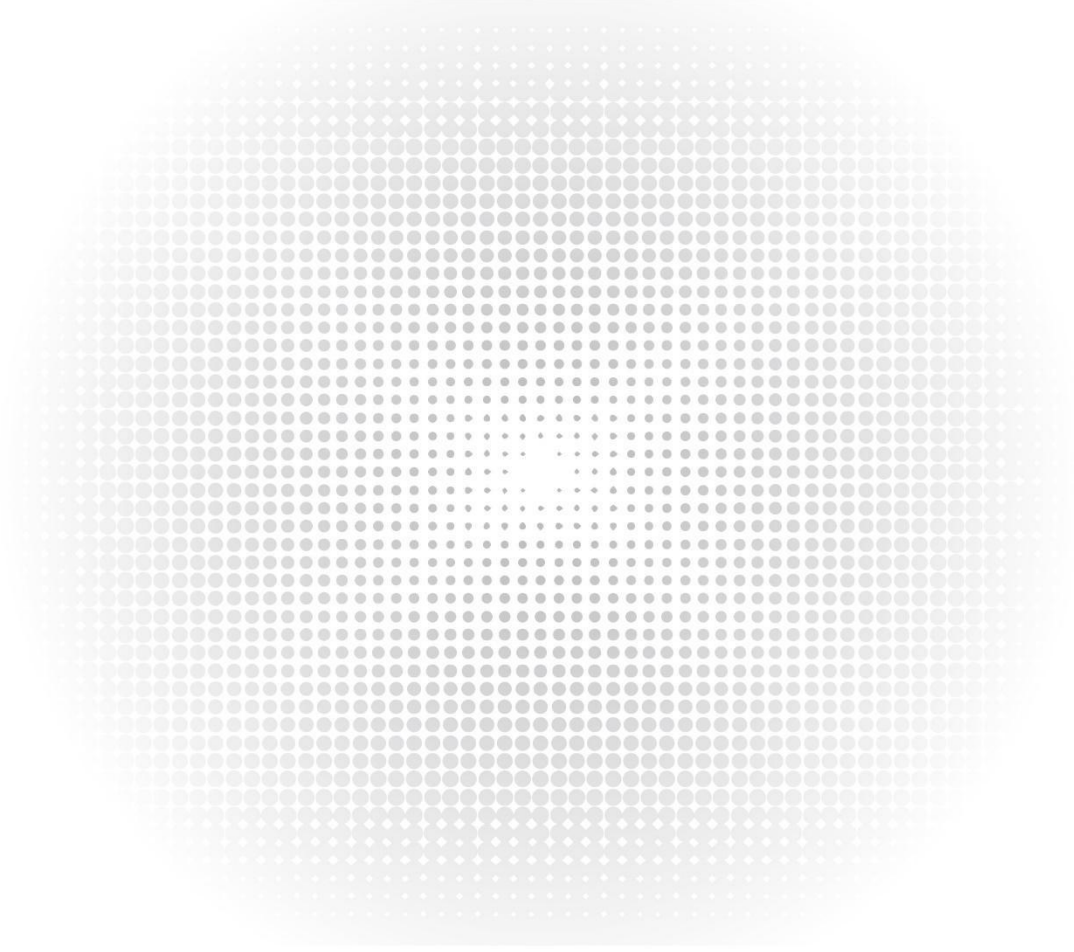
S5860 Series Switches Web Configuration Guide

Models: S5860-20SQ; S5860-24XB-U;S5860-24XMG;S5860-48XMG;S5860-48XMG-U



CONFIGURATION GUIDE

Contents

Web-Based Configuration **1**

1.1 Overview **1**

1.2 Application **1**

1.2.1 Web-based Management 1

1.3 Web Management System **3**

1.3.1 Quick Settings 6

1.3.2 Monitor 9

1.3.3 Configuration 13

1.3.4 Diagnosis 65

1.3.5 Maintain 68

1.3.6 Other Functions 72

1.4 Open WEB Server **75**

Web-Based Configuration

1.1 Overview

A user accesses the Web-based management system of a switch by using a browser (for example, IE browser) to manage the switch.

Web-based management involves two parts: Web server and Web client. A Web server is integrated onto 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 result to the client. Generally, a Web client refers to a Web browser, for example, IE browser.

At present, this document is only applicable to S5860 series switches.

Note that the web cannot be mixed with the device side. After the device side is configured, the web needs to be refreshed, for example, press F5 torefresh.

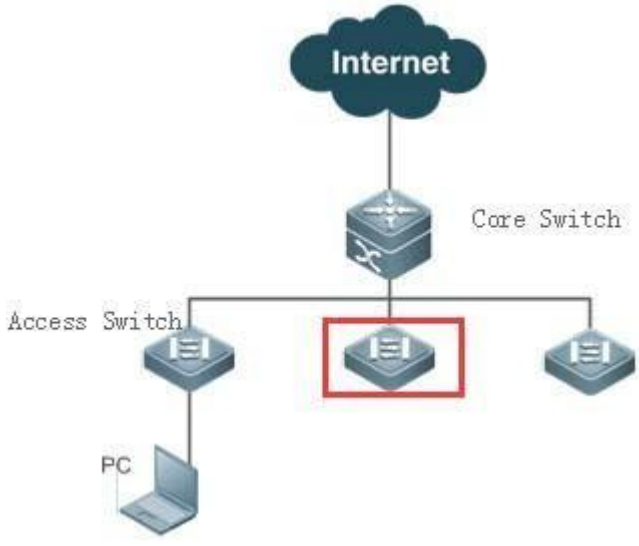
1.2 Application

Application	Description
Web-based Management management	After finishing relevant configuration, a user can access theWeb-based system through a browser.

1.2.1 Web-based

Management Scenario

As shown in the following figure, a user can access an access switch or aggregation switch through a browser on a PC to manage and configure the device.



NOTE: A user can access the Web-based management system of the switch in the red rectangle if this switch can be pinged from the PC.

Function Deployment

Configuration Environment Requirements

Requirements for Client

An administrator logs in to the Web-based management system by using the Web browser on a client to manage the switch. Generally, a client refers to a PC. It may also be other mobile terminal devices, for example, a laptop.

Browser: IE7.0, IE8.0, IE9.0, IE10.0, IE11.0, Google chrome, Firefox, and some IE kernel-based browsers (for example, 360 security browser) are all supported. Exceptions such as messy code and format error may occur when other browsers are used.

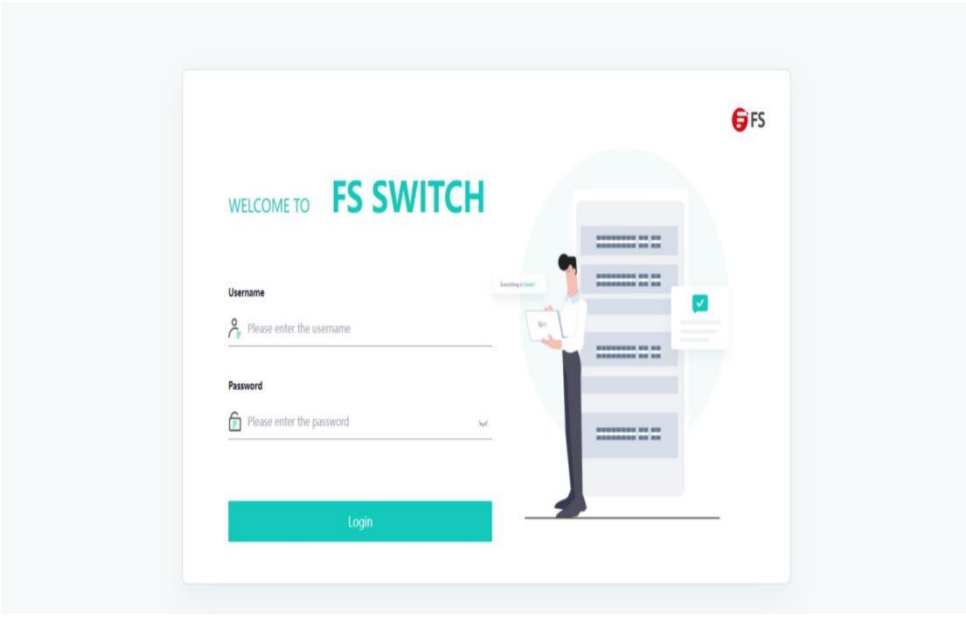
Resolution: It is recommended that the resolution be set to 1024*768, 1280*1024, or 1920*1080. Exceptions such as font alignment error and format error may occur when other resolutions are selected.

WEB configuration and command line configuration can be carried out at the same time. It should be noted that after the

command line configuration is completed, it is best to enter the "write" command to save the configuration; when you open the WEB page, please refresh the opened page. So as to ensure the synchronization of WEB configuration and command line configuration.

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.



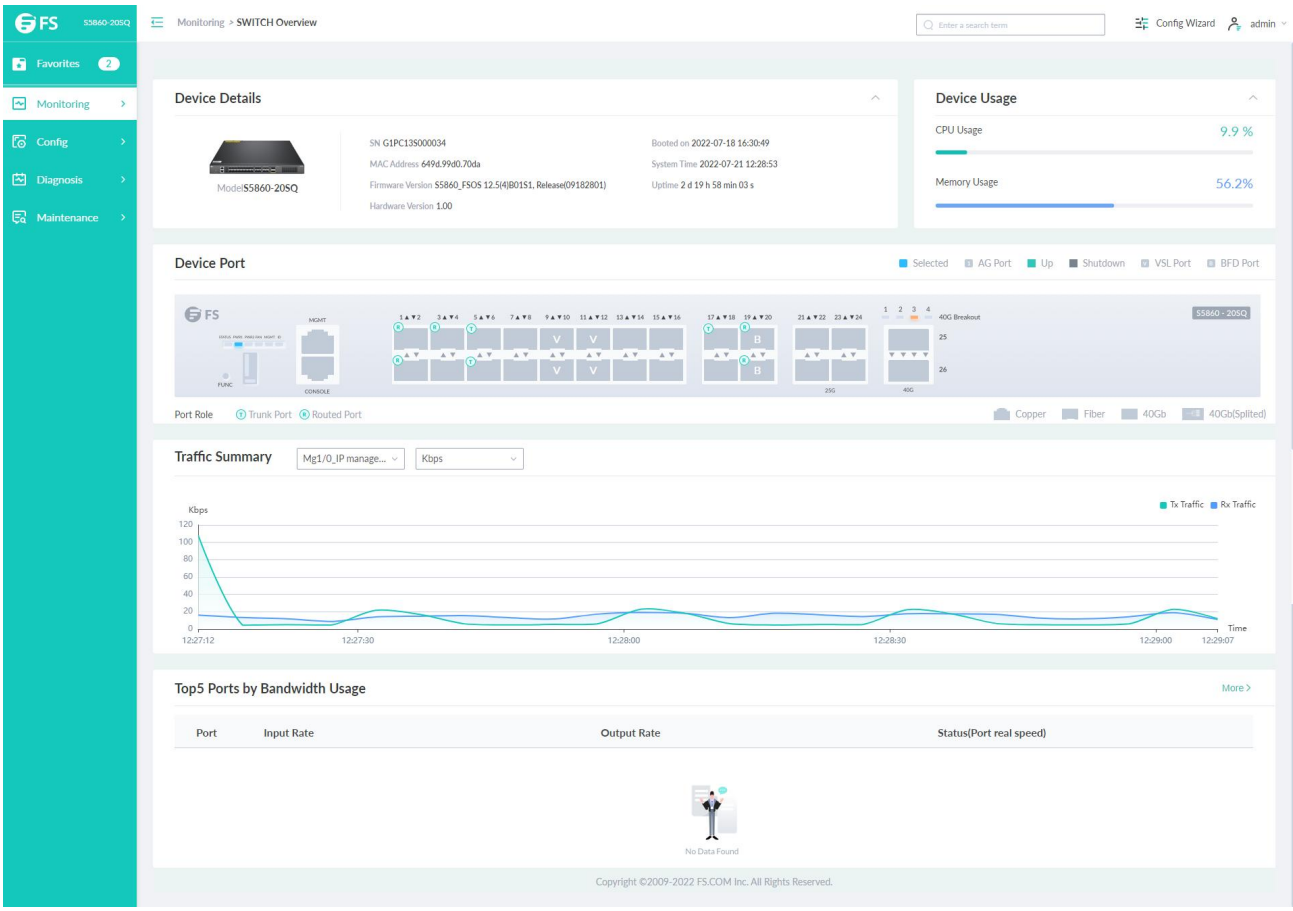
After typing the username and password, click Login. The following table lists the default username and password.

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

NOTE: The default username and password are not displayed by running the show running-config command.

When logging in with the default user name and password, the system will ask to change the password for security reasons;

After passing authentication, the home page of the Web-based management platform is displayed, as shown in the following figure.



NOTE: For details about the Web page, see Web Management System.

1.3 Web Management System

Basic Concepts

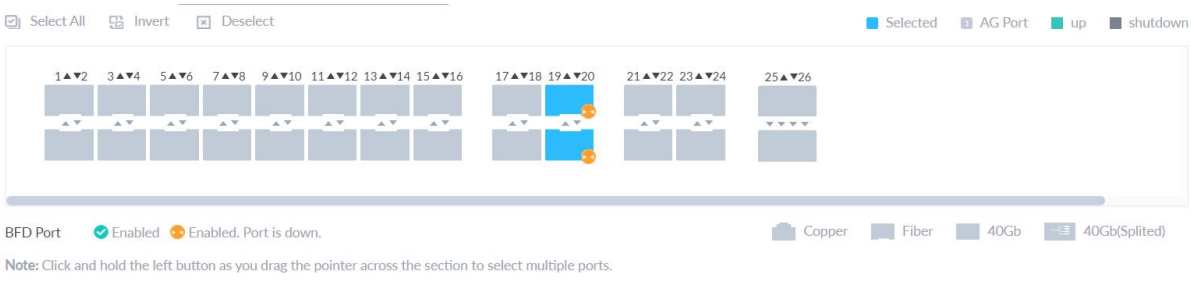
Various Icons and Buttons on the GUI

Icon/Button	Note
	Edit, click this icon to edit the currently selected record
	delete
	Status switch icon
	Optional port, click or frame selection can make the port become "selected port"
	Shutdown port

	Select the port
	Aggregation port, the number in the port represents the aggregation port number
	Trunk port is reflected in the panel of VLAN management/VLAN setting page
	The port is powered on
	VSL port
	BFD port, withdraw cash in the panel of the switch overview page
	40G port
	40G split port
Save	Save button to submit and save the entered information
	Add settings
	Delete settings
*	Required item, if the symbol behind the input box indicates that the option is required
	Description flag
	Attention sign
	Fail

System Operations

1) Standalone Device Panel



Panel operation

You can click the <port> on the panel or drag the mouse to select multiple <ports> to make the <port> become <selected port>, and then set the selected <port>, such as adding port description, port mirroring And port speed limit, etc.

Device panel selected port diagram

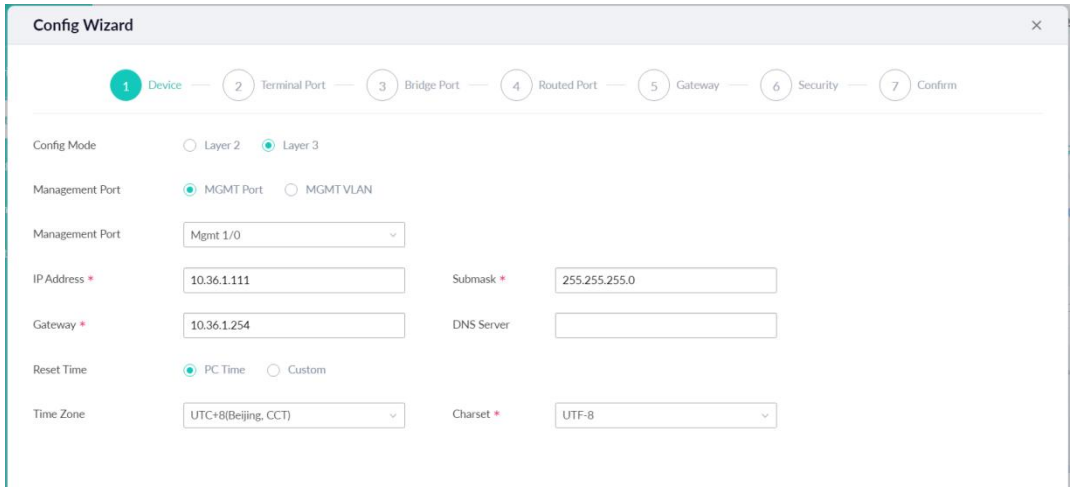
Feature

The following table describes the functions in the secondary menu on the left of the Web page.

Feature	Description
Quick Configuration	Simple network construction can be carried out on the equipment
Switch Overview	You can view port information and device overview
Spanning Tree State	Can view spanning tree status and port role information
RLDP Status	You can view the RLDP switch and the port information that enables RLDP detection
DHCP Client List	You can view the addresses assigned by the switch address pool
DHCP Server Status	Can view DHCP server and configured address pool
VSU Status	Only exists when the device is in stacking mode, you can view the topology diagram that composes the stacking
VLAN Management	You can set VLAN and Trunk port
Port Management	You can perform basic settings on the port, and set port aggregation, port mirroring, and port speed limit
Routing Settings	You can set up routing
DHCP Server	Can set up DHCP, static address assignment and client list
VRRP	Can set up VRRP
MAC Address	Can carry on static address setting and filtering address setting
VSU Configuration	The device can be configured for stand-alone and stacking mode conversion
SpanningTreeProtocol	You can set the global basic information of spanning tree and spanning tree port settings
RLDP settings	RLDP global configuration and port configuration
ACL	You can set the ACL list, ACL time, and apply ACL.
Port protection	Port protection can be set.
Port security	Port security settings and security binding can be performed.
Storm control	Can carry out storm control.
DHCP Snooping	You can set up DHCP Snooping.
Anti-ARP attack	You can set anti-gateway ARP spoofing, ARP inspection settings, DAI settings and ARP table entries.
IP Source Guard	You can set the interface and bind users.
NFPP	You can view NFPP anti-attack related content.
IGMP Snooping	You can set IGMP Snooping.
QOS	You can perform classification settings, policy settings, and stream settings.

DHCP relay	You can set up DHCP relay.
Online real-name authentication	Can carry out external web authentication and advanced configuration.
ping detection	Connectivity test for IP address or domain name
tracert detection	Tracert detection of IP address or domain name
One-click collection	Collect information on the device with one click
System log	You can set the syslog log server and view the system log.
System log monitoring	Log can be queried according to grade and module name
upgrade	Can be upgraded locally.
Reboot	Restart the device
Configuration management	Can perform configuration backup, restore factory settings and system character set settings
system time	Revise the system time
Log server	Set whether the log function is enabled on the device
DNS	Can set DNS
WEB configuration management	You can set the administrator password, basic configuration
Telnet	Set Telnet and SSH function and password
SNMP	Can set V2 and V3 version

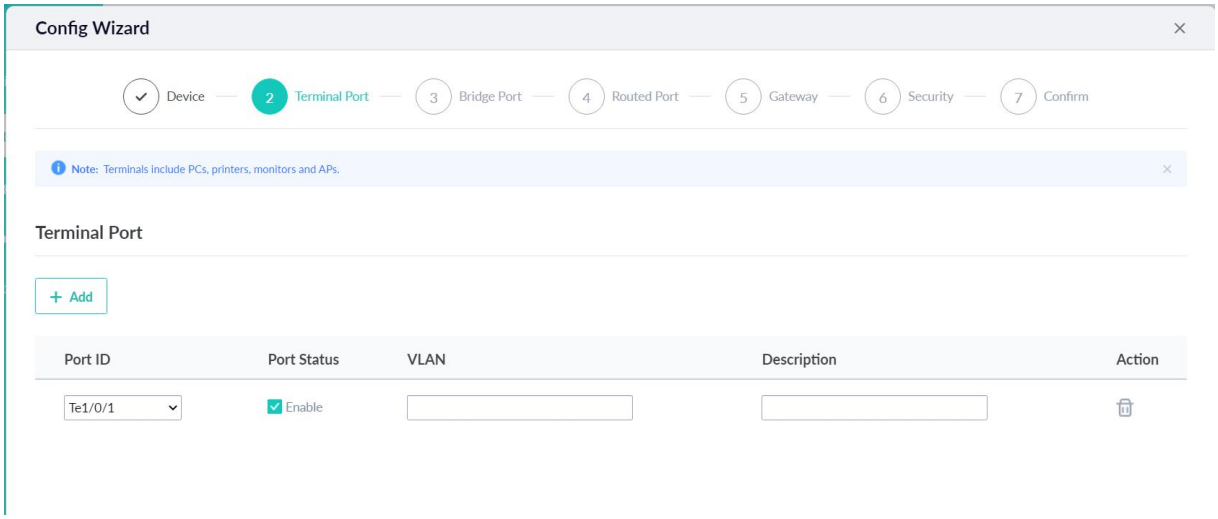
1.3.1 Quick Settings



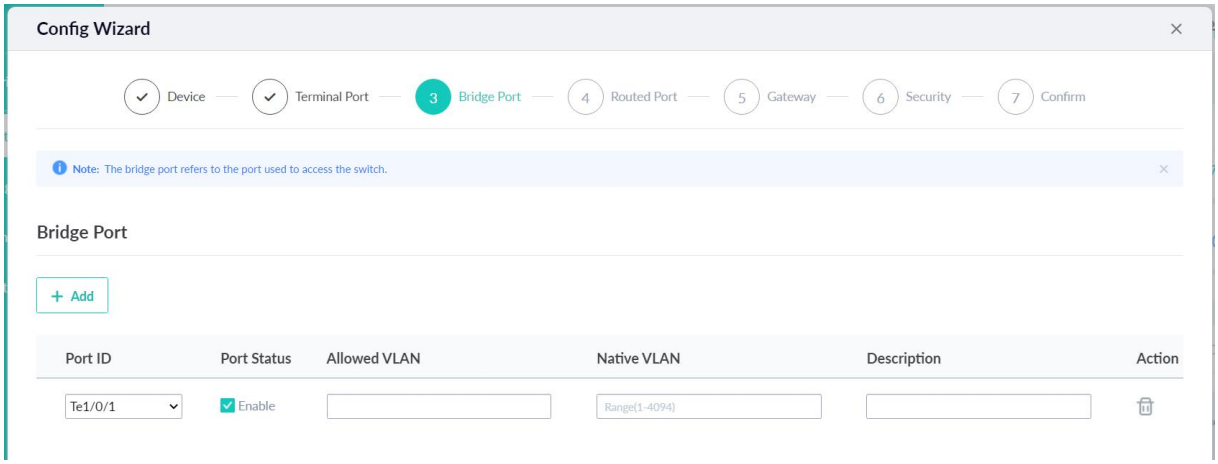
1. Equipment management

Configure the management VLAN ID, IP address, subnet mask, default gateway and DNS server settings, click "Next" to continue the configuration.

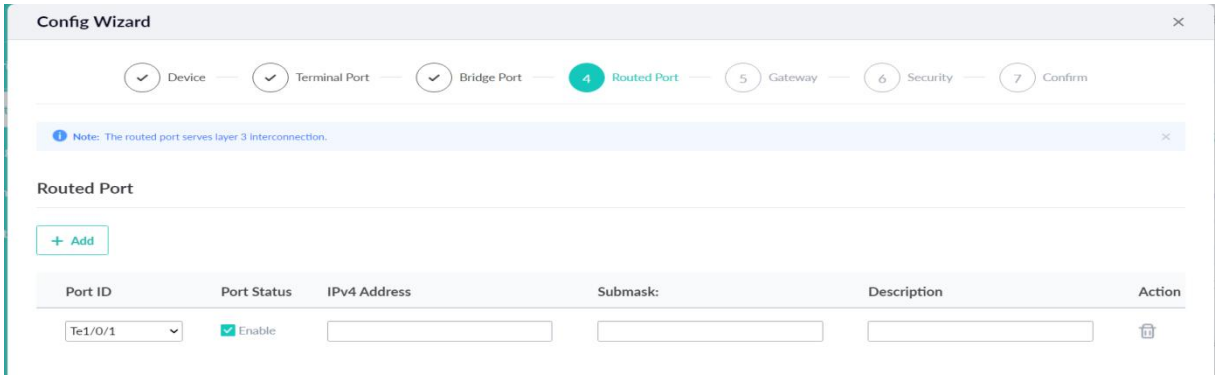
2. Terminal interface



3. Connect switch interface

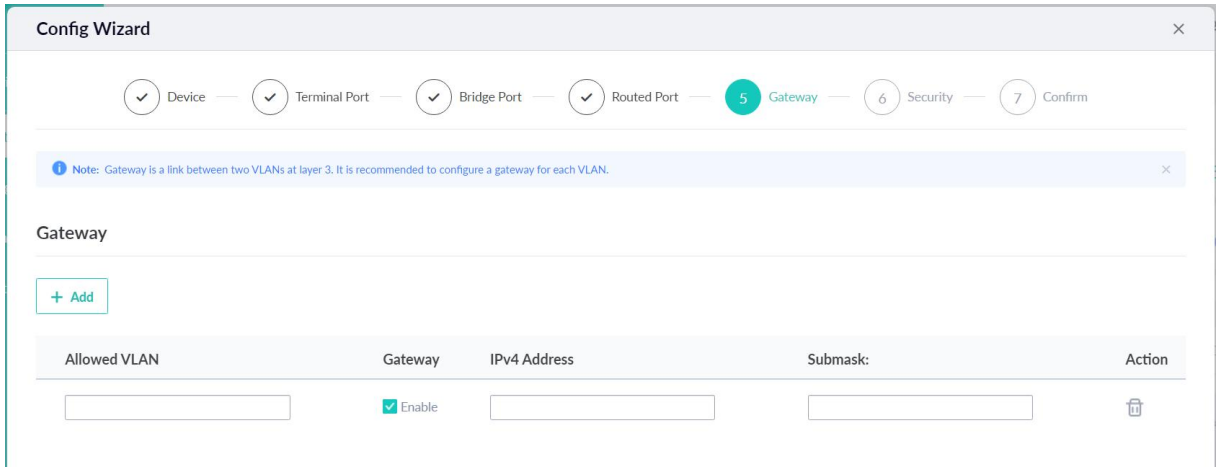


4. Router interface

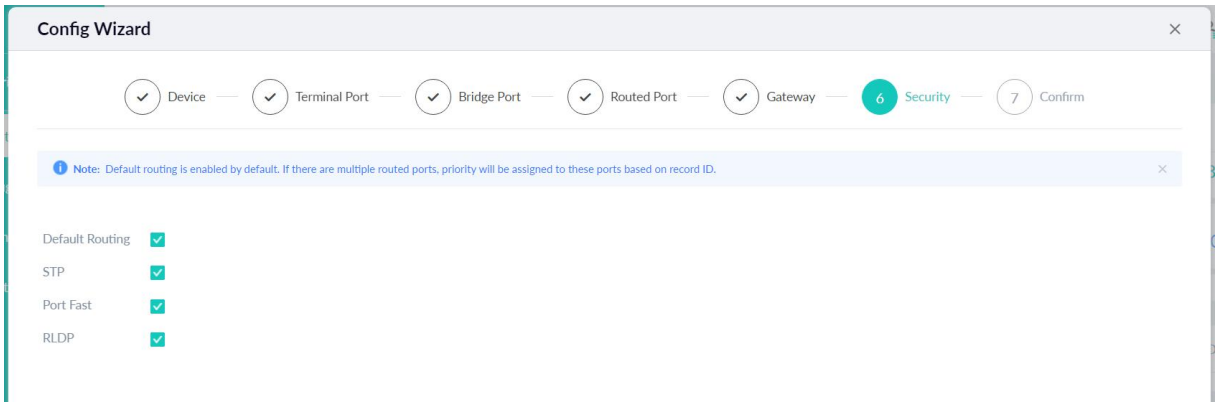


5. Downlink port configuration

After the configuration is successful, the quick configuration pop-up window will automatically close. If you modify the managed IP address of the device, follow the prompts to choose whether to adjust to the new management address.



6. Security configuration



7. Save configuration

After the configuration is successful, the quick configuration pop-up window will automatically close. If you modify the managed IP address of the device, follow the prompts to choose whether to adjust to the new management address.

1.3.2 Monitor

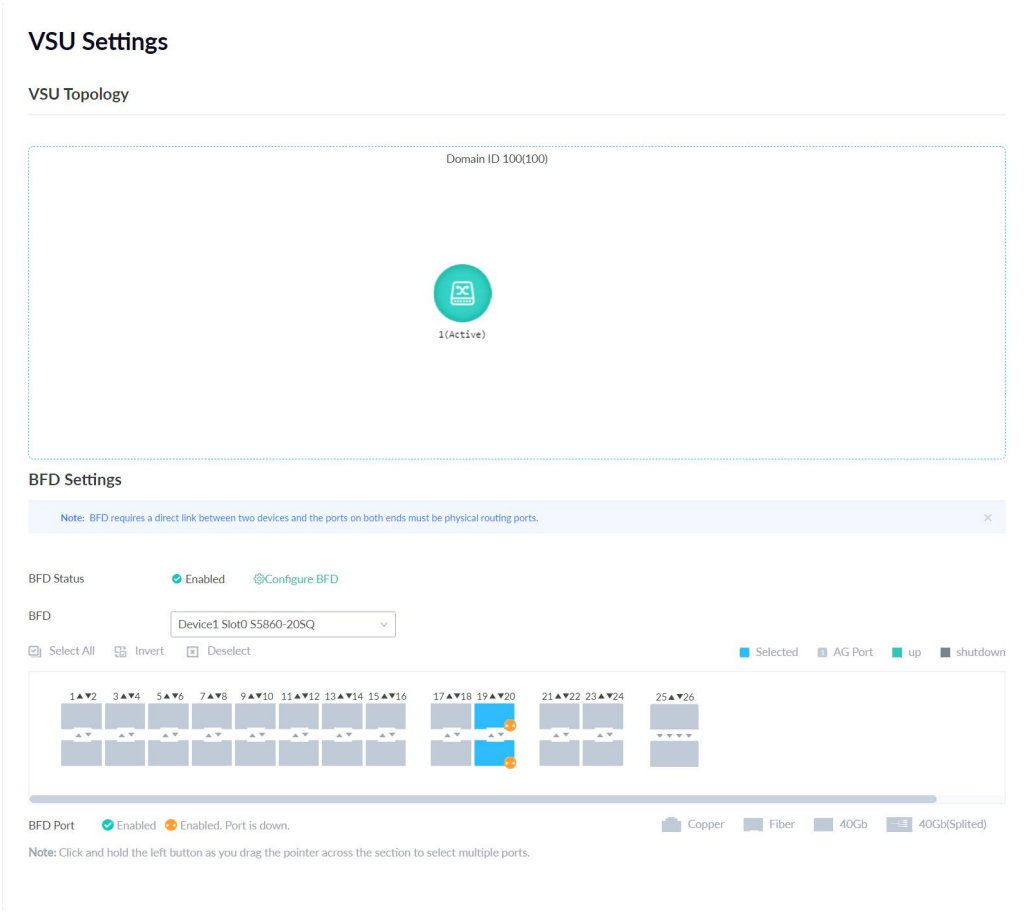
Through the first level menu "Commonly used", you can enter the second level menu. Including homepage, VLAN management, port management, POE settings, system restart.

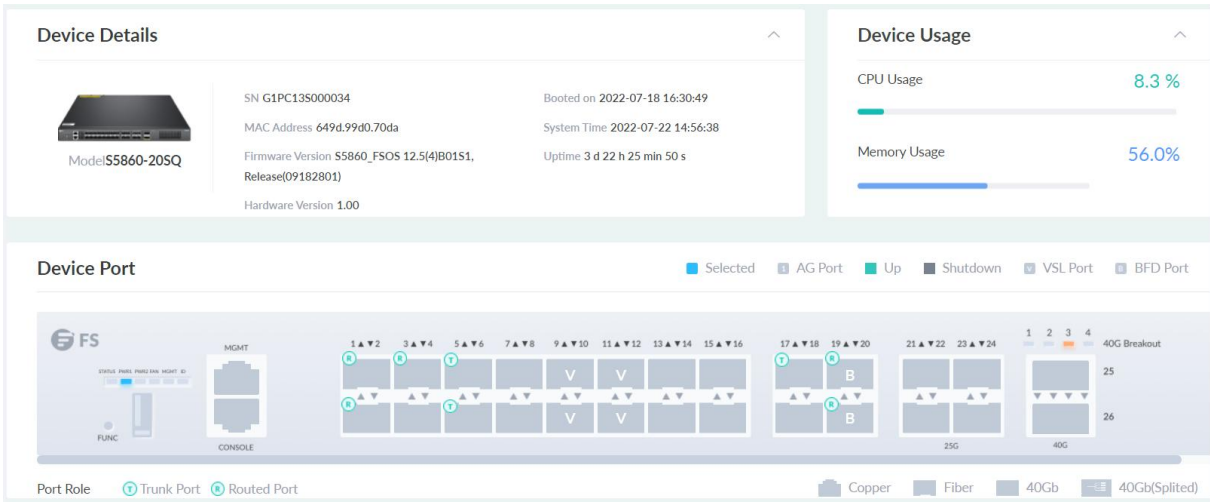
Switch Overview

"Switch Overview" allows you to view the basic information of the device at a glance, such as device MAC address, device model, system running time, version information, device cpu and memory, various status of device ports, traffic trends of device interfaces and interface information Bandwidth utilization.

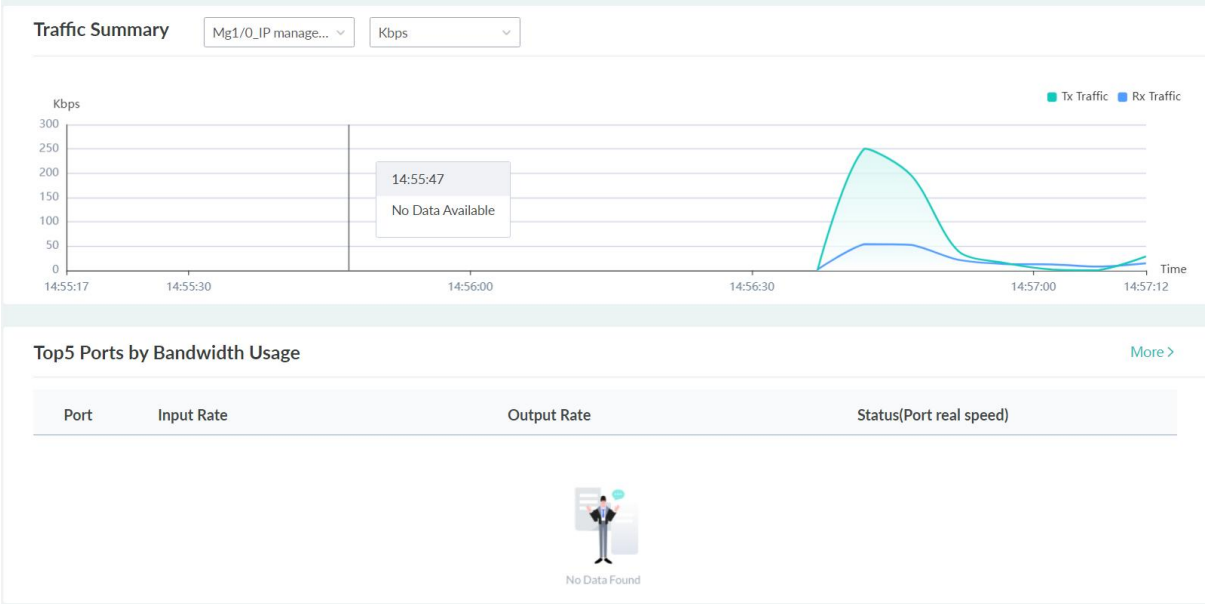
Stand-alone scene

Stacking scene





TOP5 interface bandwidth utilization, click on the "More" pop-up page



Anti-loop Monitoring

Anti-loop monitoring uses spanning tree status and RLDP status to monitor the loop status.

Spanning Tree State

Show spanning tree status and mode, port role and STP usage status

RLDP Status

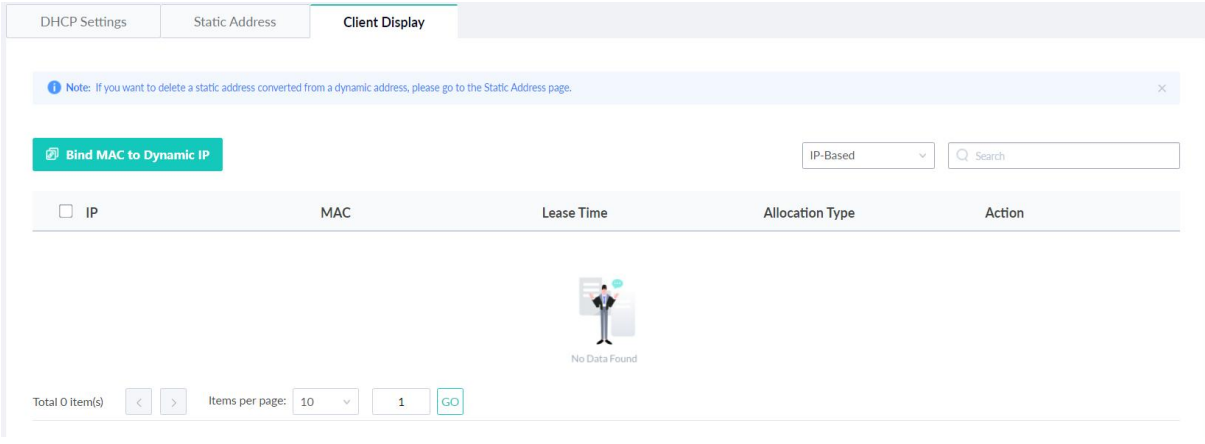
Display RLDP status, port application mode, violation handling method and status.

DHCP

DHCP monitoring is monitored in two dimensions: DHCP service status and DHCP client list.

DHCP Client List

Display the users assigned by the address pool on the switch.



DHCP Server Status

Display the status of the DHCP server and the usage of the address pool.

1.3.3 Configuration

Through the first level menu "configuration", you can enter the second level menu, network, advanced configuration, security, advanced configuration.

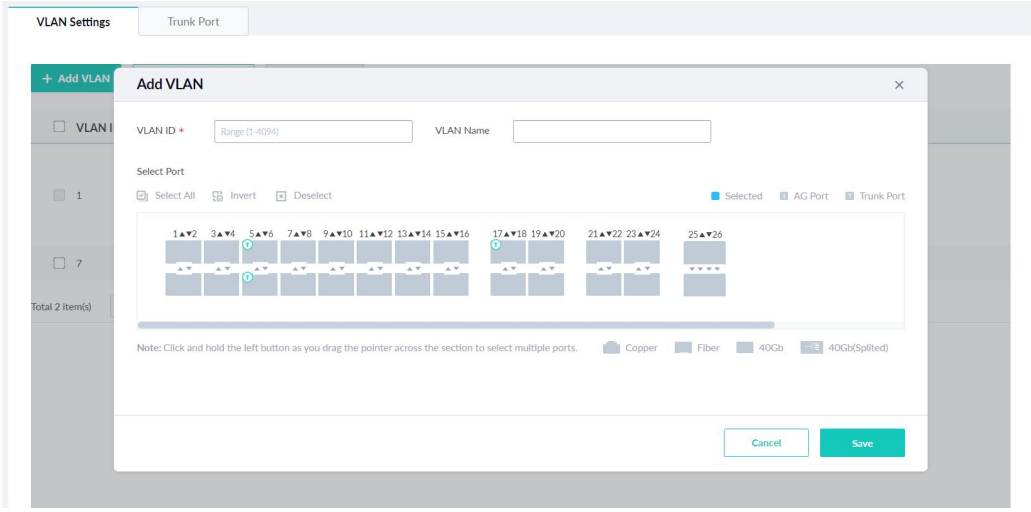
Network

VLAN Management

The VLAN management page contains two parts: "VLAN Settings" and "Trunk Port Settings".

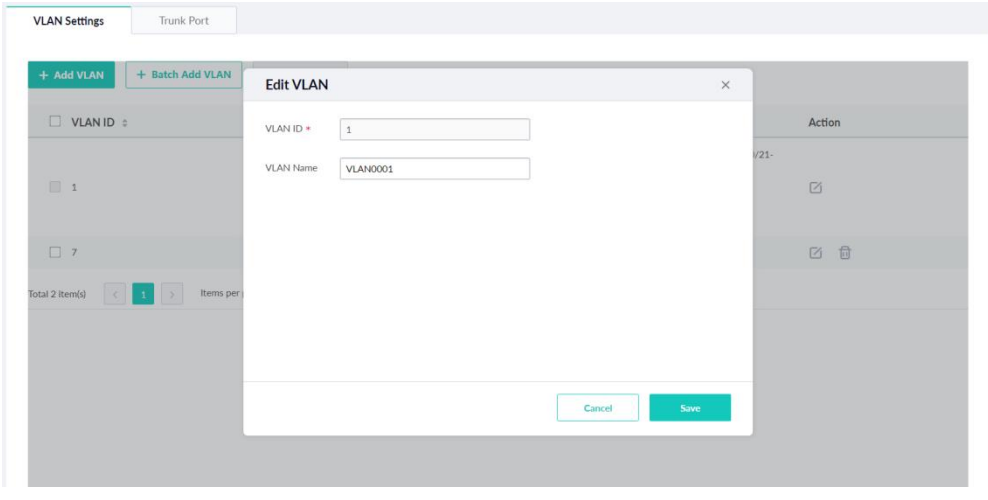
VLAN settings

1. Add VLAN



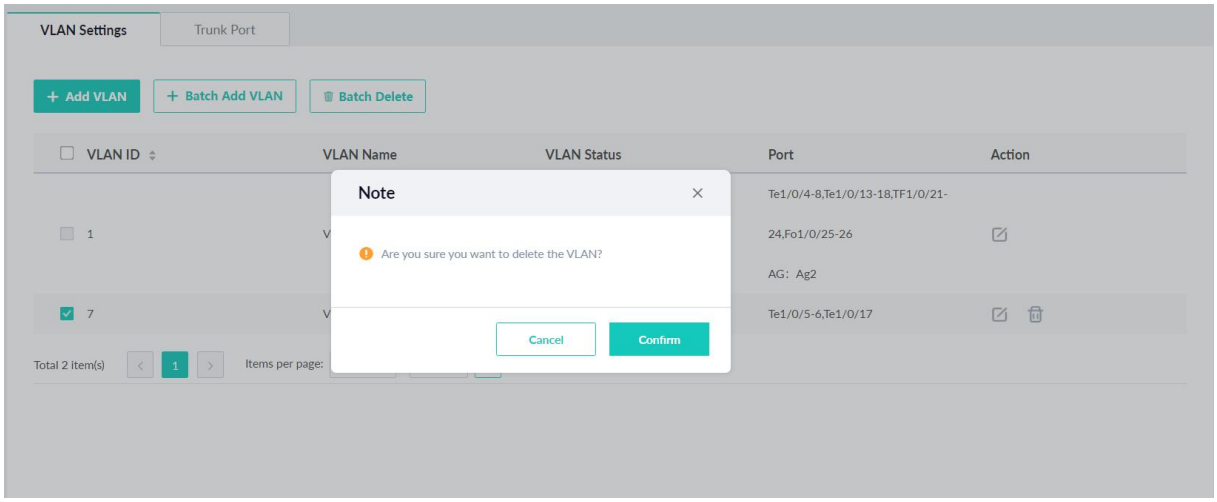
To set a VLAN, you must fill in the VLAN ID, and other information is optional. After clicking "Finish Configuration" and prompting "Setup successful", it will be displayed in the VLAN list.

