3onedata



IES6300TSN-8GT2GS-2LV
Industrial Ethernet Switch
User Manual

Document Version: 02

Issue Date: 09/17/2022

Copyright © 2022 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 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:	sale@3onedata.com
Fax:	+86-0755-26703485
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

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 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.

Revision Record

Version No.	Date	Revision note
01	05/07/2022	Product release
02	2022-07-27	Software upgrade

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
2.1 SYSTEM INFORMATION 4
3 SYSTEM CONFIGURATION 7
3.1 FUNCTION PREVIEW 7
3.2 NETWORK SETTING 10
3.3 USER SETTINGS 11
3.4 LOG INFORMATION 13
3.5 SSH HTTP SETTINGS 14
3.6 DIAGNOSE TEST 16
3.6.1 Ping 16
3.6.2 TRACEROUTE 17
3.6.3 SFP DDM 17
4 PORT CONFIGURATION 19
4.1 PORT SETTINGS 19
4.2 EGRESS RATE LIMIT 21
4.2.1 Egress Rate Limit 21
4.2.2 Custom Type 24
4.3 PORT MIRRORING 25
4.4 ALARM SETTINGS 26
4.4.1 Alarm Trigger 26
4.4.2 Alarm Receivers 35
4.5 LINK AGGREGATION 38
4.5.1 Static Link Aggregation 39
4.5.2 LACP Configuration 40
4.6 PORT ISOLATION 41
4.7 PORT STATISTICS 42
4.7.1 Port Statistics 42
4.7.2 Detail Port Stats 43

Copyright © 3onedata Co., Ltd.

4.8 CABLE TEST 44
5 LAYER 2 CONFIGURATION 46
5.1 VLAN CONFIGURATION 46
5.1.1 VLAN 802.1Q 46
5.1.2 PVLAN 47
5.1.3 Port 49
5.1.4 Manage VLAN 49
5.2 MAC CONFIGURATION 50
5.2.1 MAC Configuration 50
5.2.2 Static MAC 52
5.3 IGMP SNOOPING 53
5.3.1 IGMP Snooping 53
5.3.2 IGMP Monitoring-VLAN 54
5.3.3 Static Multicast 55
5.3.4 Static Routing Port 56
5.4 SPANNING-TREE CONFIGURATION 57
5.4.1 Bridge Configuration 57
5.4.2 Instance Configuration 59
5.4.3 Bridge Ports 60
5.4.4 Instance Port Configuration 61
5.5 RING CONFIGURATION 62
5.5.1 Global Configuration 63
5.5.2 Node Configuration 63
5.6 ERPS CONFIGURATION 68
5.6.1 Timer 68
5.6.2 Loop 69
5.6.3 Instance Configuration 70
5.7 LOOP DETECTION 72
5.7.1 Global Configuration 72
5.7.2 Port Configuration 73
6 NETWORK SECURITY 75
6.1 ACCESS CONTROL 75
6.2 802.1X CONFIGURATION 76
6.2.1 Global Configuration 77
6.2.2 Port Configuration 78
7 ADVANCED CONFIGURATION 80
7.1 QOS CONFIGURATION 80
7.2 LLDP CONFIGURATION 85
7.2.1 Global Configuration 85
7.2.2 Port Setting 87
7.2.3 Neighbors 88
7.3 SNMP CONFIGURATION 89
7.3.1 Global Configuration 90

Copyright © 3onedata Co., Ltd.

7.3.2 V3 User 91
7.4 DHCP SERVER CONFIGURATION 93
7.4.1 DHCP Server 93
7.4.2 DHCP Address Pool 94
7.4.3 Client List 95
7.4.4 Static DHCP 96
7.4.5 Port Address Binding 97
7.5 DHCP-SNOOPING CONFIGURATION 97
7.5.1 Global Configuration 98
7.5.2 Static Binding 99
7.5.3 Port Configuration 100
7.6 DNS SETTINGS 101
7.7 NTP CONFIGURATION 102
7.8 PTP CONFIGURATION 104
7.9 TSN CONFIGURATION 118
7.9.1 802.1Qav Configuration 118
7.9.2 802.1Qbv Configuration 120
8 SYSTEM MAINTENANCE 124
8.1 CONFIGURE FILE MANAGEMENT 124
8.1.1 Global Configuration 124
8.1.2 Manage Configuration File 125
8.2 RESTORE FACTORY DEFAULTS 126
8.3 UPGRADE 126
8.3.1 TFTP 126
8.3.2 Upload 127
9 FAQ 129
9.1 SIGN IN PROBLEMS 129
9.2 CONFIGURATION PROBLEM 129
9.3 INDICATOR PROBLEM 130
10 MAINTENANCE AND SERVICE 132
10.1 INTERNET SERVICE 132
10.2 SERVICE HOTLINE 132
10.3 PRODUCT REPAIR OR REPLACEMENT 133
11 APPENDIX: DESCRIPTION OF LOG ID 134

Copyright © 3onedata Co., Ltd.

1 Log in the Web Interface

1.1 System Requirements for WEB Browsing

Using this equipment, 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 6.0 or above
Operating system	Windows XP/7/8/10

1.2 Setting IP Address of PC

The switch default management 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.

Copyright © 3onedata Co., Ltd.

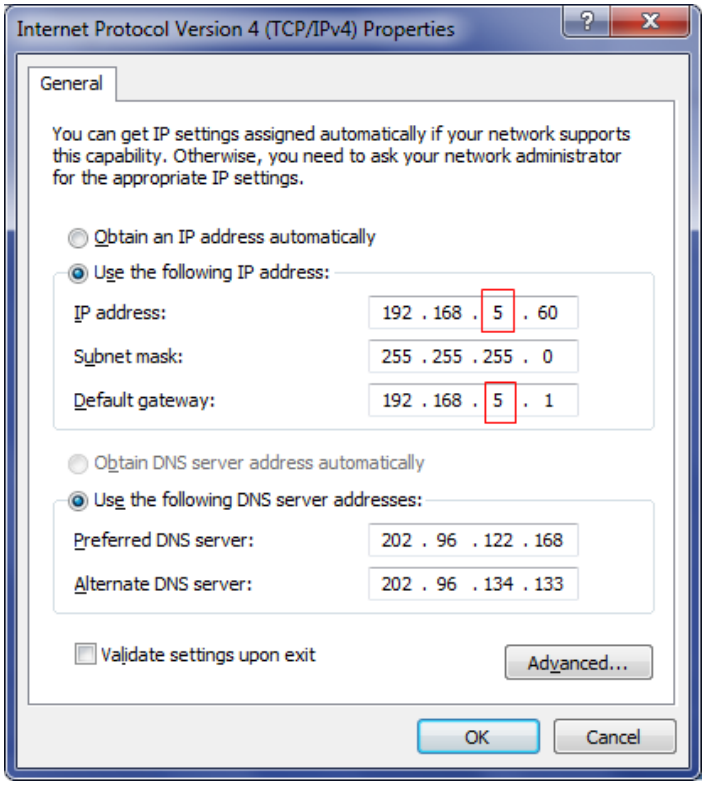
Eg: Assume that the IP address of the device is 192.168.1.254, the IP address of the current PC is 192.168.5.60, change the network segment "5" of the IP address of the PC to "1".

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:

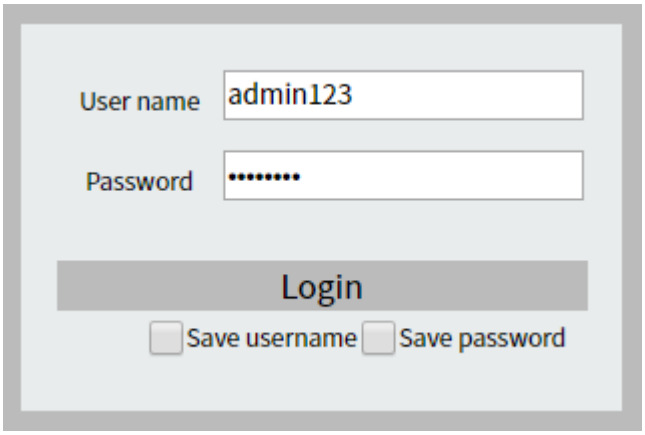
Step 1 Run the computer browser.

Step 2 Enter device’s IP address in the address bar of the browser.

Step 3 Click the “Enter” key.

Copyright © 3onedata Co., Ltd.

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.
- The default password is valid for 90 days. After the password expires, the corresponding user will not be able to log in to the WEB, so he/she needs to log in to CLI to reset the password. The new password supports 8-31 valid characters, including at least two kinds of characters of uppercase letters, lowercase letters, numbers and special characters. Special characters can include "! @#￥%^&*()-+<>”. Password validity can be modified or disabled through CLI.

Step 5 Click "Login".

Step 6 End.

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

Copyright © 3onedata Co., Ltd.

2 System Information

2.1 System Information

Function Description

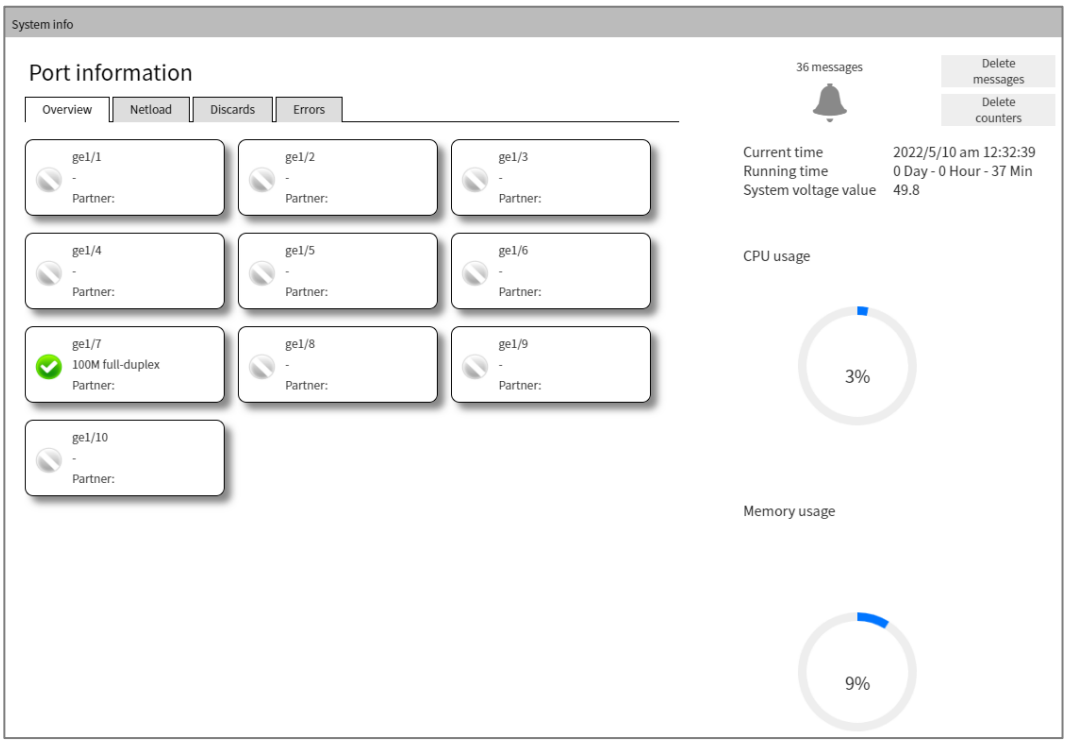
On the System Information page, you can view connection information of device interface, network load, dropped frames, error frames and log reports.

