Ruijie RG-WLAN Series Access Points

Web-Based Configuration Guide, Release 11.1(5)B40P2

Copyright Statement

Exemption Statement

Preface

Thank you for using our products. This manual matches the RGOS Release 11.1(5)B40P2.

Audience

This manual is intended for:

- Network engineers
- Technical support and servicing engineers
- Network administrators

Obtaining Technical Assistance

- Ruijie Networks Website: https://www.ruijienetworks.com/
- Technical Support Website: https://ruijienetworks.com/support
- Case Portal: http://caseportal.ruijienetworks.com
- Community: http://community.ruijienetworks.com
- Technical Support Email: service_rj@ruijienetworks.com
- Skype: service_rj@ruijienetworks.com

Related Documents

Documents	Description
Command Reference	Describes the related configuration commands, including command modes, parameter descriptions, usage guides, and related examples.
Hardware Installation and Reference Guide	Describes the functional and physical features and provides the device installation steps, hardware troubleshooting, module technical specifications, and specifications and usage guidelines for cables and connectors.

Conventions

This manual uses the following conventions:

Convention	Description
boldface font	Commands, command options, and keywords are in **boldface**.
italic font	Arguments for which you supply values are in *italics*.
[ ]	Elements in square brackets are optional.

{ x | y | z }	Alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.

Symbols

Means reader take note. Notes contain helpful suggestions or references.

Means reader be careful. In this situation, you might do something that could result in equipment damage or loss of data.

1 Web-based Configuration

1.1 Overview

A user accesses the Web-based management system using a browser such as Internet Explorer (IE) to manage the AP device.

Web-based management involves two parts: Web server and Web client. A Web server is integrated into a device to receive and process requests sent from a client (for example, read a Web file or execute a command request) and returns the processing results to the client. Generally, a Web client refers to a Web browser.

Currently, this file is applicable to only AP devices.

1.2 Application

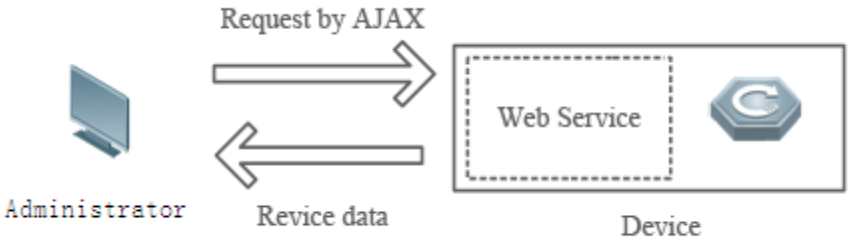
Application	Description
Web-based Management	After configuring, a user can access the Web-based management system through a browser.

1.2.1 Web-based Management

Scenario

As shown in the following figure, an administrator can access a device through a browser on a PC to manage the device.

Figure 1-1



Note	The Web management system integrates configuration commands and sends them to the device through AJAX requests. Web service is enabled on the device to process HTTP requests to return requested data.

Function Deployment

Configuration Environment Requirements

Requirements for Client

- An administrator logs in to the Web-based management system using the Web browser on a client to manage the device. Generally, a client refers to a PC. It may also be other mobile terminal devices, for example, a laptop.
- Browsers supported: IE7.0, IE8.0, IE9.0, IE10.0, IE11.0, Google chrome, Firefox, and some IE kernel-based browsers (for example, Maxthon). Exceptions such as messy code and format errors may occur when other browsers are used.
- Resolution: It is recommended that the resolution be set to 1024 x 768, 1280 x 1024, or 1440 x 960. Exceptions such as font alignment error and format error may occur when other resolutions are selected.

Requirements for server

- The Web service must be enabled for the AP device.
- Login authentication information for Web-based management must be configured for the AP device.
- A management IP address must be configured for the AP device.

Default Configuration

The following table lists the Web management system default configuration.

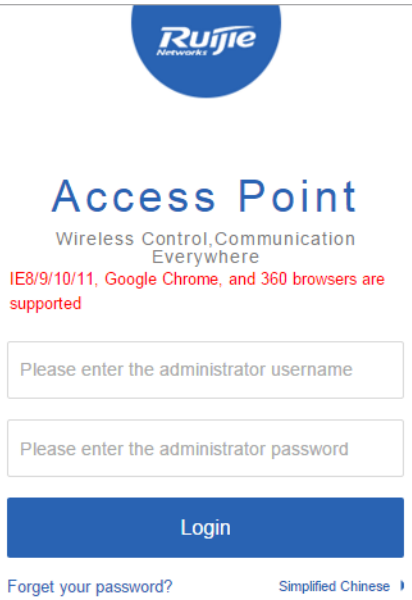
Feature	Default Settings
Web service	Enabled
Management IP	192.168.110.1

Default Username/Password	Permission Description
admin/admin	Super administrator with all permissions.

Login

You can type **http://X.X.X.X** (management IP address) in the address bar of a browser and press **Enter** to access the login page, as shown in the following figure.

Figure 1-2 Login page



After typing the username and password, click **Login**.

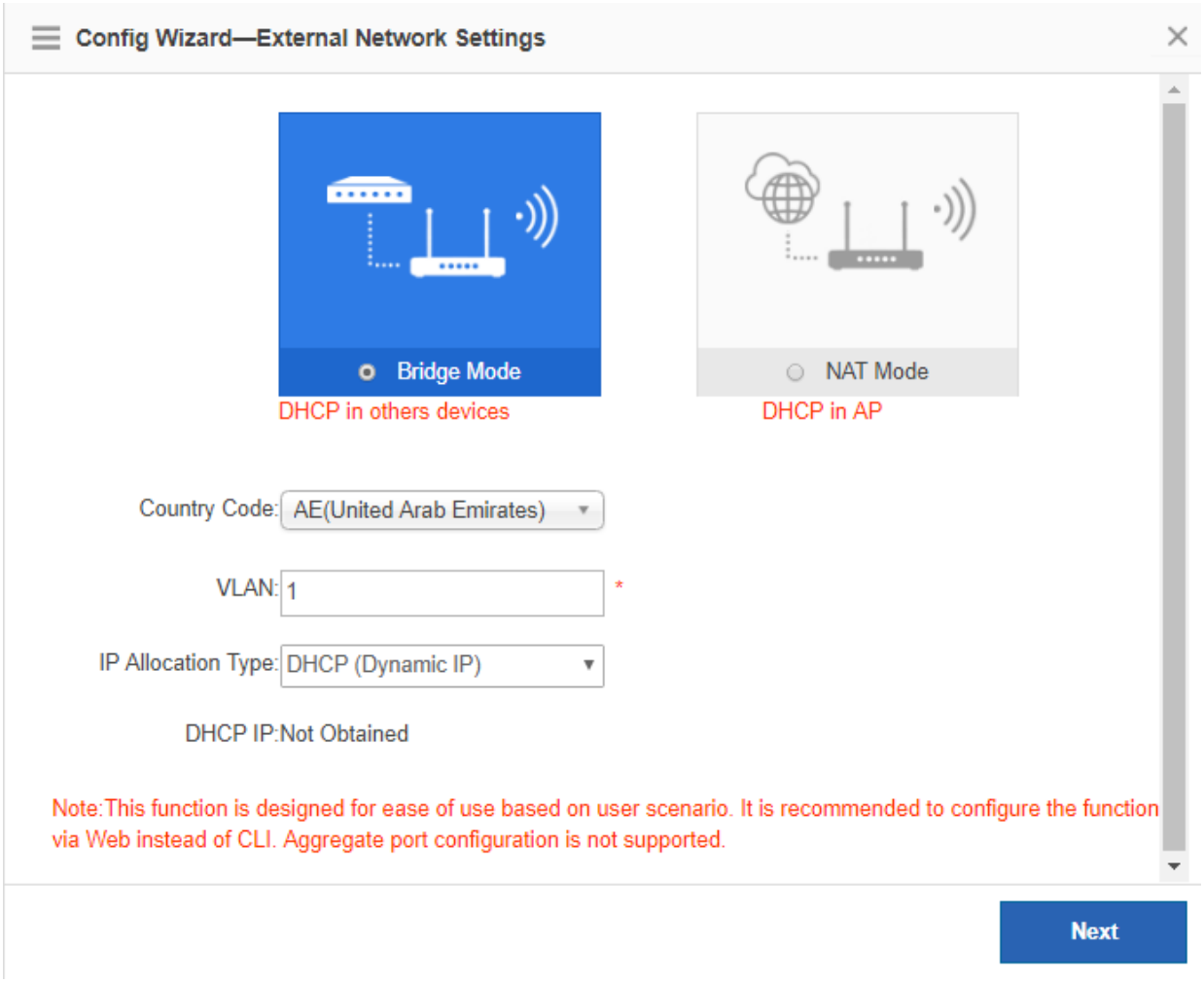
Enter the username and password. Click **Login** to access the Web management system.

Click **Online Service** for configuration help.

1.3 Configuration

1.3.1 Config Wizard

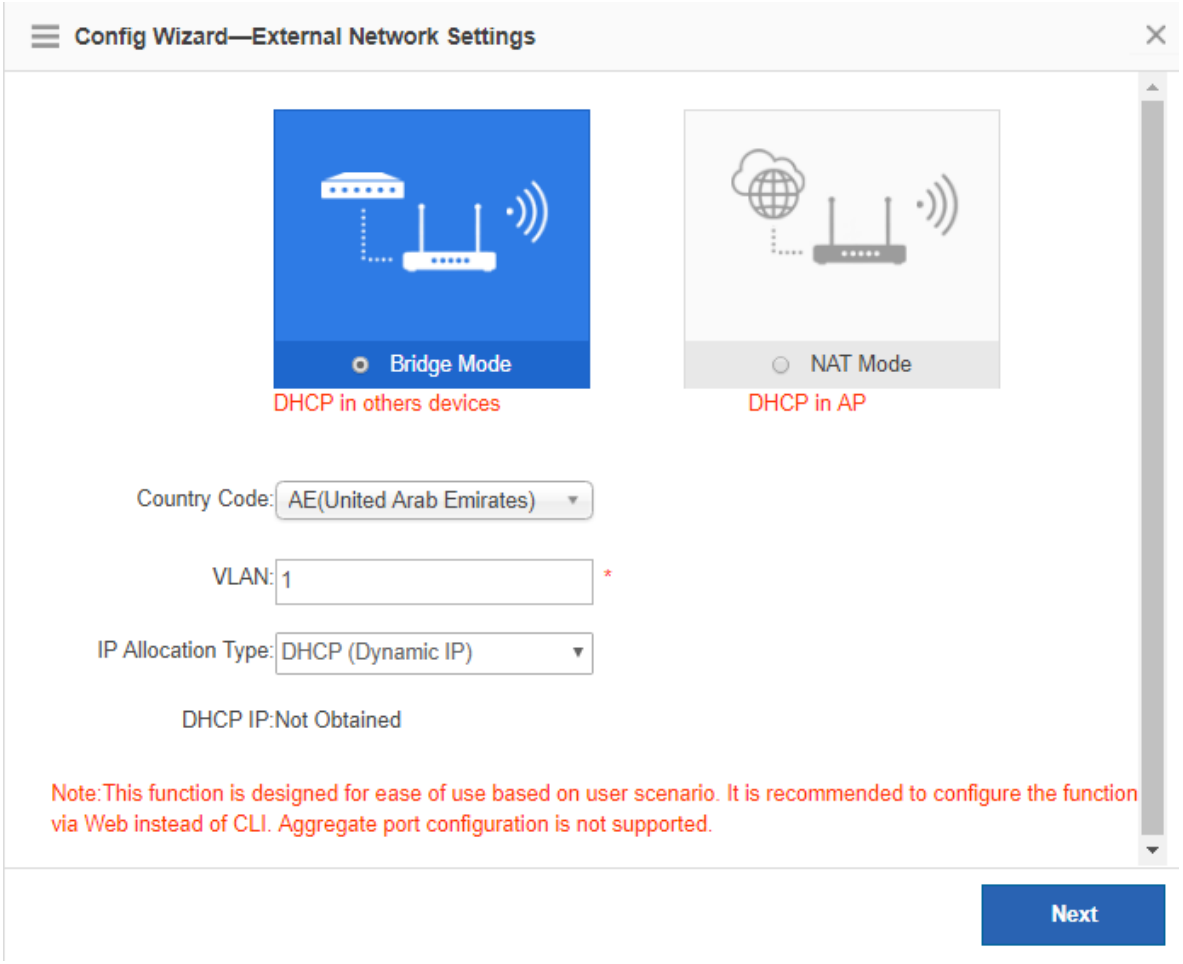
Build a WiFi network for STAs to access for Internet services.



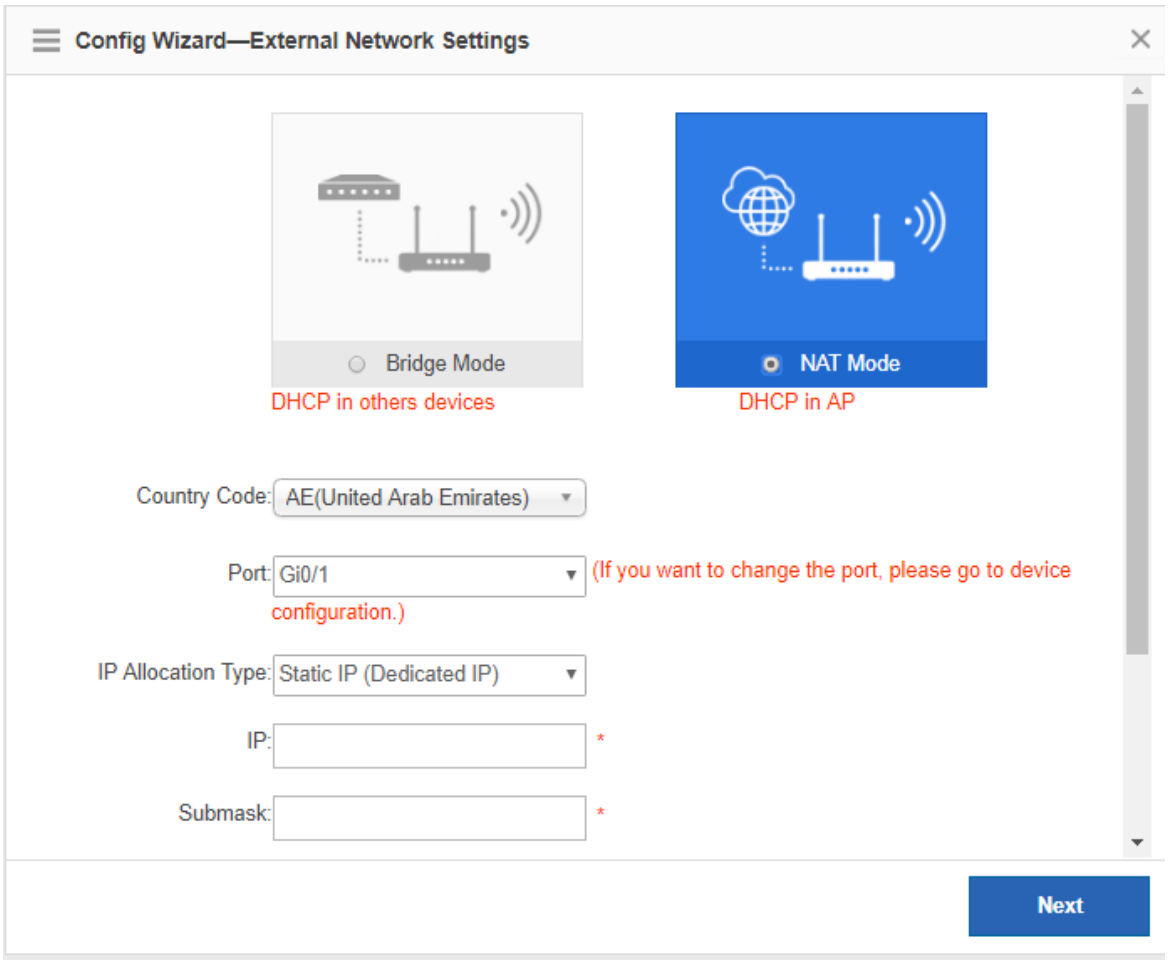
1) The **Config Wizard** page is displayed after successfully logging in to the Web if the device is in the default factory setting state, as shown in the preceding figure.

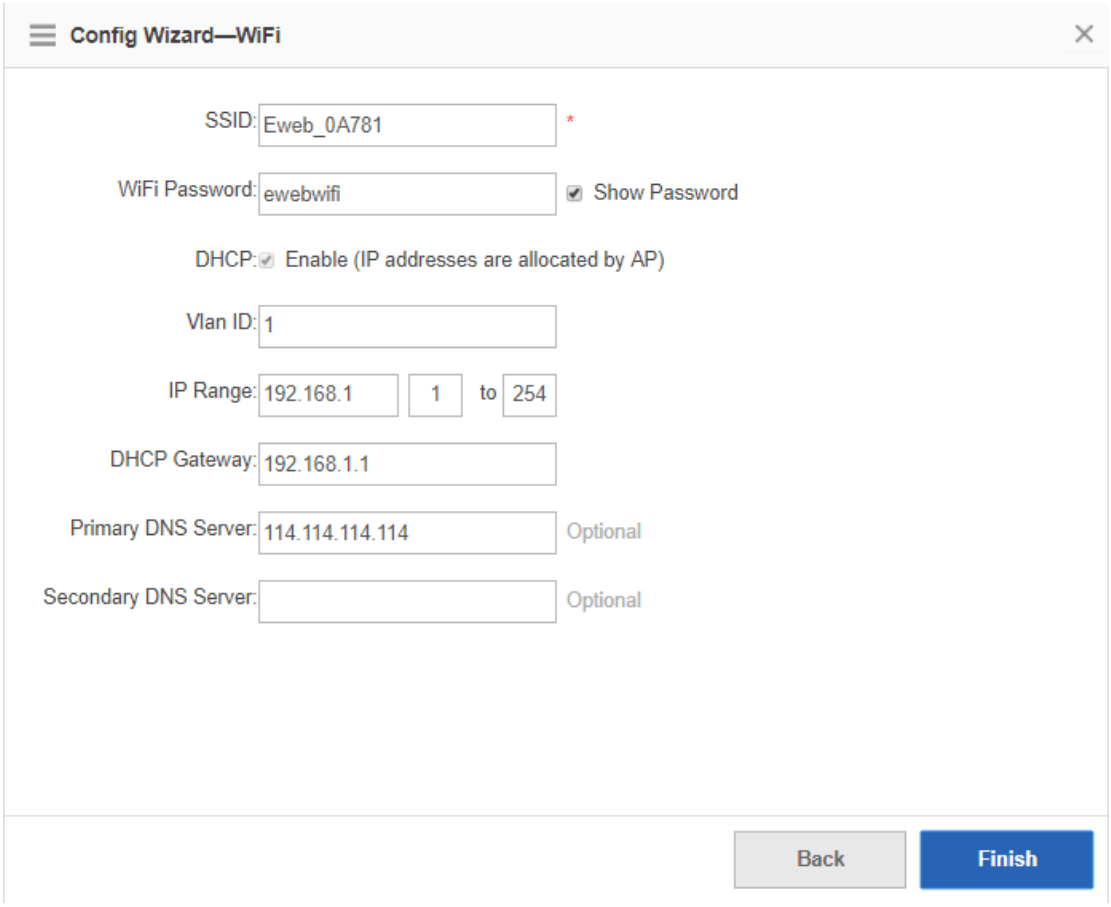
2) The **Config Wizard** page is also displayed when you click the **Config Wizard** link in the upper-right corner on the homepage.

The device supporting NAT can work in AP access mode or wireless routing mode.



A device not supporting NAT can work only in AP access mode.


Config Wizard—External Network Settings
Bridge Mode
DHCP in others devices
NAT Mode
DHCP in AP
Country Code:
AE(United Arab Emirates)
Port:
Gi0/1
(If you want to change the port, please go to device configuration.)
IP Allocation Type:
Static IP (Dedicated IP)
IP:
Submask:
Next



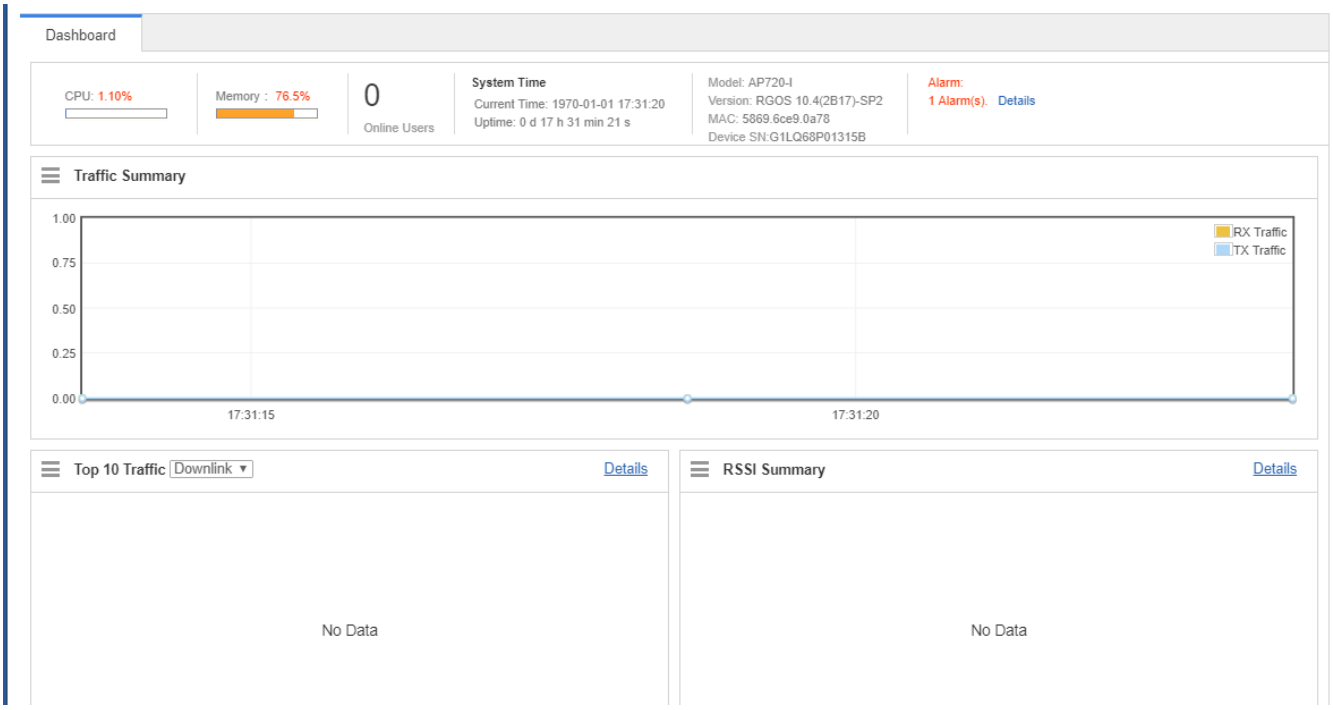
Configure the WiFi parameters, and click **Finish** to finish the configuration.

- After the AP device is initialized, please configure the AP device through the **Config Wizard** page.
- All quick settings are scenario-based settings. And some of the configuration is delivered by default. If configurations such as NAT, interface, or address pool are changed via CLI or MACC system, it is recommended to not change the configuration again via Quick Settings, otherwise there could be incompatibility.
- If the AP device is in access mode, it is recommended to build the gateway and address pool on the other device. If the AP device is in routing mode, it is recommended to build the gateway and address pool on the AP device and configure the NAT for it.

1.3.2 Monitor

1.3.2.1 Dashboard

The dashboard enables viewing basic information for the AP device, including the device MAC address, device model, system alarm information, flow trends of AP device ports, latest trends of all management APs, and STA information corresponding to each management AP. In addition, it enables you to know the distribution condition of STA signal strength in real time.

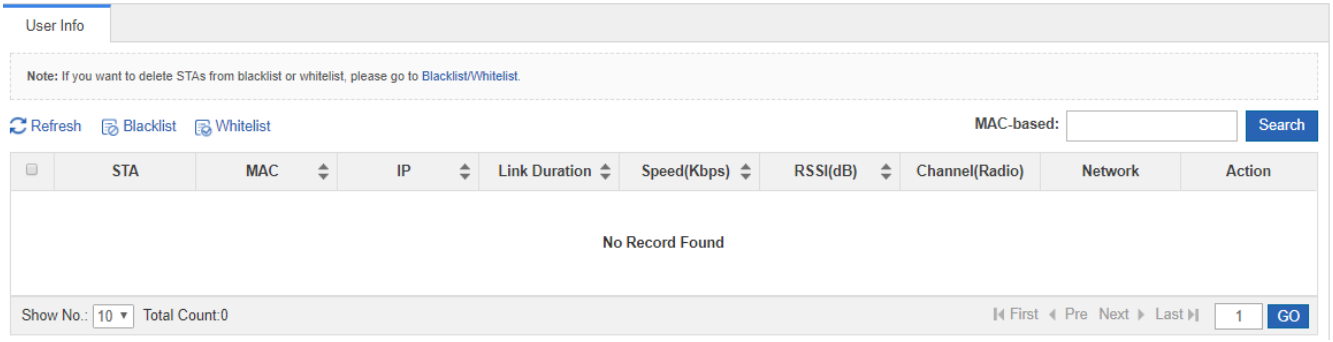


Click the **Details** link in the upper-right corner to view more system alarm information.

Click the **View Detail** link in the lower left corner to view the STA details on the displayed page, for example, the MAC address and RSSI.

1.3.2.2 User Info

User information is displayed here.



1.3.3 Network

1.3.3.1 WiFi/WLAN

A Wireless Local Area Network (WLAN) refers to a network system that allows different PCs to communicate and share resources with each other by interconnecting different PCs through wireless communication technologies. The essence of a

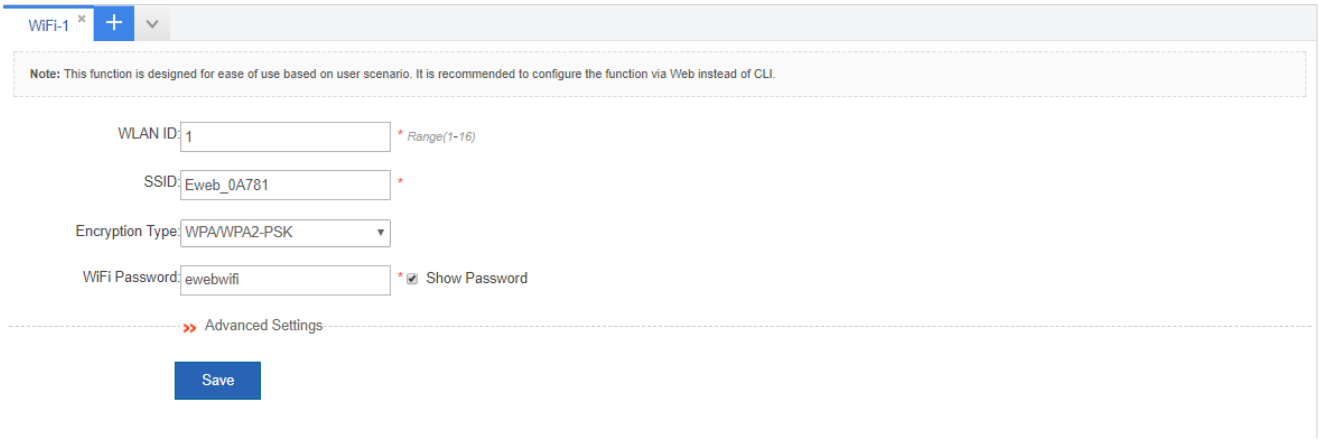
WLAN is that PCs are interconnected with each other in wireless rather than wired mode, thus constructing a network and allowing terminals to move more flexibly.

Wi-Fi or WiFi is a technology for wireless local area networking with devices based on the IEEE 802.11 standards. Devices that can use Wi-Fi technology include personal computers, video-game consoles, smartphones, digital cameras, tablet computers, smart TVs, digital audio players and modern printers. Wi-Fi compatible devices can connect to the Internet via a WLAN and a wireless access point. Such an access point (or hotspot) has a range of about 20 meters (66 feet) indoors and a greater range outdoors. Hotspot coverage can be as small as a single room with walls that block radio waves, or as large as many square kilometers achieved by using multiple overlapping access points.

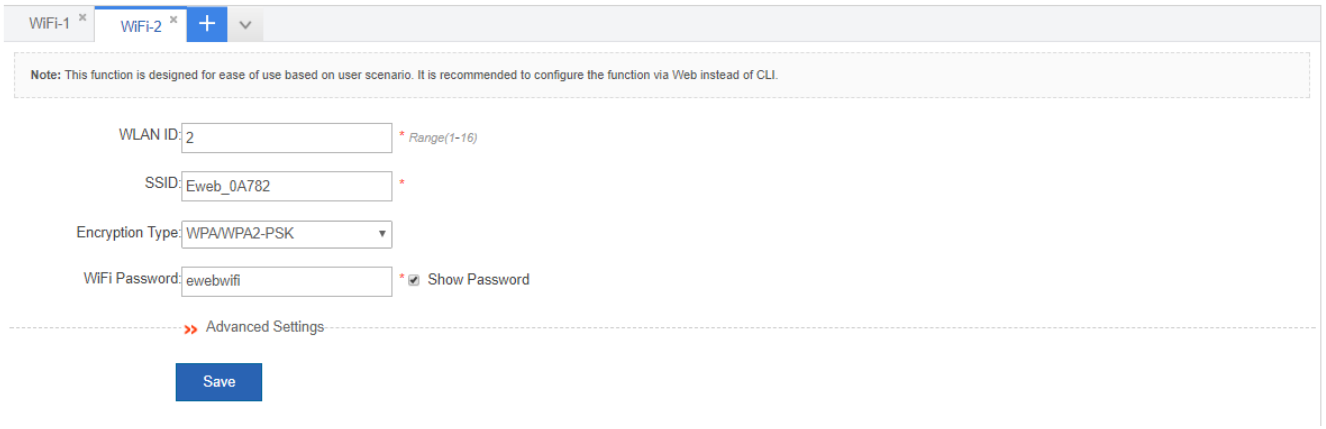
Service Set Identifier (SSID), also referred to as ESSID: It is used to distinguish different networks, that is, identifying an ESS. An SSID contains a maximum of 32 characters. A WNIC configured with different SSIDs can access different networks. SSIDs are usually broadcasted by an AP or a wireless router. The scanning function delivered with the XP can be used to view SSIDs within the current area. In consideration of security, SSIDs may not be broadcasted. In this case, users need to manually set SSIDs to access corresponding networks. To be simple, an SSID is the name of a WLAN. Only computers with the same SSID can communicate with each other.

The WLAN allows wireless STAs to access the AP through WiFi for Internet services. Multiple WLANs can be added or deleted.

The following figure shows the page for adding a WLAN.



- Adding WiFi/WLAN

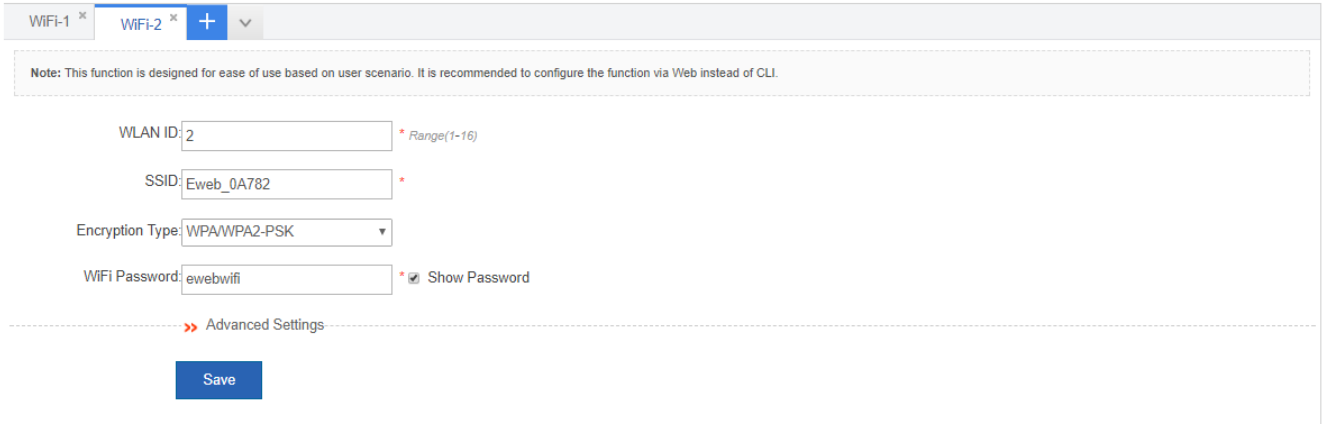


1) Click  , and a new panel for WiFi configuration is displayed.

2) Set the WiFi parameters.

3) Click **Save** to finish the configuration.

- Editing the WLAN

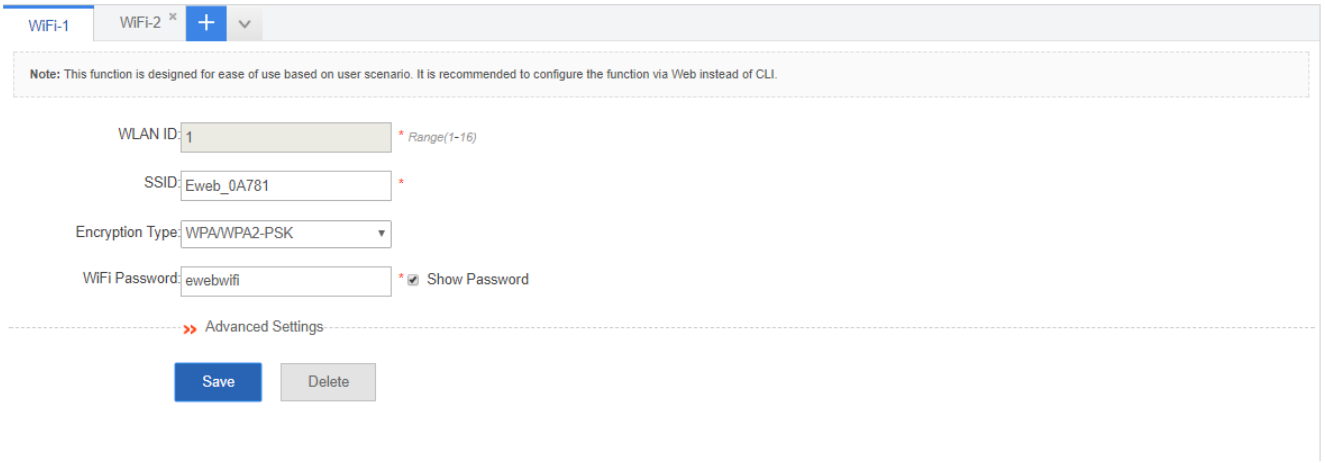


1) Click the WiFi panel you want to edit.