2. Edit VLAN



Click the <Edit> button under the operation column of the last column of "VLAN List", the page will display the VLAN information. After editing the information, click <Complete Configuration> to prompt "Setup Successful".

3. Delete VLAN



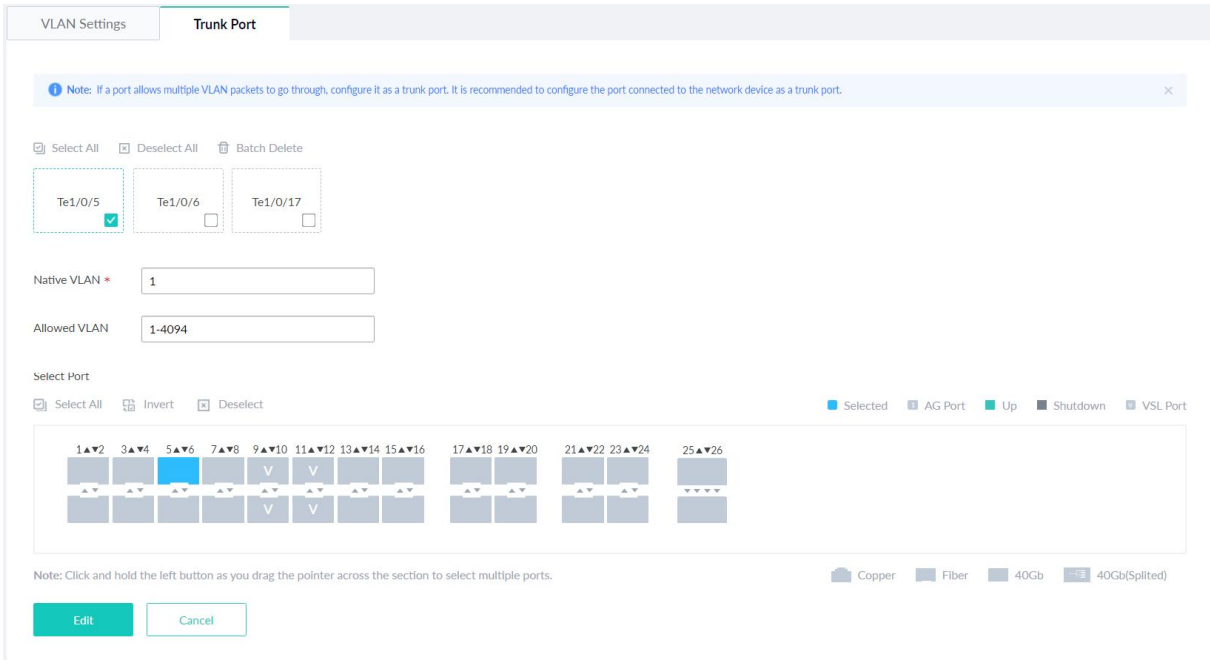
1) Select multiple records in "VLAN List" and click "Delete Selected VLAN" to delete data in batches.

2) Click the <Delete> icon under the operation column of the last column of "VLAN List", and prompt "OK to delete the selected vlan", click OK and prompt "Delete successfully" to complete the deletion. VLAN 1 is the default VLAN and cannot bedeleted.

VLAN1 is the default VLAN, the page only provides modification functions and cannot be deleted.

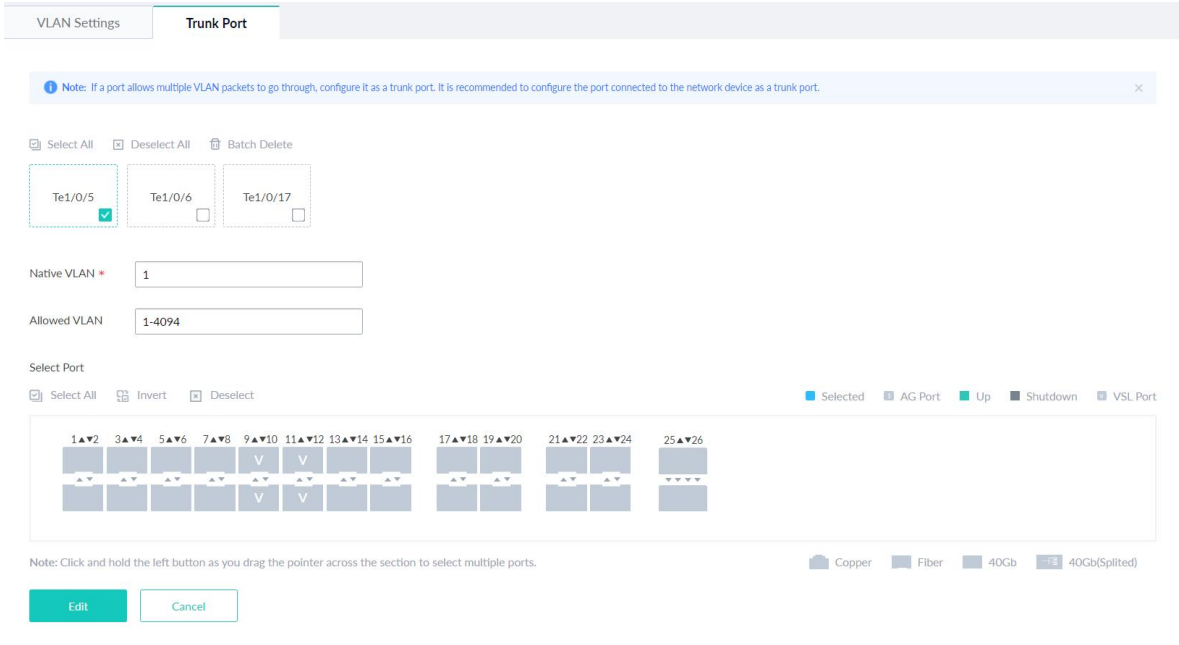
Trunk port settings

1. Add Trunk port



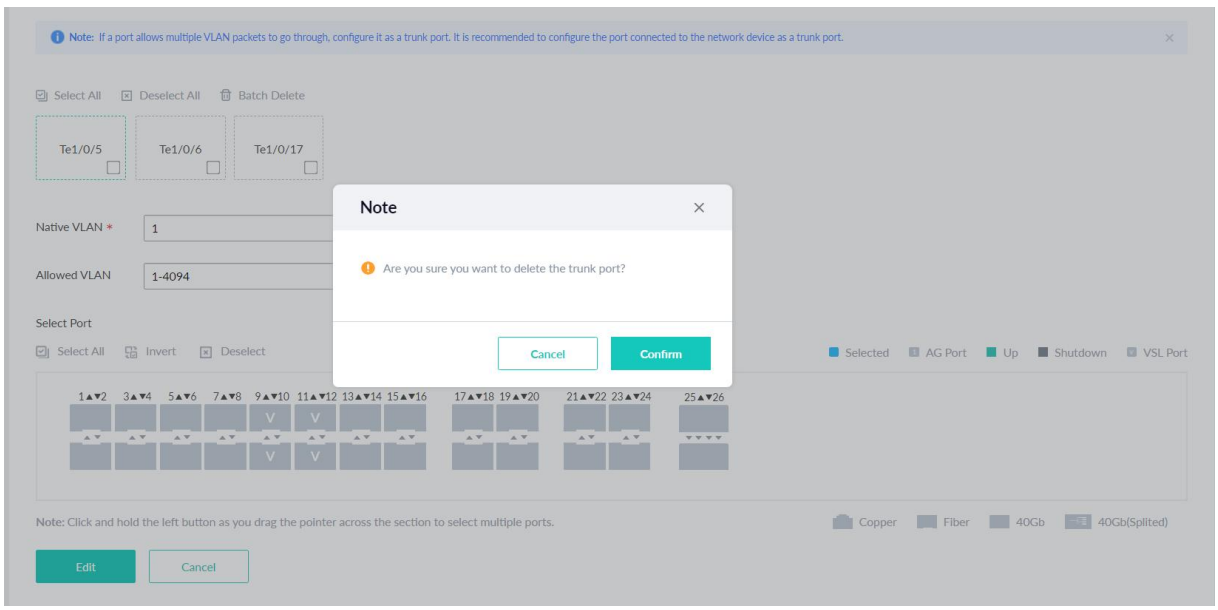
Select the panel port, fill in the Native Vlan and allowed VLAN (such as 3-5, 8, 10), click "Save Settings" to prompt "Setup Successful" to complete the adding operation, the added Trunk will be displayed in the Trunk Port List.

2. Edit Trunk Port



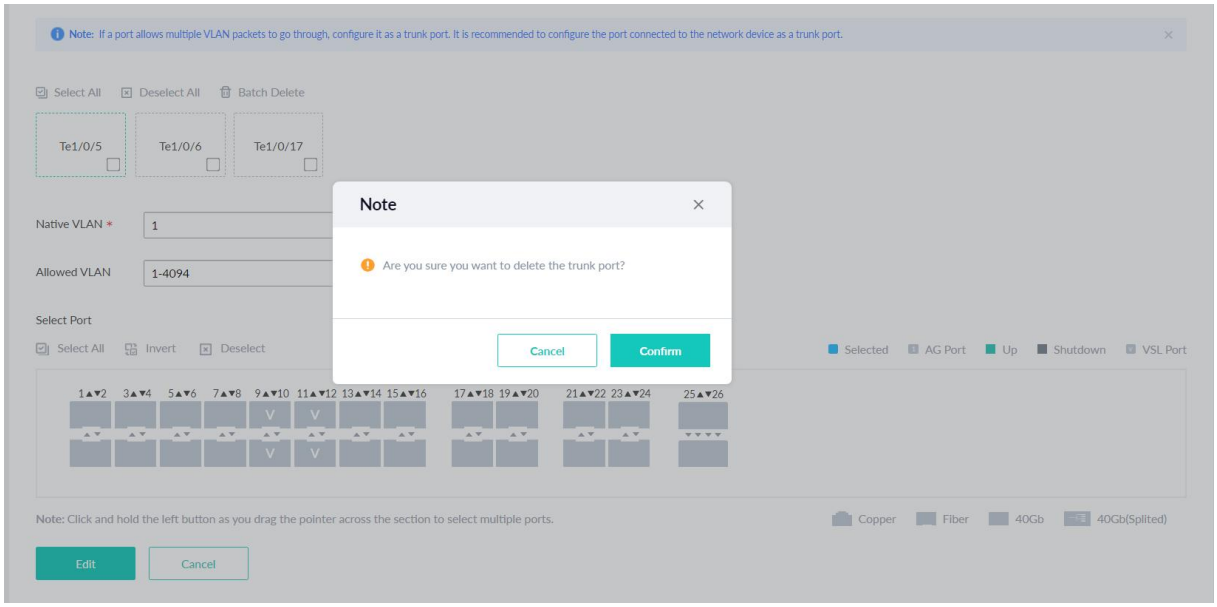
Click on a Trunk port in the "Trunk Port List", the page will display the Trunk port information, after editing and modifying the information, click <Edit Settings> to prompt "Setup successful".

3. Delete Trunk Port



In the "Trunk Port List", move the mouse to a Trunk port, select the <Delete> icon, and prompt "Are you sure you want to delete this Trunk port?", click OK and prompt "Delete successfully" to complete the deletion.

4. Delete Trunk Ports in batch

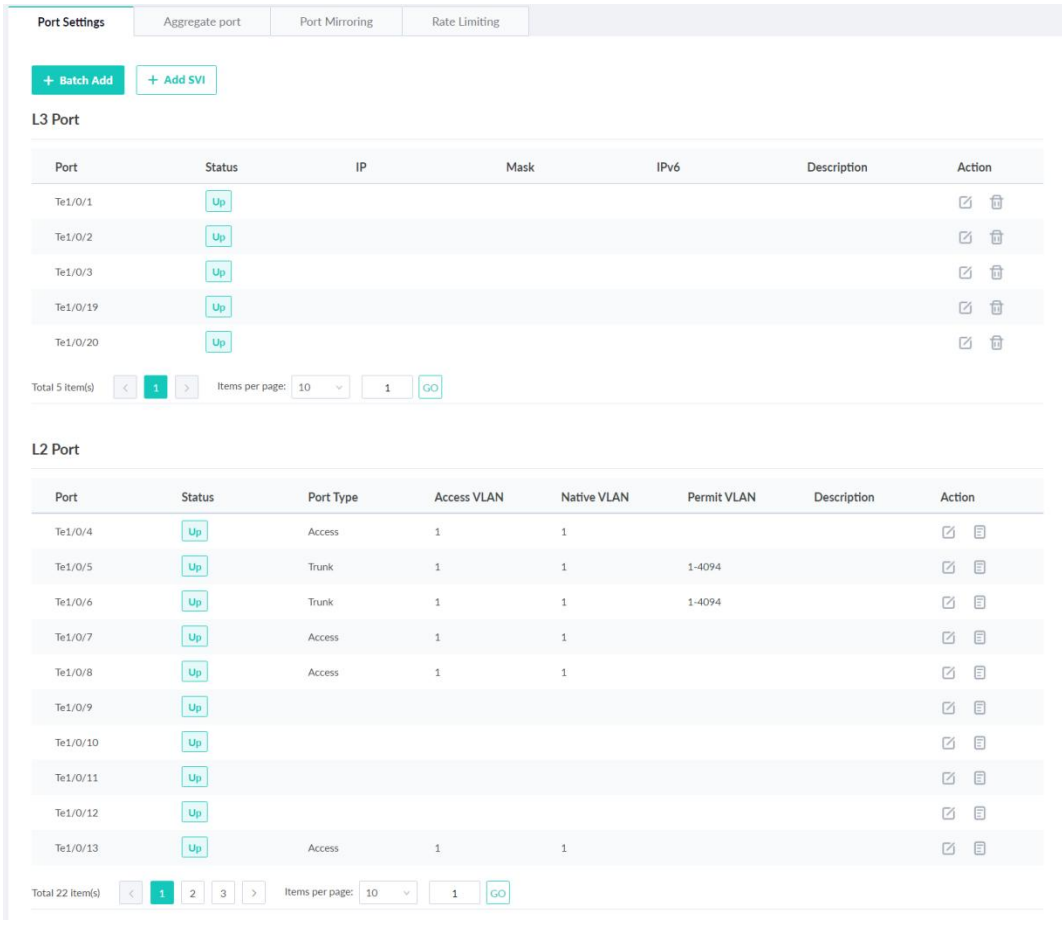


Select the Trunk port to be deleted in the "Trunk Port List", select the <Batch Delete> icon, and prompt "Are you sure you want to delete the Trunk Port?", click OK and prompt "Delete successfully" to complete the deletion.

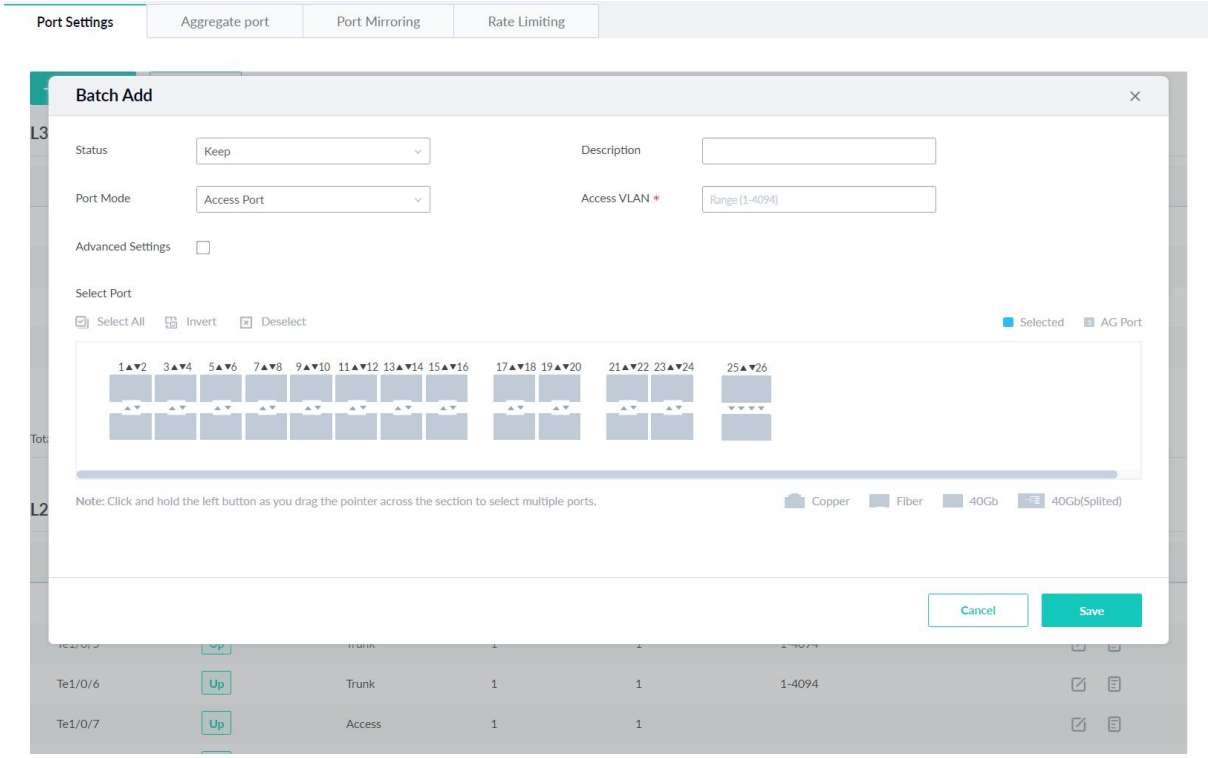
Port Management

"Port Management" can perform basic port settings, port aggregation, port mirroring, and port speed limit settings.

☆ **Basic settings**

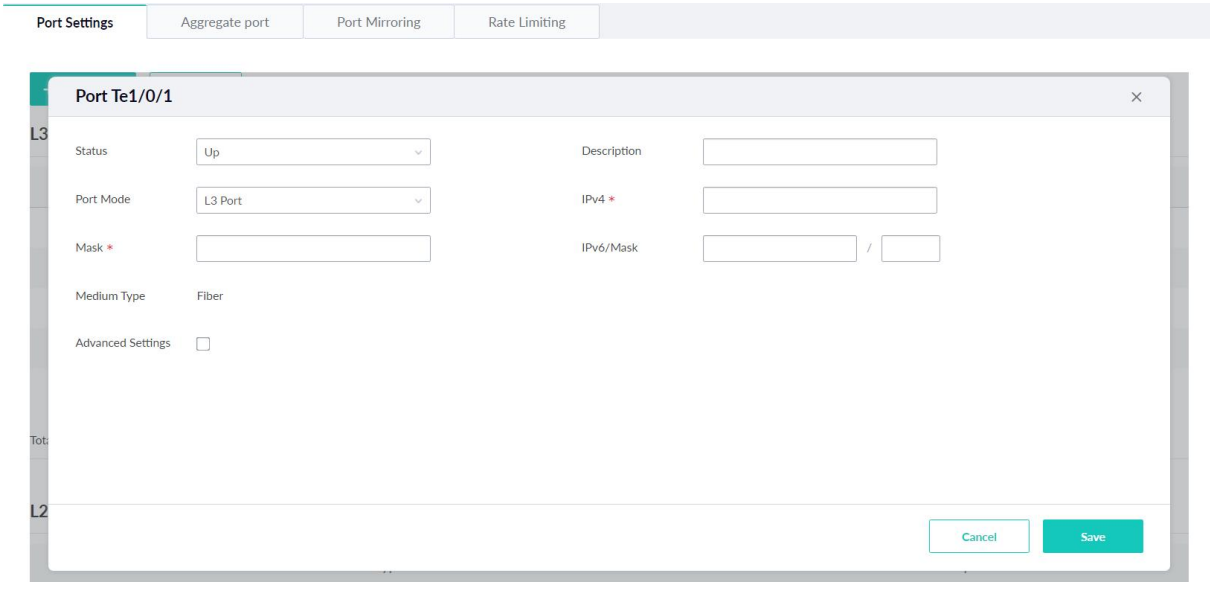


1. Set Ports in batch



First select the port that needs to be configured, and then select the port status, speed, mode, etc., among which "no modification" means to keep the original configuration. In batch setting, you can set only one or two items in batch by setting "no modification".

2. Edit port



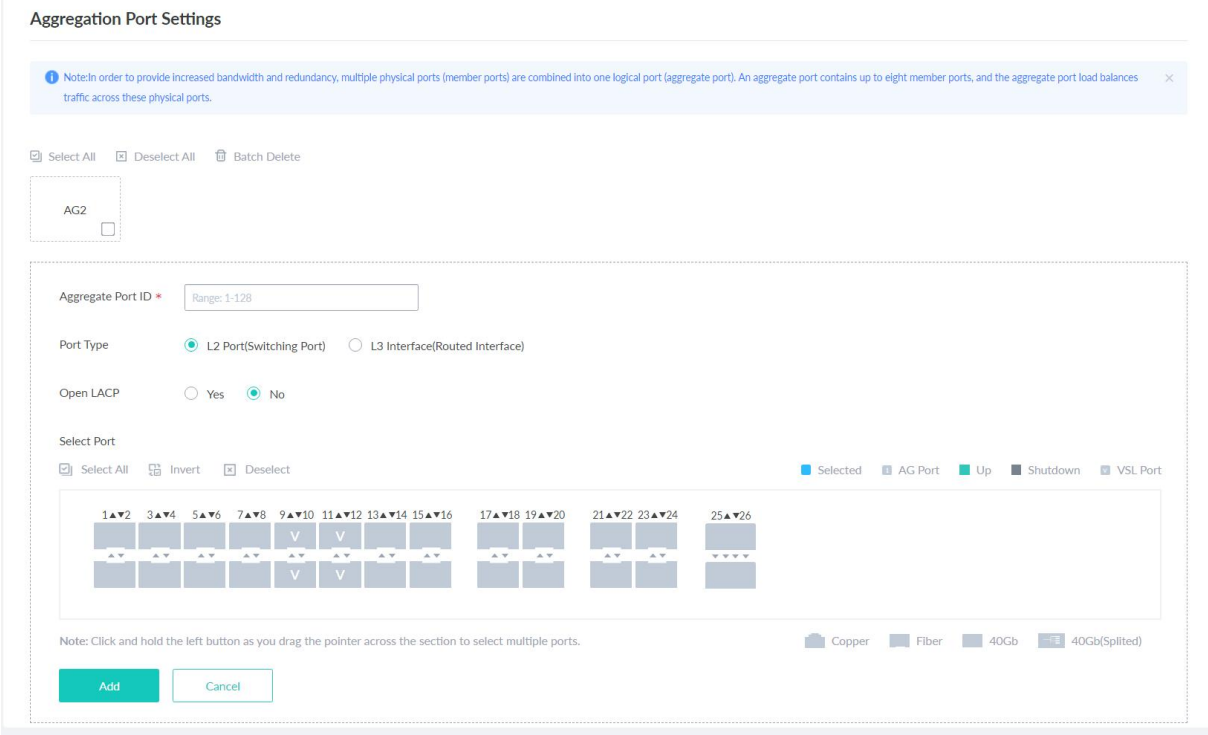
In the "Port List", the <Edit> icon under the operation bar in the last column will display the information of the port on the page. After editing the information, click <Complete Configuration> to prompt "Setup Successful".

☆ Port aggregation

1. Add polymerization port

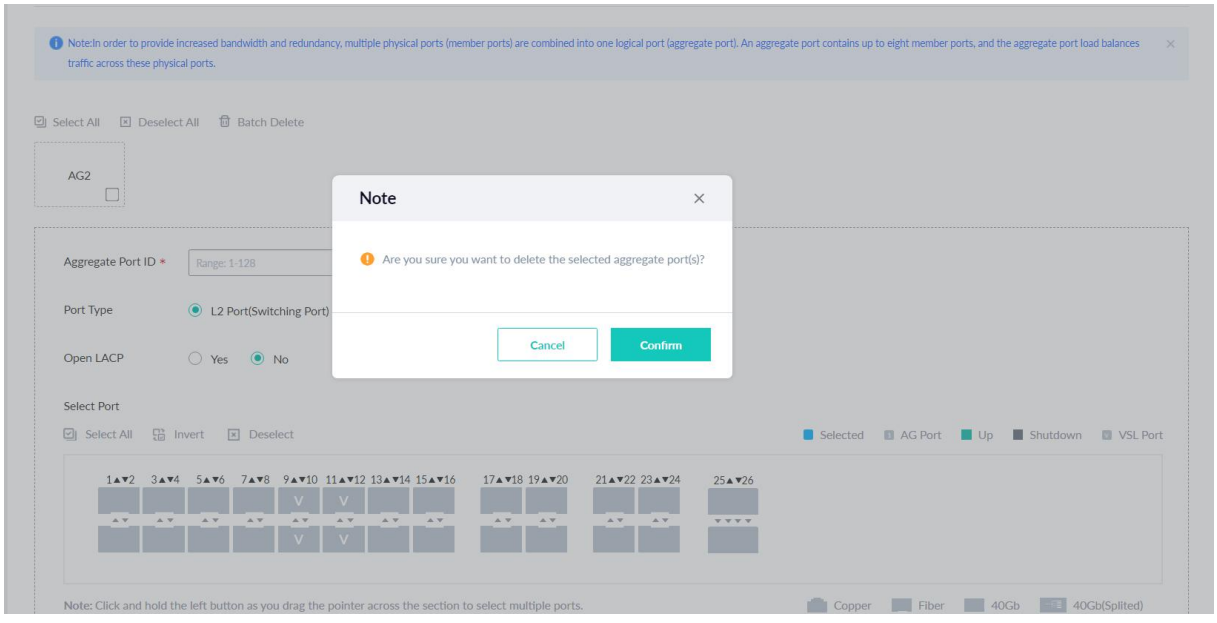
Enter the aggregate port number and select the member port and press "Add Setting", and the message "Setup successful" is displayed to complete the adding operation of the aggregate port. After the addition is successful, the panel will display <Aggregation Port>.

2. Edit aggregation port



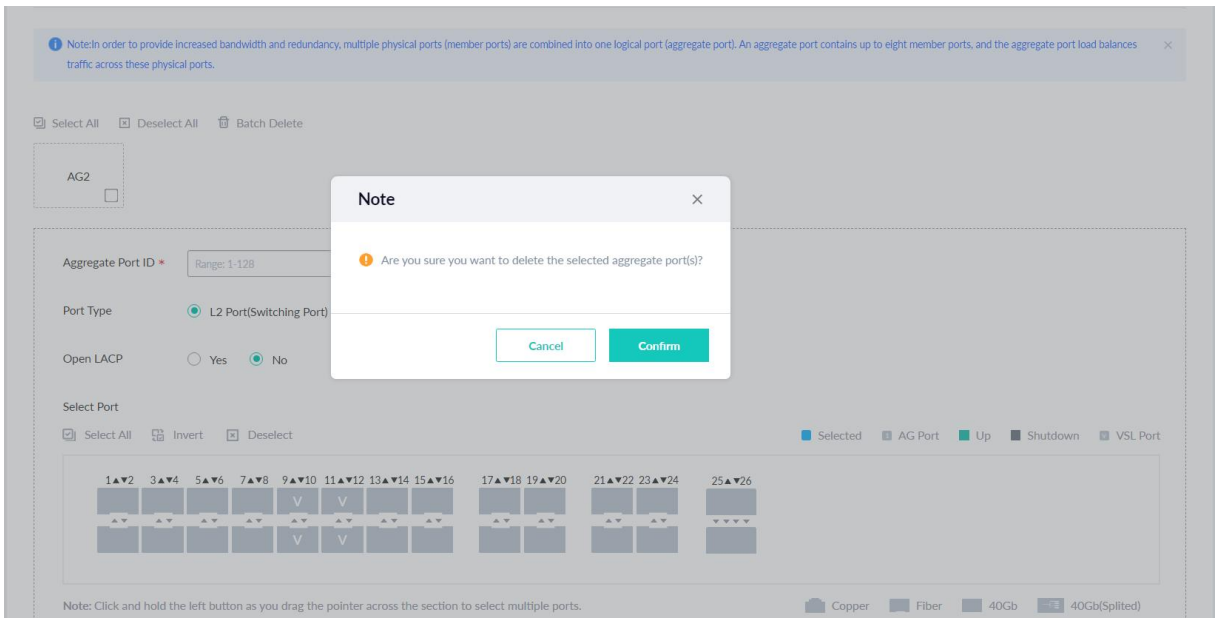
The aggregation port displayed on the panel is <unselectable port>. If you want to edit and modify them, you can click an aggregation port in the "Port Aggregation List", then the "Member Port" will become selected, click on the port You can uncheck it, and then click "Edit Settings" to modify the aggregation port.

3. Delete aggregation port



In the "Port Aggregation List", move the mouse to the aggregation port, click the <Delete> icon, and a confirmation box will prompt whether to delete the aggregation port. Click OK to delete the aggregation port. After deletion, the panel will be deleted. Aggregate port> becomes <optional port>.

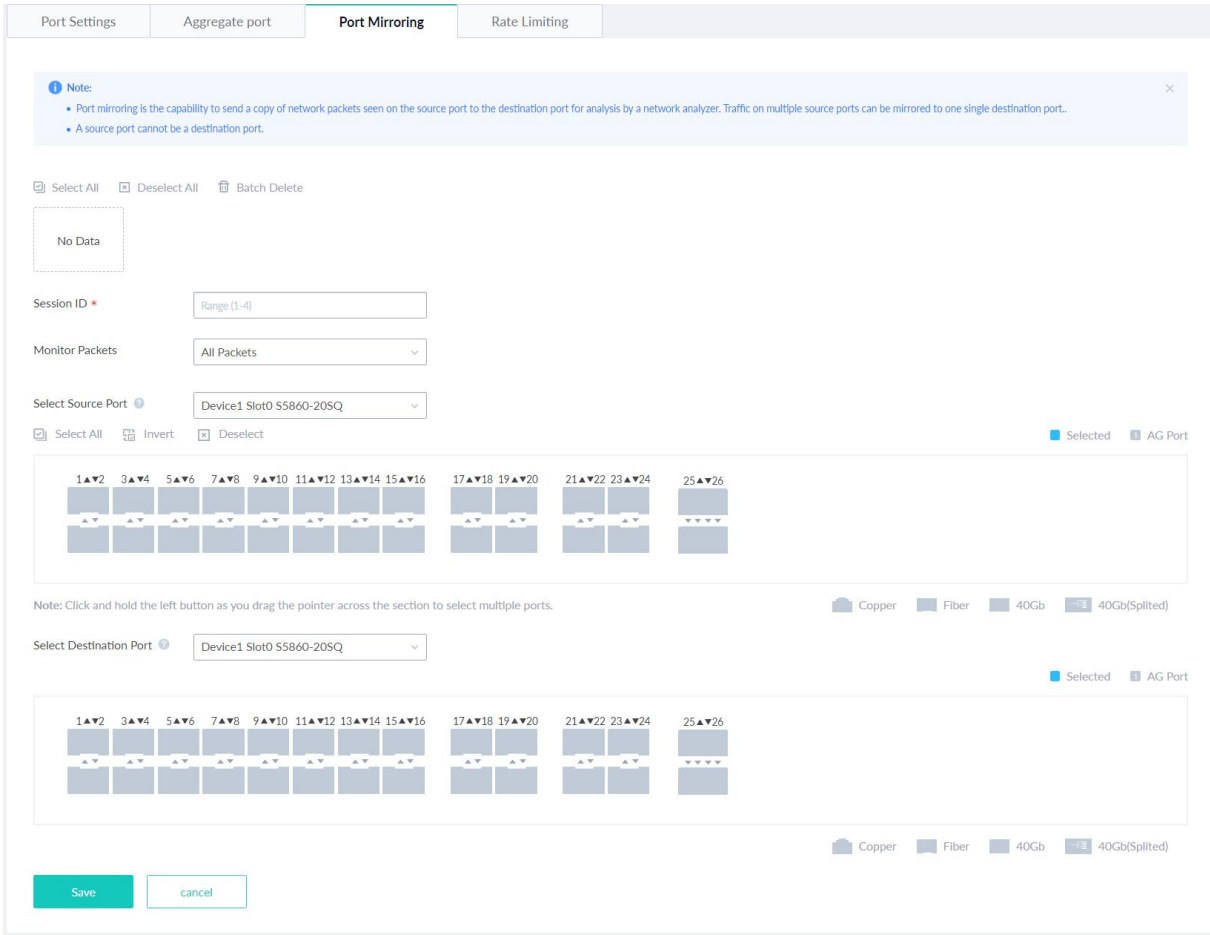
4. Batch delete aggregation ports



In the "Port Aggregation List", select the aggregation port to be deleted, click the <Batch Delete> icon, a confirmation box will be prompted whether to delete the aggregation port, click OK to delete the aggregation port, and the panel will be deleted after deletion The <aggregation port> becomes <optional port>.

Ports with ARP inspection function enabled, ports for ARP spoofing of important devices, ports with MAC VLAN function and monitoring ports in port mirroring cannot be added to the aggregation, and the panel displays as <unavailable port>, put the mouse on <unavailable port> It will prompt that these functions are enabled on the port and cannot be selected.

☆ Port mirroring

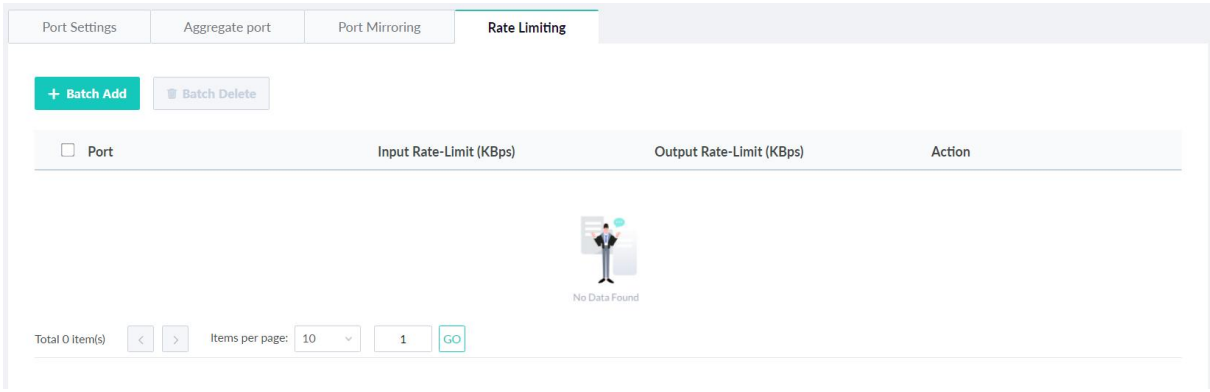


The port mirroring page is initialized to edit status, because multiple mirroring ports are allowed to be set on the web. There are two panels on the page. The port selected in the upper panel will be the source port (mirrored port, multiple selections are available), and only one port can be selected as the destination port (mirrored port) in the lower panel. After selecting or modifying the port on the panel, click the <Configuration Mirror> button to prompt "Setup successful!".

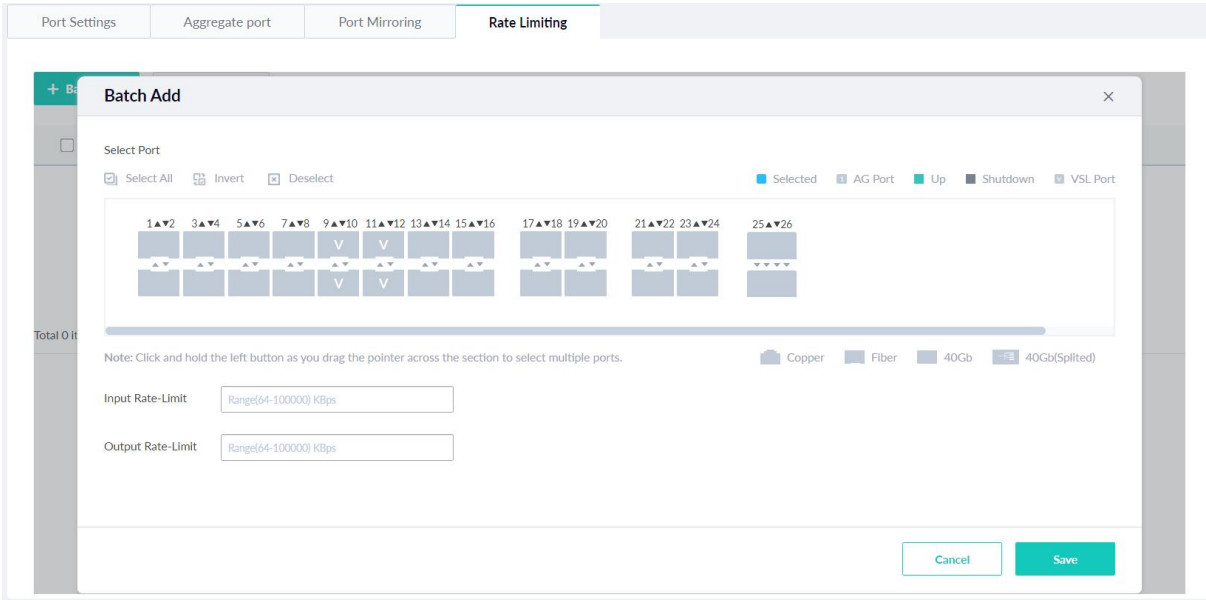
The current port mirroring status displayed on the panel is in the editing state. After the user has modified the port, but does not want to edit it, he can click the <Refresh> button to restore the panel to display the current port mirroring configuration status.

The member port that has been added to the aggregation port cannot be used as the destination port and source port, and the destination port and source port cannot be the same.

Port speed limit

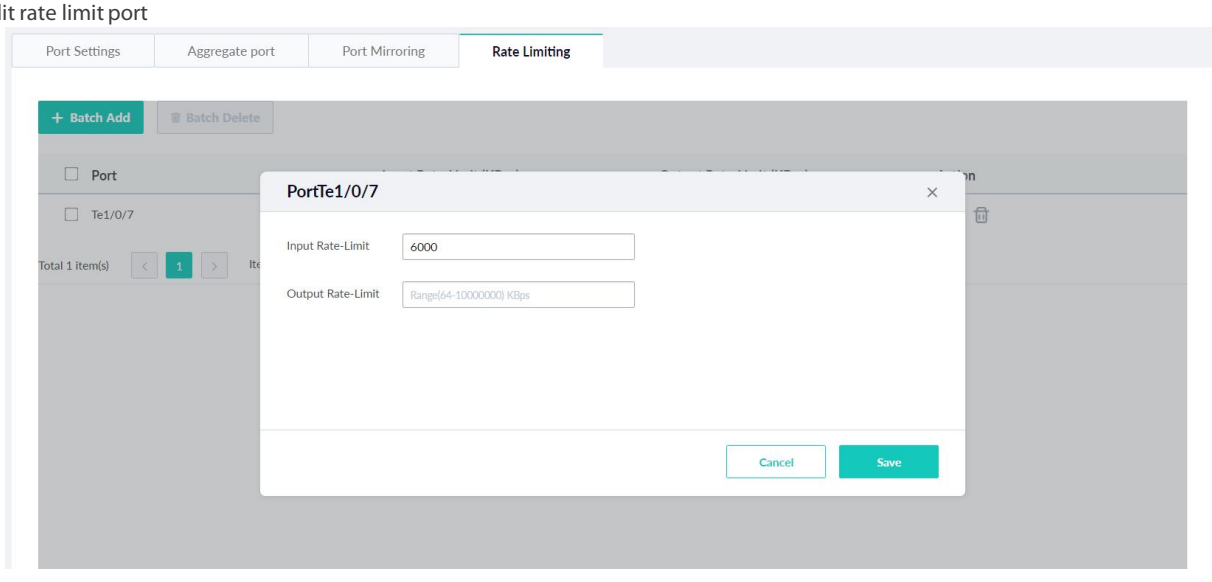


1.Add speed limit port



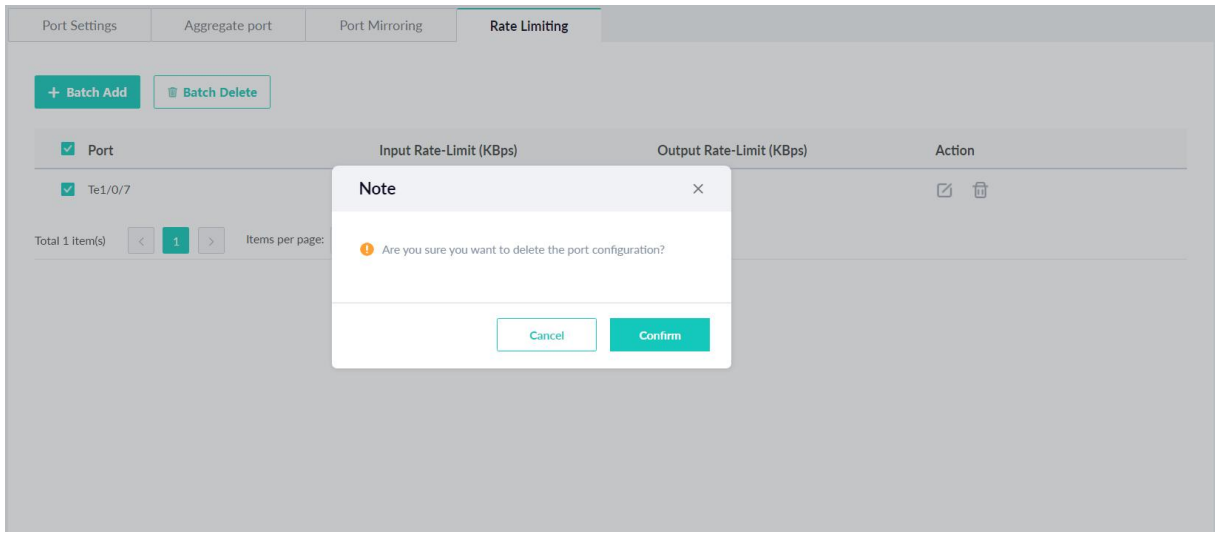
To set the speed limit port, you must fill in one of the input speed limit and output speed limit. Click "Save configuration" to prompt "Set successfully" and it will be displayed in the port speed limit list.