Operation Path

Click to open: “System Information”.

Interface Description

System information interface as follows:



Copyright © 3onedata Co., Ltd.

The main element configuration description of state information interface:

Interface Element	Description
Port Information	**Port Information area box**
Overview	Port status information, such as port working status, IP address of the opposite end, port speed and duplex mode.
Netload	Port network load status.
Discards	Statistics on the number of port dropped data frames.
Errors	Statistics on the number of port error data frames.
Message	**Report Area Frame**
Message	Log numbers, click the report icon to view the log information content.
Delete messages	Delete button is used to delete the contents of log information.
Delete counter	Delete button is used to clear the number of logs.
Current time	Current system time information. Users can specify the time zone and server in “NTP Configuration”.
Running time	Current device running time after power on.
System voltage value	Display the voltage of the current power, its unit V.
CPU usage	CPU usage of the current device. Note: When the CPU utilization rate and memory utilization rate are lower than 90%, the system is running normally.
Memory usage(%)	Memory usage of the current device. Note: When the CPU utilization rate and memory utilization rate are lower than 90%, the system is running normally.

Note

Port information icon is as follows:

- No fault: the port communication is normal and has no fault;
- Alarm: the port has a fault, but it doesn't cause the abnormal communication. The alarm information can be processed locally;
- Fault: the port has a fault, and the port can't communicate normally, so the fault information should be dealt with in time;

Copyright © 3onedata Co., Ltd.

-  No connection/no communication: the port is not connected, and the device/network fails to communicate.

Copyright © 3onedata Co., Ltd.

3 System Configuration

3.1 Function Preview

Function Description

On the "Function Preview" page, you can view device configuration information such as device information, IP configuration, system configuration, port configuration, alarm configuration, layer 2 configuration, network security, advanced configuration and system maintenance, etc. You can enter the corresponding function configuration interface through the link button.

Operation Path

Open in order: "System Configuration > Function Preview".

Interface Description

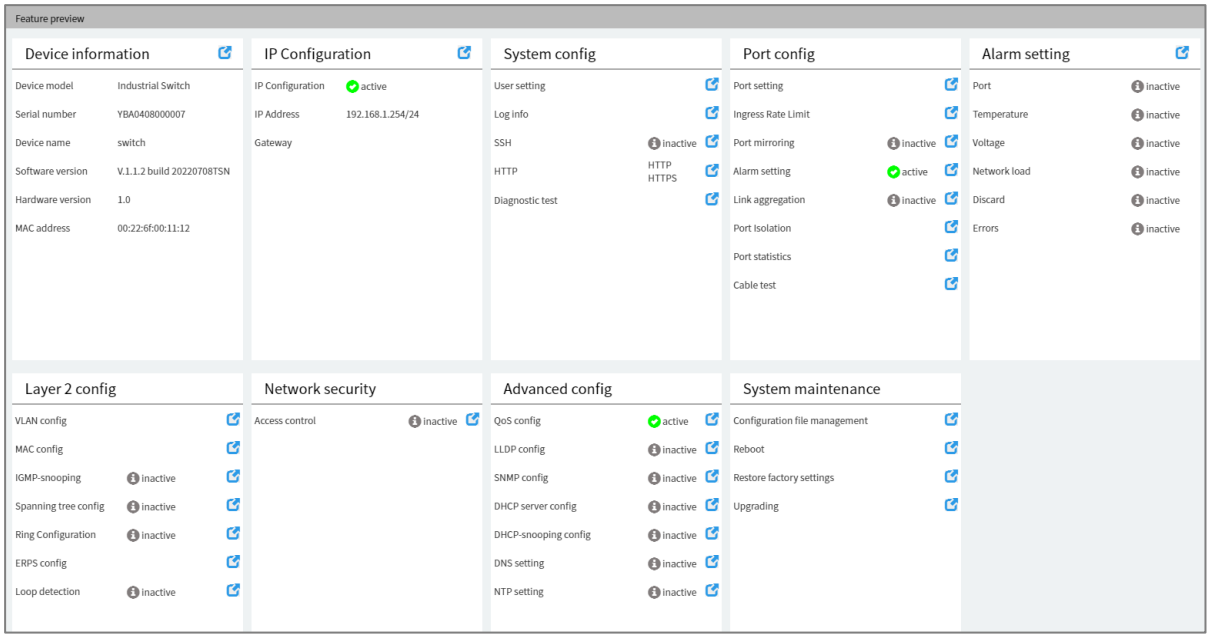
The function preview interface is as follows:

Note

The function status is shown as follows:

- Active: indicates that the corresponding function is active
- Standby: indicates that the corresponding function is inactive

Copyright © 3onedata Co., Ltd.



The main elements configuration description of system configuration interface:

Interface Element	Description
Device Information	**Device area box and edit button**
Device model.	Equipment model name.
Serial number.	SN code, product serial number.
Device name	Device Type
Software version	Software version information currently in use.
Hardware version	Hardware version information currently in use.
MAC address	Hardware address of device factory configuration.
IP Configuration	**Configure IP area box and edit button**
IP Configuration	Current IP address status of the device.
IP Address	IP address and subnet mask information of the device.
Gateway	Current gateway information of the device.
System Configuration	**System Configuration area box**
System Configuration	System configuration functions and link button options are as follows: • User setting • Log Info • SSH: SSH service status • HTTP: HTTP or HTTPS status - HTTP: HTTP enable - HTTPS: HTTPS enable - HTTP HTTPS: HTTP and HTTPS enable

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	• Diagnose Test
Port Configuration	**Port configuration area box**
Port configuration	Port configuration functions and link button options are as follows: • Port setting • Ingress Rate Limit • Port mirroring • Alarm settings • Link aggregation • Port Isolation • Port Statistics • Cable test
Alarm Settings	**Alarm Settings area box**
Alarm setting	Set alarm function and link button options are as follows: • Port • Temperature • Voltage • Network Load • Discard • Errors
Layer 2 Configuration	**Layer 2 Configuration Area Box**
Layer 2 Configuration	Layer 2 configuration functions and link button options are as follows: • VLAN Configuration • MAC Configuration • IGMP-snooping • Spanning-tree Configuration • Ring Configuration • ERPS Configuration • Loop Detection
Network Security	**Network Security Area Box**
Network Security	Network security features and link button options are as follows: • Access Control
Advanced Configuration	**Advanced Configuration Area Box**
Advanced Configuration	Advanced configuration functions and link button options are as follows:

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	• QOS Configuration • LLDP Configuration • SNMP Configuration • DHCP Server Configuration • DHCP-Snooping Configuration • DNS Configuration • NTP Configuration
System Maintenance	**System Maintenance Area Box**
System Maintenance	System maintenance functions and link button options are as follows: • Configuration file management • Reboot • Restore factory settings • Upgrading

3.2 Network Setting

Function Description

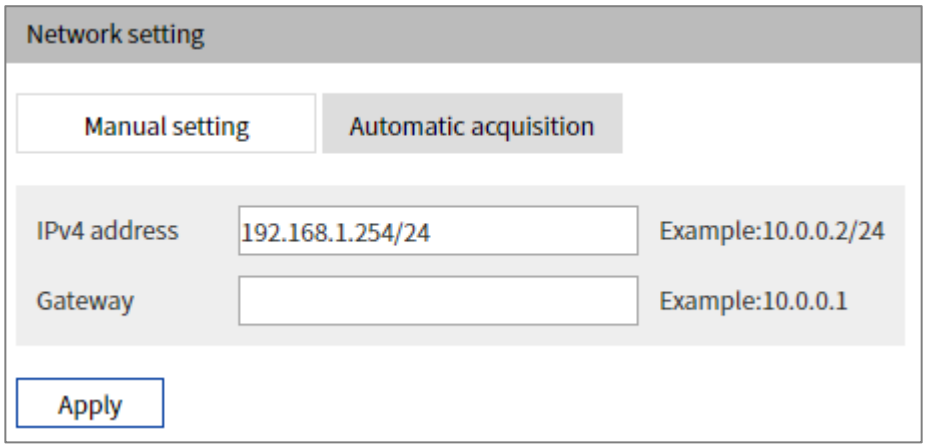
On the “Network Settings” page, user can set the IP address and gateway of this device. Network supports two modes, DHCP and manual settings.

Operation Path

Open in order: " System Configuration > Network Setting".

Interface Description

Network Setting interface as follow:



Copyright © 3onedata Co., Ltd.

The main element configuration description of network setting interface:

Interface Element	Description
Network Setting	The access method of IPv4 address, manual configuration and DHCP. • "Auto-takeover", auto-acquisition means that the DHCP function is enabled. At this time, the IP address of the device can be obtained through the HyperTerminal; • “Manual adjustment”, that is entering static IP address. User needs to fill in IPV4 address and gateway manually.
IPv4 address	Manually enter the IP address and subnet mask information of the device, for example: 10.0.0.0/24.
Gateway	Fill in the gateway address information of the device, for example: 10.0.0.1.

3.3 User Settings

Function Description

On the "User Config" page, user can add and delete username, user needs to enter username and password to access the device, the initial username and password are: admin123.

Due to the security policy requirements of the device, in order to reduce the significant risks caused by password leakage, the default validity period of passwords is 90 days; After the password expires, the corresponding user will not be able to log in to the WEB via HTTP/HTTPS, so it is necessary to log in to CLI via CONSOLE/TELNET/SSH to reset the password.

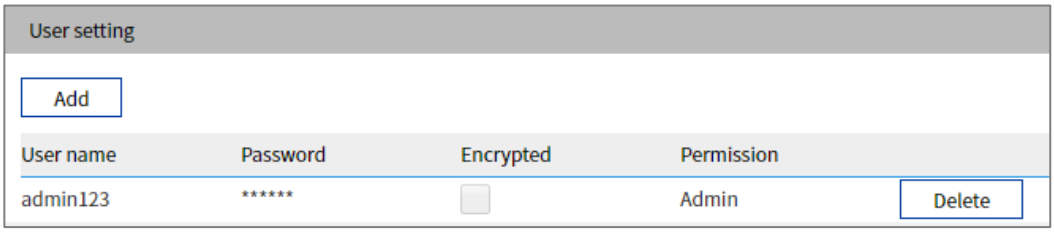
Operation Path

Open in order: "System Configuration > User Configuration".

Interface Description

User settings interface as follows:

Copyright © 3onedata Co., Ltd.