2) Edit the WiFi configuration.

3) Click **Save**. The **Edit succeeded** message is displayed.

- Deleting WLANs



1) Click the WiFi panel you want to delete.

2) Click **Delete**.

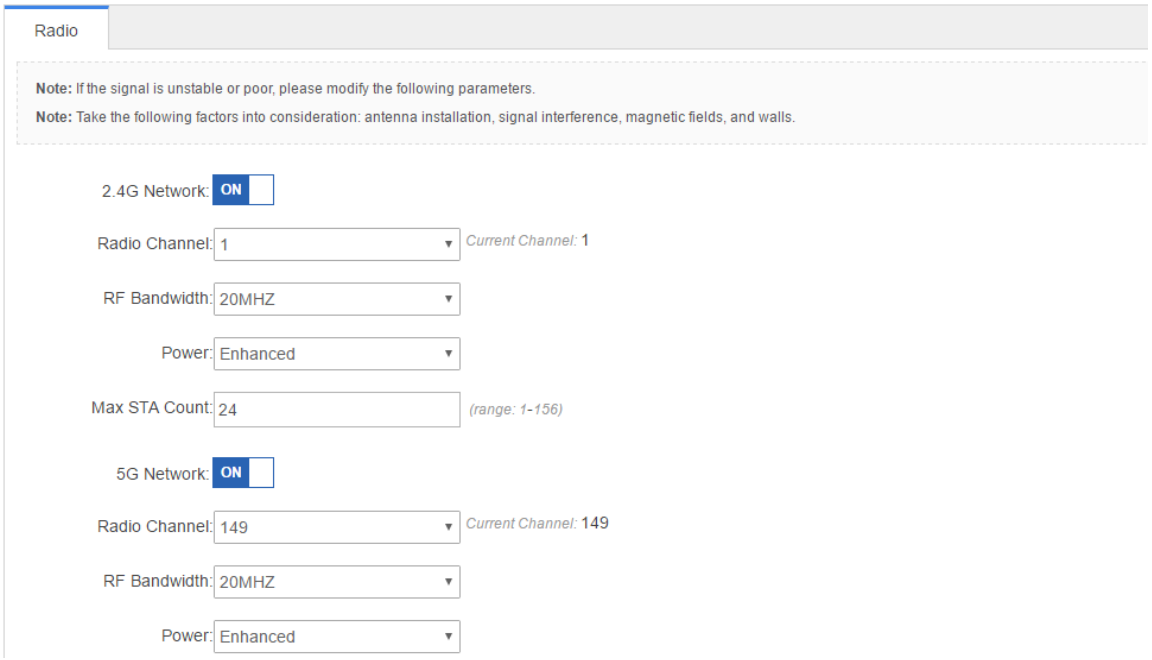
3) Click **OK** in the dialog box displayed to finish the deletion operation.

1.3.3.2 Wireless Radio Settings

Wireless channels transmit RF medium between APs and wireless STAs. The use of channels varies with different countries and frequency bands. For example, the 2.4 GHz frequency band can be configured with 13 channels (channel 1 to channel 13), and the 5 GHz frequency band can be configured with five channels (channels 149, 153, 157, 161, and 165). The overlapping channels in the 2.4 GHz frequency band generate interference. It is recommended that these channels be configured as non-overlapping channels (for example, channels 1, 6, and 11) to avoid radio signal collision. The five channels in the 5 GHz frequency band do not overlap or generate interference.

Wireless channel settings are mainly about adjusting the strength of the WiFi signal sent out by the device. Channel parameters can be set for the 2.4G and 5G networks.

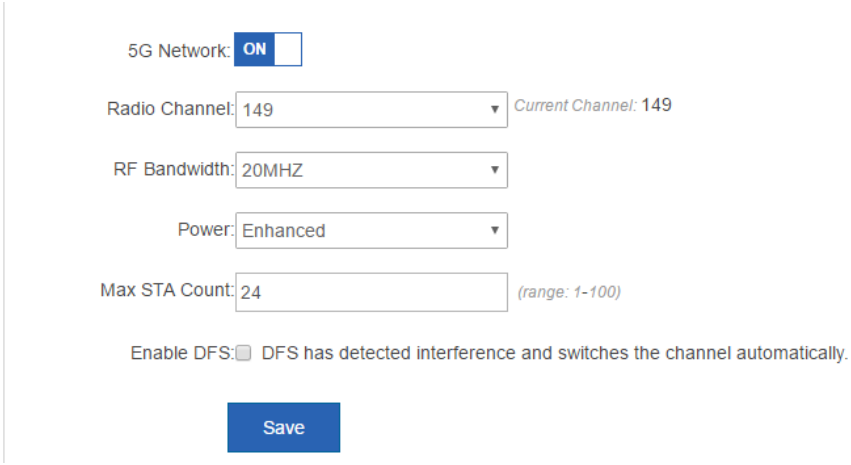
- Enabling a 2.4G network



1) Click ON to enable or disable the 2.4G network.

2) Click Enforce switch from 2.4GHz to 5GHz Network to forcibly switch the network type.

- Enabling the 5G network



1) Click ON to enable or disable the 5G network.

2) Click **Enforce switch from 5GHz to 2.4GHz Network** to forcibly switch the network type to a 2.4G network.

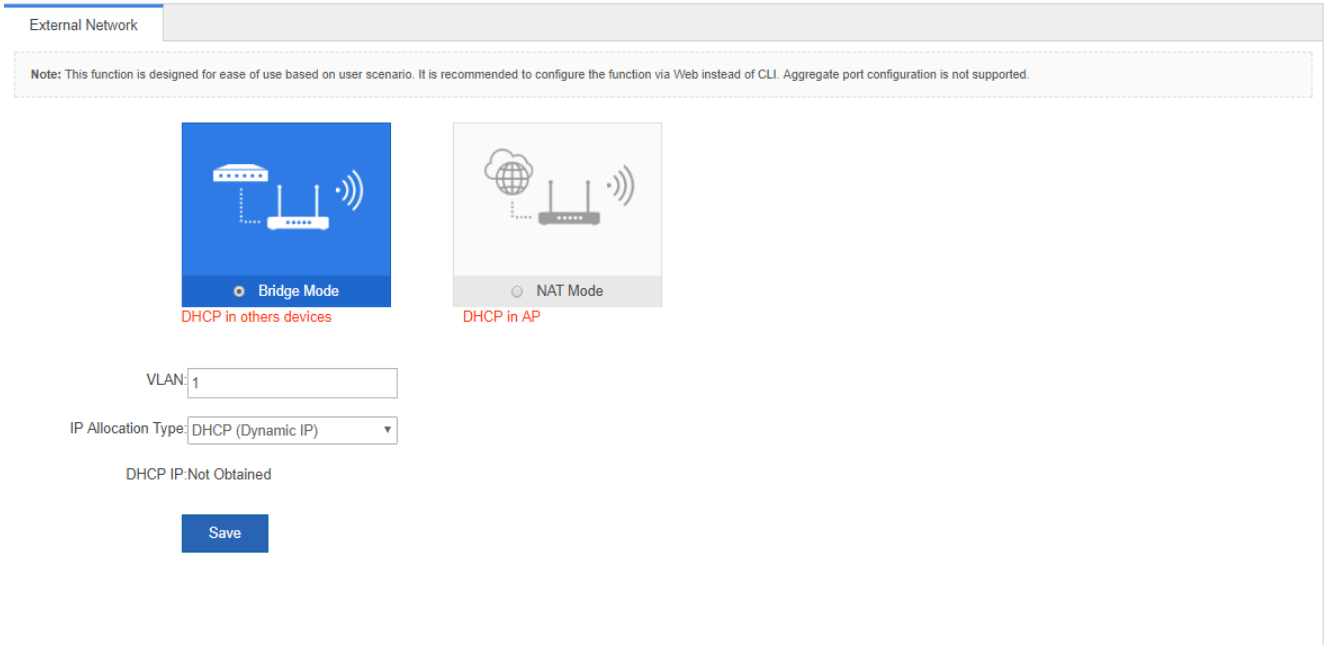
1.3.3.3 External Network Settings

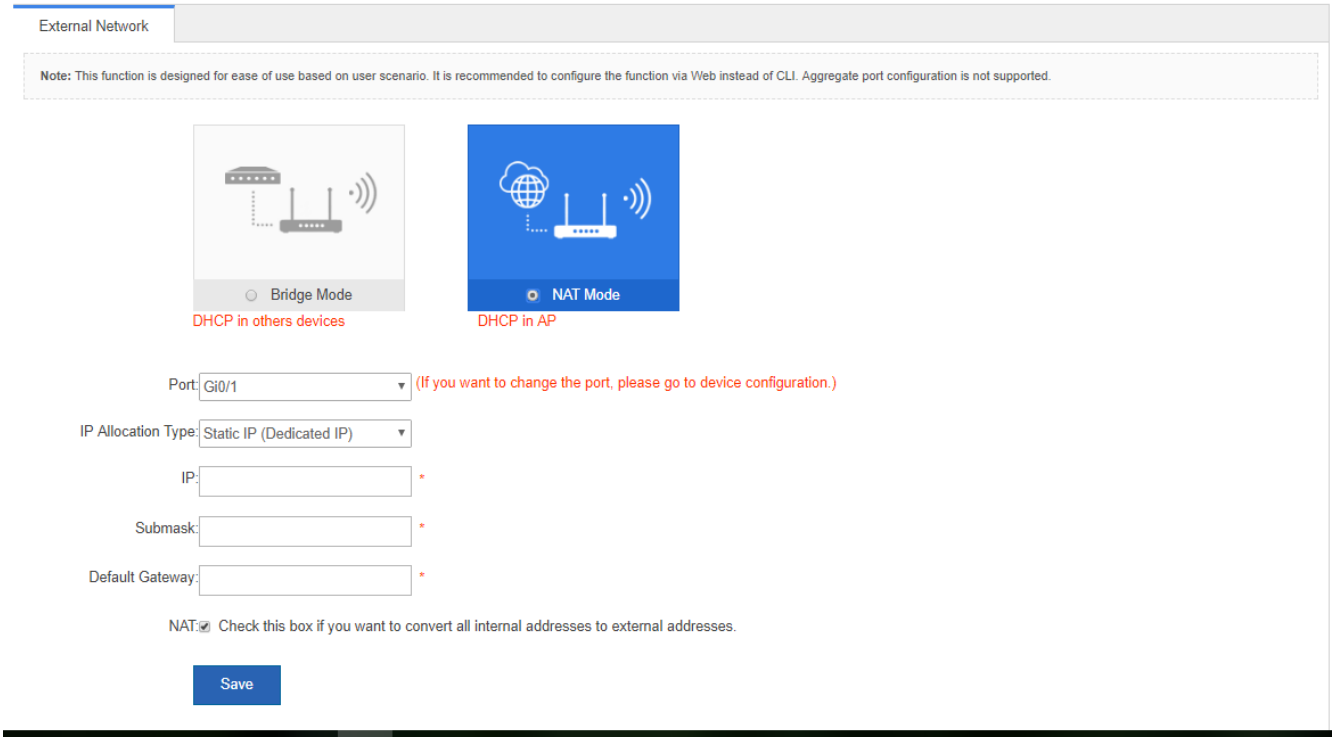
External network settings are mainly about configuration of the communication mode between the AP and external network. Two communication modes are available: Bridge mode and NAT mode.

In **Bridge Mode**, the Ruijie APs act as bridges, allowing wireless clients to obtain their IP addresses from an upstream DHCP server.

In **NAT Mode**, the Ruijie APs run as DHCP servers to assign IP addresses to wireless clients out of a private 10.x.x.x IP address pool behind a NAT.

The AP you use might not support this function, which is subject to the actual menu items.





You can select the AP working mode to determine the AP role and then configure based on the corresponding working mode.

Set corresponding parameters and save the configuration.

1.3.3.4 Wireless Bridging

Multiple APs are connected to each other in a wireless repeater or bridging mode to connect distributed networks and spread wireless signals. An AP device can be regarded as a repeater. It spreads the front-end network and elongates the WiFi transmission distance for association and connection of STAs far away. Wireless bridging supports the 2.4G network and 5G network bridging.

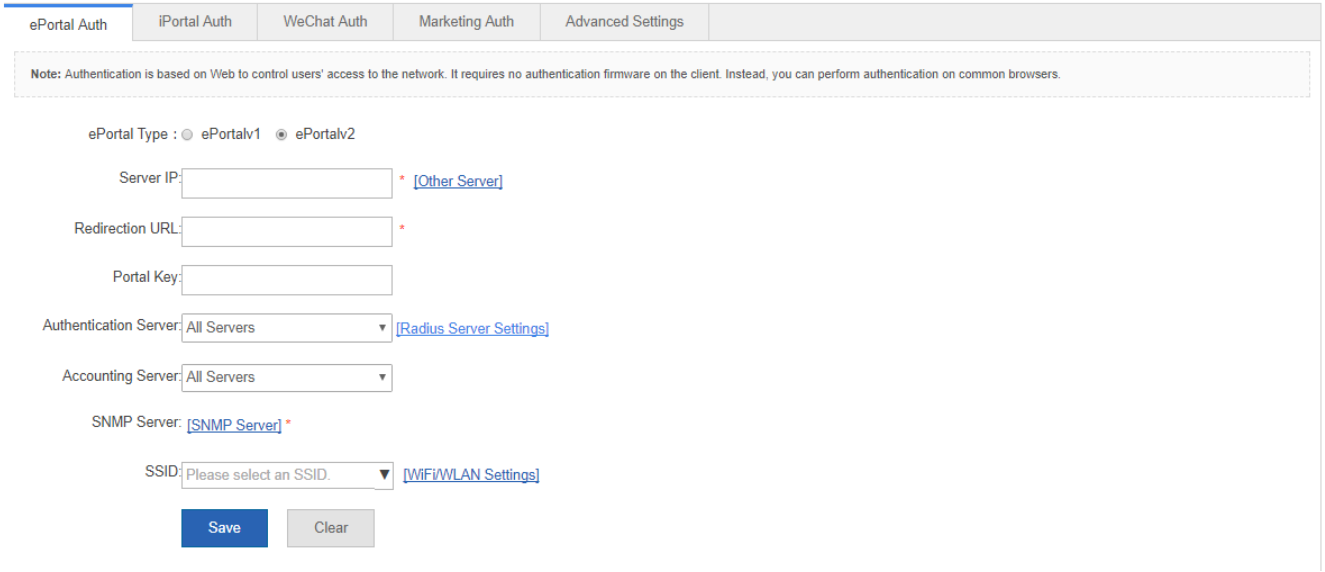
Enable the 2.4G or 5G network bridging function as required, select the **Central Base Station** operating mode, and click **Save** to finish configuration.

1.3.3.5 Authentication

Web authentication allows you to control user access to the Internet. The users can perform authentication on the browser without installing any application, which is easy and convenient. Web authentication can be classified into iPortal authentication and ePortal authentication based on the server location.

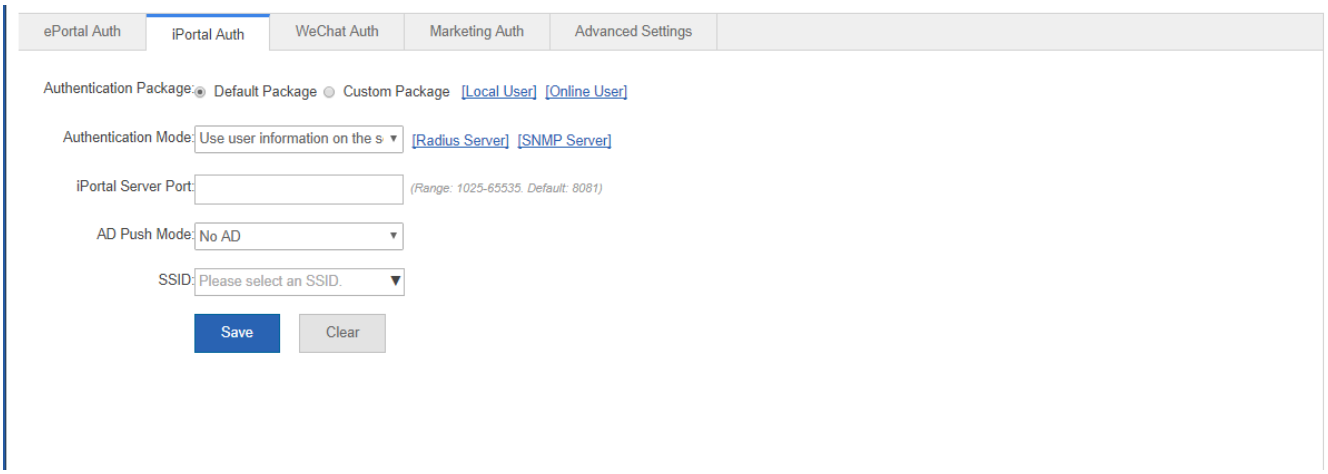
↘ ePortal Authentication

Unauthenticated users will be redirected to the specified website for authentication. If the Portal is not built into the AC, please select ePortal authentication.



↘ iPortal Authentication

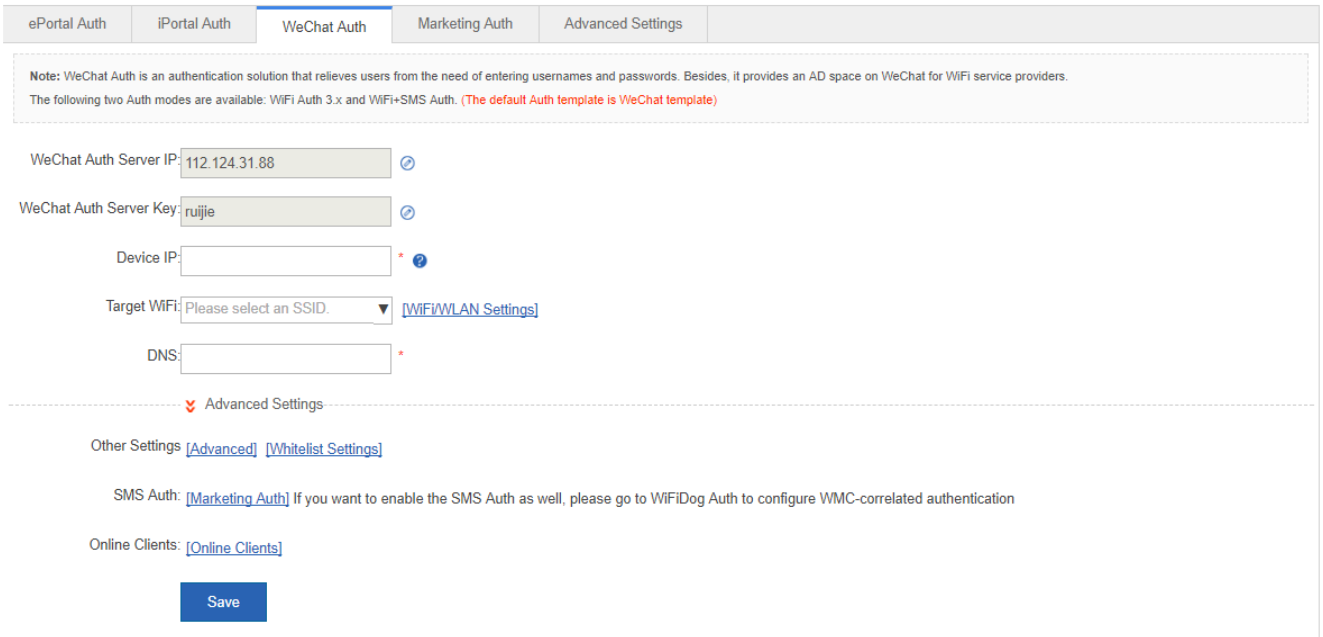
Unauthenticated users will be redirected to the specified website for authentication. If the Portal is built into the AC, please select iPortal authentication.



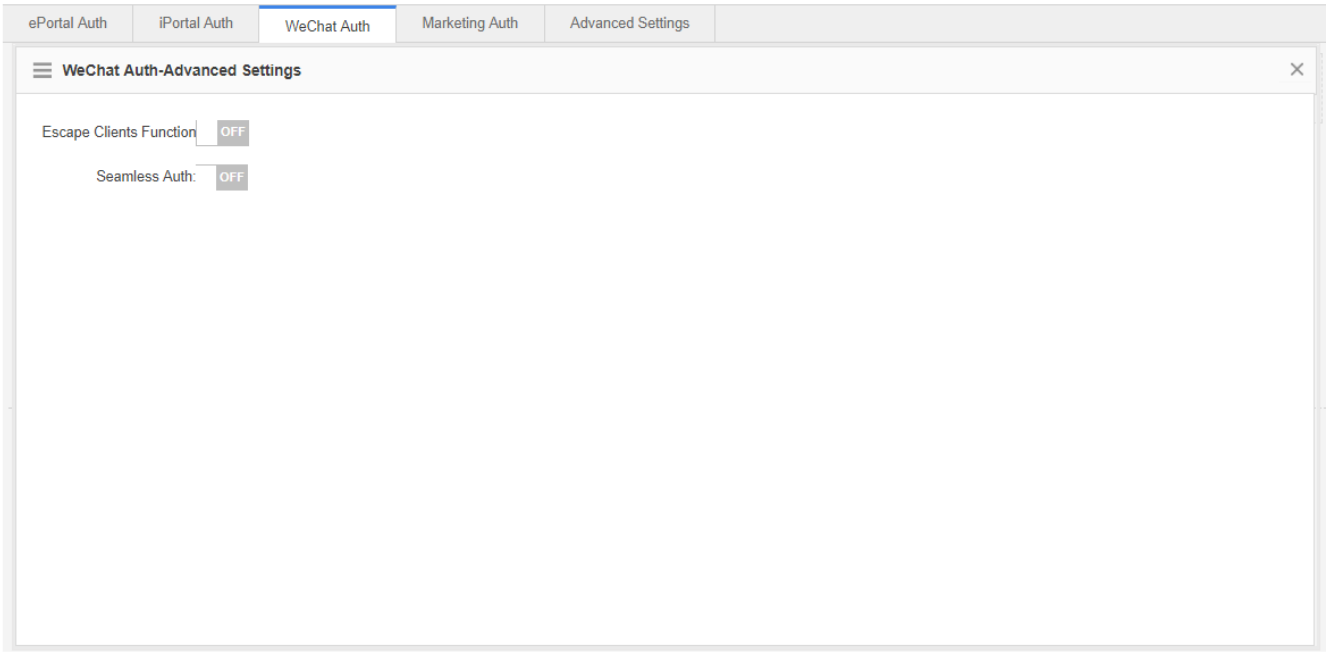
WeChat Authentication

WeChat Auth is an authentication solution that relieves users from the need of entering usernames and passwords. Besides, it provides an AD space on WeChat for WiFi service providers.

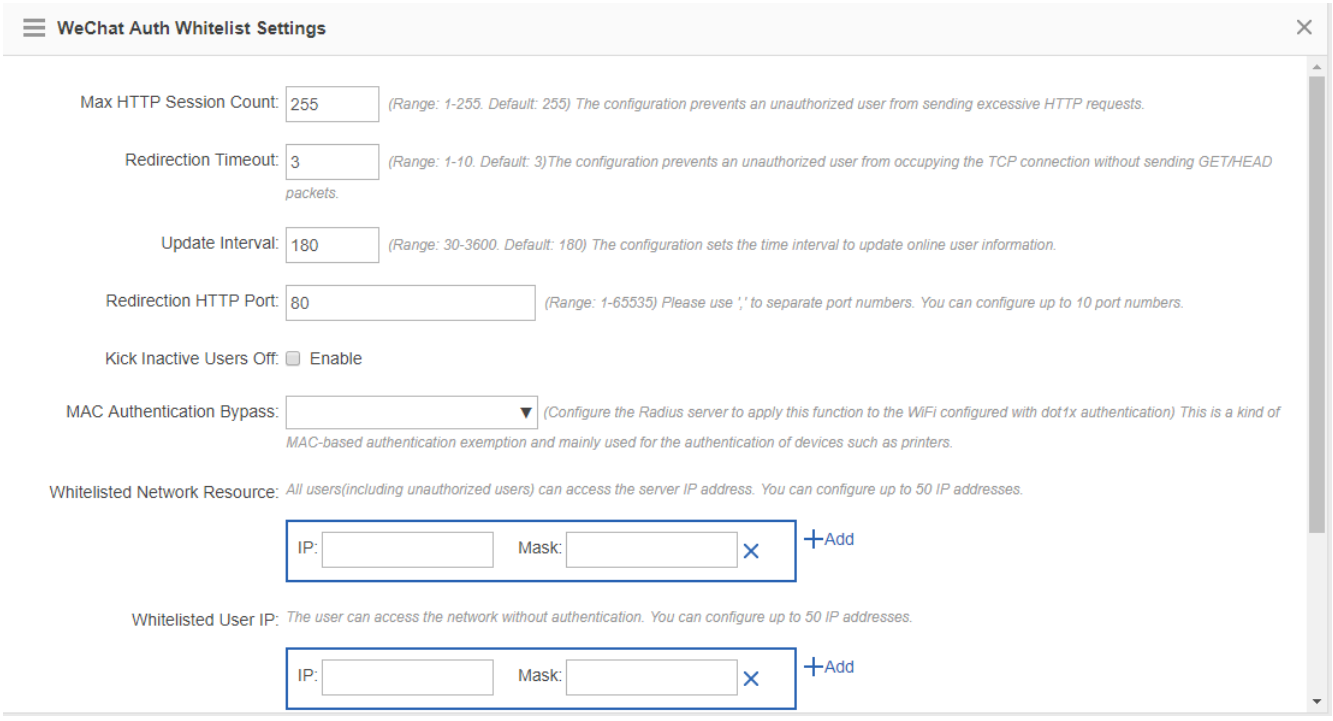
The following two authentication modes are available: WiFi Auth 3.x and WiFi+SMS Auth. (The default is the WeChat template)



Choose **Advanced Settings** > **Other Settings** > **Advanced**.



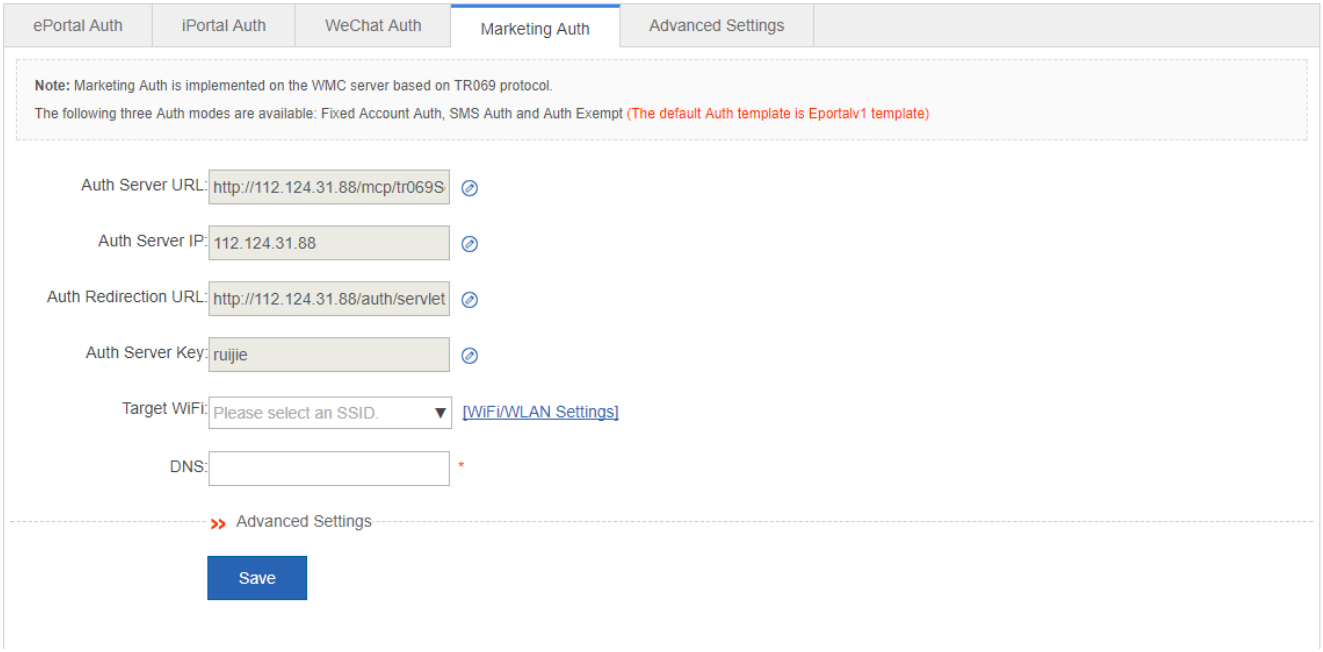
Choose **Advanced Settings** > **Other Settings** > **Auth Exempt**.



Marketing Authentication

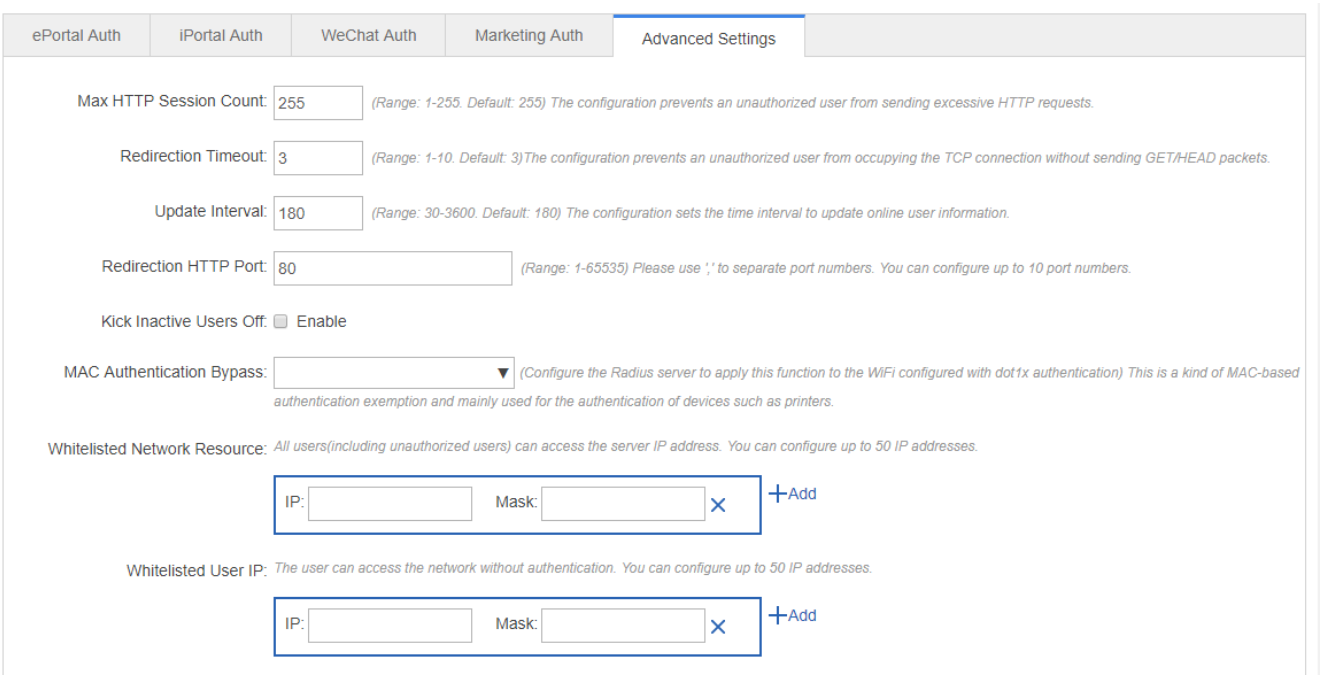
Marketing authentication is implemented on the WMC server based on the TR069 protocol.

The following three authentication modes are available: Fixed Account Auth, SMS Auth, and Auth Exempt (The default is the ePortalv1 template).



Advanced Settings

Advanced Settings provide some optional features applicable to both Web authentication V1 and Web authentication V2.

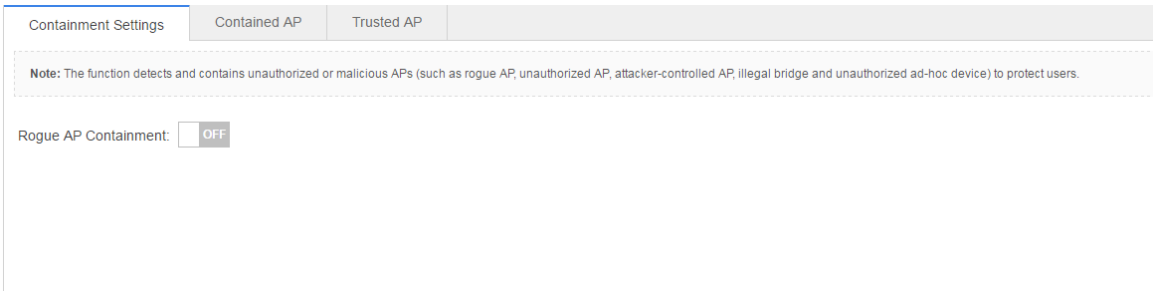


1.3.4 Security

1.3.4.1 Containment

Rogue APs may exist in a WLAN. Rogue APs may have security vulnerabilities and can be manipulated by attackers to seriously threaten and endanger network security. The containment function can be enabled on the AP to attack rogue devices and prevent other wireless STAs from being associated with rogue devices.

