Instructizon Manual for DCN Access Controller

Contents

1. Foreword

1.1 Chapter Arrangement

Part I Guide to AC Quick Configuration;

Part II AC Functions and Operation

Part III Configuration Examples (in Common Scenario)

This manual takes DCWS-6028-C/EAC-660 as an example. In view of differences in hardware and software among various models of product, all problems relating to product specifications shall be confirmed with Digital China Networks Limited.

1.2 Provisions

1.2.1. GUI Format

Description	Symbol	Example
Menu Items & Submenu Items	[]	【 Basic Network 】 →[Port Management]
Successive Selection Menu Items & Submenu Items	→	【 Basic Network 】 →[Port Management]
Drop-down Box, Radio Button, CheckBox	""	Set "IP Pool Name"
Module & Window Name	【】	【Monitor】

1.2.2. Abbreviations

Abbreviations	Meaning

AC	DCN access controller
AP	DCN access point
STA	Station (e.g. mobile phones, tablets, PC, etc.)
Portal	STA access network, authentication web page
Radius	External Radius server, user authentication and billing

1.2.3. Symbol Marks

In this manual, eye-catching symbol marks are used to indicate items that need special attention. Their meanings are as follows:

Caution: remind the user of maters that need attention during operation. Improper operation may lead to setting failure, data loss or equipment damage.

Notes: provide necessary supplements to and explanations of operations.

1.2.4. Technical Support

User Support Email: dcn_technicians@digitalchina.com

Company Website: www.dcnglobal.com

1.2.5. Acknowledgement

Thank you for using our product and instruction manual. If you have any opinions or suggestions, please contact us by phone, forum or email. We will highly appreciate it.

2. Initial Configuration

This section describes the methods of accessing, networking and configuration necessary for the first deployment of AC.

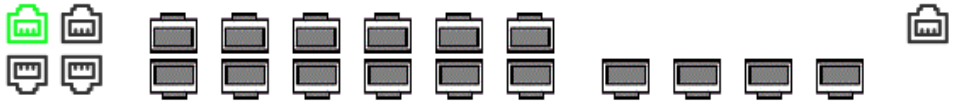
2.1Networking

All service ports for AC system are defaulted to vlan1; address: 192.168.1.1/24.

Port details depend on the equipment.

1. 6028-C port:

2. EAC-660 port:



After start during initialization, connect portable PC to the service electrical interface with a cable, and then configure PC IP address manually to be 192.168.1.2/24.

Networking Example:

Figure 1 Initial Topology

Real-time access address: http://192.168.1.1; initial user name: admin; initial password: admin.

1. For AC system access, Chrome, Firefox, 360 Browser (Never Slow Mode) or IE11 above is recommended;

2. When configuring AC for the first time, wireless IP address shall be saved. If not saved, the current Vlan address will be displayed but isn't effective.

2.2 Basic Network Deployment

2.2.1. Basic Network Topology 1

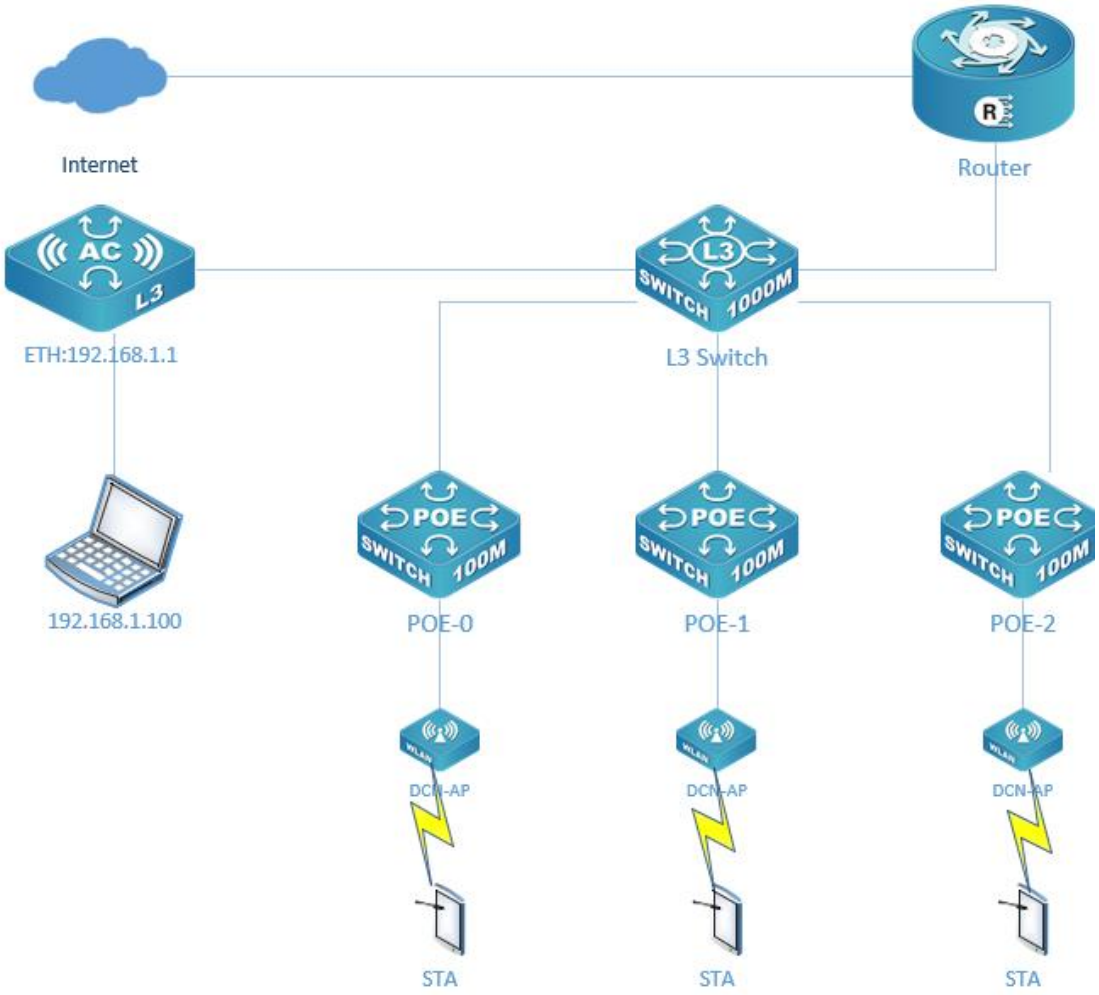


Figure 2: Topology for Independent Use of AC

2.2.1.1. Networking introduction

Layer 3 Switch: configure DHCP address pool to provide IP address for subordinate network devices, DCN-AP and terminals. DHCP Option43 is used to configure AC IP to ensure that AP can gain access to AC after obtaining the address.

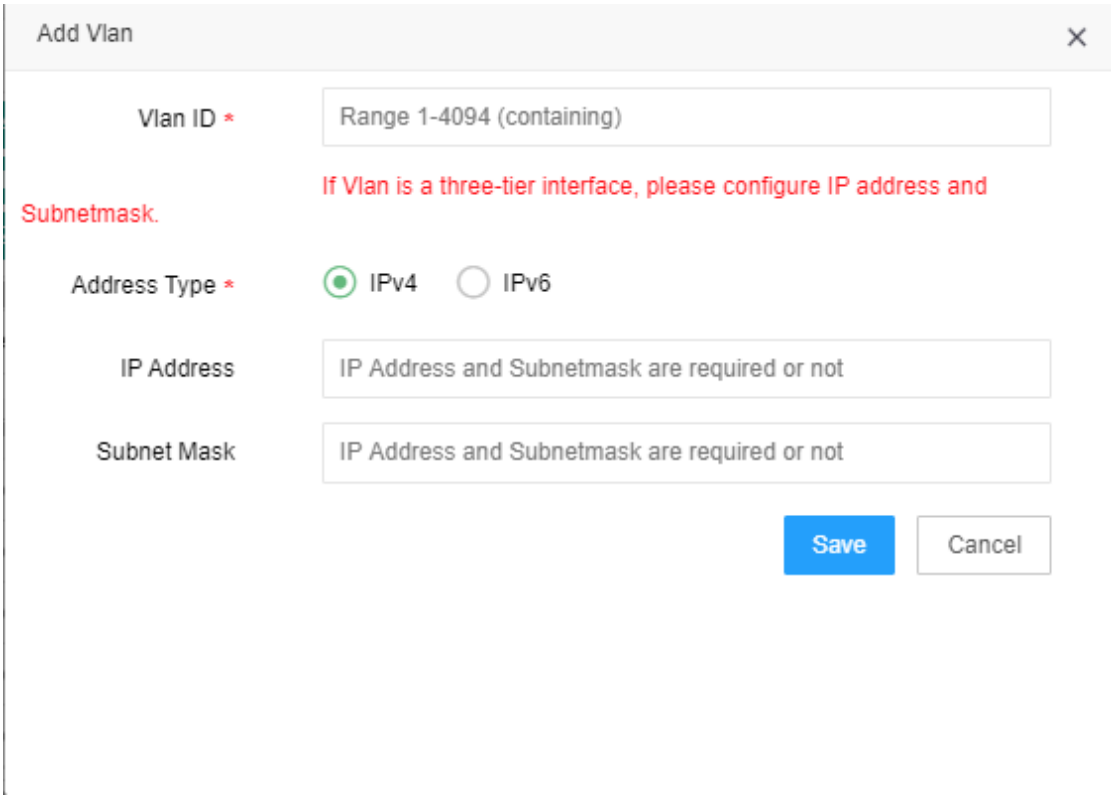
Authentication: This network uses AC built-in portal and authentication system.

2.2.1.2. Network configuration

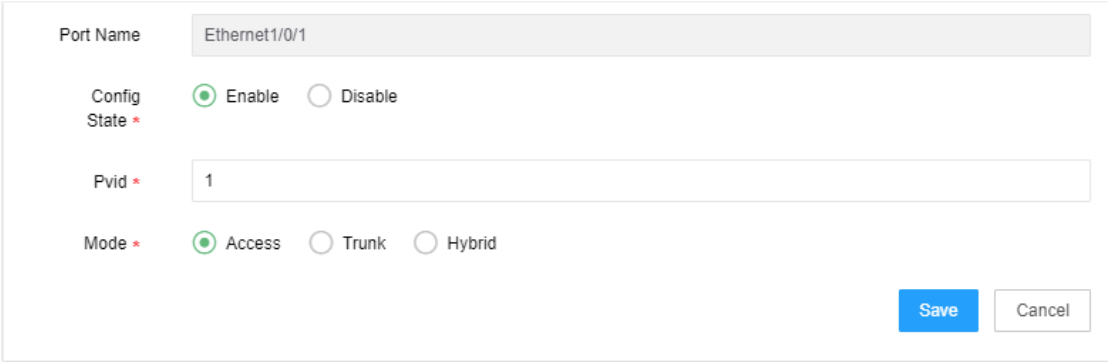
i. AC network configuration:

1. Connect PC to the service port, then configure it to IP address in the same network segment: 192.168.1.10 to gain access to AC Web interface;

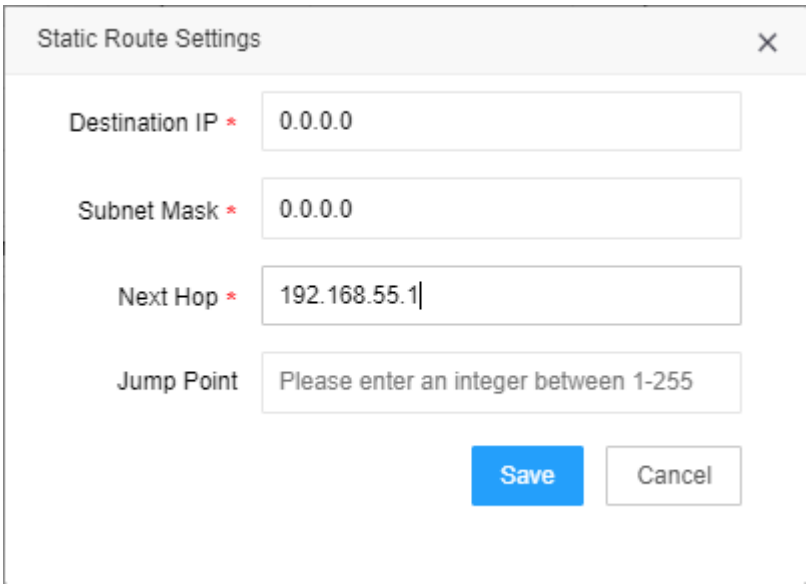
2. Configure AC to IP address in the same network segment as Layer 3 Switch interface. Click【Basic Network】 -[Vlan Management]- Add Vlan  to configure Vlan and IP address. Then, click "Save".



3. Configure AC Vlan to be the same as Layer 3 Switch interface Vlan. Click【Basic Network】 -[Port Configuration], select the connection interface and then click "  " to configure Vlan.



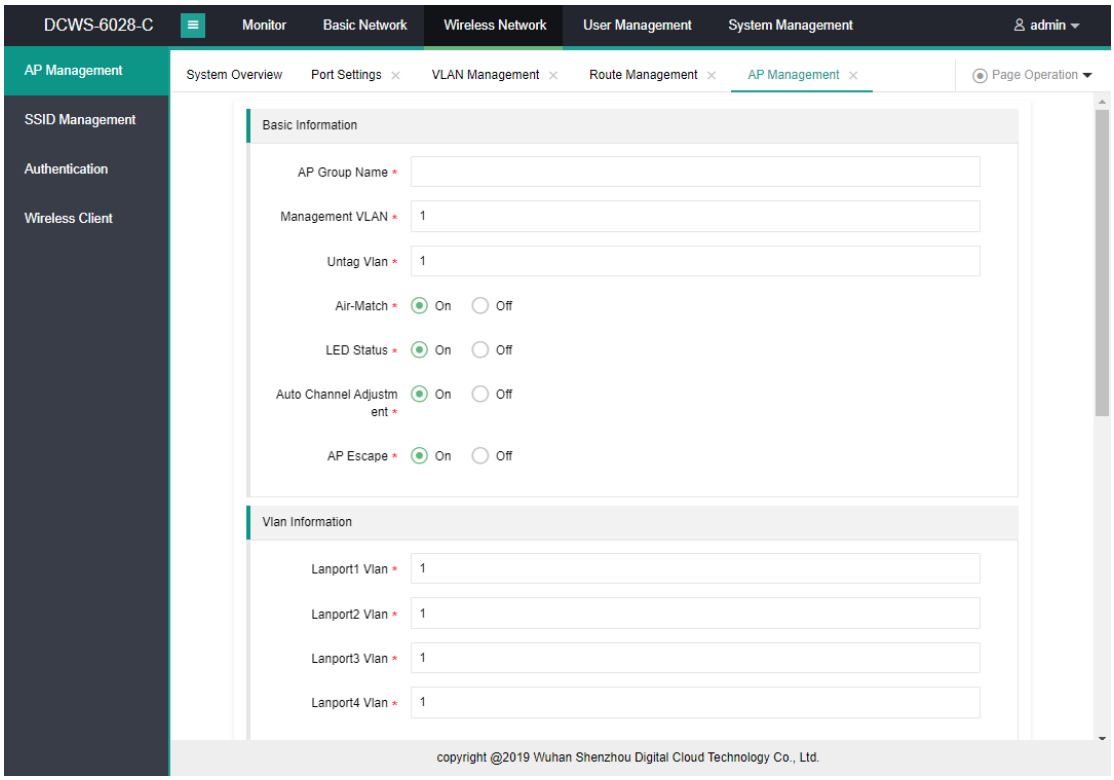
4. Configure the default route for AC to guarantee its access to the Internet. Click【Basic Network】- [Route Management] - Add Route , and then select the default route of Layer 3 Switch.



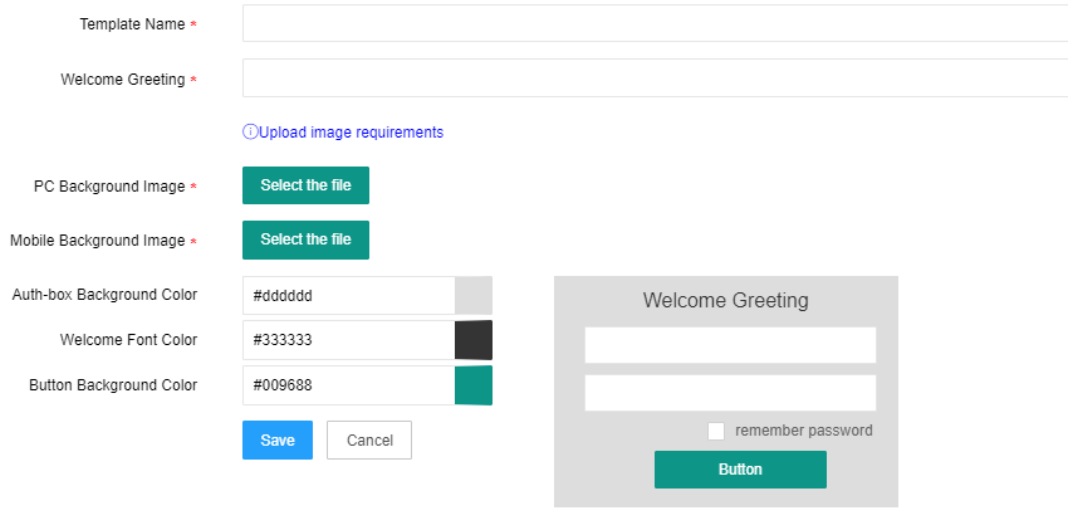
5. Enable the wireless function.【Basic Network】- [Vlan Management], click the wireless configuration button " " on the upper list, then select corresponding Vlan as the wireless address for the system.

ii. AC wireless configuration

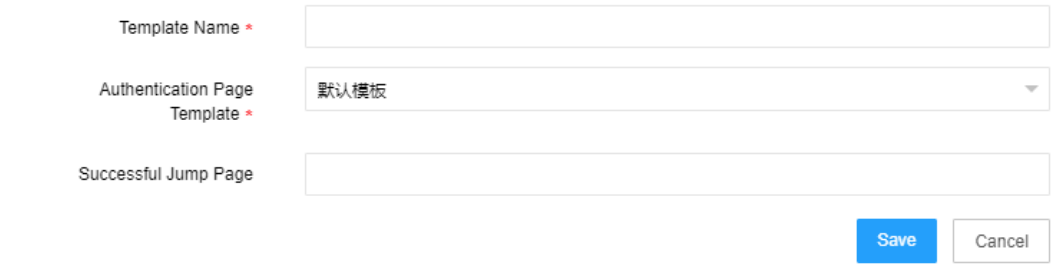
1. Add an AP group to facilitate the overall configuration of AP. Click 【Wireless Network】- [AP Management] - Add AP Group to configure AP group attributes.



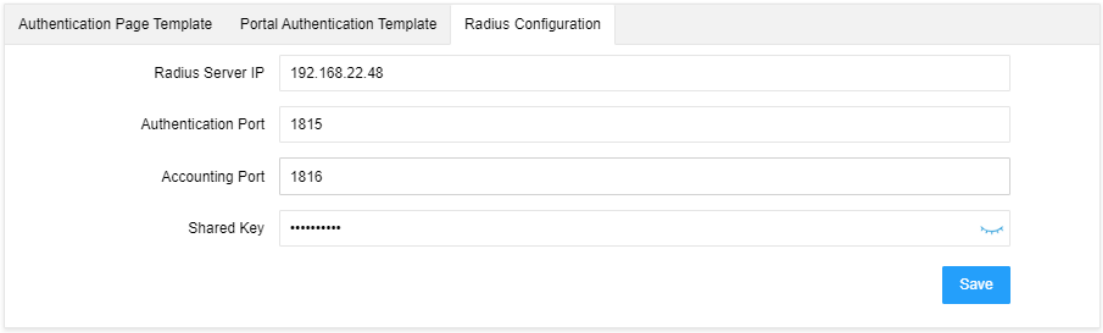
2.Add an authentication page template. Click【Wireless Network】- [Authentication Management] - Authentication Page Template - Add Template + to add a Web page template for redirect configuration.



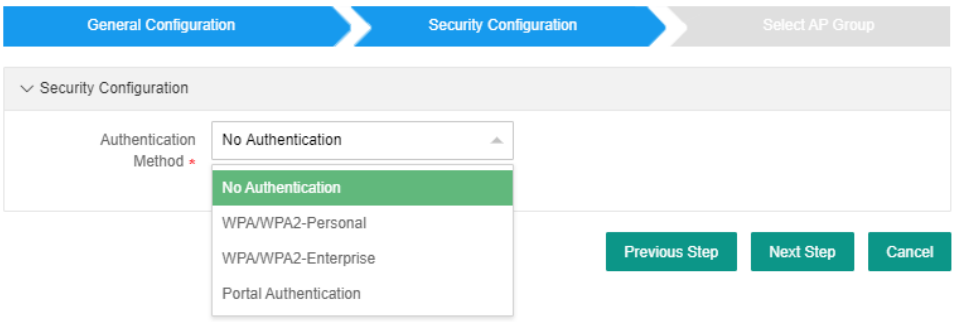
3.Add a Portal authentication template. Click【Wireless Network】- [Authentication Management] - Portal Authentication Template - Add Template + to add a new template for jump during redirect configuration.