The main element configuration description of user settings interface:

Interface Element	Description
Username	The visitor's ID cannot be empty, supports 5-31 valid characters, including uppercase and lowercase letters, numbers or combinations, and no special characters.
Password	The visitor's password cannot be empty, supports 5-31 valid characters. Note: The password contains at least two kinds of characters of uppercase letters, lowercase letters, numbers and special characters, and the special characters can contain "! @#￥%^&*()-+<>".
Encrypted	Encryption mode check box: • Check: use encrypted password • Uncheck: use cleartext password
Permission	The visitor's privileges in the WEB are: • Auditor: it has partial access rights, and can view the information page of device system log. • User: except network settings, user settings, SSH HTTP settings, access control and system maintenance, other WEB pages can be accessed and configured normally. • Admin: Administrators have the highest privileges.

Note

The default password is valid for 90 days, which can be modified or disabled through CLI. The relevant commands are as follows:

- Modify the period of validity of the password, such as "switch(config)#username WORD password-control aging <0-365> <30-86399>".
- Disable the period of validity of the password, such as "switch(config)# no username WORD password-control aging".

And WORD is username, the unit of <0-365>is day,the unit of <30-86399> is second.

Copyright © 3onedata Co., Ltd.

3.4 Log Information

Function Description

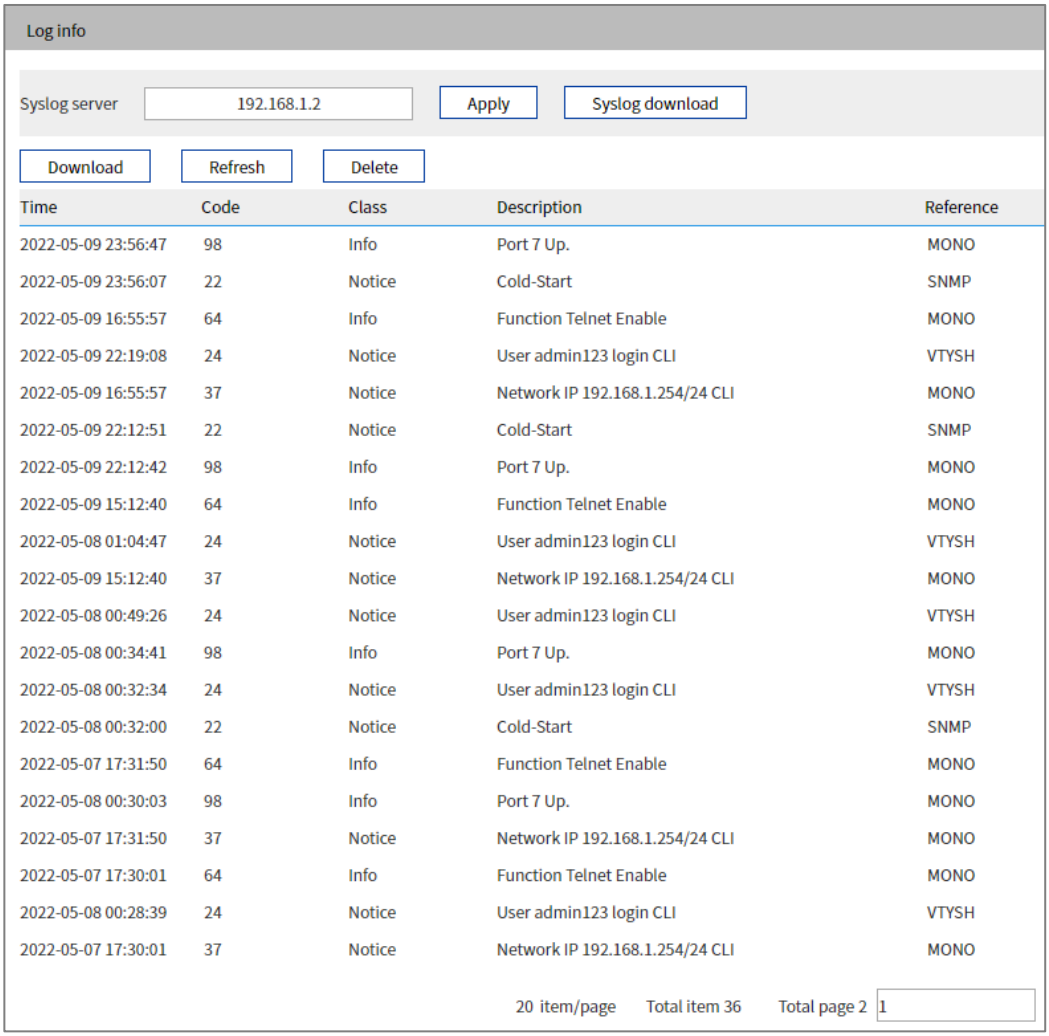
On the page of “Log information”, user can check the log information of the device, supports remote monitoring and local downloading.

Operation Path

Open in order: “System Maintenance > Log Information”.

Interface Description

Log information interface as follow:



Main elements configuration description of log information interface:

Interface Element	Description
Syslog server	The IP address of the log server can remotely monitor the log information of the device system. Click the "Syslog download"

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	button to download "sys.log" locally.
Time	The date and time when the log information occurred.
Code	Please refer to the Appendix for the corresponding ID, specific description and level of the log events.
Class	The corresponding levels of log information events are shown as follows: • False • Notice • Information
Description	Description of log information events.
Reference	Log Information Module.
Operation	The operation button options are as follows: • Download: Download the current log information "user.log" file to the local host; • Refresh: Refresh the log information and reload the log list; • Delete: Clear all current log information.

3.5 SSH HTTP Settings

Function Description

On the “SSH HTTP Settings” page, you can enable/disable service functions such as SSH, TELNET, HTTP and HTTPS, and configure the port number corresponding to the protocol.

The full English name of SSH is Secure Shell. SSH is a security protocol based on application layer and transmission layer. SSH is a reliable protocol which provides security for remote login sessions and other network services. Using SSH protocol can effectively prevent information leakage in the process of remote management, and can also prevent DNS and IP spoofing. In addition, the transmitted data is compressed so that the transmission speed can be increased.

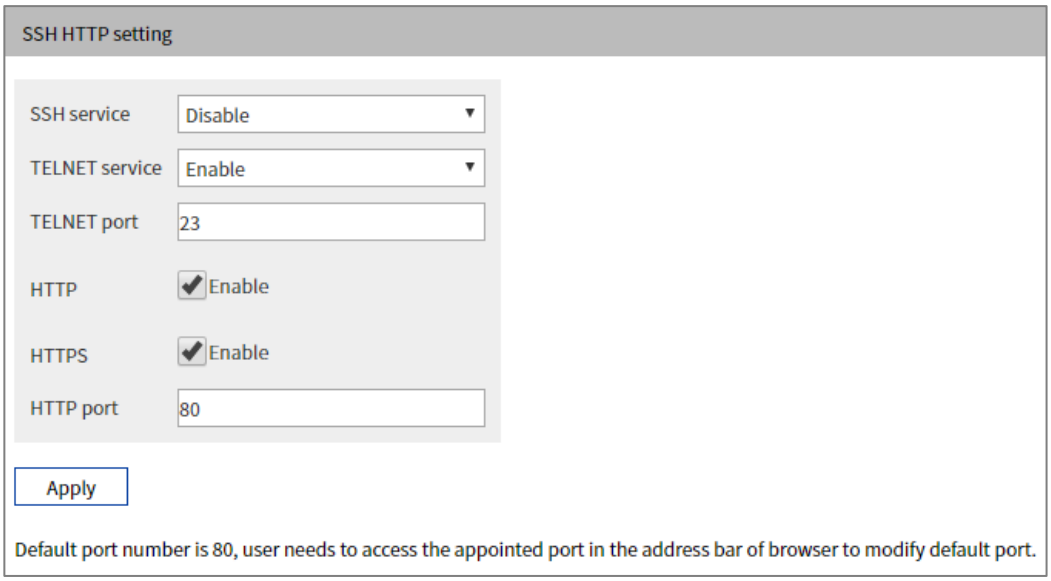
Operation Path

Open in order: "System Configuration > SSH HTTP Configuration".

Copyright © 3onedata Co., Ltd.

Interface Description

SSH HTTP configuration interface is as follows:



The main element configuration description of SSH HTTP settings interface:

Interface Element	Description
SSH service	SSH service function status, the options are as follows: • Disable; • Enable.
TELNET Service	TELNET service function status, the options are as follows: • Disable; • Enable.
TELNET port	TELNET service port number, default port number is 23.
HTTP	Device HTTP protocol function status, enable check box. Note: Format via HTTP access: HTTP://192.168.1.254:80, IP address is the IP address of the device; When using the default port number, the port number can be omitted.
HTTPS	Device HTTPS protocol function status, enable checkbox. Note: Format via HTTP access: HTTP://192.168.1.254:443, IP address is the IP address of the device; When using the default port number, the port number can be omitted.
HTTP port	HTTP protocol service port number, the default port number is 80, if the default port is modified, specify the port number in the browser address bar while accessing.

Copyright © 3onedata Co., Ltd.

3.6 Diagnose Test

3.6.1 Ping

Function Description

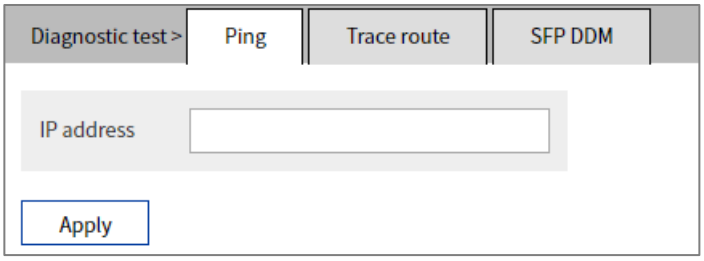
On the "Ping" page, users can use the Ping command to check whether the network is clear or the network connection speed. Ping utilizes the uniqueness of network machine IP address to send a data packet to the target IP address, and then ask the other side to return a similarly sized packet to determine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

Operation Path

Open in order: "System Config > Diagnosis > Ping".

Interface Description

The Ping interface is as follows:



The main elements configuration description of Ping configuration interface:

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

Copyright © 3onedata Co., Ltd.

3.6.2 TRACEROUTE

Function Description

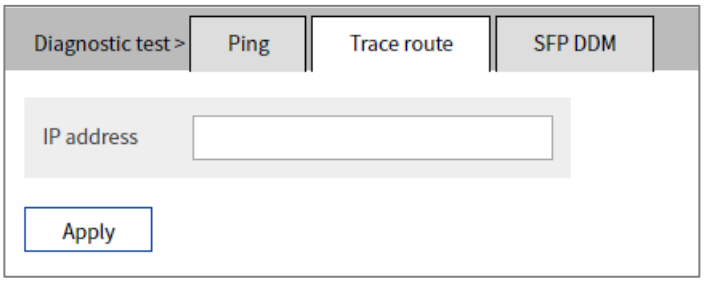
In the "Traceroute" page, users can test the network situation between the switch and the target host. Traceroute measures how long it takes by sending small packets to the destination device until they return. Each device on a path Traceroute returns three test results. Output result includes each test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

Operation Path

Open in order: "System Config > Diagnosis > Traceroute".