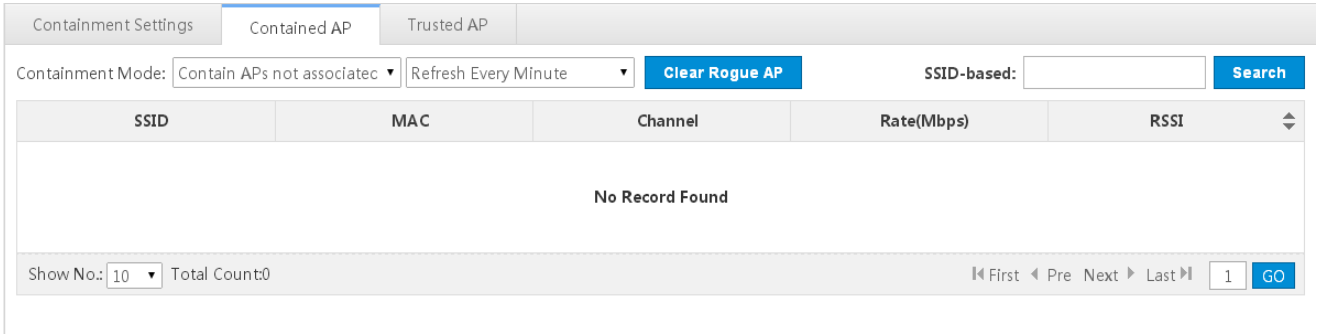
Containment Settings



Click 

to enable or disable rogue AP containment for the device.

Contained AP

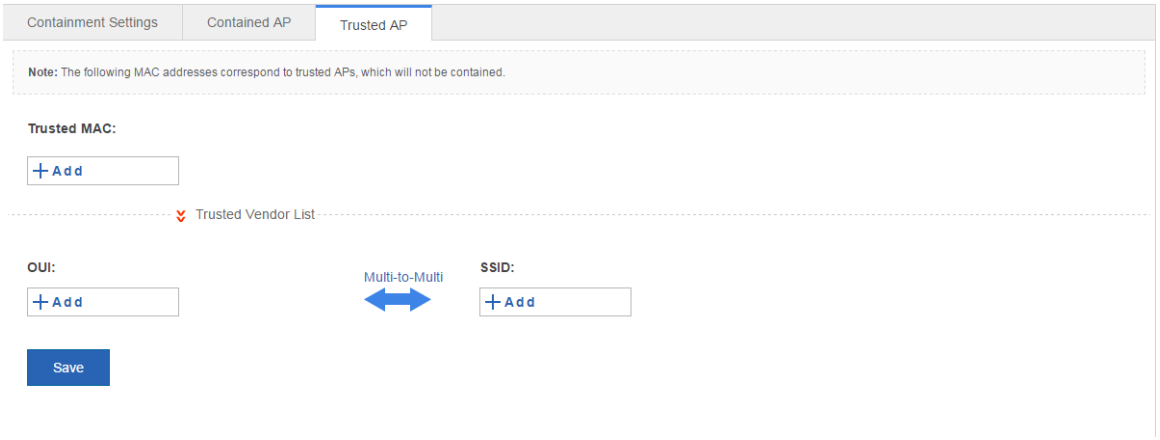


You can select the containment mode and view the WiFi list corresponding to the contained rogue APs.

You can click **Clear Rogue AP** to clear all contained APs.

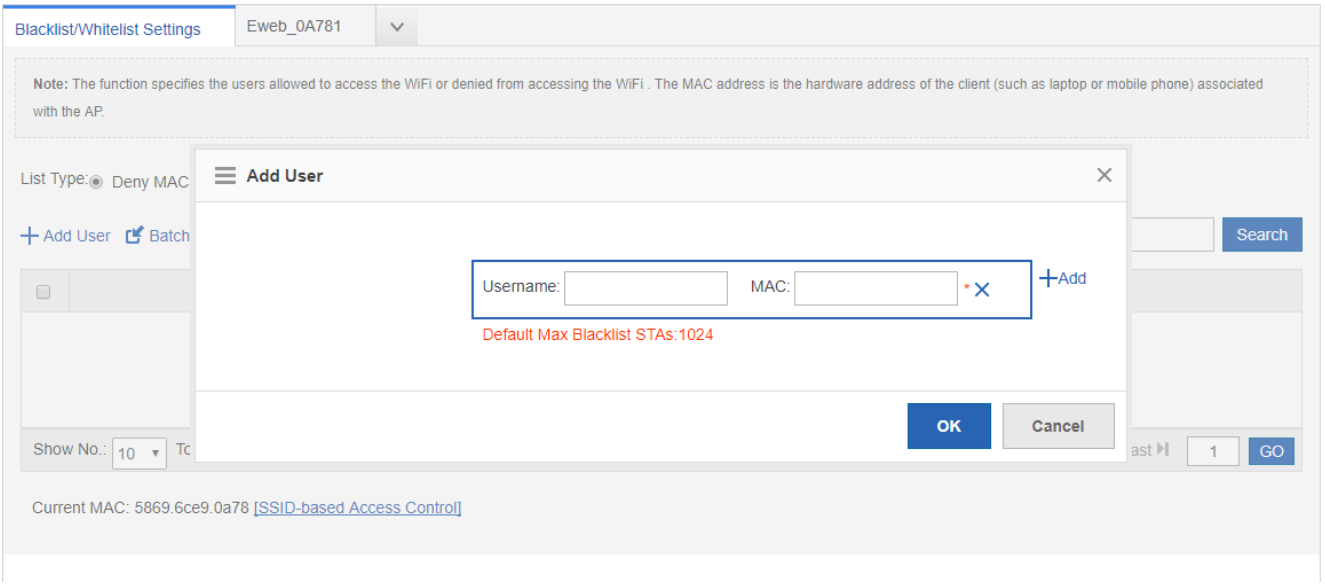
Trusted AP

When the rogue AP containment function is enabled, the APs not authorized will be contained. However, some APs are trusted devices and special processing is required. You can configure the MAC addresses of trusted devices.



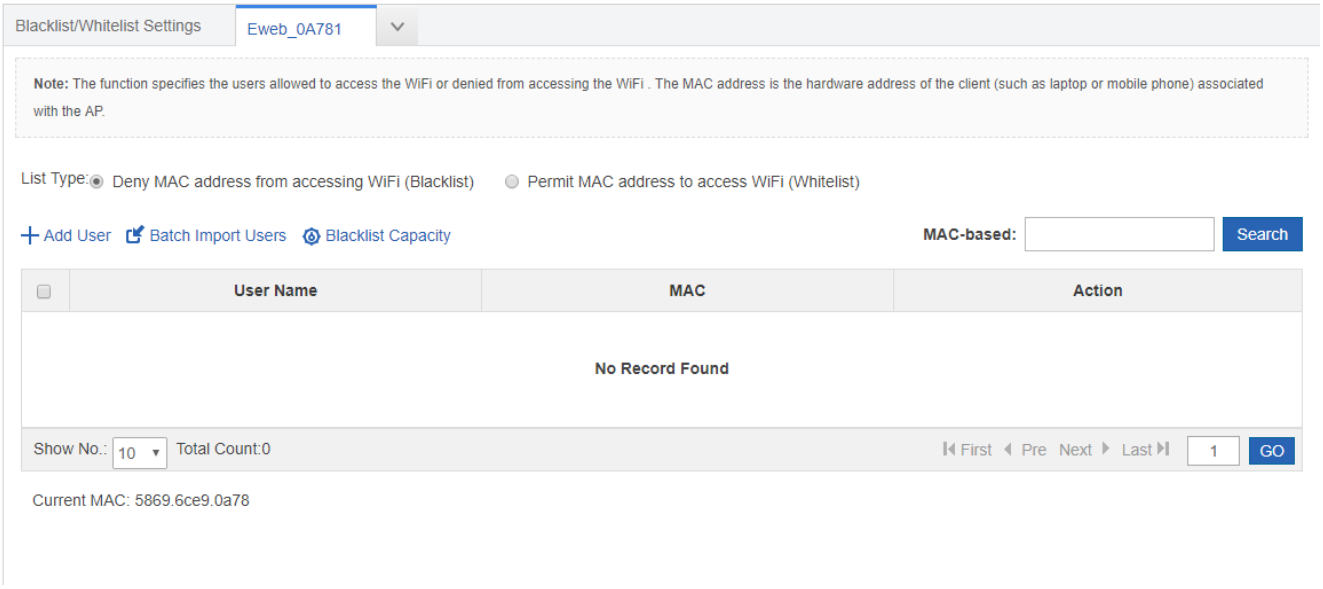
1.3.4.2 Blacklist/Whitelist

To increase wireless security, access for wireless users can be controlled by allowing or not allowing specified users WiFi access.



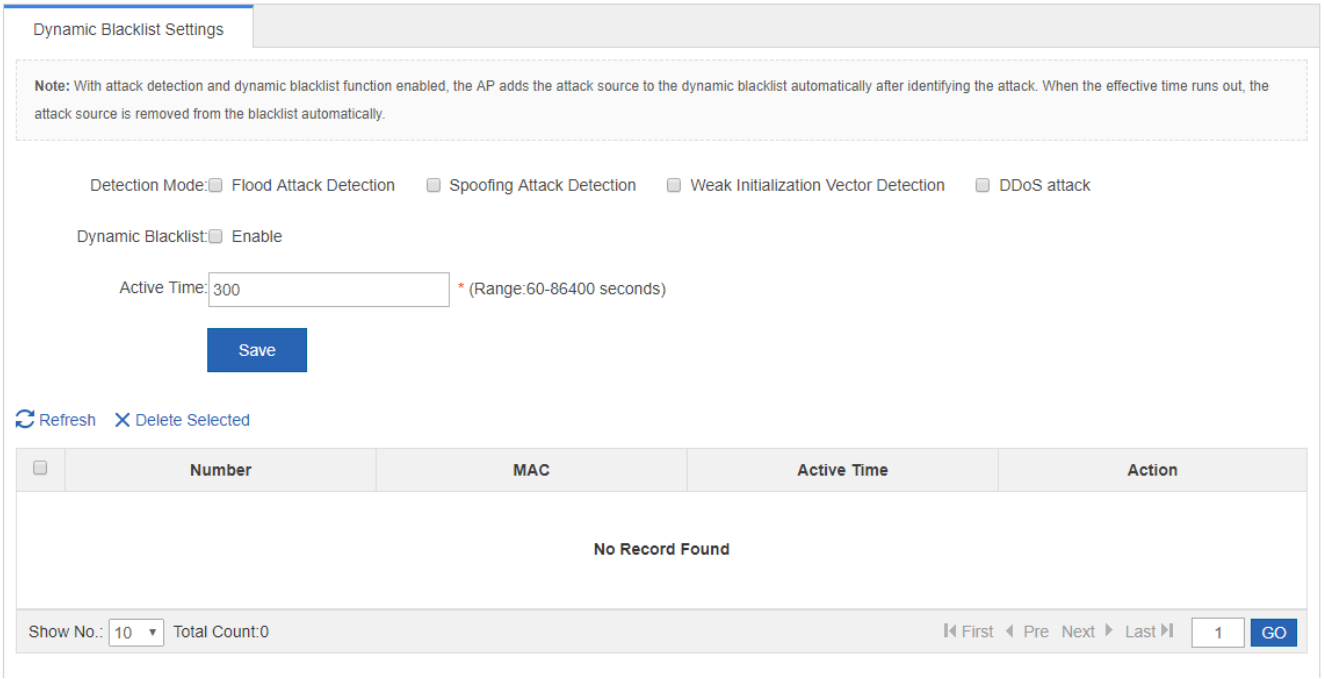
Click the Add icon to add a MAC address for a user. You can add multiple MAC addresses.

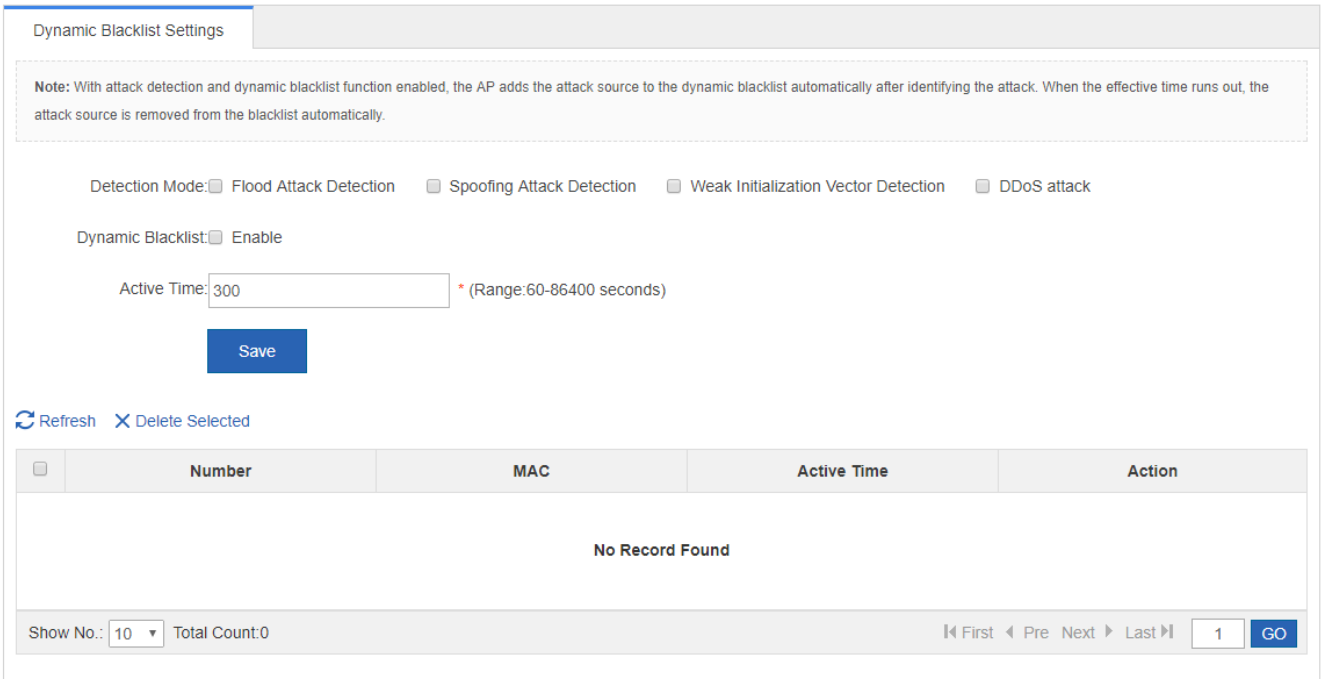
Click the **SSID-based Access Control** link to configure the blacklist and whitelist for each WiFi.



1.3.4.3 Dynamic Blacklist

Add malicious attack sources to the dynamic blacklist to prohibit access.





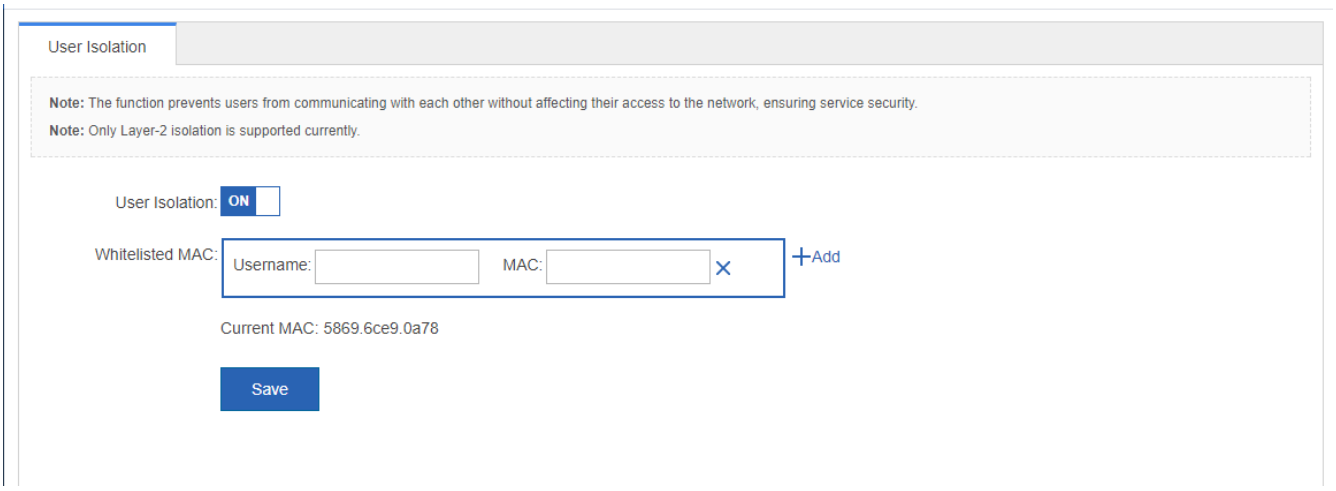
1) Set the parameters and then save the configuration.

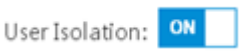
2) Select the blacklist from the list.

3) Click **Delete Selected Item** and then click **OK** in the displayed dialog box to finish deleting.

1.3.4.4 Prohibiting Mutual Access of Internal and External Networks

To ensure network security and prevent unwitting information transfer, you can prohibit communication between internal network users by means of configuration. Some special users (users who can access each other) can be identified based on the user name and MAC address.



1) Click  to enable or disable mutual access for internal network users.

2) Click to delete the MAC address of the user.

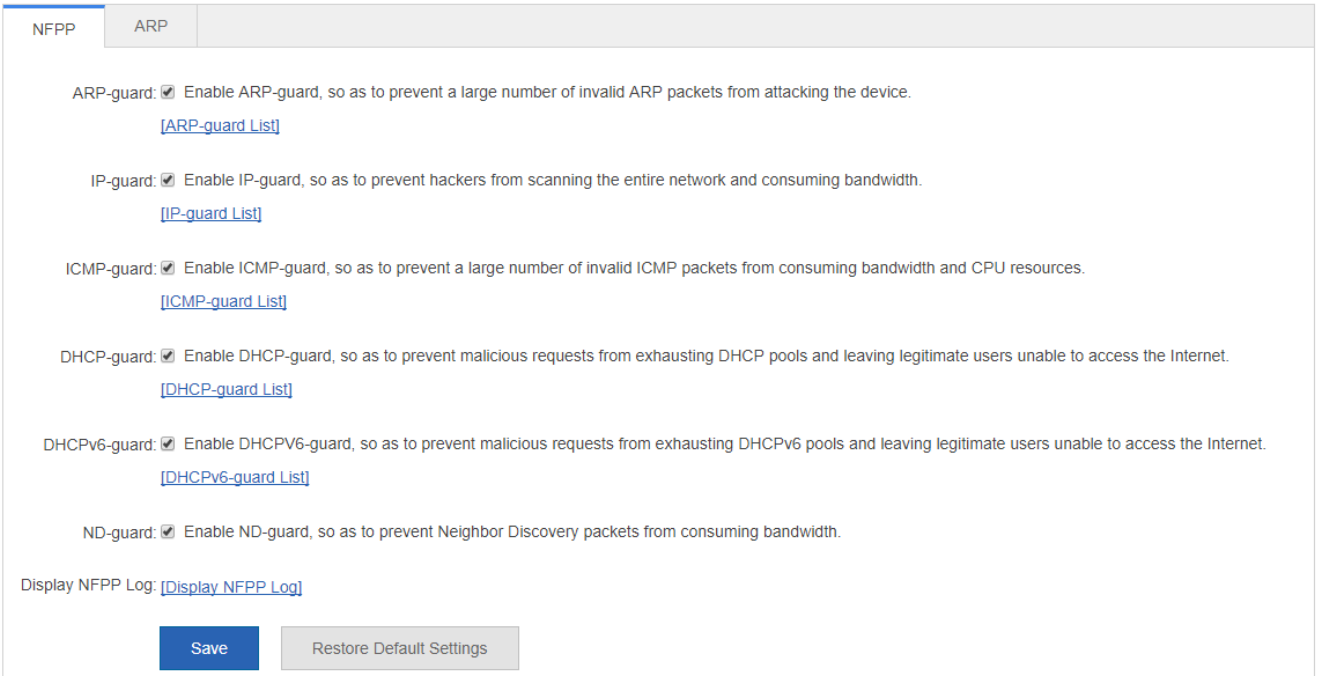
3) Click the **Add** icon to add a MAC address for a mutual-access user. You can add multiple MAC addresses.

4) Click **Save** to finish the configuration.

1.3.4.5 Anti-attack/ARP Table

Some malicious attacks are always found in the network environment. These attacks may bring about an extremely heavy burden for the switch, resulting in the switch using an excessive amount of CPU power and giving rise to a potential operational failure.

NFPP



1) **ARP-guard**: Enables ARP-guard configuration. Click the **ARP-guard List** link to view the host where ARP attack is detected.

2) **IP-guard**: Enables IP-guard configuration. Click the **IP-guard List** link to view the host where IP scanning is detected.

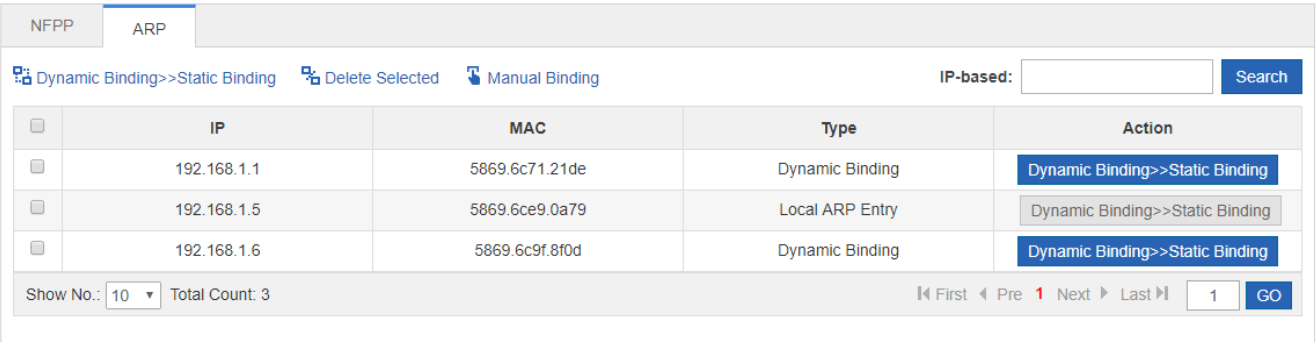
3) **ICMP-guard**: Enables ICMP-guard configuration. Click the **ICMP-guard List** link to view the host where an ICMP attack is detected.

4) **DHCP-guard**: Enables DHCP-guard configuration. Click the **DHCP-guard List** link to view the host where a DHCPv4 attack is detected.

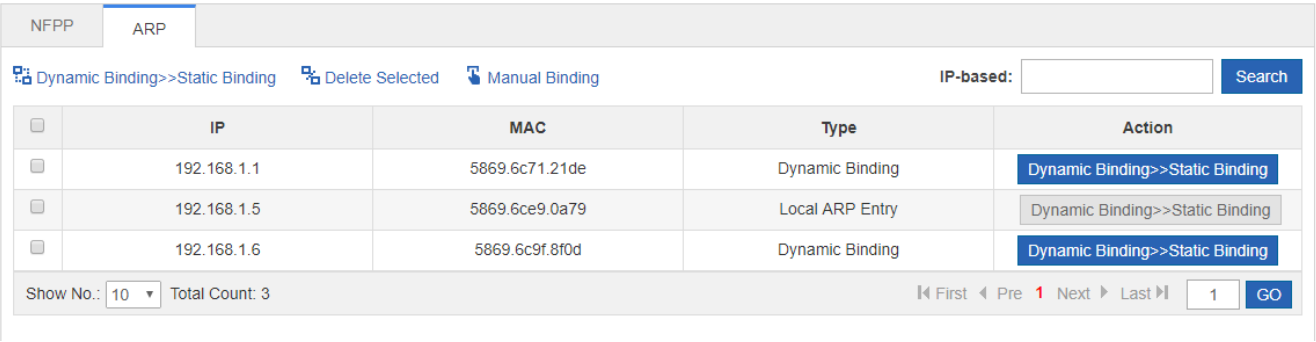
5) **DHCPv6-guard**: Enables DHCPv6-guard configuration. Click the **DHCPv6-guard List** link to view the host where a DHCPv6 attack is detected.

6) **ND-guard**: Enables ND-guard configuration.

ARP



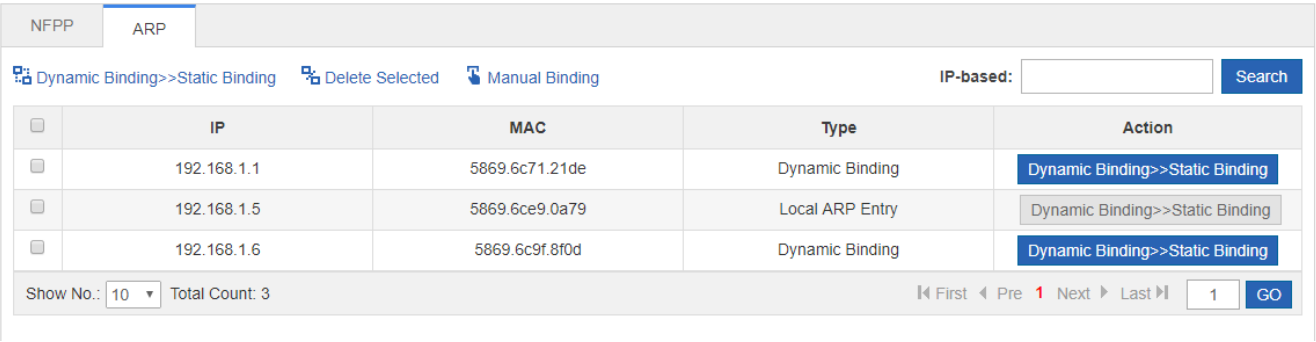
- Dynamic Binding>>Static Binding



1) Select one or multiple records from the ARP list.

2) Click the **Dynamic Binding>>Static Binding** icon to switch from dynamic binding to static binding in batches.

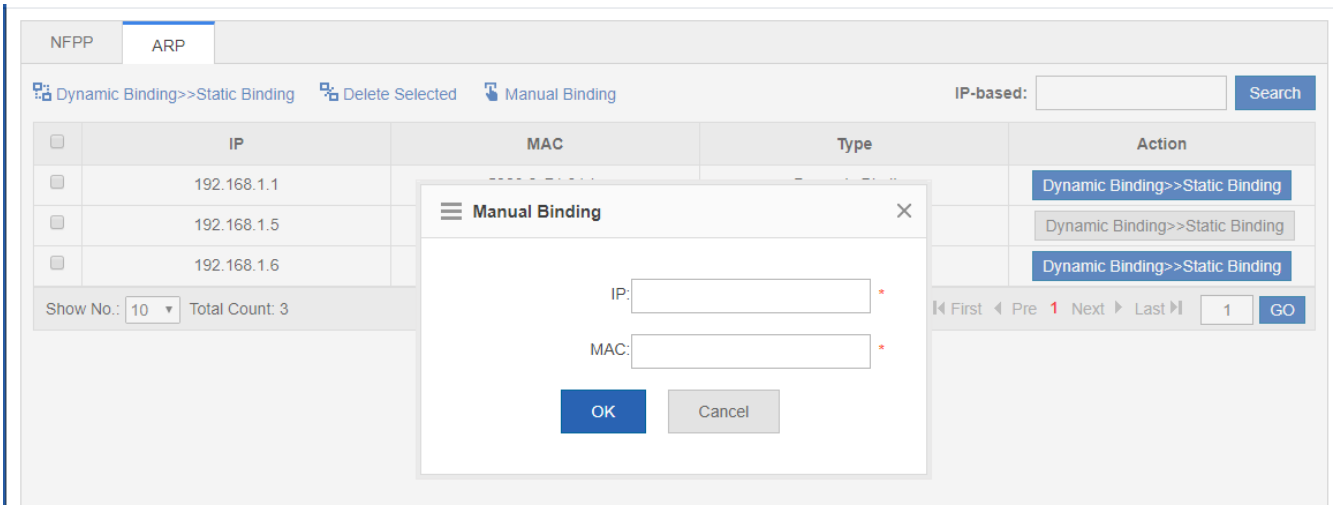
- Remove static Binding



1) Select one or multiple records from the ARP list.

2) Click the **Remove static Binding** icon to remove static binding in batches.

- Manual Binding



1) Click the **Manual Binding** icon.

2) Set the IP address and MAC address.

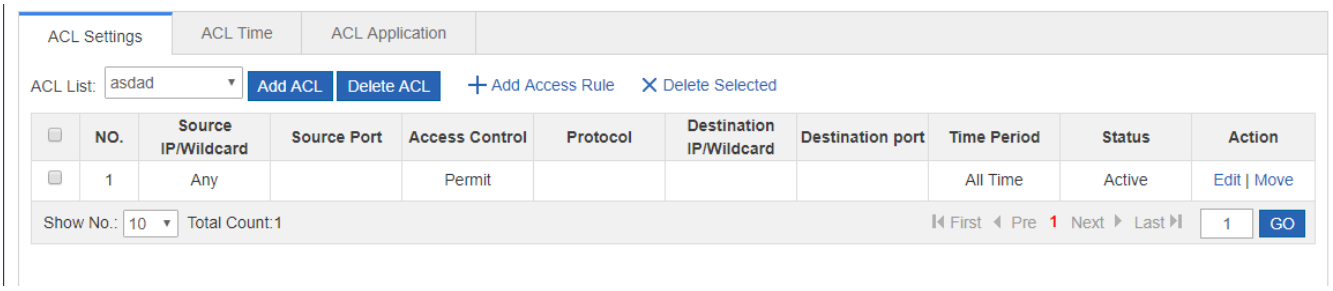
Click **OK**. The newly bound ARP is displayed in the ARP list after the **Save operation succeeded** message is displayed.

1.3.4.6 ACL

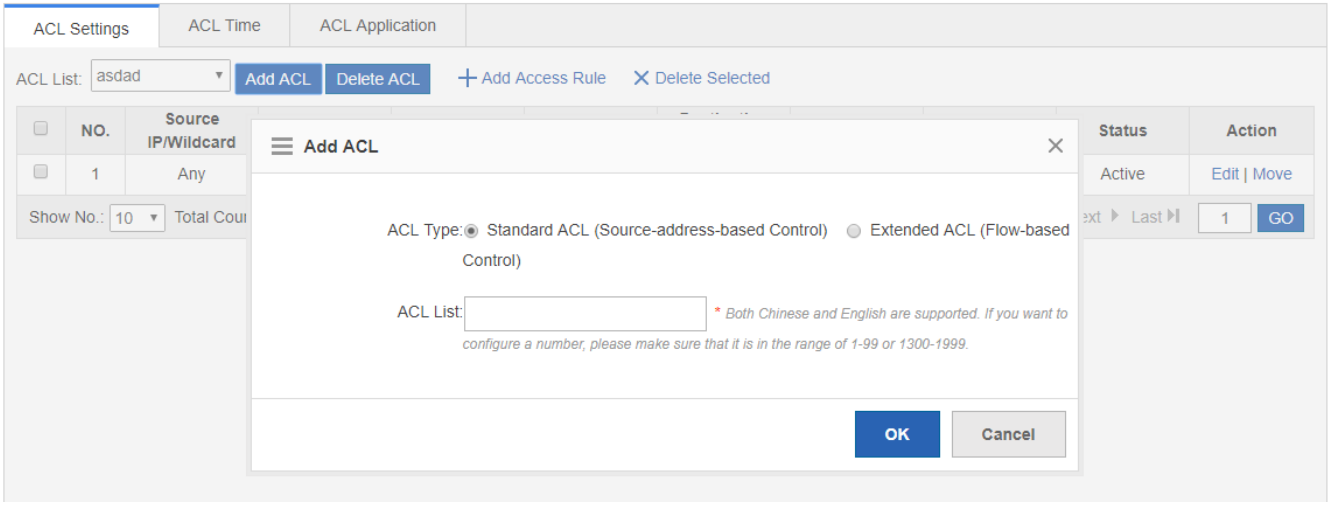
When receiving a packet on a port, the input ACL checks whether the packet matches the ACE entry for this port. When the device intends to output a packet through a port, the output ACL checks whether the packet matches the ACE entry for this port.

When there are different filtration rules, multiple rules may be applied simultaneously and only several of them can be applied. If a packet matches an ACE entry, this packet is processed (permitted or denied) according to the action policy defined by this ACE.

ACL List

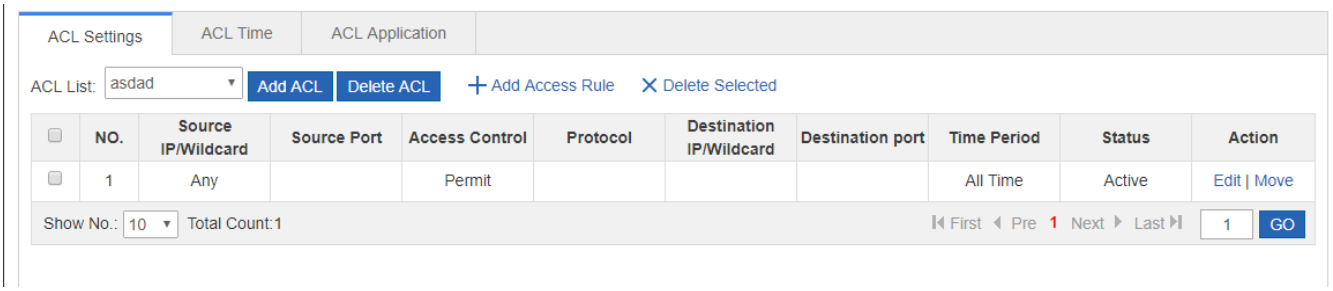


- Adding an ACL



Click **Add ACL** and set the configuration items in the dialog box displayed. Click **OK**. The newly added ACL is displayed in the **ACL List** drop-down list on the left after the **Save operation succeeded** message is displayed.