2.Edit rate limit port



Click the <Edit> icon under the operation column of the last column of "Port Speed Limit List", the page will display the port speed limit information, after editing the information, click <Save Configuration> to prompt "Setup successful".

3.Delete rate limit port



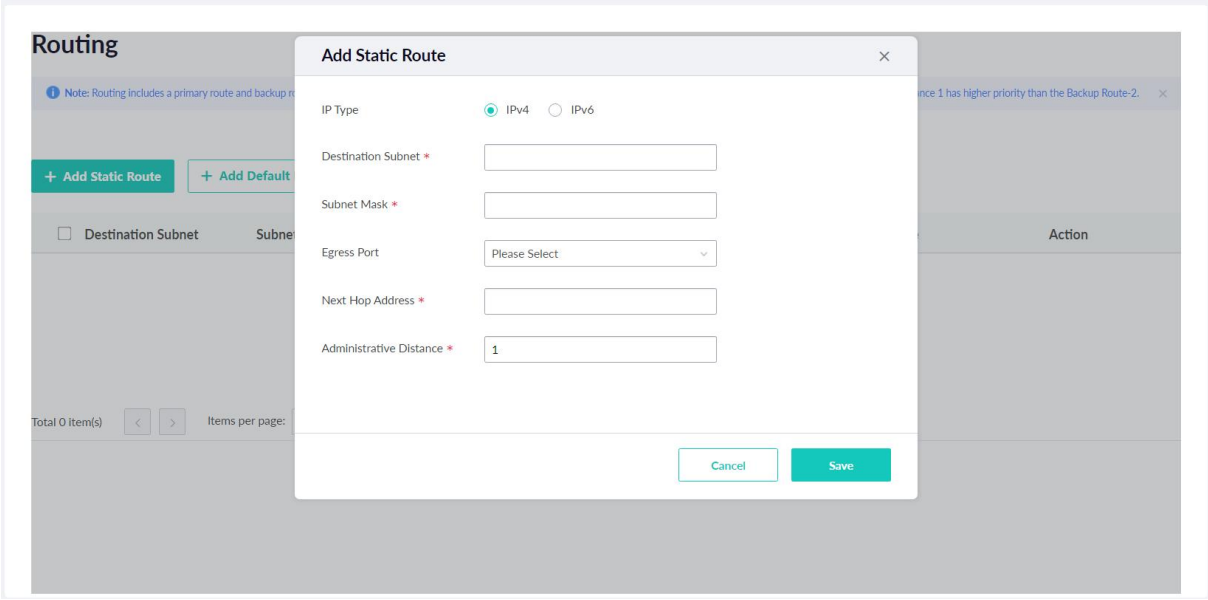
1) Select multiple records in the "Port Rate Limit List", and click "Delete Rate Limit Ports in Batch" to delete data in batches.

2) Click the <Delete> icon under the operation column of the last column of "Port Speed Limit List", and prompt "Are you sure to delete the selected port configuration?", click OK and prompt "Delete Successful" to complete the deletion.

Routing settings

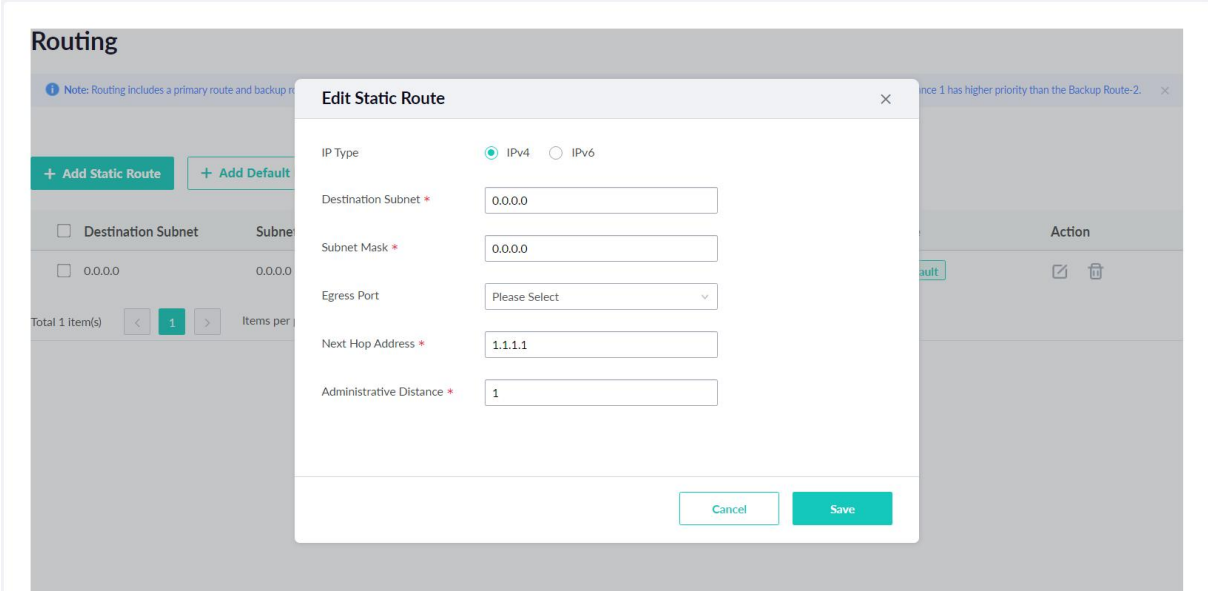
"Route Settings" can manage routing.

1.Add static route



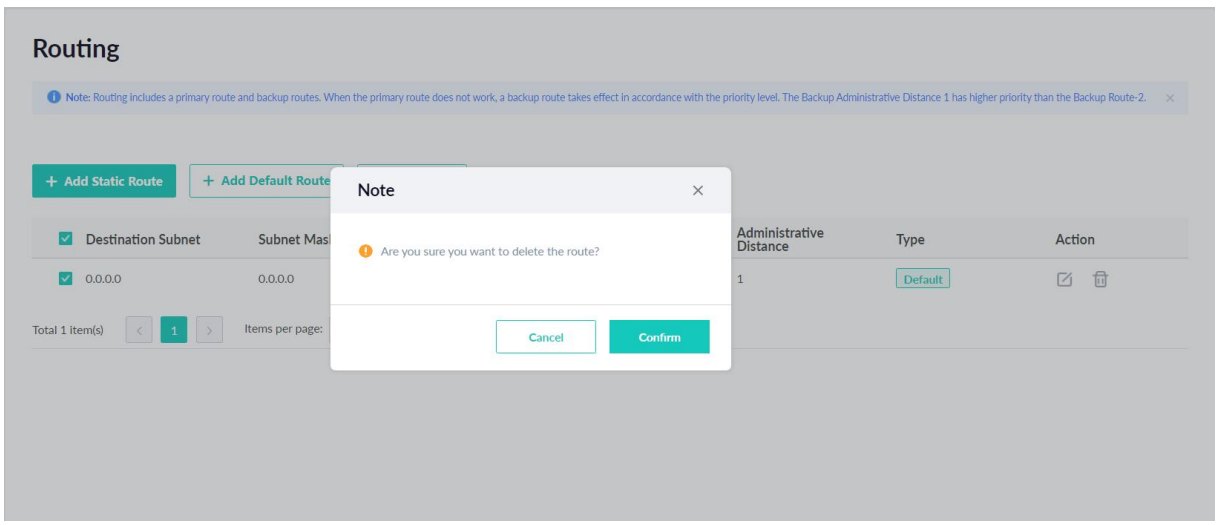
Set static route, select IP type, destination network segment, destination network segment mask and next hop address are require fields, click "Complete configuration" and prompt "Setup successful", it will be displayed in the routing list.

2. Edit routing



Click the <Edit> icon under the operation bar in the last column of "Route List", the page will display the information of the route, after editing the information, click <Complete Configuration> to prompt "Setup successful".

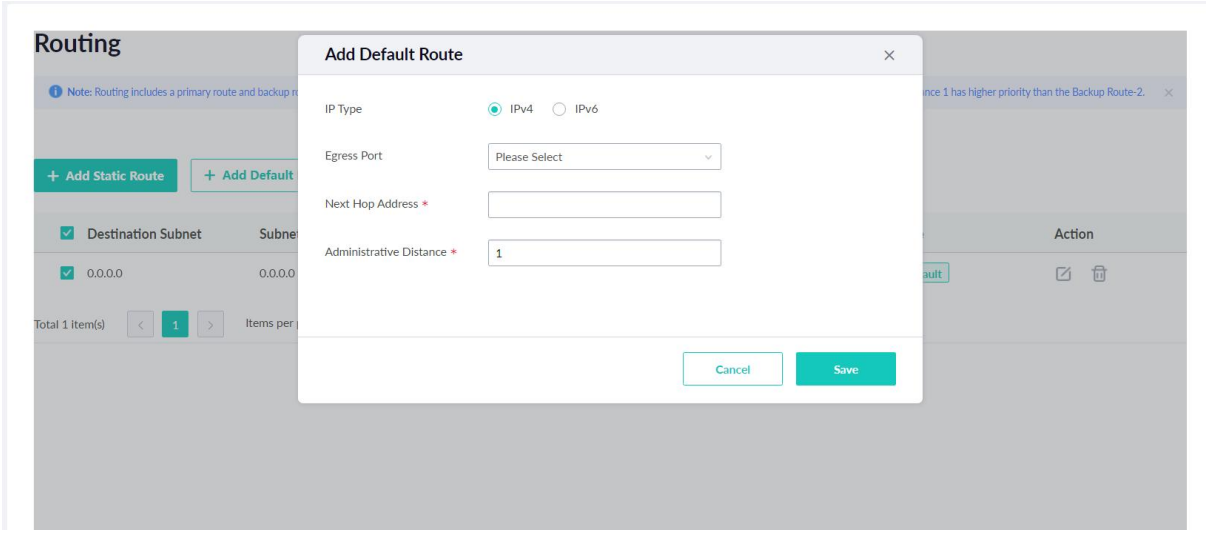
3. Delete route



1) Select multiple records in "Route List" and click "Delete Selected Route" to delete data in batches.

2) Click the <Delete> icon under the operation column of the last column of "Route List", and prompt "OK to delete?", click OK and prompt "Delete successfully" to complete the deletion.

4. Add default route



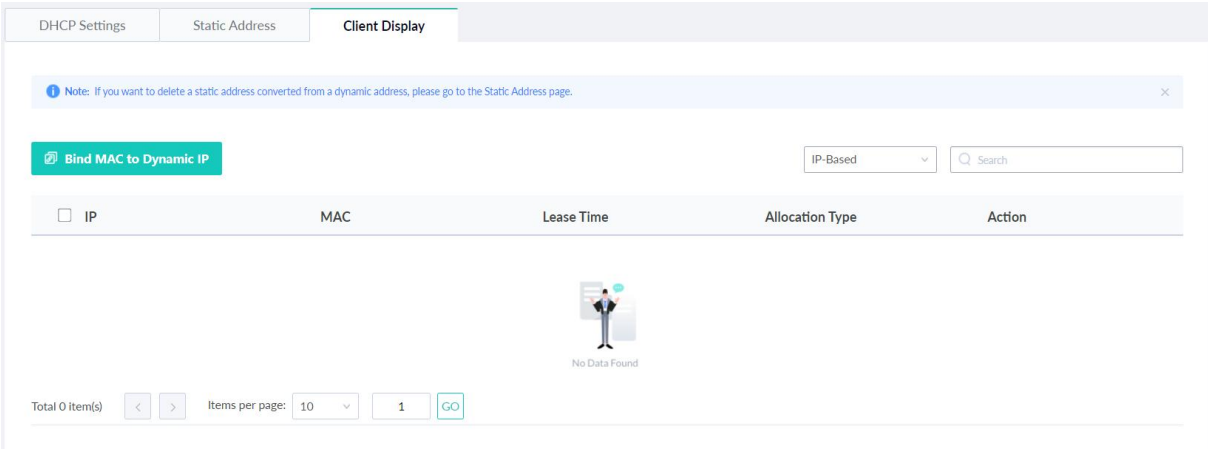
Set the default route, select the IP type, the next hop address is a required field, click "complete configuration" to prompt "setup successful", it will be displayed in the routing list.

Route selection is divided into main route and backup route. When the main route fails to take effect, the backup route will be used. The backup route follows the configured priority. The priority of backup route 1 is higher than the priority of backup route 2.

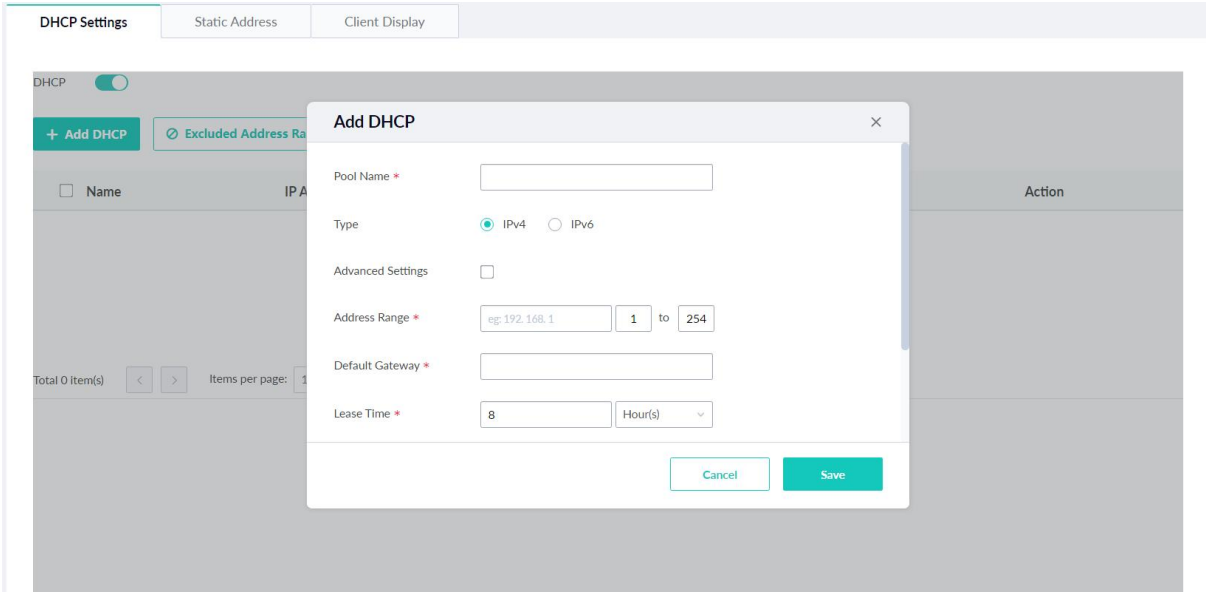
DHCP server

"DHCP server" can perform DHCP configuration, static address assignment and client list.

DHCP configuration

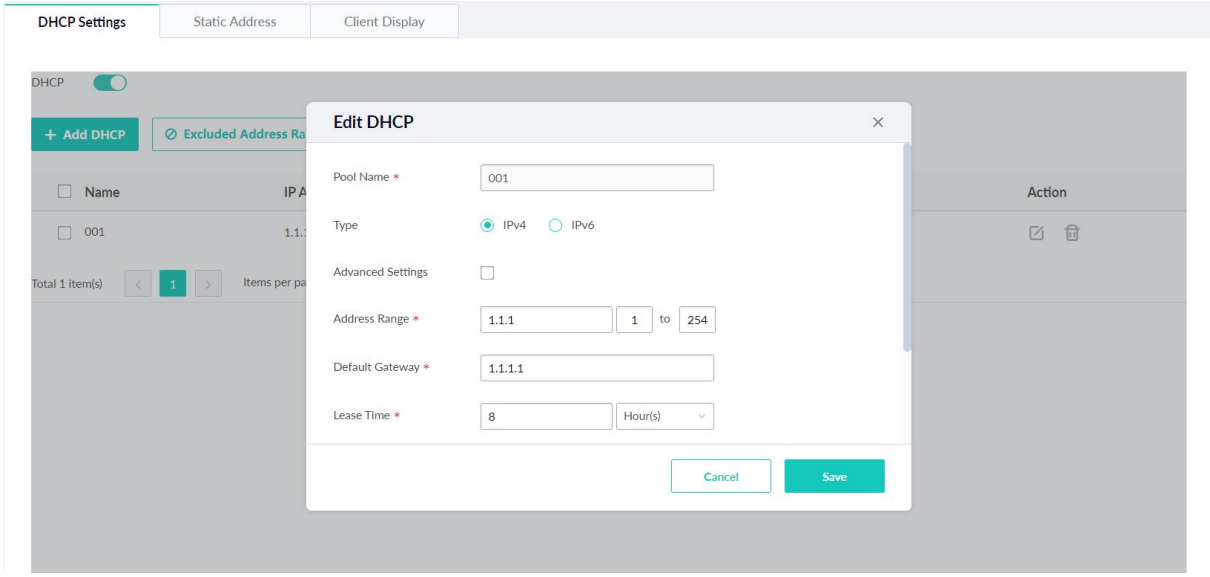


1.Add DHCP



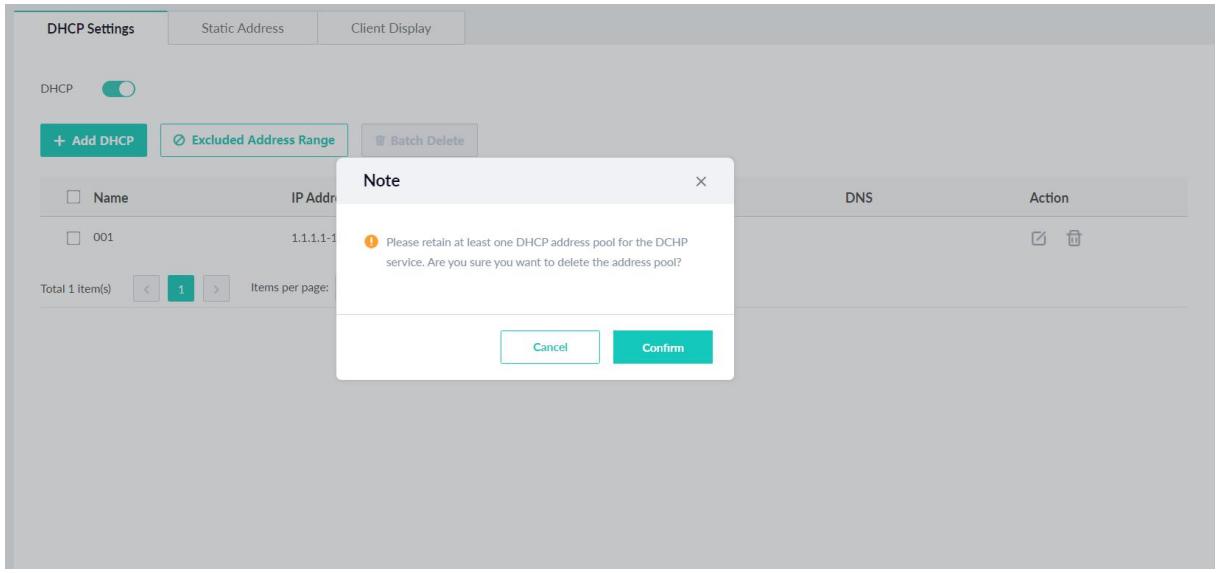
Set the address pool name, IP allocation network segment, mask, default gateway, and lease time, and click "Complete configuration" to prompt "Setup successful", it will be displayed in the DHCP list.

2.Edit DHCP



Click the <Edit> icon under the operation column of the last column of "DHCP List", the page will display the DHCP information, after editing the information, click <Complete Configuration> to prompt "Setup successful".

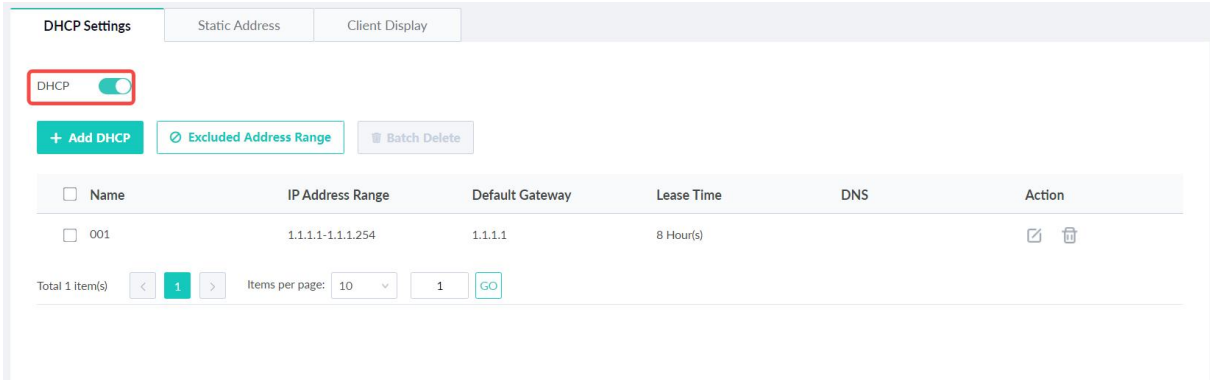
3.Remove DHCP



1) Select multiple records in the "DHCP List" and click "Delete Selected DHCP" to delete data in batches.

2) Click the <Delete> icon under the operation column of the last column of "DHCP List", and prompt "Are you sure to delete the selected DHCP?", click OK and prompt "Delete successfully" to complete the deletion.

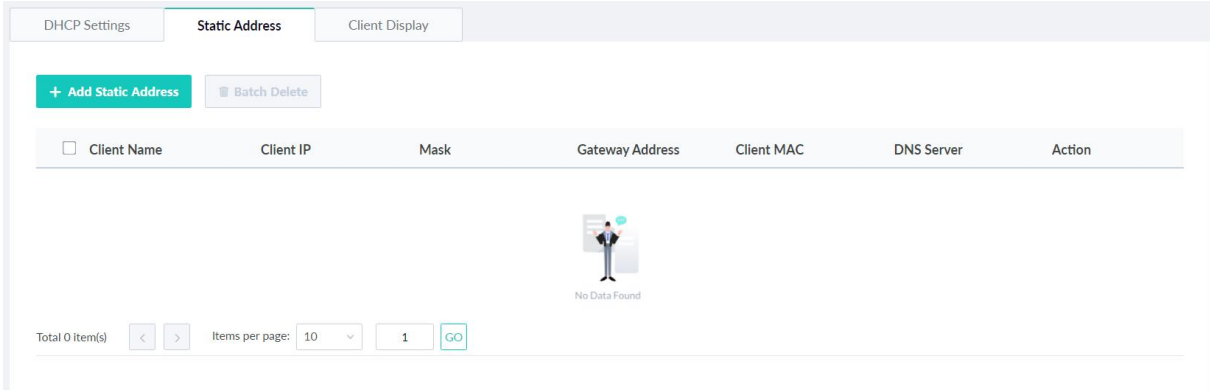
4.Turn on DHCP



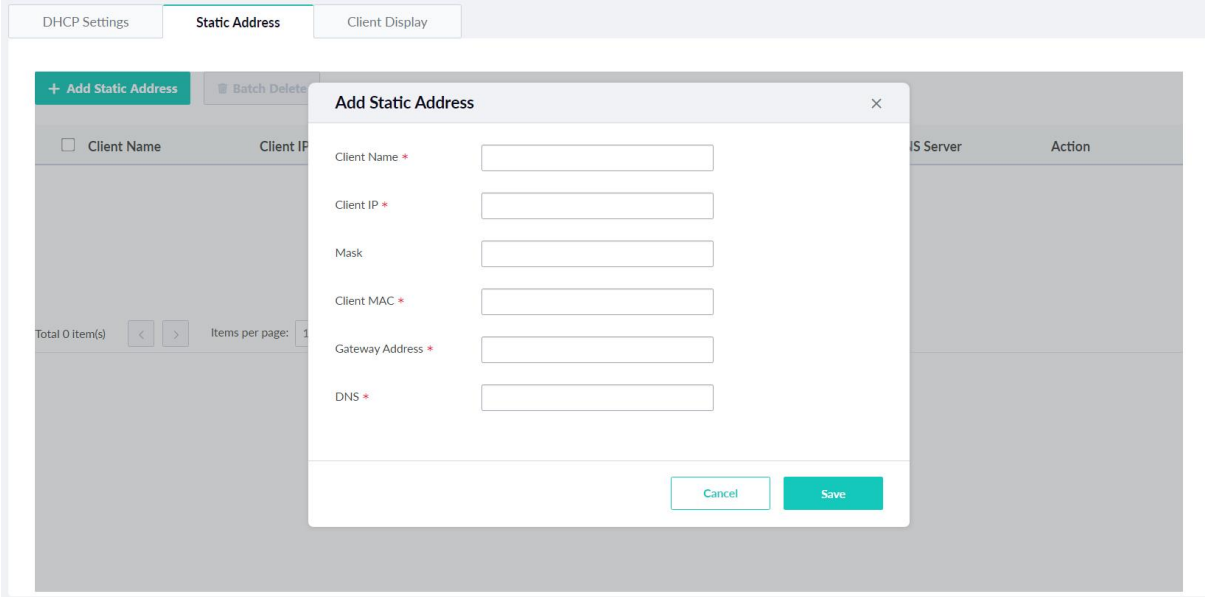
Click <DHCP Service Switch> to enable DHCP service.

☆ Static address allocation

The static address allocation page is as follows:

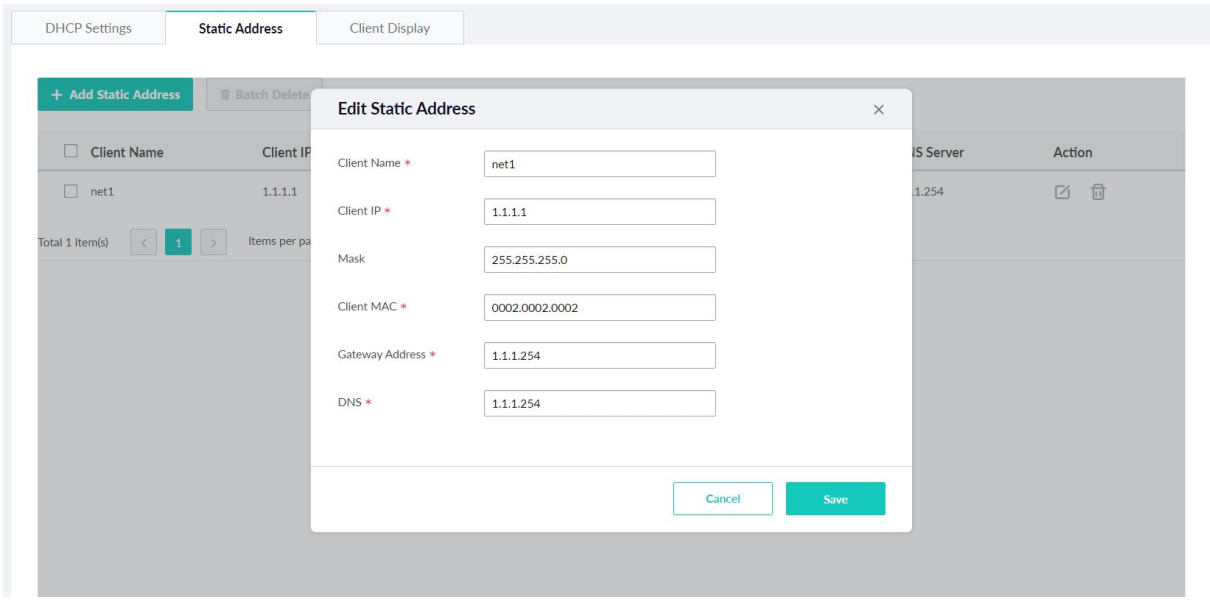


1.Add static address



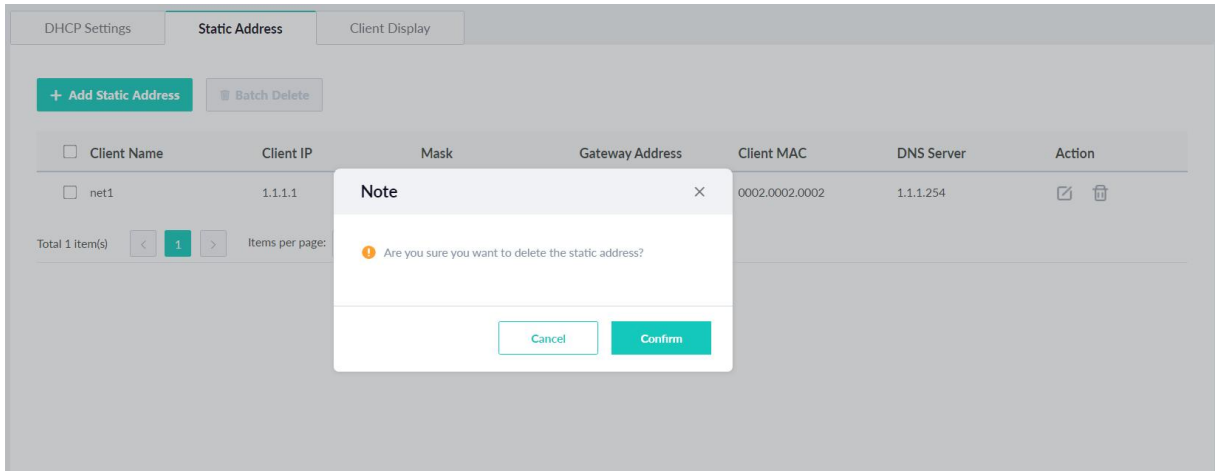
Set the client name, client IP, and client MAC address are mandatory, other configurations are optional, click "complete configuration" to prompt "setup successful", it will be displayed in the static address list.

2.Edit static address



Click the <Edit> icon under the operation column of the last column of "Static Address List", the page will display the information of the static address. After editing the information, click <Complete Configuration> to prompt "Setup successful".

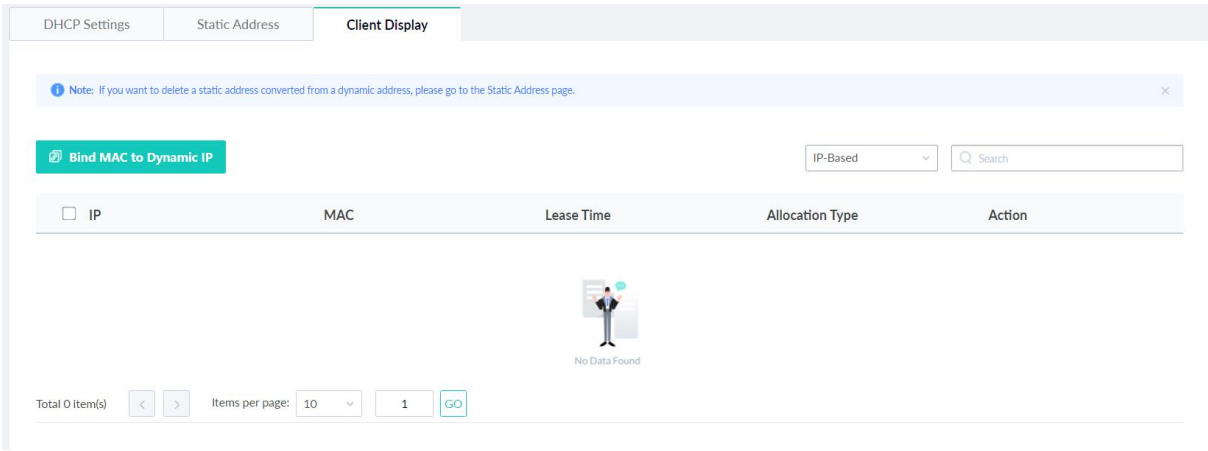
3.Delete static address



1) Select multiple records in the "Static Address List" and click "Delete Selected Address" to delete data in batches.

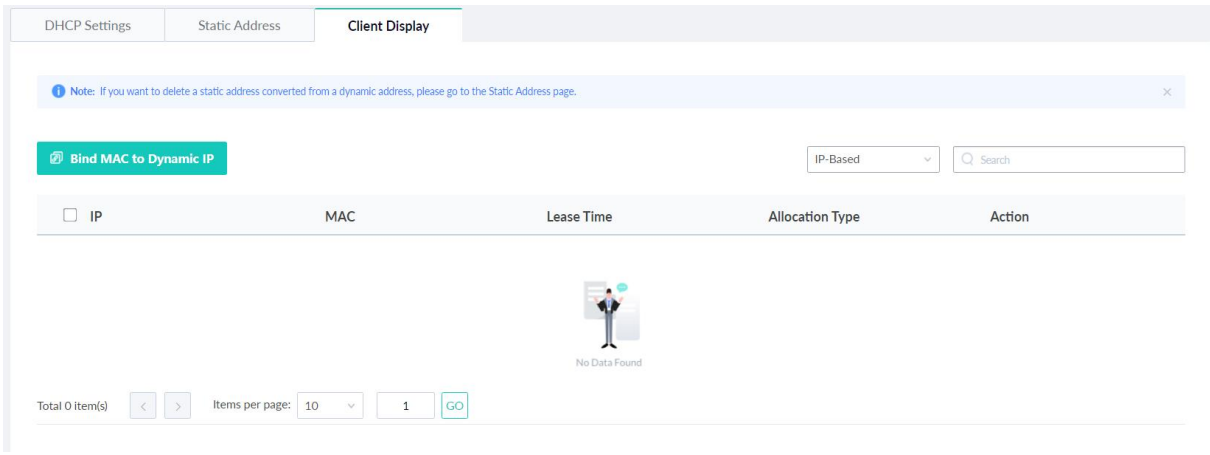
2) Click the <Delete> icon in the operation column of the last column of "Static Address List", and prompt "Are you sure to delete this static address?", click OK and prompt "Delete successfully" to complete the deletion.

☆ Client list



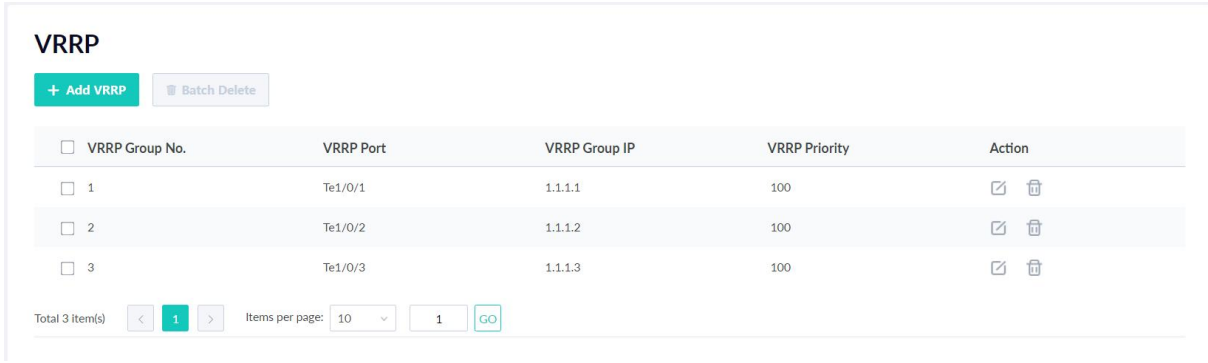
The client list page is as follows:

1.Query IP address

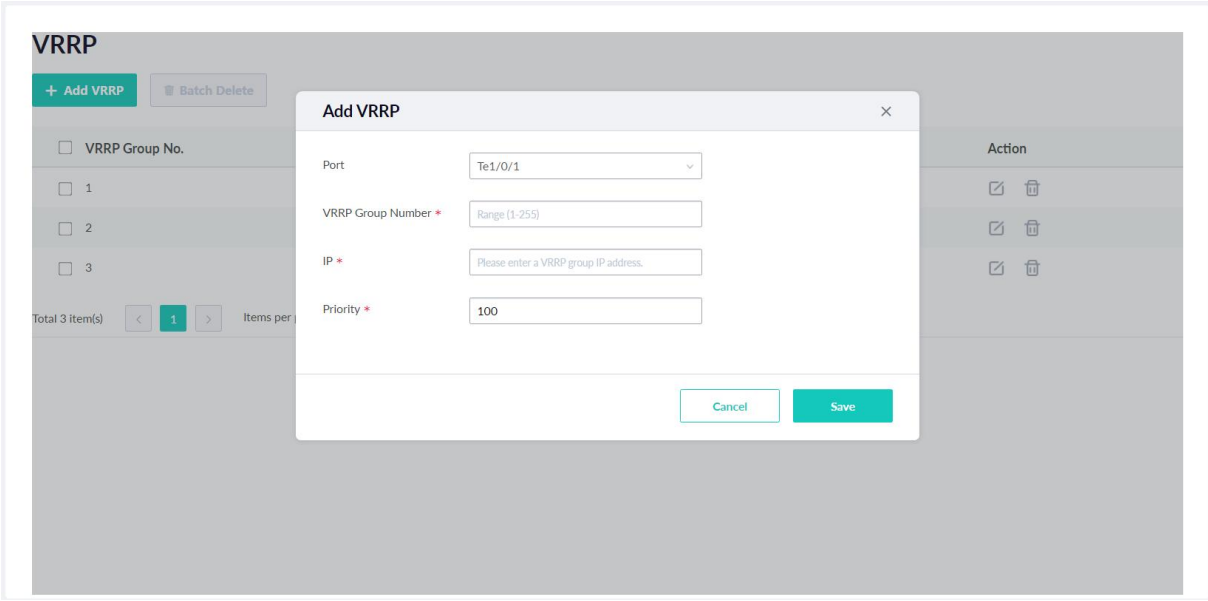


Enter the IP address in the search box to query.

VRRP configuration

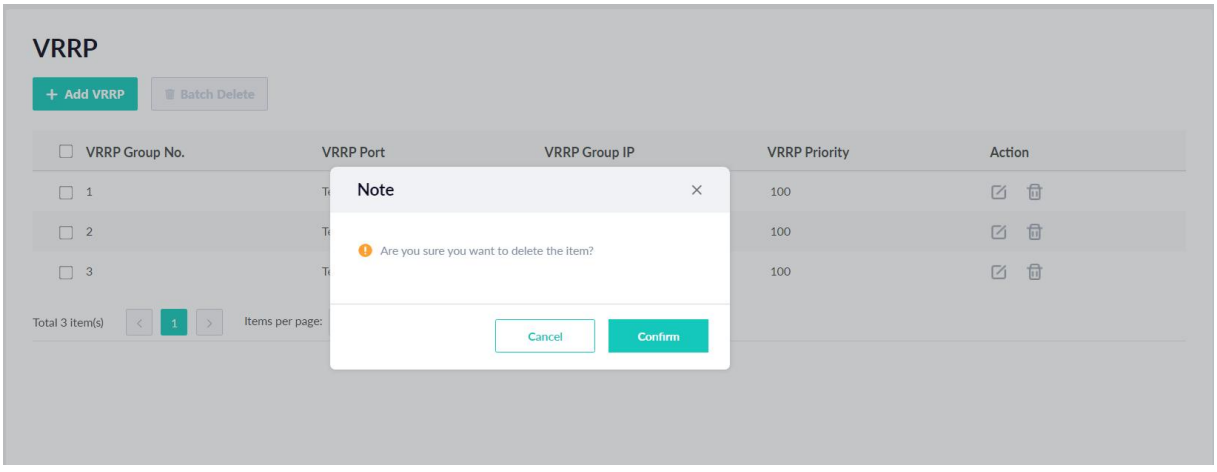


1.Add VRRP



Set the VRRP interface, VRRP group number, and VRRP group IP are mandatory, and other configurations are optional. Click "Complete Configuration" and prompt "Setup Successfully" and it will be displayed in the VRRP list.

