3onedata



ICS5400TSN-24GT16GS4XS Series Layer 3 Industrial Ethernet Switch

User Manual

Document Version: 01

Issue Date: 01/11/2023

Copyright © 2023 3onedata Co., Ltd. All rights reserved.

No company or individual is allowed to duplicate or transmit this manual in any forms without written permission issued by 3onedata Co., Ltd.

Trademark statement

3onedata, 3onedata and 3One data are the registered trademark owned by 3onedata Co., Ltd. And other trademarks mentioned in this manual belong to their corresponding companies.

Note

Purchased product, service or features should be constrained by 3onedata commercial contracts and clauses. The whole or part product, service or features described in this document may beyond purchasing or using range. 3onedata won't make any statement or warranty for this document content unless any other appointment exists.

Due to product version upgrading or other reason, this document content will be upgraded periodically. Unless other appointment exists, this document only for usage guide, all statement, information and suggestion in this document won't constitute any warranty.

3onedata



3onedata Co., Ltd.

Headquarter address:	3/B, Zone 1, Baiwangxin High Technology Industrial park, Nanshan District, Shenzhen, 518108 China
Technology support:	support@3onedata.com
Service hotline:	+86-400-880-4496
E-mail:	sales@3onedata.com
Fax:	+86 0755-2670-3485
Website:	http://www.3onedata.com

Preface

This Switch User Manual has introduced:

- Product features
- Product network management configuration
- Overview of related principles of network management


Note

The reference model for the screenshot in this manual is 16 Gigabit SFP + 24 Gigabit copper ports + 4 10Gigabit SFP+. In addition to the differences in the supported power supply number and port type, the interface functions and operation of other models in this series are similar.

Audience

This manual applies to the following engineers:

- Network administrators
- Technical support engineers
- Network engineer

Port Convention

The port number in this manual is only an example, and does not represent the actual port with this number on the device. In actual use, the port number existing on the device shall prevail.

Text Format Convention

Format	Description
" "	Words with “” represent the interface words. Such as: “Port No.”.
>	Multi-level path is separated by ">". Such as opening the local

3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.

Format	Description
	connection path description: Open "Control Panel> Network Connection> Local Area Connection".
Light Blue Font	It represents the words clicked to achieve hyperlink. The font color is as follows: 'Light Blue'.
About this chapter	The section 'about this chapter' provide links to various sections of this chapter, as well as links to the Principles Operations Section of this chapter.

Symbols

Format	Description
 Notice	Remind the announcements in the operation, improper operation may result in data loss or equipment damage.
 Warning	Pay attention to the notes on the mark, improper operation may cause personal injury.
 Note	Make a necessary supplementary instruction for operation description.
 Key	Configuration, operation, or tips for device usage.
 Tips	Pay attention to the operation or information to ensure success device configuration or normal working.

Button Operation Convention

Format	Description
	There is a logout button in the upper right corner of the webpage. After clicking it, the webpage returns to the login page.
	There is a port button in the upper right corner of the webpage. Click or press F2 to view the port status, and press F2 or Esc to close the port status page.
	There is a restart button in the upper right corner of the webpage. After clicking, a restart confirmation box pops up. After confirmation, the device will restart.
	There is a Save button in the upper right corner of the webpage. Click it to save the current device configuration. After setting the device, the save icon will flash to remind the

3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.

Format	Description
	user to save the configuration, so as to avoid losing unsaved configuration information due to restart and other operations.
Add	Click the Add button to add a line of configuration. Note that repeated configuration may result in data overwrite.
Delete	Check the line to be deleted, and then click the Delete button to delete the configuration.
Config	Check the line to be configured, and then click the configure button to enter the configuration page.
	Click the function status button to switch the function status,  means on and  means off.
Apply	Click the Set button to submit the current configuration.
Clear	Click the “Clear” button to clear the information of current page.
Refresh	Click the Refresh button to refresh the information of current page.

Revision Record

Version No.	Date	Revision note
01	01/11/2023	Product release

Copyright © 3onedata Co., Ltd.

Contents

PREFACE 1
CONTENTS I
1 LOG IN THE WEB INTERFACE 1
1.1 SYSTEM REQUIREMENTS FOR WEB BROWSING 1
1.2 SETTING IP ADDRESS OF PC 1
1.3 LOG IN THE WEB CONFIGURATION INTERFACE 2
2 SYSTEM INFORMATION 4
3 LOGIN CONFIGURATION 6
3.1 IP ADDRESS 6
3.1.1 IPv4 6
3.1.2 IPv6 7
3.2 USERS 8
3.3 PROTOCOL AUTHORIZATION 9
4 PORT CONFIGURATION 11
4.1 PORT SETTINGS 11
4.2 LINK AGGREGATION 13
4.2.1 Link Aggregation 13
4.2.2 Aggregation protection 16
4.3 PORT RATE LIMIT 17
4.4 STORM SUPPRESSION 19
4.5 PORT MIRRORING 21
4.6 PORT ISOLATION 22
4.7 PORT STATISTICS 23
4.7.1 Port Statistics-Overview 23
4.7.2 Port Statistics-Port 24
5 LAYER 2 CONFIGURATION 26
5.1 VLAN 26
5.1.1 VLAN Configuration 26
5.1.2 Access Configuration 27
5.1.3 Trunk Configuration 29
5.2 MAC 30
5.2.1 Global Configuration 31
5.2.2 Static MAC 32
5.2.3 Static Multicast MAC 33

3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.

5.2.4 MAC Information 33
5.3 SPANNING TREE 35
5.3.1 Global Configuration 35
5.3.2 Instance Configuration 37
5.3.3 Port Configuration 38
5.3.4 Instance Port Configuration 40
5.4 RING 42
5.5 MRP 47
5.6 ERPS 49
5.6.1 Timer Configuration 49
5.6.2 Ring Configuration 51
5.6.3 Instance Configuration 52
5.7 IGMP-SNOOPING 55
5.7.1 Global Configuration 55
5.7.2 Interface Configuration 56
5.7.3 Routing Port Configuration 57
5.7.4 Routing port information 58
5.8 IPV6 MLD-SNOOPING 59
5.8.1 Global Configuration 59
5.8.2 Interface Configuration 60
5.8.3 Routing Port Configuration 62
5.8.4 Routing port information 62
5.9 LINK FLAPPING PROTECTION 63
5.9.1 Global Configuration 64
5.9.2 Port Configuration 65
5.10 PORT LOOPBACK DETECTION 66
5.11 IPDT 68
5.12 IPV6DT 69
5.13 SMART-LINK 70
5.13.1 Global Configuration 70
5.13.2 Interface Configuration 72
6 IP NETWORK SETTING 74
6.1 INTERFACE 74
6.1.1 Layer 3 Interface 74
6.1.2 Loopback Interface 75
6.2 ARP 76
6.2.1 ARP Information 77
6.2.2 Static ARP 78
6.2.3 ARP Parameter Configuration 78
6.3 IPV4 79
6.3.1 IPv4 Routing Table 79
6.3.2 IPv4 Static Route 80
6.4 NAT 81

3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.

7 UNICAST ROUTING TABLE 84
7.1 RIP 84
7.1.1 Global Configuration 84
7.1.2 Network Configuration 87
7.1.3 Interface Configuration 87
7.2 RIPNG 88
7.2.1 Global Configuration 89
7.2.2 Interface Configuration 90
7.3 OSPF 91
7.3.1 Global Configuration 92
7.3.2 Network Configuration 93
7.3.3 Interface Configuration 94
7.4 OSPFV3 95
7.4.1 Global Configuration 96
7.4.2 Interface Configuration 97
7.5 ISIS 98
7.5.1 Global Configuration 99
7.5.2 Interface Configuration 100
7.6 VRRP 102
7.7 IPv6 VRRP 103
8 MULTICAST ROUTING 106
8.1 MULTICAST ROUTING 106
8.1.1 Multicast Routing Switch 106
8.1.2 Multicast routing information 107
8.2 IPv6 MULTICAST ROUTING 108
8.2.1 Multicast Routing Switch 108
8.2.2 Multicast routing information 108
8.3 IGMP SNOOPING 109
8.3.1 Interface Configuration 109
8.3.2 SSM-Map configuration 111
8.3.3 Multicast Group Information 113
8.4 IPv6 MLD 114
8.4.1 Interface Configuration 114
8.4.2 SSM-Map configuration 115
8.4.3 Multicast Group Information 116
8.5 PIM-SM 117
8.5.1 Global Configuration 118
8.5.2 Static RP Configuration 120
8.5.3 C-RP Configuration of Interface 121
8.5.4 Interface Configuration 122
8.6 PIM-DM 123
8.7 IPv6-PIM-SM 125
8.7.1 Global Configuration 125

3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.

8.7.2 Static RP Configuration 126
8.7.3 C-RP Configuration of Interface 127
8.7.4 Interface Configuration 128
8.8 IPV6-PIM-DM 129
9 NETWORK MANAGEMENT 131
9.1 SNMP 131
9.1.1 SNMP Switch 131
9.1.2 View 132
9.1.3 Community 133
9.1.4 SNMP Group 134
9.1.5 V3 User 135
9.1.6 Trap Alarm 136
9.2 LLDP 137
9.2.1 Global Configuration 137
9.2.2 Port Configuration 138
9.2.3 Neighbor Information 140
9.3 DHCP-SERVER 141
9.3.1 DHCP Switch 141
9.3.2 DHCP Pool Configuration 142
9.3.3 MAC Binding 143
9.3.4 Port Binding 144
9.3.5 Client List 144
9.4 DHCP-RELAY 145
10 TSN MANAGEMENT 147
10.1 PTP 147
10.1.1 Clock Configuration 148
10.1.2 Port Configuration 150
10.2 QBV 152
10.2.1 Global Configuration 152
10.2.2 Port Configuration 153
10.2.3 GCL 155
10.2.4 MAX SDU 157
10.3 QBU 158
10.4 STREAM 160
10.5 CB 162
10.6 QCI 164
10.6.1 Flow Meter 164
10.6.2 Stream Gate 166
10.6.3 GCL 167
10.6.4 Stream Filter 168
11 SYSTEM MAINTENANCE 171
11.1 NETWORK DIAGNOSIS 171
11.1.1 Ping 171

Copyright © 3onedata Co., Ltd.

11.1.2 Traceroute 172
11.1.3 Network Cable Diagnosis 172
11.1.4 SFP Digital Diagnosis 174
11.2 TIME 175
11.2.1 NTP Configuration 175
11.2.2 Time Zone Configuration 176
11.3 ALARM 177
11.3.1 Port Alarm 177
11.3.2 Power Alarm 178
11.4 CONFIGURATION FILE MANAGEMENT 179
11.4.1 Current configuration 179
11.4.2 Configuration File Update 180
11.4.3 Restore Factory Settings 181
11.5 UPGRADE 182
11.6 LOG INFORMATION 183
11.6.1 Log Information 183
11.6.2 Syslog Server 185
12 FAQ 186
12.1 SIGN IN PROBLEMS 186
12.2 CONFIGURATION PROBLEM 186
12.3 INDICATOR PROBLEM 187
13 MAINTENANCE AND SERVICE 189
13.1 INTERNET SERVICE 189
13.2 SERVICE HOTLINE 189
13.3 PRODUCT REPAIR OR REPLACEMENT 189

3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.

1 Log in the Web Interface

1.1 System Requirements for WEB Browsing

Using this device, the system should meet the following conditions.

Hardware and Software	System requirements
CPU	Above Pentium 586
Memory	Above 128MB
Resolution	Above 1024x768
Color	256 color or above
Browser	Internet Explorer 9.0 or above
Operating system	Windows 7/8/10 or above

1.2 Setting IP Address of PC

The default management IP address of the device as follows:

IP Settings	Default Value
IP Address	192.168.1.254
Subnet mask	255.255.255.0

When configuring a device through the Web:

- Before conducting remote configuration, please confirm the route between computer and device is reachable.
- Before making a local configuration, make sure that the IP address of the computer and the serial server are on the same subnet.

Note:

3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.

While configuring the device for the first time, if it's the local configuration mode, first confirm the network segment of current PC is 1.

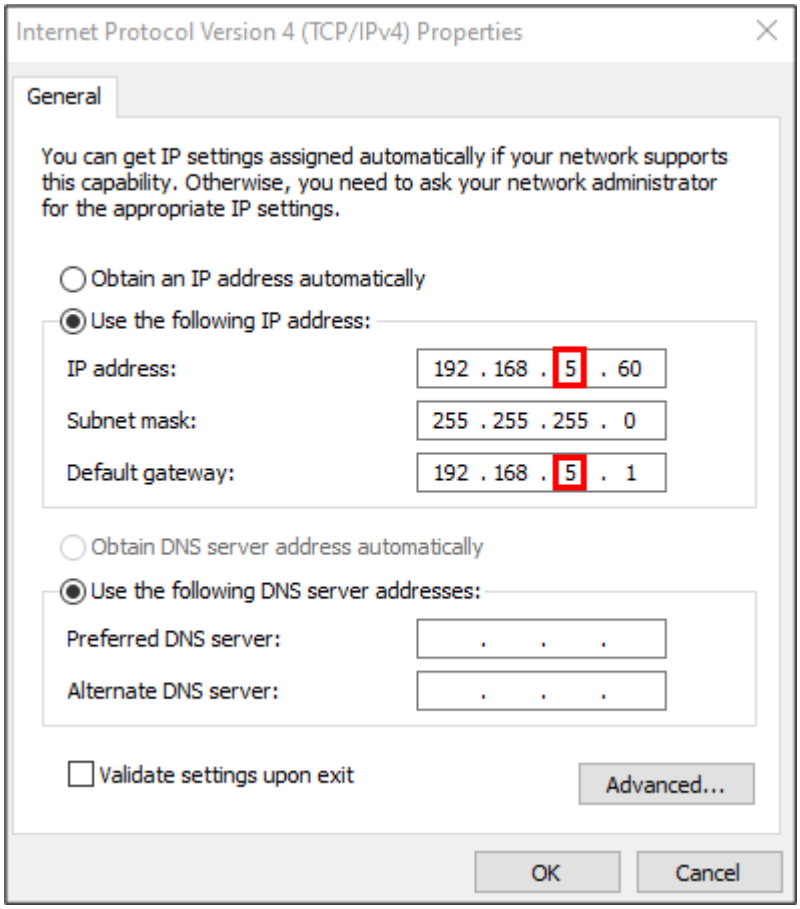
Eg: Assume that the IP address of the current PC is 192.168.5.60, change the network segment "5" of the IP address to "1".

Operation Steps

Amendment steps as follow:

Step 1 Open "Control Panel> Network Connection> Local Area Connection> Properties> Internet Protocol Version 4 (TCP / IPv4)> Properties".

Step 2 Change the selected "5" in red frame of the picture below to "1".



Step 3 Click “OK”, IP address is modified successfully.

Step 4 End.

1.3 Log in the Web Configuration Interface

Operation Steps

Login in the web configuration interface as follow:

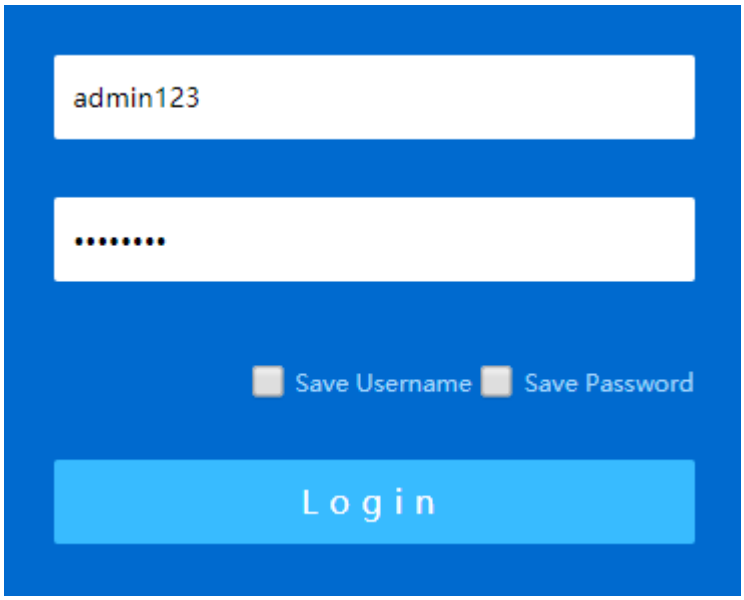
Step 1 Run the computer browser.

Copyright © 3onedata Co., Ltd.

Step 2 Enter the address of the device "http://192.168.1.254" in the address bar of the browser.

Step 3 Click the “Enter” key.

Step 4 Pop-up dialog box as shown below, enter the user name and password in the login window.



Note:

- The default username and password are “admin123”; please strictly distinguish capital and small letter while entering.
- Default user account has the administrator privileges.
- When the user has not operated the Web network management configuration page for a long time, the system will log out and return to the Web login page after timeout; By default, the timeout of Web page login is 15 minutes.
- When the number of consecutive password login errors of a user reaches the limit (default is 5 times), the user will be restricted from logging in for the following time (default is 10 minutes).

Step 5 Click "Login".

Step 6 End.

After login in successfully, user can configure relative parameters and information according to demands.

3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.

2 System Information

Function Description

View port status such as port type and connection status.

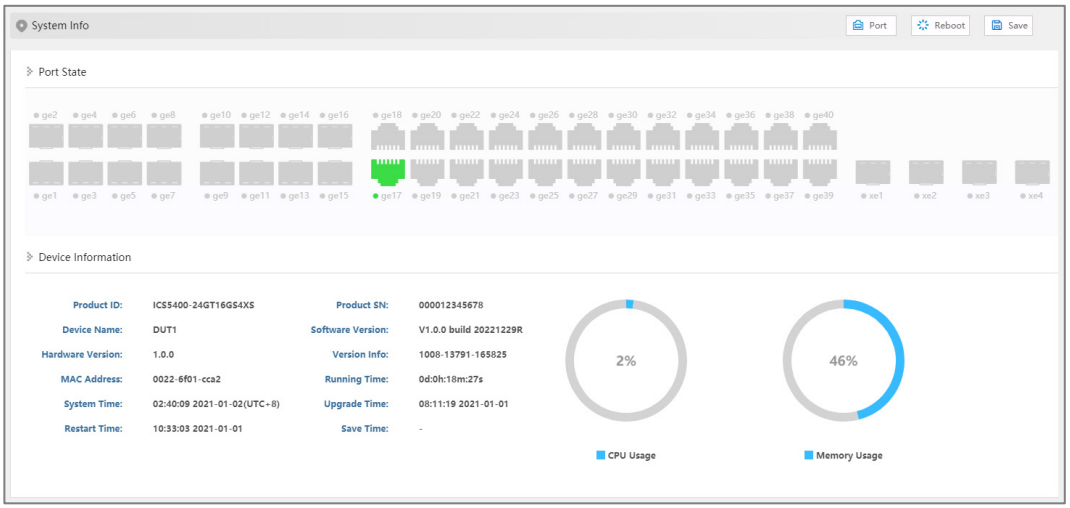
Check device information such as product model, software and hardware version, etc.

Operation Path

Open in the navigation bar: “System Information”.

Interface Description

System information interface as follows:



The main element configuration description of state information interface:

Interface Element	Description
Port state	Display port icon and port connection status of the device: •  Copper port icon, highlighting indicates that the port is connected.

3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.

Interface Element	Description
	• Copper port icon, grayed out indicates that the port is not connected or disabled. •  Fiber port icon, highlighting indicates that the port is connected. • Fiber port icon, grayed out indicates that the port is not connected or disabled.
Device information	Basic information of software, hardware and operation of the device. • Product ID • Device Name • Hardware Version • MAC Address • System Time • Restart Time • Product SN • Software Version • Version Information • Uptime • Upgrade Time • Save Time • CPU Usage • Memory Usage

3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.

3 Login Configuration

3.1 IP Address

3.1.1 IPv4

Function Description

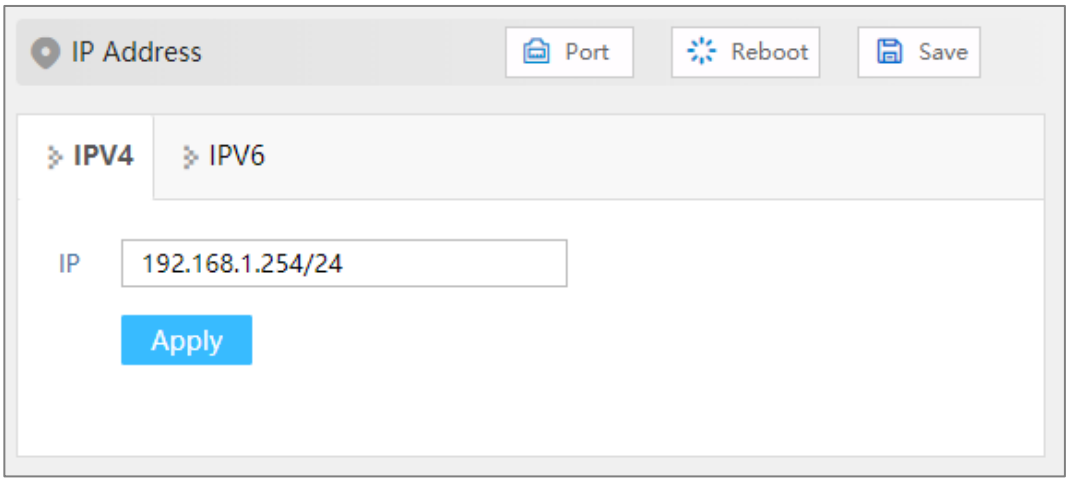
Configure the IPv4 address of the vlanif1 interface.

Operation Path

Open in order: "Login Configuration > IP Address > IPV4".

Interface Description

The IPV4 interface is as follows:



Main elements configuration descriptions of IPV4 interface:

Interface Element	Description
IP	The IPv4 address and subnet mask of the vlanif1 interface of the device. The default IP is 192.168.1.254/24.

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	Note: After modifying the IP of the device, re-enter the corresponding IP address to access the WEB interface.

3.1.2 IPv6

Function Description

Add or delete IPv6 address of vlanif1 interface.

An IPv6 address is 128 bits long and is written as eight groups of four hexadecimal digits (base 16 digits represented by the numbers 0-9 and the letters A-F). Each group is separated by a colon (:). For the convenience of writing, IPv6 also provides a compression format. The specific compression rules are:

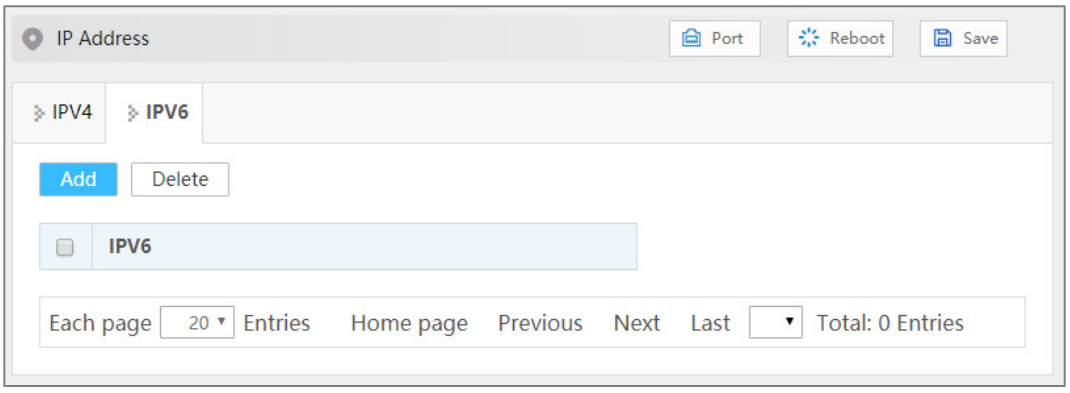
- The leading "0" in each group can be omitted.
- The address contains two or more consecutive groups of 0s, which can be replaced by double colons "::".

Operation Path

Open in order: "Login Configuration > IP Address > IPV6".

Interface Description

The IPV6 interface is as follows:



Main elements configuration descriptions of IPV6 interface:

Interface Element	Description
IPV6	IPv6 address and prefix length of vlanif1 interface of device.

Copyright © 3onedata Co., Ltd.

3.2 Users

Function Description

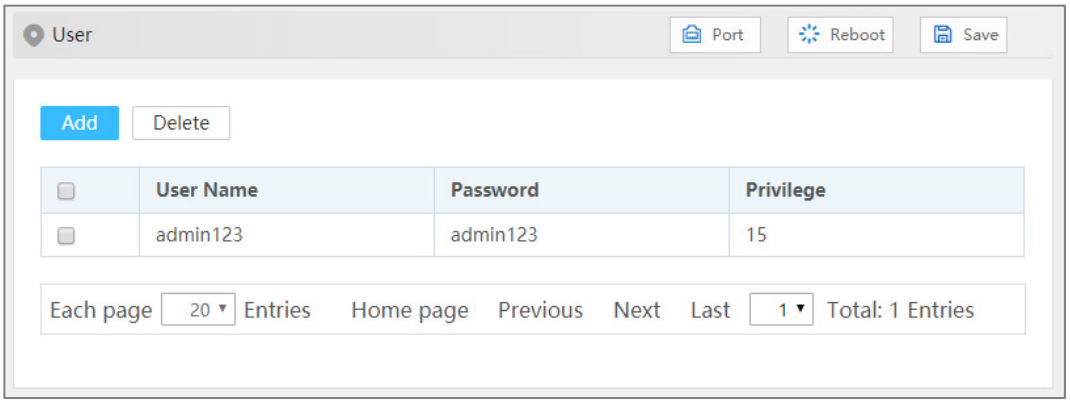
To add and delete user, user needs to enter username and password to access the device, the initial username and password are: admin123.

Operation Path

Open in order: "Login Configuration > User".

Interface Description

User interface as follows:



The main element configuration description of user interface:

Interface Element	Description
Username	Identification of the visitor. Note: • User name supports 1-16 valid characters, consisting of uppercase letters, lowercase letters, numbers or special characters (! @ _-). • User name does not support sensitive characters such as root, daemon, bin, sys, sync, mail, proxy, www-data, backup, operator, haldaemon, dbus, ftp, nobody, sshd, default, etc.
Password	Password used by the visitor. Note: • Password supports 8-16 valid characters, consisting of combination of two or more of uppercase letters, lowercase letters, numbers, special characters (~! @ # $% _-.). • The password is valid for 90 days by default, and the password needs to be revised after it expires.
Privilege	The visitor's privilege is 0-15, and it supports 16 priorities in 4 categories.

Interface Element	Description
	• 0: visit level; You can only view the system information, IP address and log information of the device, and conduct network diagnosis (Ping, Traceroute). • 1: view level; The configuration information of the device can be viewed, but the configuration of the device cannot be modified. • 2: configuration level; User can view the configuration information of the device and configure some functional parameters of the device, but cannot manage the device. • 3-15: manage level, user has all privileges of the device, including downloading, uploading, rebooting, modifying device information and other other operations. Notice: • Users can view, delete, or add other users whose priority does not exceed their own. • If the added user name already exists, the original user information will be overwritten.

3.3 Protocol Authorization

Function Description

Configure device TELNET service and SSH service.

The CLI interface of the device can be accessed through TELNET protocol and SSH2.0 protocol. TELNET transmission process uses TCP protocol for plaintext transmission, and SSH (Secure Shell) protocol provides secure remote login, ensuring the safe transmission of data.

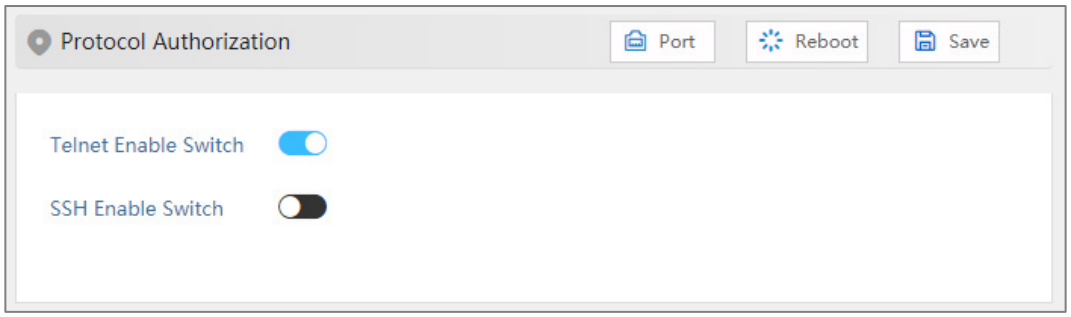
Operation Path

Open in order: "Login Configuration > Protocol Authorization".

Interface Description

Protocol authorization interface is as below:

Copyright © 3onedata Co., Ltd.



Configuration description of main elements of the protocol authorization interface:

Interface Element	Description
Telnet enable	TELNET service enable switch button, which is enabled by default.
SSH enable	SSH service enable switch button, which is disabled by default.

4 Port Configuration

4.1 Port Settings

Function Description

Set port parameters individually or in batches.

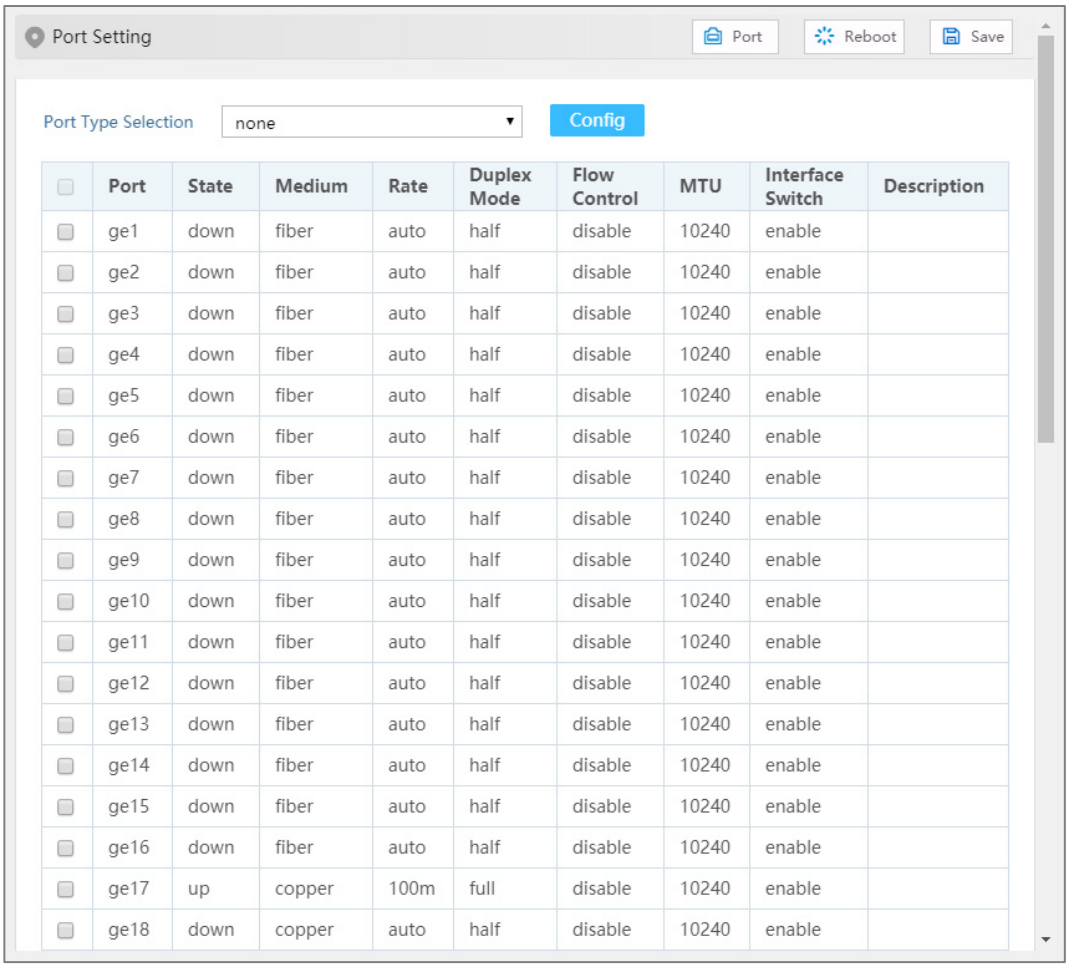
Operation Path

Open in order: "Port Configuration > Port Setting".

Interface Description

Port setting interface as follows:

3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.



Port	State	Medium	Rate	Duplex Mode	Flow Control	MTU	Interface Switch	Description
ge1	down	fiber	auto	half	disable	10240	enable	
ge2	down	fiber	auto	half	disable	10240	enable	
ge3	down	fiber	auto	half	disable	10240	enable	
ge4	down	fiber	auto	half	disable	10240	enable	
ge5	down	fiber	auto	half	disable	10240	enable	
ge6	down	fiber	auto	half	disable	10240	enable	
ge7	down	fiber	auto	half	disable	10240	enable	
ge8	down	fiber	auto	half	disable	10240	enable	
ge9	down	fiber	auto	half	disable	10240	enable	
ge10	down	fiber	auto	half	disable	10240	enable	
ge11	down	fiber	auto	half	disable	10240	enable	
ge12	down	fiber	auto	half	disable	10240	enable	
ge13	down	fiber	auto	half	disable	10240	enable	
ge14	down	fiber	auto	half	disable	10240	enable	
ge15	down	fiber	auto	half	disable	10240	enable	
ge16	down	fiber	auto	half	disable	10240	enable	
ge17	up	copper	100m	full	disable	10240	enable	
ge18	down	copper	auto	half	disable	10240	enable	

Main elements configuration description of port settings interface:

Interface Element	Description
Port type selection	Select ports of the same type in batches for configuration, and the options are as follows: • none • fe:100M port • ge: Gigabit port • xe: 10Gigabit port • sa: static aggregation group • po: dynamic aggregation group Note: The port type is based on the actual port of the device.
Port	The corresponding port name of the device Ethernet port.
State	Ethernet port connection status, display status as follows: • down: represent the port is disconnected; • up: represent the port is connected.
Medium	The connection types of Ethernet ports, the status are shown

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	as follows: • fiber: fiber port medium. • copper: copper port medium.
Rate	The default is self-adaption mode, and the display status is as follows: • auto: self-adaption; • 10m: 10M; • 100m: 100M; • 1g: Gigabit. • 2500m：2.5G • 10g: 10 Gigabit.
Duplex Mode	The default is self-adaption mode, and the display status is as follows: • auto: self-adaption; • half: half-duplex • full: full duplex
Flow Control	Port flow control status, the display status is as follows: • disable • Both: Enable port data sending or receiving flow control.
Max-Frame	Ethernet port transmitted maximum data frame length, the value range is 64-10240.
Interface Switch	Enable or disable Ethernet port. Options are as follows: • enable • disable
Description	Port description information, which supports 0-32 characters and consists of uppercase letters, lowercase letters, numbers or special characters (! @ _-).

4.2 Link Aggregation

4.2.1 Link Aggregation

Function Description

Link aggregation is the shorter form of Ethernet link aggregation; it binds multiple Ethernet physical links into a logical link, achieving the purpose of increasing the link

Copyright © 3onedata Co., Ltd.

bandwidth. At the same time, these bundled links can effectively improve the link reliability by mutual dynamic backup.

The Link Aggregation Control Protocol (LACP) protocol based on the IEEE802.3ad standard is a protocol for implementing dynamic link aggregation. Devices running this protocol exchange LACPDU (Link Aggregation Control Protocol Data Unit, Link Aggregation Control Protocol Data Unit) to exchange link aggregation related information.

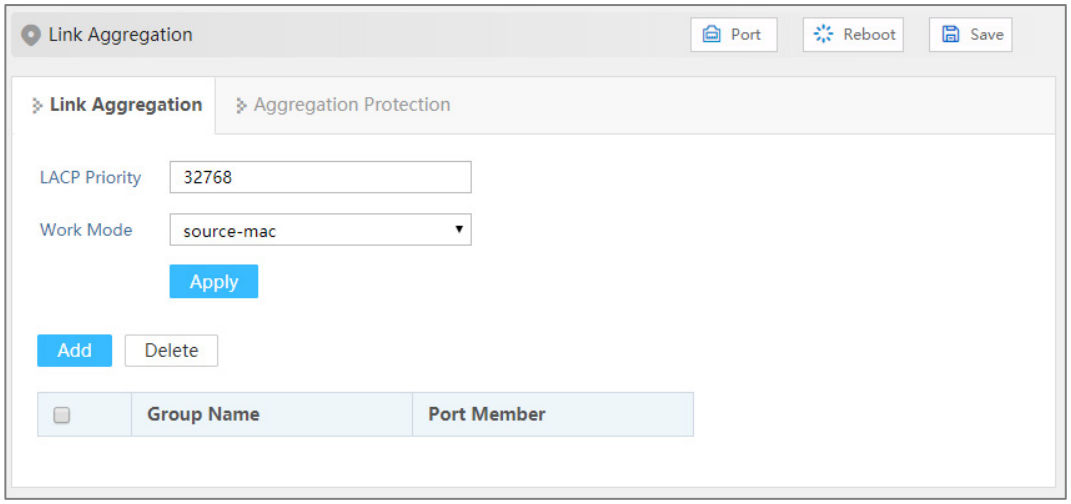
Based on the enabling or disabling of LACP protocol, the link aggregation can be divided into two modes, static aggregation and dynamic aggregation.

Operation Path

Open in order: "Port Configuration > Link Aggregation > Link Aggregation".

Interface Description

Link Aggregation interface as below:



The main element configuration description of Link Aggregation interface:

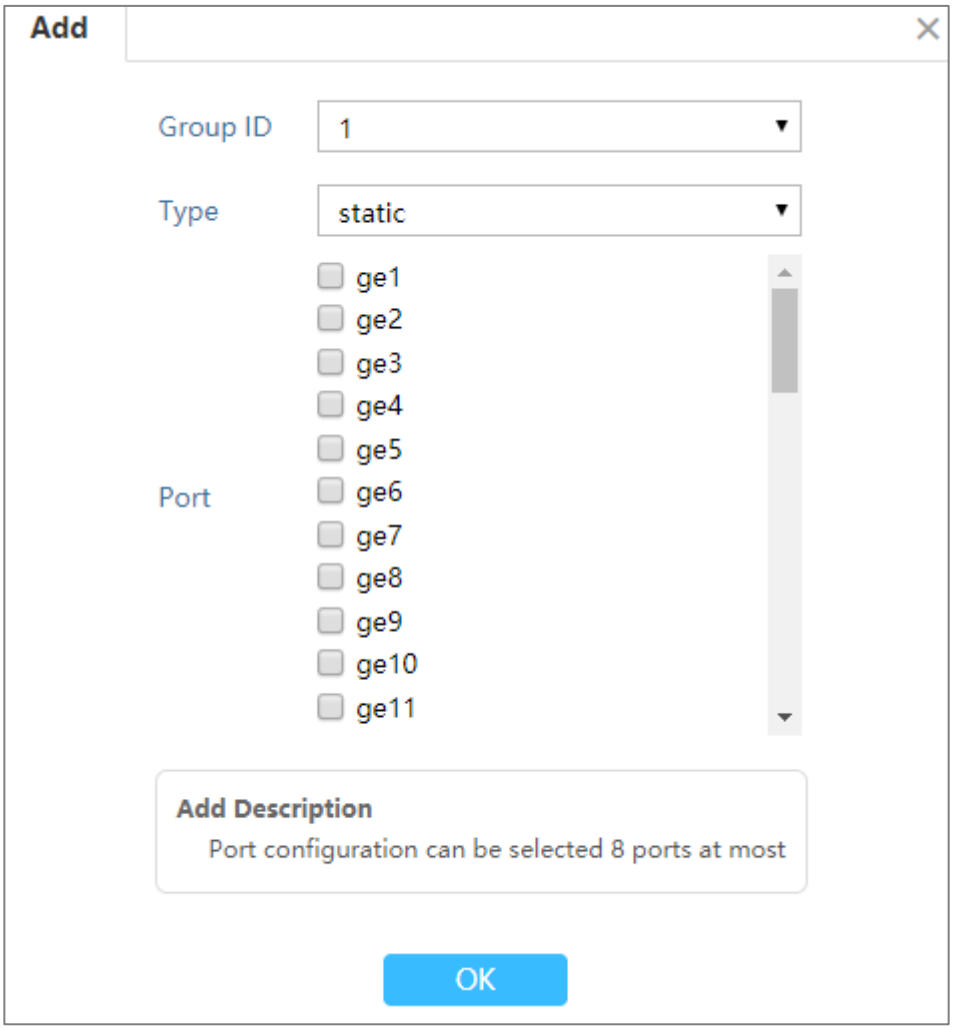
Interface Element	Description
LACP Priority	Priority level setting of dynamic aggregation system, the setting range is 1-65535, defaults to 32768. Note: The lower the priority value of the system LACP is, the higher the priority is, and the activity interface of the device with high system priority is selected at both ends of the aggregation link.
Work Mode	Configure the load balancing mode of the aggregation group. The options are as follows: • source-mac: Load balance mode based on source MAC • destination-mac: Load balance mode based on destination MAC • source-dest-ip: Load balance mode based on source and

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	destination IP • source-dest-mac: Load balance mode based on source and destination MAC • source-dest-port: The load balancing mode is based on the source and destination TCP/UDP ports.
Group Name	Group type and ID, sa is a static aggregation group, po is a dynamic aggregation group, and the aggregation group ID supports up to 12 groups. Each group can configure up to 8 ports to join aggregation.
Port Member	Port member in the link aggregation group.

Interface Description: Add

The Link Aggregation-Add interface as follows:



The main elements configuration description of Link Aggregation-Add interface:

Copyright © 3onedata Co., Ltd.

Interface Element	Description
Group ID	The ID number of the aggregation group, which can support up to 12 groups.
Type	Type of aggregation group: • static: static aggregation • dynamic: dynamic aggregation
Aggregation Mode	Dynamic Aggregation Group Mode: • active: active mode, in which the port actively initiates the aggregation negotiation process. • passive: the mode in which the port passively receives the aggregate negotiation process. Note: Under dynamic type, display this configuration.
Port	Port members in this aggregation group. Each group can configure up to 8 ports to join the aggregation.

4.2.2 Aggregation protection

Function Description

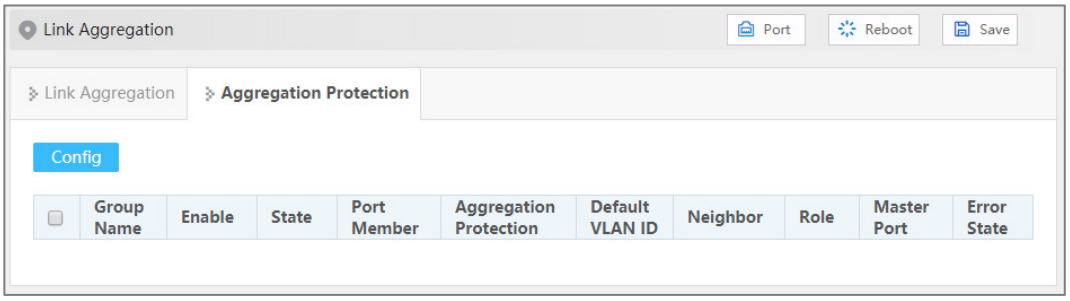
Configure static aggregation protection.

Operation Path

Open in order: "Port Configuration > Link Aggregation > Aggregation Protection".

Interface Description

The aggregation protection interface is shown as follows:



Description of configuration of main elements of aggregation protection interface:

Interface Element	Description
Group Name	The name of the static aggregation group set in Link Aggregation.
Enable	The enabled state of the aggregation group.

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	• Enable • Disable
State	Status of the aggregation group port. • Up: as long as any port member is Up, the status of the aggregation group is up; • Down: if all port members are Down, the status of the aggregation group is Down.
Port Member	Port member in the aggregation group.
Aggregation Protection	The enabled state of the aggregation protection. • Enable • Disable
Default VLAN ID	The VLAN where that aggregate group port reside.
Neighbor	MAC address of the opposite device of aggregation group. Note: If no device is connected to the opposite end, the MAC address is displayed as 0000.0000.0000.
Role	Elected roles in this device and the opposite device • Master: the one with a smaller MAC address is elected as Master • Slave: the one with a larger MAC address is elected as Slave
Master Port	The second link port of the master device is the master port.
Error State	Error message prompt of aggregation protection: • Neighbor timed out • Loop: forming a loop • Link error (such as generating a large number of error frames).

4.3 Port Rate Limit

Function Description

Limit the egress bandwidth and ingress bandwidth of the port.

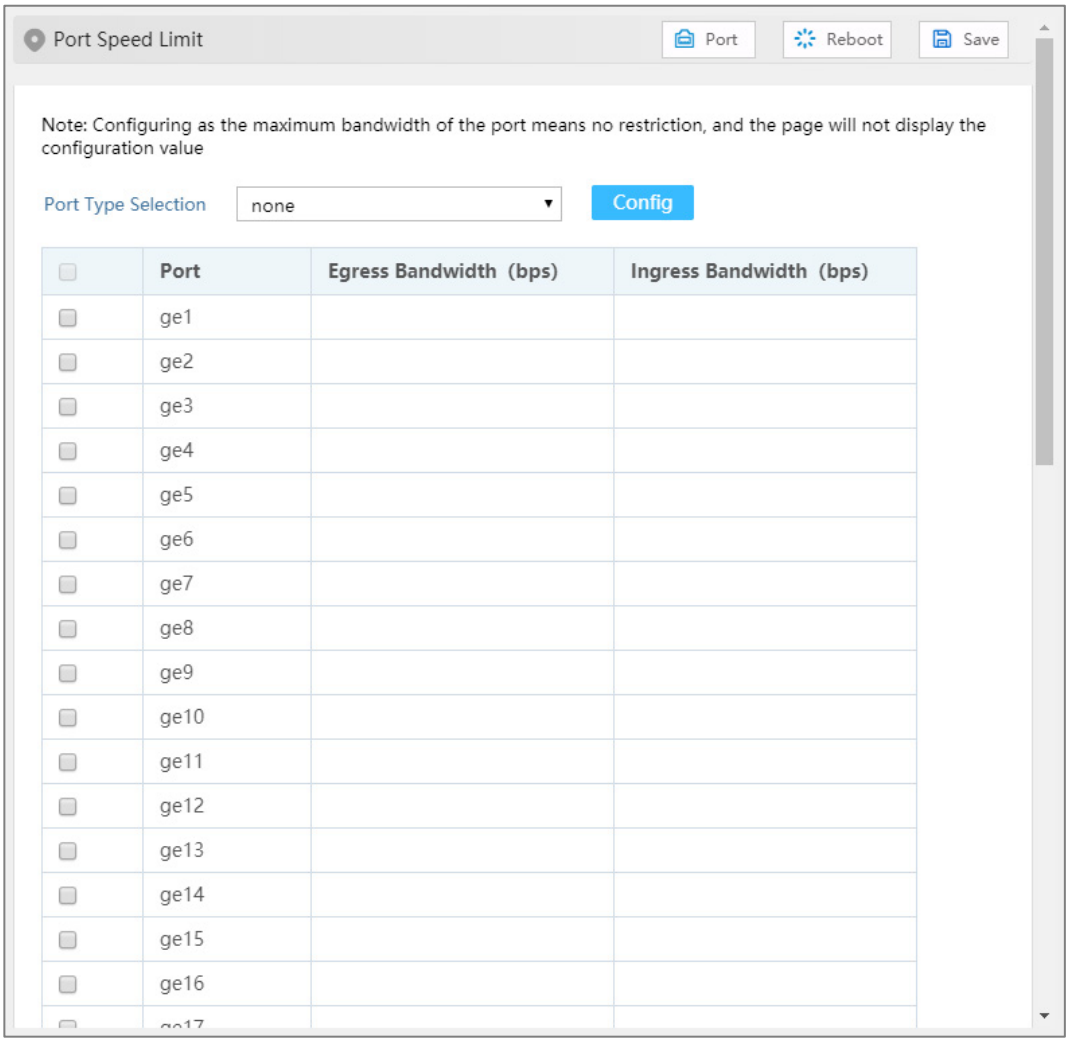
Operation Path

Open in order: "Port Configuration > Port RateLimit".

Interface Description

Port rate limit interface as follows:

Copyright © 3onedata Co., Ltd.



The main element configuration description of port rate limit interface:

Interface Element	Description
Port	The corresponding port name of the device Ethernet port.
Egress Bandwidth (bps)	The limitation of port on the bandwidth of egress data transmission.
Ingress Bandwidth (bps)	The limitation of port on the bandwidth of ingress data transmission. Note: Supports unit selection of K/M/G when configuring the bandwidth. In WEB display, unit conversion will be conducted and similar values will be taken according to the input value and the unit.

Note

- When using the port rate limit, flow control should be enabled, otherwise the rate between devices will no longer be a smooth curve;
- When using the port rate limit, packet loss should not occur unless the flow control is

Copyright © 3onedata Co., Ltd.

disabled. The representation of packet loss is the fluctuating transmission speed.

- Port speed limit has high requirements on network cable quality, otherwise lots of conflict packets and broken packet would appear.

4.4 Storm Suppression

Function Description

Configure the maximum broadcast, multicast or unknown unicast packet flow the port allows.

When the sum of each port broadcast, unknown multicast or unknown unicast flow achieves the value user sets, the system will discard the packets beyond the broadcast, unknown multicast or unknown unicast flow limit, so that the proportion of overall broadcast, unknown multicast or unknown unicast flow can be reduced to limited range, ensuring the normal operation of network business.

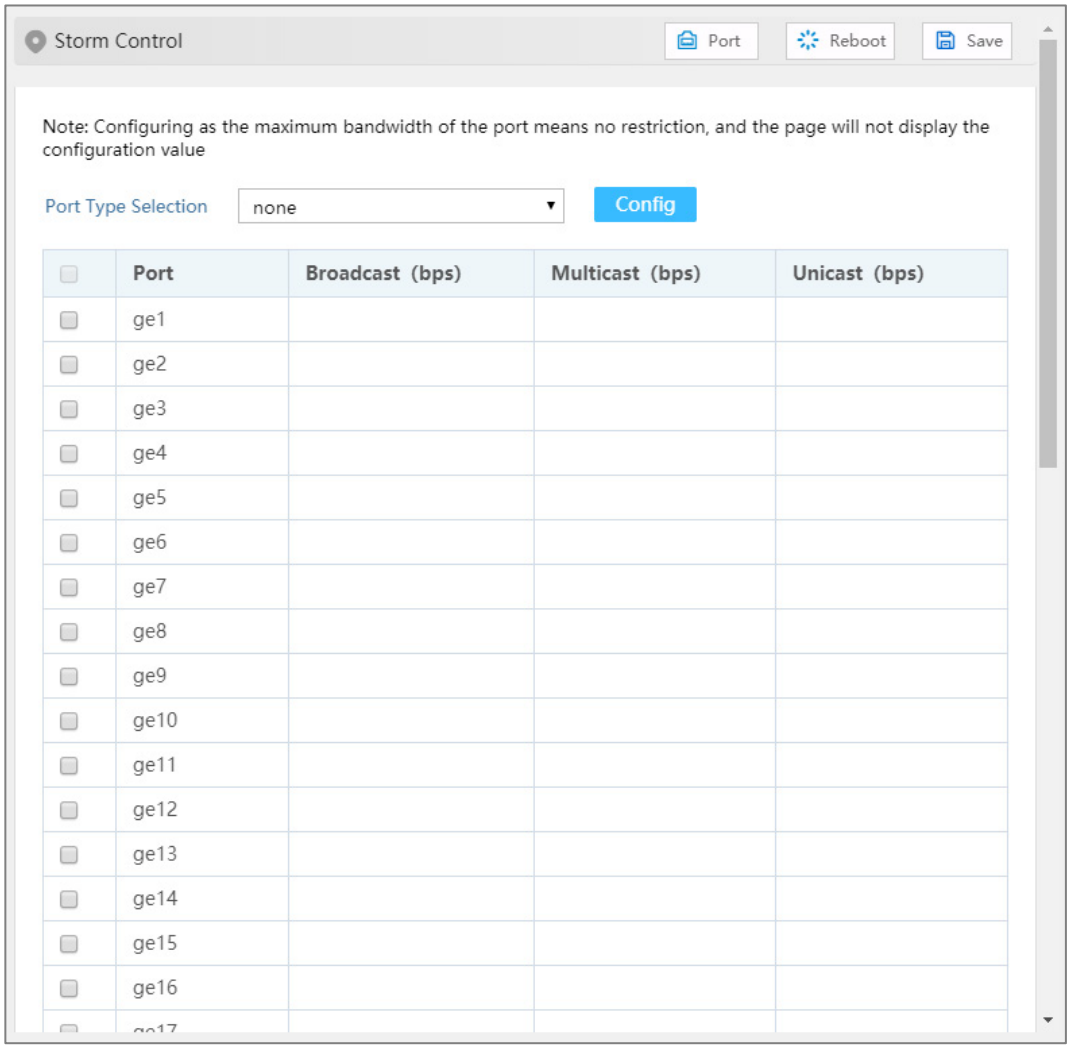
Operation Path

Open in order: "Port Configuration > Storm Suppression".