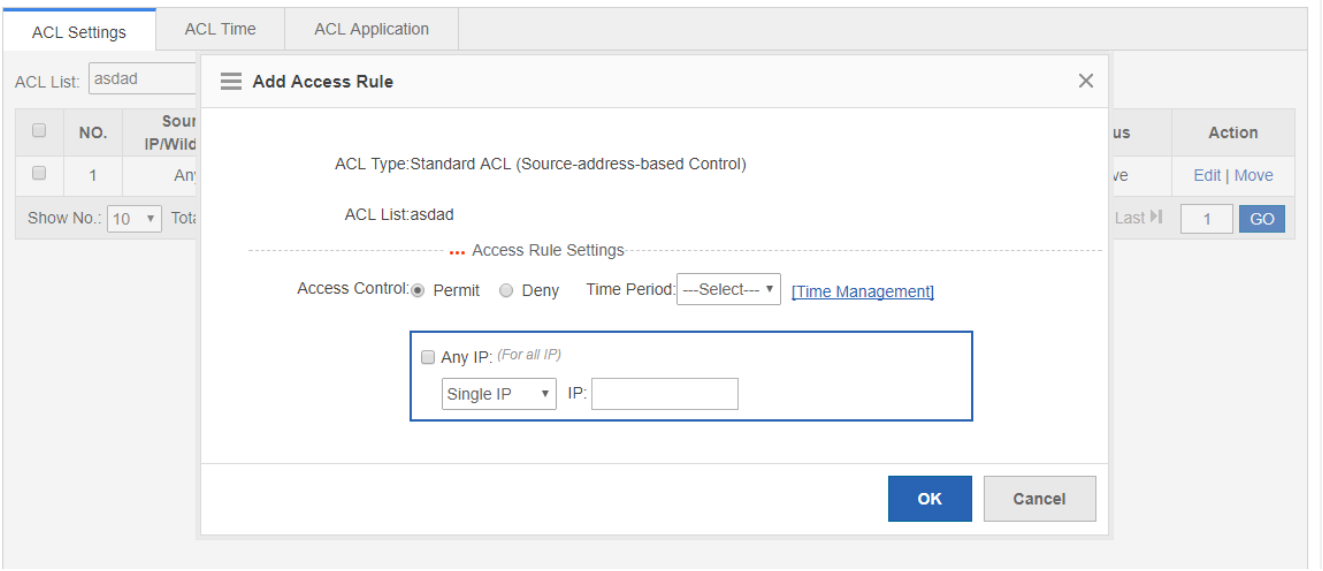
- Deleting an ACL



1) Select the ACL from the **ACL List** drop-down list.

2) Click **Delete ACL** to finish deleting.

- Adding an access rule



1) Click **Add Access Rule**.

2) Set the configuration items in the dialog box displayed.

3) Click **OK**. The newly added access rule is displayed in the access rule list after the Save operation succeeded message is displayed.

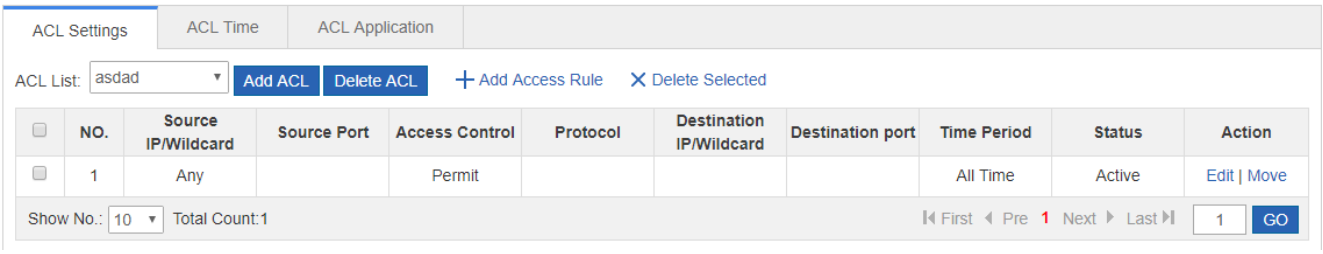
- Editing an access rule

1) Click the **Edit** button for an access rule in the access rule list.

2) The configuration for the access rule is displayed in the dialog box and the configuration can be edited.

3) Click **OK**. The **Save operation succeeded** message is displayed.

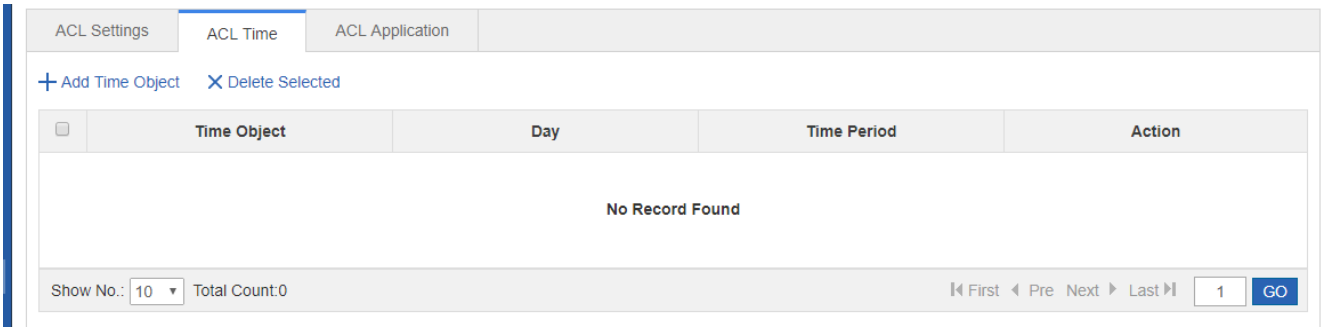
- Deleting an access rule



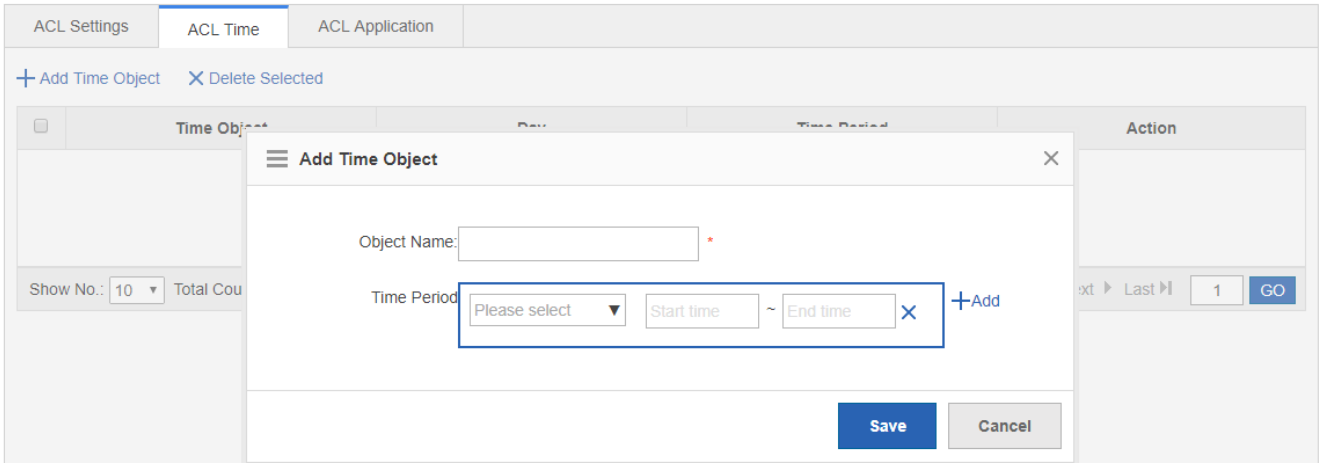
1) Select one or multiple records from the access rule list.

Click **Delete Selected Access Rule** and then click **OK** in the displayed dialog box to finish deleting.ACL Time

ACLs based on time can be enabled. For example, you can set ACLs to take effect in different time segments for a week, but first a time object must be configured.

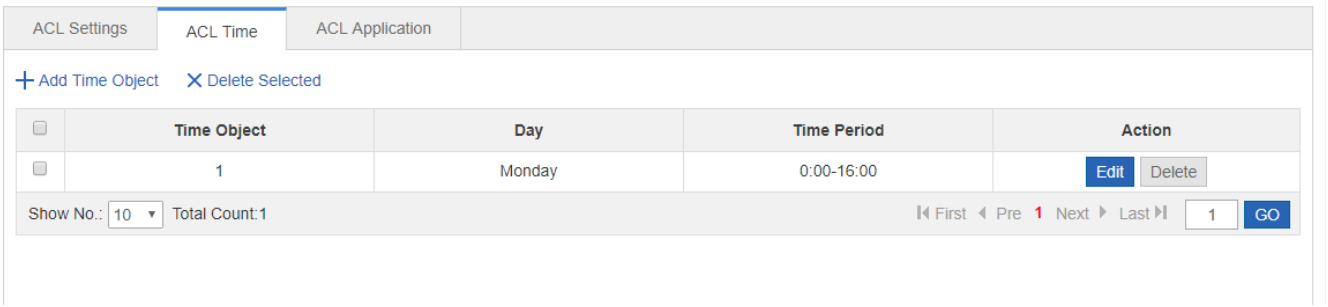


- Adding a time object



Click **Add Time Object**, then set the configuration items in the dialog box displayed, and click **Save**. The newly added time object is displayed in the time object list after the **Save operation succeeded** message is displayed.

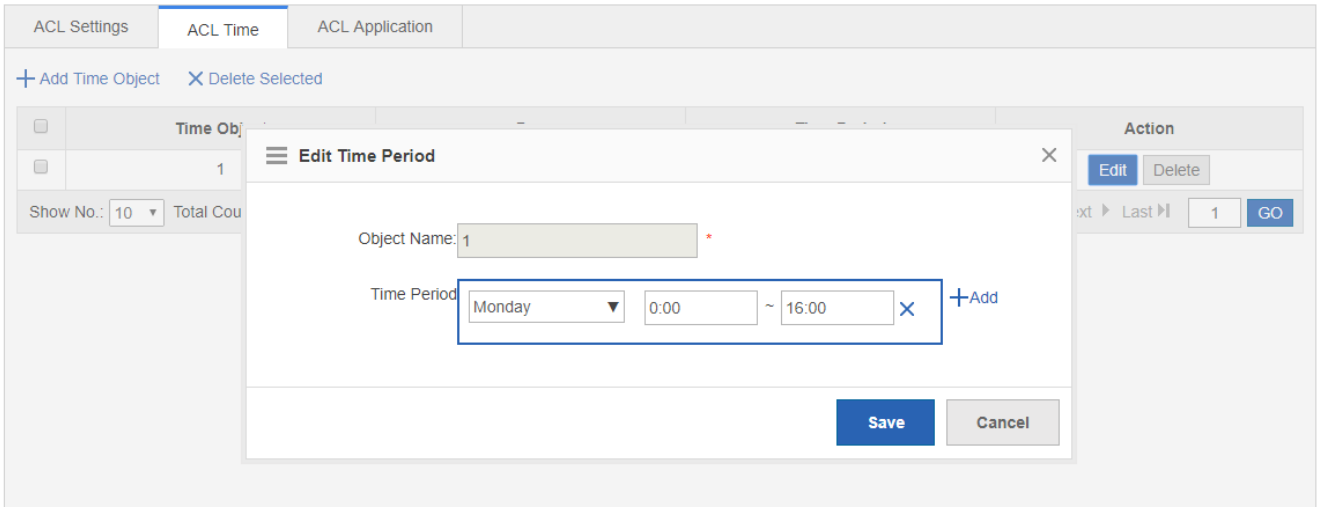
- Deleting time objects in batches



1) Select one or multiple records from the time object list.

2) Click **Delete Selected Time Object** and then click **OK** in the dialog box displayed to finish deleting.

- Editing a time object

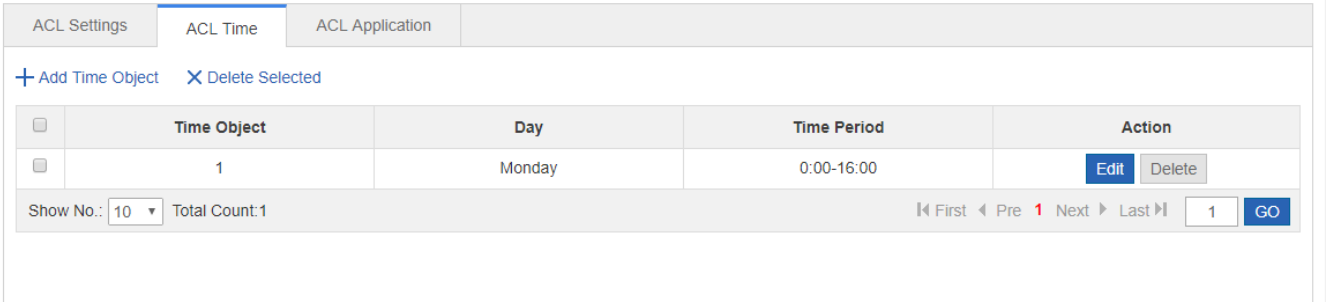


1) Click the **Edit** button for a time object in the list.

2) The configuration about the time object is displayed in the dialog box. Then edit the configuration.

3) Click **Save**. The **Save operation succeeded** message is displayed.

- Deleting a time object



Click the **Delete** button for a time object in the list.

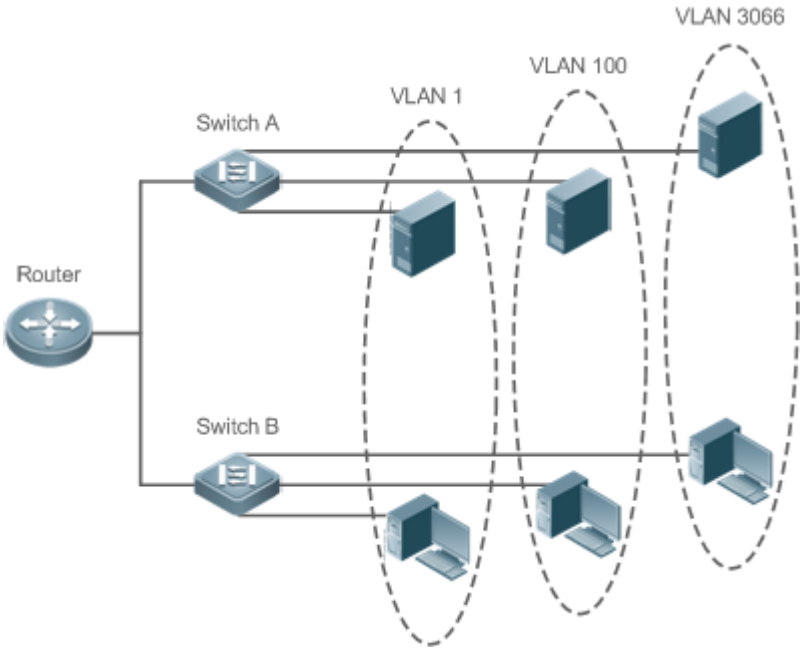
1.3.5 Advanced

1.3.5.1 VLAN

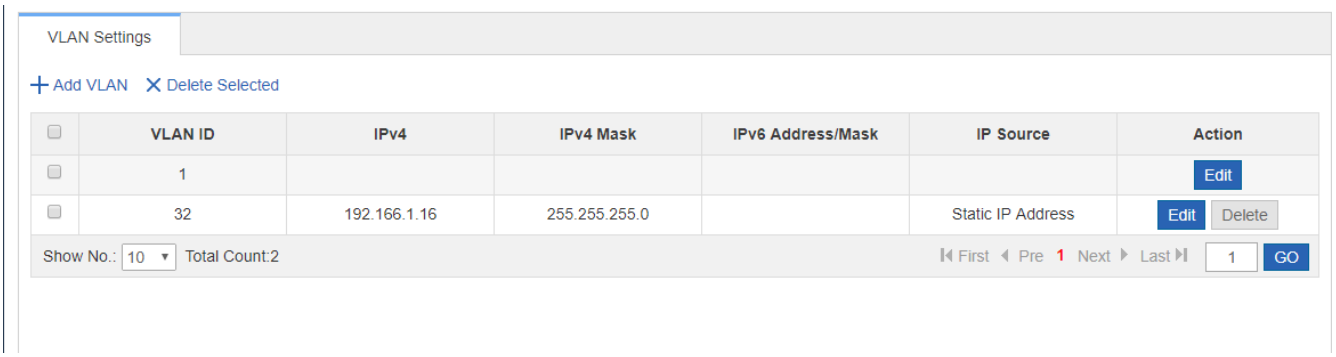
A Virtual Local Area Network (VLAN) is a logical network created based on a physical network. A VLAN can be categorized into Layer-2 networks of the OSI model.

A VLAN has the same properties as a common LAN, except for physical location limitation. Unicast, broadcast and multicast frames of Layer 2 are forwarded and transmitted within a VLAN, keeping traffic segregated.

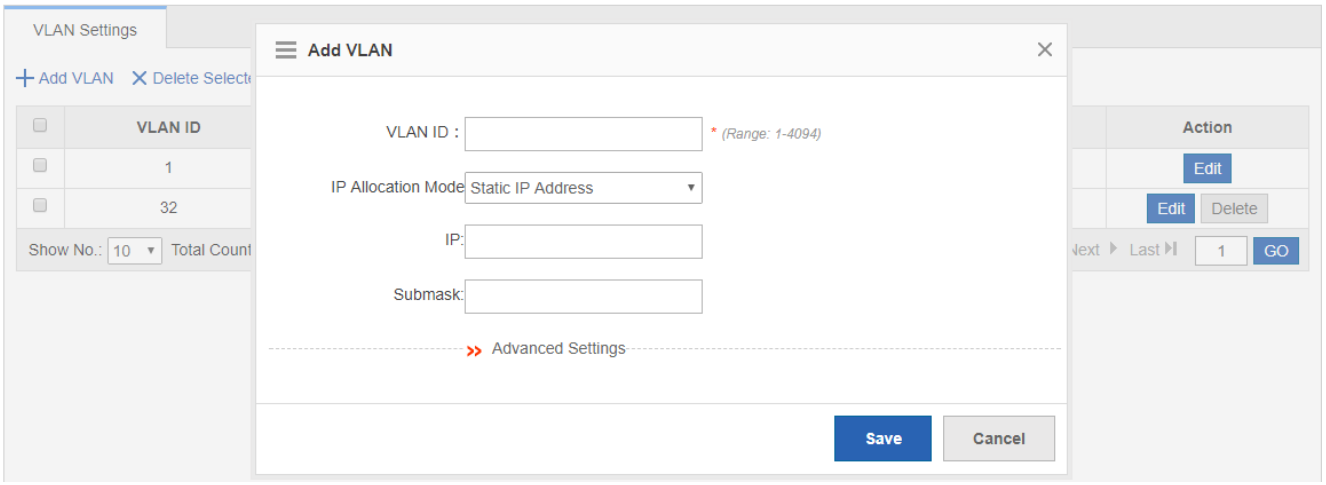
We may define a port as a member of a VLAN, and all terminals connected to this port are parts of a virtual network that supports multiple VLANs. You do not need to adjust the network physically when adding, removing and modifying users. Communication among VLANs is realized through Layer-3 devices, as shown in the following figure.



The VLANs supported by Ruijie products comply with the IEEE802.1Q standard. A maximum of 4094 VLANs (VLAN ID 1-4094) are supported, among which VLAN 1 cannot be deleted.



- Adding a VLAN



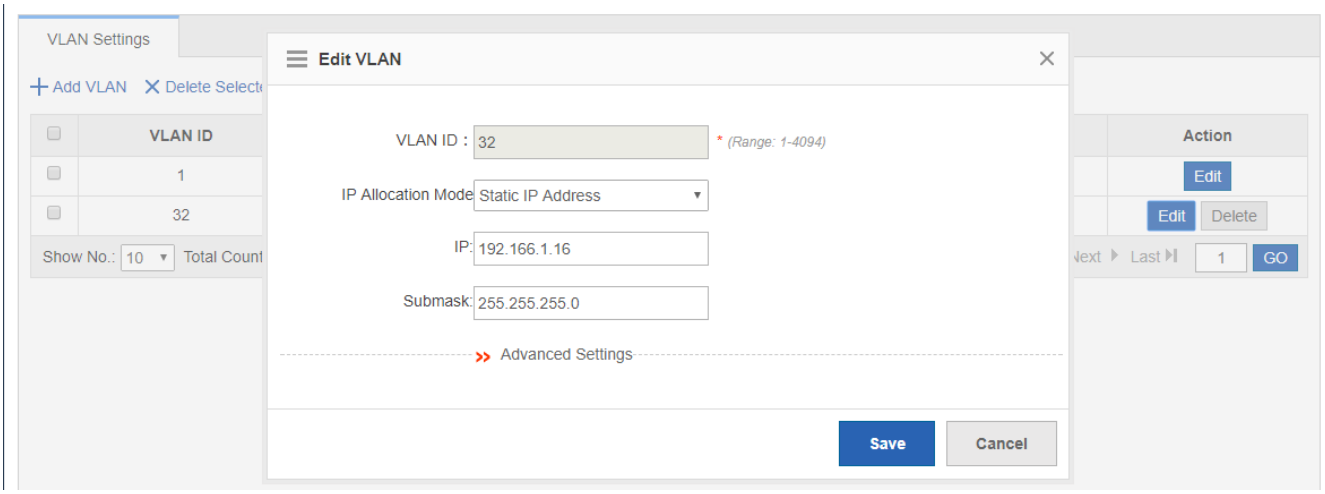
Click **Add VLAN**. A dialog box is displayed, as shown in the preceding figure. Set corresponding parameters in the dialog box and click **Save**. The newly added VLAN is displayed in the VLAN list after the **Add operation succeeded** message is displayed.

- Deleting VLANs in batches

1) Select the VLAN to be deleted from the list.

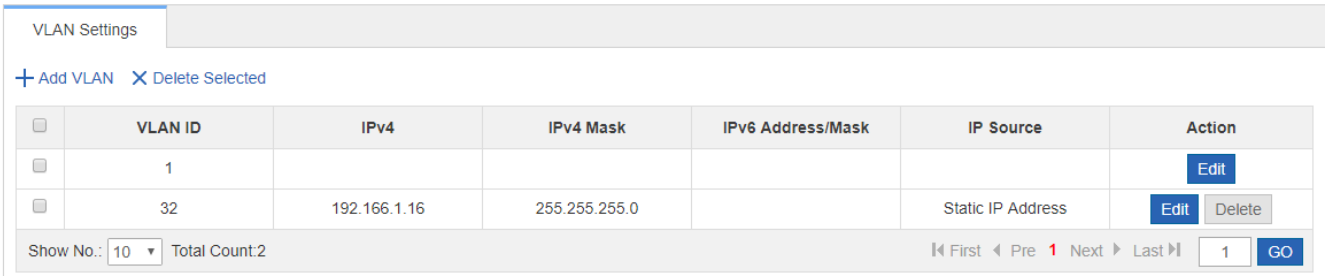
2) Click **Delete Selected VLAN** to finish deleting.

- Editing a VLAN



Click the **Edit** button. A dialog box is displayed, as shown in the preceding figure. Click **Save**. The **Save operation succeeded** message is displayed.

- Deleting a VLAN



Click the **Delete** button for a VLAN in the list and then click **OK** in the displayed dialog box to finish deleting .

1.3.5.2 Port

A port is a physical entity that is used for connections on the network devices.

Speed

Generally, the speed of an Ethernet physical port is determined through negotiation with the peer device. The negotiated speed can be any speed within the interface capability. You can also configure any speed within the interface capability for the Ethernet physical port on the Web page.

When you configure the speed of an AP port, the configuration takes effect on all of its member ports. (All these member ports are Ethernet physical ports.)

Duplex Mode

- Set the duplex mode of the interface to full-duplex so that the interface can receive packets while sending packets.
- Set the duplex mode of the interface to half-duplex so that the interface can receive or send packets at a time.
- Set the duplex mode of the interface to auto-negotiation so that the duplex mode of the interface is determined through auto negotiation between the local interface and peer interface.

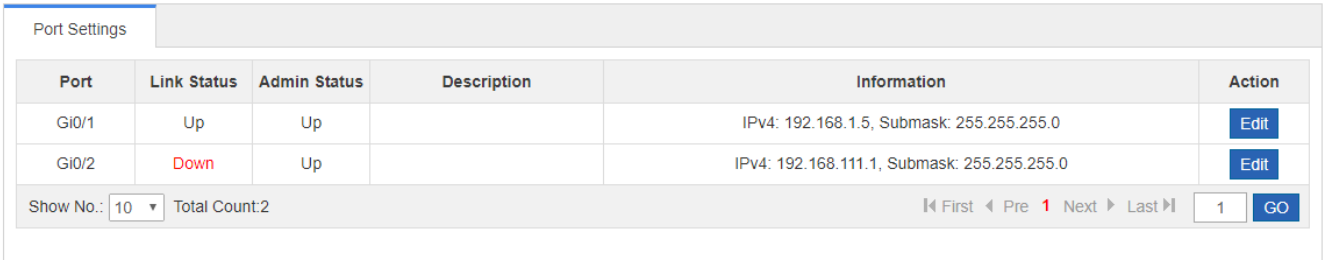
Interface Name

You can configure the name of an interface based on the purpose of the interface. For example, if you want to assign GigabitEthernet 1/1 for exclusive use by user A, you can describe the interface as "Port for User A."

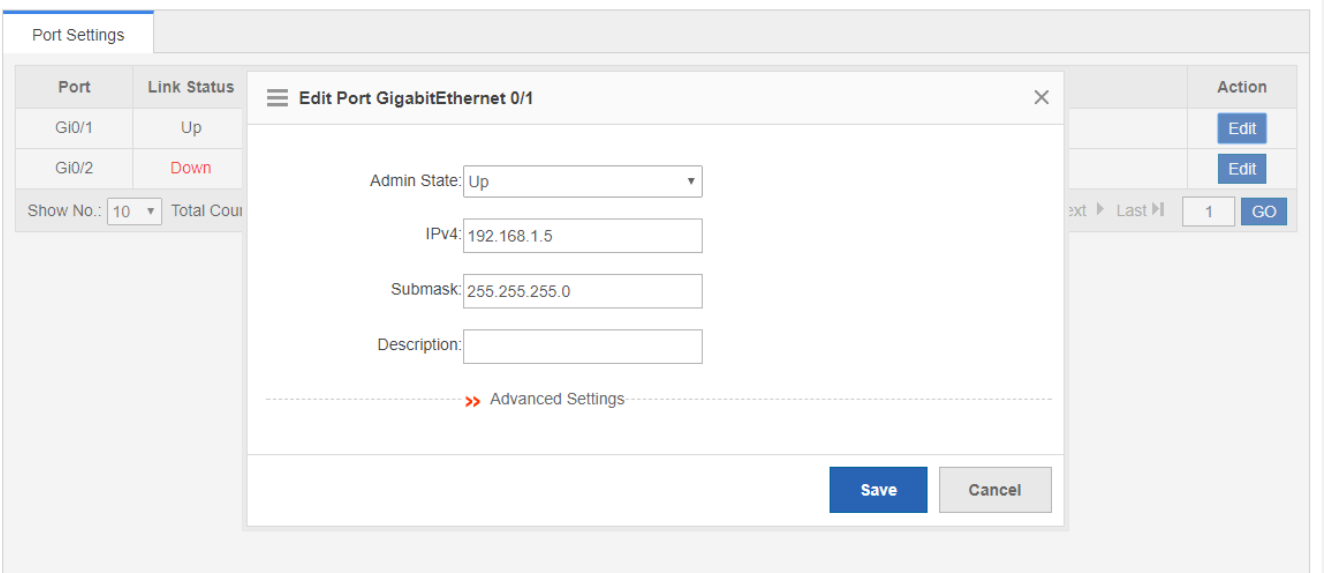
Administrative Status

You can configure the administrative status of an interface to disable the interface as required. If the interface is disabled, no frame will be received or sent on this interface, and the interface will loss all its functions. You can enable a disabled interface by configuring the administrative status of the interface. Two types of interface administrative status are defined: Up and Down. The administrative status of an interface is Down when the interface is disabled, and Up when the interface is enabled.

Port Settings



- Editing port settings



1) Click the **Edit** button for a port in the list.

2) The configuration for the port is displayed in the dialog box. Next, edit the configuration.

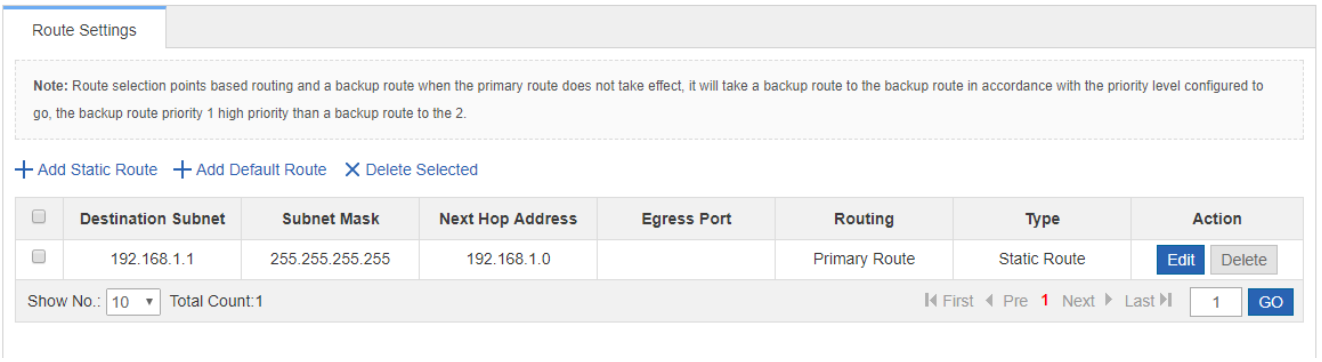
3) Click **Save**. The **Save operation succeeded** message is displayed.

1.3.5.3 Route

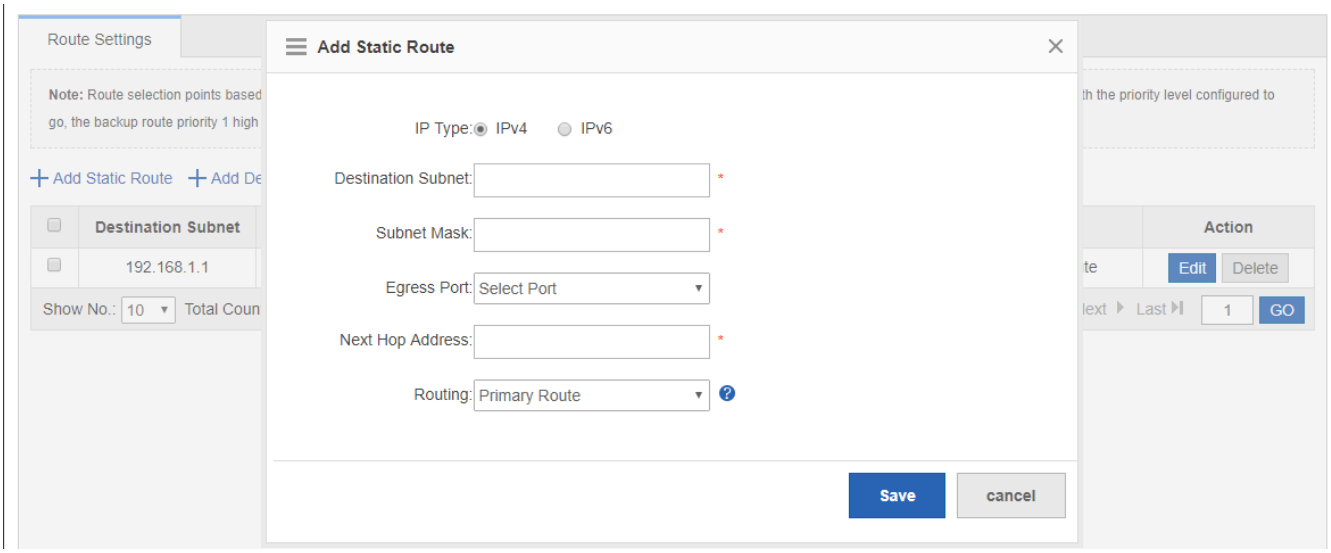
Routing is the process of selecting a path for traffic in a network, or between or across multiple networks.

Static routing is a form of routing that occurs when a router uses a manually-configured routing entry. In many cases, static routes are manually configured by a network administrator by adding in entries into a routing table, though this may not always be the case.

Default route is a setting on a computer that defines the packet forwarding rule to use when no specific route can be determined for a given Internet Protocol (IP) destination address. All packets for destinations not established in the routing table are sent via the default route.