4.Radius configuration will be necessary if 1 x authentication is used. Click 【Wireless Network】- [Authentication Management] - Radius Configuration.

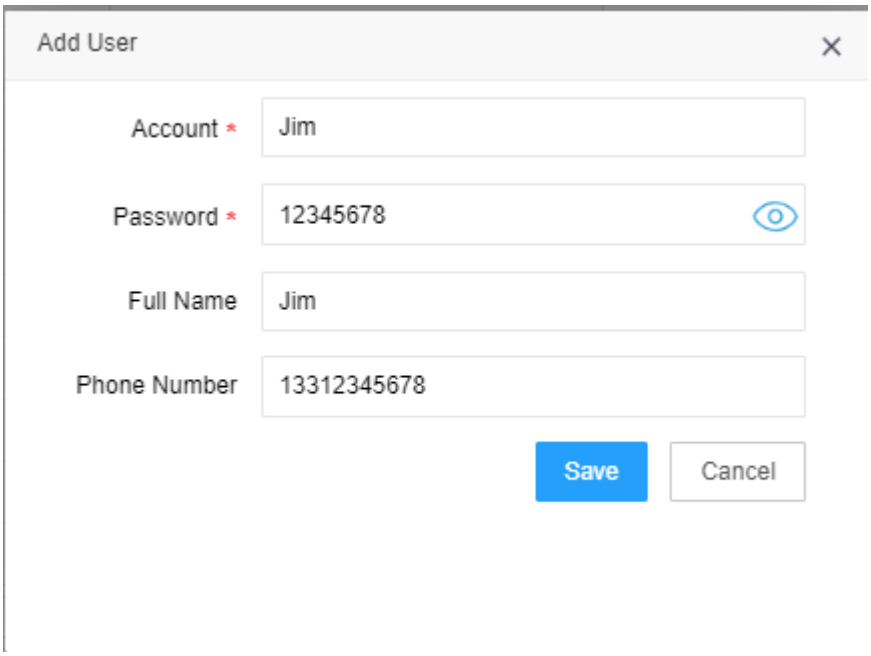


5.Create a new SSID with different authentication modes: No Authentication, WPA/WPA2-Personal, WPA/WPA2-Enterprise or Portal Authentication. Steps: click 【Wireless Network】- [SSID Management]- Add SSID  .



6.Create a built-in user for built-in authentication. Click 【User Management】- Add User  .

The user in the figure below can be used for portal authentication.



iii. Monitor

After AC gets started, online AP and user access information, etc. can be viewed through the monitor. See below for further details.

iv. System management

System management covers the configuration of ImCloud address, version upgrade, country code, license management, NTP, backup/restore and restart/factory reset. See below for further details.

This topology applies to small networking scenarios where one AC can meet user requirements.

2.2.2. Basic Network Topology 2

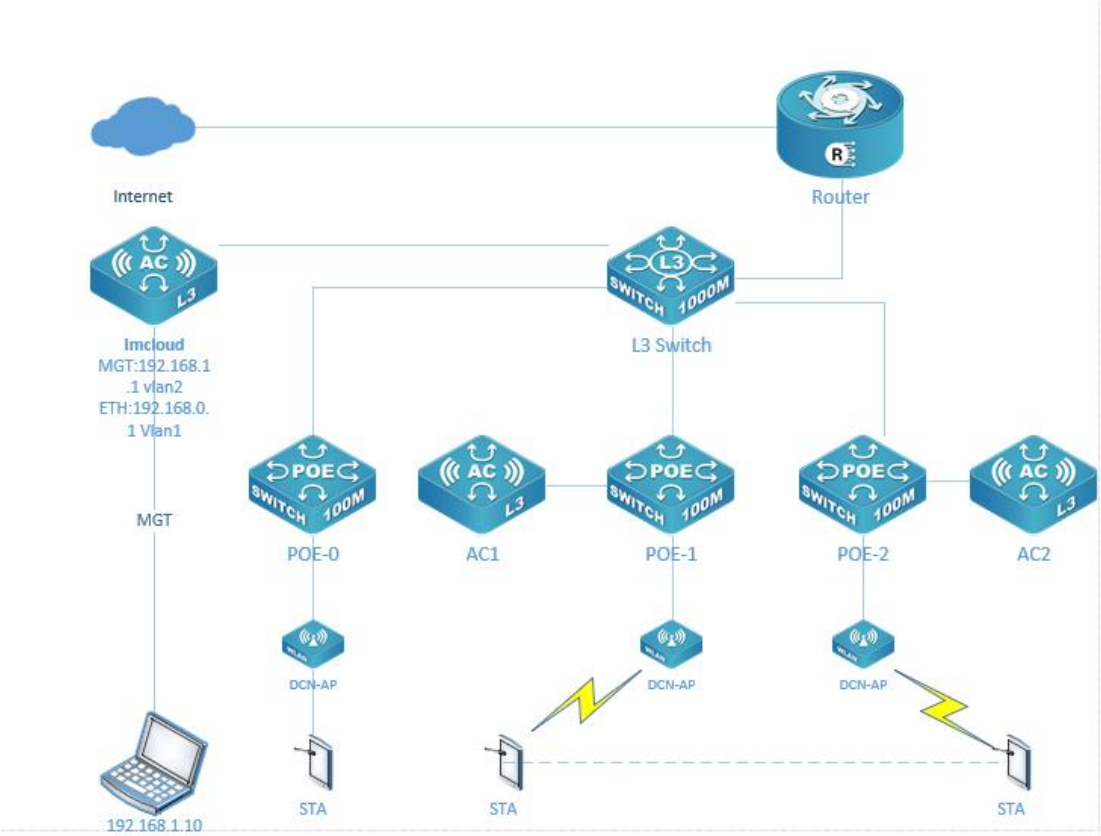


Figure 3 Topology in which AC is Managed by ImCloud as Tier-2 AC

2.2.2.1. Networking introduction

Layer 3 Switch: used for configuring DHCP address pool to provide IP address for subordinate network devices, DCN-AP and terminals. A variety of DHCP Option43 are used to configure AC/Imcloud IP to ensure that AP can go online from different ACs after obtaining the address.

Imcloud: AC1 and AC2 can go online on Imcloud by configuring the wireless management ip. The user can configure AC1 and AC2 via Imcloud.

Authentication: This network uses Imcloud built-in portal and authentication system.

i. AC network configuration

IP and gateway are to be configured based on network environment.

ii. AC wireless configuration

The wireless configuration for all ACs will be uniformly done by ImCloud.

This topology applies to large networking scenarios where one AC can't meet user requirements.

2.3 Basic Configuration Procedure

1. Conduct basic network configuration for AC according to the network topology;

2. Upload approved authorization files;

3. Configure the necessary AP group, in which APs can be managed and configured in different ways;

4. Configure the authentication page template;

5. Configure the Portal authentication template and bind it;

6. Enter User Management to create new built-in users for STA access authentication;

7. Add SSID and bind it to the authentication template created in Step 5 during portal configuration;

8. Use DHCP option43 to configure the Ipv4 address for AC;

9. Power up AP and check the AP list on AC. After AP is connected, STA will connect with user's SSID for portal authentication.

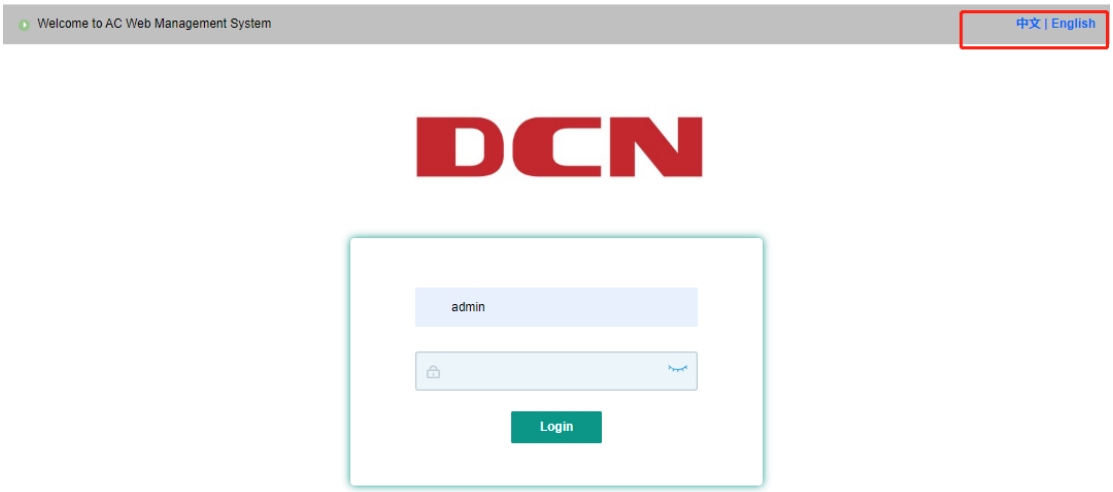
3. AC Operating Instructions

This section describes the function operations, status displays and operational guidelines, etc. during AC usage.

3.1 System Access

3.1.1. Access

Open a browser and enter AC IP address to get access to the login page.

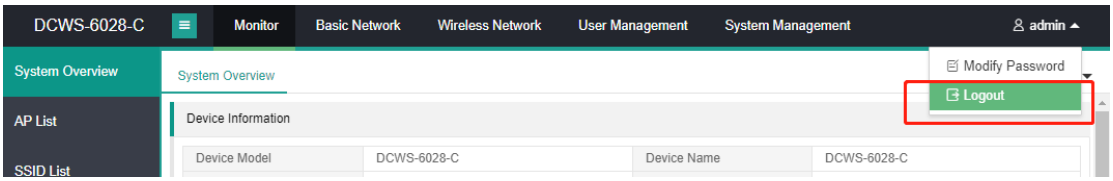


3.1.2. Login

Enter username and password, then click "login" (default username and password are admin and admin respectively)

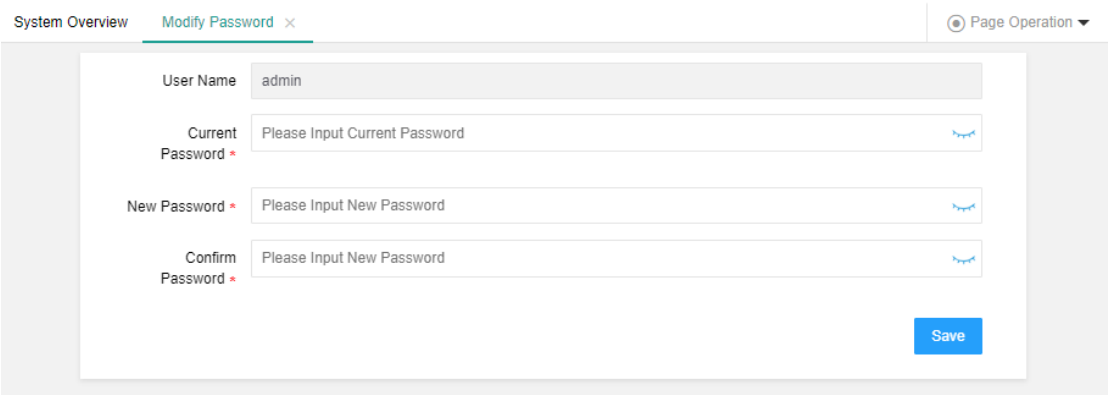
3.1.3. Logout

After login, the user may log out. Click "admin" at the upper right side of the page and then click "logout" button. The page will get back to the login page.



3.1.4. Change Login Password

After login, the user may log out. Click "admin" at the upper right side of the page and then click "Change Password" button to modify the login password of the user "admin".



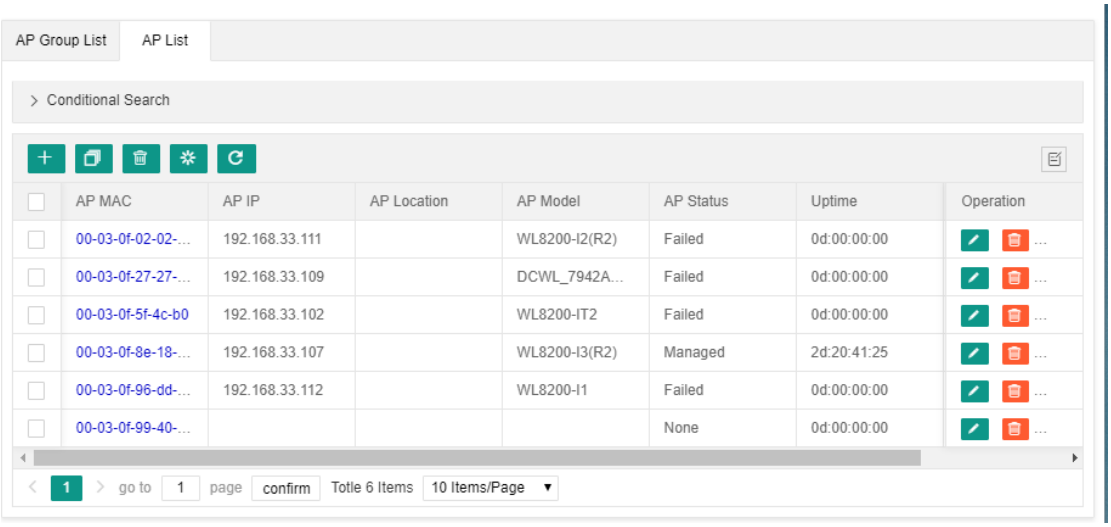
3.2Monitor

3.2.1. System Overview

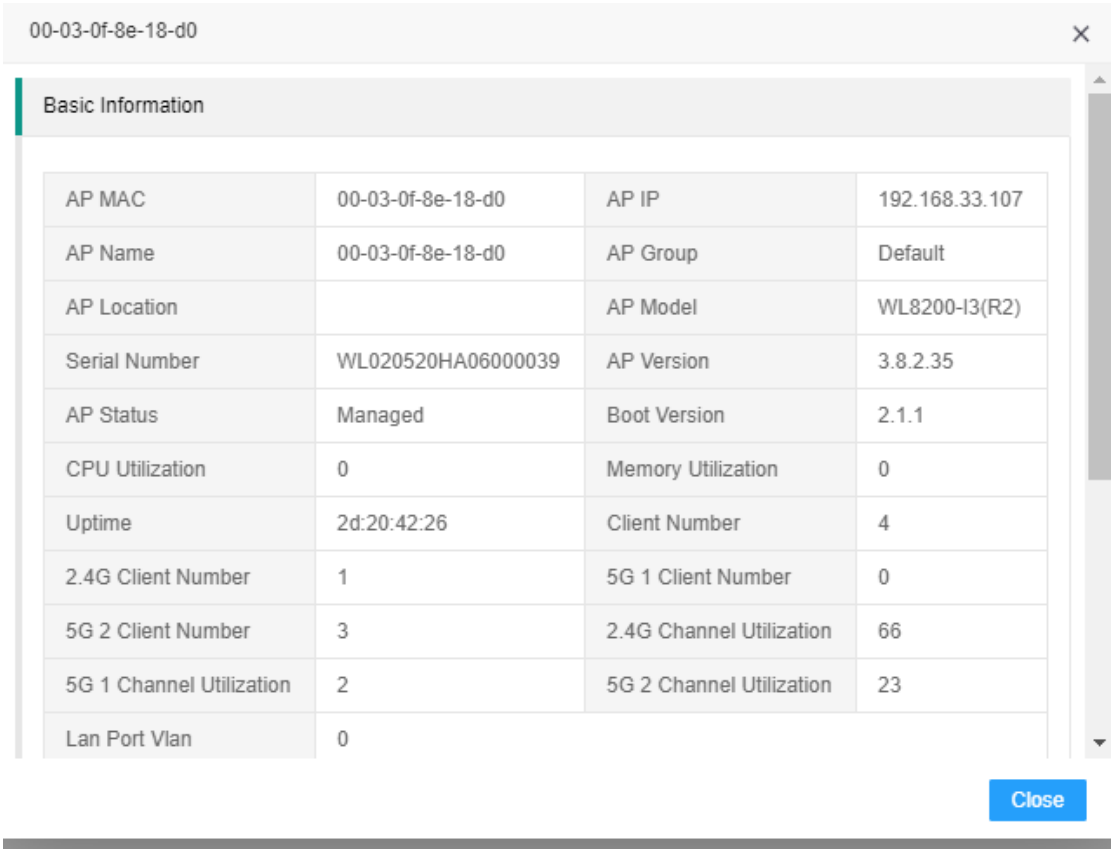
【Monitor】→ [System Overview]: this screen displays the basic information of device by charts/graphs, including device information, port monitoring, device status, AP status, number of client users, AP channel utilization, client signal intensity distribution, client model distribution - OS/manufacturer, client link protocol distribution, number of clients from AP access (TOP5), client-side traffic from AP access (TOP5), and load-based AP distribution;

3.2.2. AP List

【Monitor】→ [AP List]: displays AP information and supports user query based on the following criteria: AP group, AP ip, AP mac and AP status;



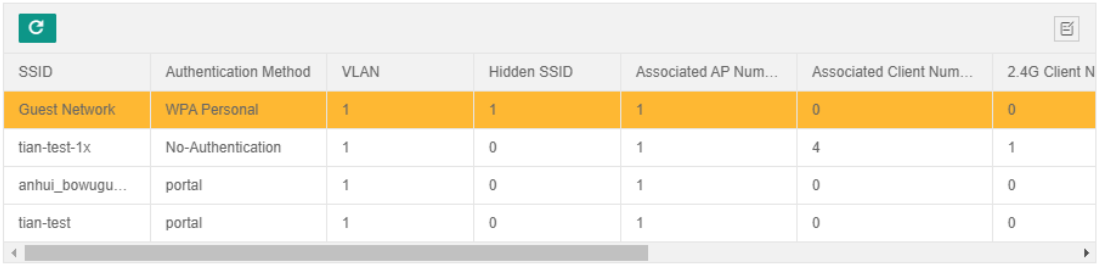
AP details can be displayed by clicking "AP mac information" under "AP list", as shown below:



This AP List doesn't support AP configuration. AP configuration is available in other menu.

3.2.3. SSID List

【Monitor】→ [SSID List]: displays AC SSID configuration information, including SSID, authentication mode, vlan, hidden SSID, number of associated APs, number of associated clients, number of 2.4G clients, number of 5G1 clients, number of 5G2 clients, sent traffic and received traffic.



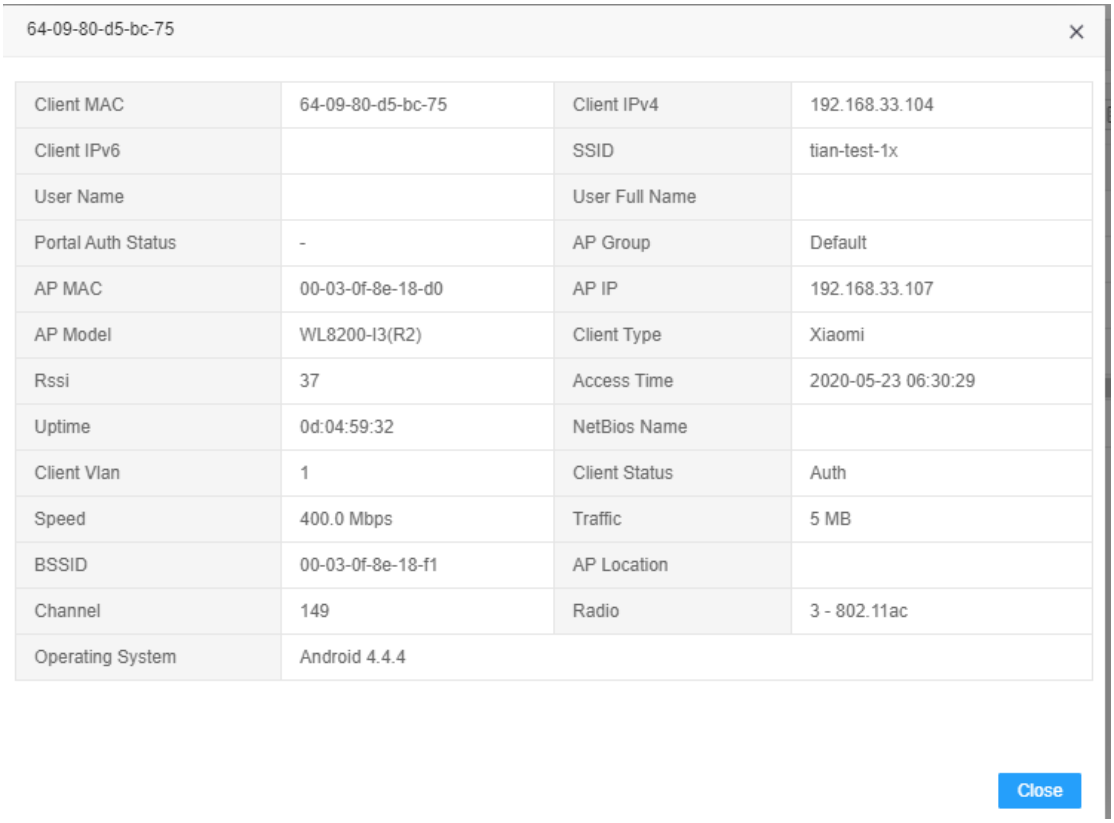
SSID	Authentication Method	VLAN	Hidden SSID	Associated AP Num...	Associated Client Num...	2.4G Client N
Guest Network	WPA Personal	1	1	1	0	0
tian-test-1x	No-Authentication	1	0	1	4	1
anhui_bowugu...	portal	1	0	1	0	0
tian-test	portal	1	0	1	0	0

This SSID List doesn't support SSID configuration and editing. SSID configuration is available in other menu.

