ESW4L3 Series Switches

Web-based configuration guide

Legal Notice

Warranty

This publication is subject to change.

Teldat S.A. offers no warranty whatsoever for information contained in this manual.

Teldat S.A. is not liable for any direct, indirect, collateral, consequential or any other damage connected to the delivery, supply, or use of this manual.

Preface

Intended Audience

This document is intended for:

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

Technical Support

- Windbit Networks Website: https://www.windbit.com/

Conventions

1. Conversions

Convention	Description
Bold font	Commands, command options, and keywords appear in **bold**.
Italic font	Arguments for which you supply values appear in *italic*.
[ ]	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.
&<1-n>	The argument before the (&) sign can be inserted consecutively 1-n times.
//	Double slashes at the beginning of a line of code indicate a comment line.

2. Signs

The signs used in this document are described as follows:

❗ **Warning**

An alert that calls attention to important rules and information and may result in data loss or equipment damage if not heeded.

⚠ **Caution**

An alert that calls attention to essential information that if not understood or followed can result in function failure or performance degradation.

ⓘ **Note**

An alert that contains additional or supplementary information that if not understood or followed will not lead to serious consequences.

✓ **Specification**

An alert that contains a description of product or version support.

3. Note

The manual offers configuration information (including model, port type and command line interface) for indicative purpose only. In case of any discrepancy or inconsistency between the manual and the actual version, the actual version prevails.

1 Configuring Switch Eweb

1.1 Overview

This document describes how to use the eWeb management system. You can use the eWeb management system to configure common settings for switches.

You can access the eWeb management system through a browser (such as Google Chrome) to manage switches.

1.2 Typical Applications

Typical Application	Description
Managing Switches Through the eWeb Management System	Once switches are properly configured, you can access the eWeb management system through a browser to manage these switches.

1.2.1 Managing Switches Through the eWeb Management System

Configuration Environment Requirements

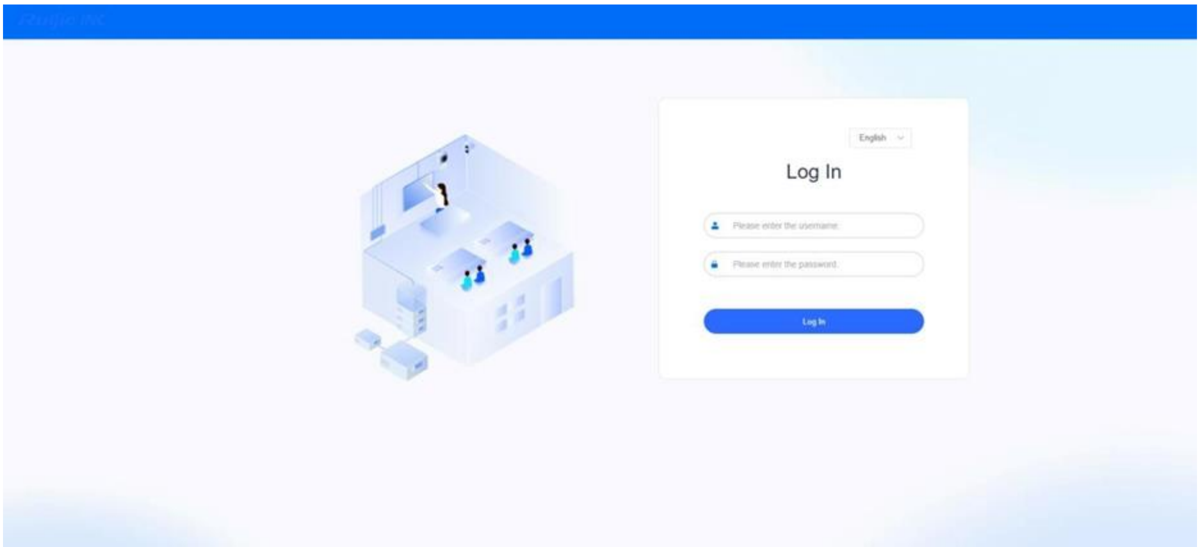
Client requirements:

1. Client: A client refers to a PC or a mobile terminal such as a laptop. A network administrator can log into the eWeb graphical user interface (GUI) of a switch from the client’s browser to manage switches.
2. Browser: Google Chrome is recommended. Exceptions such as garbled characters or formatting errors may occur if an unsupported browser is used.
3. Resolution: You are advised to set the resolution to 1600 x 900 or 1920 x 1080. If other resolutions are used, font and formatting issues may occur.

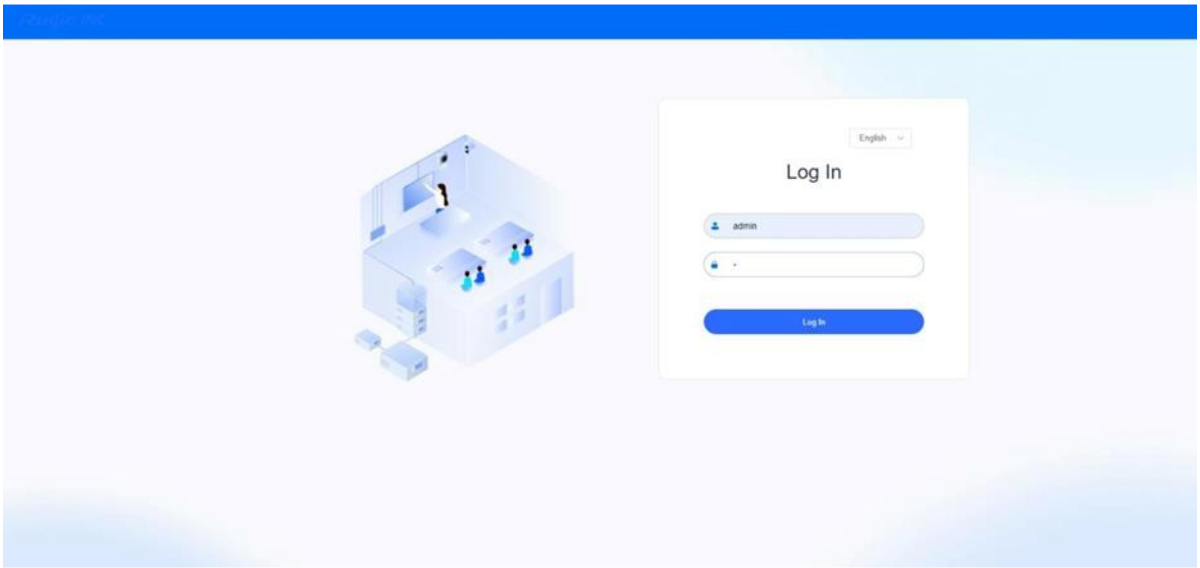
1.3 eWeb Management System

1.3.1 Logging In

Enter the switch IP address in your browser’s address bar. Make sure the IP address is reachable. The login page is displayed.



1. Enter the username and password and click on **Log In**. The main interface of the eWeb management system is displayed.
2. If you cannot remember your username or password, click on **Forgot Password?**
3. If you need customer service assistance, contact the local technical support.
4. To prevent login through brute-force cracking, your account will be locked for 10 minutes after 5 failed attempts. You cannot log in during the locking period.



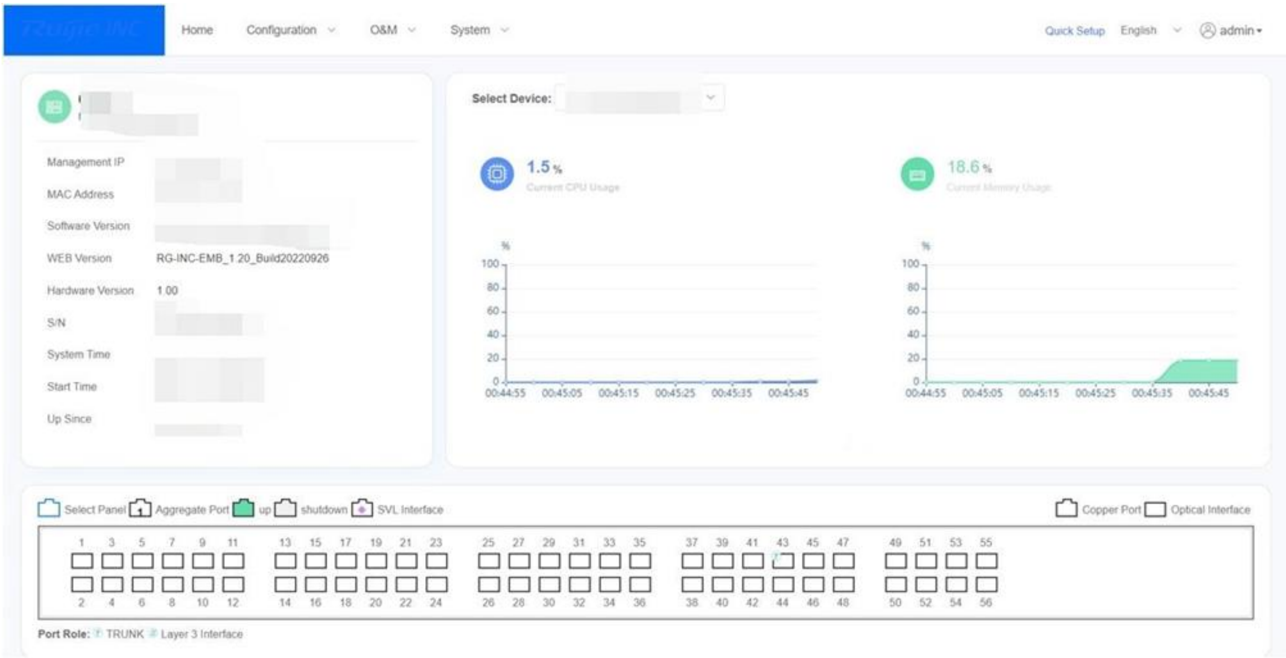
admin

Note

To use the eWeb management system, ensure that the web component has been installed on the switch and the web service has been enabled (if the web service is not enabled, run the enable service web-server command in config mode to enable it). Otherwise, the login page is not displayed. In most situations, the web component is integrated in the rgos.bin system by default. However, if it is not installed, you can install it via the upgrade file mentioned in this release note.

1.3.2 Main Interface

The main eWeb management system interface is displayed.



Management IP

MAC Address

Software Version

WEB Version RG-INC-EMB_1.20_Build20220926

Hardware Version 1.00

S/N

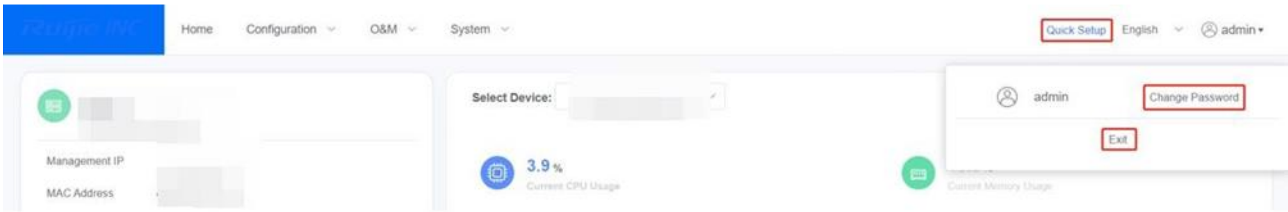
System Time

Start Time

Up Since

1. Header

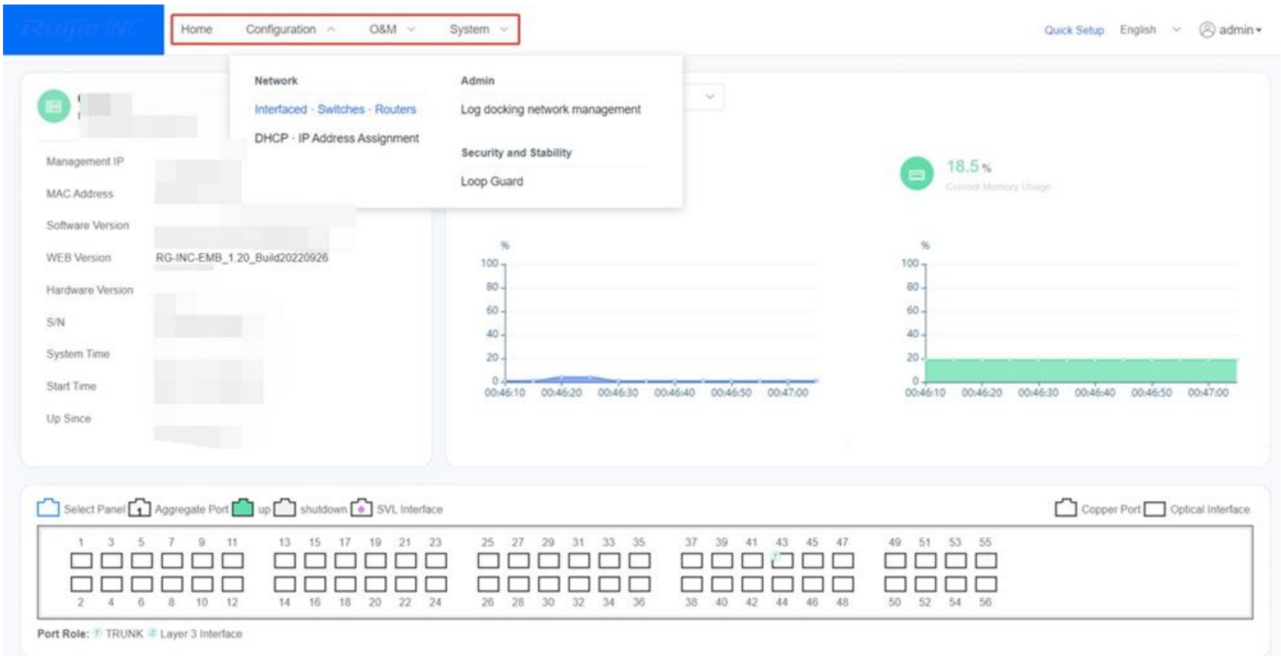
This area displays the links to common functions, including Quick Setup, Change Password, and Exit. You can click these links to switch to specific configuration pages.



- **Change Password**: After you click **Change Password**, the **Change Password** page is displayed. You can enter the old password and the new password to reset the password.
- **Exit**: When device management is complete, you can click Exit to exit the main interface and return to the login page.

2. Navigation Menu

This area displays main tabs of the eWeb management system.



Management IP [redacted]
MAC Address [redacted]
Software Version [redacted]
WEB Version RG-INC-EMB_1.20_Build20220926
Hardware Version
S/N [redacted]
System Time [redacted]
Start Time
Up Since [redacted]

3. Main Operation Area

In this area, you can perform configurations on the eWeb management system. When you click the shortcut menu at the top of the page, the detailed configuration page is displayed.

1.3.3 Quick Setup

The switch is not configured when you log in to the eWeb management system for the first time. To simplify the configuration, you can use the **Quick Setup** wizard to configure common settings for the switch.

Note

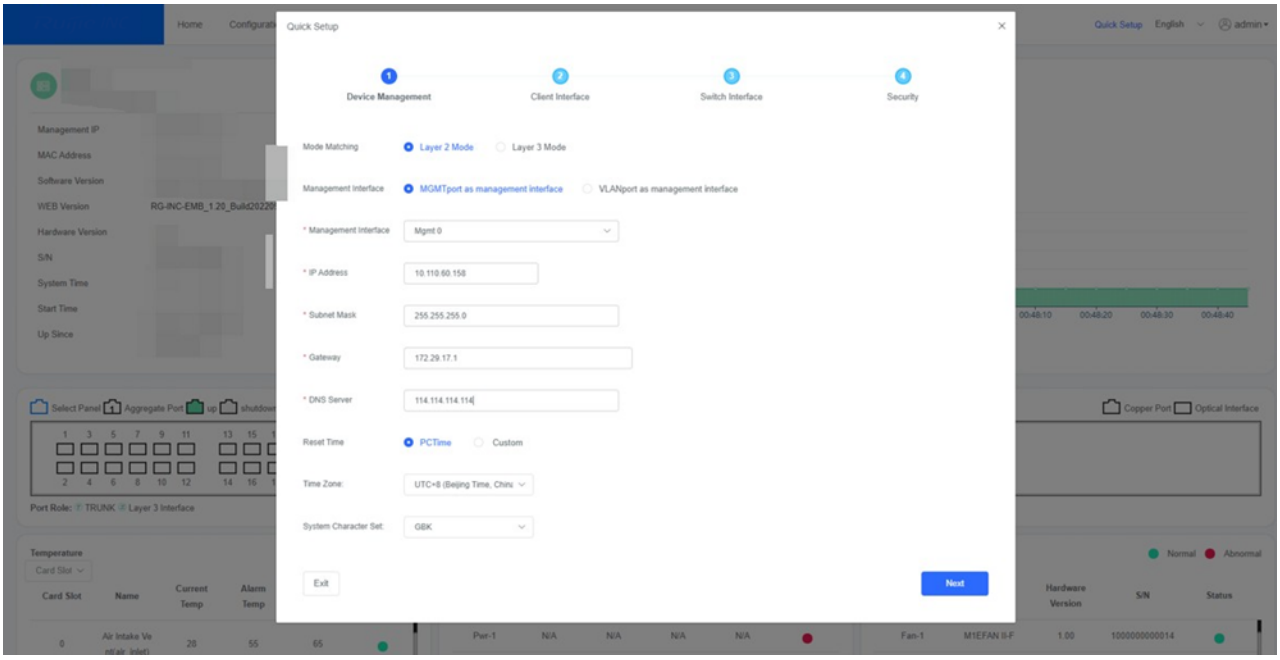
You can click **Quick Setup** in the upper-right corner of the main interface of the eWeb management system to open the **Quick Setup** wizard.

1. Quick Setup

Layer 2 Mode

There are four steps in this mode.

(1) Device Management



Quick Setup

Mode Matching: ● Layer 2 Mode ○ Layer 3 Mode

Management Interface: ● MGMTport as management interface ○ VLANport as management interface

* Management Interface: Mgmt 0

* IP Address: 10.110.60.158

* Subnet Mask: 255.255.255.0

* Gateway: 172.29.17.1

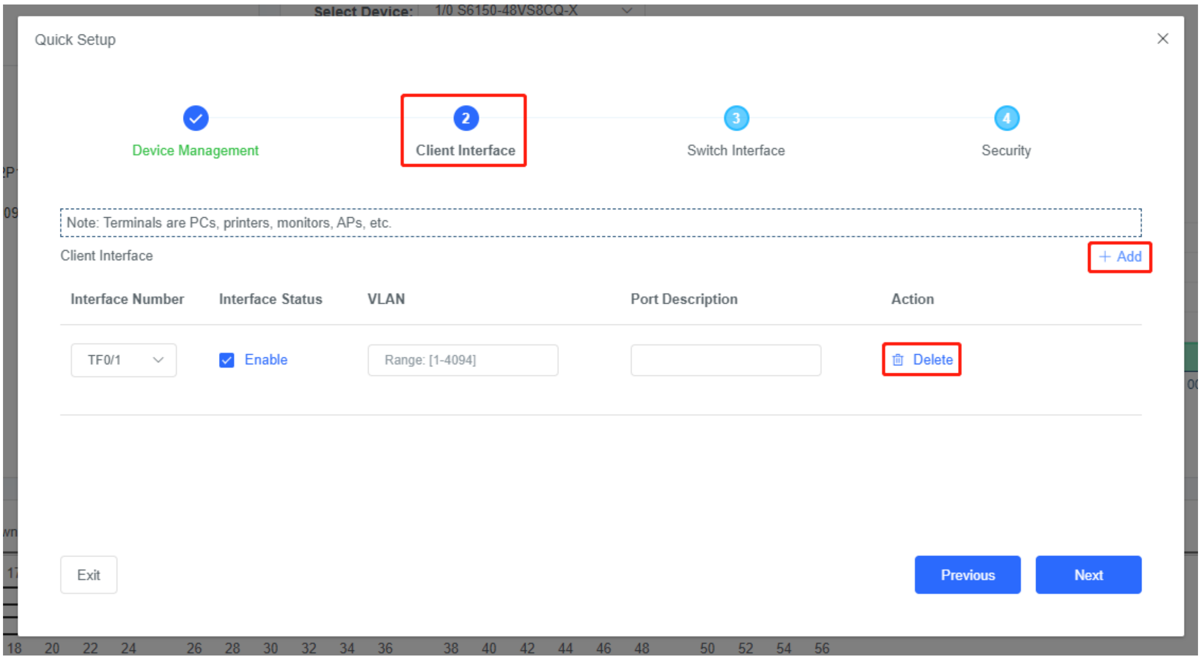
* DNS Server: 114.114.114.114

Reset Time: ● PCTime ○ Custom

Time Zone: UTC+8 (Beijing Time, Chin

System Character Set: GBK

(2) Client Interface



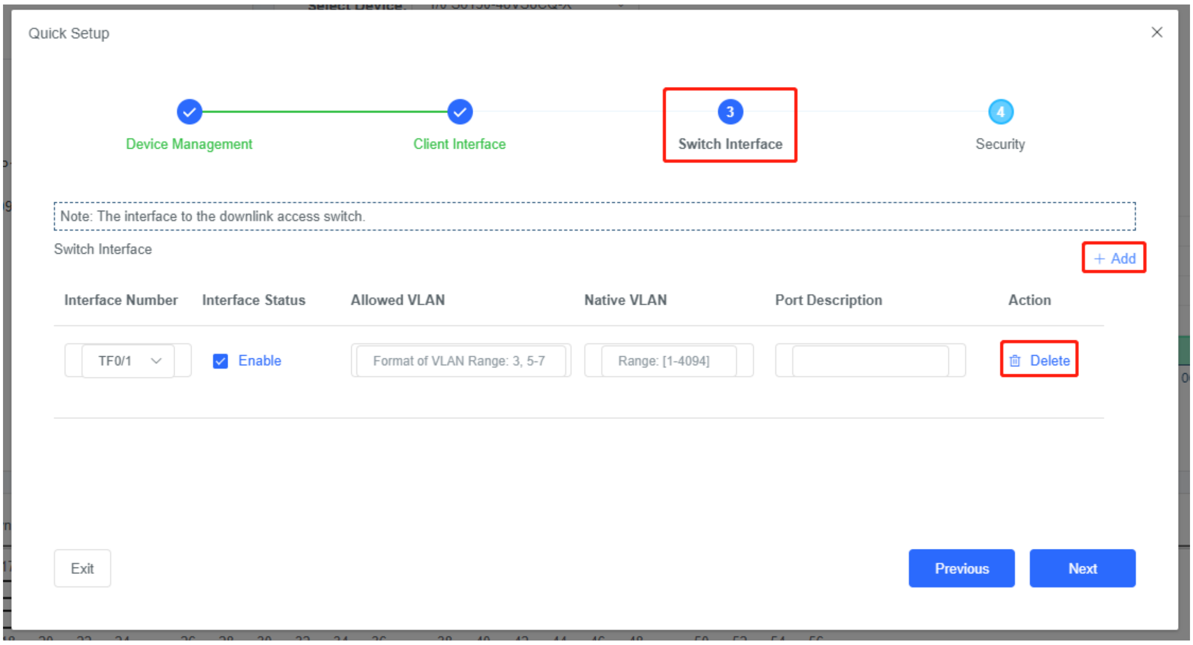
Quick Setup

Note: Terminals are PCs, printers, monitors, APs, etc.

Client Interface

Interface Number	Interface Status	VLAN	Port Description	Action
TF0/1	☑ Enable	Range: [1-4094]		Delete

(3) Switch Interface

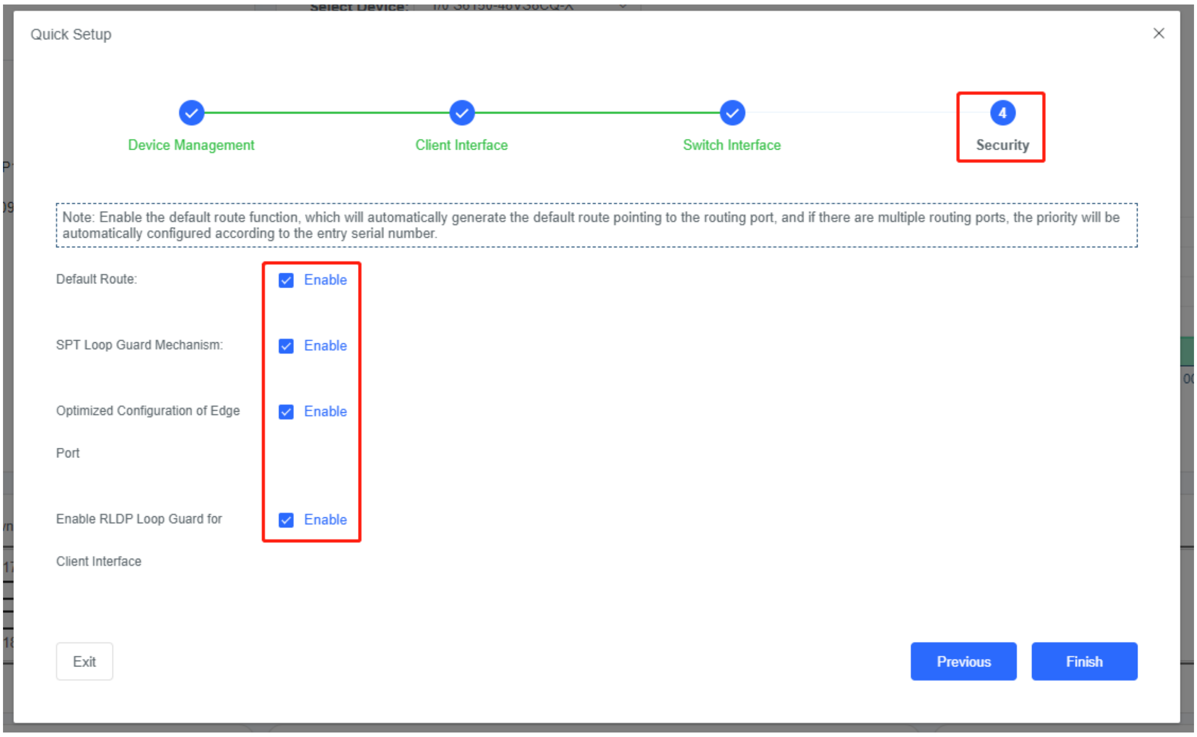


Note: The interface to the downlink access switch.

Switch Interface

Interface Number	Interface Status	Allowed VLAN	Native VLAN	Port Description	Action
TF0/1	☑ Enable	Format of VLAN Range: 3, 5-7	Range: [1-4094]		Delete

(4) Security



Note: Enable the default route function, which will automatically generate the default route pointing to the routing port, and if there are multiple routing ports, the priority will be automatically configured according to the entry serial number.

Default Route: ☑ Enable

SPT Loop Guard Mechanism: ☑ Enable

Optimized Configuration of Edge Port ☑ Enable

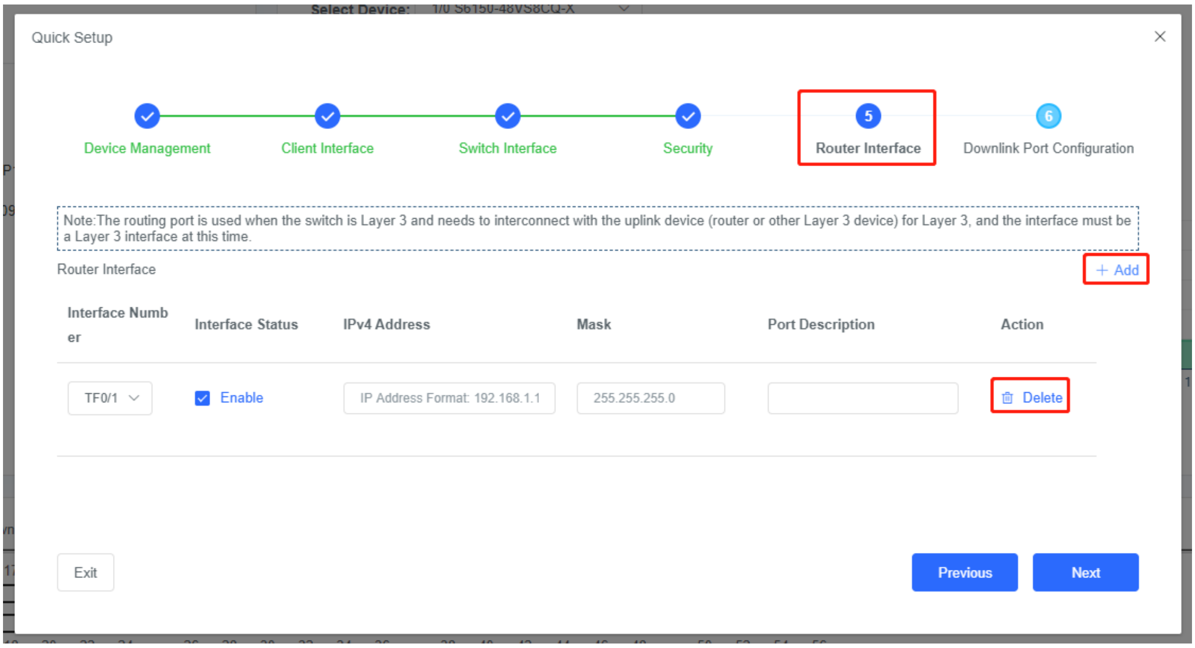
Enable RLDP Loop Guard for Client Interface ☑ Enable

Layer 3 Mode

There are six steps in this mode.

The first four steps are the same as those in Layer 2 mode, so only the last two steps are described here.

