NAS Config

IP 192.168.10.3 ▾ Add

192.168.10.3
192.168.1.41
192.168.100.2
10.121.253.246

□	IP
□	192.168.10.3

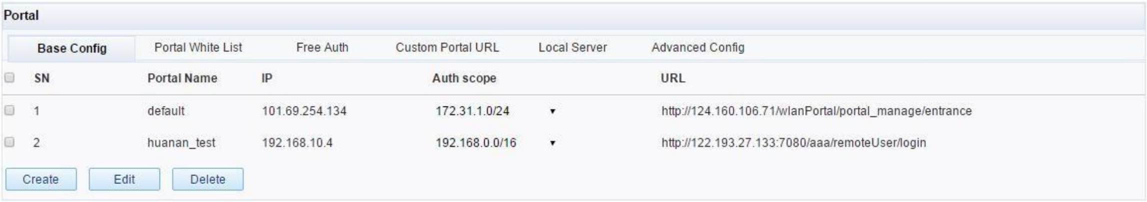
Delete

Fig. 13-5 Configuration for Adding/Deleting NAS IP Address

13.2.2 Portal Configuration

Portal authentication is a kind of WEB authentication, and Portal authentication website is normally called portal site; in the case of unauthorized user, the device forces the user to log in to a particular site, where the user has free access to services there. When user needs to use other information at the Internet, he/she must be authenticated at portal site so as to have access to Internet resources. User could initiatively visit portal site (Portal page), and enter user name and password for authentication; this method is called active authentication. The user attempting to visit other extranets through HTTP will be forced to visit Portal authentication website, where Portal authentication is started; this method is called mandatory authentication.

Fig. 13-6 shows a Portal configuration page that is divided into [basic configuration], [pre-authentication white list], [authentication exemption] and [local server].



Portal

Base Config | Portal White List | Free Auth | Custom Portal URL | Local Server | Advanced Config

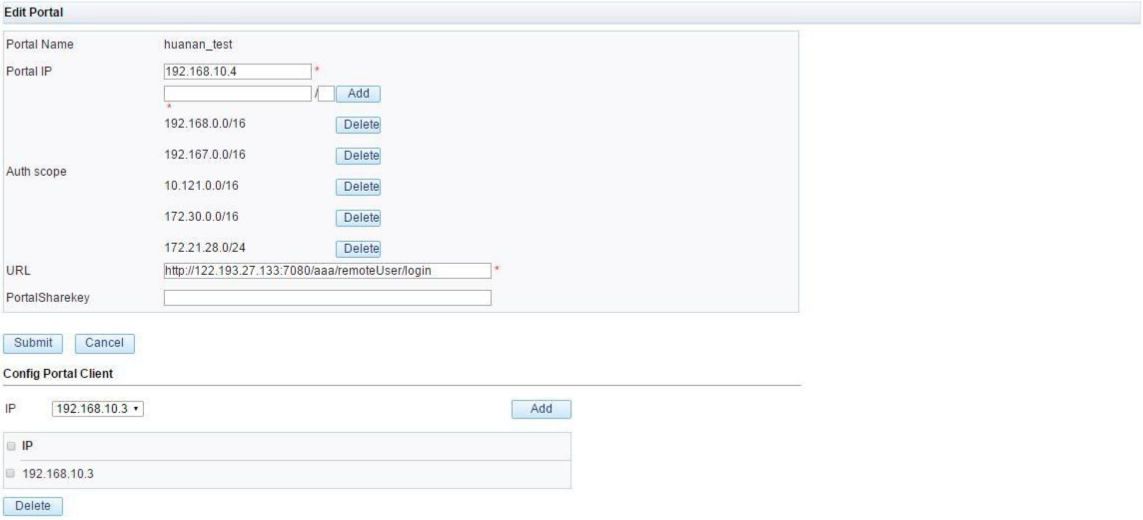
□	SN	Portal Name	IP	Auth scope	URL
□	1	default	101.69.254.134	172.31.1.0/24 ▾	http://124.160.106.71/wlanPortal/portal_manage/entrance
□	2	huanan_test	192.168.10.4	192.168.0.0/16 ▾	http://122.193.27.133:7080/aaa/remoteUser/login

Create Edit Delete

Fig. 13-6 Portal Configuration Page

• Basic Configuration

Click on the [basic configuration] item in the page as shown in Fig. 13-6, and click on <create> button to create Portal configuration data as shown in Fig. 13-7. Furthermore, user could choose a created portal configuration and click on <edit> to open the page as shown in Fig. 13-7.



Edit Portal

Portal Name	huanan_test
Portal IP	192.168.10.4 *
	/ Add
	192.168.0.0/16 Delete
	192.167.0.0/16 Delete
Auth scope	10.121.0.0/16 Delete
	172.30.0.0/16 Delete
	172.21.28.0/24 Delete
URL	http://122.193.27.133:7080/aaa/remoteUser/login *
PortalSharekey	

Submit Cancel

Config Portal Client

IP 192.168.10.3 ▾ Add

□	IP
□	192.168.10.3

Delete

Fig. 13-7 Portal Configuration

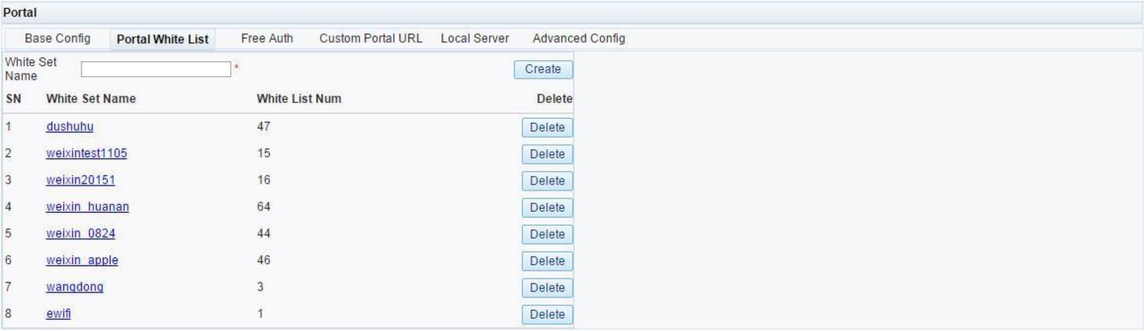
The Portal configuration page parameter description is as shown in Table 13-1.

Configuration Item	Description
Portal Name	Used to identify the name of added Portal
Portal Address	Portal server address
Authentication Scope	Force Portal to push the user address range acted upon
URL	The URL for access redirection (i.e. the URL of Portal server) is mandatorily pushed to user
IP Address Configuration at Portal Client	Since AC serves as NAS network element, this configuration is the IP address of AC and Portal server interface

Table 13-1 Portal Configuration Page Parameter Description

• Pre-authentication White List

Click on the [pre-authentication white list] item in the page as shown in Fig. 13-6. User could add and delete white list set in this page; enter the white list set name to be added behind white list set name, and click on <create> button to view the test white list set created as shown in Fig. 13-8.

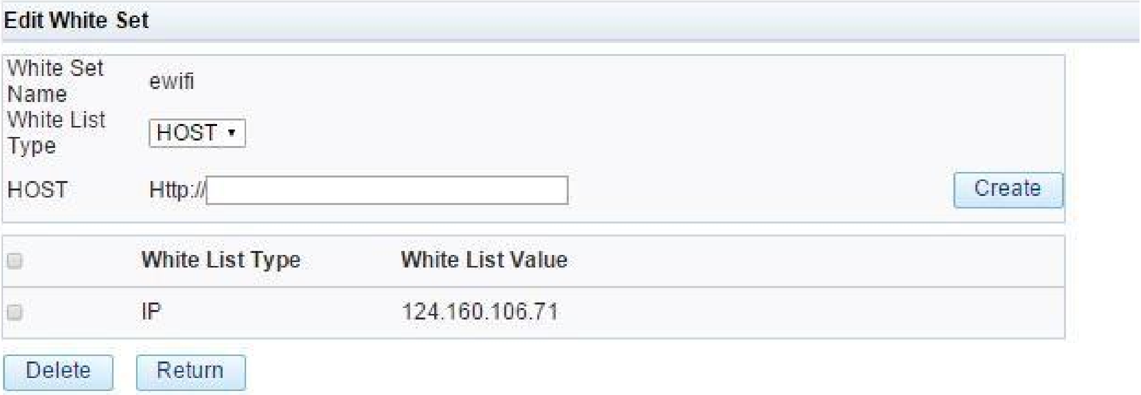


White Set Name *

SN	White Set Name	White List Num	Delete
1	dushuhu	47	Delete
2	weixintest1105	15	Delete
3	weixin20151	16	Delete
4	weixin_huanan	64	Delete
5	weixin_0824	44	Delete
6	weixin_apple	46	Delete
7	wangdong	3	Delete
8	ewifi	1	Delete

Fig. 13-8 Pre-authentication White List

Click on the successfully created white list set to open the white list set configuration page as shown in Fig. 13-9.



White Set Name: ewifi

White List Type: HOST ▾

HOST: Http://

□	White List Type	White List Value
□	IP	124.160.106.71

Fig. 13-9 Edit White List Set

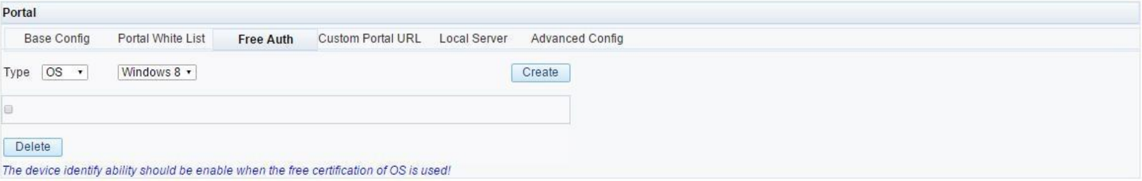
The white list set configuration page parameter description is as shown in Table 13-2.

Configuration Item	**Description**
White List Type	Indicate the whitelist type, i.e. HOST or IP (host address)
HOST	Host name of white list configured
IP	IP address of white list configured

Table 13-2 Pre-authentication White List Page Parameter Description

- Authentication Exemption

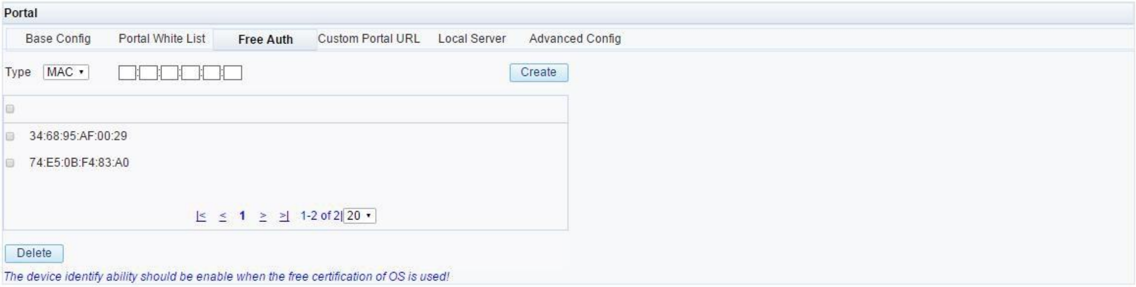
Click on the [authentication exemption] item in the page as shown in Fig. 13-6. User could add and delete authentication exemption item in this page; when the type is set to "operating system" (as shown in Fig. 13-10), authentication exemption is conducted for operating system; when the type is set to "MAC" (as shown in Fig. 13-11), authentication exemption is conducted for user's MAC address.



Type OS ▾ Windows 8 ▾

The device identify ability should be enable when the free certification of OS is used!

Fig. 13-10 Authentication Exemption of Operating System



Type MAC ▾ □:□:□:□:□:□

□ 34:68:95:AF:00:29

□ 74:E5:0B:F4:83:A0

|< < 1 > >| 1-2 of 2 20 ▾

The device identify ability should be enable when the free certification of OS is used!

Fig. 13-11 MAC Authentication Exemption

The authentication exemption configuration page parameter description is as shown in Table 13-3.

Configuration Item	**Description**
Type	The type of authentication exemption could be set to <operating system> and <MAC>; in case of operating system, the operating system to be exempted from authentication could be selected; in case of MAC, the MAC address to be exempted from authentication could be entered

Table 13-3 Authentication Exemption Configuration Page Parameter Description

• Local Server

Click on the [local server] item in the page as shown in Fig. 13-6 to open the page as shown in Fig. 13-12. User could configure local server in this page.

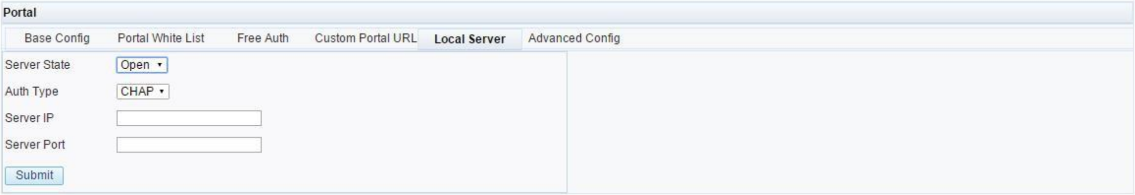


Fig. 13-12 Local Server

The local server page parameter description is as shown in Table 13-4.

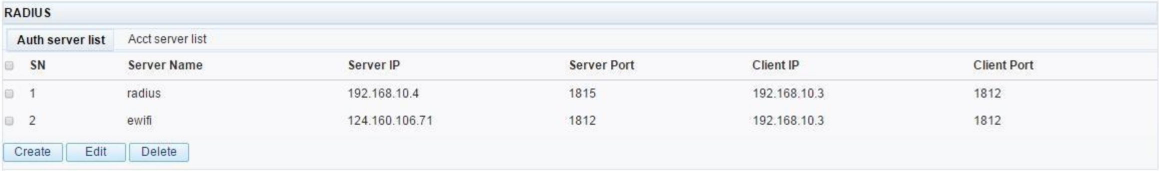
Configuration Item	**Description**
Server State	The state of local Portal server (ON/OFF)
Authentication Type	The type of portal authentication (CHAP/PAP)
Server Address	The address of local portal server
Server Port Number	Port number of local portal server

Table 13- 4 Local Server Parameter Description

13.2.3 RADIUS Configuration

Radius (Remote Authentication Dial In User Service) authentication means "remote authentication dial-in user service". As a C/S protocol, Radius takes AC as its client, and its server side could be established with 2003/2008 server or connected with mobile telecommunication standard protocol-based RADIUS-SERVER. RADIUS protocol features flexible authentication mechanism that supports PEAP and certificate authentication etc. Upon completion of authentication, different users could be billed to realize the unified management and billing of various wireless users.

As shown in Fig. 13-13, RADIUS configuration consists of [authentication server list] and [billing server list].



RADIUS

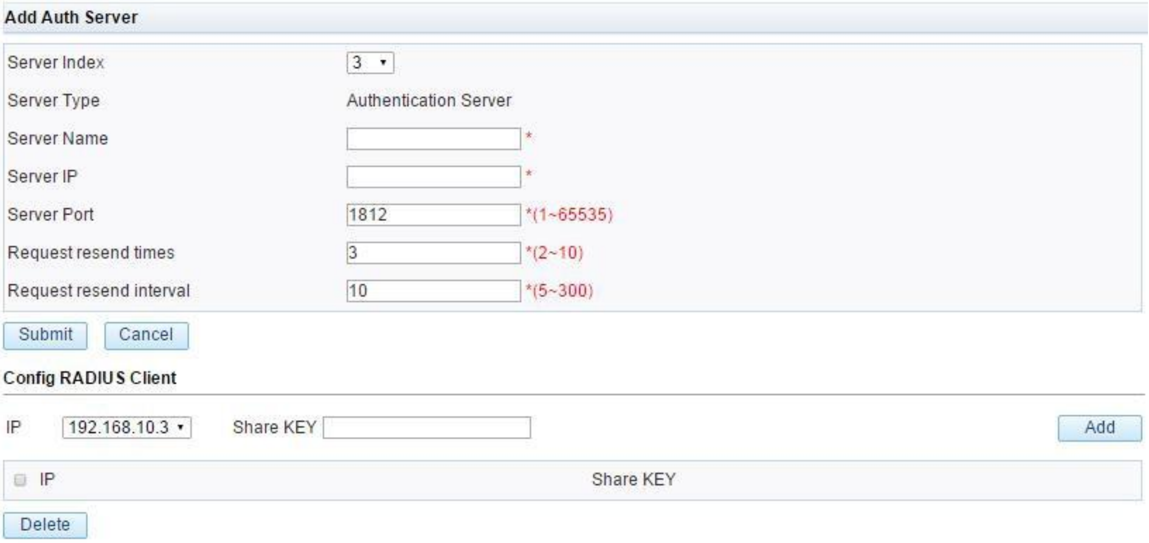
Auth server list | Acct server list

□ SN	Server Name	Server IP	Server Port	Client IP	Client Port
□ 1	radius	192.168.10.4	1815	192.168.10.3	1812
□ 2	ewifi	124.160.106.71	1812	192.168.10.3	1812

Fig. 13-13 RADIUS Configuration

• Authentication Server List

User could create, edit and delete authentication server list data in Fig. 13-14.



Add Auth Server

Server Index	3 ▾
Server Type	Authentication Server
Server Name	*
Server IP	*
Server Port	1812 *(1~65535)
Request resend times	3 *(2~10)
Request resend interval	10 *(5~300)

Config RADIUS Client

IP 192.168.10.3 ▾ Share KEY

□ IP	Share KEY

Fig. 13-14 Create Authentication Server List

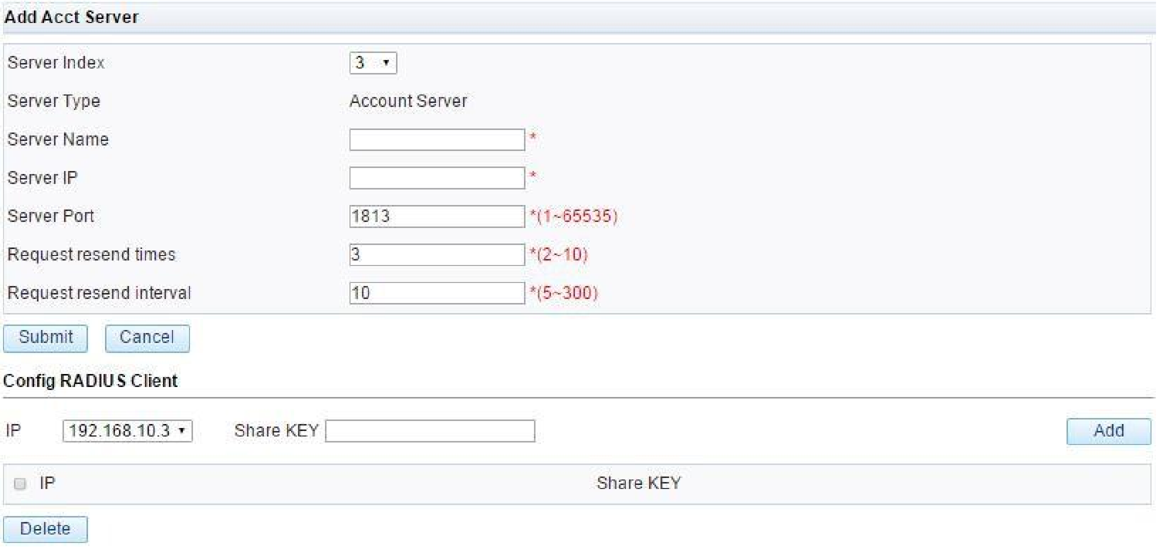
Please refer to Table 13-5 Parameter description in authentication server page for the parameter description in authentication server creation page.

Configuration Item	Description
Server Number	The ID number of RADIUS server added to system. No more than 20 IDs
Server Type	Distinguish between authentication and billing
Server Name	The name of authentication server added by user
Server Address	Radius authentication server address
Server Port	The Radius authentication service port number varies depending on the port number of Radius authentication service activated at server side; the default port number 1812 is normally employed
Request Repeat Count	The number of request repeats (3 by default) upon authentication message interaction failure
Request Repeat Interval	Request repeat interval upon authentication message interaction failure (10s by default)
IP Address Configuration at RADIUS Client	Since AC serves as NAS network element, this configuration is the IP address of AC and RADIUS server interface
Shared Key	The pre-shared key for secure channel between AC and RADIUS server that must be consistent with RADIUS server configuration

Table 13-5 Parameter Description in Authentication Server Page

- Billing Server List

User could create, edit and delete billing server user data in the billing server list as shown in Fig. 13-15.