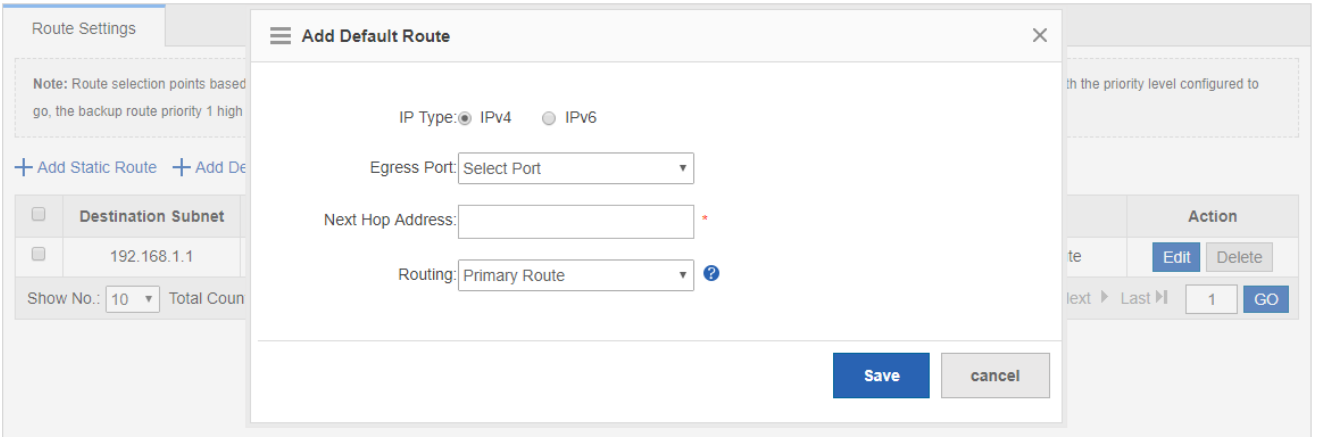


- Adding a static route



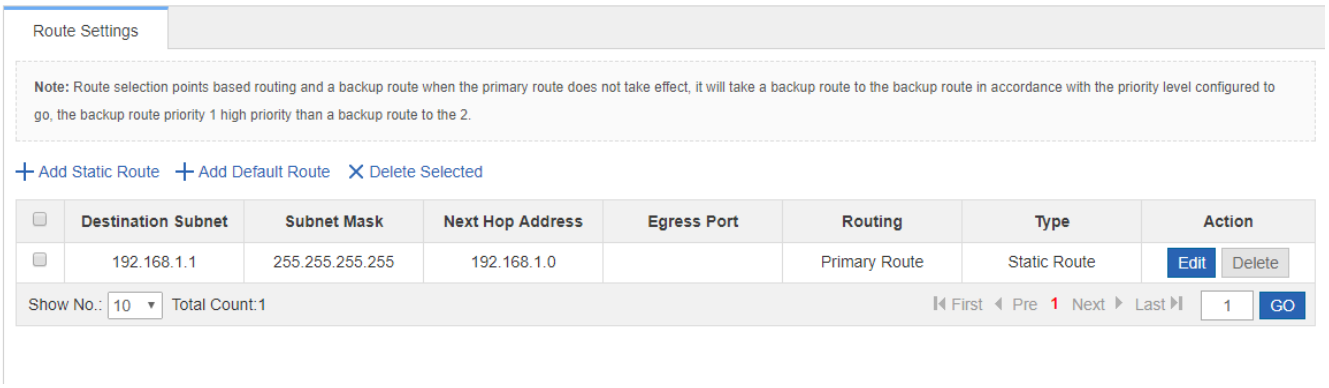
Click **Add Static Route**, set the configuration items in the dialog box displayed, and click **Save**. The newly added static route is displayed in the route list after the **Save operation succeeded** message is displayed.

- Adding the default route



Click **Add Default Route**. Set the configuration items in the displayed dialog box, and click **Save**. The newly added route is displayed in the route list after the **Save operation succeeded** message appears.

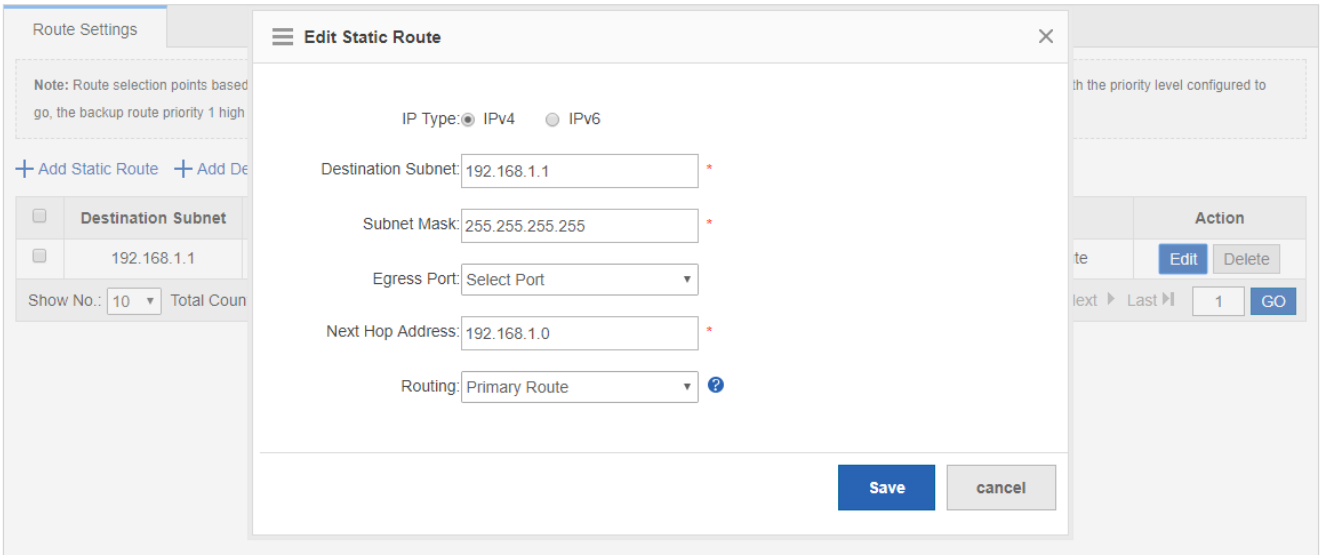
- Deleting routes in batches



1) Select the route from the list.

2) Click **Delete Selected Route** to finish deleting.

- Editing a route

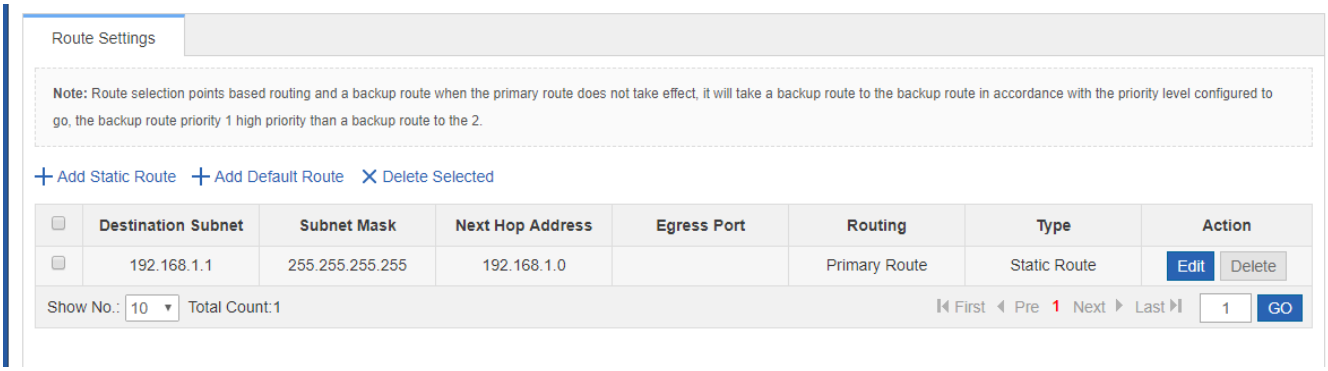


1) Click the **Edit** button for a route in the list.

2) A dialog box is displayed, as shown in the preceding figure. The configuration for the route is displayed. Next, edit the configuration.

3) Click **Save**. The **Save operation succeeded** message is displayed.

- Deleting a route



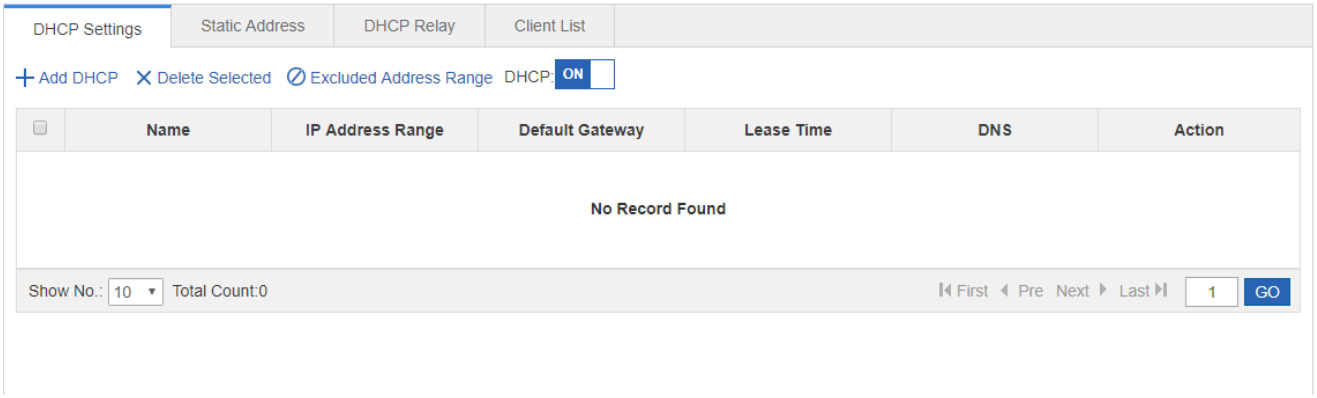
Click the **Delete** button for a route in the list and then click **OK** in the displayed dialog box to finish deleting.

1.3.5.4 DHCP

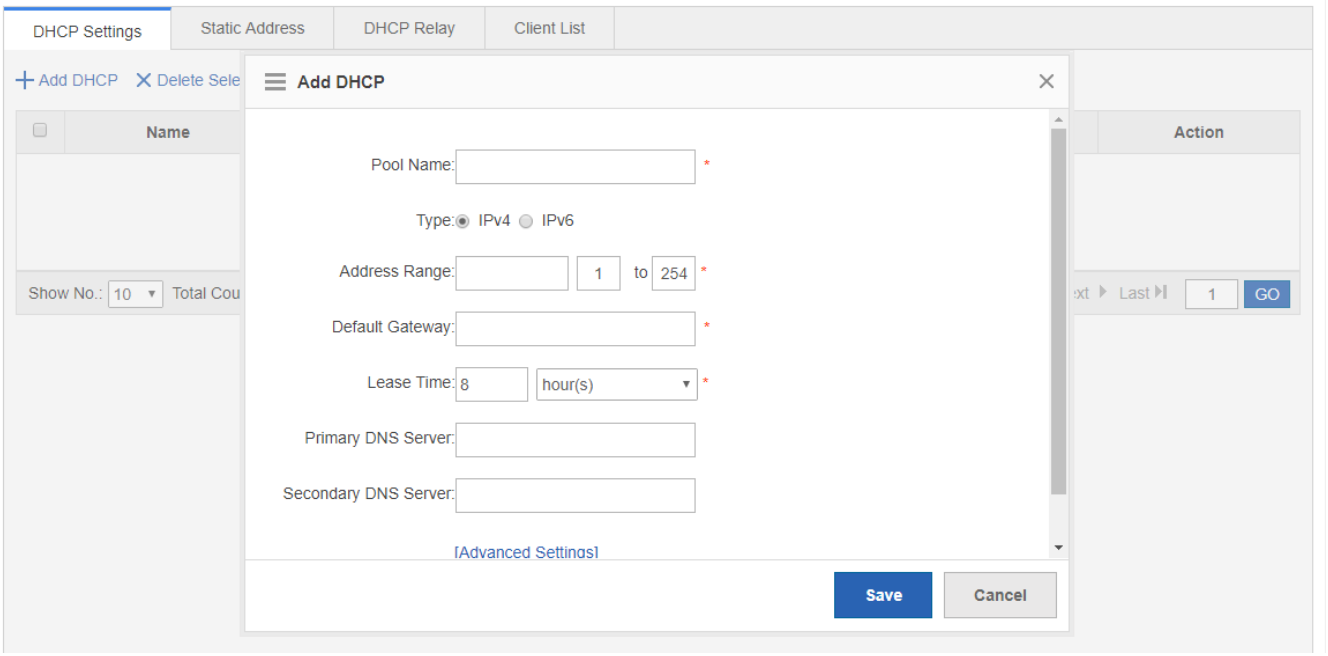
Dynamic Host Configuration Protocol (DHCP) is a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway. RFCs 2131 and 2132 define DHCP as an Internet Engineering Task Force (IETF) standard based on Bootstrap Protocol (BOOTP), a protocol with which DHCP shares many implementation details. DHCP allows hosts to obtain required TCP/IP configuration information from a DHCP server.

DHCP supports three mechanisms for IP address allocation. In "automatic allocation", DHCP assigns a permanent IP address to a client. In "dynamic allocation", DHCP assigns an IP address to a client for a limited period of time (or until the client explicitly relinquishes the address). In "static allocation", a client's IP address is assigned by the network administrator, and DHCP is used simply to convey the assigned address to the client. A particular network will use one or more of these mechanisms, depending on the policies of the network administrator.

DHCP Settings

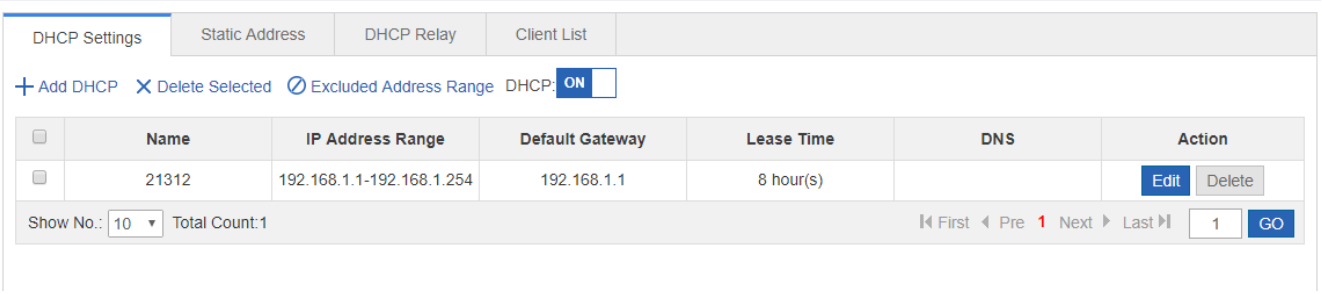


- Adding a DHCP Pool



Click **Add DHCP**, set the configuration items in the dialog box displayed, and click **Save**. The newly added DHCP pool is displayed in the DHCP pool list after the **Save operation succeeded** message is displayed.

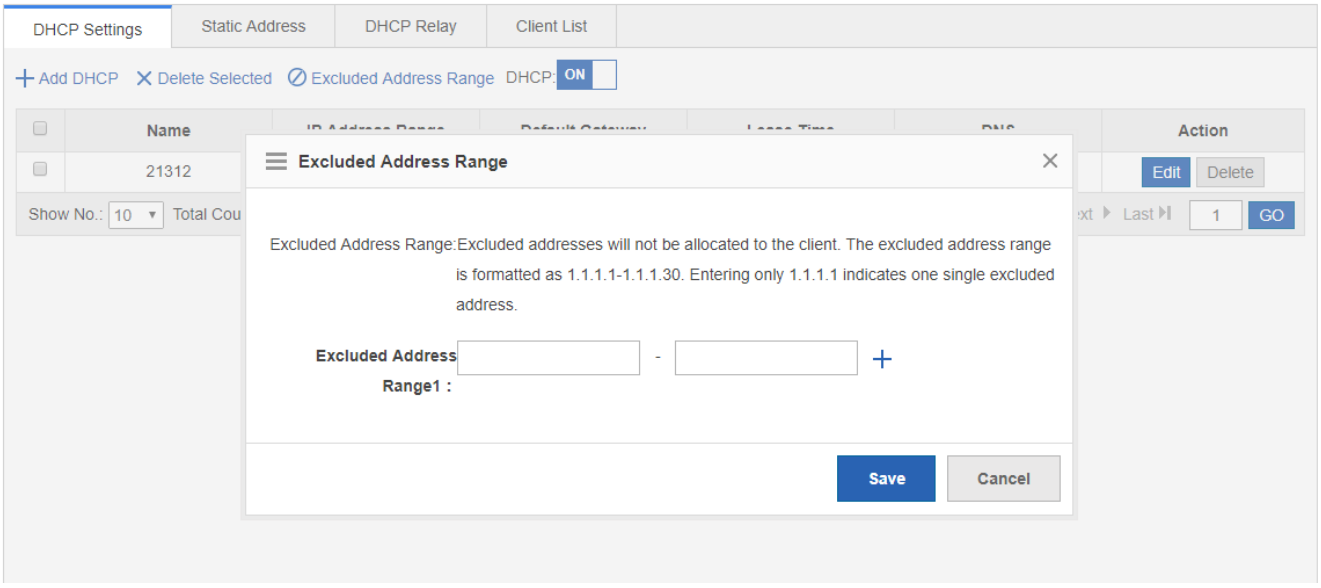
- Deleting DHCPs in batches



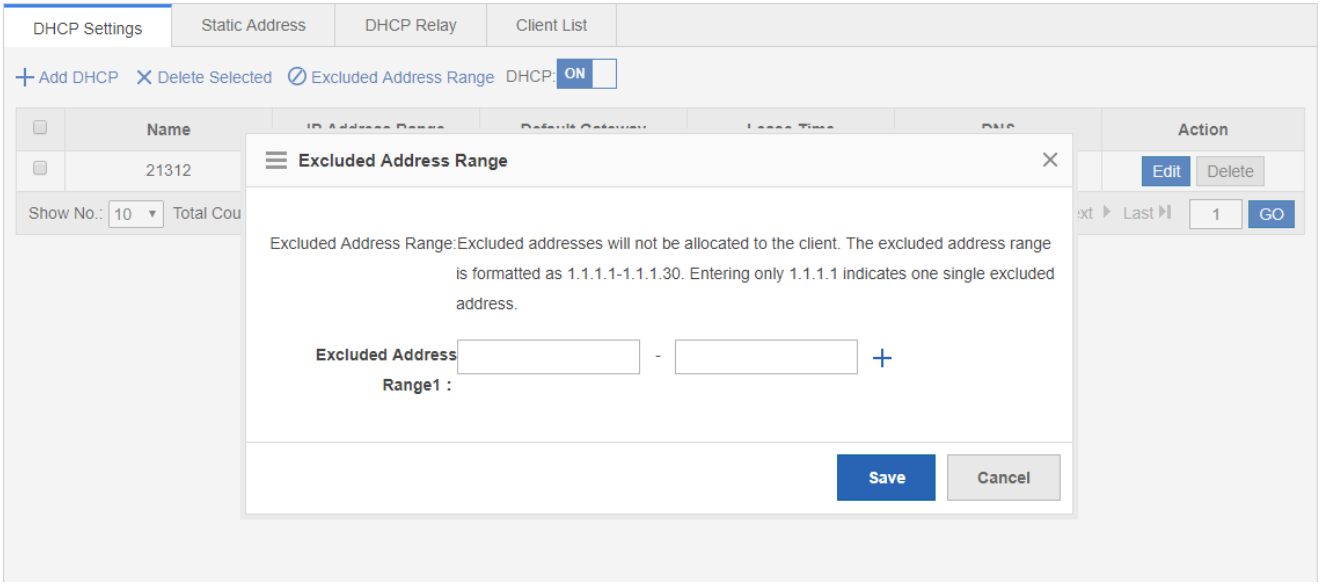
1) Select the DHCP pool from the list.

2) Click **Delete Selected DHCP** and then click **OK** in the dialog box displayed to finish deleting.

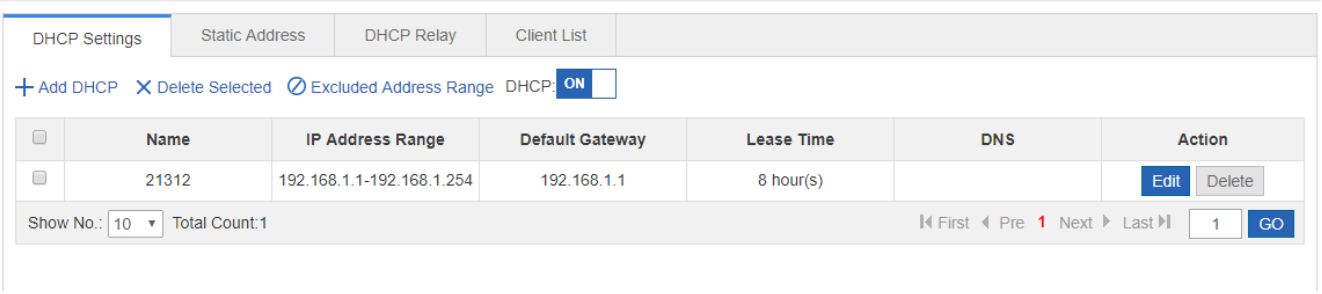
- Configuring excluded address range



Click **Excluded Address Range**. A dialog box is displayed, as shown in the preceding figure. Set the configuration items in the displayed dialog box, and click **Save**. The newly configured address range is displayed in the DHCP pool list after the **Save operation succeeded** message is displayed.

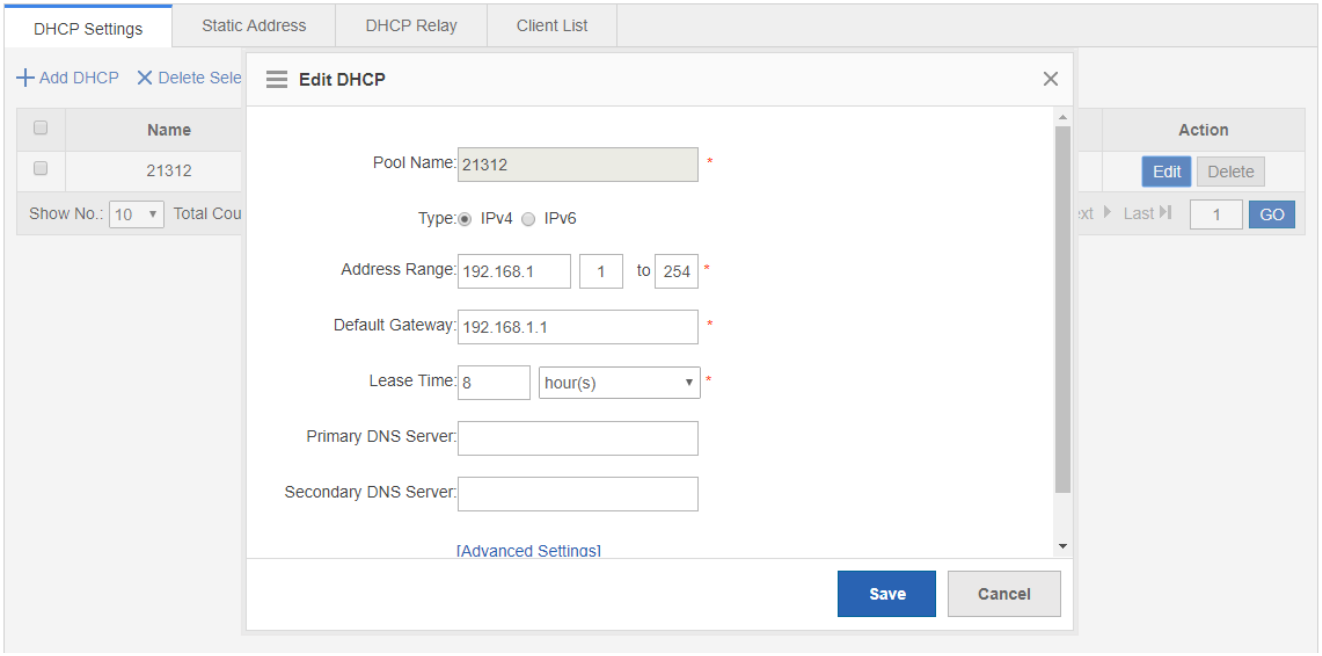


- DHCP service



Click  to enable or disable the DHCP service.

- Editing a DHCP pool

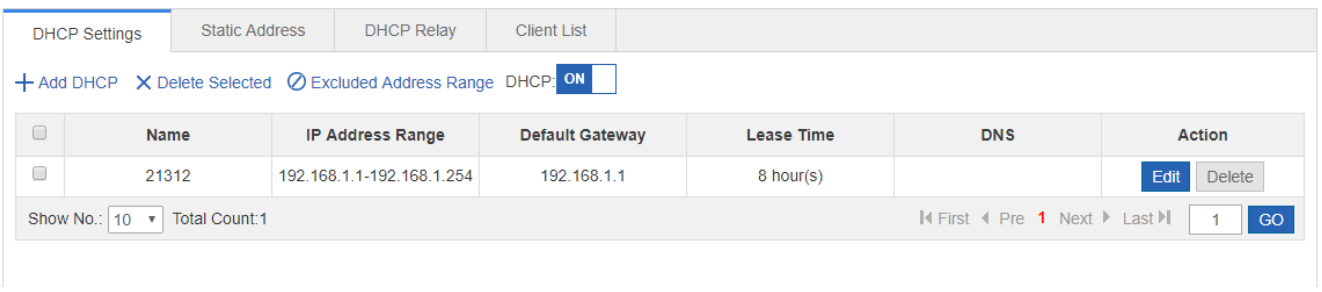


1) Click the **Edit** button for a DHCP pool in the list.

2) The configuration for the DHCP pool is displayed in the dialog box. Next, edit the configuration.

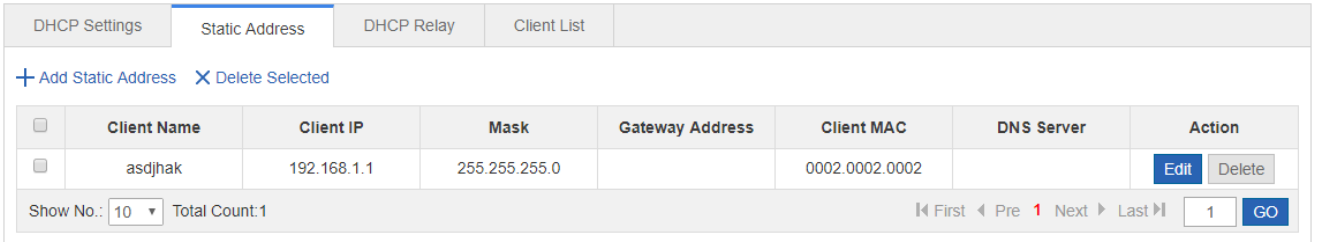
3) Click **Save**. The **Save operation succeeded** message is displayed.

- Deleting a DHCP pool

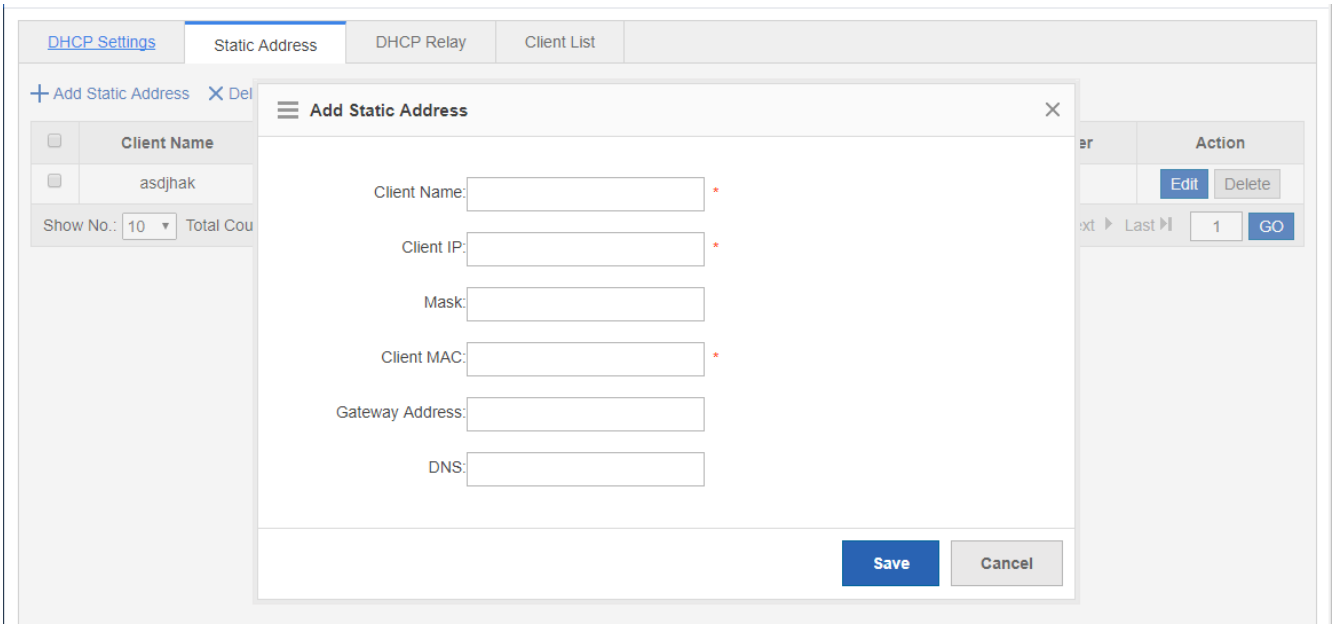


Click **Delete** to finish deleting.

Static Address

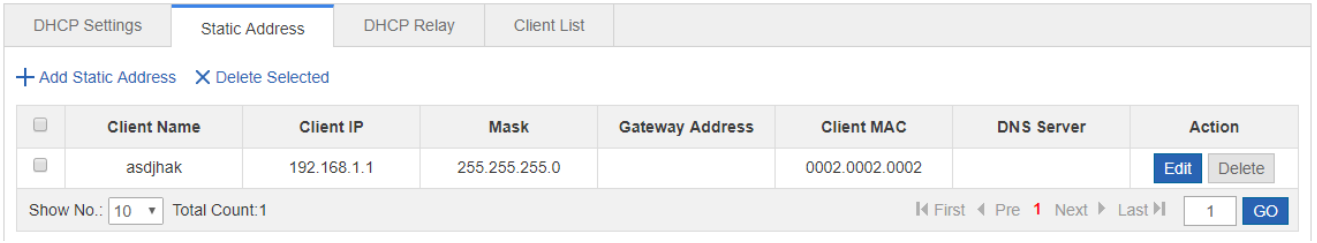


- Adding a static address



Click **Add Static Address**, set the configuration items in the displayed dialog box, and then click **Save**. The newly added static address is displayed in the list after the **Save operation succeeded** message is displayed.

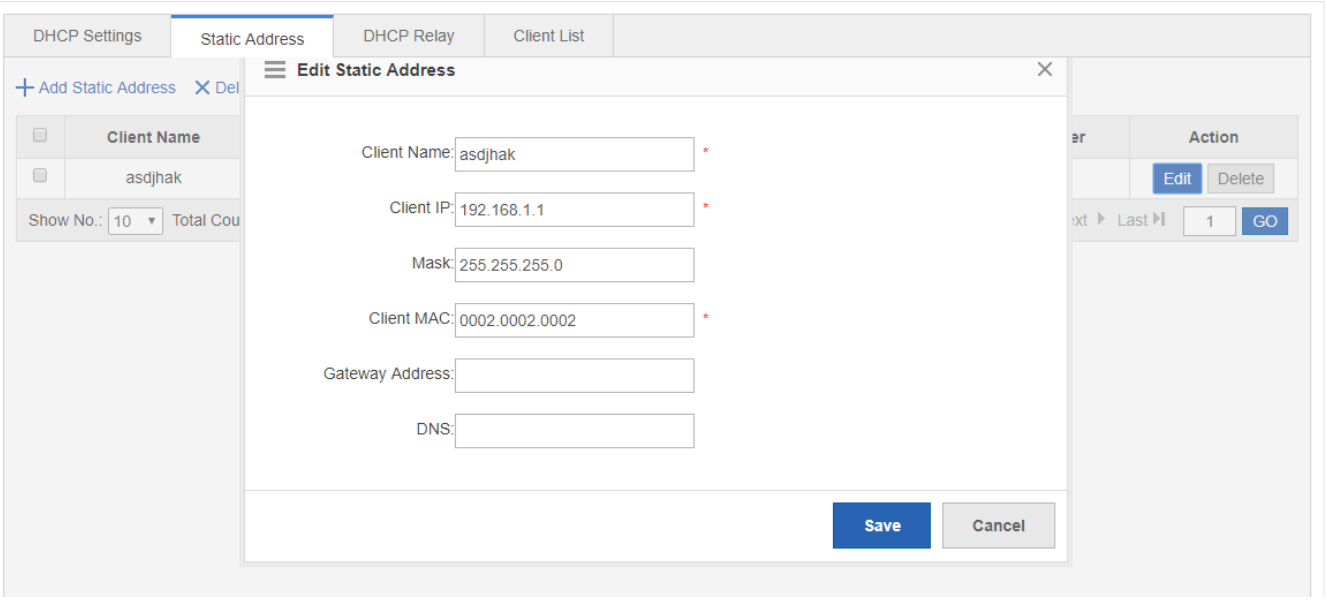
- Deleting static addresses in batches



1) Select the static address from the list.

2) Click **Delete Selected Address** and then click **OK** in the dialog box displayed to finish deleting.

- Editing a static address

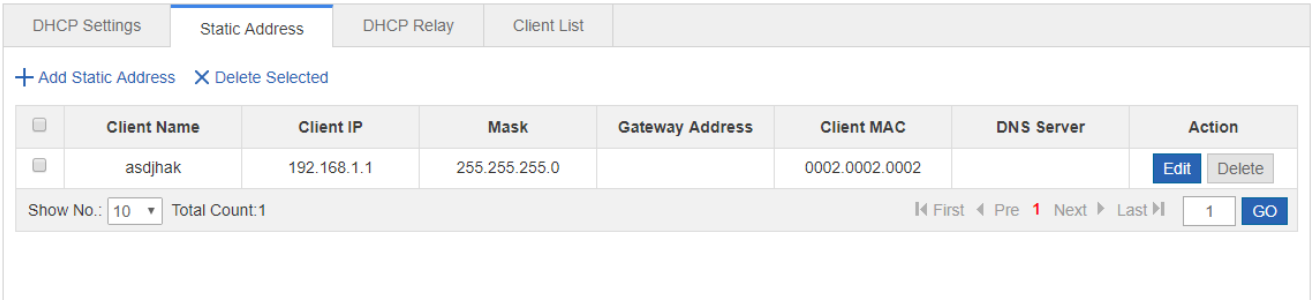


1) Click the **Edit** button for a static address in the list. A dialog box is displayed.

2) The configuration for the static address is displayed in the dialog box. Next, edit the configuration.