(1) Router Interface (Layer 3 Mode)

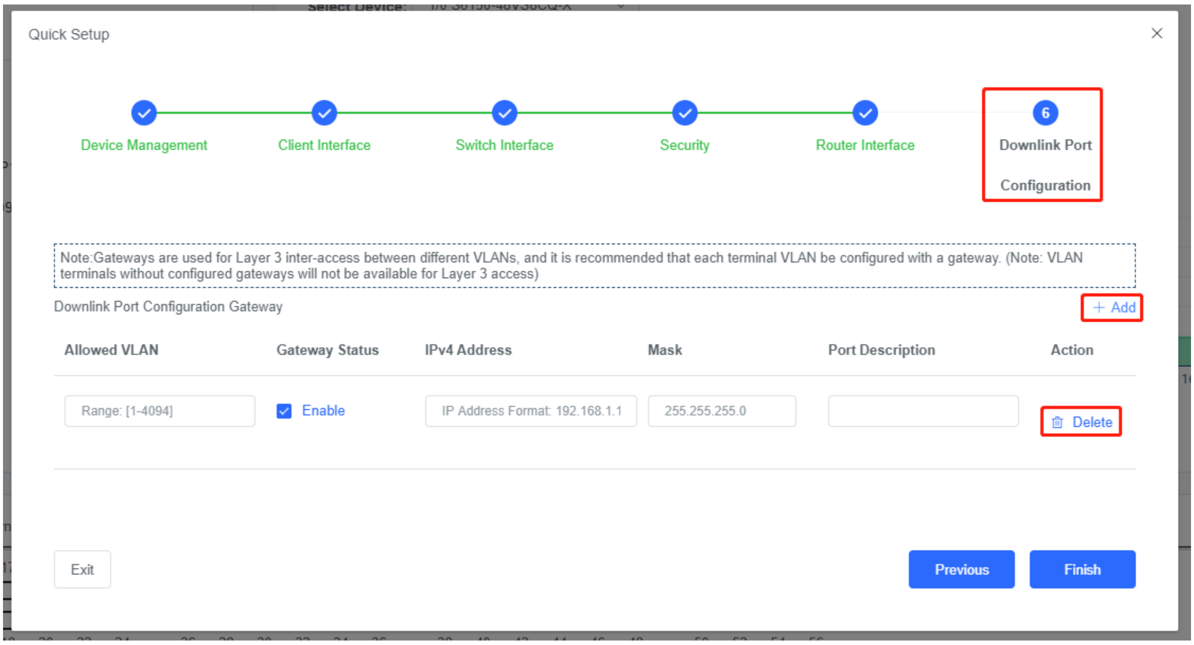


Note:The routing port is used when the switch is Layer 3 and needs to interconnect with the uplink device (router or other Layer 3 device) for Layer 3, and the interface must be a Layer 3 interface at this time.

Router Interface

Interface Number	Interface Status	IPv4 Address	Mask	Port Description	Action
TF0/1	☑ Enable	IP Address Format: 192.168.1.1	255.255.255.0		Delete

(2) Downlink Port Configuration (Layer 3 Mode)



Note:Gateways are used for Layer 3 inter-access between different VLANs, and it is recommended that each terminal VLAN be configured with a gateway. (Note: VLAN terminals without configured gateways will not be available for Layer 3 access)

Downlink Port Configuration Gateway

Allowed VLAN	Gateway Status	IPv4 Address	Mask	Port Description	Action
Range: [1-4094]	☑ Enable	IP Address Format: 192.168.1.1	255.255.255.0		Delete

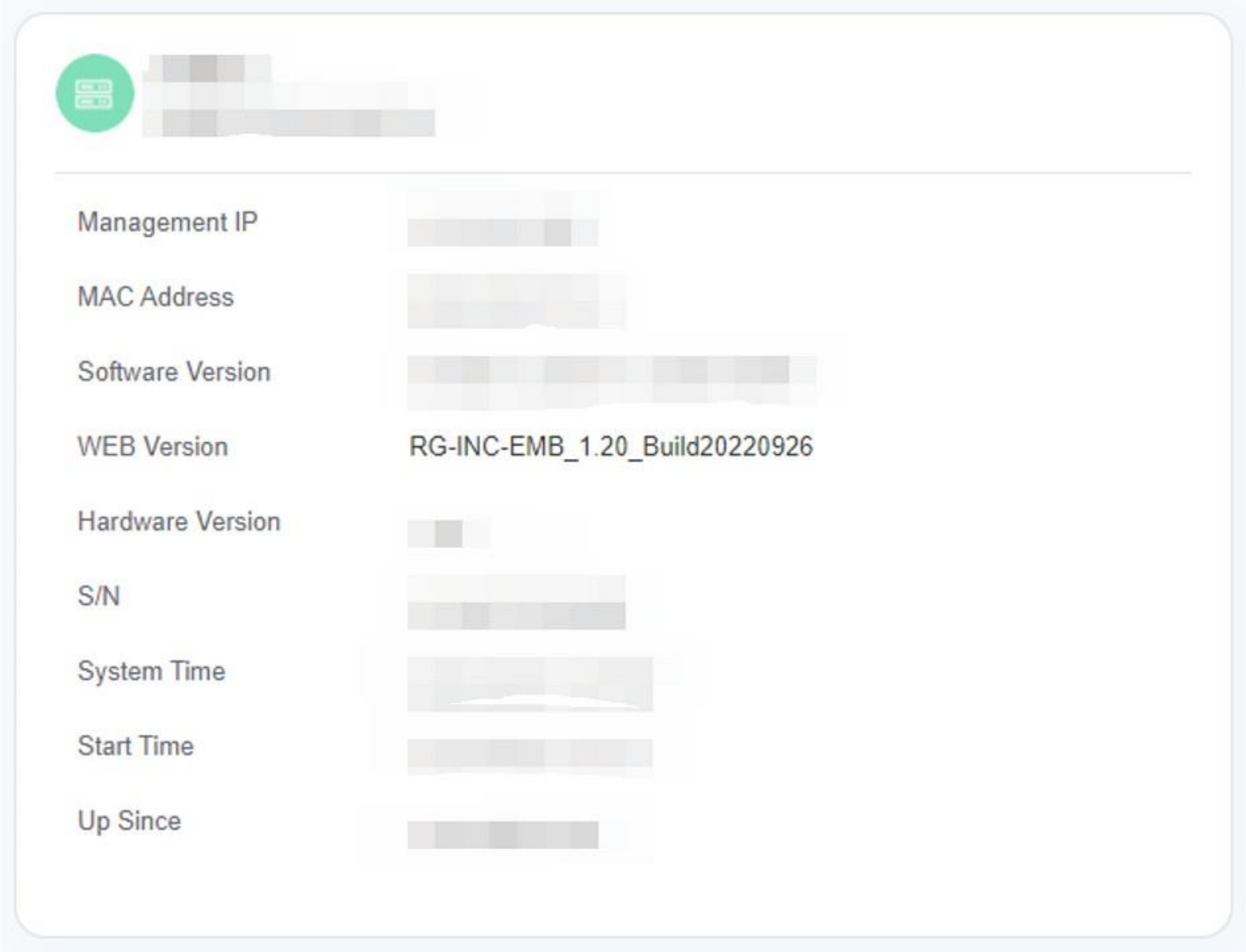
1.3.4 Home Page

After you log into the eWeb management system, you will be automatically redirected to the home page. You can also click on **Home**, in the navigation menu, to switch to the home page.

On this page, you can view the CPU, memory usage, system version, current system time, and other switch information. By analyzing the top 5 interface traffic, you can identify common network problems on this page and quickly solve any problems.

1. Switch Overview

At the top of the home page, you can view the switch name, model, management IP address, MAC address, software version, hardware version, serial number, system time, startup time, and uptime. You can reset the system time on the **System Time** page by choosing **O&M** > **Basic Configuration** > **System Time**.

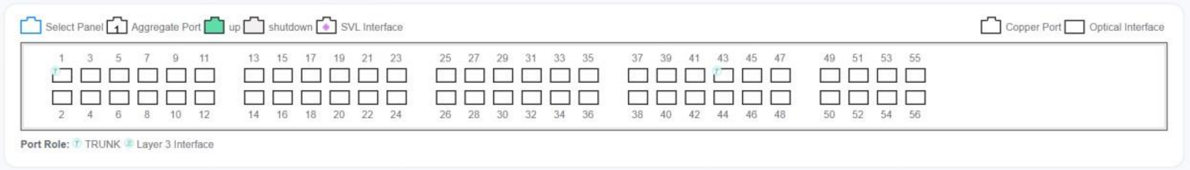


[redacted]

Management IP	[redacted]
MAC Address	[redacted]
Software Version	[redacted]
WEB Version	RG-INC-EMB_1.20_Build20220926
Hardware Version	[redacted]
S/N	[redacted]
System Time	[redacted]
Start Time	[redacted]
Up Since	[redacted]

2. Interfaces

In the upper part of the home page is the interface panel where interface information is displayed. The panel shows the basic interface configurations, such as interface type, state, aggregated interface, and virtual switching link (SVL) interface.

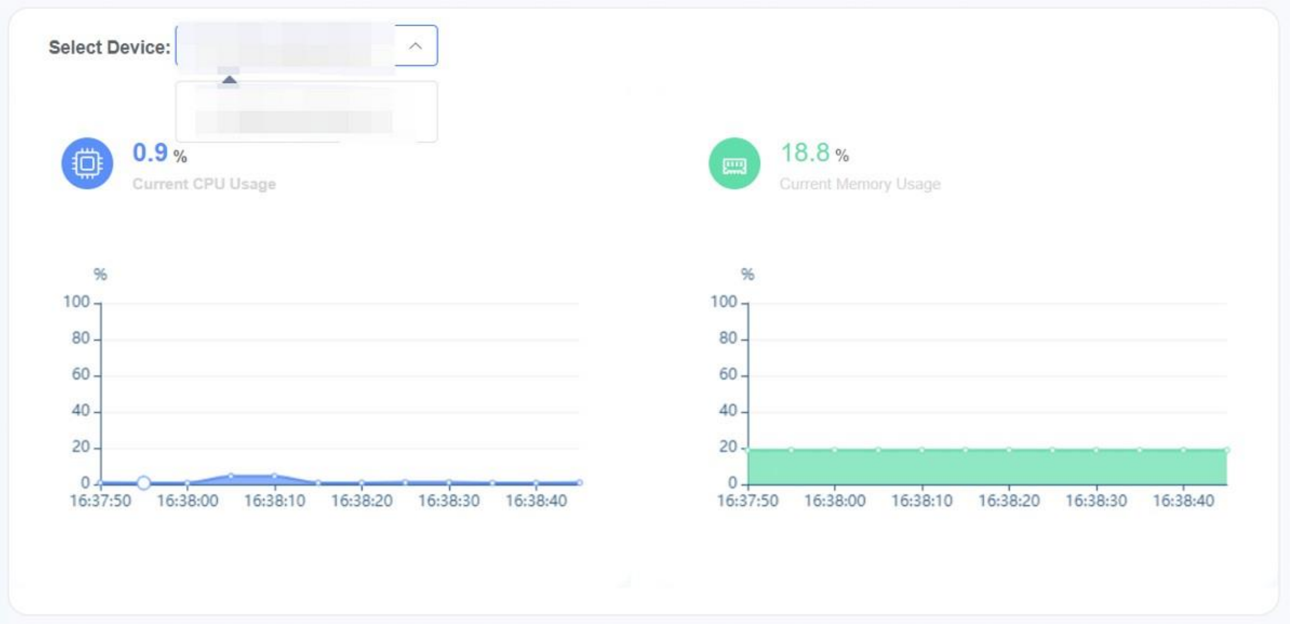


3. CPU/Memory Usage

The CPU and memory usage of the switch is displayed at the top of the home page.

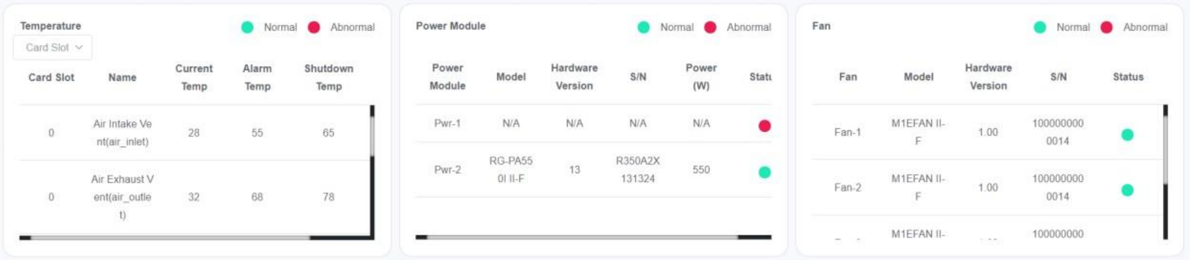
CPU: indicates the CPU usage of the switch service module.

Memory: indicates the memory usage of the switch service module.



4. Temperature/Power Module/Fan

The middle part of the home page displays the temperature, power module status, fan status of the switch at different positions.



Temperature

Card Slot

Card Slot	Name	Current Temp	Alarm Temp	Shutdown Temp
0	Air Intake Vent(air_inlet)	28	55	65
0	Air Exhaust Vent(air_outlet)	32	68	78

Power Module

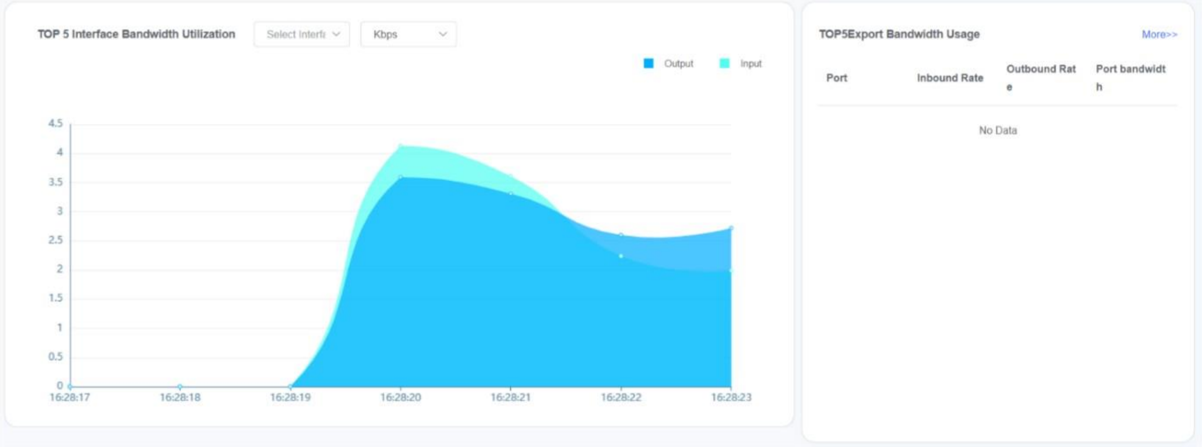
Power Module	Model	Hardware Version	S/N	Power (W)	Statı
Pwr-1	N/A	N/A	N/A	N/A	🟥
Pwr-2	RG-PA550I II-F	13	R350A2X131324	550	🟩

Fan

Fan	Model	Hardware Version	S/N	Status
Fan-1	M1EFAN II-F	1.00	1000000000014	🟩
Fan-2	M1EFAN II-F	1.00	1000000000014	🟩
	M1EFAN II-		100000000	

In the **Temperature** panel, you can view the temperature of a card slot by selecting a card clot from the **Card Slot** drop-down list box.

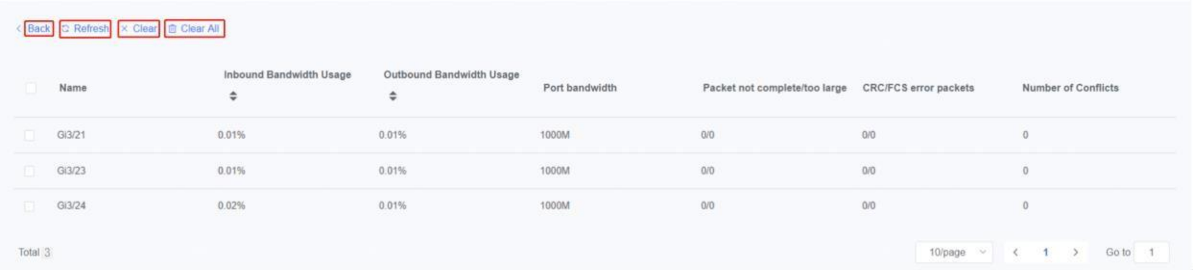
5. Bandwidth



Port	Inbound Rate	Outbound Rate	Port bandwidth

No Data

You can click on **More,** in the **Top 5 Interface Bandwidth Utilization** panel, to learn more details on the use of interface bandwidth.



	Name	Inbound Bandwidth Usage	Outbound Bandwidth Usage	Port bandwidth	Packet not complete/too large	CRC/FCS error packets	Number of Conflicts
□	Gi3/21	0.01%	0.01%	1000M	0/0	0/0	0
□	Gi3/23	0.01%	0.01%	1000M	0/0	0/0	0
□	Gi3/24	0.02%	0.01%	1000M	0/0	0/0	0

Total 3

Back: returns to the home page.

Refresh: re-queries the interface bandwidth utilization.

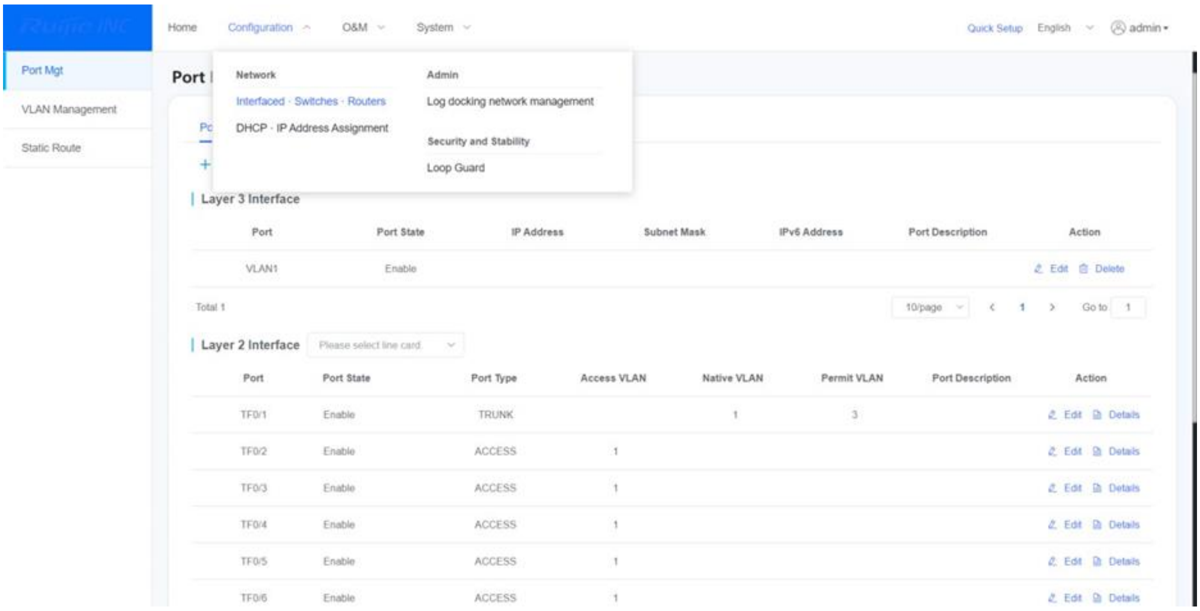
Clear: deletes statistics about a selected interface, such as the number of error packets and conflicting count.

Clear All: deletes statistics about all interfaces, such as the number of error packets and conflicting count.

1.3.5 Configuration

1. Port Management

Port Configuration

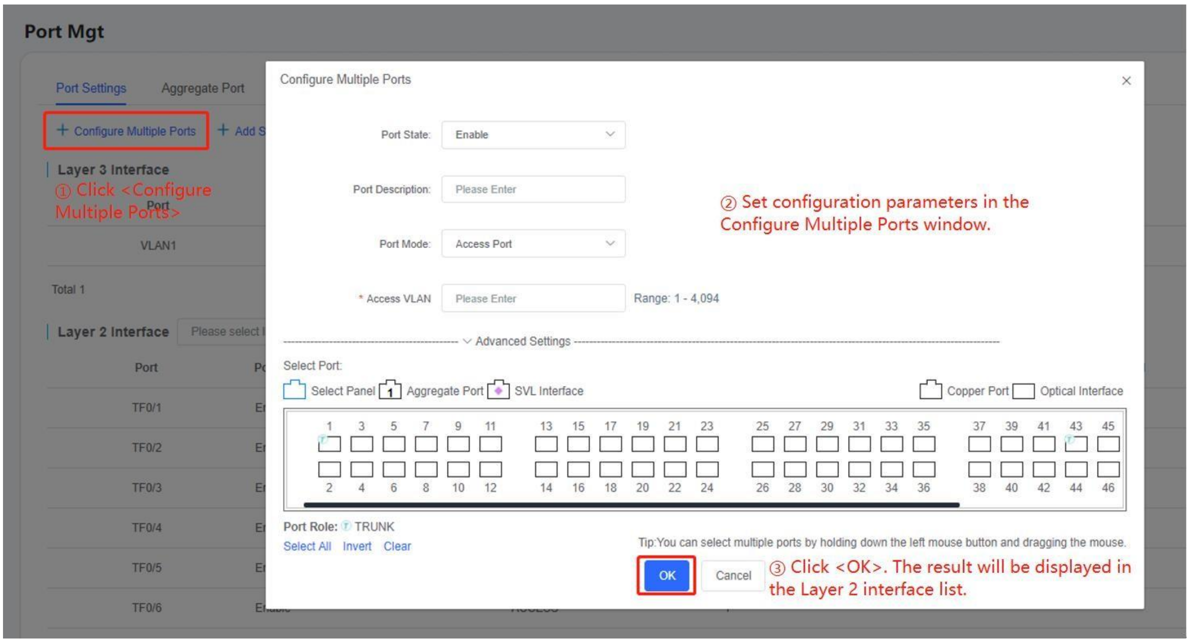


Port	Port State	IP Address	Subnet Mask	IPv6 Address	Port Description	Action
VLAN1	Enable					Edit Delete

Total 1

Port	Port State	Port Type	Access VLAN	Native VLAN	Permit VLAN	Port Description	Action
TF0/1	Enable	TRUNK		1	3		Edit Details
TF0/2	Enable	ACCESS	1				Edit Details
TF0/3	Enable	ACCESS	1				Edit Details
TF0/4	Enable	ACCESS	1				Edit Details
TF0/5	Enable	ACCESS	1				Edit Details
TF0/6	Enable	ACCESS	1				Edit Details

- **Configuring multiple ports**



① Click <Configure Multiple Ports>

Port State: Enable

Port Description: Please Enter

Port Mode: Access Port

* Access VLAN: Please Enter Range: 1 - 4,094

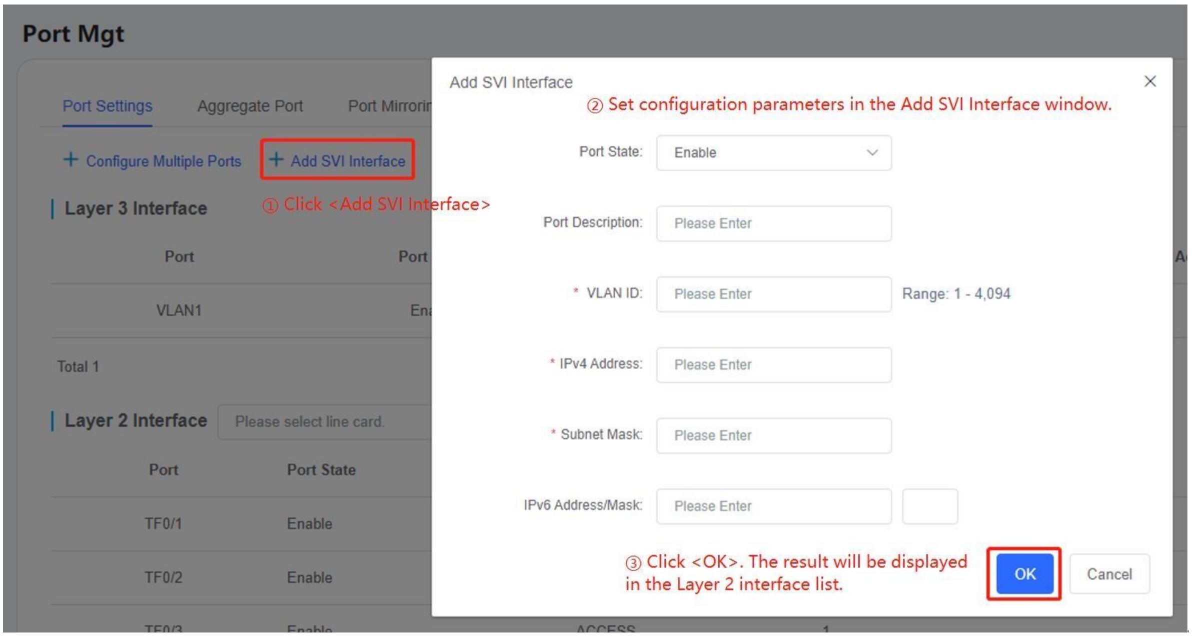
② Set configuration parameters in the Configure Multiple Ports window.

Port Role: TRUNK

Tip:You can select multiple ports by holding down the left mouse button and dragging the mouse.

③ Click <OK>. The result will be displayed in the Layer 2 interface list.

- **Adding an SVI**



① Click <Add SVI Interface>

② Set configuration parameters in the Add SVI Interface window.

Port State: Enable

Port Description: Please Enter

* VLAN ID: Please Enter Range: 1 - 4,094

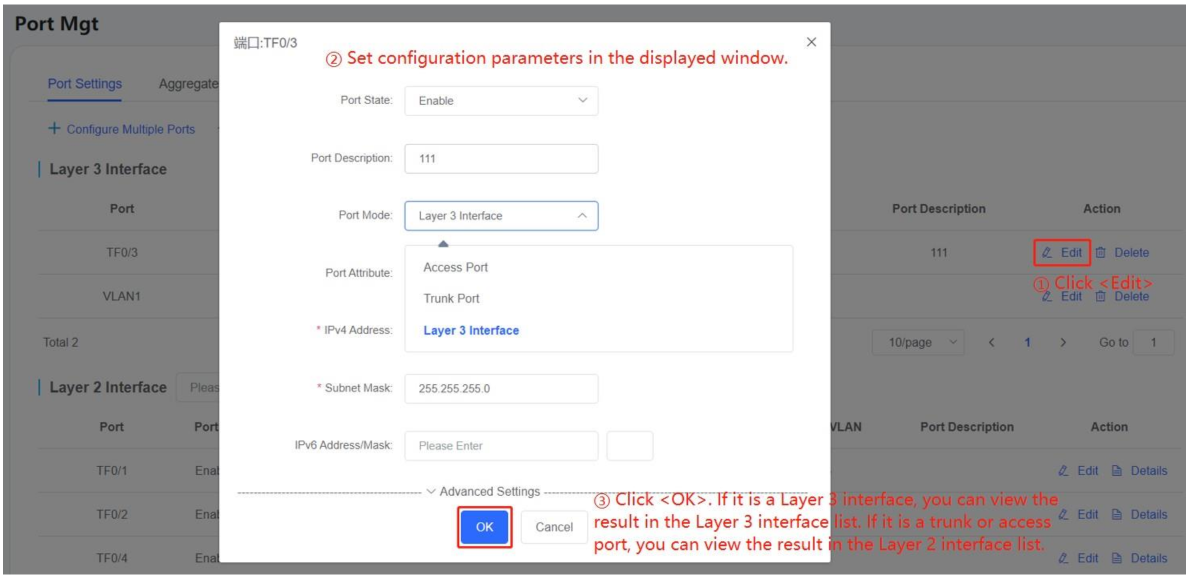
* IPv4 Address: Please Enter

* Subnet Mask: Please Enter

IPv6 Address/Mask: Please Enter

③ Click <OK>. The result will be displayed in the Layer 2 interface list.

- **Editing a Layer 3 interface**



端口:TF0/3

② Set configuration parameters in the displayed window.

Port State: Enable

Port Description: 111

Port Mode: Layer 3 Interface

Port Attribute:

* IPv4 Address:

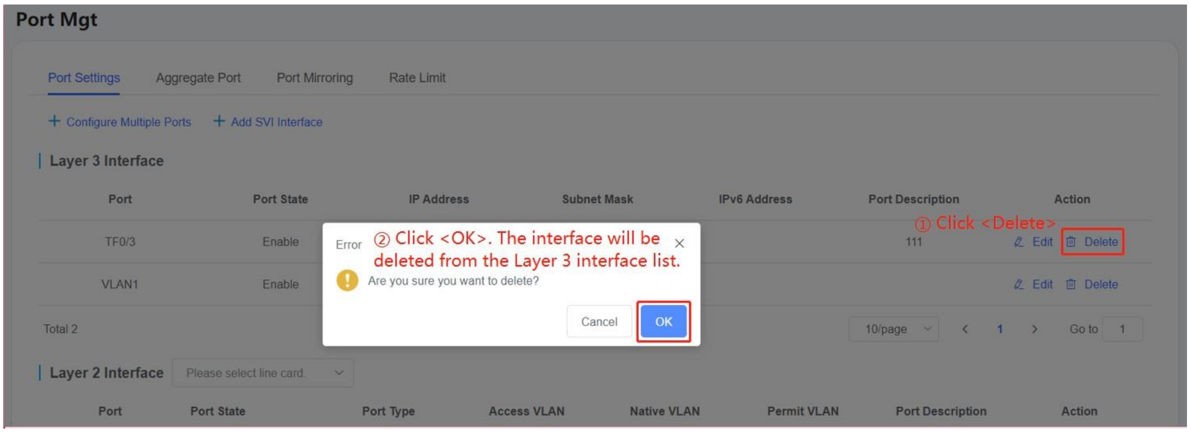
* Subnet Mask: 255.255.255.0

IPv6 Address/Mask: Please Enter

① Click <Edit>

③ Click <OK>. If it is a Layer 3 interface, you can view the result in the Layer 3 interface list. If it is a trunk or access port, you can view the result in the Layer 2 interface list.