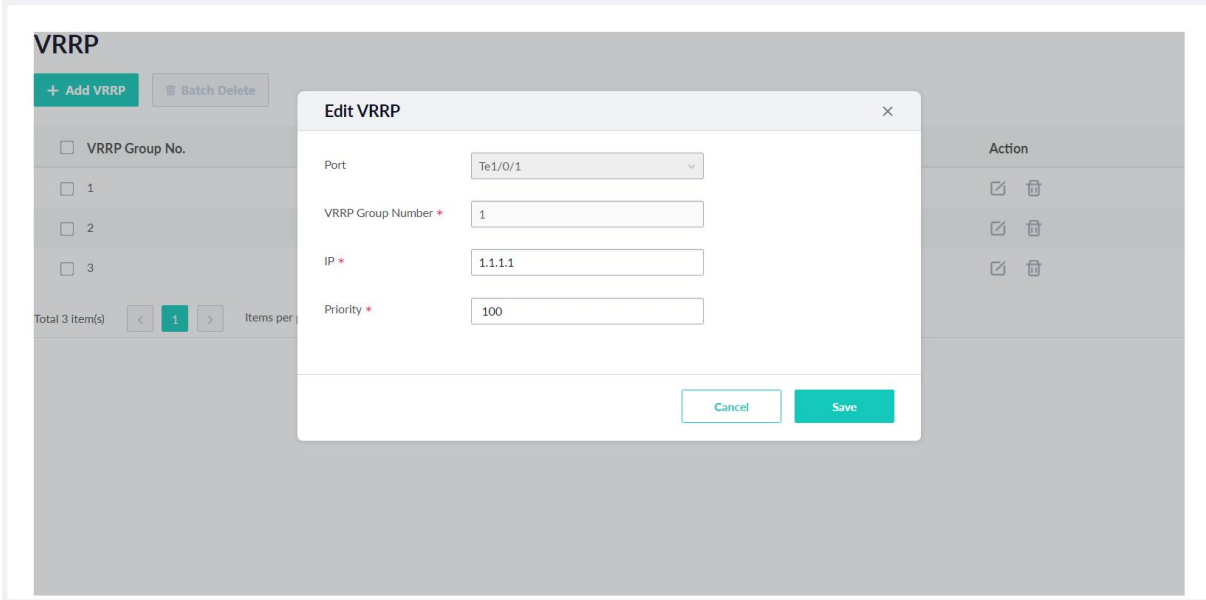
2.Delete VRRP in batches



1) Select multiple records in the "VRRP list" and click "Delete selected VRRP" to delete the data in batches.

2) Click the <Delete> icon under the operation column of the last column of "VRRP List", and prompt "Are you sure you want to delete?", click OK and prompt "Delete successful" to complete the deletion.

3.Edit VRRP

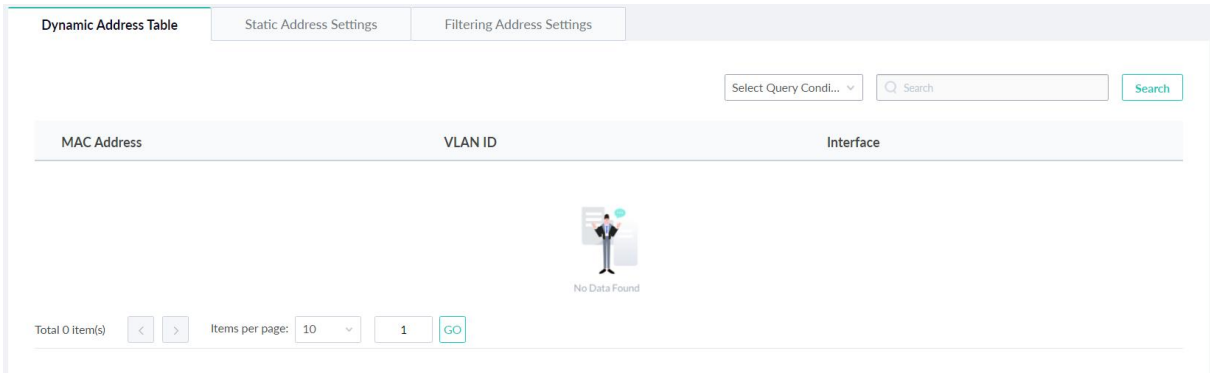


Click the <Edit> icon under the operation column of the last column of "VRRP List", the page will display the VRRP information, after editing the information, click <Complete Configuration> to prompt "Setup successful".

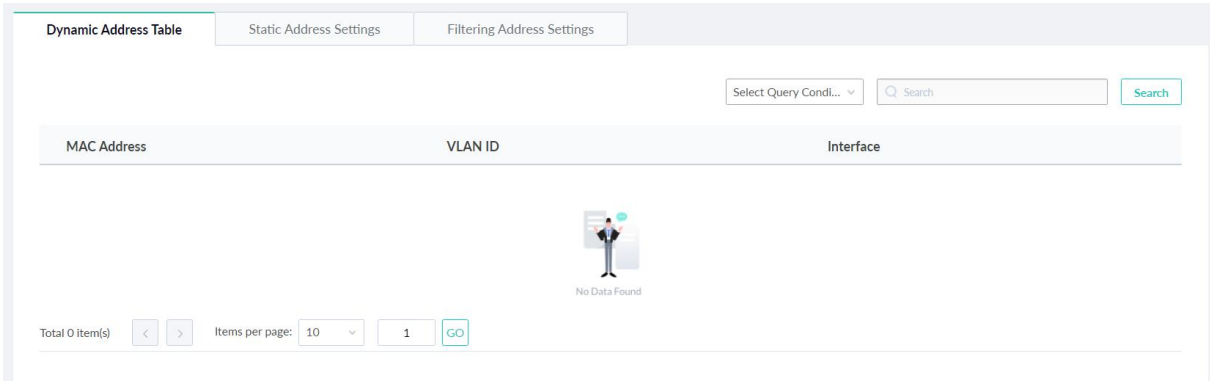
MAC address

The MAC address management page contains three parts: "Dynamic Address Table", "Static Address Setting" and "Filtering Address Setting".

☆ **Dynamic address table**



1.Query dynamic addresses according to conditions



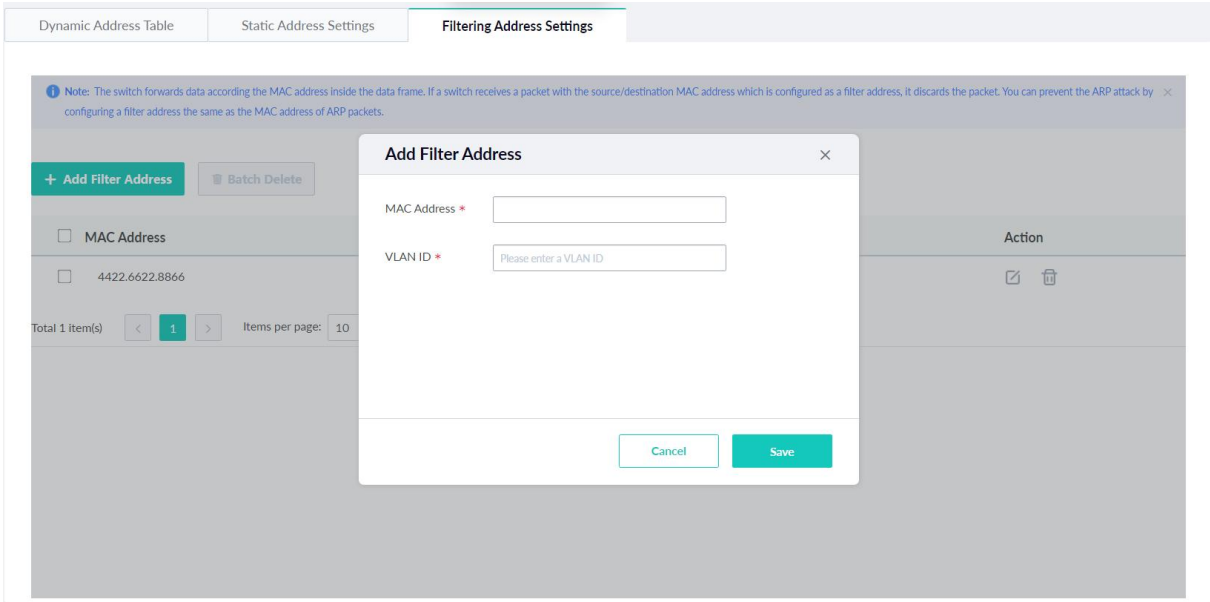
Query by MAC, Query by VLAN, Query by interface

1) Select multiple records in the "Static Address List" and click "Delete Selected Static Address" to delete data in batches.

2) Click the <Delete> icon under the operation column of the last column of "Static Address List", and prompt "OK to delete the selected static address", click OK and prompt "Delete Successfully" to complete the deletion.

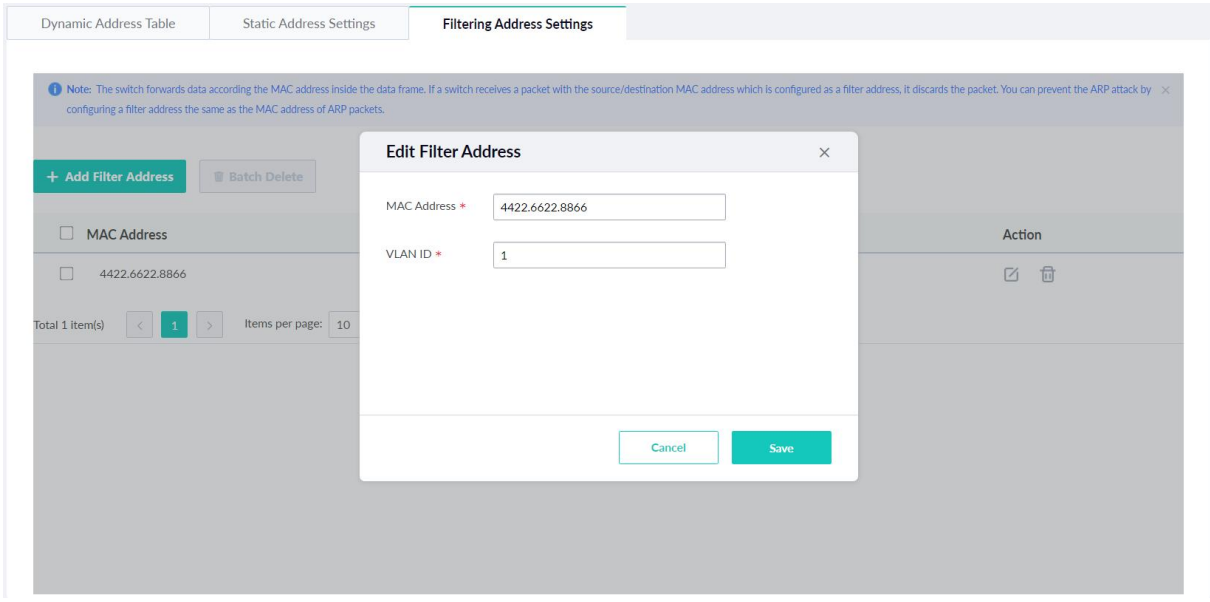
☆ Filter address settings

1.Add filter address



To set the filter address, you must fill in the MAC address and VLAN ID, click "Save Configuration" and prompt "Setup Successfully", it will be displayed in the static address list.

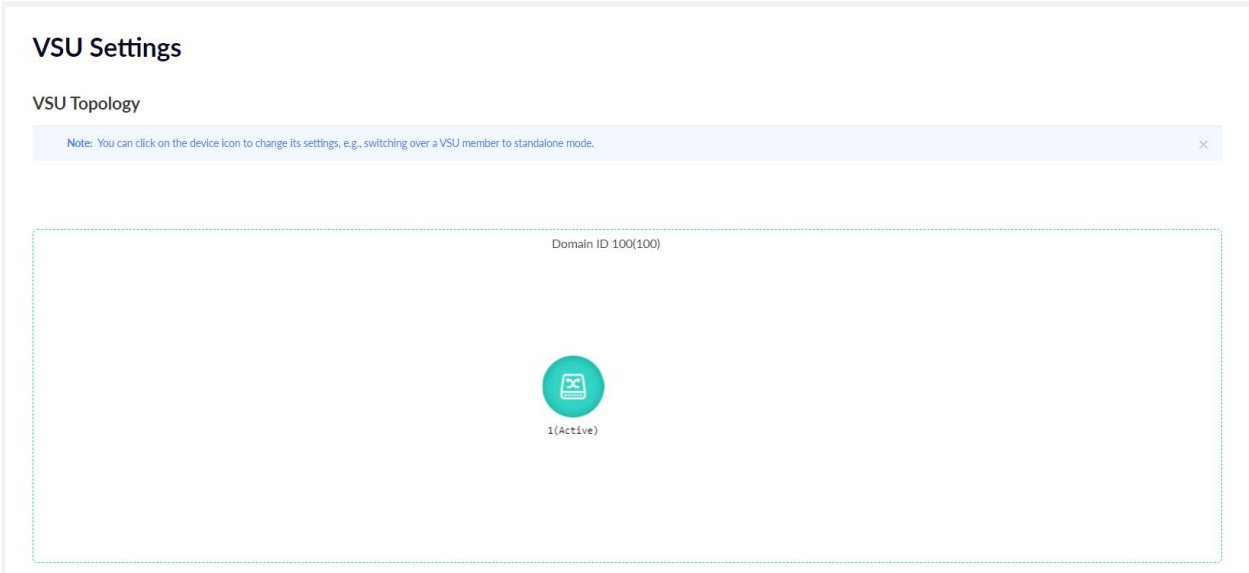
2.Edit filter address

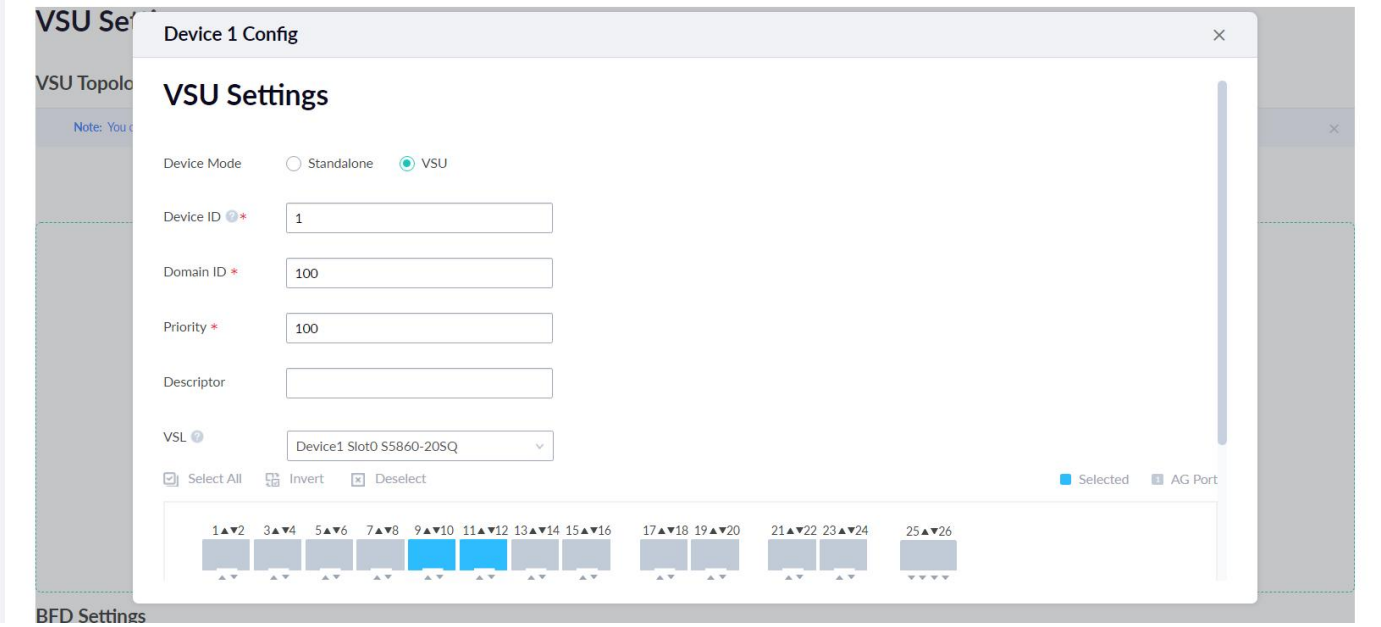


Click the <Edit> icon under the operation column of the last column of "Filtered Address List", the page will display the information of the filtered address, after editing the information, click <Save Configuration> to prompt "Setup successful".

☆ VSU mode

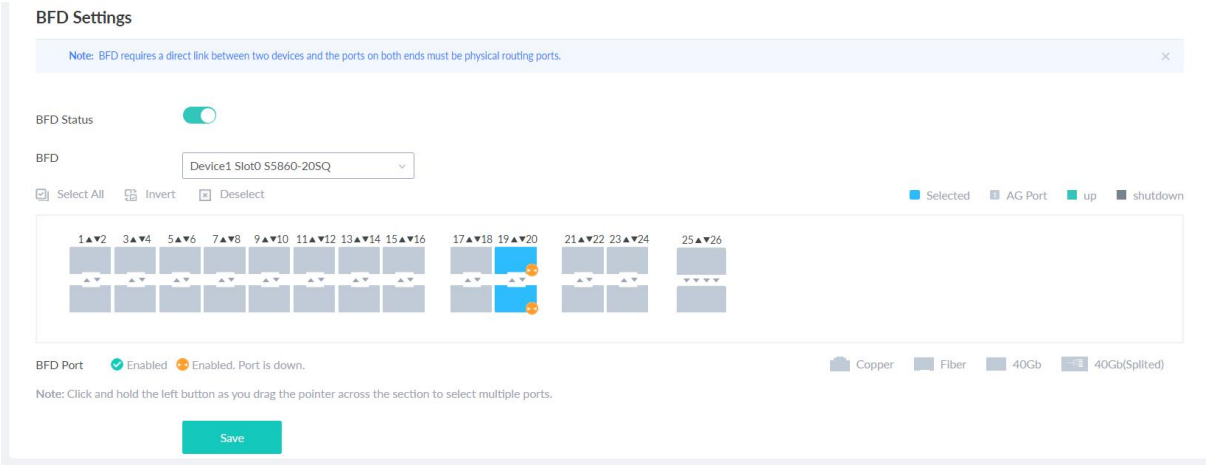
The Stacking mode page is as follows:





Click the icon to configure a single device, switch device mode, revise device ID, domain ID, priority, device description and VSL port.

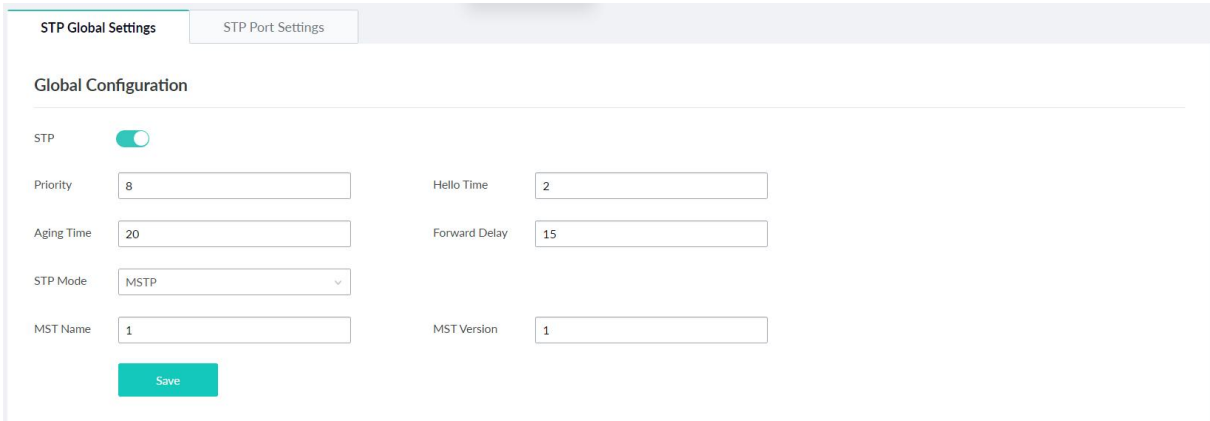
Dual host detection in stacking scenario



Spanning Tree Protocol

"Spanning Tree Protocol" can set the global parameters of the spanning tree and the port settings of the spanning tree.

☆ Spanning tree global settings

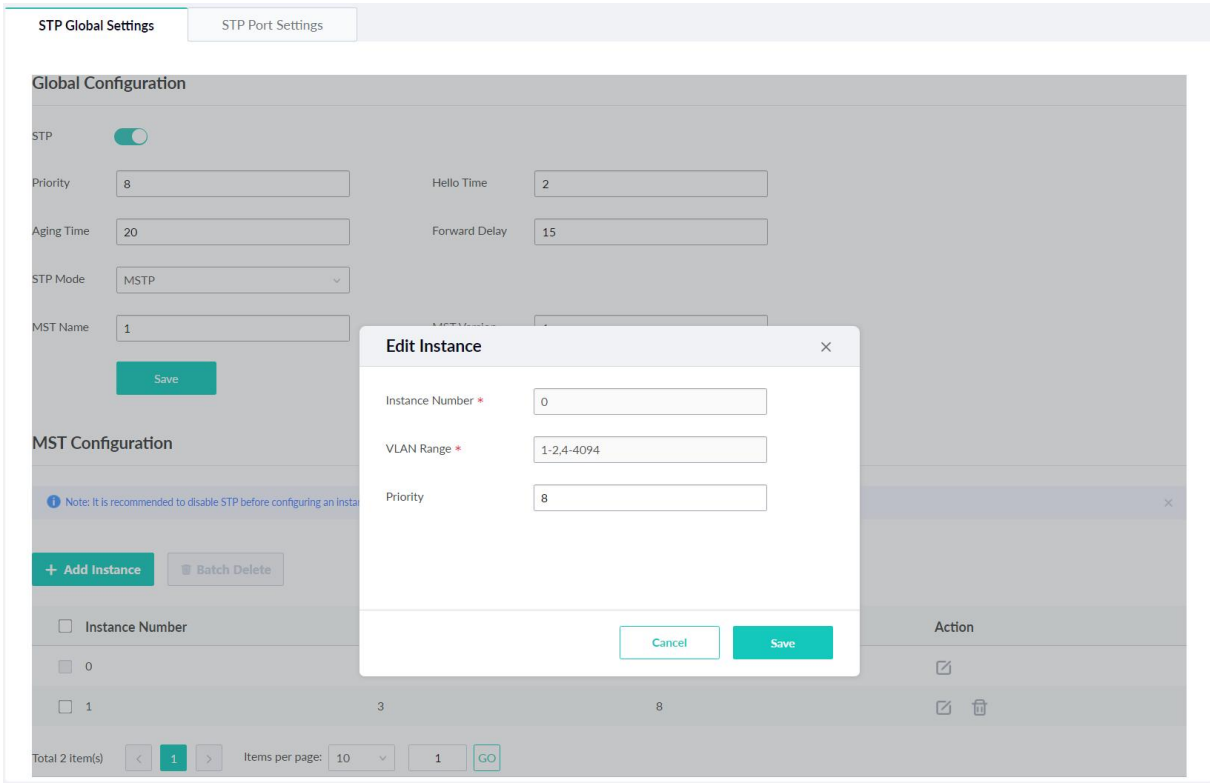


The global parameters of the spanning tree can be configured. When the spanning tree mode is selected as "MSTP", the MST instance can be set.

1. Add instance

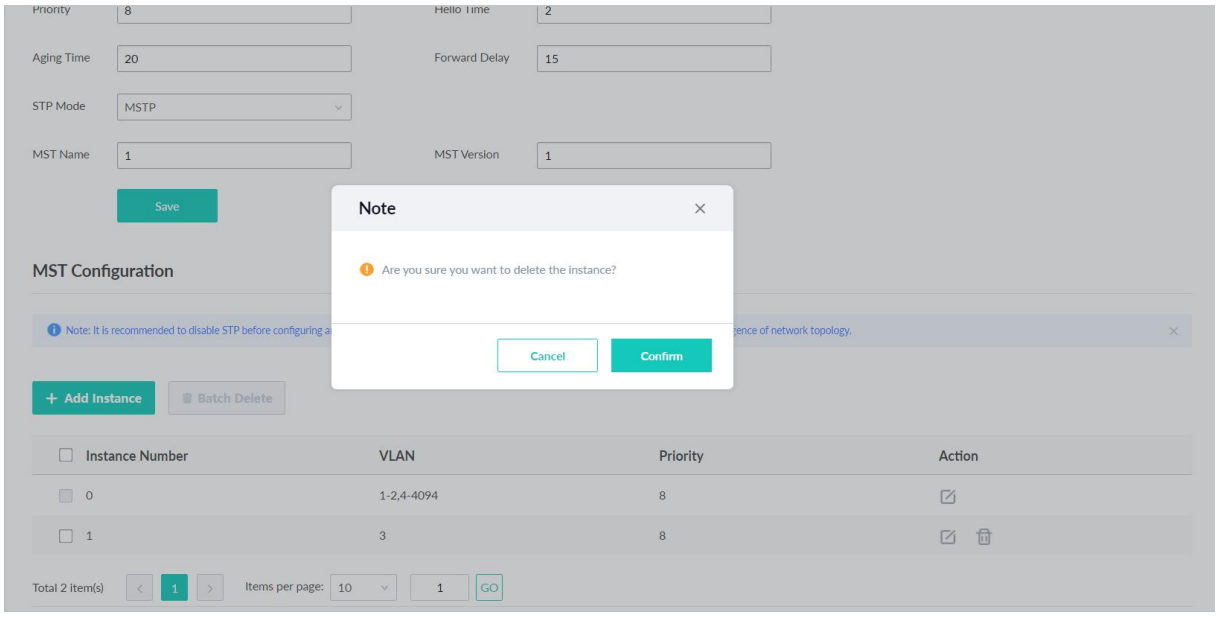
To set an instance, you must fill in the instance value and VLAN range, and other information is optional. After clicking "Complete Configuration" and prompting "Setup Successful", it will be displayed in the instance list.

2.Edit example



Click the <Edit> icon under the operation column of the last column of "Instance List", the page will display the information of the instance, after editing the information, click <Complete Configuration> to prompt "Setup Successful".

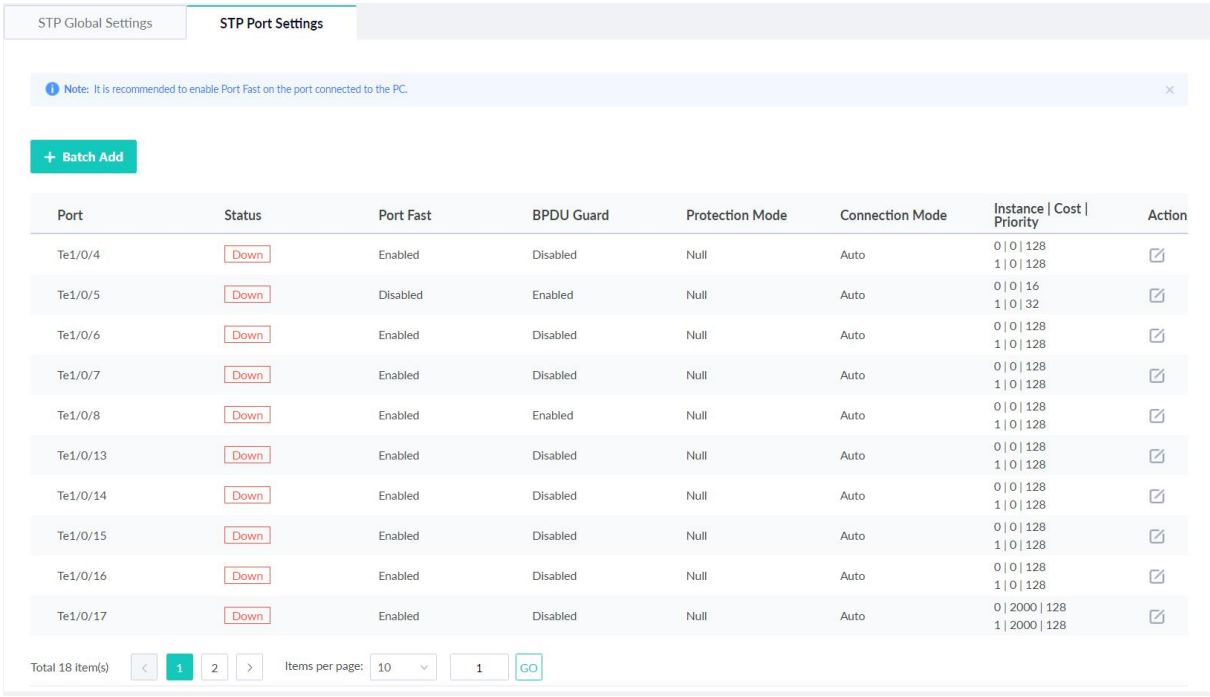
3.Delete instance



1) Select multiple records in the "Instance List" and click "Delete Selected Instances" to delete data in batches.

2) Select and click the <Delete> icon under the operation column of the last column of "Instance List", and prompt "Are you sure to delete the selected instance?", click OK and prompt "Delete successfully" to complete the deletion. Instance 0 is the default instance that cannot be deleted.

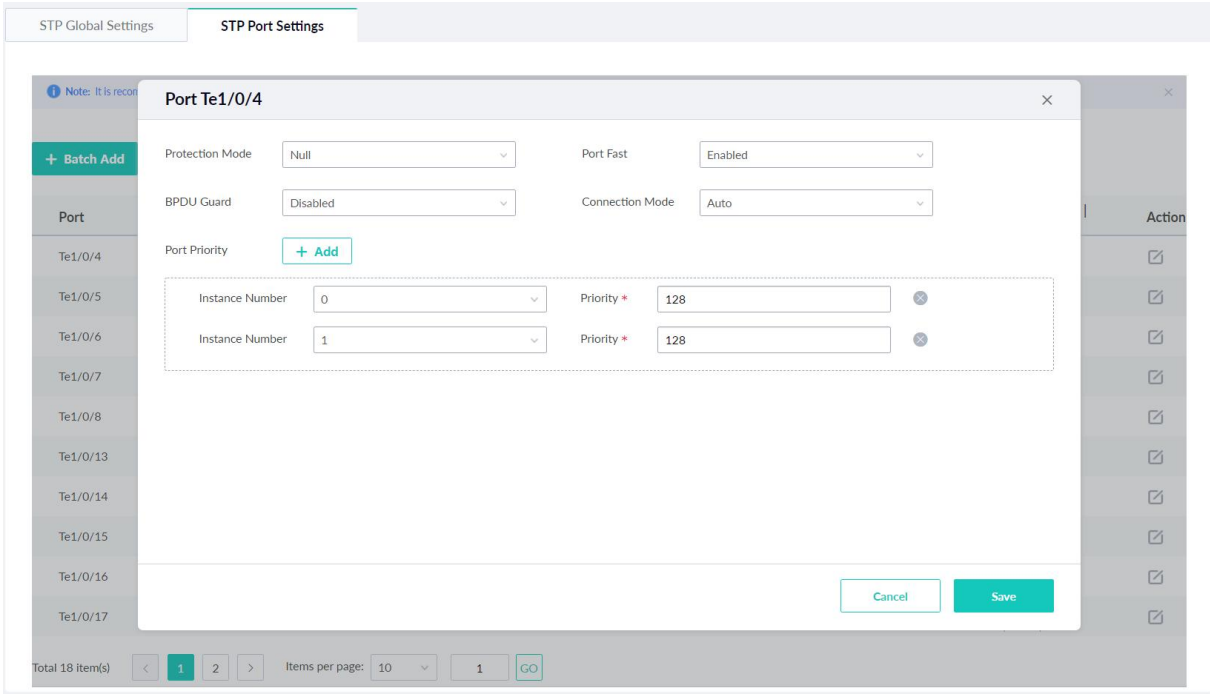
Spanning tree port settings



1. Batch settings

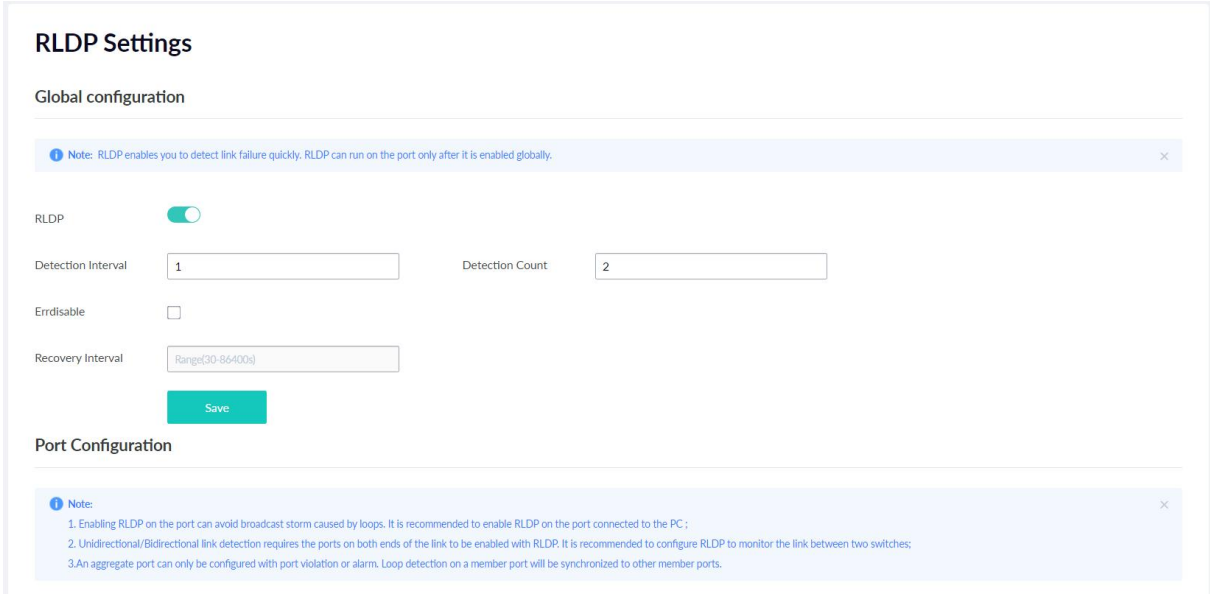
Select the protection mode, Port Fast, BPDU filter, connection type, port priority, etc., and select the port for batch setting.

2.Edit settings

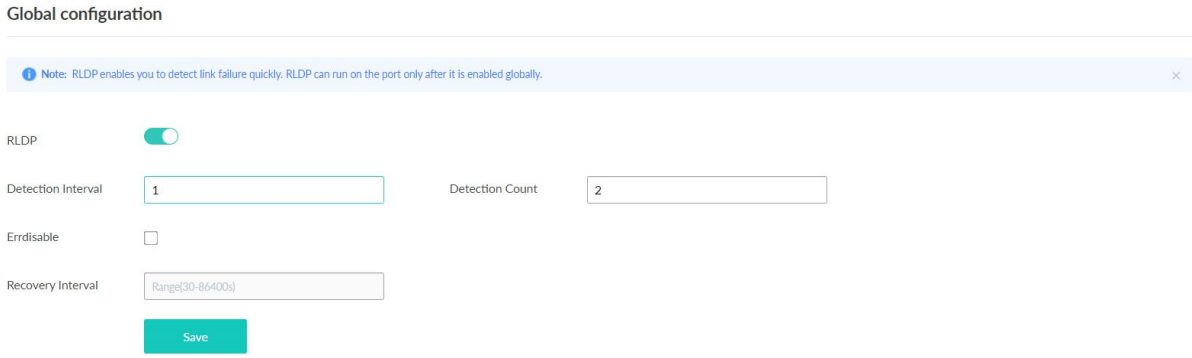


In the "Spanning Tree Port List", the <Edit> icon under the operation column of the last column will display the information of the port on the page. After editing the information, click <Complete Configuration> to prompt "Setup successful".

RLDP settings



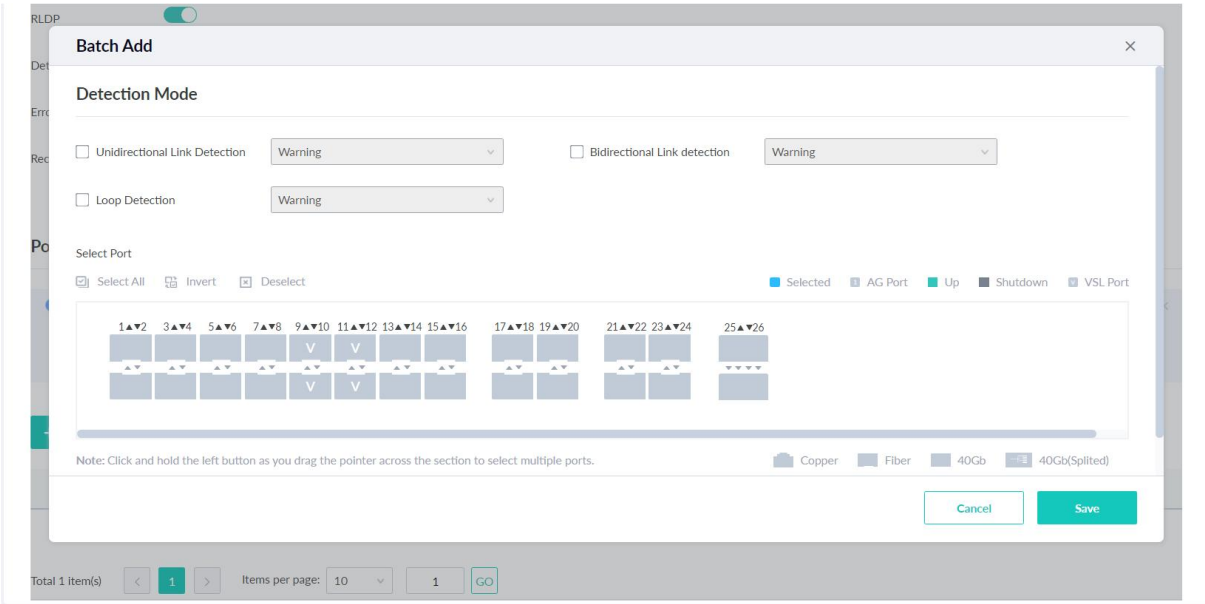
1. RLDP global settings



Click the RLDP switch button to enable or disable the RLDP function. Configure the detection interval, detection times and recovery period when it is turned on, and click the <Save Settings> button to prompt "Setup successful"

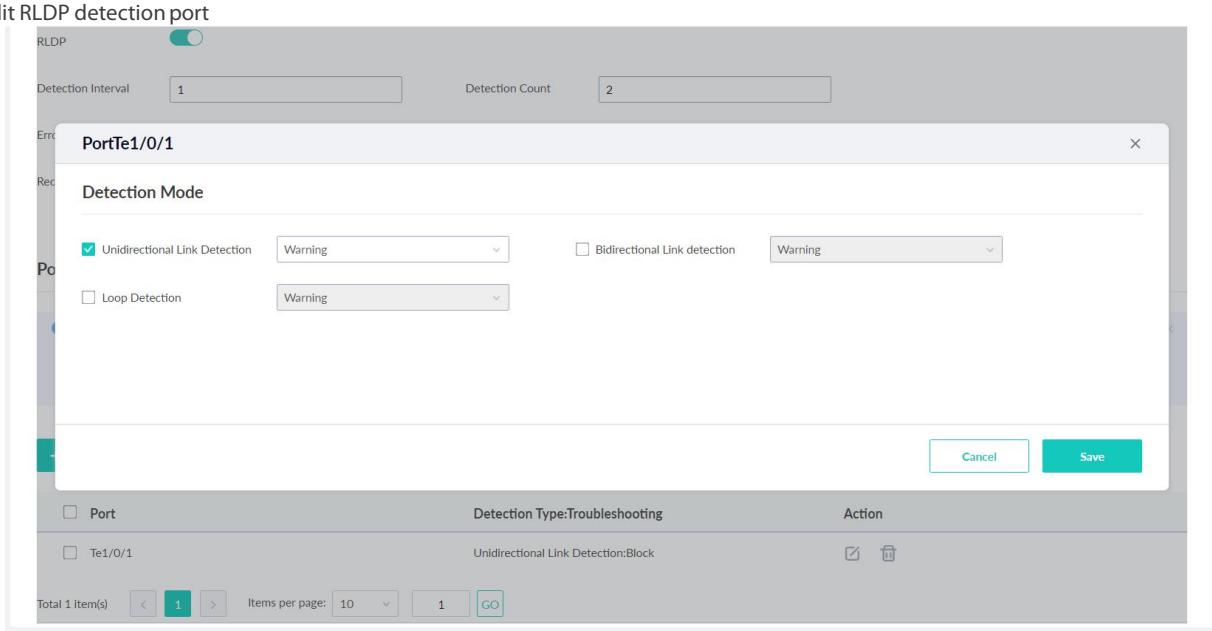
2. Port RLDP settings

3. Add RLDP detection port



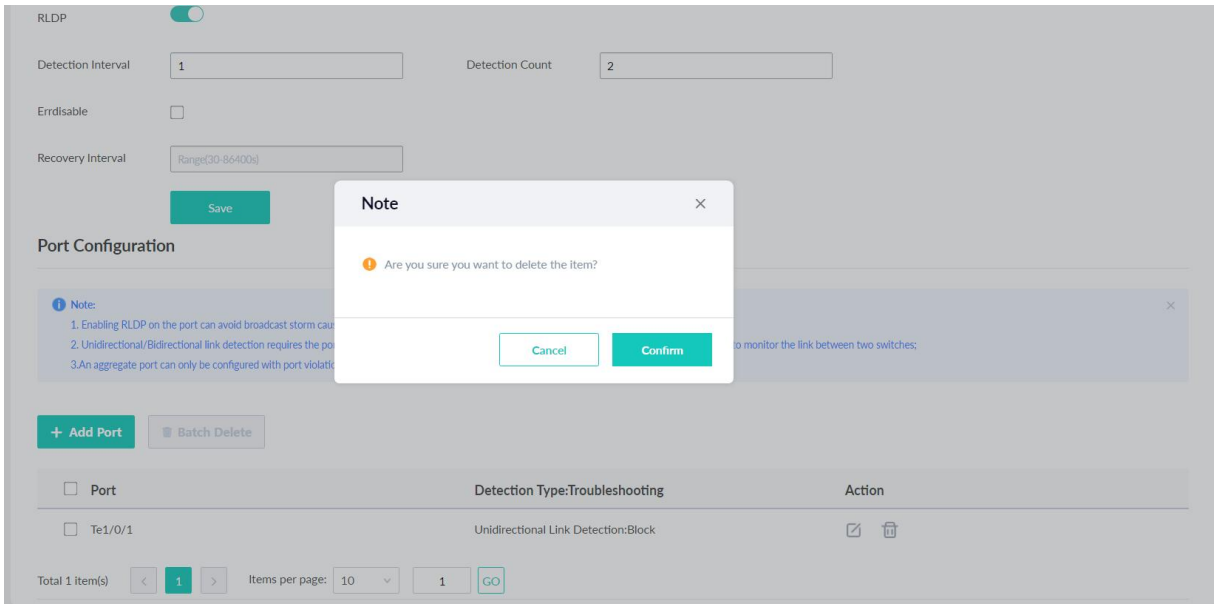
Select "Detection Type", "Troubleshooting" and the port and then press "Add Setting", it prompts "Set successfully" to complete the RLDP detection port addition operation. After successful addition, it will be displayed in "RLDP Detection PortList".