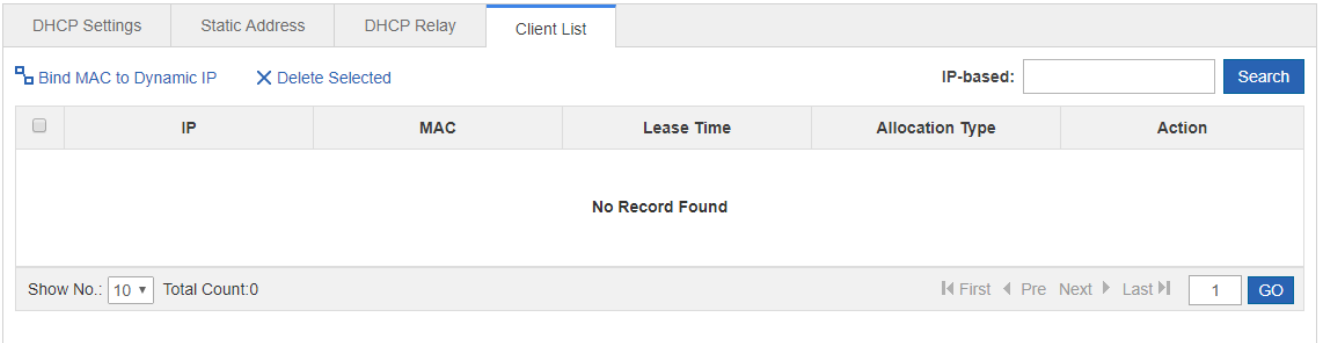
3) Click **Save**. The **Save operation succeeded** message is displayed.

- Deleting a static address

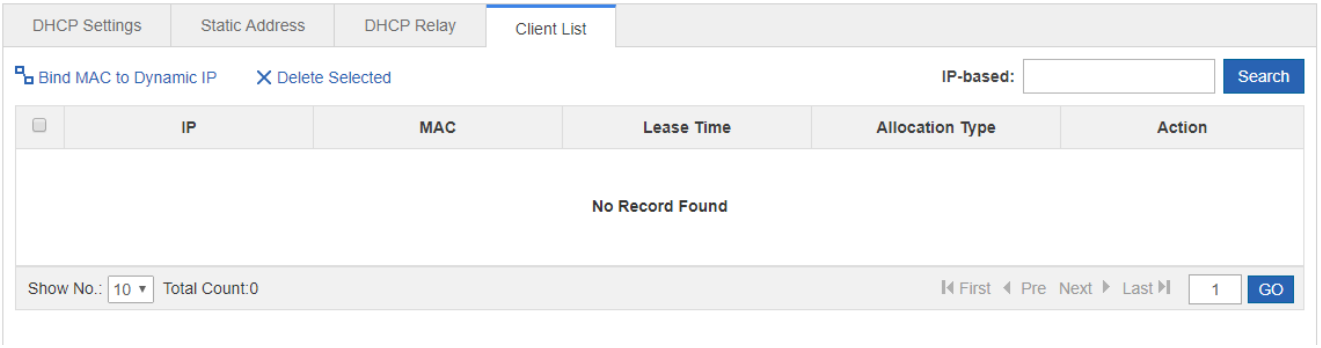


Click the **Delete** button for a static address in the list to finish deleting.

Client List



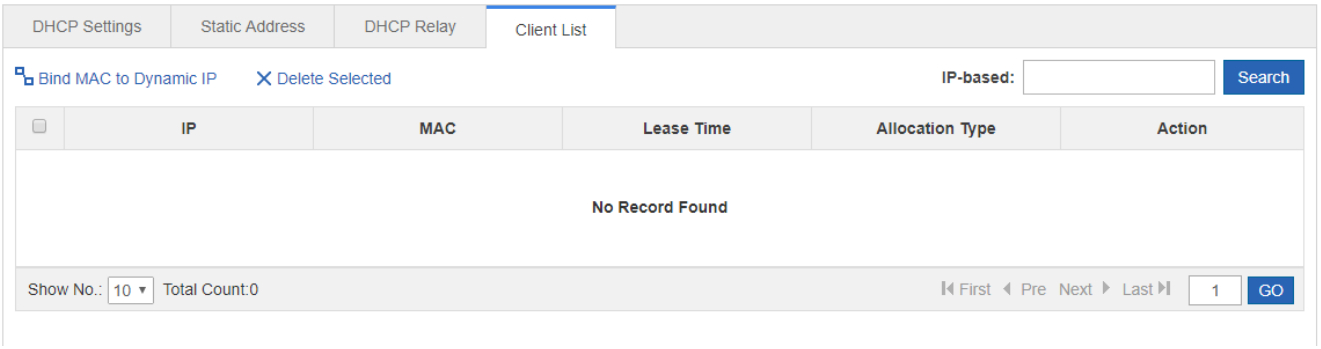
- Binding a MAC address to a dynamic IP address



1) Select the static address from the list.

2) Click **Bind MAC to Dynamic IP** and then click **OK** in the displayed dialog box to finish deleting.

- Querying clients based on IP address:



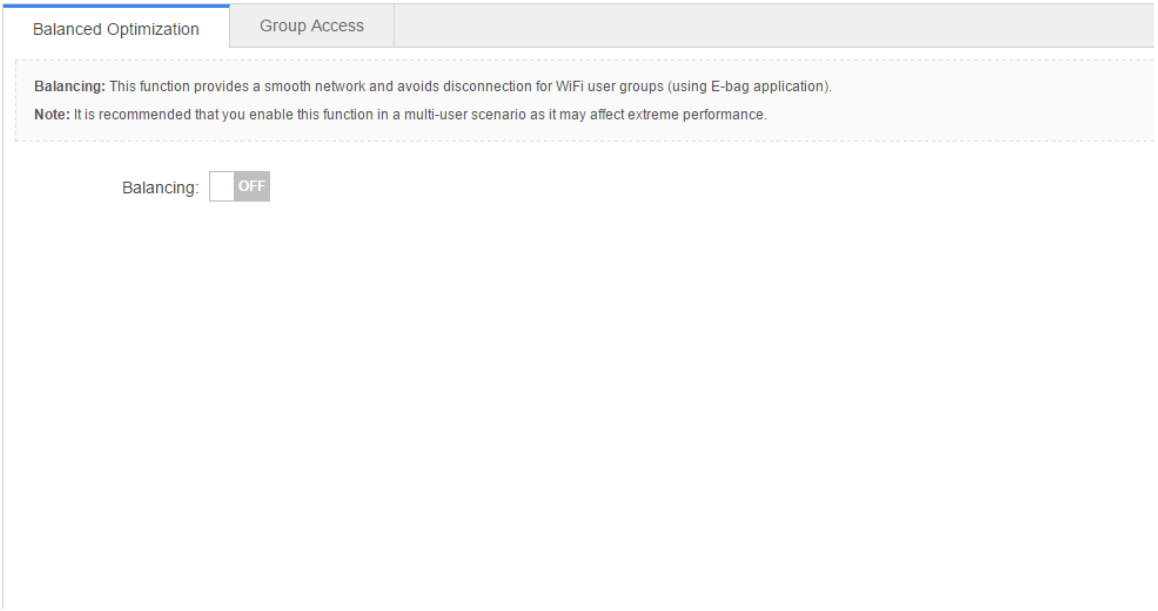
Input the IP address in the text box. Click **Search**. The search results meeting the criterion are displayed in the list.

1.3.5.5 E-bag Optimization

Your AP might not support this function, as it is subject to the actual menu items.

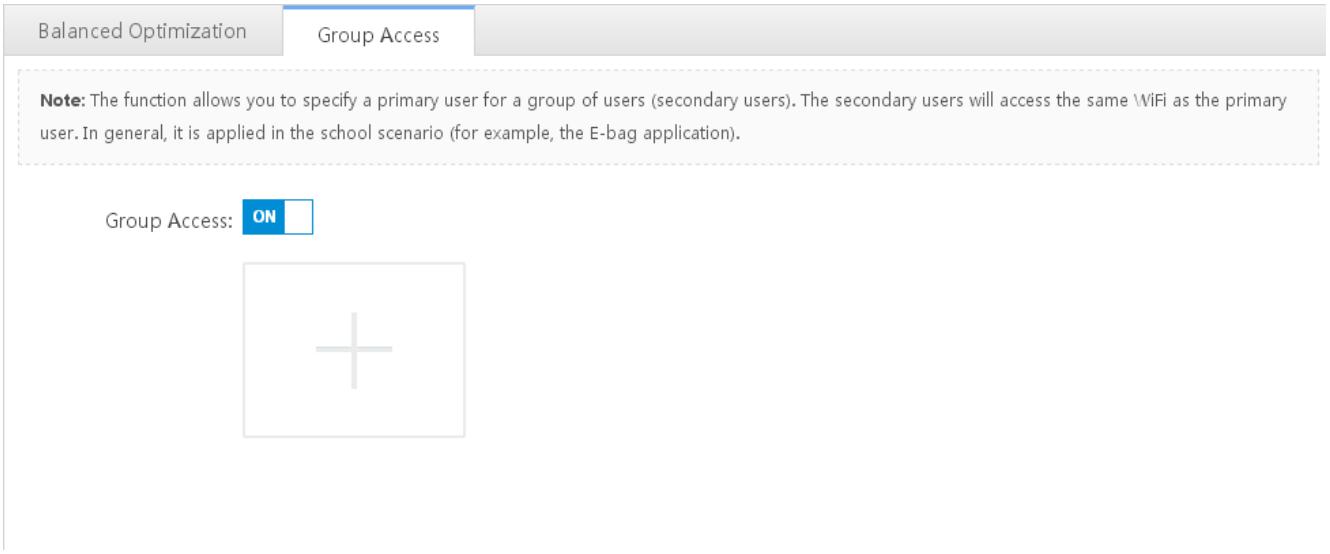
This function is mainly applicable to the E-bag solution for schools. Balanced optimization ensures a smooth network experience and avoids disconnection when a user uses the E-bag application.

Balanced Optimization



It is recommended to enable this function in a multi-user scenario as it may affect performance.

Group Access



Click the 

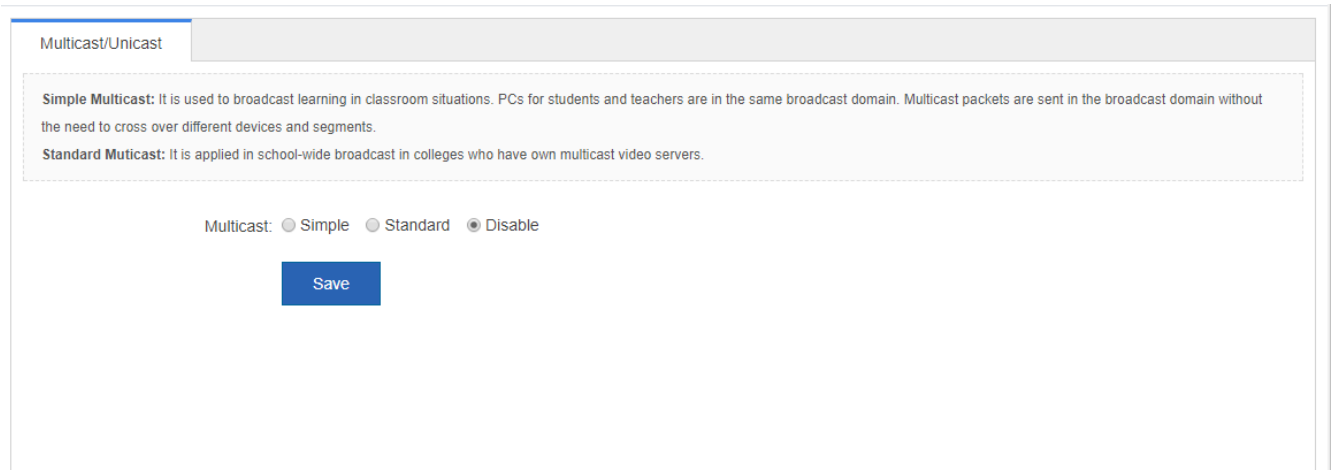
button to enable or disable the Group Access function.

Configure the user binding relationship. Configure bound primary user and secondary user data.

1.3.5.6 Unicast/Multicast

Unicast refers to a one-to-one transmission from one point in the network to another point; that is, one sender and one receiver, each identified by a network address.

Multicast is group communication where information is addressed to a group of destination computers simultaneously. Multicast can be one-to-many or many-to-many distribution. Multicast should not be confused with physical layer point-to-multipoint communication.

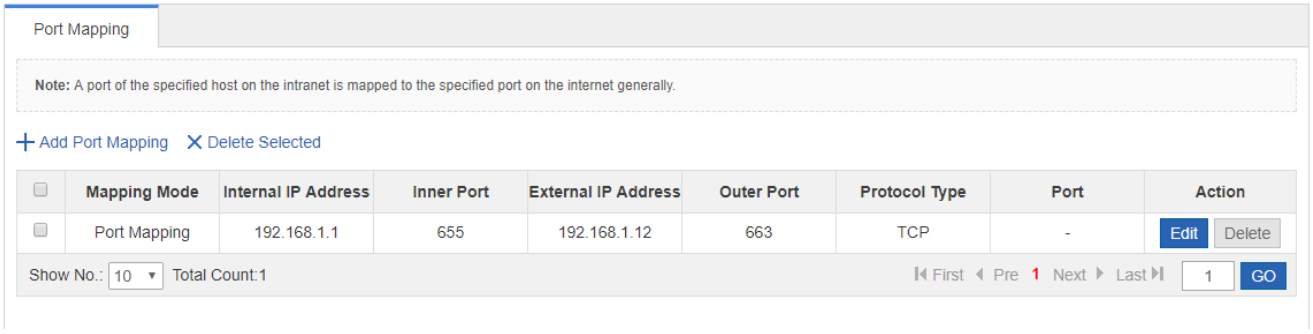


Set parameters as required, and then click **Save**.

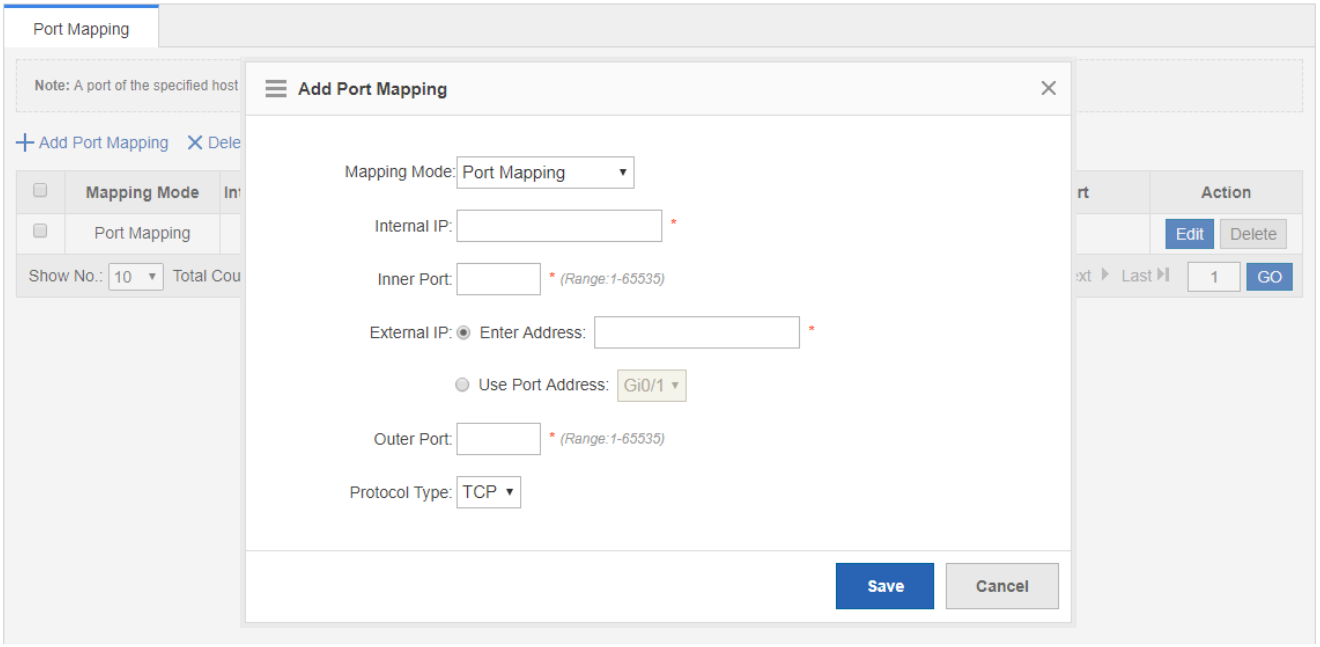
1.3.5.7 Port Mapping

Generally, this function is used to map a specified port of a specified host in the internal network to a specified port of an external network address.

Your AP might not support this function, as it is subject to the actual menu items.

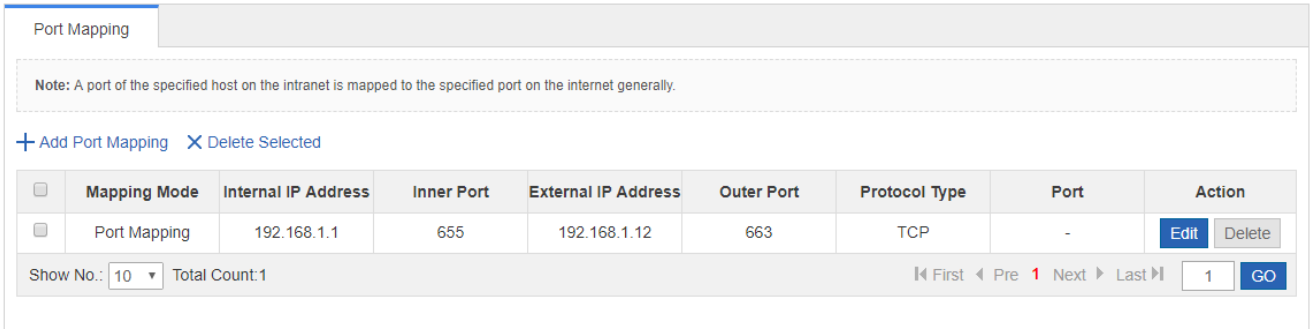


- Adding port mapping



Click **Add Port Mapping**, set the configuration items in the dialog box displayed, and then click **Save**. The newly added port mapping is displayed in the list after the **Save operation succeeded** message is displayed.

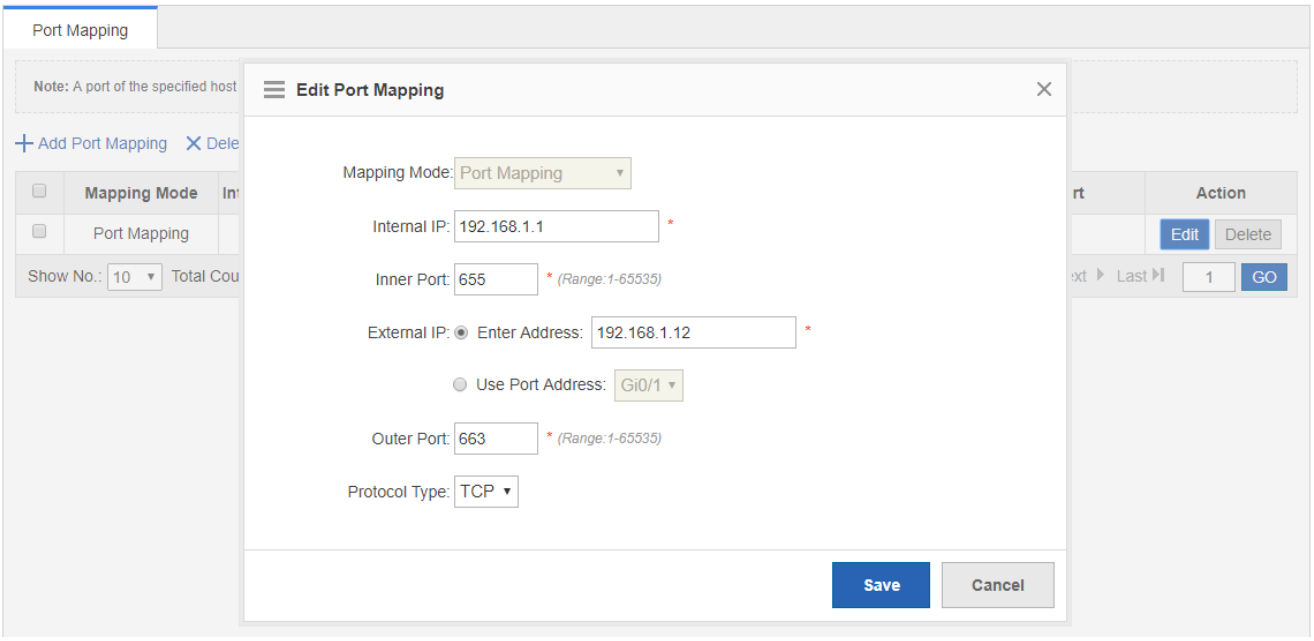
- Batch deleting port mapping entries



1) Select the port mapping from the list.

2) Click **Delete Selected Port Mapping** and then click **OK** in the displayed dialog box to finish deleting.

- Editing port mapping

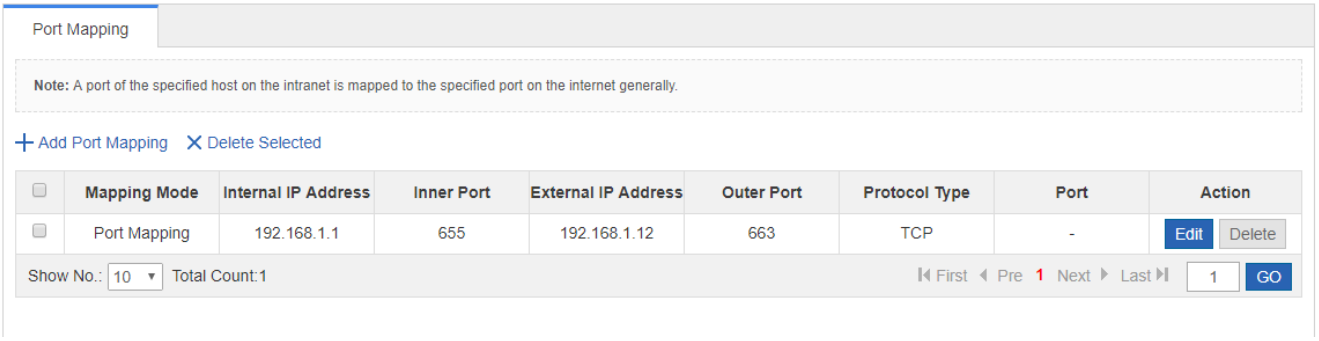


1) Click the **Edit** button for a port mapping in the list.

2) The configuration for port mapping is displayed in the dialog box. Next, edit the configuration.

3) Click **Save**. The **Save operation succeeded** message is displayed.

- Deleting port mapping



Click the **Delete** button for a port mapping entry in the list to finish deleting.

1.3.5.8 CWMP

CPE WAN Management Protocol (CWMP) provides a general framework of unified device management, related message specifications, management methods, and data models, so as to solve difficulties in unified management and maintenance of dispersed customer-premises equipment (CPEs), improve troubleshooting efficiency, and save O&M costs.

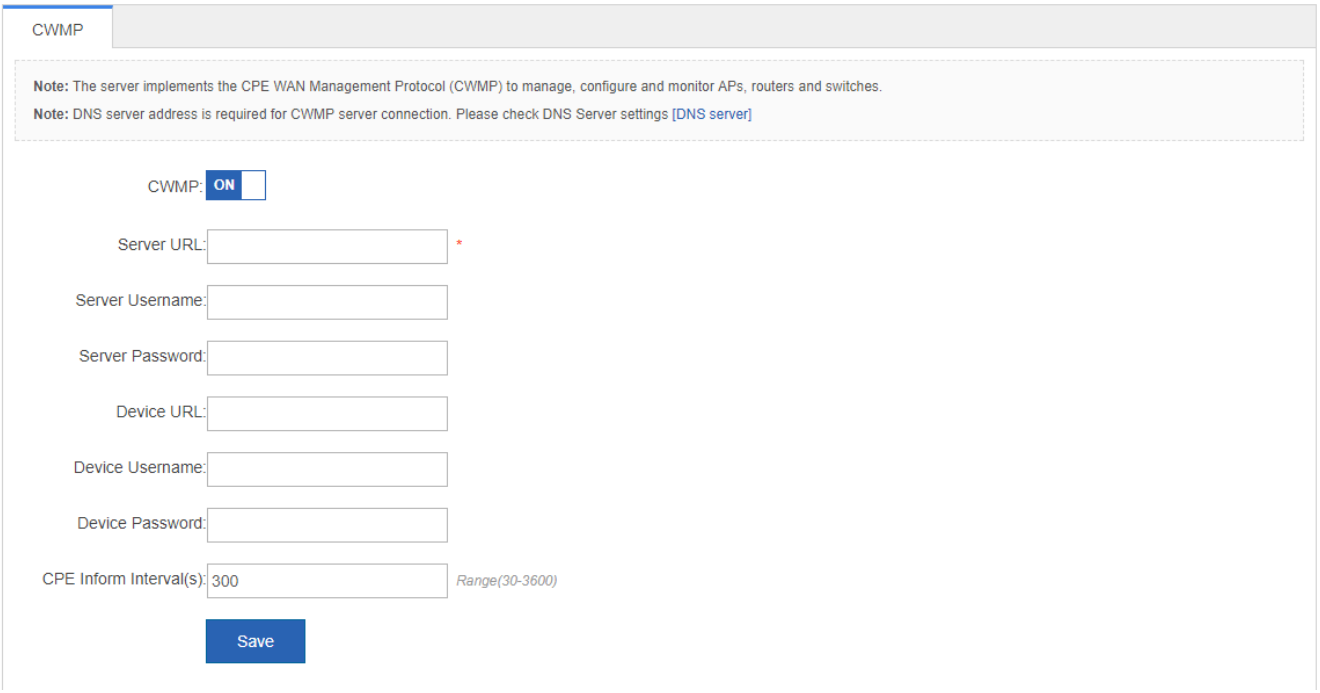
- **CPE**: Customer Premises Equipment
- **ACS**: Auto-Configuration Server

- **RPC**: Remote Procedure Call
- **DM**: Data Model

For details about TR069 protocol specifications, visit http://www.broadband-forum.org/technical/trlist.php.

The server implements the CPE WAN Management Protocol (CWMP) to manage, configure and monitor APs, routers and switches.

If CWMP is not displayed in the menu, this function is not supported.

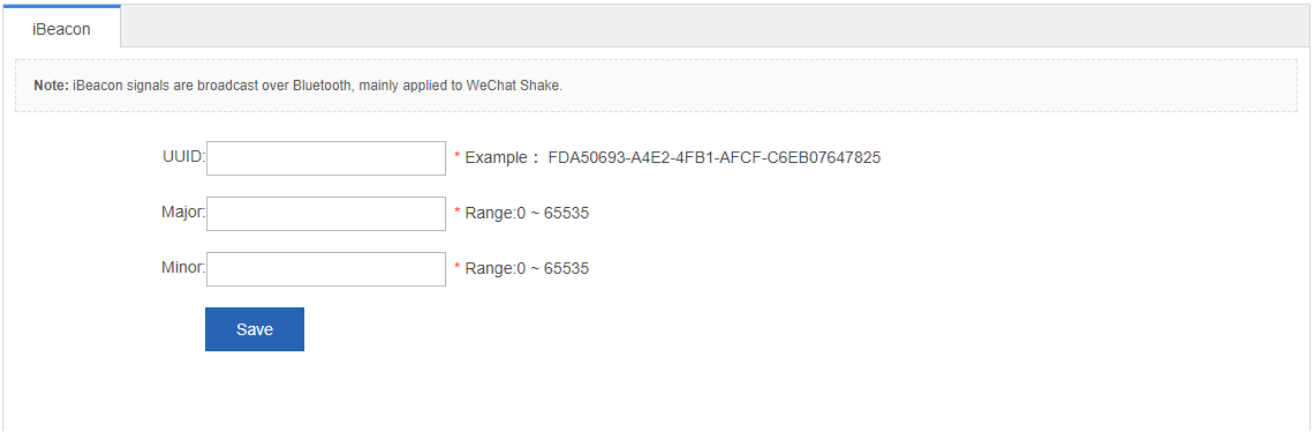


1.3.5.9 iBeacon

iBeacon uses Bluetooth low energy proximity sensing to transmit a universally unique identifier picked up by a compatible app or operating system. The identifier and several bytes sent with it can be used to determine the device's physical location, track customers, or trigger a location-based action on the device such as a check-in on social media or a push notification.

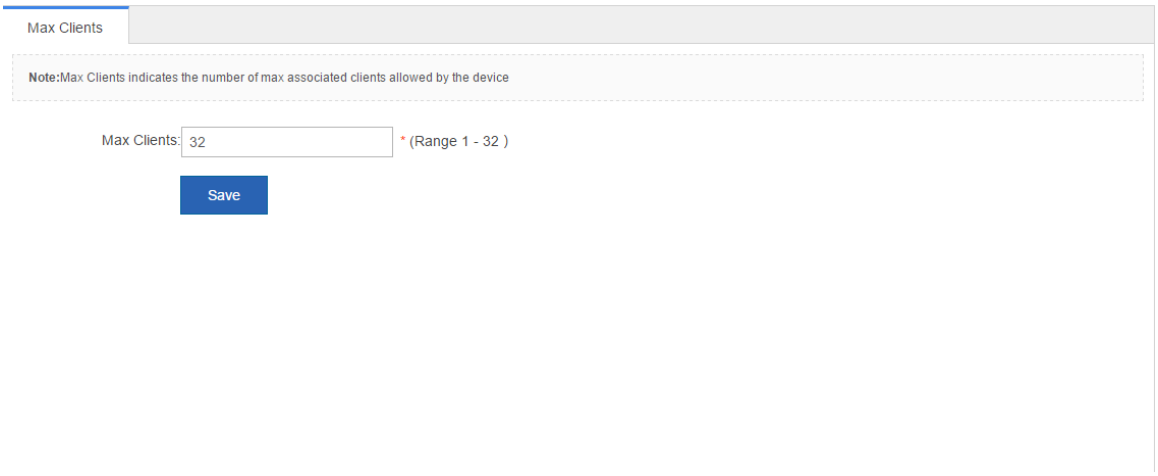
iBeacon signals are broadcast over Bluetooth, and mainly applied to WeChat Shake.

If iBeacon is not displayed in the menu, this function is not supported.



1.3.5.10 Max Clients

It is used to configure the maximum number of associated STAs.



1.3.6 System

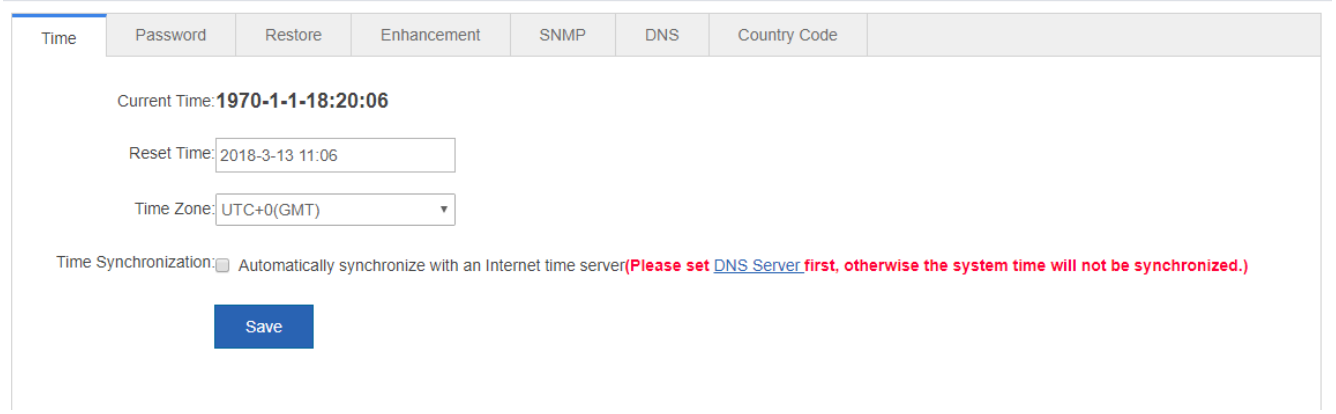
1.3.6.1 System Settings

Time

The network device system clock records the time of events on the device. For example, the time shown in system logs is obtained from the system clock. Time is recorded in the format of *year-month-day, hour:minute:second*, day of the week.