- **Deleting a Layer 3 interface**



Port	Port State	IP Address	Subnet Mask	IPv6 Address	Port Description	Action
TF0/3	Enable				111	Edit Delete
VLAN1	Enable					Edit Delete

Port	Port State	Port Type	Access VLAN	Native VLAN	Permit VLAN	Port Description	Action

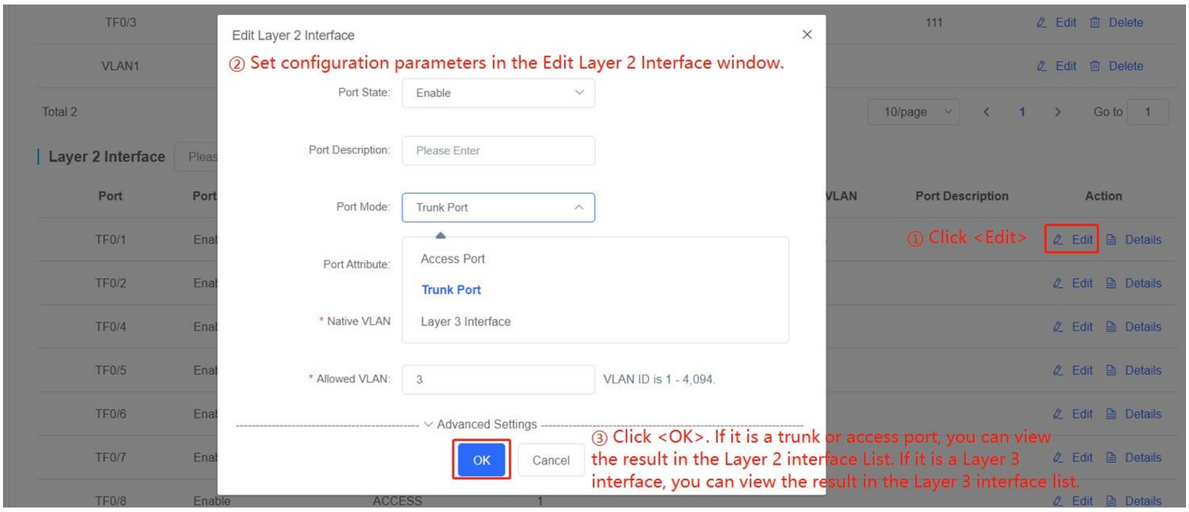
① Click <Delete>

Error

② Click <OK>. The interface will be deleted from the Layer 3 interface list.

Are you sure you want to delete?

- **Editing a Layer 2 interface**



Edit Layer 2 Interface

② Set configuration parameters in the Edit Layer 2 Interface window.

Port State: Enable

Port Description: Please Enter

Port Mode: Trunk Port

Port Attribute:

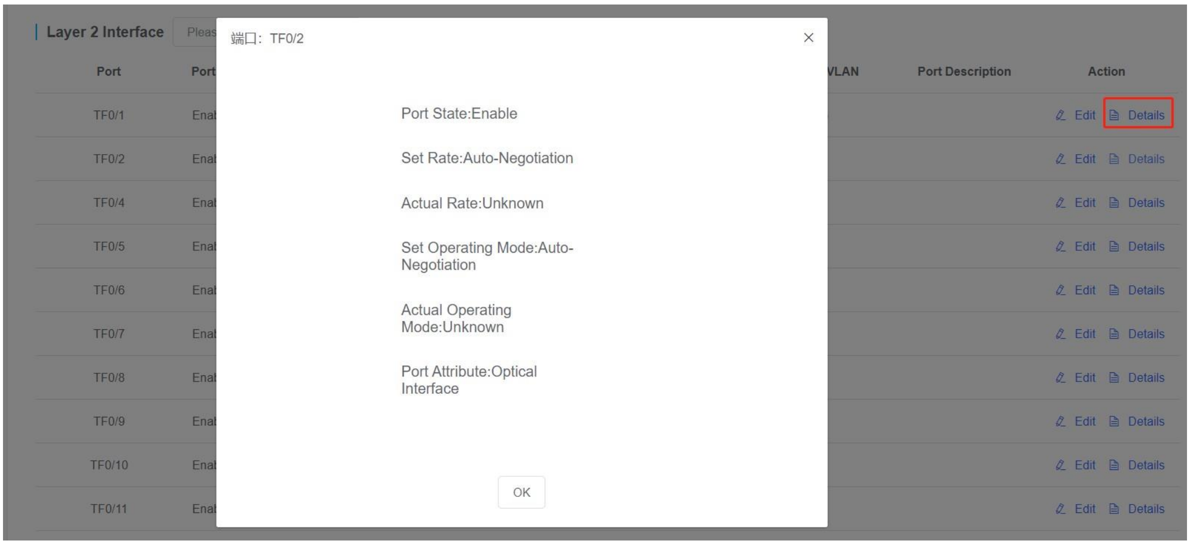
* Native VLAN

* Allowed VLAN: 3 VLAN ID is 1 - 4,094.

① Click <Edit>

③ Click <OK>. If it is a trunk or access port, you can view the result in the Layer 2 interface List. If it is a Layer 3 interface, you can view the result in the Layer 3 interface list.

- **Layer 2 interface details**



端口：TF0/2

Port State:Enable

Set Rate:Auto-Negotiation

Actual Rate:Unknown

Set Operating Mode:Auto-Negotiation

Actual Operating Mode:Unknown

Port Attribute:Optical Interface

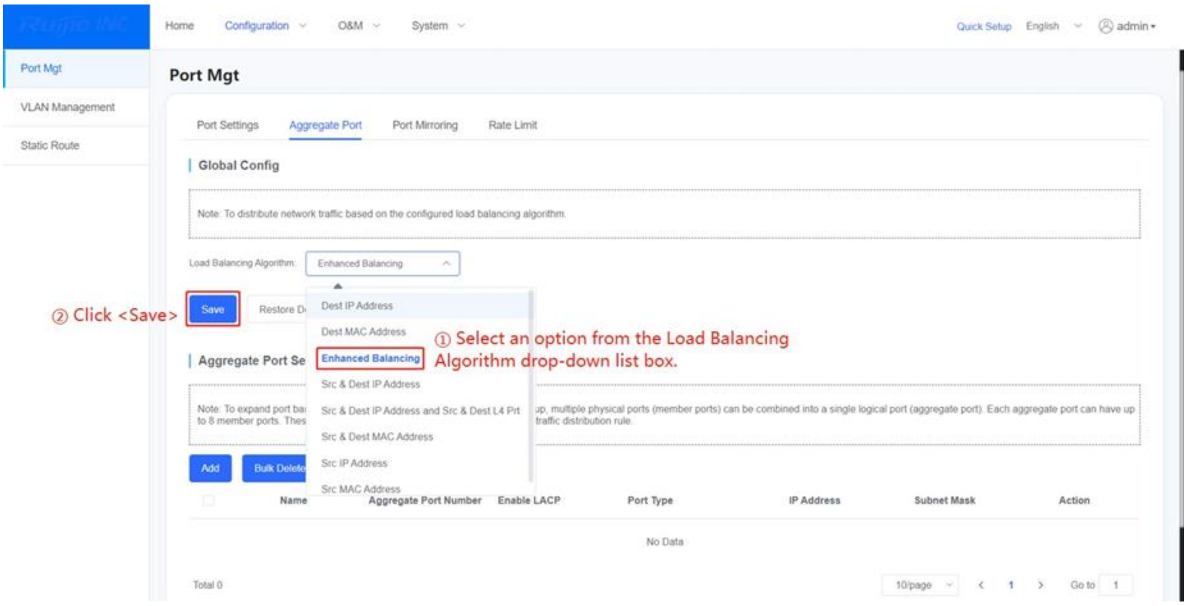
Click **Details**. You can view detailed information about a selected port.

Port Aggregation

Note

To increase bandwidth or provide redundancy, multiple physical ports (member ports) can be combined into a single logical port (aggregate port). Each aggregate port can have up to 8 member ports. These member ports transmit network traffic based on traffic distribution rules.

- **Saving configurations**



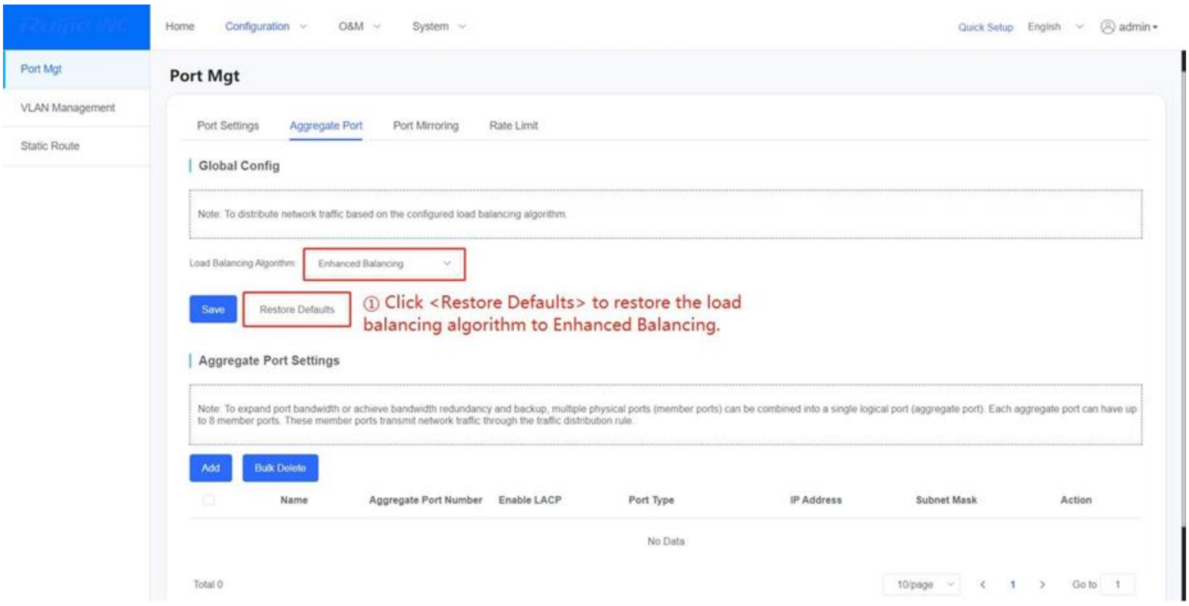
Note: To distribute network traffic based on the configured load balancing algorithm.

Load Balancing Algorithm: Enhanced Balancing

② Click <Save>

① Select an option from the Load Balancing Algorithm drop-down list box.

- **Restoring default settings**



Port Mgt

Global Config

Note: To distribute network traffic based on the configured load balancing algorithm.

Load Balancing Algorithm: Enhanced Balancing

① Click <Restore Defaults> to restore the load balancing algorithm to Enhanced Balancing.

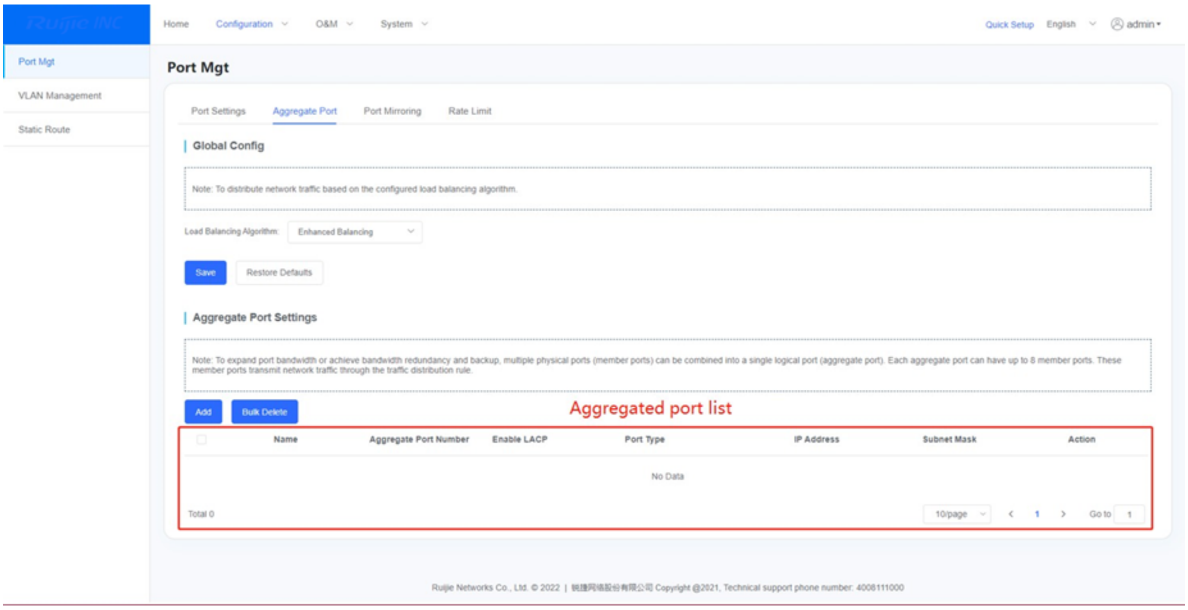
Aggregate Port Settings

Note: To expand port bandwidth or achieve bandwidth redundancy and backup, multiple physical ports (member ports) can be combined into a single logical port (aggregate port). Each aggregate port can have up to 8 member ports. These member ports transmit network traffic through the traffic distribution rule.

	Name	Aggregate Port Number	Enable LACP	Port Type	IP Address	Subnet Mask	Action
No Data							

Total 0

- **Querying the aggregate port list**



Port Mgt

Global Config

Note: To distribute network traffic based on the configured load balancing algorithm.

Load Balancing Algorithm: Enhanced Balancing

Aggregate Port Settings

Note: To expand port bandwidth or achieve bandwidth redundancy and backup, multiple physical ports (member ports) can be combined into a single logical port (aggregate port). Each aggregate port can have up to 8 member ports. These member ports transmit network traffic through the traffic distribution rule.

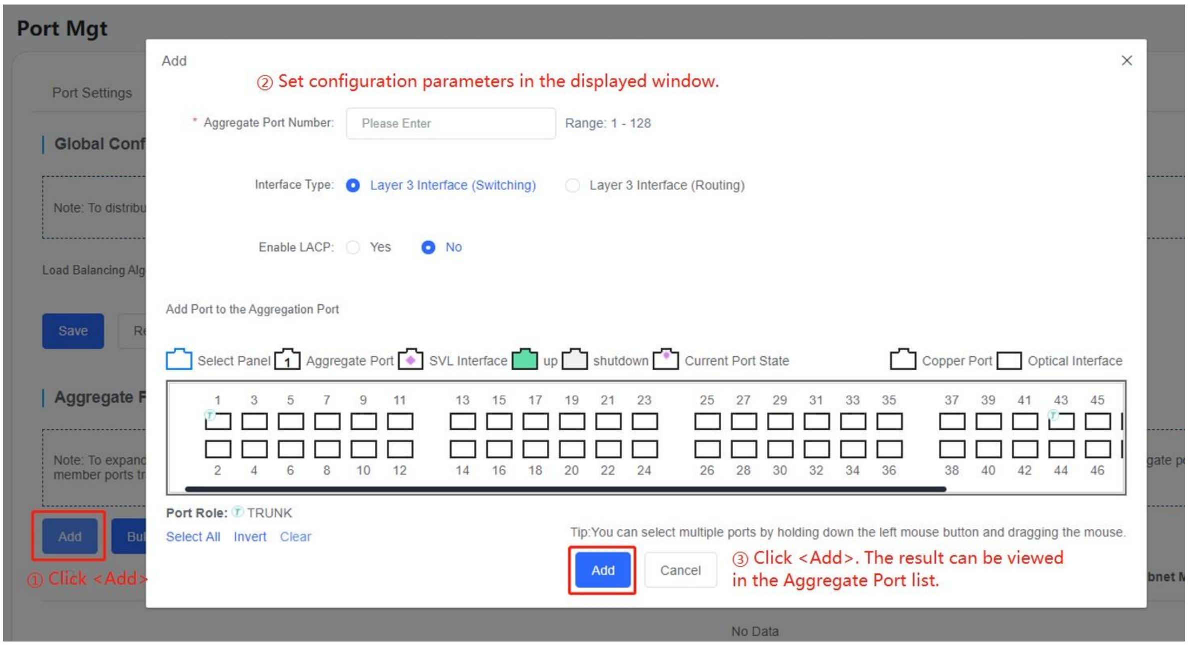
Aggregated port list

	Name	Aggregate Port Number	Enable LACP	Port Type	IP Address	Subnet Mask	Action
No Data							

Total 0

Ruijie Networks Co., Ltd. © 2022 | 锐捷网络股份有限公司 Copyright @2021, Technical support phone number: 4008111000

- **Adding an aggregate port**



Port Mgt

Add

② Set configuration parameters in the displayed window.

* Aggregate Port Number: Please Enter Range: 1 - 128

Interface Type: ● Layer 3 Interface (Switching) ○ Layer 3 Interface (Routing)

Enable LACP: ○ Yes ● No

Add Port to the Aggregation Port

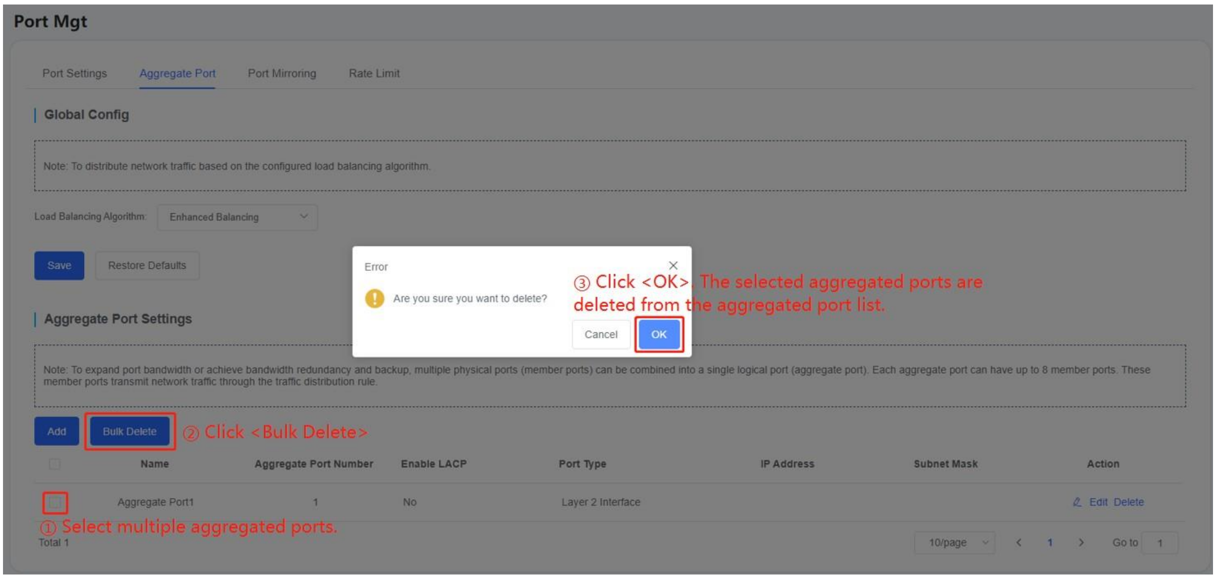
Port Role: TRUNK

Tip:You can select multiple ports by holding down the left mouse button and dragging the mouse.

① Click <Add>

③ Click <Add>. The result can be viewed in the Aggregate Port list.

- **Deleting multiple aggregate ports**



Port Mgt

Global Config

Note: To distribute network traffic based on the configured load balancing algorithm.

Load Balancing Algorithm: Enhanced Balancing

Aggregate Port Settings

Note: To expand port bandwidth or achieve bandwidth redundancy and backup, multiple physical ports (member ports) can be combined into a single logical port (aggregate port). Each aggregate port can have up to 8 member ports. These member ports transmit network traffic through the traffic distribution rule.

Error

Are you sure you want to delete?

③ Click <OK>. The selected aggregated ports are deleted from the aggregated port list.

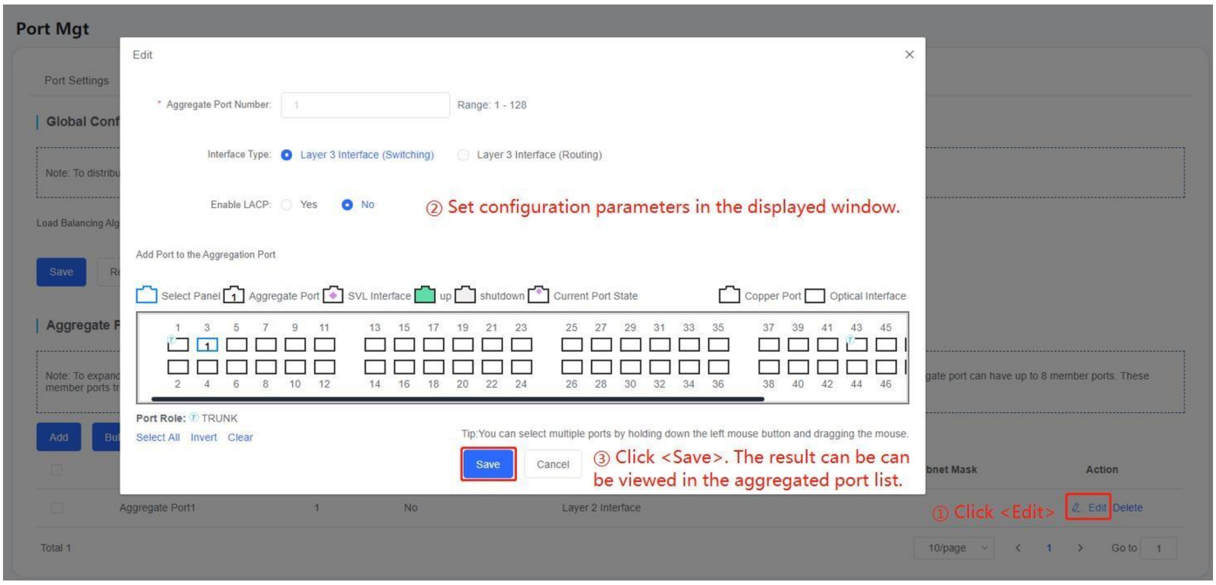
② Click <Bulk Delete>

① Select multiple aggregated ports.

Name	Aggregate Port Number	Enable LACP	Port Type	IP Address	Subnet Mask	Action
Aggregate Port1	1	No	Layer 2 Interface			Edit Delete

Total 1

- **Editing an aggregate port**



Edit

* Aggregate Port Number: 1 Range: 1 - 128

Interface Type: ● Layer 3 Interface (Switching) ○ Layer 3 Interface (Routing)

Enable LACP: ○ Yes ● No

② Set configuration parameters in the displayed window.

Add Port to the Aggregation Port

Port Role: TRUNK

Tip:You can select multiple ports by holding down the left mouse button and dragging the mouse.

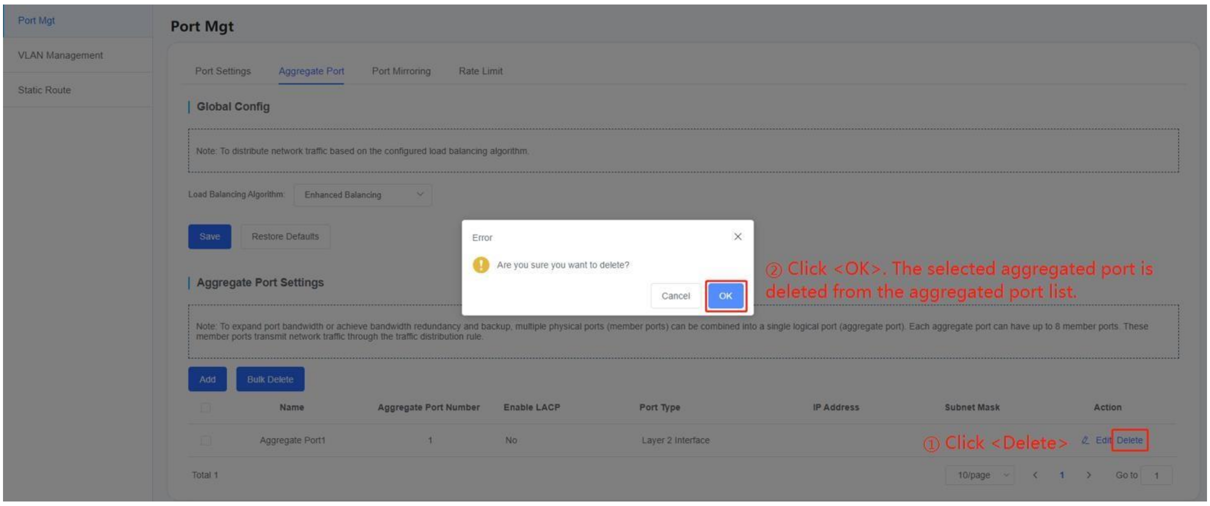
③ Click <Save>. The result can be can be viewed in the aggregated port list.

Name	Aggregate Port Number	Enable LACP	Port Type	Subnet Mask	Action
Aggregate Port1	1	No	Layer 2 Interface		Edit Delete

① Click <Edit>

Total 1

- **Deleting an aggregate port**



Note: To distribute network traffic based on the configured load balancing algorithm.

Load Balancing Algorithm: Enhanced Balancing

Error

Are you sure you want to delete?

② Click <OK>. The selected aggregated port is deleted from the aggregated port list.

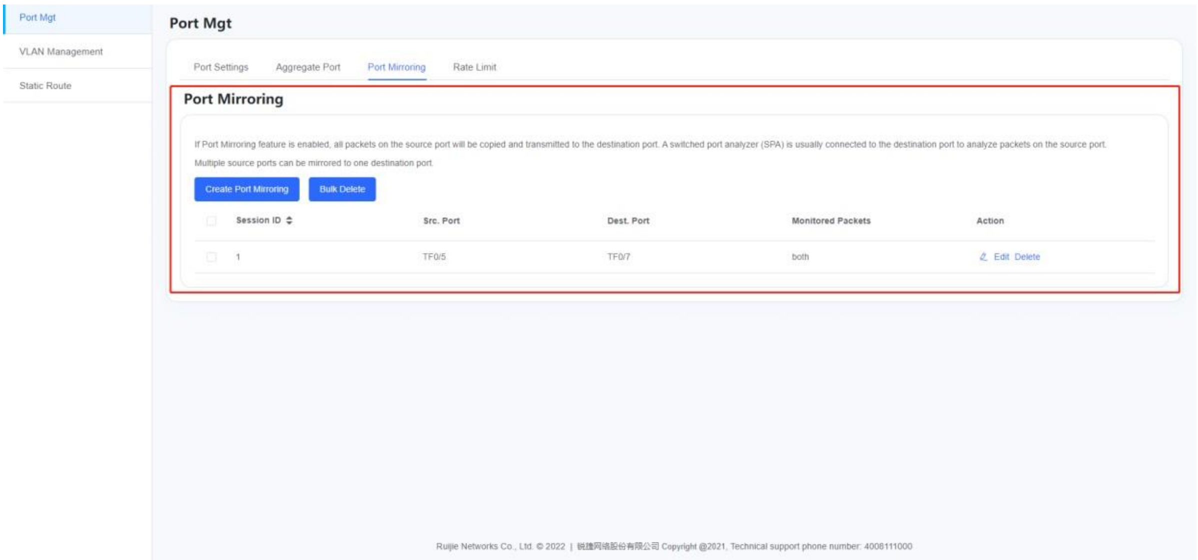
Note: To expand port bandwidth or achieve bandwidth redundancy and backup, multiple physical ports (member ports) can be combined into a single logical port (aggregate port). Each aggregate port can have up to 8 member ports. These member ports transmit network traffic through the traffic distribution rule.

Name	Aggregate Port Number	Enable LACP	Port Type	IP Address	Subnet Mask	Action
Aggregate Port1	1	No	Layer 2 Interface			Edit Delete

① Click <Delete>

Total 1

Port Mirroring

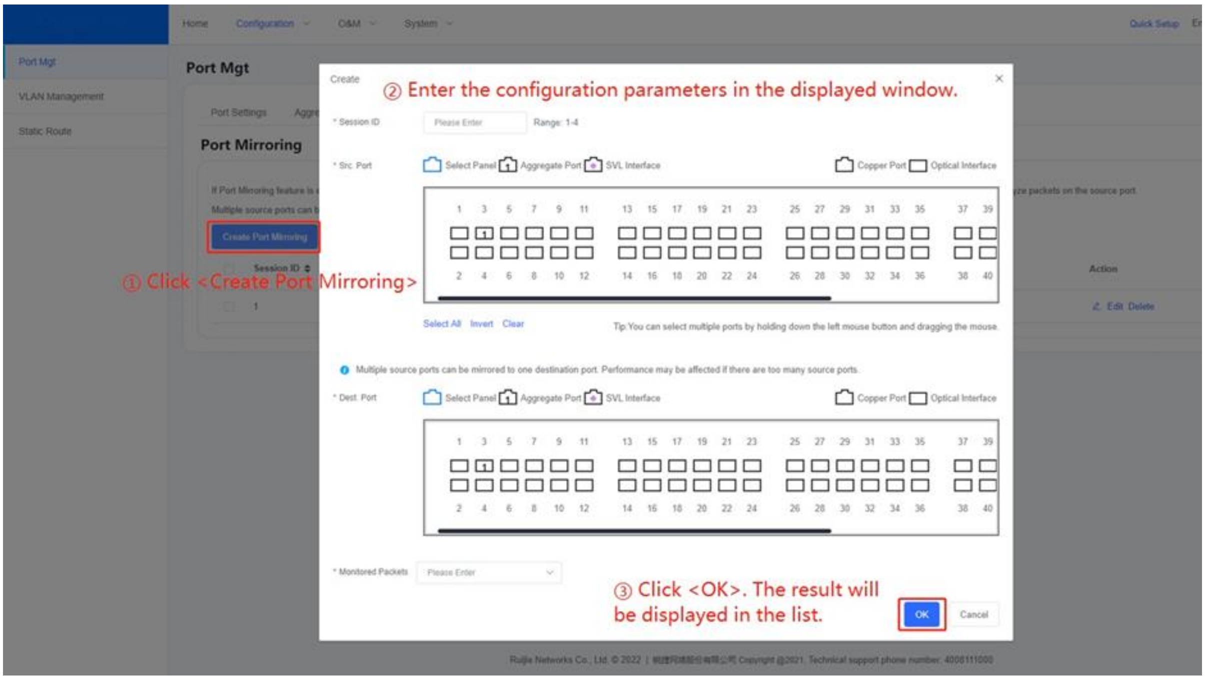


If Port Mirroring feature is enabled, all packets on the source port will be copied and transmitted to the destination port. A switched port analyzer (SPA) is usually connected to the destination port to analyze packets on the source port. Multiple source ports can be mirrored to one destination port.