Interface Description

TRACEROUTE interface as follows:



The main element configuration description of Traceroute interfaces:

Interface Element	Description
IP Address	IP address of the destination device, fill in the IP address of the opposite device that needs to be detected.

3.6.3 SFP DDM

Function Description

On the “SFP DDM” page, DDM (Digital Diagnostic Monitor) function is supported. User can monitor SFP parameter in real time. This function has greatly facilitated the troubleshooting process of optical fiber link and the cost of on-site debugging.

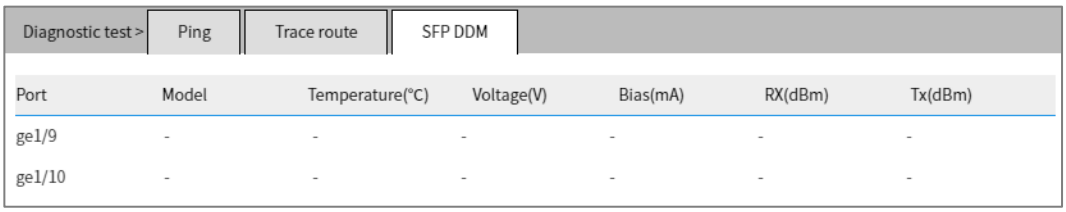
Operation Path

Open in order: "System Config > Diagnostic test > SFP DDM".

Copyright © 3onedata Co., Ltd.

Interface Description

DDM interface as follows:



The main element configuration description of DDM interface:

Interface Element	Description
Port	Port that supports DDM detection function.
Model	SFP optical module type.
Temperature(℃)	This device's SFP temperature. Its unit is ℃. The operating temperature of this SFP module should be within the temperature range of normal operation.
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(mA)	The bias current of laser. Its unit is mA.
RX(dBm)	Optical input power, referring to the lowest optical power of receiving in certain rate and bit error rate.
Tx(dBm)	Optical output power, referring to the output power of optical source in the sending end of optical module.

Copyright © 3onedata Co., Ltd.

4 Port Configuration

4.1 Port Settings

Function Description

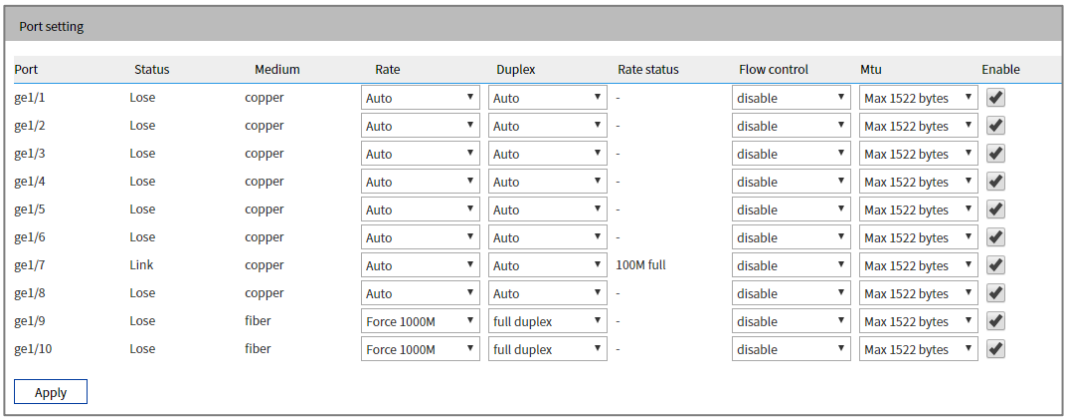
On the "Port Setting" page, user can check port type, rate and connection state, set rate mode, duplex mode, port enable, flow control and other parameters.

Operation Path

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

Interface Description

Port setting interface as follows:



Main elements configuration description of port settings interface:

Interface Element	Description
Port	The corresponding port name of the device Ethernet port.
State	Ethernet port connection status, display status as follows: • LOSE: represent the port is disconnected; • LINK: represent the port is connected.

Copyright © 3onedata Co., Ltd.

Interface Element	Description
Medium	Ethernet port connection type, display medium as follows: • COPPER: copper port; • FIBER: fiber port.
Rate	The working speed of current Ethernet port, optional speeds as follows: • Auto: self-adaption. • Force 10M. • Force 100M. • Force 1000M.
Duplex	Duplex mode of Ethernet port, optional modes as follows: • Auto: full duplex and half duplex self-adaption. • Full duplex. • Half duplex
Rate Status	Port speed and duplex mode, the display status is as follows: • -: port is disconnected; • 1000M full: Gigabit full duplex; • 100M full: 100M full duplex; • 100M half: 100M half duplex; • 10M full: 10M full duplex; • 10M half: 10M half duplex;
Flow control	Port flow control status, options as follows: • Close: disable; • tx: enable the port to send data flow control; • rx: enable flow control of port data receiving; • All: Enable port data sending and receiving flow control.
Mtu	The maximum Ethernet data frame length passed through the port can be selected as follows: • Max 1522 bytes • Max 2048 bytes • Max 10240 bytes
Enable	Enable Ethernet port. Notice: If user doesn't check the port "Enable" checkbox, the port won't be connected to use.

Copyright © 3onedata Co., Ltd.

4.2 Egress Rate Limit

4.2.1 Egress Rate Limit

Function Description

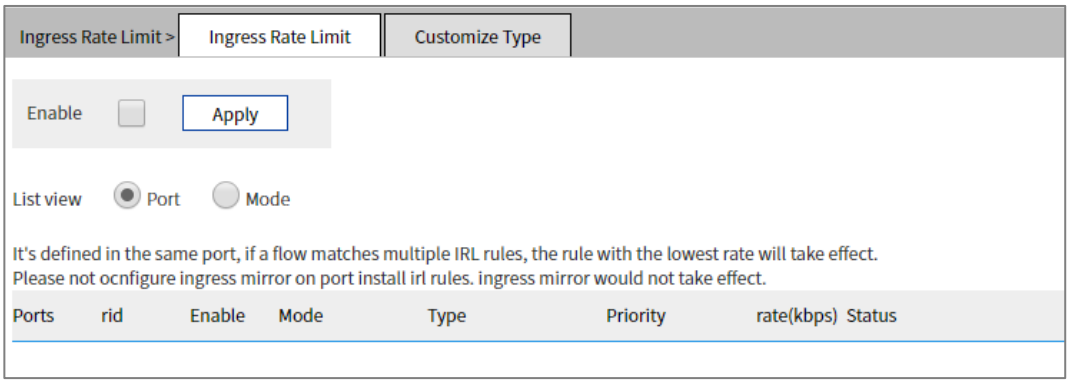
On the "Ingress Rate-Limit" page, user can limit the communication flow of each port or cancel the port flow limit. This device provides ingress speed limit based on port bandwidth, storm, protocol, custom, etc. User can select a fixed speed, the device will discard the packet or adopt flow control to limit the transmission speed or receiving speed of opposite device according to the flow control is enabled or not.

Operation Path

Open in order: "Port Configuration > Ingress Rate-Limit > Ingress Rate-Limit".

Interface Description

Ingress Rate-Limit interface as follows:



The main element configuration description of Ingress Rate-Limit interface:

Interface Element	Description
Enable	The ingress speed limit enable check box, after it is checked, click the "Apply" button to start adding speed limit rules.
List View	Ingress speed limit list display mode, the options are as follows: • Port: according to port classification, each speed limit rule is displayed. • Mode: according to the mode classification, each speed limit rule is displayed.
Port	The corresponding port name of the device Ethernet port.

Copyright © 3onedata Co., Ltd.

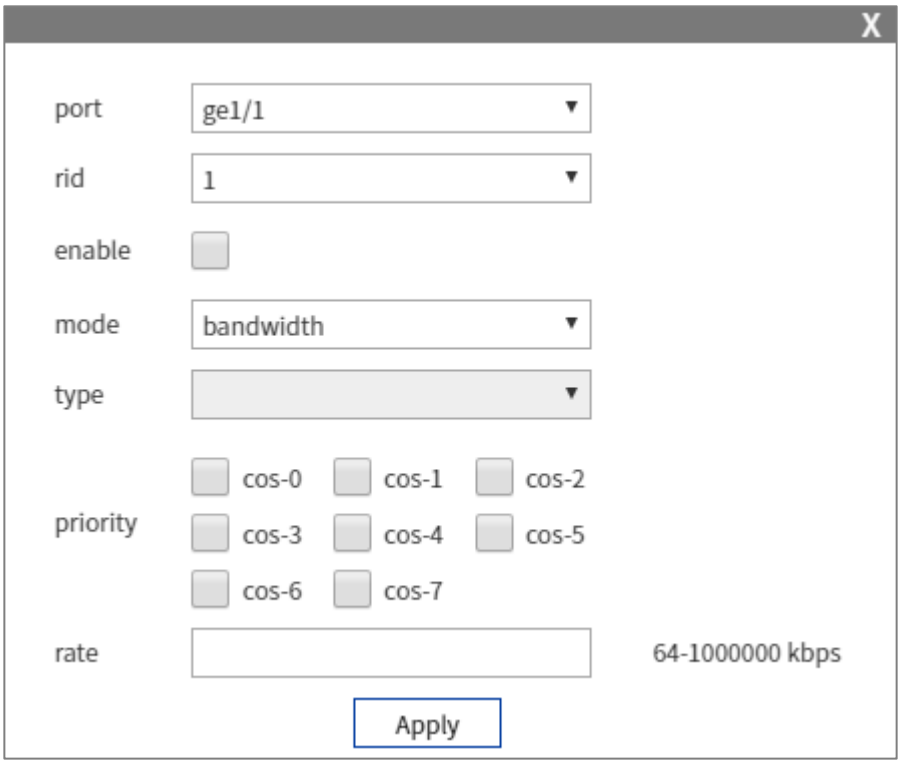
Interface Element	Description
rid	Speed limit rule ID, the port can support multiple speed limit rules. Note: Making rules in the same port, if a flow matches multiple IRL rules, the rule with the lowest rate will take effect.
Enable	Speed limit rule enables configuration status.
Mode	Port speed limit is based on bandwidth, storm, protocol, custom and other modes.
Type	The data frame type of the speed limit.
Priority	CoS priority of speed-limited data frames.
Rate(kbps)	The port's limit value for the data transmission rate of the entrance, in kbps.
Status	Speed limit rule enable state.

Note

- Do not configure the ingress mirror on the speed-limited port, in which case the ingress mirror will not take effect.
- 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 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.

Click "Add" button to add an ingress speed limit rule.