4. Edit RLDP detection port



Click the <Edit> icon under the operation column of the last column of "RLDP Detection Port List", the page will display the information of the RLDP detection port. After editing the information, click <Complete Configuration> to prompt "Setup successful".

5. Delete RLDP detection port



1) Select multiple records in the "RLDP detection port list" and click "Delete RLDP detection ports in batch" to delete data in batches.

2) Click the <Delete> icon under the operation column of the last column of "RLDP Detection Port List", and prompt "Are you sure to delete the selected data?", click OK and prompt "Delete successfully" to complete the deletion.

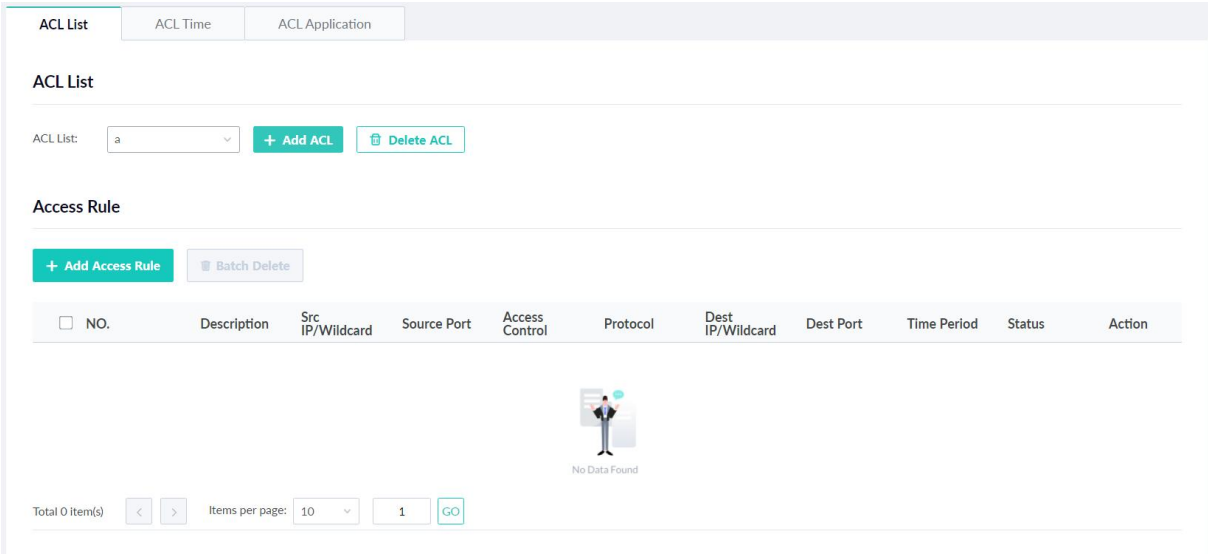
Safety

ACL

Input ACL When the device interface receives a packet, check whether the packet matches an ACE of the interface's input ACL; output ACL When the device is ready to output a packet from an interface, check whether the packet matches the interface output ACL Match one of the ACEs.

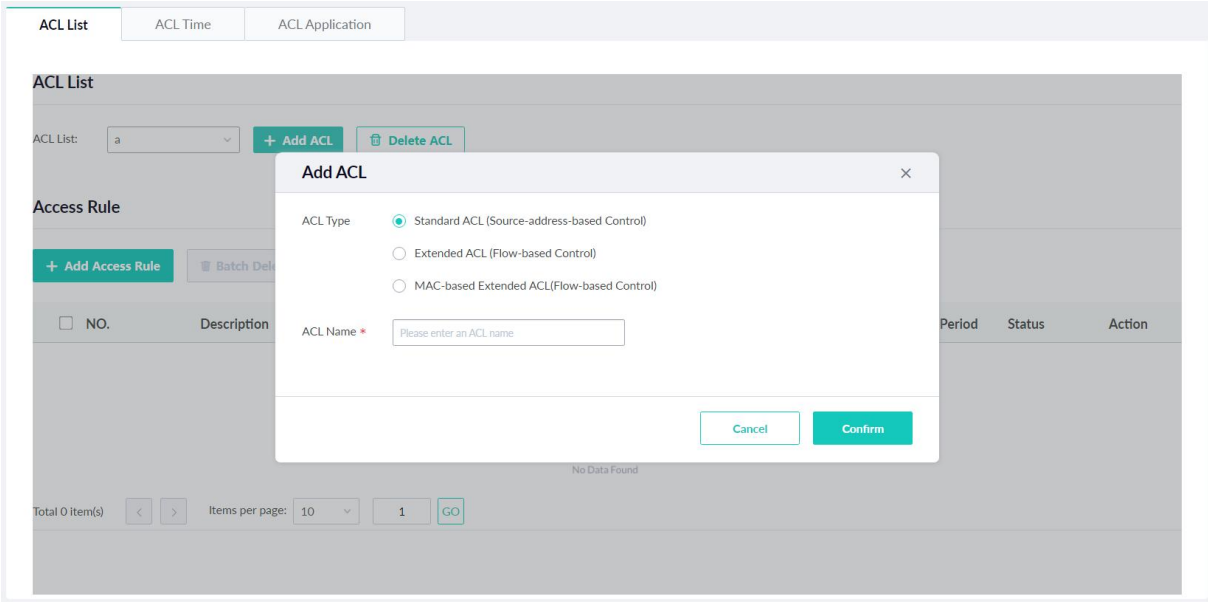
When formulating different filtering rules, multiple rules may be applied at the same time, or only a few of them may be applied. As long as it conforms to a certain ACE, the packet (Permit or Deny) is processed according to the ACE definition.

☆ ACL list



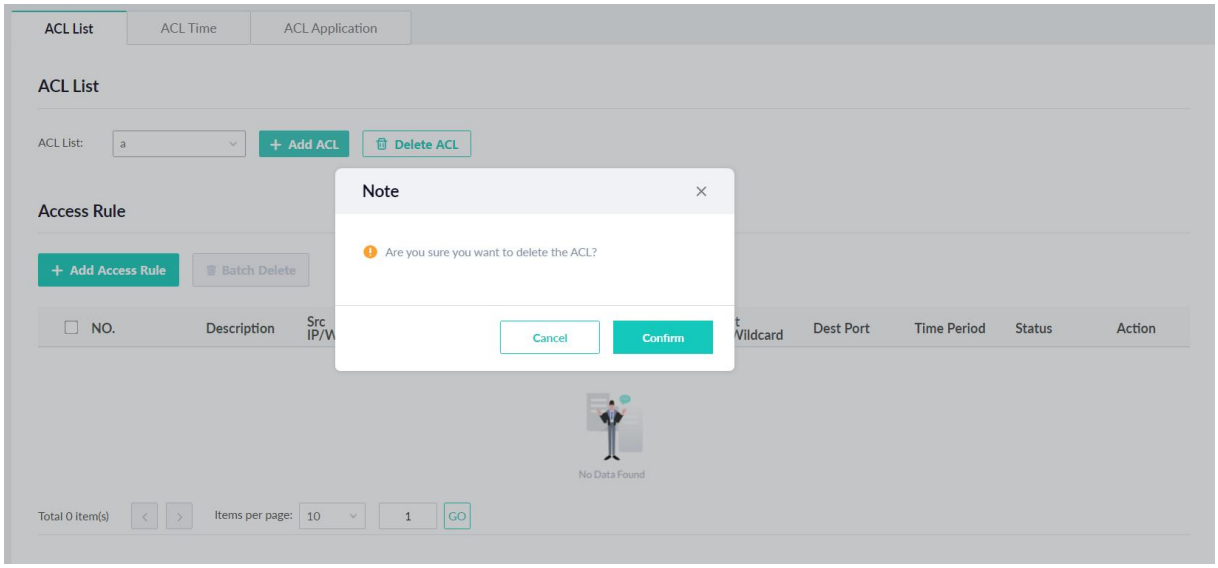
1.Add ACL

Click the "Add ACL" button and set the content in the pop-up box. The ACL list is a required field. Click "OK" to prompt "Setup successful". You can see the added ACL in the ACL list drop-down box.

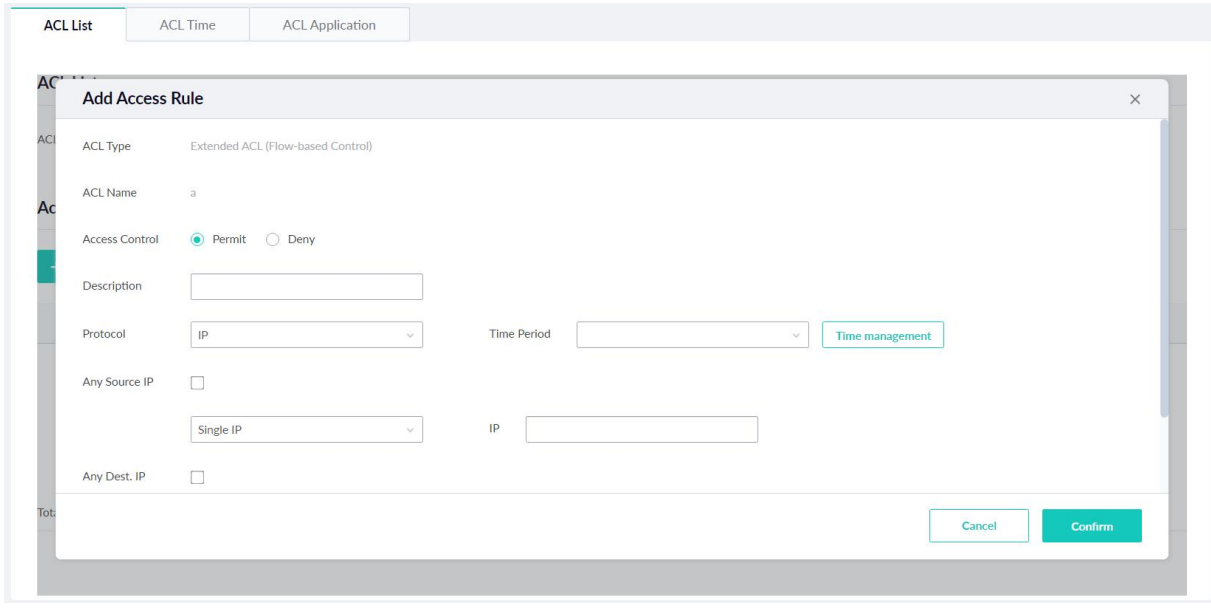


2.Remove ACL

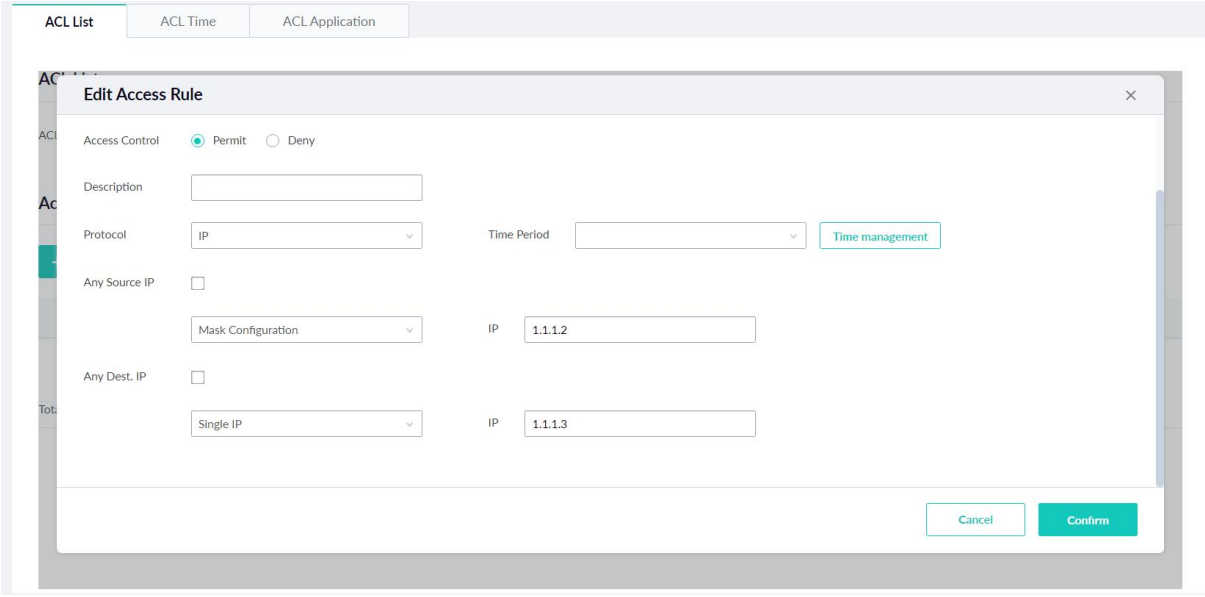
Select the ACL to be deleted in the ACL list drop-down box, click the "Delete ACL" button, and prompt "Delete successfully".



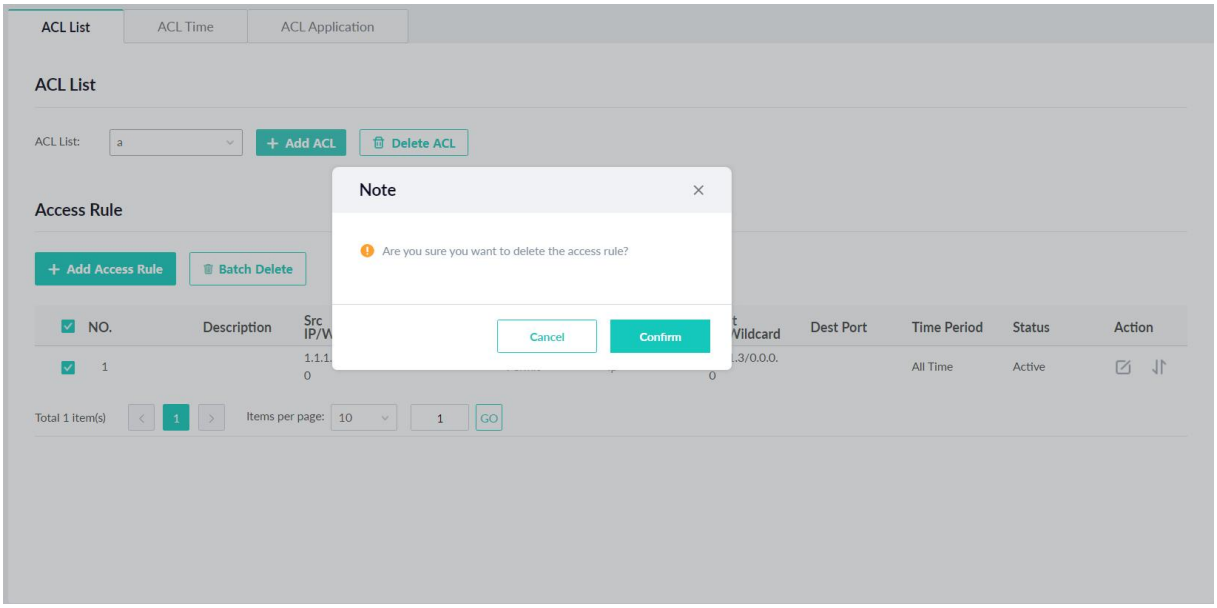
3.Add ACE rules



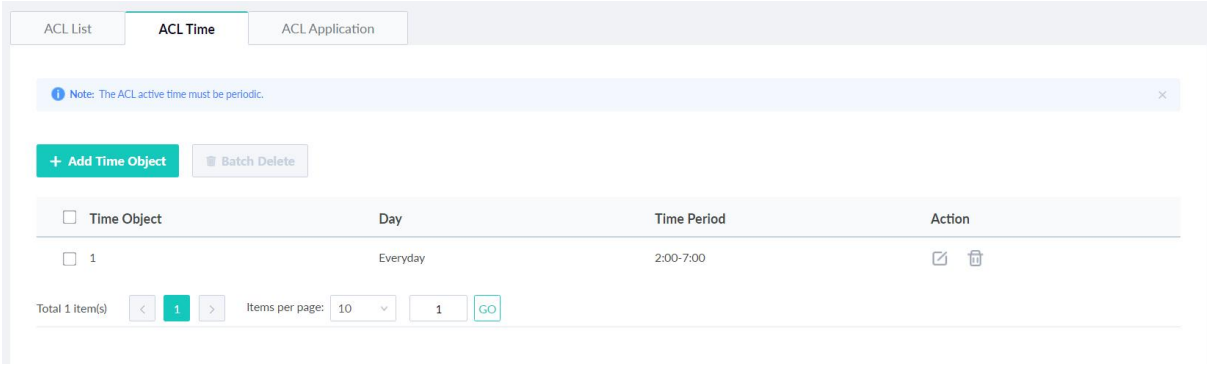
4.Edit ACE rules



5.Delete ACE rules

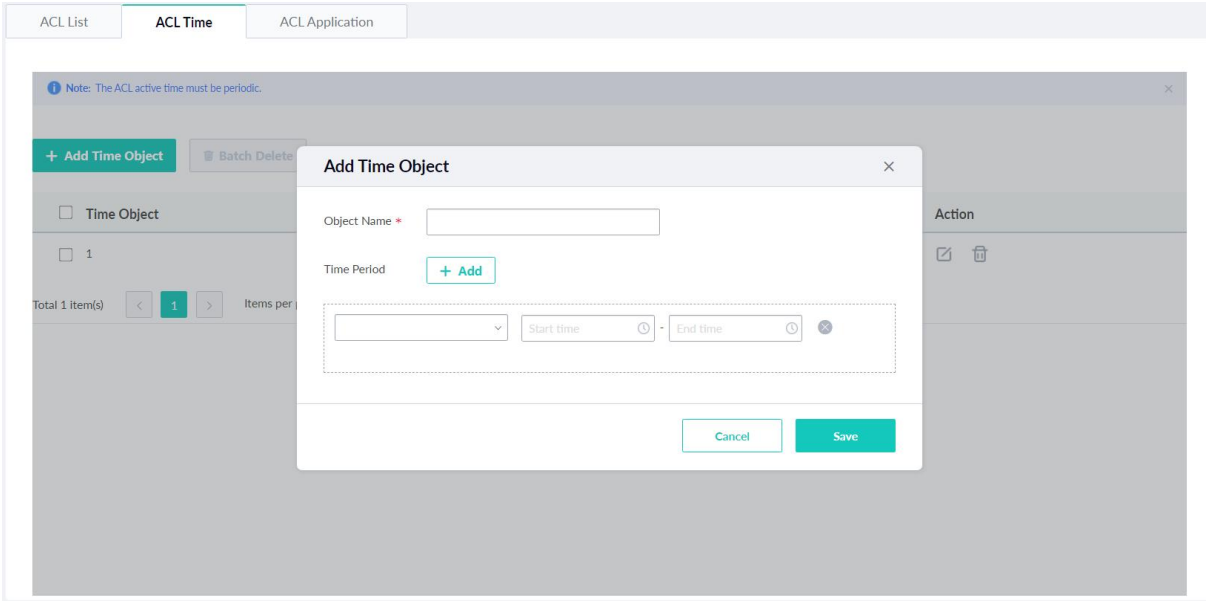


☆ ACL effective time

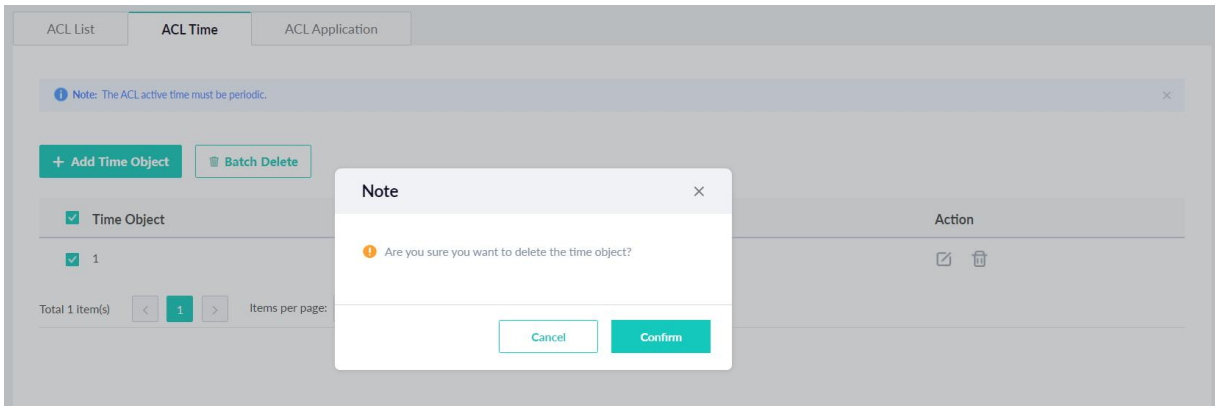


You can make ACLs run based on time, for example, make ACLs take effect during certain periods of a week. To meet this requirement, you must first configure a time object.

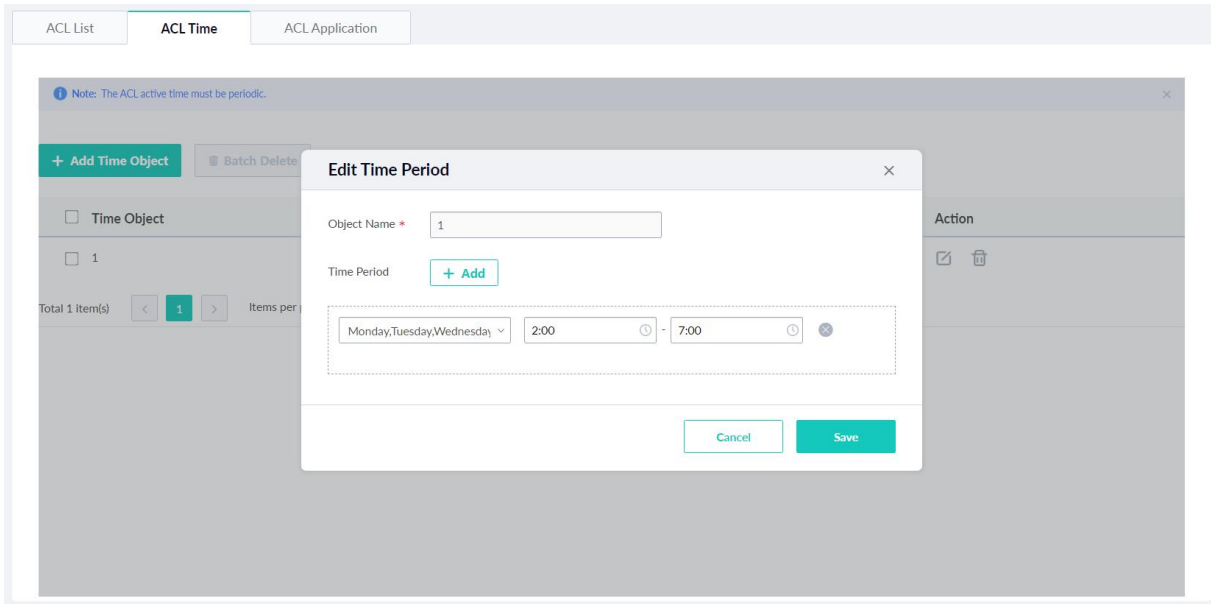
1.Add time object



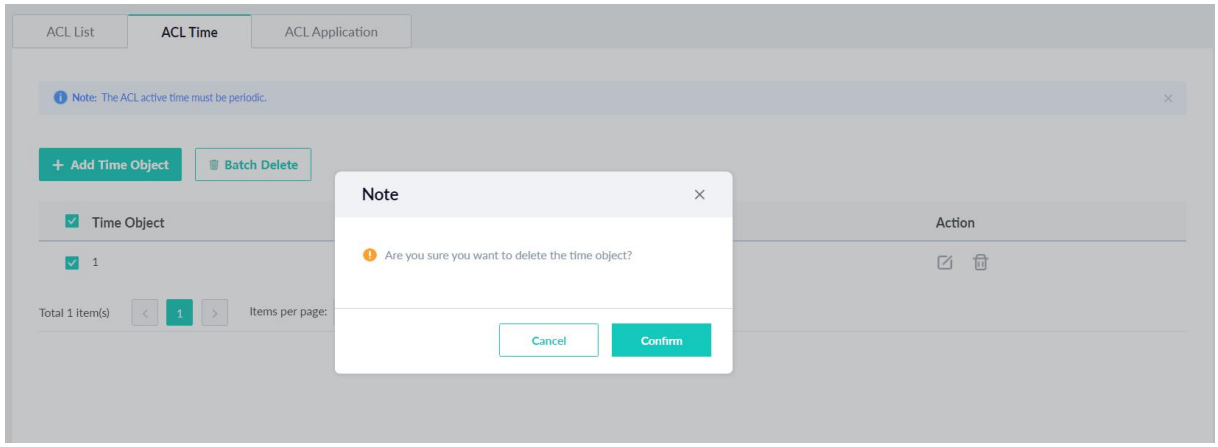
2.Batch delete time objects



3.Edit time object



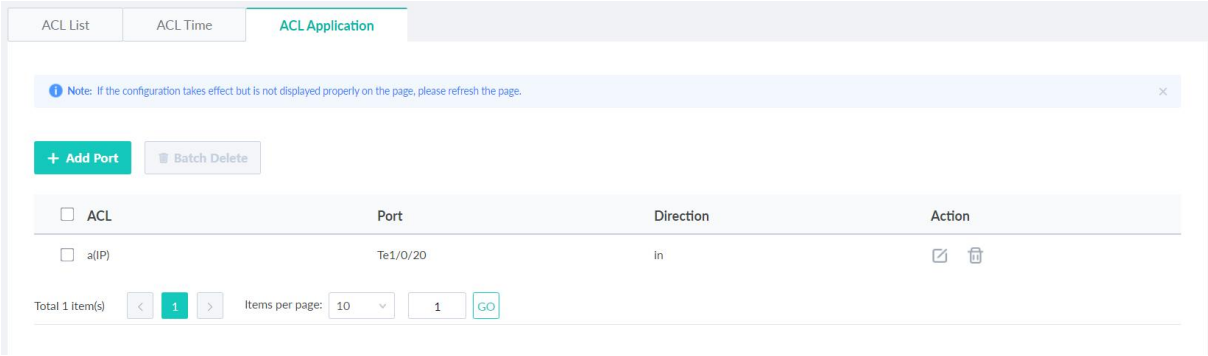
4.Delete time object



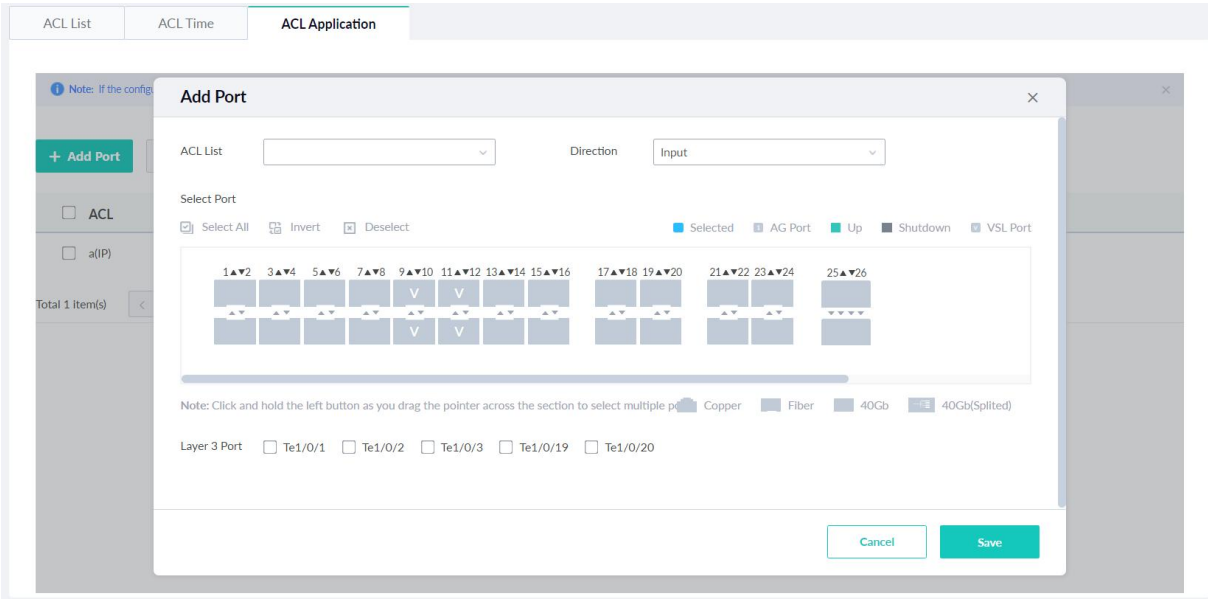
ACL application

It is by configuring ACL rules and applying them to the corresponding ports or VLANs to restrict specific user access or restrict users from accessing specific networks.

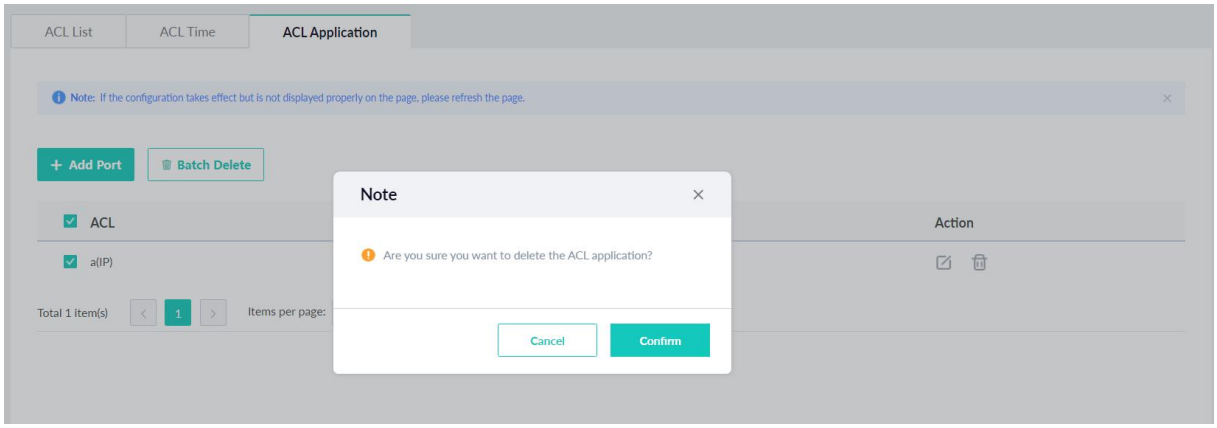
After ACL is applied to the port, there may be no way to echo it immediately, you need to refresh the page to echo



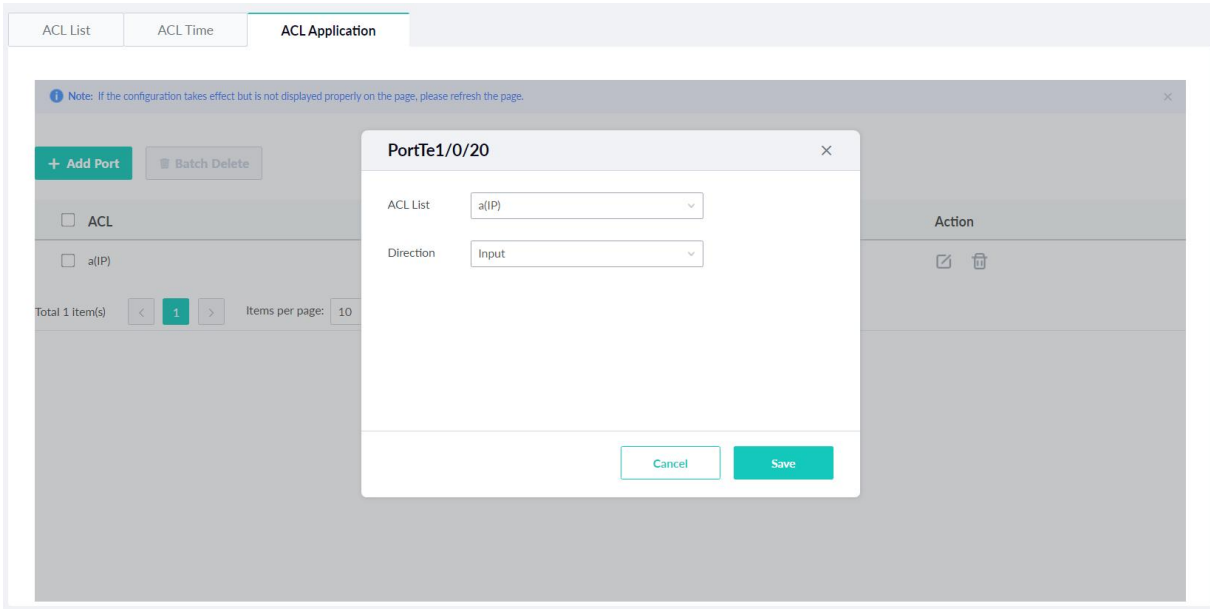
1.Add ACL application



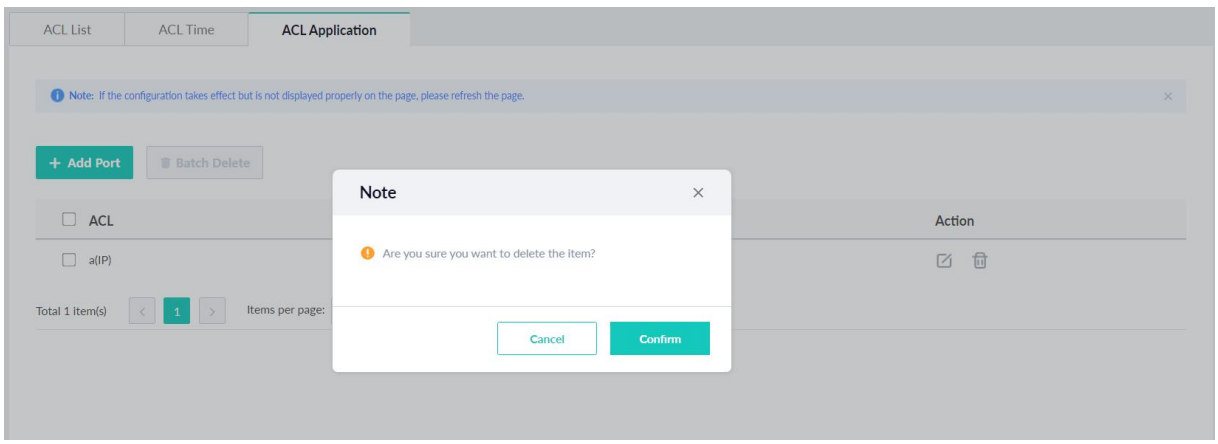
2.Delete ACLs in batch



3.Edit ACL application



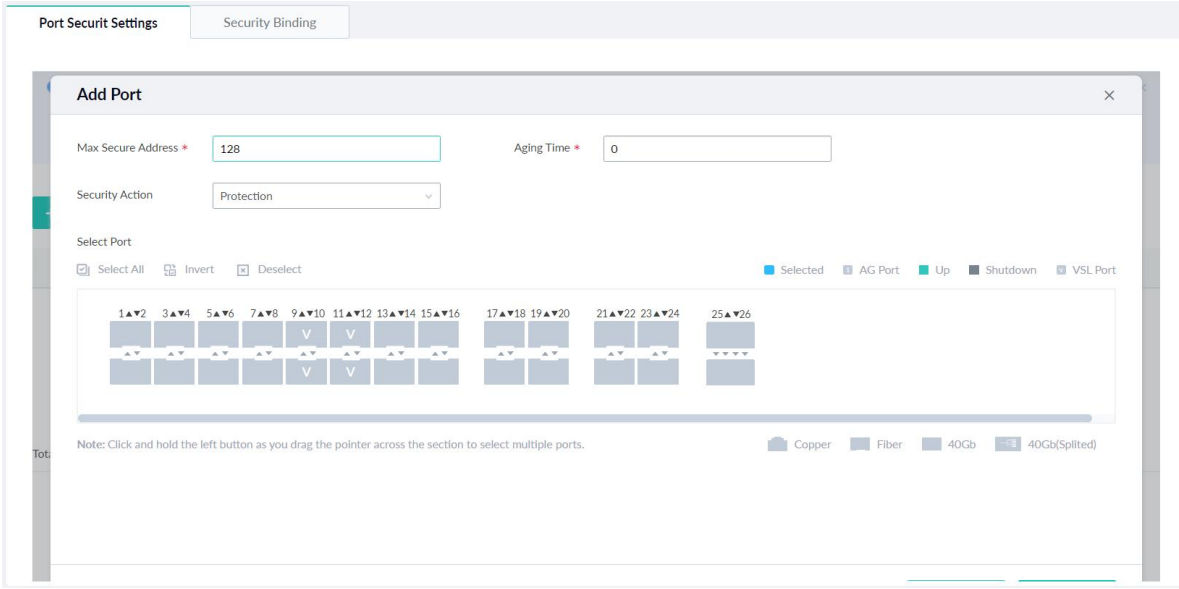
4.Delete ACL application



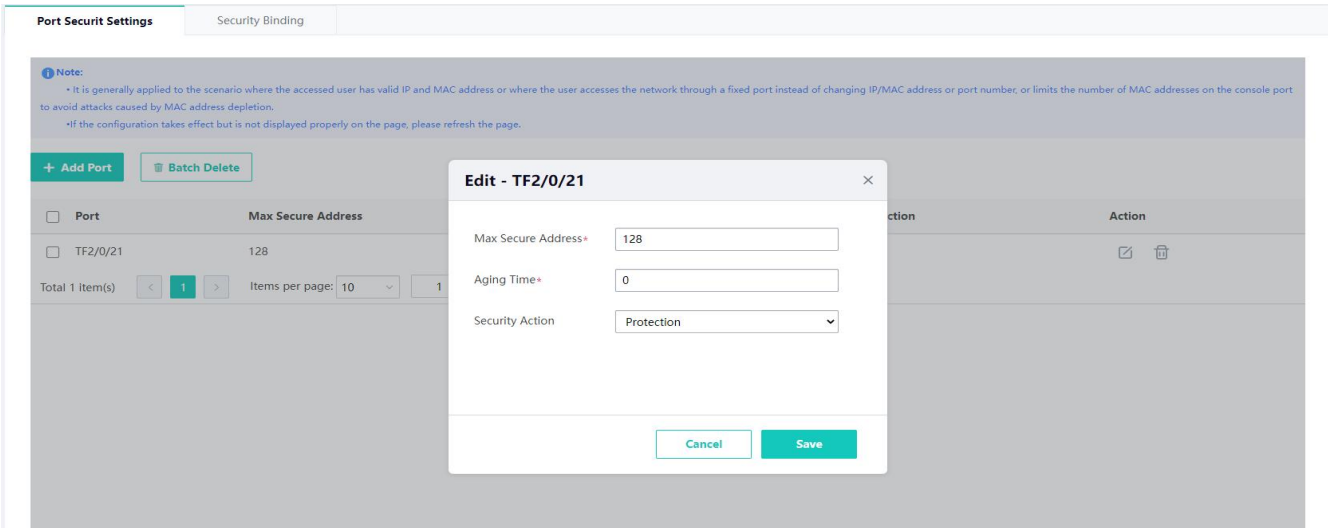
Port security

☆ basic settings

1.Add a security port

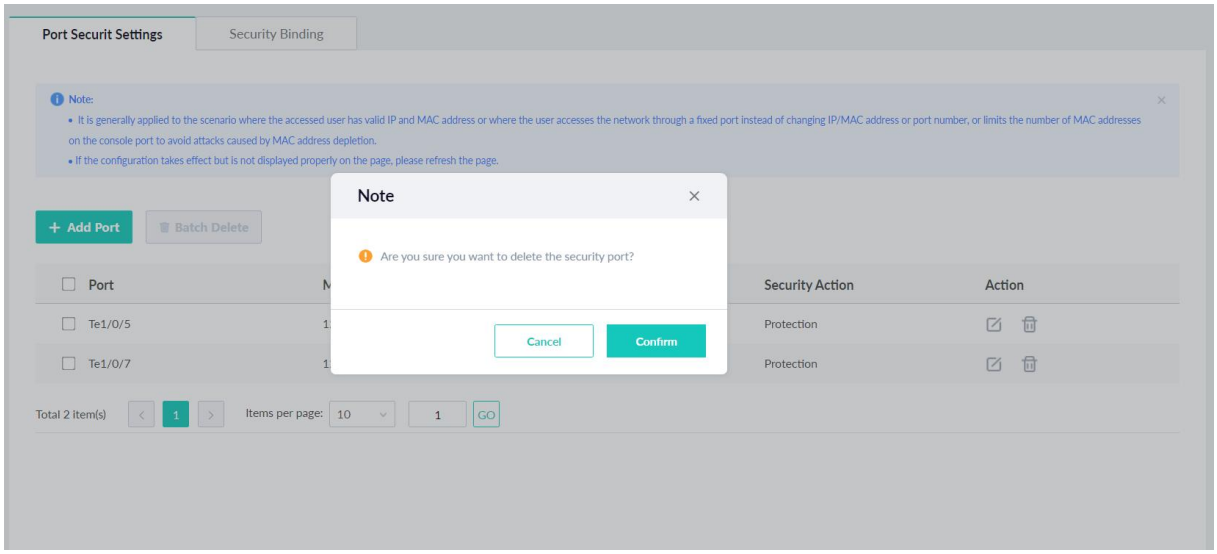


2.Edit security port



Click the <Edit> icon under the operation column of the last column of "User Security Port List", the page will display the information bound to the user, after editing the information, click <Complete Configuration> to prompt "Setup successful".