Interface Description

Storm control interface as follows:

3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.



Main elements configuration description of storm suppression interface:

Interface Element	Description
Port	The corresponding port name of the device Ethernet port.
Broadcast (bps)	The device procedure can suppress the transmission speed of broadcast packet Note: Broadcast packet, namely, the data frame with the destination address of FF-FF-FF-FF-FF-FF.
Multicast (bps)	Port suppression to the transmission speed of unknown multicast data packet. Note: Multicast packet, namely, the destination address is XX-XX-XX-XX-XX-XX data frame, the second X is odd number, such as: 1, 3, 5, 7, 9, B, D, F, other X represents arbitrary number.
Unicast (bps)	Port suppression to the transmission speed of unknown unicast data packet. Note:

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	Unknown unicast packet, namely, the MAC address of the data frame doesn't exist in the MAC address table of the device, which needs to be forwarded to all ports.

Note

Supports unit of K/M/G when click the "Config" button to configure the rate. In WEB display, unit conversion will be conducted and similar values will be taken according to the input value and the unit.

4.5 Port Mirroring

Function Description

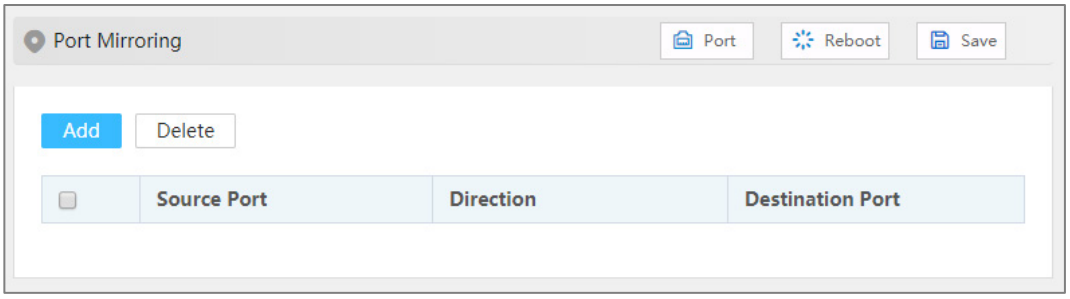
Copy the data from the origin port to appointed port for data analysis and monitoring.

Operation Path

Open in order: "Port Configuration > Port Mirroring".

Interface Description

Port mirror interface as follows:



The main element configuration description of port mirror interface:

Interface Element	Description
Source port	Data source port, which can be one or more, from which the device will collect data in the specified direction.
Direction	Data direction of the source port, options are as follows: • transmit: the message sent by the source port will be mirrored to the destination port. • receive: the packet received by the source port will be mirrored to the destination port. • both: the packet received or sent by the source port will be mirrored to the destination port.
Destination port	The destination port of device mirroring. The device only

3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.

Interface Element	Description
	supports one destination port.

Note

- The function must be shut down in normal usage, otherwise all senior management functions based on port are not available, such as RSTP, IGMP snooping etc.
- Mirror function only deals with FCS normal packet; it cannot handle the wrong data frame

4.6 Port Isolation

Function Description

Port isolation is used for the layer 2 isolation between messages. It could add different ports to different VLANs, but waste limited VLAN resources. Adopting isolate-port characteristics can achieve isolation of ports within the same VLAN. After adding the ports to isolation group, user can achieve the layer 2 data isolation of ports within isolation group. Port isolation function has provided safer and more flexible networking scheme for users.

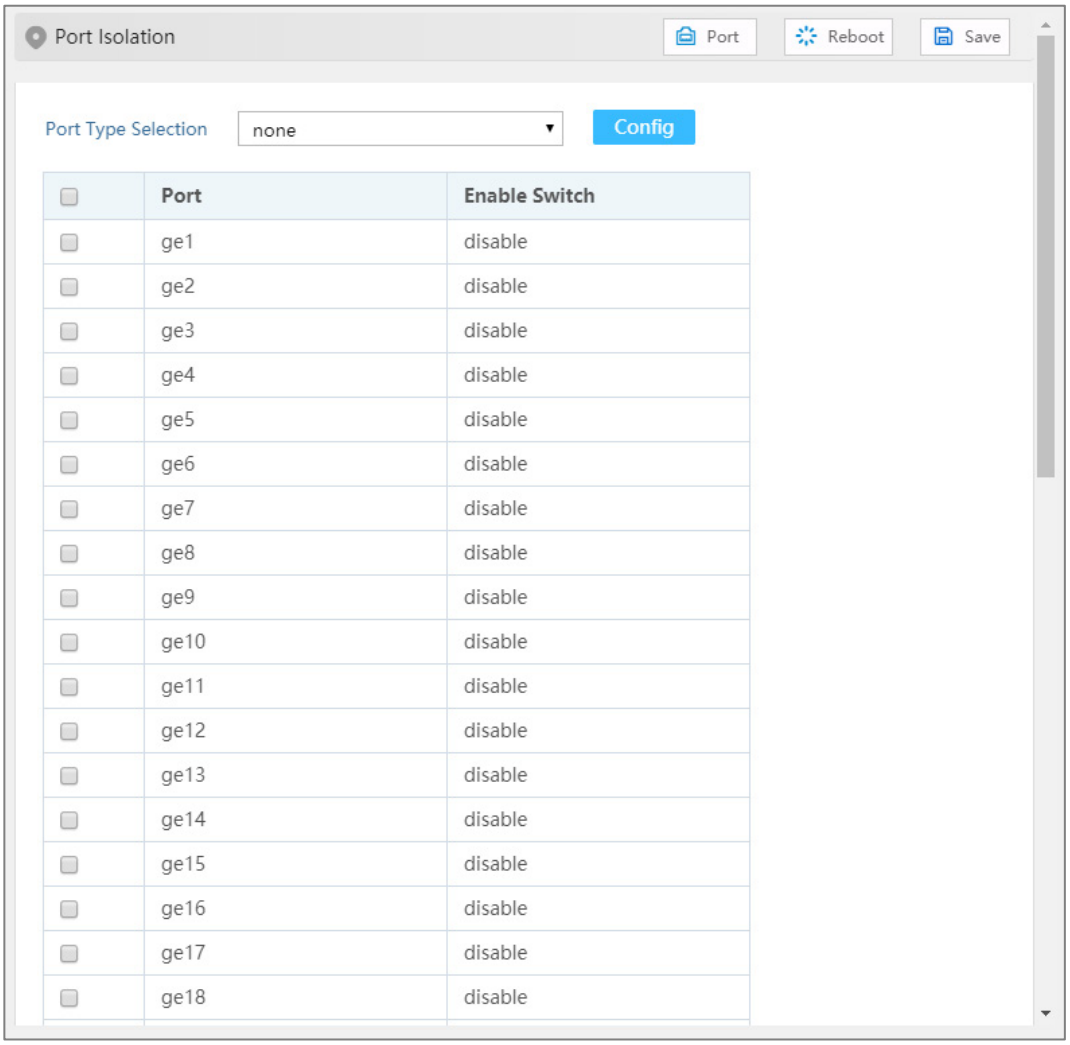
Operation Path

Open in order: "Port Configuration > Port Isolation".

Interface Description

Isolate-port configuration interface as follows:

3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.



The main element configuration description of isolate-port config interface:

Interface Element	Description
Port	The corresponding port name of the device Ethernet port.
Enable	Port isolation enable status can be displayed as follows: • disable • enable

4.7 Port Statistics

4.7.1 Port Statistics-Overview

Function Description

Check the number of messages and bytes, discarded messages and error messages sent and received by each port.

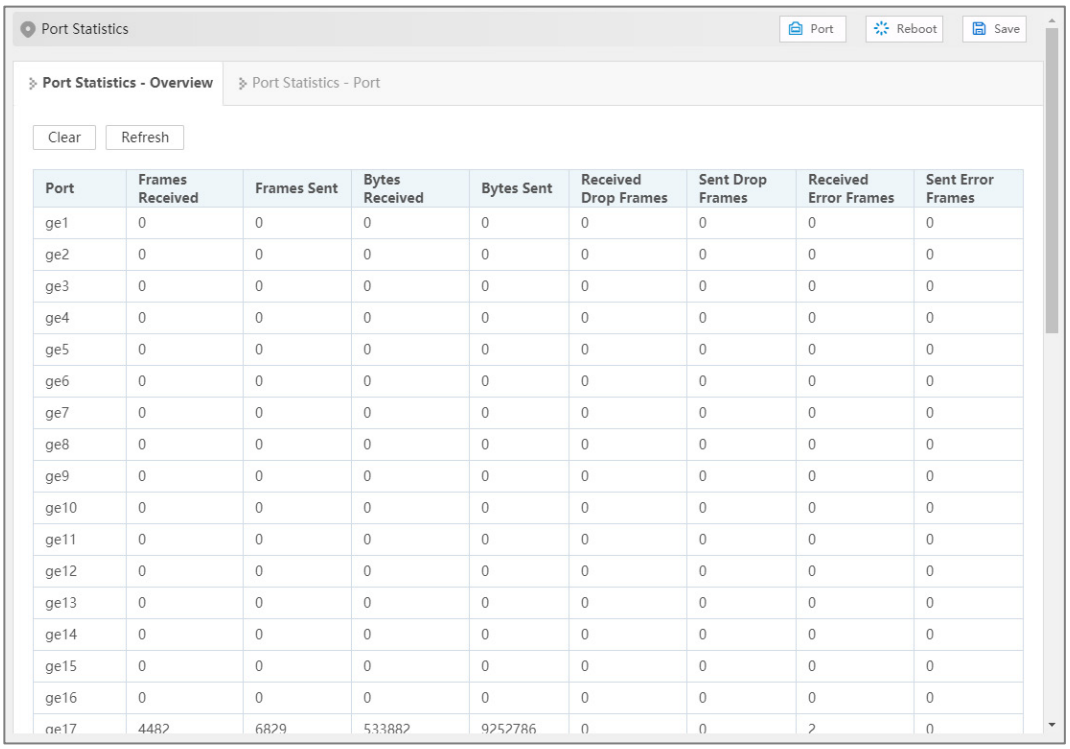
3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.

Operation Path

Open in order: "Port Configuration > Port statistics > Port Statistics-Overview".

Interface Description

Port Statistics-Overview interface as follows:



Port	Frames Received	Frames Sent	Bytes Received	Bytes Sent	Received Drop Frames	Sent Drop Frames	Received Error Frames	Sent Error Frames
ge1	0	0	0	0	0	0	0	0
ge2	0	0	0	0	0	0	0	0
ge3	0	0	0	0	0	0	0	0
ge4	0	0	0	0	0	0	0	0
ge5	0	0	0	0	0	0	0	0
ge6	0	0	0	0	0	0	0	0
ge7	0	0	0	0	0	0	0	0
ge8	0	0	0	0	0	0	0	0
ge9	0	0	0	0	0	0	0	0
ge10	0	0	0	0	0	0	0	0
ge11	0	0	0	0	0	0	0	0
ge12	0	0	0	0	0	0	0	0
ge13	0	0	0	0	0	0	0	0
ge14	0	0	0	0	0	0	0	0
ge15	0	0	0	0	0	0	0	0
ge16	0	0	0	0	0	0	0	0
ge17	4482	6829	533882	9252786	0	0	2	0

4.7.2 Port Statistics-Port

Function Description

Check the classification statistics of the total number of messages sent and received by the designated port and the number of bytes of messages.

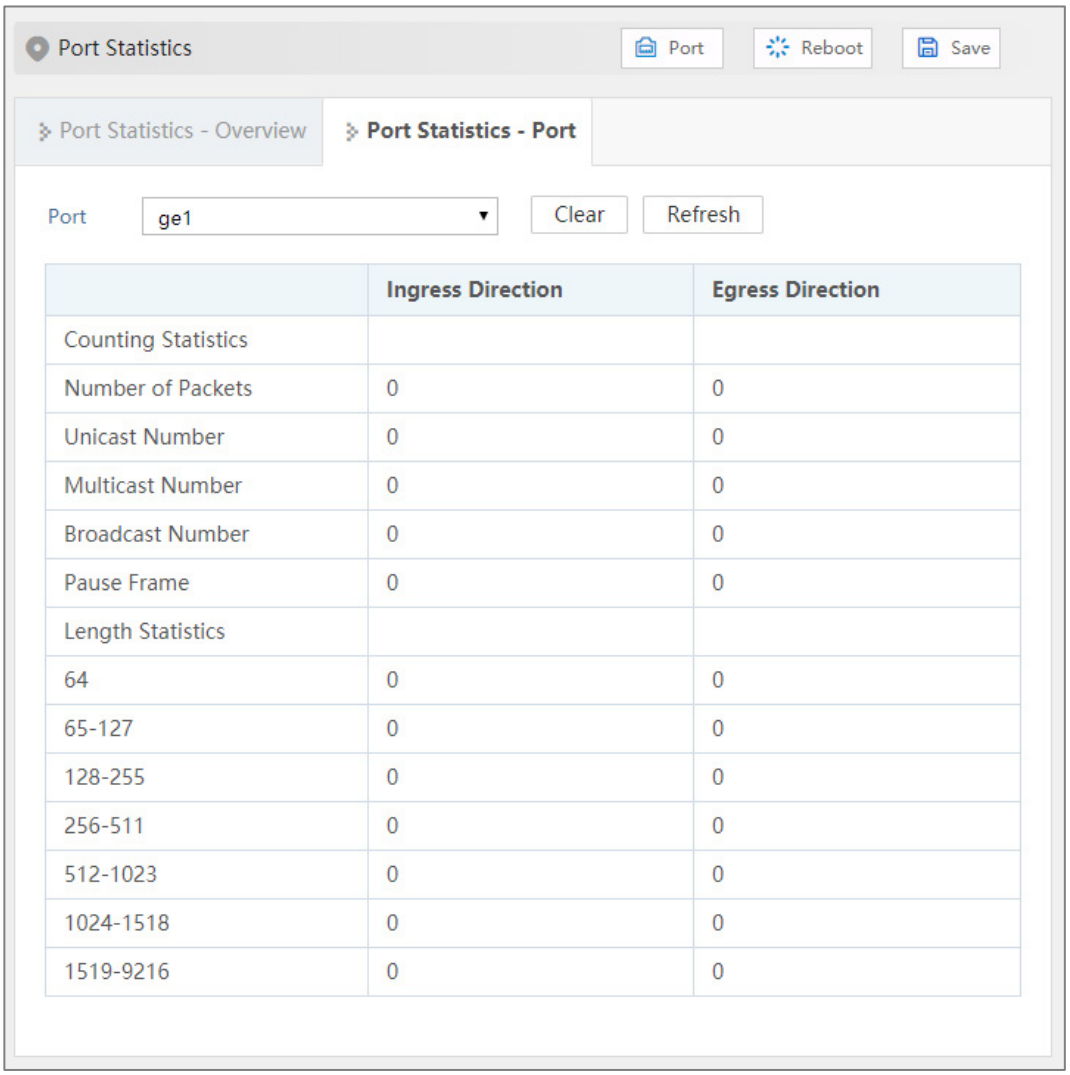
Operation Path

Open in order: "Port Configuration > Port statistics > Port Statistics-Port".

Interface Description

Port Statistics-Port interface as follows:

Copyright © 3onedata Co., Ltd.



	Ingress Direction	Egress Direction
Counting Statistics		
Number of Packets	0	0
Unicast Number	0	0
Multicast Number	0	0
Broadcast Number	0	0
Pause Frame	0	0
Length Statistics		
64	0	0
65-127	0	0
128-255	0	0
256-511	0	0
512-1023	0	0
1024-1518	0	0
1519-9216	0	0

3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.

5 Layer 2 Configuration

5.1 VLAN

VLAN is Virtual Local Area Network. VLAN is the data switching technology that logically (note: not physically) divides the LAN device into each network segment (or smaller LAN) to achieve the virtual working group (unit).

VLAN advantages mainly include:

- Port isolation. Ports in different VLAN, even in the same switch, can't intercommunicate. Such a physical switch can be used as multiple logical switches.
- Network security. Different VLAN can't directly communicate with each other, which has eradicated the insecurity of broadcast information.
- Flexible management. Changing the network user belongs to needn't to change ports or connection; only needs to change the firmware configuration.

That is, ports within the same VLAN can intercommunicate; otherwise, ports can't communicate with each other. A VLAN is identified with VLAN ID, and ports with the same VLAN ID belong to a same VLAN.

5.1.1 VLAN Configuration

Function Description

Create VLAN and edit VLAN description.

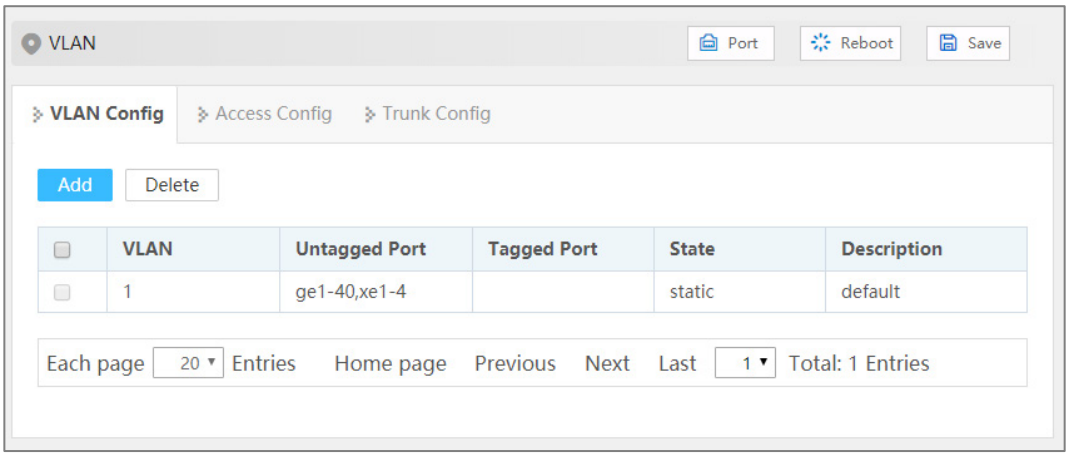
Operation Path

Open in order: "Layer 2 Configuration > VLAN > VLAN-config".

Interface Description

Vlan configuration interface as follows:

3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.



The main element configuration description of Vlan configuration interface.

Interface Element	Description
VLAN	VLAN ID number, value range is 1-4094.
Untagged port	Untagged port member to conduct untagged process to sending data frame.
Tagged port	Tag port member to conduct tagged process to sending data frame.
State	VLAN Status: • Static: static VLAN • Dynamic: dynamic VLAN
Description	VLAN description information, which supports 0-32 characters and consists of uppercase letters, lowercase letters, numbers or special characters (! @ _-).

5.1.2 Access Configuration

Function Description

Configure the PVID (Port Default VLAN ID) of the Access interface, or modify it to Trunk interface.

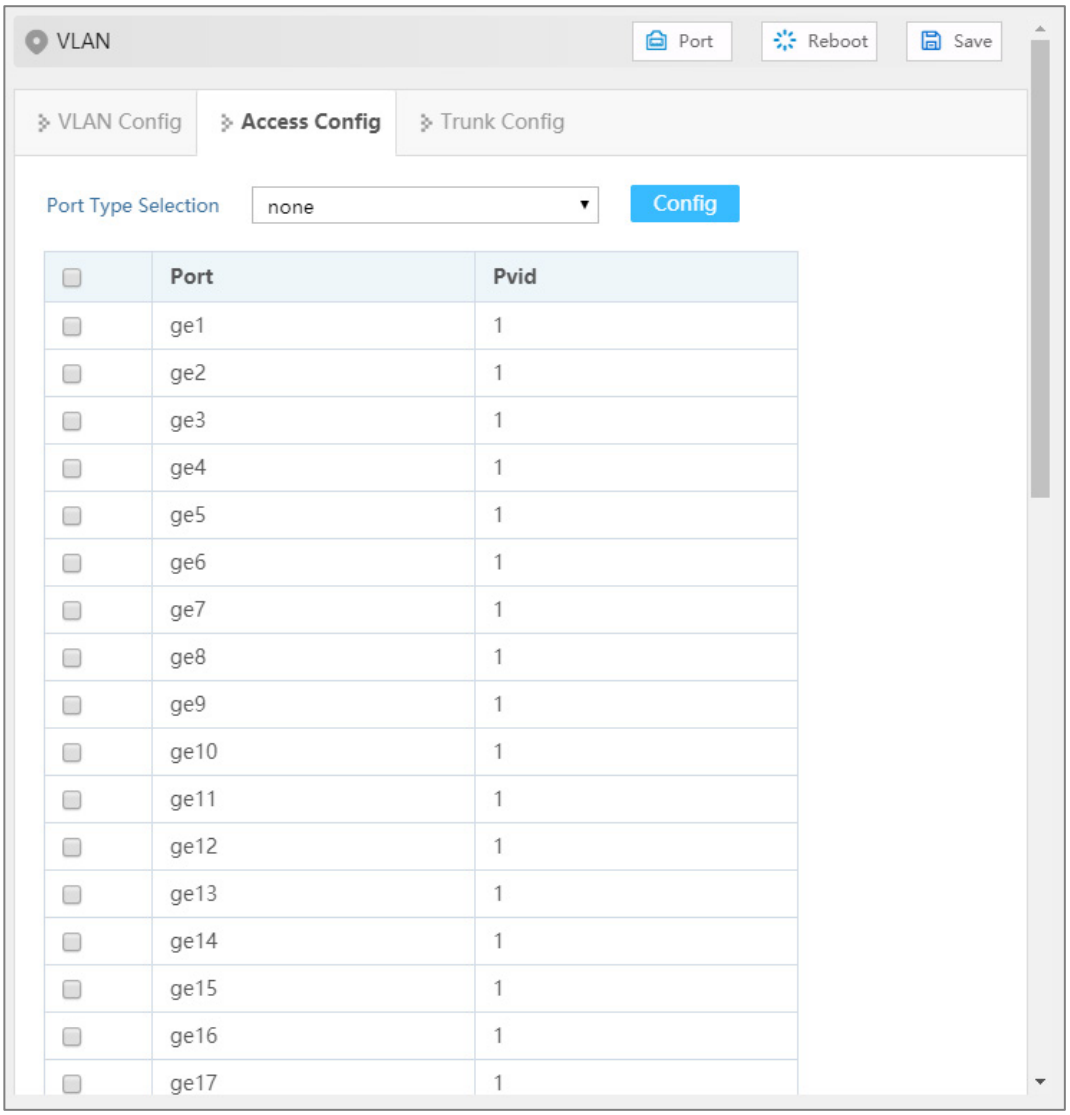
Operation Path

Open in order: "Layer 2 Configuration > VLAN > Access Configuration".

Interface Description

Access configuration interface as follow:

Copyright © 3onedata Co., Ltd.



The main element configuration description of Access configuration interface.

Interface Element	Description
Port	The corresponding port name of the device Ethernet port.
Pvid	Port Default VLAN ID, which is the default VLAN of the port. Default is 1, value range is 1-4094. Note: Each port has a PVID property, when the port receives Untag messages, it adds Tag mark on them according to PVID. When the port transmits data message with the same Tag mark as PVID, it would erase the Tag mark and then transmit the message. The PVID of all ports default to 1.
Configuration	Check the port and click “Configure” to reset PVID and port mode. • Access: port only belongs to 1 VLAN(which is the default VLAN), all ports of the switch are Access mode by default and all PVID are 1.

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	• Trunk: port can belong to multiple VLAN, Trunk port can allow the messages of multiple VLANs to pass with Tag, but only allow the messages of one VLAN to transmit without tag (strip Tag) from this kind of interface. Commonly used in the connection between network devices.

5.1.3 Trunk Configuration

Function Description

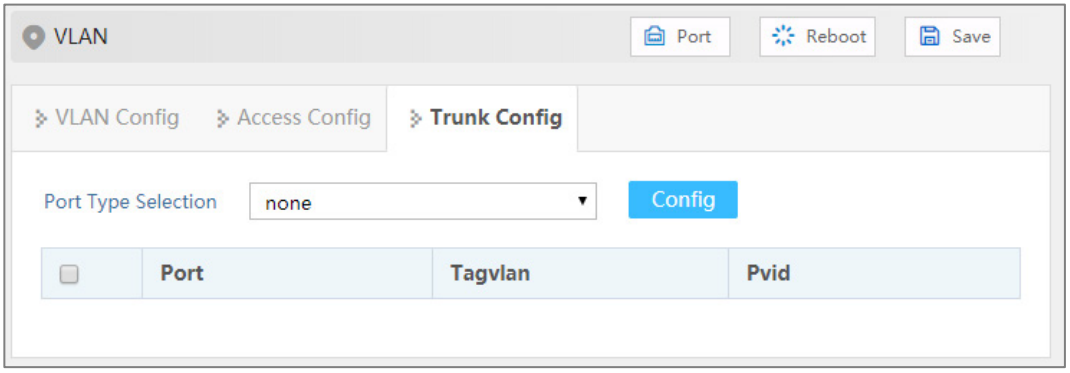
Configure the pvid value and tagvlan of Trunk port, or modify it to Access interface.

Operation Path

Open in order: "Layer 2 Configuration > VLAN > Trunk Configuration".

Interface Description

Trunk configuration interface as follows:



The main element configuration description of Trunk configuration interface:

Interface Element	Description
Port	The corresponding port name of the device Ethernet port.
Tagvlan	The VLAN ID number that the port allows to pass.
Pvid	Port Default Vlan ID, which is the default VLAN of the port. Default is 1, value range is 1-4094.
Configuration	Check the port and click “Configure” to configure the VLAN and PVID of the port, as well as the processing of PVID when sending messages.

Copyright © 3onedata Co., Ltd.

Process for Port Receiving Message

Interface type	Process for Receiving Untagged Message	Process for Receiving Tagged Message
Access	Receive this message and tag it with default VLAN ID.	Receive the message when the VLAN ID is the same as default VLAN ID, if not, discard the message.
Trunk		Receive this message when the VLAN ID is in the list of VLAN ID that allow to pass through the interface, if not, discard the message.

Process for Port Sending Message

Interface type	The process of transmit frame
Access	Strip the PVID Tag of the message first, then transmit it.
Trunk	Sending the message when the VLAN ID is the VLAN ID allowed by the interface; In addition, if the VLAN ID is the same as the default VLAN ID, the Tag can be removed or reserved according to the configuration, and send the message.

5.2 MAC

MAC (Media Access Control) address is the hardware identity of network device; the switch forwards the message according to MAC address. MAC address has uniqueness, which has guaranteed the correct retransmission of message. Each switch is maintaining a MAC address table. In the table, MAC address is corresponding to the switch port. When the switch receives data frames, it decides whether to filter them or forward them to the corresponding port according to the MAC address table. MAC address is the foundation and premise that switch achieves fast forwarding.

3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.

5.2.1 Global Configuration

Function Description

Set the aging time of dynamic MAC addresses.

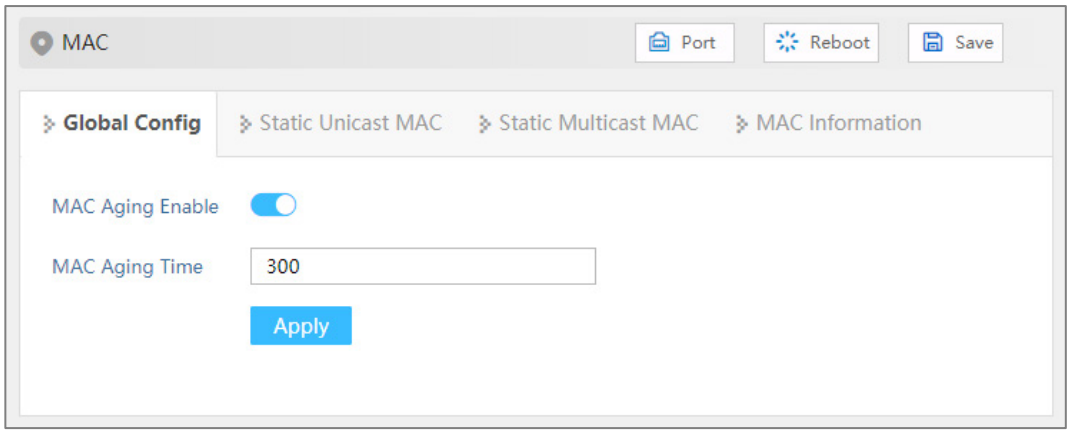
Each port in the switch is equipped with automatic address learning function, it stores the frame source address (source MAC address, switch port number) that port sends and receives in the address table. Ageing time is a parameter influencing the switch learning process; the default value is 300 seconds. When the timekeeping starts after an address record is added to the address table, if each port doesn't receive the frame whose source address is the MAC address within the ageing time, then these addresses will be deleted from dynamic forwarding address table (source MAC address, destination MAC address and their corresponding switch port number).

Operation Path

Open in order: "Layer 2 Config > MAC > Global Config".

Interface Description

Global configuration interface is as follows:



The main element configuration description of global configuration interface:

Interface Element	Description
MAC Aging Enable	Enable switch of MAC address aging.
MAC Aging Time	MAC address aging-time, unit is second, default value is 300, and range is 10-1000000.

Copyright © 3onedata Co., Ltd.

5.2.2 Static MAC

Function Description

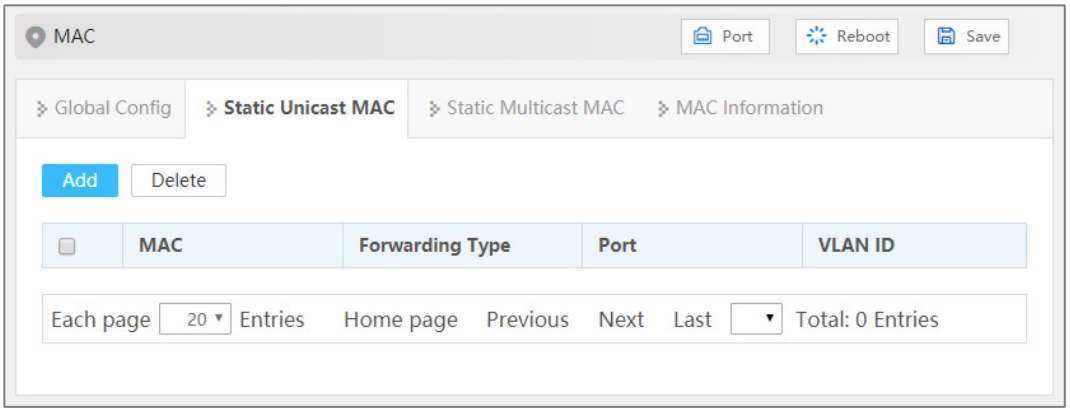
Source unicast MAC address binding and filtering will not age.

Operation Path

Open in order: "Layer 2 Configuration > MAC > Static Mac".

Interface Description

Static MAC interface as follows:



The main element configuration description of static MAC interface:

Interface Element	Description
MAC	The unicast MAC address bound by the interface, such as 0001.0001.0001.
Forwarding Type	MAC forwarding type, as shown below: • Discard • Forward
Port	The Binding Port Number.
VLAN ID	The VLAN ID number to which the data sent by this MAC address belongs, for example, 1-4094. Note: Input VLAN ID is the existing ID.

Note

- The function is a sort of security mechanism, please carefully confirm the setting, otherwise, part of the devices won't be able to communicate;
- Please don't adopt multicast address as the entering address;
- Please don't enter reserved MAC address, such as the local MAC address.

Copyright © 3onedata Co., Ltd.

5.2.3 Static Multicast MAC

Function Description

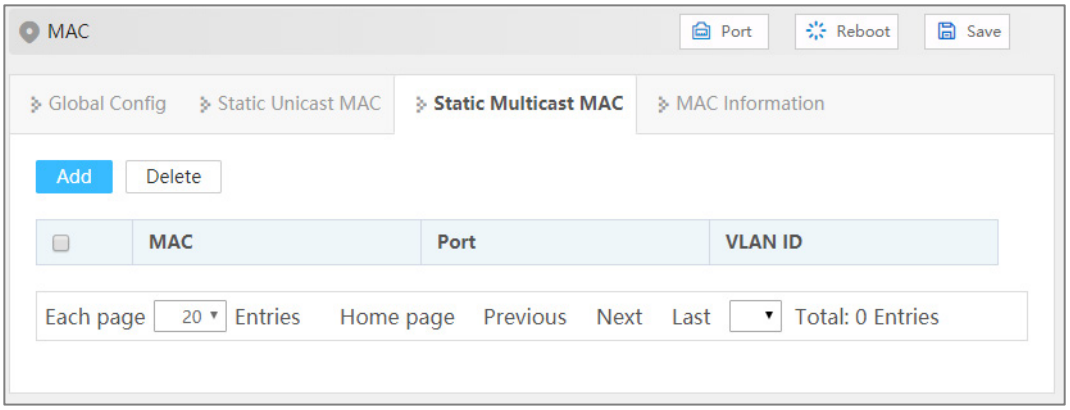
Source multicast MAC address binding will not age.

Operation Path

Open in order: "Layer 2 Configuration > MAC > Static Multicast MAC".

Interface Description

Static multicast MAC interface as follows:



The main element configuration description of static multicast MAC interface:

Interface Element	Description
MAC	Multicast MAC address bound to the interface, for example: 0100.5e01.0001.
Port	The Binding Port Number.
VLAN ID	The VLAN ID number to which the data sent by this MAC address belongs, for example, 1-4094. Note: Input VLAN ID is the existing ID.

5.2.4 MAC Information

Function Description

Check the MAC address table information.

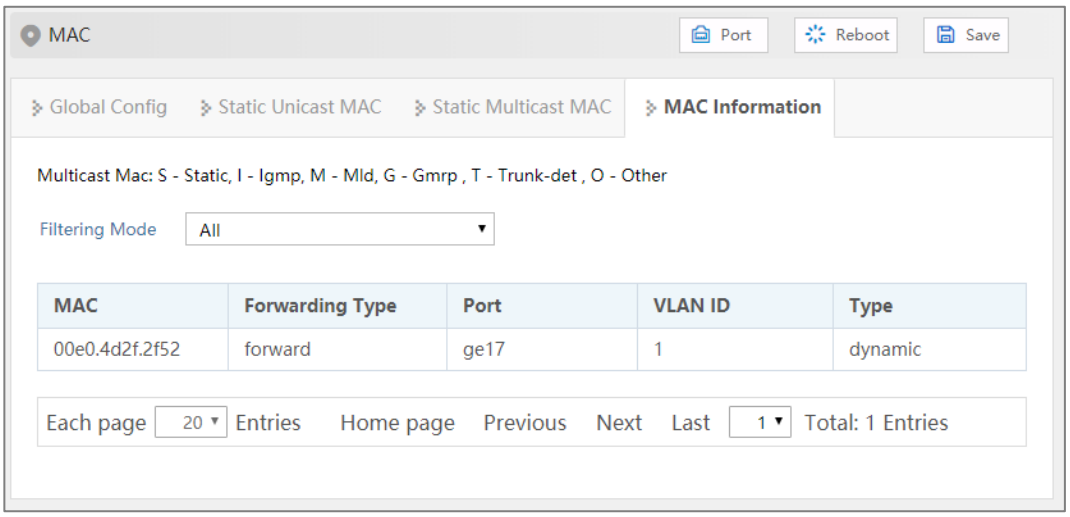
Operation Path

Open in order: "Layer 2 Configuration > MAC > MAC Information".

3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.

Interface Description

MAC Information interface as follow:



The main element configuration description of MAC information interface:

Interface Element	Description
Filtering Mode	Drop-down list of MAC mode to filter the display of the MAC address list of the specified type. The options are as follows: • All • Dynamic Unicast • Dynamic Multicast • Static Multicast • Static Unicast
MAC	The dynamic MAC addresses that the device have learned or the static MAC address information that user has configured.
Forwarding Type	MAC forwarding type, as shown below: • Discard • Forward
Port	Corresponding port number of the MAC address.
VLAN ID	VLAN ID number the data MAC address sending belongs to.
Type	The type of MAC address, it displays as follows: • dynamic • static

3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.

5.3 Spanning Tree

Spanning-tree protocol is a sort of layer 2 management protocol; it can eliminate the network layer 2 circuit via selectively obstructing the network redundant links. At the same time, it has link backup function. Here are three kinds of spanning-tree protocols:

- STP (Spanning Tree Protocol)
- RSTP (Rapid Spanning Tree Protocol)
- MSTP (Multiple Spanning Tree Protocol)

Spanning-tree protocol has two main functions:

- First function is utilizing spanning-tree algorithm to establish a spanning-tree that takes a port of a switch as the root to avoid ring circuit in Ethernet.
- Second function is achieving the convergence protection purpose via spanning-tree protocol when Ethernet topology changes.

Compared to STP, RSTP, MSTP can converge the network more quickly when network structure changes; MSTP is compatible with STP and RSTP, and is better than STP and RSTP. It can not only quickly converge but also send different VLAN along each path to provide better load sharing system for redundant link.

5.3.1 Global Configuration

Function Description

Configure the relevant parameters of spanning tree.

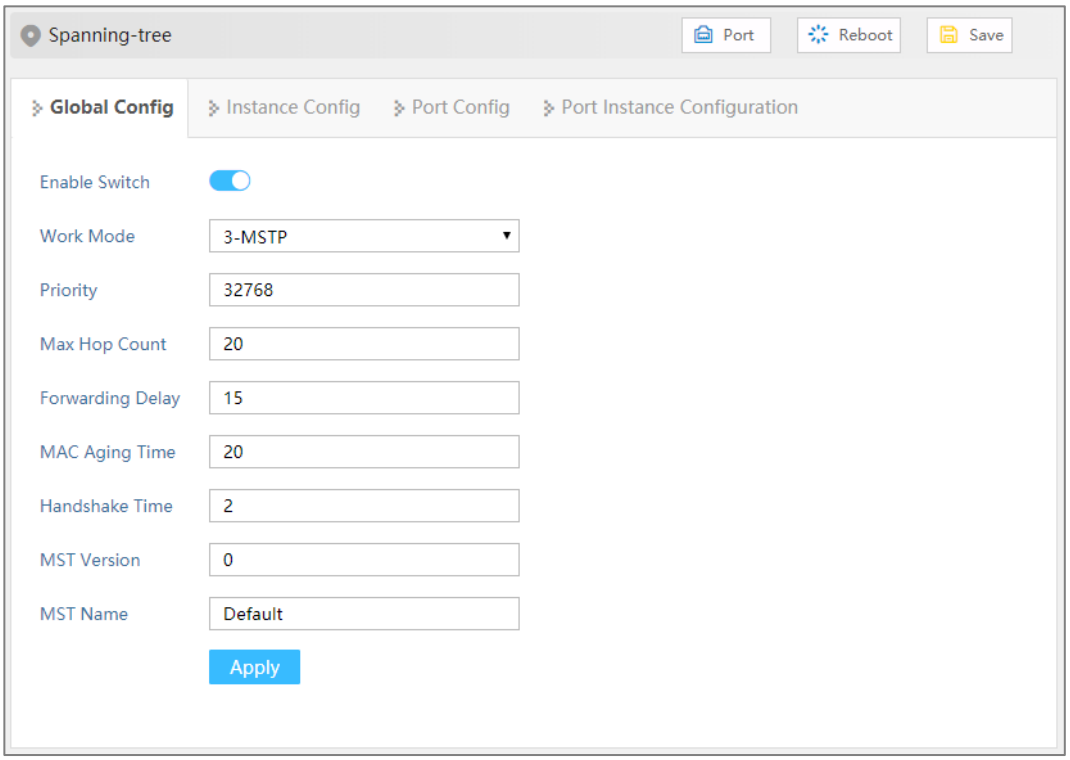
Operation Path

Open in order: "Layer 2 Configuration > Spanning-tree > Global Configuration".

Interface Description

Global configuration interface is as follows:

Copyright © 3onedata Co., Ltd.



The main element configuration description of global configuration interface:

Interface Element	Description
Enable	Spanning-tree enable switch. Disable by default
Work mode	Defaults to MSTP, there are three modes for spanning-tree protocol choice: • 0-STP: Spanning-tree • 2-RSTP: Rapid spanning tree • 3-MSTP: Multiple spanning-trees Note: In RSTP or MSTP mode, when the connection with STP device is found, the port will automatically migrate to STP compatible mode to work.
Priority	Bridge priority level, value range is 0-61440. Note: Smaller the priority level value is, higher the priority level is. It must be a multiple of 4096.
Max Hop Count	The maximum hop in MST region, defaults to 20, the value range is 1-40. Note: The maximum hop in MST region has limited the size of MST region. The maximum hop configured on a domain root will be used as the maximum hop in MST region.
Forwarding Delay	Port state transition delay, defaults to 15s, the value range is 4-30.
MAC Aging Time	The maximum lifetime of the message in the device, defaults

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	to 20s, the value range is 6-40. It's used to determine whether the configuration message times out.
Handshake Time	Message sending cycle,defaults to 2s, the value range is 1-10. Note: • The spanning tree protocol sends configuration information every Hello time to check whether the link is faulty. • In order to avoid frequent network flap, forwarding delay, aging time and handshake time should satisfy the following formula: 2× (forwarding delay -1)≥ aging time ≥2× (handshake time -1).
MST Version	MSTP revision level, defaults to 0, the value range is 0-65535. Note: When the MST region name, revision level, instance-to-VLAN mapping relation are the same, the two or more bridges will belong to a same MST region.
MST Name	MST domain name, defaults to Default, up to 32 characters.

5.3.2 Instance Configuration

Function Description

Configure instance-to-VLAN mapping.

Multiple Spanning Tree Regions (MST Regions) are composed of multiple devices in the switched network and the network segments between them.

In a MST region, multiple spanning trees can be generated through MSTP. Each spanning tree is independent to others and corresponding to special VLAN. Each spanning tree is called an MSTI (Multiple Spanning Tree Instance).

VLAN mapping table is an attribute of MST region, and it's used to describe the mapping relation between VLAN and MSTI.

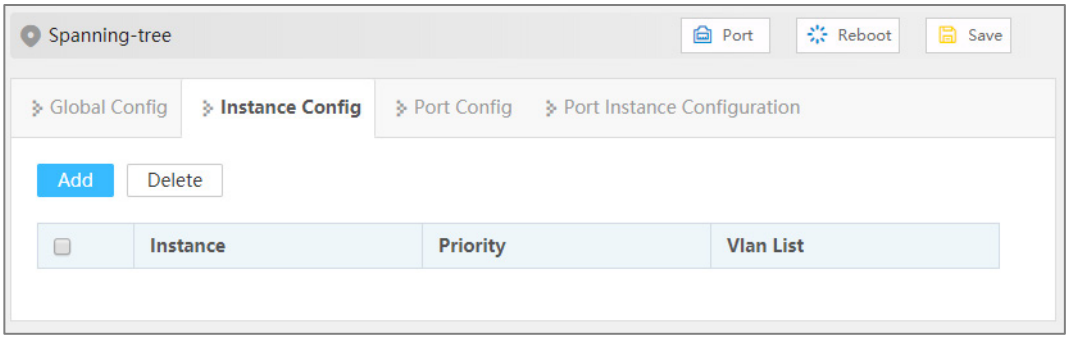
Operation Path

Open in order: "Layer 2 Configuration > Spanning-tree > Instance Configuration".

Interface Description

Instance configuration interface as follows:

Copyright © 3onedata Co., Ltd.



The main element configuration description of instance configuration interface:

Interface Element	Description
Instance	Instance ID number of Multiple Spanning-tree. The value range is 1-16.
Priority	Device priority level, value range is 0-61440, default to 32769, step is 4096. During adding, choose a priority based on 0-15 times the value on the 4096. Note: The priority of a device participates in spanning tree calculation. Its size determines whether the device can be selected as the root bridge of a spanning tree.
VLAN list	The list of VLANs mapped to MSTI instances, each VLAN can only correspond to one MSTI. Note: VLAN mapping table is an attribute of MST region, and it's used to describe the mapping relation between VLAN and MSTI. MSTP achieves load balancing based on the VLAN mapping table.

5.3.3 Port Configuration

Function Description

Enable port to participate in spanning-tree and configure port type, link type and BPDU protection function.

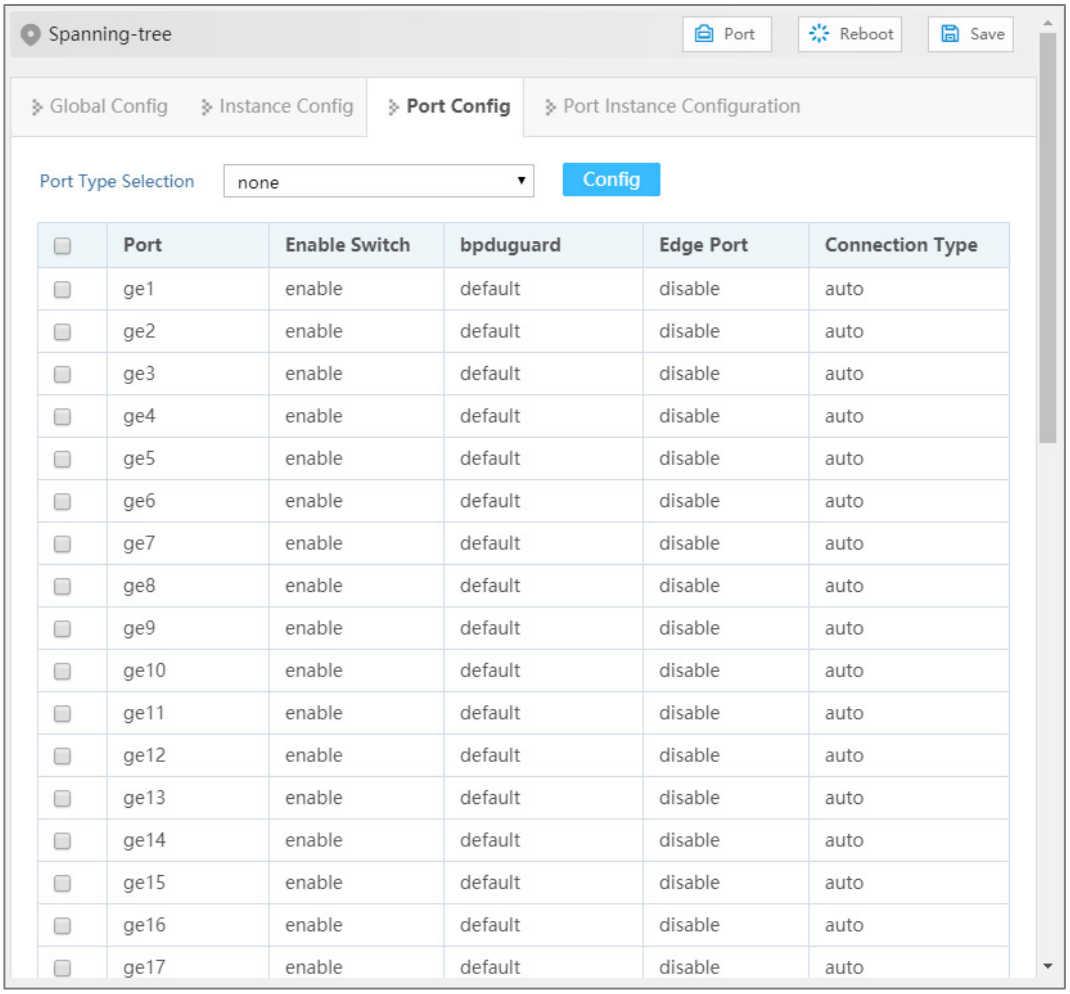
Operation Path

Open in order: "Layer 2 Configuration > Spanning-tree > Port Configuration".

Interface Description

Check port configuration interface as below:

Copyright © 3onedata Co., Ltd.



The main element configuration description of port configuration interface:

Interface Element	Description
Port	The corresponding port name of the device Ethernet port.
Enable	The enable status of ports participating in spanning tree can be shown as follows: • Enable • Disable：disable
BPDU Guard	BPDU (Bridge Protocol Data Unit) protection function. After starting the BPDU protection, if the edge port receives the BPDU message that should not exist, the edge port will be closed, and it can return to normal after a certain time. Edge Port BPDU Guard State: • Default: global configuration protection status • Enable • Disable：disable
Edge port	The port that directly connects to terminal instead of other switches. The edge port does not participate in the spanning

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	tree operation, and can be directly transferred to the Forwarding state by Disable. Enable state of edge port: • Enable • Disable：disable
Connection type	Fast entry of the port into the forwarding state requires that the port must be a point-to-point link, not a shared media link. Port link type: • Auto: if the port is full duplex, it is judged as a point-to-point link; If it is half-duplex, it is judged as a non-point-to-point link. • Point-to-point: point-to-point link. • Shared: Non point-to-point link.

5.3.4 Instance Port Configuration

Function Description

Configure port priority and cost

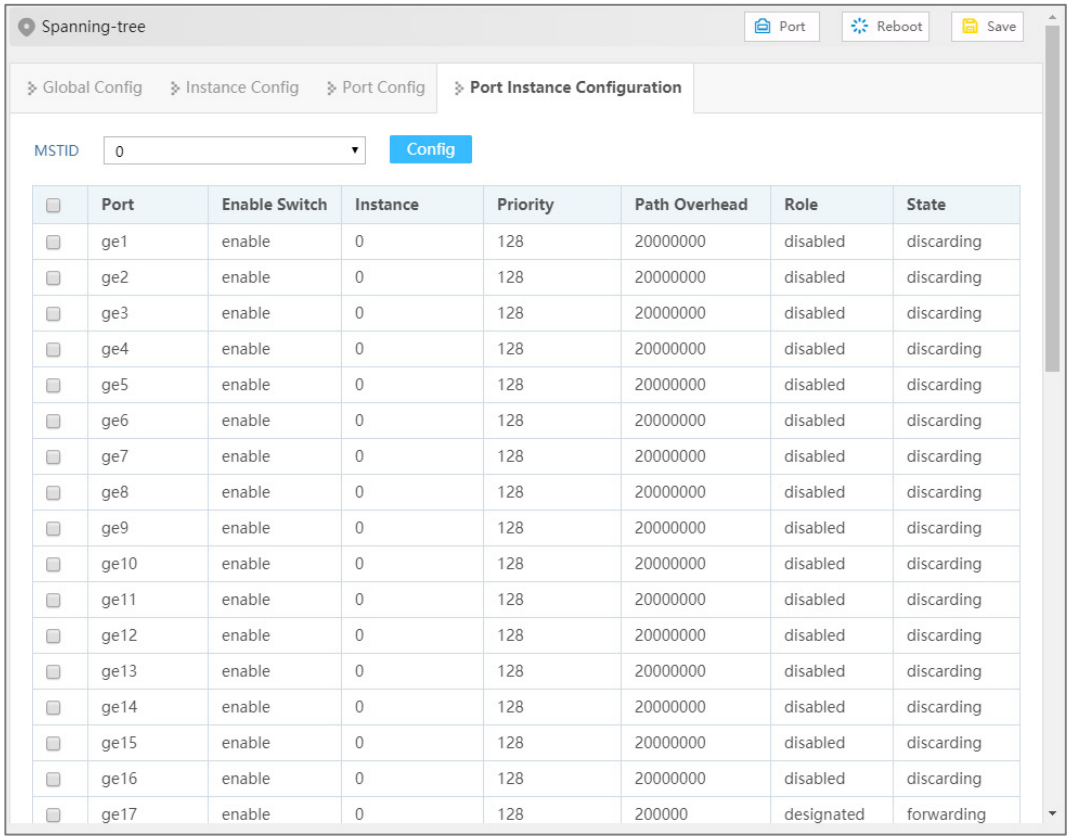
Operation Path

Open in order: "Layer 2 Configuration > Spanning-tree > Inst Port Configuration".