The interface of Add is as follows:



The main element configuration description of Add interface:

Interface Element	Description
Port	Port drop-down list, configure the port with speed limit.
rid	The drop-down list of speed limit rule ID, which supports up to 4 speed limit rules.
Enable	Enable check box, and check it to enable the speed limit rule.
Mode	The drop-down list of Rate-Limit mode, options as follows: • Bandwidth: Limit the bandwidth of the port ingress. • Storm: Limit the ingress rate of broadcast frame. • Protocol: Limit the ingress rate of the specified protocol data frame. • Custom: Limit the ingress rate of custom data frames.

Type	Drop-down list of data frame type, options as follows:
	• When the mode is Storm, the following options are supported:
	  • -unknown-unicast.
	  • -unknown-multicast.
	  • - broadcast.
	  • -flood.
	• When the mode is Protocol, the following options are

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	supported: arp, tcpData, tcpCtrl, udp, other, tcp, tcpudp, arptcpudp. • When the mode is Custom, it is necessary to configure "Custom Type" in advance, and the following options are supported: Custom1, Custom2 or Custom3.
Priority	CoS priority check box, with values of 0-7.
Rate	Rate limit value, ranging from 64 to 100,000, unit: kbps.

4.2.2 Custom Type

Function Description

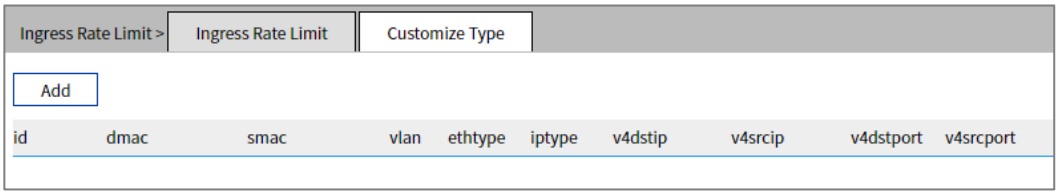
On the "Custom Type" page, users can customize the type of IPv4 data frame that needs speed limit.

Operation Path

Open in order: "Port Configuration > Ingress RateLimit > Custom Type".

Interface Description

The Customize type interface is as follow:



The main elements configuration description of Customize type interface:

Interface Element	Description
ID	Custom type ID, support ID range 1-3.
DMAC	The destination MAC address of the data frame, such as 0000-0000-0001.
SMAC	The source MAC address of the data frame, such as 0000-0000-0002.
VLAN	The VLAN ID of the frame, ranging from 1 to 4094.
Ethtype	The type of data frame, ranging from 0x1 to 0xfff.
iptype	The protocol type of the data frame, ranging from 1 to 255.

Copyright © 3onedata Co., Ltd.

Interface Element	Description
v4dstp	The destination IP address of the frame.
v4srcip	The source IP address of the frame.
V4dstport	The destination port number of the frame, ranging from 1-65535.
v4srcport	The source port number of the frame, ranging from 1-65535.

4.3 Port Mirroring

Function Description

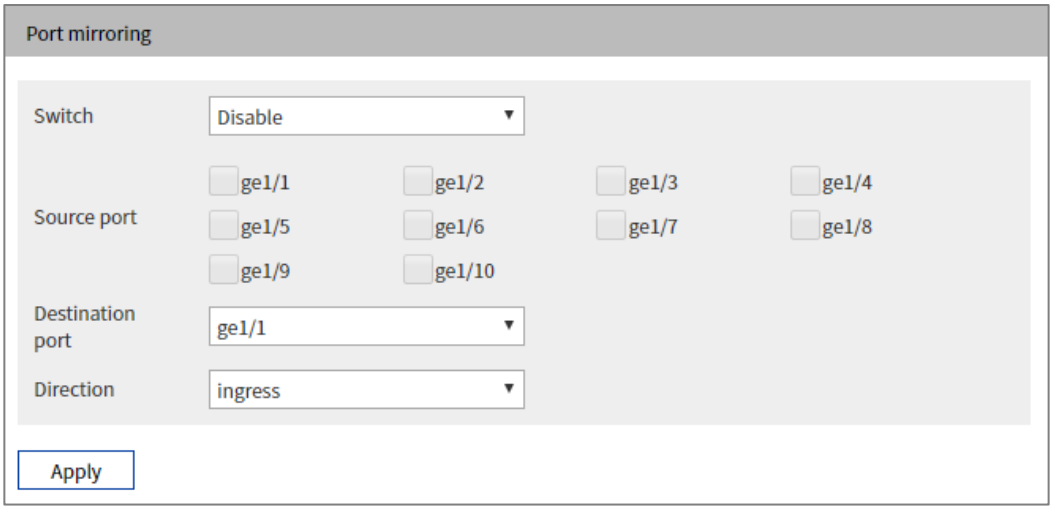
On the "Port mirroring" page, user can copy the data from the origin port to appointed port for data analysis and monitoring.

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
Switch	Port mirroring enable drop-down list, options are as follows: • Disable • Enable
Source port	A set of monitored ports, which will collect data from these ports in the specified direction, and the mirror port can be one

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	or more.
Destination port	A port for monitoring, and the device outputs data from the port to the specified direction.
Direction	This parameter specifies the direction of monitoring port data. Monitor can choose according to their own needs. • ingress: import data, the packet received by the port will be mirrored to the destination port; • egress: export data, the message sent by the port will be mirrored to the destination port; • Both: all data, mirror the port receiving and sending packets at the same time.

4.4 Alarm Settings

On the page of "Alarm Warning", user can configure alarm function; when the equipment runs abnormally, it can promptly notify the administrator, and quickly repair the equipment to avoid excessive loss.

4.4.1 Alarm Trigger

Function Description

The trigger events are as follows:

- Port Alarm;
- Temperature Alarm;
- Voltage Alarm;
- Network Load;
- Packet Loss Alarm;
- Error Frame Alarm;

Operation Path

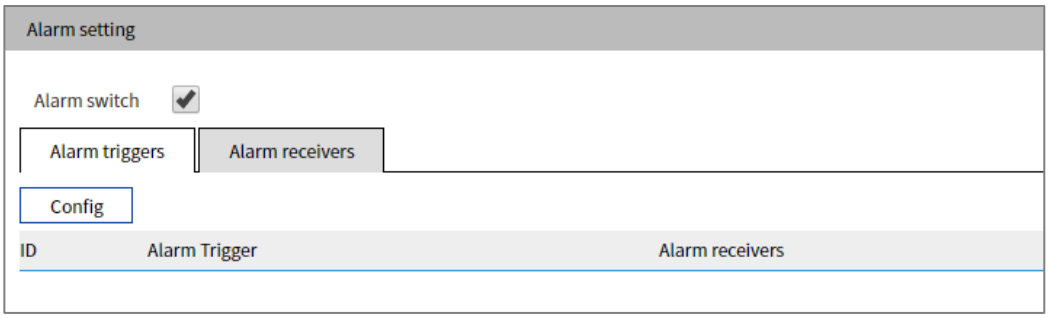
Open in order: "Port Config > Alarm Settings".

Click the “Alarm Trigger” tab.

Interface Description

Alarm Trigger interface as below:

Copyright © 3onedata Co., Ltd.



Configuration description of main elements of the Alarm Trigger interface:

Interface Element	Description
Alarm switch	Alarm status check box, when checked, the alarm function can be turned on.
ID	Alarm ID
Alarm Trigger	Trigger an alarm event, and support alarms such as port, temperature, voltage, network load, packet loss, error, etc.
Alarm Receivers	The alarm receiving mode supports SNMP Trap and e-mail.
Buttons	Configuration: Configure alarm triggering events. Edit: Edit the current alarm entry. Delete: delete the the current alarm entry.

4.4.1.1 Port Alarm

Operation Path

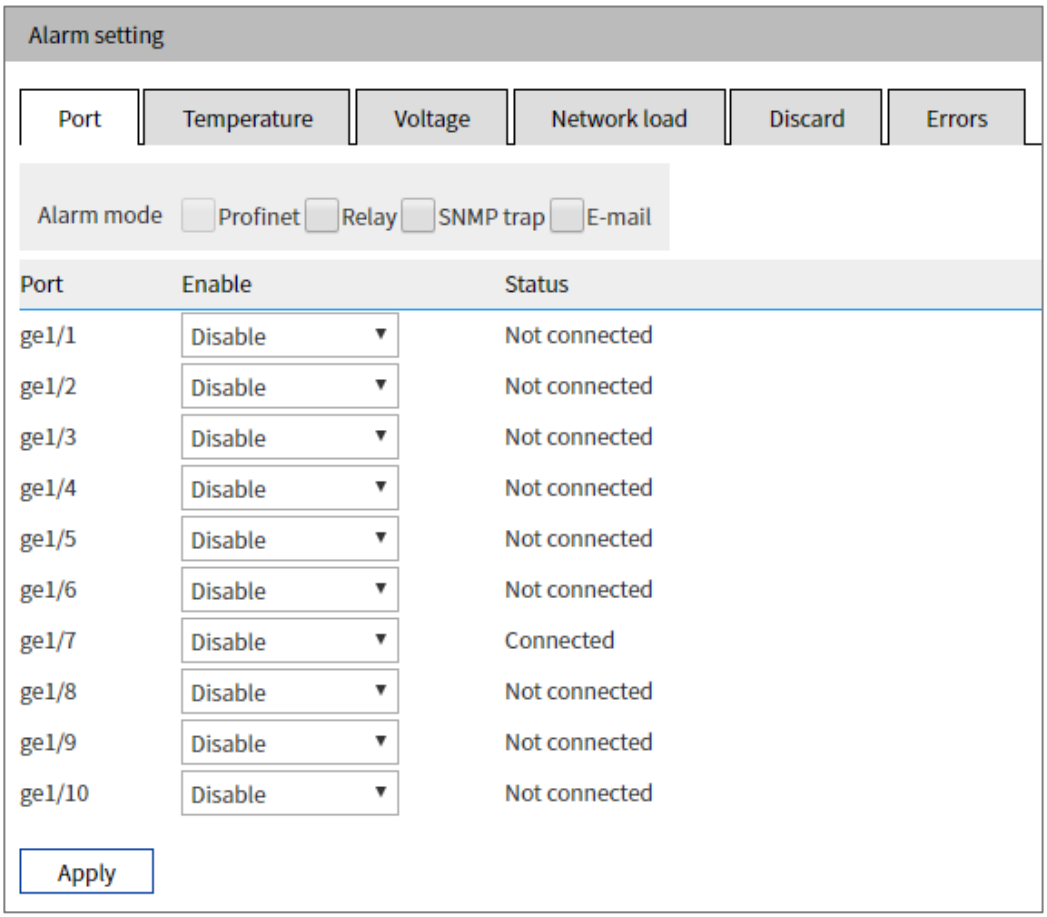
Open in order: "Port Config > Alarm Settings".

On the “Alarm Trigger” page, click the “Configure” button and click the “Port” tab.

Interface Description

Port interface as below:

Copyright © 3onedata Co., Ltd.