3.Delete security port

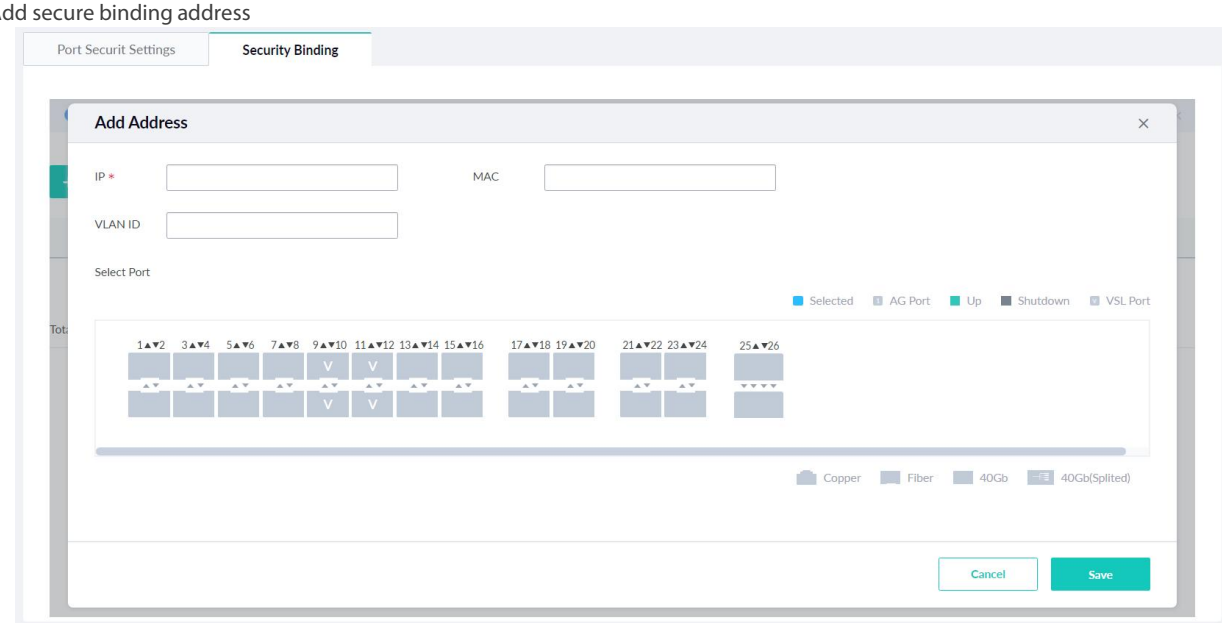


1) Select multiple records in the "Security Port List" and click "Delete Selected Security Ports" to delete data in batches.

2) Click the <Delete> icon under the operation column of the last column of "Security Port List", and prompt "Are you sure to delete the selected security port?", click OK and prompt "Delete successfully" to complete the deletion.

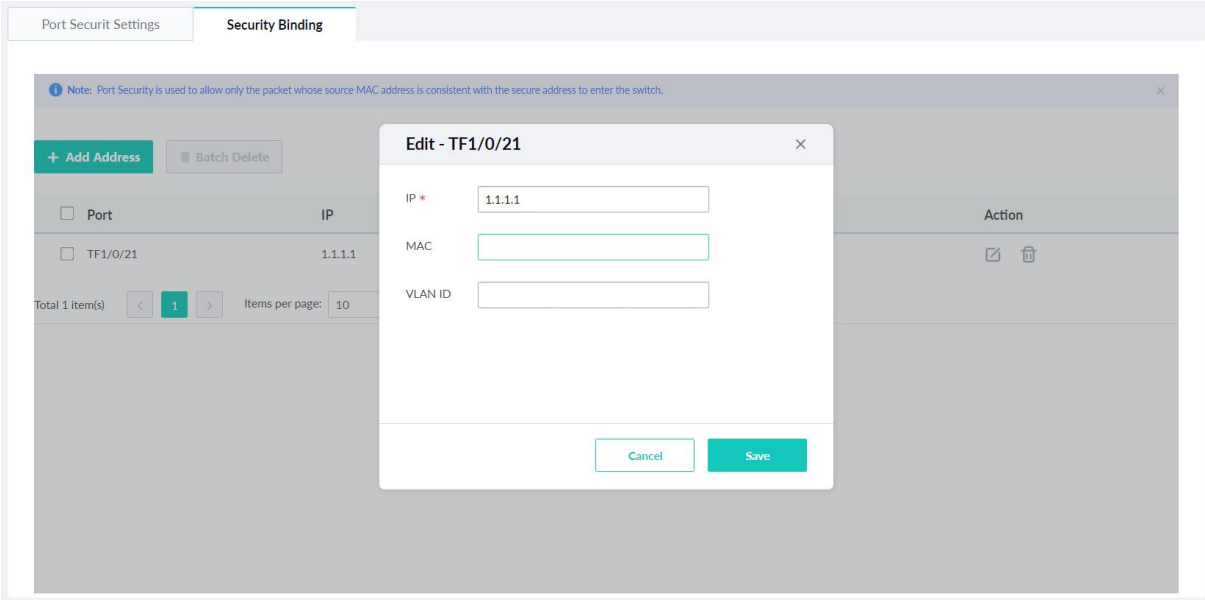
☆ Secure binding

1.Add secure binding address



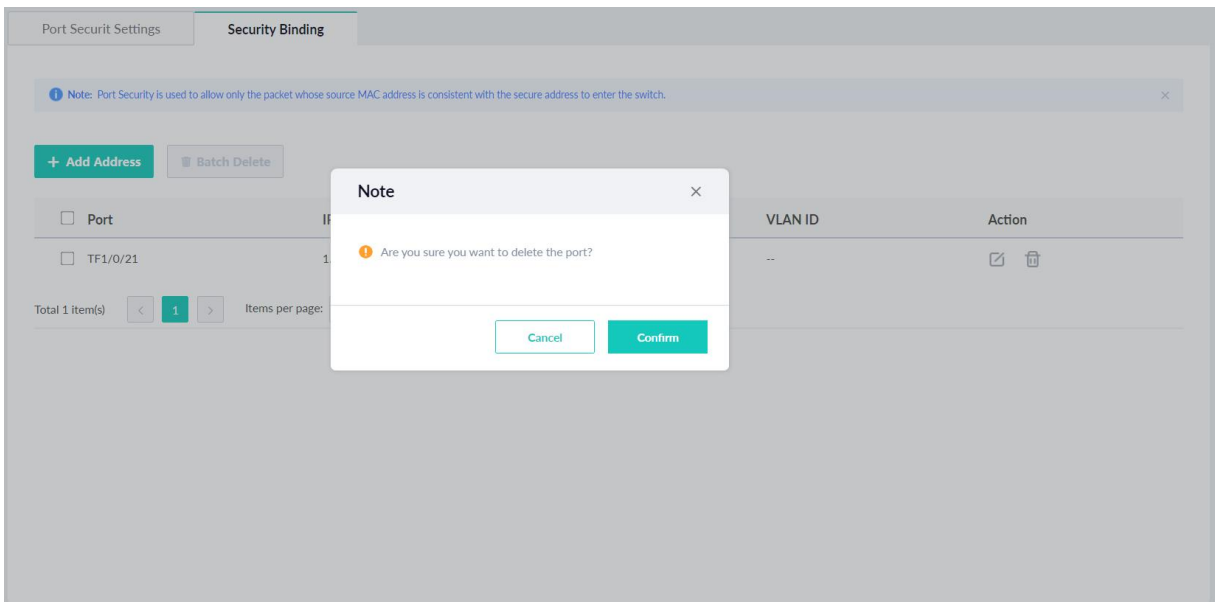
Set the security binding address, the IP address is required, others are optional, click "complete configuration" and prompt "setup successful", it will be displayed in the security binding address list.

2.Edit security port



Click the <Edit> icon under the operation column of the last column of "Security Binding Address List", the page will display the user's binding information, after editing the information, click <Complete Configuration> to prompt "Setup successful".

3.Delete the secure binding address list

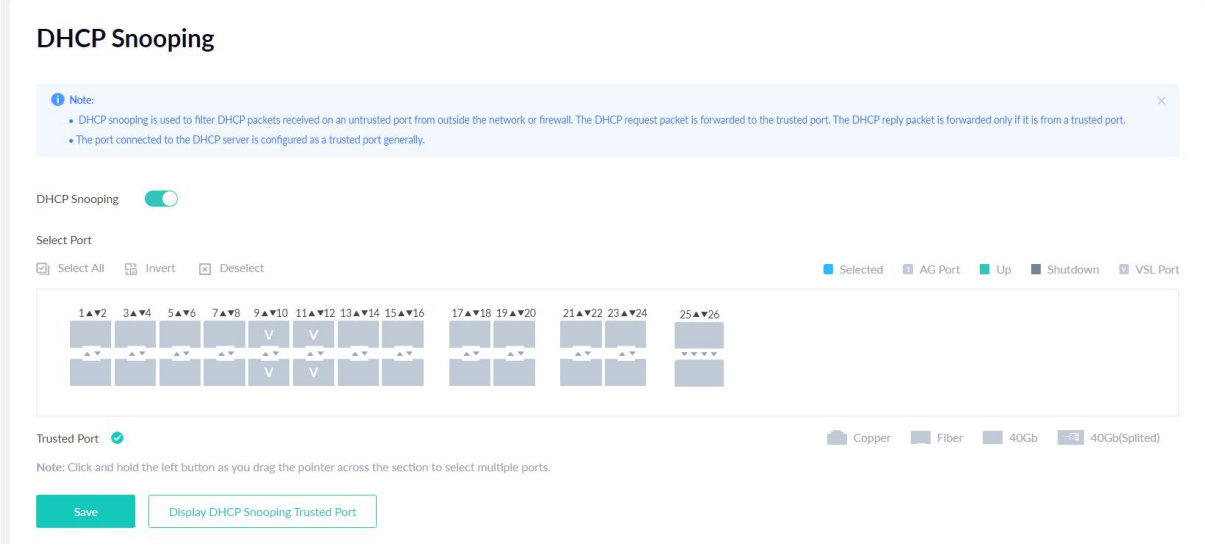


1) Select multiple records in the "Security binding address list", and click "Delete selected security binding ports" to delete data in batches.

2) Click the <Delete> icon under the operation column of the last column of "Security Binding Address List", prompt "Are you sure you want to delete the selected security binding port?", click OK and prompt "Delete Successful" to complete the deletion.

DHCP Snooping

The DHCP Snooping page is as follows:



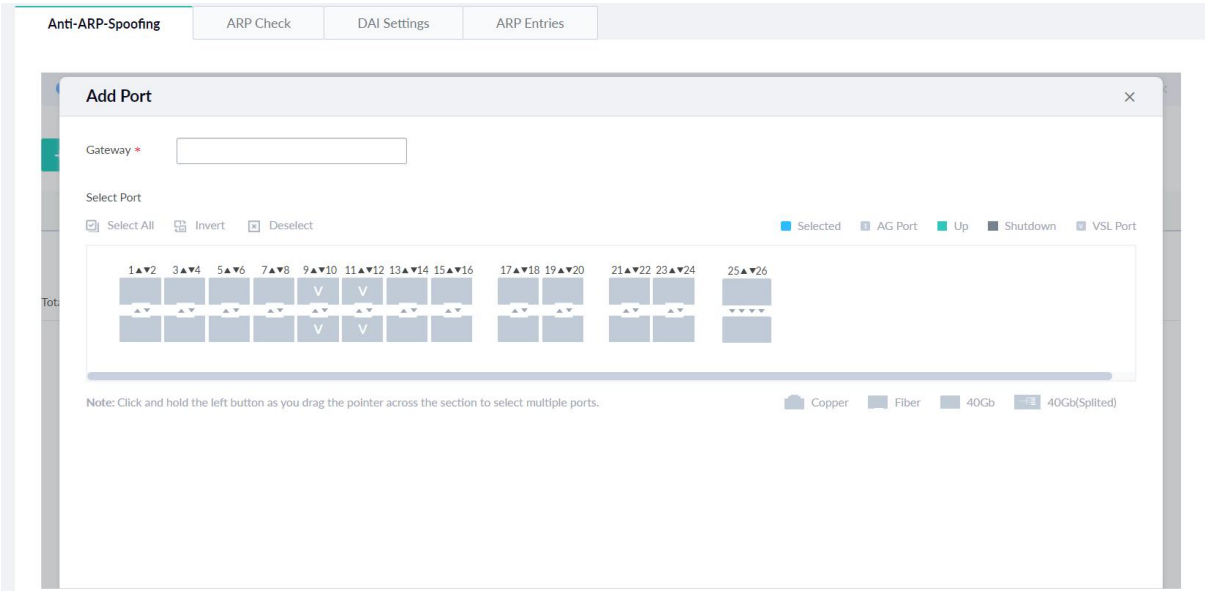
The port connected by the DHCP SERVER needs to be set as a DHCP trusted port, and the DHCP SERVER on the untrusted port cannot work normally. The currently configured trusted port means that the DHCP trusted port is enabled on the port. The user can directly select the port on the panel and click the <Save Settings> button.

Anti-ARP attack

"Anti-ARP Attack" can be used to prevent gateway ARP spoofing settings, ARP inspection settings, DAI settings and ARP table entries.

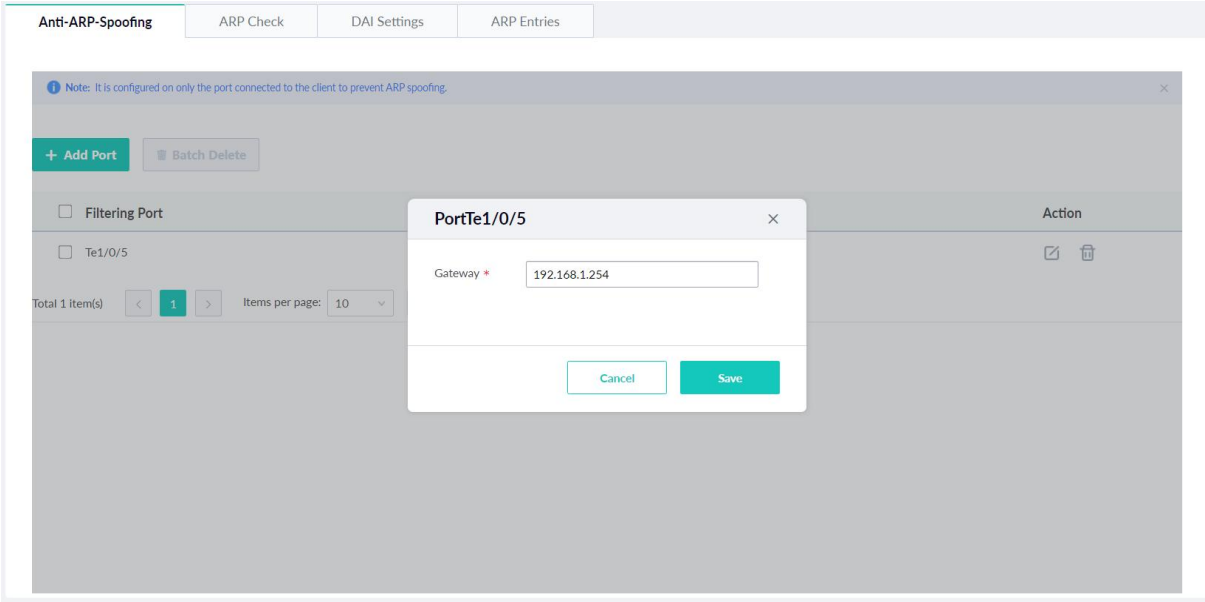
Anti-Gateway ARP Spoofing

1.Add filtering port:



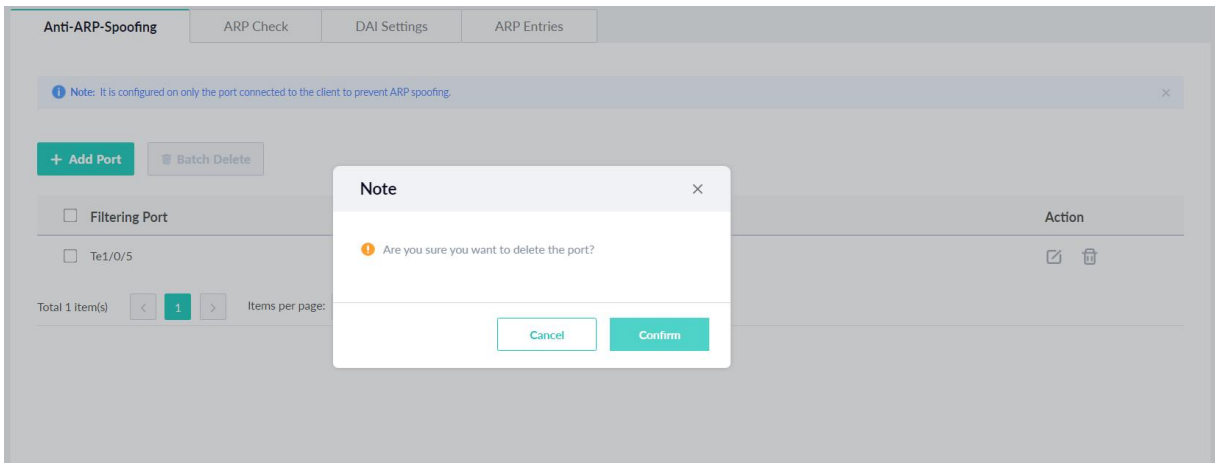
To set the filter port, you must fill in the IP address, click "complete configuration" and prompt "setting successful", it will be displayed in the filter port list.

2.Edit filter port



Click the <Edit> icon under the operation column of the last column of "Filter Port List", and the page will display the information of the filtered port. After editing the information, click <Complete Configuration> to prompt "Setup successful".

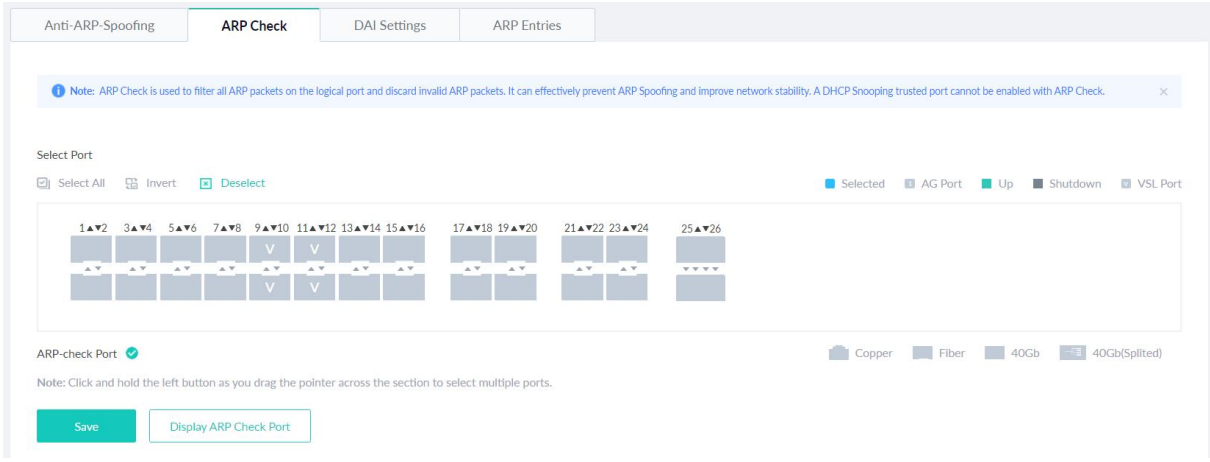
3.Delete filter port



1) Select multiple records in the "Filter Port List", and click "Delete Selected Filter Port" to delete data in batches.

2) Click the <Delete> icon under the operation column of the last column of "Filtered Port List", and prompt "Are you sure to delete the selected filtered port data?", click OK and prompt "Delete Successfully" to complete the deletion.

ARP inspection settings

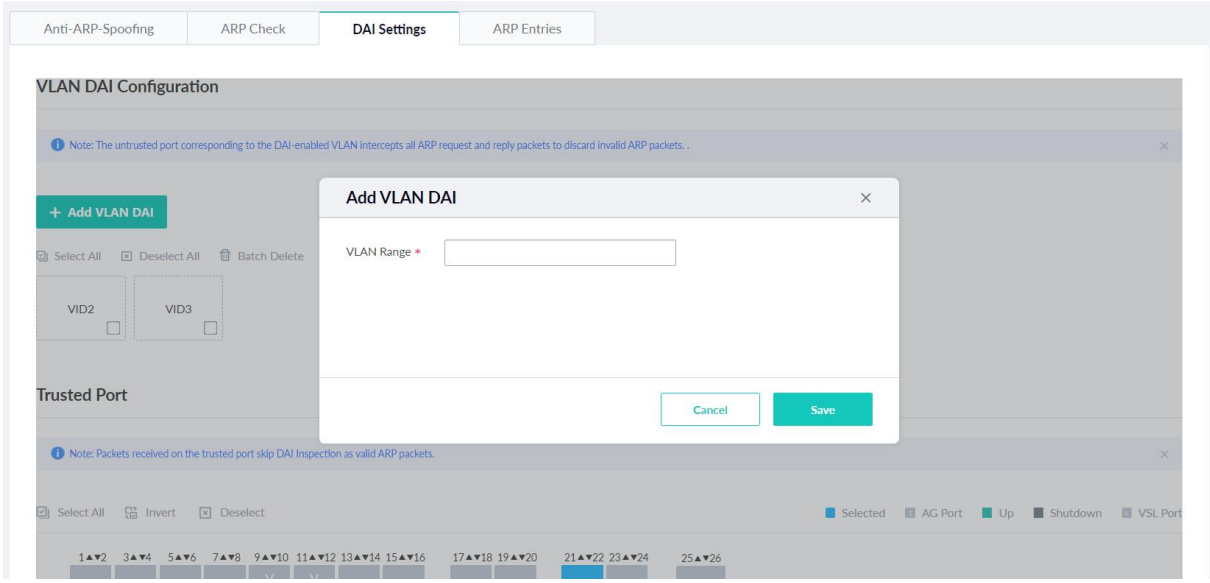


The current port displayed on the panel has opened the ARP inspection setting state and is in the editing state. After the user has modified the port, but does not want to edit it, he can click the <Display Current ARP Inspection Port> button to restore the panel to display the current ARP inspection configuration state.

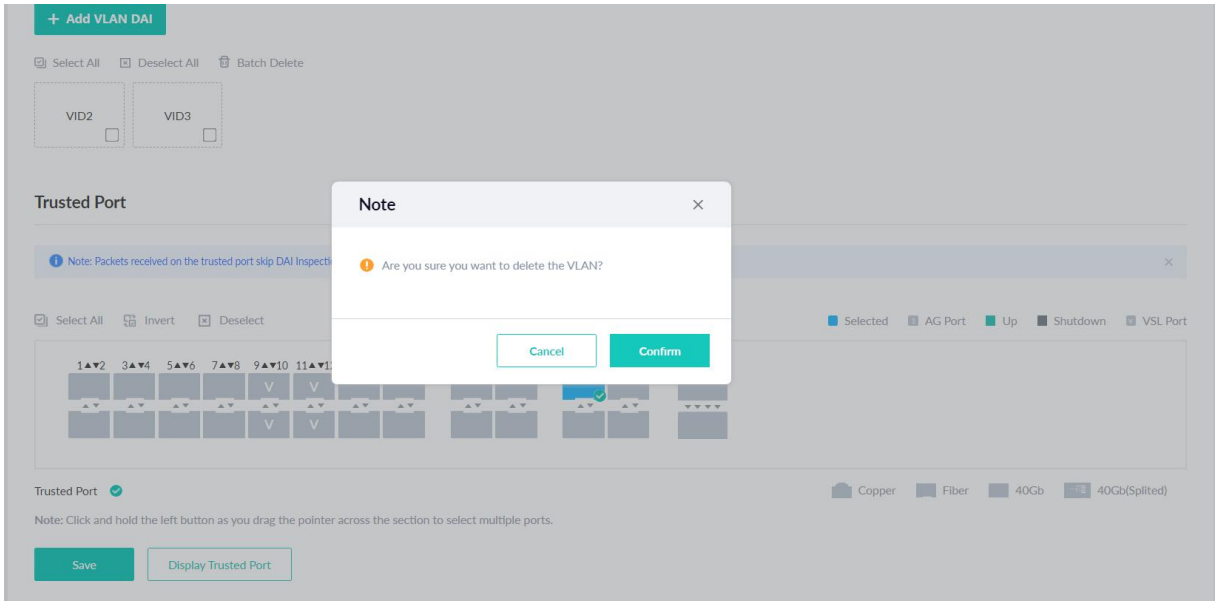
The port of the DHCP Snooping trusted port cannot enable ARP inspection.

DAI settings

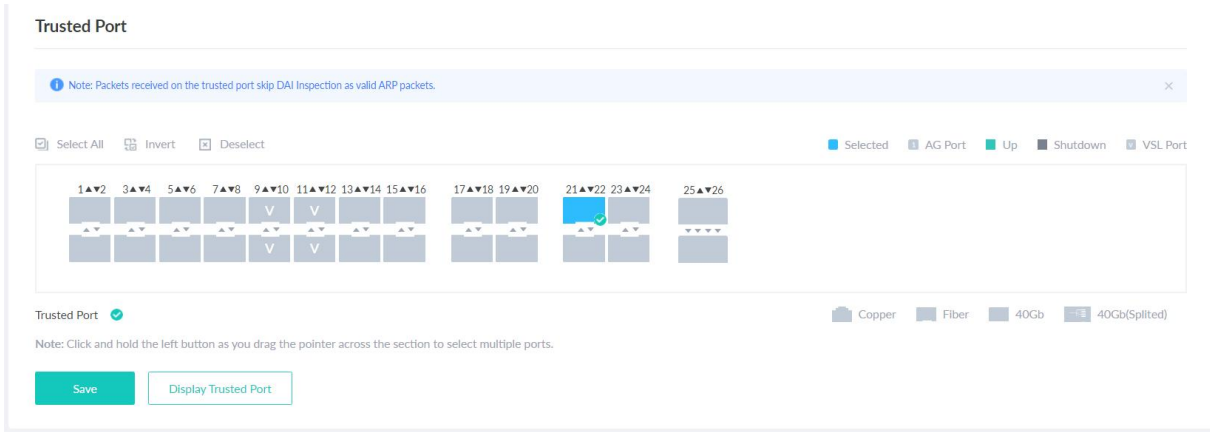
1.VLAN DAI setting added



2.VLAN DAI delete



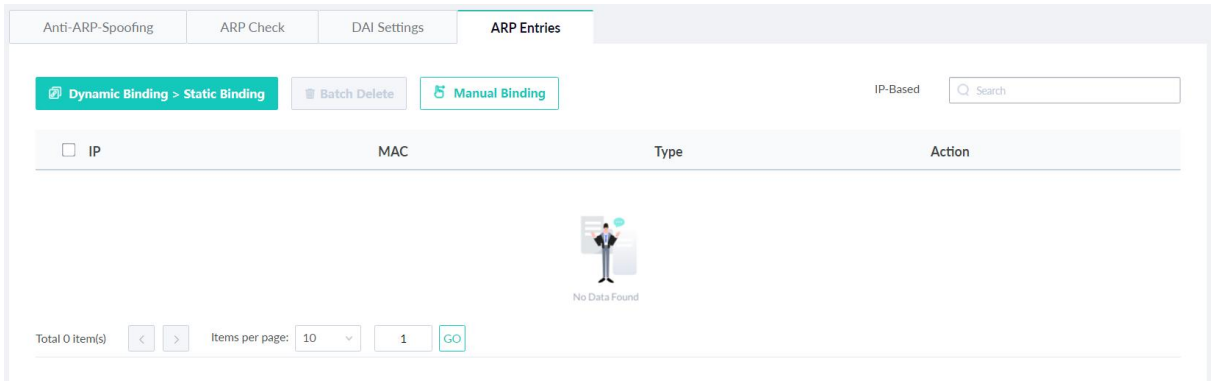
3.DAI confidence



The setting status of the currently opened DAI trusted port displayed on the panel is in the editing state. After the user has modified the port, but does not want to edit it, he can click the <Show current DAI trusted port> button to restore the panel to display the current DAI trusted port configuration status.

☆ ARP entry

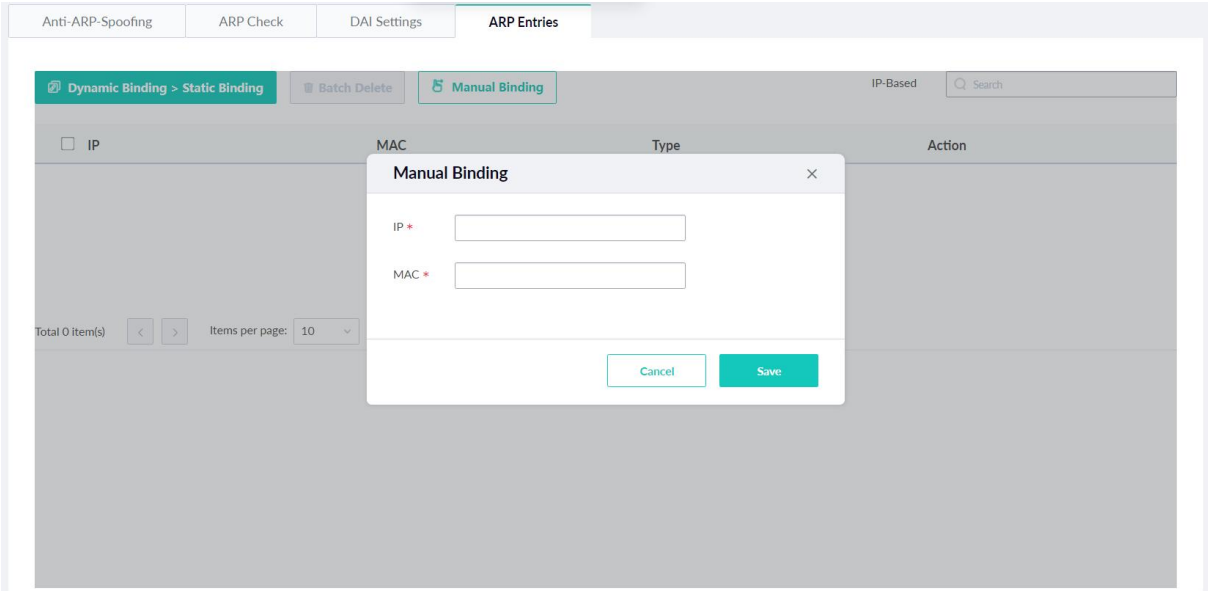
1.Dynamic >> Static binding



1) You can select multiple pieces of dynamic data in the "ARP table entry list" to batch setas static binding data.

2) Click the <dynamic to static binding> icon under the operation column of the last column of "ARP entry list" to prompt "Setup successful".

2.Manual binding



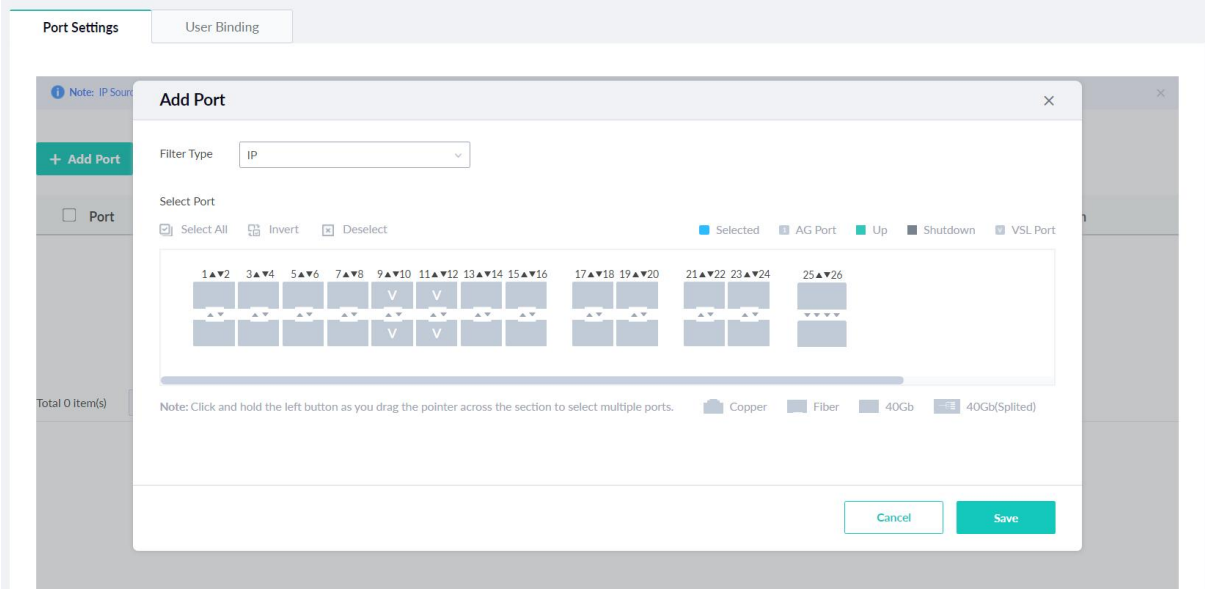
Set static binding data, IP address and MAC address are required fields, click "OK" to prompt "Setup successful", it will be displayed in "ARP table entry list".

IP Source Guard

"IP Source Guard" can carry out interface configuration and user binding.

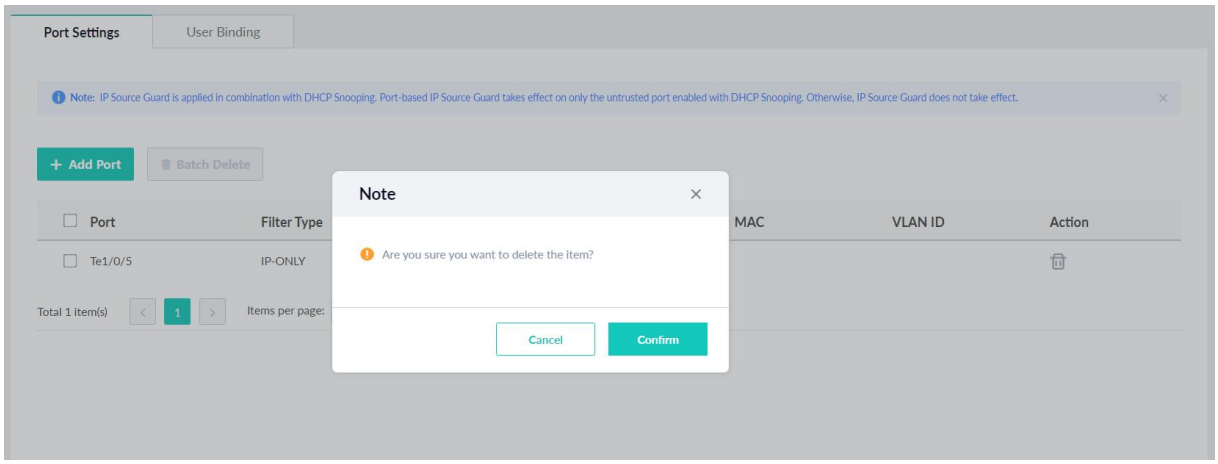
☆ **Interface configuration**

1.Add IP Source Guard port



Set to enable the IP Source Guard port, select the filter type and port, click "Finish configuration" and prompt "Setup successful", it will be displayed in the IP Source Guard port list.

2.Delete IP Source Guard port list



1) Select multiple records in "IP Source Guard Port List", click "Delete Selected IP Source Guard Port List" to delete data in batches.

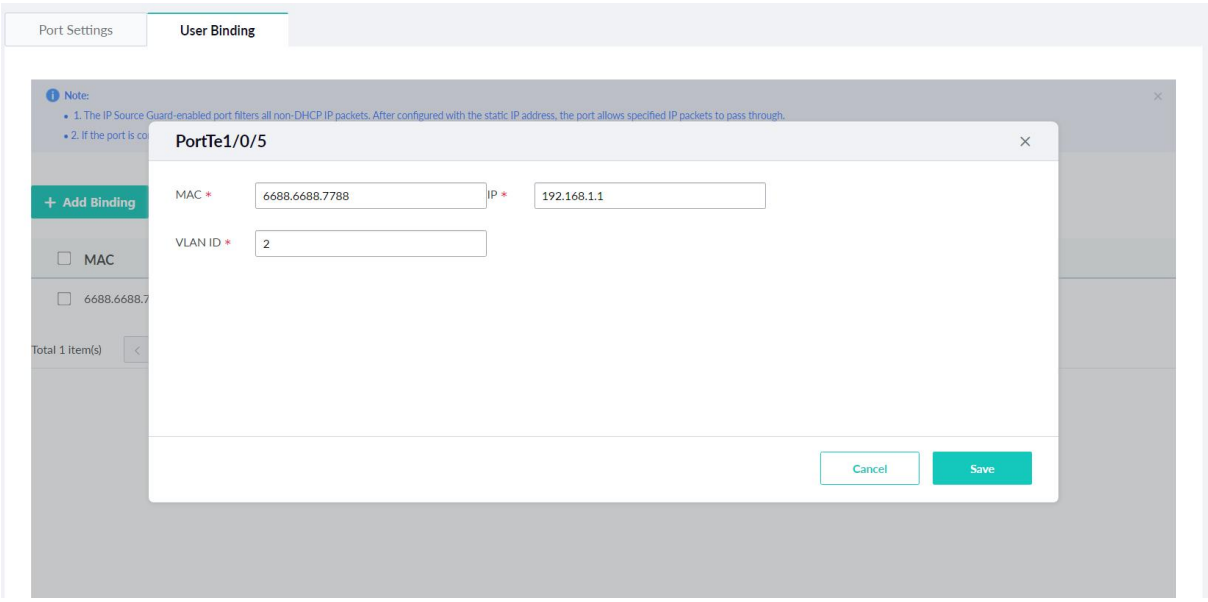
2) Click the <Delete> icon under the operation column of the last column of "IP Source Guard Port List", and prompt "Are you sure to delete the selected data?", click OK and prompt "Delete successfully" to complete the deletion.

☆ User binding

1.Add user binding

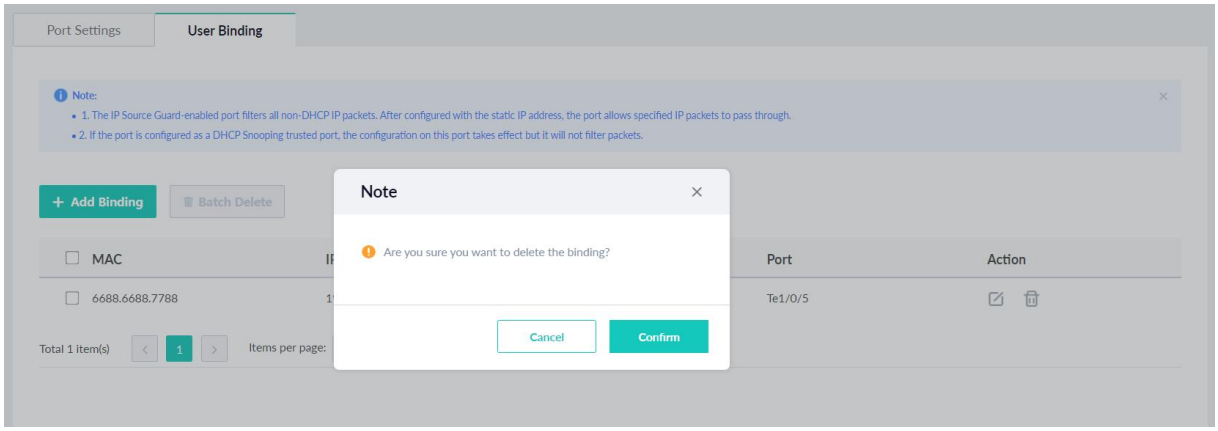
Set user binding, MAC address, IP address, VLAN ID are required, click "complete configuration" and prompt "setup successful", it will be displayed in the user binding list.

2.Edit user binding



Click the <Edit> icon under the operation column of the last column of "User Bound Port List", the page will display the user's binding information, after editing the information, click <Complete Configuration> to prompt "Setup successful".

3.Delete user binding list

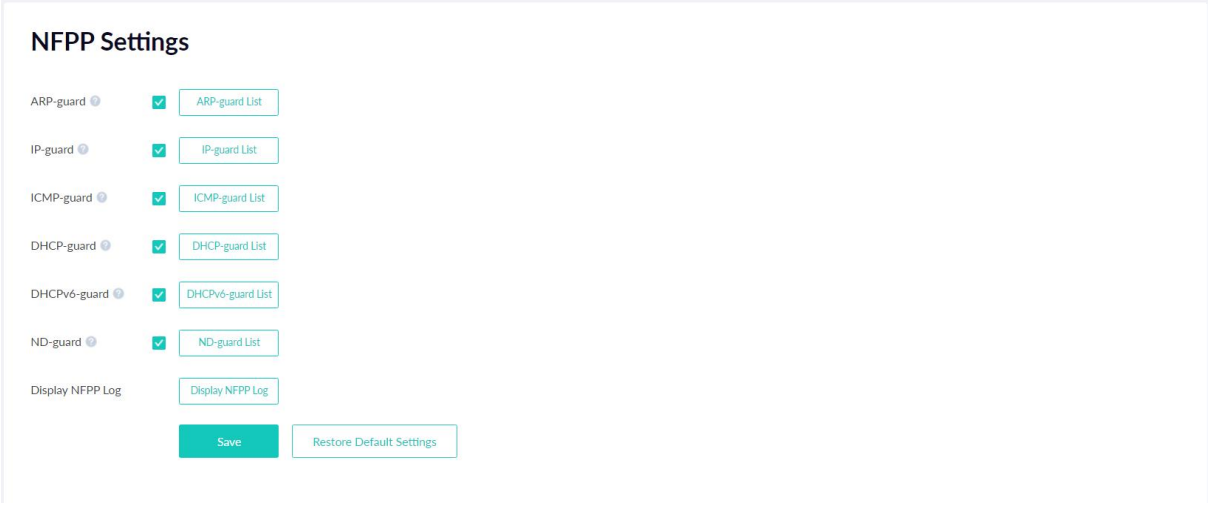


1) Select multiple records in the "User Binding List" and click "Delete Selected Binding" to delete data in batches.