Session ID	Src. Port	Dest. Port	Monitored Packets	Action
1	TF0/5	TF0/7	both	Edit Delete

Ruijie Networks Co., Ltd. © 2022 | 锐捷网络股份有限公司 Copyright @2021, Technical support phone number: 4008111000

- **Creating port mirroring**



① Click <Create Port Mirroring>

② Enter the configuration parameters in the displayed window.

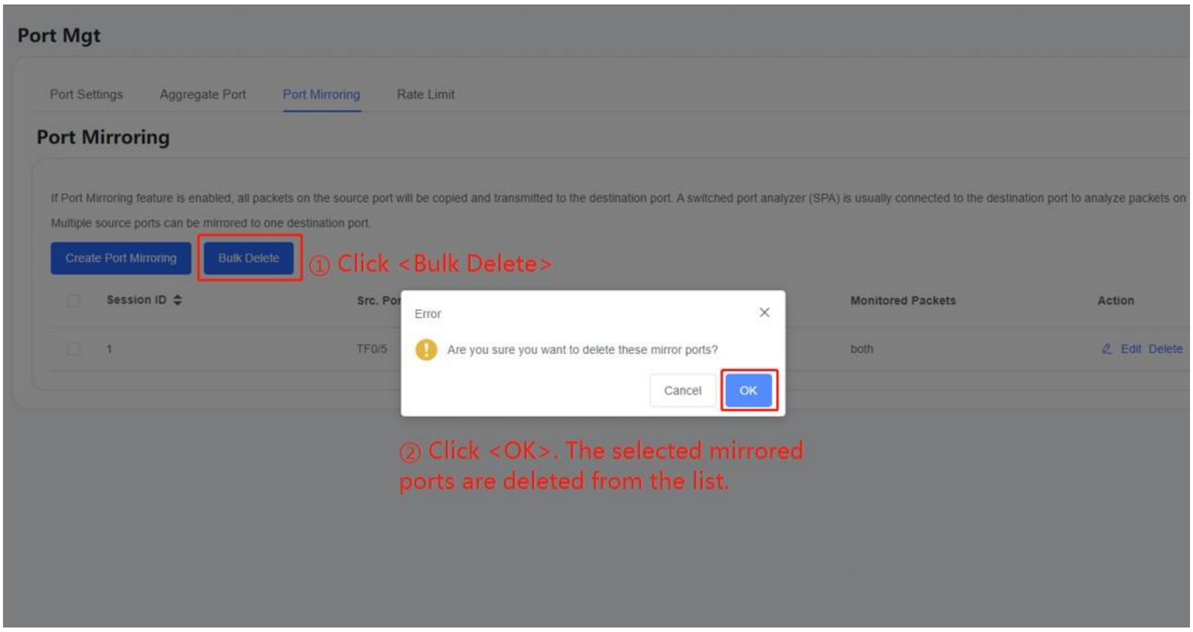
Tip: You can select multiple ports by holding down the left mouse button and dragging the mouse.

Multiple source ports can be mirrored to one destination port. Performance may be affected if there are too many source ports.

③ Click <OK>. The result will be displayed in the list.

Ruijie Networks Co., Ltd. © 2022 | 锐捷网络股份有限公司 Copyright @2021. Technical support phone number: 4008111000

- **Deleting multiple mirrored ports**



If Port Mirroring feature is enabled, all packets on the source port will be copied and transmitted to the destination port. A switched port analyzer (SPA) is usually connected to the destination port to analyze packets on

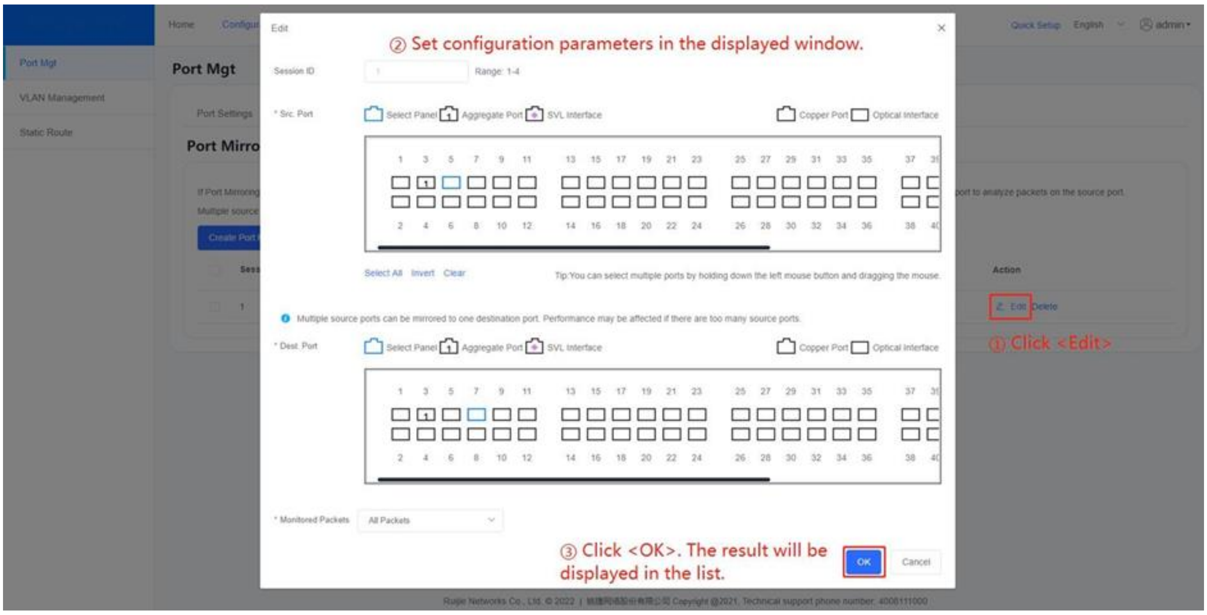
Multiple source ports can be mirrored to one destination port.

① Click <Bulk Delete>

Are you sure you want to delete these mirror ports?

② Click <OK>. The selected mirrored ports are deleted from the list.

- **Editing a mirrored port**



Edit

② Set configuration parameters in the displayed window.

Session ID: 1 Range: 1-4

* Src. Port

Select All Invert Clear

Tip:You can select multiple ports by holding down the left mouse button and dragging the mouse.

Multiple source ports can be mirrored to one destination port. Performance may be affected if there are too many source ports.

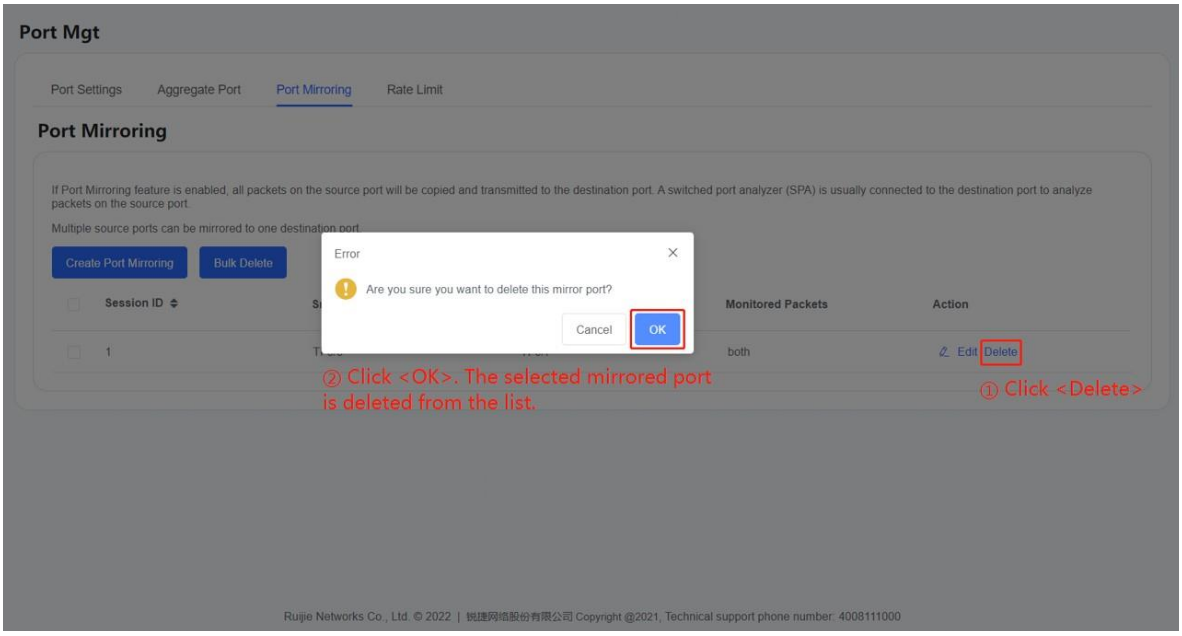
* Dest. Port

* Monitored Packets: All Packets

① Click <Edit>

③ Click <OK>. The result will be displayed in the list.

- **Deleting a mirrored port**



Port Mgt

Port Mirroring

If Port Mirroring feature is enabled, all packets on the source port will be copied and transmitted to the destination port. A switched port analyzer (SPA) is usually connected to the destination port to analyze packets on the source port.

Multiple source ports can be mirrored to one destination port.

Error

Are you sure you want to delete this mirror port?

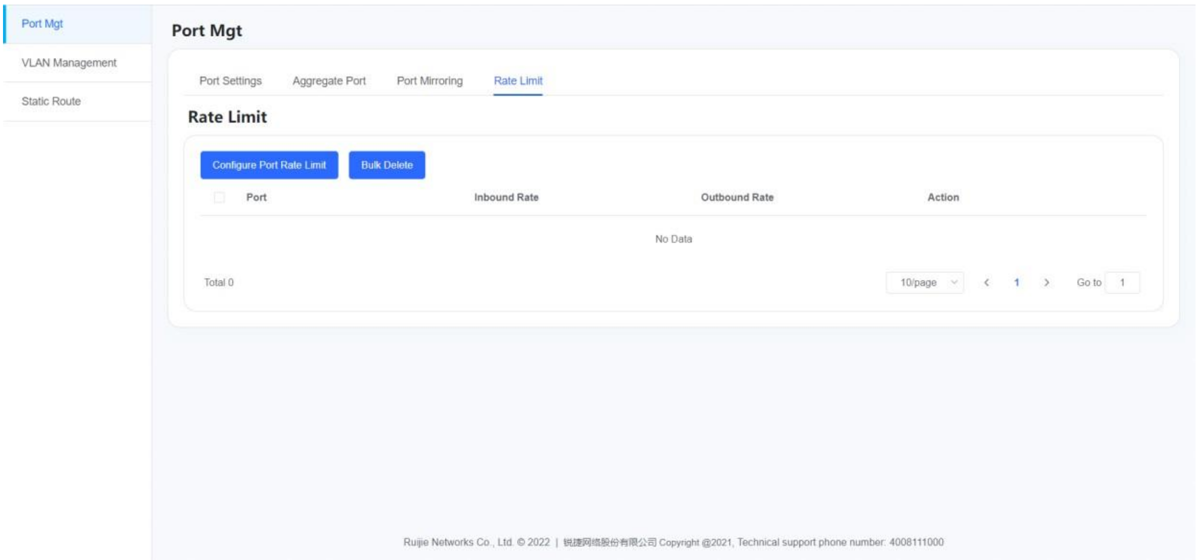
Session ID			Monitored Packets	Action
1			both	Edit Delete

① Click <Delete>

② Click <OK>. The selected mirrored port is deleted from the list.

Port Settings
Aggregate Port
Port Mirroring
Rate Limit
Create Port Mirroring
Bulk Delete
Cancel
OK
Ruijie Networks Co., Ltd. © 2022 | 锐捷网络股份有限公司 Copyright @2021, Technical support phone number: 4008111000

Rate Limiting



Port Mgt

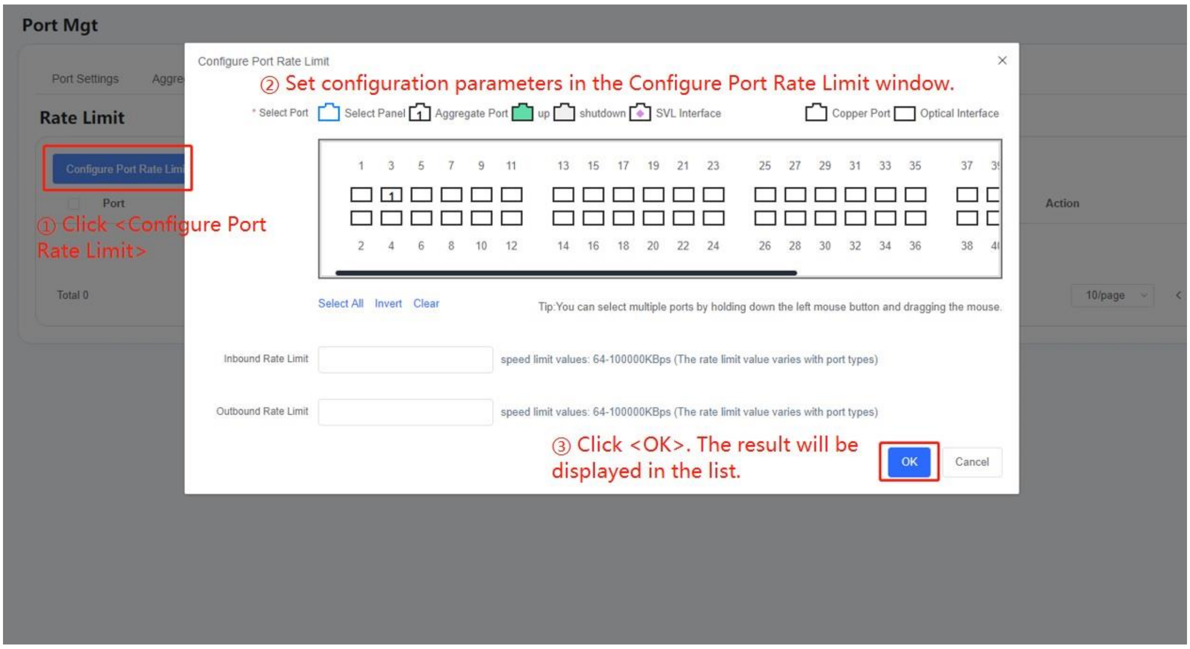
Rate Limit

□	Port	Inbound Rate	Outbound Rate	Action
		No Data		

Total 0

Ruijie Networks Co., Ltd. © 2022 | 锐捷网络股份有限公司 Copyright @2021, Technical support phone number: 4008111000

- **Configuring port rate limiting**



① Click <Configure Port Rate Limit>

② Set configuration parameters in the Configure Port Rate Limit window.

③ Click <OK>. The result will be displayed in the list.

Configure Port Rate Limit

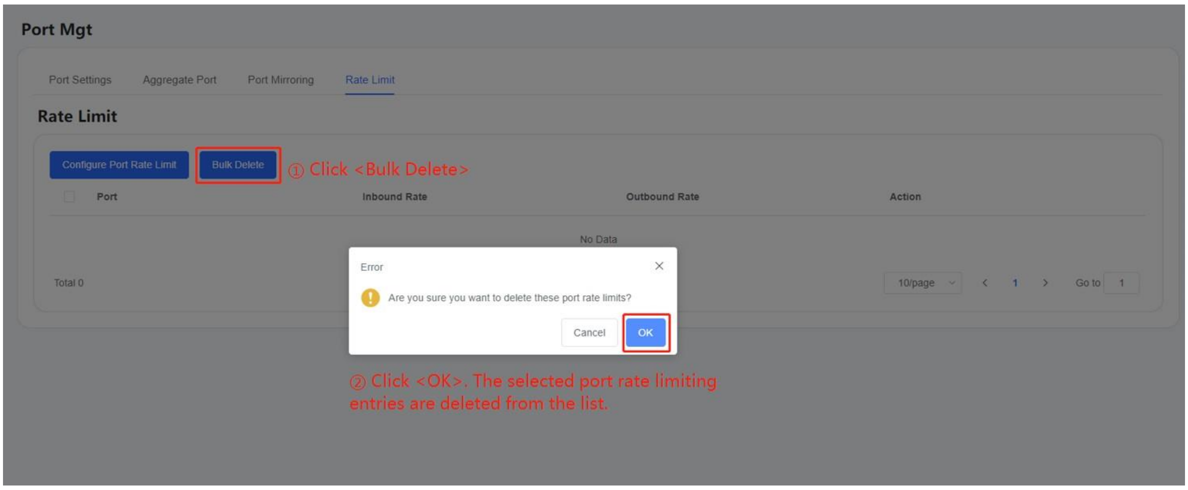
* Select Port

Tip:You can select multiple ports by holding down the left mouse button and dragging the mouse.

Inbound Rate Limit: speed limit values: 64-100000KBps (The rate limit value varies with port types)

Outbound Rate Limit: speed limit values: 64-100000KBps (The rate limit value varies with port types)

- **Deleting multiple rate limiting entries**

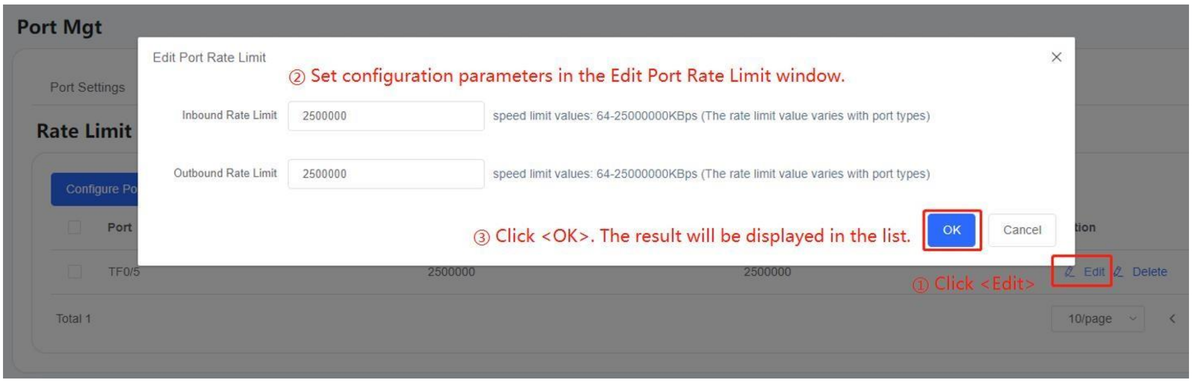


Are you sure you want to delete these port rate limits?

① Click <Bulk Delete>

② Click <OK>. The selected port rate limiting entries are deleted from the list.

- **Editing a port rate limiting entry**



Inbound Rate Limit: 2500000 speed limit values: 64-25000000KBps (The rate limit value varies with port types)

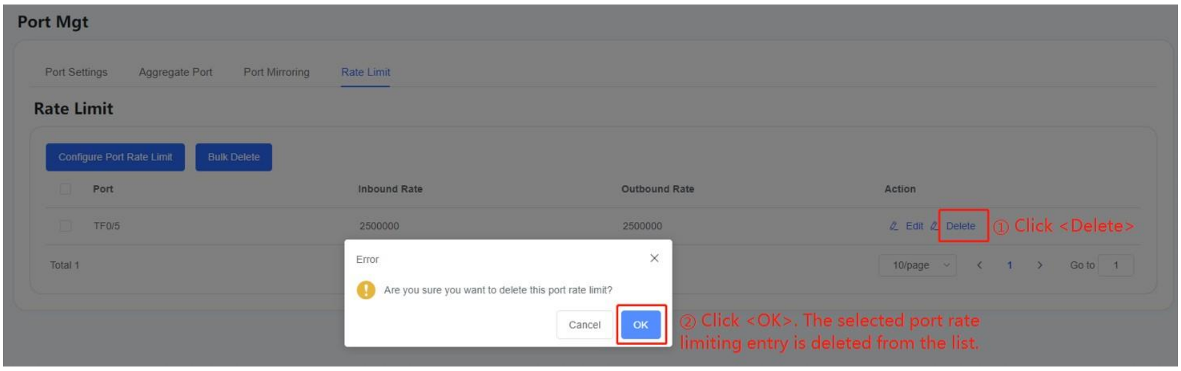
Outbound Rate Limit: 2500000 speed limit values: 64-25000000KBps (The rate limit value varies with port types)

① Click <Edit>

② Set configuration parameters in the Edit Port Rate Limit window.

③ Click <OK>. The result will be displayed in the list.

- **Deleting a port rate limiting entry**



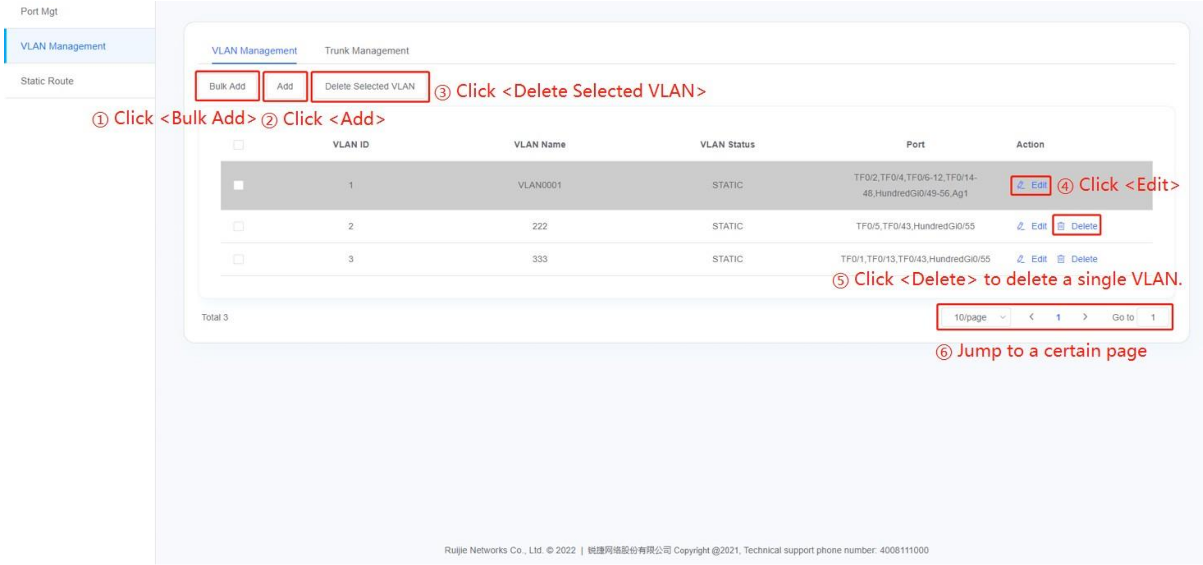
Are you sure you want to delete this port rate limit?

① Click <Delete>

② Click <OK>. The selected port rate limiting entry is deleted from the list.

2. VLAN Management

VLAN Management



① Click <Bulk Add> ② Click <Add> ③ Click <Delete Selected VLAN>

□	VLAN ID	VLAN Name	VLAN Status	Port	Action
□	1	VLAN0001	STATIC	TF0/2,TF0/4,TF0/6-12,TF0/14-48,HundredGi0/49-56,Ag1	Edit
□	2	222	STATIC	TF0/5,TF0/43,HundredGi0/55	Edit Delete
□	3	333	STATIC	TF0/1,TF0/13,TF0/43,HundredGi0/55	Edit Delete

④ Click <Edit>

⑤ Click <Delete> to delete a single VLAN.

Total 3

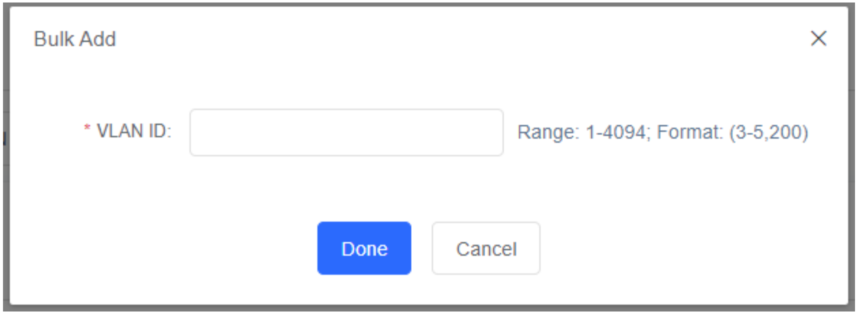
⑥ Jump to a certain page

Ruijie Networks Co., Ltd. © 2022 | 锐捷网络股份有限公司 Copyright @2021, Technical support phone number: 4008111000

- **Adding multiple VLANs**

To add multiple VLANs, click Bulk Add and the **Bulk Add** window is displayed. Enter the VLAN ID and click Done .

- **Adding a single VLAN**

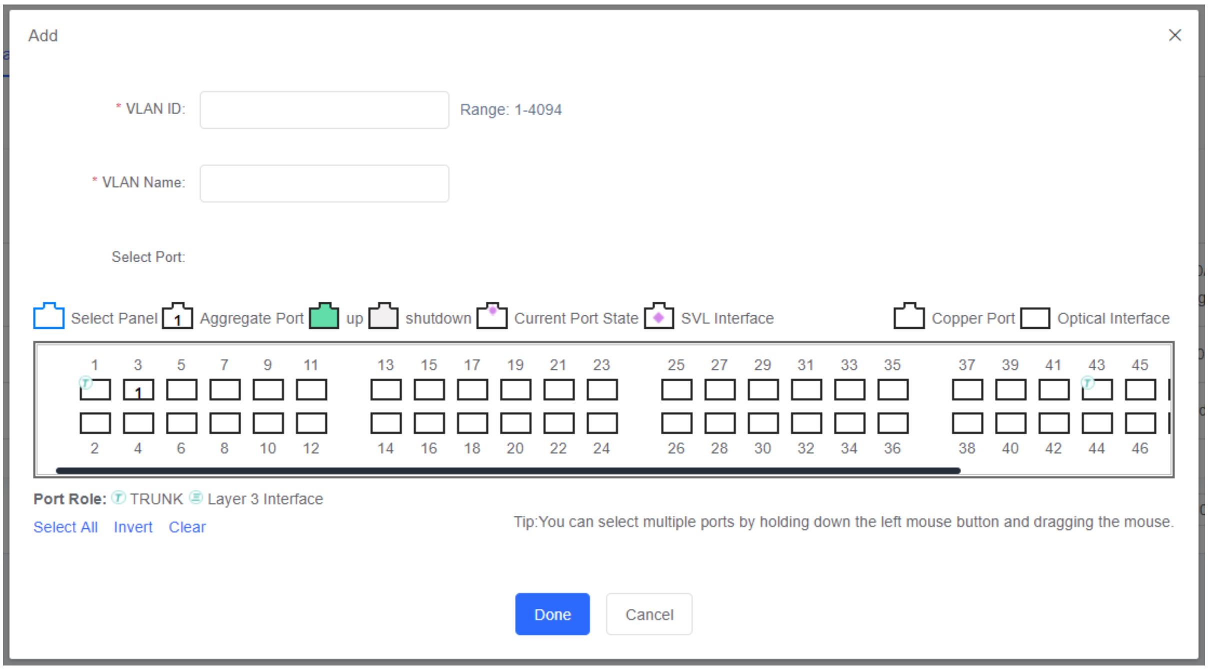


Bulk Add

* VLAN ID:

Range: 1-4094; Format: (3-5,200)

To add a single VLAN, click Add and the **Add** window is displayed. Set configuration parameters and click Done .



Add

* VLAN ID: Range: 1-4094

* VLAN Name:

Select Port:

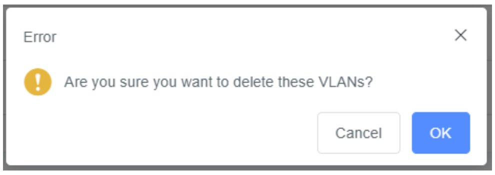
Port Role: TRUNK Layer 3 Interface

Select All Invert Clear

Tip:You can select multiple ports by holding down the left mouse button and dragging the mouse.

- **Deleting multiple VLANs**

To delete the selected VLANs, click on □ before each VLAN to select multiple VLANs, then click Delete Selected VLAN. The error message is displayed. Click OK.

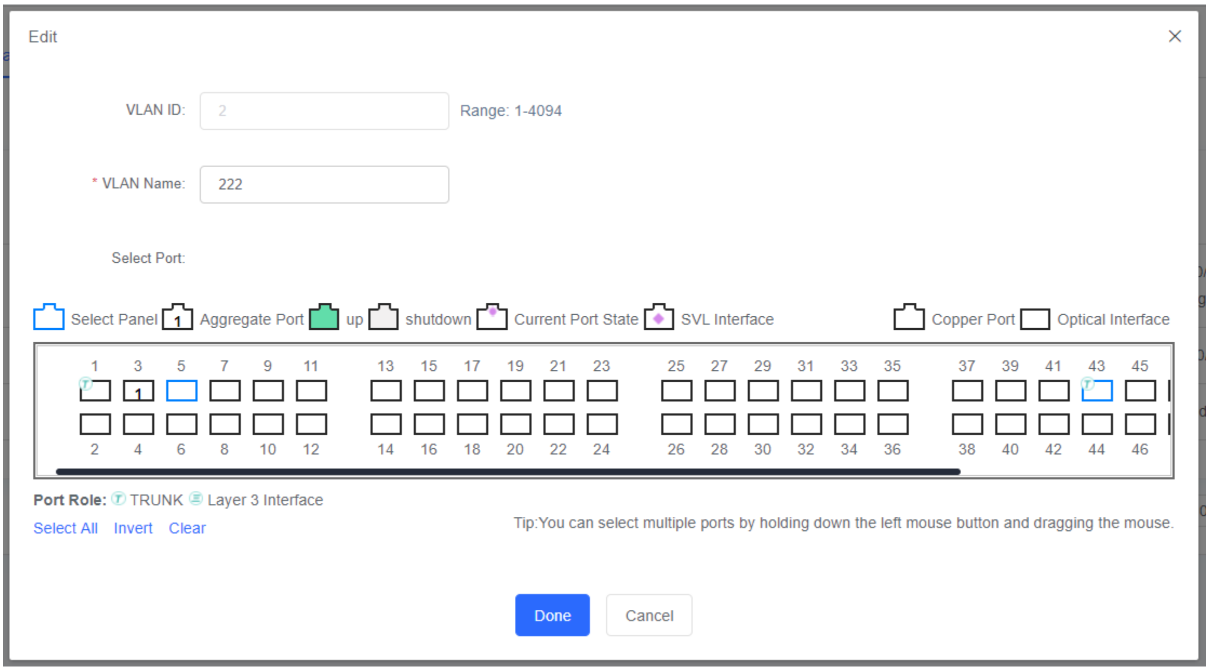


Error

Are you sure you want to delete these VLANs?