Interface Description

Instance port configuration interface as follows:

3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.



Port	Enable Switch	Instance	Priority	Path Overhead	Role	State
ge1	enable	0	128	20000000	disabled	discarding
ge2	enable	0	128	20000000	disabled	discarding
ge3	enable	0	128	20000000	disabled	discarding
ge4	enable	0	128	20000000	disabled	discarding
ge5	enable	0	128	20000000	disabled	discarding
ge6	enable	0	128	20000000	disabled	discarding
ge7	enable	0	128	20000000	disabled	discarding
ge8	enable	0	128	20000000	disabled	discarding
ge9	enable	0	128	20000000	disabled	discarding
ge10	enable	0	128	20000000	disabled	discarding
ge11	enable	0	128	20000000	disabled	discarding
ge12	enable	0	128	20000000	disabled	discarding
ge13	enable	0	128	20000000	disabled	discarding
ge14	enable	0	128	20000000	disabled	discarding
ge15	enable	0	128	20000000	disabled	discarding
ge16	enable	0	128	20000000	disabled	discarding
ge17	enable	0	128	200000	designated	forwarding

The main element configuration description of instance port configuration interface:

Interface Element	Description
MSTID	Choose multiple Spanning-tree ID number.
Port	The corresponding port name of the device Ethernet port.
Enable	Port enable status: • Enable: participate in spanning-tree; • Disable: not participate in spanning-tree.
Instance	Instance ID number port belongs to.
Priority	Port priority, the value range is 0-240, the step size is 16, the default value is 128, and the priority based on 0-15 times the value of 16 can be selected. Note: Port priority level in bridge, port priority level is higher when the value is smaller. The higher the priority, the more likely it is to be a root port.
Path Overhead	The path cost from network bridge to root bridge, defaults to 20000000. Value range: 1-200000000. Note: When the configuration cost is the default value, the actual cost of link up port is converted according to the port rate, the rate of 10M corresponds to the cost of 2000000, and 100M corresponds to the cost of 200000.

Copyright © 3onedata Co., Ltd.

Interface Element	Description
Role	Role • unkn: Unknown; • root: Root port; • desg: Designated port; • altn: Alternate port; • back: Backup port; • disa: Disable port.
State	Port status in spanning-tree: • Disable: Port close status; • Blocking: Blocked state; • Listening: Monitoring state. • Discarding: Discarding status • Learning: Learning state; • Forwarding: Forwarding state;

5.4 Ring

Ring is a private ring network algorithm developed and designed for highly reliable industrial control network applications that require link redundancy backup. Its design concept is completely in accordance with international standards (STP and RSTP) implementation, and do the necessary for industrial control application optimization, with Ethernet link redundancy, fault fast automatic recovery ability.

Ring adopts the design of no master station. The devices running the Ring protocol discover the loop in the network by exchanging information with each other, and block a certain port. Finally, the ring network structure is trimmed into a tree network structure without loop, thus preventing messages from circulating continuously in the ring network, and avoiding the reduction of processing capacity caused by repeated reception of the same message. In a multi-Ring network composed of 250 switches, when the network is interrupted or fails, the ring can ensure that the user network automatically resumes link communication within 20 ms.

Ring needs to manually divide the ring network ports in advance, support multiple ring network types such as single ring, coupled ring, chain and Dual Homing, and provide visual management of network topology. In a single Ring, Ring supports master/slave and no master configuration to meet various network environment requirements.

Function Description

Configure Ring private protocol ring network.

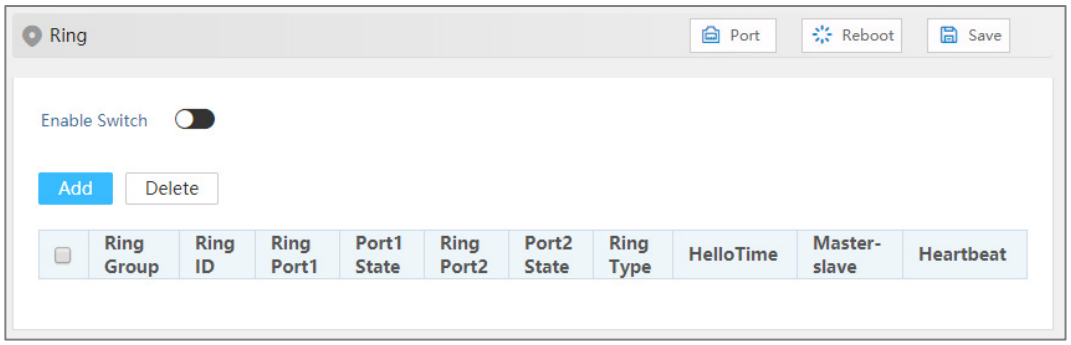
Copyright © 3onedata Co., Ltd.

Operation Path

Open in order: "Layer 2 Configuration > Ring".

Interface Description

Ping interface as follows:



The main element configuration description of Ring interface.

Interface Element	Description
Enable	Enable switch, which can enable the Ring ring network function after being enabled.
Ring group	Support ring group 1-12, it can create multiple ring networks at the same time.
Ring ID	When multiple switches form a ring, the current ring ID would be network ID. Different ring network has different ID. Value range is 1-255. Note: The ring network identification must remain the same in one ring network.
Ring Port 1	The network port 1 on the switch device used to form a ring. Note: When the ring network type is "Couple", ring port 1 is the "Coupled Port". Coupling port is the port that connects different network identities.
Port1 State	Conduction state of ring network port 1.
Ring port2	The network port 2 on the switch used to form a ring. Note: When the ring network type is “Couple”, ring port 2 is the “console port”. Console port is the port in the chain where two rings intersect.
Port2 Status	Conduction state of ring port 2.
Ring Type	According to the requirement in the scene, user can choose different ring type. • Single: single ring, using a continuous ring to connect all device together.

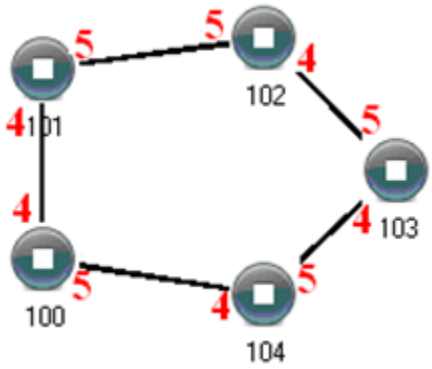
3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.

Interface Element	Description
	• Couple: couple ring is a redundant structure used for connecting two independent networks. • Chain: chain can enhance user's flexibility in constructing all types of redundant network topology via an advanced software technology. • Dual-homing: two adjacent rings share one switch. User could put one switch in two different networks or two different switching equipments in one network.
Hello Time	Hello_time is the sending time interval of Hello packet; via the ring port, CPU sends information packet to adjacent device for confirming the connection is normal or not. Value range is 0-300.
Master-slave	Single ring supports no master station and one master and multiple slave modes (optional): • No-master station mode: When all the single-loop devices are slave stations, the single-loop structure is no-master station. • One-Master Multi-Slave mode: When the device is set as master device and one end of it is backup link, it can enable backup link to ensure the normal operation of the network when failure occurs in ring network.
Heartbeat	Heartbeat detection mechanism. When this configuration is enabled, the network association will periodically send heartbeat messages to detect whether the corresponding devices are in live state, thus enhancing the reliability of the network.

Single Ring Configuration

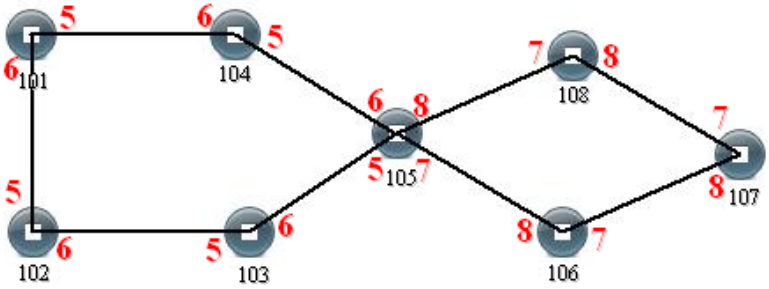
Enable Single, enable ring group 1 (other ring group is OK), Set the device port 4 and port 5 to ring port, and set other switches to the same configuration as the switch above, Enable these devices, and adopt network cable to connect port 4 and port 5 of the switch, then search it via network management software, the ring topology structure picture as below:

3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.



Double Ring Configuration

Double ring as shown below, in the figure, double ring is the tangency between two rings, and the point of tangency is NO. 105 switch.



Configuration Method:

Step 1 Adopt single ring configuration method to configure port 5 and port 6 of NO. 101, 102, 103, 104, 105 switches as the ring port, and the ring group is 1;

Step 2 Adopt single ring configuration method to configure port 7 and port 8 of NO. 105, 106, 107 and 108 switches as the ring ports and the ring group 2;

Step 3 Adopt network cable to connect the ring group 1;

Step 4 Adopt network cable to connect the ring group 2;

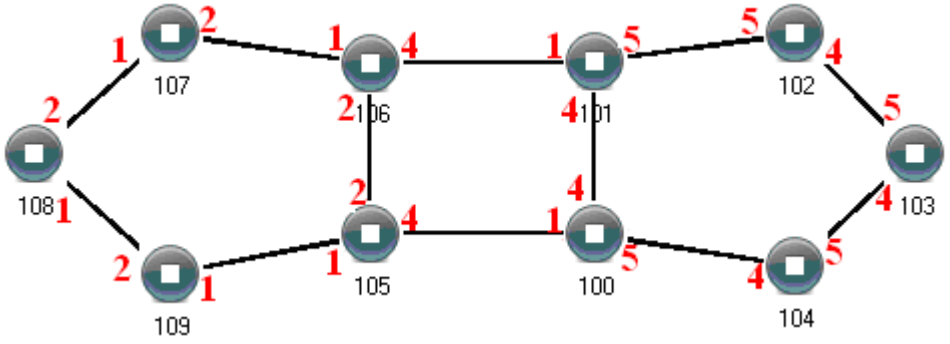
Step 5 Search the topology structure picture via network management software;

Since NO. 105 devices belong to two ring groups, the network IDs of the two ring groups cannot be the same.

Coupling Ring Configuration

Coupling ring basic framework as the picture below:

Copyright © 3onedata Co., Ltd.



Operation method:

Step 1 Enable ring network group 1 and 2: (Hello_time could be disabled, but the time could not be set to make Hello packet send too fast, otherwise it would effect CPU processing speed seriously);

Step 2 Set the ring port of NO. 105, 106 device ring group to port 1 and port 2, network identification to 1, ring type to Single; Set the coupling port of ring group 2 to port 4, console port to 2, ring identification to 3, ring type to Coupling.

Step 3 Set the ring port of NO. 100, 101 device ring group 1 to port 4 and port 5, network identification to 2, ring type to Single; Set the coupling port of ring group 2 to port 1, console port to port 4, ring identification to 3, ring type to Coupling.

Step 4 Set the ring port of NO. 107, 108 and 109 device ring group 1 to port 1 and port 2, network identification to 1, ring type to Single; Set the ring port of NO. 102, 103 and 104 device ring group 1 to port 4 and port 5, network identification to 2, ring type to Single.

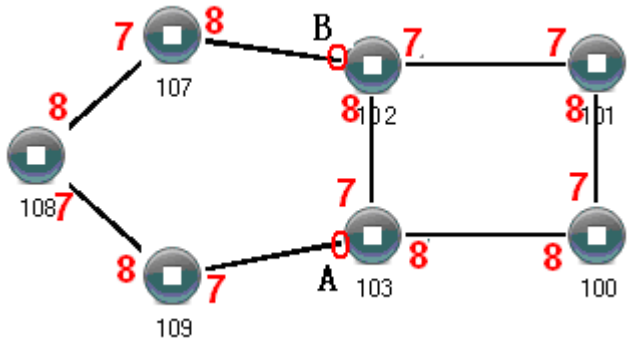
Step 5 Connect the port 4 and port 5 of five devices NO. 100-104 to the single ring in turn, adopt network cable to connect the port 1 and port 2 of four devices NO. 105-109 to the single ring in turn, Then adopt Ethernet cable to connect port 4 of NO. 106 device to port 1 of NO. 101 device, port 4 of NO. 105 device to port 1 of NO. 100 device, coupling ring combination is completed.

Console ports are two ports connected to NO. 105 device and NO. 106 device in the above picture. The two ports connected to NO. 100 device and NO. 101 device are also called console ports.

Chain Configuration

Chain basic framework as the picture below:

3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.



Operation method:

Step 1 Enable ring group1: (Hello_time could be disabled, but the time shouldn't be set to send Hello packet too fast, otherwise it would affect the processing speed of CPU seriously).

Step 2 Set the ring port of NO. 100, 101, 102 and 103 device ring group 1 to port 7 and port 8, network identification to 1, ring type to Single. Set the ring port of NO. 107, 108 and 109 devices ring group 1 to port 7 and port 8, network identification to 2, ring type to Chain.

Step 3 Adopt network cable to connect the port 7 and port 8 of three devices NO. 107-109, adopt network cable to connect the port 7 and port 8 of four devices NO. 100-103 to the single ring in turn, Then adopt network cable to connect port 7 of NO. 107 device and port 7 of NO. 109 device to normal ports of NO. 102 and 103 device, chain combination is complete.

Note

- Port that has been set to port aggregation can't be set to rapid ring port, and one port can't belong to multiple rings;
- Network identification in the same single ring must be consistent, otherwise it cannot form a normal ring or normal communicate;
- Network identification in different ring must be different;
- When forming double ring and other complex ring, user should notice whether the network identification in the same single ring is consistent, and network identification in different single ring is different.

5.5 MRP

MRP (Media Redundancy Protocol), in MRP ring network, one device is regarded as redundancy manager, and the others are redundancy client. MRP supports up to 50

Copyright © 3onedata Co., Ltd.

devices, and when the loop network is interrupted, the loop reconfiguration time is less than 200ms.

Function Description

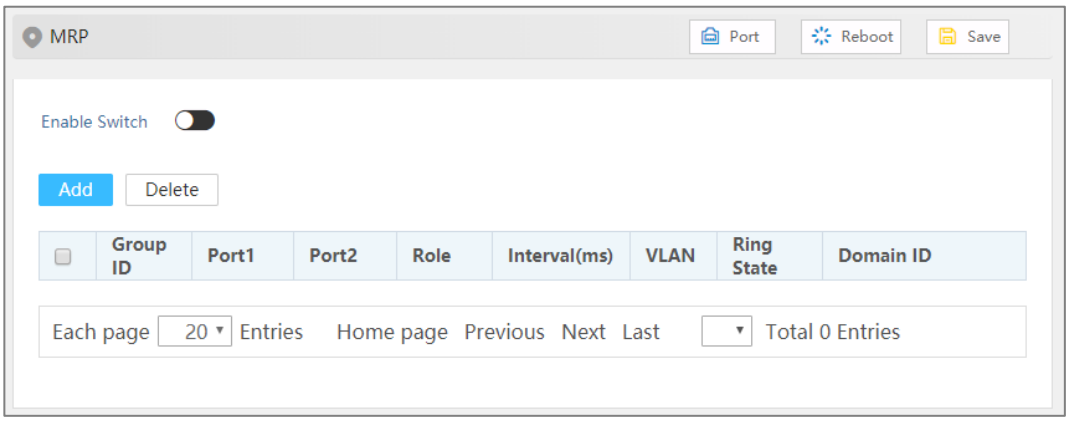
Configure MRP ring network.

Operation Path

Open in order: "Layer 2 Configuration > MRP".

Interface Description

MRP interface is as below:



Main elements configuration descriptions of MRP interface:

Interface Element	Description
Enable	Enable switch, which can enable the MRP ring network function after being enabled.
Group ID	The ID of ring network, its value range is 1-50.
Port1	Ring network port 1, the ports that make up the ring network and the forwarding state of port data.
Port2	Ring network port 2, the ports that make up the ring network and the forwarding state of port data.
Role	The redundant role of device in the ring network can be selected as follows: • manager: media redundancy manager • client: media redundancy client
Interval (ms)	When the MRP ring network is disconnected, the ring network reconfigures the convergence time. The options are as follows: • 10ms • 30ms

3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.

Interface Element	Description
	• 200ms • 500ms
VLAN	VLAN ID used by MRP management message, its value range is 1-4094.
Ring Network State	Status of MRP ring network, Open or Close.
Domain ID	MRP ring network group domain ID, the format is x.x.x.x.x.x.x.x.x.x.x.x.x.x.x.x.

5.6 ERPS

Ethernet Ring Protection Switching (ERPS) is the Ethernet Ring Network Link Layer Technology with high reliability and stability. ERPS is a protocol defined by the International Telecommunication Union Telecommunication Standardization Sector (ITU-T) to eliminate loops at layer 2. Because the standard number is ITU-T G.8032/Y1344, ERPS is also called G.8032. ERPS defines Ring Auto Protection Switching (RAPS) Protocol Message and protection switching mechanisms. It can prevent the broadcast storm caused by data loop when the Ethernet ring is intact. When the Ethernet ring link failure occurs, it has high convergence speed that can rapidly recover the communication path between each node in the ring network.

5.6.1 Timer Configuration

Function Description

Configure the parameters of ERPS ring network timer After the failure of the node device or link in the ERPS ring is restored, in order to prevent the flap, the timer to the ERPS ring will be enabled to help reduce the interruption time of traffic flow.

In ERPS protocol, timers used mainly include WTR (Wait to Restore) Timer, Guard and Hold Timer.

- WTR timer

  If an RPL owner port is unblocked due to a link or node fault, the involved port may not go Up immediately after the link or node recovers. Blocking the RPL owner port may cause network flapping. Blocking the RPL owner port may cause network flapping. To prevent this problem, the node where the RPL owner port resides starts the wait to restore (WTR) timer after receiving an RAPS (NR)

Copyright © 3onedata Co., Ltd.

message. The WTR Timer will be turned off if SF(Signal Fail) RAPS messages are received from other ports before the timer expires. If the node does not receive any RAPS (SF) message before the timer expires, it blocks the RPL owner port when the timer expires and sends NR-RB (RPL Block, RPL) RAPS message. After receiving this RAPS (NR, RB) message, the nodes set their recovered ports on the ring to the Forwarding state.

- Guard timer

  Device involved in link failure or node failure sends NR(No Request) RAPS message to other device after failure recovery or clearing operation, and starts Guard Timer at the same time, and does not process NR RAPS message before the timer expires, in order to prevent receiving expired NR RAPS message. Before the Guard timer expires, the device does not process any RAPS (NR) messages to avoid receiving out-of-date RAPS (NR) messages. After the Guard timer expires, if the device still receives an RAPS (NR) message, the local port enters the Forwarding state.

- Hold Timer

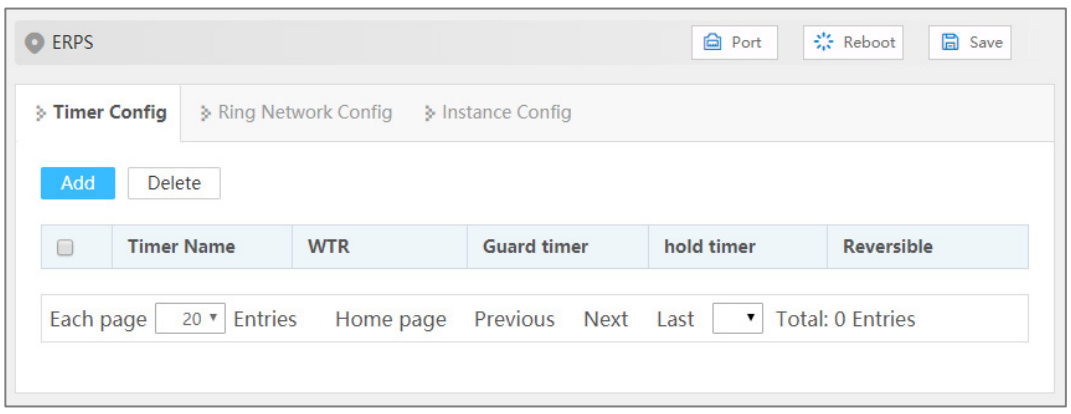
  On Layer 2 networks running ERPS, there may be different requirements for protection switching. For example, on a network where multi-layer services are provided, after a server fails, users may require a period of time to rectify the server fault so that clients do not detect the fault. Users can set the Hold timer. If the fault occurs, the fault is not immediately sent to ERPS until the Hold Timer expires and the fault is still not recovered.

Operation Path

Open in order: "Layer 2 Configuration > ERPS > Timer Configuration".

Interface Description

Timer configuration interface as follows:



Main elements configuration description of timer configuration interface:

Copyright © 3onedata Co., Ltd.

Interface Element	Description
Timer Name	The name of ERPS timer, which supports 1-32 characters and consists of uppercase letters, lowercase letters, numbers or special characters (! @ _-).
WTR	WTR timer, value range is 1-12, unit: minute.
GuardTimer	Guard timer, its value range is 1-200, unit 10ms.
HoldTimer	Hold timer, its value range is 0-100, unit 100ms.
Revertive	ERPS reversible mode status, options as follows: • enable If the failed link recovers, the RPL owner port will be blocked again after waiting for WTR time. Blocked links are switched back to RPL. • disable If the failed link recovers, the WTR timer is not started, and the original faulty link is still blocked and will be switched to RPL.

5.6.2 Ring Configuration

Function Description

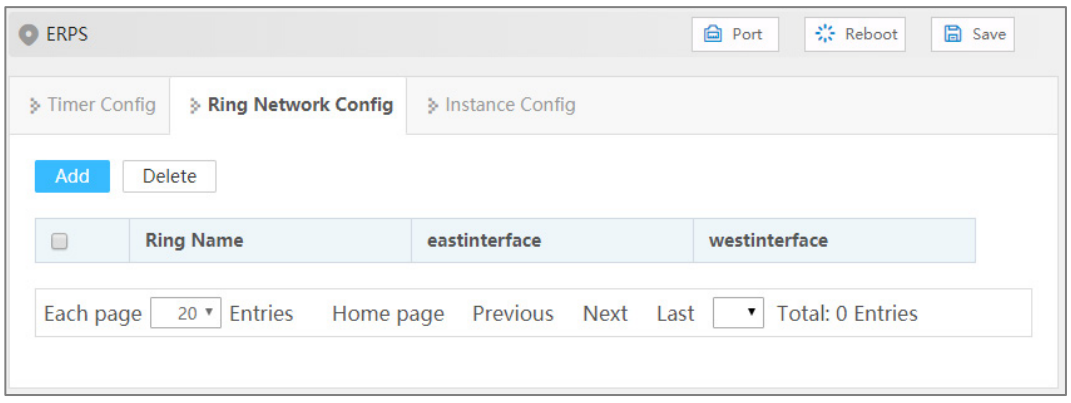
Configure ERPS ring port.

Operation Path

Open in order: "Layer 2 Configuration > ERPS Configuration > Ring Configuration".

Interface Description

Ring configuration interface as follows:



The main element configuration description of ring configuration interface:

Interface Element	Description

Interface Element	Description
Ring Name	The name of ERPS ring network, which supports 1-32 characters, consists of uppercase letters, lowercase letters, numbers or special characters (! @ _-).
East Interface	ERPS ring port. Note: When the device is an intersecting node, only EastInterface can be configured for some ports of the sub-ring.
West Interface	ERPS ring port. Notice: • ERPS loop ports can be normal physical ports or static aggregation groups. • ERPS ring port cannot be opened at the same time with other layer 2 ring network protocols, when ERPS guard instance is not 0, it can be opened at the same time with MSTP. • ERPS ring ports can't be the same ports. • ERPS ring ports must be trunk ports and allow the ring instance VLAN to pass.

5.6.3 Instance Configuration

Function Description

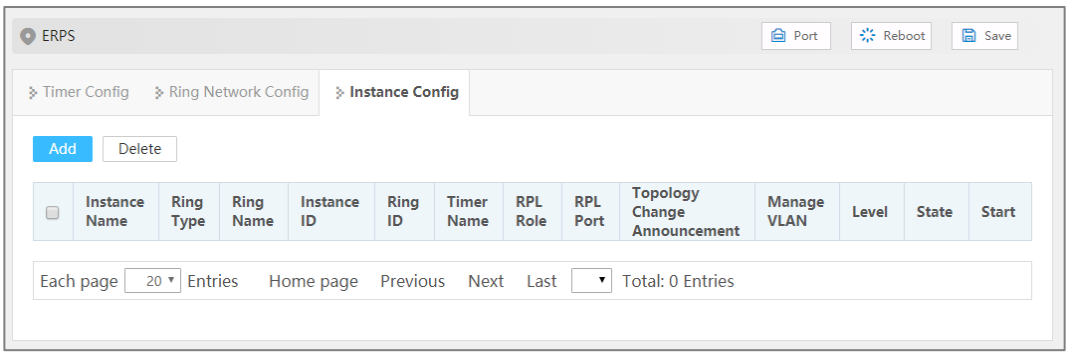
Configure ERPS ring network instance.

Operation Path

Open in order: "Layer 2 Configuration >ERPS Configuration > Instance Configuration".

Interface Description

Instance configuration interface as follows:



The main element configuration description of instance configuration interface:

Copyright © 3onedata Co., Ltd.

Interface Element	Description
Instance Name	The name of the ERPS instance, which supports 1-32 characters, consists of uppercase letters, lowercase letters, numbers or special characters (! @ _-).
Ring Type	ERPS instance ring network type, the options are as follows: • Major-ring: main ring, closed ring. • Sub-ring: a sub-ring, an unclosed ring, forms a multi-ring network such as an intersecting ring with the main ring.
Ring Name	ERPS Ring Name. Note: The ring name should be created in advance in ERPS "Ring Network Configuration", and the ring network port should be specified.
Instance ID	The ID of ERPS protection instance, its value range is 0-16. The VLAN in which RAPS PDUs and data packets are transmitted must be mapped to an Ethernet Ring Protection (ERP) instance so that ERPS forwards or blocks the packets based on configured rules. Note: • By default, all VLAN in MST domain are mapped to instance 0. • The mapping with VLAN instance can be created in spanning tree instance configuration.
Ring ID	The ID of ERPS ring network, its value range is 1-239. The ring ID is used to uniquely identify an ERPS ring, and all nodes on the same ERPS ring should be configured with the same ring ID. Note: ERPS ring ID will be the last byte of the MAC destination of the RAPS message.
Timer Name	The name of the timer, which supports the default parameter timer or customization in the timer configuration.
RPL Role	Each device in ERPS ring is called a node. The node role is decided by user configuration, they are divided into following types: • owner: owner node is responsible for blocking and unblocking the port in RPL of the node to prevent loop forming and conduct link switching. • neighbor: neighbor node is connected to Owner node on RPL. Cooperating to the Owner node, it blocks and unblocks the ports on RPL of the node and conduct link

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	switching. • non-owner: non-owner node is responsible for receiving and forwarding the protocol packet and data packet in the link.
RPL-Port	Port connected by RPL link, the options are as follows: • West-interface • East-interface
Topology Change Announcement	Notify the network topology change of this ERPS ring to other ERPS rings, and the enabling status is as follows: • Enable • Disable：disable
Manage VLAN	The VLAN channel of protocol packet, its value range is 1-4094.
Level	ERPS ring network level, the value range is 0-7. The higher the ring network level, the greater the value. When the R-APS message needs to be transmitted across the ring, it can only be crossed by the ring with high rank to low rank.
State	The instance statuses of ERPS are as follows: • ERPS_INIT: initial state, which is the initialized state when the protocol starts. • ERPS__IDLE: idle state, it would enter this state when the ring topology is complete; • ERPS_FS: force-switch state, it would enter this state when force-switch command is implemented. • ERPS_MS: manual-switch state, it would enter this state when manual-switch command is implemented. • ERPS_PROTECTION: protection state, it would enter this state when the ring link has failure. • ERPS_PENDING: pending state, it would enter this state when the ring link has recovered from failure.
Start	ERPS instance startup status: • start • stop

3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.

5.7 IGMP-Snooping

IGMP Snooping (Internet Group Management Protocol Snooping) is an IPv4 layer 2 multicast Protocol. It maintains the egress interface information of Group broadcast by snooping for the multicast protocol messages sent between the layer 3 multicast device and the user host, so as to manage and control the forwarding of multicast data message in the data link layer.

5.7.1 Global Configuration

Function Description

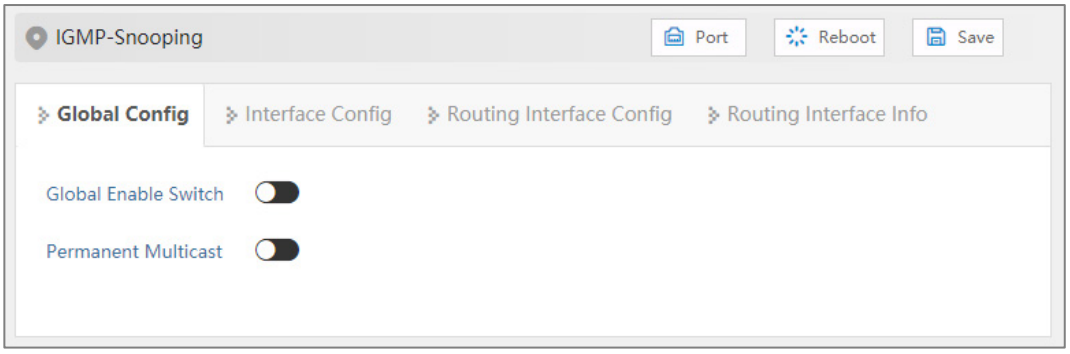
Enable/disable IGMP-Snooping and resident multicast.

Operation Path

Open in order: "Layer 2 Configuration > IGMP-Snooping > Global Configuration".

Interface Description

Global configuration interface is as follows:



The main element configuration description of global configuration interface:

Interface Element	Description
Global Enable Switch	Global enable configuration of IGMP-Snooping. By enabling IGMP Snooping, layer 2 devices can dynamically establish layer 2 multicast forwarding entries by listening to the IGMP protocol messages between the IGMP querier and the user host, thus realizing layer 2 multicast.
Permanent Multicast	Do not age the received IGMP report member groups.

3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.

5.7.2 Interface Configuration

Function Description

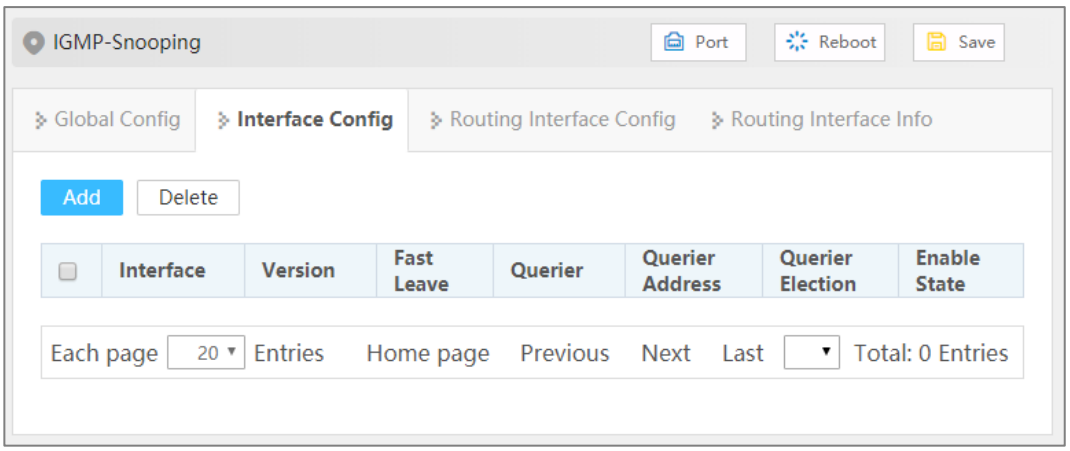
Configure parameters related to IGMP Snooping of VLANIF interface.

Operation Path

Open in order: "Layer 2 Config > IGMP-snooping > Interface Config".

Interface Description

Interface configuration interface as follows:



The main element configuration description of interface configuration interface:

Interface Element	Description
Interface	VLANIF interface, the value range is 1-4094.
Version	Different versions of IGMP Snooping can handle corresponding versions of IGMP protocol. IGMP Snooping protocol version, with the following options: • 1 • 2 • 3
Fast Leave	The enabled state of the multicast group fast leave. After enabling fast leave, when the switch receives the IGMP Leave message sent by the host from a certain port and leaves a certain multicast group, it directly deletes the port from the multicast forwarding table without waiting for the port aging, which can save bandwidth and resources. Note: When there are multiple receivers under the port, this function will cause other receivers in the same multicast group to interrupt

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	receiving multicast data. It is recommended to configure this function on a port with only one receiver connected.
Querier	Enable status of IGMP Snooping inquirer. After the IGMP Snooping querier function is enabled, the switch will regularly send IGMP querier messages to all interfaces (including router ports) in the VLAN by broadcast. If the IGMP querier already exists in the multicast network, it will cause the IGMP querier to be re-elected.
Querier Address	The source IP address of IGMP Snooping querier when sending inquiry message.
Querier Election	Enable election status of IGMP Snooping querier. IGMPv2 uses an independent inquirer election mechanism. When there are multiple multicast routers on the shared network segment, the router with the smallest IP address becomes an inquirer, while the non-inquirer no longer sends universal group inquiry messages.
Enable State	IGMP Snooping enable status, enabling IGMP snooping on global or VLAN interface. Note: Only when IGMP snooping is enabled on the global and VLAN interfaces can the configuration of the other IGMP snooping properties on that interface take effect.

5.7.3 Routing Port Configuration

Function Description

Configure multicast router ports.

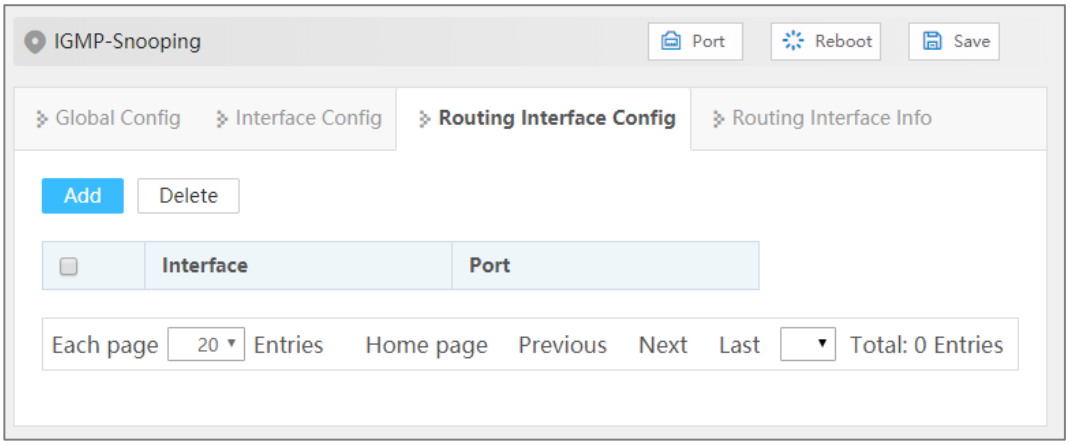
Operation Path

Open in order: "Layer 2 Config > IGMP Snooping > Routing Port Configuration".

Interface Description

Routing port configuration interface is as below:

Copyright © 3onedata Co., Ltd.



Main elements configuration description of routing port configuration interface:

Interface Element	Description
Interface	VLANIF interface, the value range is 1-4094.
Port	The static router port in VLAN is generally the interface of Layer 2 device towards the upstream Layer 3 multicast device. If it is necessary to forward the IGMP Report/Leave message from an interface to the upstream IGMP querier stably for a long time, the interface can be configured as a static router port.

5.7.4 Routing port information

Function Description

Check the router port information of IGMP Snooping in VLAN, including static router port and dynamic router port.

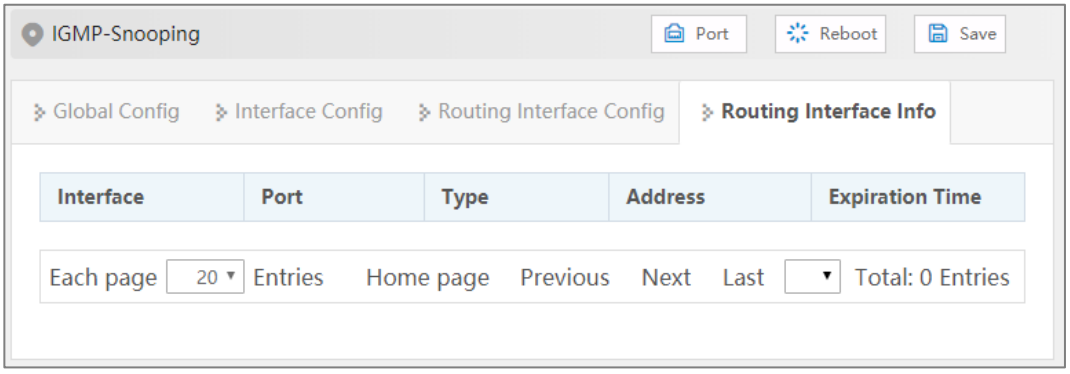
Operation Path

Open in order: "Layer 2 Config > IGMP Snooping Configuration > Routing Port Information".

Interface Description

Routing port information interface is as follows:

Copyright © 3onedata Co., Ltd.



Configuration description of main elements of routing port information interface:

Interface Element	Description
Interface	VLANIF interface, the value range is 1-4094.
Port	Router port in VLAN.
Type	The type of router port, including dynamic and static.
Address	IP Address.
Expiration Time	The remaining aging time of dynamic router port.

5.8 IPv6 MLD-Snooping

MLD Snooping (Multicast Listener Discovery Snooping) is an IPv6 layer 2 multicast Protocol. It maintains the egress port information of Group broadcast by snooping for the multicast protocol messages sent between the layer 3 multicast device and the user host, so as to manage and control the forwarding of multicast data message in the data link layer.

5.8.1 Global Configuration

Function Description

Enable/disable Mld-Snooping and resident multicast.

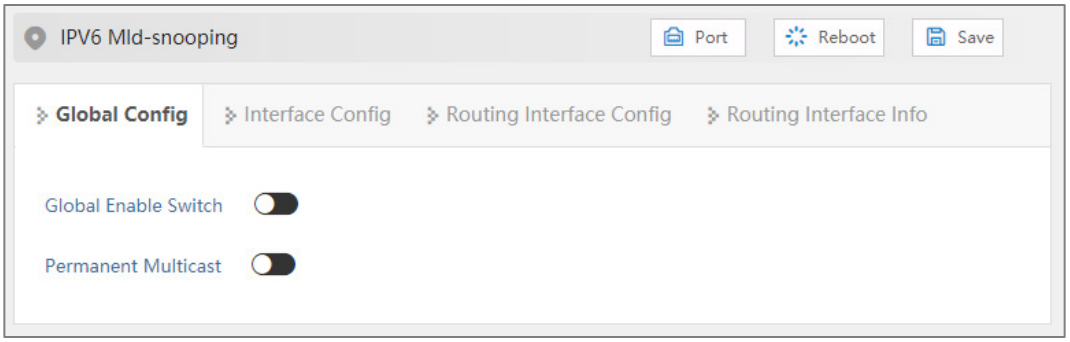
Operation Path

Open in order: "Layer 2 Configuration > MLD-Snooping Configuration > Global Configuration".

Interface Description

Global configuration interface is as follows:

Copyright © 3onedata Co., Ltd.



The main element configuration description of global configuration interface:

Interface Element	Description
Global Enable	Global enable configuration of MLD-Snooping. By enabling MLD Snooping, layer 2 devices can dynamically establish layer 2 multicast forwarding entries by listening to the MLD protocol messages between the MLD querier and the user host, thus realizing layer 2 multicast.
Permanent Multicast	Configure the multicast group as a resident multicast group without aging or leaving.

5.8.2 Interface Configuration

Function Description

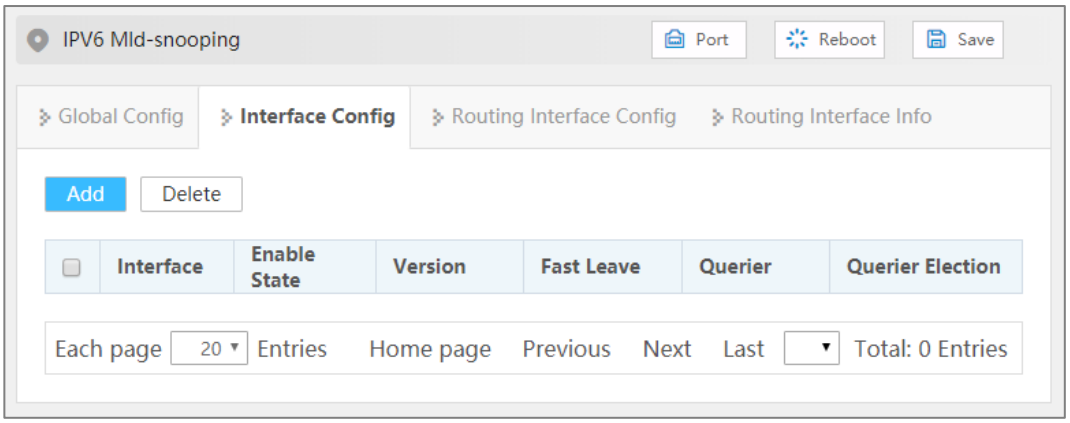
Configure parameters related to MLD Snooping of VLANIF interface.

Operation Path

Open in order: "Layer 2 Config > MLD-Snooping > Interface Config".

Interface Description

Interface configuration interface as follows:



Copyright © 3onedata Co., Ltd.

The main element configuration description of interface configuration interface:

Interface Element	Description
Interface	VLANIF interface, the value range is 1-4094.
Enable State	MLD Snooping enable status, enabling MLD snooping on global or VLAN interface. Note: Only when MLD snooping is enabled on the global and VLAN interfaces can the configuration of the other MLD snooping properties on that interface take effect.
Version	Different versions of MLD Snooping can handle corresponding versions of MLD protocol. MLD Snooping protocol version, with the following options: • 1 • 2
Fast Leave	The enabled state of the multicast group fast leave. After enabling fast leave, when the switch receives the MLD Done message sent by the host from a certain port and leaves a certain multicast group, it directly deletes the port from the multicast forwarding table without waiting for the port aging, which can save bandwidth and resources. Note: When there are multiple receivers under the port, this function will cause other receivers in the same multicast group to interrupt receiving multicast data. It is recommended to configure this function on a port with only one receiver connected.
Querier	Enable status of MLD Snooping inquirer. After the MLD Snooping querier function is enabled, the switch will regularly send MLD querier messages to all interfaces (including router ports) in the VLAN by broadcast. If the MLD querier already exists in the multicast network, it will cause the MLD querier to be re-elected.
Querier Election	Enable election status of MLD Snooping querier. When there are multiple multicast routers on the shared network segment, the router with the smallest IPv6 address becomes an inquirer, while the non-inquirer no longer sends universal group inquiry messages.

3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.

5.8.3 Routing Port Configuration

Function Description

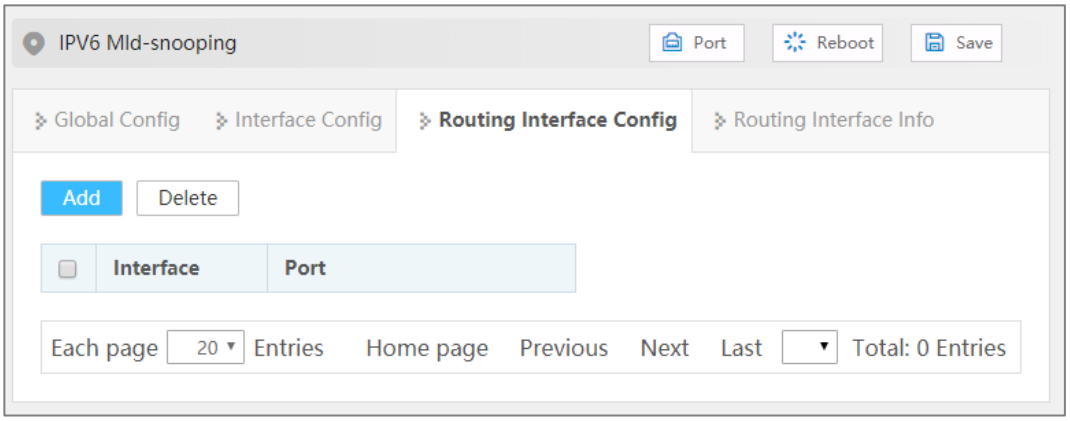
Configure multicast router ports.

Operation Path

Open in order: "Layer 2 Config > Mld-Snooping> Routing Port Configuration".

Interface Description

Routing port configuration interface is as below:



Main elements configuration description of routing port configuration interface:

Interface Element	Description
Interface	VLANIF interface, the value range is 1-4094.
Port	The static router port in VLAN is generally the interface of Layer 2 device towards the upstream Layer 3 multicast device. When it is necessary to receive and forward multicast data from an interface stably for a long time, the interface can be configured as a static router port.

5.8.4 Routing port information

Function Description

Check the router port information of MLD Snooping in VLAN, including static router port and dynamic router port.

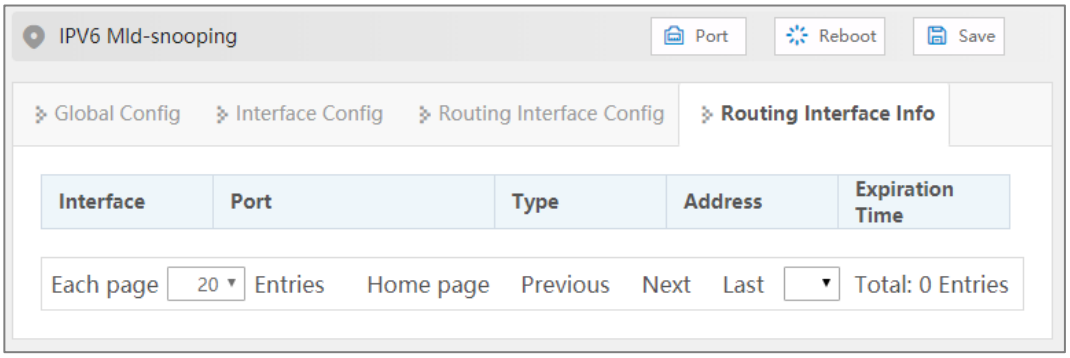
Operation Path

Open in order: "Layer 2 Config > IGMP Snooping > Routing Port Information".

Copyright © 3onedata Co., Ltd.

Interface Description

Routing port information interface is as follows:



Configuration description of main elements of routing port information interface:

Interface Element	Description
Interface	VLANIF interface, the value range is 1-4094.
Port	Router port in VLAN.
Type	The type of router port, including dynamic and static.
Address	IP Address.
Expiration Time	The remaining aging time of dynamic router port.

5.9 Link Flapping Protection

Network jitter or network cable failure will cause frequent Up/Down changes in the physical state of device interface, which will lead to link flapping and frequent changes in network topology, thus affecting user communication. For example, in the application of active-standby link, when the physical Up/Down state of the main link interface changes frequently, the service will switch back and forth between the active-standby link, which will not only increase the device burden, but also cause the loss of service data.

In order to solve the above problems, users can configure the link flapping protection function, and close the interface whose physical Up/Down state changes frequently to keep it remain Down, so that the network topology will stop changing frequently back and forth.

3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.

5.9.1 Global Configuration

Function Description

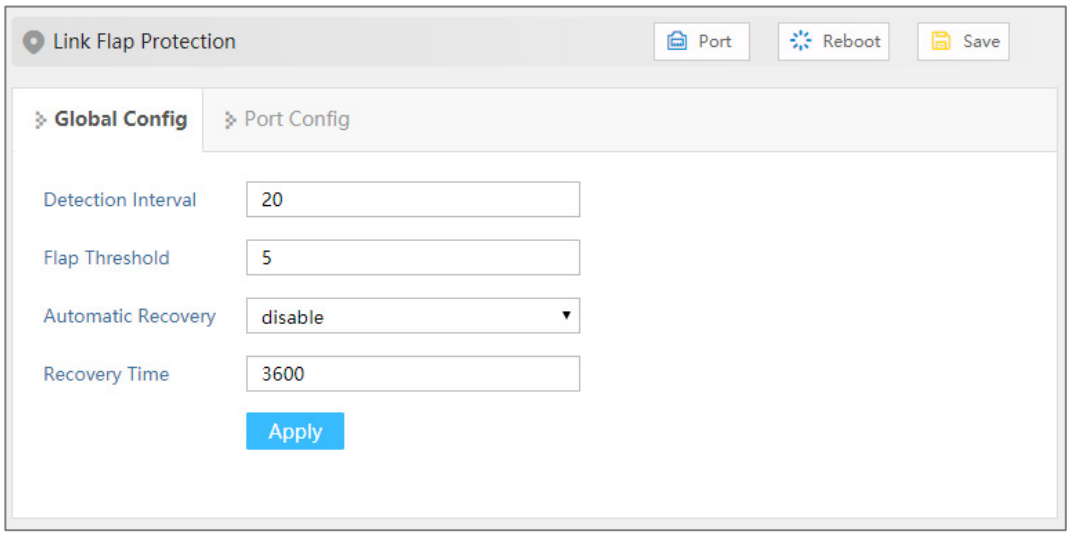
Configure relative parameters of link flapping protection.

Operation Path

Open in order: "Layer 2 Configuration > Link Flapping Protection > Global Configuration".

Interface Description

Global configuration interface is as follows:



The main element configuration description of global configuration interface:

Interface Element	Description
Detection Interval	The value range of link detection interval is 10-100s, and the default value is 20s.
Flap Threshold	The threshold value of the number of oscillations detected by the link. If the number of oscillations exceeds the threshold value within the time specified by the "detection interval", an alarm log will be generated and the port will be set to shutdown. The range is from 3 to 100, default value is 5.
Automatic Recovery	Automatic recovery enable configuration. After being enabled, the port will automatically return to normal within the specified time.
Recovery Time	The value range of the time when the port automatically returns to normal is 30-86400s, and the default value is

3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.

Interface Element	Description
	3600s.