Add Acct Server

Server Index	3 ▾
Server Type	Account Server
Server Name	*
Server IP	*
Server Port	1813 *(1~65535)
Request resend times	3 *(2~10)
Request resend interval	10 *(5~300)

Fig. 13-15 Create Billing Server List

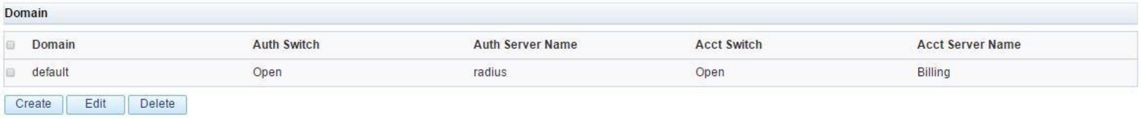
Please refer to Table 13-6 for parameter description in billing server creation page.

Configuration Item	**Description**
Server Number	The ID number of RADIUS server added to system. No more than 20 IDs
Server Type	Distinguish between authentication and billing
Server Name	The name of billing server added by user
Server Address	Radius billing server address
Server Port	The Radius billing service port number varies depending on the port number of Radius billing service activated at server side; the default port number 1813 is normally employed
Request Repeat Count	The number of request repeats (3 by default) upon billing message interaction failure
Request Repeat Interval	Request repeat interval upon billing message interaction failure (10s by default)
IP address Configuration at RADIUS Client	Since AC serves as NAS network element, this configuration is the IP address of AC and RADIUS server interface
Shared Key	The pre-shared key for secure channel between AC and RADIUS server that must be consistent with RADIUS server configuration

Table 13-6 Parameter Description in Billing Server Page

13.2.4 Domain Configuration

Control and manage the domains corresponding to user's authentication service and billing service by adding domain configuration; as shown in Fig. 13-16, user could add, edit and delete domain configuration in [domain configuration] page.

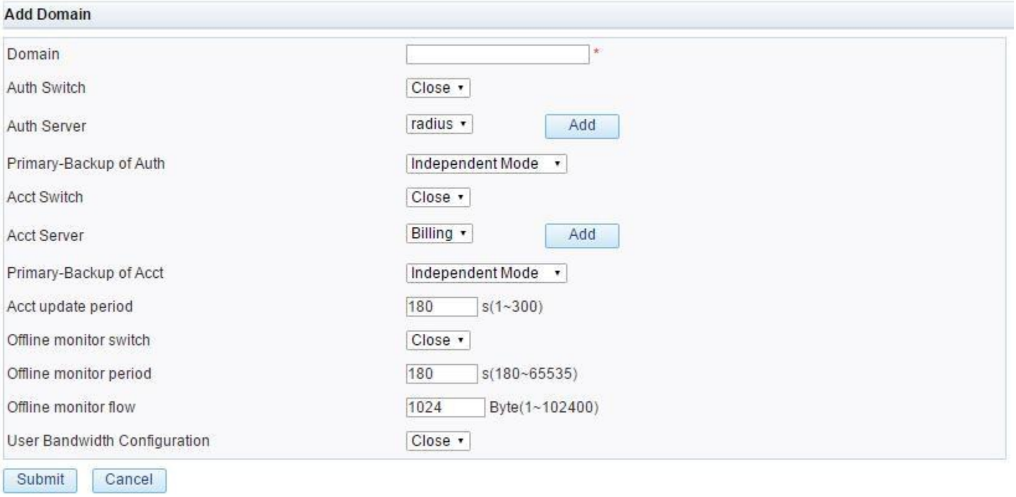


Domain

□ Domain	Auth Switch	Auth Server Name	Acct Switch	Acct Server Name
□ default	Open	radius	Open	Billing

Fig. 13-16 Domain Configuration Page

Click on <Submit> button to create domain configuration as shown in Fig. 13-17.



Add Domain

Domain	*
Auth Switch	Close
Auth Server	radius
Primary-Backup of Auth	Independent Mode
Acct Switch	Close
Acct Server	Billing
Primary-Backup of Acct	Independent Mode
Acct update period	180 s(1~300)
Offline monitor switch	Close
Offline monitor period	180 s(180~65535)
Offline monitor flow	1024 Byte(1~102400)
User Bandwidth Configuration	Close

Fig. 13-17 Create Domain Configuration

The domain configuration page parameter description is as shown in Table 13-7.

Configuration Item	Description
Domain Name	Create the name of domain
Authentication Service on/off	Enable or disable authentication service
Authentication Server	The server referenced from authentication server list
Authentication Active-standby State	In "independent mode" there is only one authentication server in the system; in "active-standby mode" there are two authentication servers in the system, i.e. a master server, and a backup server
Billing Server on/off	Enable or disable billing service
Billing Server	The server referenced from billing server list
Billing Active-standby State	In "independent mode" there is only one billing server in the system; in "active-standby mode" there are two billing servers in the system, i.e. a master server, and a backup server
Billing Update Cycle	The transmission interval of traffic billing message prepared by AC for billing server
Offline Monitoring on/off	Offline monitoring on/off

Offline Monitoring Cycle	If the traffic within "offline monitoring cycle" at a client is less than "offline monitoring traffic", the billing server deems the client as "off-line".
Offline Monitoring Traffic	If the traffic within "offline monitoring cycle" at a client is less than "offline monitoring traffic", the billing server deems the client as "off-line".
User Bandwidth Limitation	This function could be enabled for Portal authentication user bandwidth limitation

Table 13-7 Domain Configuration Page Parameter Description

Note: Where the domain name is not specified or given, user could use default domain name for configuration. The [domain] added by user must completely matches the user domain name defined in RADIUS server; since the complete user name of every user in the domain should be in the form "user@domain", authentication is impossible in case of domain name error.

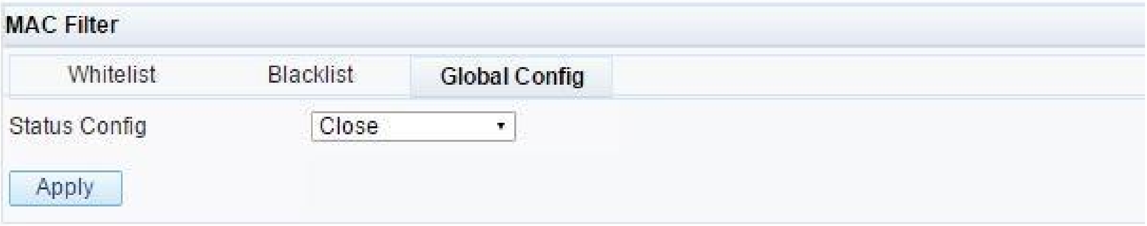
Chapter 14 Access Control

14.1 Access Control Overview

Wireless controller (AC) performs access management of STA through access control by filtrating the MAC address of STA.

14.2 MAC Address Filter Configuration

[MAC address filter] configuration falls into [white list], [blacklist] and [global configuration] as shown in Fig. 14-1.

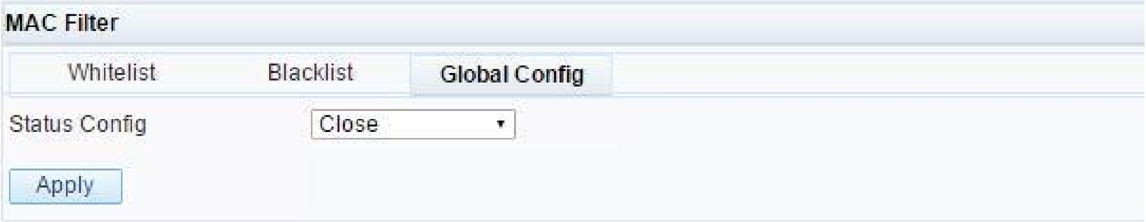

MAC Filter

Status Config: Close

Fig. 14-1 MAC Address Filter Configuration

- Global Configuration

[Global configuration] globally enables AC to control STA access MAC address filter in white list mode or blacklist mode. When AC functions in white list mode, the white list configured by user takes effect, and only the STAs in white list can get associated and go online; when AC runs in blacklist mode, the blacklist configured by user takes effect, and all STAs in blacklist can't get associated and go online as shown in Fig. 14-2.



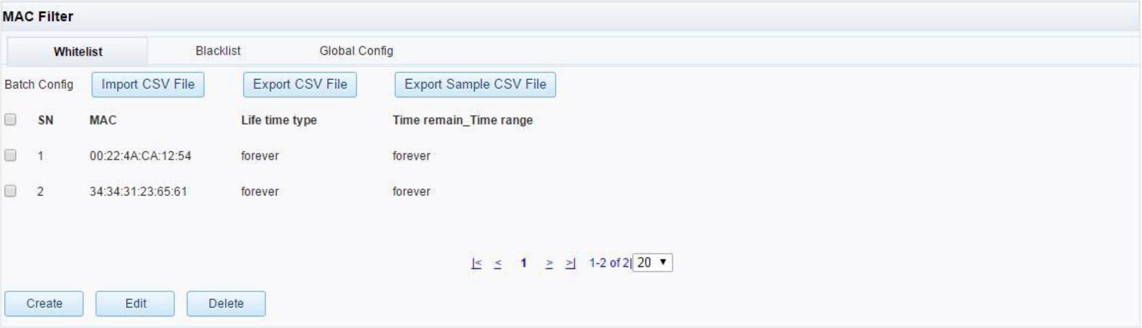
Status Config: Close ▾

Fig. 14-2 Global Configuration

- White List Configuration

In the [white list] configuration page, the white list could be created, edited and deleted, while batch operation could be performed through CSV file import/export as shown in Fig. 14-3.

White list can't take effect unless the [global configuration] is in "enabled white list" state; only the user terminals in white list have access to WLAN network within lifetime.



□	SN	MAC	Life time type	Time remain_Time range
□	1	00:22:4A:CA:12:54	forever	forever
□	2	34:34:31:23:65:61	forever	forever

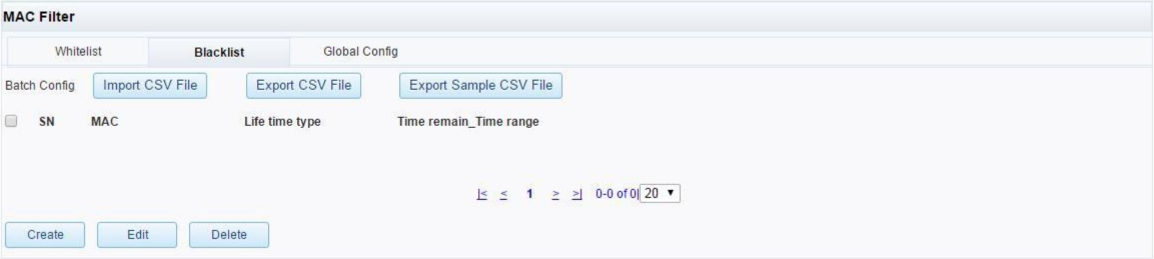
1-2 of 2| 20 ▾

Fig. 14-3 White List Configuration

- Blacklist Configuration

In the [blacklist] configuration page, the blacklist could be created, edited and deleted, while batch operation could be performed through CSV file import/export as shown in Fig. 14-4.

Blacklist can't take effect unless the [global configuration] is in "enabled blacklist" state. In such a case, the user terminals in blacklist have no access to WLAN network within lifetime.



□	SN	MAC	Life time type	Time remain_Time range

0-0 of 0| 20 ▾

Fig. 14-4 Blacklist Configuration

Configuration Item	Description
MAC Address	User terminal STA's MAC address
TTL Type	The effective time of blacklist and white list falls into "permanent validity", duration and time period. "Permanent validity" means blacklist and white list are not time-limited; "duration" means blacklist and white list are effective during the period starting from their creation; "time period" means blacklist and white list are effective within the rule time range; the "time period" shall be configured in [time rule]
Time remain_Time range	The remaining effective time of blacklist and white list. When the type of production time is set to "permanent validity", the "remaining time" indicates "permanent validity"; when the type of production time is set to "duration", the remaining time indicates the remaining effective time of blacklist and white list; when the type of production time is set to "time period", the remaining time indicates all time period names
Import CSV File	Collectively import the blacklists and white lists to be added to wireless controller through CSV file
Export CSV File	Export current blacklist and white list as CSV files
Download Sample CSV	Download sample CSV file

Table 14-1 Blacklist and White List Configuration Page Parameter Description

14.3 HAP Filter Configuration

Please refer to Section 7-6.

14.4 Wireless Access Control

Please refer to Sections 5-4 and 6-3.

14.5 Time Rule

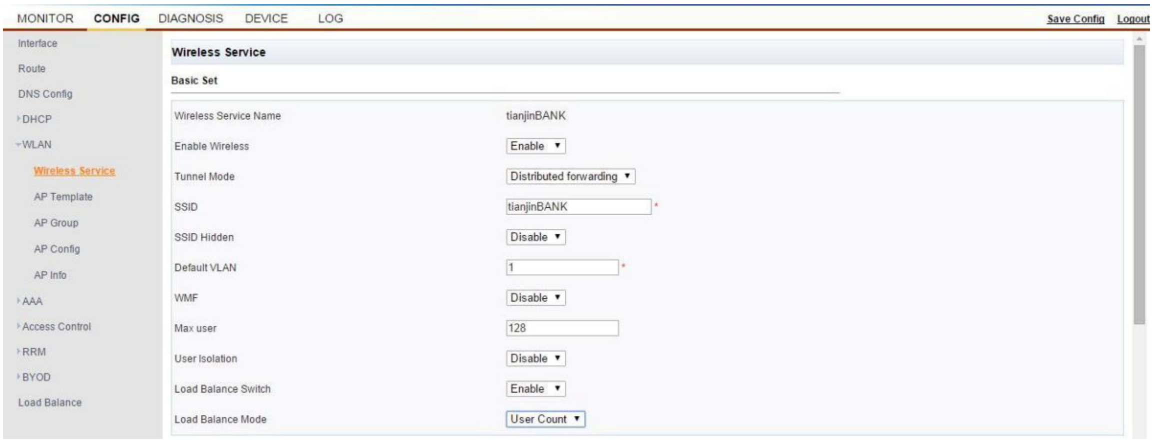
Please refer to Section 12.2.

Chapter 15 Load Balancing

15.1 On/off Control

Load balancing is turned on/off based on wireless service. An AP could be bound with several wireless services. When load balancing on/off is issued to AP, load balancing is determined to be based on the number of users or traffic according to the first wireless service turned on for load balancing.

Load balancing on/off is configured in "network configuration -> WLAN configuration -> wireless service" as shown in the figure.



Wireless Service

Basic Set

Wireless Service Name	tianjinBANK
Enable Wireless	Enable
Tunnel Mode	Distributed forwarding
SSID	tianjinBANK *
SSID Hidden	Disable
Default VLAN	1 *
WMF	Disable
Max user	128
User Isolation	Disable
Load Balance Switch	Enable
Load Balance Mode	User Count

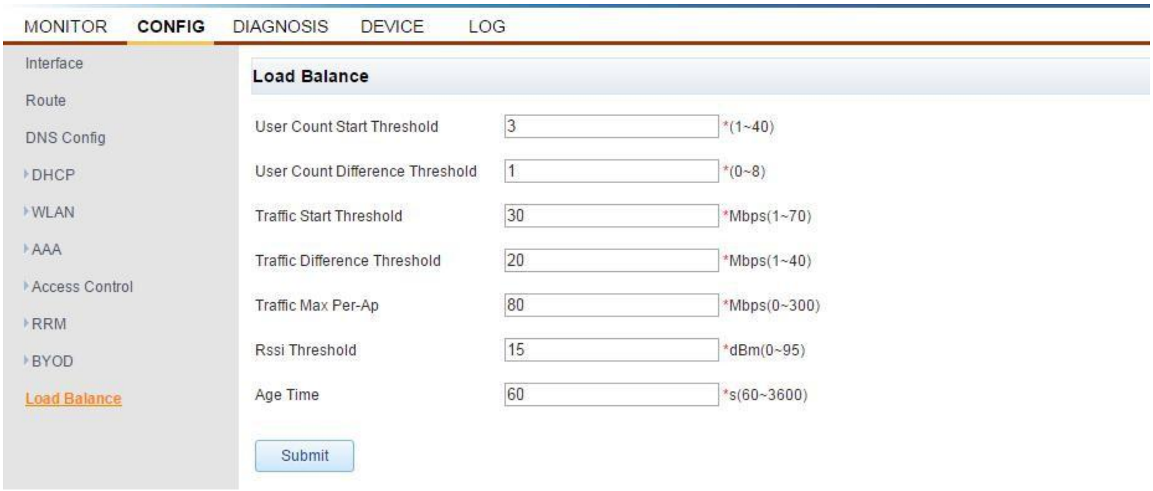
Fig. 15-1 Load balancing on/off configuration

Configuration Item	Description
Load Balance Switch	Enable/disable load balancing
Load Balance Mode	Based on the number of users or traffic

Table 15-1 Load Balancing Switch Parameter Description

15.2 Global Parameter Setup

Load balancing-related global parameters are configured in "network configuration -> load balancing".



Load Balance

User Count Start Threshold: 3 *(1~40)

User Count Difference Threshold: 1 *(0~8)

Traffic Start Threshold: 30 *Mbps(1~70)

Traffic Difference Threshold: 20 *Mbps(1~40)

Traffic Max Per-Ap: 80 *Mbps(0~300)

Rssi Threshold: 15 *dBm(0~95)

Age Time: 60 *s(60~3600)

Fig. 15-2 Global Configuration of Load Balancing

Configuration Item	**Description**
User Count Start Threshold	Load balancing is not judged unless the number of users connected at the AP to be associated with STA ≥ user count start threshold in the case of load balancing based on the number of users
User Count Difference Threshold	For the load balancing judgment in the case of load balancing based on the number of users, the judgment fails if the number of users connected at the AP to be associated with STA > the mean load + difference threshold, in which case STA access will be rejected
Traffic Start Threshold	In the case of traffic-based load balancing, the ON traffic value for judgment is calculated based on the max. traffic and traffic ON threshold of AP; load balancing is not judged unless the current traffic value at the AP to be associated with STA ≥ the traffic start threshold
Traffic Difference Threshold	Percentage; for the load balancing judgment in the case of traffic-based load balancing, the judgment fails if the current traffic value at the AP to be associated with STA > the mean load + traffic difference threshold, in which case STA access will be rejected
Traffic Max Per-Ap	In the case of traffic-based load balancing, the threshold and difference values for judgment are calculated based on the max. traffic of AP, the traffic ON threshold (percentage) and the traffic difference threshold (percentage).
Rssi Threshold	Rssi threshold is issued to AP, where the STA < this threshold is not reported to AC
Age Time	Aging time is issued to AP, where the STA dynamic list is aged based on this aging time

Table 15-2 Global Parameter Description of Load Balancing

Chapter 16 Fault Diagnosis

“[Fault diagnosis] > [PING]" is used to determine the intercommunity between AC and the connected device. As shown in Fig. 16-1, user could enter the IP of connected device, and click on <start> button to check the connection between AC and that address, when the diagnostic result log is displayed in the page; click on <stop> button to stop PING operation. <clear> button is used to clear the log record displayed in management page. Please refer to Fig. 16-2 for the displayed diagnosis log.