- **Editing a VLAN**

To edit a VLAN, click Edit, and the **Edit** window is displayed. Set configuration parameters and click Done.



Edit

VLAN ID: 2 Range: 1-4094

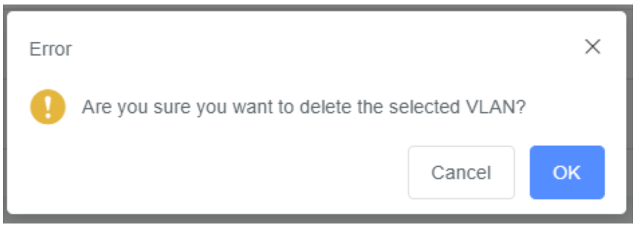
* VLAN Name: 222

Select Port:

Tip:You can select multiple ports by holding down the left mouse button and dragging the mouse.

- **Deleting a VLAN**

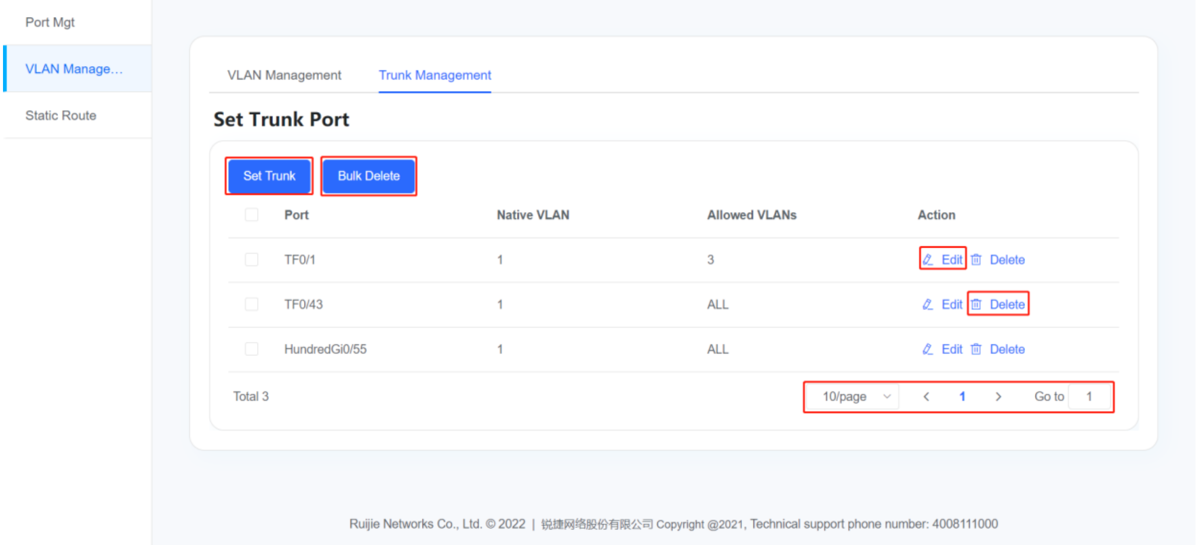
To delete a VLAN, click Delete . The **Error** dialog box is displayed. Click OK .



Error

Are you sure you want to delete the selected VLAN?

Trunk Management



Set Trunk Port

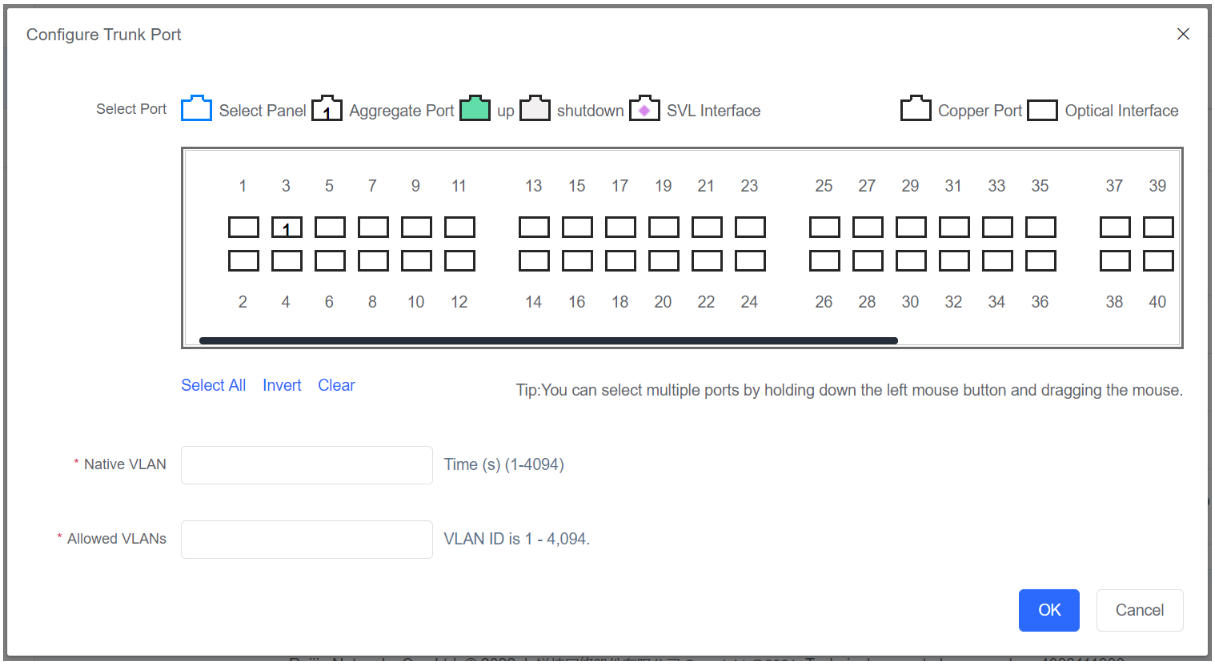
Port	Native VLAN	Allowed VLANs	Action
TF0/1	1	3	Edit Delete
TF0/43	1	ALL	Edit Delete
HundredGi0/55	1	ALL	Edit Delete

Total 3 10/page 1 Go to 1

Ruijie Networks Co., Ltd. © 2022 | 锐捷网络股份有限公司 Copyright @2021, Technical support phone number: 4008111000

- **Setting a Trunk port**

To set a trunk port, click Set Trunk . The **Configure Trunk Port** window is displayed. Set configuration parameters and click OK .



Configure Trunk Port ×

Select Port: Select Panel, Aggregate Port, up, shutdown, SVL Interface, Copper Port, Optical Interface

Select All Invert Clear

Tip:You can select multiple ports by holding down the left mouse button and dragging the mouse.

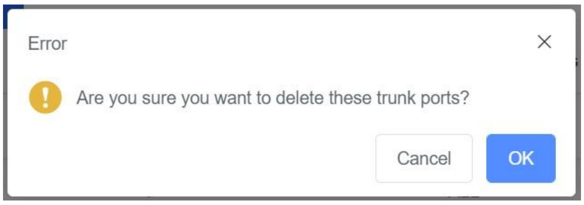
* Native VLAN: Time (s) (1-4094)

* Allowed VLANs: VLAN ID is 1 - 4,094.

OK Cancel

- **Deleting multiple trunk ports**

To delete multiple trunk ports, click on □ next to each trunk port to select multiple trunk ports, and then click Bulk Delete. The **Error** dialog box is displayed. Click OK.



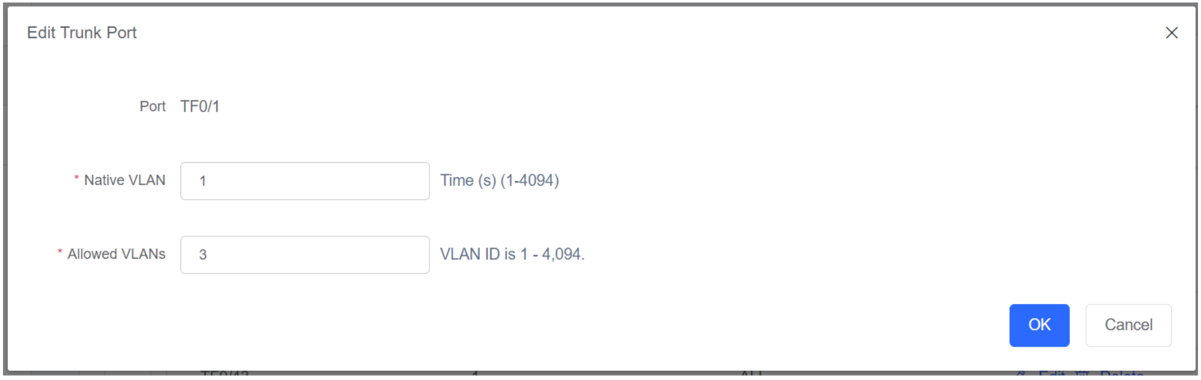
Error ×

Are you sure you want to delete these trunk ports?

Cancel OK

- **Editing a trunk port**

To edit a Trunk port, click Edit. The Edit Trunk Port window is displayed. Set configuration parameters and click OK.



Edit Trunk Port ×

Port TF0/1

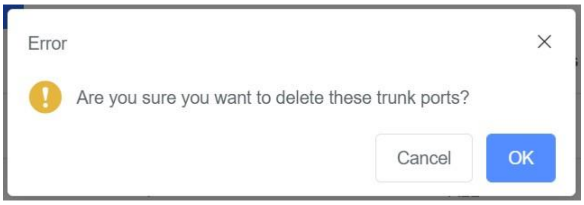
* Native VLAN: 1 Time (s) (1-4094)

* Allowed VLANs: 3 VLAN ID is 1 - 4,094.

OK Cancel

- **Deleting a trunk port**

To delete a selected trunk port, click Delete. The **Error** dialog box is displayed. Click OK.



Error

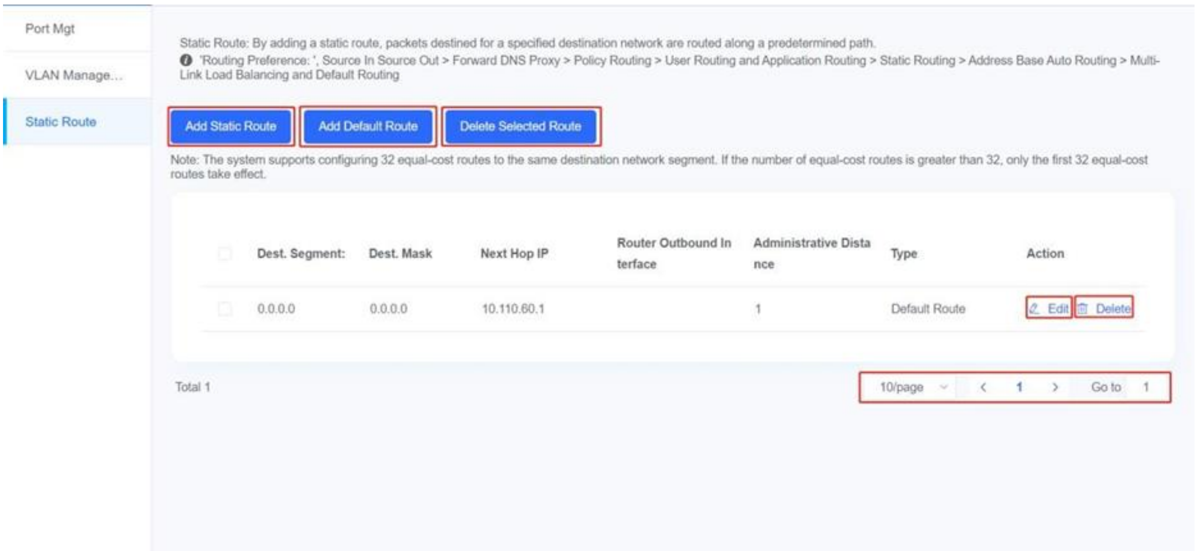
Are you sure you want to delete these trunk ports?

3. Static Route

Packets destined for a specific destination network are routed along a pre-determined path when a static route is configured. The routing priority is source in source out > forward DNS proxy > policy-based routing > user-defined routing and app-based routing > static route > auto routing > multi-link load balancing and default route.

Note

The system supports up to 32 equal-cost routes to the same destination subnet. If more than 32 equal-cost routes are configured, only the ones configured first will be taken into account.



Static Route: By adding a static route, packets destined for a specified destination network are routed along a predetermined path.

'Routing Preference: ', Source In Source Out > Forward DNS Proxy > Policy Routing > User Routing and Application Routing > Static Routing > Address Base Auto Routing > Multi-Link Load Balancing and Default Routing

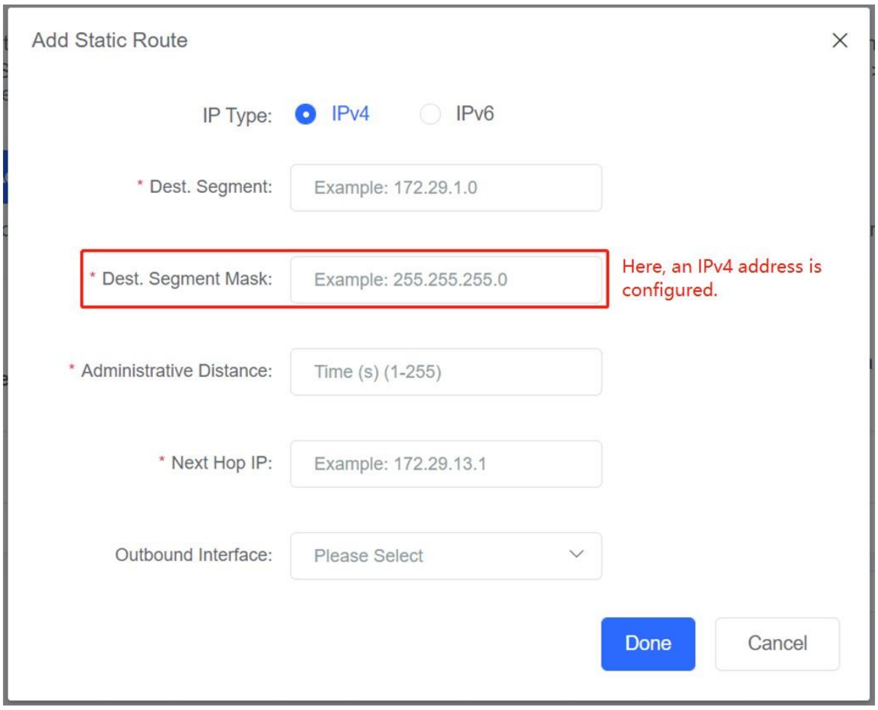
Note: The system supports configuring 32 equal-cost routes to the same destination network segment. If the number of equal-cost routes is greater than 32, only the first 32 equal-cost routes take effect.

□	Dest. Segment:	Dest. Mask	Next Hop IP	Router Outbound Interface	Administrative Distance	Type	Action
□	0.0.0.0	0.0.0.0	10.110.60.1		1	Default Route	Edit Delete

Total 1

- **Adding a static route**

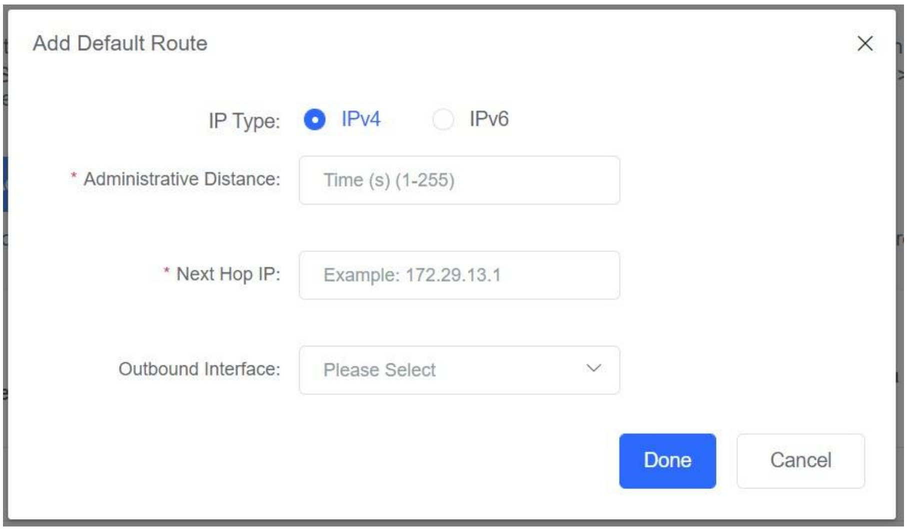
To add a static route, click **Add Static Route**. The **Add Static Route** window is displayed. Set configuration parameters and click Done .


Add Static Route
IP Type: ● IPv4 ○ IPv6
* Dest. Segment: Example: 172.29.1.0
* Dest. Segment Mask: Example: 255.255.255.0
* Administrative Distance: Time (s) (1-255)
* Next Hop IP: Example: 172.29.13.1
Outbound Interface: Please Select
Done
Cancel

Here, an IPv4 address is configured.

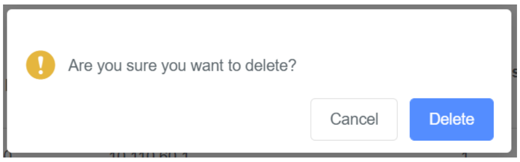
- **Adding a default route**

To add a default route, click Add Default Route. The **Add Default Route** window is displayed. Set configuration parameters and click Done .


Add Default Route
IP Type: ● IPv4 ○ IPv6
* Administrative Distance: Time (s) (1-255)
* Next Hop IP: Example: 172.29.13.1
Outbound Interface: Please Select
Done
Cancel

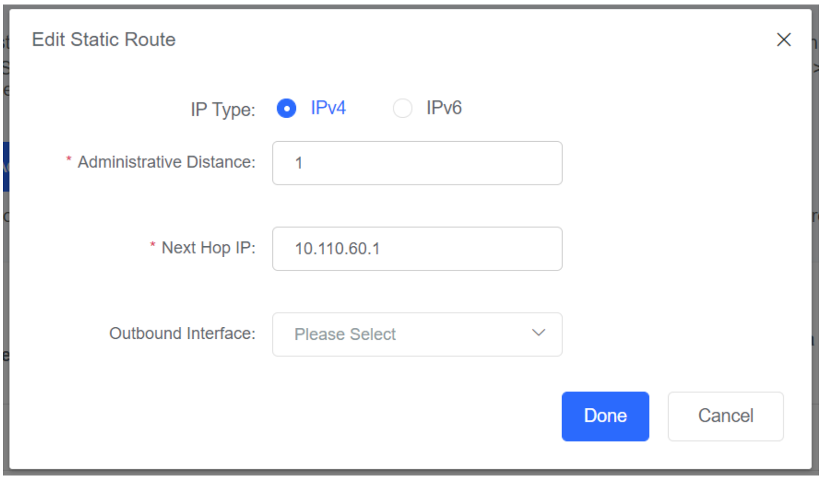
- **Deleting the selected routes**

To delete the selected routes, click on □ next to each route to select multiple routes, and then click Delete Selected Route. A dialog box is displayed. Click Delete .



- **Editing a static route**

To edit a route, click Edit. The **Edit Static Route** window is displayed. Set configuration parameters and click Done.



Edit Static Route

IP Type: ● IPv4 ○ IPv6

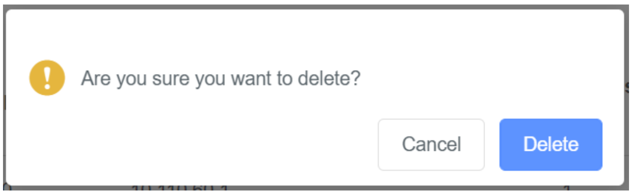
* Administrative Distance: 1

* Next Hop IP: 10.110.60.1

Outbound Interface: Please Select

- **Deleting a static route**

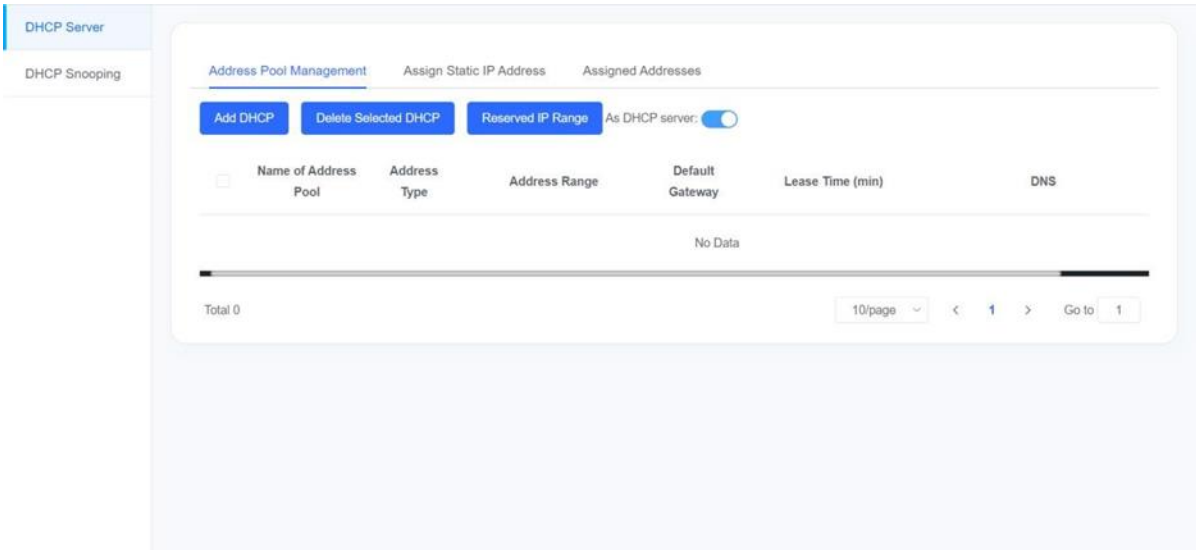
To delete a static route, click Delete. A dialog box is displayed. Click Delete.



4. DHCP Server

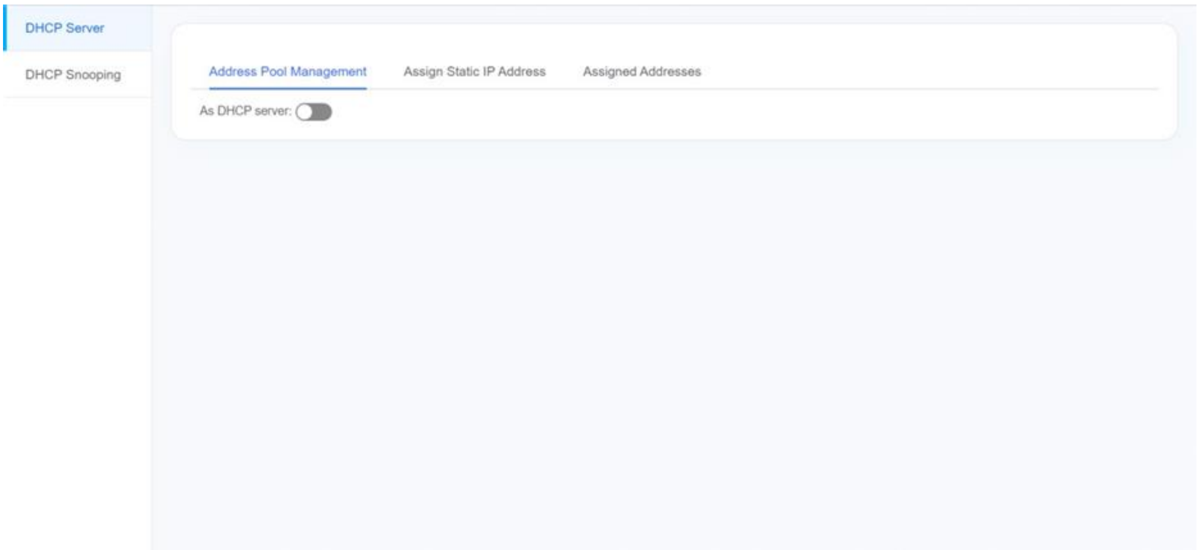
DHCP Address Pool Management

- **Enabling the DHCP server**

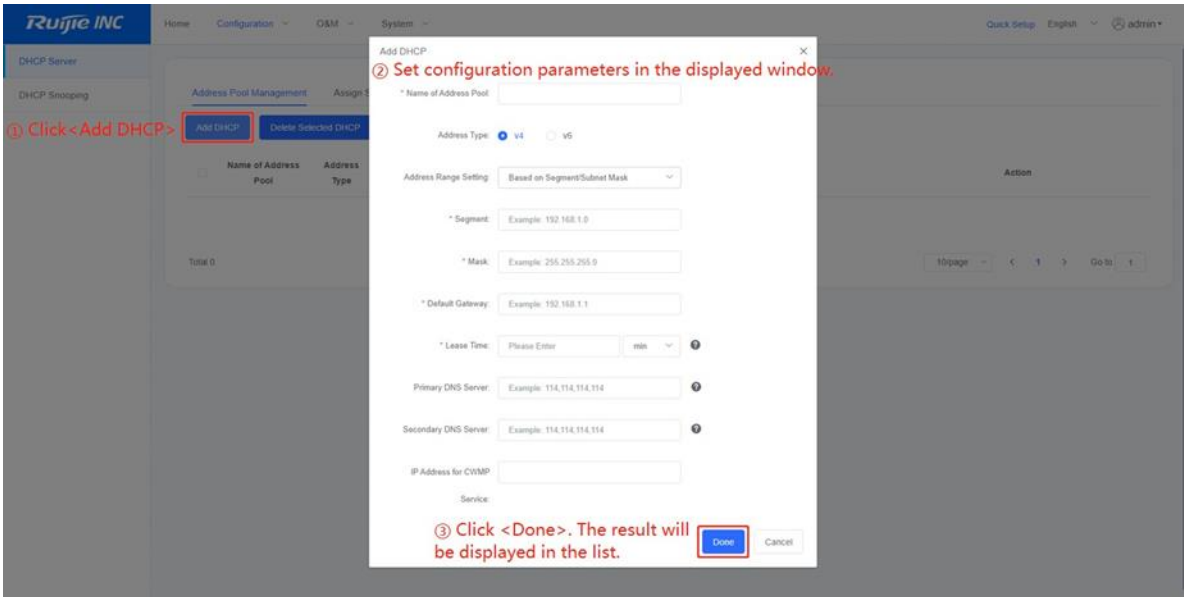


Name of Address Pool	Address Type	Address Range	Default Gateway	Lease Time (min)	DNS
No Data					

- **Disabling the DHCP server**



- **Adding a DHCP address pool**

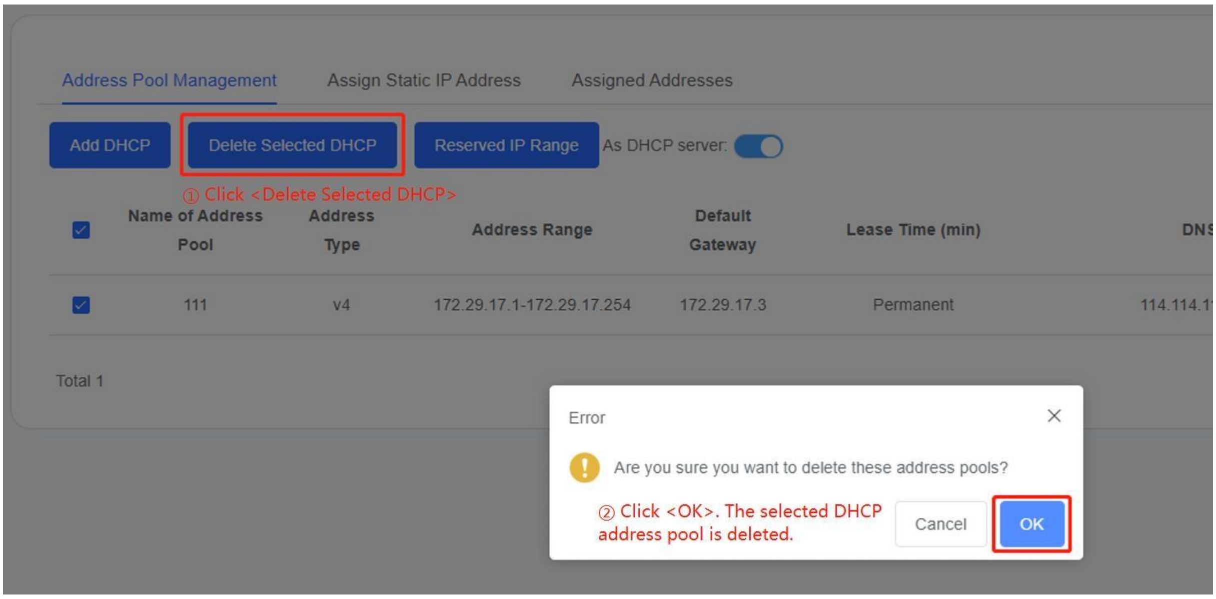


① Click<Add DHCP>

② Set configuration parameters in the displayed window.

③ Click <Done>. The result will be displayed in the list.