The main element configuration description of port interface:

Interface Element	Description
Alarm mode	Alarm mode check box, the options are as follows: • Profinet: display the alarm mode of Profinet. If the device is configured on the configuration software and related alarm items are configured, the corresponding Profinet check box will be checked. Display Checked, the page can't modify the related alarm items. • Relay: alarm by changing the state of relay. • SNMP Trap: send Trap alarm information through SNMP protocol. • E-mail: Send alarm information by mail.
Port	The corresponding port name of the device Ethernet port.
Enable	Port alarm function status, options as follows: • Enable; • Disable. Note: After enable port alarm, when port occurs abnormal status, such as connection break down, the device will output a signal to hint the

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	abnormal operation of device.
Status	Port link status, display items as follows: • Not connected; • Connected.

4.4.1.2 Temperature Alarm

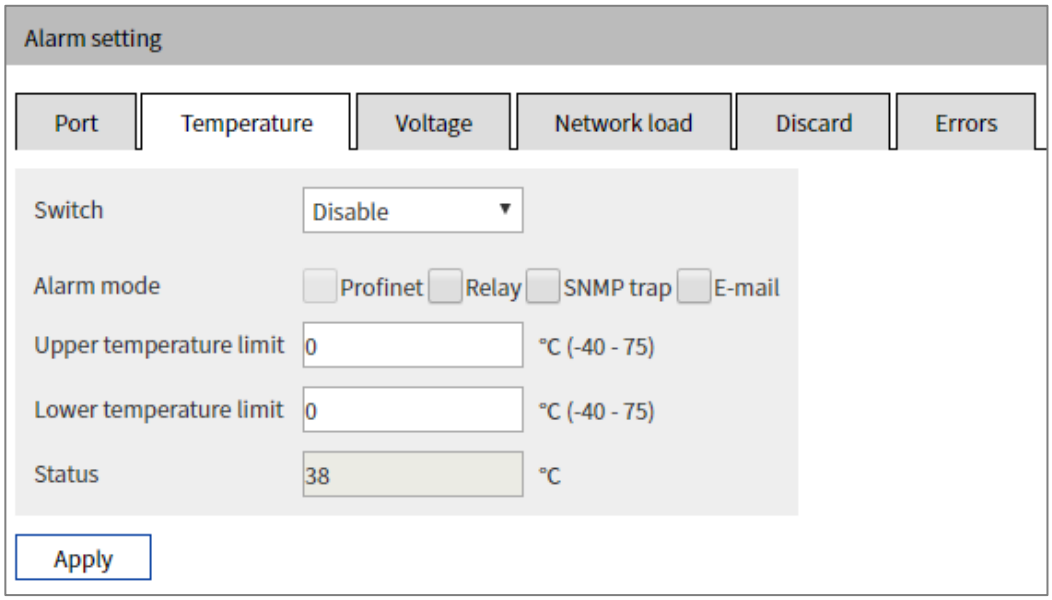
Operation Path

Open in order: "Port Config > Alarm Settings".

On the Alarm Trigger page, click the Configure button and click the Temperature tab.

Interface Description

Temperature interface is as below:



Configuration description of main elements of the Temperature interface:

Interface Element	Description
Switch	The drop-down list of Temperature alarm status. The options are as follows: • Disable; • Enable.
Alarm mode	Alarm mode check box, the options are as follows: • Profinet: display the alarm mode of Profinet. If the device is configured on the configuration software and related

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	alarm items are configured, the corresponding Profinet check box will be checked. Display Checked, the page can't modify the related alarm items. • Relay: alarm by changing the state of relay. • Trap: send Trap alarm information through SNMP protocol. • E-mail: Send alarm information by mail.
Upper temperature limit	The upper limit alarm value of the working temperature of the device, unit: ℃.
Lower temperature limit	The lower limit alarm value of the working temperature of the device, unit: ℃.
Status	Current operation temperature of the device.

4.4.1.3 Voltage Alarm

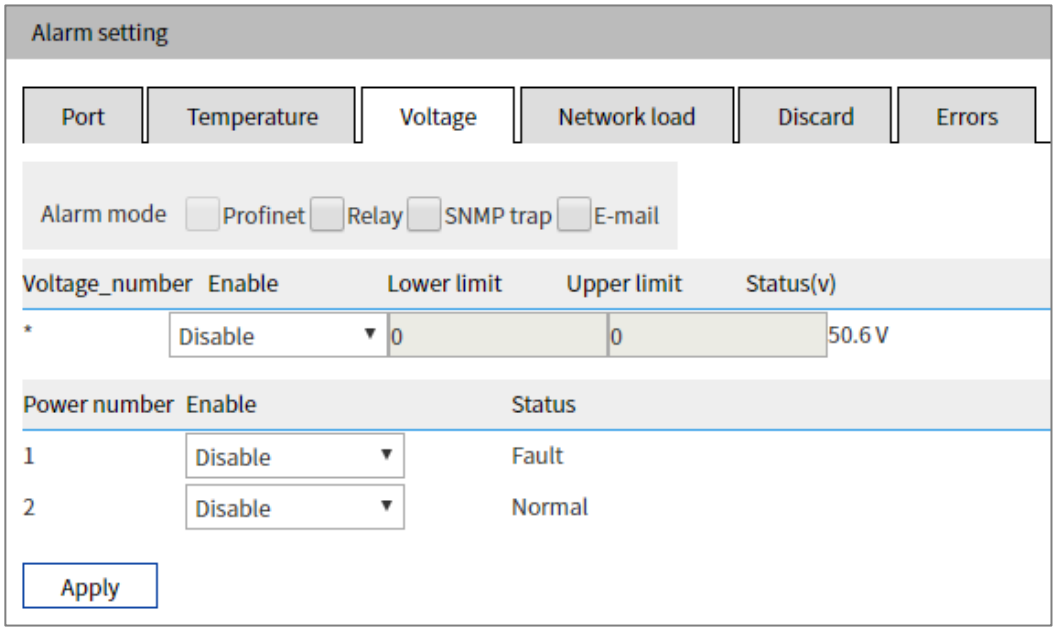
Operation Path

Open in order: "Port Config > Alarm Settings".

On the Alarm Trigger page, click the Configure button and the Voltage tab.

Interface Description

Voltage interface is as below:



Copyright © 3onedata Co., Ltd.

The main element configuration description of the Voltage interface:

Interface Element	Description
Alarm mode	Alarm mode check box, the options are as follows: • Profinet: display the alarm mode of Profinet. If the device is configured on the configuration software and related alarm items are configured, the corresponding Profinet check box will be checked. Display Checked, the page can't modify the related alarm items. • Relay: alarm by changing the state of relay. • Trap: send Trap alarm information through SNMP protocol. • E-mail: Send alarm information by mail.
Power	The corresponding number of this device's power supply
Enable	The state of power supply voltage alarm function, options are as follows: • Disable • Enable
Lower limit	The lower limit value of the input voltage of the device, unit: V.
Upper limit	The upper limit value of the input voltage of the device, unit: V.
Status	The state of the input voltage of the power supply.
Power	The corresponding number of this device's power supply
Enable	The state of power supply alarm function, options are as follows: • Disable • Enable Note: • DC provides 2 power supplies, when one power supply goes wrong, another power supply can supply electricity soon, dual power supply hot standby is supported. • After enabling power supply alarm, the device will output alarm signal to hint abnormal operation of power supply when power supply runs abnormally.
Status	The power supply status of the device.

Copyright © 3onedata Co., Ltd.

4.4.1.4 Network Load Alarm

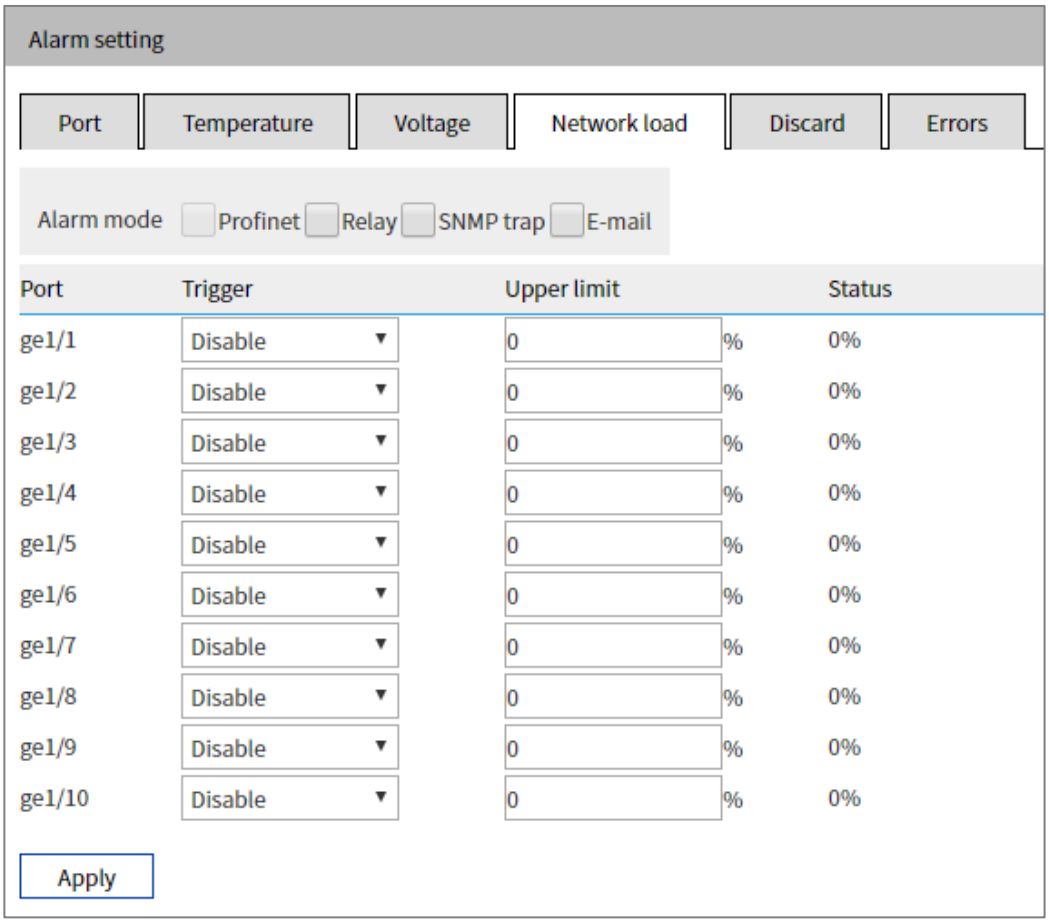
Operation Path

Open in order: "Port Config > Alarm Settings".

On the Alarm Trigger page, click the Configure button and click the Network Load tab.

Interface Description

Network load interface is as follows:



The main element configuration description of network load interface:

Interface Element	Description
Alarm mode	Alarm mode check box, the options are as follows: • Profinet: display the alarm mode of Profinet. If the device is configured on the configuration software and related alarm items are configured, the corresponding Profinet check box will be checked. Display Checked, the page can't modify the related alarm items.