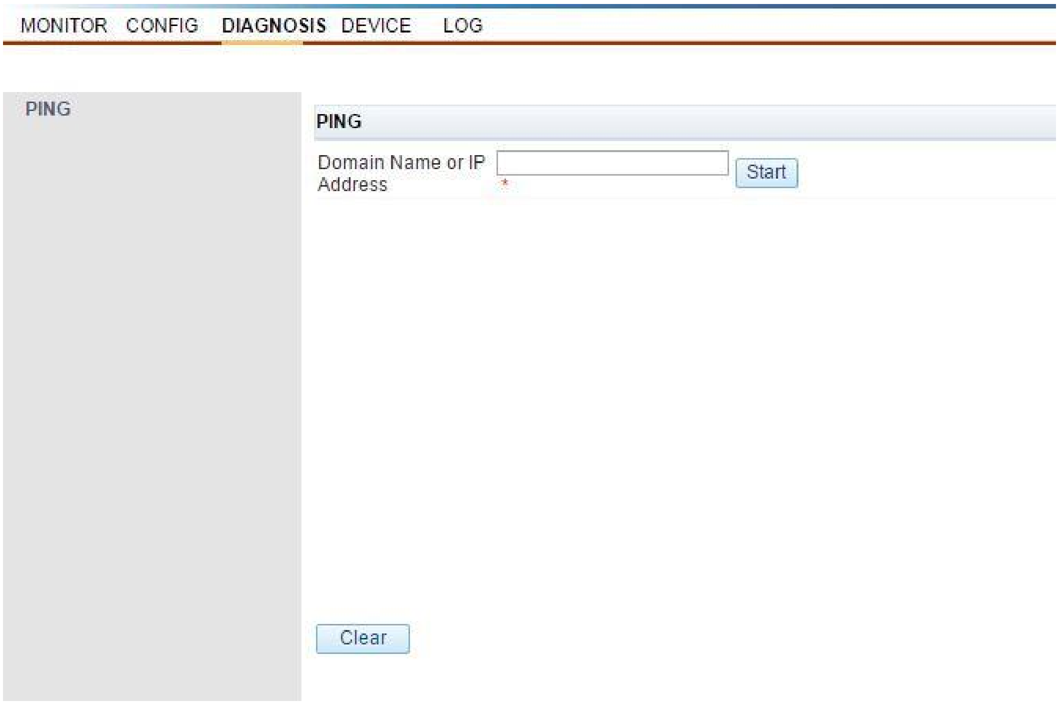
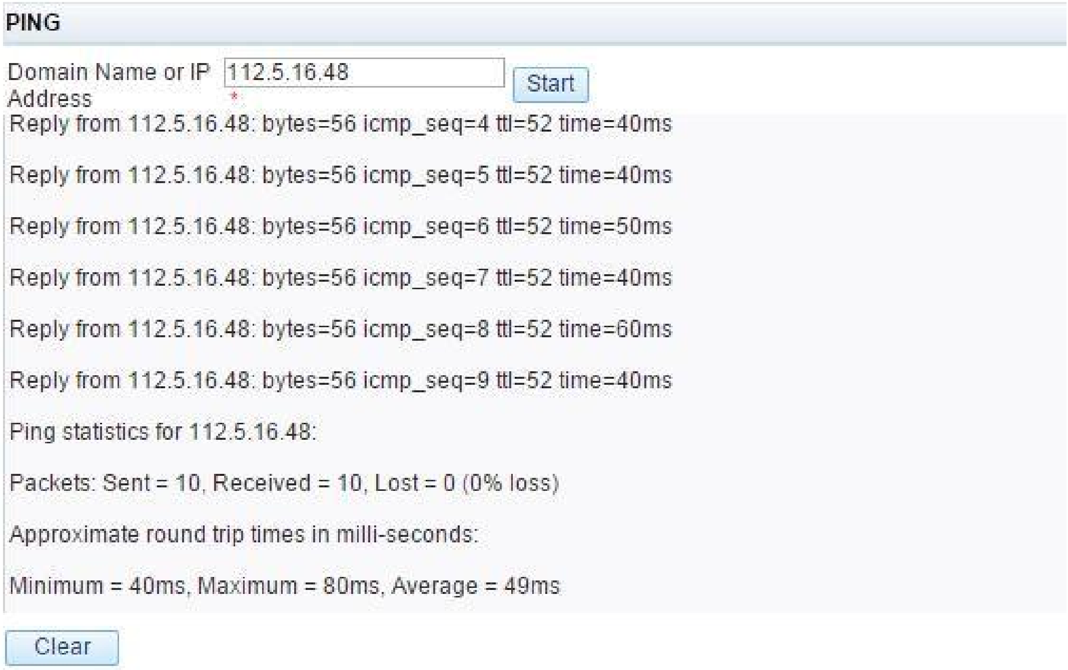


Fig. 16-1 Fault Diagnosis



Domain Name or IP Address * 112.5.16.48

```
Reply from 112.5.16.48: bytes=56 icmp_seq=4 ttl=52 time=40ms

Reply from 112.5.16.48: bytes=56 icmp_seq=5 ttl=52 time=40ms

Reply from 112.5.16.48: bytes=56 icmp_seq=6 ttl=52 time=50ms

Reply from 112.5.16.48: bytes=56 icmp_seq=7 ttl=52 time=40ms

Reply from 112.5.16.48: bytes=56 icmp_seq=8 ttl=52 time=60ms

Reply from 112.5.16.48: bytes=56 icmp_seq=9 ttl=52 time=40ms

Ping statistics for 112.5.16.48:

Packets: Sent = 10, Received = 10, Lost = 0 (0% loss)

Approximate round trip times in milli-seconds:

Minimum = 40ms, Maximum = 80ms, Average = 49ms
```

Fig. 16-2 Displayed PING Diagnosis Log

Please refer to Table 16-1 for page parameter description.

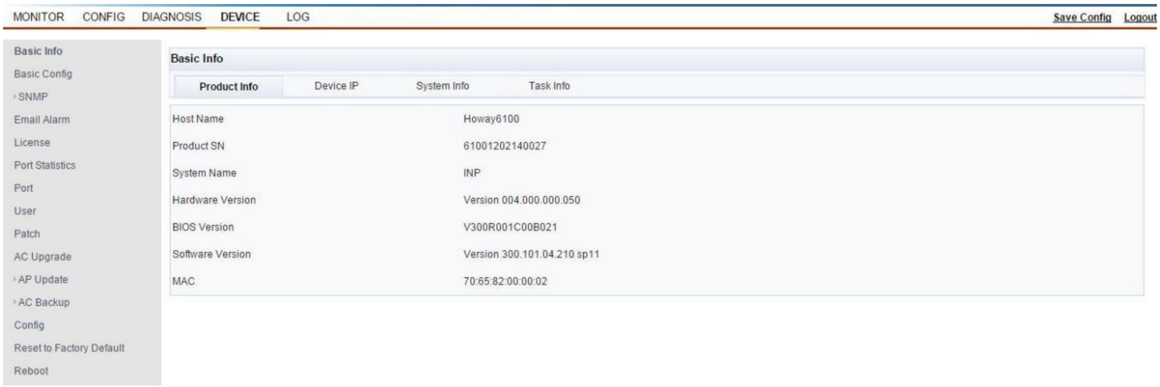
Configuration Item	Description
URL	Destination address of PING diagnosis
Timeout	Determine the delay time of PING diagnosis

Table 16-1 PageParameter Description

Chapter 17 Device Management

17.1 General Information

[General information] includes the device [product information], [Device management address], [system information], and [task information]. as shown in Fig. 17-1.

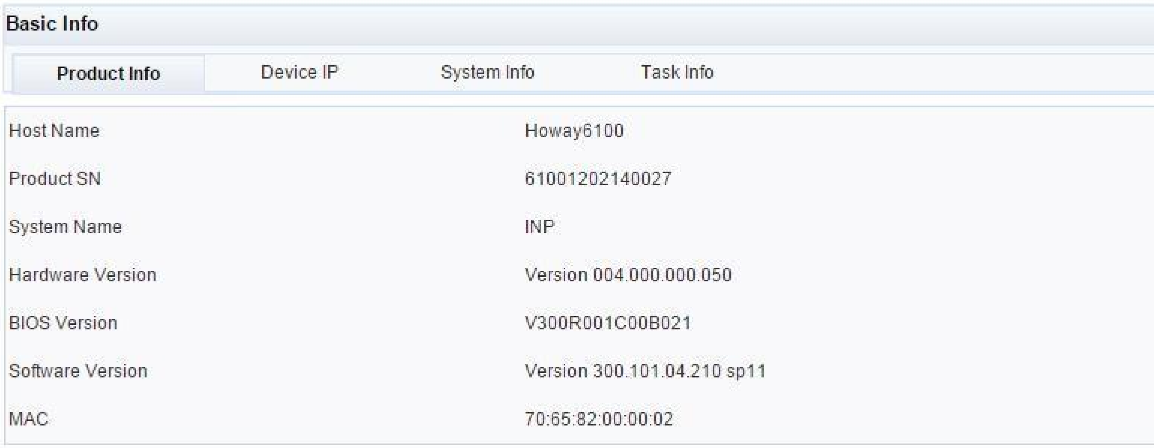


Host Name	Howay6100
Product SN	61001202140027
System Name	INP
Hardware Version	Version 004.000.000.050
BIOS Version	V300R001C00B021
Software Version	Version 300.101.04.210 sp11
MAC	70:65:82:00:00:02

Fig. 17-1 General Information

17.1.1 Product Information

The content of [product information] is as shown in Fig. 17-2. [Product information] page shows [host name], [system name], [hardware version number], [BIOS version number], [software version number], and [MAC address].



Basic Info

Product Info | Device IP | System Info | Task Info

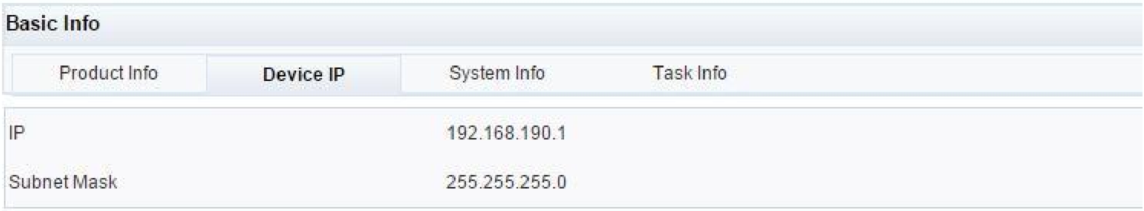
Host Name	Howay6100
Product SN	61001202140027
System Name	INP
Hardware Version	Version 004.000.000.050
BIOS Version	V300R001C00B021
Software Version	Version 300.101.04.210 sp11
MAC	70:65:82:00:00:02

Fig. 17-2 Product Information

Note: [Host name] could be set in “[device management] > [basic configuration]" page.

17.1.2 Device Management Address

The content of [device management address] page is as shown in Fig. 17-3.



Basic Info

Product Info | Device IP | System Info | Task Info

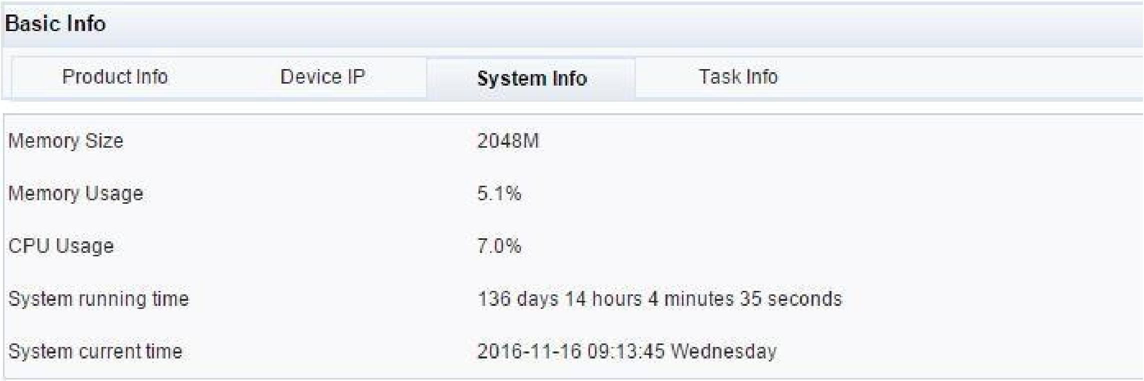
IP	192.168.190.1
Subnet Mask	255.255.255.0

Fig. 17-3 Device Management Address

Note: [Device management address] shows the interface address of default VLAN; the default [IP address] is "192.168.1.1"; the device management address could be set in “[network configuration] > [interface configuration]" page.

17.1.3 System Information

[System information] shows device memory capacity, memory utilization, CPU utilization, system runtime, and current system time as shown in Fig. 17-4.

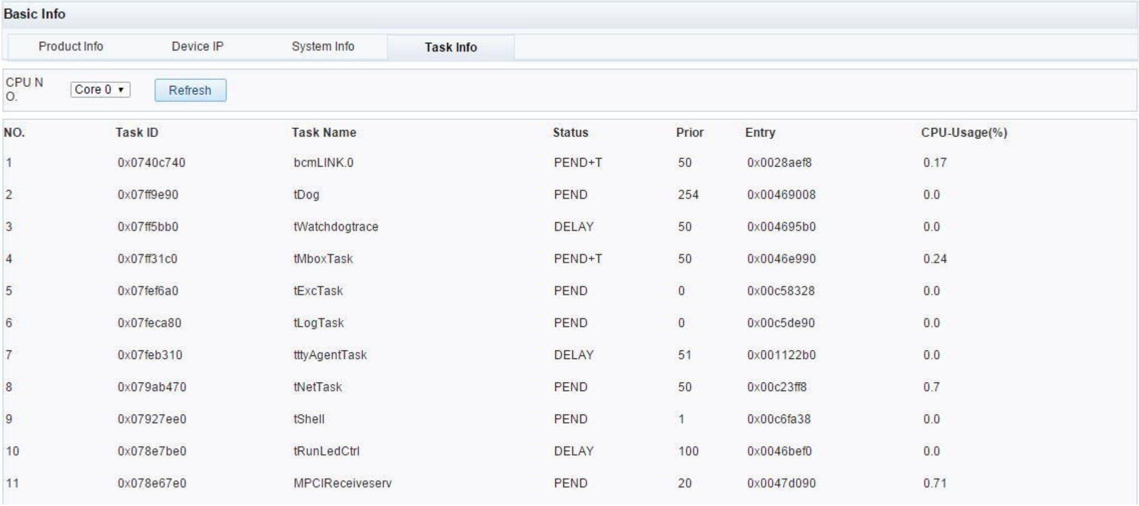


Memory Size	2048M
Memory Usage	5.1%
CPU Usage	7.0%
System running time	136 days 14 hours 4 minutes 35 seconds
System current time	2016-11-16 09:13:45 Wednesday

Fig. 17-4 System Information

17.1.4 Task Information

[Task information] shows the details of currently executing task at each CPU of wireless controller as shown in Fig. 17-5.



CPU NO. Core 0

NO.	Task ID	Task Name	Status	Prior	Entry	CPU-Usage(%)
1	0x0740c740	bcmLINK.0	PEND+T	50	0x0028aef8	0.17
2	0x07ff9e90	tDog	PEND	254	0x00469008	0.0
3	0x07ff5bb0	tWatchdogtrace	DELAY	50	0x004695b0	0.0
4	0x07ff31c0	tMboxTask	PEND+T	50	0x0046e990	0.24
5	0x07fef6a0	tExcTask	PEND	0	0x00c58328	0.0
6	0x07feca80	tLogTask	PEND	0	0x00c5de90	0.0
7	0x07feb310	tttyAgentTask	DELAY	51	0x001122b0	0.0
8	0x079ab470	tNetTask	PEND	50	0x00c23ff8	0.7
9	0x07927ee0	tShell	PEND	1	0x00c6fa38	0.0
10	0x078e7be0	tRunLedCtrl	DELAY	100	0x0046bef0	0.0
11	0x078e67e0	MPCIReceiveserv	PEND	20	0x0047d090	0.71

Fig. 17-5 Task Information

17.2 Basic Setup

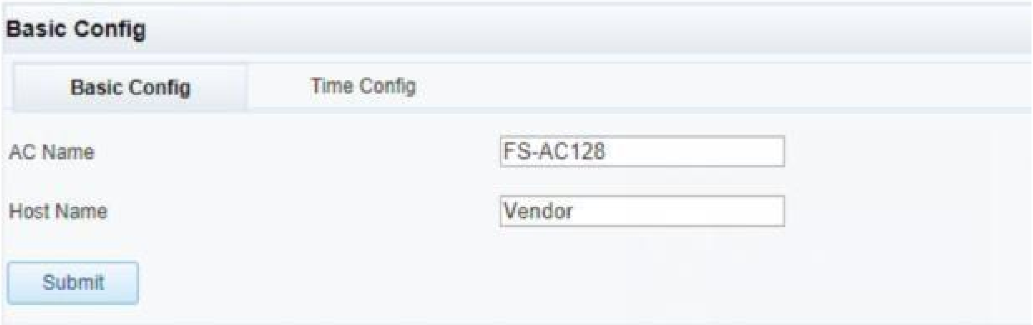
17.2.1 Basic Setup Description

The “[device management] > [basic setup]" interface involves the configuration of [host name] and [AC name] of device, as well as the setup of device time. [Time setup] supports manual configuration of system time and automatic synchronization with NTP (network time protocol) server time. Wireless controller could serve as NTP SERVER that offers clock synchronization for other clients, and could be used as NTP Client for time synchronization with upper NTP server.

NTP is a time synchronization protocol defined by RFC 1305 for time synchronization between time server and client. NTP enables the clocks of all devices within network to keep in line with each other and assure extraordinary accuracy, thereby making it possible for the device to offer a variety of unified time-based applications.

17.2.2 Basic Setup

The [basic setup page] is as shown in Fig. 17-6. User could modify [AC name] and [host name] parameters.



AC Name FS-AC128

Host Name Vendor

Fig. 17-6 Basic setup

The parameter description is shown in Table 17-1.

Configuration Item	Description
AC Name	Describe and identify AC name parameter
Host Name	Identify device host name parameter; background CLI command line host name identification

Table 17-1 Basic Setup Parameter Description

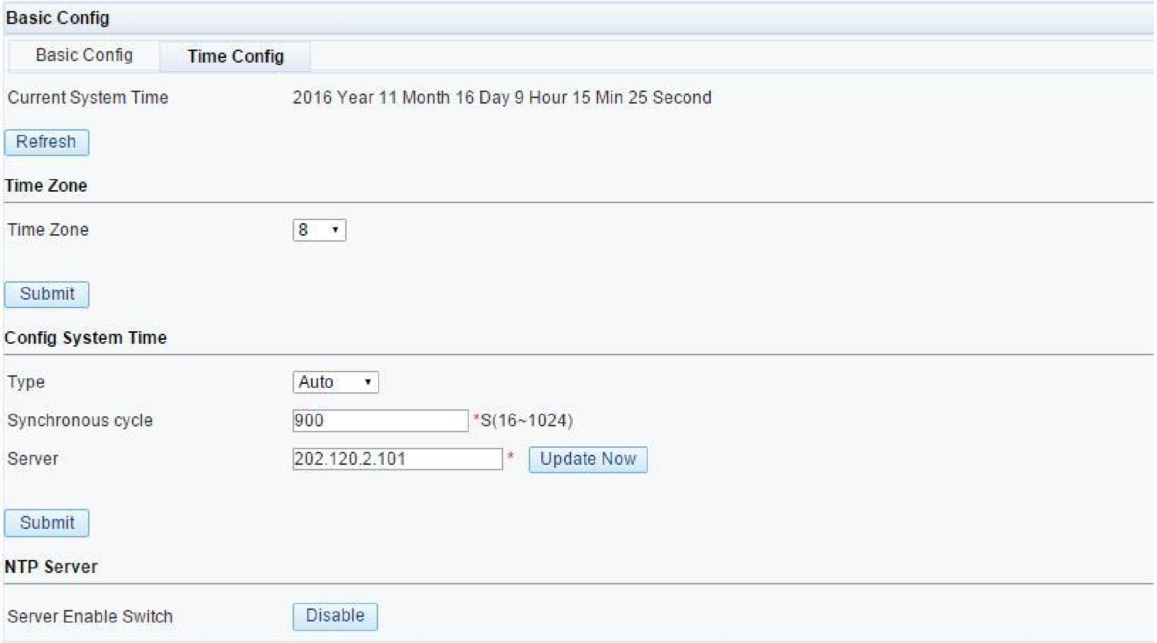
17.2.3 Time Setup

The [time setup] page is as shown in Fig. 17-7. Click on <refresh> in [time setup] option to view current time of wireless controller. [Set system time] is configured in two modes, i.e. [auto] and [manual].

[Manual synchronization]: Select correct "yy-mm-dd-hh-mm-ss", and click on <Submit> to finish the setup.

[Auto synchronization]: Set synchronizing cycle and server address, and click on <Submit>, when the wireless controller time will immediately or periodically get synchronized with server.

[NTP server] enables/disables wireless controller's NTP server; when NTP server is enabled, AC serves as NTP server, while AP could be time synchronized as NTP client with AC.



Basic Config

Current System Time 2016 Year 11 Month 16 Day 9 Hour 15 Min 25 Second

Time Zone

Time Zone: 8

Config System Time

Type: Auto

Synchronous cycle: 900 *S(16~1024)

Server: 202.120.2.101 *

NTP Server

Server Enable Switch: Disable

Fig. 17-7 Time Setup

The time setup parameter description is as shown in Table 17-2.

Configuration Item	**Description**
Time Setup	Manual configuration of device time parameter
Server	Wireless controller serves as NTP server enable switch
Server	Wireless controller serves as the NTP server address for clock synchronization of NTP client
Synchronizing Cycle	The cycle of time synchronization of wireless controller with NTP server
Server Enabled	Use wireless controller as NTP server
Refresh	Refresh the current time of wireless controller

Table 17-2 Time Setup Parameter Description

Note: When wireless controller AC enables NTP client configuration, the device time gets synchronized with NTP server time based on synchronizing cycle, and overwrites the manually configured time settings. In other words, the priority of device is higher than that of manually set time when NTP client is enabled.