- **Deleting the selected DHCP address pool**



① Click <Delete Selected DHCP>

☑	Name of Address Pool	Address Type	Address Range	Default Gateway	Lease Time (min)	DNS
☑	111	v4	172.29.17.1-172.29.17.254	172.29.17.3	Permanent	114.114.1

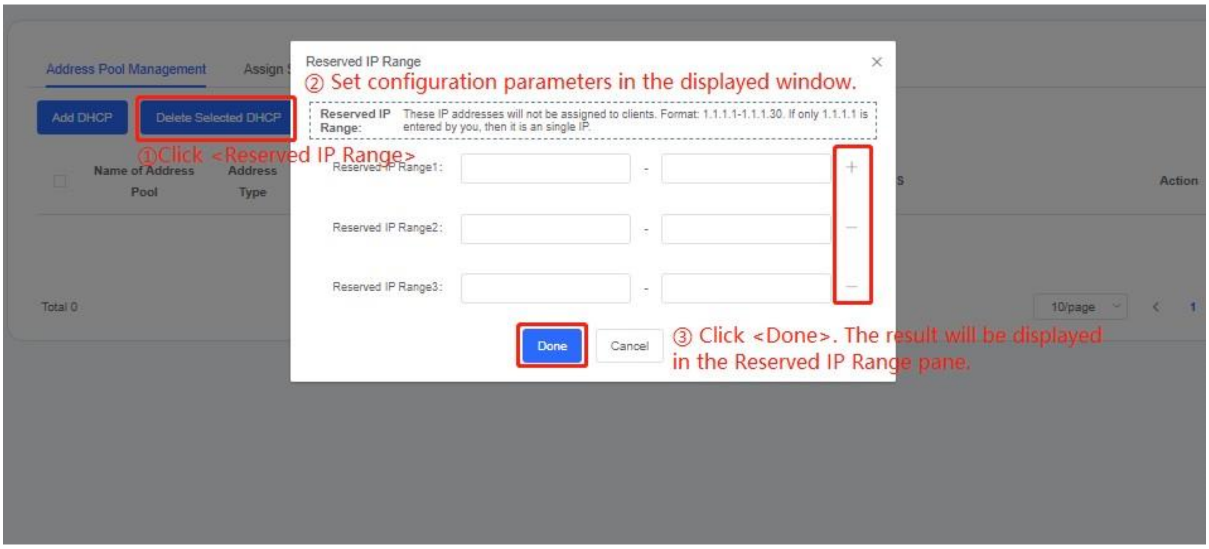
Total 1

Error

Are you sure you want to delete these address pools?

② Click <OK>. The selected DHCP address pool is deleted.

- **Configuring the reserved IP range**



①Click <Reserved IP Range>

Reserved IP Range

② Set configuration parameters in the displayed window.

Reserved IP Range: These IP addresses will not be assigned to clients. Format: 1.1.1.1-1.1.1.30. If only 1.1.1.1 is entered by you, then it is an single IP.

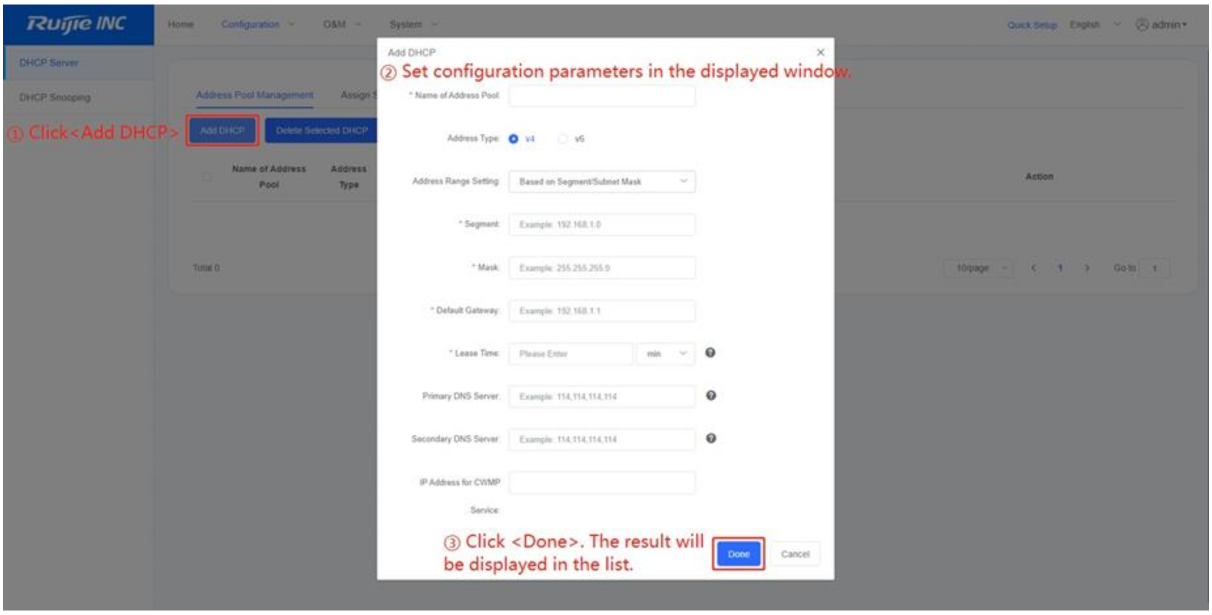
Reserved IP Range1: -

Reserved IP Range2: -

Reserved IP Range3: -

③ Click <Done>. The result will be displayed in the Reserved IP Range pane.

- **Editing a DHCP address pool**



① Click<Add DHCP>

Add DHCP

② Set configuration parameters in the displayed window.

* Name of Address Pool:

Address Type: ● v4 ○ v6

Address Range Setting: Based on Segment/Subnet Mask

* Segment: Example: 192.168.1.0

* Mask: Example: 255.255.255.0

* Default Gateway: Example: 192.168.1.1

* Lease Time: Please Enter min

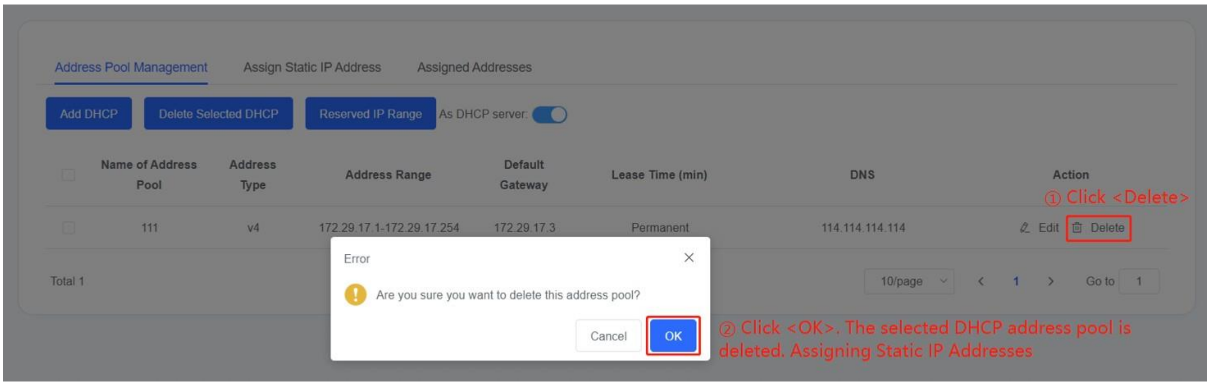
Primary DNS Server: Example: 114.114.114.114

Secondary DNS Server: Example: 114.114.114.114

IP Address for CWMP Service:

③ Click <Done>. The result will be displayed in the list.

- **Deleting a DHCP address pool**



□	Name of Address Pool	Address Type	Address Range	Default Gateway	Lease Time (min)	DNS	Action
□	111	v4	172.29.17.1-172.29.17.254	172.29.17.3	Permanent	114.114.114.114	Edit Delete

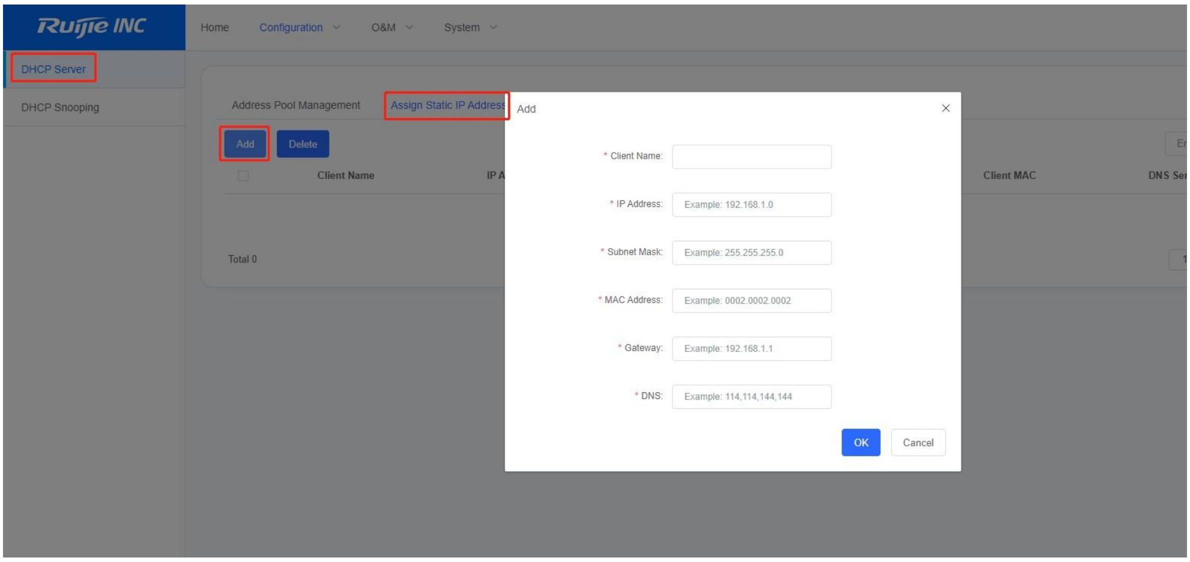
① Click <Delete>

Error

Are you sure you want to delete this address pool?

② Click <OK>. The selected DHCP address pool is deleted. Assigning Static IP Addresses

- Choose **DHCP Server** > **Assign Static IP Address** > **Add** to access the **Add static IP address** page and add a static IP address.



Add

* Client Name:

* IP Address: Example: 192.168.1.0

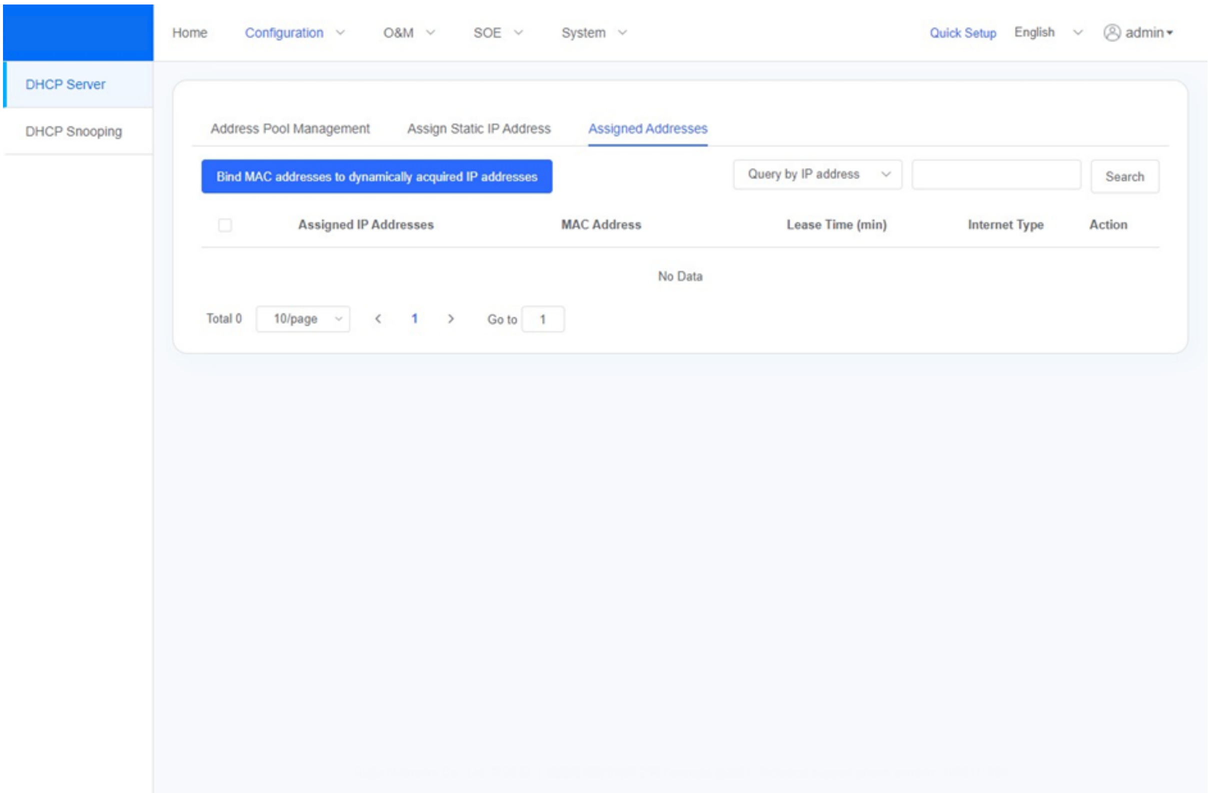
* Subnet Mask: Example: 255.255.255.0

* MAC Address: Example: 0002.0002.0002

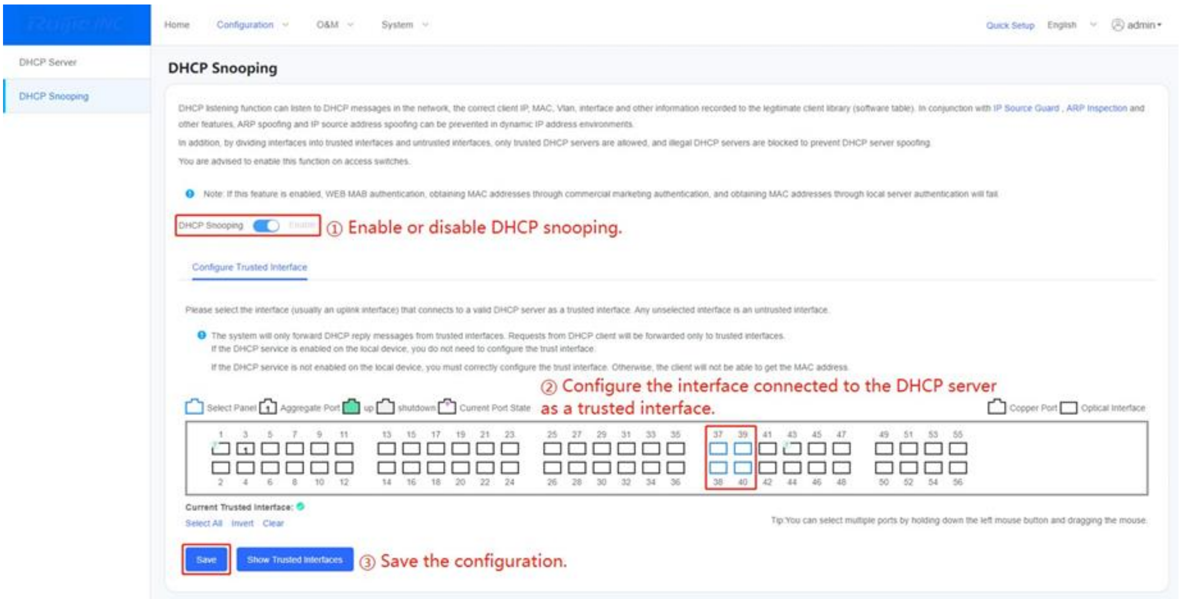
* Gateway: Example: 192.168.1.1

* DNS: Example: 114.114.144.144

The Assigned IP Addresses Page



5. Configuring DHCP Snooping



DHCP Snooping

DHCP listening function can listen to DHCP messages in the network, the correct client IP, MAC, Vlan, interface and other information recorded to the legitimate client library (software table). In conjunction with IP Source Guard , ARP Inspection and other features, ARP spoofing and IP source address spoofing can be prevented in dynamic IP address environments.

In addition, by dividing interfaces into trusted interfaces and untrusted interfaces, only trusted DHCP servers are allowed, and illegal DHCP servers are blocked to prevent DHCP server spoofing.

You are advised to enable this function on access switches.

Note: If this feature is enabled, WEB MAB authentication, obtaining MAC addresses through commercial marketing authentication, and obtaining MAC addresses through local server authentication will fail.

① Enable or disable DHCP snooping.

Please select the interface (usually an uplink interface) that connects to a valid DHCP server as a trusted interface. Any unselected interface is an untrusted interface.

The system will only forward DHCP reply messages from trusted interfaces. Requests from DHCP client will be forwarded only to trusted interfaces.
If the DHCP service is enabled on the local device, you do not need to configure the trust interface.

If the DHCP service is not enabled on the local device, you must correctly configure the trust interface. Otherwise, the client will not be able to get the MAC address.

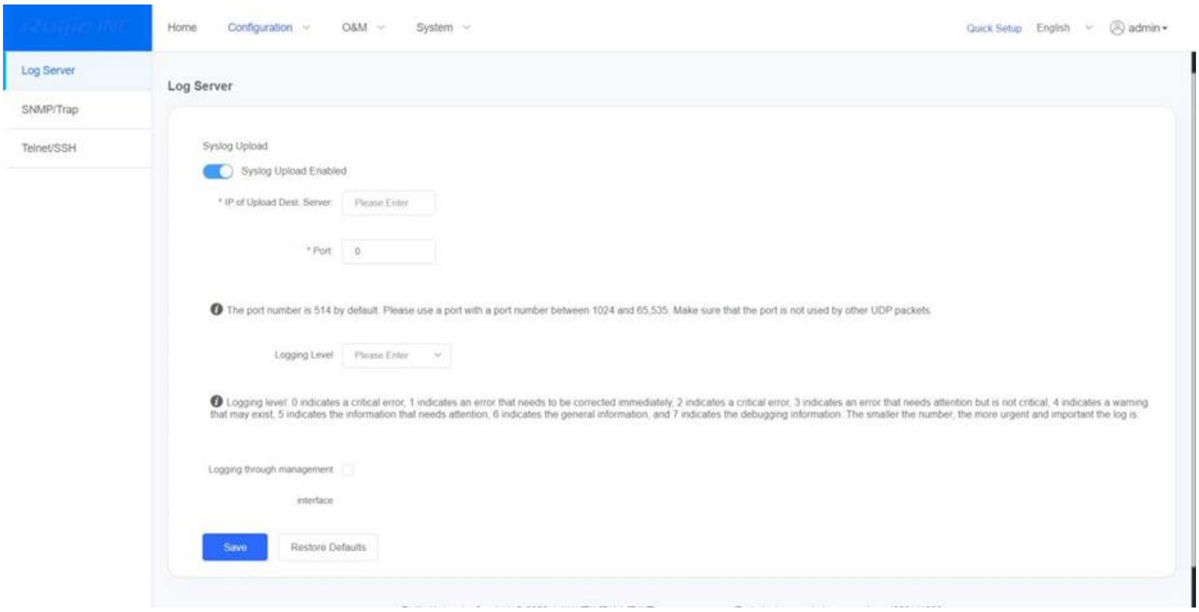
② Configure the interface connected to the DHCP server as a trusted interface.

Tip:You can select multiple ports by holding down the left mouse button and dragging the mouse.

③ Save the configuration.

6. Logs

Configuring the Log Server



Log Server

Syslog Upload

Syslog Upload Enabled

* IP of Upload Dest. Server: Please Enter

* Port: 0

The port number is 514 by default. Please use a port with a port number between 1024 and 65,535. Make sure that the port is not used by other UDP packets.

Logging Level: Please Enter

Logging level: 0 indicates a critical error, 1 indicates an error that needs to be corrected immediately, 2 indicates a critical error, 3 indicates an error that needs attention but is not critical, 4 indicates a warning that may exist, 5 indicates the information that needs attention, 6 indicates the general information, and 7 indicates the debugging information. The smaller the number, the more urgent and important the log is.

Logging through management interface □

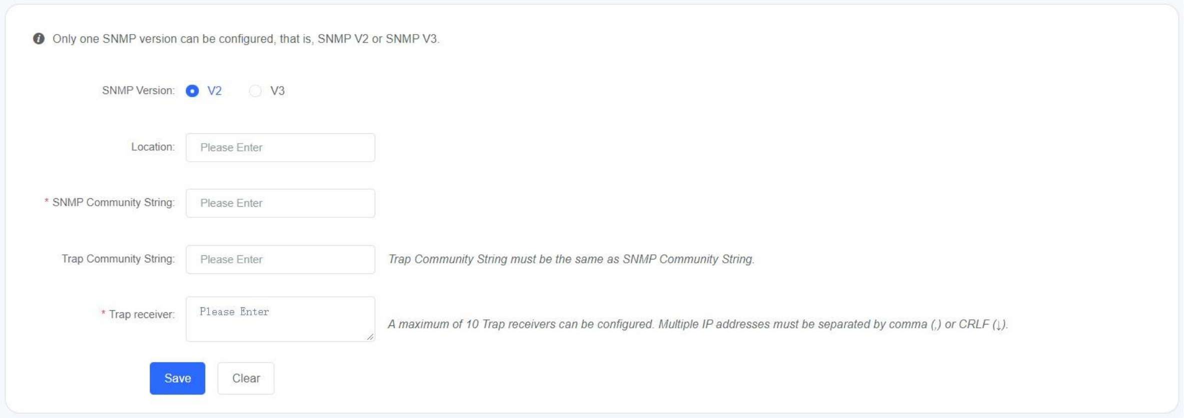
Save | Restore Defaults

Configuring SNMP or the Trap Function

The Simple Network Management Protocol (SNMP) enables a network administrator to easily monitor and manage nodes on a network.

- **SNMP Version**: indicates the SNMP version supported by the switch, which can be SNMPv2 or SNMPv3.
- **Location**: indicates the location of the switch.
- **SNMP Community String**: is used by the management host to connect to a switch.
- **Trap Community String**: is used to connect to the management host. When an alarm is generated on a switch, the switch can send the alarm to the management host.
- **Trap receiver**: refers to the management host that receives alarms from a switch. A maximum of 10 trap receivers can be configured.

SNMPv3 is more secure than SNMPv2. The encryption password and authentication password of SNMP users need to be configured.



Only one SNMP version can be configured, that is, SNMP V2 or SNMP V3.

SNMP Version: ● V2 ○ V3

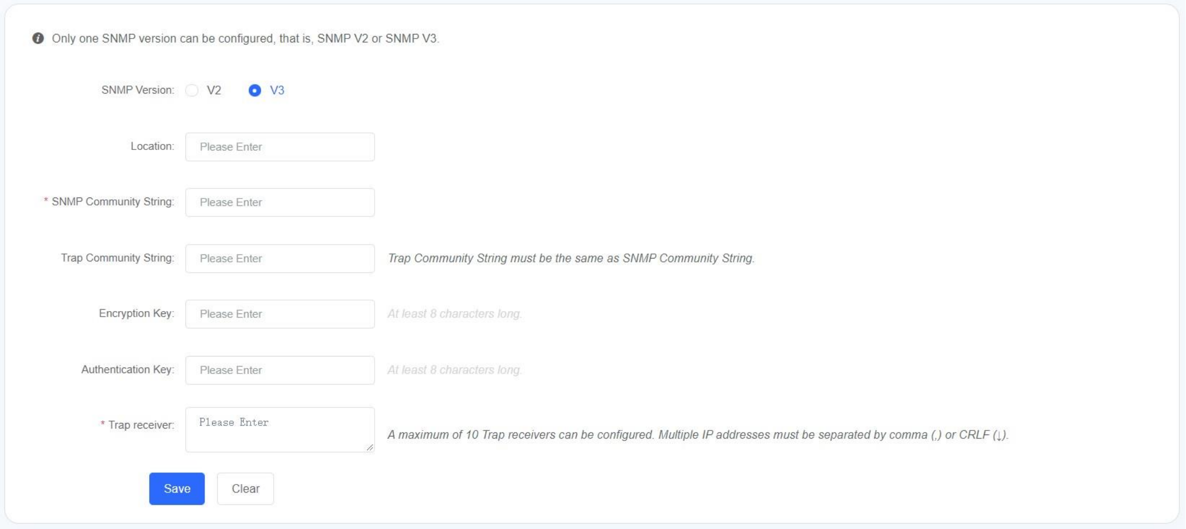
Location: Please Enter

* SNMP Community String: Please Enter

Trap Community String: Please Enter *Trap Community String must be the same as SNMP Community String.*

* Trap receiver: Please Enter *A maximum of 10 Trap receivers can be configured. Multiple IP addresses must be separated by comma (,) or CRLF (↓).*

Save | Clear



Only one SNMP version can be configured, that is, SNMP V2 or SNMP V3.

SNMP Version: ○ V2 ● V3

Location: Please Enter

* SNMP Community String: Please Enter

Trap Community String: Please Enter *Trap Community String must be the same as SNMP Community String.*

Encryption Key: Please Enter *At least 8 characters long.*

Authentication Key: Please Enter *At least 8 characters long.*

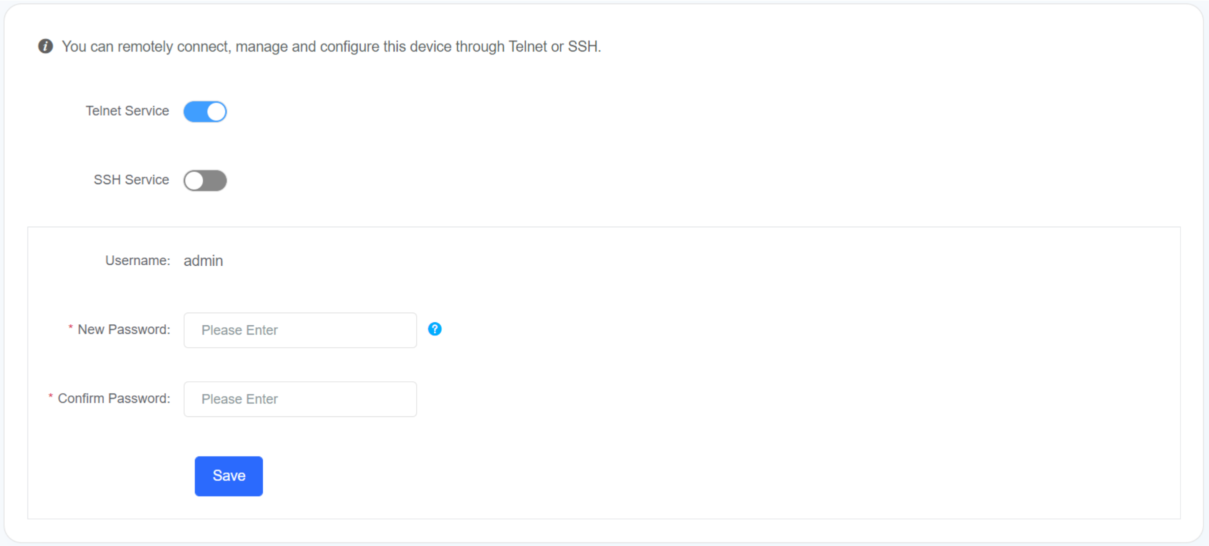
* Trap receiver: Please Enter *A maximum of 10 Trap receivers can be configured. Multiple IP addresses must be separated by comma (,) or CRLF (↓).*

SNMP V2: Select ● V2 . Set configuration parameters and click Save to submit the configuration.

SNMP V3: Select ● V3 . Set configuration parameters and click Save to submit the configuration.

Clear: Click Clear to clear the SNMPv2 or SNMPv3 configuration.

Configuring Telnet or SSH



You can remotely connect, manage and configure this device through Telnet or SSH.

Telnet Service

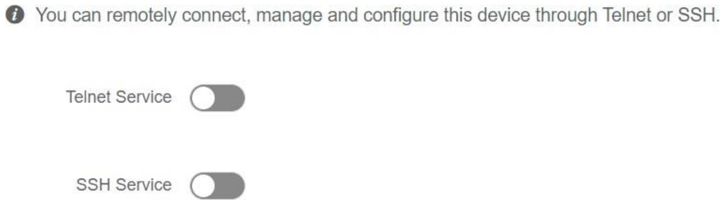
SSH Service

Username: admin

* New Password: Please Enter

* Confirm Password: Please Enter

Telnet/SSH: Click Telnet Service to enable or disable the Telnet service, and click SSH Service to enable or disable the SSH service. The default username is **admin**. Set configuration parameters and click Save to submit Telnet or SSH configurations. When both the Telnet service and SSH service are disabled, you do not need to set a password.



You can remotely connect, manage and configure this device through Telnet or SSH.

Telnet Service

SSH Service

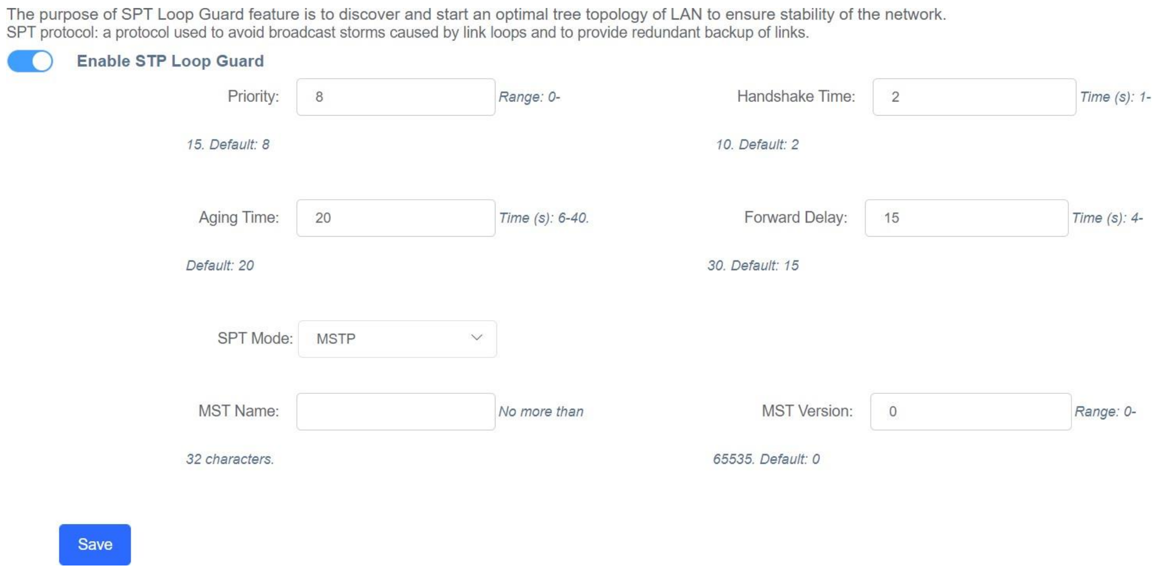
When configuring a switch through Telnet, you must log in with this password.