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	• Relay: alarm by changing the state of relay. • Trap: send Trap alarm information through SNMP protocol. • E-mail: Send alarm information by mail.
Port	The corresponding port name of the device Ethernet port.
Trigger	Trigger the drop-down list of network load alarm enable. The options are as follows: • Enable • Disable
Upper limit	Percentage of upper limit value that triggers network load alarm.
Status	Network bandwidth load status.

4.4.1.5 Packet Loss Alarm

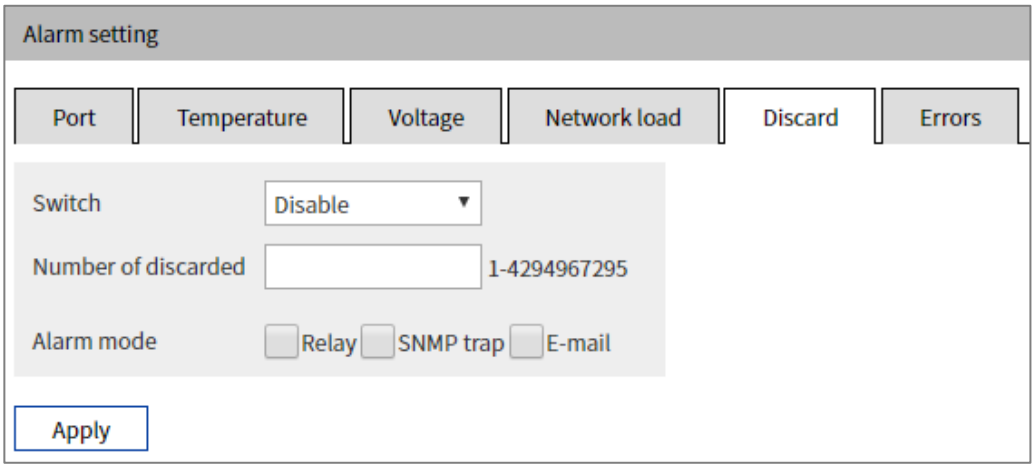
Operation Path

Open in order: "Port Config > Alarm Settings".

On the Alarm Trigger page, click the Configure button and the Packet Loss tab.

Interface Description

Dropped Packets interface is as below:



Configuration description of main elements of the Dropped Packets interface:

Interface Element	Description

Copyright © 3onedata Co., Ltd.

Interface Element	Description
Switch	The status of packet loss alarm, options: • Disable • Enable
Number of discarded	Number of dropped frames triggering packet loss alarm.
Alarm mode	Alarm mode check box, the options are as follows: • E-mail: Send alarm information by mail. • SNMP Trap: send Trap alarm information through SNMP protocol. • Relay: alarm by changing the state of relay.

4.4.1.6 Error Alarm

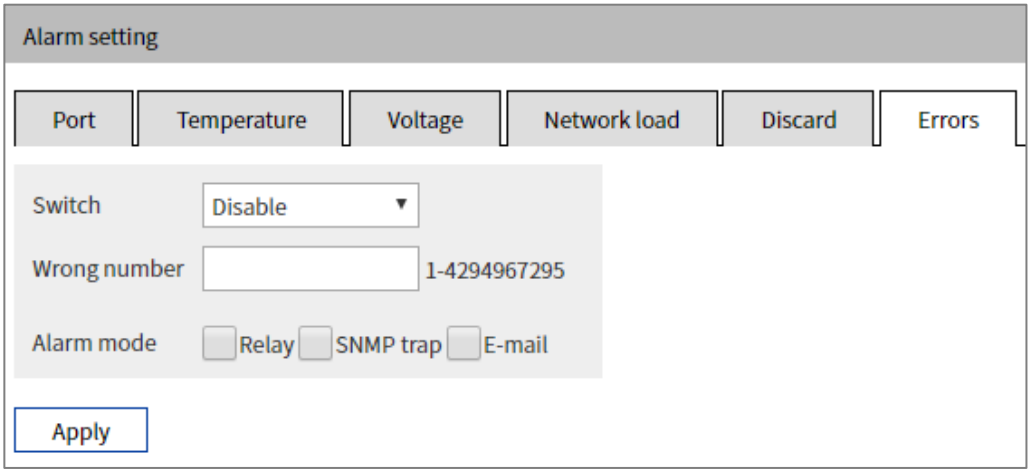
Operation Path

Open in order: "Port Config > Alarm Settings".

On the Alarm Trigger page, click the Configure button and click the Error tab.

Interface Description

Error interface as follows:



The main element configuration description of the Error interface:

Interface Element	Description
Switch	Frame alarm status, options: • Disable • Enable

Copyright © 3onedata Co., Ltd.

Interface Element	Description
Wrong number	The number of error frames that trigger an error alarm.
Alarm mode	Alarm mode check box, the options are as follows: • Relay: alarm by changing the state of relay. • SNMP Trap: send Trap alarm information through SNMP protocol. • E-mail: Send alarm information by mail.

4.4.2 Alarm Receivers

Function Description

The alarm receiving mode is as follows:

- SNMP Trap
- E-mail

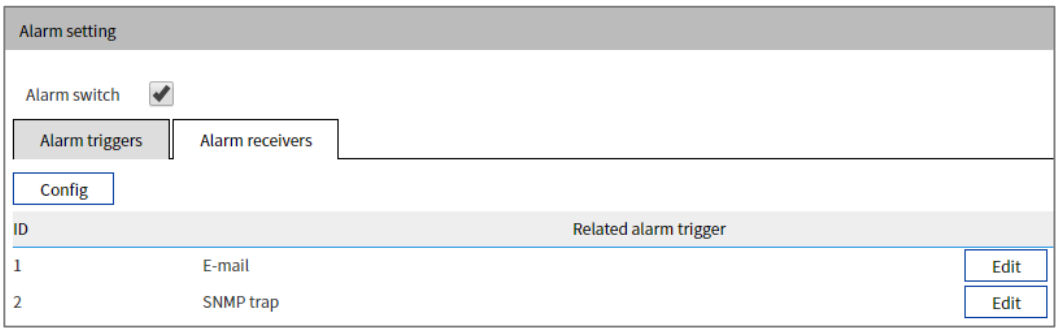
Operation Path

Open in order: "Port Config > Alarm Settings".

Click the Alarm Receiving tab.

Interface Description

Alarm receiving interface is as below:



The main element configuration description of the Alarm receiving interface:

Interface Element	Description
Alarm switch	Alarm status check box, when checked, the alarm function can be turned on.
ID	Alarm ID
Alarm receiving	The alarm receiving mode and configuration information, it supports SNMP Trap and e-mail.

Copyright © 3onedata Co., Ltd.

Interface Element	Description
Related alarm trigger	Alarm triggering events supported by the receiving mode, such as port, temperature, voltage, network load, packet loss, error and other alarms.
Buttons	Configuration: Configure the alarm receiving mode. Edit: edit the current alarm receiving method.

4.4.2.1 Trap Settings

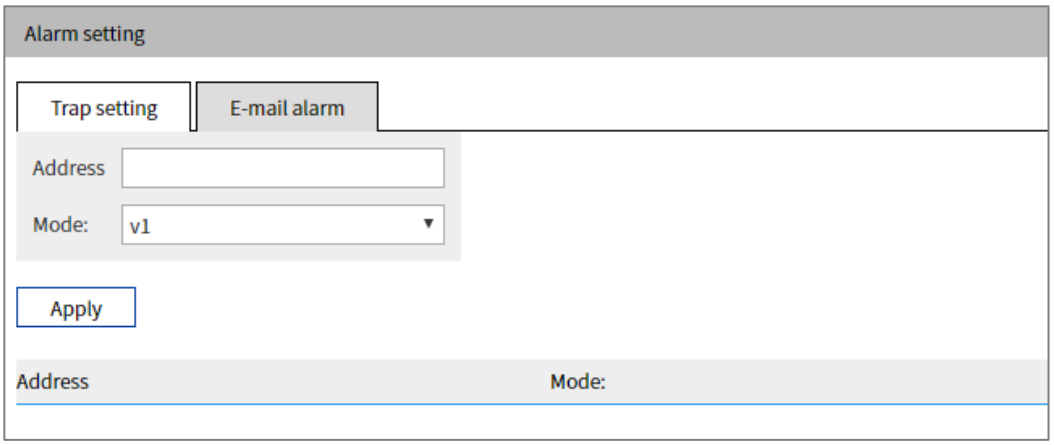
Operation Path

Open in order: "Port Config > Alarm Settings".

On the Alarm Receiving page, click the Configure button and click the Trap Settings tab.

Interface Description

Trap settings interface as follows:



The main element configuration description of Trap settings interface:

Interface Element	Description
Address	Destination IP address of SNMP trap message
Mode	SNMP version drop-down list, the options are as follows: • v1 • v2c

Copyright © 3onedata Co., Ltd.

4.4.2.2 Email Alerts

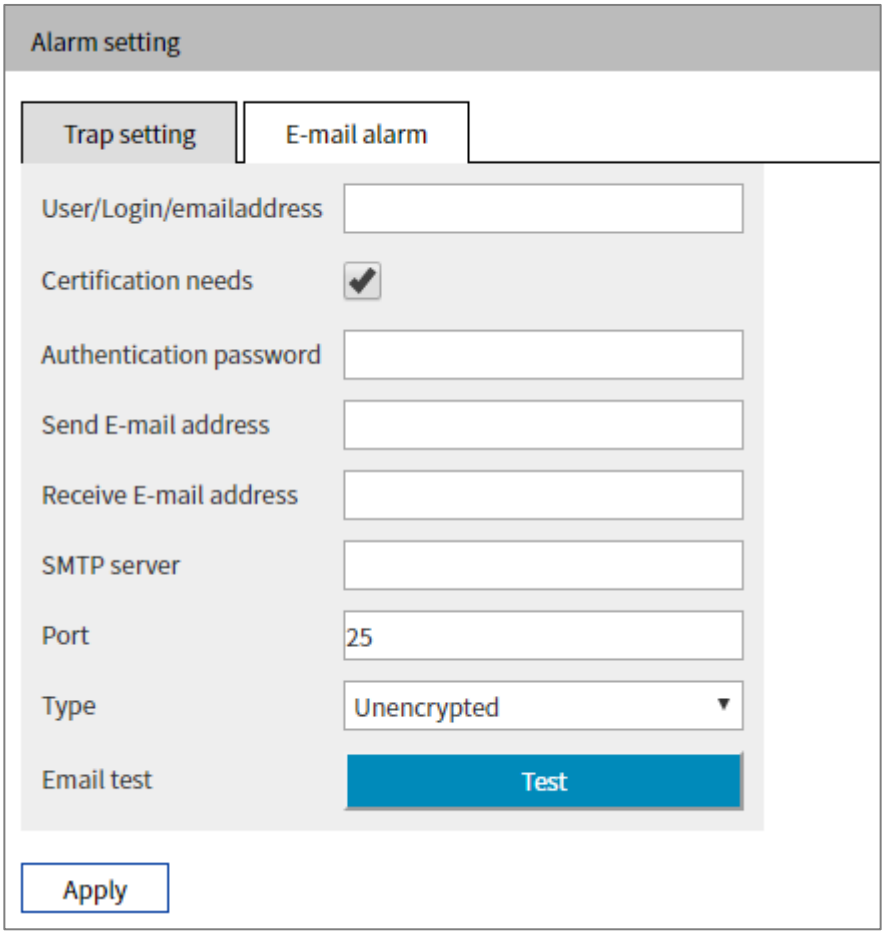
Operation Path

Open in order: "Port Config > Alarm Settings".