17.3 License Configuration

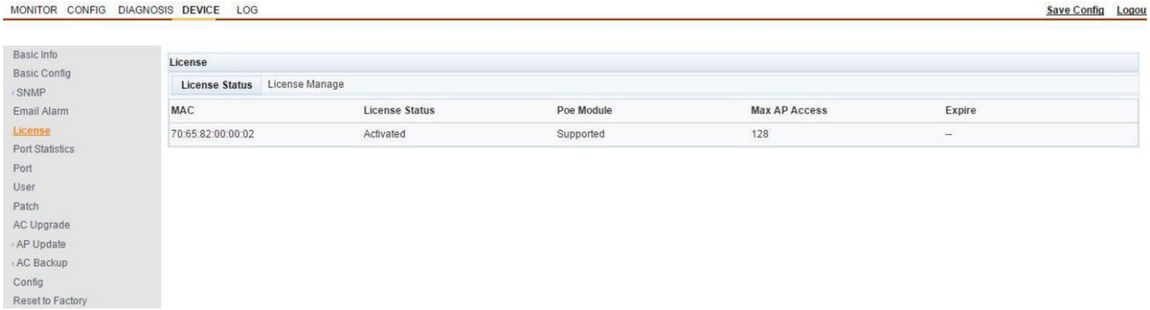
17.3.1 License Description

License protects software copyright and prevents system image being used directly; in addition, it could restrict service specifications and enable POE module.

License file exists with file name "License.dat" in flash file system, and is composed of a character string.

License corresponds to the MAC address and hardware identification code of each service board, whose license file is unique and can't be used for other service boards.

[License configuration] includes [License state] and [License management] as shown in Fig. 17-8.

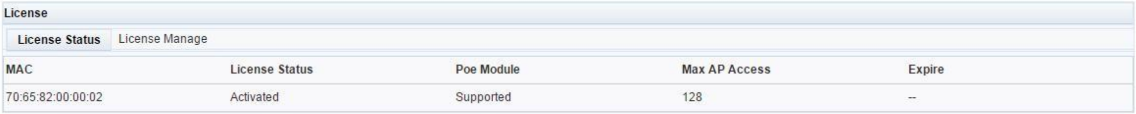


MAC	License Status	Poe Module	Max AP Access	Expire
70:65:82:00:00:02	Activated	Supported	128	--

Fig. 17-8 License Configuration

17.3.2 License State

[License state] page shows the license registration status of all service boards in AC as shown in Fig. 17-9.



MAC	License Status	Poe Module	Max AP Access	Expire
70:65:82:00:00:02	Activated	Supported	128	--

Fig. 17-9 License State

Please refer to Table 17-3 for license parameter description.

Configuration Item	**Description**
MAC Address	MAC address of service board
State	The license state of service board includes "active" and "inactive"
POE Module	License controls the POE module state, including "supported" and "not supported"
Max. Number of APs Accessible	The allowable number of APs accessible to wireless controller according to license
Validity Period	The validity period of license; "--" means "permanently valid"

Table 17-3 License State Parameter Description

17.3.3 License Management

[License management] includes license import and license export; please refer to Fig. 17-10. There are three update modes for license file import: HTTP import, FTP import, and authorization code import. License file is prepared by the Company based on market customers' business requirements.

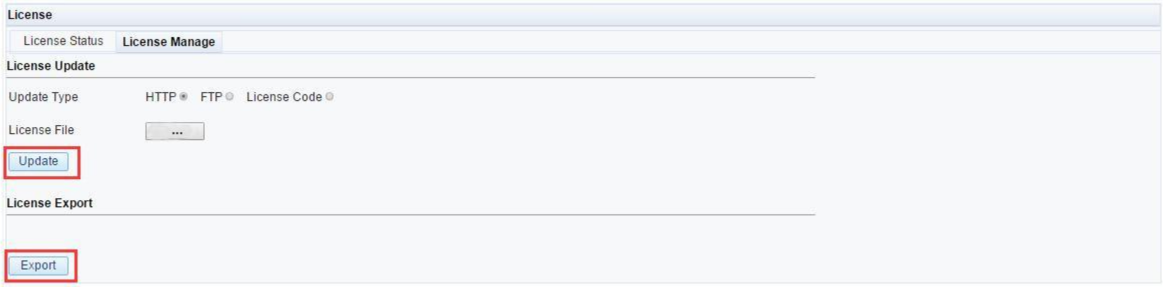


Fig. 17-10 License Management

• License Import through HTTP Update
As shown in Fig. 17-10, user could set [License import] to "HTTP", and click on <browse> button behind [License file] input box, when the file selection window appears, where user could import the prepared license file in local management PC; upon successful update, the page shows the text "License Update Succeeded"; if the imported license file fails to match with service board information, a prompting message reading "UPDATE FAILED" appears.

• License Import through FTP Update
License update with FTP is shown in Fig. 17-11; user needs an external FTP server directed to license file path, and could then set [license file name], [FTP server IP], [user name] and [password] in the page as shown in Fig. 17-11, and click on <update> button.

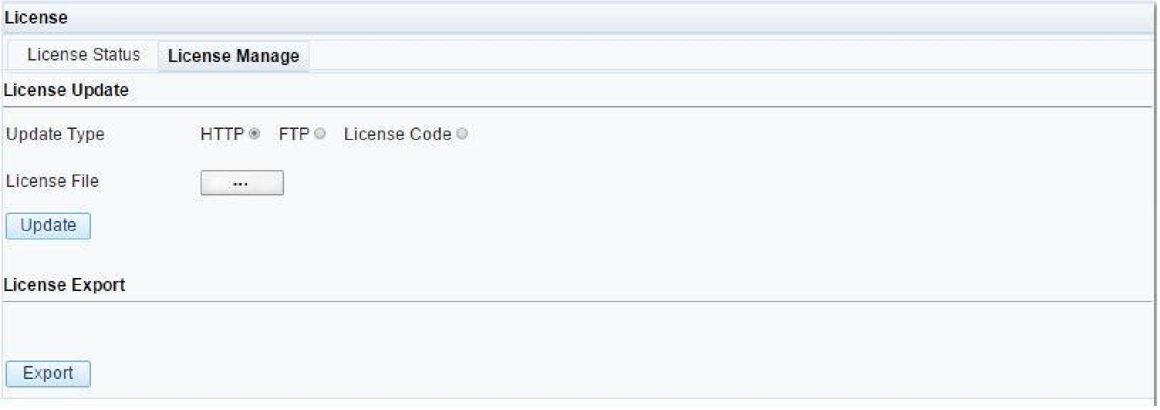


Fig. 17-11 License Import through FTP Update

The parameter description for license file import through FTP update is shown in Table 17-4.

Configuration Item	**Description**
License File Name	Correspond to the license file name of updated service board
Server IP	The FTP server IP address for device to get license file
User Name	FTP's user name
Password	Password of FTP

Table 17-4 Parameter Description of File Import for License Update

- License Import through Authorization Code Update

Update license by entering authorization code; as shown in Fig. 17-12, enter the license in [authorization code] box (authorization code format "license:XXX"), and click on <update>.

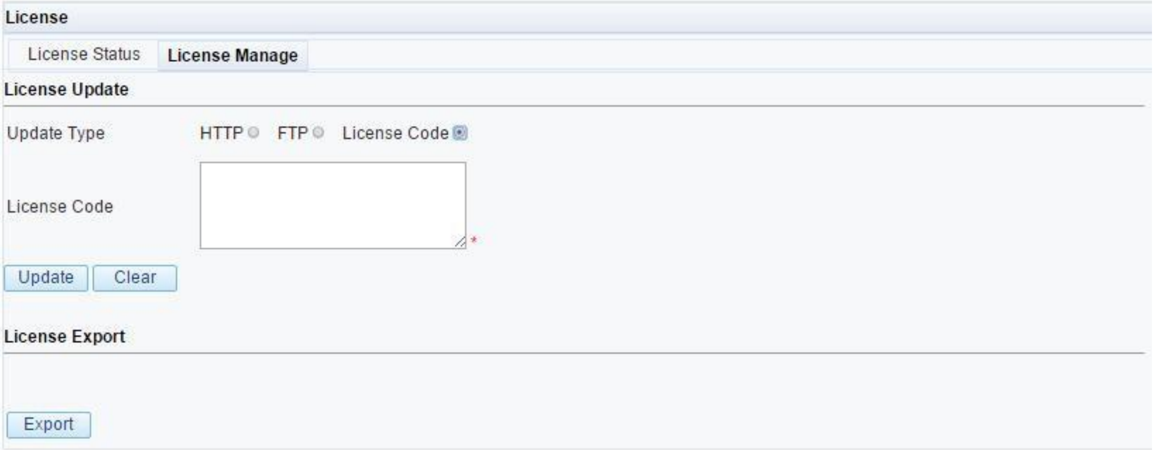


Fig. 17-12 License Import through Authorization Code Update

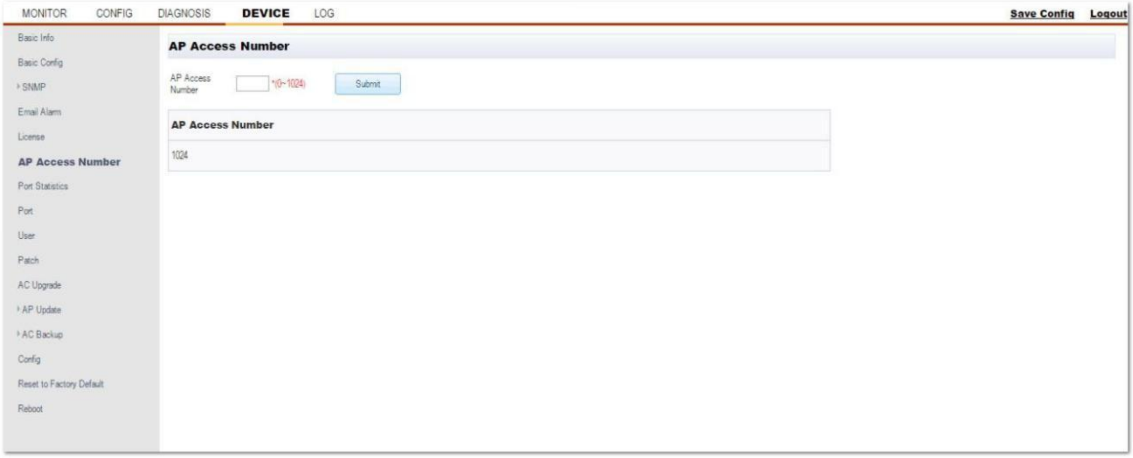
- License Export

The license export page is shown in Fig. 17-12; user could click on <export> to export the license file of service board to management PC for local backup.

Note: License management for frame-type AC; each service board has its own license, and the configuration page offers slot information selection; when updating and exporting license file, user could select the service board in corresponding slot. In addition, [License state] shows the license state information of all service boards.

17.4 The Number of APs Connected

The max. number of APs connected is subject to license, and the max. number of APs connected must not exceed the license limit; user could define the number of registered online APs by setting the number of APs connected. Please refer to Fig. 17-13 for configuration page for the number of APs connected.



AP Access Number

AP Access Number *(0~1024)

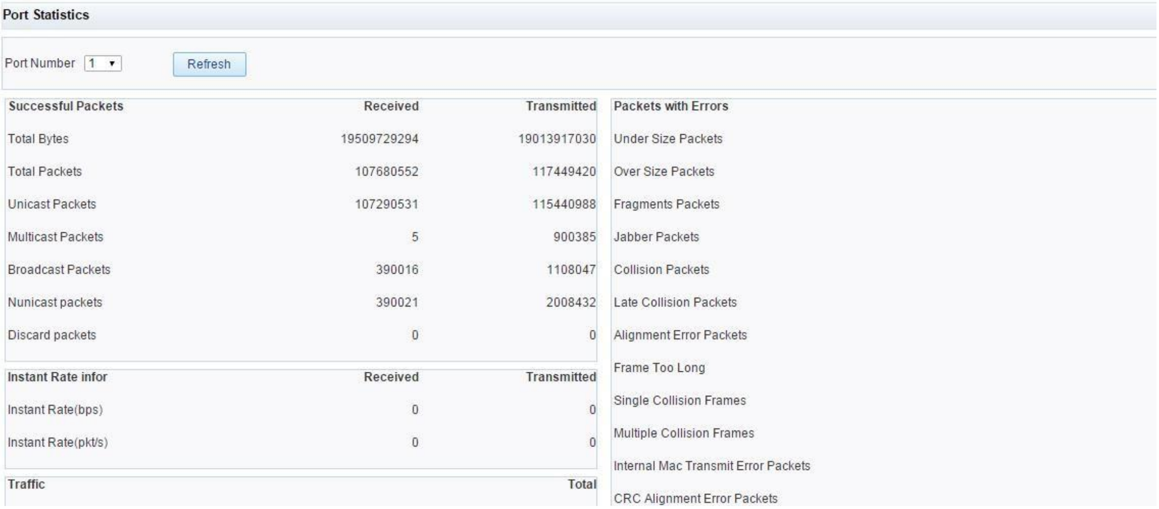
AP Access Number
1024

Fig. 17-13 The Number of APs Connected

Note: The setup page for the number of APs connected to frame-type AC; the limit could be defined for each service board; the page shows [slot board] number; user could set target board as needed.

17.5 Port Information

User could view the message receiving/transmitting data status of each physical port on each device in [port information] page as shown in Fig. 17-14.



Port Statistics

Port Number 1

Successful Packets	Received	Transmitted
Total Bytes	19509729294	19013917030
Total Packets	107680552	117449420
Unicast Packets	107290531	115440988
Multicast Packets	5	900385
Broadcast Packets	390016	1108047
Nunicast packets	390021	2008432
Discard packets	0	0

Instant Rate infor	Received	Transmitted
Instant Rate(bps)	0	0
Instant Rate(pkt/s)	0	0

Traffic	Total

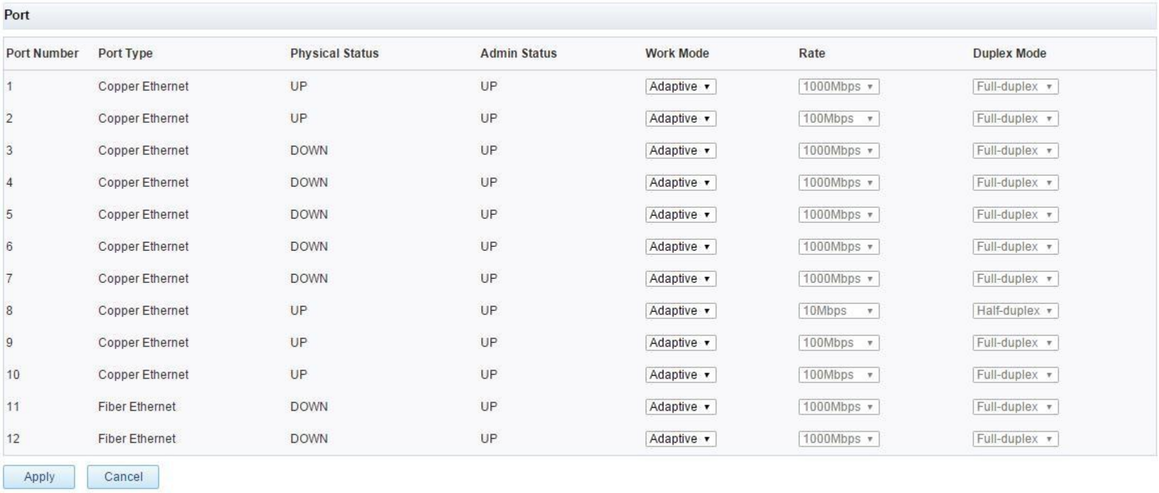
Packets with Errors
Under Size Packets
Over Size Packets
Fragments Packets
Jabber Packets
Collision Packets
Late Collision Packets
Alignment Error Packets
Frame Too Long
Single Collision Frames
Multiple Collision Frames
Internal Mac Transmit Error Packets
CRC Alignment Error Packets

Fig. 17-14 Port Information

Note: The port information page of frame-type AC shows the combination of [slot number] and [port], which enables user to view port information by selecting the service board and physical port of corresponding slot.

17.6 Port Management

In the [port management] page, user could view the type, physical state and management state of physical port, and configure the operating mode, rate and duplex mode of port. Please refer to Fig. 17-15



Port Number	Port Type	Physical Status	Admin Status	Work Mode	Rate	Duplex Mode
1	Copper Ethernet	UP	UP	Adaptive	1000Mbps	Full-duplex
2	Copper Ethernet	UP	UP	Adaptive	100Mbps	Full-duplex
3	Copper Ethernet	DOWN	UP	Adaptive	1000Mbps	Full-duplex
4	Copper Ethernet	DOWN	UP	Adaptive	1000Mbps	Full-duplex
5	Copper Ethernet	DOWN	UP	Adaptive	1000Mbps	Full-duplex
6	Copper Ethernet	DOWN	UP	Adaptive	1000Mbps	Full-duplex
7	Copper Ethernet	DOWN	UP	Adaptive	1000Mbps	Full-duplex
8	Copper Ethernet	UP	UP	Adaptive	10Mbps	Half-duplex
9	Copper Ethernet	UP	UP	Adaptive	100Mbps	Full-duplex
10	Copper Ethernet	UP	UP	Adaptive	100Mbps	Full-duplex
11	Fiber Ethernet	DOWN	UP	Adaptive	1000Mbps	Full-duplex
12	Fiber Ethernet	DOWN	UP	Adaptive	1000Mbps	Full-duplex

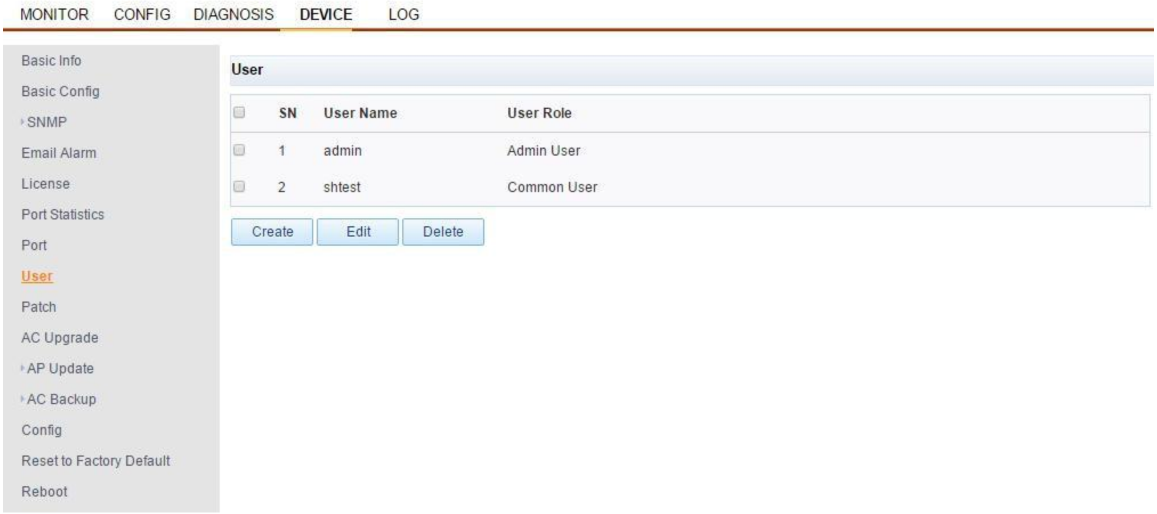
Fig. 17-15 Port Management

- Physical ports of wireless controller AC are divided into Gbps electrical port and Gbps optical port, and all the ports function adaptively.

- Gbps optical port functions adaptively by default, and does not support mandatory 100Mbps/10Mbps duplex & half-duplex mode. The physical port type of frame-type AC is dependent on attributes of the daughter card accompanying the service board. It's composed of Gbps electrical port, Gbps optical port and 10-gigabit card. The system automatically identifies the attribute and type of physical port based on the accompanying daughter card.

17.7 User Management

User could configure administrator account through [user management]. The default super administrator account is "admin"; this default account number can't be deleted, but its password could be modified. Please refer to Fig. 17-16.

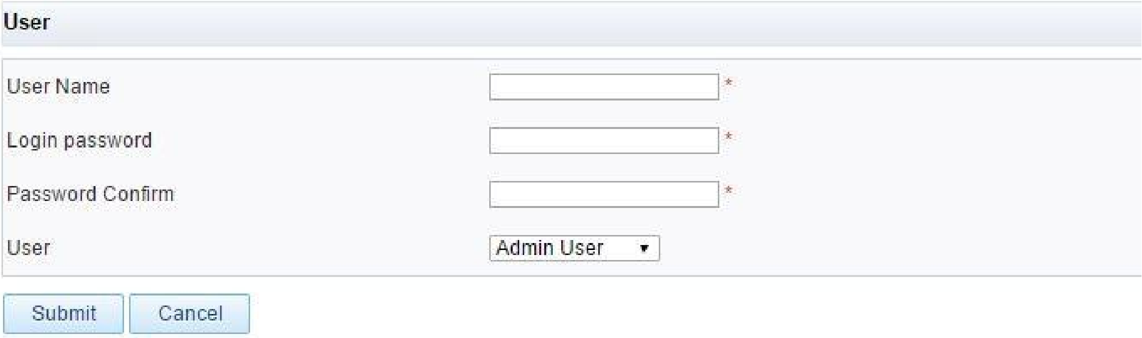


□	SN	User Name	User Role
□	1	admin	Admin User
□	2	shtest	Common User

Fig. 17-16 User Management

17.7.1 Create Administrator User

User could log into device with super administrator account "admin"; click on the <create> button in the page as shown in Fig. 17-16 to open the page shown in Fig. 17-17, where user could add other administrator accounts by entering parameters.