5.9.2 Port Configuration

Function Description

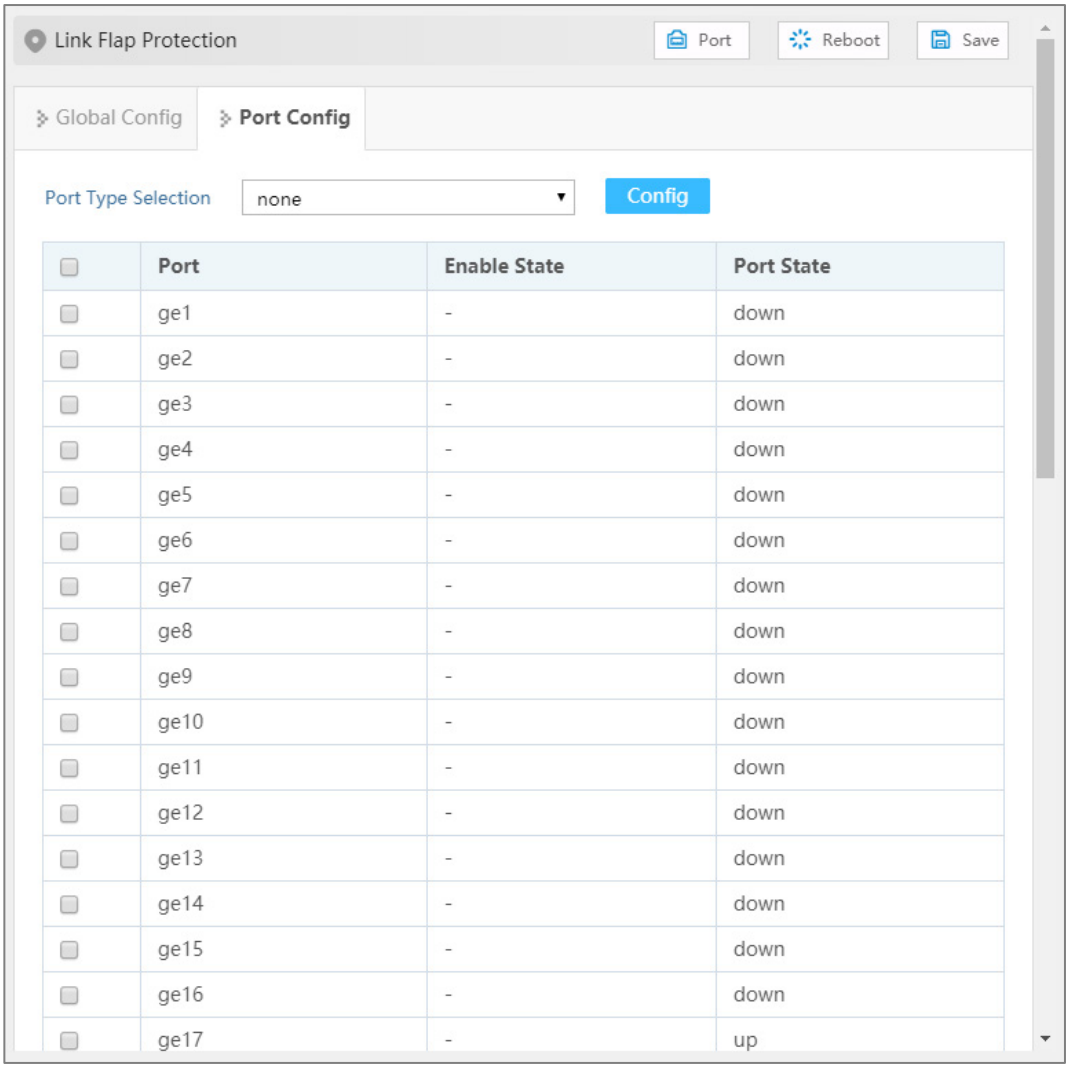
Enable link flap protection for this port.

Operation Path

Open in order: "Layer 2 Configuration > Link Flap Protection > Port Configuration".

Interface Description

Check port configuration interface as below:



The main element configuration description of port configuration interface:

Copyright © 3onedata Co., Ltd.

Interface Element	Description
Port	The corresponding port number of this device's Ethernet port.
Enable State	The enable status of port link flapping protection can be shown as follows: • ON: means enabled; • -:means disable
Port State	Ethernet port connection status, display as follows: • down: the port is not connected or forced to shutdown • up: port is connected.

5.10 Port Loopback Detection

The function of loop detection is to detect whether loop exists in external network of single port of switch. If it does, it would lead to address learning errors and broadcast storm easily, even switch and network breakdown in severe case. The influence created by port loop could be effectively eradicated when enabling port protocol and closing port with loop.

Function Description

Enable port loop detection.

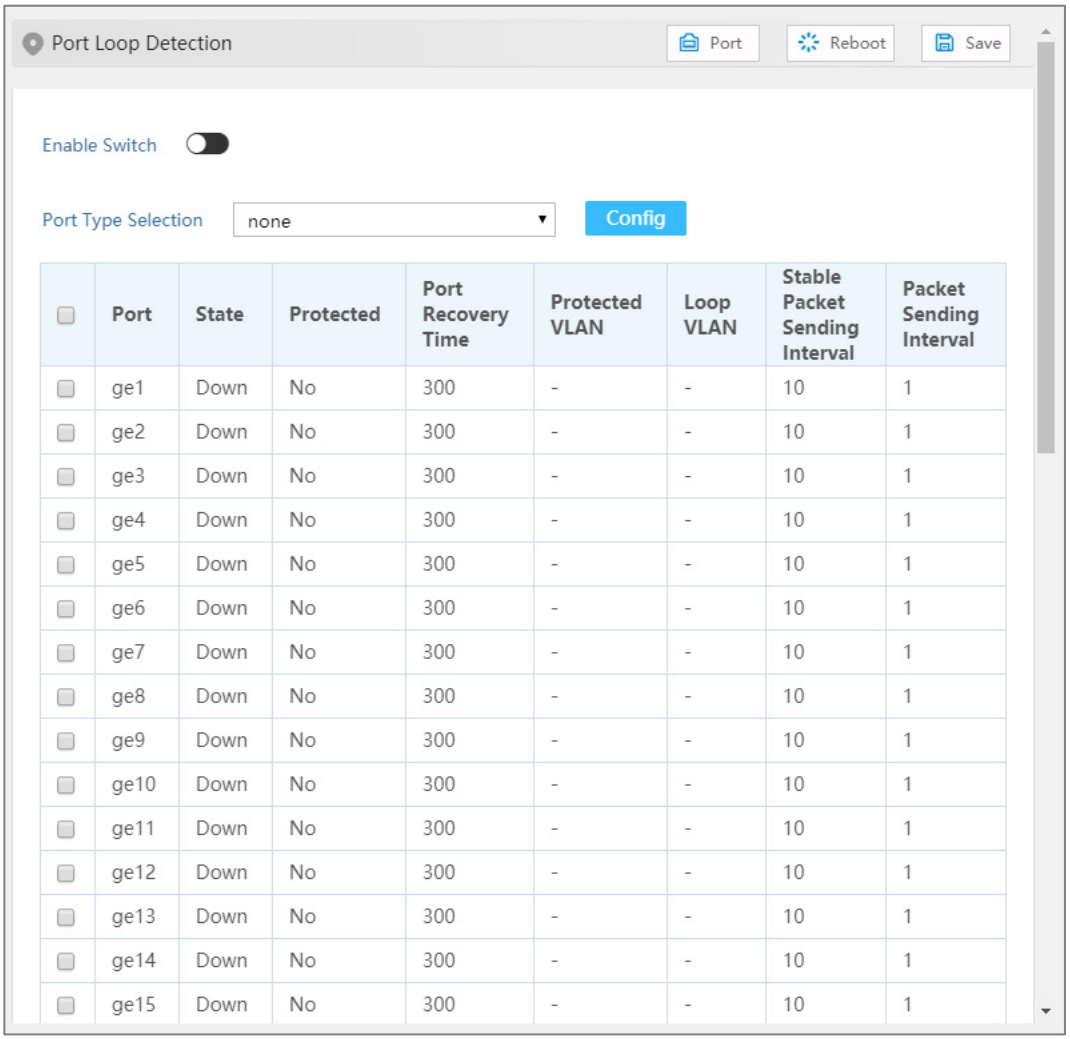
Operation Path

Open in order: "Layer 2 Config > Port Loop Detection".

Interface Description

Port loop detection interface is as follows:

Copyright © 3onedata Co., Ltd.



Port	State	Protected	Port Recovery Time	Protected VLAN	Loop VLAN	Stable Packet Sending Interval	Packet Sending Interval
ge1	Down	No	300	-	-	10	1
ge2	Down	No	300	-	-	10	1
ge3	Down	No	300	-	-	10	1
ge4	Down	No	300	-	-	10	1
ge5	Down	No	300	-	-	10	1
ge6	Down	No	300	-	-	10	1
ge7	Down	No	300	-	-	10	1
ge8	Down	No	300	-	-	10	1
ge9	Down	No	300	-	-	10	1
ge10	Down	No	300	-	-	10	1
ge11	Down	No	300	-	-	10	1
ge12	Down	No	300	-	-	10	1
ge13	Down	No	300	-	-	10	1
ge14	Down	No	300	-	-	10	1
ge15	Down	No	300	-	-	10	1

The main element configuration description of port loop detection interface:

Interface Element	Description
Enable	Global enable configuration of port loop detection.
Port	The corresponding port number of this device's Ethernet port.
State	The connection status of this port, values are: • Down: the port is physically disconnected • Up: the port is connected • Shutdown: the port is closed • No Shutdown: the port is not closed
Protected	The protected status of the port can be shown as follows: • Yes • No
Port Recovery Time	The delay time for the shutdown port to automatically return to normal after detecting the loop, ranging from 300-776000 seconds.
Protected VLAN	The VLAN ID of loop protection. The value range: 1-4094, the

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	number of VLAN ID is ≤16. Note: This parameter must be configured, otherwise there would be errors in down sending the data.
Loop VLAN	The VLAN ID of the currently generated loop.
Stable Packet Sending Interval	The normal interval time of loop detection data packet sending, value range: 10-300 seconds.
Packet Sending Interval	After the port is connected, the interval between sending loop detection packets. In this interval, three detection messages will be sent out, and then the packet-sending interval will return to the normal packet-sending interval.

5.11 IPDT

Function Description

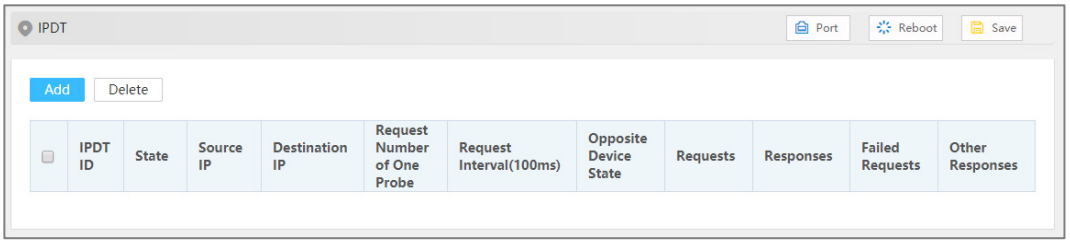
Configure IPDT (IP Detection) to detect the specified destination address (ICMP) and link it with other functions, such as VRRP.

Operation Path

Open in order: "Layer 2 Configuration > IPDT".

Interface Description

IPDT interface is as below:



Main elements configuration descriptions of IPDT interface:

Interface Element	Description
IPDT ID	IPDT session ID, value range 1-8.
State	IPDT function enable status.
Source IP	The source IP address that sends ICMP probe packet.
Dest IP	Destination IP address of ICMP probe packet.
Request Number of	The number of request packets sent by each probe, the

Copyright © 3onedata Co., Ltd.

Interface Element	Description
One Probe	value range is 1-3.
Request interval (100ms)	The time interval of each probe request, the unit is 100ms, with a value range of 5-15.
Opposite Device State	The status of the opposite device is shown as follows: • UP: the opposite end device is online normally. • DOWN: there is no response from the opposite end device, which may lead to device disconnection or link failure. • not be detected.
Requests	Display the number of probe packets sent.
Response	Display the number of probe packets answered by the destination IP.
Failed requests	Displays the number of requests that failed.
Other responses	Displays the number of probe packets responded by other devices.

5.12 IPv6DT

Function Description

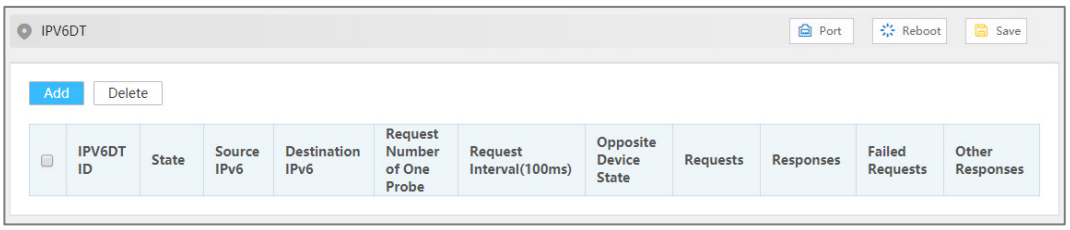
Configure IPv6DT (IPv6-Detection) to detect the specified destination IPv6address (ICMPv6) and link it with other functions, such as IPv6 VRRP.

Operation Path

Open in order: "Layer 2 Configuration > IPv6DT".

Interface Description

The IPv6DT interface is as follows:



Main elements configuration descriptions of IPv6DT interface:

Interface Element	Description
IPV6DT ID	IPv6DT session ID, value range 1-8.

Copyright © 3onedata Co., Ltd.

Interface Element	Description
State	IPv6DT function enable status.
Source IPv6	The source IPv6 address that sends ICMPv6 probe packet.
Destination IPv6	Destination IPv6 address of ICMPv6 probe packet.
Request Number of One Probe	The number of request packets sent by each probe, the value range is 1-3.
Request Interval (100ms)	The time interval of each probe request, the unit is 100ms, with a value range of 5-15.
Opposite Device State	The status of the opposite device is shown as follows: • UP: the opposite end device is online normally. • DOWN: there is no response from the opposite end device, which may lead to device disconnection or link failure. • not be detected.
Requests	Display the number of probe packets sent.
Response	Display the number of probe packets answered by the destination IPv6.
Failed requests	Displays the number of requests that failed.
Other responses	Displays the number of probe packets responded by other devices.

5.13 Smart-link

Smart Link, also known as backup link. A Smart Link consists of two interfaces, one of which is the backup of the other. Smart Link is commonly used in dual uplink networking, providing reliable and efficient backup and fast switching mechanism.

5.13.1 Global Configuration

Function Description

Configure Smart-link related parameters.

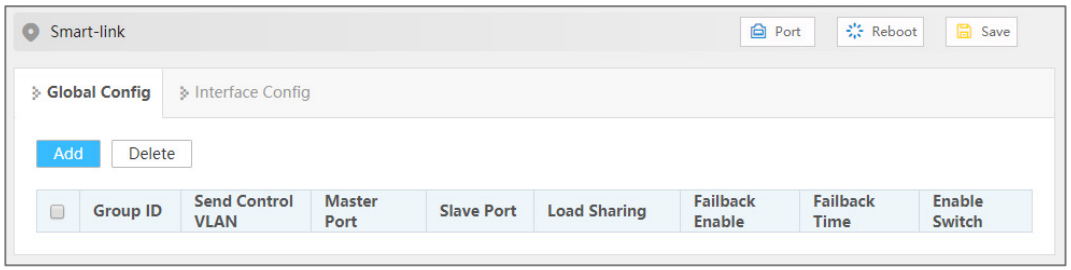
Operation Path

Open in order: "Layer 2 Config > Smart-link > Global Config".

Interface Description

Global configuration interface is as follows:

Copyright © 3onedata Co., Ltd.



The main element configuration description of global configuration interface:

Interface Element	Description
Group ID	Smart Link Group ID, the value range is 1-16.
Send Control VLAN	Sending control VLAN is the VLAN used by Smart Link group to broadcast Flush message, and its value range is 1-4094. When Smart Link switches links, Smart Link notifies related devices to refresh MAC table and ARP table entries by sending Flush message. Note: • If the sending control VLAN is configured, the peer device needs to configure the receiving control VLAN. • Different device manufacturers may have different definitions of Flush message format, so it is recommended to use this function between the device of the same manufacturer.
Master Port	When both interfaces in the Smart Link group are in the Up state, the master interface will enter the forwarding state first, while the slave interface will remain in the standby state. Note: Smart Link group port cannot be used as a member port of ring network, aggregation group, etc.
Slave Port	Slave interfaces in the Smart Link group will be blocked after the Smart Link group is started. When the link where the master interface is located fails, the slave interface will switch to the forwarding state.
Load Sharing	Load sharing instance ID, the value range is 0-16. In the load sharing mode, the backup link forwards the VLAN data traffic mapped in the specified load sharing instance, which can improve the utilization rate of the link.
Failback Enable	When the original main link recovers from faults, it will remain at the block state to keep the traffic stable without preemption. If you need to restore it to the main link, you can enable the failback function of the Smart Link group, the main link would

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	be automatically switched after the failback timer expires. Switch-back enable status, which can be displayed as follows: • Enable • Disable：disable
Failback Time	Failback delay time, it can inhibit Smart Link switching caused by link flash, the value range is 30~1200 seconds.
Enable	Smart Link function enable status can be displayed as follows: • Enable • Disable：disable

5.13.2 Interface Configuration

Function Description

Configure Smart-link interface to receive control VLAN.

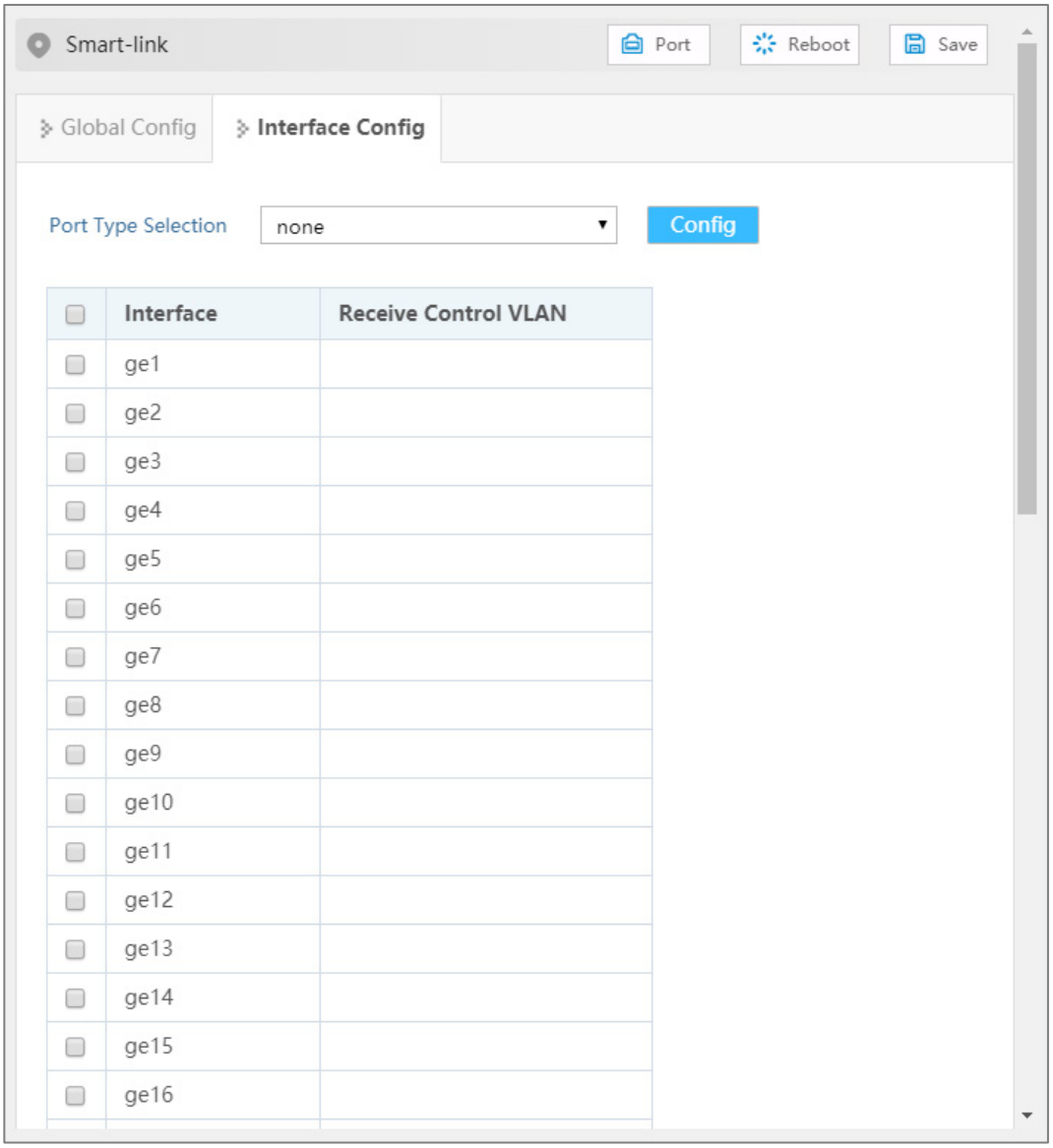
Operation Path

Open in order: "Layer 2 Config > Smart-link > Interface Config".

Interface Description

Interface configuration interface as follows:

3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.



The main element configuration description of interface configuration interface:

Interface Element	Description
Interface	The corresponding port number of this device's Ethernet port.
Receive Control VLAN	Receive control VLAN is used to receive and handle the VLAN of Flush messages, the value range is 1-4094. When Smart Link has switched links, the device would handle the Flush messages received that belong to receive control VLAN, thus refreshing MAC table and ARP table.

Copyright © 3onedata Co., Ltd.

6 IP Network Setting

6.1 Interface

6.1.1 Layer 3 Interface

Function Description

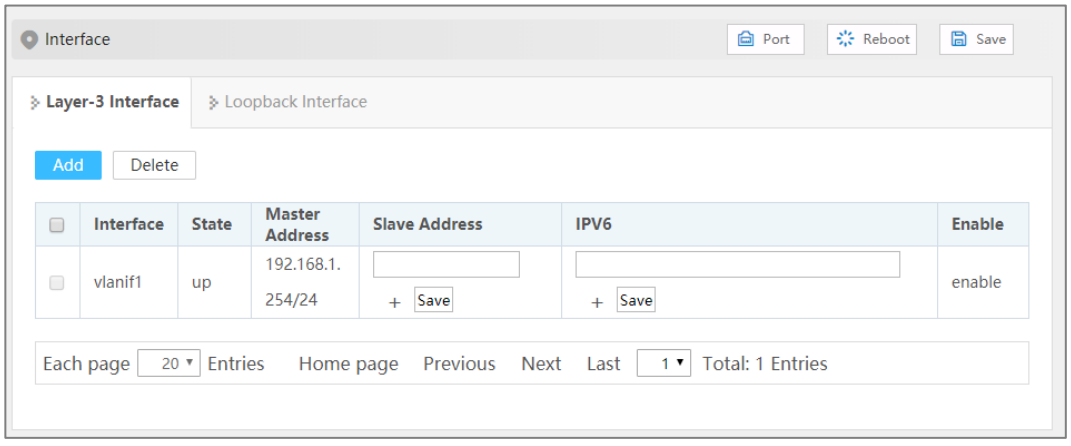
Create layer 3 VIANIF Interfaces and configure interface IP address.

Operation Path

Open in order: "IP Network Configuration > Interface > L3 Interface".

Interface Description

L3 interface configuration interface as follows:



The main element configuration description of interface configuration interface:

Interface Element	Description
Interface	VLANIF interface, the value range is 1-4094. VLANIF interface is a logical interface with layer 3 features that can be

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	used to realize inter-VLAN access and Layer 3 task deployment by configuring the IP address of VLANIF Interfaces.
State	The connection state of the VLANIF port, which can be displayed as follows: • Up: connection is normal. • Down: disconnected
Master Address	Master IPv4 address and subnet mask of VLANIF interface, such as 192.168.1.1/24.
Slave Address	Slave IPv4 address and subnet mask of VLANIF interface, such as 192.168.8.1/24. In order to connect one interface of the switch with multiple subnets, user can configure multiple IP addresses on one interface, one as the master IP address and the rest as the slave IP address.
IPV6	Ipv6 address and prefix length of VLANIF interface, such as 1::1/127.
Enable	The VLANIF interface enabled status can be displayed as follows: • enable • disable

6.1.2 Loopback Interface

Loopback interface is virtual interface, and most of the platforms support using it to simulate real interface. This interface is in virtual forever UP state, which is more stable than any other physical interface. As long as the router starts, the loopback interface would be in an active state. If there are multiple routes that arrive at this loopback address, they would not be unreachable when one of the interface of the device is down. It only be invalid when the router no longer has effect.

Function Description

Configure the parameters of loopback interface.

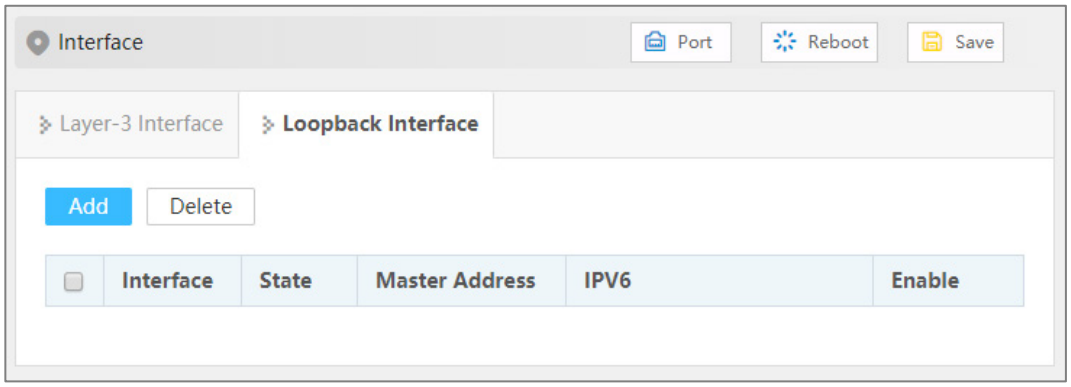
Operation Path

Open in order: "IP Network Configuration > Interface > Loopback Interface".

3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.

Interface Description

Loopback interface configuration interface as follows:



The main element configuration description of loopback interface interface:

Interface Element	Description
Interface	The name of loopback interface, value range: loopback0 or loopback1.
State	The connection state of the loopback Interface, which can be displayed as follows: • Up • Down
Master Address	Master IPv4 address and subnet mask of loopback interface, such as 10.1.1.0/24.
IPV6	Ipv6 address and prefix length of loopback interface, such as 1::1/127.
Enable	Loopback interface enable status can be displayed as follows: • enable • disable

6.2 ARP

ARP (Address Resolution Protocol) is the protocol that resolves IP address into Ethernet MAC address (or physical address).

In local area network, when the host or other network device sends data to another host or device, it must know the network layer address (IP address) and MAC address of the opposite side. So it needs a mapping from IP address to the physical address. ARP is the protocol to achieve the function.

3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.

6.2.1 ARP Information

Function Description

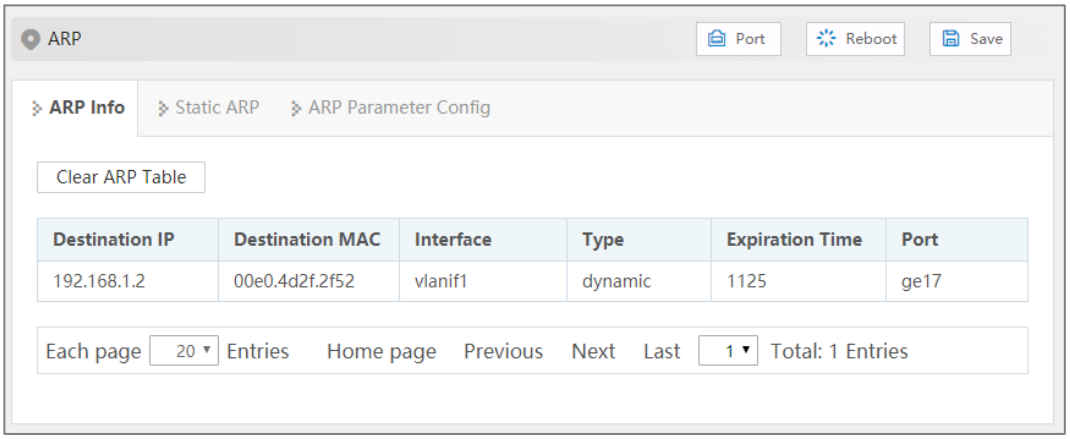
Check information such as IP address, MAC address and interface of the user via ARP table entries.

Operation Path

Open in order: "IP Network Configuration > ARP > ARP Information".

Interface Description

ARP Information interface as follow:



The main element configuration description of ARP information interface:

Interface Element	Description
Destination IP	Static binding or ARP resolves dynamically learned IP addresses.
Destination MAC	Static binding or ARP resolves dynamically learned MAC addresses.
Interface	VLANIF Interface to which ARP entry belongs.
Type	ARP table entry type, as shown below: • Static • Dynamic
Expiration Time	The remaining survive time of dynamic ARP table entries, unit: second.
Port	Ports learned to ARP table entry.

3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.

6.2.2 Static ARP

Function Description

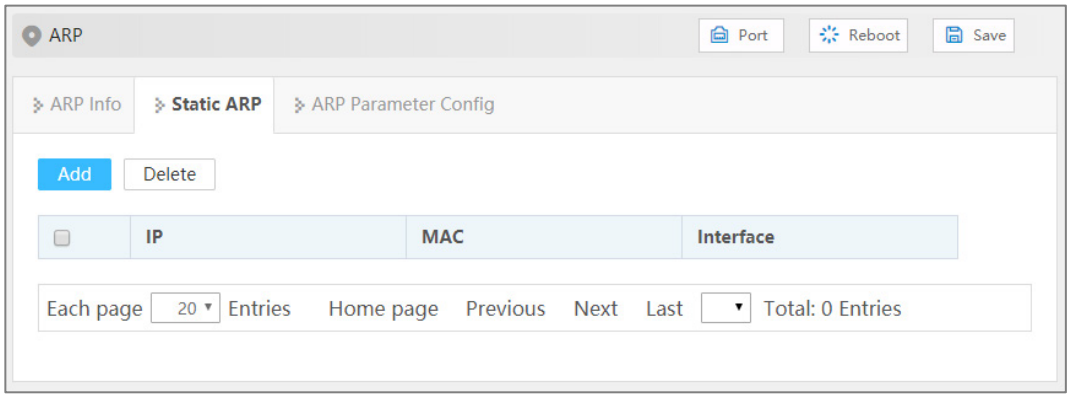
Configure static ARP entries, bind IP address and MAC address to avoid aging and prevent ARP attacks.

Operation Path

Open in order: "IP Network Configuration > ARP > Static ARP".

Interface Description

Static ARP interface as follows:



The main element configuration description of static ARP interface:

Interface Element	Description
IP	IP address of static ARP table entry, such as 192.168.1.1.
MAC	MAC address bound to static IP address such as 0001.0001.0001.
Interface	Display VLANIF Interface to which static ARP entry belongs.

6.2.3 ARP Parameter Configuration

Function Description

Configure the aging time of dynamic ARP.

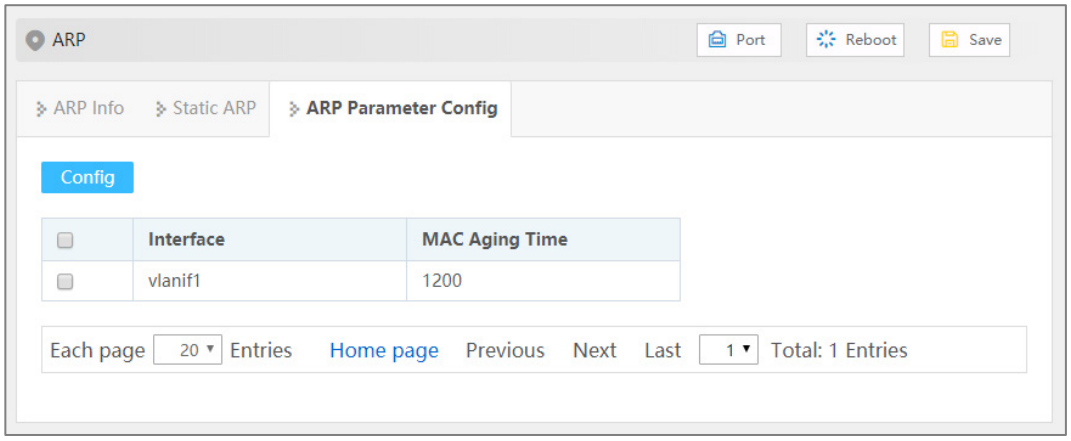
Operation Path

Open in order: "IP Network Configuration > ARP > ARP Parameters Configuration".

Interface Description

ARP parameter configuration interface as follows:

3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.



The main element configuration description of ARP age-time interface:

Interface Element	Description
Interface	Display VLANIF Interface name in ARP entry.
MAC Aging Time	Configure aging time of dynamic ARP table entries, the value range is 1-3000 seconds.

6.3 IPv4

6.3.1 IPv4 Routing Table

Function Description

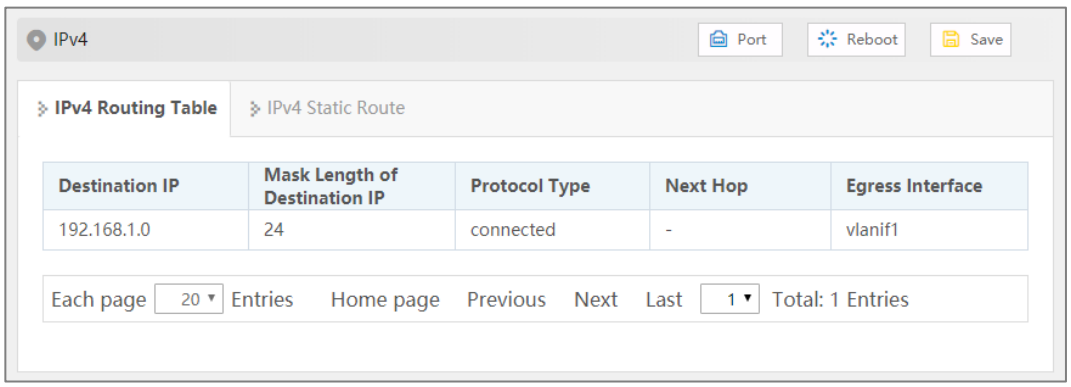
Check IPv4 routing table information.

Operation Path

Open in order: "IP Network Configuration > IPv4 > IPv4 Routing Table".

Interface Description

The IPv4 routing table interface as follows:



The main elements configuration description of IPv4 routing interface:

Interface Element	Description
Destination IP	Destination IP addresses.
Mask Length of Destination IP	The length of destination subnet mask.
Protocol Type	The routing protocol type of the current connection.
Next Hop	Gateway address information of next hop.
Egress Interface	Interface Name.

6.3.2 IPv4 Static Route

Static route refers to the route information that user or network administrator manually configures. When the network topology structure or link status changes, network administrator needs to manually modify relative static route information in the routing table. Static route usually adapts to simple network environment, under this environment, network administrator can clearly know the network topology structure, which is convenient for setting correct route information.

Function Description

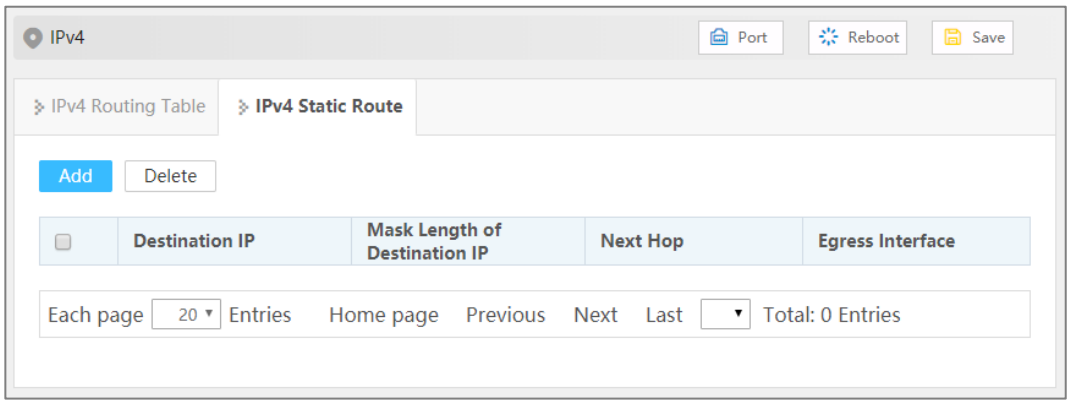
Configure IPv4 static routing.

Operation Path

Open in order: "IP Network Configuration > IPv4 > IPv4 Static Route".

Interface Description

The IPv4 Static Route interface as follows:



The main element configuration description of IPv4 Static Route interface:

Interface Element	Description

Interface Element	Description
Destination IP	Destination network IP address, such as destination address is 10.1.1.0.
Mask Length of Destination IP	Destination IP mask length. Value range is 0-32.
Next Hop	The gateway address of the next hop, format: no input or 192.3.3.3.
Egress Interface	Interface Name.

6.4 NAT

NAT(Network Address Translation) is a process of translating an IP address in an IP data header into another IP address. In practical application, NAT is mainly used to realize the function of private network accessing public network. This way of using a few public IP addresses to represent more private IP addresses will help to slow down the exhaustion of available IP address space.

Function Description

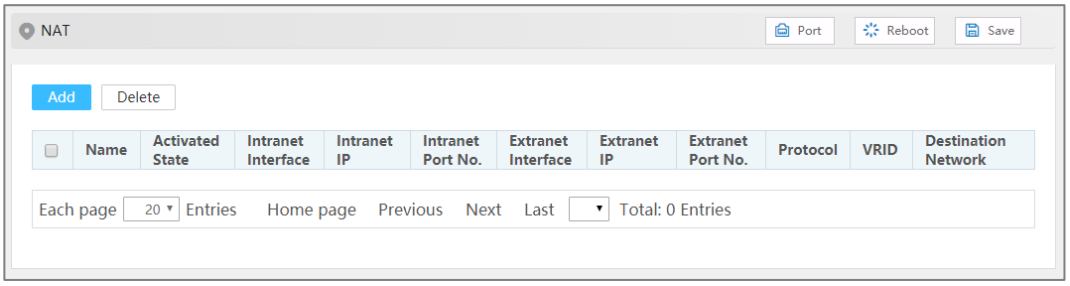
Add or delete NAT entries, and set the internal network interface and external network interface of the device.

Operation Path

Open in order: "IP Network Configuration > NAT".

Interface Description

NAT interface is as below:



Main elements configuration descriptions of NAT interface:

Interface Element	Description
Name	The NAT entry name, which supports 1-32 characters, consists of uppercase letters, lowercase letters, numbers or special characters (! @ _-).

3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.

Interface Element	Description
Activation State	Whether NAT rule is activated or not, the status is as follows: • up • down
Intranet Interface	Connect the VLAN of the intranet device, access the IP of this VLAN, and access the public network through NAT.
Intranet IP	Intranet IP that can be mapped to external network through NAT.
Intranet Port Number	Port number of intranet VLAN corresponding to port mapping protocol. Note: tcp/udp :1-65535/ no filling indicates any port; all/icmp: No distinction between port numbers.
External Network Interface	The VLAN connecting the external network device, through which the external network can access the internal network device through NAT.
Extranet IP	The external network IP mapped by the internal network IP through NAT.
Extranet Port Number	The port number of the external VLAN corresponding to the port mapping protocol. Note: tcp/udp :1-65535/ no filling indicates any port; all/icmp: No distinction between port numbers.
Protocol	Mapping port protocol, options are as follows: • All: supports tcp, udp and icmp protocol forwarding; • tcp: supports tcp protocol forwarding; • udp: supports udp protocol forwarding; • icmp: supports icmp protocol forwarding. Note: When all and icmp protocols are selected, it is not supported to input internal network port and external network port. please keep the internal network port and external network port blank.
VRID	VRID is the VRRP ID, with values ranging from 1 to 255. When the devices in the VRRP backup group are configured with the NAT address pool, it is possible for both devices to perform NAT translation on the packet, resulting in a conflict. Configuring the VRID allows you to optionally specify the Master device to do the NAT conversion, effectively avoiding collisions.
Destination Network	The destination network of internal terminal device, namely the IP address and subnet mask of the destination network,

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	such as 10.1.1.0/24.

Copyright © 3onedata Co., Ltd.

7 Unicast routing table

7.1 RIP

RIP (Routing Information Protocol) is a simple Interior Gateway Protocol (IGP) and mainly used in small network, such as Campus Network and Local Area Network with simple structure. RIP isn't used in more complex environment and large network.

RIP is simple to achieve and easier in configuration and maintenance than OSPF or IS-IS, so it's widely used in actual networking.

7.1.1 Global Configuration

Function Description

Configure RIP Global-Related parameters.

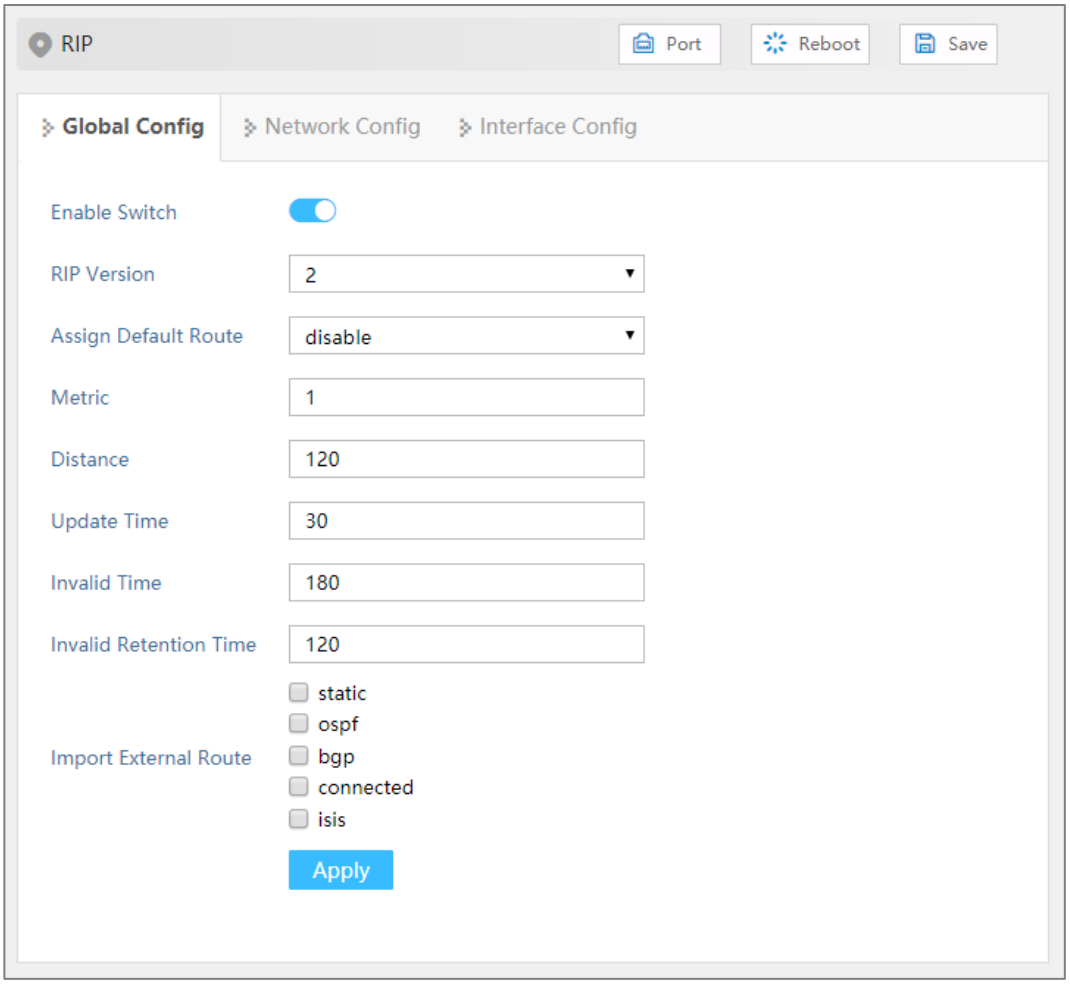
Operation Path

Open in order: "Unicast Routing > RIP > Global Configuration".

Interface Description

Global configuration interface is as follows:

3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.



The main element configuration description of global configuration interface:

Interface Element	Description
Enable	RIP function enable switch. After enabling, the RIP related parameter configuration will appear.
RIP Version	RIP version drop-down list, the default version is RIP-2, the options of version are as follows: • 1: RIP-1 is Classful Routing Protocol, it only supports releasing protocol message via broadcast mode, only natural network segments such as A, B and C can be identified. • 2: RIP-2 is a non-classified routing protocol, which is extended on the basis of RIP-1. Note: Interface can only send/receive data packets of the RIP version configured.
Assign Default Route	The default route with the destination address of 0.0.0.0 is assigned to RIP routing database, which is disabled by default. The options are as follows:

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	• enable • Disable
Metric	The metric is equal to the number of devices from this route to the destination route, with a default value of 1 and a value range of 1-15.
Distance	RIP route management distance, the default distance is 120, the value range is 1-255. When there are routes from two different routing protocols to the same destination, the smaller the management distance value of the routing protocol is, the more reliable the route obtained by the protocol is.
Update Time	Routing information update time. When the timer timeout, immediately send update message, update messages are sent every 30 seconds by default. Value range is 5-2147483647 seconds. Note: When the routing information changes, the trigger update message is immediately sent to the neighbor device instead of waiting for the update timer timeout, thus avoiding the routing loop.
Invalid Time	If no routing update message is received from the neighbor within the invalid time, the route is considered unreachable. By default it is 180 seconds, value range is 5-2147483647 seconds.
Invalid Retention Time	If the unreachable route does not receive an update message from the same neighbor before the invalid retention timer countdown ends, the route will be completely deleted from the RIP routing table. By default it is 120 seconds, value range is 5-2147483647 seconds.
Import External Route	To reallocate routes learned from other routing protocols to RIP, options are as follows: • static: static routing • ospf: Open Shortest Path First • bgp: border gateway protocol. • connected：connected route • isis: intermediate system to intermediate system IS-IS is an internal gateway protocol.

Copyright © 3onedata Co., Ltd.

7.1.2 Network Configuration

Function Description

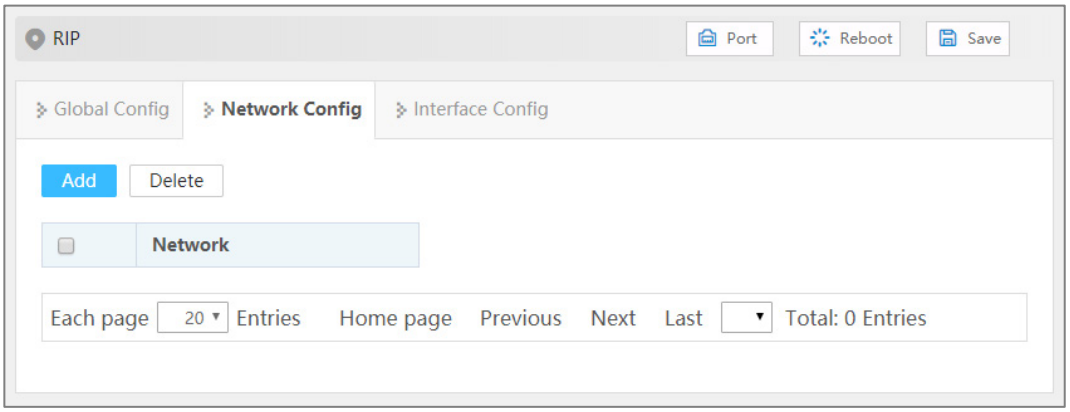
Configure RIP working network segment.

Operation Path

Open in order: "Unicast Routing > RIP > Network Configuration".

Interface Description

Network configuration interface as follows:



The main element configuration description of network configuration interface:

Interface Element	Description
Network	Network segment running RIP protocol.

7.1.3 Interface Configuration

Function Description

Configure RIP interface parameters.

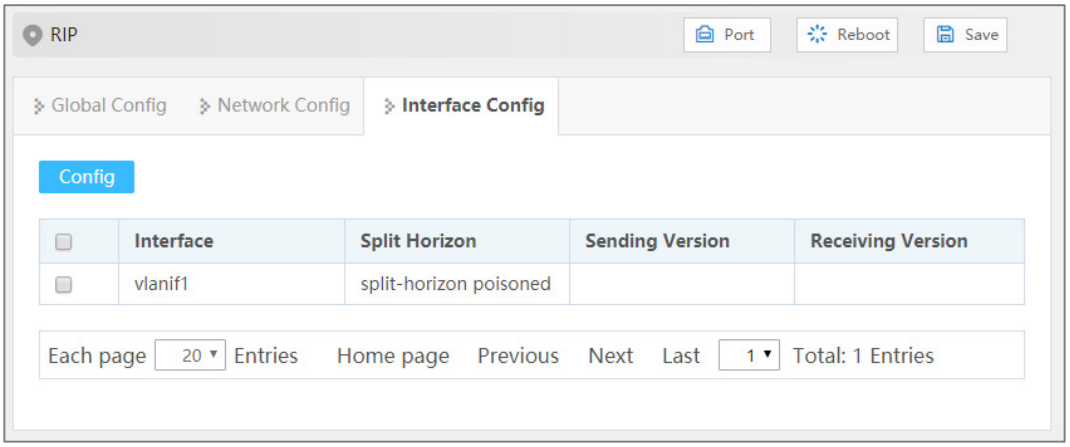
Operation Path

Open in order: "Unicast Routing > RIP > Interface Configuration".

Interface Description

Interface configuration interface as follows:

Copyright © 3onedata Co., Ltd.



The main element configuration description of interface configuration interface:

Interface Element	Description
Interface	RIP interface information.
Split Horizon	Horizontal partition. Options are as follows: • - • Split-horizon Route that RIP learns from an interface, it won't be sent from the interface to neighbor router. • Poison-reverse When RIP learns the route from an interface, it sets the routing metric to unreachable and sends it back to the neighbor router from the original interface.
Sending Version	RIP protocol version of sending data, options as follows: • - • 1 • 2 • 1 & 2 • 1-compatible
Receiving Version	RIP protocol version of receiving data, options as follows: • - • 1 • 2 • 1 & 2

7.2 RIPNG

RIPng (RIP next generation) is a simple internal gateway protocol, and an application of RIP in IPv6 network.

Copyright © 3onedata Co., Ltd.

7.2.1 Global Configuration

Function Description

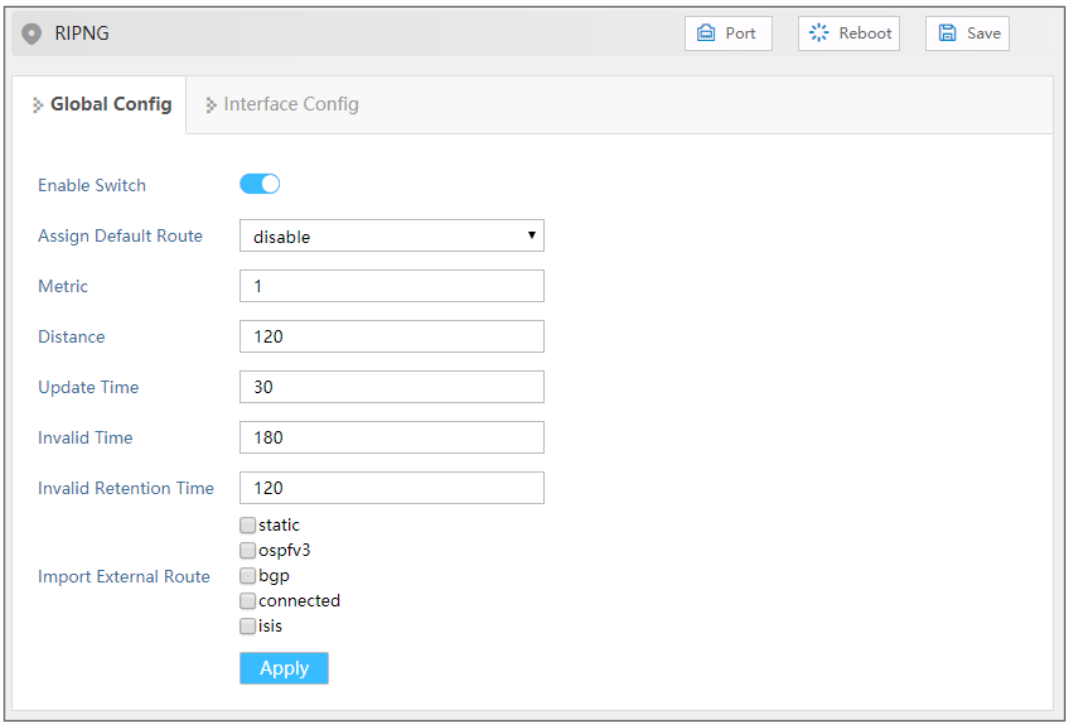
Configure RIPng global parameter.