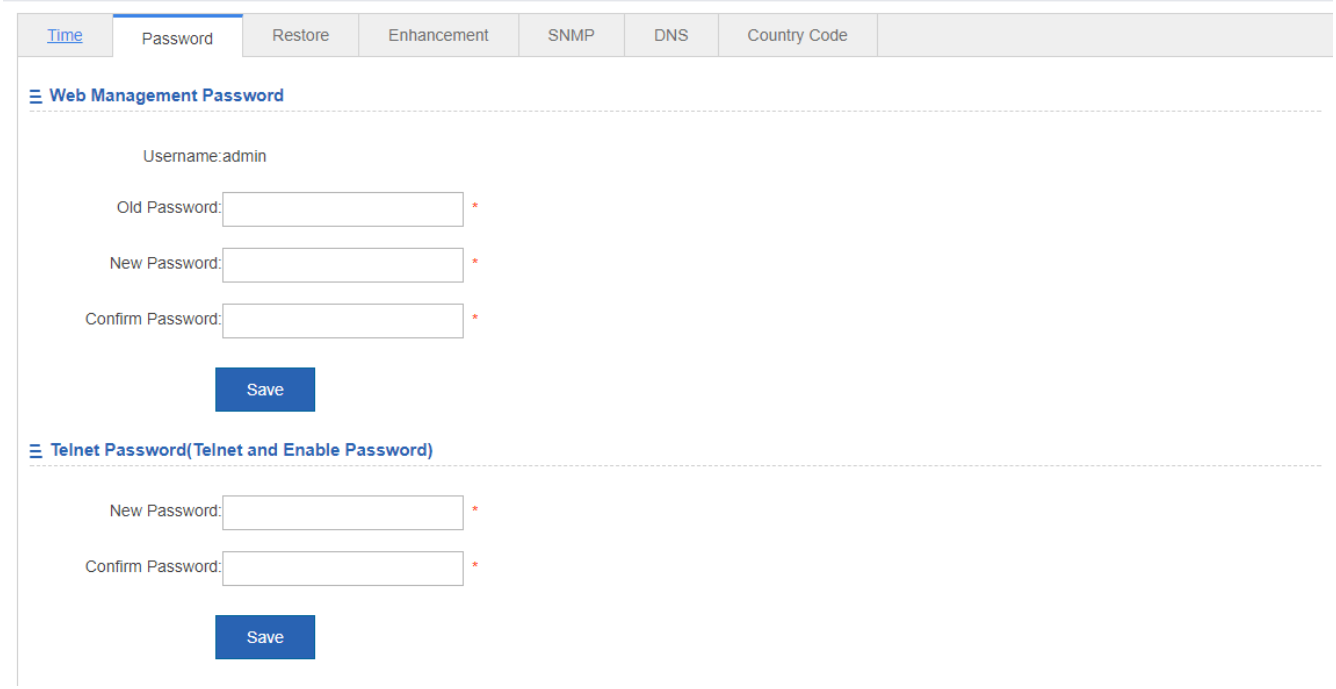
When you use a network device for the first time, set its system clock to the current date and time manually.

Set the system time based on the region for the device.



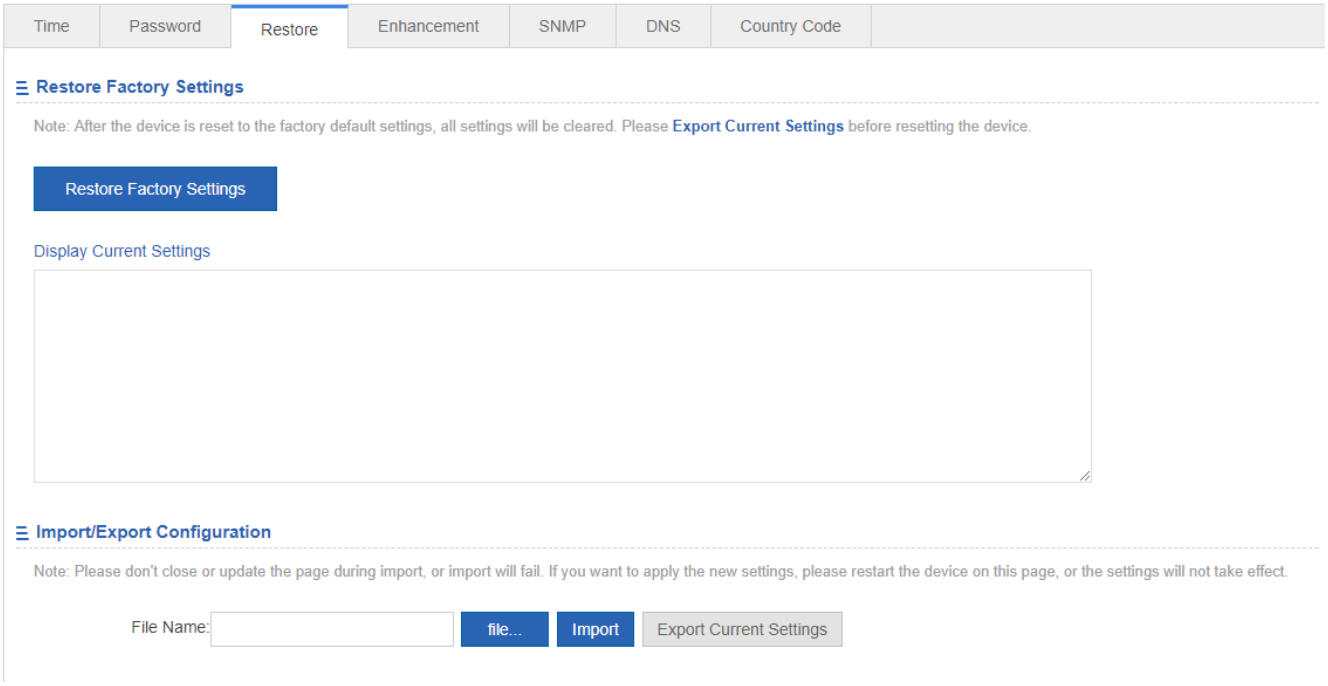
Password

To improve security for information exchanges, please change the system default password.



Restore

Restore configurations to the factory settings. The configuration can be imported and exported in batches, facilitating user operation.



After selecting a configuration file, click **Import** to import this configuration file.

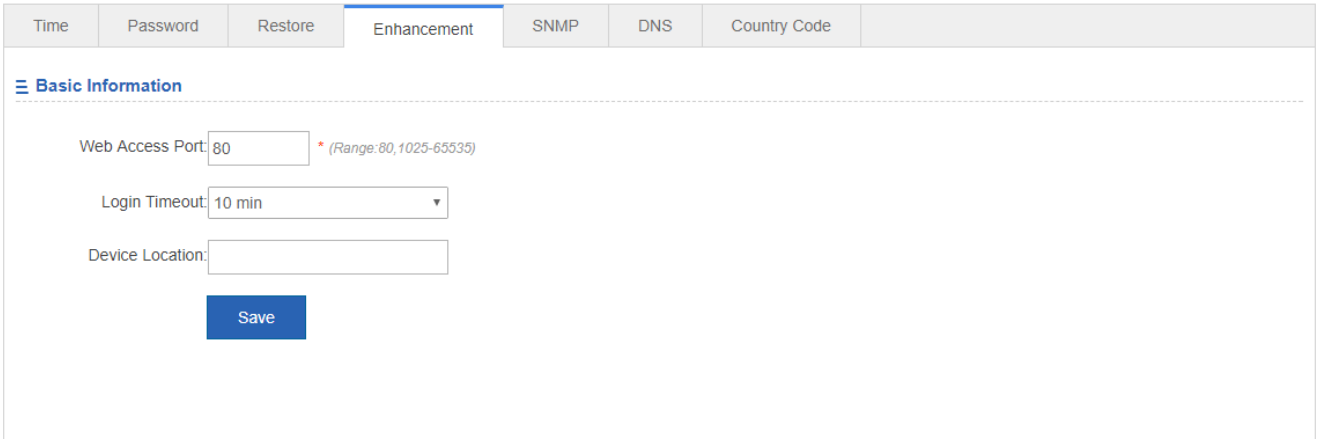
Click **Export Current Configuration** to download the latest configuration file.

Click **Restore Factory Settings** to clear the configurations and restore to the initial state.

You can click the **Display Current Configuration** button to view the configurations in the box below this button.

Enhancement

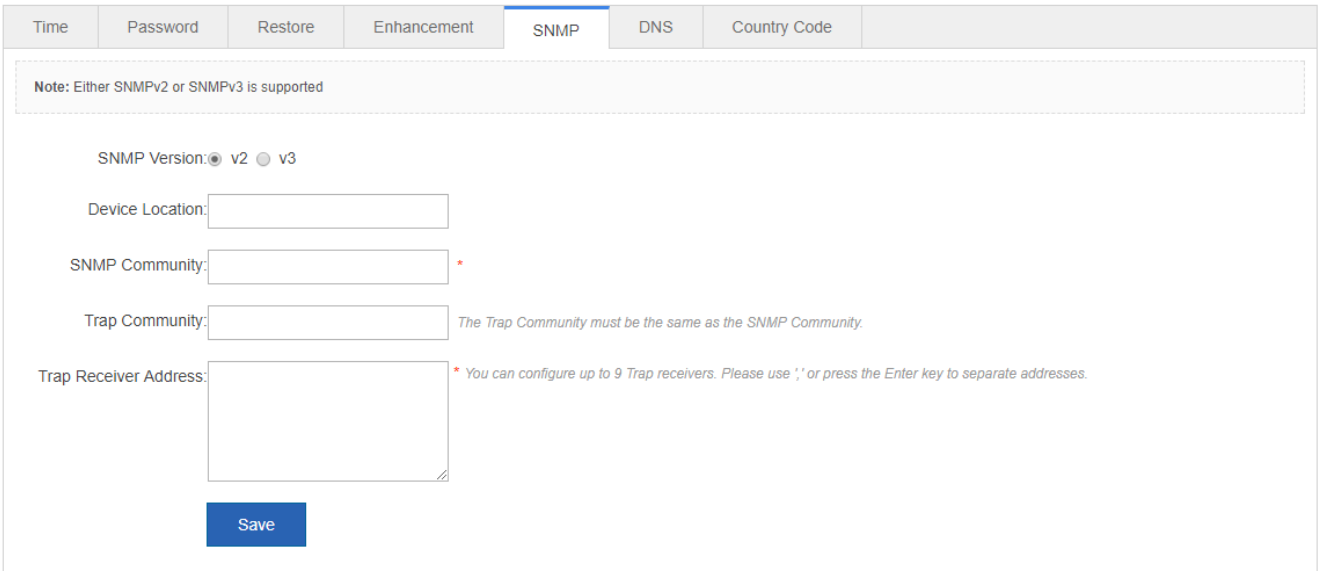
To facilitate device management, set **Device Location** for better device examination. After **Login Timeout** is set, the Web system logs out automatically when you leave for a long time, ensuring system security.



SNMP

The Simple Network Management Protocol (SNMP) is by far the dominant protocol in network management. This Protocol (SNMP) was designed to be an easily implementable, basic network management tool that could be used to meet network

management needs. It is named Simple Network Management Protocol as it is really easy to understand. A key reason for its widespread acceptance, besides being the chief Internet standard for network management, is its relative simplicity. There are different versions of SNMP, such as SNMP V1, SNMP V2c, and SNMP V3.



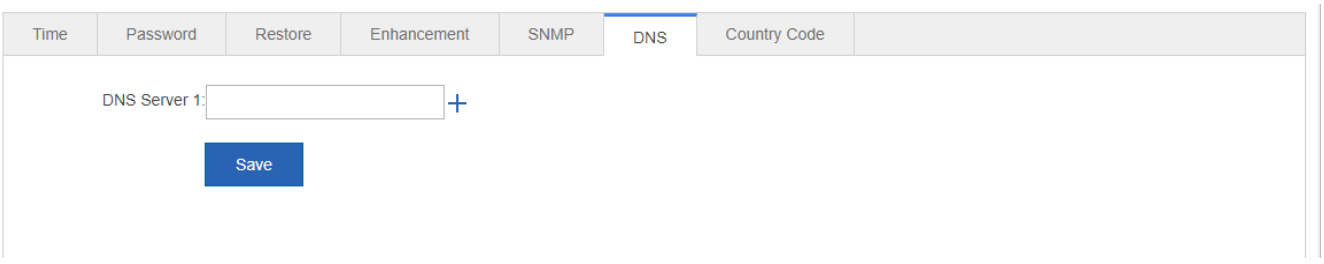
Set the configuration items, and click **Save**.

DNS

A Domain Name System (DNS) is a distributed database containing mappings between domain names and IP addresses on the Internet, which facilitate users to access the Internet without remembering IP strings that can be directly accessed by computers. The process of obtaining an IP address through the corresponding host name is called domain name resolution (or host name resolution).

DNS consists of a resolver and a DNS server. The DNS server stores the mappings between domain names and IP addresses of all hosts on the network, and implements mutual conversion between the domain names and IP addresses. Both the TCP and UDP port IDs of DNS are 53, and generally a UDP port is used.

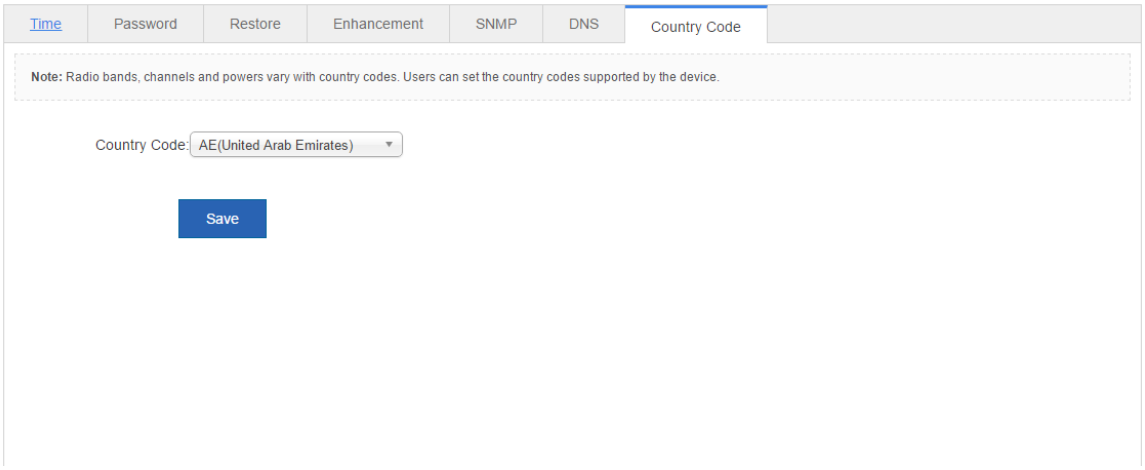
Dynamic domain name resolution (DNS) can be enabled only after the DNS server is configured.



Click + to add a DNS server.

Click × to delete a DNS server.

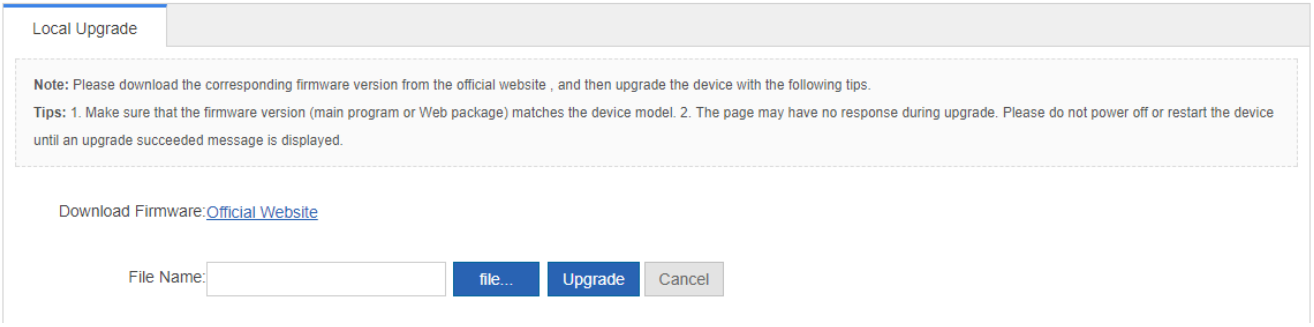
Country Code



1.3.6.2 Upgrade

Local Upgrade

Download the main program or Web package to the local device and perform local upgrade.



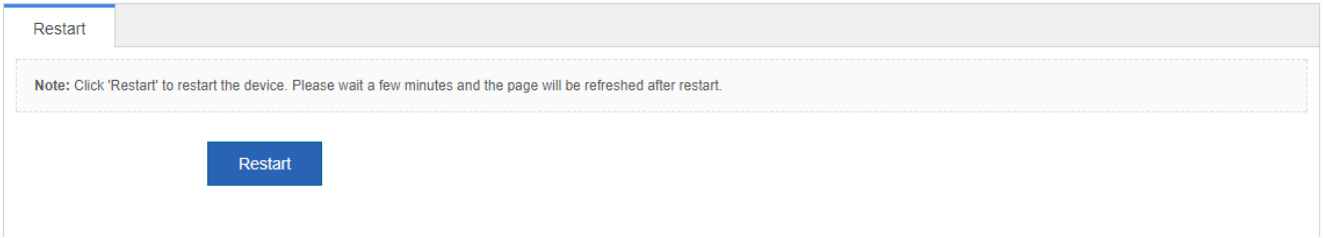
Click to select the main program or Web package to be upgraded.

You can click **Cancel** to terminate an ongoing upgrade.

Click the **DNS Server** and **Route** links to check network connection.

1.3.6.3 Restart

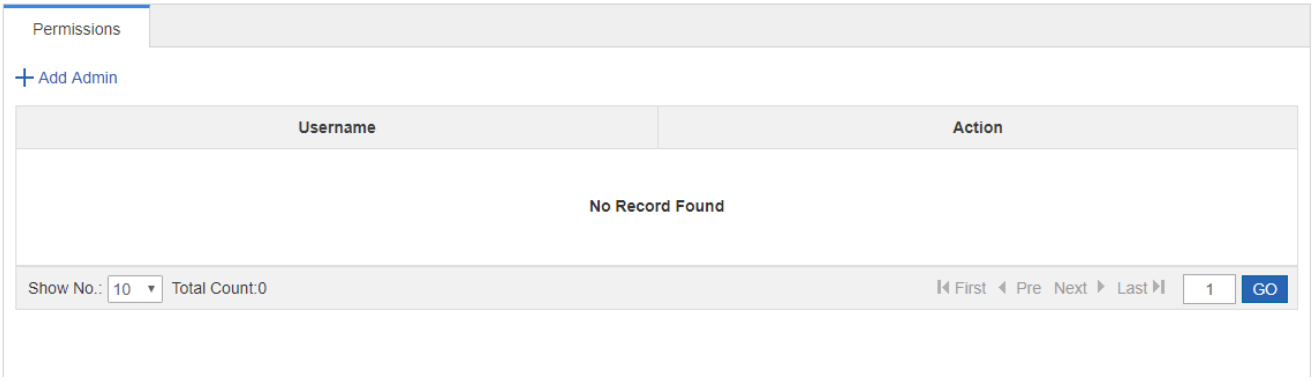
Conveniently restart the system with a click.



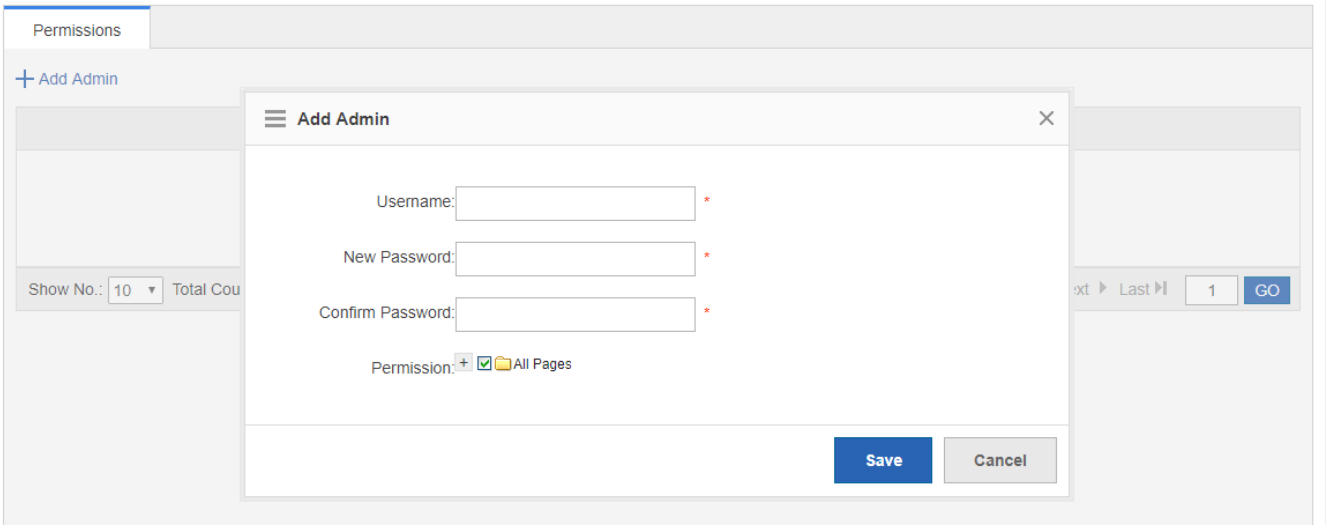
Click **Restart** to restart the device.

1.3.6.4 Permission

A system may have multiple users of different levels that correspond to different permissions. You can set or view permissions through the **Permission Settings** page. The system has two default users: user **admin**

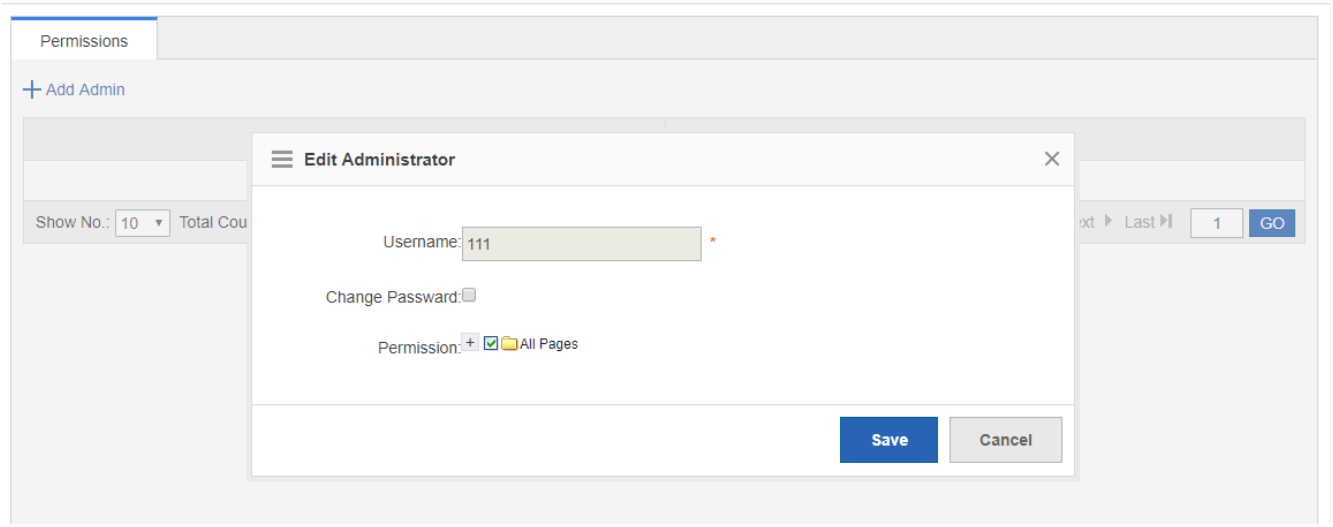


- Adding an administrator



Click **Add Administrator**. A dialog box is displayed, as shown in the preceding figure. Set the configuration items in the dialog box, and click **Save**. The newly added administrator is displayed in the list after the **Save succeeded** message is displayed.

- Editing administrator information

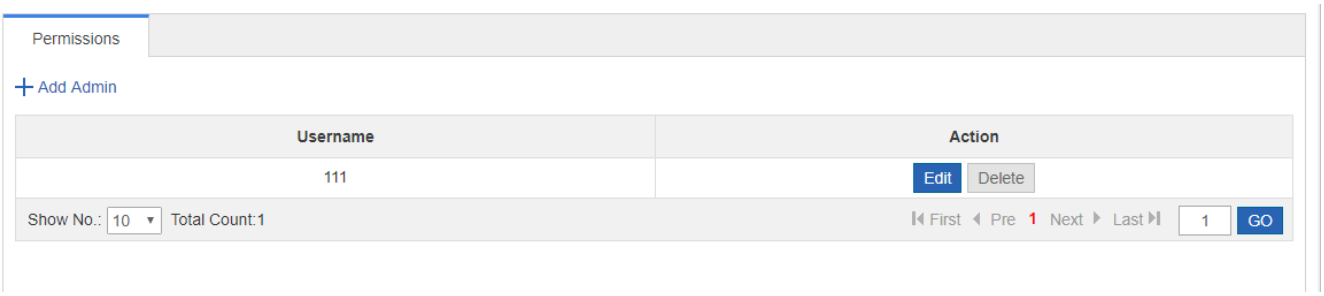


1) Click the **Edit** button for an administrator in the list.

2) A dialog box is displayed, as shown in the preceding figure. The configuration about the administrator is displayed in the dialog box. Then edit the configuration.

3) Click **Save**. The **Save operation succeeded** message is displayed.

- Deleting an administrator

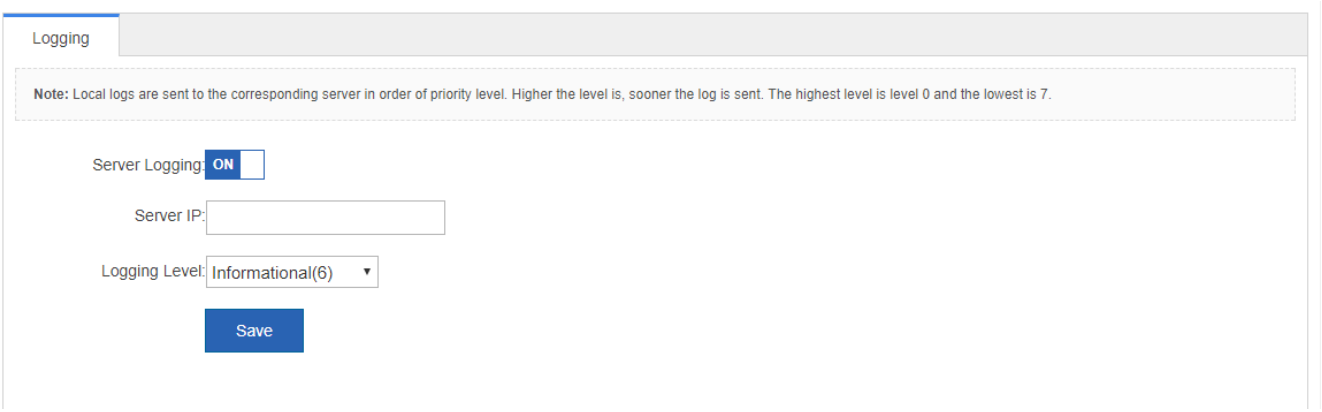


Click **Delete** to delete an administrator.

1.3.6.5 Logging

Status changes (such as link up and down) or abnormal events may occur anytime. Ruijie products provide the syslog mechanism to automatically generate messages (log packets) in fixed format upon status changes or occurrence of events. These messages are displayed on the related windows such as the Console or monitoring terminal, recorded on media such as the memory buffer or log files, or sent to a group of log servers on the network so that the administrator can analyze network performance and identify faults based on these log packets. Log packets can be added with the timestamps and sequence numbers and classified by severity level so that the administrator can conveniently read and manage log packets.

Local logs on the device are sent to a corresponding server for storage to facilitate access to these logs.

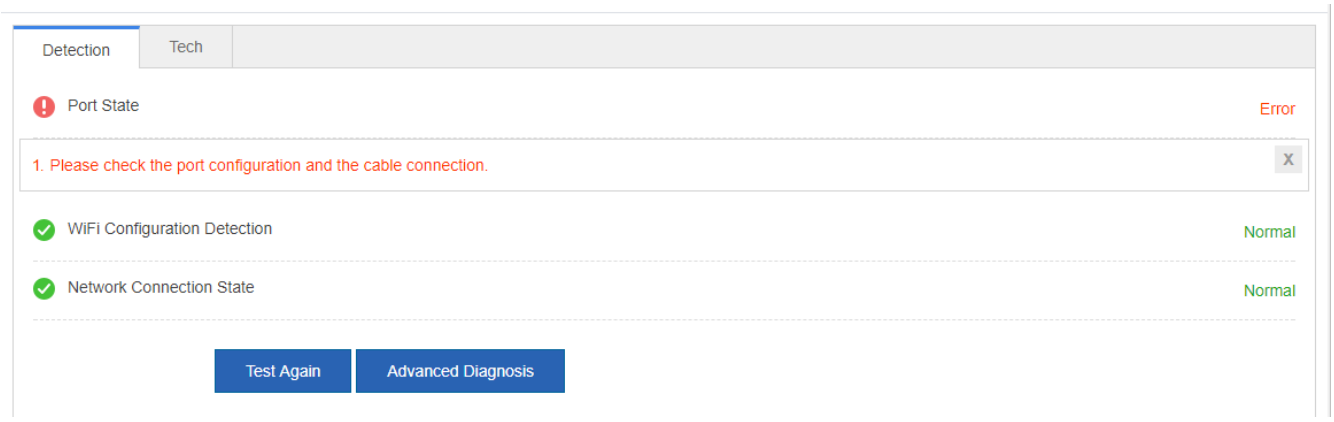


Click  to enable or disable the server logging function.

1.3.6.6 Detection Tools

The ping tool sends an Internet Control Message Protocol (ICMP) Request message to the destination host to request the for an ICMP Echo Reply message. In this way, the ping tool determines the delay and the connectivity between the two network devices.

When the network is faulty, network connections can be detected for troubleshooting.

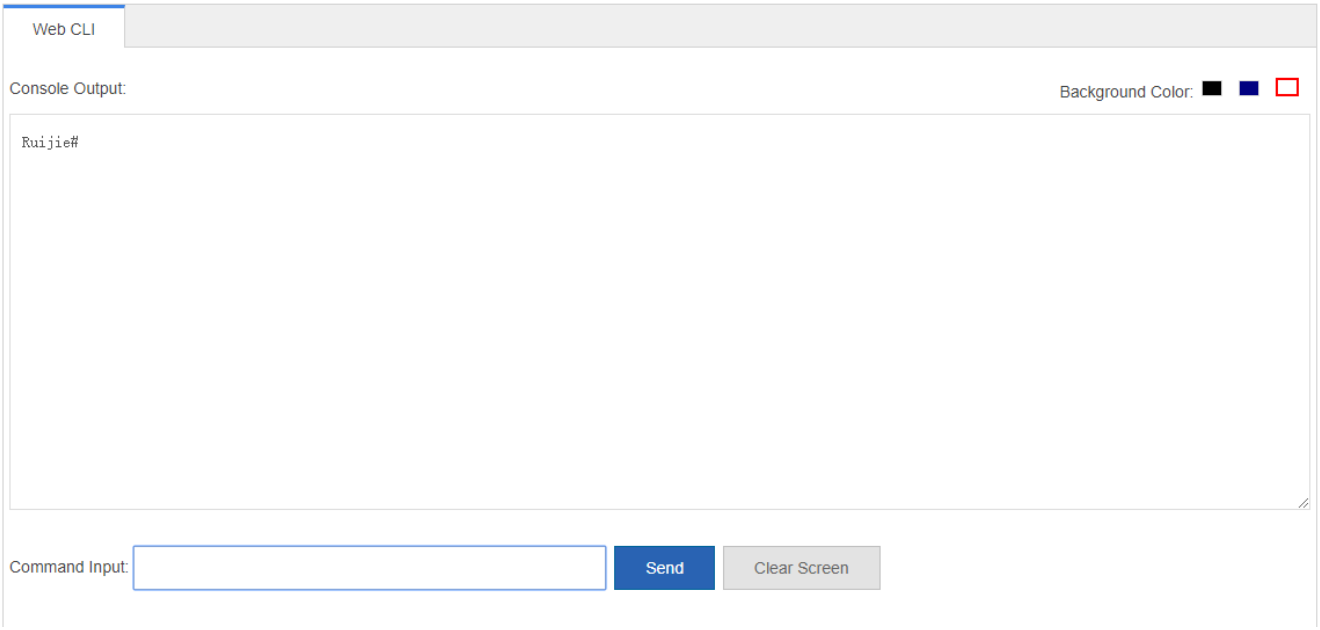


When an AP is faulty, click the **Route** link to view and configure relevant information.

Click the **Advanced Diagnosis** button to detect network connection.

1.3.6.7 Web Console

You can configure any command on the Web Console as in the Telnet operation. But you cannot log in to an AP using Telnet or entering any command in Shell mode.



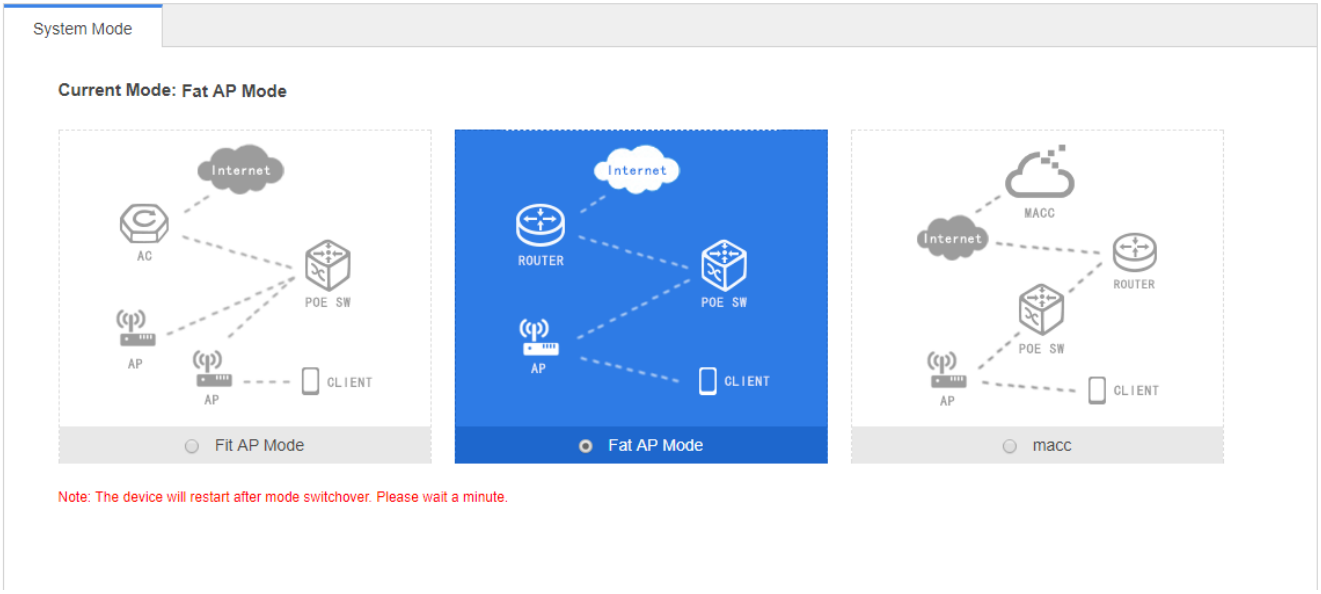
1.3.6.8 System Mode

Two types of APs are available: Fat Access Points and Fit Access Points.