User

User Name	*
Login password	*
Password Confirm	*
User	Admin User

Fig. 17-17 Create Administrator Account

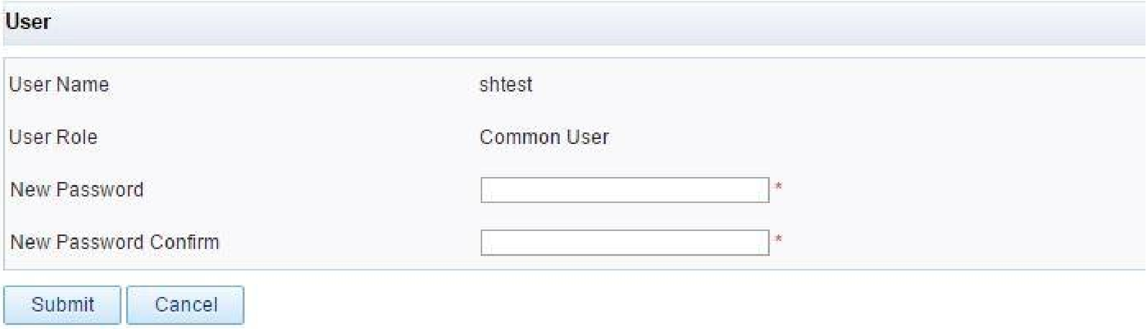
Please refer to Table 17-5 for parameter description of administrator account creation page.

Configuration Item	Description
User Name	Administrator account name
Login Password	Administrator login password
Password Confirmation	"Password confirmation" must keep in line with "login password"
User Management	Administration authority is divided into "common user" and "administrator"; "administrator" has a higher purview than "common user", and could delete "common user" account

Table 17-5 Parameter Description for Administrator Account Creation Page

17.7.2 Edit User Management

In the page as shown in Fig. 17-16, user could select the administrator user information to be edited, and click on <edit> button to modify the password for administrator account as shown in Fig. 17-18.



User

User Name	shtest
User Role	Common User
New Password	*
New Password Confirm	*

Fig. 17-18 Edit User Management

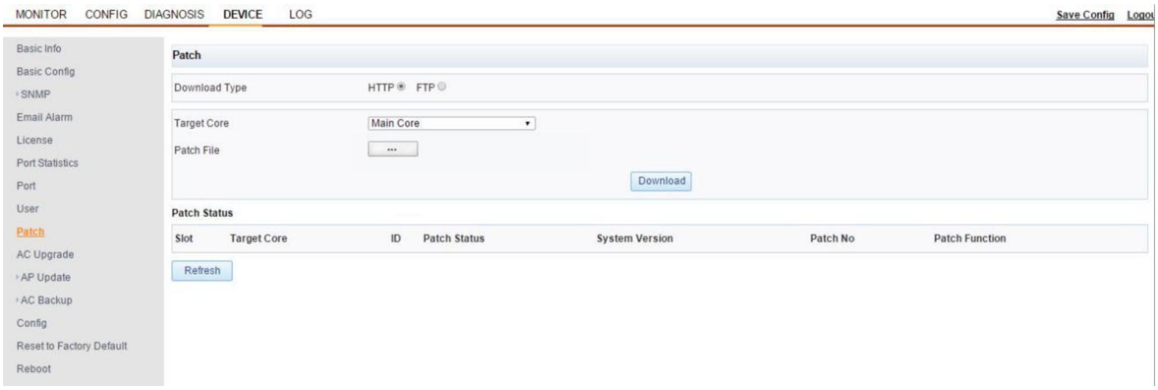
17.7.3 Delete User Management

In the page as shown in Fig. 17-16, user could select the administrator user information to be deleted, and click on <delete> button.

Note: Administrator information could be collectively deleted, but the administrator for "common user" can't delete the users with "administrator" purview. "admin" administrator can't be removed.

17.8 Hot Patching

Hot patching is an efficient cost-effective method for repairing product software version. As compared with software version upgrade, hot patching does not interrupt the running service in device, which is to say, the defect of current software version could be repaired without rebooting the device. The configuration page is as shown in Fig. 17-19.



Patch

Download Type HTTP ● FTP ○

Target Core Main Core

Patch File

Patch Status

Slot	Target Core	ID	Patch Status	System Version	Patch No	Patch Function

Fig. 17-19 Hot Patching

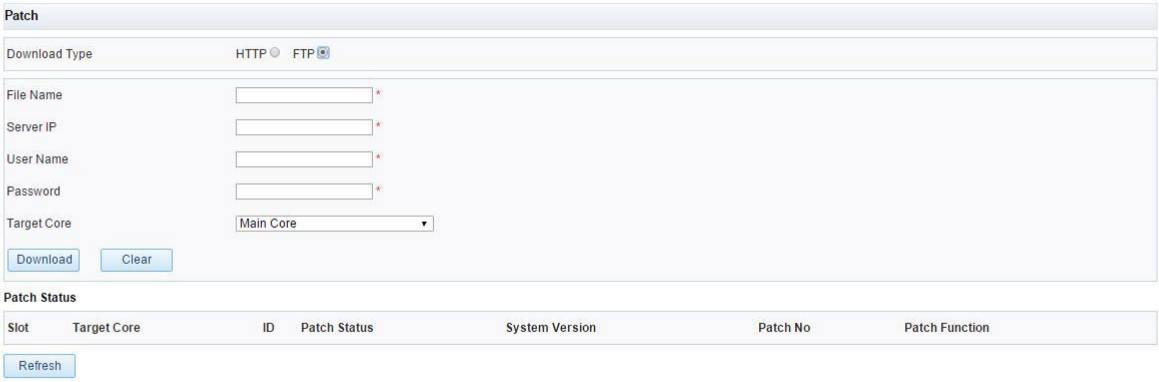
17.8.1 Download Patch through HTTP

The [download patch through HTTP] page is shown in Fig. 17-19; user could set [download mode] to "HTTP", set [target core] to "master core" or "slave core", click on the <browse> button behind [patch file] input box, select the local patch file for wireless controller AC in management PC, and click on <download> button to download patch file; besides, user could learn about patch details in [patch state] page.

Note: For frame-type AC, corresponding board to be patched could be selected in [target board] of this page.

17.8.2 Download Patch through FTP

The [download patch through FTP] page is as shown in Fig. 17-20; user needs an external FTP server directed to patch file path, and could then set the [file name], [server IP], [user name], [password] and [target core], and click on <download>.



Patch

Download Type HTTP ○ FTP ●

File Name *

Server IP *

User Name *

Password *

Target Core Main Core

Patch Status

Slot	Target Core	ID	Patch Status	System Version	Patch No	Patch Function

Fig. 17-20 Download Patch through FTP

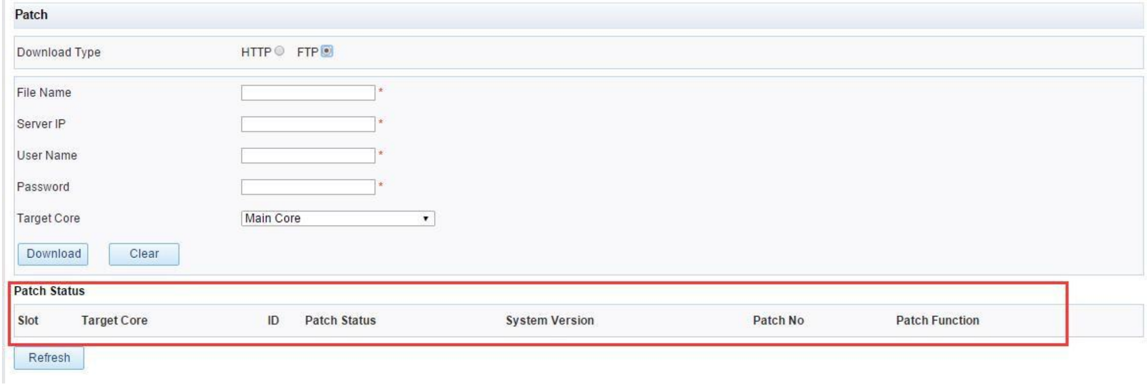
Please refer to Table 17-6 for parameter description of "download patch through FTP".

Configuration Item	Description
File Name	The patch file name corresponding to the board to be patched
Server IP	The FTP server IP address for device to get patch file
User Name	FTP's user name
Password	Password of FTP
Target Core	Select the core type ("master core" and "slave core") for the board to be patched; patch file varies depending on core type

Table 17-6 Parameter Description of Download Patch through FTP

Note: For frame-type AC, corresponding board to be patched could be selected in [target board] of this page.

Upon completion of successful patch download, the information in [patch state] is as shown in Fig. 17-21.



Patch

Download Type ○ HTTP ● FTP

File Name

Server IP

User Name

Password

Target Core: Main Core

Patch Status

Slot	Target Core	ID	Patch Status	System Version	Patch No	Patch Function

Fig. 17-21 Patch State

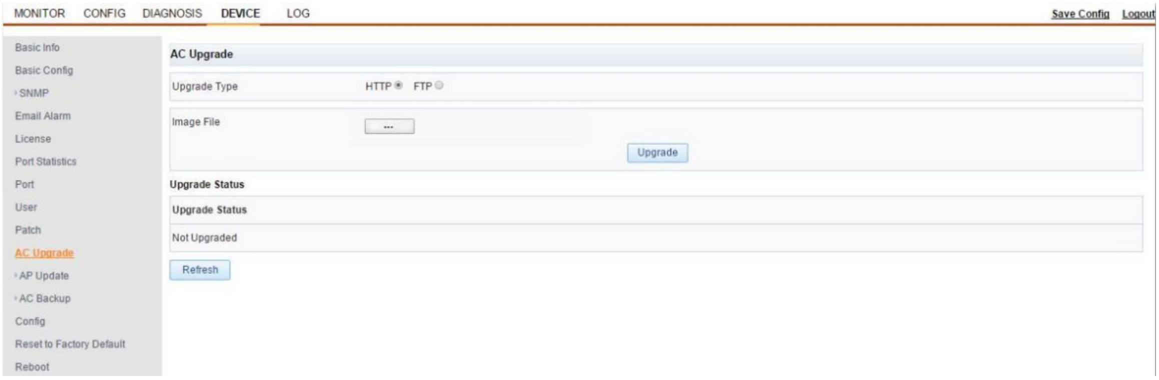
Please refer to Table 17-7 for patch state parameter description.

Configuration Item	**Description**
Activation	Activate the patch, i.e. temporary running state; the patch is no longer valid after device restart, and thus need to be reactivated
Run	"Permanent running patch", which is to say, the patch is valid even after device restart
Delete	Delete patch

Table 17-7 Patch State Parameter Description

17.9 Software Upgrade

The software upgrade page is as shown in Fig. 17-22; the upgrade methods include HTTP upgrade and FTP upgrade; the "upgrade state" shows whether or not each board is successfully upgraded.



AC Upgrade

Upgrade Type ● HTTP ○ FTP

Image File

Upgrade Status

Upgrade Status
Not Upgraded

Fig. 17-22 Software Upgrade

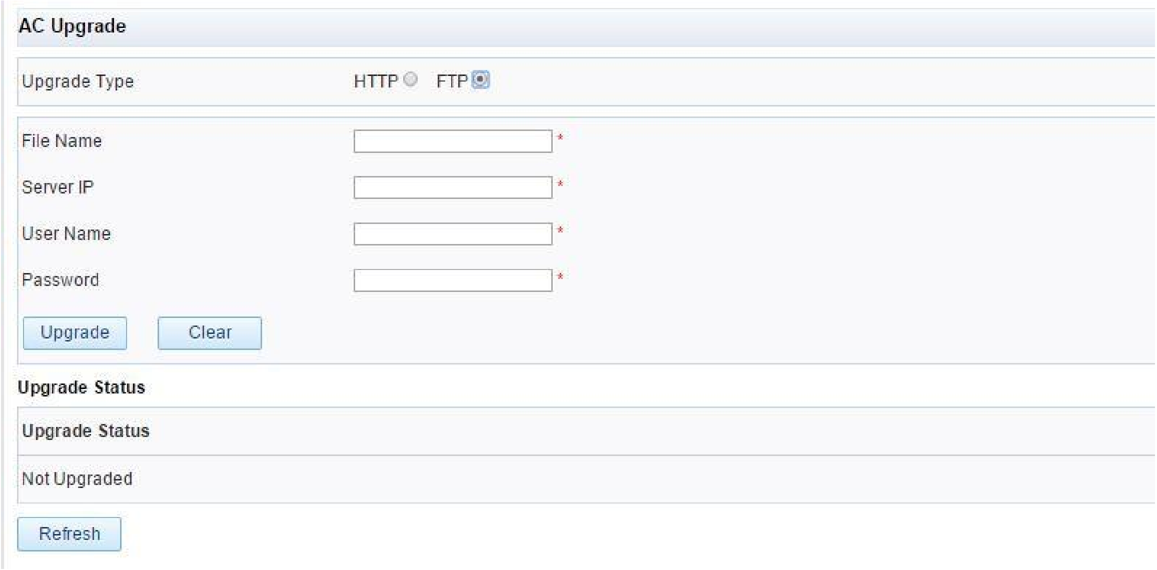
17.9.1 HTTP Upgrade

The [HTTP upgrade] page is shown in Fig. 17-22; user could set [upgrade mode] to "HTTP", click on the <browse> button behind [image file name] input box, select the local software image file for wireless controller AC in management PC, and click on <upgrade> button; besides, user could learn about upgrade details in [upgrade state] page.

Note: For frame-type AC, corresponding board could be selected in [target board] of this page for image file upgrade.

17.9.2 FTP Upgrade

The [FTP upgrade] page is as shown in Fig. 17-23; user needs an external FTP server directed to image file path, and could then set the [file name], [server IP], [user name] and [password] in "FTP upgrade page", and click on <upgrade>.



AC Upgrade

Upgrade Type HTTP ○ FTP ●

File Name: *

Server IP: *

User Name: *

Password: *

Upgrade Status

Upgrade Status
Not Upgraded

Please refer to Table 17-8 for FTP software upgrade parameter description.

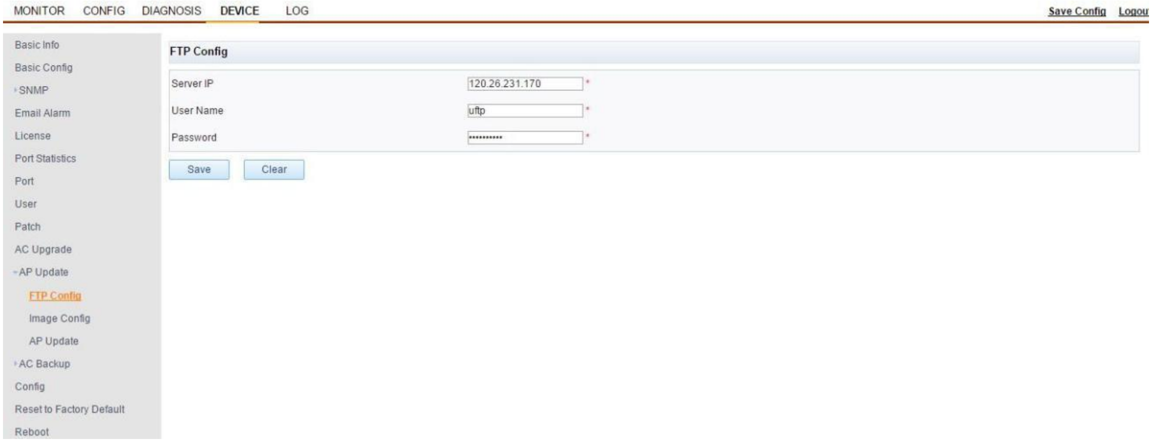
Configuration Item	Description
File Name	Correspond to the software image file name of updated service board
Server IP	The FTP server IP address for device to get software image file
User Name	FTP's user name
Password	Password of FTP

Table 17-8 FTP Software Upgrade Uarameter Description

For frame-type AC, corresponding board could be selected in [target board] of this page for image file upgrade.

17.10 AP Upgrade

[AP upgrade] involves [FTP server configuration], [AP image management] and [AP upgrade]; wireless controller AC upgrades AP through FTP or CAPWAP as shown in Fig. 17-24.



FTP Config

Server IP	120.26.231.170 *
User Name	uftp *
Password	•••••••••• *

Fig. 17-24 AP Upgrade

17.10.1 FTP Server Configuration

FTP upgrade is realized through FTP server, of which the configuration is shown in Fig. 17-24. The FTP server must be accessible to both AC and AP; in the case of FTP upgrade, AC obtains the AP upgrade image file name from FTP server; upon receipt of the upgrade command from AC, AP downloads image file from FTP server. User could enter [server IP], [user name] and [password], and click on <save> button.

17.10.2 AP Image Management

AP image management page is as shown in Fig. 17-25. User could obtain FTP upgrade image or CAPWAP upgrade image through [image acquisition]; after acquiring AP image file, AC shows AP image file information in this page for user to choose corresponding image file so as to upgrade corresponding type of AP.

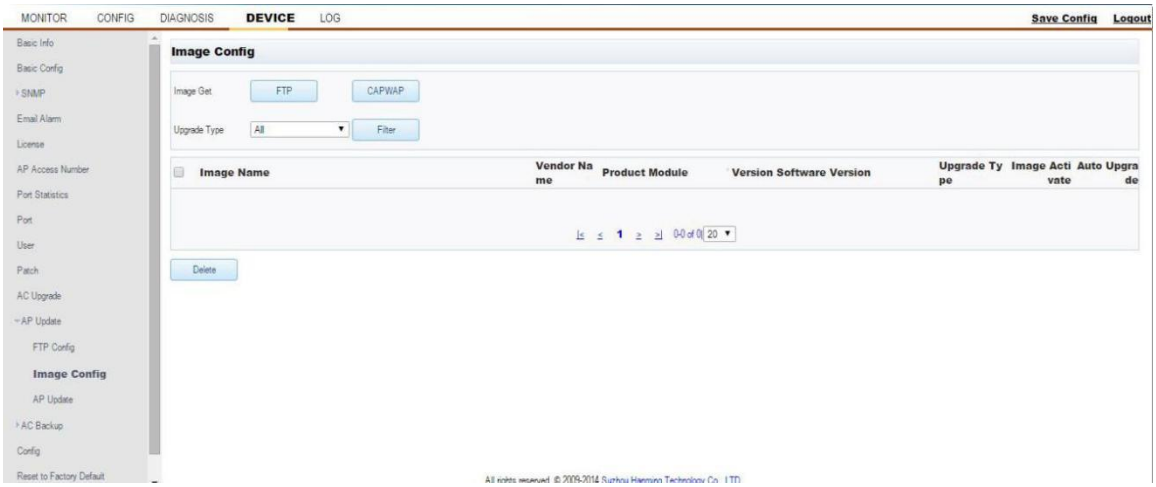


Image Config

Image Get: FTP CAPWAP

Upgrade Type: All

□	Image Name	Vendor Name	Product Module	Version Software Version	Upgrade Type	Image Activate	Auto Upgrade

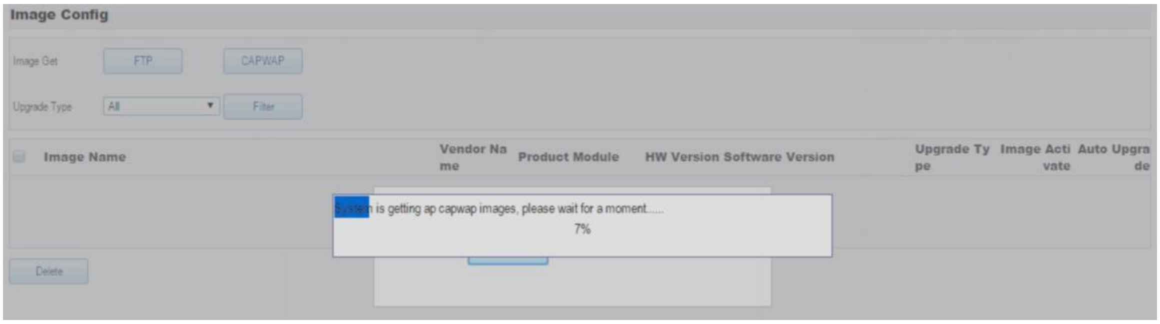
Fig. 17-25 AP Image Management

• Image Acquisition

The image acquisition methods include "FTP image" and "CAPWAP image".