Operation Path

Open in order: "Unicast Routing > RIPNG > Global Configuration".

Interface Description

Global configuration interface is as follows:



The main element configuration description of global configuration interface:

Interface Element	Description
Enable	RIPng enable switch, after enabling, RIPng related parameter configuration appears.
Assign Default Route	Publish RIPng default route (::/0) with the following options: • enable • Disable Note: When the destination address of the message cannot match any destination address of the routing table, the router will choose the default route to forward the message.
Metric	Default metric value used when routing to RIPng with external routing protocol. The metric is equal to the number of devices from this route to the destination route, with a default value of

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	1 and a value range of 1-16.
Distance	RIPng route management distance, the default distance is 120, the value range is 1-255. When there are routes from two different routing protocols to the same destination, the smaller the management distance value of the routing protocol is, the more reliable the route obtained by the protocol is.
Update Time	Routing information update time. When the timer timeout, immediately send update message, update messages are sent every 30 seconds by default. Value range is 5-2147483647 seconds. Note: When the routing information changes, the trigger update message is immediately sent to the neighbor device instead of waiting for the update timer timeout, thus avoiding the routing loop.
Invalid Time	If no routing update message is received from the neighbor within the invalid time, the route is considered unreachable. By default it is 180 seconds, value range is 5-2147483647 seconds.
Invalid Retention Time	If the unreachable route does not receive an update message from the same neighbor before the invalid retention timer countdown ends, the route will be completely deleted from the RIPng routing table. By default it is 120 seconds, value range is 5-2147483647 seconds.
Import External Route	To reallocate routes learned from other routing protocols to RIPng, options are as follows: • static: static routing • ospfv3: OSPFv3 route • bgp: BGP border gateway protocol • connected：connected route • isis: external gateway protocol

7.2.2 Interface Configuration

Function Description

Configure the interface parameters of RIPng

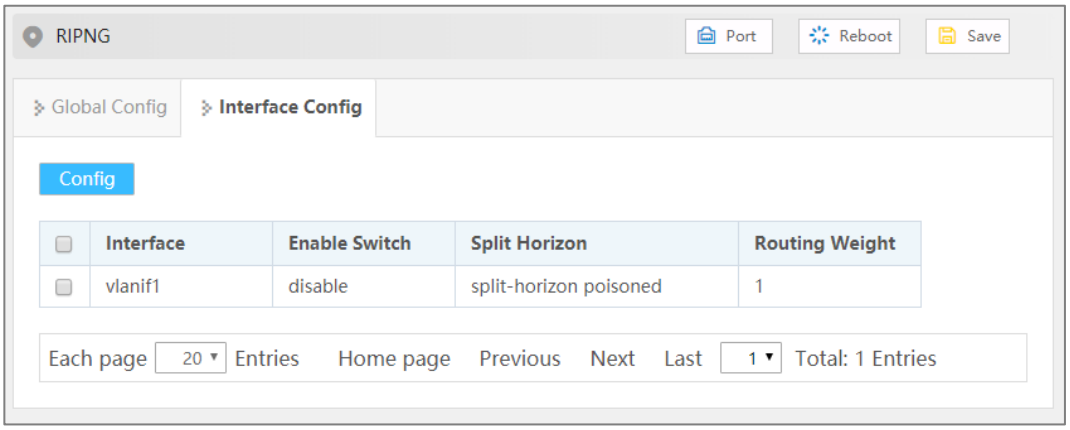
Copyright © 3onedata Co., Ltd.

Operation Path

Open in order: "Unicast Routing > RIPNG > Interface Configuration".

Interface Description

Interface configuration interface as follows:



The main element configuration description of interface configuration interface:

Interface Element	Description
Interface	RIPng interface information.
Enable Switch	RIPng enable status, options as follows: • Disable：disable • Enable
Split Horizon	Horizontal partition. Options are as follows: • Split-horizon Route that RIPng learns from an interface, it won't be sent from the interface to neighbor router. • Split-horizon poisoned When RIPng learns the route from an interface, it sets the routing metric to unreachable and sends it back to the neighbor router from the original interface.
Routing Weight	Additional routing metrics, ranging from 1 to 16. The added metric value (hop count) based on the original metric value of RIPng route can affect the route selection.

7.3 OSPF

The Open Shortest Path First (OSPF) protocol is link-state Interior Gateway Protocol (IGP) developed by the Internet Engineering Task Force (IETF).

OSPF Version 2 (RFC 2328) is currently used for the IPv4 protocol.

3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.

- Dividing an Autonomous System (AS) into one or more logical areas
- Advertising routes by sending Link State Advertisements (LSAs)
- Exchanging OSPF packets between devices in an OSPF area to synchronize routing information
- Encapsulating OSPF packets into IP packets and then sending the packets in unicast or multicast mode

RIP is a distance-vector routing protocol. Due to RIP's slow convergence, routing loops, and poor scalability, OSPF is now the most widely accepted and used IGP.

OSPF, as a link-state based protocol, can solve many problems faced by RIP. In addition, OSPF has the following advantages:

- Multicast packet transmission to reduce load on the switches that are not running OSPF
- Classless Inter-Domain Routing (CIDR)
- Load balancing among equal-cost routes
- Packet authentication

7.3.1 Global Configuration

Function Description

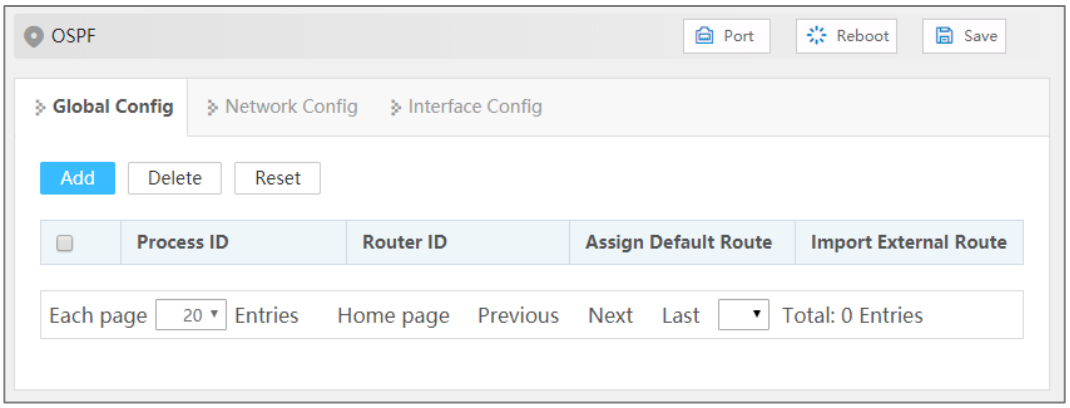
Configure OSPF process ID, router ID, default route, import external route and other information.

Operation Path

Open in order: "Unicast Routing > OSPF > Global Configuration".

Interface Description

Global configuration interface is as follows:



The main element configuration description of global configuration interface:

Interface Element	Description
Process ID	The value range of OSPF process ID is 0-65535. OSPF supports multi-processes, and many different OSPF processes can run on the same router, which do not affect each other and are independent of each other. An interface of a router can only call one OSPF process.
Router ID	Router ID is used to uniquely identify a router running OSPF in the autonomous system. The format of ID is the same as that of IP address. Each OSPF router that runs OSPF has a router ID.
Assign Default Route	Default routes have all 0s as the destination address and mask. A device uses a default route to forward packets when no matching route is discovered.
Import External Route	The routes learned from other routing protocols are introduced into the OSPF routing table, which is suitable for autonomous system boundary routers. External routing describes how to select a route to a destination address other than AS. • connected：connected route • static: static routing • rip：RIP route • bgp • isis

7.3.2 Network Configuration

Function Description

Configure the OSPF area to which each network interface of the device belongs.

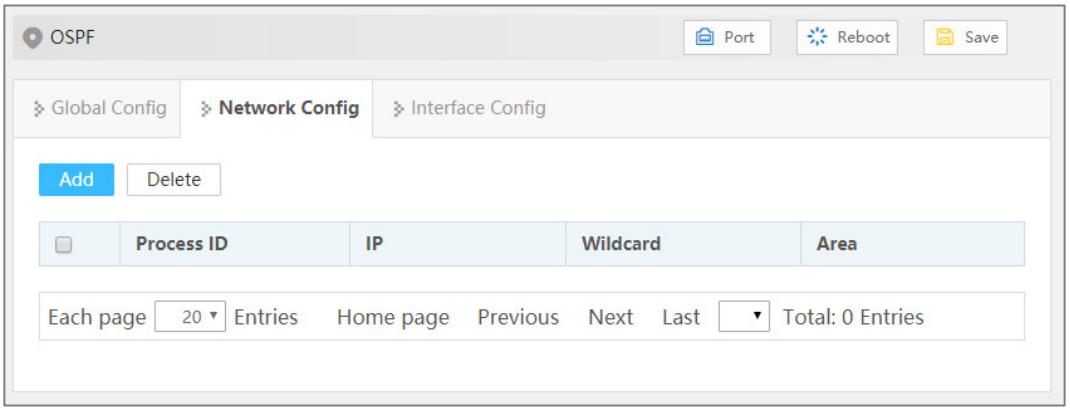
Operation Path

Open in order: "Unicast Routing > OSPF > Network Configuration".

Interface Description

Network configuration interface as follows:

Copyright © 3onedata Co., Ltd.



The main element configuration description of network configuration interface:

Interface Element	Description
Process ID	The value range of OSPF process ID is 1-65535.
IP	The network address, or network address / network prefix, of the OSPF process.
Wildcard	Wildcard of the network address.
Area	Set the OSPF area to which the network interface belongs. The identification of the OSPF area supports IP address format or integer value in the range of 0-4294967295.

7.3.3 Interface Configuration

Function Description

Configure the cost, expiration time, hello interval and DR priority of the device interface.

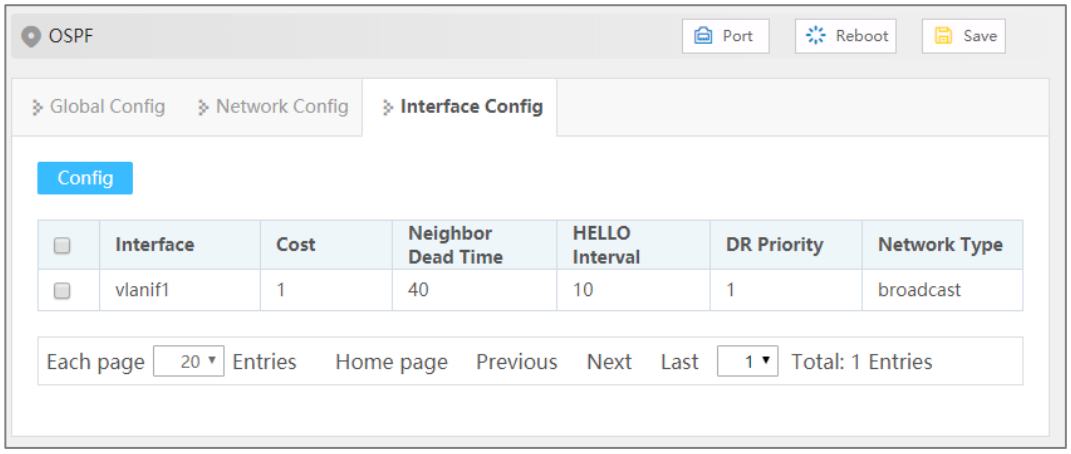
Operation Path

Open in order: "Unicast Routing > OSPF > Interface Configuration".

Interface Description

Interface configuration interface as follows:

Copyright © 3onedata Co., Ltd.



The main element configuration description of interface configuration interface:

Interface Element	Description
Interface	VLANIF interface of the device.
Cost	The cost required to run OSPF protocol on the interface. The value range is 1-65535.
Neighbor Dead Time	OSPF neighbor dead time, in seconds, value range 1-65535. If the Hello message from the neighbor is not received within this time, the neighbor is considered invalid. If the failure time between two adjacent routers is different, the neighbor relationship cannot be established.
Hello Interval	The time interval for the interface to send Hello message, in seconds, with a value range of 1-65535. The Hello message is periodically sent to the neighbor router to maintain the neighbor relationship and the election of DR (Designated Router) / BDR (Backup Designated Router).
DR Priority	DR priority of the interface, ranging from 1 to 255. The DR priority determines the qualification of the interface for election of DR/BDR. The higher the value, the higher the priority. High priority will be taken into account when voting rights conflict.

7.4 OSPFV3

OSPFv3 is an OSPF routing protocol running on IPv6, modified on the basis of OSPFv2, and is an independent routing protocol.

3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.

7.4.1 Global Configuration

Function Description

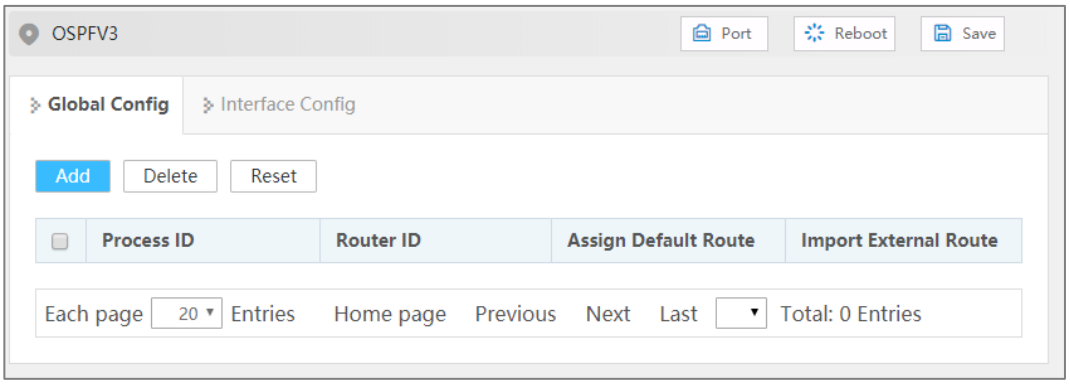
Configure OSPFv3 process ID, router ID, default route, import external route and other information.

Operation Path

Open in order: "Unicast Routing > OSPFV3 > Global Configuration".

Interface Description

Global configuration interface is as follows:



The main element configuration description of global configuration interface:

Interface Element	Description
Process ID	OSPFv3 process identification. OSPFv3 supports multiple processes. Multiple different OSPFv3 processes can be run on the same router, and they are independent of each other.
Router ID	Router ID is used to uniquely identifies an OSPF router in an AS. ID is in the same format as an IP address. Every OSPFv3 process has a router ID.
Assign Default Route	Default routes have all 0s as the destination address and mask. A device uses a default route to forward packets when no matching route is discovered.
Import External Route	The routes learned from other routing protocols are introduced into the OSPFv3 routing table, which is suitable for autonomous system boundary routers. External routing describes how to select a route to a destination address other than AS. • connected：connected route • static: static routing

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	• rip: RIP/RIPng route information protocol • bgp: BGP border gateway protocol. • isis：IS-IS intermediate system to intermediate system

7.4.2 Interface Configuration

Function Description

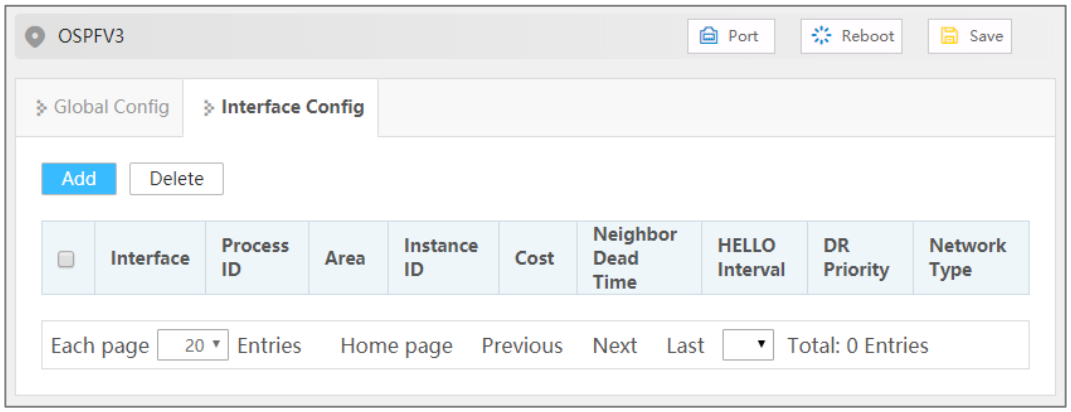
Configure the cost, expiration time, hello interval and DR priority of the device interface.

Operation Path

Open in order: "Unicast Routing > OSPFV3 > Interface Configuration".

Interface Description

Interface configuration interface as follows:



The main element configuration description of interface configuration interface:

Interface Element	Description
Interface	VLANIF interface of the device.
Process ID	OSPFv3 process identification.
Area	The ID of the OSPFv3 area, the value range is 0-4294967295 or IPv4 address format. The OSPFv3 protocol divides the autonomous system into one or more areas in a logical sense, and achieves the unification of routing information by exchanging OSPFv3 messages among devices in the areas.
Instance ID	Instance ID the interface belongs to. OSPFv3 supports multiple processes on a link, and a physical interface can be bound to multiple instances, which are distinguished by

3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.

Interface Element	Description
	different Instance ID.
Cost	The cost required to run OSPF protocol on the interface. The value range is 1-65535.
Neighbor Dead Time	OSPF neighbor dead time, in seconds, value range 1-65535. If the Hello message from the neighbor is not received within this time, the neighbor is considered invalid. If the failure time between two adjacent routers is different, the neighbor relationship cannot be established.
Hello Interval	The time interval for the interface to send Hello message, in seconds, with a value range of 1-65535. The Hello message is periodically sent to the neighbor router to maintain the neighbor relationship and the election of DR (Designated Router) / BDR (Backup Designated Router).
DR Priority	DR priority of the interface, ranging from 1 to 255. The DR priority determines the qualification of the interface for election of DR/BDR. The higher the value, the higher the priority. High priority will be taken into account when voting rights conflict.
Network Type	The network types of OSPFv3 interface correspond to different types of link layer protocols, and the network types are as follows: • Broadcast • Non-broadcast: non-broadcast point-to-multipoint NBMA type • Point-to-multipoint • Point-to-point: point-to-point P2P type

7.5 ISIS

IS-IS (intermediate system to intermediate system) belongs to IGP (Interior Gateway Protocol) and is used in the autonomous system. IS-IS is also a link-state protocol, which uses the shortest path first (SPF) algorithm to calculate the route.

3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.

7.5.1 Global Configuration

Function Description

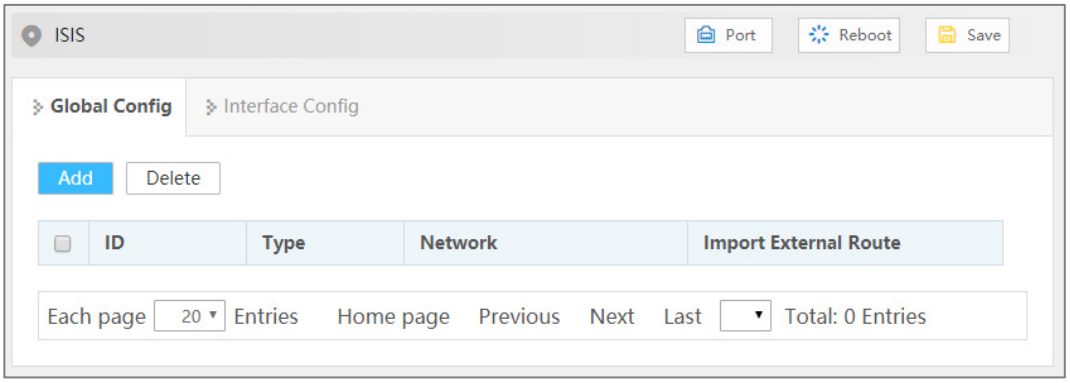
Configure IS-IS global parameter.

Operation Path

Open in order: "Unicast Routing > ISIS > Global Configuration".

Interface Description

Global configuration interface is as follows:



The main element configuration description of global configuration interface:

Interface Element	Description
ID	IS-IS process identification. IS-IS supports multi-processes, and many different IS-IS processes can run on the same router, which do not affect each other and are independent of each other.
Type	The types of IS-IS device, the options are as follows: • Level-1: The device only forms neighbor relationship with Level-1 and Level-1-2 device belonging to the same area, and is only responsible for maintaining the link state database LSDB of Level-1. • Level-2: The device can form a neighbor relationship with Level-2 devices in the same or different areas or Level-1-2 devices in other areas, and only maintain one Level-2 LSDB. • Level-1-2: The device will establish neighbors for Level-1 and Level-2 respectively, and maintain two LSDB for Level-1 and Level-2 respectively.
Network	The network entity name NET(Network Entity Title) of the

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	IS-IS process is in the format of X…X.XXXX.XXXX.XXXX.00, the front "X…X" is the area address, the middle 12 "X" is the system ID of the device, and the last "00" is SEL. Note: • The zone address is used to uniquely identify different zones in the routing domain. All switches in the same Level-1 zone must have the same zone address, and switches in the Level-2 zone can have different zone addresses. • In the whole area and backbone area, it is required to keep the system ID unique.
Import External Route	The routes learned from other routing protocols are introduced into the IS-IS routing table, which is suitable for boundary routers. Traffic in the IS-IS routing domain can reach the outside of the IS-IS routing domain. • connected：connected route • static: static routing • ospf: Open Shortest Path First • bgp: BGP border gateway protocol. • rip: RIP route information protocol • isis level-2 into level-1: route penetration from Level-2 to Level-1

7.5.2 Interface Configuration

Function Description

Configure the interface parameters of IS-IS.

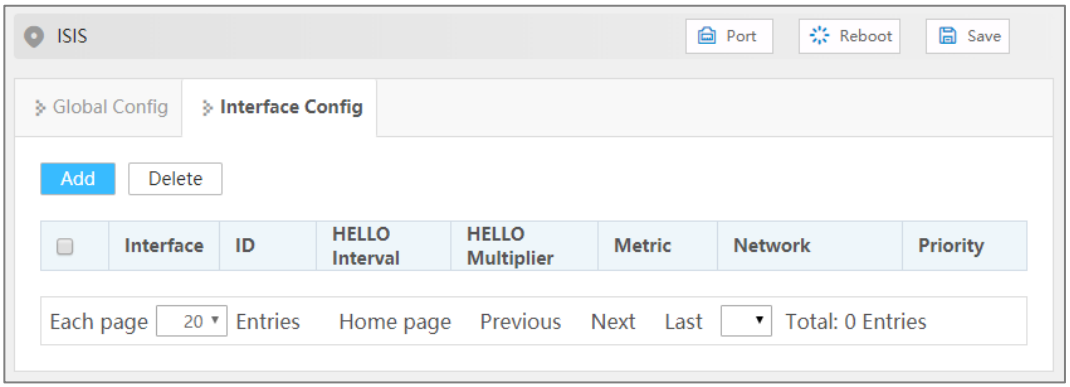
Operation Path

Open in order: "Unicast Routing > ISIS > Interface Configuration".

Interface Description

Interface configuration interface as follows:

Copyright © 3onedata Co., Ltd.



The main element configuration description of interface configuration interface:

Interface Element	Description
Interface	VLANIF interface of the device.
ID	IS-IS process identification.
Hello Interval	The time interval for the interface to send Hello message, in seconds, with a value range of 1-65535. Hello messages are periodically sent to neighbor routers to maintain the neighbor relationship.
HELLO Multiplier	The neighbor hold time is a multiple of the interval between Hello messages, and the value range is 2-100. If the device at one end of the link does not receive the Hello message sent by the device at the opposite end within the neighbor holding time, it is considered that the neighbor at the opposite end is invalid.
Metric	Link cost of IS-IS interface, the value range is 1-63.
Network	The network types of IS-IS interface correspond to different types of link layer protocols, and the network types are as follows: • Broadcast • Point-to-point: point-to-point P2P type
Priority	DIS priority of the interface, ranging from 1 to 127. The DIS priority determines the qualification of the interface for election of DIS. The higher the value, the higher the priority.

Copyright © 3onedata Co., Ltd.

7.6 VRRP

The Virtual Router Redundancy Protocol (VRRP) groups multiple routing devices into a virtual router and uses the virtual gateway device's IP address as the default gateway address. When the gateway fails, VRRP selects a new gateway to transmit service traffic to ensure reliable communication. VRRP protocol has two versions: VRRPv2 and VRRPv3. VRRPv2 applies to only the IPv4 network, and VRRPv3 applies to IPv4 and IPv6 networks.

Function Description

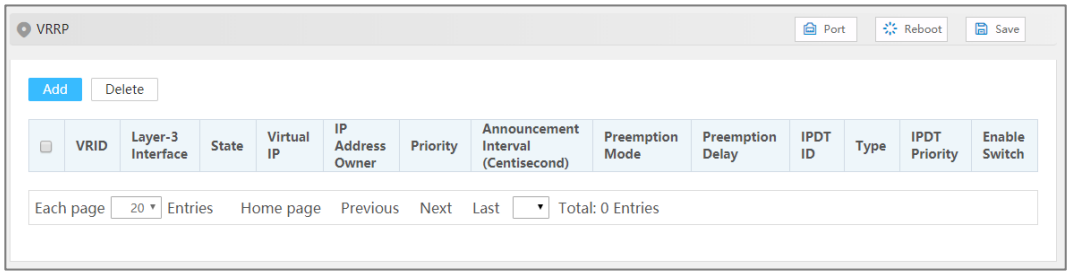
Configure IPv4 VRRP parameter.

Operation Path

Open in order: "Unicast Routing > VRRP".

Interface Description

VRRP interface is as below:



The main elements configuration description of VRRP interface:

Interface Element	Description
VRID	Virtual router ID, valid range is 1-255.
Layer 3 Interface	Layer 3 interface information, such as, vlanif1.
State	Current status, options as follows: • Init • Master • Backup
Virtual IP	Virtual router IP address, such as 192.168.1.253.
IP Address Owner	The IP address owner takes the virtual router IP address as the real interface address.
Priority	Priority defaults to 100, the valid range is 1-255. Note: When the IP address owner is configured, the default priority can only be 255.
Announcement	The Master router in the VRRP backup group will send a

Copyright © 3onedata Co., Ltd.

Interface Element	Description
interval (centisecond)	notification message to notify the routers in the VRRP backup group that they are working normally, unit: centisecond, valid range: 5-4095 (multiple of 5).
Preemption Mode	In the preemption mode, once the routers in the backup group find that their priority is higher than that of the current Master router, they will send VRRP announcement messages to the outside. It causes the router in the backup group to reelect the Master router and eventually replace the original Master router. Accordingly, the original Master router will become the Backup router. Preemption mode, options as follows: • false • true
IPDT ID	The value range of IPDT ID is 1-8.
Type	IPDT priority type, options are as follows: • Increased: After "Track" is enabled, the VRRP priority value is equal to the original VRRP priority value plus the IPDT priority value when the IPDT link fails. • Reduced: After "Track" is enabled, the VRRP priority value is equal to the original VRRP priority value minus the IPDT priority value when the IPDT link fails.
IPDT Priority	Port priority level, the value range is 1-253.
Enable	VRRP enable status, options as follows: • enable • disable

7.7 IPv6 VRRP

Function Description

Configure IPv6 VRRP parameter.

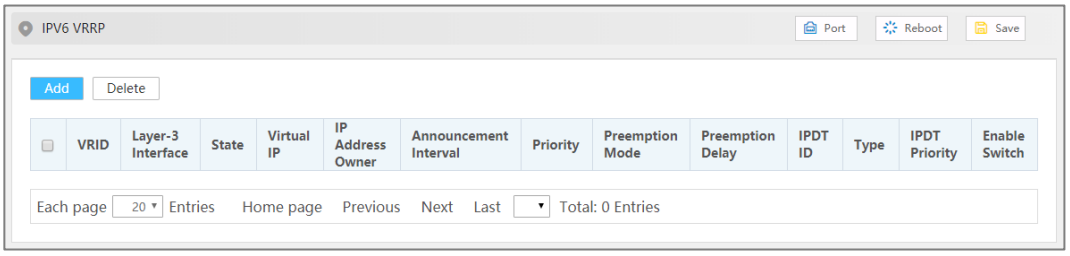
Operation Path

Open in order: "Unicast Routing > IPv6 VRRP".

Interface Description

IPv6 VRRP interface is as below:

Copyright © 3onedata Co., Ltd.



The main elements configuration description of IPv6 VRRP interface:

Interface Element	Description
VRID	Virtual router ID, valid range is 1-255.
Layer 3 Interface	Layer 3 interface information, such as, vlanif1.
State	Current status, options as follows: • Init • Master • Backup
Virtual IP	Virtual routing IPv6 address, the address within the local address range of the link, such as fe80::1.
IP Address Owner	The IP address owner takes the virtual router IP address as the real interface address.
Announcement Interval	The Master router in the VRRP backup group will send a notification message to notify the routers in the VRRP backup group that they are working normally, unit: centisecond, valid range: 5-4095 (multiple of 5).
Priority	Priority defaults to 100, the valid range is 1-255. Note: When the IP address owner is configured, the default priority can only be 255.
Preemption Mode	In the preemption mode, once the routers in the backup group find that their priority is higher than that of the current Master router, they will send VRRP announcement messages to the outside. It causes the router in the backup group to reelect the Master router and eventually replace the original Master router. Accordingly, the original Master router will become the Backup router. Preemption mode, options as follows: • false • true
Preemption Delay	Set a preemption delay for a VRRP backup group to avoid frequent primary and standby state transitions among members of the backup group. Valid range is 0-255s, the

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	default value is 0s.
Enable	VRRP enable status, options as follows: • enable • disable

Copyright © 3onedata Co., Ltd.

8 Multicast Routing

8.1 Multicast Routing

8.1.1 Multicast Routing Switch

Function Description

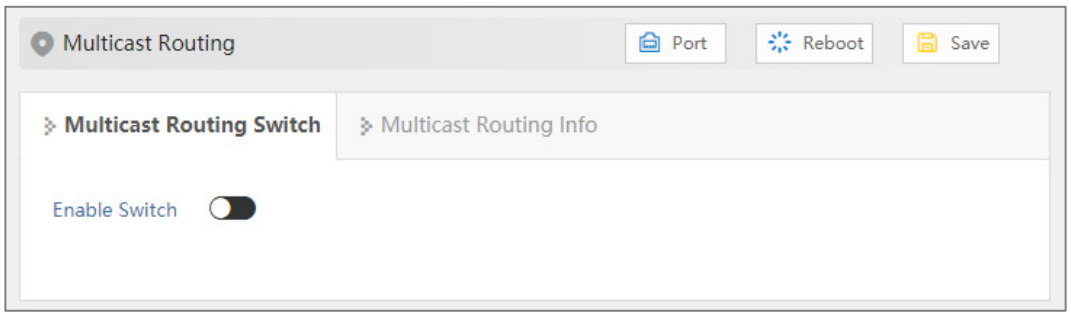
Turn on or off the layer 3 IPv4 multicast routing function.

Operation Path

Open in order: "Multicast Routing > Multicast Routing > Multicast Routing Switch".

Interface Description

The multicast routing switch interface is shown as follows:



Main elements of the multicast routing switch interface:

Interface Element	Description
Enable	Click the button to enable or disable multicast routing, swipe right to enable it, swipe left to disable it.

Copyright © 3onedata Co., Ltd.

8.1.2 Multicast routing information

Function Description

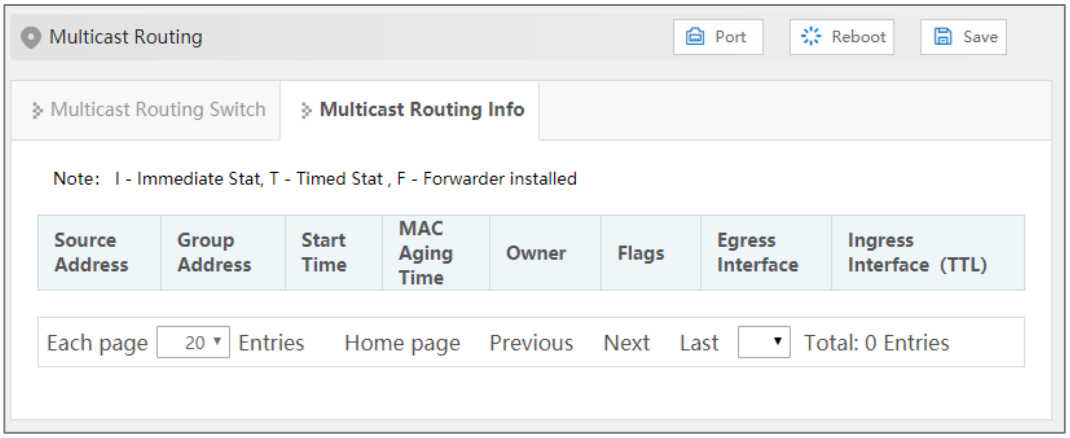
Check layer 3 multicast routing information.

Operation Path

Open in order: "Multicast Routing > Multicast Routing > Multicast Routing Information".

Interface Description

The multicast routing information interface is as follows:



Main elements of the multicast routing information interface:

Interface Element	Description
Source Address	Multicast source address
Multicast Address	Multicast group address
Startup Time	The existed time of the multicast route.
Aging Time	Multicast routing aging time.
Owner	The owner of a multicast route may be a multicast routing protocol.
Flags	Multicast routing protocol flag: • I: Immediate Stat (Immediately the statistics) • T: Timed Stat (Statistics Timer) • F: Forwarder installed (Set to forward table)
Ingress interface	Multicast data ingress interface. The interface on the local device that receives multicast data.
Egress interface (TTL)	Multicast data egress interface. The interface that forwards multicast data out.

Copyright © 3onedata Co., Ltd.

8.2 IPv6 Multicast Routing

8.2.1 Multicast Routing Switch

Function Description

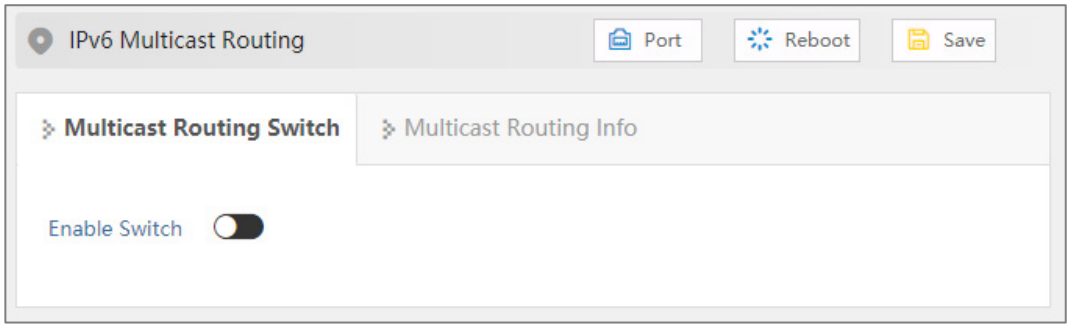
Enable IPv6 layer 3 multicast routing globally. After the multicast routing function is enabled, it can be equipped with some IPv6 layer 3 multicast protocols such as PIM(IPv6) and MLD and other IPv6 layer 3 multicast functions.

Operation Path

Open in order: "Multicast Routing > IPv6 Multicast Routing > Multicast Routing Switch".

Interface Description

The multicast routing switch interface is shown as follows:



Main elements of the multicast routing switch interface:

Interface Element	Description
Enable	IPv6 layer 3 multicast routing enable switch.

8.2.2 Multicast routing information

Function Description

Check layer 3 multicast routing information.

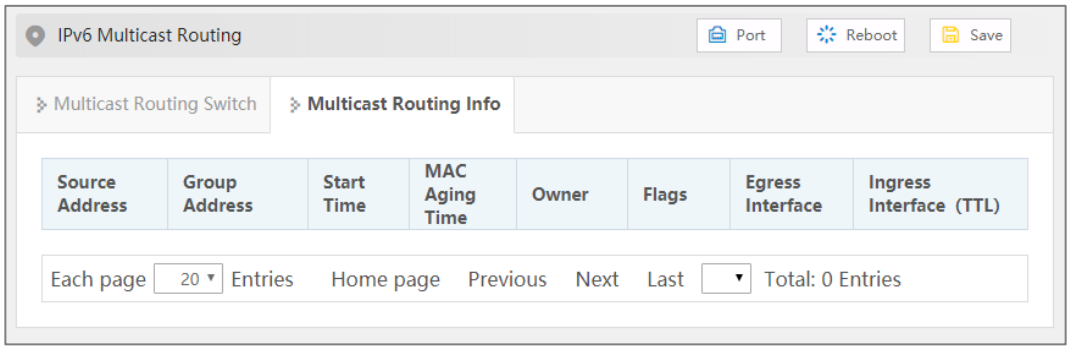
Operation Path

Open in order: "Multicast Routing > IPV6 Multicast Routing > Multicast Routing Information".

3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.

Interface Description

The multicast routing information interface is as follows:



Main elements of the multicast routing information interface:

Interface Element	Description
Source Address	Multicast source address
Group address	Multicast group address
Start Time	The existed time of the multicast route.
MAC Aging Time	Multicast routing aging time.
Owner	The owner of a multicast route may be a multicast routing protocol.
Flags	Multicast routing protocol flag: • I: Immediate Stat (Immediately the statistics) • T: Timed Stat (Statistics Timer) • F: Forwarder installed (Set to forward table)
Ingress interface	Multicast data ingress interface. The interface on the local device that receives multicast data.
Egress interface (TTL)	Multicast data egress interface. The interface that forwards multicast data out.

8.3 IGMP Snooping

8.3.1 Interface Configuration

Function Description

Configure the IGMP parameters of VLANIF interface.

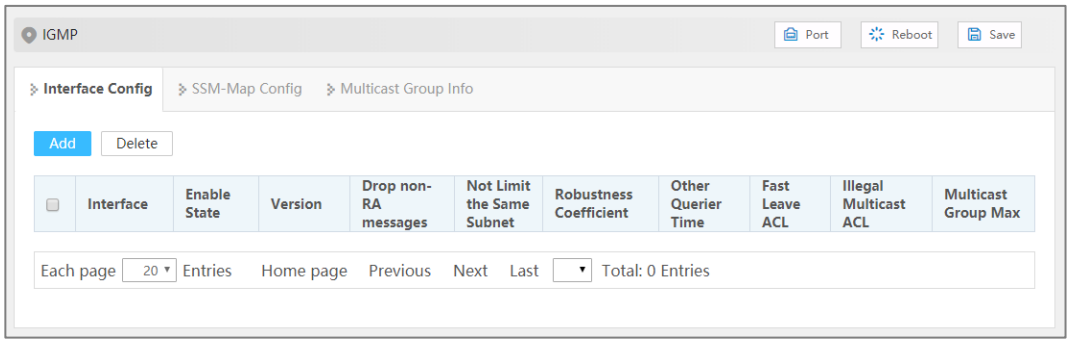
Copyright © 3onedata Co., Ltd.

Operation Path

Open in order: "Multicast Routing > IGMP > Interface Configuration".

Interface Description

Interface configuration interface as follows:



The main element configuration description of interface configuration interface:

Interface Element	Description
Interface	Layer 3 interface, such as vlanif1.
Enable State	IGMP Status: • enable • disable
Version	IGMP version, options are: • 1: IGMPv1, it defines the basic querying and reporting process of group members; • 2: IGMPv2, it adds the mechanism of polling and leaving group members on IGMPv1; • 3: IGMPv3, members are added to IGMPv2 to specify whether to receive or not to receive messages from certain multicast sources.
Drop non-RA message	RA(Router-Alert). When a network device receives a message, only the message whose destination IP address is the interface address of the device will be sent to the corresponding protocol module for processing. If the destination address of the protocol message is not the interface address of the device, check whether the IP message header carries the Router-Alert option, if so, it will be directly sent to the corresponding protocol module for processing without checking the destination address. Note: For compatibility reasons, after receiving IGMP message, the current switch will send it to IGMP protocol module for processing by default regardless of whether its IP header contains Router-Alert

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	option.
Not limit the same subnet	Limit the multicast source and interface to the same subnet, otherwise the port cannot receive multicast messages.
Robustness coefficient	Specify the robustness of the IGMP query, ranging from 2 to 7. This coefficient is used to specify the default value of the number of times an IGMP query message is sent by the IGMP query at startup, and the number of times an IGMP query message is sent by the IGMP query after the IGMP query receives the message leaving the group.
Other inquirer time	Timer time of non-inquirer. • Before the timer expires, if the inquiry message from the inquirer is received, reset the timer; • Otherwise, the original inquirer is considered invalid, and a new inquirer election process is initiated.
Fast leave ACL	By default, when the interface works in IGMP v2 or v3, after receiving IGMP leave message, it will send a specific group query message to determine whether to age multicast member entries. After configuring the fast leave ACL, if the group address specified by the leave message is within the group address range specified by the ACL, the multicast member table entry can be aged immediately.
Illegal multicast ACL	List of restricted multicast groups.
Multicast group Max	The maximum number of multicast supported.

8.3.2 SSM-Map configuration

SSM(Source-Specific Multicast) requires routers to know the multicast source designated by member hosts when they join the multicast group. A host running IGMPv3 can specify multicast source addresses in IGMPv3 Report messages. However, hosts running IGMPv1 or IGMPv2 rely on the IGMP SSM mapping function to obtain the SSM service.

3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.

The mechanism of IGMP SSM Mapping is: by statically configuring SSM address Mapping rules on the router, information in IGMPv1 and IGMPv2 report packets is converted into corresponding information to provide SSM multicast service.

After the configuration of SSM Mapping rules, when the IGMP query receives the IGMPv1 or IGMPv2 report packets from the member host, it first checks the multicast group addresses carried in the paper, and then processes them separately according to the different inspection results.

- If the Multicast group is within the range of ANY-Source Multicast, then only ASM services are provided.
- If the multicast group is within the SSM group address range (the default is 232.0.0.0 ~ 232.255.255.255) :
  - If the router does not have the SSM Mapping rule corresponding to the multicast group, the SSM service cannot be provided and the article is discarded.
  - If there are SSM Mapping rules corresponding to the multicast group on the router, according to the rules, the information contained in the report packet (member, multicast group) will be mapped to (multicast group, INCLUDE, member) information, and SSM service will be provided.

Function Description

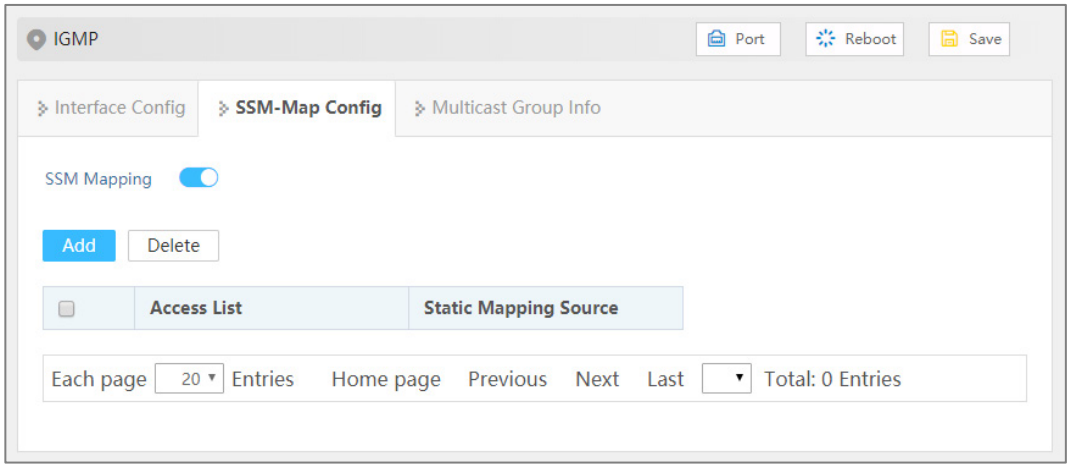
Configure SSM Mapping rule.

Operation Path

Open in order: "Multicast Routing > IGMP > SSM-Map Configuration".

Interface Description

The SSM-Map configuration interface is as follows:



Main element configuration description of SSM-Map configuration interface:

Copyright © 3onedata Co., Ltd.

Interface Element	Description
SSM Mapping	IGMP SSM Mapping Enable switch.
Access List	Access list.
Static Mapping Source	The specified multicast source address in the access list.

8.3.3 Multicast Group Information

Function Description

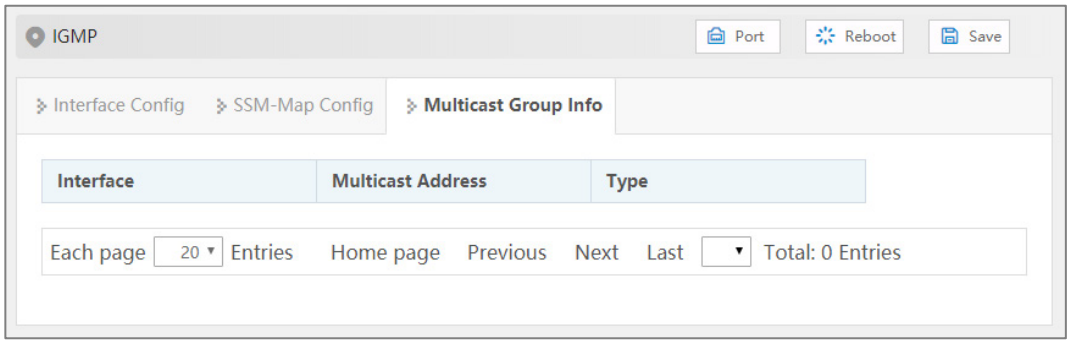
Display the multicast information received by the device interface.

Operation Path

Open in order: "Multicast Routing > IGMP > Multicast Group Information".

Interface Description

The multicast group information interface is as follows:



Main element configuration description of multicast group information interface:

Interface Element	Description
Interface	Ethernet port.
Multicast Address	The multicast address received by the interface.
Type	Multicast type: • dynamic • static

8.4 IPv6 MLD

MLD(Multicast Listener Discovery) is a protocol responsible for IPv6 multicast member management, which is used to establish and maintain the multicast group member relationship between IPv6 member hosts and their immediate neighboring multicast routers. MLD realizes the group member management function by interacting MLD messages between member hosts and multicast routers, and the MLD messages are encapsulated in IPv6 messages.

8.4.1 Interface Configuration

Function Description

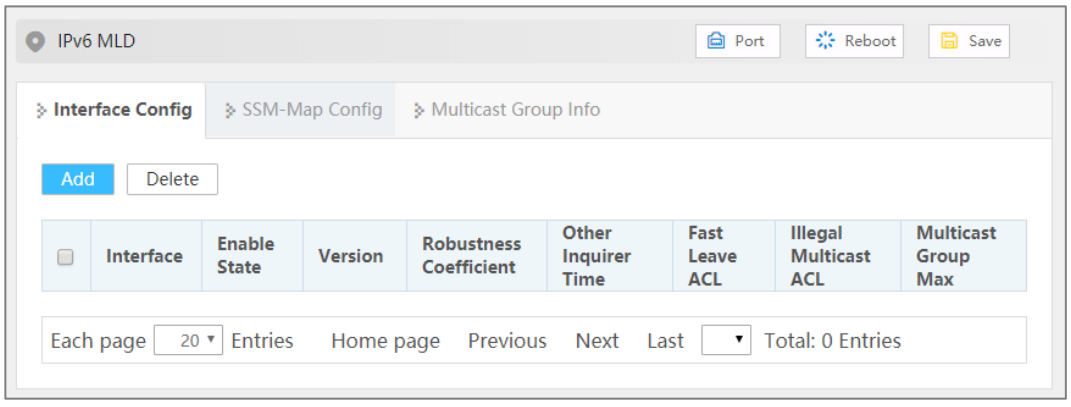
Configure MLD parameters of VLANIF interface.

Operation Path

Open in order: "Multicast Routing > IPv6 MLD > Interface Configuration".

Interface Description

Interface configuration interface as follows:



The main element configuration description of interface configuration interface:

Interface Element	Description
Interface	Layer 3 interface, such as vlanif1.
Enable state	The MLD enabled status can be displayed as follows: • enable • disable
Version	MLD version, options are: • 1: the working mechanism of MLDv1 is the same as that of IGMPv2.

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	• 2. based on MLDv1, the main function of MLDv2 is that member hosts can specify whether to receive or not to receive messages from some multicast sources, corresponding to IGMPv3.
Robustness Coefficient	Specify the robustness of the MLD query, ranging from 2 to 7. This coefficient is used to specify the default value of the number of times an MLD query message is sent by the MLD query at startup, and the number of times an IGMP query message is sent by the IGMP query after the IGMP query receives the message leaving the group.
Other Inquirer Time	Live time of other queriers If the non-inquirer fails to receive the inquiry message within the "life time of other MLD inquirers", the inquirer will be deemed invalid and the inquirer election will be automatically initiated.
Fast Leave ACL	By default, after receiving MLD leave message, it will send a specific group query message to determine whether to age multicast member entries. After configuring the fast leave ACL, if the group address specified by the leave message is within the group address range specified by the ACL, the multicast member table entry can be aged immediately.
Illegal Multicast ACL	List of restricted multicast groups.
Multicast Group Max	The maximum number of multicast supported.

8.4.2 SSM-Map configuration

SSM(Source-Specific Multicast) requires routers to know the multicast source designated by member hosts when they join the multicast group. A host running MLDv2 can specify multicast source addresses in MLDv2 Report messages. However, in some cases, member hosts can only run MLDv1. In order to enable them to use SSM services, the router needs to provide MLD SSM Mapping function.

Function Description

Configure MLD SSM Mapping rules.

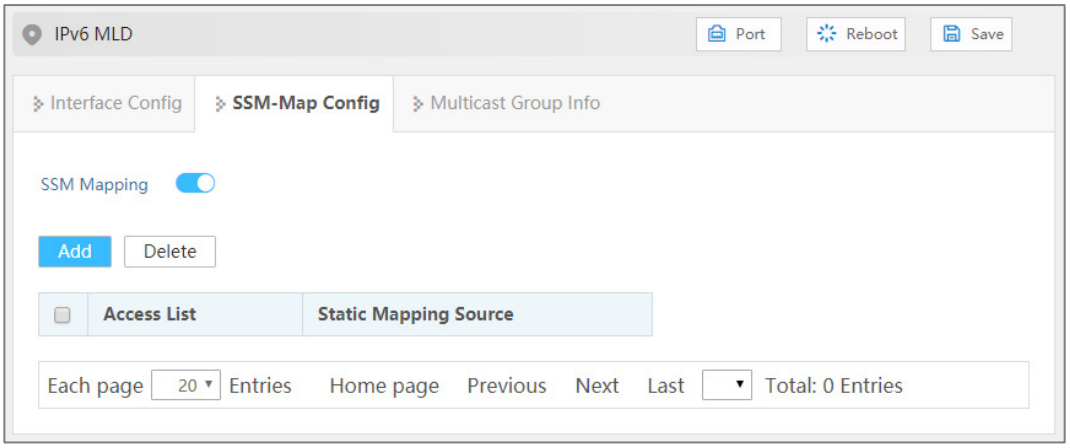
Copyright © 3onedata Co., Ltd.

Operation Path

Open in order: "Multicast Routing > IPv6 MLD > SSM-Map Configuration

Interface Description

The SSM-Map configuration interface is as follows:



Main element configuration description of SSM-Map configuration interface:

Interface Element	Description
SSM Mapping	MLD SSM Mapping enable switch.
Access List	Access list.
Static Mapping Source	The specified multicast source IPv6 address in the access list.

8.4.3 Multicast Group Information

Function Description

Display the multicast information received by the device interface.