3.2.4. Wireless Client List

【Monitor】→ [Wireless Client List]: displays AP client information and supports user query based on the following criteria: client IP and client MAC;

AP client details can be displayed by clicking "Client MAC" information under "AP Client List", as shown below:

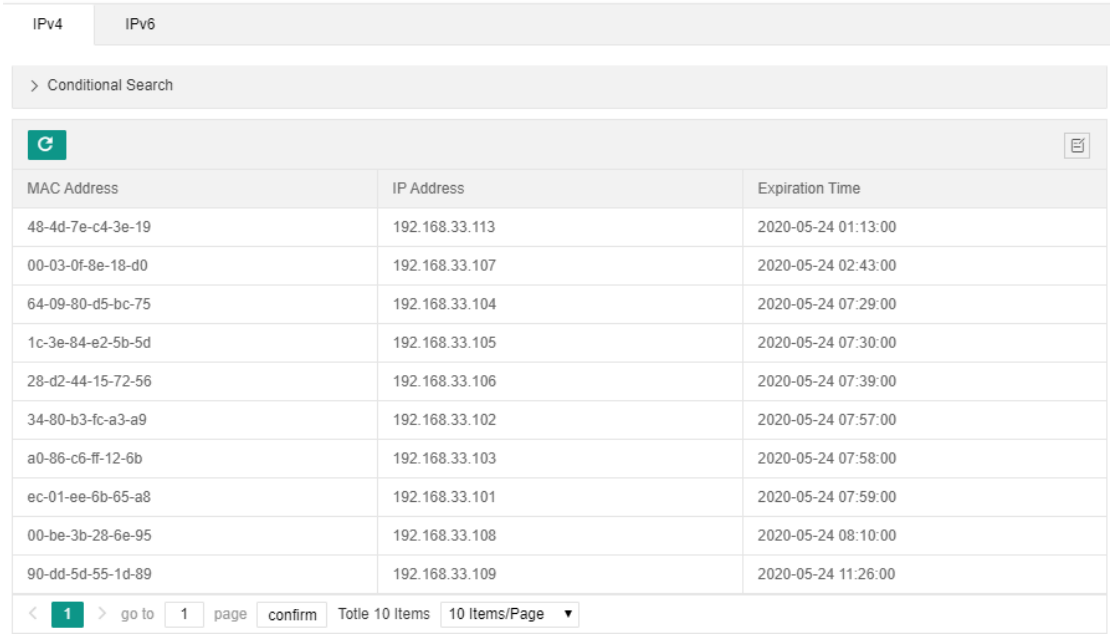


This AP Client List doesn't support forced offline of AP client. Forced offline of AP client is available in other menu.

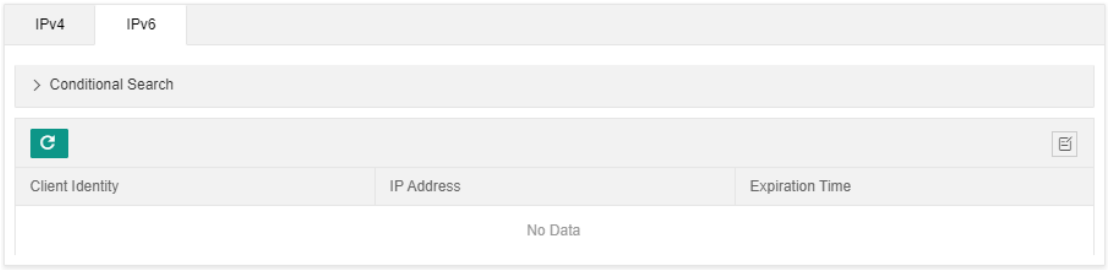
3.2.5. DHCP User List

【Monitor】→ [DHCP Client List]: when DHCP server is started on AC, DHCP client information will be displayed in the "DHCP Client List" under "Monitor", including IPV4 and IPV6 DHCP client information. This list supports user query based on the following criteria: mac address and IP address for ipv4; client identifier and IP address for ipv6.

IPV4 DHCP Client List displays the following: mac address, IP address and expiry time;



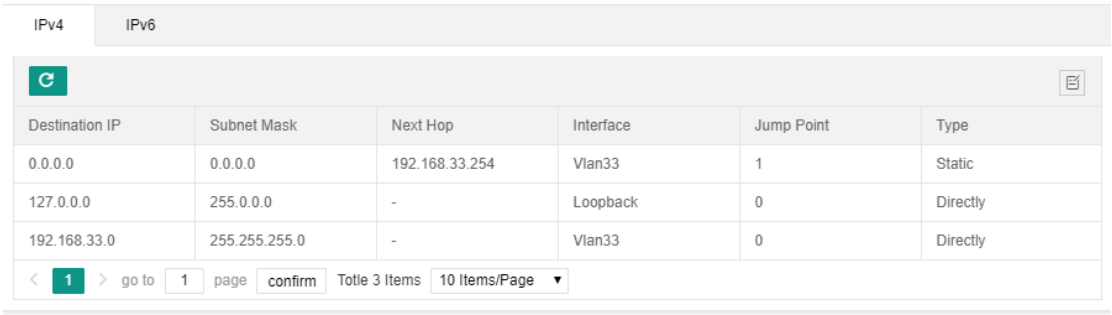
IPV6 DHCP Client List displays the following: client identifier, IP address and expiry time;



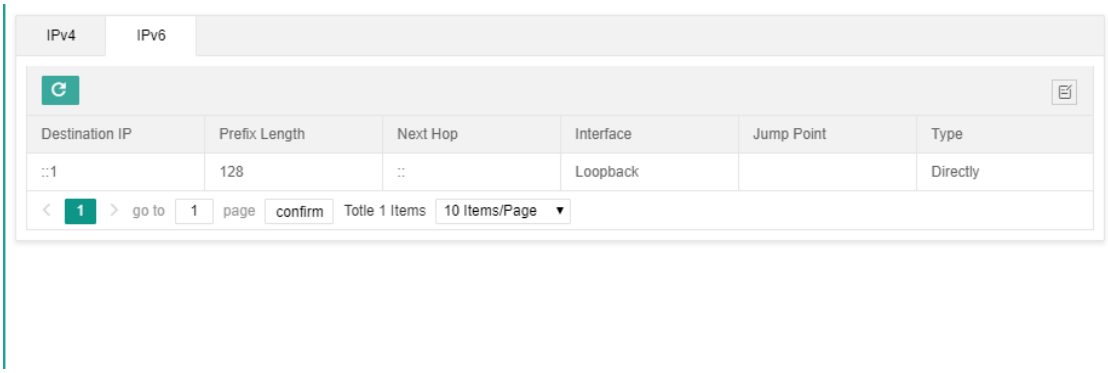
3.2.6. Routing Information

【Monitor】→ [Routing Information]: shows the current routing information list of AC, including IPV4 and IPV6 routing information;

Ipv4 routing information list displays the following: destination ip, subnet mask, next hop, interface, hop point and type;



Ipv6 routing information list displays the following: destination ip, prefix length, next hop, interface, hop point and type;

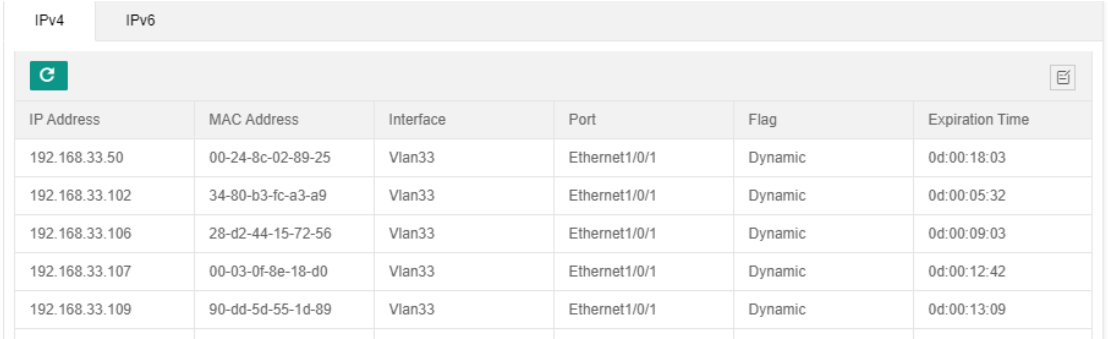


This Routing Information List doesn't support Route Edit. Route Add, Edit and Delete functions are available in other menu.

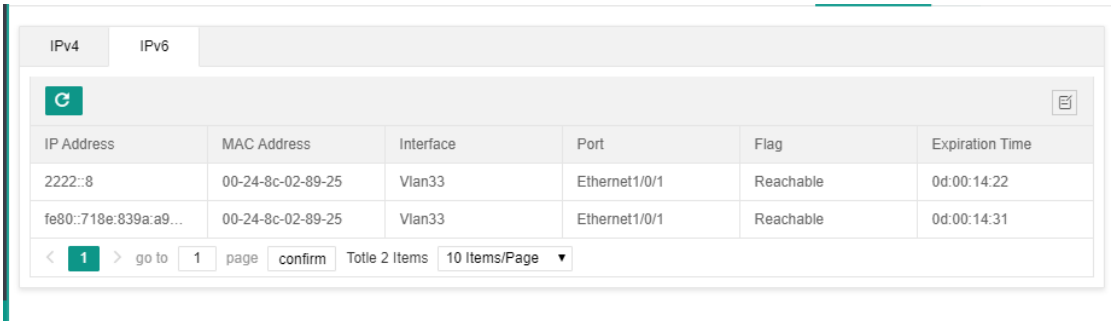
3.2.7. ARP Information

【Monitor】→ [ARP Information]: displays ARP information list learned by AC, including ipv4 and ipv6 ARP information;

Ipv4 ARP information includes the following: ip address, mac address, interface, port, identifier and expiry time;



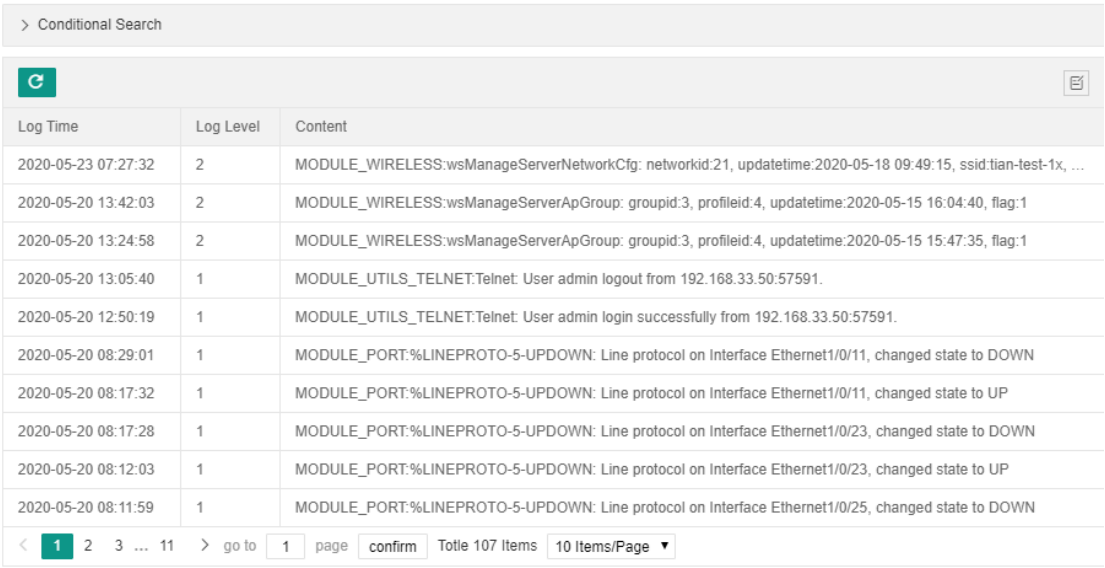
Ipv6 ARP information includes the following: ip address, mac address, interface, port, identifier and expiry time;



3.2.8. Log and Alarm

"Log and Alarm" List under "Monitor": displays AC web operation logs and supports user query based on the following criteria: time range and contents;

"Log and Alarm" List displays the following: log time, log level and contents;



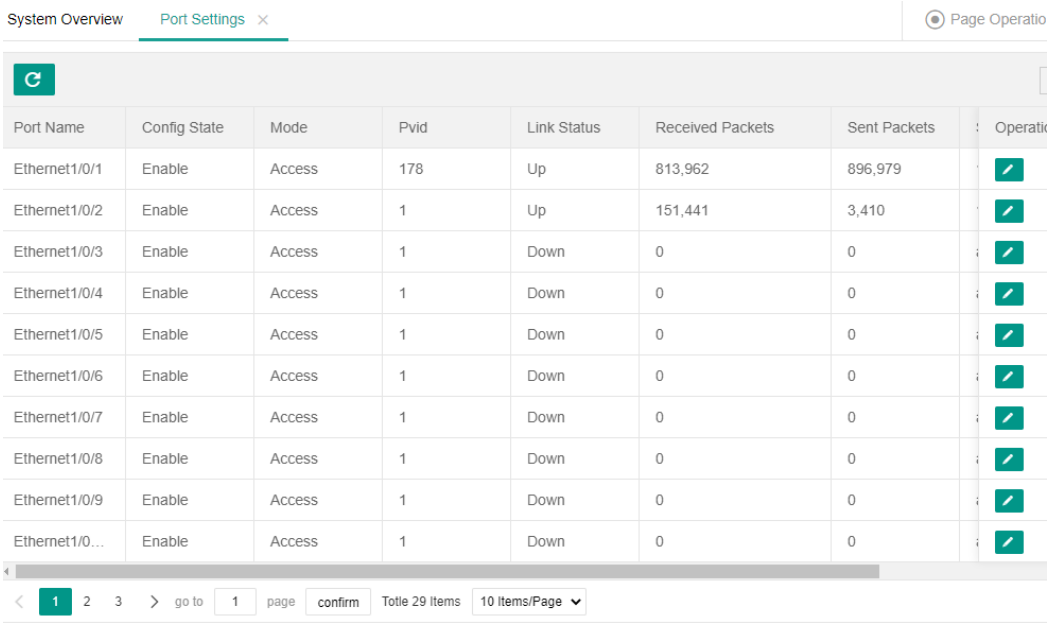
3.3Basic Network

3.3.1. Port Management

【Basic Network】→ [Port Management]: check the status of device port and modify the Vlan configuration for port.

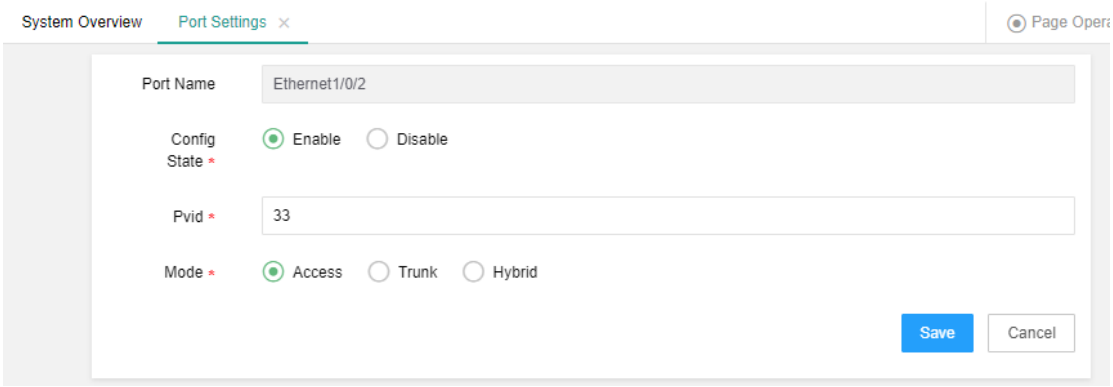
3.3.1.1. Check Port

【Basic Network】→ [Port Management]: check the current status of port via the following list, including port name, configuration status, port mode, port PVID, link status, number of received packets, number of sent packets, rate and duplex mode.



3.3.1.2. Edit Port

【Basic Network】→ [Port Management] → select the port to be changed, click the rightmost edit button  and enter the edit page. The user can choose to configure the port configuration status, Pvid and mode.

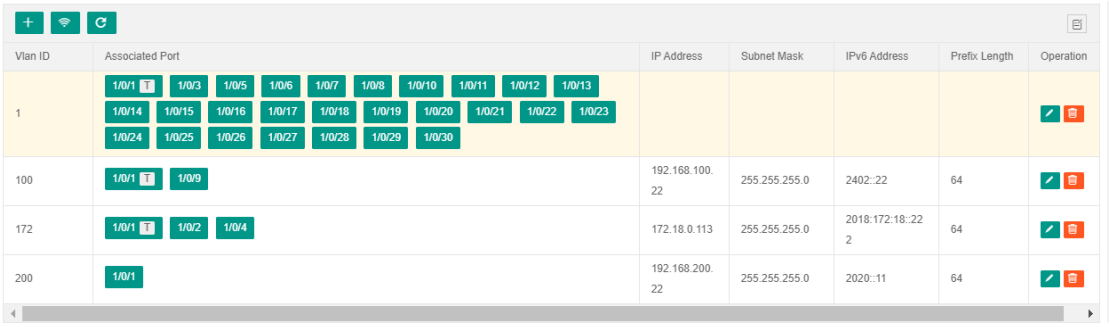


3.3.2. Vlan Management

【Basic Network】→ [VLAN Management]: view the current Vlan list, configure or add Vlan and Ip (Ipv6) address, configure wireless binding address, and configure port Vlan.

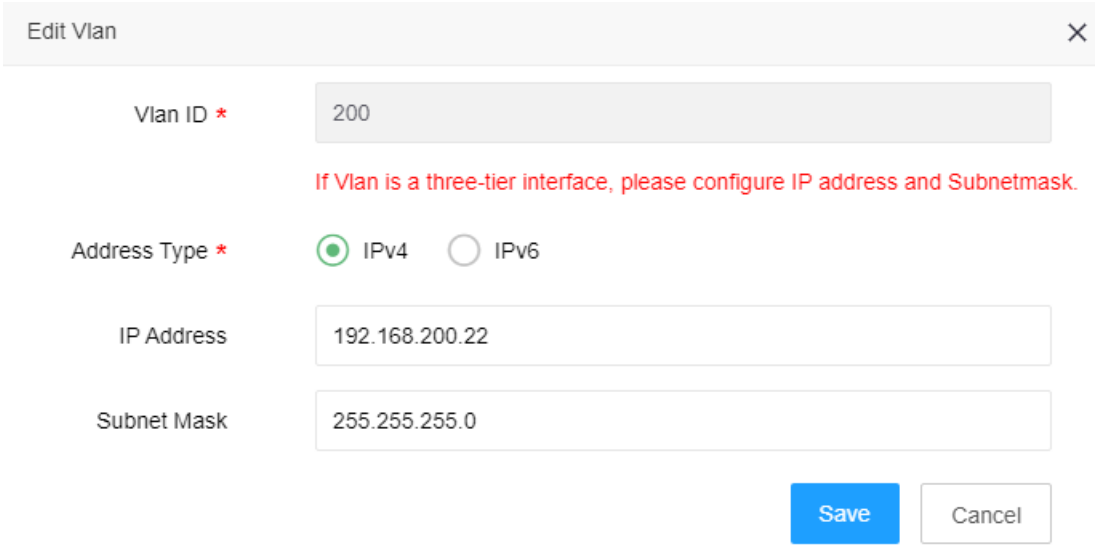
3.3.2.1. Check Vlan

【Basic Network】→ [VLAN Management]: view the Vlan list of AC system, corresponding associated port, Ipv4 address and Ipv6 address.