FTP image: Upon the setup of FTP server and the correct configuration of parameters in [FTP server configuration] page, user could put the upgrade image file of AP under FTP's mapping directory, and click on <FTP image> button, when the wireless controller AC would automatically determine AP's image file under FTP server mapping directory, and extract and show the image file name of AP and other information in [AP image management] page.

CAPWAP image: When user clicks on [CAPWAP image], the page offers a dialog box for importing AP image file to wireless controller; user could click on <browse> button, and select and upload the AP's image file to AC as shown in Fig. 17-26. Upon the successful upload of AP image file, the [AP image management] page shows information about AP image file.



System is getting ap capwap images, please wait for a moment......
7%

Fig. 17-26 CAPWAP Image Acquisition

Note: Storage mode of CAPWAP image file in wireless controller: Image file is stored in local FLASH memory in the case of box-type wireless controller and frame-type ST series of wireless controllers. The master control board of frame-type AC shall be provided with CF memory card for storage of AP's image file.

• Delete Image File

User could click on <delete> button in the page as shown in Fig. 17-25 to delete the information about AP image file acquired by ftp or the AP image file acquired through CAPWAP and its information. Since the AP image file for CAPWAP image upgrade is stored locally in wireless controller AC, user must check the storage space available and delete old AP image file if necessary when uploading new AP image file.

• Image File Information Filter Criteria

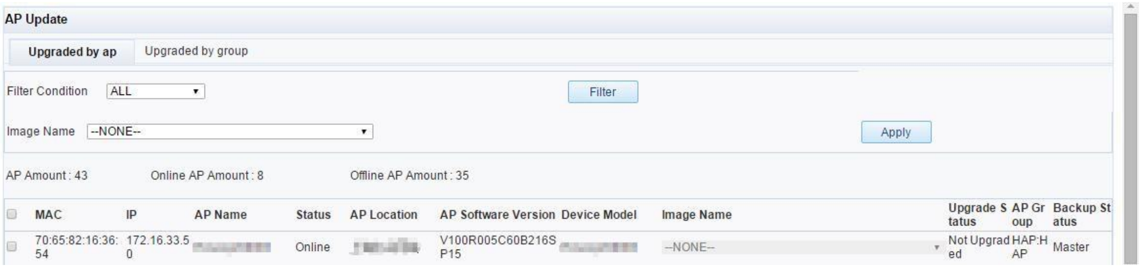
For the image file in [AP image management] page, the filter criteria [upgrade type] could be used to screen the mirror image record information to be displayed. [Upgrade type] parameter is set to "all" by default; user could filter images by "FTP upgrade" and "CAPWAP upgrade".

• AP Image File Activation

The image file list in [AP image management] page only shows the management of AP image file information by wireless controller; the AP image can't be used for AP upgrade in [AP upgrade] page unless the image file of [AP image management] is [activated].

17.10.3 AP Upgrade

[AP upgrade] includes [AP-based upgrade] and [AP group-based upgrade] as shown in Fig. 17-27.



AP Update

Filter Condition ALL ▾ Filter

Image Name --NONE-- ▾ Apply

AP Amount : 43   Online AP Amount : 8   Offline AP Amount : 35

□	MAC	IP	AP Name	Status	AP Location	AP Software Version	Device Model	Image Name	Upgrade Status	AP Group	Backup Status
□	70:65:82:16:36:54	172.16.33.50	[redacted]	Online	[redacted]	V100R005C60B216SP15	[redacted]	--NONE-- ▾	Not Upgraded	HAP:HAP	Master

Fig. 17-27 AP Upgrade

- AP-based Upgrade

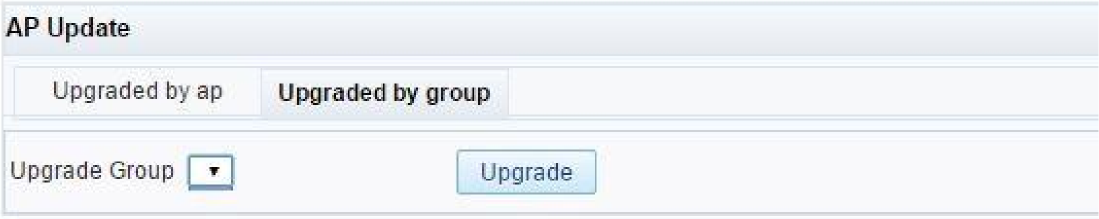
[AP-based upgrade]: In the case of go-on-line registration of AP at wireless controller AC, the [AP-based upgrade] page shows the information about all online APs. To upgrade a certain AP, user could choose the AP to be upgraded and the upgrade image, and click on <upgrade> button. User could view AP upgrade process through [upgrade state].

User could select several online AP records, select the AP image file in [image name], and click on <apply> button, when all selected APs are associated with this AP image file; click on <upgrade> button for batch upgrade of APs.

- AP group-based Upgrade

[AP group-based upgrade]: Upon the go-on-line registration of AP at wireless controller, user could configure AP group in “[network configuration] > [WLAN configuration] > [AP group]", select the AP image file, and add the online AP to AP group in “[network configuration] > [WLAN configuration] > [AP configuration]".

In the “[device management] > [AP upgrade] > [AP group-based upgrade]" page, user could select the AP group to be upgraded in [upgrade group], and click on <upgrade> button to upgrade all APs in the AP group as shown in Fig. 17-28.



AP Update

Upgrade Group ▾ Upgrade

Fig. 17-28 AP Group-based Upgrade

• Description of FTP Upgrade and CAPWAP Upgrade Process

FTP upgrade process: Wireless controller obtains AP's Image file information from FTP-SERVER mapping directory through FTP, including the identified name and version of image file etc. Then, the wireless controller issues the CAPWAP control message command to selected online AP based on user's configuration so as to determine the AP image file to be upgraded. Upon receipt of upgrade command message from wireless controller, AP automatically downloads AP image file from FTP-SERVER, and then performs upgrading automatically; upon successful upgrading, AP sends the message of successful upgrade back to wireless controller. Then, the [upgrade state] in [AP upgrade] page of wireless controller AC shows the text "UPGRADE SUCCEEDED".

CAPWAP upgrade process: Wireless controller uploads AP's upgrade file to its local memory (FLASH or CF card) through HTTP; when user issues CAPWAP upgrade command to AP, the wireless controller issues an upgrade command to the AP, when AP image file is transferred to the to-be-upgraded AP through CAWAP message encapsulation. Upon the completion of downloading image file from wireless controller AC, the AP is automatically upgraded. Upon successful upgrading, the AP sends the message of successful upgrade back to wireless controller.

Note: For AP upgrade, the wireless controller AC checks the version information of image file and AP; provided that the image file version is the same with AP version or that the device model information fails to match with image information, the AP will not be upgraded, when a corresponding prompting message is displayed.

• Automatic Upgrade

Wireless controller AC could automatically upgrade AP. Upon the go-on-line registration of AP at wireless controller, user could configure AP group in “[network configuration] > [WLAN configuration] > [AP group]", select the AP image file, and add the online AP to AP group in "[network configuration] > [WLAN configuration] > [AP configuration]". Set the [auto upgrade] of AP image file referenced by AP group to "enabled" state in the “[device management] > [AP upgrade] > [AP image management]" page as shown in Fig. 17-29.

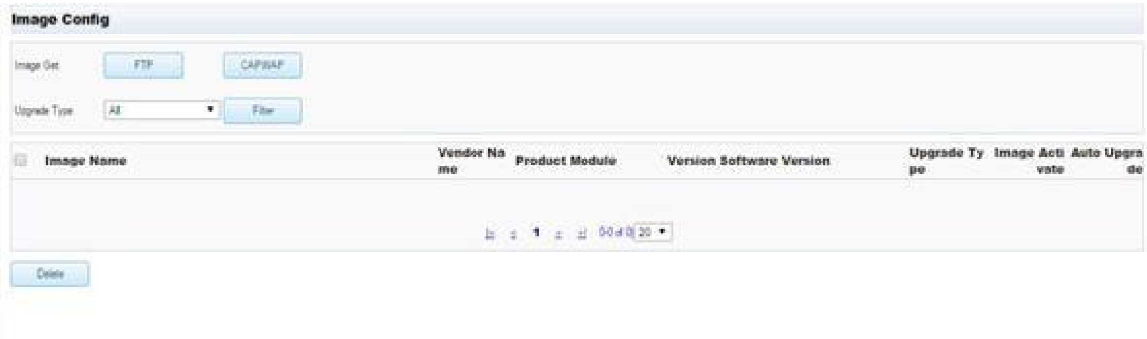


Image Config

Image Get

Upgrade Type: All

□	Image Name	Vendor Name	Product Module	Version Software Version	Upgrade Type	Image Activate	Auto Upgrade

Fig. 17-29 Auto Upgrade

17.11 Configuration Management

User could export configuration and import configuration through HTTP and FTP in [configuration management] page as shown in Fig. 17-30.

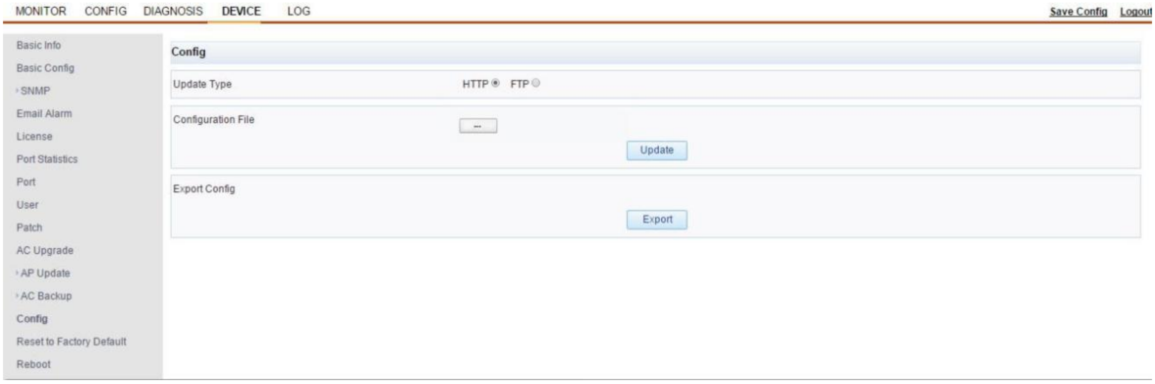


Fig. 17-30 Configuration Management

17.11.1 Update Configuration File through HTTP

Import configuration through HTTP, set [update mode] to "HTTP", click on <browse> button behind the [configuration file name] input box, select the local configuration file of management PC as shown in Fig. 17-31, and click on <update> to import configuration file. A prompting message is displayed upon successful import; the imported configuration file takes effect after rebooting the device.

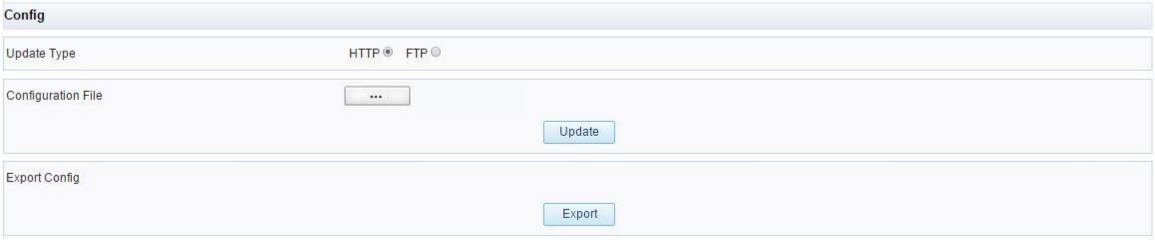


Fig. 17-31 Update Configuration File through HTTP

17.11.2 Update Configuration File through FTP

In the [configuration management] page as shown in Fig. 17-30, set the [update mode] to "FTP" so as to update configuration file through FTP as shown in Fig. 17-32; user could set up FTP-SERVER, put the configuration file in mapping directory, properly enter the configuration parameter information of FTP, and click on <update> button to upload the configuration file to wireless controller for configuration update; user could restart the device based on the prompting message upon successful update so as to bring the configuration into effect.

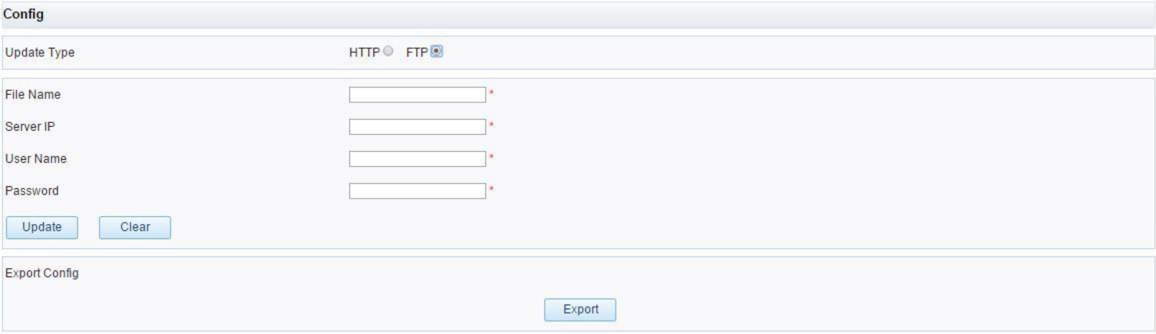


Fig. 17-32 Update Configuration File through FTP

17.11.3 Export Configuration

Click on <export> button in [configuration management] page, when the browser indicates the text reading "select save path"; the configuration file could be saved locally in management PC. Back up the configuration data as shown in Fig. 17-33.

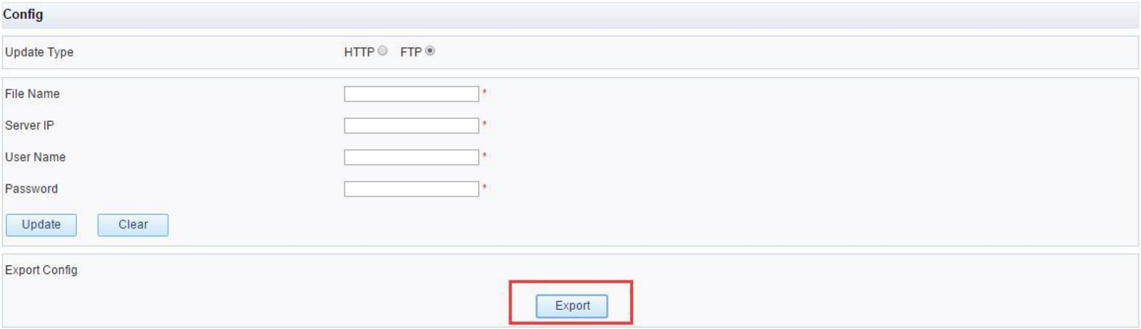


Fig. 17-33 Export Configuration

17.12 Restore Factory Default

User could click on <factory reset> button in the “[configuration management] > [restore factory default]" page to restore factory default of the device as shown in Fig. 17-34.

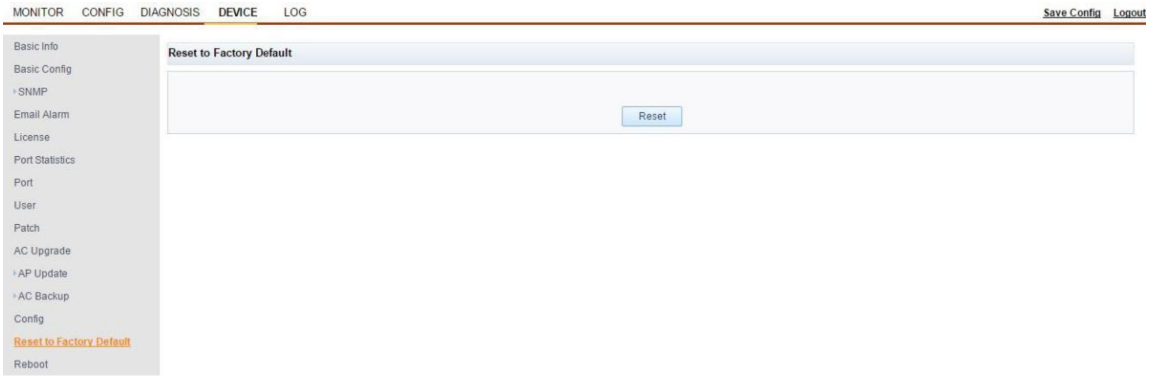


Fig. 17-34 Restore Factory Default

Warning: The factory default of on-stream device in network shall be restored with caution.

17.13 System Reboot

User could click on <reboot> button in the "[configuration management] > [system reboot]" page to reboot the device as shown in Fig. 17-35.

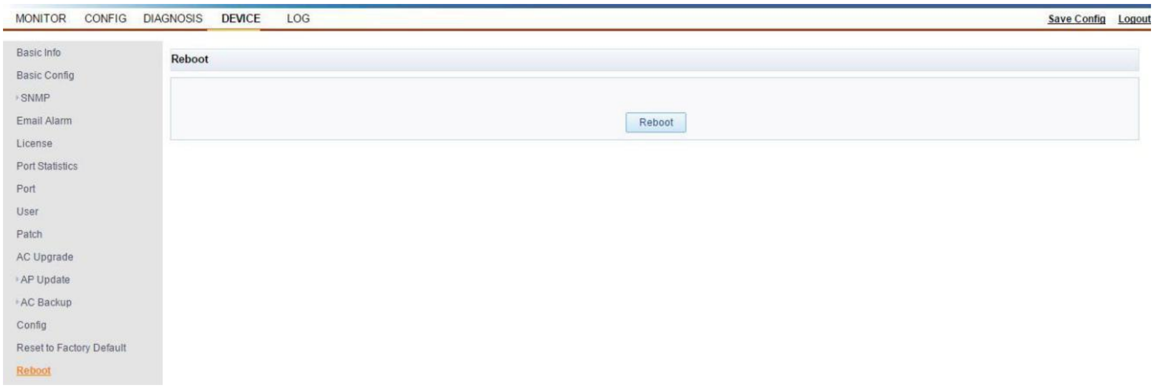


Fig. 17-35 System Reboot

Warning: The on-stream device in network shall be rebooted with caution.

17.14 Save Configuration

User could click on the <save configuration> button at upper right corner of the wireless controller management page as shown in Fig. 17-36 to save the configured data; the configured user data will not get lost after device reboot.

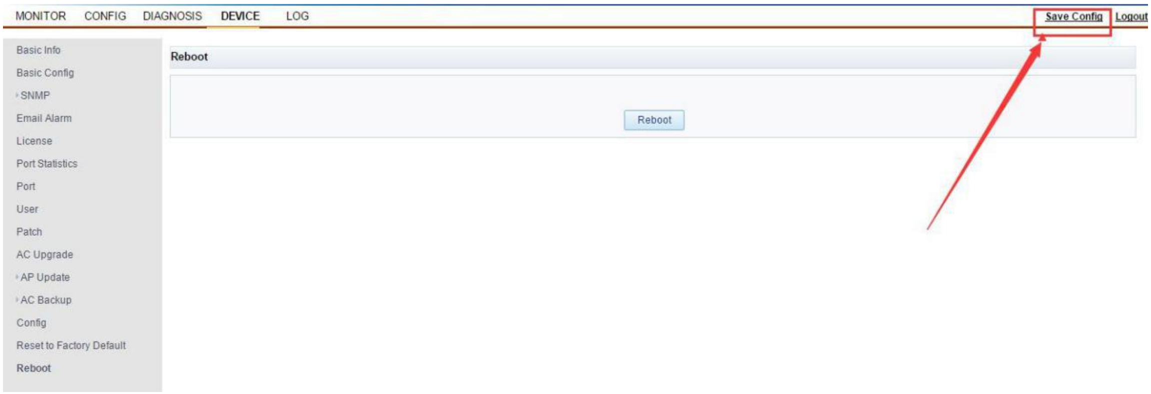
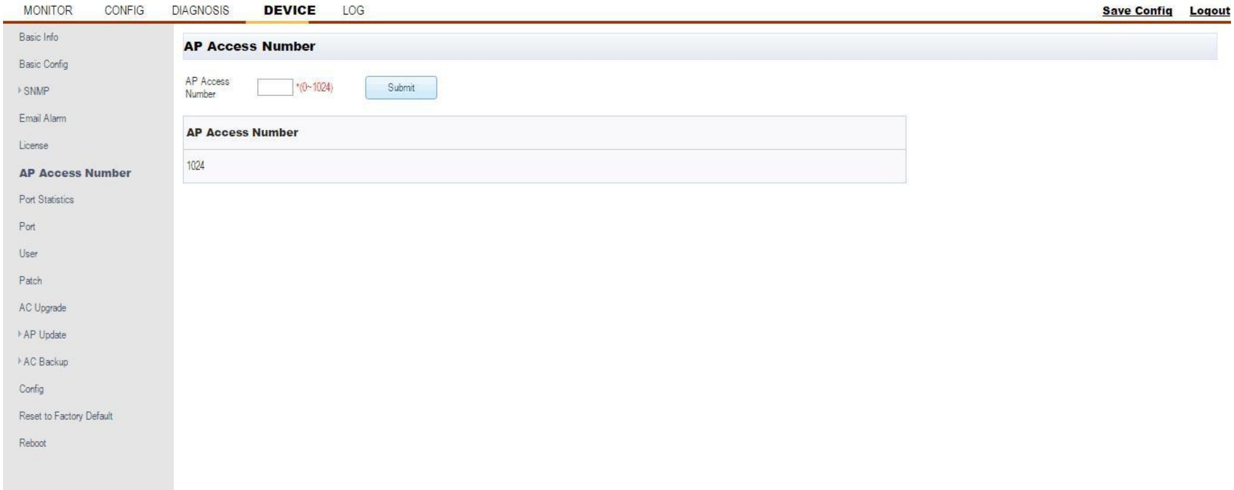


Fig. 17-36 Save Configuration

17.5 Logout

User could click on the <logout> button at upper right corner of the wireless controller management page as shown in Fig. 17-37, when the administrator account logs out of wireless controller AC's main management interface, and the login page appears.