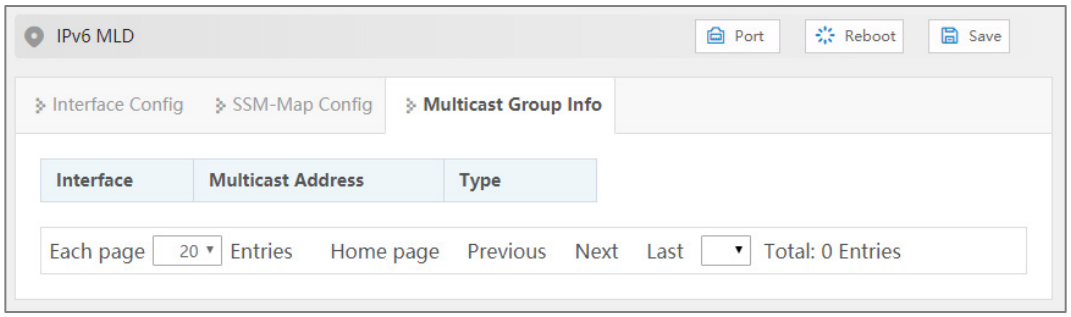
Operation Path

Open in order: "Multicast Routing > IPv6 MLD > Multicast Group Information".

Interface Description

The multicast group information interface is as follows:

Copyright © 3onedata Co., Ltd.



Main element configuration description of multicast group information interface:

Interface Element	Description
Interface	Ethernet port.
Multicast Address	The multicast address received by the interface.
Type	Multicast type: • dynamic • static

8.5 PIM-SM

PIM (Protocol Independent Multicast) is unrelated to unicast routing protocol, it uses the routing information of unicast routing table to perform RPF(Reverse Path Forwarding) check on multicast messages, and creates multicast routing table entries after passing the check, thus forwarding multicast messages.

PIM protocol include: PIM-DM (PIM-Dense Mode) and PIM-SM (PIM-Sparse Mode).

PIM-SM is a multicast routing protocol in sparse mode, which uses "Pull mode" to transmit multicast data. It is usually suitable for large and medium-sized networks with relatively scattered multicast group members and a wide range. Its basic principle is as follows:

- PIM-SM assumes that all hosts do not need to receive multicast data, but only forward it to the hosts that explicitly propose that they need multicast data. The core task of PIM-SM to realize multicast forwarding is to construct and maintain RPT(Rendezvous Point Tree). RPT selects a router in PIM domain as a common root node RP(Rendezvous Point), and multicast data is forwarded to receivers along RPT through RP.
- The router connecting the receiver sends a Join Message to the RP corresponding to a multicast group, and the message is delivered to the RP hop by hop, and the path it passes forms a branch of RPT;

3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.

- If a multicast source wants to send multicast data to a multicast group, the DR(Designated Router (DR) on the multicast source side is responsible for registering with the RP, and sending a Register Message to the RP by unicast, which triggers the establishment of SPT after reaching the RP. After that, the multicast source sends the multicast data to RP along SPT. When the multicast data reaches RP, it is copied and sent to the receiver along RPT.

The working mechanism of PIM-SM can be summarized as follows:

- Neighbor Discovery
- DR election
- RP Discovery
- Construct RPT
- Multicast source note
- SPT Switchover
- Assertion

8.5.1 Global Configuration

Function Description

Configure global parameters of PIM-SM.

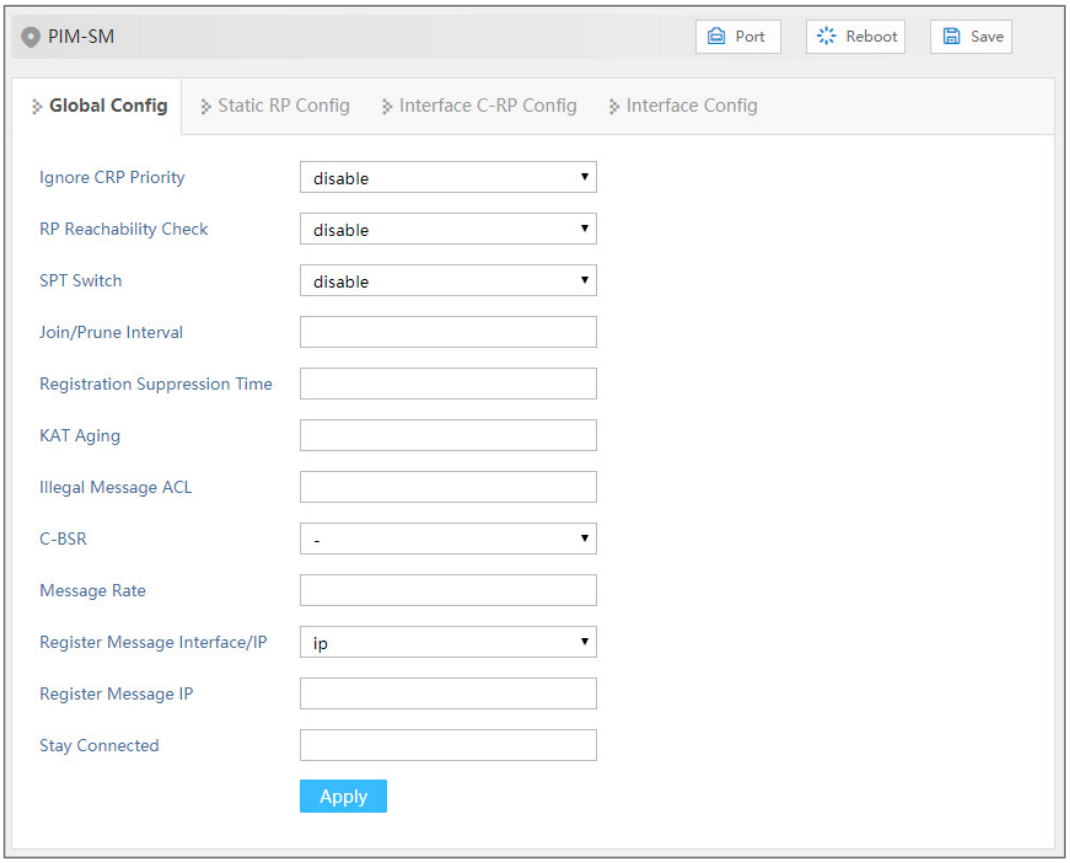
Operation Path

Open in order: "Multicast Routing > PM-SM > Global Configuration".

Interface Description

Global configuration interface is as follows:

Copyright © 3onedata Co., Ltd.



The main element configuration description of global configuration interface:

Interface Element	Description
Ignore CRP Priority	When selecting the RP corresponding to multicast, whether to ignore the priority of CRP and choose according to IP address. The one with the larger IP address is elected.
RP Reachability Check	Whether it is necessary to check the reachability of RP when sending the registration message; if it is not, it means that it cannot be registered.
SPT Switch	RP is a necessary transit station for all multicast messages. when the multicast message rate gradually increases, it will create a huge burden on RP. PIM-SM allows RP or group member DR to reduce the burden of RP by triggering SPT switching.
Join/Prune Interval	Time interval for PIM router to send join/pruning messages.
Registration Suppression Time	The time interval from receiving the registration stop message to resend the registration message, the value range is 1 ~ 65535s.
KAT Aging	The aging time of KAT timer after receiving the registration message ranges from 1 to 65535 in seconds.

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	Note: By default, after receiving the registration message, the aging time of KAT timer = registration inhibition time * 3+registration detection time.
Illegal Message ACL	Configure illegal neighbor source address range. Note: By default, there are no restrictions on the neighbor source addresses that an interface can learn from.
C-BSR	C-BSR Interface Configuration. • vlanif: vlanif interface • loopback: loopback interface
Message Rate	The rate of receiving and processing multicast service messages ranges from 1 to 65535, and the unit is one/second.
Register Message Interface /IP	The VLAN interface, source IP address or loopback interface that sends the registration message.
Register Message IP	The source IP address of the registered message.
Stay Connected	Multicast source lifetime, ranging from 60-65535 seconds.

8.5.2 Static RP Configuration

Function Description

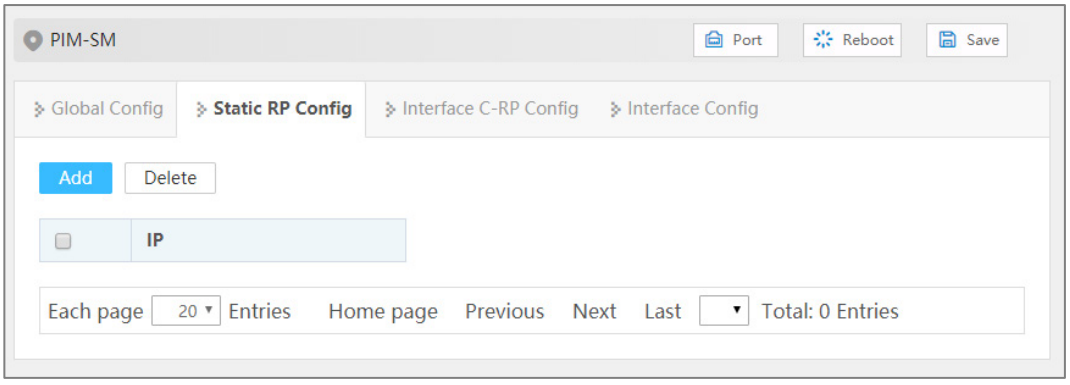
Set static RP manually.

Operation Path

Open in order: "Multicast Routing > PIM-SM > Static RP Configuration".

Interface Description

Static RP configuration interface as follow:



Copyright © 3onedata Co., Ltd.

The main element configuration description of static RP configuration interface:

Interface Element	Description
IP Address	Configure the IP address of the static RP. Note: • The address must be a legal unicast IP address, and should not be configured as the address of the 127.0.0.0/8 network segment. • When there is only one RP in the network, static RP can be manually configured instead of dynamic RP, which can avoid the frequent information interaction between C-RP and BSR occupying bandwidth.

8.5.3 C-RP Configuration of Interface

Function Description

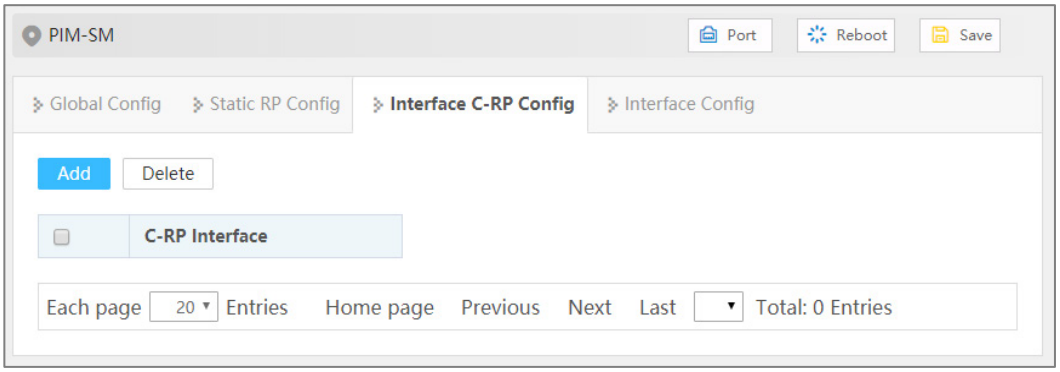
Add and delete C-RP interfaces.

Operation Path

Open in order: "Multicast Routing > PM-SM > Interface C-RP Configuration".

Interface Description

The interface C-RP configuration interface is as follows:



Main element configuration description of interface C-RP configuration interface:

Interface Element	Description
C-RP interface	To configure the C-RP interface: • vlanif: vlanif interface • loopback: loopback interface

Copyright © 3onedata Co., Ltd.

8.5.4 Interface Configuration

Function Description

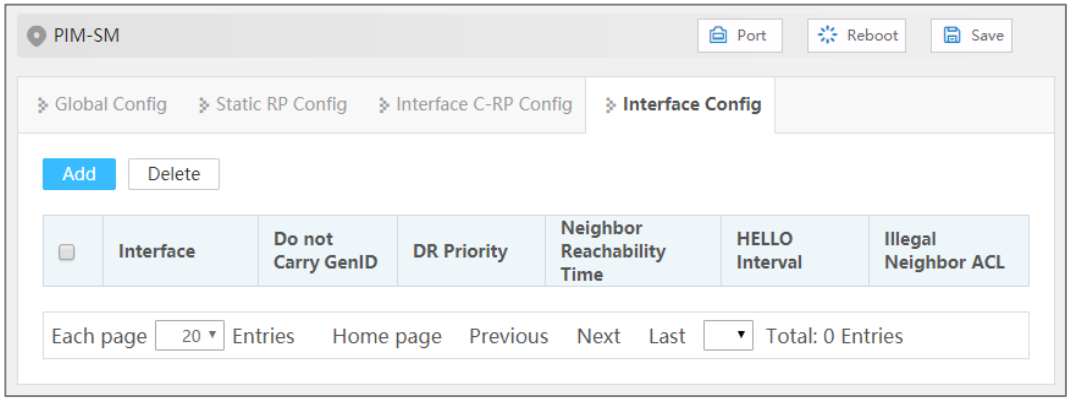
Set interface PIM-SM parameters.

Operation Path

Open in order: "Multicast Routing > PM-SM > Interface Configuration".

Interface Description

Interface configuration interface as follows:



The main element configuration description of interface configuration interface:

Interface Element	Description
Interface	Configure interface: • vlanif: vlanif interface • loopback: loopback interface
Do not carry GenID	The interface is configured to send hello messages without carrying GenID information. Note: GenID is a random value at the initial creation of the interface to identify unique interface information. With this information, users can detect whether the neighbor device has been restarted.
DR priority	Specify the priority of running for DR from 0 to 4294967294. Note: The higher the value, the higher the priority.
Neighbor Reachability Time	Specify the time to keep PIM neighbor reachable, the value range is 1 ~ 65535, and the unit is seconds. Note: If specified as 65535 seconds, the PIM neighbor is always reachable.
Hello Interval	Time period for sending Hello messages between PIM routers.

Copyright © 3onedata Co., Ltd.

Interface Element	Description
Illegal Neighbor ACL	Illegal neighbor source address range.

8.6 PIM-DM

PIM-DM is a multicast routing protocol in dense mode, which uses "Push mode" to transmit multicast data. It is usually suitable for small networks with relatively dense multicast group members. Its basic principle is as follows:

- PIM-DM assumes that each subnet in the network has at least one multicast group member, so multicast data will be Flooding to all nodes in the network. Then, PIM-DM prune the branches without multicast data forwarding, leaving only the branches containing receivers. This "Flooding-Prune" phenomenon occurs periodically, and the pruned branches can also be restored to forwarding status periodically.
- In order to reduce the time required for the node to return to the forwarding state when the multicast group members appear on the branched node, PIM-DM actively resumes its forwarding of multicast data by using the Graft mechanism.

Generally speaking, the forwarding path of data packets in dense mode is a Source Tree (a forwarding tree with multicast source as its root and multicast group members as its branches and leaves). Source Tree is also called SPT(Shortest Path Tree) because it uses the shortest path from multicast source to receiver.

The working mechanism of PIM-DM can be summarized as follows:

- Neighbor Discovery
- Build SPT
- Graft
- Assertion

Function Description

Configure PIM-DM parameters.

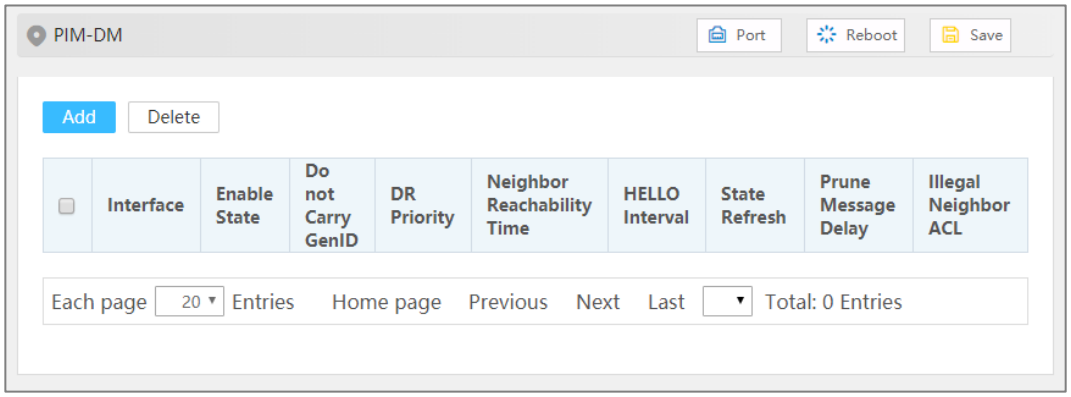
Operation Path

Open in order:"Multicast Routing > PIM-DM".

Interface Description

PIM-DM interface is as below:

Copyright © 3onedata Co., Ltd.



Main elements configuration descriptions of PIM-DM interface:

Interface Element	Description
Interface	Configure interface: • vlanif: vlanif interface • loopback: loopback interface
Enable State	Enable status of interface PIM-DM.
Do not Carry GenID	The interface is configured to send hello messages without carrying GenID information. Note: GenID is a random value at the initial creation of the interface to identify unique interface information. With this information, users can detect whether the neighbor device has been restarted.
DR Priority	Specify the priority of running for DR from 0 to 4294967294. Note: The higher the value, the higher the priority.
Neighbor Reachability Time	Specify the time to keep PIM neighbor reachable, the value range is 1 ~ 65535, and the unit is seconds. Note: If specified as 65535 seconds, the PIM neighbor is always reachable.
Hello Interval	Time period for sending Hello messages between PIM routers.
State Refresh	The time interval for refreshing the pruning timer status, which can prevent the clipped interface from resuming forwarding due to the timeout of pruning timer, the value range is 1-100 seconds.
Prune Message Delay	The delay time of transmitting Prune message on the shared network segment, which ranges from 0 to 32767 milliseconds.
Illegal Neighbor ACL	Illegal neighbor source address range.

3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.

8.7 IPv6-PIM-SM

8.7.1 Global Configuration

Function Description

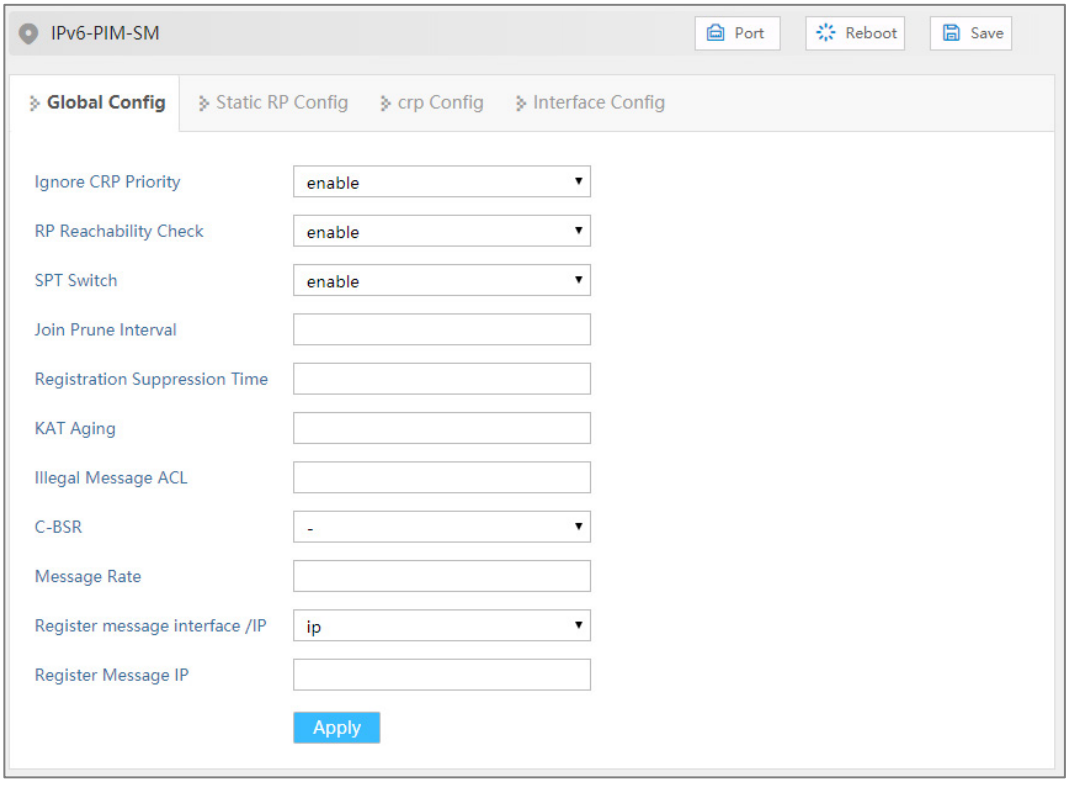
Configure global parameters of IPv6-PIM-SM.

Operation Path

Open in order: "Multicast Routing > IPv6-PIM-SM > Global Configuration".

Interface Description

Global configuration interface is as follows:



The main element configuration description of global configuration interface:

Interface Element	Description
Ignore CRP Priority	When selecting the RP corresponding to multicast, whether to ignore the priority of CRP and choose according to IP address. The one with the larger IP address is elected.
RP Reachability Check	Whether it is necessary to check the reachability of RP when sending the registration message; if it is not, it means that it

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	cannot be registered.
SPT Switch	RP is a necessary transit station for all multicast messages. when the multicast message rate gradually increases, it will create a huge burden on RP. PIM-SM allows RP or group member DR to reduce the burden of RP by triggering SPT switching.
Join Prune interval	Time interval for PIM router to send join/pruning messages.
Registration Suppression Time	The time interval from receiving the registration stop message to resend the registration message, the value range is 1 ~ 65535s.
KAT Aging	The aging time of KAT timer after receiving the registration message ranges from 1 to 65535 in seconds. Note: By default, after receiving the registration message, the aging time of KAT timer = registration inhibition time * 3+registration detection time.
Illegal Message ACL	Configure illegal neighbor source address range. Note: By default, there are no restrictions on the neighbor source addresses that an interface can learn from.
C-BSR	C-BSR Interface Configuration. • vlanif: vlanif interface • loopback: loopback interface
Message Rate	The rate of receiving and processing multicast service messages ranges from 1 to 65535, and the unit is one/second.
Register Message Interface /IP	The VLAN interface, source IP address or loopback interface that sends the registration message.
Register Message IP	The source IP address of the registered message.

8.7.2 Static RP Configuration

Function Description

Set static RP manually.

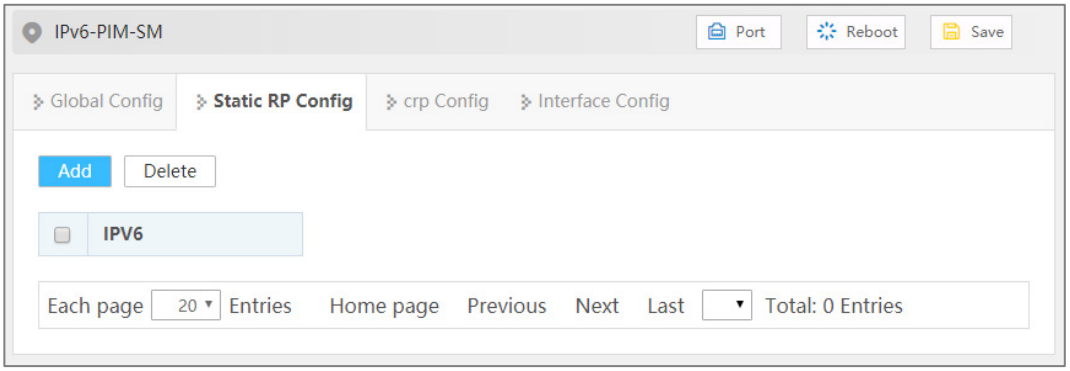
Operation Path

Open in order: "Multicast Routing > IPv6-PIM-SM > Static RP Configuration".

Copyright © 3onedata Co., Ltd.

Interface Description

Static RP configuration interface as follow:



The main element configuration description of static RP configuration interface:

Interface Element	Description
IPv6	Configure the IPv6 address of the static RP. Note: When there is only one RP in the network, static RP can be manually configured instead of dynamic RP, which can avoid the frequent information interaction between C-RP and BSR occupying bandwidth.

8.7.3 C-RP Configuration of Interface

Function Description

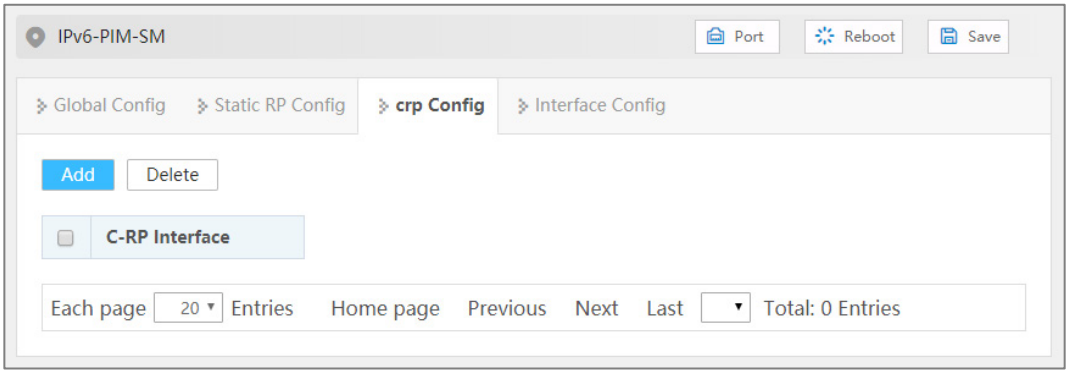
Add and delete C-RP interfaces.

Operation Path

Open in order: "Multicast Routing > IPv6-PIM-SM > Interface C-RP Configuration".

Interface Description

The interface C-RP configuration interface is as follows:



Copyright © 3onedata Co., Ltd.

Main element configuration description of interface C-RP configuration interface:

Interface Element	Description
C-RP interface	To configure the C-RP interface: • vlanif: vlanif interface

8.7.4 Interface Configuration

Function Description

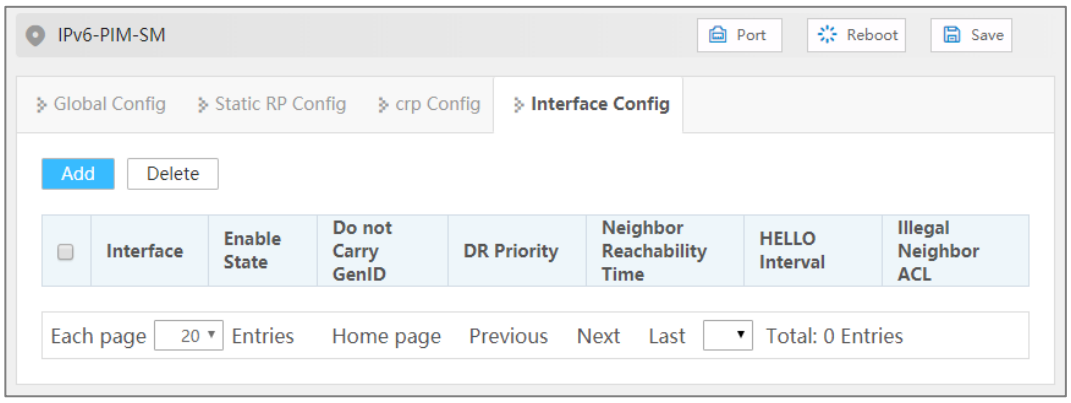
Set interface IPv6-PIM-SM parameters.

Operation Path

Open in order: "Multicast Routing > IPv6-PIM-SM > Interface Configuration".

Interface Description

Interface configuration interface as follows:



The main element configuration description of interface configuration interface:

Interface Element	Description
Interface	Configure interface: • vlanif: vlanif interface
Enable state	PIM-SM status. • enable • disable
Do not carry GenID	The interface is configured to send hello messages without carrying GenID information. Note: GenID is a random value at the initial creation of the interface to identify unique interface information. With this information, users can detect whether the neighbor device has been restarted.
DR Priority	Specify the priority of running for DR from 0 to 4294967294. Note:

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	The higher the value, the higher the priority.
Neighbor Reachability Time	Specify the time to keep PIM neighbor reachable, the value range is 1 ~ 65535, and the unit is seconds. Note: If specified as 65535 seconds, the PIM neighbor is always reachable.
Hello Interval	Time period for sending Hello messages between PIM routers.
Illegal Neighbor ACL	Illegal neighbor source address range.

8.8 IPv6-PIM-DM

Function Description

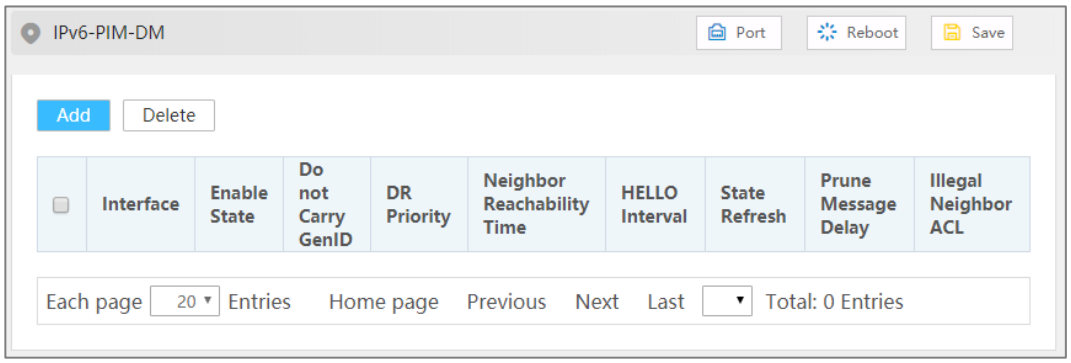
Configure IPv6-PIM-DM parameter.

Operation Path

Open in order:"Multicast Routing > IPv6-PIM-DM".

Interface Description

IPv6-PIM-DM interface is as below:



Main elements configuration descriptions of IPv6-PIM-DM interface:

Interface Element	Description
Interface	Configure interface: • vlanif: vlanif interface
Enable State	Enable status of interface PIM-DM.
Do not carry GenID	The interface is configured to send hello messages without carrying GenID information. Note:

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	GenID is a random value at the initial creation of the interface to identify unique interface information. With this information, users can detect whether the neighbor device has been restarted.
DR Priority	Specify the priority of running for DR from 0 to 4294967294. Note: The higher the value, the higher the priority.
Neighbor Reachability Time	Specify the time to keep PIM neighbor reachable, the value range is 1 ~ 65535, and the unit is seconds. Note: If specified as 65535 seconds, the PIM neighbor is always reachable.
Hello Interval	Time period for sending Hello messages between PIM routers.
State Refresh	The time interval for refreshing the pruning timer status, which can prevent the clipped interface from resuming forwarding due to the timeout of pruning timer, the value range is 1-100 seconds.
Prune Message Delay	The delay time of transmitting Prune message on the shared network segment, which ranges from 0 to 32767 milliseconds.
Illegal Neighbor ACL	Illegal neighbor source address range.

3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.

9 Network Management

9.1 SNMP

Now, the broadest network management protocol in network is SNMP (Simple Network Management Protocol). SNMP is the industrial standard that is widely accepted and comes into use, it's used for guaranteeing the management information transmission between two points in network, and is convenient for network manager search information, modify information, locate faults, complete fault diagnosis, conduct capacity plan and generate a report. SNMP adopts polling mechanism and only provides the most basic function library, especially suit for using in minitype, rapid and low price environment. SNMP implementation is based on connectionless transmission layer protocol UDP, therefore, it can achieve barrier - free connection to many other products.

9.1.1 SNMP Switch

Function Description

Enable/disable SNMP function.

Operation Path

Open in order: "Network Management > SNMP > SNMP Switch".

Interface Description

SNMP switch configuration interface as follows:

3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.



The main element configuration description of SNMP switch configuration interface.

Interface Element	Description
Enable	SNMP enable switch, which is enabled by default Note: If the agent side has opened, the SNMP server can't be closed.

9.1.2 View

Function Description

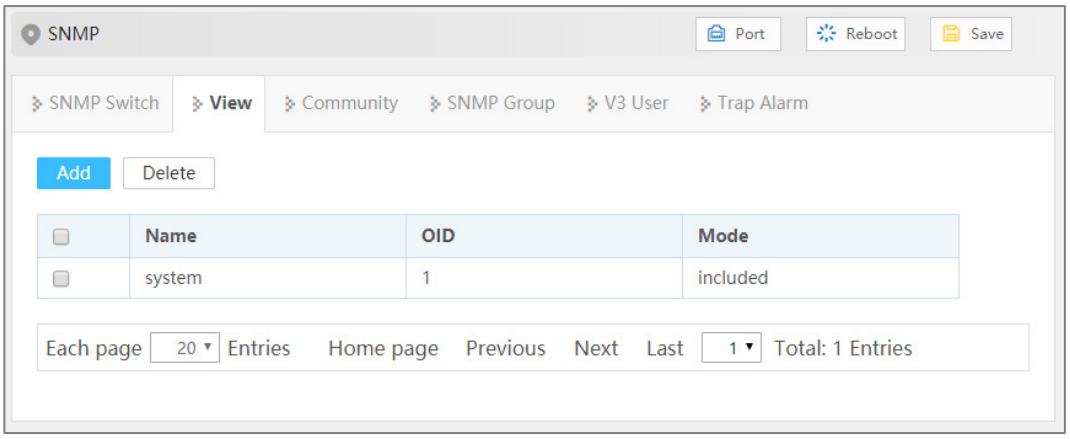
Add/delete SNMP view.

Operation Path

Open in order: "Network Management > SNMP > View".

Interface Description

View interface as below:



The main element configuration description of view interface:

Interface Element	Description
Name	SNMP view name definition, support 32 characters input.
OID	Node location information of MIB tree where the device resides.

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	Note: • OID object identifier, a component node of MIB, uniquely identified by a string of numbers that represent the path. • The information of OID could be viewed via the third-party software MG-SOFT MIB Browser.
Mode	Node OID dealing method, options as below: • Included: It contains all objects under the node subtree; • Excluded: Eliminate all objects beyond the node subtree.

9.1.3 Community

Function Description

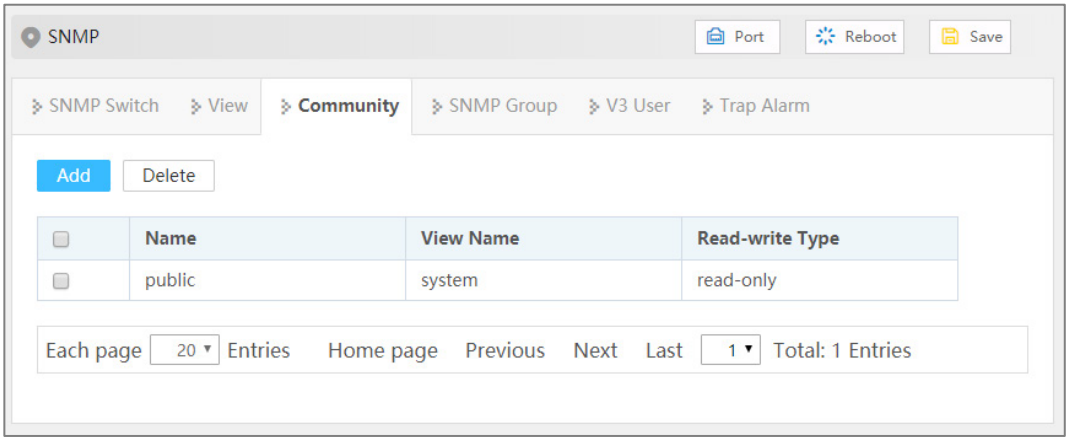
Add/delete SNMP community. Define MIB view that community name can access, set MIB object access privilege of community name as read-write privilege or read-only privilege.

Operation Path

Open in order: “Network Management > SNMP > Community”.

Interface Description

Community interface as below:



The main element configuration description of community interface:

Interface Element	Description
Name	Group name, including numbers or letters, with a length of no more than 32 characters.
View Name	SNMP view name.

Interface Element	Description
Read-write Type	View read-write permissions, options are as follows: • Read only • Read and write

9.1.4 SNMP Group

Function Description

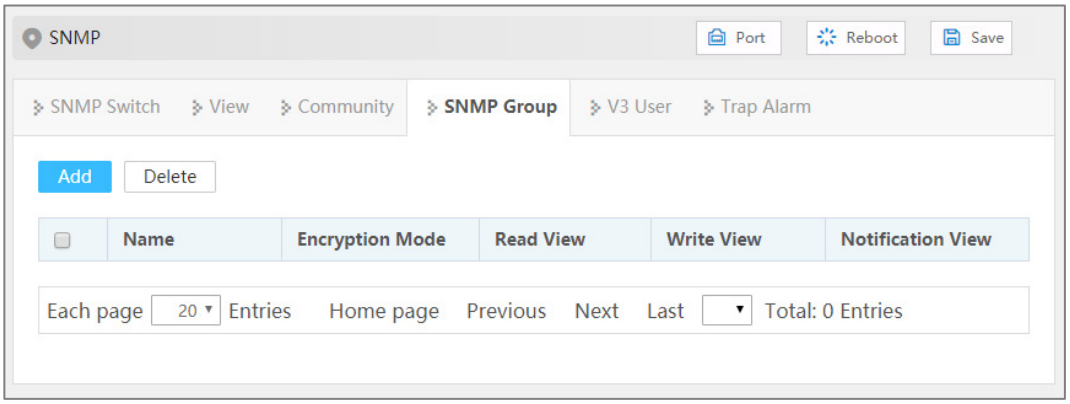
Configure a new SNMP group and set the secure mode and corresponding SNMP view of the SNMP group.

Operation Path

Open in order: “Network Management > SNMP > SNMP Group”.

Interface Description

SNMP Group interface as follows:



Main elements configuration description of SNMP Group interface:

Interface Element	Description
Name	SNMP group name, ranging from 1 to 32 bytes.
Encryption Mode	Whether to authenticate and encrypt the message, values: • auth: indicates that the message is authenticated but not encrypted; • noauth: indicates that the message is neither authenticated nor encrypted; • priv: indicates that the message is authenticated and encrypted.
Read-view	Specify the read view of the group.

3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.

Interface Element	Description
Write View	Specify the write and read view of the group
Notification view	Specify the notification view of the group.

9.1.5 V3 User

Function Description

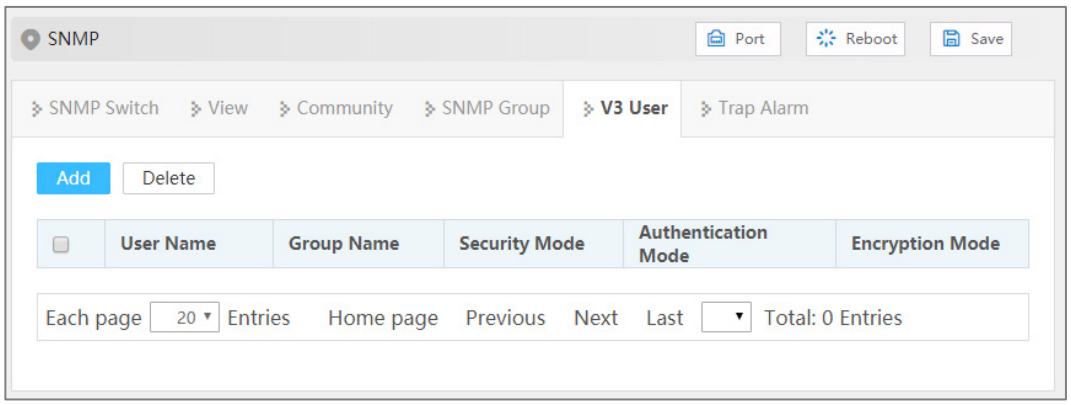
SNMPv3 adopts User-Based Security Model (USM) authentication mechanism. Network manager can configure authentication and encryption function. Authentication is used to verify the validity of the packet sender and prevent unauthorized users from accessing it. Encryption encrypts the transmission packet between NMS and Agent to prevent eavesdropping. It adopts authentication and encryption function to provide higher security for the communication between NMS and Agent.

Operation Path

Open in order: "Network Management > SNMP > V3 Users".

Interface Description

V3 user interface as follows:



The main element configuration description of V3 user interface:

Interface Element	Description
User Name	SNMP v3 user name definition, can only contain numbers, letters, or @_! , no longer than 32 characters.
Group Name	Group name, ranging from 1 to 32 bytes. Note: Group name must be created snmp group, and only created group

Interface Element	Description
	can create SNMP v3 users.
Security Mode	Whether to authenticate and encrypt the message, values: • auth: indicates that the message is authenticated but not encrypted; • noauth: indicates that the message is neither authenticated nor encrypted; • priv: indicates that the message is authenticated and encrypted.
Authentication mode	Authentication mode type, acceptable value: • Md5: Information abstract algorithm 5; • Sha: Secure hash algorithm.
Encryption Mode	V3 user data encryption algorithm, options as follows: • Des: Adopt data encryption algorithm; • Aes: Adopt advanced encryption standard.

9.1.6 Trap Alarm

Function Description

Base on TCP/IP protocol, SNMP usually adopts UDP port 161 (SNMP) and 162 (SNMP-traps), SNMP protocol agent exists in the network device and adopts information specific to the device (MIBs) as the device interface; these network devices can be monitored or controlled via Agent. When a trap event occurs, the message is transmitted by SNMP Trap. At this point, an available trap receiver can receive the trap message.

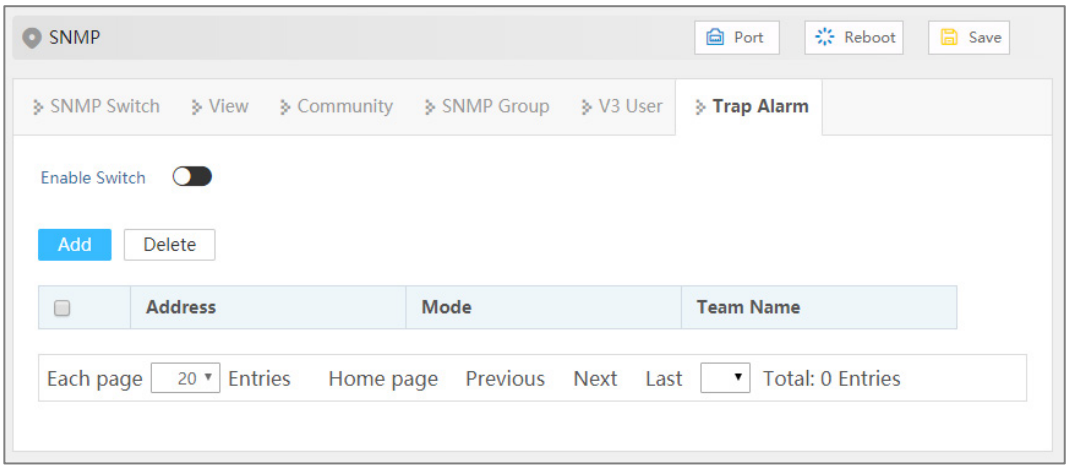
Operation Path

Open in order："Network Management > SNMP > trap Alarm".

Interface Description

Trap alarm interface as below:

Copyright © 3onedata Co., Ltd.



The main element configuration description of Trap alarm interface:

Interface Element	Description
Enable	SNMP Trap alarm enable switch.
Address	IP address of SNMP management device, used for receiving alarm information, such as PC.
Mode	SNMP management device version, options as below: • v1 • v2c
Team Name	Group name.

9.2 LLDP

LLDP (Link Layer Discovery Protocol) is a link layer discovery protocol defined in IEEE 802.1ab. LLDP is a standard layer-2 discovery method, which can organize the management address, device identification, interface identification and other information of local devices and publish it to its neighbor devices. After receiving the information, the neighbor devices save it in the form of standard MIB(Management Information Base) for the network management system to query and judge the communication status of links.

9.2.1 Global Configuration

Function Description

Configure LLDP global parameter.

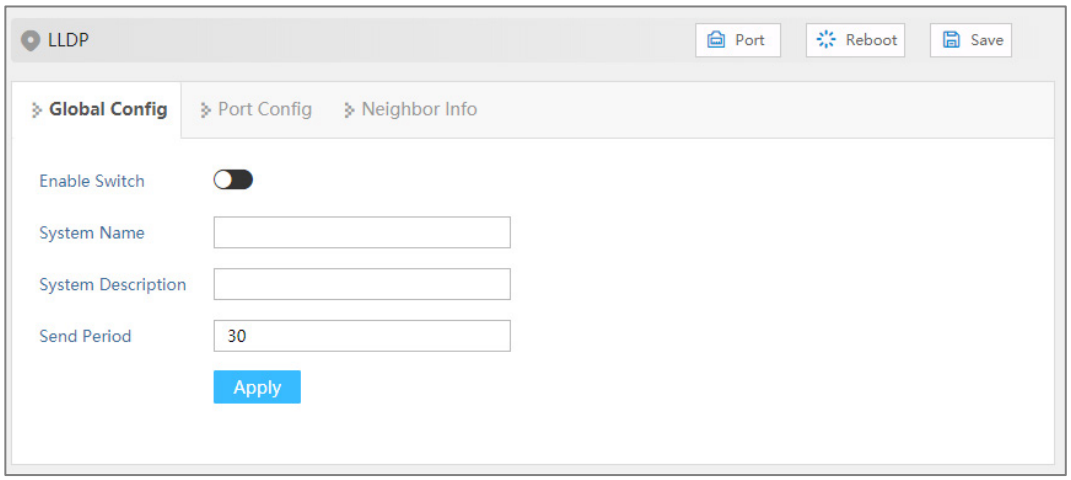
3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.

Operation Path

Open in order: "Network Management > LLDP > Global Configuration".

Interface Description

Global configuration interface is as follows:



The main element configuration description of global configuration interface:

Interface Element	Description
Enable	LLDP enable switch.
System Name	The system name, which supports 0-32 characters, consists of uppercase letters, lowercase letters, numbers or special characters (! @ _-).
System Description	The system description information, which supports 0-32 characters, consisting of uppercase letters, lowercase letters, numbers or special characters (! @ _-).
Send Period	LLDP message sending cycle, the value range is 5-32768. When no device status changes, the device periodically sends LLDP messages to its adjacent nodes. Note: Type of TLV(Type/Length/Value) encapsulated by LLDP message, which can include system name and system description.

9.2.2 Port Configuration

Function Description

Configure the sending and receiving mode and management address of the port.

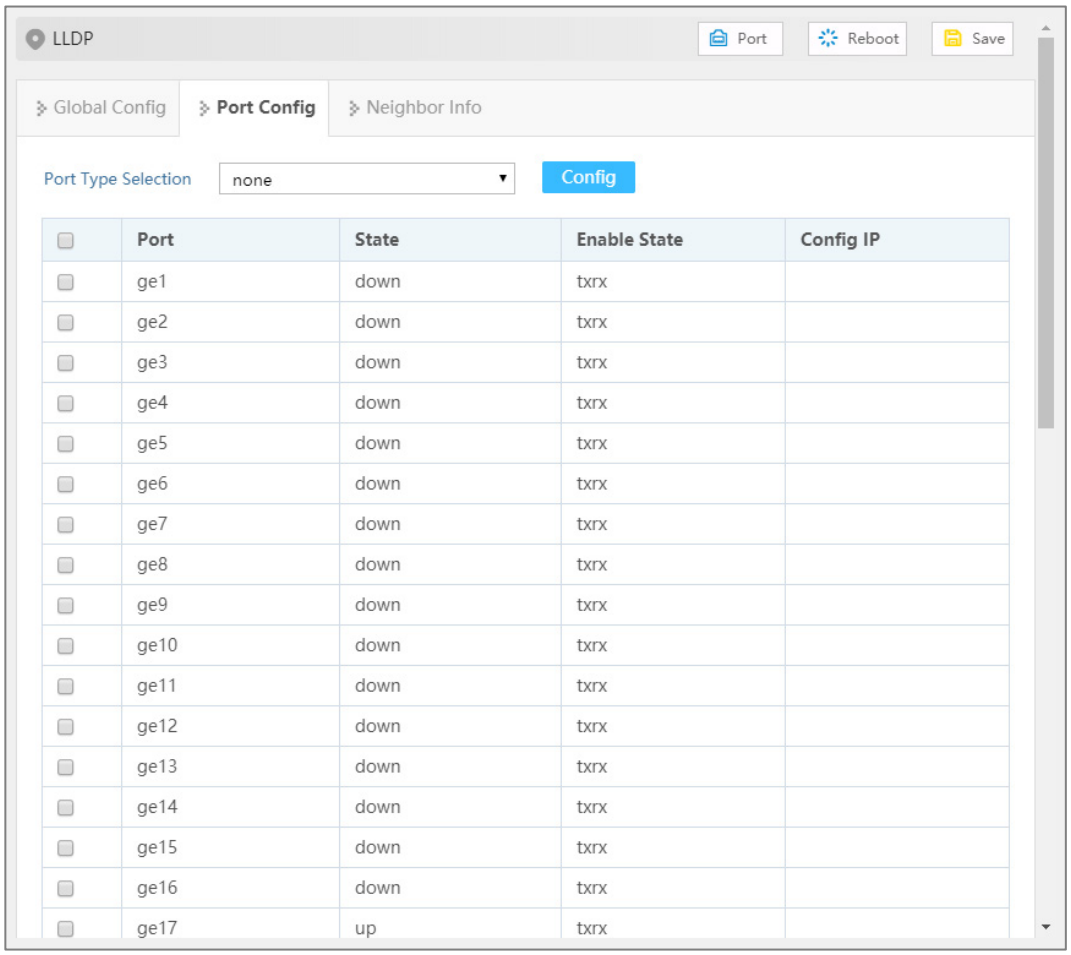
3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.

Operation Path

Open in order: "Network Management > LLDP > Port Configuration".

Interface Description

Check port configuration interface as below:



The main element configuration description of port configuration interface:

Interface Element	Description
Port	The corresponding port name of the device Ethernet port.
Port state	Ethernet port connection status, display status as follows: • down: port is disconnected • up: port is connected
Enable state	The options of LLDP working states of device port are as follows: • txonly: working mode is Tx, only sending and not receiving LLDP message. • rxonly: working mode Rx, only receiving and not sending LLDP message. • txrx: working mode is TxRx, both sending and receiving

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	LLDP message. • disable: work mode is Disable, it neither transmits nor receives LLDP message. Note: When global LLDP is enabled, the work mode of LLDP is TxRx by default.
Config IP	Corresponding LLDP management IP address of the port. Note: • LLDP management address is the address to be marked and managed by network management system. Management address can definitely mark a device, which is beneficial to the drawing of network topology and network management. Management address is encapsulated in Management Address TLV field of LLDP message and sent to adjacent nodes. • The management address released by the port in the LLDP message defaults to the main IP address of the smallest VLAN of the VLANs this port is in. If the VLAN is not configured with a main IP address, it will be 0.0.0.0.

9.2.3 Neighbor Information

Function Description

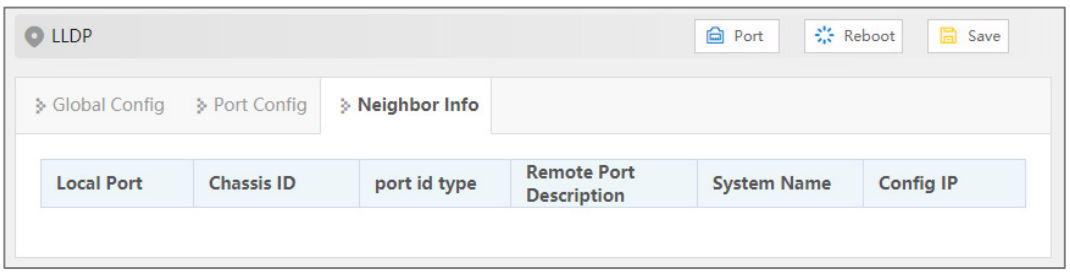
View neighbor-related information.

Operation Path

Open in order: " Network Management > LLDP > Neighbor Information".