Note

Remember the new password for login next time.

7. STP Loop Guard

Global Settings



The purpose of SPT Loop Guard feature is to discover and start an optimal tree topology of LAN to ensure stability of the network.
SPT protocol: a protocol used to avoid broadcast storms caused by link loops and to provide redundant backup of links.

Enable STP Loop Guard

Priority: 8 *Range: 0-15. Default: 8*

Handshake Time: 2 *Time (s): 1-10. Default: 2*

Aging Time: 20 *Time (s): 6-40. Default: 20*

Forward Delay: 15 *Time (s): 4-30. Default: 15*

SPT Mode: MSTP

MST Name: *No more than 32 characters.*

MST Version: 0 *Range: 0-65535. Default: 0*

Save

Enable or disable STP Loop Guard: Click Enable STP Loop Guard to enable or disable STP loop guard.

Global Settings: Enable **STP Loop Guard** and set configuration parameters. There are three STP modes, which are STP, RSTP, and MSTP. Click Save to submit the global settings.

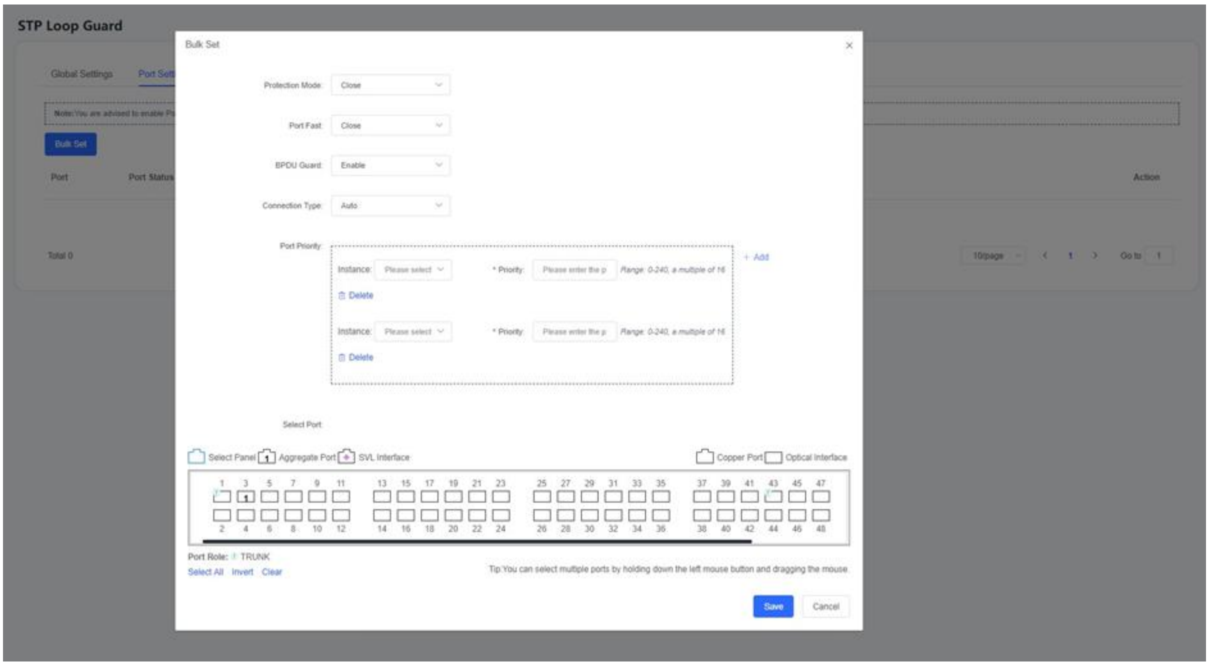
Port Settings

Note

You are advised to enable **Port Fast** on the port directly connected to a PC.

1. Setting the STP loop guard function for multiple ports

Click Bulk Set . The **Bulk Set** window is displayed. Set configuration parameters. Add or delete the port priority by clicking + Add or 🗑 Delete . Select multiple ports and click Save to submit the configuration. The result will the appear on the list.



STP Loop Guard

Bulk Set

Protection Mode: Close

Port Fast: Close

BPDU Guard: Enable

Connection Type: Auto

Port Priority:

Instance: Please select * Priority: Please enter the p Range: 0-240, a multiple of 16

Instance: Please select * Priority: Please enter the p Range: 0-240, a multiple of 16

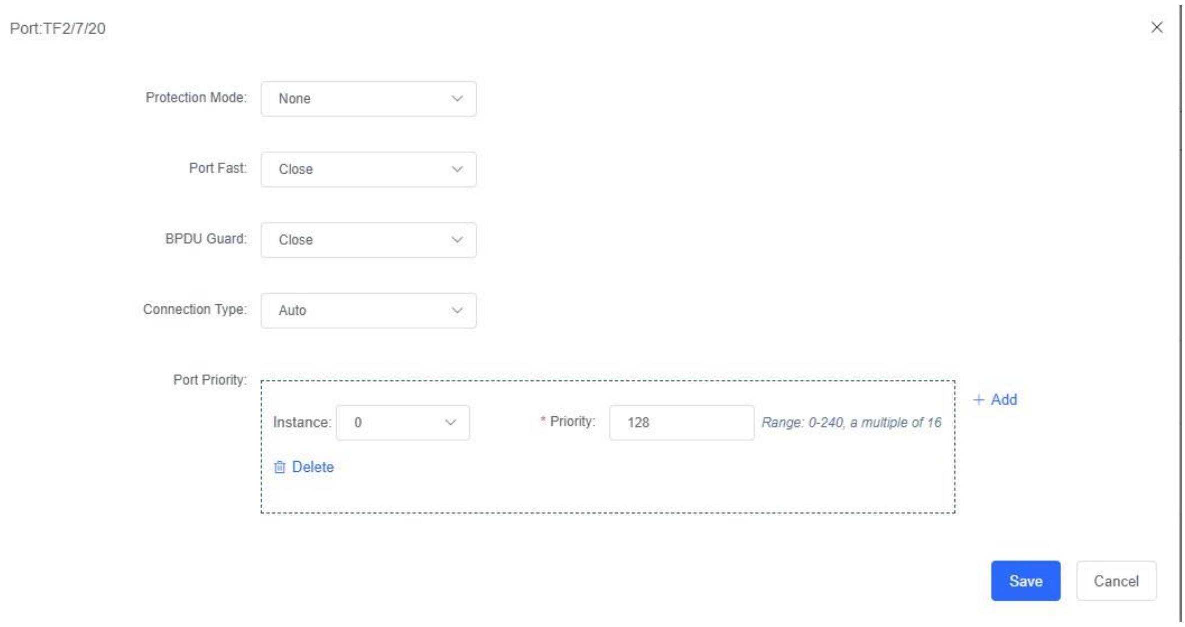
Select Port

Port Role: TRUNK

Tip:You can select multiple ports by holding down the left mouse button and dragging the mouse

2. Editing the STP loop guard function for a single port

Click Edit in the **Action** column. A window is displayed. Set configuration parameters. Add or delete the port priority by clicking + Add or Delete. Click Save to submit the configuration. Then the result will be displayed in the list.



Port:TF2/7/20

Protection Mode: None

Port Fast: Close

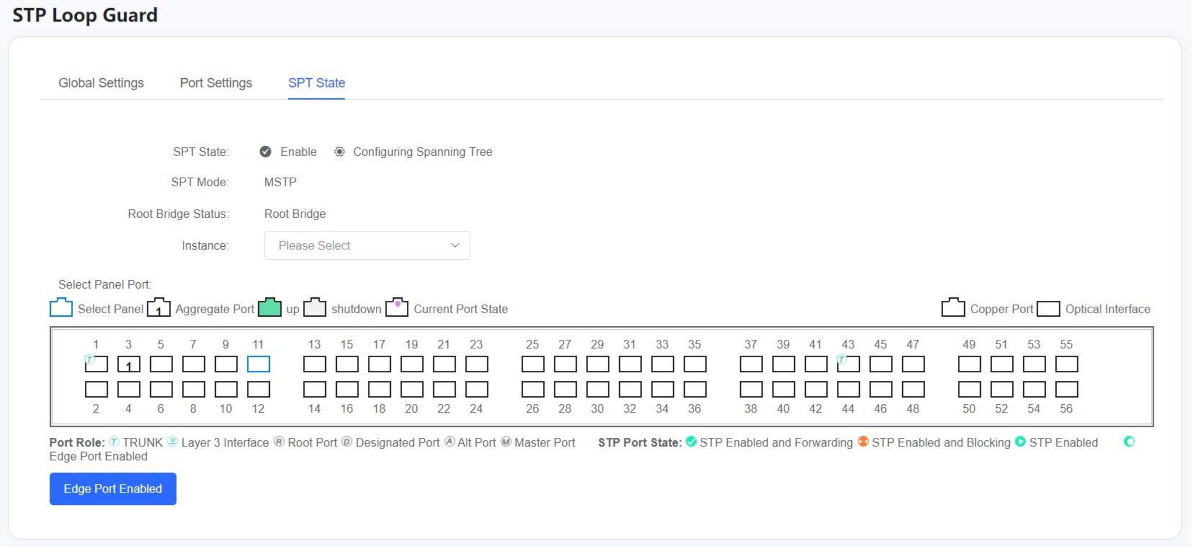
BPDU Guard: Close

Connection Type: Auto

Port Priority:

Instance: 0 * Priority: 128 Range: 0-240, a multiple of 16

STP State



STP Loop Guard

SPT State: ● Enable ◉ Configuring Spanning Tree

SPT Mode: MSTP

Root Bridge Status: Root Bridge

Instance: Please Select

Select Panel Port:

Port Role: Ⓣ TRUNK Ⓛ Layer 3 Interface Ⓡ Root Port Ⓓ Designated Port Ⓐ Alt Port Ⓜ Master Port **STP Port State:** ● STP Enabled and Forwarding ● STP Enabled and Blocking ● STP Enabled ● Edge Port Enabled

Disable Edge Port: Select the Up port 23 and click Edge Port Enabled. The icon of Port 23 is changed to 23.

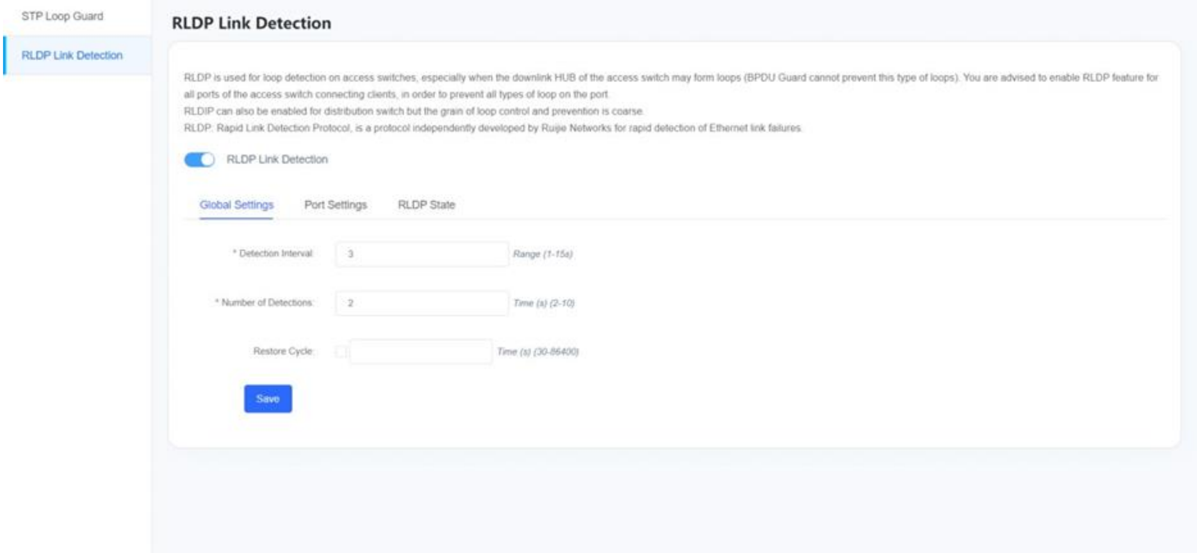
Enable Edge Port: Select the Up port 23 and click Edge Port Enabled. The icon of Port 23 is changed to 23.

8. RLDP

The Rapid Link Detection Protocol (RLDP) is independently developed by Ruijie Networks for rapid detection of Ethernet link failures. It is used for loop detection on access switches where a loop occurs on the downstream hub of the access switch (BPDU guard cannot prevent this type of loops). We recommend enabling RLDP on the access switch ports connected to clients to prevent all types of loops.

RLDP can also be enabled for distribution switches, but the loop guard performance is coarse-grained.

Global Settings



STP Loop Guard

RLDP Link Detection

RLDP Link Detection

RLDP is used for loop detection on access switches, especially when the downlink HUB of the access switch may form loops (BPDU Guard cannot prevent this type of loops). You are advised to enable RLDP feature for all ports of the access switch connecting clients, in order to prevent all types of loop on the port.
RLDIP can also be enabled for distribution switch but the grain of loop control and prevention is coarse.
RLDP: Rapid Link Detection Protocol, is a protocol independently developed by Ruijie Networks for rapid detection of Ethernet link failures.

● RLDP Link Detection

Global Settings | Port Settings | RLDP State

* Detection Interval: 3 *Range (1-15s)*

* Number of Detections: 2 *Time (s) (2-10)*

Restore Cycle: □ *Time (s) (30-86400)*

Save

1. **Save**: After you have entered the detection interval, number of detections, and restoration cycle (optional), click Save to save the global settings.

2. **RLDP Link Detection**: Click ● RLDP Link Detection to enable or disable RLDP.

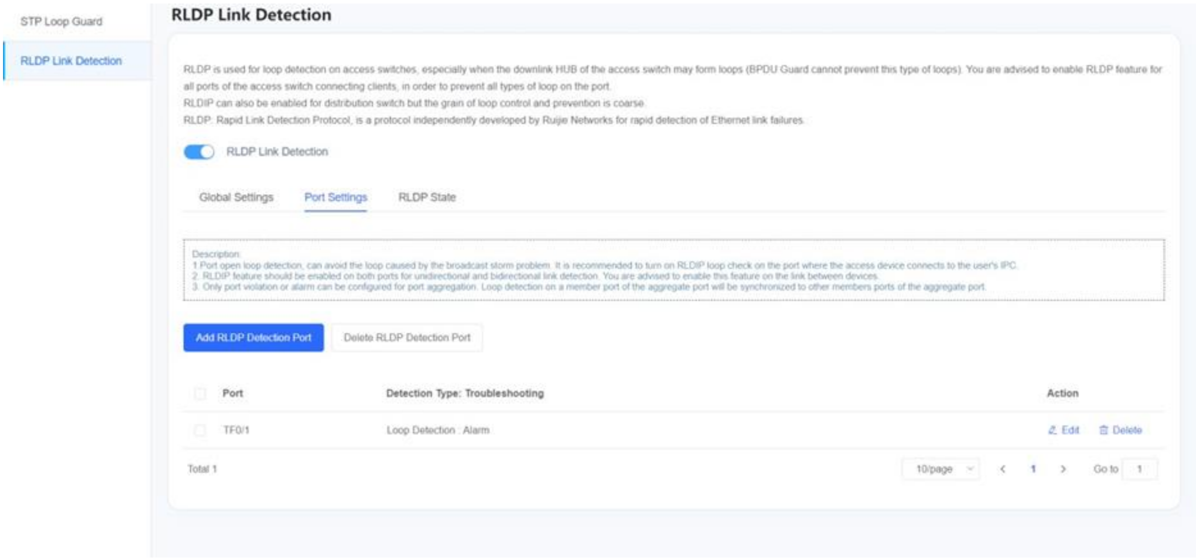
Port Configuration

Note

(1) Enabling loop detection on a port can prevent broadcast storm caused by loops. You are advised to enable loop detection on ports of the access switch connecting to a client.

(2) RLDP must be enabled on both ports for unidirectional and bidirectional link detection. You are advised to enable RLDP on the link between switches.

(3) Only port violation or alarm detection types can be configured for aggregate ports. Loop detection ona member port of the aggregate port will be synchronized to other member ports of the aggregate port.



STP Loop Guard

RLDP Link Detection

RLDP Link Detection

RLDP is used for loop detection on access switches, especially when the downlink HUB of the access switch may form loops (BPDU Guard cannot prevent this type of loops). You are advised to enable RLDP feature for all ports of the access switch connecting clients, in order to prevent all types of loop on the port.
RLDIP can also be enabled for distribution switch but the grain of loop control and prevention is coarse.
RLDP: Rapid Link Detection Protocol, is a protocol independently developed by Ruijie Networks for rapid detection of Ethernet link failures.

● RLDP Link Detection

Global Settings | Port Settings | RLDP State

Description:
1.Port open loop detection, can avoid the loop caused by the broadcast storm problem. It is recommended to turn on RLDIP loop check on the port where the access device connects to the user's IPC.
2. RLDIP feature should be enabled on both ports for unidirectional and bidirectional link detection. You are advised to enable this feature on the link between devices.
3. Only port violation or alarm can be configured for port aggregation. Loop detection on a member port of the aggregate port will be synchronized to other members ports of the aggregate port.

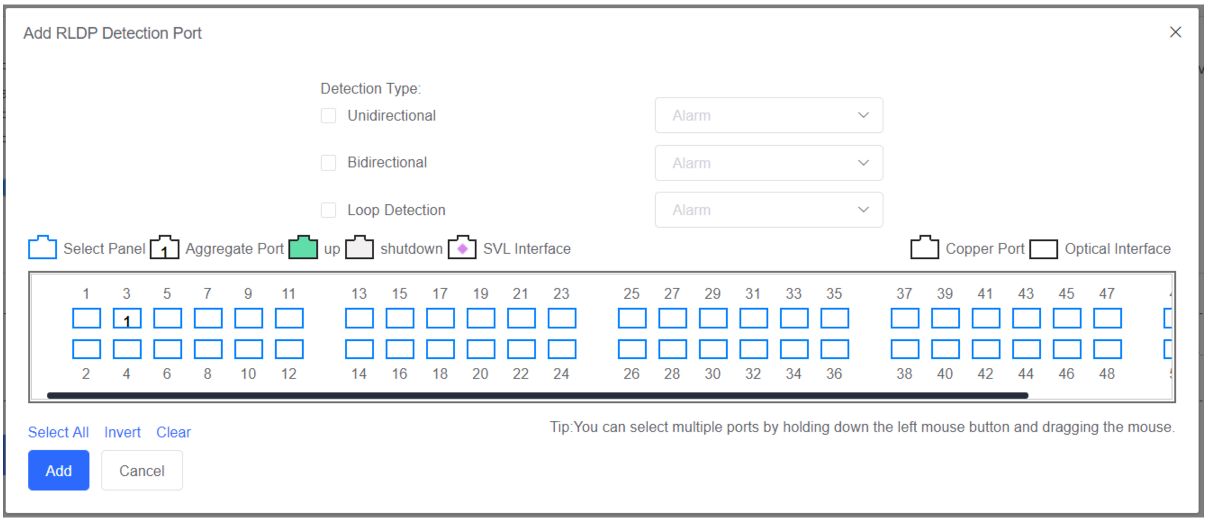
Add RLDP Detection Port | Delete RLDP Detection Port

□	Port	Detection Type: Troubleshooting	Action
□	TF0/1	Loop Detection : Alarm	Edit Delete

Total 1 10/page < 1 > Go to 1

1. Adding an RLDP-enabled port

Click Add RLDP Detection Port . The **Add RLDP Detection Port** window is displayed.



Add RLDP Detection Port

Detection Type:

□ Unidirectional — Alarm

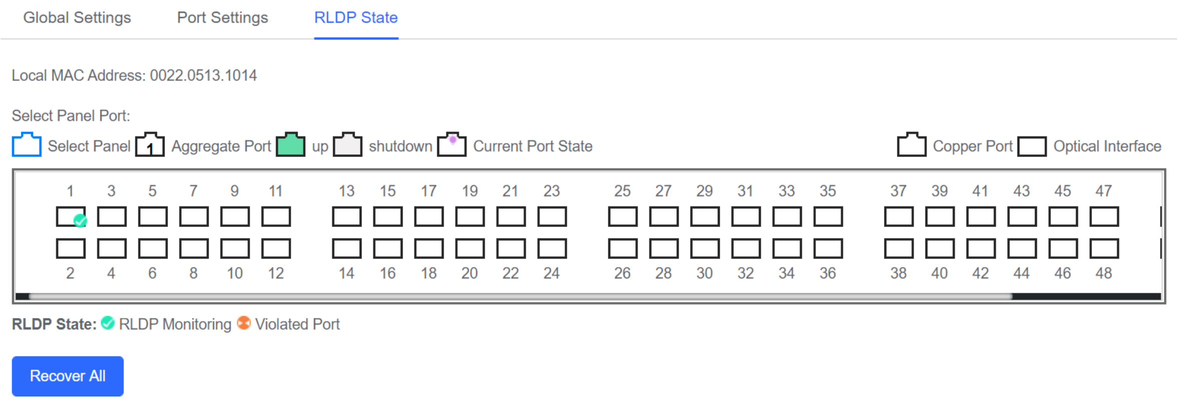
□ Bidirectional — Alarm

□ Loop Detection — Alarm

Tip:You can select multiple ports by holding down the left mouse button and dragging the mouse.

RLDP involves unidirectional link detection, bidirectional link detection, and loop detection. Options in the drop-down list boxes corresponding to these three types include **Alarm**, **Disable port learning and forwarding**, **Port violation**, and **Disable SVI**. You can select multiple ports one by one, or using the Select All Invert Clear button. Click Add to submit the configuration. The result will be displayed in the list.

RLDP State



Local MAC Address: 0022.0513.1014

Select Panel Port:

RLDP State: ✓ RLDP Monitoring ● Violated Port

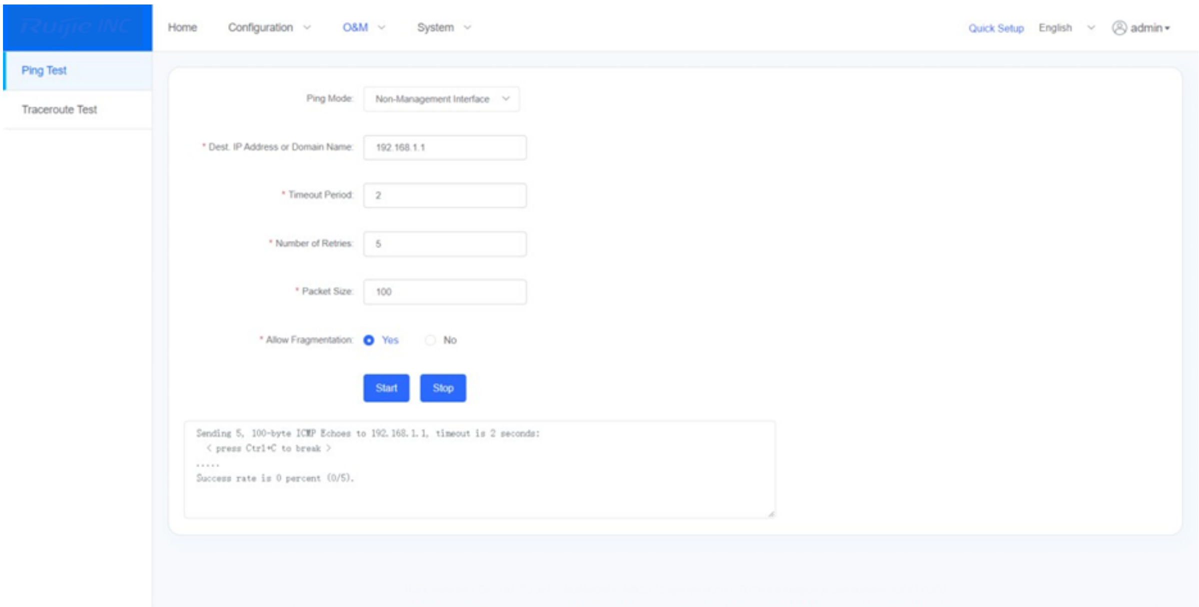
RLDP State: You can select RLDP Monitoring or Violated Port.

Restore All: You can click Recover All to recover all violated ports.

1.3.6 O&M

1. Ping or Tracert

Performing a Ping Test



Ping Mode: Non-Management Interface

* Dest. IP Address or Domain Name: 192.168.1.1

* Timeout Period: 2

* Number of Retries: 5

* Packet Size: 100

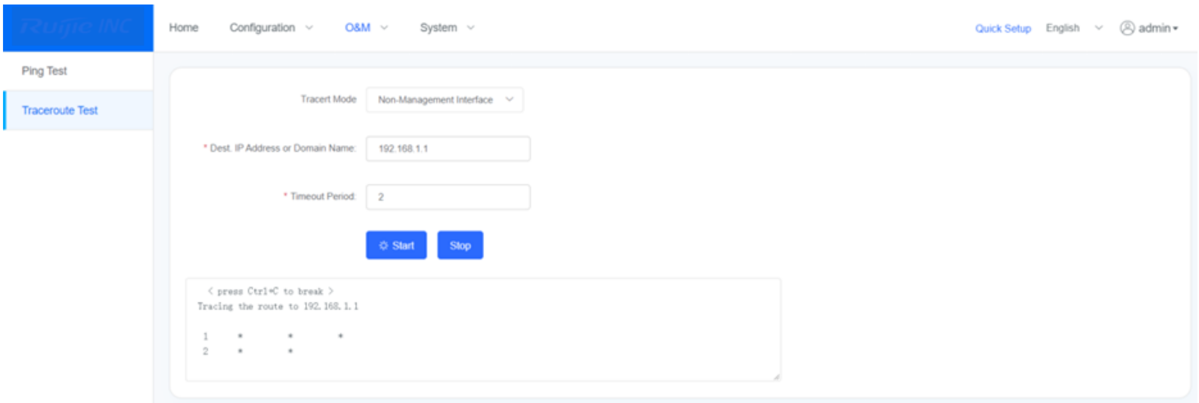
* Allow Fragmentation: ● Yes ○ No

```
Sending 5, 100-byte ICMP Echoes to 192.168.1.1, timeout is 2 seconds:
  < press Ctrl+C to break >
.....
Success rate is 0 percent (0/5).
```

1. Start: Select **Non-Management Interface** from the **Ping Mode** drop-down list box to select the ping mode. You can select **Non-Management Interface** and **Management Interface**, and there may be multiple management interfaces. Enter the destination IP address or domain name, timeout period, number of attempts, and packet size. The **Allow Fragmentation** item is displayed only when **Ping Mode** is set to **Non-Management Interface**. After setting configuration parameters, click Start to run the ping test. After the ping test is complete, the test results will be displayed.

2. **Stop**: Click Stop to stop the current ping test.

Performing a Tracert Test



Tracert Mode: Non-Management Interface

* Dest. IP Address or Domain Name: 192.168.1.1

* Timeout Period: 2

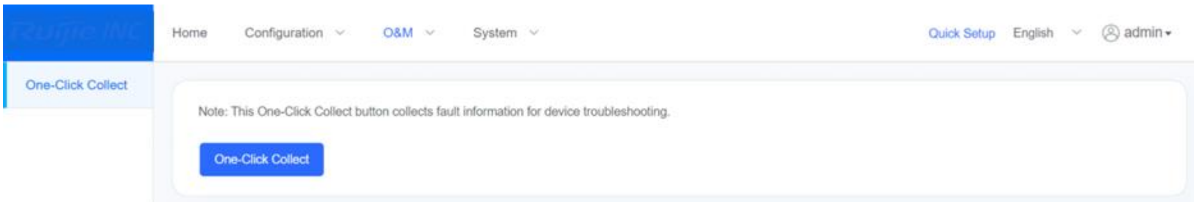
```
  < press Ctrl+C to break >
Tracing the route to 192.168.1.1

 1    *      *      *
 2    *      *
```

1. **Start**: Select **Non-Management Interface** from the **Tracert Mode** drop-down list box to select the tracert mode. You can select **Non-Management Interface** and **Management Interface**, and there may be multiple management interfaces. Enter the destination IP address or domain name and timeout period. Click Start to run the tracert test. After the tracert test is complete, the test results will be displayed.

2. **Stop**: Click Stop to stop the current tracert test.

2. Performing One-Click Collection

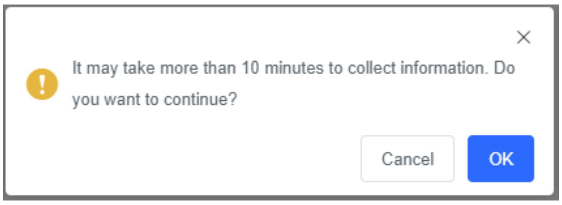
You can use the **One-Click Collect** function to collect switch fault information for troubleshooting.



Note: This One-Click Collect button collects fault information for device troubleshooting.

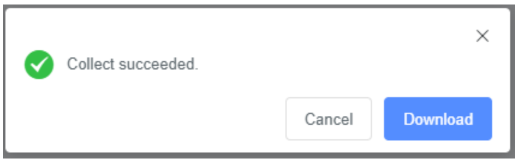
Collecting fault information may take about 10 minutes. After the collection is complete, you can download the collected fault information to a file named **tech_ vsd0_ 20210716142650.tar.gz**.

One-Click Collect: Click One-Click Collect. The **Error** dialog box is displayed.



It may take more than 10 minutes to collect information. Do you want to continue?

Click OK. The collecting process starts, and Collecting... is displayed. After the collection process is complete, the **Error** dialog box is displayed.