AP Access Number

AP Access Number *(0~1024)

AP Access Number
1024

Fig. 17-37 Logout

Chapter 18 SNMP management

18.1 SNMP overview

(1) Automatic network management: Through nodes of the SNMP platform on networks, network administrators can search and modify information, discover and diagnose faults, realize capacity planning and generate reports.

(2) Shielding the physical differences of different devices and realizing automatic management for the products of different manufacturer: SNMP can manage the devices of different manufacturer because it provides the most basic function sets only and management tasks are relatively independent from the physical features of managed devices and the networking technologies of lower layers. Thus, SNMP is particularly suitable for small, fast and low-cost networks.

- Operating mechanism of SNMP

SNMP network elements include NMS and Agent.

NMS (Network Management Station) is a workstation for running SNMP client program. It can provide friendly human-machine interfaces to make it convenient for network administrators to realize most of network management.

Agent is a process on a device. It receives and processes the request messages from NMS. In some emergencies such as shown interface status changes, it inform NMS of them automatically.

In an SNMP network, NMS serves as the administrator and Agent the managed object. Management message interaction between NMS and Agent is realized through SNMP.

- Four basic operations of SNMP

Get: For NMS to query the value of a variable of Agent

Set: For NMS to reset the values of one or multiple objects in the Agent database (MIB, Management Information Base)

Trap: For Agent to send alarm messages to NMS

Inform: For NMS to send alarm messages to other NMSs

- Version of SNMP

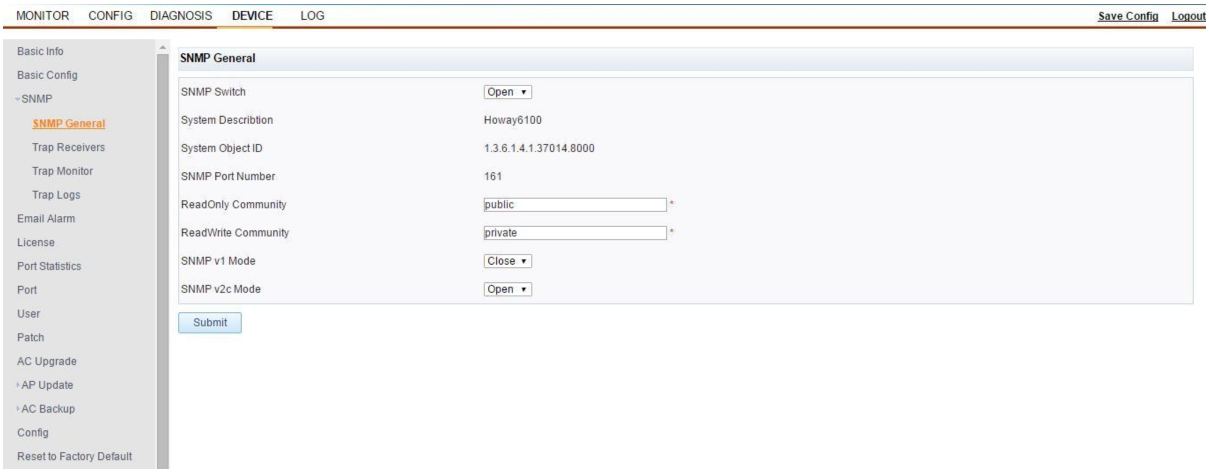
At present, wireless controller (AC) of the device supports SNMP v1/v2c version.

SNMP v1 realizes authentication through a community name. The community name defines the relation between NMS and Agent of SNMP. If the community name of a message is not authenticated by the device, the message will be discarded. The community name serves like a password for restricting the access of NMS to Agent.

SNMP v2 realizes authentication through a community name too. It is compatible with SNMP v1 and has the extra functions as below: more operation types (GetBulk and InformRequest), more data types (such as Counter64) and more error codes for better error distinguishing.

18.2 SNMP management configuration

As shown in Fig. 18-1, the management configuration of ”SNMP” includes “SNMP General”, “TRAP Receivers”, “TRAP Monitor” and ”TRAP Logs”.



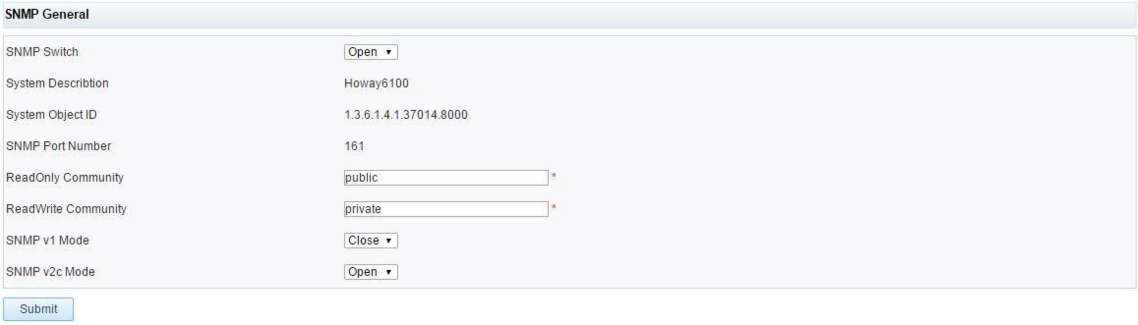
SNMP General

SNMP Switch	Open ▾
System Describtion	Howay6100
System Object ID	1.3.6.1.4.1.37014.8000
SNMP Port Number	161
ReadOnly Community	public *
ReadWrite Community	private *
SNMP v1 Mode	Close ▾
SNMP v2c Mode	Open ▾

Fig. 18-1 SNMP Management Configuration

18.2.1 SNMP General

See Fig. 18-2 page. The SNMP service is disabled by default.



SNMP General

SNMP Switch	Open ▾
System Describtion	Howay6100
System Object ID	1.3.6.1.4.1.37014.8000
SNMP Port Number	161
ReadOnly Community	public *
ReadWrite Community	private *
SNMP v1 Mode	Close ▾
SNMP v2c Mode	Open ▾

Fig. 18-2 SNMP General

See Table 18-1 for the parameters.

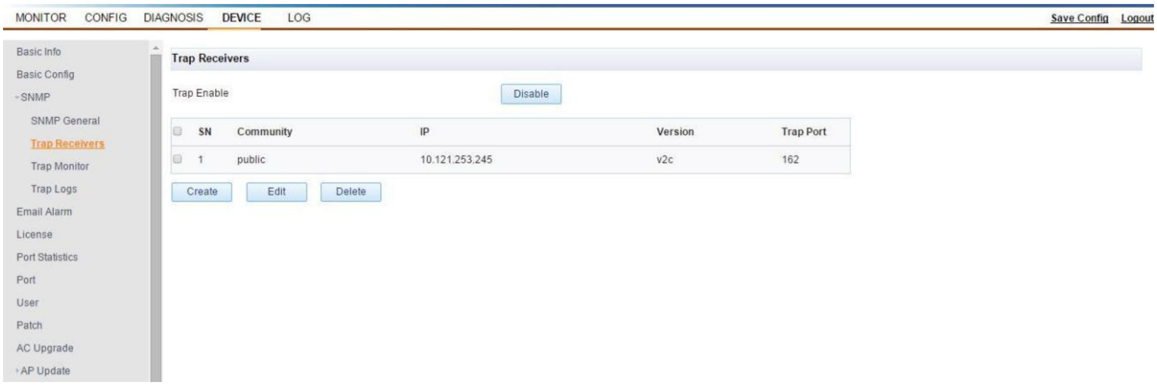
Configuration Item	Description
SNMP Switch	Enable switch for SNMP (default: "Close")
System Description	Description of the system name (values are identified by the system automatically, depending on the device model)
System Node	OID number of the manufacturer (self-contained information of the system)
Port No.	Communication port of SNMP (default: 161)
Read Only Community	Password for the read-only access of NMS to Agent
Read/Write Community	Password for the read-write access of NMS to Agent
SNMP v1 Mode	Enable switch for the SNMP v1 mode
SNMP v2c Mode	Enable switch for the SNMP v2c mode

Table 18-1 Parameters of SNMP

18.2.2 TRAP Receivers

Fig. 18-3 shows the TRAP receiver configuration page. On this page, the TRAP receiver configuration can be changed through buttons " Create", " Edit" and " Delete"; the AC can be configured with multiple server addresses to receive TRAP messages and send TRAP messages to multiple SNMP servers.

To enable the TRAP configuration, enable the SNMP configuration service on the page as shown in Fig. 18-2 and the TRAP switch in sequence.



Trap Receivers

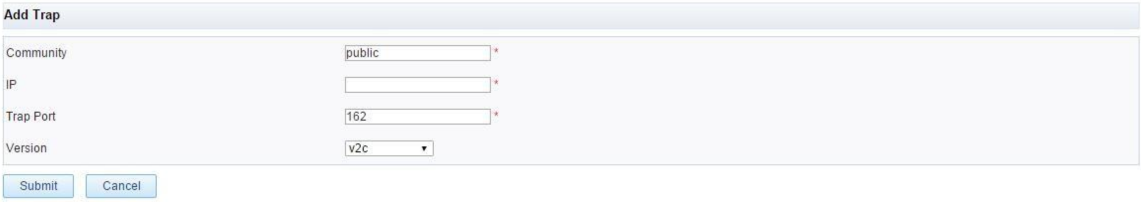
Trap Enable

□	SN	Community	IP	Version	Trap Port
□	1	public	10.121.253.245	v2c	162

Fig. 18-3 TRAP Receivers

Create

Click "Create" on the page as shown in Fig. 18-3. Configure correct TRAP parameters on the page as shown in Fig. 18-4 appearing later.



Add Trap

Community	public *
IP	*
Trap Port	162 *
Version	v2c ▼

Fig. 18-4 Create TRAP Receiver

See Table 18-2 for the parameters.

Configuration Item	Description
Community	For SNMP authentication from NMS via Agent. If network authentication is necessary according to the configuration, Agent will authenticate the community name and the NMS IP address. If the authentication fails, Agent will send a Trap message about authentication failure to NMS.
IP	Address of the SNMP TRAP server
TRAP Port	Number of the TRAP protocol interaction port (default: 162)
Version	Protocol version of TRAP messages: v1 or v2c

Table 18-2 Parameters for TRAP Receiver Creation

Edit

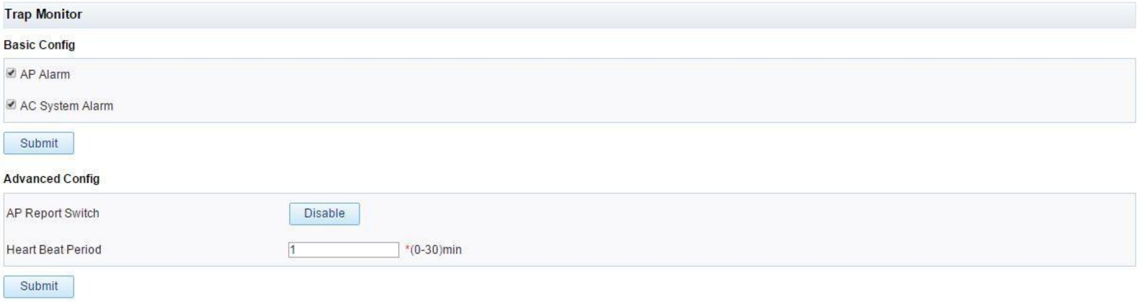
Select the target TRAP receiver data to be edited and click "Edit" to edit the content of "Community", "IP", "TRAP Port" or "Version".

Delete

Select the target TRAP receiver data to be deleted and click "Delete". The deletion can be done in batches.

18.2.3 TRAP Monitor

As shown in Fig. 18-5, the message types under "Trap Monitor" include "AP Alarm" and "AC System Alarm". User can "AP Alarm" to upload a TRAP alarm on the AP to the SNMP server, or " AC System Alarm" to upload a TRAP alarm on the AC to the SNMP server.



Trap Monitor

Basic Config

☑ AP Alarm

☑ AC System Alarm

Submit

Advanced Config

AP Report Switch: Disable

Heart Beat Period: 1 *(0-30)min

Submit

Fig. 18-5 TRAP Monitor

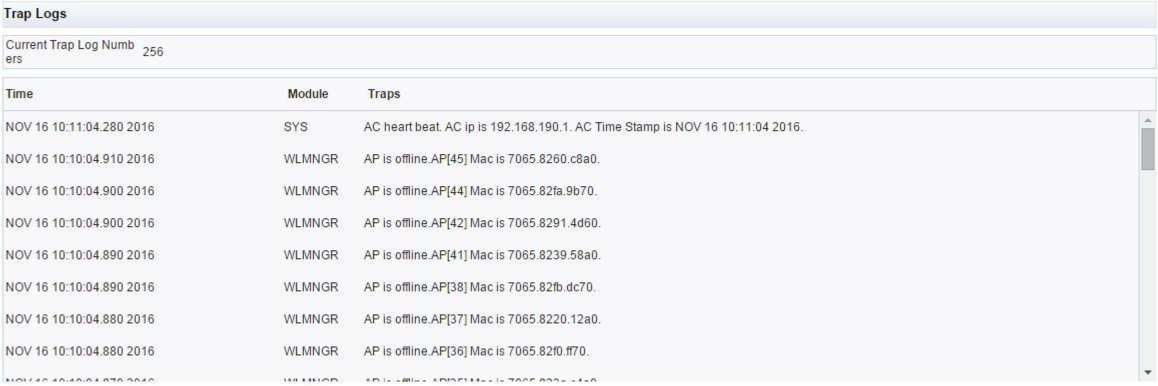
See table 18-3 Parameters of Trap Monitor.

Configuration Item	Description
AP Alarm	For setting the necessity or unnecessity for the AC to monitor AP alarms
AC System Alarm	For setting the necessity or unnecessity for the AC to monitor AC system alarms
AP Report Switch	Enable/disable
AC Heart Beat Period	Period of sending of heart beat messages by AC

Table 18-3 Parameters of Trap Monitor

18.2.4 TRAP Logs

If “TRAP Receivers” and “TRAP Monitor” have been enabled, user can view trap logs on the “TRAP Logs” page under “SNMP” which is a submenu of “device Management”. See Fig.18-6. “TRAP Logs” can display 256 logs. It can be refreshed via the “Refresh” button to display the latest trap logs. To clear the logs in the log list, click “ Clear”.



Trap Logs

Current Trap Log Numbers 256

Time	Module	Traps
NOV 16 10:11:04.280 2016	SYS	AC heart beat. AC ip is 192.168.190.1. AC Time Stamp is NOV 16 10:11:04 2016.
NOV 16 10:10:04.910 2016	WLMNGR	AP is offline.AP[45] Mac is 7065.8260.c8a0.
NOV 16 10:10:04.900 2016	WLMNGR	AP is offline.AP[44] Mac is 7065.82fa.9b70.
NOV 16 10:10:04.900 2016	WLMNGR	AP is offline.AP[42] Mac is 7065.8291.4d60.
NOV 16 10:10:04.890 2016	WLMNGR	AP is offline.AP[41] Mac is 7065.8239.58a0.
NOV 16 10:10:04.890 2016	WLMNGR	AP is offline.AP[38] Mac is 7065.82fb.dc70.
NOV 16 10:10:04.880 2016	WLMNGR	AP is offline.AP[37] Mac is 7065.8220.12a0.
NOV 16 10:10:04.880 2016	WLMNGR	AP is offline.AP[36] Mac is 7065.82f0.ff70.

Fig. 18-6 TRAP Logs

Chapter 19 Email Alarm

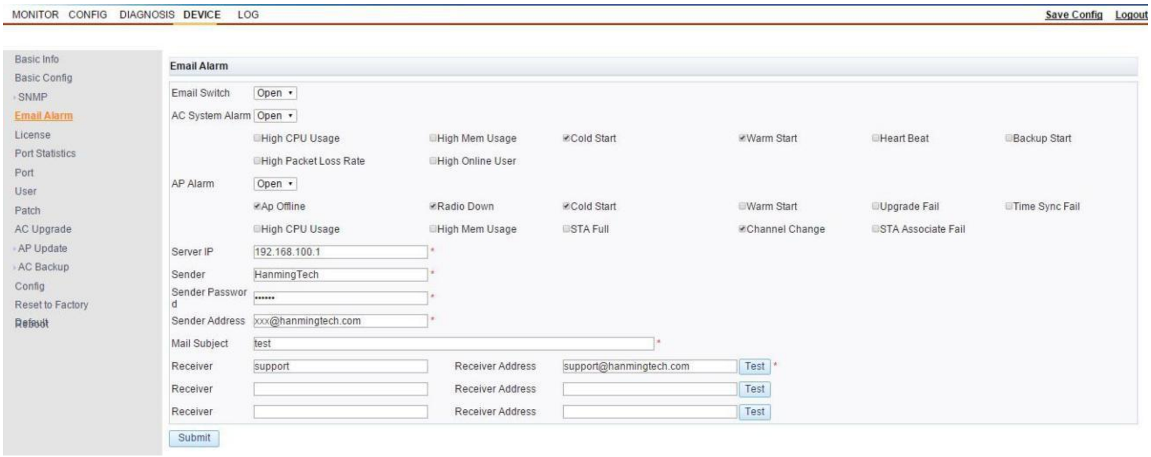
19.1 Overview

In the Email alarm function, the AC customizes alarms and sends them to the given email addresses to inform administrators of the operation faults of AC or the offline events of APs on the networks in time.

The AC sends email alarms through SMTP (Simple Mail Transfer Protocol) which can send emails reliably and efficiently. As an email service based on FTP, SMTP mainly transmits emails between systems and notifies incoming emails.

19.2 Configuration

Email alarm can be configured by the AC as shown in Fig. 19-1.



Email Alarm

Email Switch: Open

AC System Alarm: Open

☐ High CPU Usage ☐ High Mem Usage ☑ Cold Start ☑ Warm Start ☐ Heart Beat ☐ Backup Start

☐ High Packet Loss Rate ☐ High Online User

AP Alarm: Open

☑ Ap Offline ☑ Radio Down ☑ Cold Start ☐ Warm Start ☐ Upgrade Fail ☐ Time Sync Fail

☐ High CPU Usage ☐ High Mem Usage ☐ STA Full ☑ Channel Change ☐ STA Associate Fail

Server IP: 192.168.100.1 *

Sender: HanmingTech *

Sender Password: •••••• *

Sender Address: xxx@hanmingtech.com *

Mail Subject: test *

Receiver	support	Receiver Address	support@hanmingtech.com	Test *
Receiver		Receiver Address		Test
Receiver		Receiver Address		Test

Fig. 19-1 Configuration of Email Alarm

See Table 19-1 for the parameters.

Configuration Item	**Description**
Email Switch	Switch for Email alarm
AC System Alarm	For informing the receiver of any AC system alarm through an email
AP Alarm	For informing the receiver of any AP alarm through an email
Server IP	IP address of the email server
Sender	Sender of the email alarm
Sender Password	Email box password of sender of the email alarm
Sender Address	Email address of the sender
Mail Subject	Subject of the email
Receiver	Receiver of the email alarm

Table 19-1 Parameters of Email Alarm Configuration

Chapter 20 Dual-CAPWAP-link hot backup

20.1 Overview

The goal of system stability in the WLAN field is to make sure wireless terminal STA as network users can realize continuous and stable communication as much as possible. It is not significant that STA has communication link switching or not in the whole continuous and stable communication. Thus, CAPWAP primary and backup links can be established for APs and two ACs. In this way, APs can still provide continuous and stable wireless communication service for STA through the backup link even after an AC has failed. Fig. 20-1 is a block diagram of dual-CAPWAP-link hot backup.