Interface Description

Neighbor information interface as follows:



Main elements configuration description of neighbor information interface:

Interface Element	Description
Local Port	Local port number of local switch connected to adjacent

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	devices.
Chassis ID	Neighbor device ID.
port id type	Subtype of neighbor port ID.
Remote Port Description	Port number of neighbor device.
System Name	System name of the neighbor device.
Config IP	Management IP address of neighbor device or port.

9.3 DHCP-Server

DHCP(Dynamic Host Configuration Protocol) is usually applied to large LAN environment. Its main functions are centralized management and IP address distribution, which enables the host in the network to acquire IP address, Gateway address, DNS server address dynamically and improve the usage of addresses.

9.3.1 DHCP Switch

Function Description

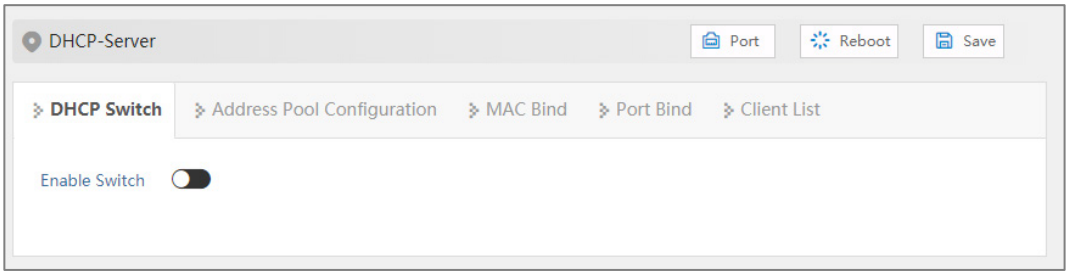
Enable/Disable DHCP Server.

Operation Path

Open in order: "Network Management > DHCP-Server> DHCP Switch".

Interface Description

DHCP switch configuration interface as follows:



The main element configuration description of DHCP switch configuration interface.

Interface Element	Description
Enable	The enable switch of DHCP server, when enabled, it can assign IP addresses to other devices connected to this

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	device.

9.3.2 DHCP Pool Configuration

After user defines DHCP range and exclusion range, surplus addresses constitute an address pool; addresses in the address pool can be dynamically distributed to hosts in network. Address pool is valid only for the method of automated IP acquisition; manual IP configuration can ignore this option only if conforming to the rules.

Function Description

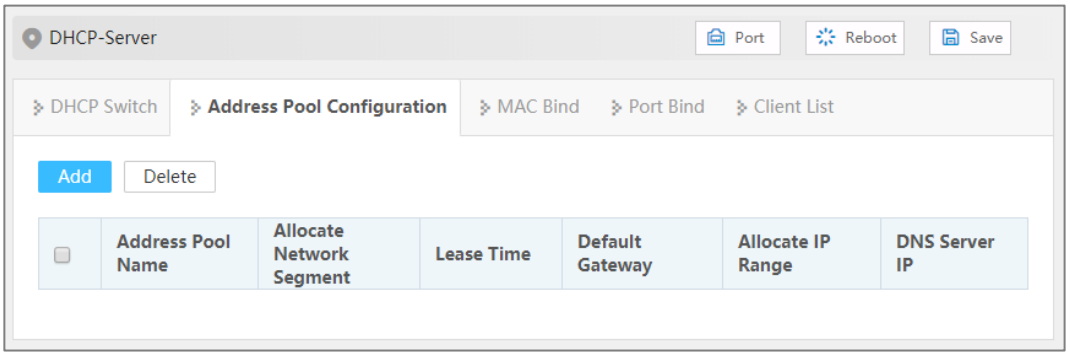
Add, delete the address pool and check the configuration information of address pool.

Operation Path

Open in order: "Network Management > DHCP > Pool Configuration".

Interface Description

DHCP address pool configuration interface as follows:



The main element configuration description of DHCP pool configuration interface:

Interface Element	Description
Address Pool Name	The name of address pool, up to 32 characters.
Allocate Network Segment	Address pool distributes the IP address network segment of client, for example: 192.168.0.1/24.
Lease Time	IP address utilization valid time of client, format: day, hour, minute, range is 0-30 day, 0-24h and 0-59m, which are separated by space. Note: When the time of ip address obtained by dhcp client reaches the lease time, it needs to renew it otherwise the ip address would be invalid and dhcp client needs to request ip address again.

Copyright © 3onedata Co., Ltd.

Interface Element	Description
Default Gateway	Default client gateway address, example: 192.168.1.0/24
Allocate IP Range	The lowest address and the highest address in the DHCP address pool. The address that belongs to the range could be distributed effectively.
DNS Server IP	IP address of DNS server.

9.3.3 MAC Binding

Function Description

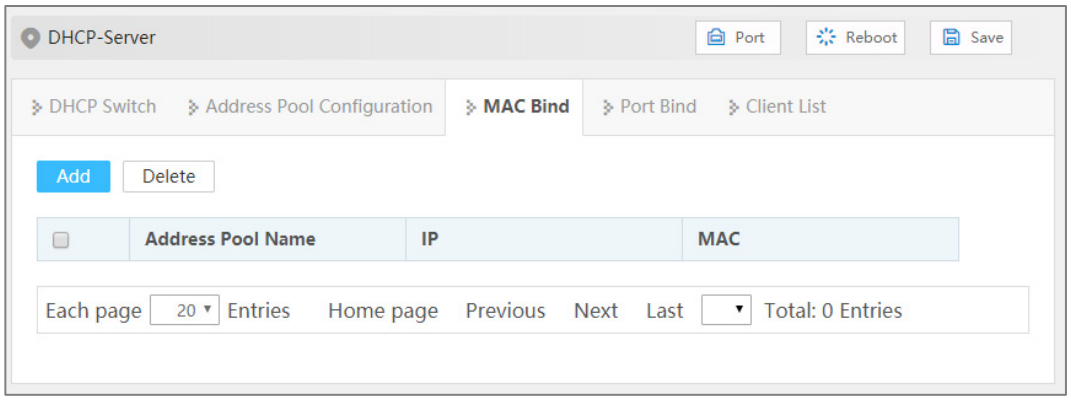
Bind the IP address assigned by the address pool to the MAC address of the device.

Operation Path

Open in order: "Network Management > DHCP Server > MAC Bind".

Interface Description

MAC binding interface is as follows:



The main element configuration description of MAC binding interface:

Interface Element	Description
Address Pool Name	The name of DHCP address pool.
IP	IP addresses distributed by DHCP address pool, IP addresses obtained by this MAC address.
MAC	The MAC address of the IP-bound device.

Copyright © 3onedata Co., Ltd.

9.3.4 Port Binding

Function Description

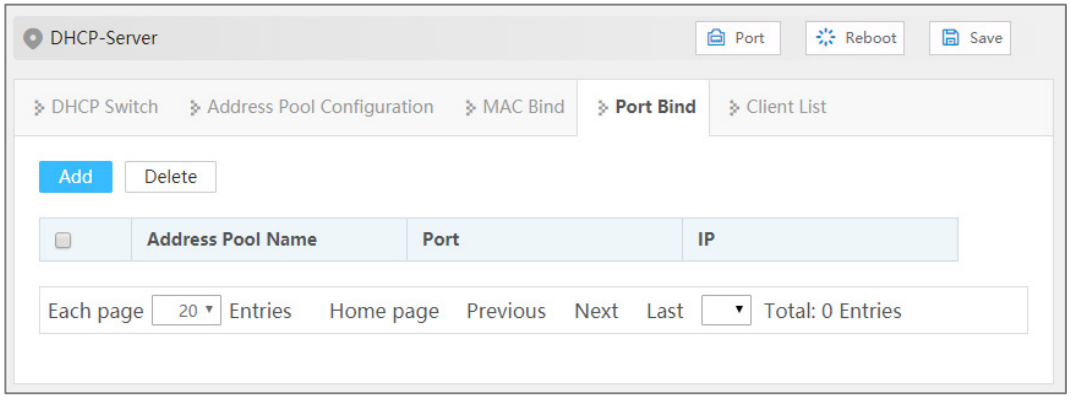
The IP address that can be assigned by the binding port.

Operation Path

Open in order: "Network Management > DHCP Server > Port Bind".

Interface Description

Port binding interface as follows:



The main element configuration description of port binding interface:

Interface Element	Description
Address Pool Name	The name of DHCP address pool.
Port	The corresponding port name of the device Ethernet port.
IP	IP address that DHCP address pool distributes, the IP addresses that client gains in the port.

9.3.5 Client List

Function Description

Check the information of DHCP client.

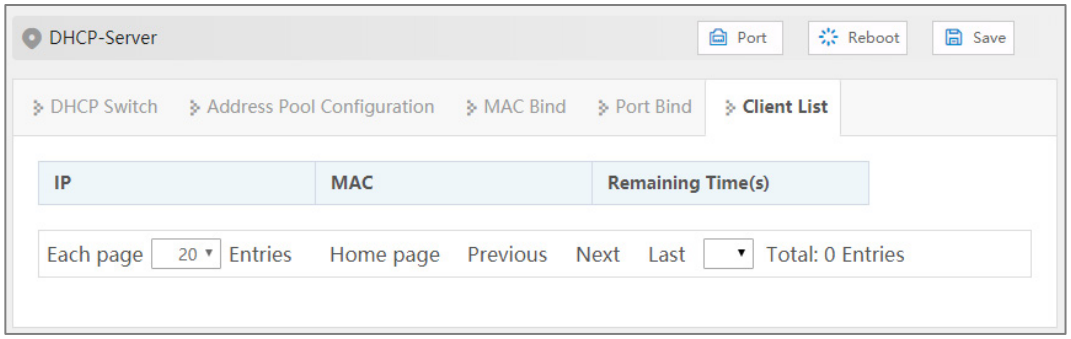
Operation Path

Open in order: "Network Management > DHCP-Server > Client List".

Interface Description

Client list interface as follows:

Copyright © 3onedata Co., Ltd.



The main element configuration description of client list interface:

Interface Element	Description
IP	IP address of DHCP client-side device.
MAC	MAC address of DHCP client device.
Remaining time (s)	Aging time of IP address acquired by DHCP client.

9.4 DHCP-Relay

DHCP relay agent forwards DHCP messages between a DHCP server and DHCP clients, and helps the DHCP server to dynamically allocate network parameters to the DHCP clients. When a DHCP server is on a different network segment from the DHCP client, the DHCP server can not receive request messages from the DHCP client, a DHCP relay agent must be deployed to forward DHCP messages to the DHCP server.

Function Description

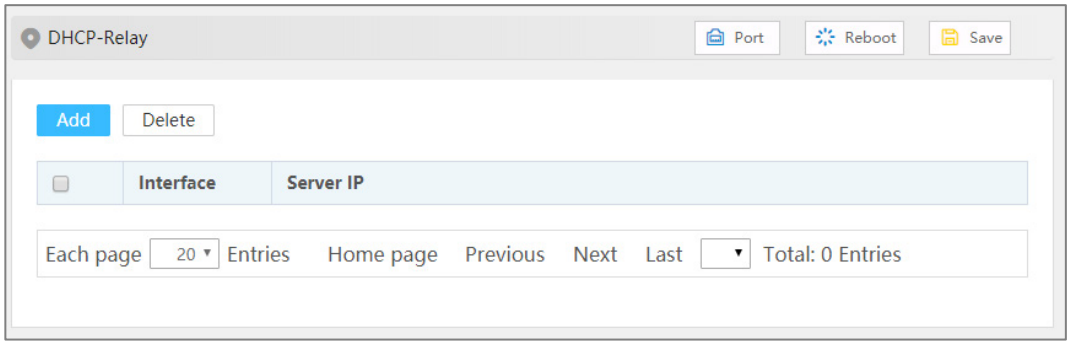
Configure the related parameters of the Relay interface.

Operation Path

Open in order: "Network Settings > DHCP-Relay".

Interface Description

DHCP-Relay interface is as follows:



Copyright © 3onedata Co., Ltd.

Main element configuration description of DHCP-Relay interface:

Interface Element	Description
Interface	Interface Name.
Server IP	IP address of DHCP server represented by DHCP relay.

3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.

10 TSN Management

TSN(Time Sensitive Network) is a new generation network standard based on Ethernet. It provides a general time-sensitive mechanism for the MAC layer of Ethernet protocol, so as to realize the deterministic transmission of key data such as voice, video and industrial automation instructions with low latency and high reliability in Ethernet. TSN is a set of protocol standards, mainly including clock synchronization, flow control, reliability, security and other parts. In the actual application process, the corresponding protocol combination can be selected according to the application requirements.

10.1 PTP

PTP(Precision Time Protocol) is a time synchronization protocol for high-precision frequency synchronization and phase synchronization between network nodes. IEEE1588 is the basic protocol of PTP, which specifies the principle of high-precision clock synchronization in the network and the specification of message interaction processing. Therefore, PTP is also called IEEE1588 for short. The 1588 is divided into two versions: 1588v1 and 1588v2. The 1588v1 can only achieve sub-millisecond time synchronization accuracy, while the 1588v2 can achieve sub-microsecond synchronization accuracy, which can realize both phase synchronization and frequency synchronization. Today, 1588v1 is basically replaced by 1588v2. Based on IEEE 1588, PTP derived IEEE 802.1AS and other protocols. Different PTP protocol standards have different usage scenarios and different functions, but their principles are basically the same. On the basis of IEEE1588, IEEE802.1AS refines it to form a more targeted time synchronization mechanism. It only supports two-step and P2P mode, but does not support UDP protocol and single-step and E2E mode.

3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.

10.1.1 Clock Configuration

Function Description

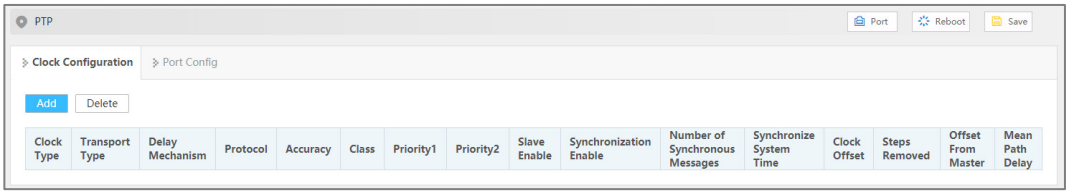
Configure the PTP clock.

Operation Path

Open in order: "TSN Management > PTP > Port Configuration".

Interface Description

Clock setting interface as follows:



Main elements configuration description of clock configuration interface:

Interface Element	Description
Clock Type	Clock node options as follows: • boundary: Boundary Clock This clock node has multiple PTP interfaces in the same PTP domain to participate in time synchronization. It synchronizes the time from the upstream clock node through one interface, and issues the time to the downstream clock node through the other interfaces. In addition, when the clock node is used as the clock source, the time can be released to the downstream clock node through multiple PTP interfaces. • ordinary: Ordinary Clock This clock node has only one PTP interface in the same PTP domain to participate in time synchronization, and it synchronizes time from the upstream clock node through this interface. In addition, when the clock node is used as the clock source, the time can be released to the downstream clock node through only one PTP interface. • transparent: transparent clock. This clock node has multiple PTP interfaces, but it only forwards PTP protocol messages between these interfaces and corrects the forwarding delay, and does not synchronize the time

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	through any interface.
Transport type	The encapsulation types used for transmitting PTP messages are as follows: • ethernet：Ethernet encapsulation • udp v4：IPv4 UDP encapsulation • udp v6: IPv6 UDP encapsulation
Delay mechanism	Link delay measurement mechanism, options are as follows: • e2e: Request response mechanism E2E(End to End), which calculates the time difference according to the overall path delay time between master and slave clocks. If there is a transparent clock between the master clock and the slave clock, the transparent clock does not calculate the average path delay. • p2p: Peer-to-peer delay mechanism, which calculates the time difference according to the delay time of each link between master and slave clocks. If there is a transparent clock between the master clock and the slave clock, the transparent clock will participate in calculating the path delay of each link.
Protocol	Clock protocol type, options are as follows: • ieee1588 • 8021as
Accuracy	The time accuracy of the clock source, it ranges from 0 to 255. The smaller the value, the higher the accuracy. Note: When each clock node in PTP domain dynamically selects the optimal clock through BMC protocol, it will compare it according to the order of the first priority, time level, time accuracy, clock deviation and second priority of the clock carried in the Announce message, and the winner will become the optimal clock.
Class	The time level of the clock source, it ranges from 0 to 255. The smaller the value, the higher the level.
Priority 1	Priority 1 of the clock source. Value range is 0-255, smaller value represents higher priority.
Priority 2	Priority 2 of the clock source. Value range is 0-255, smaller value represents higher priority.
Slave enable	When the clock node is an ordinary clock, the restrictions on the slave clock are as follows:

3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.

Interface Element	Description
	• disable: Cancel the restriction that the local clock cannot be elected as the master clock. • enable: only as a slave clock, limiting that the local clock cannot be elected as the master clock.
Synchronization Enable	Synchronization enable, options as follows: • enable • disable
Number of synchronous messages	Number of synchronous messages, ranging from 50 to 500.
Synchronize system time	Update the master clock time of PTP domain to the system clock, with the following options: • enable • disable
Clock offset	The logarithmic variance of the offset scale of the clock source, which measures the time offset. The value range is 0-65535.
Steps removed	Displays the number of hops from the current clock to the main clock.
Offset from master	Displays the deviation between the current clock and the main clock time.
Mean Path Delay	Displays the path delay of the current clock from the master clock or neighboring nodes.

10.1.2 Port Configuration

Function Description

Configure PTP port.

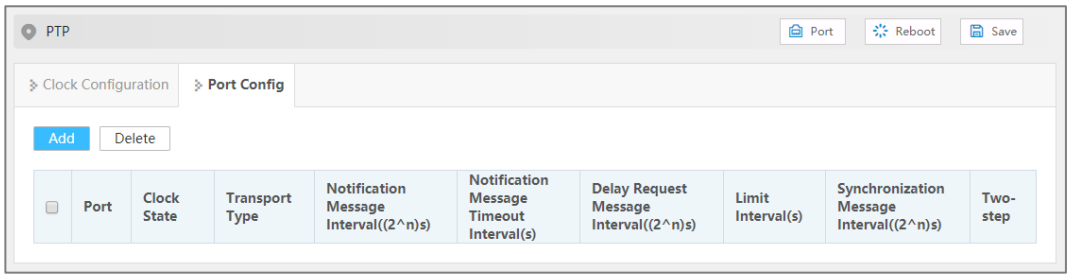
Operation Path

Open in order: "TSN Management > PTP > Port Configuration".

Interface Description

Check port configuration interface as below:

Copyright © 3onedata Co., Ltd.



The main element configuration description of port configuration interface:

Interface Element	Description
Port	The corresponding port name of the device Ethernet port.
Clock state	Display port PTP clock state.
Transport type	The encapsulation type used for transmitting PTP messages at the port can be selected as follows: • ethernet：Ethernet encapsulation • udp v4：IPv4 UDP encapsulation • udp v6: IPv6 UDP encapsulation
Notification Message Interval ((2^n)s)	The time interval for the main node to periodically send the Announce message, with the range of 0-4th power second of 2.
Notification Message Timeout Interval (s)	The timeout of receiving the Announce message from the node is a multiple of the period of sending the Announce message from the master node, and the value range is 2-10.
Delay_Req Message Interval ((2^n)s)	The time interval for sending the delay request message, the value range is 0-5th power second of 2.
Limit Interval (s)	The minimum time interval for sending the Delay_Req message, the value range is 1-10th power second of 2.
Synchronous Message Interval ((2^n)s)	Specifies the time interval for sending Sync message, ranging from is -3-3th power second of 2.
Two-Step	The dual-step clock mode is enabled, and the options are as follows: • enable: the carrying mode of time stamp is two-step mode, that is, neither the Sync message nor the Pdelay_Resp message carries the time stamp of the time when this message was sent, but is carried by other subsequent messages.

3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.

Interface Element	Description
	• disable: the carrying mode of timestamp is single-step mode, that is, the event messages Sync and Pdelay_Resp have the timestamp of the sending time of this message, and the announcement of time information is completed at the same time of message sending and receiving.

10.2 QBV

The enhancement function of scheduled traffic of IEEE 802.1QBV (Enhancements for Scheduled Traffic) belongs to the flow control part of TSN protocol family. According to the characteristics of device flows, time-sensitive flows and non-time-sensitive flows are mapped to queues of different interfaces, and then the data flows in the queues are controlled by TAS(Time Aware Shaper). In TAS, the concept of a transmission gate is introduced, which has two states of "open" and "close". The data stream can only be transmitted when the state of the door is open, and the state of the door is defined in the gating list. The 802.1Qbv function cycle executes the gating list to schedule the forwarding of messages in the queue, which can guarantee the bandwidth and delay of those queues with strict requirements on transmission time.

10.2.1 Global Configuration

Function Description

Configure global parameters of 802.1Qbv.

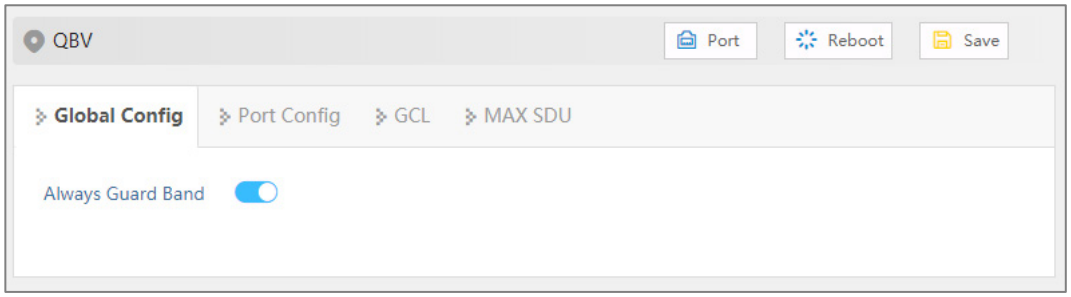
Operation Path

Open in order: "TSN Management > QBV > Global Configuration".

Interface Description

Global configuration interface is as follows:

Copyright © 3onedata Co., Ltd.



The main element configuration description of global configuration interface:

Interface Element	Description
Always Guard Band	802.1Qbv guard band is the buffer band between two nodes in TSN forwarding scheduling control list. The protection band is used to ensure that the device can completely forward the currently transmitted data frame when scheduling the 802.1Qbv forwarding queue.

10.2.2 Port Configuration

Function Description

Configure 802.1Qbv port parameter.

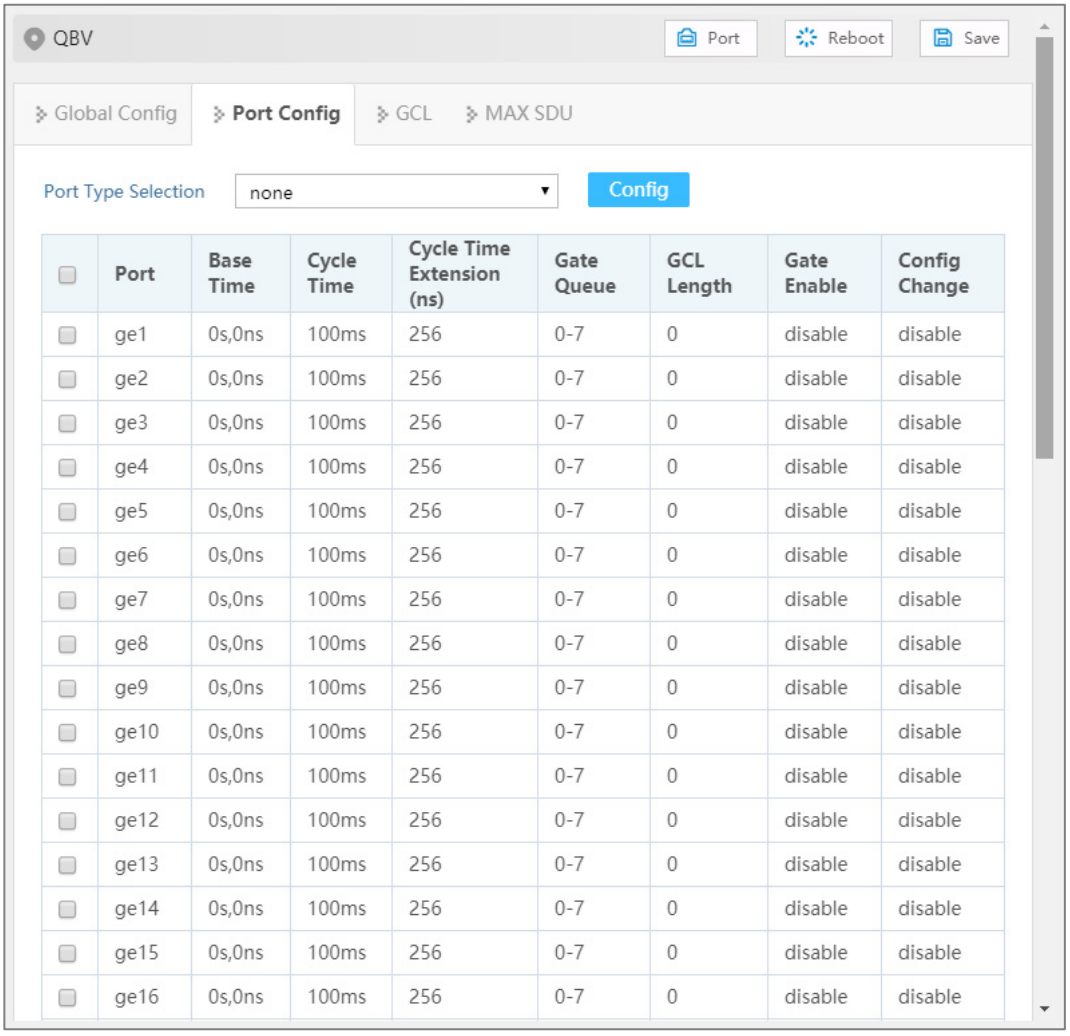
Operation Path

Open in order: "TSN Management > QBV > Port Configuration".

Interface Description

Check port configuration interface as below:

3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.



Port	Base Time	Cycle Time	Cycle Time Extension (ns)	Gate Queue	GCL Length	Gate Enable	Config Change
ge1	0s,0ns	100ms	256	0-7	0	disable	disable
ge2	0s,0ns	100ms	256	0-7	0	disable	disable
ge3	0s,0ns	100ms	256	0-7	0	disable	disable
ge4	0s,0ns	100ms	256	0-7	0	disable	disable
ge5	0s,0ns	100ms	256	0-7	0	disable	disable
ge6	0s,0ns	100ms	256	0-7	0	disable	disable
ge7	0s,0ns	100ms	256	0-7	0	disable	disable
ge8	0s,0ns	100ms	256	0-7	0	disable	disable
ge9	0s,0ns	100ms	256	0-7	0	disable	disable
ge10	0s,0ns	100ms	256	0-7	0	disable	disable
ge11	0s,0ns	100ms	256	0-7	0	disable	disable
ge12	0s,0ns	100ms	256	0-7	0	disable	disable
ge13	0s,0ns	100ms	256	0-7	0	disable	disable
ge14	0s,0ns	100ms	256	0-7	0	disable	disable
ge15	0s,0ns	100ms	256	0-7	0	disable	disable
ge16	0s,0ns	100ms	256	0-7	0	disable	disable

The main element configuration description of port configuration interface:

Interface Element	Description
Port	The corresponding port name of the device Ethernet port.
Base Time	The management value of the benchmark is expressed as the IEEE 1588 Precision Time Protocol (PTP) time scale. Base time is used to calculate when the device executes the scheduling algorithm.
Cycle Time	The cycle time of the periodic execution of the port gating list, which consists of values and units. Periodic time unit, which can be milliseconds, microseconds or nanoseconds. The default value is 100 milliseconds.
Cycle Time Extension	When a new cycle time is configured, the maximum time allowed to extend the port gating cycle time is nanosecond, with the range of 256-99999999 and the default value of 256 nanoseconds.

3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.

Interface Element	Description
Gate Queue	When there is no active door control list on the port, the initial value of the port door control list. Selected or configured gate queue, and the gating is in the "on" state; On the contrary, the gating is in the "off" state.
GCL Length	The length parameter of the management gate control list of the port. Valid range is 0 to 256. The integer value indicates the number of entries of the door control element in the door control list. The length of the gating list should be configured before configuring the gating list GCL.
Gate Enable	The enabled state of the port traffic scheduling function.
Config Change	Changing the configuration parameter indicates the start of the configuration change. After changing the configuration, the configured administrator value would be Oper value, and displayed in Monitor/TSN/TAS web. • If the parameter benchmark time is a future value, this configuration would be changed at the benchmark time. • If the benchmark time is a past value, this configuration would be changed as soon as possible. Actually, it will be in about 2 seconds, within an integer cycle time before the benchmark time configuration value. In this way, the synchronization between the schedules in the elements across the scheduling network can be maintained.

10.2.3 GCL

Function Description

Configure the gate control list GCL of the port to realize the scheduling of the port forwarding queue and the forwarding of messages.

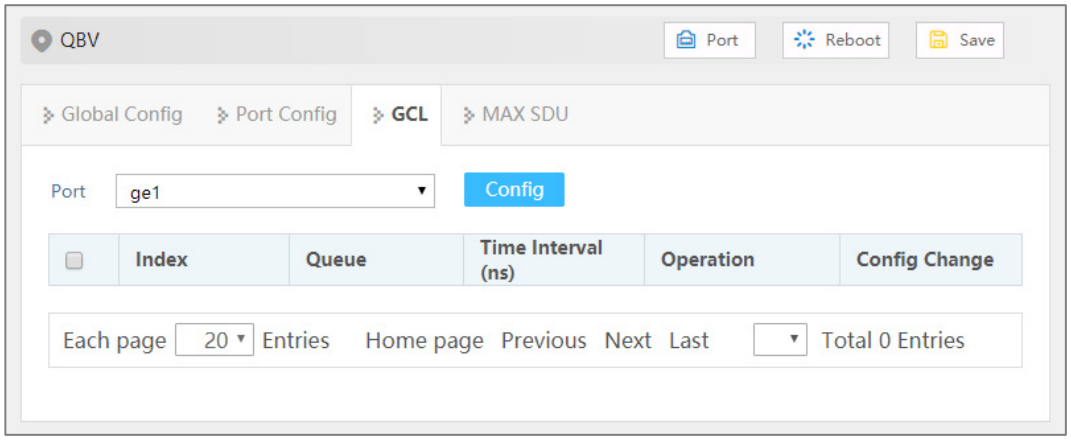
Operation Path

Open in order: "TSN Management > QBV > GCL".

Interface Description

GCL interface is as below:

Copyright © 3onedata Co., Ltd.



Main elements configuration descriptions of GCL interface:

Interface Element	Description
Index	Gate index flag, the maximum value corresponds to the length of GCL.
Queue	The queue number of data transmission allowed when the gate is open, and the value range is 0-7.
Time Interval	The duration of the on/off state is the time interval to the next state, and the value range is 1-99999999 nanoseconds.
Operation	The gate operation options are as follows: • set: it means that the state of the door is immediately set to the state set by the gating parameters, and changes to the next state after the duration (time interval to the next state) is over. This operation is the default operation. • set-hold: all operations defined by the set operation are performed, except that the beginning of this operation marks a point in the sequence of gate operations, in which the MAC associated with the port will stop sending preemptible frames. If frame preemption is not supported or enabled, this operation is the same as the set operation. • set-release: all operations defined by the set operation are performed. In addition, the beginning of this operation marks a point in the sequence of gate operations, at which the MAC related to the port is allowed to resume transmission of preemptible frames; If a fast frame is currently being transmitted by the MAC, the recovery preemptible frame takes effect at the end of the

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	transmission. If frame preemption is not supported or enabled, this operation is the same as the set operation.
Config Change	The door pre-configuration changes the enabling state.

10.2.4 MAX SDU

Function Description

Configure the maximum SDU size parameter value of the flow category supported by the port. The maximum SDU size parameter is used to calculate the guard band time, which is = MAX SDU*8/LINK_SPEED (sec). If frame preemption is enabled and the gate operation is set-hole, the guard band time in the preemptible queue is automatically selected as the minimum fragment size of frame preemption plus 64 bytes, and the queue is preemptible. If frame preemption is enabled and the queue is not opened in the set-hold gate operation, the queue is called a preemptible queue.

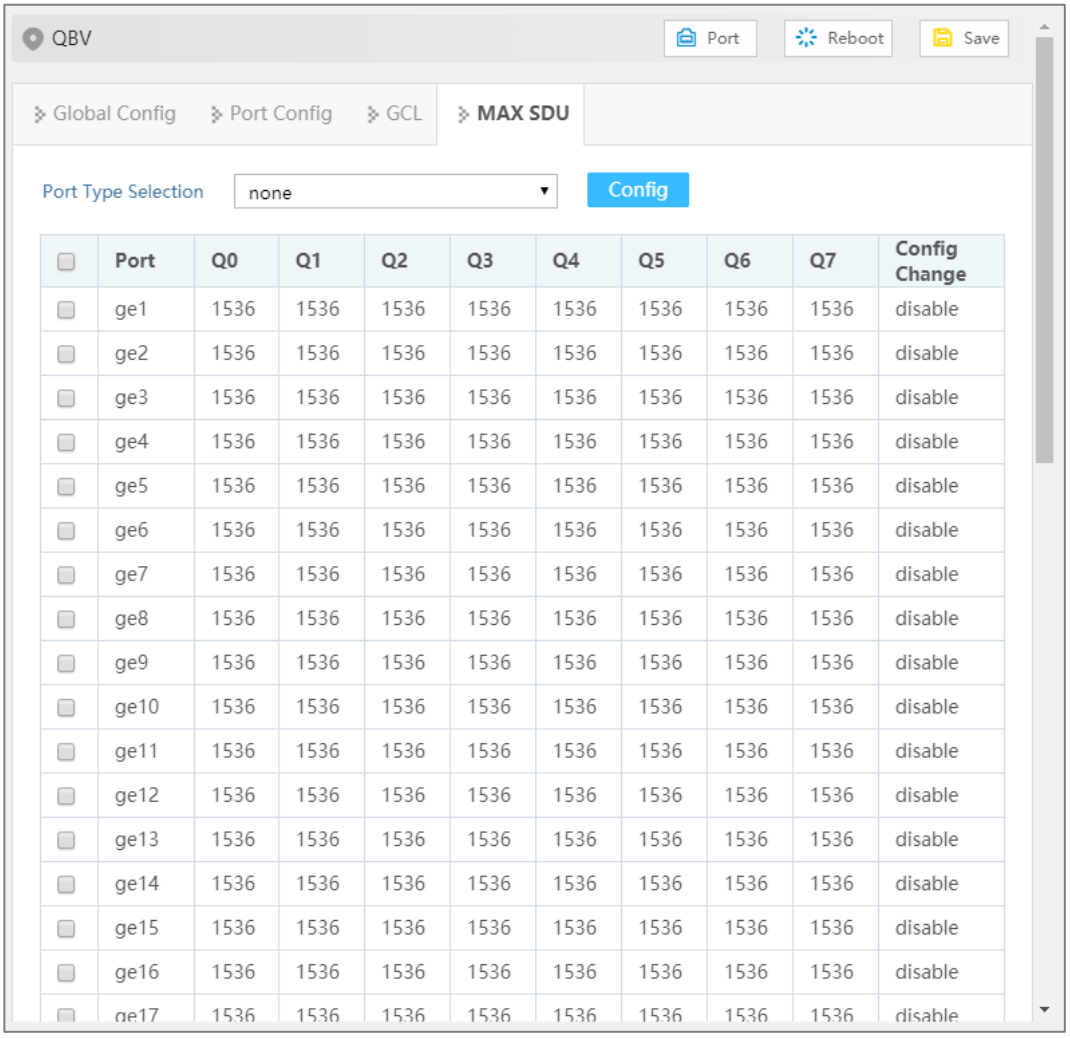
Operation Path

Open in turn: "TSN Management > QBV > MAX SDU".

Interface Description

MAX SDU interface as follows:

3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.



Port	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Config Change
ge1	1536	1536	1536	1536	1536	1536	1536	1536	disable
ge2	1536	1536	1536	1536	1536	1536	1536	1536	disable
ge3	1536	1536	1536	1536	1536	1536	1536	1536	disable
ge4	1536	1536	1536	1536	1536	1536	1536	1536	disable
ge5	1536	1536	1536	1536	1536	1536	1536	1536	disable
ge6	1536	1536	1536	1536	1536	1536	1536	1536	disable
ge7	1536	1536	1536	1536	1536	1536	1536	1536	disable
ge8	1536	1536	1536	1536	1536	1536	1536	1536	disable
ge9	1536	1536	1536	1536	1536	1536	1536	1536	disable
ge10	1536	1536	1536	1536	1536	1536	1536	1536	disable
ge11	1536	1536	1536	1536	1536	1536	1536	1536	disable
ge12	1536	1536	1536	1536	1536	1536	1536	1536	disable
ge13	1536	1536	1536	1536	1536	1536	1536	1536	disable
ge14	1536	1536	1536	1536	1536	1536	1536	1536	disable
ge15	1536	1536	1536	1536	1536	1536	1536	1536	disable
ge16	1536	1536	1536	1536	1536	1536	1536	1536	disable
ge17	1536	1536	1536	1536	1536	1536	1536	1536	disable

The main element configuration description of MAX SDU interface:

Interface Element	Description
Port	The corresponding Ethernet port name of the device.
Q0-Q7	The maximum size of SDU allowed by each queue under the port, in bytes, ranging from 64 to 10240, with the default value of 1536.
Confg Change	Port pre-configuration changes enable configuration.

10.3 QBU

IEEE 802.1Qbu(Frame Preemption) mechanism can interrupt the transmission of standard Ethernet frames or super-long frames to allow the transmission of high-priority frames, and then continue to transmit the previously interrupted messages. 802.3br divided the given bridge interfaces into two MAC services, namely

Copyright © 3onedata Co., Ltd.

pMAC(preemptable MAC) and eMAC(express MAC). Based on the implementation of 802.3br, 802.1Qbu divides data messages into pMAC frames and eMAC frames according to their grades. The transmitting pMAC frame can be preempted by eMAC frame. After the transmission of eMAC frame is completed, the transmission of pMAC frame can be resumed.

Function Description

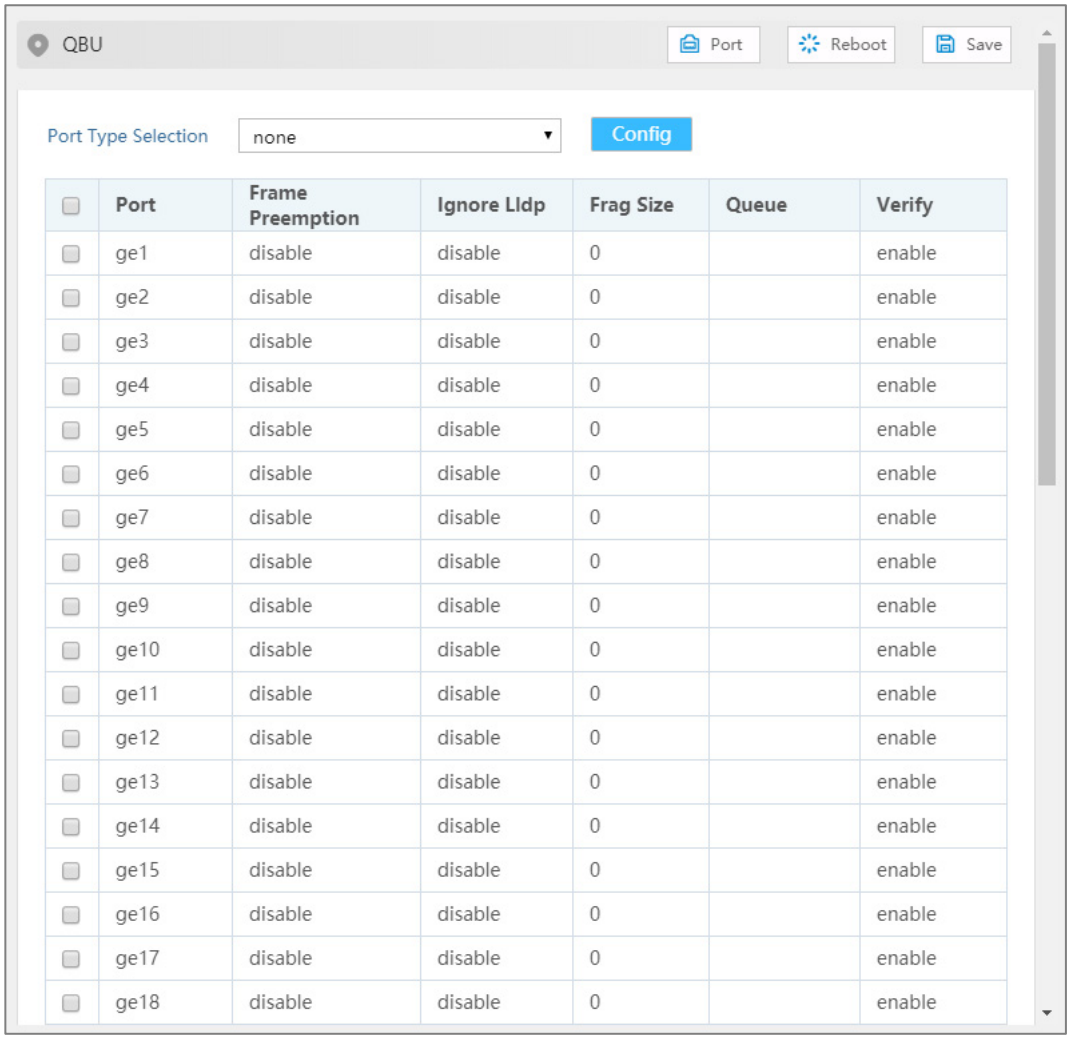
Configure 802.1Qbu Related Parameters

Operation Path

Open in order: “TSN Management > QBU”.

Interface Description

QBU interface is as below:



Main elements configuration descriptions of QBU interface:

Interface Element	Description
Port	The corresponding port name of the device Ethernet port.

Copyright © 3onedata Co., Ltd.

Interface Element	Description
Frame Preemption	Frame Preemption function status, options as follows: • enable • disable
Ignora Lldp	After enabling ignore LLDP, do not wait to receive LLDP messages before the sending direction starts frame preemption; If the frame preemption function is enabled, frame preemption will be activated.
Queue	This parameter is the management value of preemption status of priority. • If this option is selected, the preemptable service of the port will be used to transmit the frames with priority, and the value is preemptable. • If this option is not checked, the express service of this port will be used to transmit the frames waiting for priority, and preemption is enabled on this port. The value is express.
Verify	The 802.3br MAC merge verification of the port disables the value of the sending parameter. This value determines whether the authentication function is disabled (TRUE) or enabled (FALSE) in the MAC merge sublayer of the transmission direction.

10.4 Stream

TSN stream is the key traffic flow in TSN network that needs deterministic transmission. After receiving the message, the interface judges whether the traffic is TSN stream according to the flow characteristics. The flow characteristic parameters include the source MAC address, destination MAC address and VLAN ID of the message. The more stream characteristic parameters specified on the interface, the more accurate the matching.

Function Description

Configure stream instance.

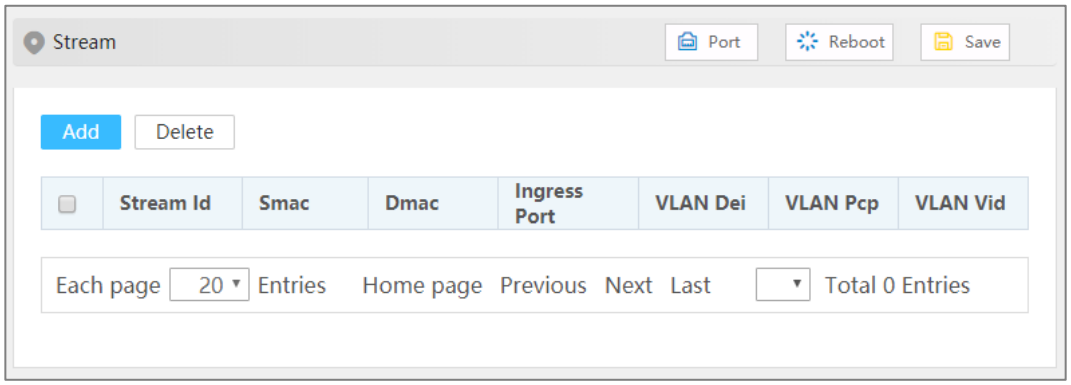
Operation Path

Open in order: “TSN Management > Stream”.

Copyright © 3onedata Co., Ltd.

Interface Description

Stream interface is as below:



Main elements configuration descriptions of Stream interface:

Interface Element	Description
Stream Id	Stream instance ID, the value range is 1-127.
Smac	The source MAC address of the instance, the options are as follows: • any: Match any source MAC address to enter the stream instance. • mac: matches the specific source MAC address to enter the stream instance.
Dmac	The destination MAC address propagation type of the instance, with the following options: • any: Any destination MAC address, including unicast, multicast and broadcast. • broadcast: Broadcast MAC. • mac: unicast MAC, which can specify a specific destination MAC address. • multicast: Multicast MAC.
Ingress Port	The port mapped to the stream instance.
VLAN Dei	The DEI(Drop Eligible Indicator) of an instance drops the priority indication, and the value range is 0-1. • 0: means Not Allowed to be discarded (not allowed) • 1: indicates that it is allowed to be discarded (Required) Note: • The 802.1Q VLAN tag TCI(Tag Control Information) part of the header of the data frame consists of three parts: DEI, PCP/PRI and VID. • DEI (Drop Eligible Indicator), used in conjunction with

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	PCP/PRI field, jointly indicates the discard priority of frames. For example, when the network is congested, these messages are discarded first.
VLAN Pcp	PCP(Priority Code Point) of an instance is the QoS priority of a frame, and its value ranges from 0 to 7. Note: The higher the priority value, the higher the priority. During network congestion, data frame with higher priority would be preferentially sent.
VLAN Vid	VLAN ID of stream instance, value range is 1-4094.

10.5 CB

IEEE 802.1CB (Frame Replication and Elimination for Reliability, FREP). The 802.1CB protocol is mainly responsible for the redundant backup transmission of data, and uses the redundancy mechanism to solve the information error or loss caused by network failure in the ring network. When sending, it will label and sequence code specific data, and copy the transmission on different paths. At the link convergence point, the replication information will be identified and eliminated to prevent the upper application of the receiving node from processing multiple duplicate data.

Function Description

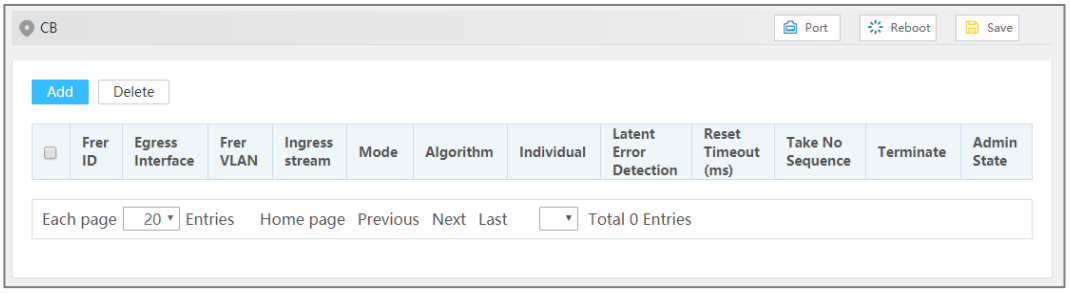
Configure 802.1CB Related Parameters.

Operation Path

Open in order: “TSN Management > CB”.

Interface Description

CB interface is as below:



Main elements configuration descriptions of CB interface:

Interface Element	Description

Copyright © 3onedata Co., Ltd.

Interface Element	Description
Frer ID	The ID of FRER instance, its value range is 1-127.
Egress Interface	The egress port of the FRER instance, with a maximum of 8 egress ports.
Frer VLAN	VLAN ID to which the inbound stream is classified, value range is 1-4094.
Ingress stream	The list of ingress stream IDs mapped to the FRER instance. In the sequence generation mode, only one stream ID can be specified.
Mode	FRER sequence mode of the instance, the options are as follows: • generation: sequence generation mode • recovery: sequence recovery mode
Algorithm	Type of sequence recovery algorithm in the FRER instance, the options are as follows: • vector: vector recovery algorithm • match: matching recovery algorithm
Individual	Individual recovery function. Each member flow will run the recovery function before submitting it to the composite recovery function. • disable • enable
Latent Error Detection	Latent error detection function, the options are as follows: • disable • enable
Reset Timeout	The reset time parameter of the sequence recovery function, with a value range of 1-4095, is in milliseconds.
Take No Sequence	Accept all frames, whether they are marked with R-tag or not, with the following options: • disable • enable
Terminate	Before sending the frame packet at the exit, remove the R-tag label of the data frame, and the following options are available: • disable • enable

3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.

Interface Element	Description
Admin State	FRER instance enable configuration status, options as follows: • disable • enable

10.6 QCI

IEEE 802.1QCI (Per-Stream Filtering and Policing). 802.1Qci uses Stream ID to identify a single stream, and then filters, gates, schedules and counts each stream to ensure that the filtered data is forwarded at the specified time.

10.6.1 Flow Meter

Function Description

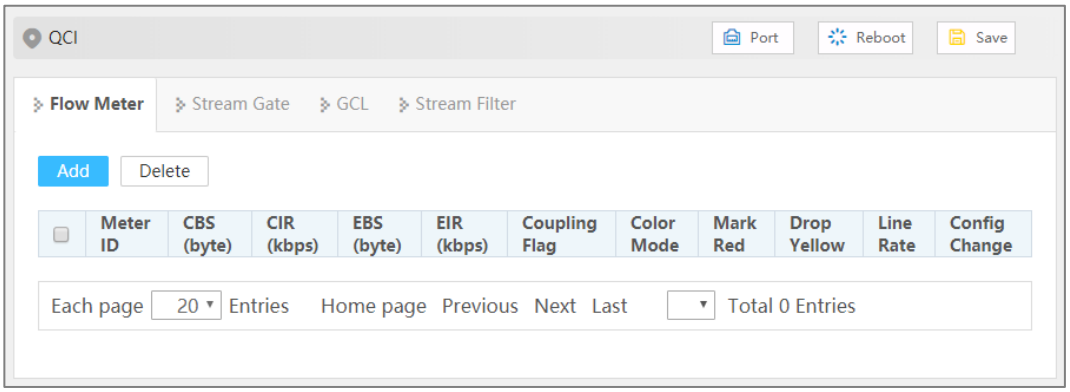
Configure the flow meter instance.

Operation Path

Open in turn: "TSN Management > QCI > Flow Meter".

Interface Description

Flow Meter interface as below:



The main element configuration description of Flow Meter interface:

Interface Element	Description
Meter ID	The ID of Flow Meter instance, its value range is 0-1022.
CBS (byte)	The promised burst size of burst traffic is 0-4294967294.
CIR (kbps)	Committed information rate, indicating the rate of putting tokens into the token bucket, the unit is bit/s, and the value

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	range is 0-4294967294.
EBS (byte)	Excess burst size, which is used to define the maximum burst amount before all traffic exceeds CIR. The value range is 0-4294967294.
EIR (kbps)	Excess information rate, the range of which is 0-4294967294.
Coupling Flag	Coupling flag, which is used to indicate whether the remaining token after the transmission of the "green" data frame can be used for the transmission of the "yellow" data frame. The options are as follows: • disable • enable
Color Mode	Color mode setting, the options are as follows: • disable: Color-blind mode, color is not enabled and color is not distinguished. • enable: color sensitive mode, which enables color and is color sensitive.
Mark Red	After the flow metering is enabled, mark all data frames in red, which means that all data frames will be discarded. The options are as follows: • disable: indicates the normal color mark of the passed data frame. • enable: indicates that all passed data frames are marked in red and discarded.
Drop Yellow	Discard the data frame marked yellow, with the following options: • disable: indicates that data frames marked with yellow are not discarded. • enable: indicates that the data frame marked yellow is discarded.
Line Rate	Port egress speed limit type, options are as follows: • disable: disable/Data Rate • enable: enable/Line Rate
Config Change	Turn on the flow metering function.