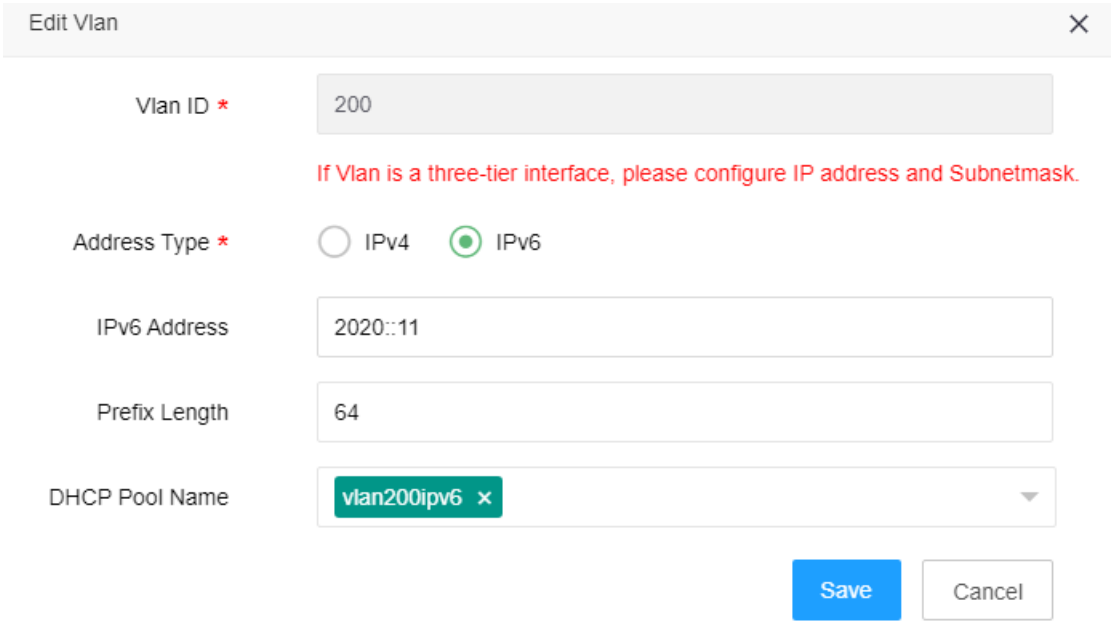


3.3.2.2. Change Vlan

(1) 【Basic Network】→ [VLAN Management]: click the right button  to change the Ipv4 address and mask of the Vlan.



(2) When editing the Vlan, select Ipv6 as the address type. The user may modify the Ipv6 address, prefix length and address pool name of the Vlan.



Select the address pool name as the action taken for DHCPv6 configuration. Here's a brief introduction to DHCPv6 configuration processes:

1. 【Basic Network】→ [DHCP Server]] → select Ipv6 to enable DHCPv6;

2. Add DHCPv6 address pool and save it;

3. Vlan will bind the address pool to the corresponding interface;

4. Router advertisement (RA) configuration shall be done in serial port if needed (it can't be realized in current Web)

ipv6 address 2222::100/64

no ipv6 nd suppress-ra

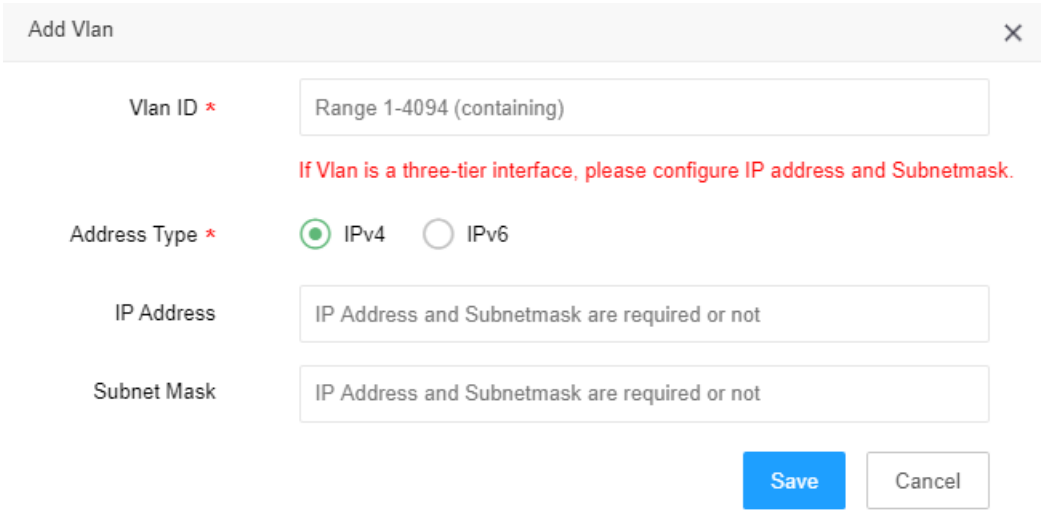
ipv6 nd managed-config-flag

ipv6 nd other-config-flag

ipv6 nd prefix 2222::/64

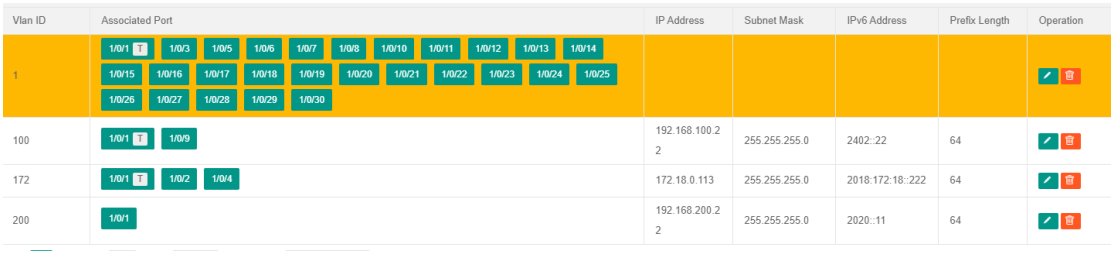
3.3.2.3. Add Vlan

【Basic Network】→ [VLAN Management]: select the Add button  at the top left to configure Vlan ID, address type, IP address and subnet mask, then click "Save". The Vlan is added successfully.



3.3.2.4. Delete Vlan

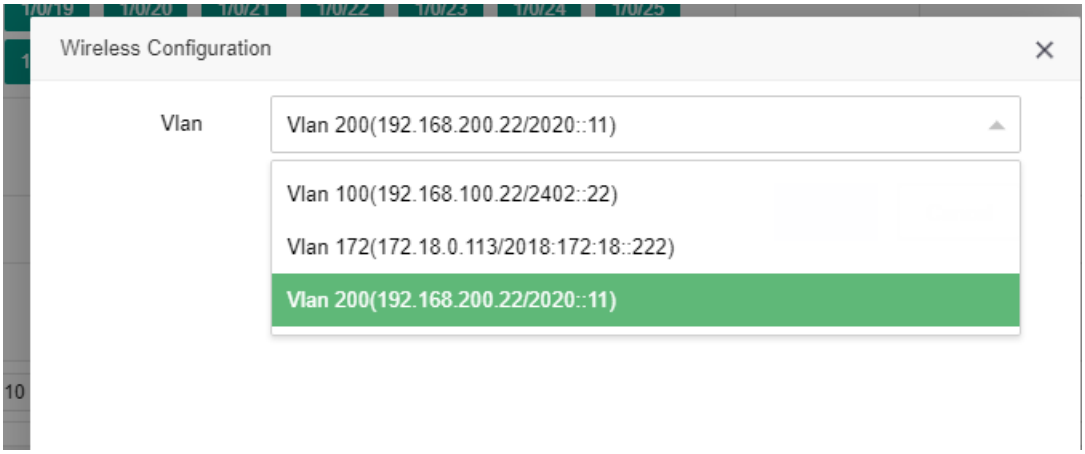
【Basic Network】→ [VLAN Management]: select the right Delete button  , and click OK to delete the Vlan.



When the Vlan is deleted, the corresponding Pvid of the Vlan will also be deleted and the Vlan will restore to the default Vlan1.

3.3.2.5. Configure Wireless Address

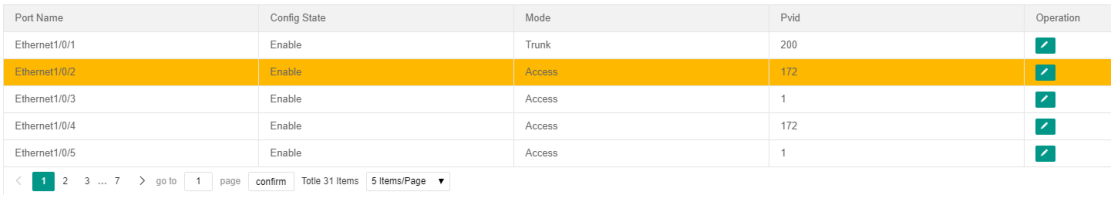
【Basic Network】→ [Vlan Management]: click the wireless configuration button  on the top of the list, then select the corresponding Vlan as the wireless address of the system.



3.3.2.6. Check and Configure Port Vlan

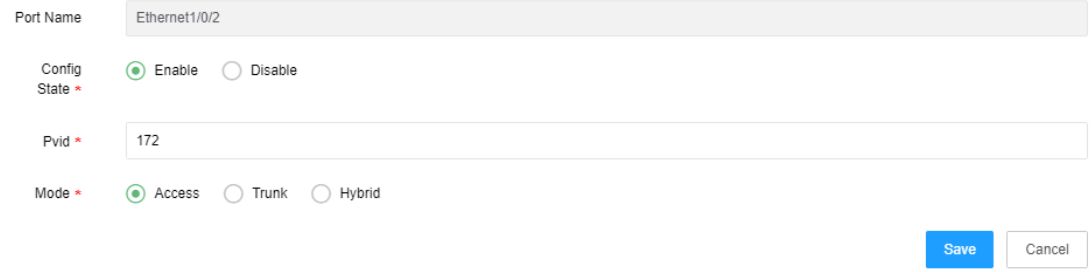
(1) Check port Vlan information

【Basic Network】→ [Vlan Management]: the port list below will display the port configuration information.



(2) Configure port Vlan

【Basic Networ】→ [Vlan Management]: click the right Edit button  to edit the port Vlan.



The ultimate effect of port Vlan configuration here is the same as the result of "3.3.1.2 Change Port".

3.3.3. DHCP Service

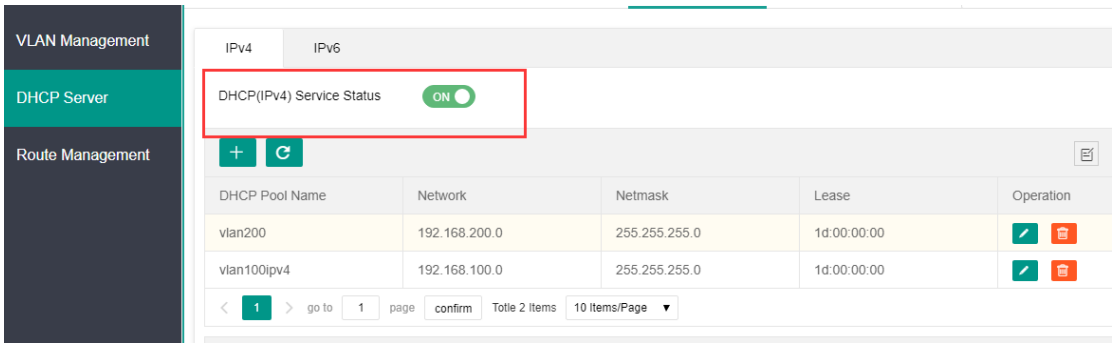
AC can serve as a DHCP server for Ipv4 and Ipv6.

3.3.3.1. DHCP (IPv4) Service

DHCP Ipv4 service provides Ipv4 IP address, default gateway, Option43 and DNS server configuration for terminals. Reserved address can also be configured for specific clients.

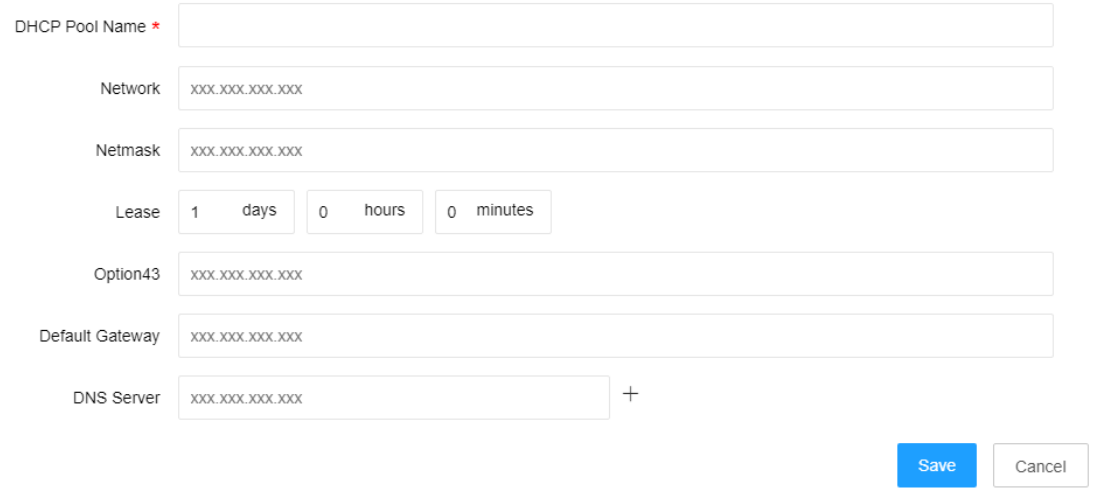
i. DHCP (IPv4) service switch

【Basic Networ】→ [DHCP Server]: the server switch is turned off by default, and the configured address pool will become effective only when the service switch is turned on.



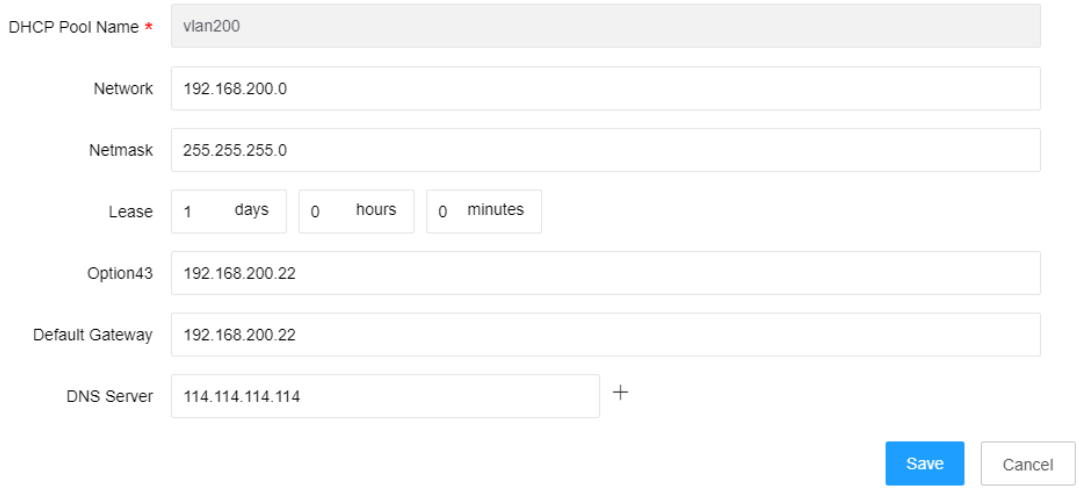
ii. Add DHCP (IPv4) address pool

【Basic Networ】→ [DHCP Server]: click "Add Address Pool" button , fill in the address pool name, network, mask, lease period, Option43, default gateway and DNS server, then click "Save".



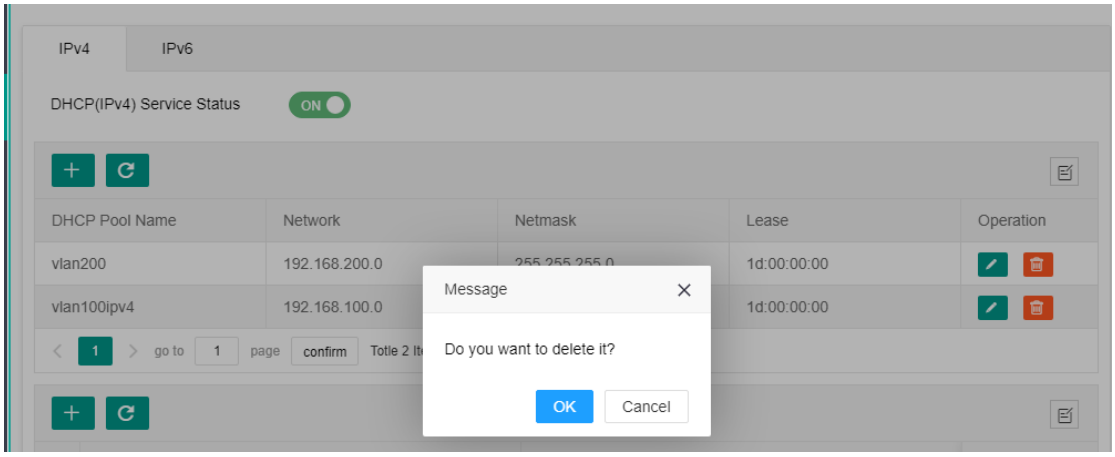
iii. Change DHCP (IPv4) address pool

【Basic Networ】→ [DHCP Server]: select the address pool, click "Change" button to change the address pool name, network, mask, lease period, Option43, default gateway and DNS server, then click "Save".



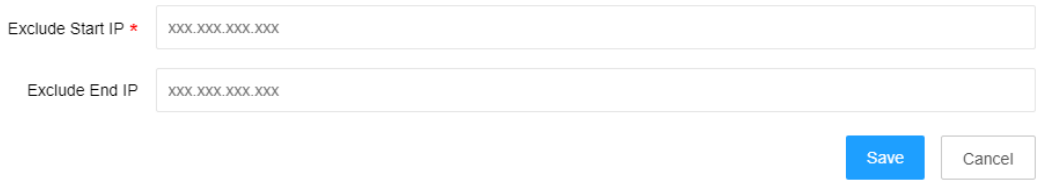
iv. Delete DHCP (IPv4) address pool

【Basic Networ】→ [DHCP Server]: select the address pool, click "Delete" button to delete the corresponding address pool. Click "OK" to save.



v. Configure DHCP (IPv4) reserved address

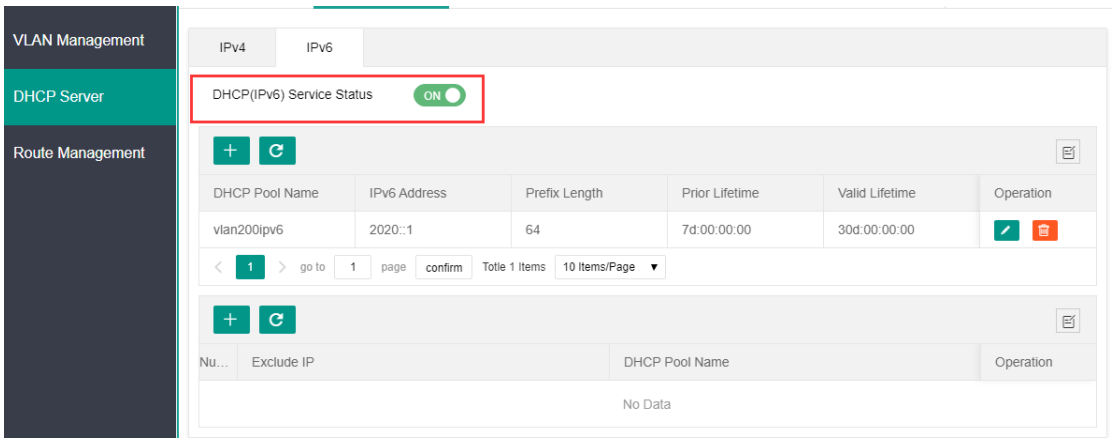
【Basic Networ】→ [DHCP Server]: click "Add Reserved Address" button  to add reserved address field, which won't be assigned to the client.