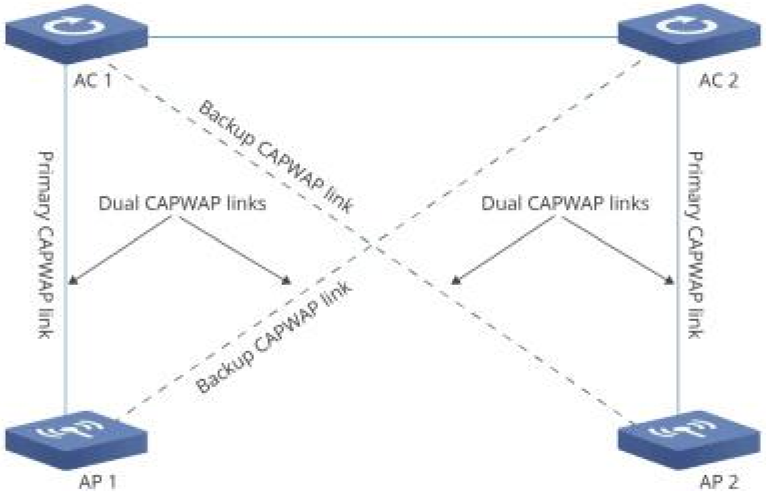


Fig. 20-1 Block Diagram of Dual-CAPWAP-link Hot backup

Two key technologies for dual-CAPWAP-link hot backup for ACs:

(1) Dual CAPWAP links: An AP is associated with the primary AC and the backup AC at the same time through two logic CAPWAP channels to realize quick seamless switching between the two ACs when either of them has failed.

(2) Quick link detection: Faults of the peer AC can be detected quickly through quick heart beat detection.

Service status data: It includes AP real-time information, STA real-time information, STA authentication dialog status information, etc. During the operation of the ACs, these data are established dynamically and updated in real time. For the service status data (AP information and STA information) exclusive in the WLAN field, execute batch backup (a BAC real-time backup channel on the bottom layer) with a unit of AP while a backup CAPWAP channel is being established between each AP and the backup AC to realize a millisecond-level switching speed for the two ACs. In the process, only the STA information needs to be backed up (the AP information is established automatically during establishment of the backup CAPWAP channel); execute real-time bacukup for the STA information when any STA status information (such as online, offline, roaming or authentication) on the primary AC has changed.

20.2 Configuration

20.2.1 Steps

Main steps:

1) “Primary/Backup AC” configuration: Configure “Backup Link” and “Backup Group“ on the “Primary/Backup AC” page under “Device Management”.

2) “DHCP Hot backup” configuration: If AP/STA needs to acquire an address from the AC, enable the DHCP service on the AC and click “Network Configuration”, “DHCP Configuration” and “Global Configuration” in sequence to configure DHCP hot backup data. Please refer to the content about DHCP global configuration in section 5.3.

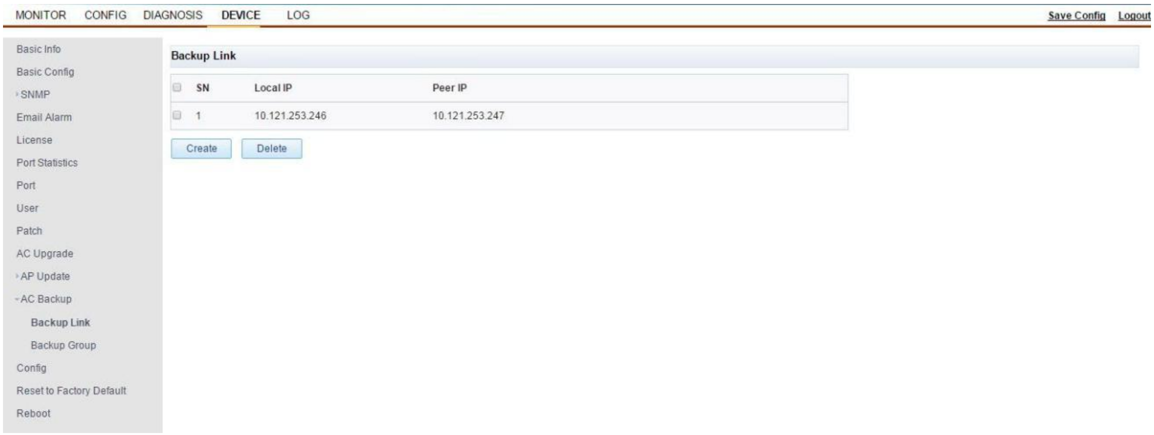
3) “AP Group Hot Backup” configuration: Click “Network Configuration”, “WLAN Configuration” and “AP Group” in sequence to configure AP group hot backup. Please refer to the content about AP backup group configuration in section 7.4.4.

4) “Service Configuration Data” synchronization: Configure the same DHCP address pool, wireless service configuration and AP template data for the two ACs.

5) “AP Configuration” application: An AP is online on the two ACs at the same time. Click “Network Configuration”, “WLAN Configuration” and “AP configuration” on each of the ACs in sequence to use the same AP group hot backup. Please refer to the content about joining in or exiting from an AP group in section 7.4.5.

20.2.2 Primary/Backup AC

“Primary/Backup AC” configuration includes “Backup Link” and “Backup Group”. See Fig. 20-2.



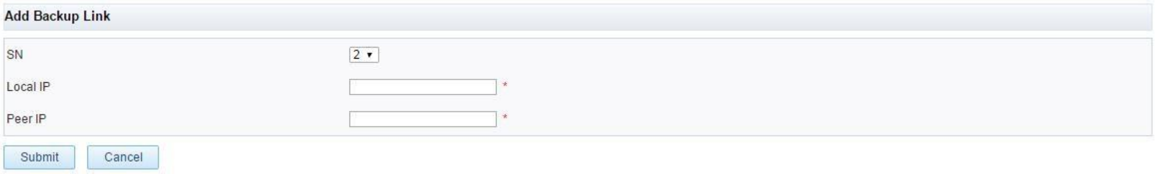
Backup Link

□	SN	Local IP	Peer IP
□	1	10.121.253.246	10.121.253.247

Fig. 20-2 Primary/Backup AC

• Backup Link

Its main parameters are its local IP address and peer IP address. It supports mutually backed up ACs, namely, the AC IP addresses can be used as IP address of the backup link, as long as communication can be realized between the local IP address and the peer IP address. Data of all the backup groups of the two ACs can be backed up by a single backup link, thus controlling broadcast domains of the AC IP addresses effectively. To create a backup link, click “Create” on a page as shown in Fig. 20-2. See Fig. 20-3.



Add Backup Link

SN: 2 ▾

Local IP: *

Peer IP: *

Fig. 20-3 Backup Link

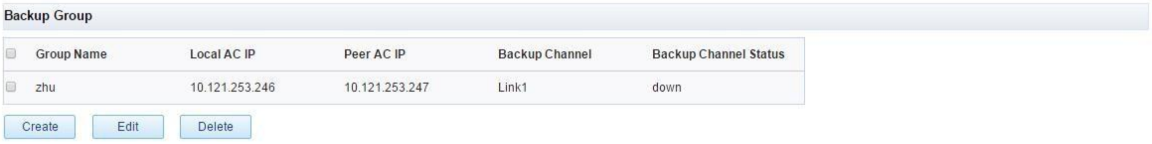
See Table 20-1 for the parameters.

Configuration Item	Description
SN	ID number of the backup link to be created (at most eight backup links can be created)
Local IP	IP address of the local AC of the backup link
Peer IP	IP address of the peer AC of the backup link

Table 20-1 Parameters of Backup Link

• Backup Group

It is used for determining the primary AC and the backup AC, distributing AC IP addresses for AP and binding the link relation of the two ACs. See Fig. 20-4.

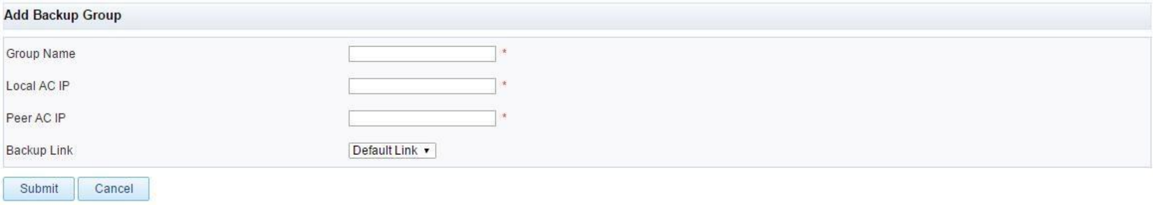


Backup Group

□	Group Name	Local AC IP	Peer AC IP	Backup Channel	Backup Channel Status
□	zhu	10.121.253.246	10.121.253.247	Link1	down

Fig. 20-4 Backup Group

To create a backup group, click “Create” on a page as shown in Fig. 20-4. See Fig. 20-5.



Add Backup Group

Group Name	*
Local AC IP	*
Peer AC IP	*
Backup Link	Default Link ▾

Fig. 20-5 Backup Group Creation

See Table 20-2 for the parameters.

Configuration Item	**Description**
Group Name	Name of the backup group (it should be the same on the two ACs)
Local AC IP	IP of the local AC (AC IP address acquired by the AP)
Peer AC IP	IP of the peer AC (AC IP address acquired by the AP)
Backup Link	If “Default Link” is selected, data configuration will not be necessary on the “Backup Link” page. “Default Link” means that the AC IP address configured on the “Backup Group” page is used as the backup channel between the two ACs. Select the backup channel from the dropdown box.

Table 20-2 Parameters of Backup Group Creation

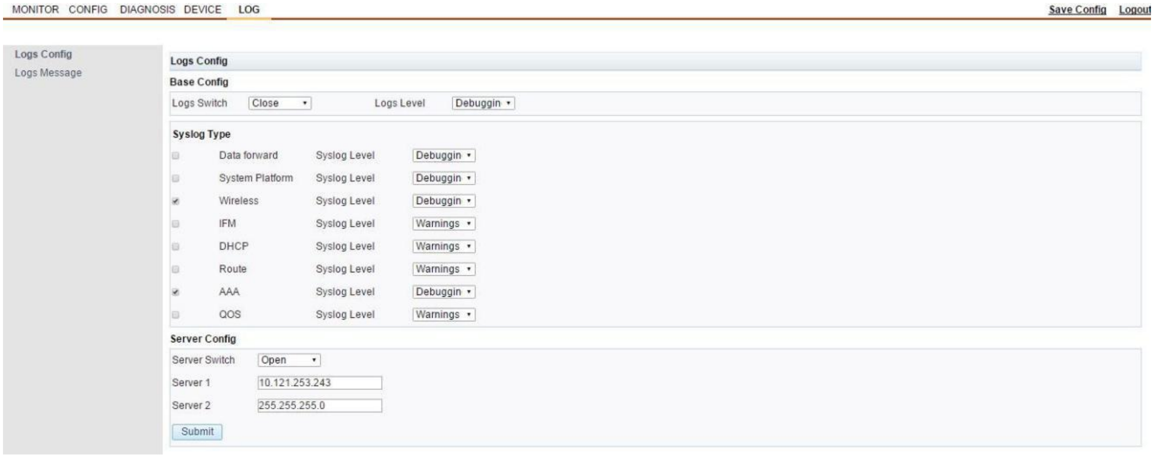
To edit or delete the data of a backup group created, click “Edit” or “Delete” on the page as shown in Fig. 20-4.

Note: After a backup link has been established for the two ACs, user can click “Device Management”, “Primary/Backup AC” and “backup group” in sequence to view the information under “Backup Channel Status”. If it is “Up”, it suggests that both the backup link communication and the hot backup channel are normal; if it is “Down”, it suggests that the backup link communication is abnormal and the backup link address between the two ACs should be checked.

Chapter 21 Log

21.1 Overview

The syslog include a lot of information of the network and the device, including their operation status, configuration changes, etc. They are significant for administrators to figure out status of the network and the device and take targeted actions for problems or safety hazards of the network. Information in the syslog can be saved in the buffer, viewed on the “Log Message” management page and, after setting on the syslog server, sent as syslog message to the log host. See Fig. 21-1 for the “Log” page.



Logs Config

Base Config

Logs Switch	Close	Logs Level	Debuggin

Syslog Type

☐	Data forward	Syslog Level	Debuggin
☐	System Platform	Syslog Level	Debuggin
☑	Wireless	Syslog Level	Debuggin
☐	IFM	Syslog Level	Warnings
☐	DHCP	Syslog Level	Warnings
☐	Route	Syslog Level	Warnings
☑	AAA	Syslog Level	Debuggin
☐	QOS	Syslog Level	Warnings

Server Config

Server Switch	Open
Server 1	10.121.253.243
Server 2	255.255.255.0

Fig. 21-1 Log

21.2 Configuration

“Log” configuration includes “Logs Config” and “Logs Message”.

21.2.1 Log Configuration

As shown in Fig. 20-1, user can view messages on the “Logs Message” page under “Log” view “Log Switch” and “ Log Level”. “ Log Level” lists eight log levels (ranked from higher ones to lower ones according to priority).

User can select a module under “Syslog Type” and the corresponding syslog level and configure “Server Config”. The AC will send the related syslog message to the designated server according to the configuration.

Configuration Item	**Description**
Logs Switch	Enable switch for log
Log Level	Eight basic log levels ranked by priority from high to low or from low to high according to log details, including “Emergencies”, “Alerts”, “Critical”, “Errors”, “Warnings”, “Notifications”, “Informational” and “Debugging”
Syslog Type	Including “Data Forward”, “System Platform”, “Wireless”, “IFM”, “DHCP”, “Route”, “AAA ” and “QOS”
Server Switch	Enable switch for the Syslog server
Server 1	IP address of Syslog server 1
Server 2	IP address of Syslog server 2

Table 21-1 Parameters of Log Configuration

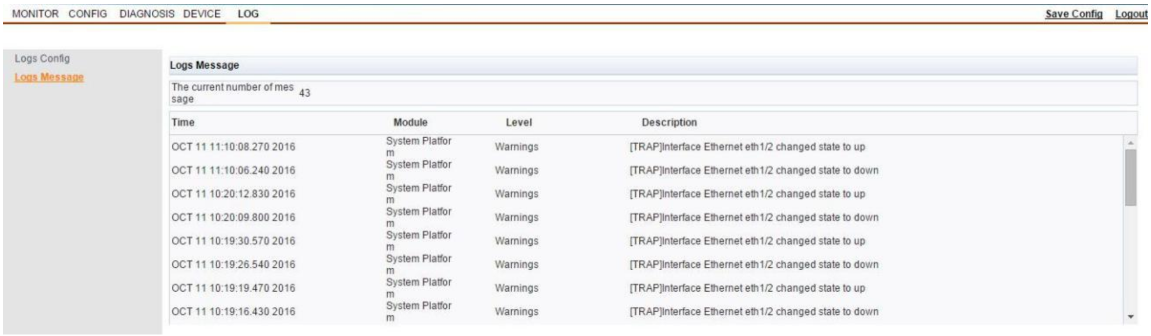
Note:

Constraint: The syslog level under “Syslog Type” depends on the syslog level under “Basic Config” of “Logs Config”. Priority of the syslog message should be not lower than the syslog level under “Basic Config” of “Logs Config”.

Level of “Server Switch” should be lower than level of the enable switch under “Basic Config” of “Logs Config”.

21.2.2 Logs Message

Fig. 21-2 shows the “Logs Message” page. After setting the log level and the switch, user can view log messages on this page. Each log message includes “Time”, “Module”, “Level” and “Description”. To display the latest log message, click “Refresh”. To clear the logs in the log list, click “ Clear”.

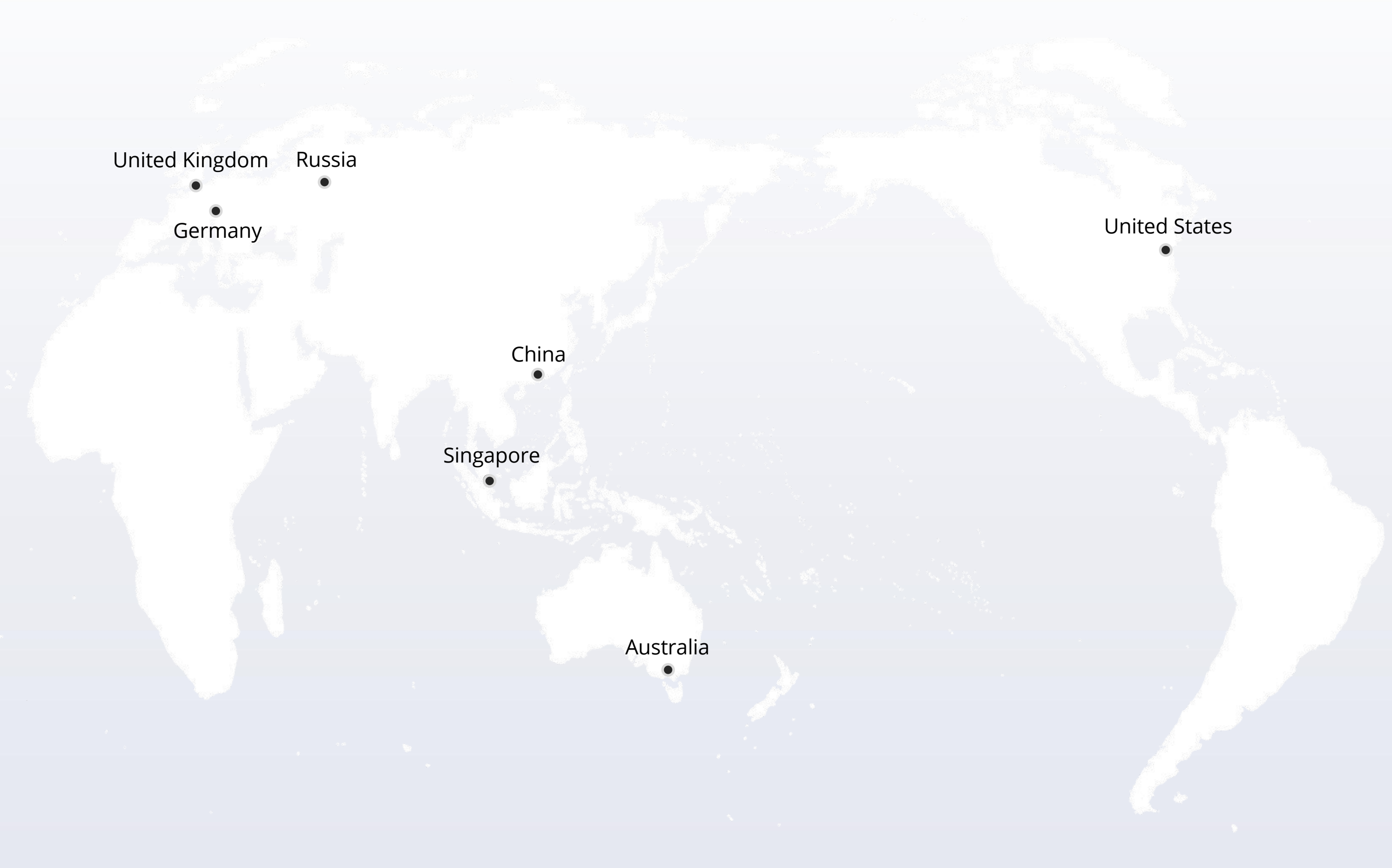


Logs Message

The current number of message 43

Time	Module	Level	Description
OCT 11 11:10:08.270 2016	System Platform	Warnings	[TRAP]Interface Ethernet eth1/2 changed state to up
OCT 11 11:10:06.240 2016	System Platform	Warnings	[TRAP]Interface Ethernet eth1/2 changed state to down
OCT 11 10:20:12.830 2016	System Platform	Warnings	[TRAP]Interface Ethernet eth1/2 changed state to up
OCT 11 10:20:09.800 2016	System Platform	Warnings	[TRAP]Interface Ethernet eth1/2 changed state to down
OCT 11 10:19:30.570 2016	System Platform	Warnings	[TRAP]Interface Ethernet eth1/2 changed state to up
OCT 11 10:19:26.540 2016	System Platform	Warnings	[TRAP]Interface Ethernet eth1/2 changed state to down
OCT 11 10:19:19.470 2016	System Platform	Warnings	[TRAP]Interface Ethernet eth1/2 changed state to up
OCT 11 10:19:16.430 2016	System Platform	Warnings	[TRAP]Interface Ethernet eth1/2 changed state to down

Fig.21-2 Logs Message



https://www.fs.com

The information in this document is subject to change without notice. FS has made all efforts to ensure the accuracy of the information, but all information in this document does not constitute any kind of warranty.