Copyright © 3onedata Co., Ltd.

10.6.2 Stream Gate

Function Description

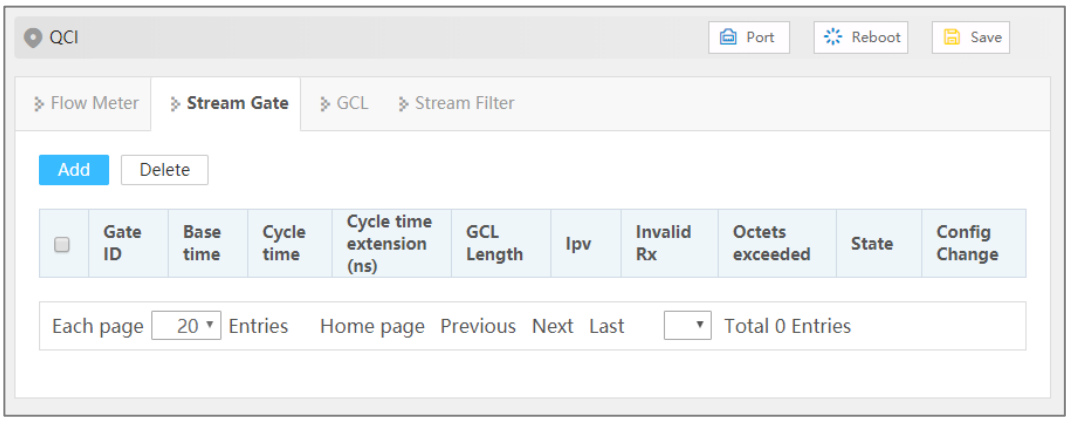
Configure the flow gating instance.

Operation Path

Open in turn: "TSN Management > QCI > Stream Gate".

Interface Description

Stream Gate interface as below:



The main element configuration description of Stream Gate interface:

Interface Element	Description
Gate ID	The ID of Stream Gate instance, its value range is 0-1022.
Base time(s)	The management benchmark time of the system, with values ranging from 0-4294967294 seconds and 0-99999999 nanoseconds.
Cycle time	The cycle time of the gating list, ranging from 0-99999999, is in ms, ns or us.
Cycle time extension	The management extension Cycle time of the gating list ranges from 256-99999999, and the unit is determined by the unit of Cycle Time.
GCL Length	The length of the gating list needs to be configured before setting specific gating parameters, and the value range is 0-4.
Ipv	The internal priority value corresponding to the whole gating instance, ranging from 0 to 7. After setting, the data frame corresponding to the internal priority value will be mapped to this gating instance for processing.

3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.

Interface Element	Description
Invalid Rx	When this function is enabled, the data received when the queue door is closed is considered invalid, and the invalid data will be discarded. By default, this function is turned off.
Octets exceeded	After this function is enabled, if the size of the accepted data exceeds the number of bytes of the maximum service unit set by the queue, it will be regarded as invalid data, which will be discarded and the default function will not be turned on.
State	Set the initial state of the front door of the running gate list. The options are as follows: • close • open
Config Change	When gating is enabled, the modified configuration will be stored in the cache area first. You need to enable this function to write the cached configuration before you can apply the updated configuration. Options are as follows: • disable • enable

10.6.3 GCL

Function Description

Configure gating list parameters.

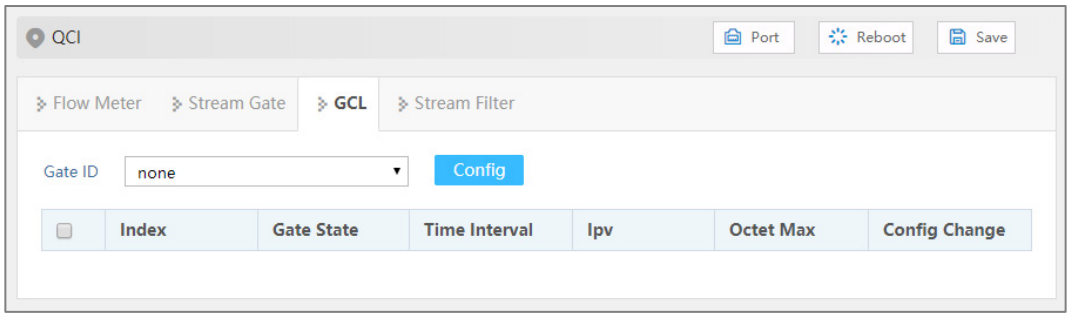
Operation Path

Open in order: "TSN Management > QCI > GCL".

Interface Description

GCL interface is as below:

Copyright © 3onedata Co., Ltd.



Main elements configuration descriptions of GCL interface:

Interface Element	Description
Index	Sequence number of the gating list, with the maximum value corresponding to the length of GCL Length.
Gate State	Current gate status, options as follows: • close • open
Time Interval	The duration of the current gate, with a value range of 0-99999999, and the unit is ms, ns or us.
Ipv	Data frames passing through this queue will be given the set ipv value. The internal priority value of the data in the queue corresponding to the gate ranges from 0 to 7.
Octet Max	The maximum byte data frame size that the queue can handle, if it exceeds, it will be judged whether to discard the data according to the enabling condition. The number of bytes of the maximum service unit allowed by the queue corresponding to the gate ranges from 0 to 10000.
Config Change	When gating is enabled, the modified configuration will be stored in the cache area first. You need to enable this function to write the cached configuration before you can apply the updated configuration.

10.6.4 Stream Filter

Function Description

Configure the flow filtering instance.

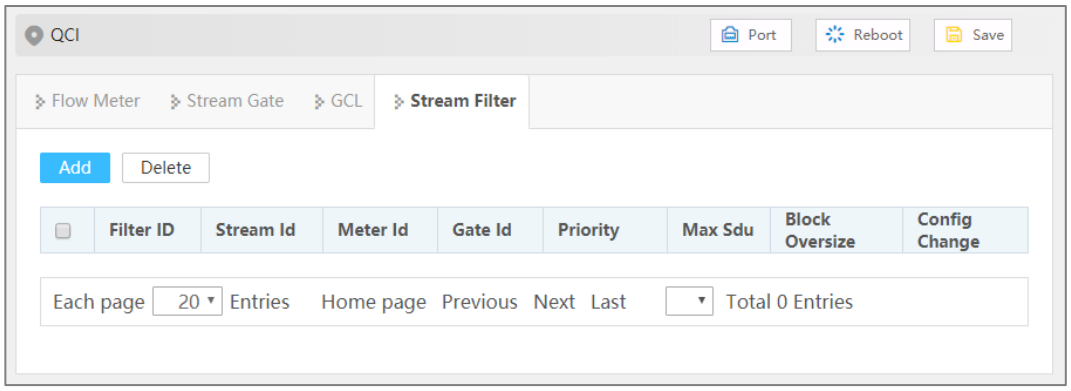
Copyright © 3onedata Co., Ltd.

Operation Path

Open in turn: "TSN Management > QCI > Stream Filter".

Interface Description

Stream Filter interface as below:



The main element configuration description of Stream Filter interface:

Interface Element	Description
Filter ID	The ID of Stream Filter instance, its value range is 0-1022.
Stream Id	List of instance IDs.
Meter Id	Flow measurement instance ID list, which transfers the business flow after flow filtering to the specified flow measurement ID.
Gate Id	The list of flow gating instance IDs, which specifies the business flow after the flow filter, is passed to the specified flow gating ID.
Priority	Configure priority value, options are as follows: • 0-7: Single priority value. • any: a wildcard value that matches any priority value.
Max Sdu	The maximum SDU size of PSFP, ranging from 0 to 65535. Set the maximum SDU size. Frames exceeding this SDU size will not pass through the stream filter. If all other stream filtering conditions are met, frames not exceeding this SDU size can pass through the stream filter.
Block Oversize	Enable parameter of flow blocking caused by oversize frame. Options are as follows: • enable: enables the function of filtering the frame size to start the flow blocking. • disable: The function of filtering the frame size to start stream blocking is disabled.

3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.

Interface Element	Description
Config Change	Used to save configuration. When gate enables configuration change, it is necessary to issue config-change before applying the configuration. • enable • disable

3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.

11 System Maintenance

11.1 Network Diagnosis

11.1.1 Ping

Function Description

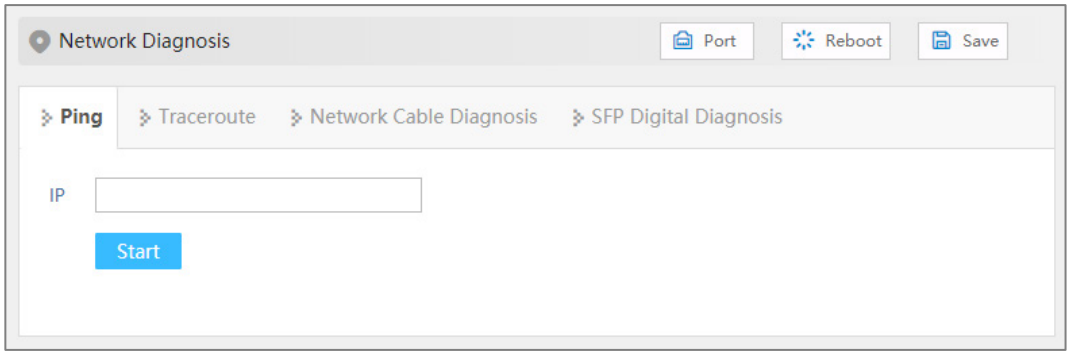
Ping is used to check whether the network is open or network connection speed. Ping utilizes the uniqueness of network machine IP address to send a data packet to the target IP address, and then ask the other side to return a similarly sized packet to determine whether two network machines are connected and communicated, and confirm the time delay.

Operation Path

Open in order: "System Maintenance > Network Diagnosis > Ping".

Interface Description

The Ping interface is as follows:



The main elements configuration description of Ping configuration interface:

Interface Element	Description

Interface Element	Description
IP	The IPv4 or IPv6 address of the detected device, that is, the destination address. The device can check the network intercommunity to other devices via the ping command.

11.1.2 Traceroute

Function Description

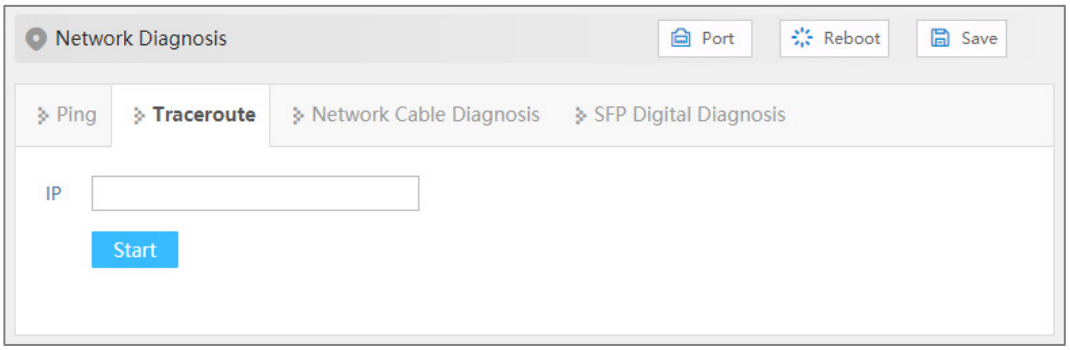
Test the network situation between the switch and the target host. Traceroute measures how long it takes by sending small packets to the destination device until they return. Each device on a path Traceroute returns three test results. Output result includes each test time (ms), device name (if exists) and the IP address.

Operation Path

Open in order: "System Maintenance > Network Diagnosis > Traceroute".

Interface Description

Traceroute interface as follows:



The main element configuration description of Traceroute interface:

Interface Element	Description
IP	Destination device IPv4 or IPv6 address, fill in the opposite device IP address that needs test.

11.1.3 Network Cable Diagnosis

Function Description

It can detect whether there is a fault in the cable used by the copper port of the device. When the cable is in normal condition, the length in the detection information refers to

Copyright © 3onedata Co., Ltd.

the total length of the cable. When the cable is in abnormal condition, the length in the detection information refers to the length from this interface to the fault location. The 8-wire network cable has 4 groups of differential lines, and the device can detect the length and status of each group of differential lines.

Note

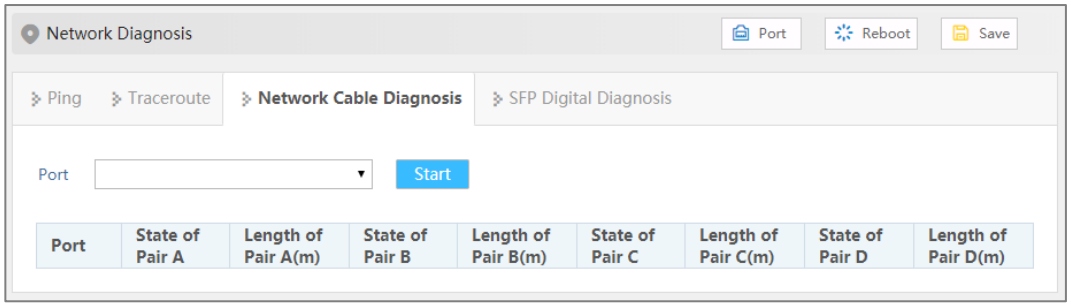
- The accuracy of detecting cable length is about 5 meters, and the test results are for reference only. The test results of different types or different manufacturers may be different.
- When testing, it will affect the normal use of the interface business in a short time, and may also cause the interface of UP to oscillate.

Operation Path

Open in order: "System Maintenance > Network Diagnosis > Network Cable Diagnosis".

Interface Description

Network cable diagnosis interface screenshot is as follows:



Main elements configuration description of network cable diagnosis interface:

Interface Element	Description
Port	The corresponding port name of the device Ethernet port.
State of Pair A/B/C/D	The state of the differential line, such as OK (normal), OPEN (open circuit), SHORT (short circuit), CROSS (cross/crosstalk), etc.
Length of Pair A/B/C/D (m)	Length of the differential line, unit: meter.

3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.

11.1.4 SFP Digital Diagnosis

Function Description

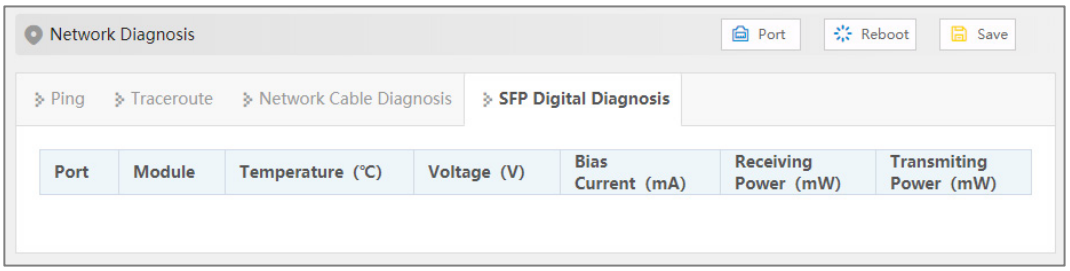
Monitor SFP parameters in real time. This function has greatly facilitated the troubleshooting process of optical fiber link and the cost of on-site debugging.

Operation Path

Open in order: "System Maintenance > Network Diagnosis > SFP Digital Diagnosis".

Interface Description

The SFP digital diagnostic interface is as follows:



The main element configuration description of SFP digital diagnosis interface:

Interface Element	Description
Port	The corresponding port name of the device Ethernet port.
Module	Parameter information of optical module:
Temperature(℃)	This device's SFP temperature. Its unit is ℃. The operating temperature of this SFP module should be within the
Voltage (V)	The voltage that this device offers SFP. Its unit is V. Overvoltage could lead to the breakdown of CMOS device; under voltage would disable the normal operation of lasers.
Bias current (mA)	The bias current of laser.
Receiving power (mW)	Optical input power, referring to the lowest optical power of receiving in certain rate and bit error rate.
Transmiting power (mW)	Optical output power, referring to the output power of optical source in the sending end of optical module.

3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.

11.2 Time

11.2.1 NTP Configuration

NTP protocol refers to Network Time Protocol. Its destination is to transmit uniform and standard time in international Internet. Specific implementation scheme is appointing several clock source websites in the network to provide user with timing service, and these websites should be able to mutually compare to improve the accuracy. It can provide millisecond time correction, and is confirmed by the encrypted way to prevent malicious protocol attacks.

Function Description

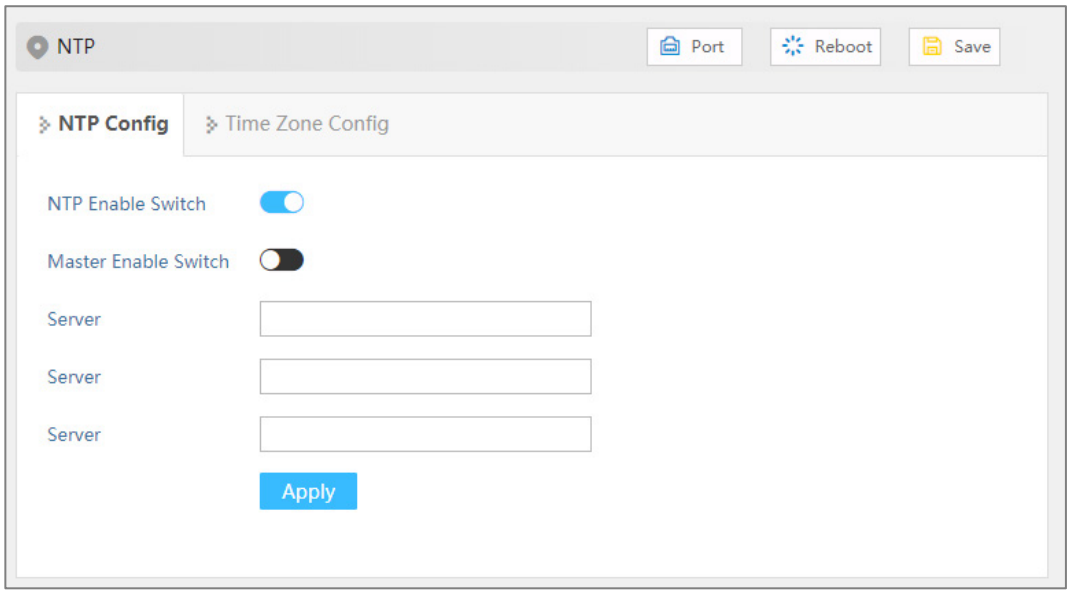
Configure the device time and NTP server information.

Operation Path

Open in order: "System Maintenance > Time > NTP Configuration".

Interface Description

NTP configuration interface is as follows:



The main element configuration description of NTP configuration interface:

Interface Element	Description
NTP Enable	NTP protocol enable switch.
Master Enable Switch	Master enable switch, after enabled, the device starts NTP service, and uses the local clock of the device as NTP master clock to provide clock source for other devices.

Copyright © 3onedata Co., Ltd.

Interface Element	Description
Server	IP address of NTP server, for example: 192.168.1.1. Note: As NTP client, the system will synchronize time with NTP server every 11 minutes.

11.2.2 Time Zone Configuration

Function Description

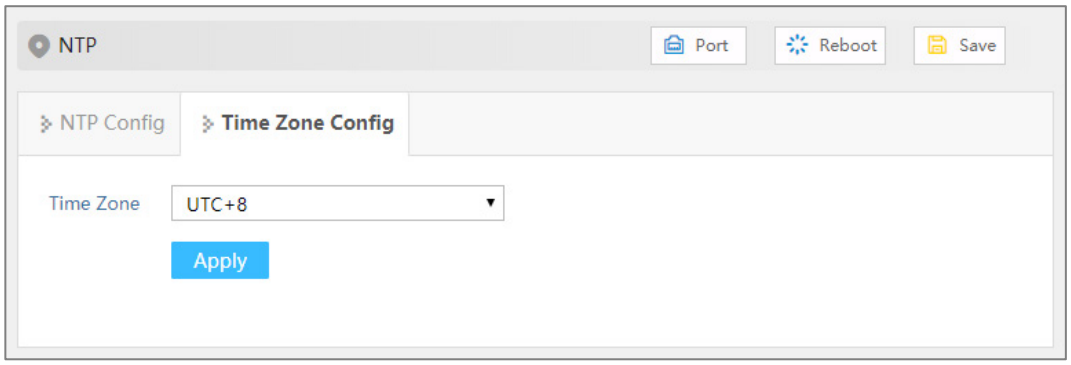
Configure the device time zone.

Operation Path

Open in order: "System Maintenance > Time > Time Zone Configuration".

Interface Description

Time Zone Configuration interface as follows:



Main elements configuration description of time zone configuration interface:

Interface Element	Description
Time Zone	UTC(Universal Time Coordinated) time zone. Due to different regions, users can freely set the system clock according to the regulations of their own country or region.

Copyright © 3onedata Co., Ltd.

11.3 Alarm

11.3.1 Port Alarm

Function Description

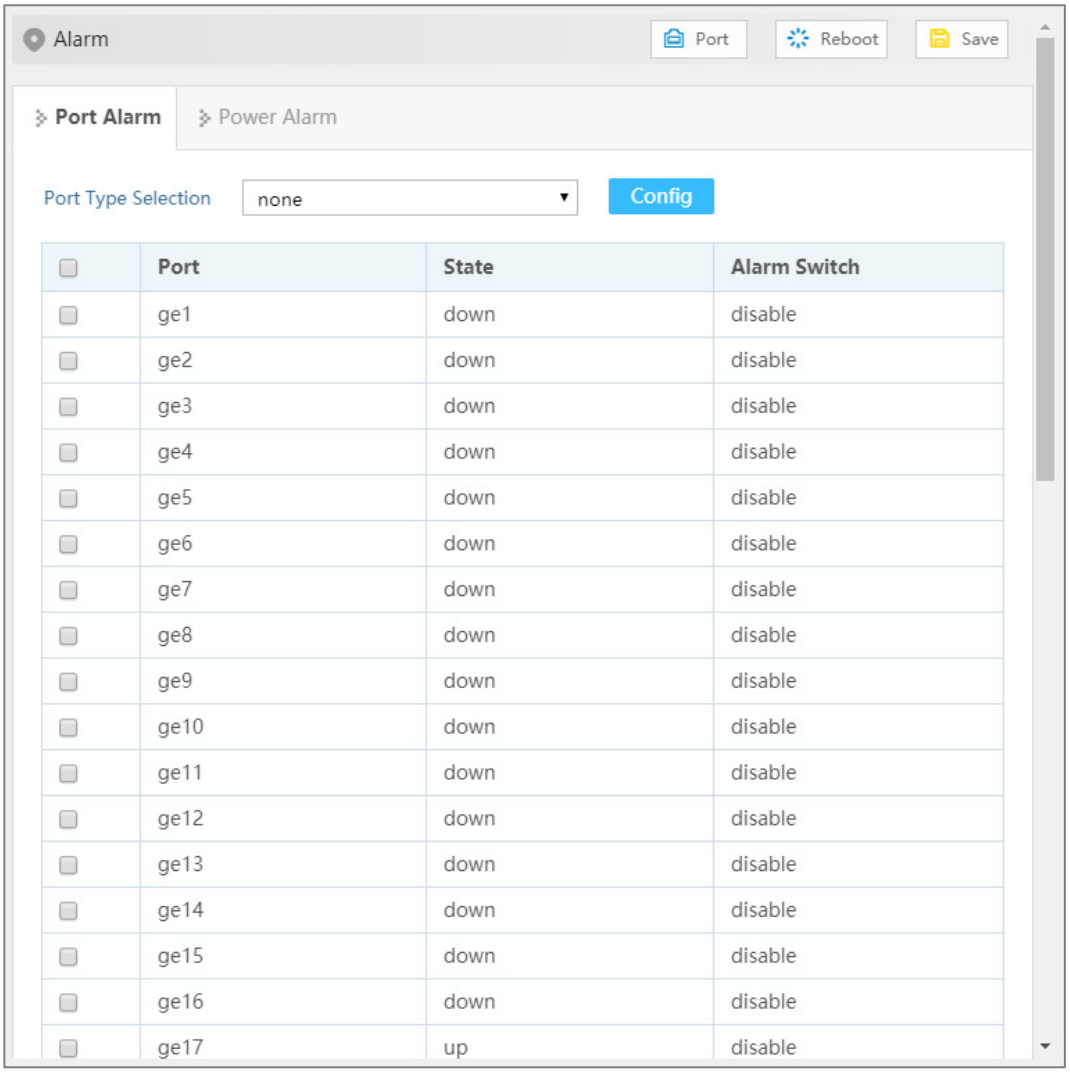
Configure the port alarm function. When the device port is in an abnormal state, the administrator can be informed in time, and the device state can be quickly repaired to avoid excessive loss.

Operation Path

Open in order: "System Maintenance > Alarm > Port Alarm".

Interface Description

Port alarm interface as below:



The main element configuration description of alarm information interface:

Copyright © 3onedata Co., Ltd.

Interface Element	Description
Port	The corresponding port name of the device Ethernet port.
State	Port link status, display items as follows: • up • down
Alarm Switch	Port alarm function status, options as follows: • Enable • Disable Note: After enabling port alarm, when port occurs abnormal status, such as connection break down, the device will output a alarm signal to hint the abnormal operation of device via network management software, alarm indicator or relay.

11.3.2 Power Alarm

Function Description

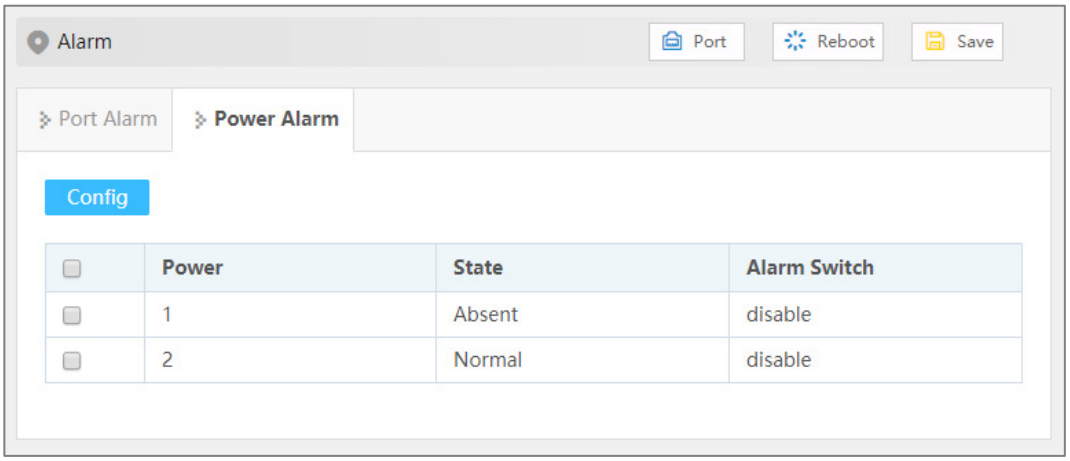
Configure the alarm functions of the power supply.

Operation Path

Open in order: "System Maintenance > Alarm > Power Alarm".

Interface Description

Power alarm interface as below:



Main elements configuration description of power alarm interface:

Interface Element	Description
Power	The corresponding name of this device's power supply
State	Device power link status, display items as follows: • Normal

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	• Absent
Alarm Switch	The state of power supply alarm function, options: • Enable • Disable Note: The alarm is applicable to dual power supplies. After it is enabled, when one of the power supplies is disconnected or fails, the device will output a alarm signal to hint the abnormal operation of device power via network management software, alarm indicator or relay.

11.4 Configuration File Management

11.4.1 Current configuration

Function Description

Check current configuration information.

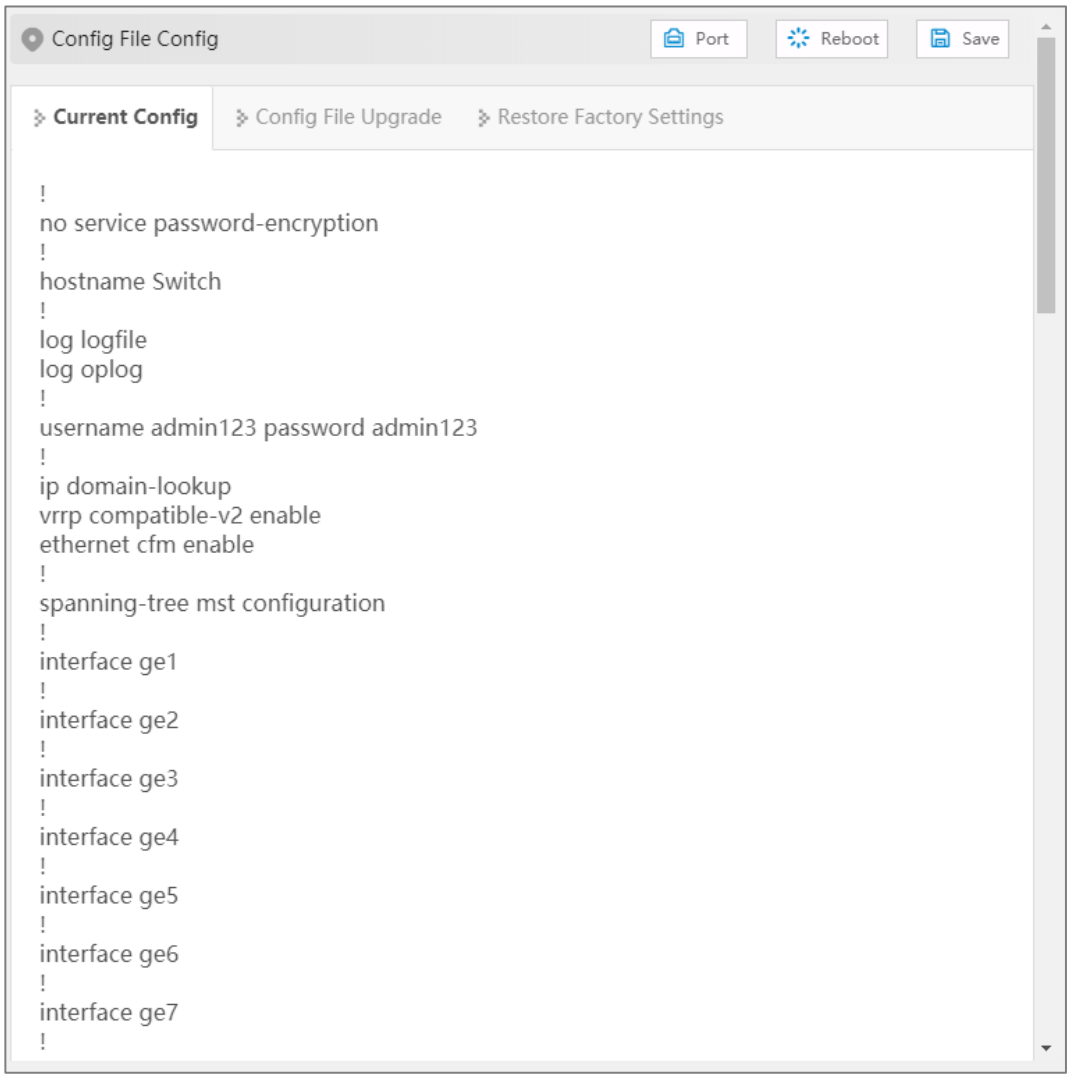
Operation Path

Open in order: "System Management > Configuration File Settings > Current Configuration".

Interface Description

The current configuration interface is as follows:

Copyright © 3onedata Co., Ltd.



11.4.2 Configuration File Update

Function Description

Upload and upload configuration file.

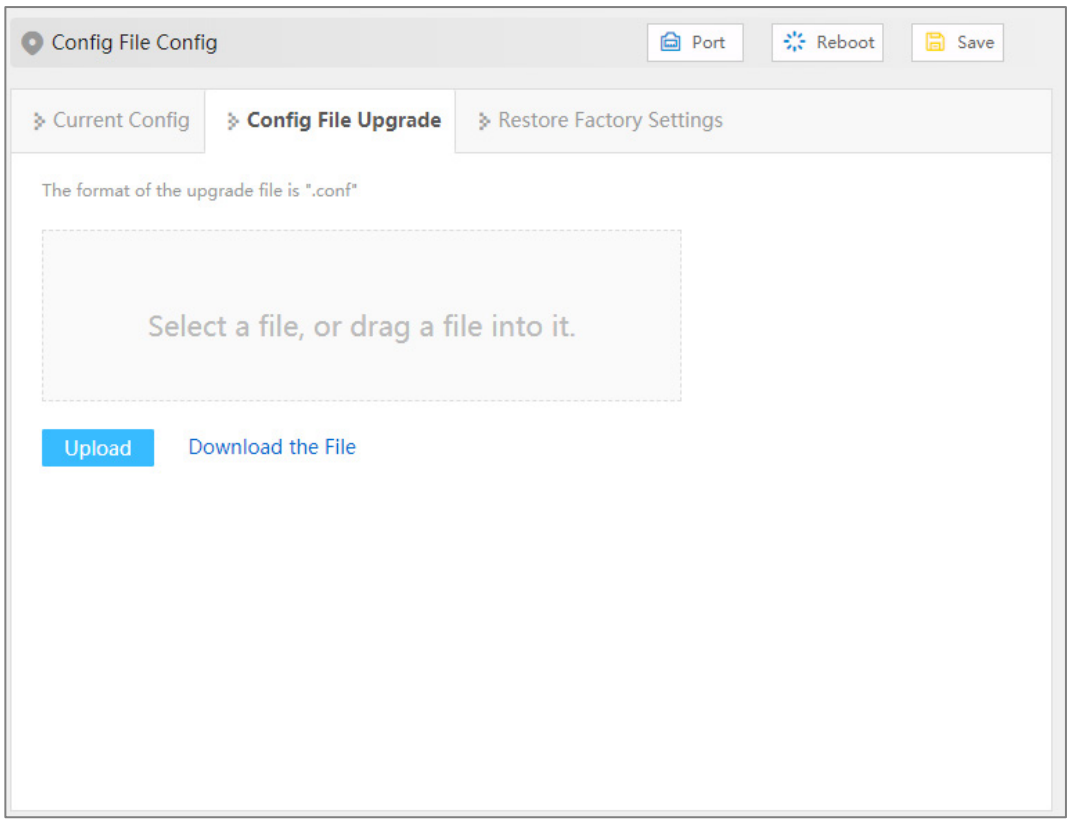
Operation Path

Open in order: "System Management > Configuration File Settings > Configuration File Upgrade".

Interface Description

Configuration file upgrade interface as follows:

Copyright © 3onedata Co., Ltd.



The main element configuration description of configuration file upgrade interface:

Interface Element	Description
Select a file, or drag a file into it	To select the uploaded configuration file, click this area to select the local configuration file, or drag the local configuration file directly into this area.
Upload	After selecting the uploaded configuration file, click the "Upload" button to start uploading the configuration.
Download the file	Click to download the configuration file of the current device. The default file name is "device.conf".

11.4.3 Restore Factory Settings

Function Description

Restore device to factory settings.

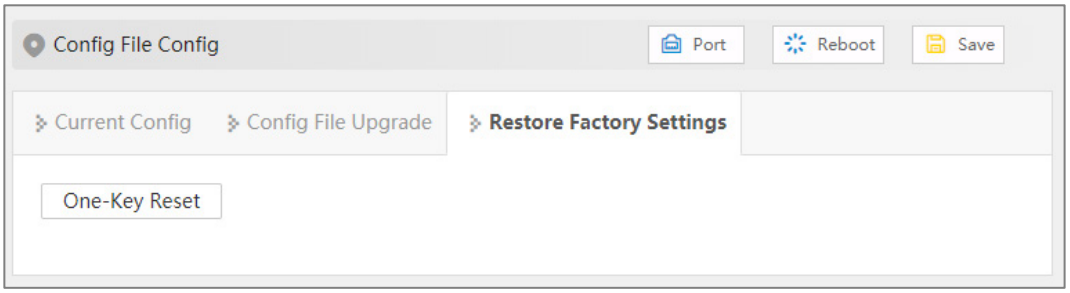
Operation Path

Open in order: "System management > Configure Management > Restore Factory Setting".

Copyright © 3onedata Co., Ltd.

Interface Description

Restore Factory Settings interface is as follows:



The main element configuration description of restore factory settings interface:

Interface Element	Description
One-Key Reset	Click "One-key recovery" button, and the configuration file will be restored to the factory configuration.

11.5 Upgrade

Function Description

Update and upgrade the device program.

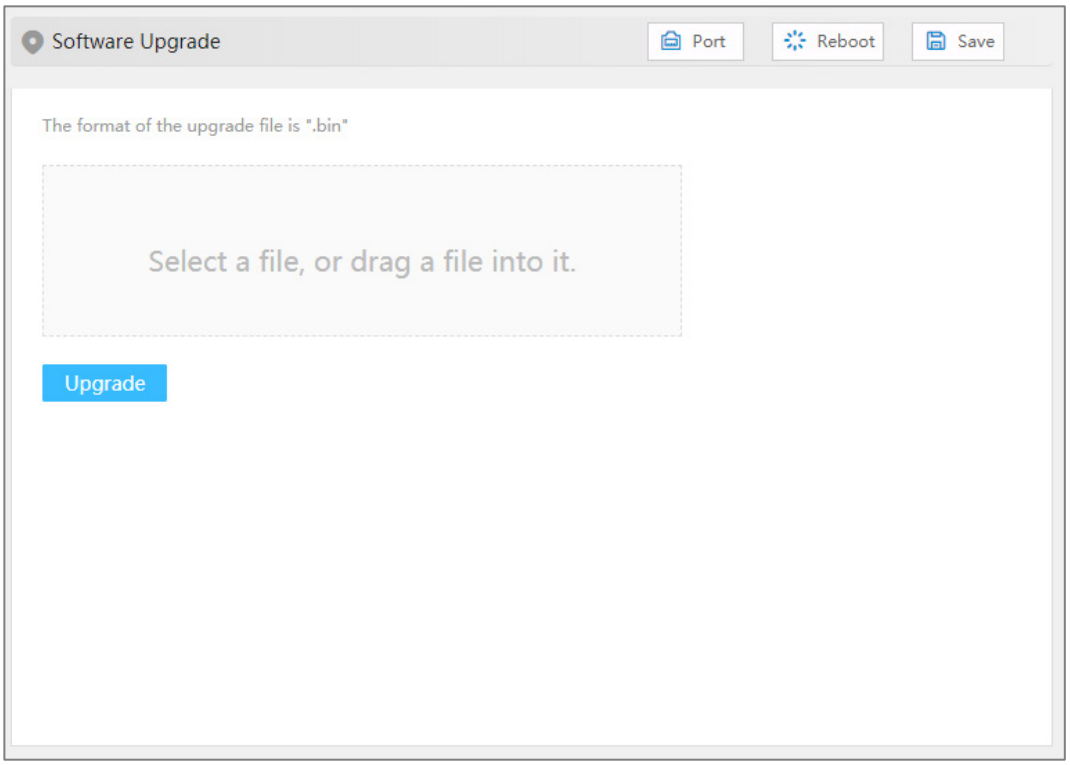
Operation Path

Open in order: "System management > Software Upgrade".

Interface Description

The software update interface as follows:

Copyright © 3onedata Co., Ltd.



The main elements configuration description of software update interface:

Interface Element	Description
Select a file, or drag a file into it	For the upgrade files, click this area to select the local upgrade files, or drag the local upgrade files directly into this area.
Upgrade	After selecting the upgraded files, click the "Upgrade" button to start the upgrade process. Note: Generally, upgrade firmware is in ".bin" format.

11.6 Log Information

11.6.1 Log Information

Function Description

Check the log information of the device. Log information mainly records user operation, system failure, system safety and other information, including user log, security log and diagnostic log.

- User log: records user operations and system operation information.
- Security log: records information including account management, protocol,

anti-attack and status.

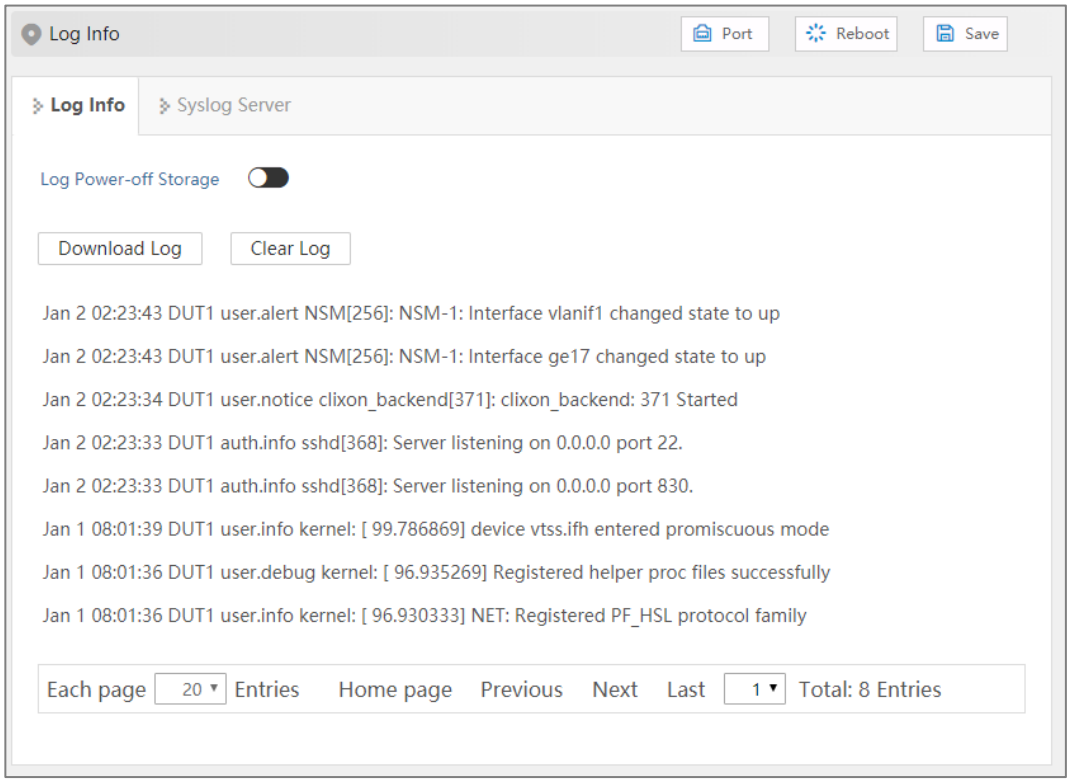
- Diagnostic log: records information that assists in problem identification.

Operation Path

Open in order: "System Maintenance > Log Information > Log Information".

Interface Description

Log information interface as follow:



Main elements configuration description of log information interface:

Interface Element	Description
Log Power-Off Storage	Log information is stored in FLASH, log information will not be lost after power failure.
Download Log	Click the "Download Log" button to download the current log information to the local.
Clear Log	Click the “clear log” button to clear the current log information record.

3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.

11.6.2 Syslog Server

Function Description

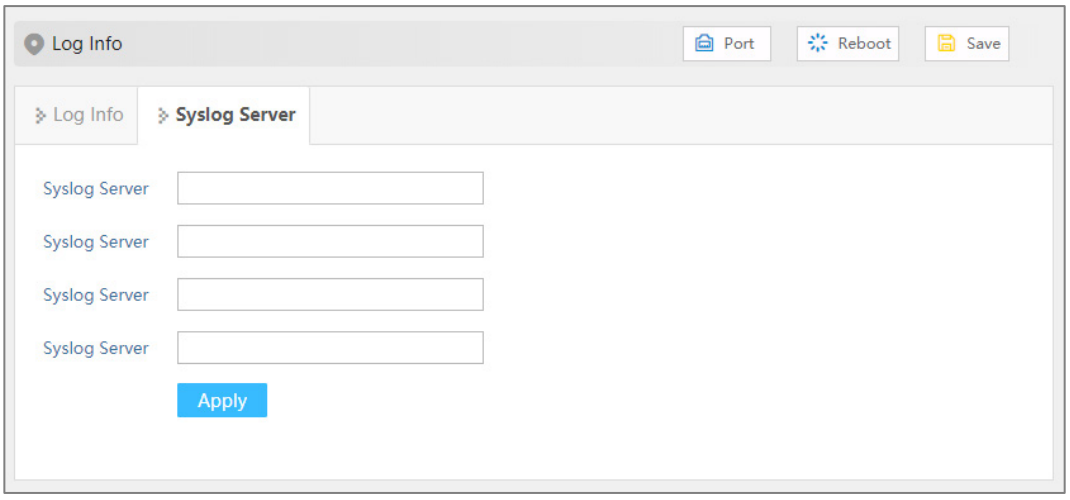
Configure the Syslog server IP address, and the system log information can be sent to the configured syslog server.

Operation Path

Open in order: "System Maintains > Log Information > Syslog Server".

Interface Description

The Syslog server interface as follows:



Syslog server interface main elements configuration instructions:

Interface Element	Description
Syslog Server	IP address of Syslog server Note: • Supports port configuration and the input format is IP: port, for example: 192.168.1.1:80. • Users can configure up to 4 syslog servers at a time. If the configuration of one or more syslog servers need to be canceled, delete the input box and click Set.

Copyright © 3onedata Co., Ltd.

12 FAQ

12.1 Sign in Problems

1. **Why the web page display abnormally when browsing the configuration via WEB?**

   Before accessing the WEB, please eliminate IE cache buffer and cookies. Otherwise, the web page will display abnormally.

2. **What should I do if I forget my login password?**

   IF you forget the login password, you can initialize the password by restoring factory settings. The specific method is to search by BlueEyes_Ⅱ software and use restore factory setting function, then the password will be initialized. Both of the initial user name and password are "admin123".

3. **Is configuring via WEB browser same to configuring via BlueEyes_Ⅱ software?**

   Both configurations are the same, without conflict.

12.2 Configuration Problem

1. **Why the bandwidth can't be increased after configuring Trunking (port aggregation) function?**

   Check whether the port attributes set to Trunking are consistent, such as rate, duplex mode, VLAN and other attributes.

2. **How to deal with the problem that part of switch ports are impassable?**

   When some ports on the switch are impassable, it may be network cable, network

Copyright © 3onedata Co., Ltd.

adapter and switch port faults. User can locate the faults via following tests:

- Keep connected computer and switch ports unchanged, change other network cables;
- Keep connected network cable and switch port unchanged, change other computers;
- Keep connected network cable and computer unchanged, change other switch port;
- If the switch port faults are confirmed, please contact supplier for maintenance.

3. **How about the order of port self-adaption state detection?**

   The port self-adaption state detection is conducted according to following order: 1000Mbps full duplex, 100Mbps full duplex, 100Mbps half-duplex, 10Mbps full duplex, 10Mbps half-duplex, detect in order from high to low, connect automatically in supported highest speed.

12.3 Indicator Problem

1. **Why is the power supply indicator off?**

   Possible reasons include:

   - Not connected to the power socket; troubleshooting, connected to the power socket.
   - Power supply or indicators faults; troubleshooting, change the power supply or device test.
   - Power supply voltage can't meet the device requirements; troubleshooting, configure the power supply voltage according to the device manual.

2. **Link/Act indicator isn't bright, what's the reason?**

   Possible reasons include:

   - The network cable portion of Ethernet copper port is disconnected or bad contact; troubleshooting, connect the network cable again.
   - Ethernet terminal device or network card works abnormally; troubleshooting, eliminate the terminal device fault.
   - Not connected to the power socket; troubleshooting, connected to the power socket.
   - Interface rate doesn't match the pattern; troubleshooting, examine whether the device transmission speed matches the duplex mode.

3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.

3. **Ethernet copper port and fiber port indicator are connected normally, but can't transmit data, what's the reason?**

   When the system is power on or network configuration changes, the device and switch configuration in the network will need some time. Troubleshooting, after the device and switch configuration are completed, Ethernet data can be transmitted; if it's impassable, power off the system, and power on again.

4. **Why does the communication crashes after a period of time, namely, it cannot communicate, and it returns to normal after restarting?**

   Reasons may include:

   - Surrounding environment disturbs the product; troubleshooting, product grounding adopts shielding line or shields the interference source.
   - Site wiring is not normative; Troubleshooting, optical fiber, network cable, optical cable cannot be arranged with power line and high-voltage line.
   - Network cable is disturbed by static electricity or surge; Troubleshooting, change the shielded cable or install a lightning protector.
   - High and low temperature influence; troubleshooting, check the device temperature usage range.

3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.

13 Maintenance and Service

Since the date of product delivery, our company provides 5-year product warranty. According to our company's product specification, during the warranty period, if the product exists any failure or functional operation fails, our company will repair or replace the product for users free of charge. However, the commitments above do not cover damage caused by improper usage, accident, natural disaster, incorrect operation or improper installation.

In order to ensure that consumers benefit from our company's managed switch products, consumers can get help and solutions in the following ways:

- Internet Service;
- Service Hotline;
- Product repair or replacement;

13.1 Internet Service

More useful information and tips are available via our company website. Website: http://www.3onedata.com

13.2 Service Hotline

Users of our company's products could call technical support office for help. Our company has professional technical engineers to answer your questions and help you solve the product or usage problems ASAP. Free service hotline: +86-4008804496

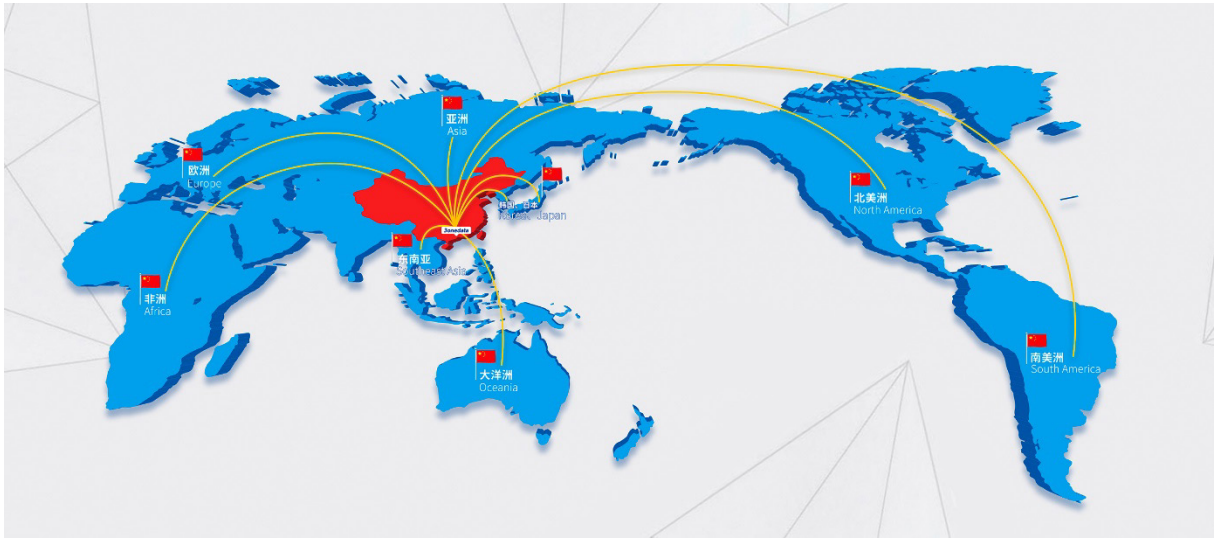
13.3 Product Repair or Replacement

As for the product repair, replacement or return, customers should firstly confirm with the company's technical staff, and then contact the salesmen to solve the problem.

3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.

According to the company's handling procedure, customers should negotiate with our company's technical staff and salesmen to complete the product maintenance, replacement or return.

3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.



3onedata Co., Ltd.

Headquarter Address:	3/B, Zone 1, Baiwangxin High Technology Industrial Park, Song Bai Road, Nanshan District, Shenzhen, 518108, China
Technology Support:	tech-support@3onedata.com
Service Hotline:	4008804496
Official Website:	http://www.3onedata.com