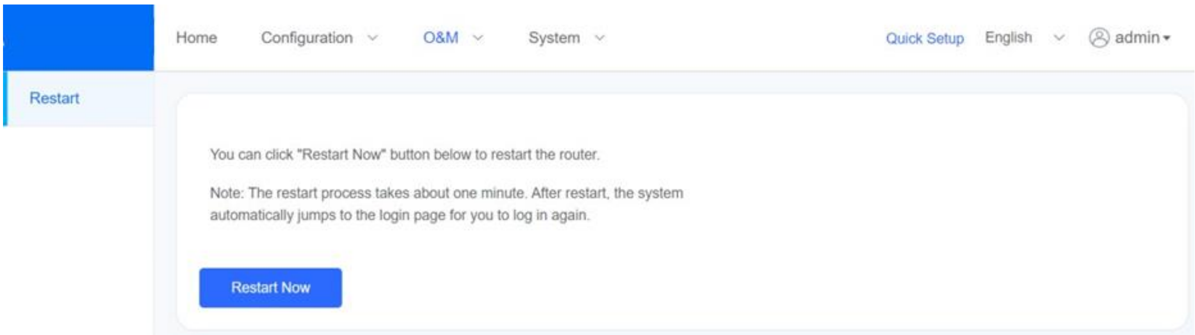


Collect succeeded.

Click Download to download the collected information in a **tar.gz** compressed file.

3. Restarting the Switch

Click **Restart Now** to restart a switch. The restart process takes about 1 minute. Do not perform any operation during this period. After the switch is successfully restarted, the current page will be refreshed automatically.



You can click "Restart Now" button below to restart the router.

Note: The restart process takes about one minute. After restart, the system automatically jumps to the login page for you to log in again.

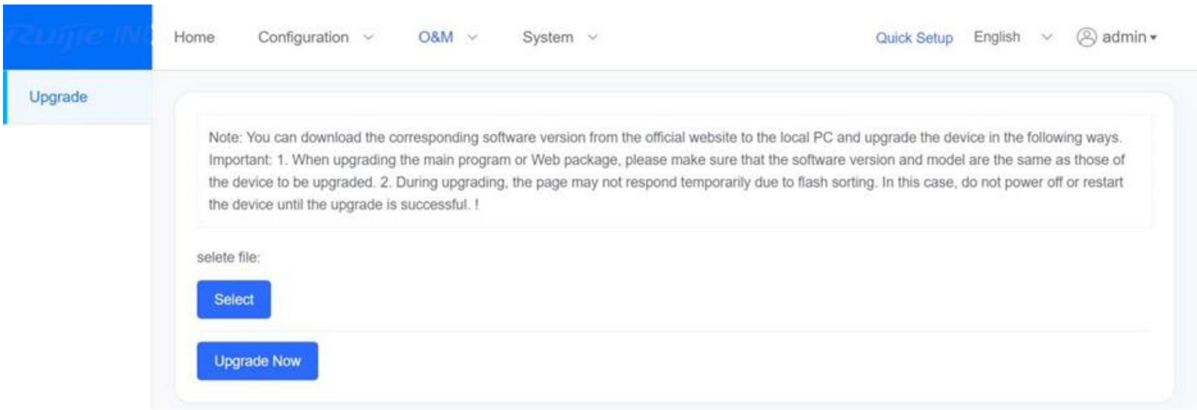
4. Upgrading the Switch

Note

Please download the required software version file and use it to upgrade the switch.

Caution

1. When upgrading the main program or the web package, ensure that the version and model are the same as those of the current switch.
2. During upgrading, there may be no response temporarily due to flash loading. In this case, do not power off or restart the switch until the upgrade is successful.

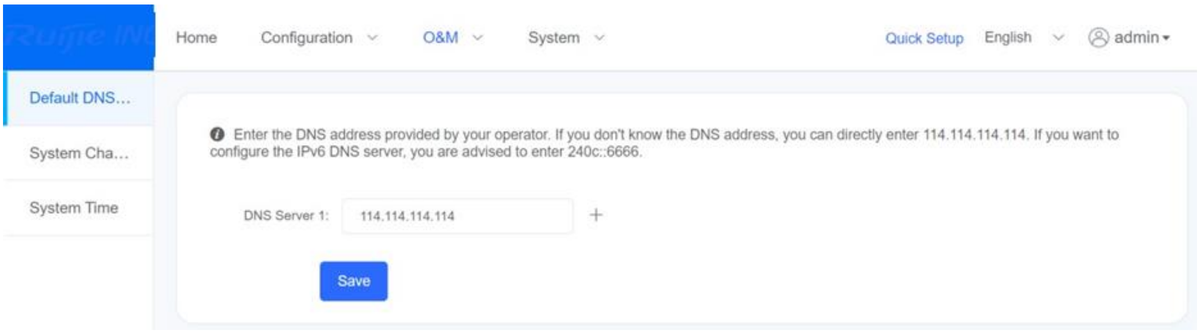


Note: You can download the corresponding software version from the official website to the local PC and upgrade the device in the following ways. Important: 1. When upgrading the main program or Web package, please make sure that the software version and model are the same as those of the device to be upgraded. 2. During upgrading, the page may not respond temporarily due to flash sorting. In this case, do not power off or restart the device until the upgrade is successful. !

selete file:

5. Basic Configurations

Default DNS Server

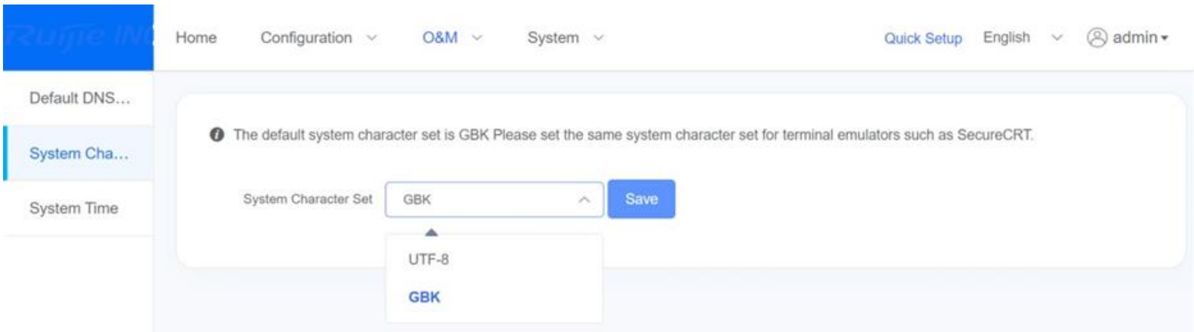


Enter the DNS address provided by your operator. If you don't know the DNS address, you can directly enter 114.114.114.114. If you want to configure the IPv6 DNS server, you are advised to enter 240c::6666.

DNS Server 1: 114.114.114.114

1. You can click + to add a DNS server, click × to delete a DNS server, or click Save to submit the configuration.

System Character Set

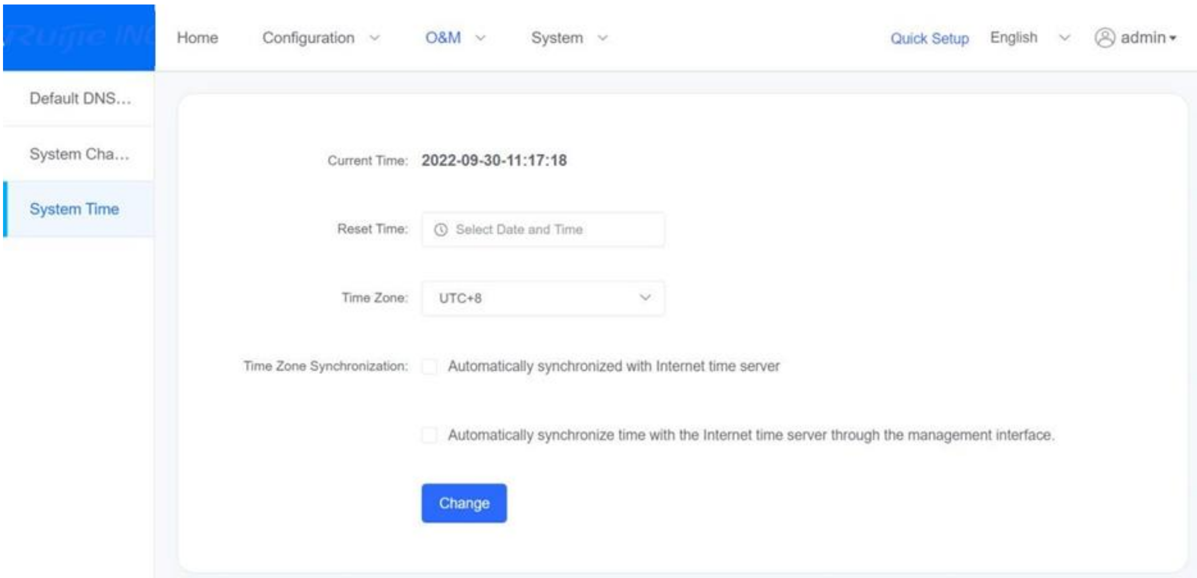


The default system character set is GBK Please set the same system character set for terminal emulators such as SecureCRT.

System Character Set: GBK

System character set: There are two options in the **System Character Set** drop-down list box, which are **UTF-8** and **GBK**. The default value is **UTF-8**. After a character set is selected, click Save to save the configuration.

System Time



Current Time: 2022-09-30-11:17:18

Reset Time: Select Date and Time

Time Zone: UTC+8

Time Zone Synchronization: □ Automatically synchronized with Internet time server

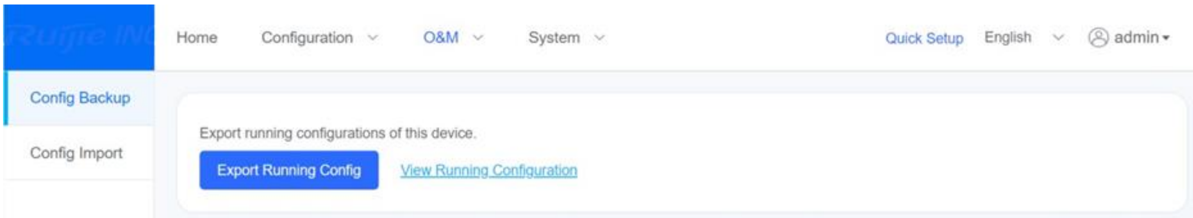
□ Automatically synchronize time with the Internet time server through the management interface.

You can manually select the system time or select **Time Zone Synchronization** to automatically synchronize the switch system time with the Internet time server.

6. Configuration Management

Performing Configuration Backup

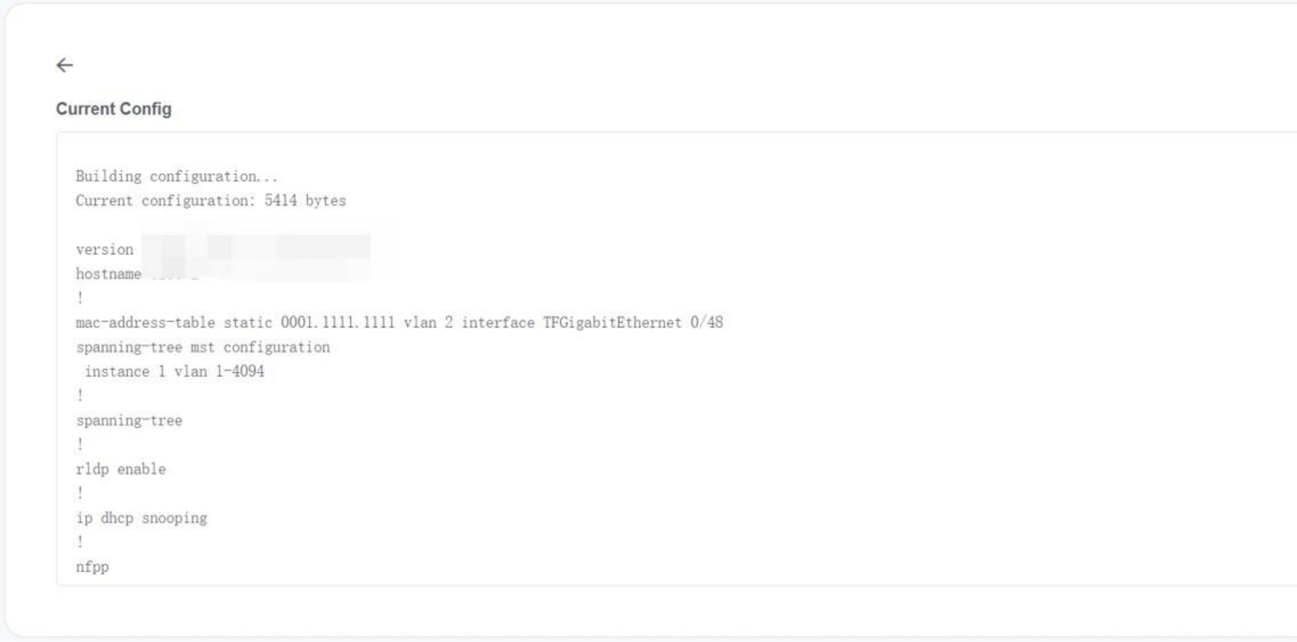
The configuration backup function enables you to import or view the running configuration of the switch.



Export running configurations of this device.

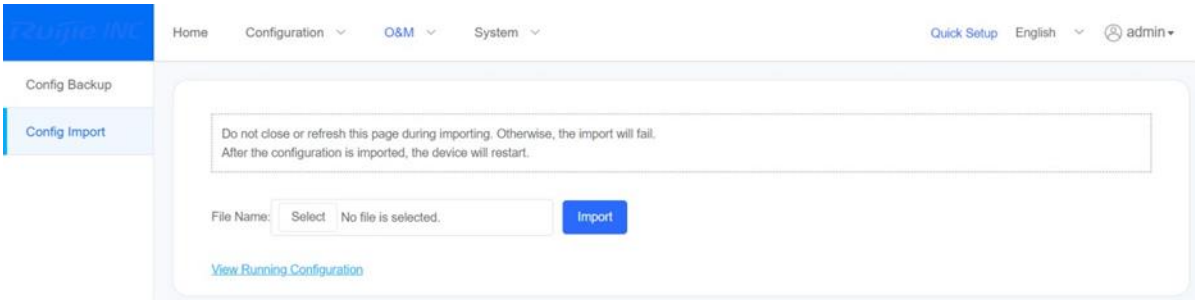
1. **Export running configuration**: You can click Export Running Config to generate the **config.text** text file.

2. **View running configuration**: You can click View Running Configuration to switch to the **Current Config** page.



```
Building configuration...
Current configuration: 5414 bytes

version [redacted]
hostname [redacted]
!
mac-address-table static 0001.1111.1111 vlan 2 interface TFGigabitEthernet 0/48
spanning-tree mst configuration
 instance 1 vlan 1-4094
!
spanning-tree
!
rldp enable
!
ip dhcp snooping
!
nfpp
```

Importing Configurations



Do not close or refresh this page during importing. Otherwise, the import will fail.
After the configuration is imported, the device will restart.

File Name: Select No file is selected. Import

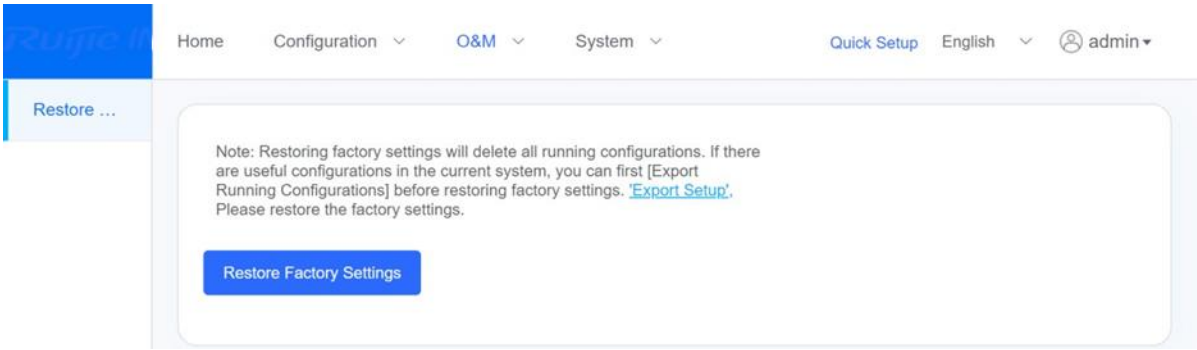
View Running Configuration

1. **Import configurations**: You can click Select to select the configuration file to be imported, and then click Import to import the configuration file.

2. **View running configuration**: You can click View Running Configuration to switch to the **Current Config** page.

7. Restoring Factory Settings

You can click **Restore Factory Settings** to delete all the configurations of the switch and restore the switch to factory settings. To save the current configuration, you are advised to export the current configuration by clicking **Export Setup**.

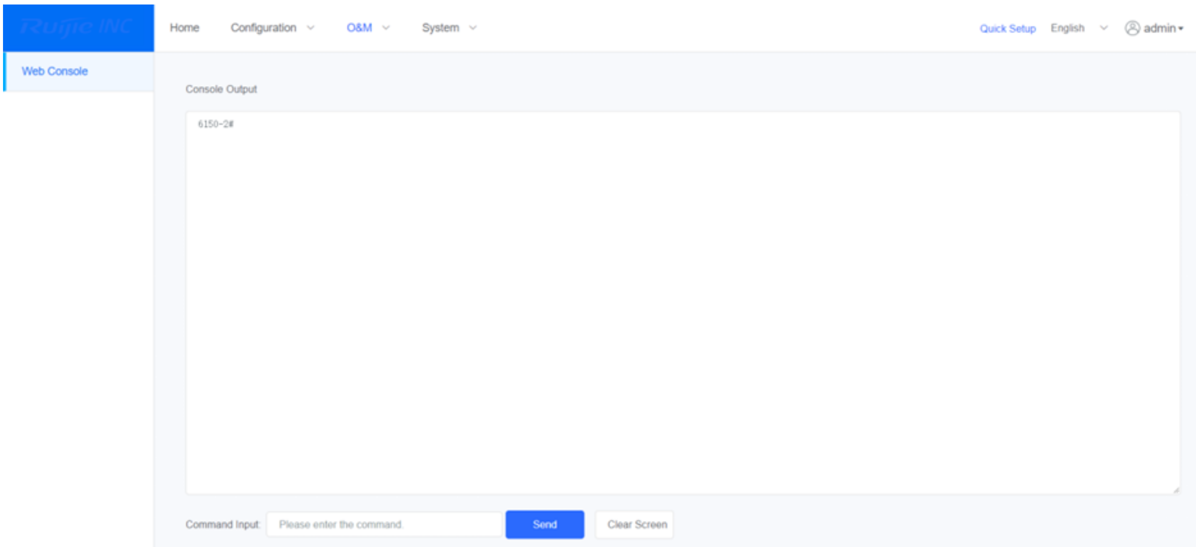


Note: Restoring factory settings will delete all running configurations. If there are useful configurations in the current system, you can first [Export Running Configurations] before restoring factory settings. 'Export Setup',
Please restore the factory settings.

Restore Factory Settings

8. Web Console

The web console simulates the connection of a client connection tool such as xshell, rt, mobaxterm to the controller of the switch.



```
6150-2#
```

Command Input: Please enter the command.

1. Enter a command in Command Input: Please enter the command. and click Send. The command execution result will be displayed in the console.

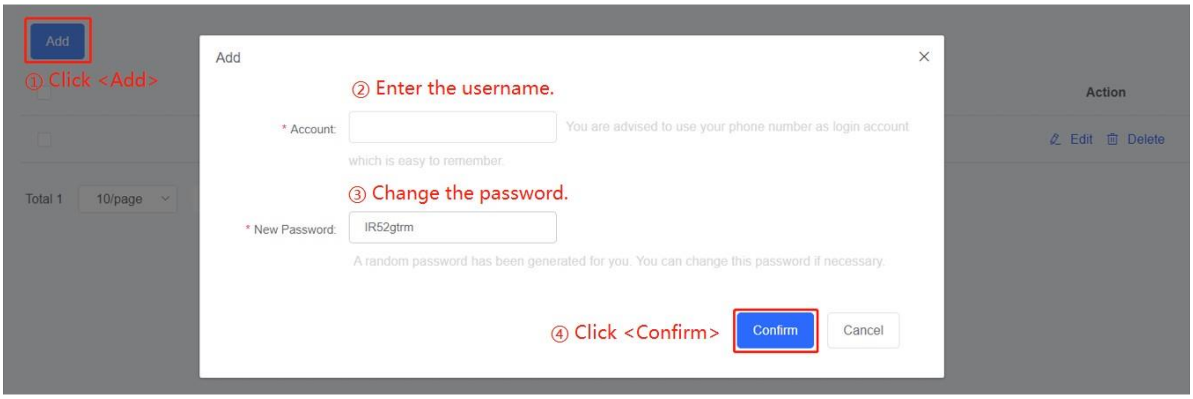
2. Click Clear Screen to clear the output result.

1.3.7 System

1. Admin Account

In addition to the admin account that comes with the eWeb management system, you can also create and maintain other accounts (only the network administrator has this privilege).

1. Adding an account



① Click <Add>

② Enter the username.

* Account: You are advised to use your phone number as login account which is easy to remember.

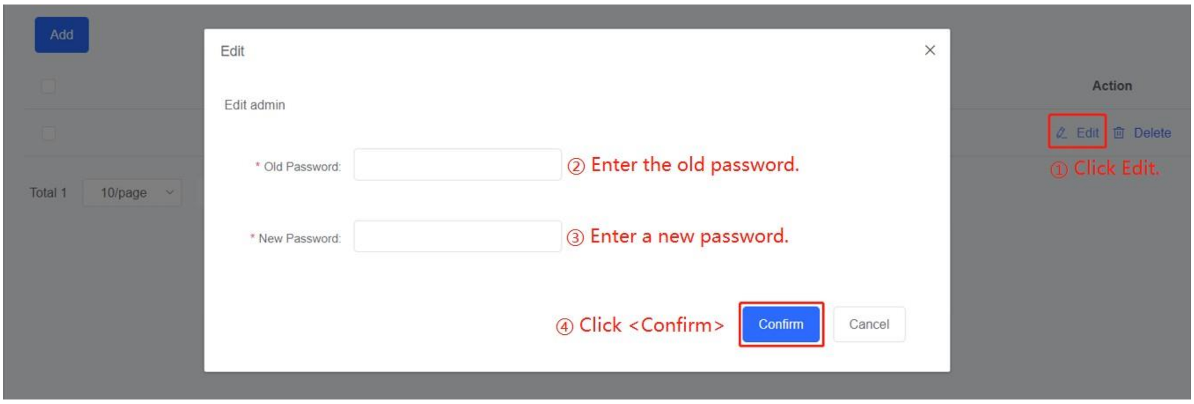
③ Change the password.

* New Password: IR52gtrm

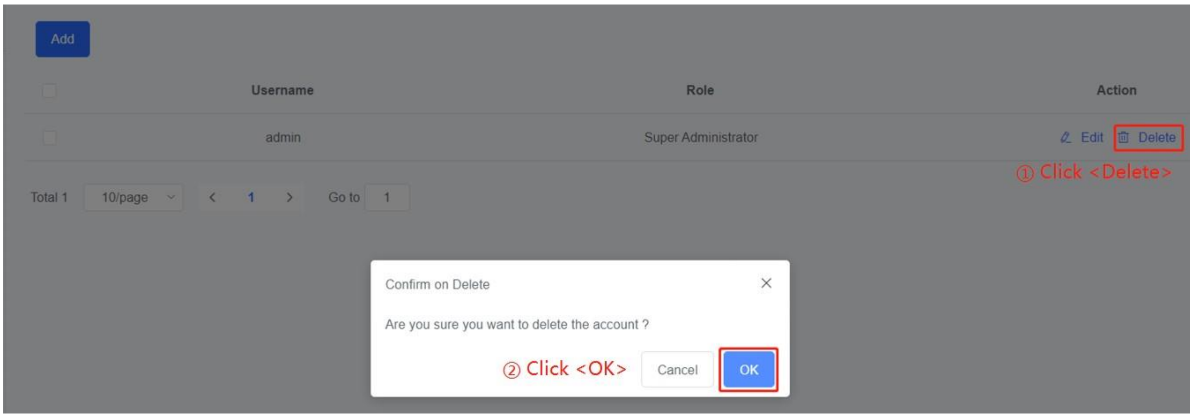
A random password has been generated for you. You can change this password if necessary.

④ Click <Confirm>

2. Changing the password



3. **Deleting an account** (the admin account cannot be deleted)



	Username	Role	Action
□	admin	Super Administrator	Edit Delete

Total 1 10/page < 1 > Go to 1

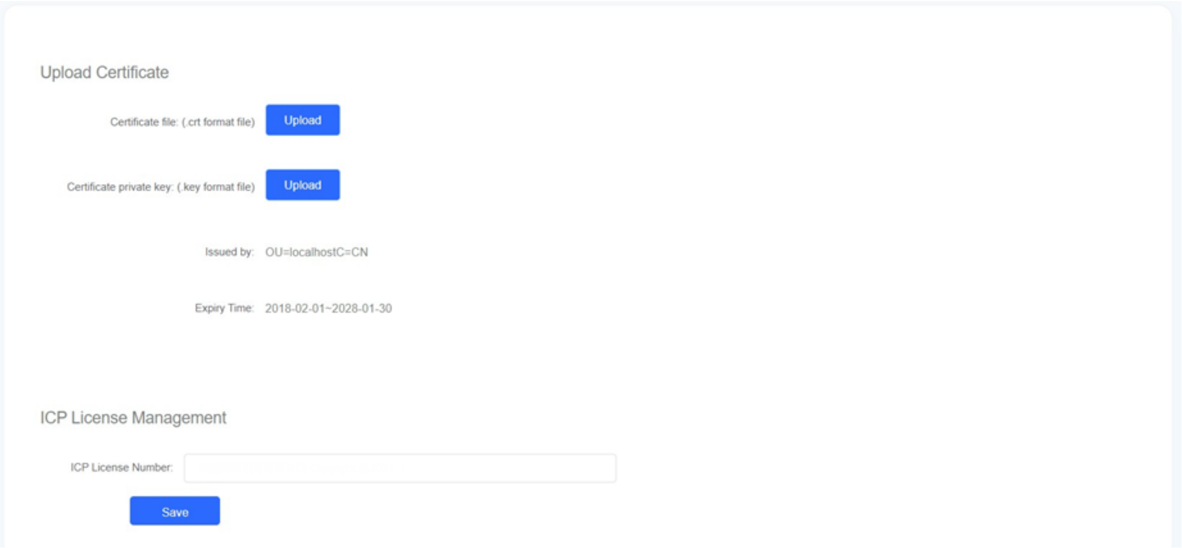
① Click <Delete>

Confirm on Delete

Are you sure you want to delete the account ?

② Click <OK>

2. Certificates and Registration



Upload Certificate

Certificate file: (.crt format file) Upload

Certificate private key: (.key format file) Upload

Issued by: OU=localhostC=CN

Expiry Time: 2018-02-01~2028-01-30

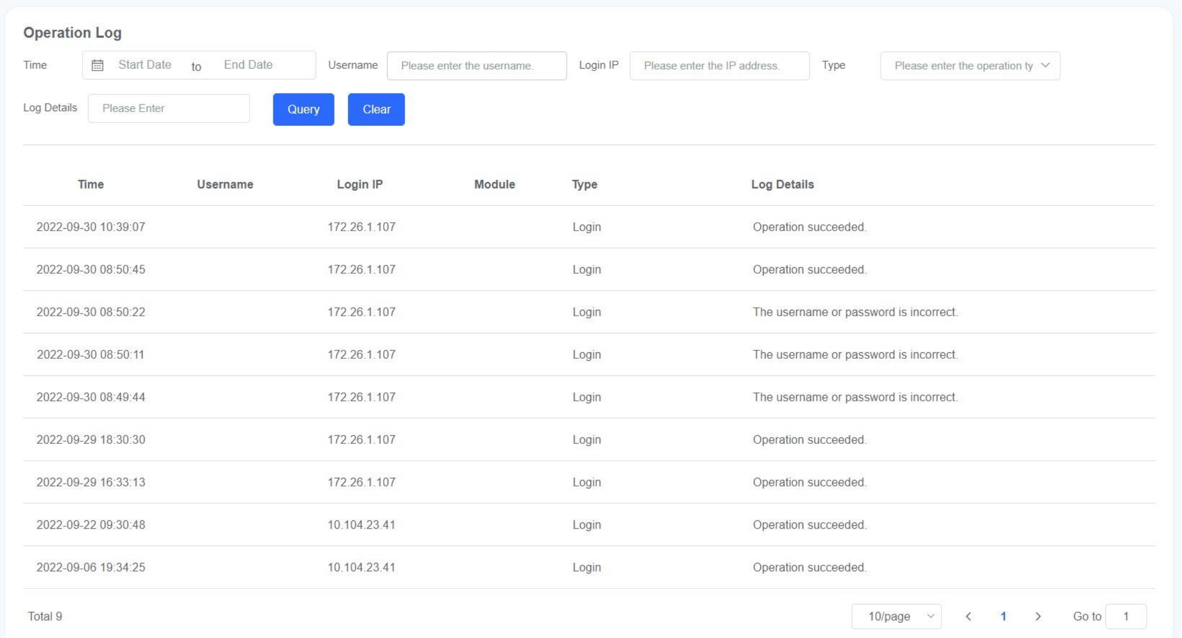
ICP License Management

ICP License Number:

Save

3. Operation Log

The operation log records users' key operations. You can query the operation log based on the search criteria.



Operation Log

Time: Start Date to End Date Username: Please enter the username. Login IP: Please enter the IP address. Type: Please enter the operation ty

Log Details: Please Enter

Time	Username	Login IP	Module	Type	Log Details
2022-09-30 10:39:07		172.26.1.107		Login	Operation succeeded.
2022-09-30 08:50:45		172.26.1.107		Login	Operation succeeded.
2022-09-30 08:50:22		172.26.1.107		Login	The username or password is incorrect.
2022-09-30 08:50:11		172.26.1.107		Login	The username or password is incorrect.
2022-09-30 08:49:44		172.26.1.107		Login	The username or password is incorrect.
2022-09-29 18:30:30		172.26.1.107		Login	Operation succeeded.
2022-09-29 16:33:13		172.26.1.107		Login	Operation succeeded.
2022-09-22 09:30:48		10.104.23.41		Login	Operation succeeded.
2022-09-06 19:34:25		10.104.23.41		Login	Operation succeeded.

Total 9 10/page < 1 > Go to 1