3.3.3.2. DHCPv6 Service

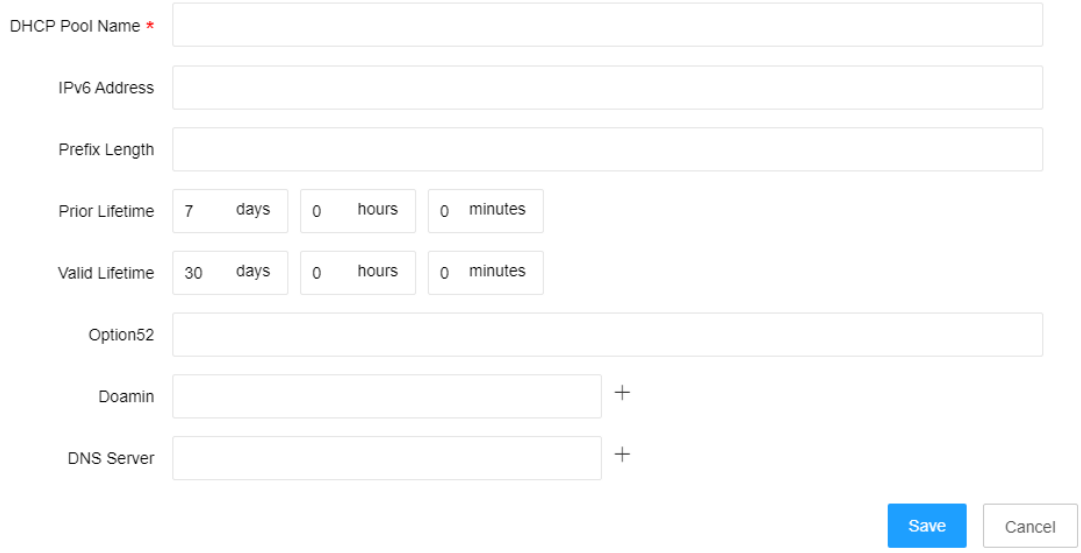
vi. DHCPv6service switch

【Basic Networ】→ [DHCP Server]: switch to Ipv6, the server switch is turned off by default, and the configured DHCPv6 address pool will become effective only when the server switch is turned on.



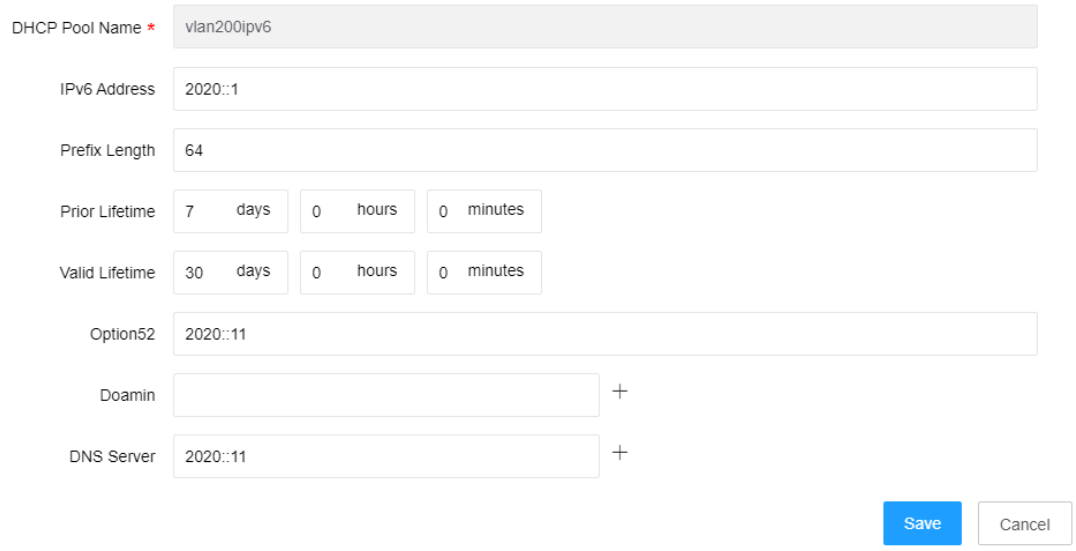
vii. Add DHCPv6 address pool

【Basic Networ】→ [DHCP Server]: switch to Ipv6, add a new address pool, fill in the address pool name, IPv6 address field, lifetime, Option52, domain name and DNS server, then click "Save".



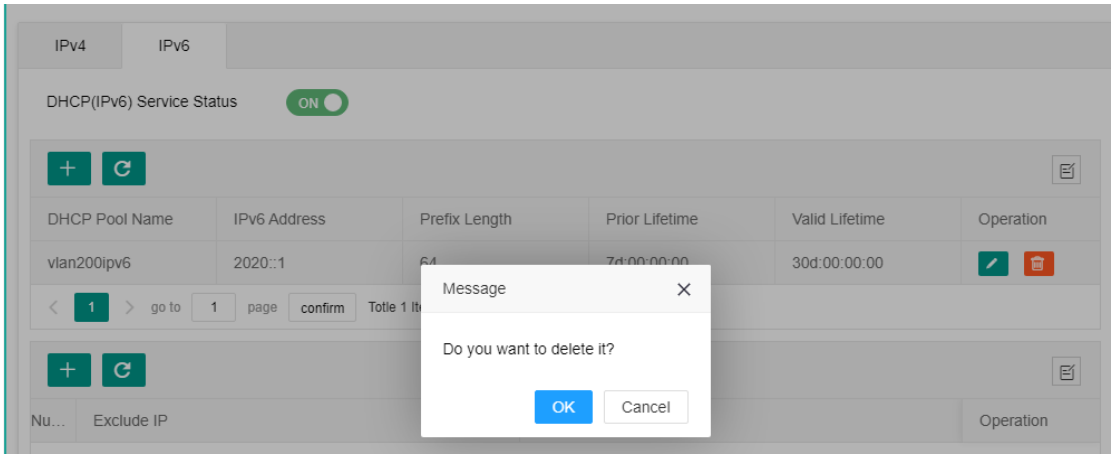
viii. Change DHCPv6 address pool

【Basic Networ】→ [DHCP Server]: switch to Ipv6, modify the address pool in the list and various information, then click "Save".



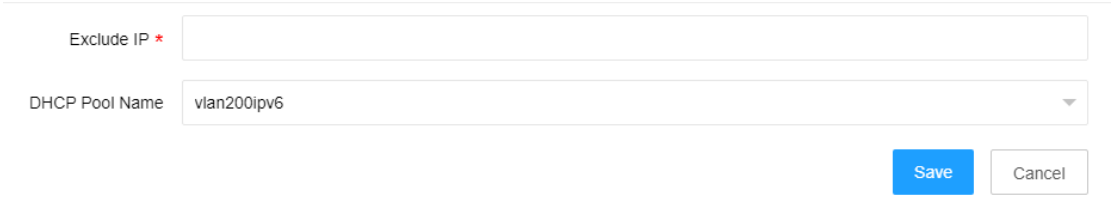
ix. Delete DHCPv6 address pool

【Basic Networ】→ [DHCP Server]: switch to Ipv6, select the address pool in the list, click the right "Delete" button and click "OK".



x. Configure DHCPv6 reserved address

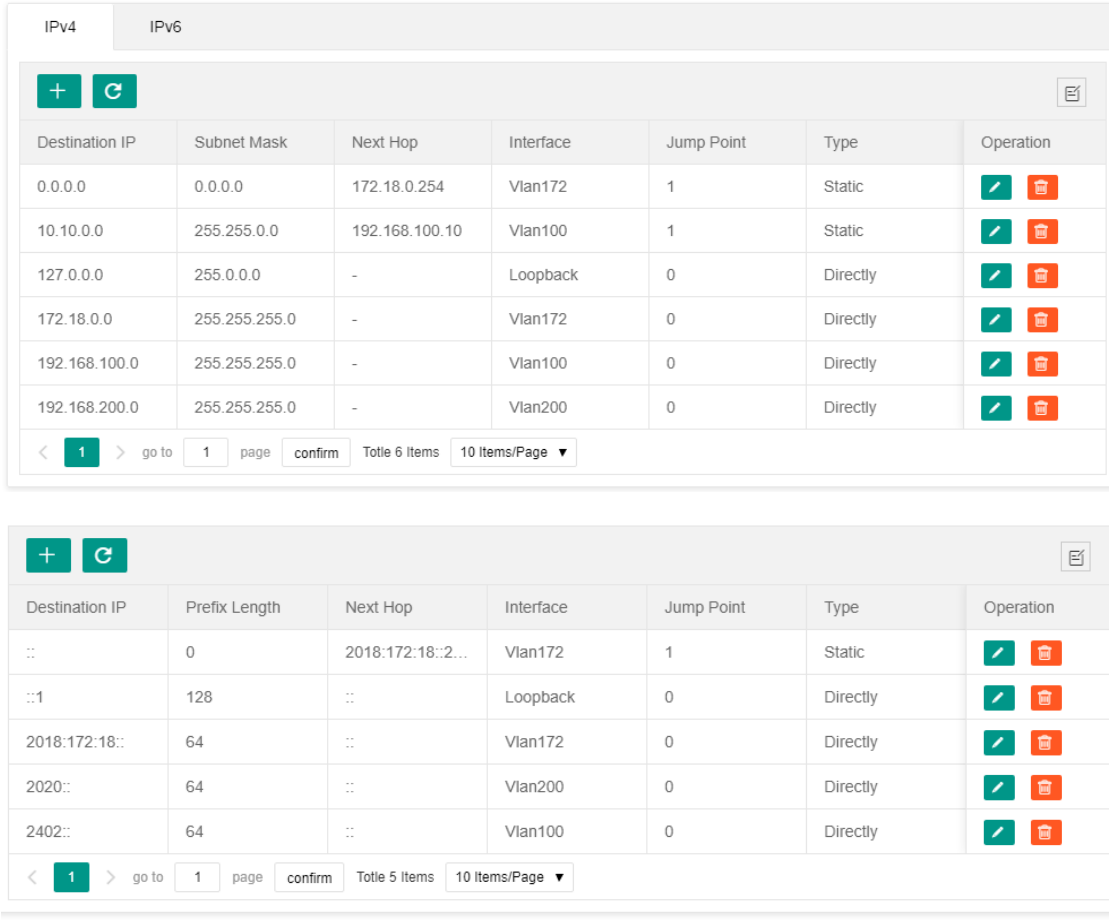
【Basic Network】→ [DHCP Server]: switch to Ipv6, click "Add Reserved Address" button , select the address pool and fill in the reserved address. Unlike Ipv4, Ipv6 can be only configured with a single reserved address instead of address field.



3.3.4. Routing Management

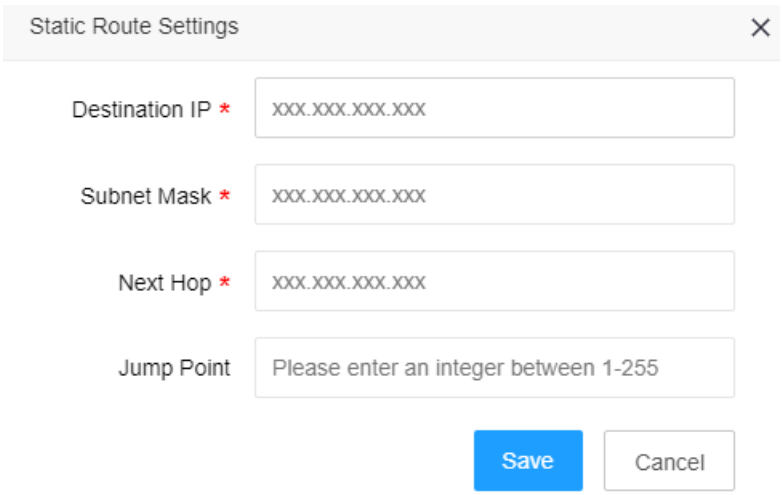
3.3.4.1. Check Routing

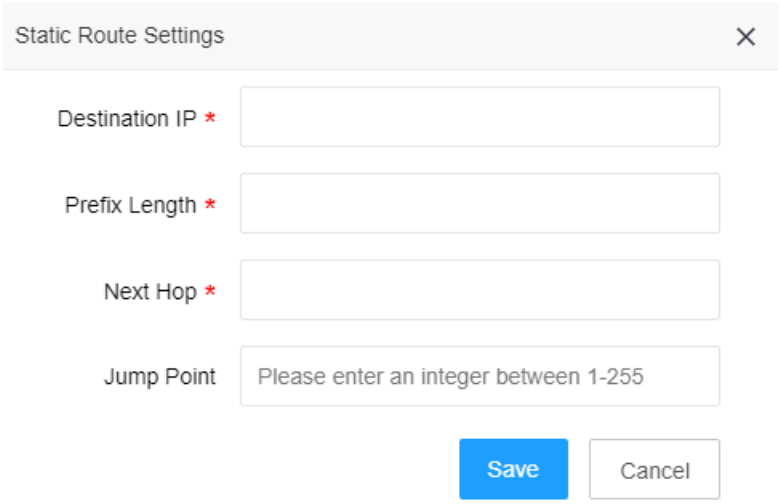
【Basic Network】→ [Route Management]: switch to Ipv4/Ipv6 and see all routing information.



3.3.4.2. Add Static Routing

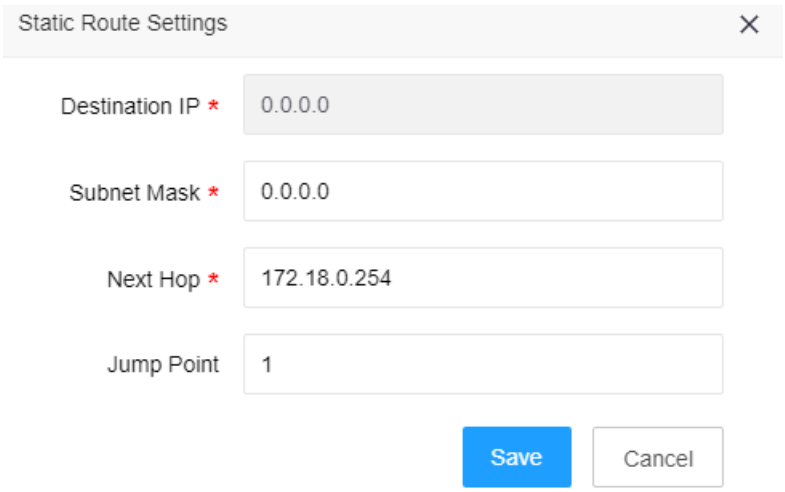
【Basic Network】→ [Route Management]: switch to Ipv4/Ipv6, click "Add" button  , fill in all items and click "Save".

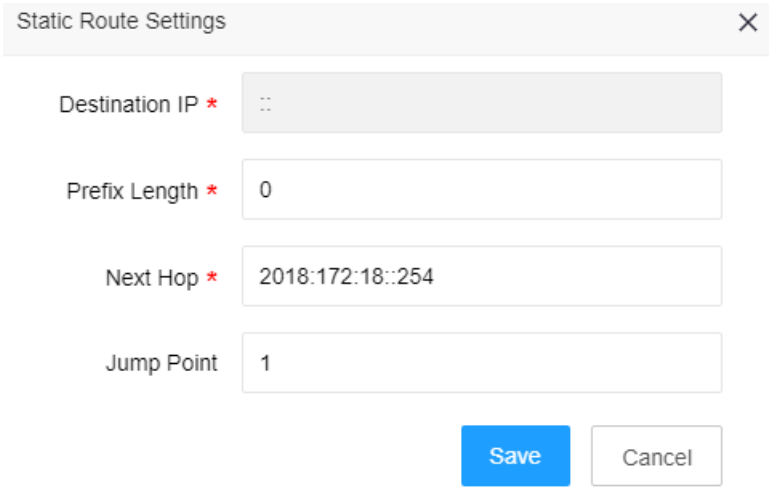




3.3.4.3. Edit Routing

【Basic Network】→ [Route Management]: switch to Ipv4/Ipv6, select the routing entry to be edited, click "Edit" button to make modifications, and then, click "Save".





3.3.4.4. Delete Routing

【Basic Network】→ [Route Management]: switch to Ipv4/Ipv6, select the routing entry, click the right "Delete" button and click "OK".

3.4 Wireless Network

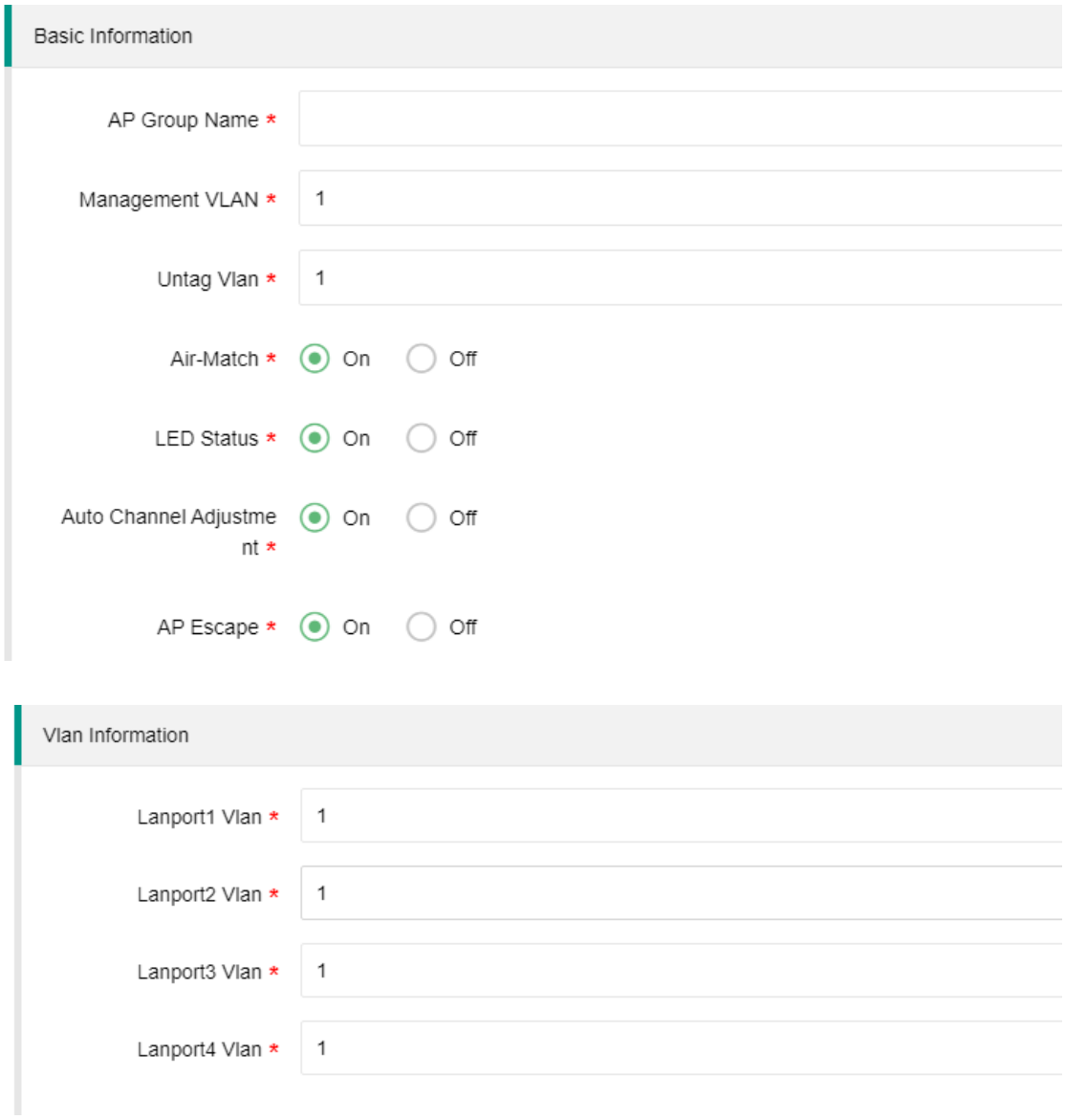
The wireless network module is used to display AP/STA information and to configure AP/SSID/authentication.