2) Click the <Delete> icon under the operation column of the last column of "User Binding List", and prompt "Are you sure to delete the binding?", click OK and prompt "Delete successfully" to complete the deletion.

NFPP

The NFPP page is as follows:

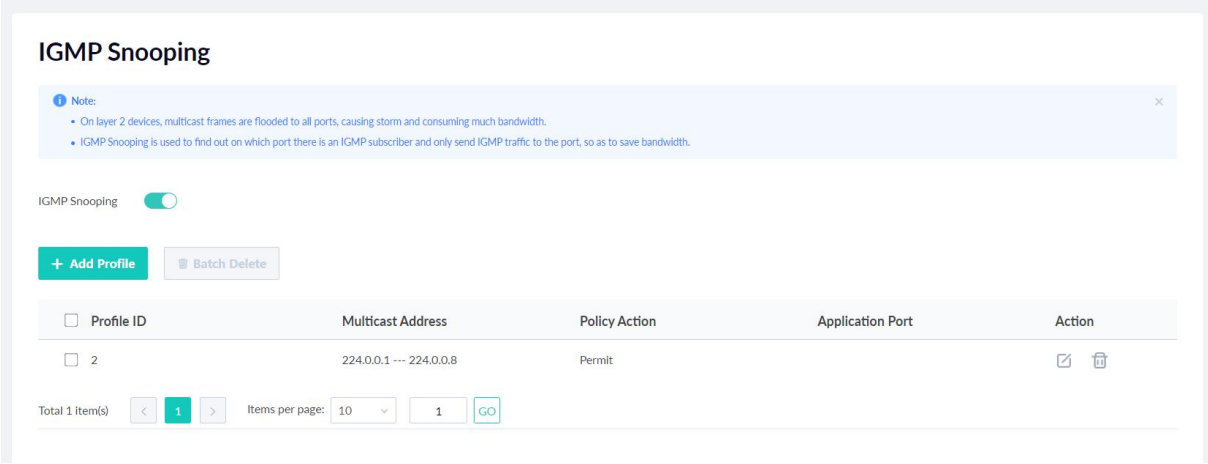


You can turn on or off each anti-attack function, click "Save Settings" to prompt "Setup successful", when you want to restore the default settings, click the "Restore Default Settings" button

advanced

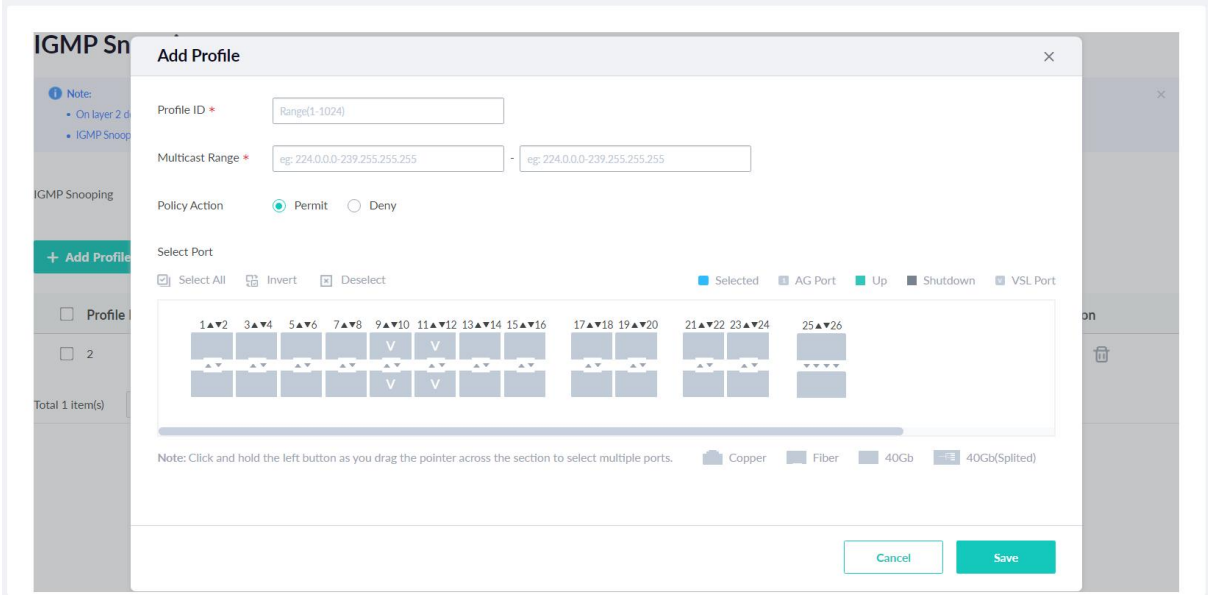
IGMP Snooping

The page of IGMP settings is as follows:

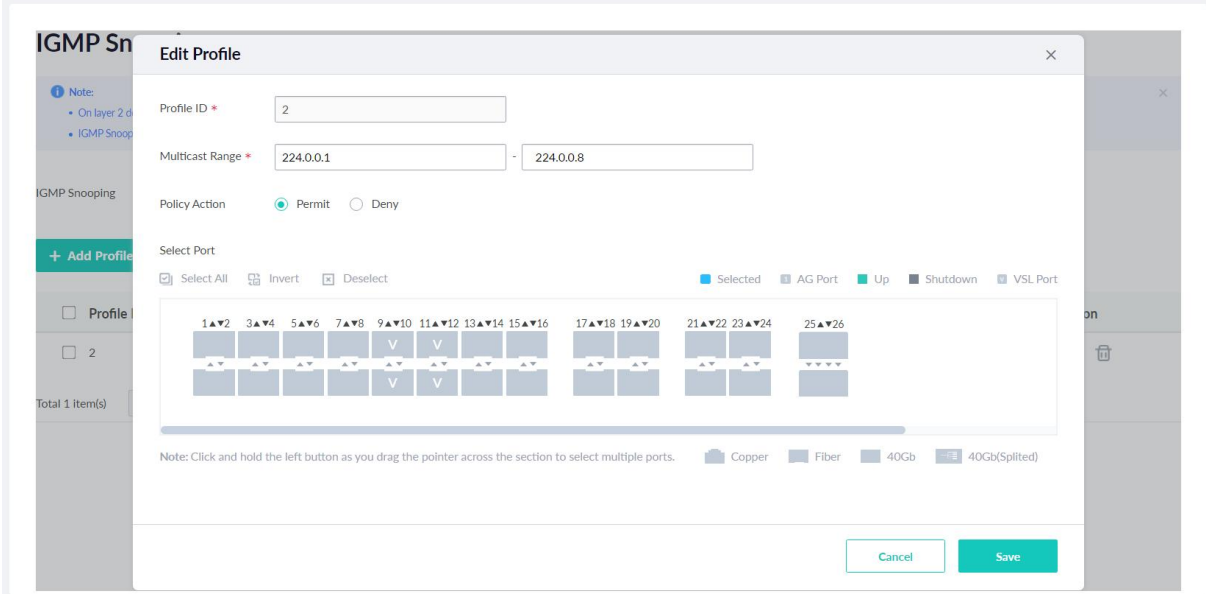


1.Add group policy

To set a group policy, you must fill in the group policy identifier and the multicast address range, and other information is optional. After clicking "Save Configuration" and prompting "Setup successful", it will be displayed in the group policy list.



2.Edit Group Policy



Click the <Edit> icon under the operation column of the last column of "Group Policy List", the page will display the information of the group policy, after editing the information, click <Save Configuration> to prompt "Setup successful".

3.Delete Group Policy

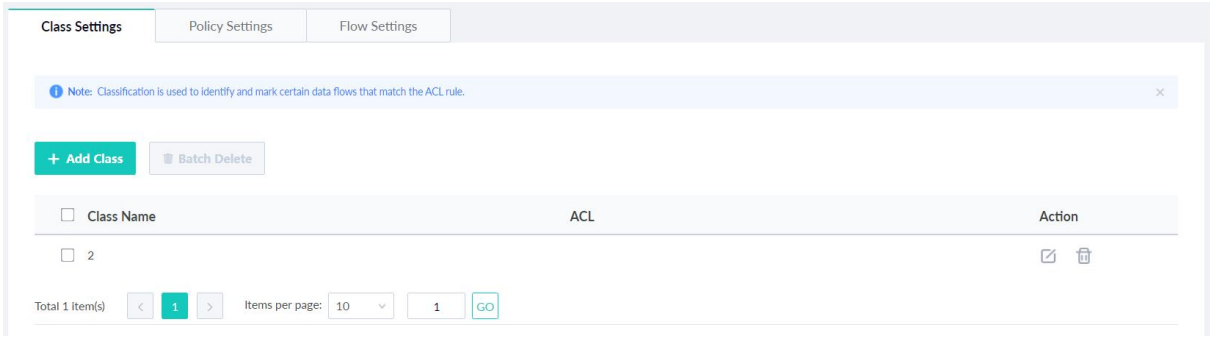
1) Select multiple records in the "Group Policy List" and click "Delete Selected Group Policy" to delete data in batches.

2) Click the <Delete> icon under the operation column in the last column of "Group Policy List", and prompt "Are you sure you want to delete this selection?", click OK and prompt "Delete successfully" to complete the deletion.

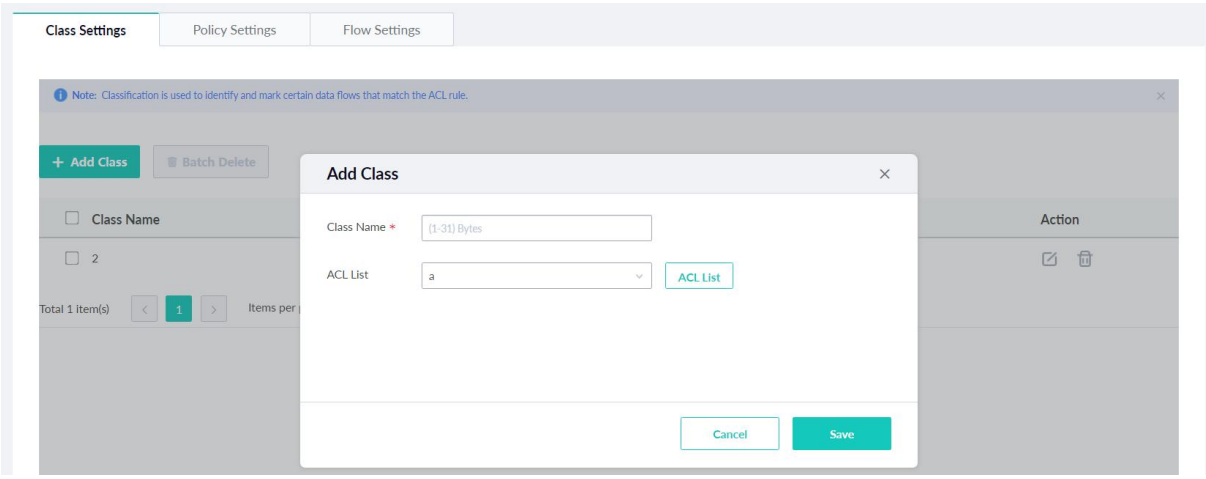
QOS

☆ Classification settings

The category setting page is as follows:



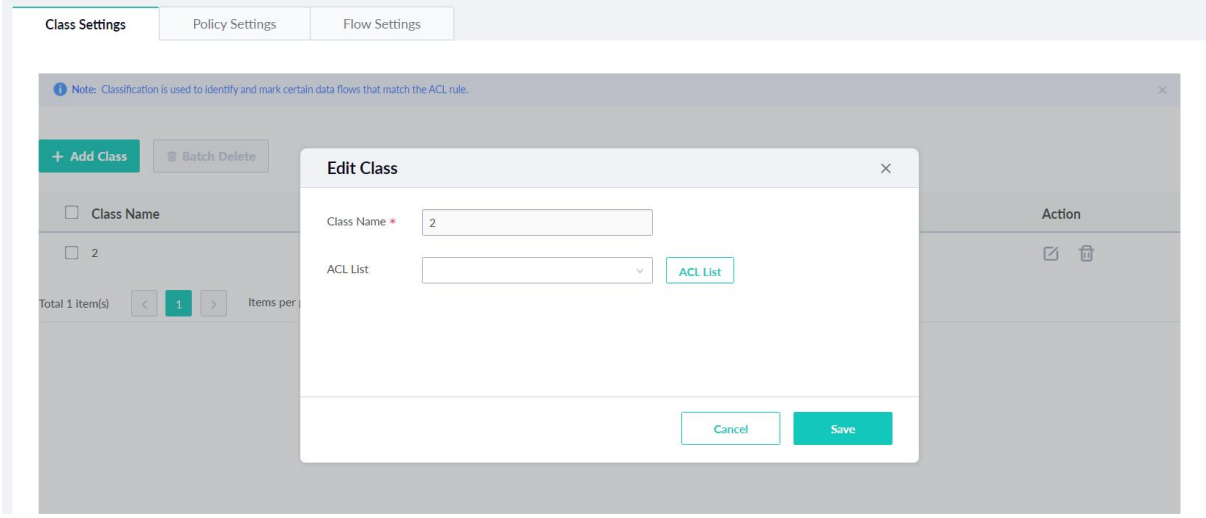
1.add category



Set the category, the category name is required, select the ACL list, click "Save configuration" and prompt "Setup successful", it will be displayed in the category list.

2.Edit category

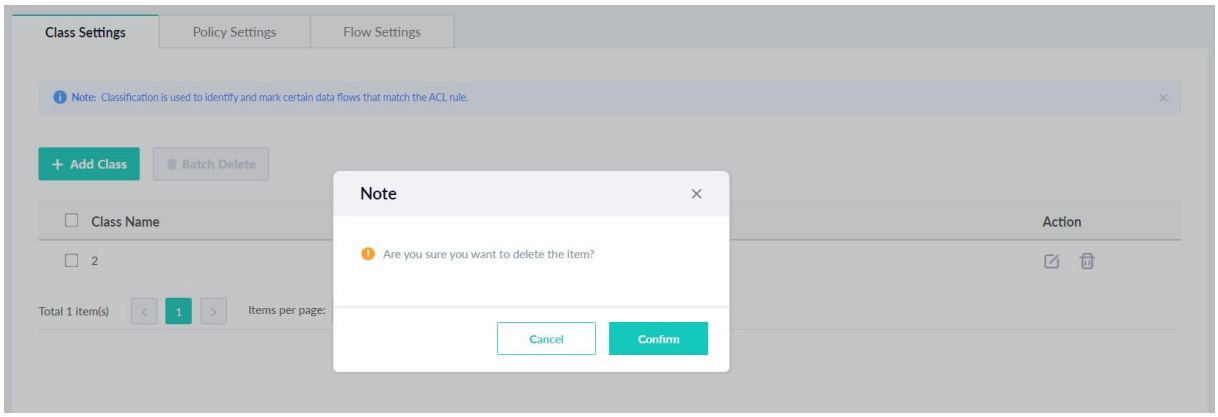
Click the <Edit> icon under the operation bar in the last column of "Category List", the page will display the information of the category, after editing the information, click <Save Configuration> to prompt "Setup successful".



3.Delete category

1) Select multiple records in the "Category List", click "Delete Selected Categories" to delete data in batches.

2) Click the <Delete> icon in the operation column of the last column of "Category List", and prompt "Are you sure to delete this item?", click OK and prompt "Delete successfully" to complete the deletion.

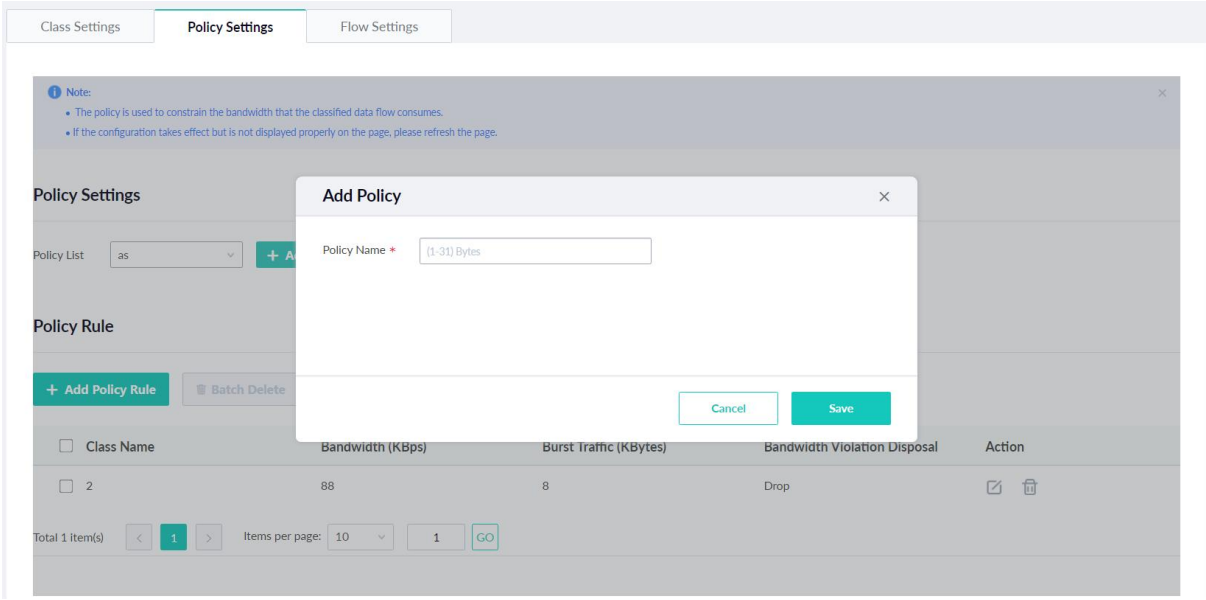


☆ Policy setting

The policy setting page is as follows:

1.Add strategy

Set the strategy, the name of the strategy is required, click "complete configuration" and prompt "setup successful", it will be displayed in the strategy list.

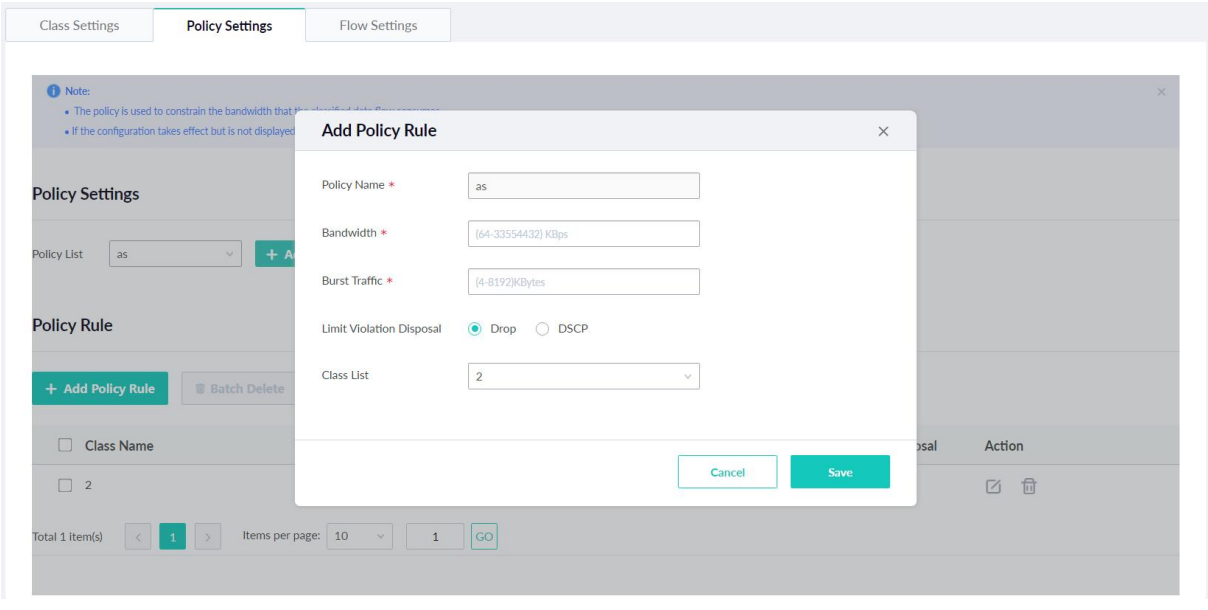


2.Delete strategy

Select a policy in the "Policy List", click the <Delete Policy> icon, and prompt "Are you sure you want to delete this item?", click OK and prompt "Delete successfully" to complete the deletion

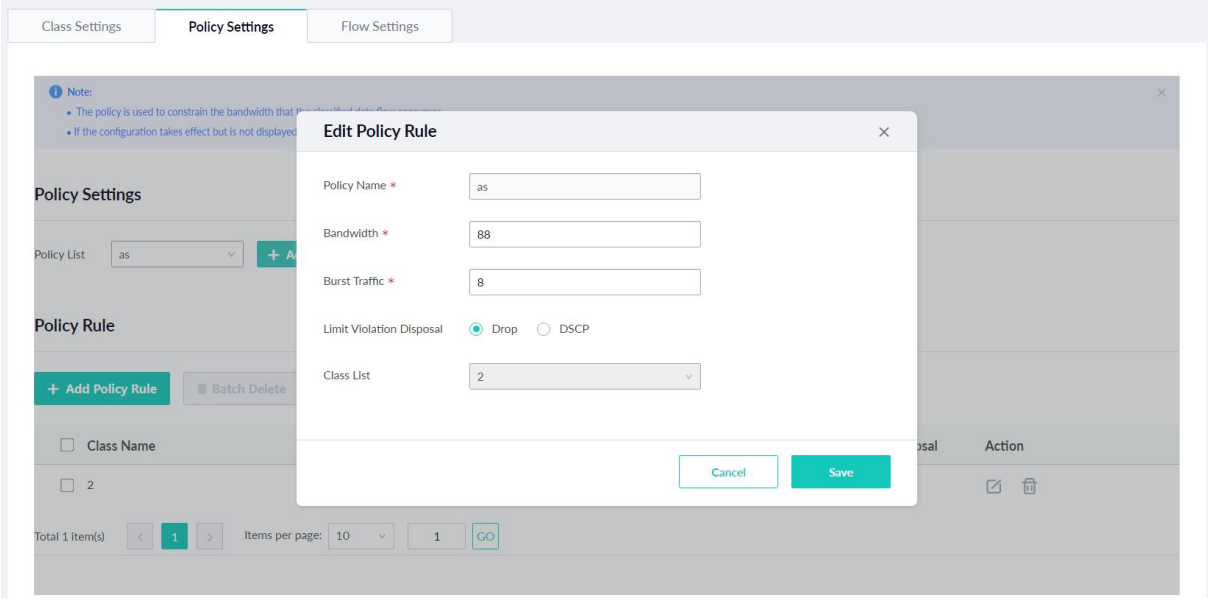
3.Add policy rules

Set policy rules. Bandwidth and burst traffic are mandatory, and other configurations are optional. After clicking "Finish configuration" and prompting "Setup successful", it will be displayed in the list of policy rules.



4.Edit policy rules

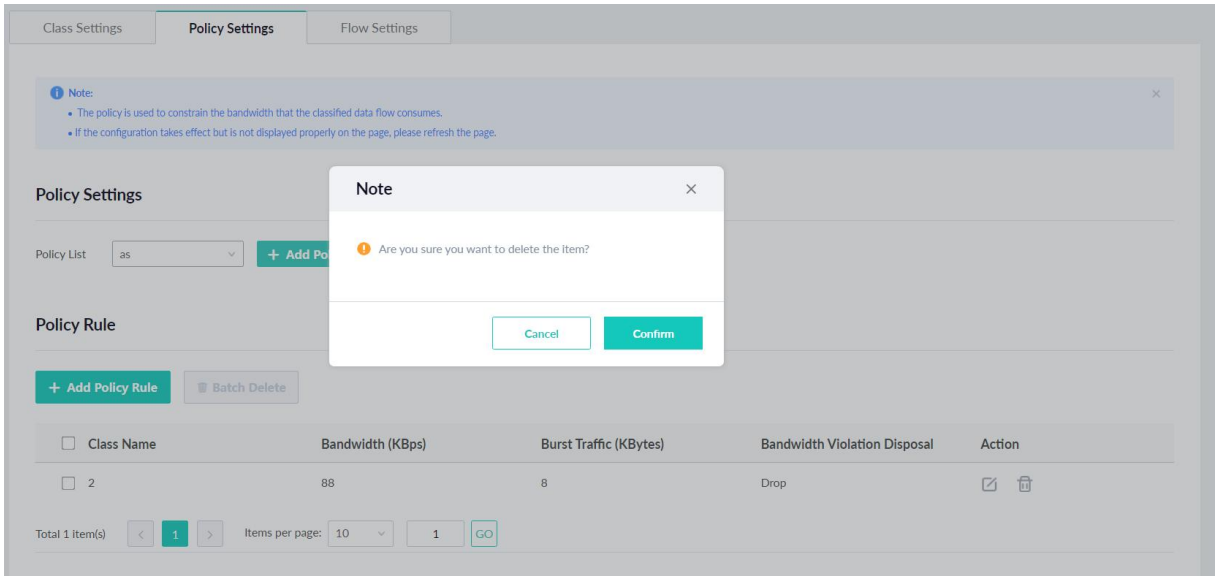
Click the <Edit> icon under the operation column of the last column of "Policy Rule List", the page will display the information of the policy rule. After editing the information, click <Complete Configuration> to prompt "Setup successful".



5.Delete policy rule

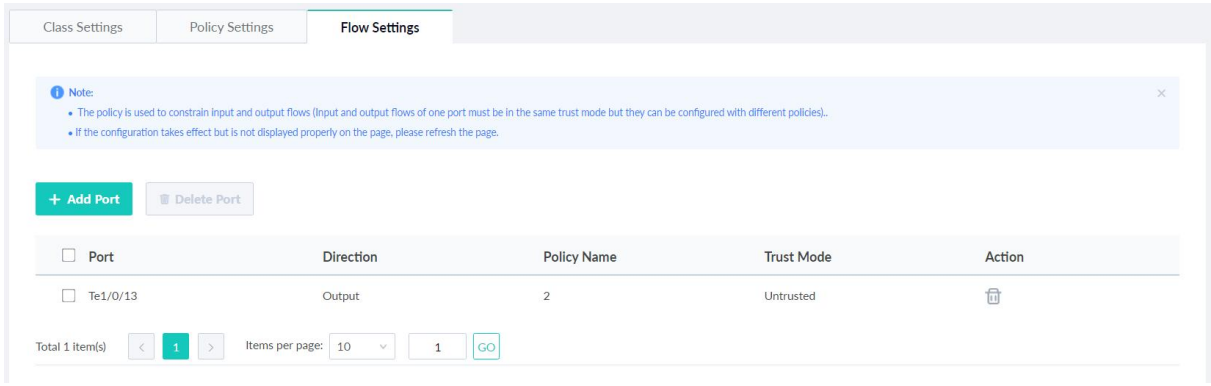
1) Select multiple records in the "Policy Rule List" and click "Delete Selected Rule" to delete data in batches.

2) Click the <Delete> icon under the operation column in the last column of "Policy Rule List", and prompt "Are you sure to delete this item?", click OK and prompt "Delete successfully" to complete the deletion.



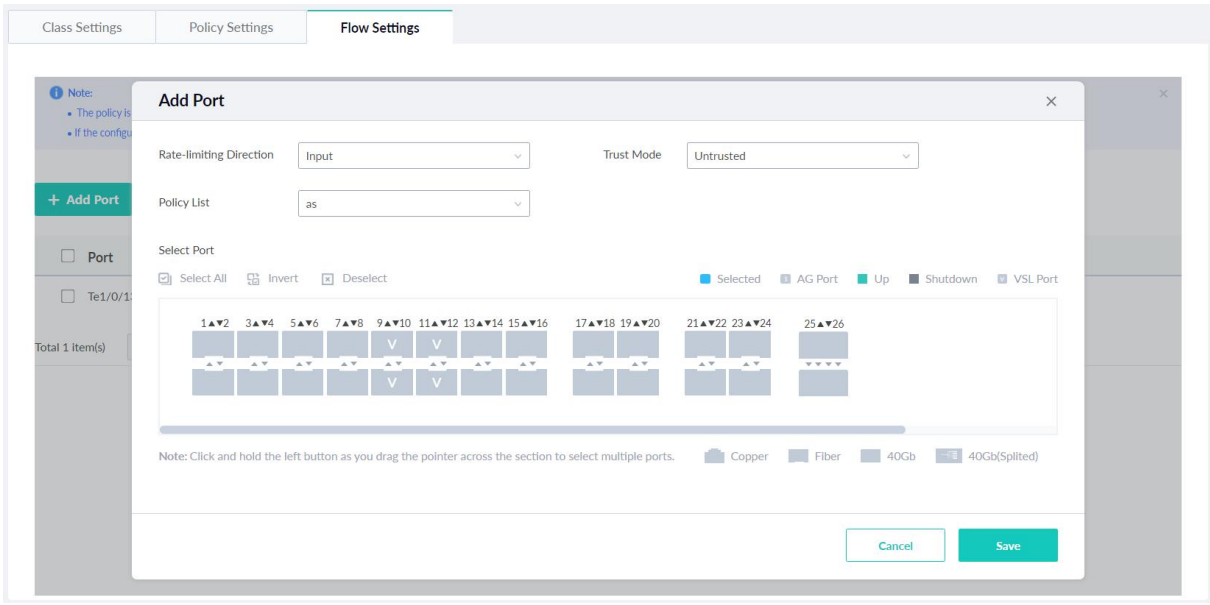
☆ Stream settings

The page of flow settings is as follows:



1.Add application policy port

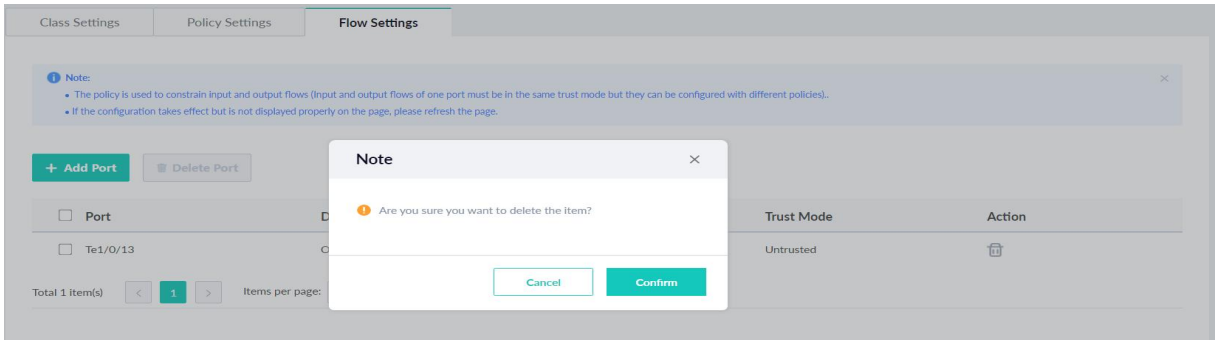
Set the application policy port, select the speed limit direction, trust mode, policy list and port, click "Save configuration" and prompt "Setup successful", it will be displayed in the application policy port list.



2.Delete application policy port

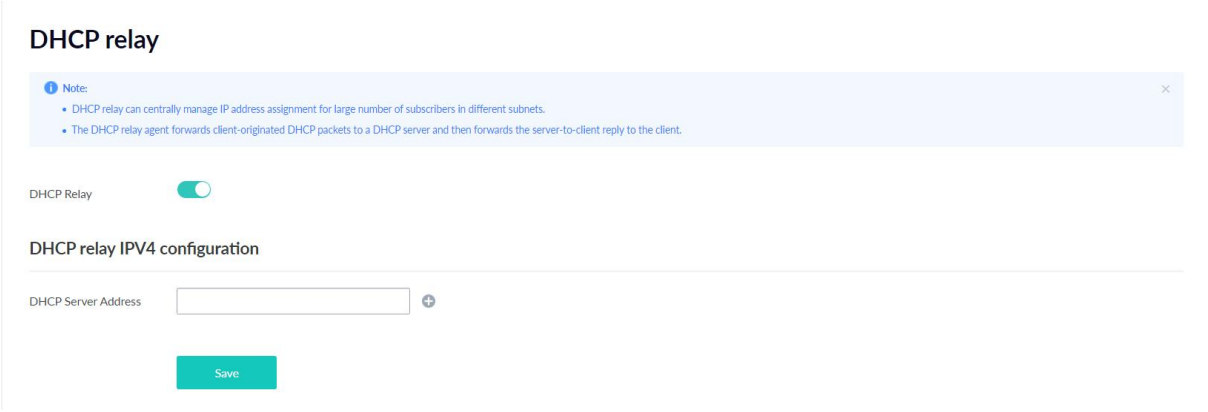
1) Select multiple records in the "Application Policy Port List" and click <Delete Selected Application Policy> to delete data in batches.

2) Click the <Delete> icon in the operation column of the last column of "Apply Policy Port List", and prompt "Are you sure to delete this item?", click OK and prompt "Delete successfully" to complete the deletion.

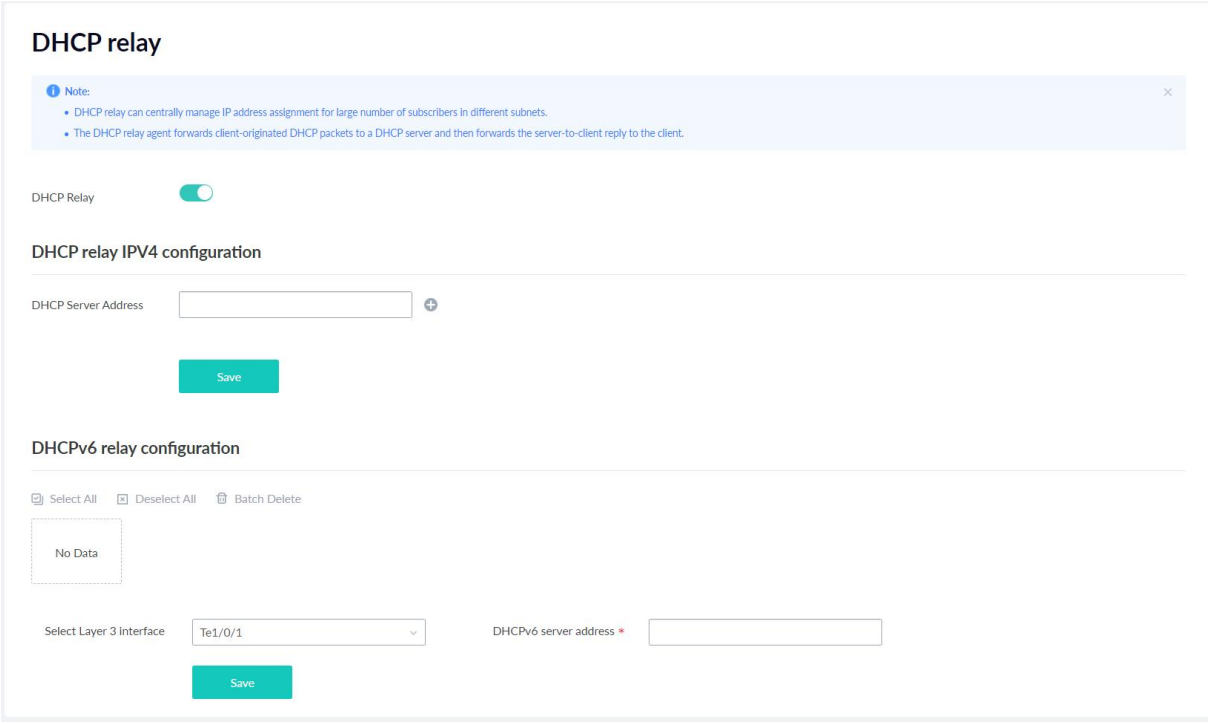


DHCP relay

The DHCP relay page is as follows:



Turn on or turn off the DHCP relay. When turned on, you can set multiple DHCP server addresses

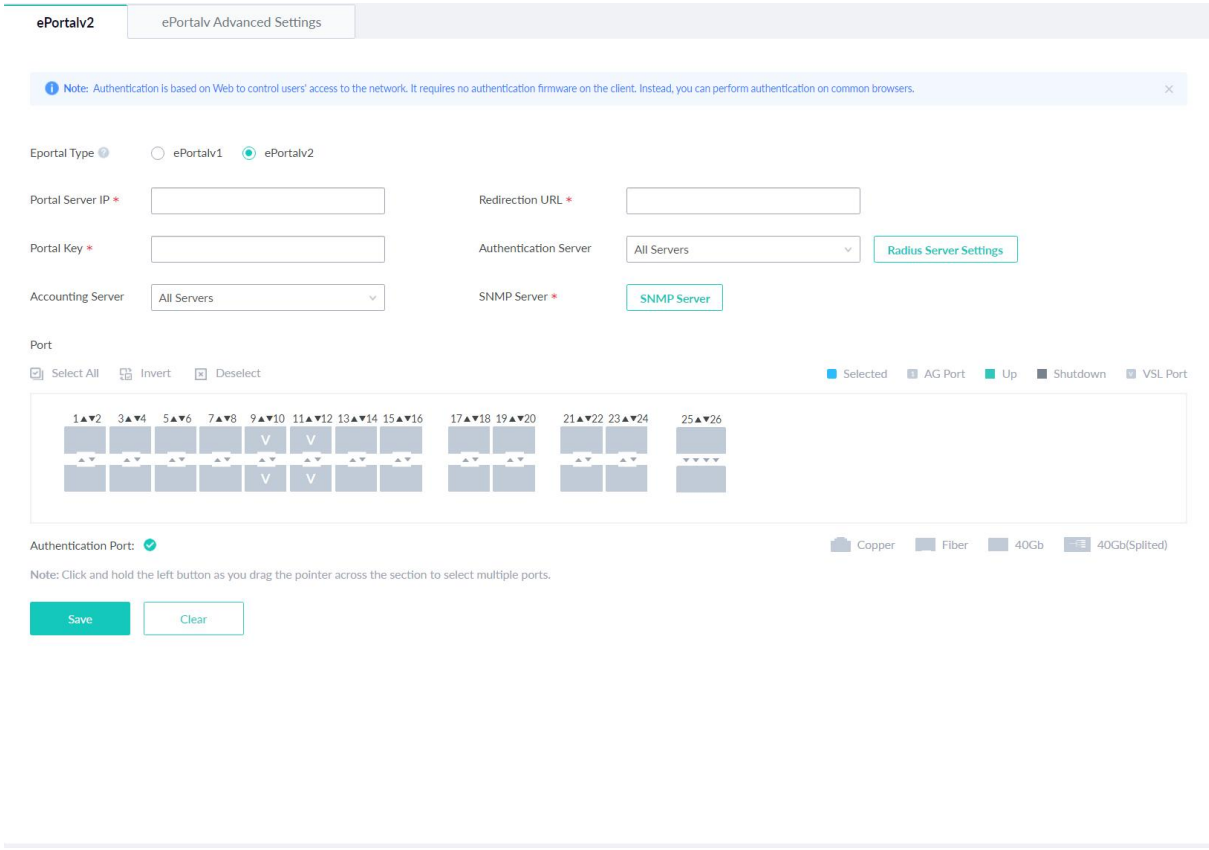


Online real-name authentication

"Internet real-name authentication" can carry out external web authentication and advanced settings.

☆ External web authentication

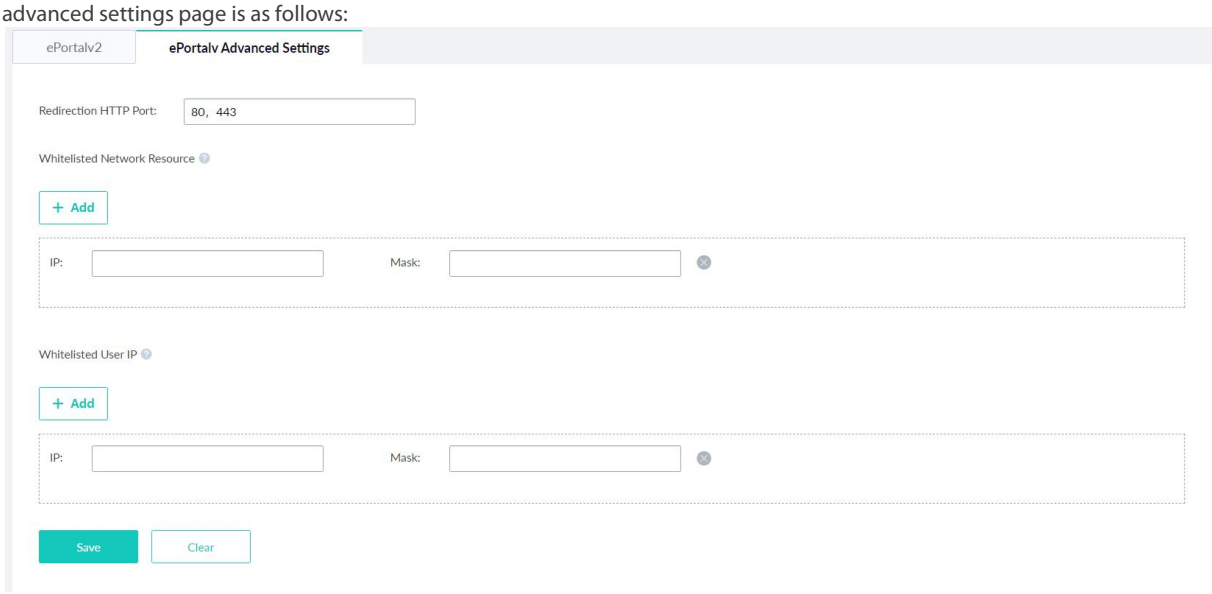
The page for external web authentication is as follows:



Server IP address, redirect homepage is required, click "Save Settings" to prompt the setting is successful.