A FAT AP is suitable for family and small-scaled networks and provides full features. Generally, one device can implement access, authentication, routing, VPN, address translation, and even the firewall functions.

A FIT AP is suitable for large-scale wireless network deployment. A dedicated wireless controller is needed to provide unified management. A FIT-AP can be used only after the wireless controller delivers configurations and it cannot complete configuration by itself.

Select the AP mode.



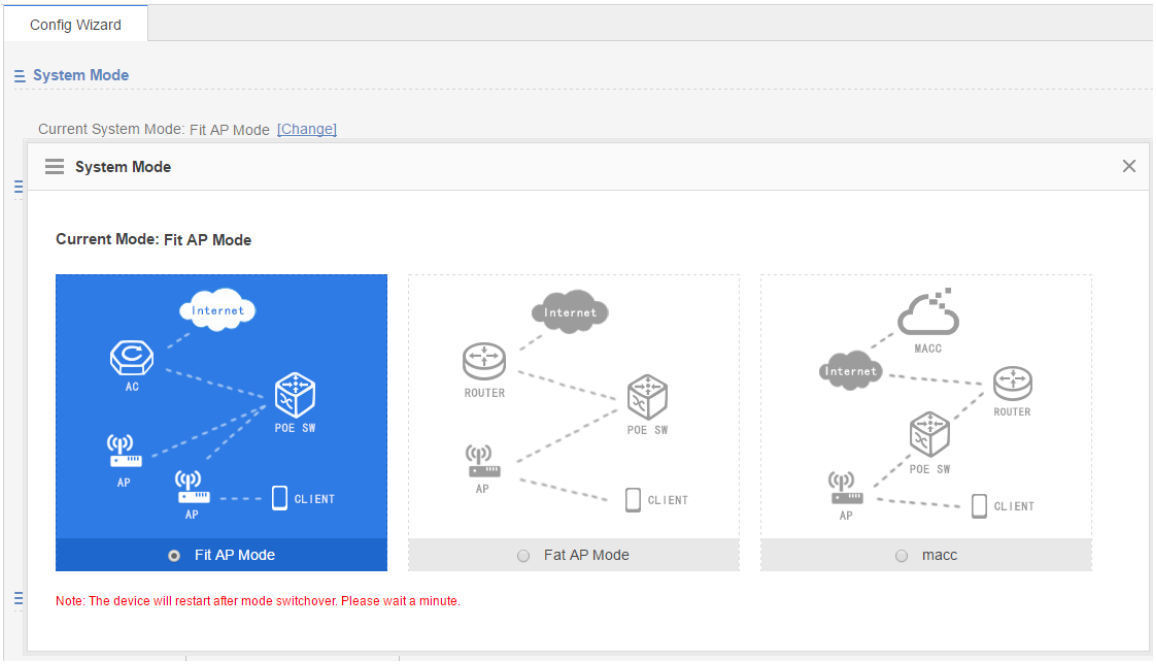
1.4 Fit AP-Eweb

1.4.1 SmartAP

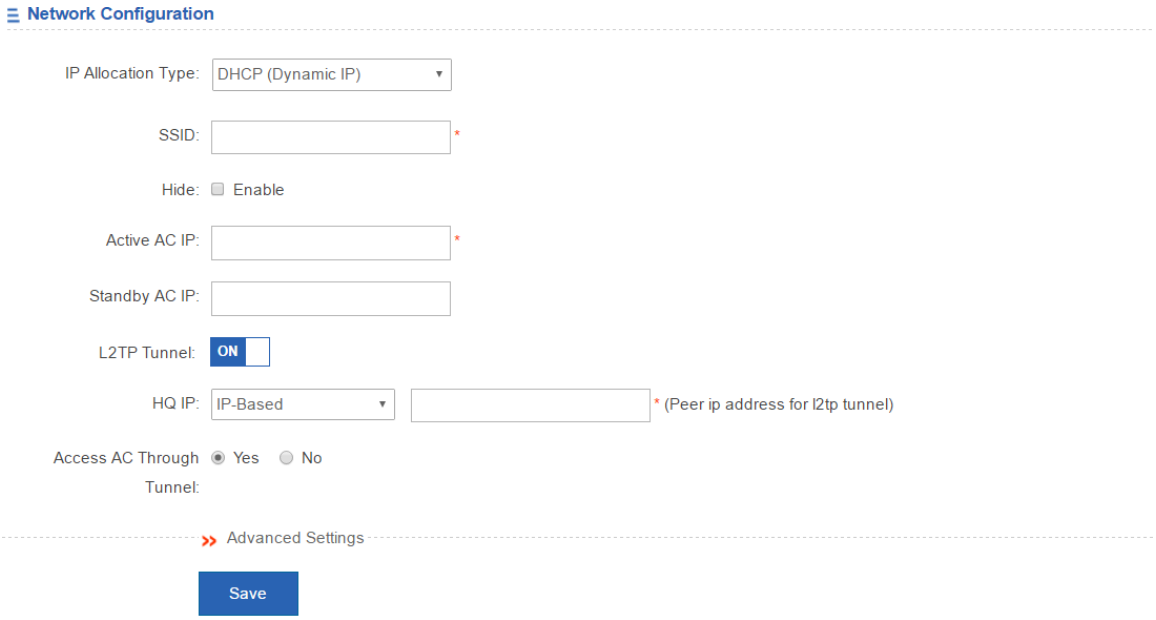
SmartAP allows you to deploy APs in mobile office scenario. Click **Config Wizard** to end the SmartAP configuration page, including **System Mode**, **Network Configuration** and **Change Web NMS Password**.

1. **System Mode**

Click **Change** and the **System Mode** window is displayed. You can select a mode among three modes available: Fit AP, Fat AP and MACC.



2. Network Configuration



3. Change Web NMS Password

1.5 Enabling the Web Server

The Web service is enabled for an AP device when this AP is delivered. By default, the IP address is 192.168.110.1. The following describes how to enable Web service on the CLI when it is disabled.

Configuration	Commands	
Configuring the Web server	**enable service web-server**	Enables the Web service.
	ip address	(Optional) Configures the IP address.
	webmaster level username password	(Optional) Configures the username and password for logging in to the Web-based management system.

Configuration Method

Enabling the Web Service

- Mandatory configuration.
- This configuration is performed on the AP device.

Configuring the IP Address

- Optional configuration.

Configuring the Username and Password for Logging in to the Web-Based Management System

- Optional configuration.
- When the Web service is enabled, the administrator username/passwords (admin/admin) and guest user/passwords (guest/guest) are created by default. The passwords of these two accounts can be changed. In addition, you can create other Web-based management accounts.

Verification

Log in to the Web page by using the preset IP address and Web-based management account and password, then check whether the login is successful.

Relevant Commands

Enabling the Web Service

Command	**enable service web-server** [**http** | **https** | **all**]
Parameter Description	**http | https | all**: Enables corresponding services. **http** enables the HTTP service, **https** enables the HTTPS service, and **all** enables both the HTTP and HTTPS services. By default, both the HTTP and HTTPS services are enabled.
Command Mode	Global configuration mode.

Configuring the IP Address

Command	**ip address** *ip-address ip-mask*
Parameter Description	*ip-addres*s: IP address. *ip-mask*: network mask.
Command Mode	Interface configuration mode.

Configuring the Account and Password for Logging in to the Web-Based Management System

Command	**webmaster level** *privilege-level* **username** *name* **password** { *password* | [**0 | 7**] *encrypted-password*
Parameter Description	*privilege-level*: indicates the level of the permission bound to the user. Three levels are available, which are 0, 1, and 2. The super administrator account (admin) created by default corresponds to level 0, a guest account (guest) corresponds to level 2, and other accounts correspond to level 1. *name*: address of the static RP. *password*: The ACL is used to limit the group address range of the static RP service. The default range is all group services. **0 | 7**: password encryption type. **0** indicates no encryption, and **7** indicates simple encryption. The default value is 0. *encrypted-password*: password.
Command Mode	Global configuration mode.
Usage Guide	N/A

Configuration Example

Configuring the Web Server

Configuration Steps	Enable the Web service. Configure the local username and password. Configure the device management IP address. The default management VLAN is VLAN 1. Configure an IP address for VLAN 1. Ensure that the management IP address can be pinged from the user's PC.

	`Ruijie# configure terminal`
	`Ruijie(config)# enable service web-server`
	`Ruijie(config)# webmaster level 0 username admin password admin`

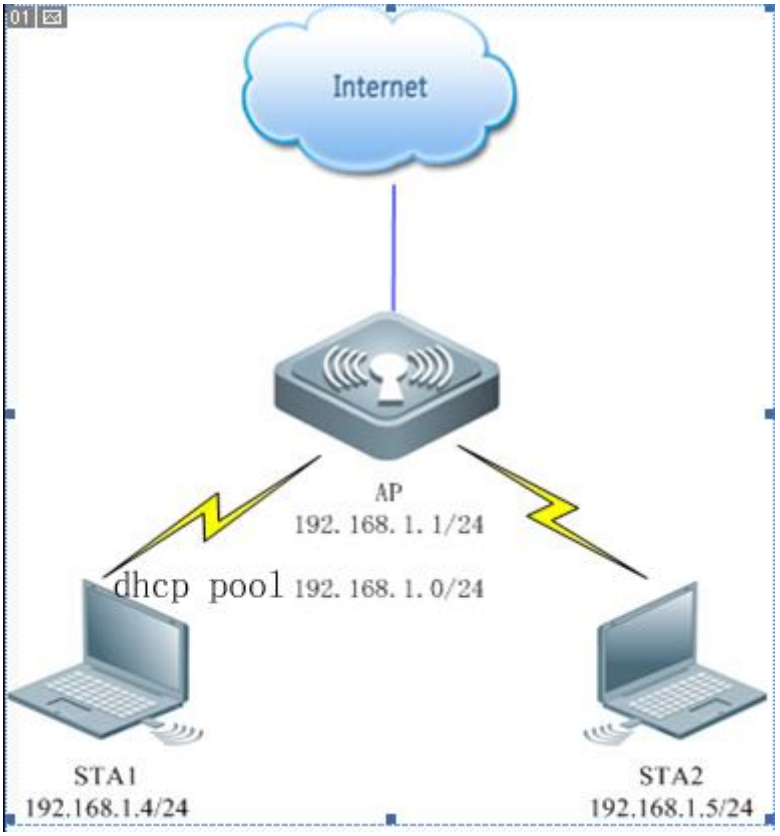
	Ruijie(config)#interface vlan 1 Ruijie(config-if-VLAN 1)#ip address 192.168.1.200 255.255.255.0 Ruijie(config)# end
Verification	Run the **show running-config** command to display related configuration commands.
	Ruijie(config)#show running-config Building configuration... Current configuration : 6312 bytes ! hostname ruijie ! ! webmaster level 0 username admin password 7 08022b181b29 webmaster level 1 username manager password 7 06073f webmaster level 2 username guest password 7 14155f083206 http update mode auto-detect ! ! interface VLAN 1 ip address 192.168.1.200 255.255.255.0 no shutdown ! line con 0 line vty 0 4 login ! ! End

1.6 Configuration Examples

1.6.1 Constructing a WLAN for the DHCP Server on the AP Device

The AP is regarded as a wireless router and constructs a small-scale network as a fat AP. The DHCP server is configured on the AP device. The following figure shows the topology.

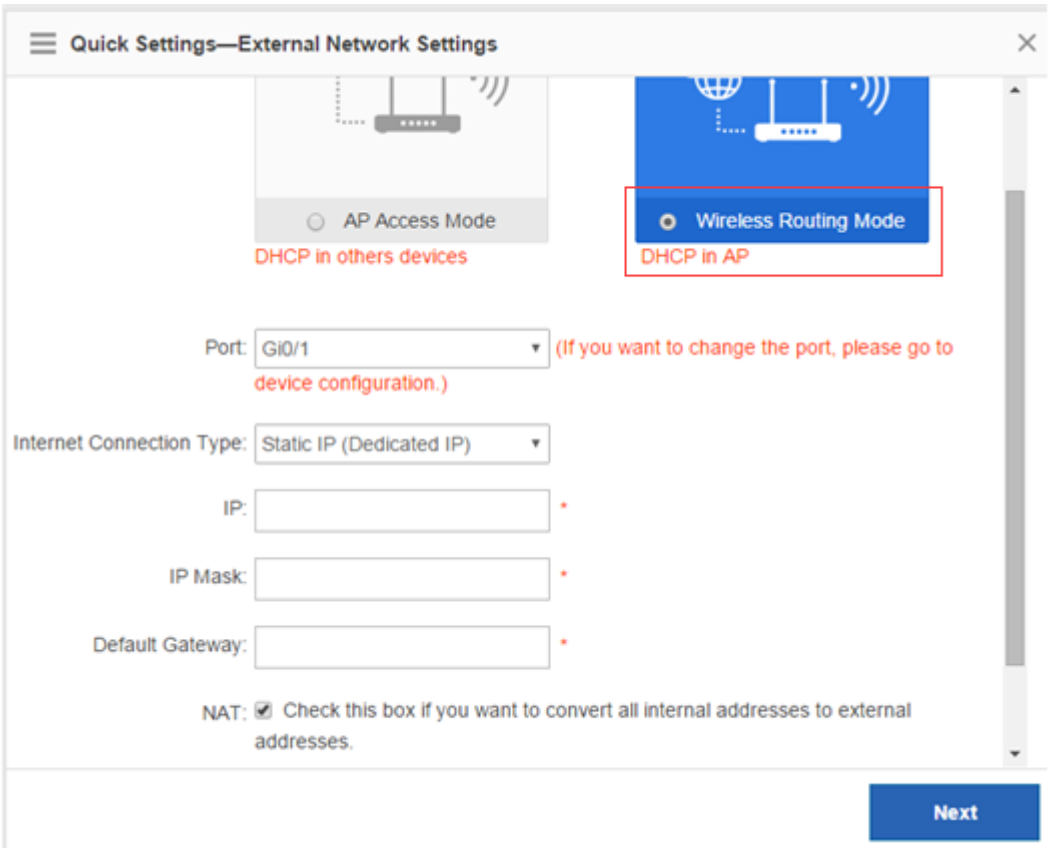
Figure 1-3 Topology 1 (AP is in routing mode)



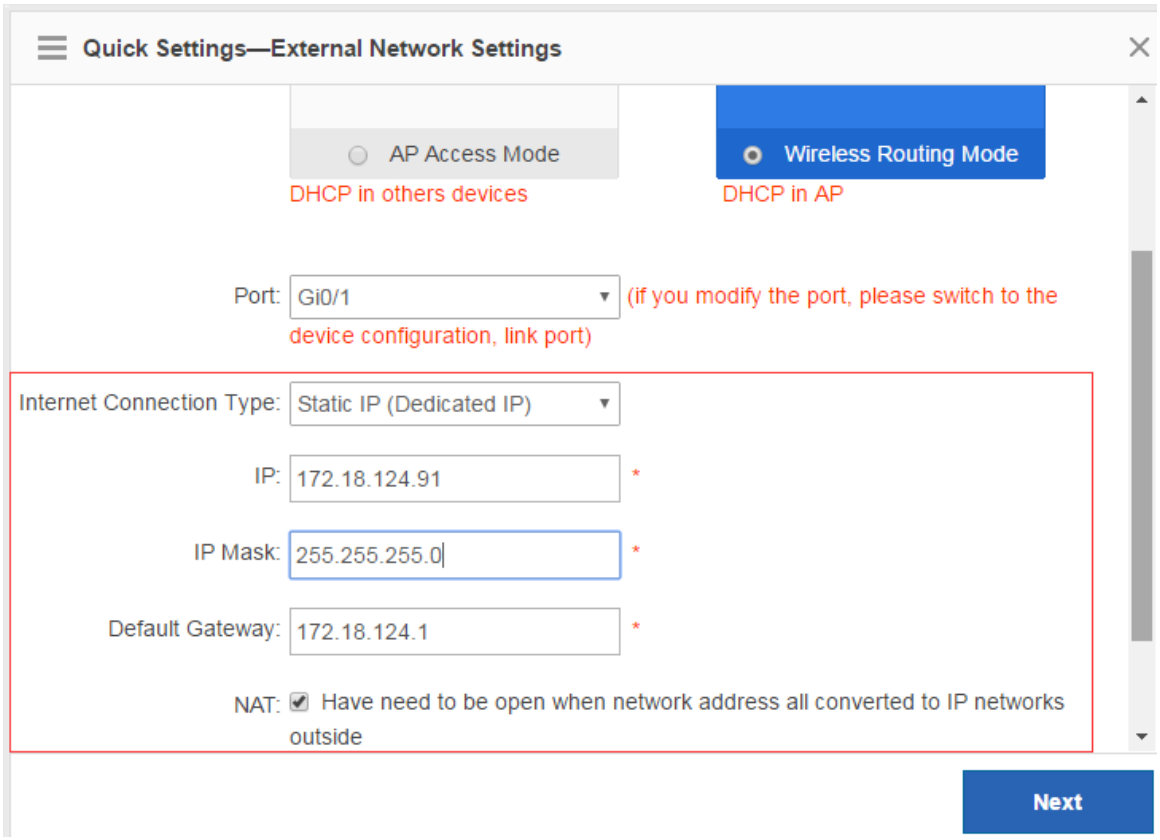
Configuration	Description and Command	
Construction of a WLAN for the DHCP server on the AP	Mandatory. It is used to configure a WLAN.	
	WiFi name	Associates internet access wireless signals for an STA
	WiFi password	An STA inputs the password for internet access.
	DHCP configuration	Allocates IP addresses to wireless STAs.

Verification

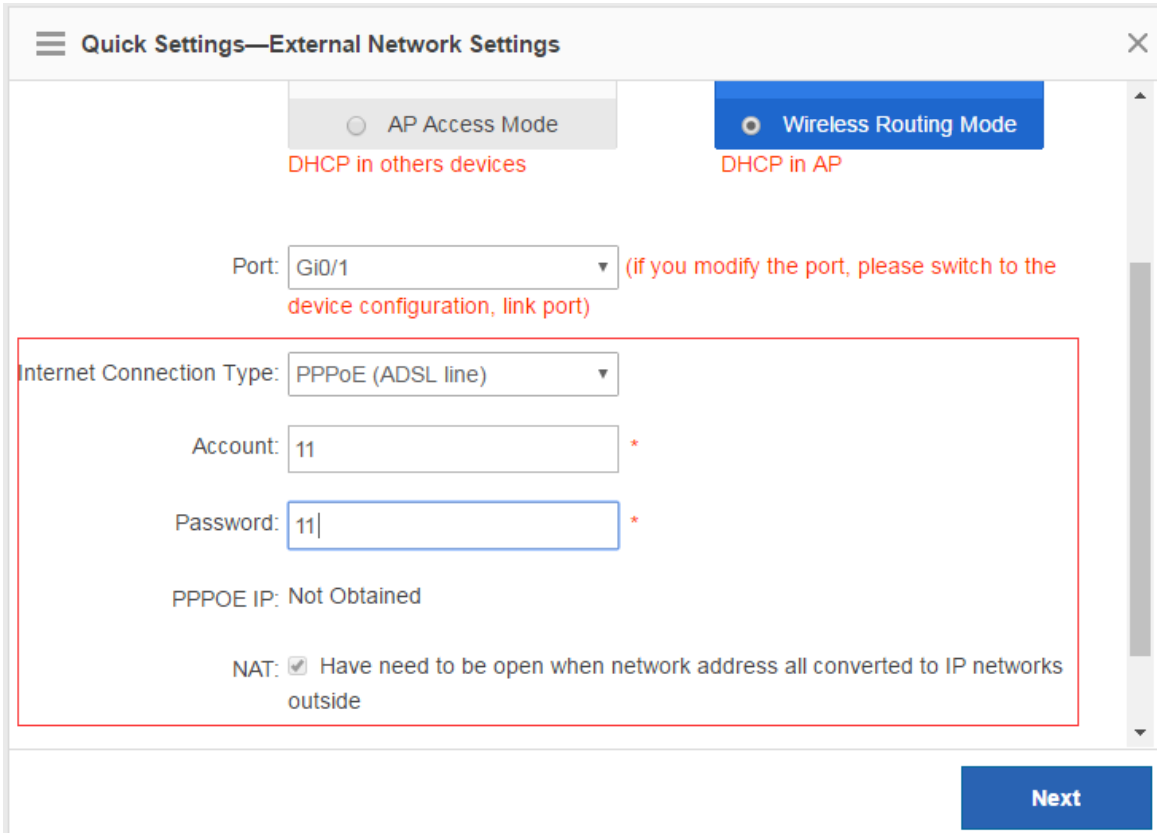
Select AP working mode and set the Internet connection type



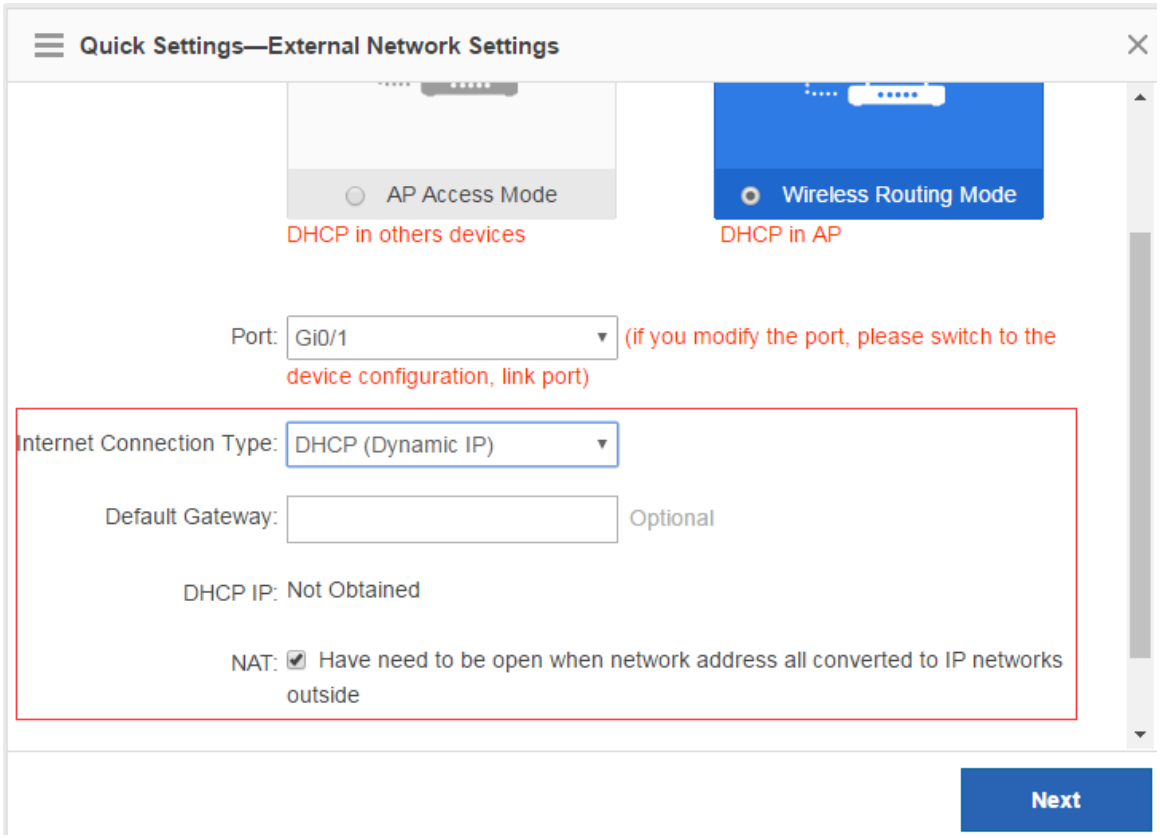
- The AP works in wireless routing mode.
- You can select the following Internet connection types when the AP works in wireless routing mode.
- Static IP (dedicated IP)



- PPPoE (ADSL line)

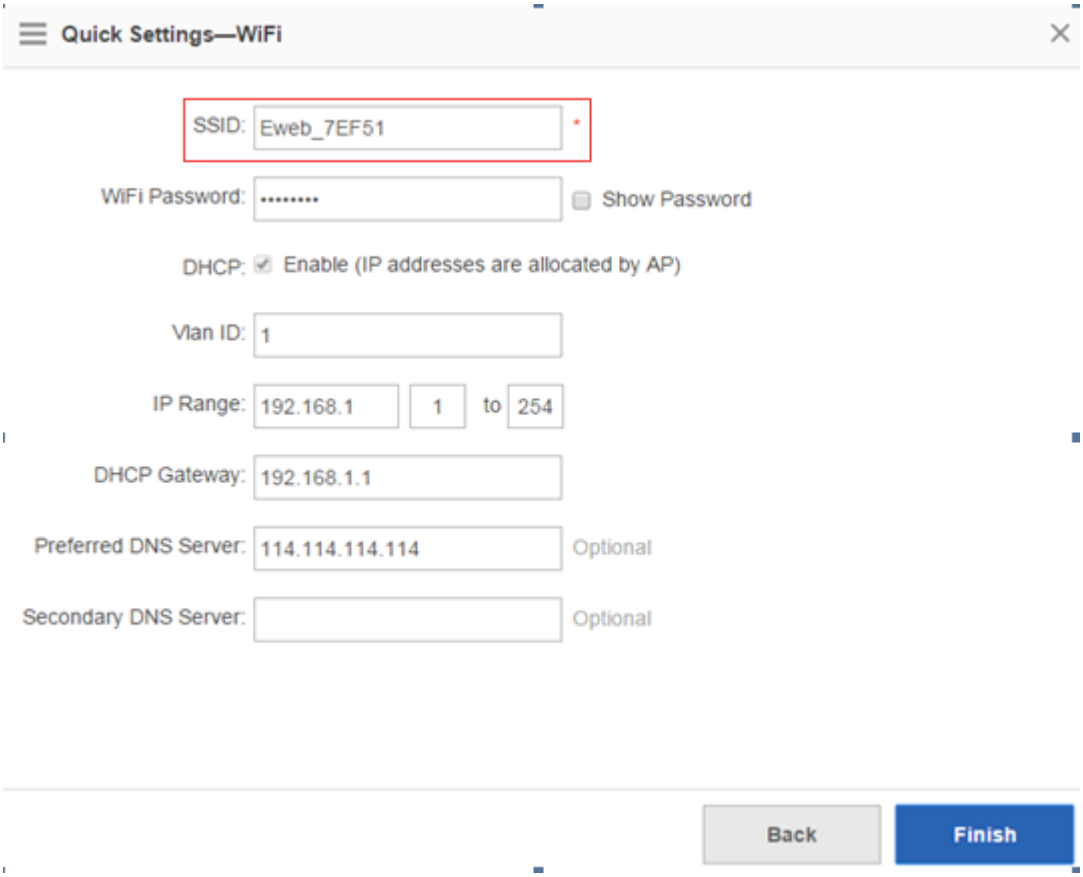


- DHCP (dynamic IP)



Configure a WiFi name (use a simple name that is easy to remember). A WiFi name contains up to 32 characters.

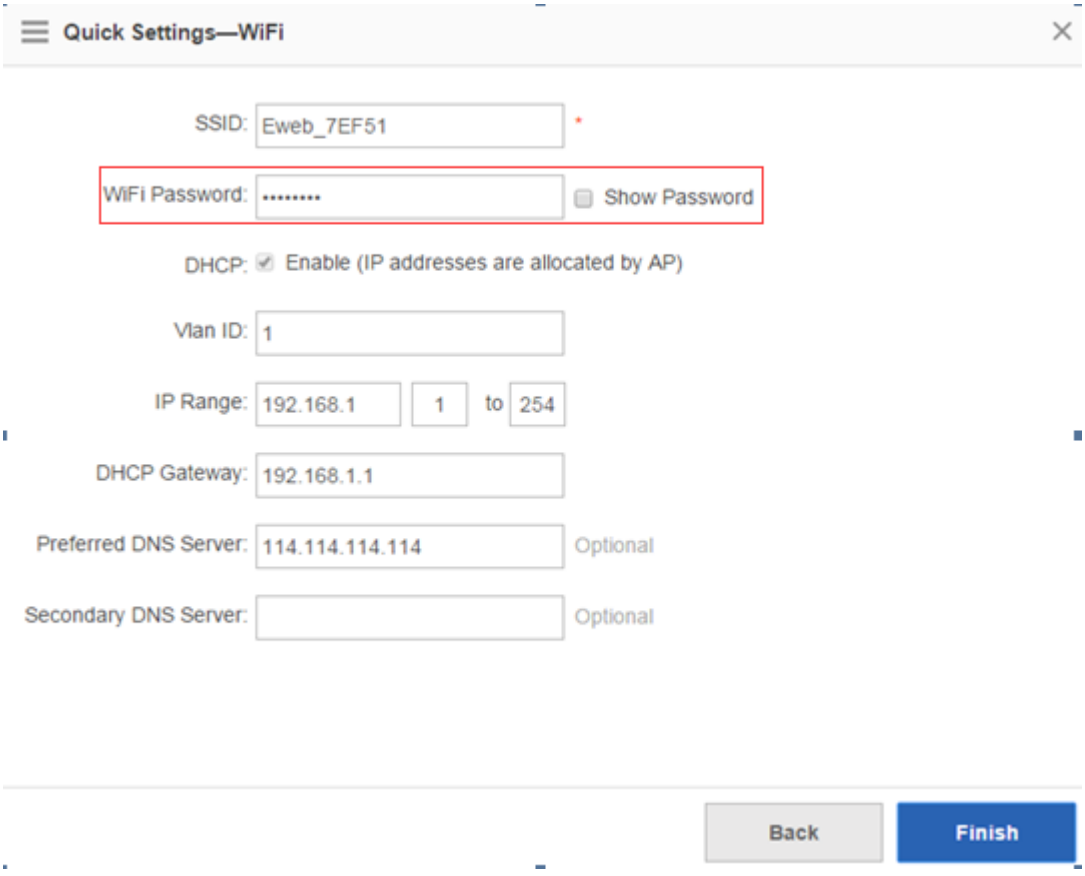
Figure 1-4 AP Quick Settings for SSID



Security configuration

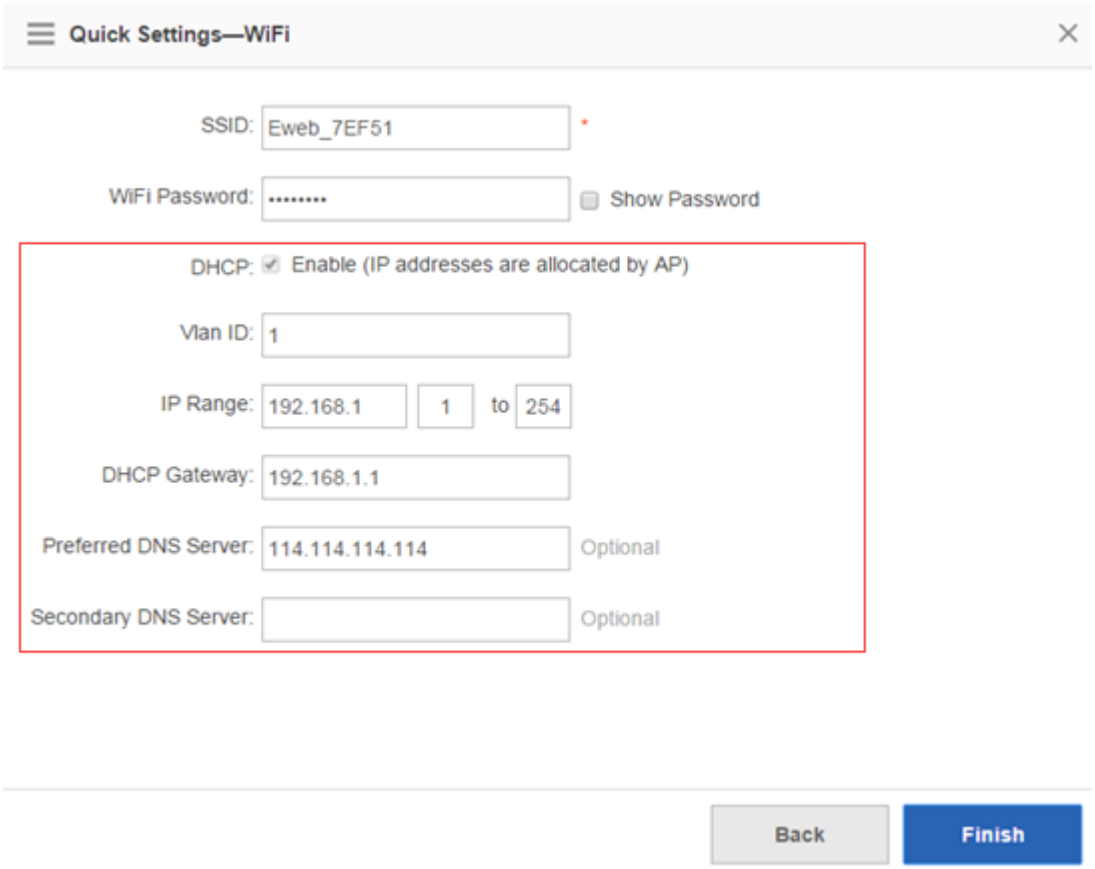
- By default, the WPA2-PSK mode is selected. A password consists of 8 to 64 characters and can be a combination of letters, digits, and special characters.

Figure 1-5 AP Quick Settings for Security



DHCP configuration

Figure 1-6 AP Quick Settings for DHCP



- IP address range: 192.168.1.0/24 to 192.168.1.254/24.
- DNS server: 192.168.58.110 (Perform configuration based on actual conditions.)
- Click **Finish**.

Verification

- Associate an STA with WiFi: Eweb_AAAA1 and obtain the IP address 192.168.1.4.
- Verify that the STA can connect to the WiFi and then visit the Web through 192.168.1.1.

If the management IP address is changed, use the new management IP address to use the Web again.