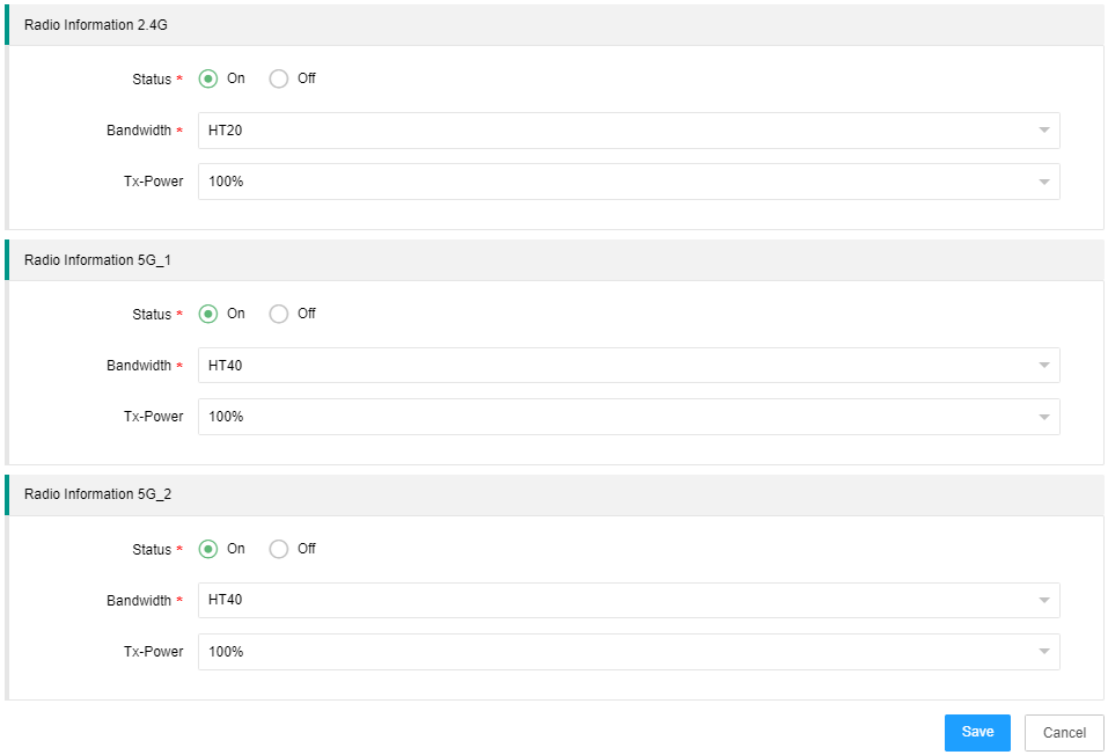
3.4.1. AP Management - AP Group List

After AP group is configured, new online AP will be assigned to the default group by default and can be reassigned to the newly established AP group. As a template for AP configuration, AP group can uniformly configure the "Basic Information", "Vlan Information" and "RF Information" for AP.

3.4.1.1. Add AP Group List

【Wireless Network】→ [AP Management]: select "AP Group List ", click "Add" button to configure the "Basic Information ", "Vlan Information" and "RF Information", and then click "Save".


Basic Information
AP Group Name *
Management VLAN * 1
Untag Vlan * 1
Air-Match * On Off
LED Status * On Off
Auto Channel Adjustment * On Off
AP Escape * On Off
Vlan Information
Lanport1 Vlan * 1
Lanport2 Vlan * 1
Lanport3 Vlan * 1
Lanport4 Vlan * 1



Description of Configuration Items

Admin Vlan: Vlan assigned by the administrator for AP group. Default Admin Vlan is 1;

Untag Vlan: Vlan whose Tag should be removed when it gets out from the uplink interface of AP. If AP or STA has the same ID, the Tag can also be removed.

Air-Match: in case of mass access, it will balance the load on each AP and radio based on the number of users.

LED state: after the LED is turned on, AP outside indicator light will reflect the current status of the AP, where normal white light indicates "power on", fast green flashing indicates that the system has been started but AP is offline or is being upgraded, slow blue flashing indicates that AP is accessible, and red normal light indicates AP failure. Due to the differences in each product, please consult the customer service or look up the AP product manual for the meaning of LED lights.

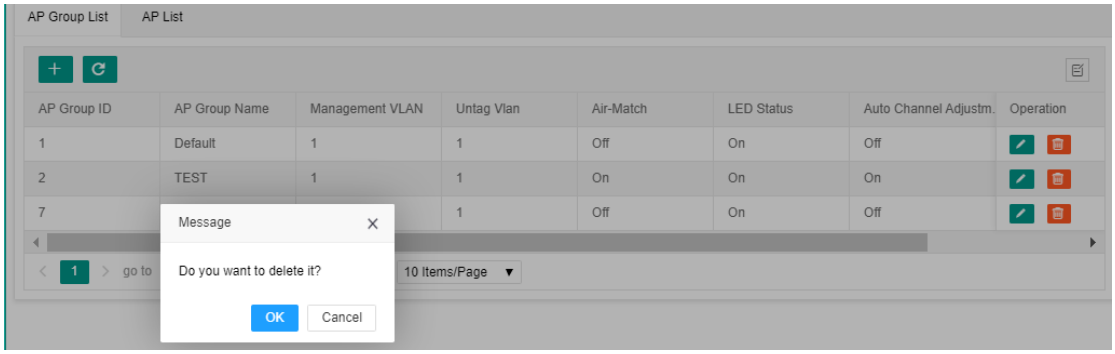
Automatic Channel Adjustment: automatic channel adjustment made by default at 5:00 a.m. to avoid interference to AP radio frequency.

AP Escape: when AC isn't accessible after AP is offline, AP can continue to provide unblocked network for authenticated wireless users.

Downlink interface Vlan: Vlan obtained by user that is connected to the downlink wired interface of AP. It can be equipped with 4 ports. The APs with different numbers of ports are configured correspondingly from top to bottom.

3.4.1.2. Delete AP Group List

【Wireless Network】→ [AP Management]: select "AP Group List", choose the AP group to be deleted, click "Delete" button and then click "Save".



Note: The "Default" AP group is not allowed to be deleted, nor can it be deleted.

3.4.1.3. Change AP Group List

【Wireless Network】→ [AP Management]: select "AP Group List", choose the AP group to be deleted, click "Edit" button to edit the "Basic Information", "Vlan Information" and "RF Information", then click "Save".

3.4.2. AP Management -AP List

3.4.2.1. Add AP

(1) Manually add AP

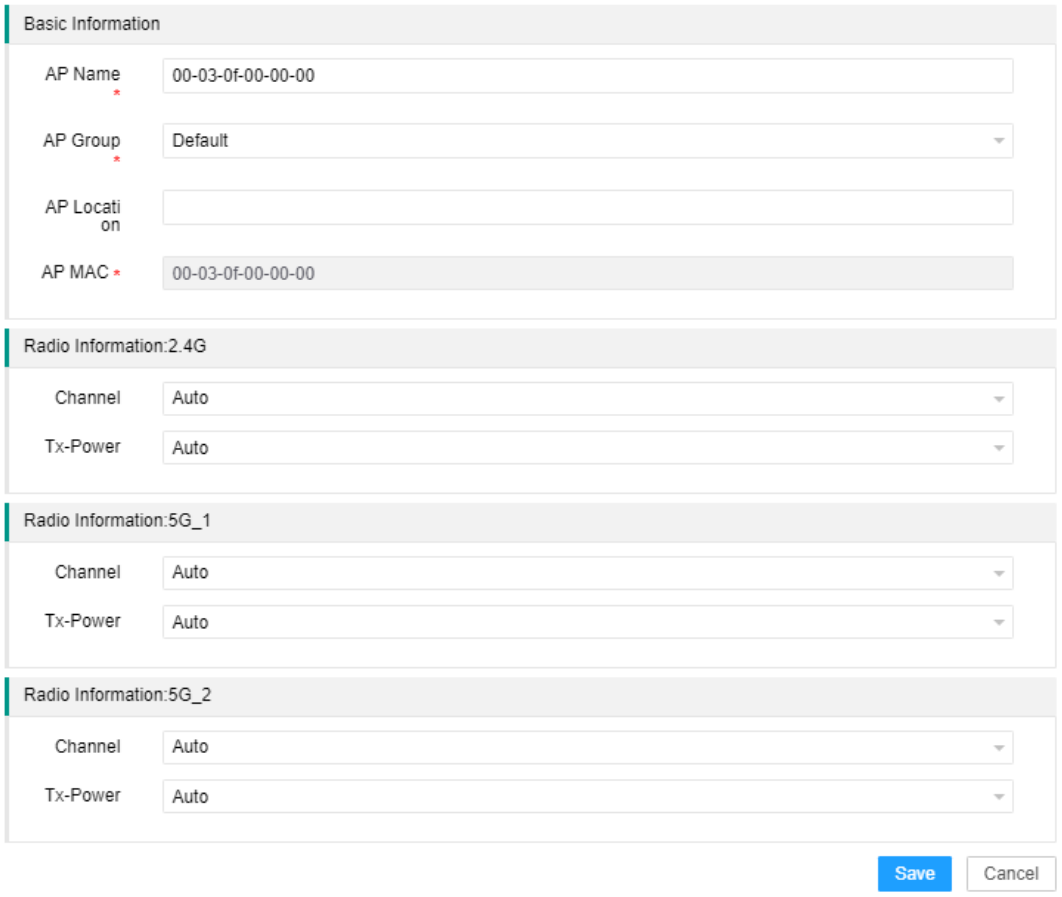
【Wireless Network】→ [AP Management]: select "AP List", click on the top of the list to configure AP name, AP group, AP location and AP MAC, then click "Save". Manually adding AP can configure the AP in advance before it goes online.

(2) Automatically add online AP

After finding AC, AP will automatically add to the default AP group once AC goes online. The name defaults to AP-MAC and AP position is vacant.

3.4.2.2. Change AP

【Wireless Network】→ [AP Management]: select "AP List", choose the corresponding AP and click "Edit" button  to edit the "Basic Information" and "RF Information". Edited "RF Information" shall be saved and take effect upon AP restart.



3.4.2.3. Delete AP

【Wireless Network】→ [AP Management]: select "AP List", choose the AP to be deleted and click "Delete" button  . Currently managed AP can't be deleted, and offline AP that has been deleted will be assigned to the default AP group once it comes online again.

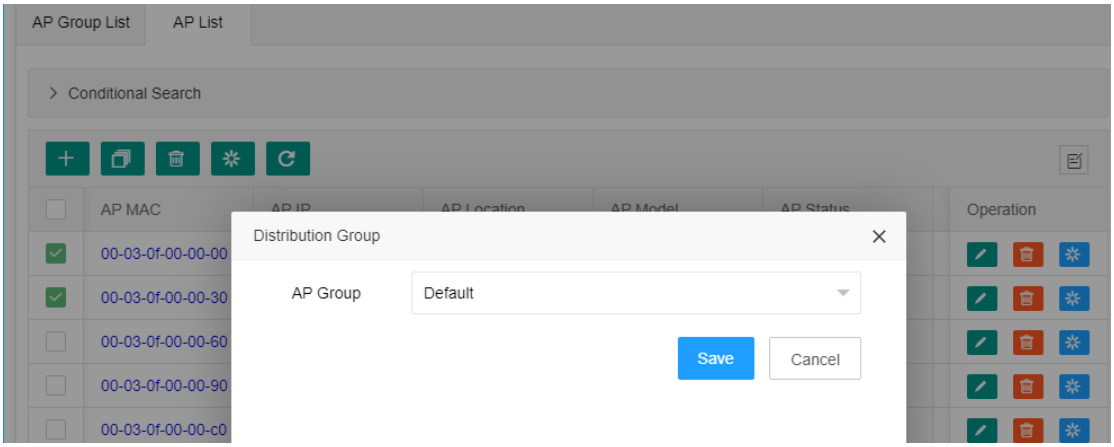
3.4.2.4. Restart AP

【Wireless Network】→ [AP Management]: select "AP List", choose the AP to be restarted and click "Restart" button  . Click "OK", AP will be restarted. Offline AP can't be restarted from AC.

3.4.2.5. Batch Operations

(1) Assign groups in batch

【Wireless Network】→ [AP Management]: select "AP List", tick APs to be assigned to the same group, click "Assign Group in Batch" button  on the top of the list. Click "Save", newly assigned APs will restart and back online.



(2) Batch delete

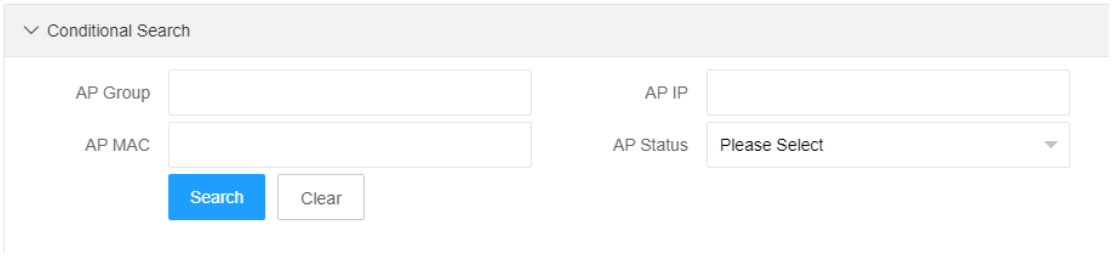
【Wireless Network】→ [AP Management]: select "AP List", tick (offline) APs to be deleted, click "Delete" button  on the top of the list. Click "OK", offline APs will be deleted successfully. Online APs can't be deleted.

(3) Batch restart

【Wireless Network】→ [AP Management]: select "AP List", tick (online) APs to be deleted, click "Restart" button  on the top of the list. Click "OK", online APs will get restarted. Offline APs can't be restarted in batches.

3.4.2.6. AP Criteria Query

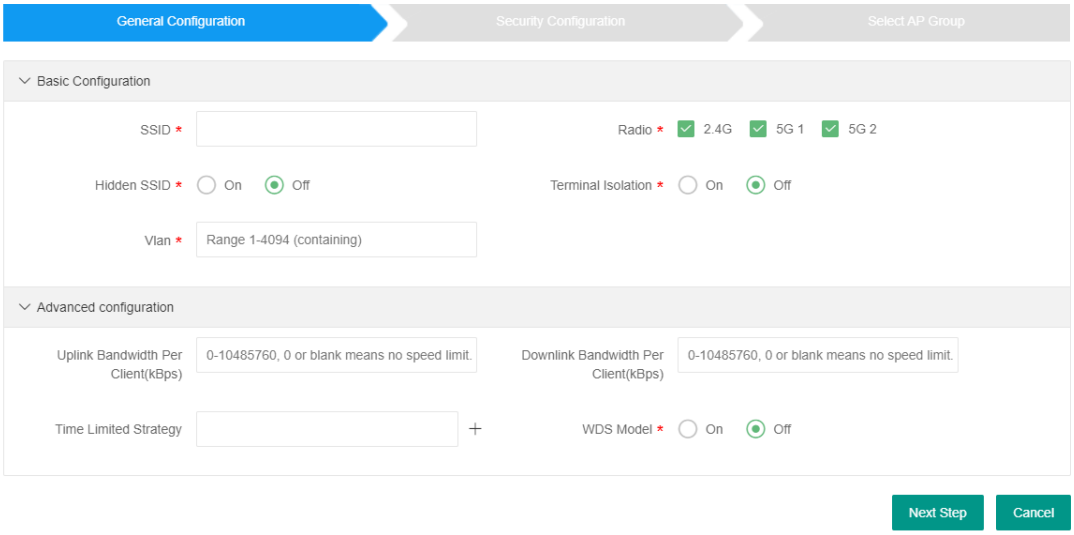
【Wireless Network】→ [AP Management]: select "AP List" and click "Conditional Search" to make queries according to different criteria. If several criteria are used simultaneously, their relation shall be "And".

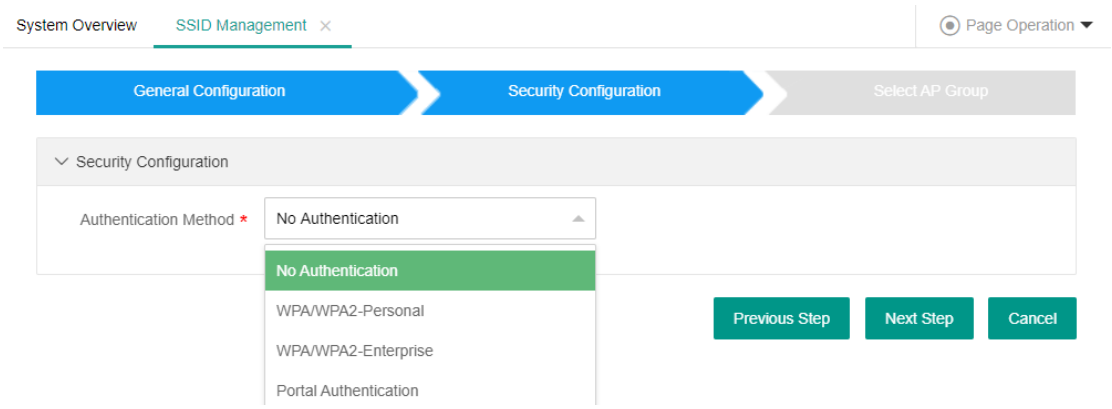


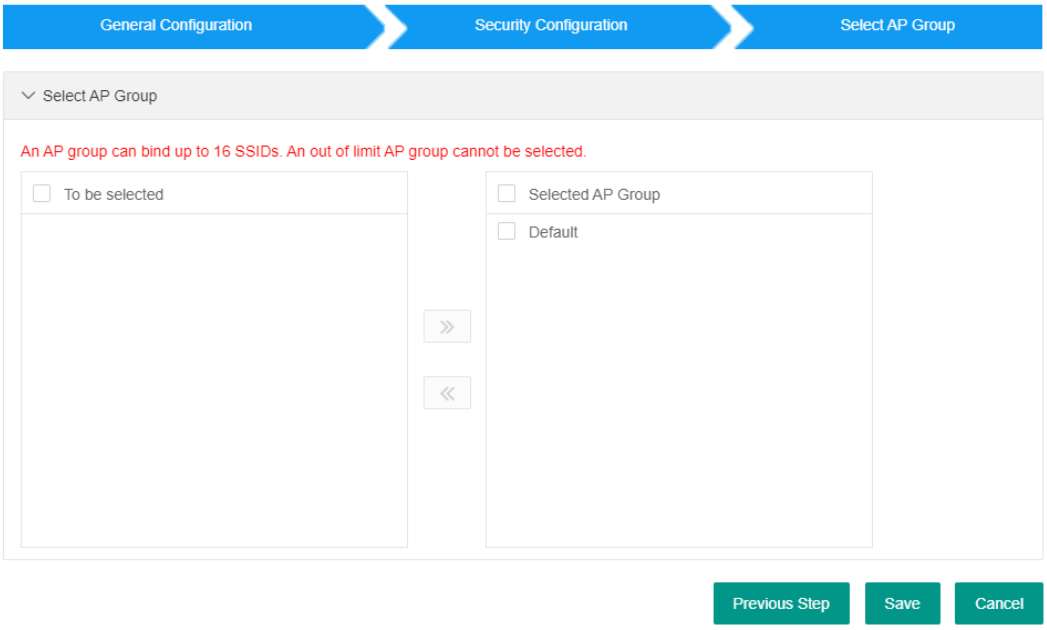
3.4.3. SSID Management

3.4.3.1. Add SSID

【Basic Network】→ [SSID Management]: click "Add" button  to make general configuration and security configuration, then select the AP group and click "Save". SSID is set up successfully.


General Configuration
Security Configuration
Select AP Group
Basic Configuration
SSID *
Radio * 2.4G 5G 1 5G 2
Hidden SSID * On Off
Terminal Isolation * On Off
Vlan * Range 1-4094 (containing)
Advanced configuration
Uplink Bandwidth Per Client(kBps)
0-10485760, 0 or blank means no speed limit.
Downlink Bandwidth Per Client(kBps)
0-10485760, 0 or blank means no speed limit.
Time Limited Strategy
WDS Model * On Off
Next Step
Cancel


System Overview
SSID Management
Page Operation
General Configuration
Security Configuration
Select AP Group
Security Configuration
Authentication Method *
No Authentication
No Authentication
WPA/WPA2-Personal
WPA/WPA2-Enterprise
Portal Authentication
Previous Step
Next Step
Cancel


General Configuration
Security Configuration
Select AP Group
Select AP Group
An AP group can bind up to 16 SSIDs. An out of limit AP group cannot be selected.
To be selected
Selected AP Group
Default
Previous Step
Save
Cancel

SSID configuration includes general configuration, security configuration and selection of AP group, wherein:

Hidden SSID： SSID isn't displayed in the SSID list when a user searches, but is accessible by entering the correct SSID name;

Terminal isolation: isolate LAN communication from users sharing the same SSID to ensure that no malicious broadcast messages affect the network quality;

Time Limit Strategy: within the time limit, SSID is closed and the user has no access;

WDS mode: in this mode, AP can use the SSID to extend wireless network with other APs;

Portal authentication: it's necessary to select the Portal authentication template, which will be introduced in Section 3.4.4;

WPA/WPA2-Enterprise: to be used in conjunction with external portal, which will be introduced in Section 3.4.4;

Binding to AP group: SSID will be broadcast by AP in the AP group only after it's bound to the AP group.