☆ ePortalv Advanced Settings

The advanced settings page is as follows:



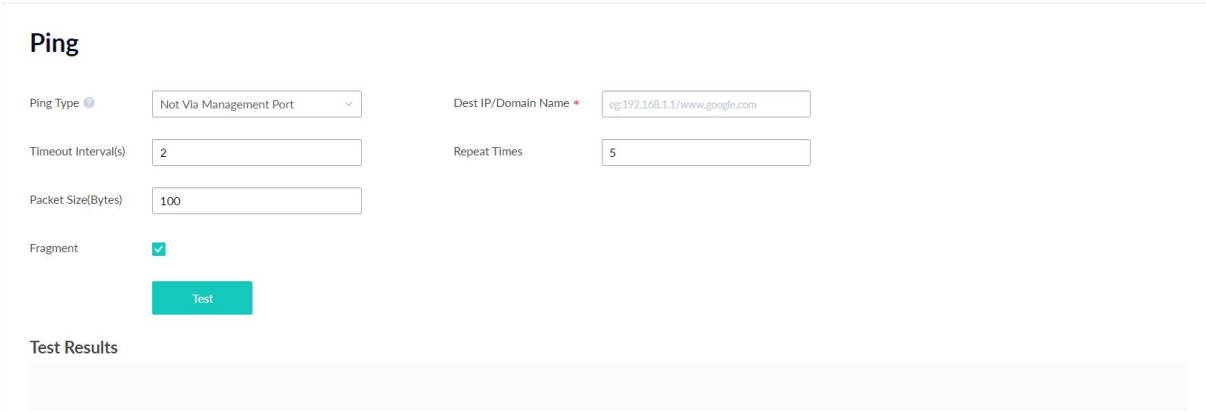
Authentication-free network resources and authentication-free users can set multiple values. Under other configuration settings, click the "Save Settings" icon to prompt that the settings are successful

1.3.4 Diagnosis

Through the first level menu "Security", you can enter the second level menu. Including DHCP Snooping, ARP attack prevention, IP Source Guard, port security, NFPP, storm control.

Network diagnosis

PING detection



PING method

Set to use out-of-band channels. It is only supported on devices that support MGMT. When the MGMT port is designated as the source interface, the management port must be selected, otherwise, the non-management port must be selected.

Destination IP address or domain name

The address or domain name to be pinged.

overtime time

Specify the timeout period.

repeat times

Specify the number of data packets sent.

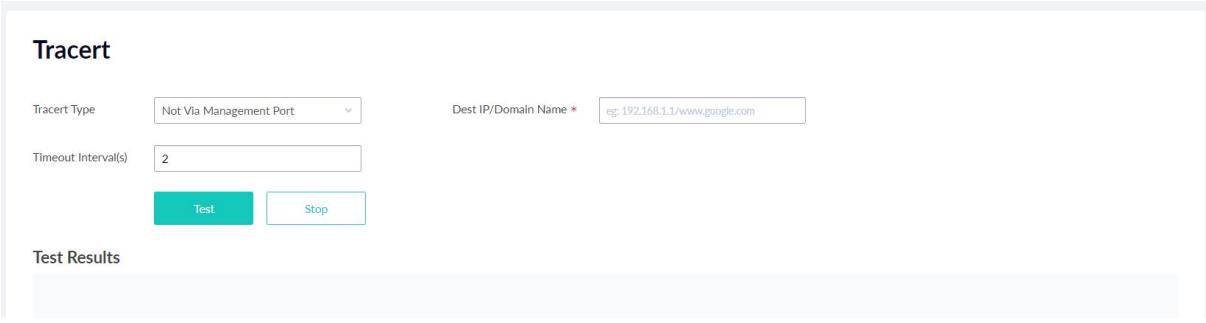
Packet size

Specify the length of the data padding segment of the sent packet.

Allow fragmentation

Set the DF flag of the IP. When the DF bit is set to 1, it means that the packet will not be segmented. The default DF bit is 0.

tracert detection



Tracert method

Set to use out-of-band channels. It is only supported on devices that support MGMT. When the MGMT port is designated as the source interface, the management port must be selected, otherwise, the non-management port must be selected.

Destination IP address domain name

Tracert's destination address or domain name address.

overtime time

The specified timeout period.

One-click collection

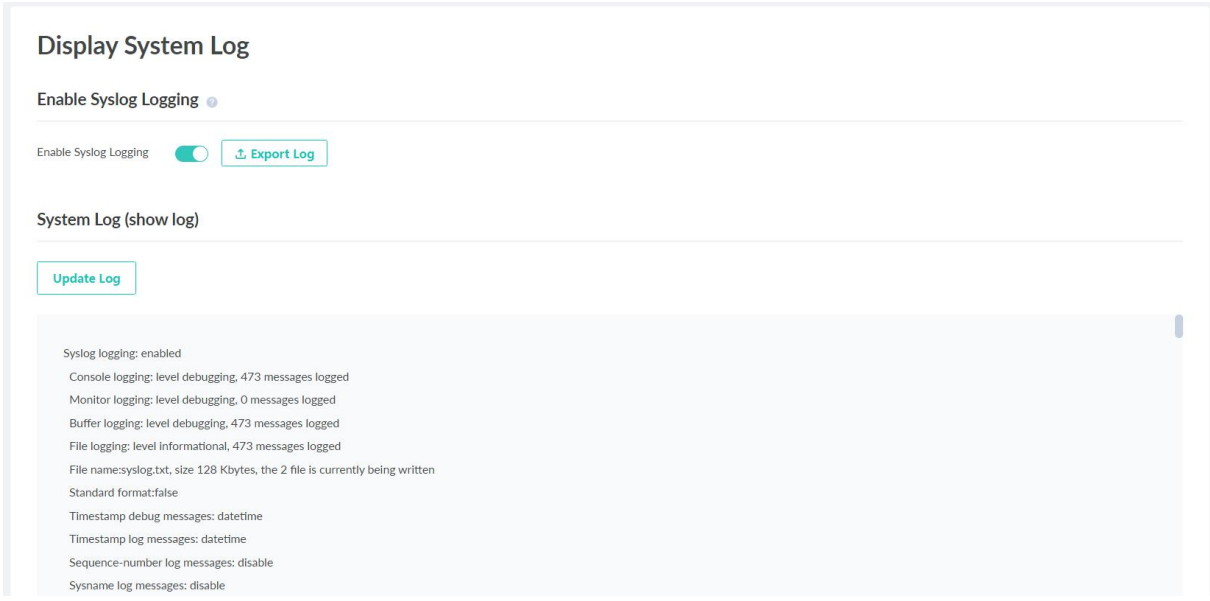
One-click collection will collect equipment fault information, which is convenient for troubleshooting equipment faults.



Log

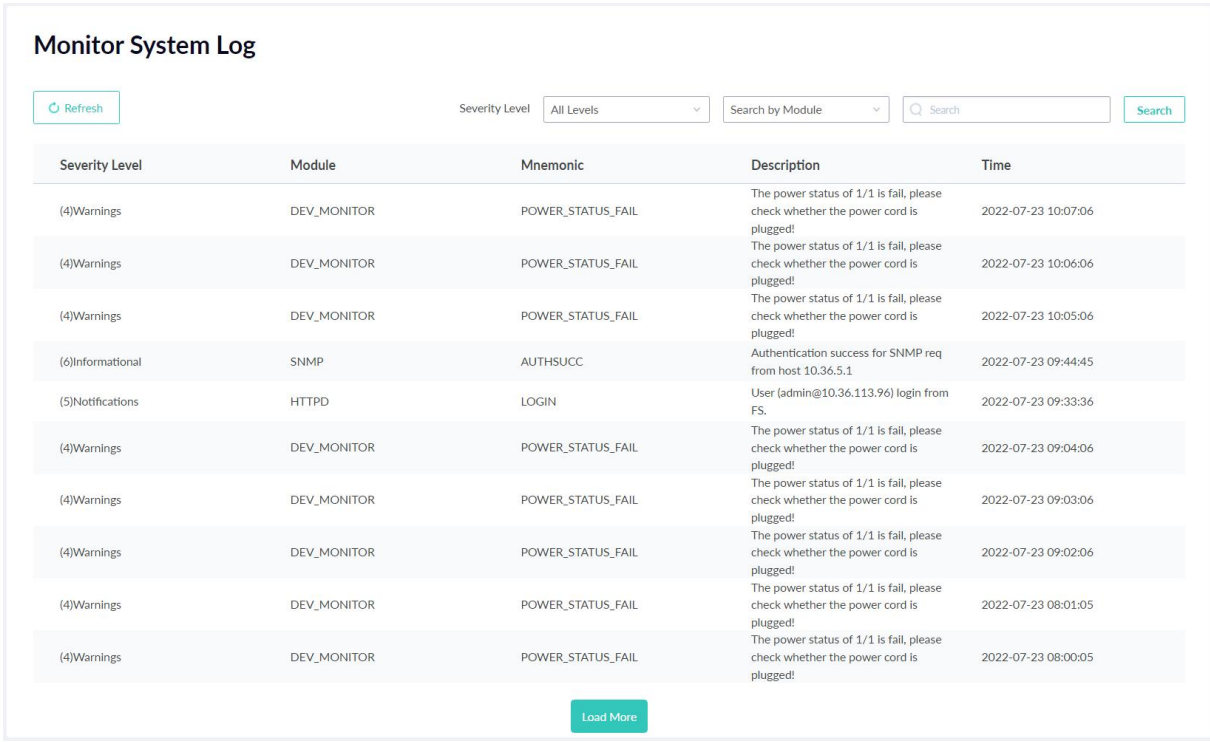
System log

Configure the syslog log to help customers locate problems in after-sales and R&D.



System log monitoring

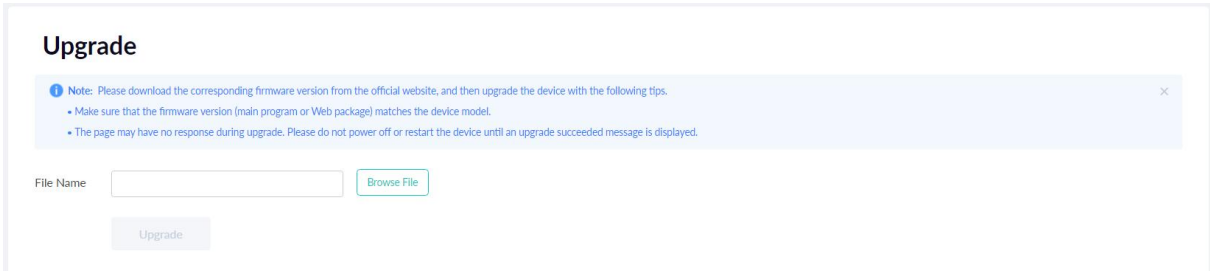
The log can be queried according to the level and module for customer assistance in after-sales and R&D positioning problems.



1.3.5 Maintain

Switch management

upgrade

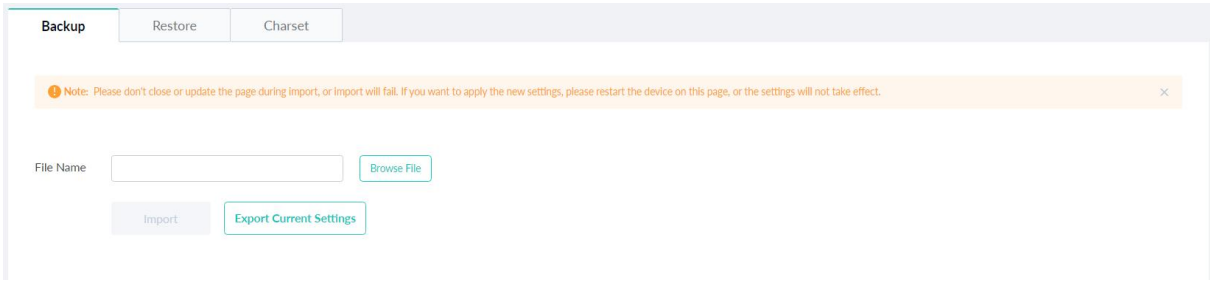


Click Browse, select the bin file saved locally, and then click the <Start Upgrade> button to implement the local upgrade operation.

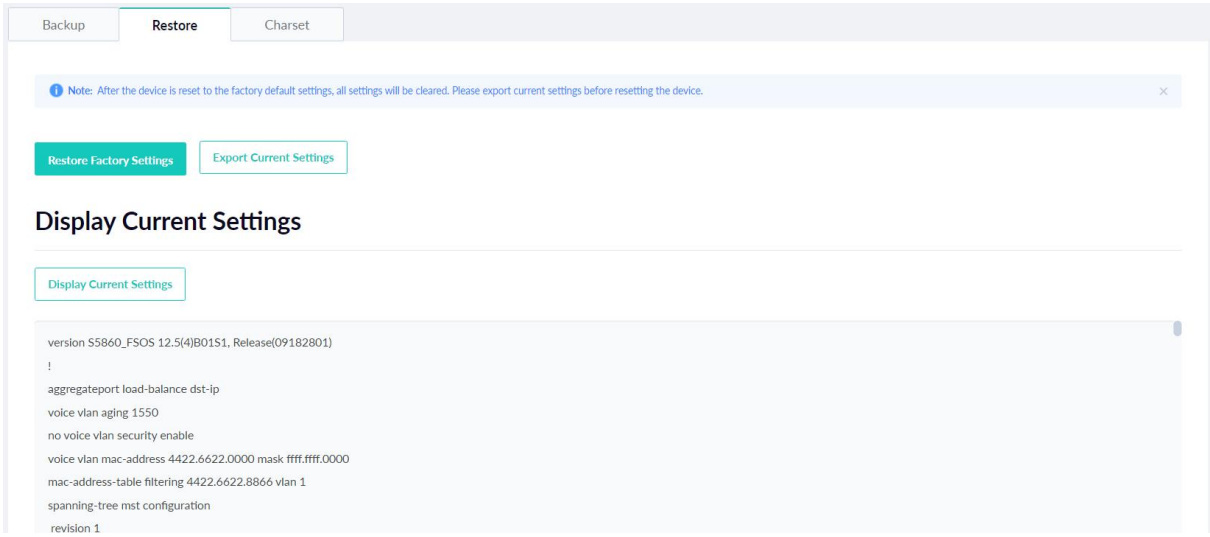
Configuration management

Configuration backup

Back up the configuration files on the device, import and export the configuration, and perform batch operations on the configuration, which is more convenient for users to operate.

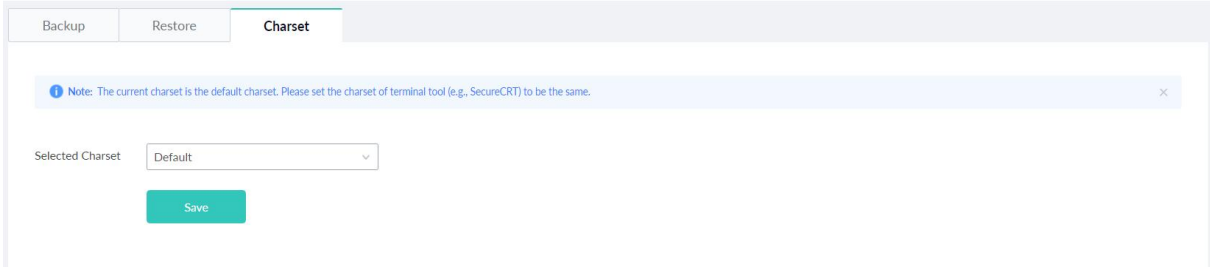


Restore factory configuration



Clear the configuration information and restore to the original state. Need to use the factory setting ip to revisit the WEB.

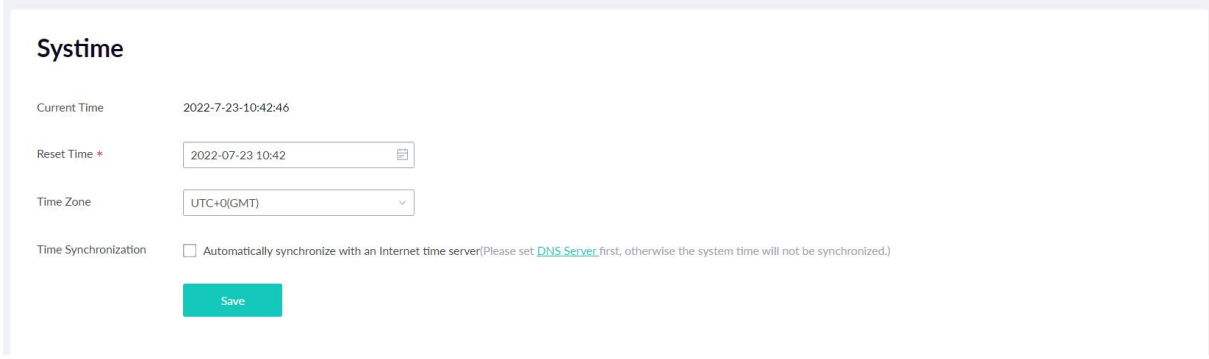
System character set



System character set, GBK, UTF-8, default, web recommends to configure UTF-8 encoding, use SecureCRT and other terminal tools, it is recommended to keep the same, otherwise there will be garbled codes.

system time

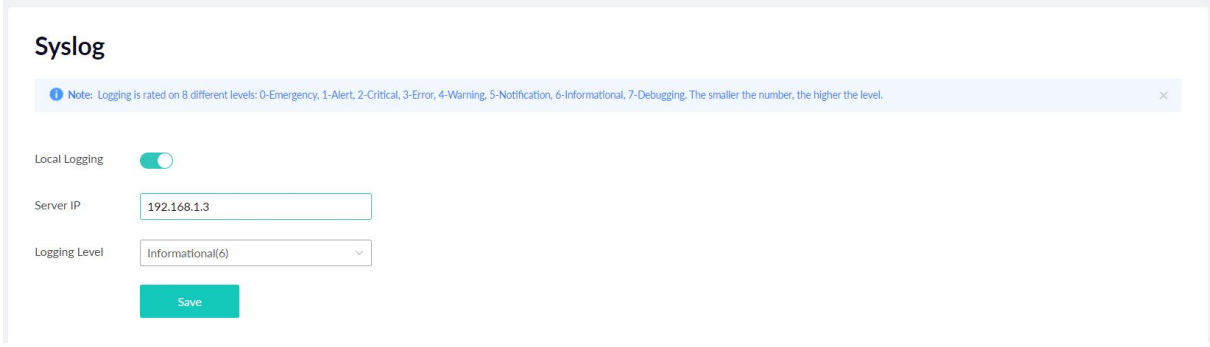
Set the system time through the area where the device is located to make the device information accurate and clear.



The page shows the current system time. You can manually set the current system time, or you can set the time by checking "Automatically synchronize with the Internet time server". Choose one of the two for configuration. Finally, click the <Save Settings> button to prompt "Save Settings Successfully" to complete the configuration.

Log server

The local log of the device is sent to the corresponding server for storage, and the history is saved for easy reference.



Set the IP address of the system log server and the log level parameters to be sent. After the setting is completed, the device will send the SYSLOG log to the corresponding server.

DNS

The DNS server is configured to perform dynamic domain name resolution.

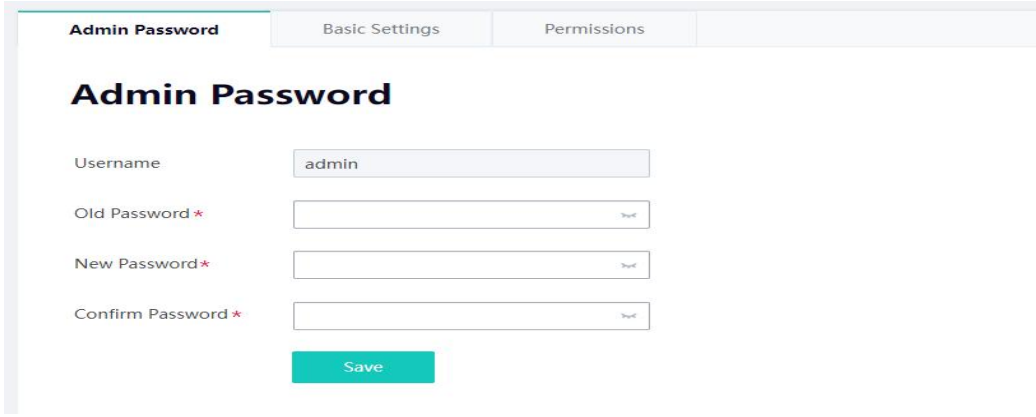


Network management configuration

WEB configuration management

☆ **Administrator password**

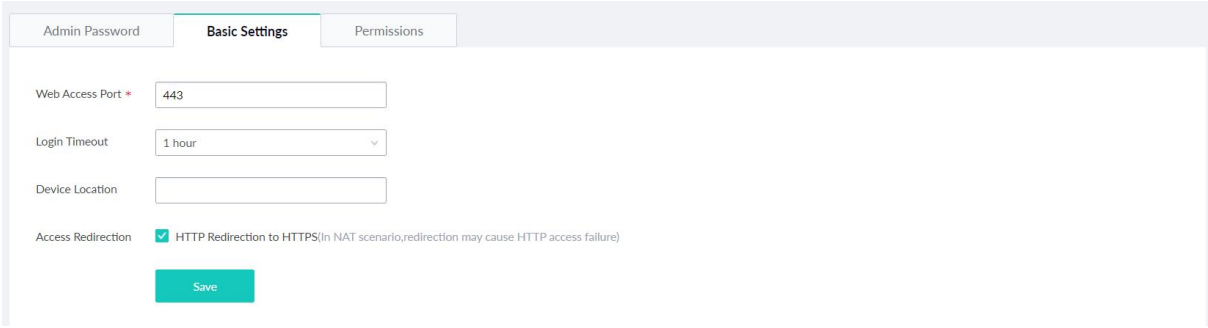
In order to improve system security and make information interaction more secure, please modify the system default password.



Web user password modification requires the old password and the new password twice. When the old password is entered incorrectly, the red text "The original password entered is incorrect" will be prompted after the input box. You need to enter the correct old password and click the <Save Configuration> button to complete the modification.

The enable password is also changed by default when changing the web network management password.

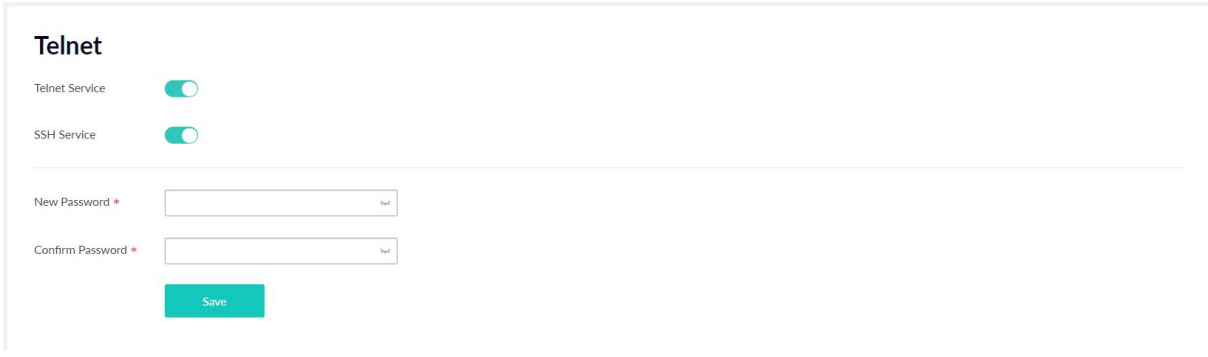
☆ Basic configuration



Basic configuration In order to facilitate the management of the device, configure the device to check the device with a better location. Set the timeout time, and the WEB will automatically exit after leaving for a long time to ensure the safety of your system.

Telnet

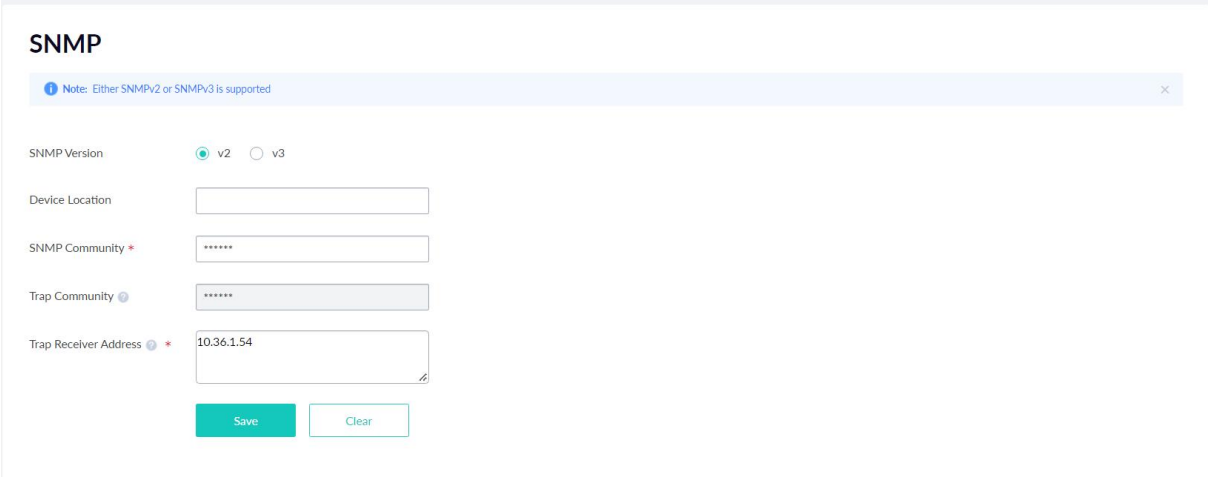
In order to improve system security and make information interaction more secure, please configure the telnet function.



To modify the telnet password, you do not need to enter the old password, just enter the same new password twice, and the other operations are the same as modifying the super user password.

SNMP

SNMP simple network management protocol, they provide a method to collect network management information from devices on the network, and can manage many network devices.



Select the SNMP version, the device ID, SNMP password and Trap receiving host are mandatory, other settings are optional, click <Save Settings> to prompt "Setup Successful".

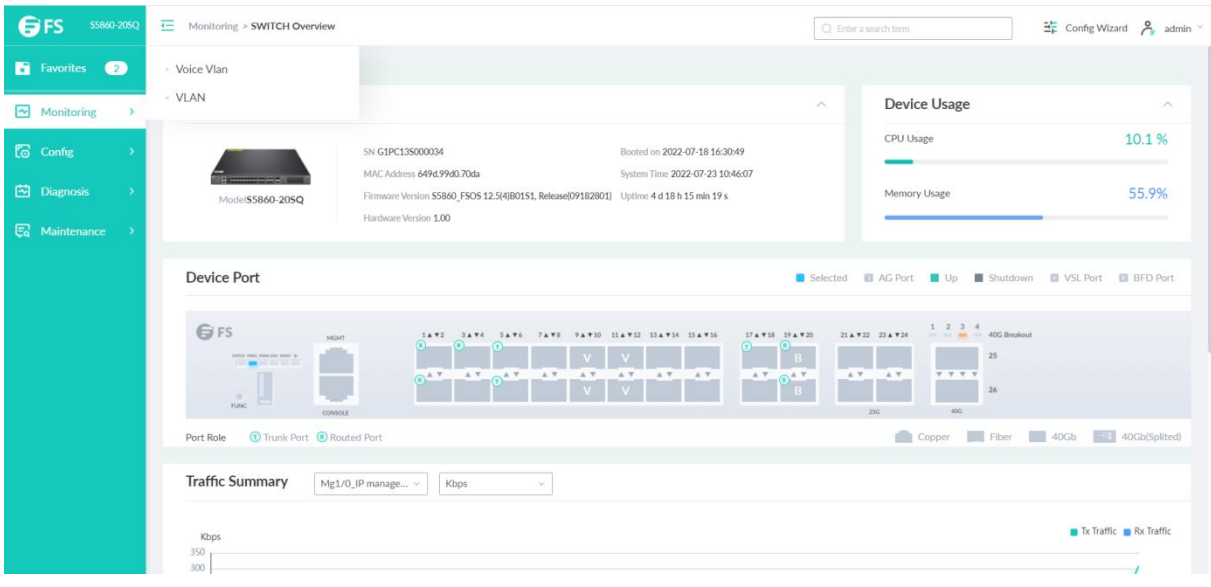
1.3.6 Other Functions

Menu favorites

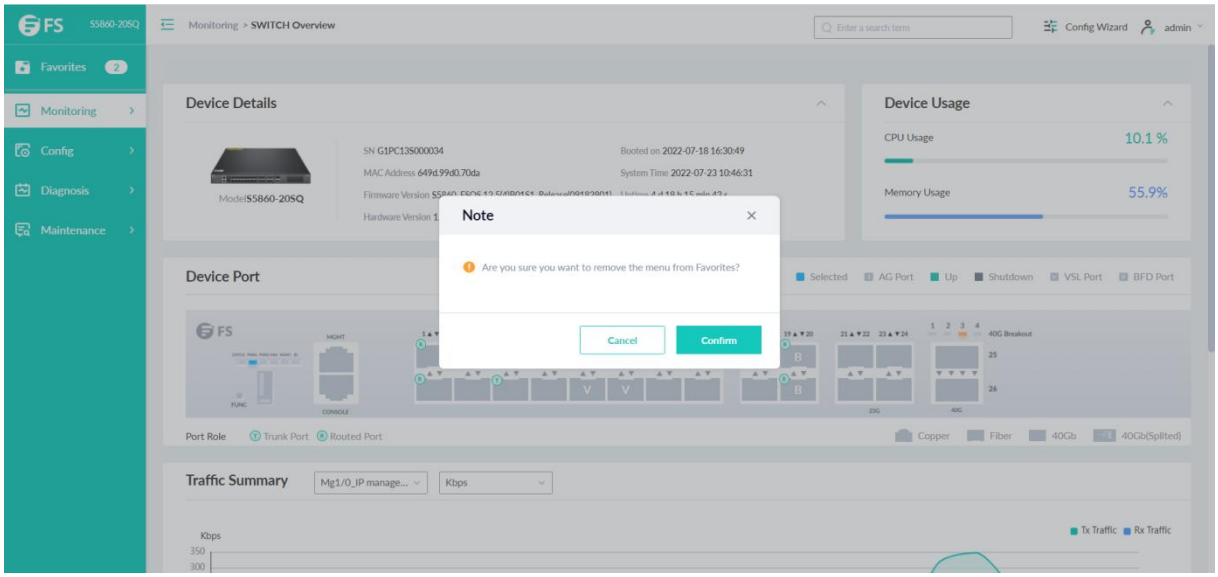
When users want to collect frequently configured functions, they can quickly click the menu and configure next time.

To ensure the meaning of favorites, currently only 10 menus can be favorited

1.Add to favorites

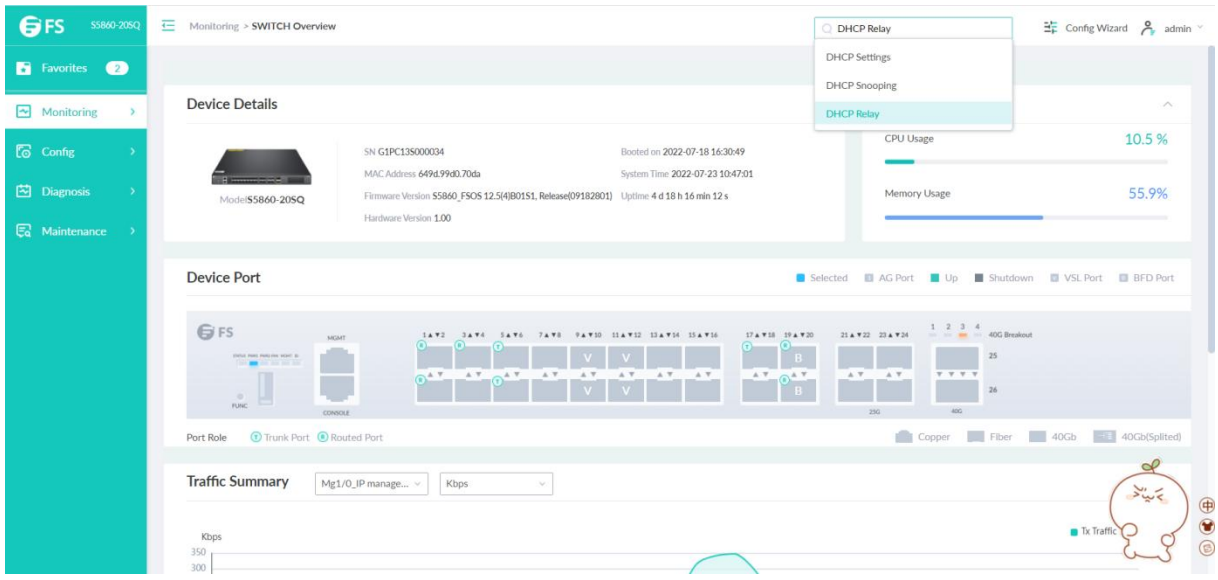


3.Unfavorite



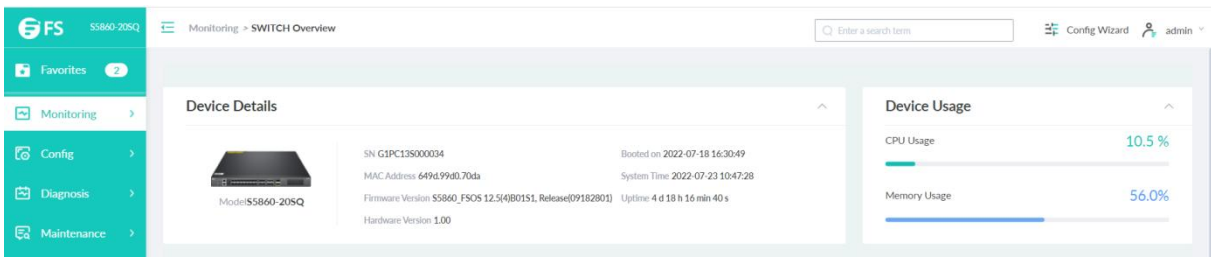
Quick query menu

The system has more and more functions, and the quick query menu is convenient for users to quickly find the functions they want.



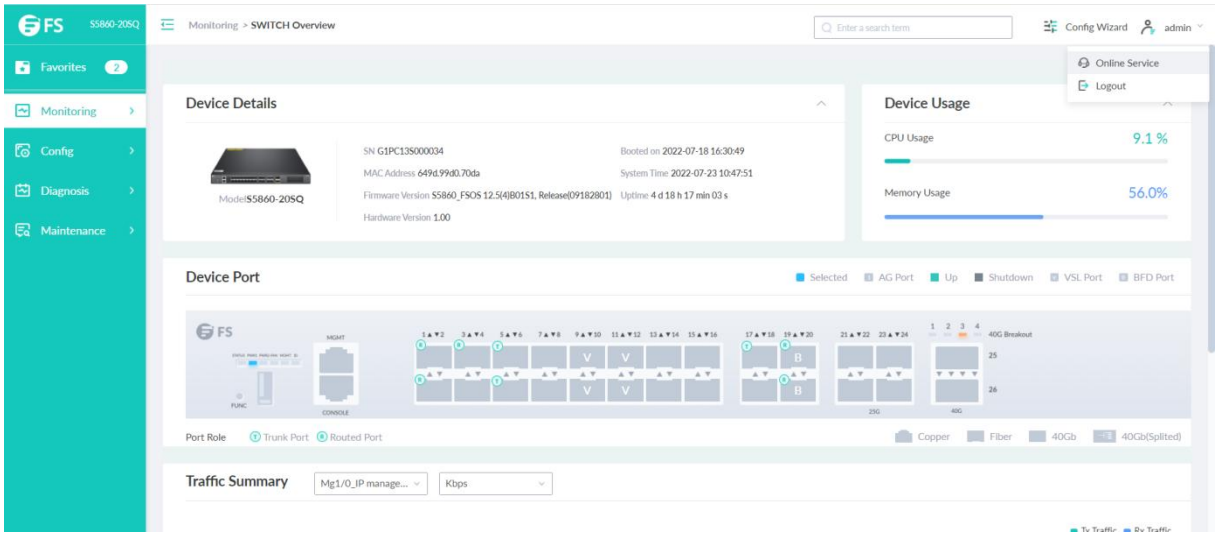
More functions of the system

1.Show current account

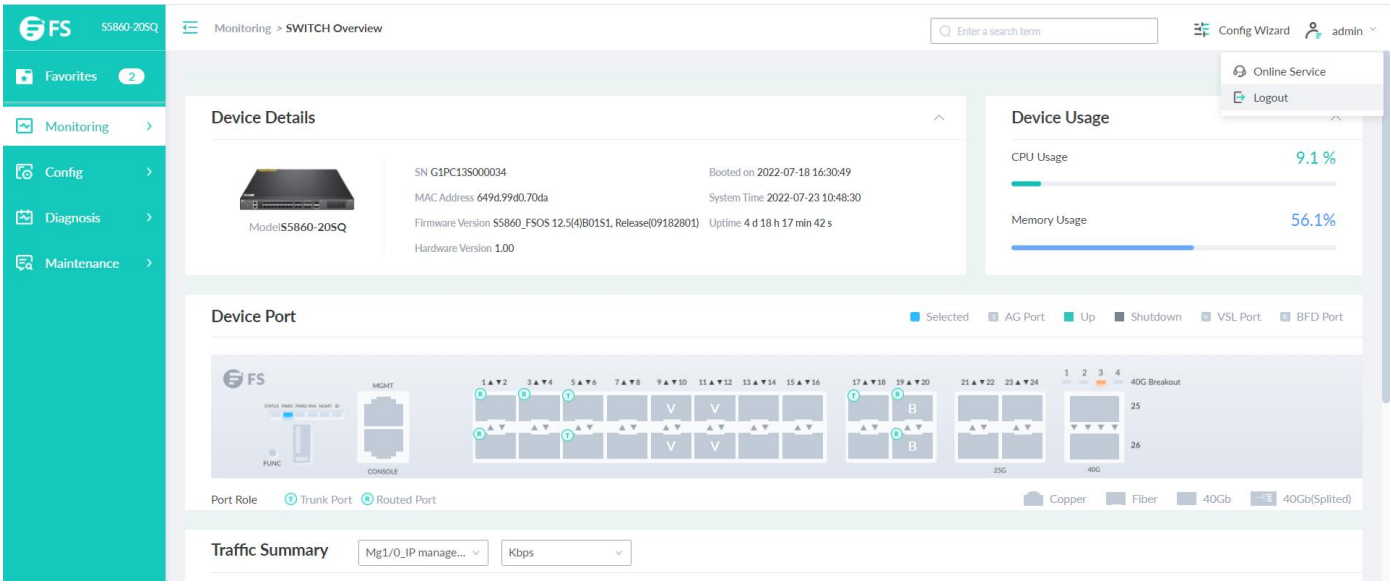


2.online service

Click on the online customer service on the page to jump to the online customer consultation question



3.Exit system



1.4 Open WEB Server

When the switch leaves the factory, the WEB service is turned on, and the default IP: 192.168.1.1

The following describes how to open it under CLI when the WEB service is closed.。

Configuration item	Related commands	
	enable service web-server	Open WEB service

Configure WEB server	ip address	Optional configuration IP address
	webmaster level username password	Optional configuration, login account password information for WEB management

Configuration method

☆ **Open WEB service**

⇌ Must be configured.

⇌ Configure on the switch.

☆ **Configure IP address**

⇌ Optional.

☆ **Configure the account and password information for logging in to WEB management**

⇌ Optional.

⇌ When the WEB service is turned on, the default administrator account admin/admin is created. The account password can be modified.

Testing method

Log in to the WEB interface through the set IP address and the account password of WEB management to check whether you can log in normally.

Related commands

☆ **Start WEB service**

【Command format】	enable service web-server [http | https | all]
【Parameter Description】	http | https | all: Open the corresponding service. http is to open HTTP service, https is to open HTTPS service, all is to open HTTP and HTTPS service at the same time. The default is to enable both HTTP and HTTPS services.
【Command Mode】	Global mode

☆ Configure IP address

【Command format】	**ip address** *ip-address ip-mask*
【Parameter Description】	*ip-address*：ip address *ip-mask*：Netmask
【Command Mode】	Interface mode

☆ Configure the account and password information for logging in to WEB management

【Command format】	**webmaster level** *privilege-level* **username** *name* **password** { *password* | [**0 | 7**] *encrypted-passw*
【Parameter Description】	*privilege-level*: User binding privilege level, divided into three levels: 0/1/2. The default super administrator account admin corresponds to level 0 permissions, and other manually created accounts correspond to level 1. *name*: The address of the static RP. *password*: Use ACL to limit the group address range of the static RP service. The default is to serve all groups. *0* | *7*: The encryption type of the password, 0 is no encryption, 7 is simple encryption. The default is 0. *encrypted-password*: password text.
【Command Mode】	Global mode
【User guides】	-

Configuration example

☆ **Configure WEB server**

[Configuration method]	● Open WEB service ● Configure the device management IP. The default management VLAN is VLAN 1. Configure the IP of VLAN 1. Ensure that the user PC can ping the management IP.
	FS# configure terminal FS(config)#enable service web-server FS(config)# webmaster level 0 username test password test FS(config)#interface vlan 1 FS(config-if-VLAN 1)#ip address 192.168.1.200 255.255.255.0 FS(config)# end
【Testing method】	View related commands through show running-config.
	FS(config)#show running-config Building configuration... Current configuration : 6312 bytes ! hostname FS ! ! webmaster level 0 username test password test //WEB management authentication user name and password, password encryption display http update mode auto-detect ! ! interface VLAN 1 ip address 192.168.1.200 255.255.255.0 //Device management IP no shutdown ! line con 0 line vty 0 4 login ! ! End