3.4.3.2. Change SSID

【Basic Network】→ [SSID Management]: select the SSID to be modified, click "Change" button to reconfigure the general configuration, advanced configuration, security configuration and selection of AP group of SSID, then click "Save".

3.4.3.3. Delete SSID

【Basic Network】→ [SSID Management]: select the SSID to be deleted, click "Delete" button . Click "OK", SSID will be deleted.

3.4.4. Authentication Management

Make configurations for the authentication of users who have access to the wireless network, mainly including Portal authentication and Enterprise 1 x authentication.

If portal authentication is used, the following 3 conditions shall be met:

1. STA has access to the portal server network.

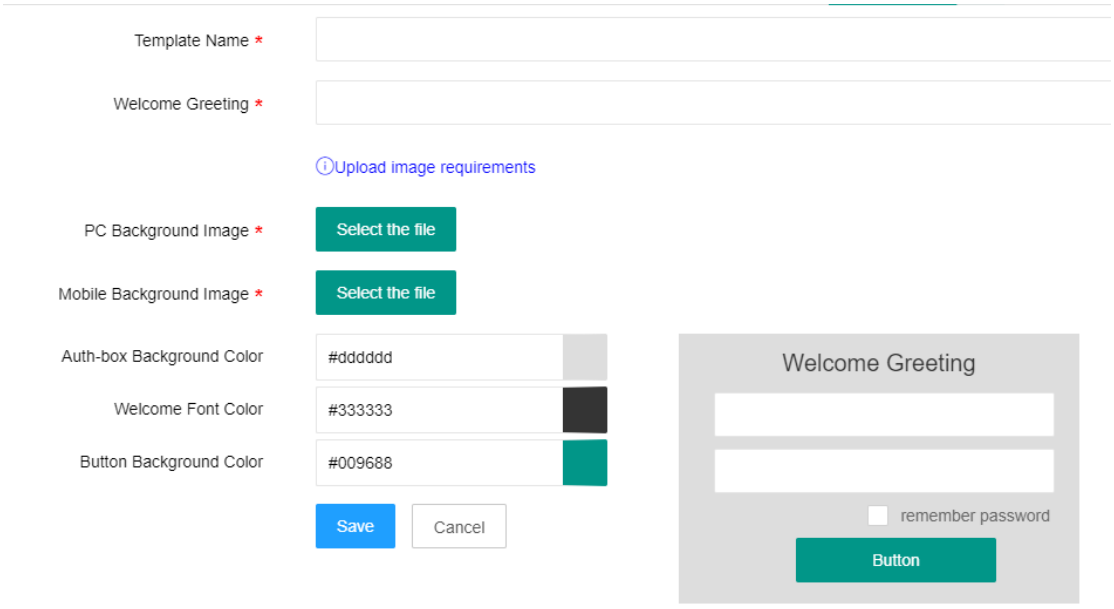
2. Correct DNS server is configured for the STA. If DNS server is incorrect or STA is not connected to the internet network, portal authentication shall be triggered manually by accessing the IP address on the browser, such as http://2.3.4.5, etc.

3. Non-Sense defaults to disabled. To enable it, you need to configure at the command line (configure fast-mac-auth in the captive portal instance).

3.4.4.1. Authentication Page Template

i. Add authentication page template

【Wireless Network】→ [Authentication Management]: select "Authentication Page Template", click "Add" button and configure the template name, welcome speech, background picture and colors. Then, click "Save", authentication page template is added successfully. You can add up to two templates.

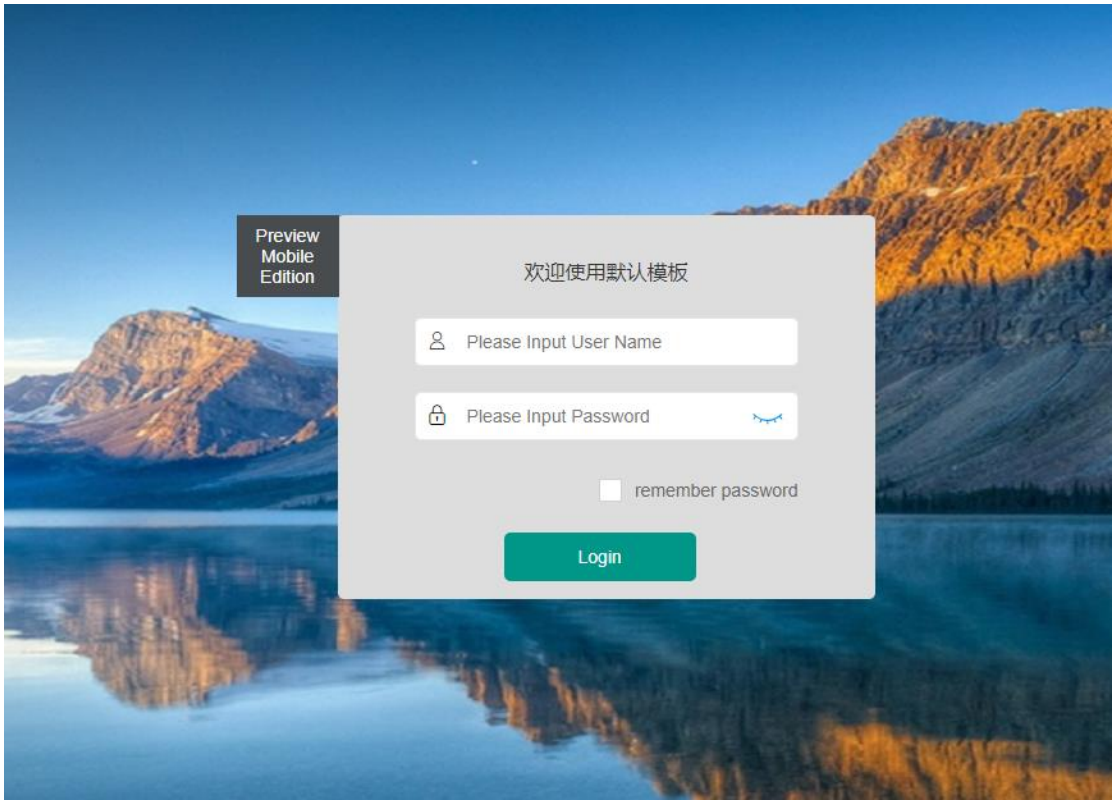


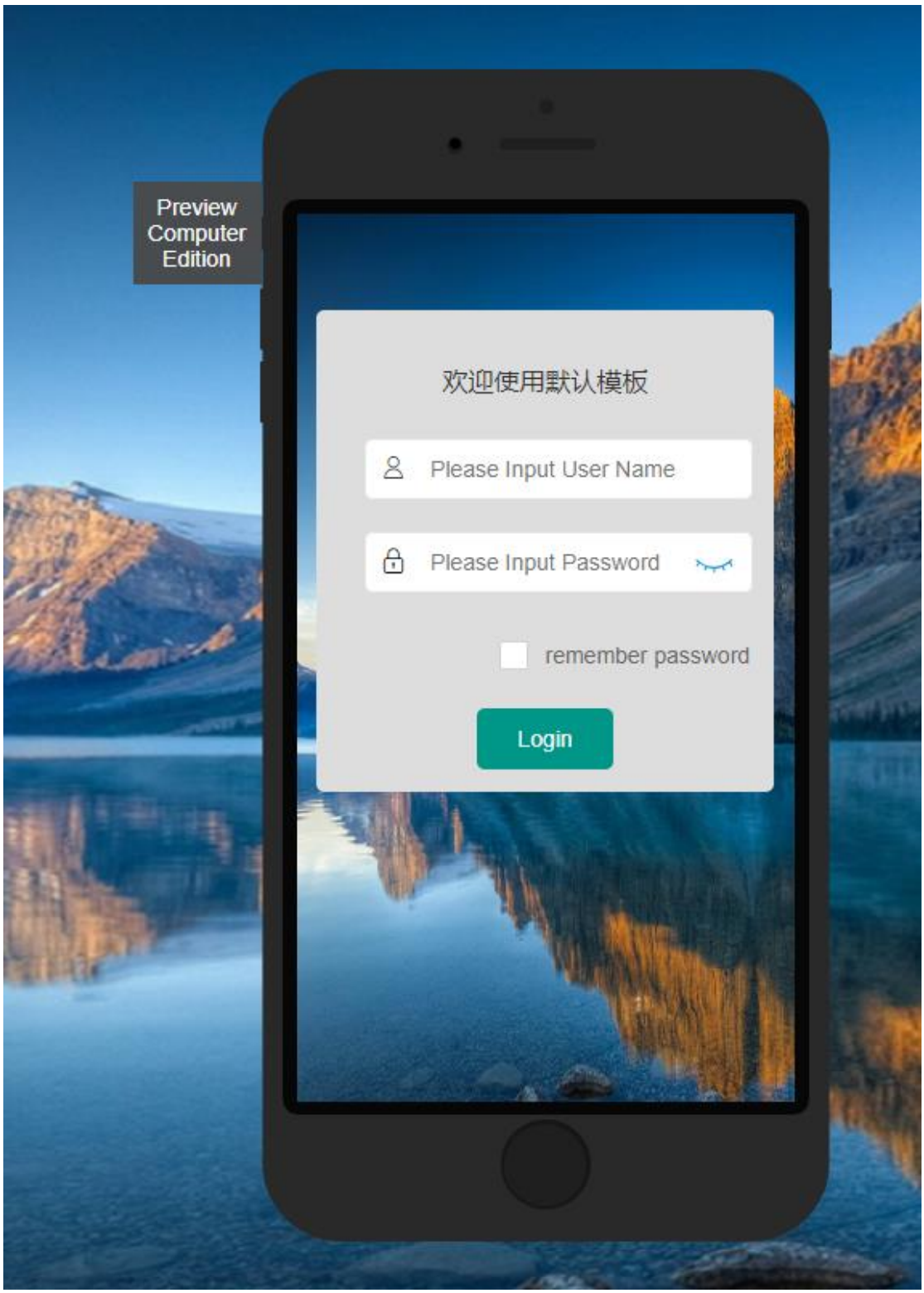
ii. Change authentication page template

【Wireless Network】→ [Authentication Management]: select "Authentication Page Template", choose the authentication page template, then click "Edit" button to edit the default and new templates.

iii. Preview authentication page template

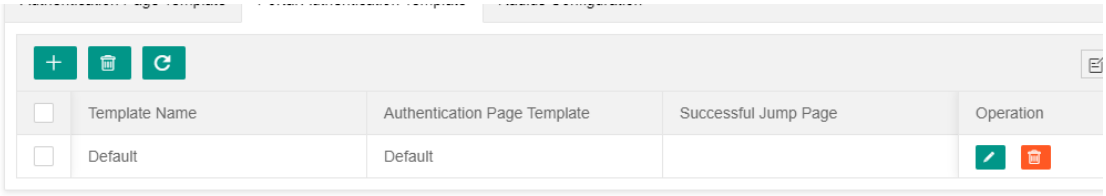
【Wireless Network】→ [Authentication Management]: select "Authentication Page Template", choose the authentication page template, then click "Preview" button and choose PC preview or mobile client preview in the pop-up page.




Preview
Computer
Edition
欢迎使用默认模板
Please Input User Name
Please Input Password
remember password
Login

iv. Delete authentication page template

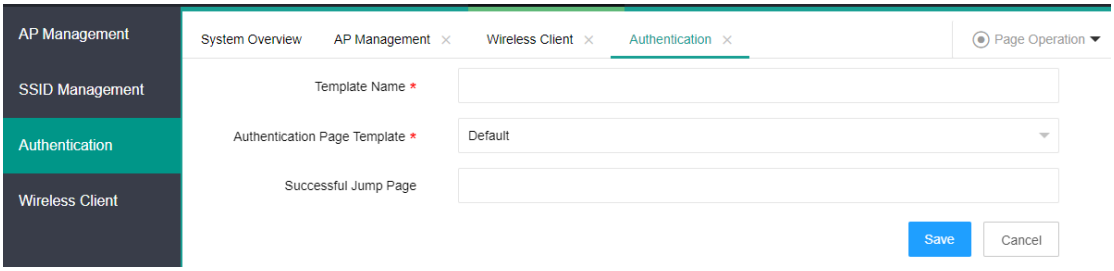
【Wireless Network】→ [Authentication Management]: select "Authentication Page Template", choose the authentication page template, then click "Delete" button. Upon confirmation, the selected template will be deleted. Default template can't be deleted.



3.4.4.2. Portal Authentication Template

i. Add authentication page template

【Wireless Network】→ [Authentication Management]: select "Portal Authentication Template", then bind the authentication page template and successful-authentication jump page. This configuration can be used for SSID Portal authentication.



If there is no successful-authentication jump page, it will automatically jump to the page visited by the user previously upon user's successful authentication.

ii. Change authentication page template

【Wireless Network】→ [Authentication Management]: select "Portal Authentication Template", choose authentication page template from the list, then click "Change" button to change all items. Click "Save", the template will be updated in the list.

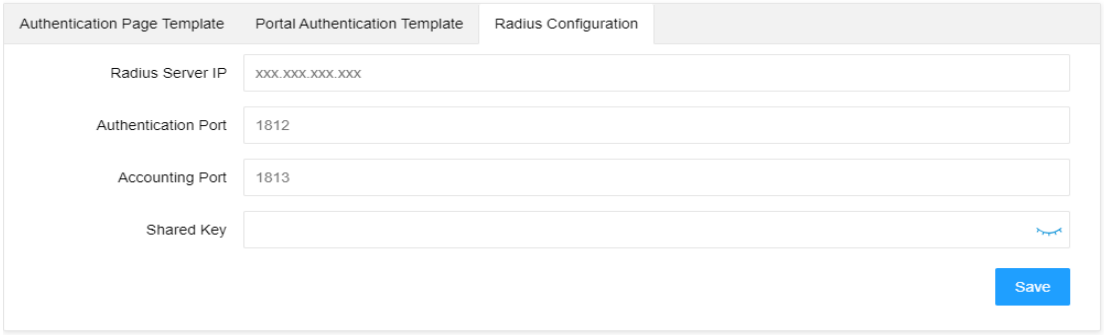
If a template name that has been bound to an SSID is changed, this SSID shall be rebound to a template.

iii. Delete authentication page template

【Wireless Network】→ [Authentication Management]: select "Portal Authentication Template", choose the authentication page template to be deleted from the list, then click "Delete" button and "OK" to delete the specified portal authentication template.

3.4.4.3. Radius Configuration Template

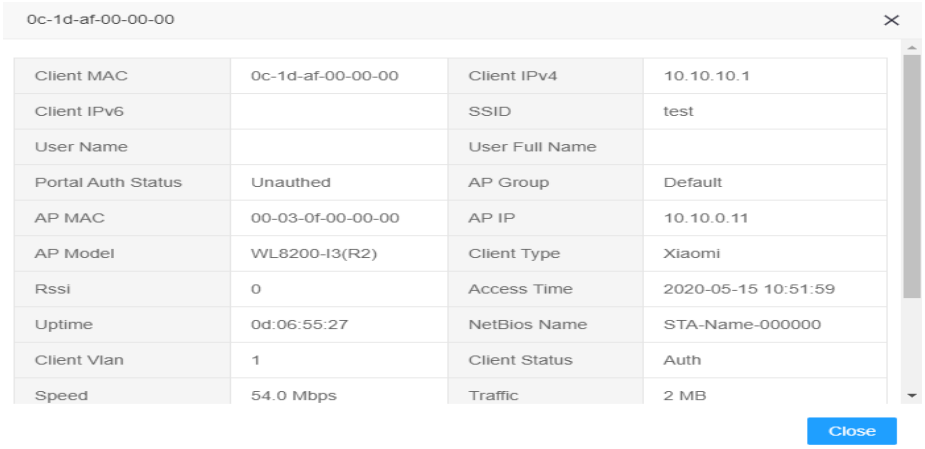
【Wireless Network】→ [Authentication Management]: select "Radius Configuration Template", then configure it after system is connected to a network and has access to an external Radius server. This configuration can be used for SSID 1x authentication.



3.4.5. AP Client

3.4.5.1. Check AP client

Upon user's access to SSID assigned by online AP under AC, click【Wireless Network】→ [Wireless Client], then click "Client MAC" in the list to see the client details.



3.4.5.2. Force Offline

Upon user's access to SSID assigned by online AP under AC, click【Wireless Network】→ [Wireless Client], then click "Force Offline" button 

in the Client List to disconnect the user from AP. Authenticated users who are forced offline need to re-authenticate for re-connection.

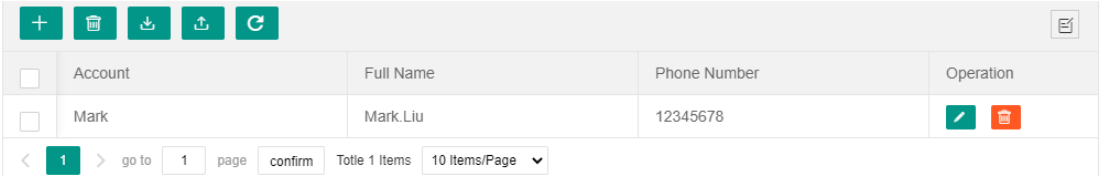
3.5 User Management

3.5.1. User Management

【User Management】: user name and password for built-in portal authentication of terminals are managed in this module. "User Management" allows to add, delete, modify, check, import and export the user information. Query criteria: account;

When adding user information, the following items can be added: account number, password, name and mobile phone number. Among them, account number and password are required, while name and mobile phone number are optional;

When importing user information, if there're plaintext and ciphertext in the import file, the plaintext shall control.

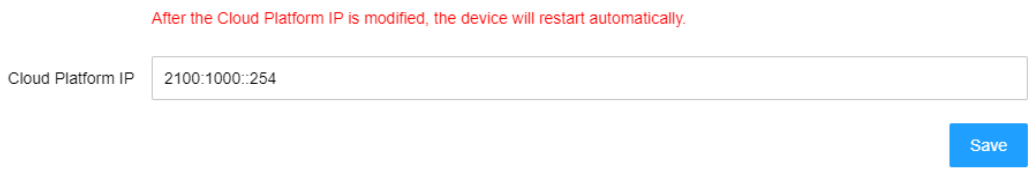


User Management here is used for the built-in portal authentication of terminals rather than for web login.

3.6 System Management

3.6.1. Cloud Management Settings

【System Management】→ [Cloud Management Settings]: if AC goes online on ImCloud as a Tier-2 AC, its cloud platform address can be configured in this module. This configuration supports both ipv4 and ipv6. User can input ip address directly without adding the prefix "http". See as below:



After cloud management settings are completed, AC will restart;

AC will synchronize ImCloud SSID and portal configurations after going online on ImColud.

3.6.2. Device Upgrade

【System Management】→ [Device Upgrade]: supports AC and AP upgrade;

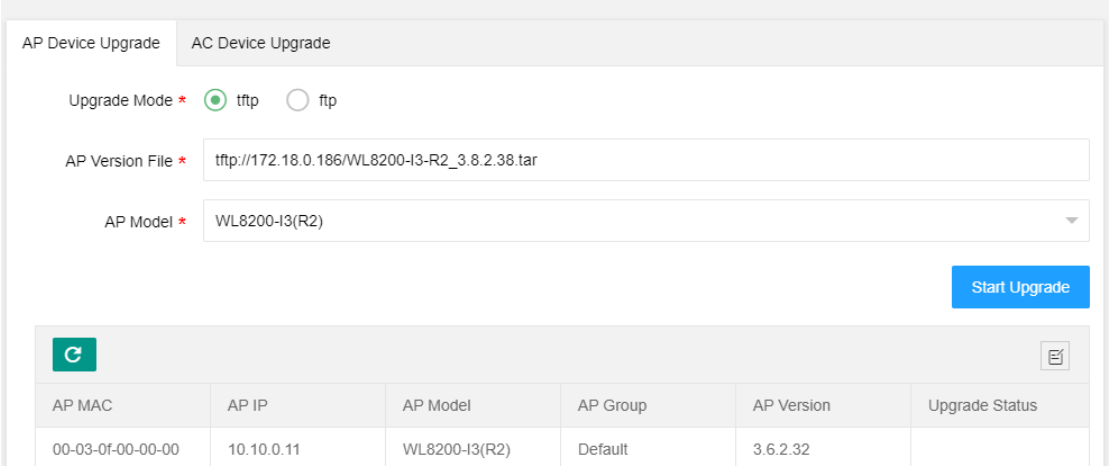
Both tftp and ftp can be used for AP upgrade, but be sure that tftp/ftp server is accessible. AP upgrade steps are as follows:

- Select tftp or ftp to upgrade
- Enter AP version information

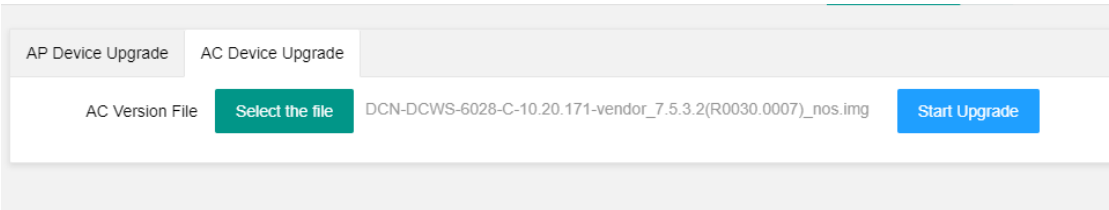
tftp://192.168.200.222/WL8200-I3-R2_3.8.2.34.tar

or ftp://1:1@192.168.200.222/ WL8200-I3-R2_3.8.2.34.tar

◆ Select AP model and corresponding AP will be listed. Then, click "Start Upgrade" button to initiate AP upgrading;

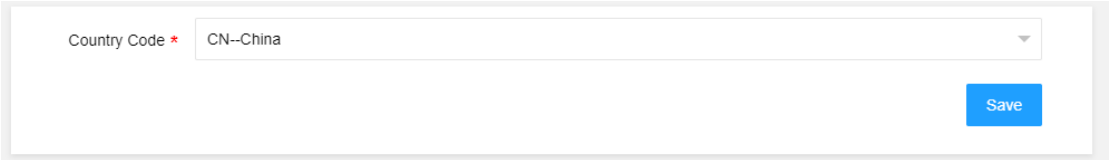


When upgrading AC web, there's no need to provide tftp server separately. Just select the local version in AC upgrade page and click "Start Upgrade" directly.



3.6.3. Country Code

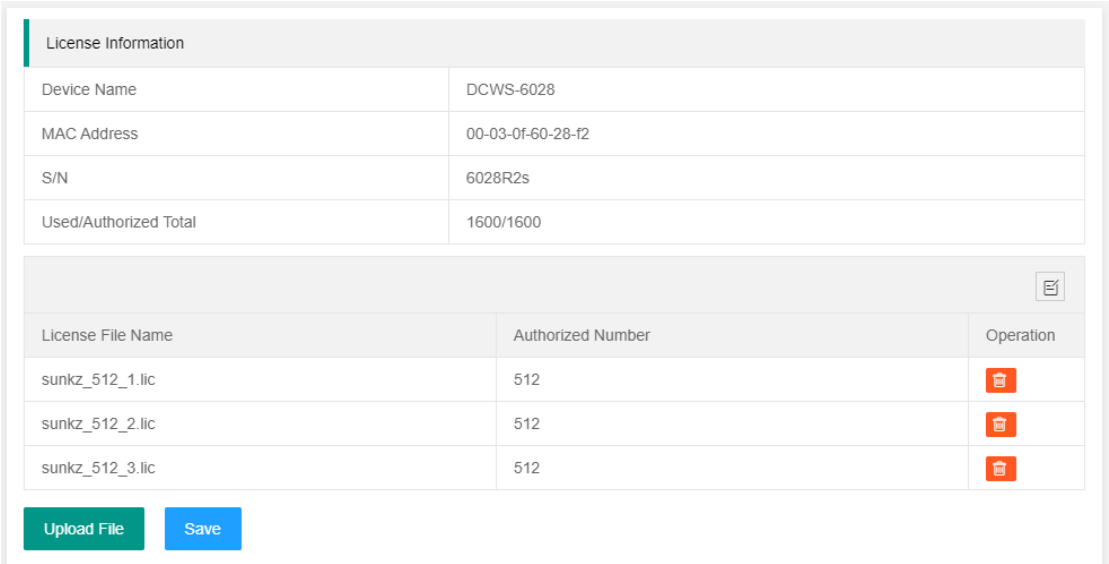
【System Management】→ [Country Code]: this configuration will be synchronized to AP.



3.6.4. License Management

【System Management】→ [License Management]: the following license information will be displayed: device name, mac address, S/N, total number of used/licensed;

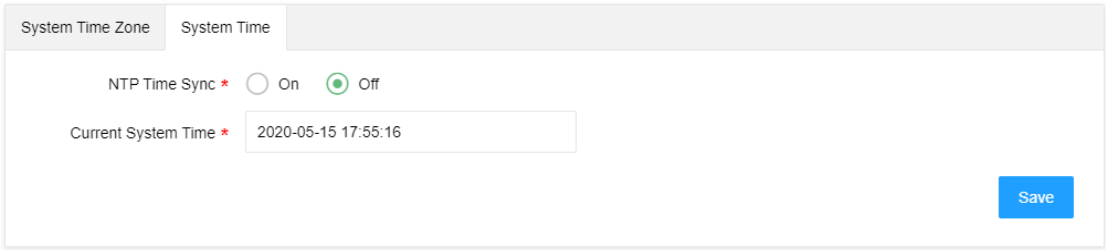
AC web supports the management of license files, including uploading and deleting;



A license file uploaded will take effect after the device is restarted.

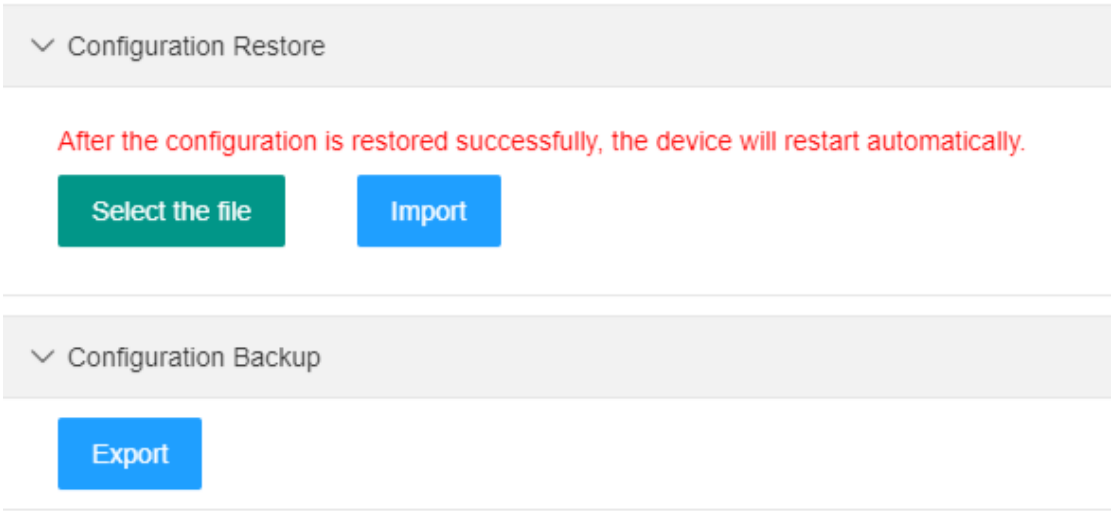
3.6.5. NTP

【System Management】→ [NTP]: including system time zone setting and system time setting. The later involves the settings of NTP time synchronization switch, time server, timing frequency and current system time.



3.6.6. Backup/Restore

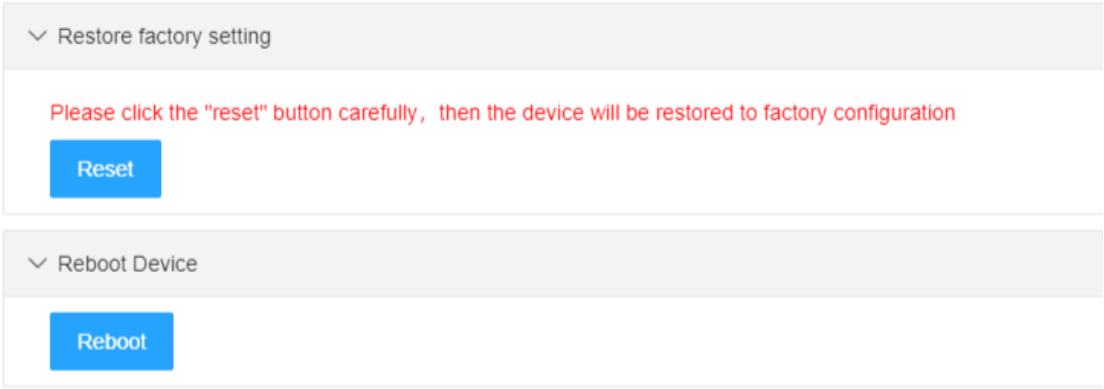
【System Management】→ [Backup/Restore]: Backup and restore AC configuration.



Backup configuration files can't be modified manually, otherwise they can't be used normally after imported.

3.6.7. Reboot/Reset

【System Management】→ [Reboot/Reset]: restart AC and restore factory settings.

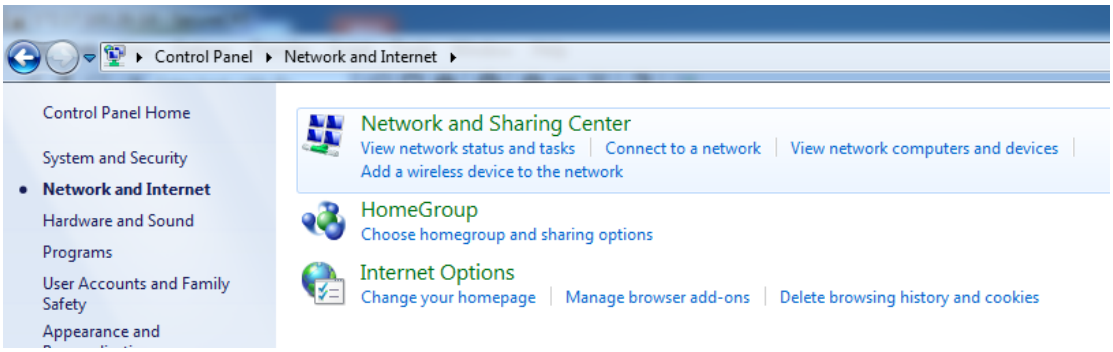


Appendix

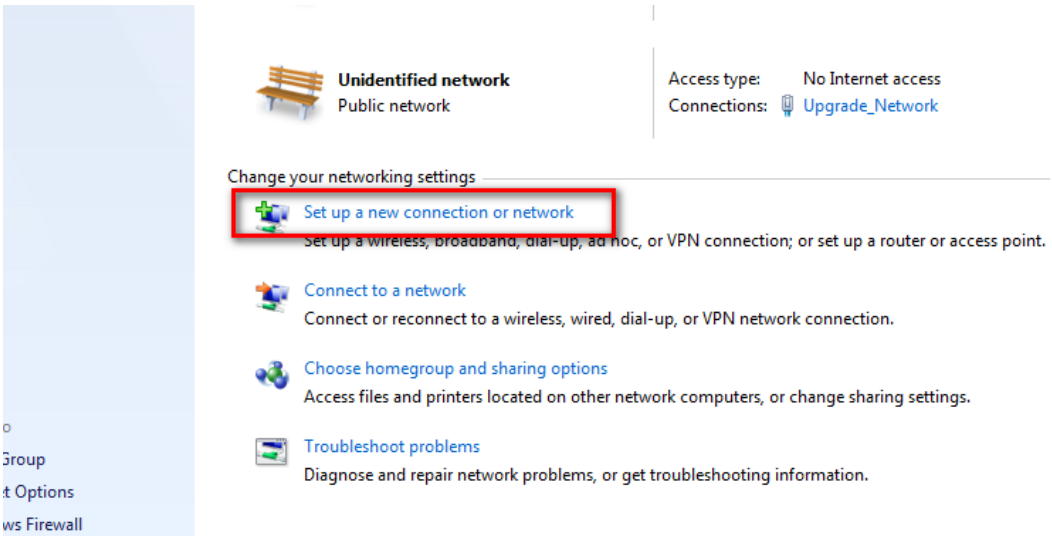
1. STA 802.1 x Configuration (For Reference)

1. Step 1:

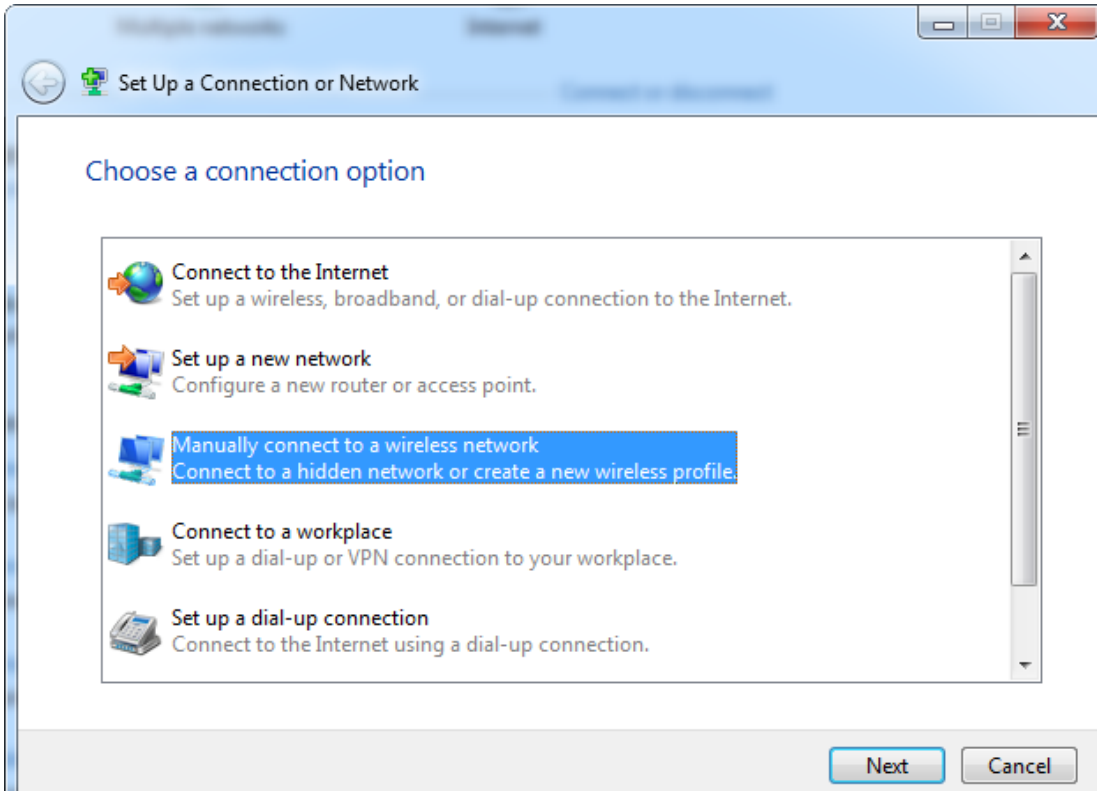
Click NIC icon. Right-click to open "Network and Sharing Center" settings.



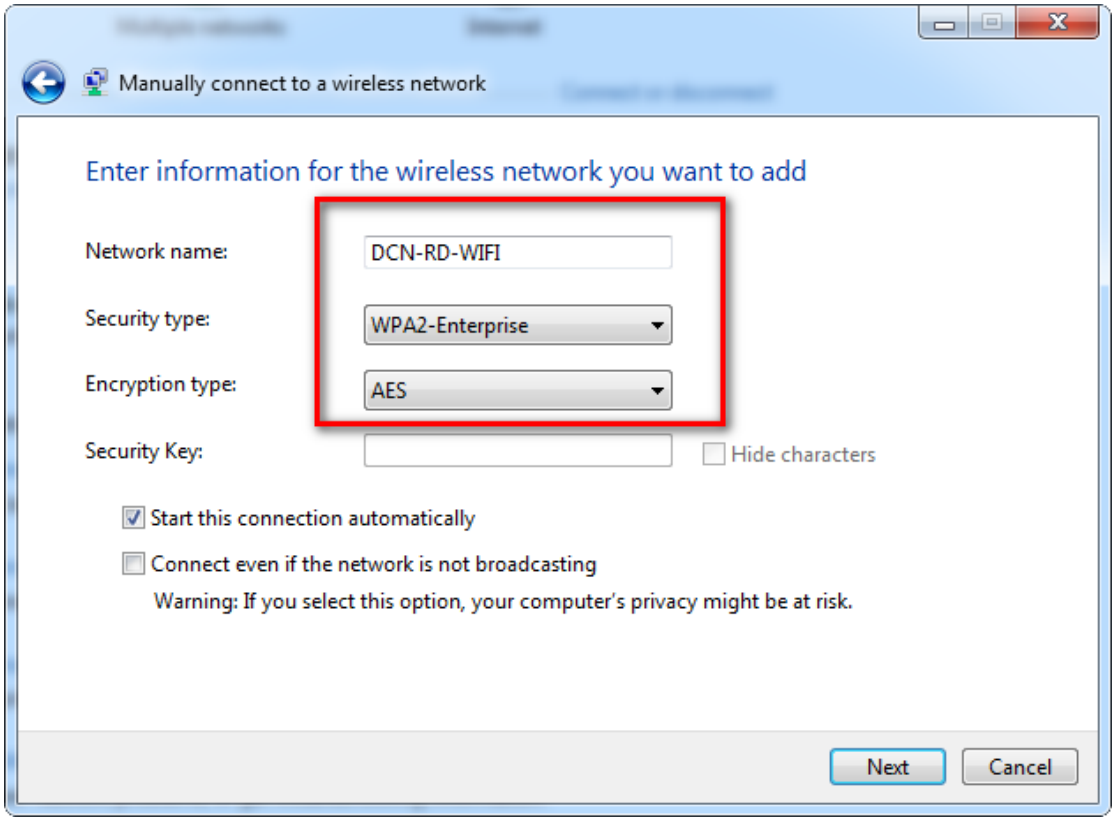
2. Step 2:click “set up a new connection or network”

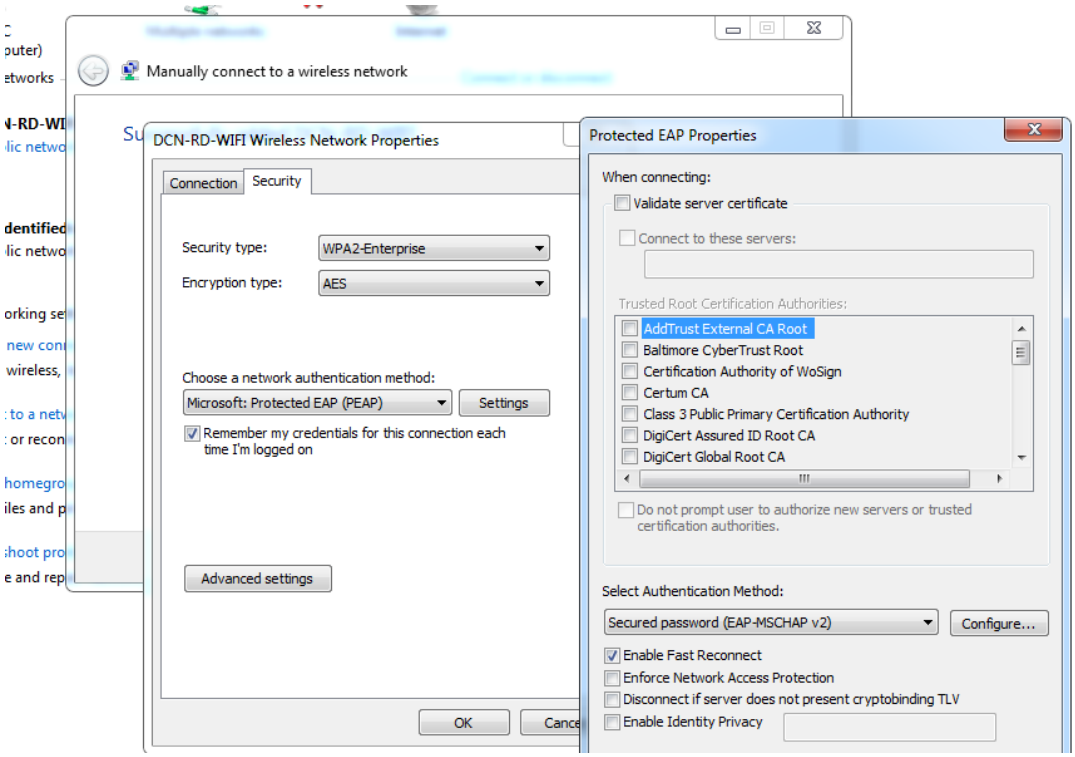


3. Step 3:choos “Manually connect to a wireless network”



4. Step 4:Input “Network name” and “Security type”, then click “Next”





5. Step 5:Connect to the AP: DCN-RD-WIFI, enter username and password, and click "OK".