On the Alarm Receiving page, click the Configure button and click the E-mail Alarm tab.

Interface Description

E-Mail Alarm interface is as follows:



Main elements configuration description of E-mail alarm interface:

Interface Element	Description
User/login/email address	Address of the mailbox server.
Certification needs	Require authentication check box.
Authentication Password	Authentication information or login password of sender's mailbox server.
Send e-mail address	E-mail address of sender, account name used for

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	logging in to the E-mail server.
Receive e-mail address	E-mail address used by abnormal event receiver.
SMTP server.	The SMTP email server address should be based on the used email account. The host IP address or used host name that provides E-mail delivery service for the device.
Port	Port number of SMTP server address.
Type	Encryption type, options: • Unencrypted • TLS • STARTTLS
Email test	The device sends an alarm email to the receiving mailbox through the sending mailbox, which is used to test whether the email is in normal communication.

4.5 Link Aggregation

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 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.

Copyright © 3onedata Co., Ltd.

4.5.1 Static Link Aggregation

Function Description

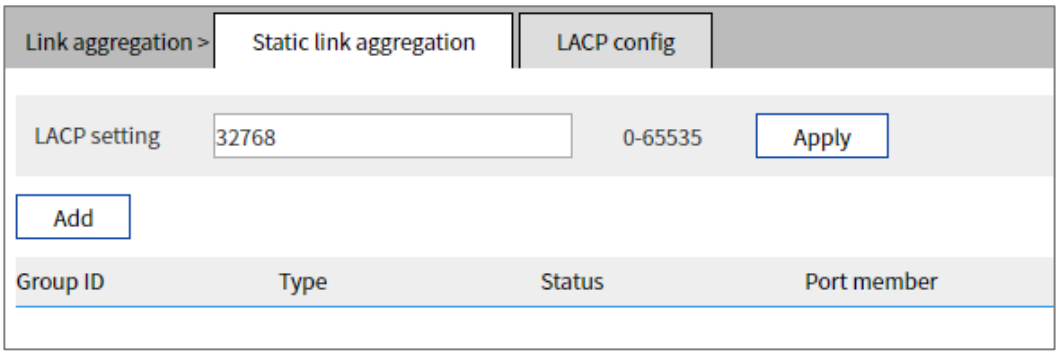
Under static aggregation mode, the member port in aggregation group disables LACP protocol, its port status is maintained manually.

Operation Path

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

Interface Description

Static Link Aggregation interface as below:



The main element configuration description of Static Link Aggregation interface:

Interface Element	Description
LACP setting	LACP priority level setting, LACP setting range 0-65535, defaults to 32768. Note: The smaller of interface LACP priority level value is, the higher priority level is, which is used for distinguishing the priority degree of selecting different ports as active port.
Group ID	Added port aggregation group ID number. The ID number of static aggregation link, support up to 14 groups, each group can configure up to 8 ports to join aggregation.
Type	Aggregation group mode: • Manual: Static aggregation; • LACP: Dynamic aggregation.
Status	Aggregation group connection state: • UP: Port member is connected; • DOWN: Port member is disconnected.
Port member	Port member in the aggregation group.

Copyright © 3onedata Co., Ltd.

4.5.2 LACP Configuration

Function Description

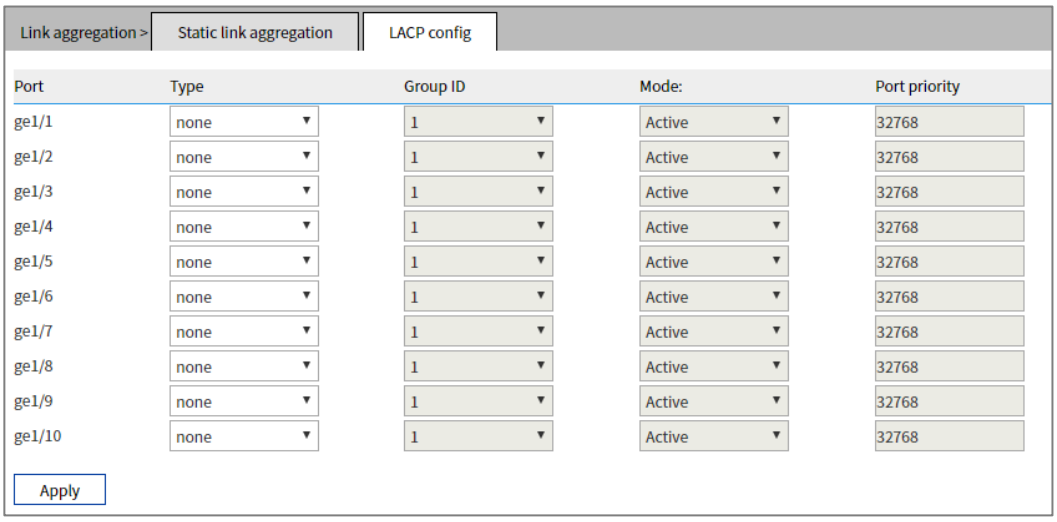
Dynamic aggregation is an aggregation method in which system automatically creates or deletes aggregation group, the port addition and deleting in the dynamic aggregation group is done automatically by LACP protocol. Only ports connected to the same device with same rate, duplex property, and basic configuration can create a dynamic aggregation. Even one port can also create dynamic aggregation, at this time, its single port aggregation. In dynamic aggregation, port LACP protocol is in enable state.

Operation Path

Open in order: "Port Config > Link Aggregation > LACP Config".

Interface Description

LACP configuration interface as follows:



The main element configuration description of LACP configuration interface:

Interface Element	Description
Port	The corresponding port name of the device Ethernet port.
Type	Setting port aggregation function: • None: Represent the port disabling link aggregation function; • Static: Represent the port is static aggregation mode; • Dynamic (LACP): Represent the port is dynamic aggregation mode.
Group ID	Group ID, the range is 1-16.

Copyright © 3onedata Co., Ltd.

Interface Element	Description
Mode	Mode refers to dynamic LACP negotiation mode, it's divided into: • Active: the port sends LACP message periodically; • Passive: the port doesn't send LACP message in normal time, once receiving the LACP message of opposite terminal, it will normally send LACP message.
Port priority.	Dynamic LACP port priority, defaults to 32768.

4.6 Port Isolation

Function Description

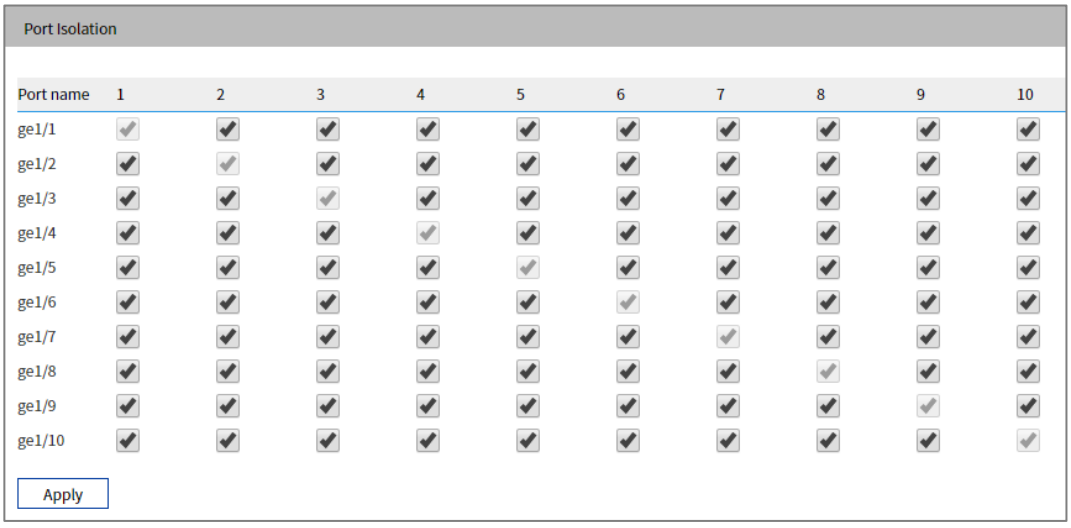
Port isolation is to isolate different interfaces of the same VLAN. Through port isolation, when the port receives external data and forwards it internally, the data can only be forwarded to the specified port member. Port isolation has provided safer and more flexible networking scheme for users.

Operation Path

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

Interface Description

Isolate-port configuration interface as follows:



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

Copyright © 3onedata Co., Ltd.

Interface Element	Description
Port name	The Ethernet port name of the device.
1-10	Port ID, which can be checked to isolate the downstream port members of the group traffic.

4.7 Port Statistics

4.7.1 Port Statistics

Function Description

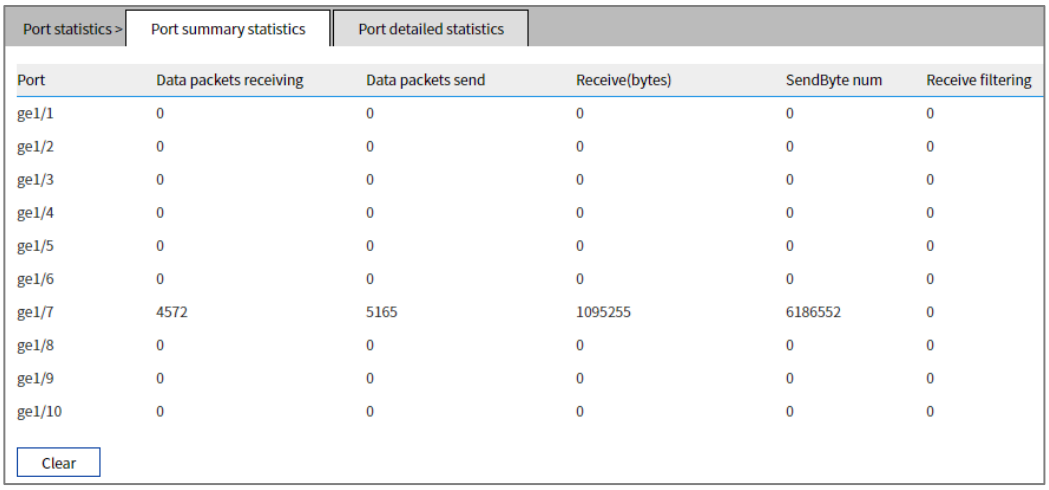
On the "Port Stats" page, user can check the data packet and byte number that each port sends or receives,

Operation Path

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

Interface Description

Port Statistics interface as follows:



Copyright © 3onedata Co., Ltd.

4.7.2 Detail Port Stats

Function Description

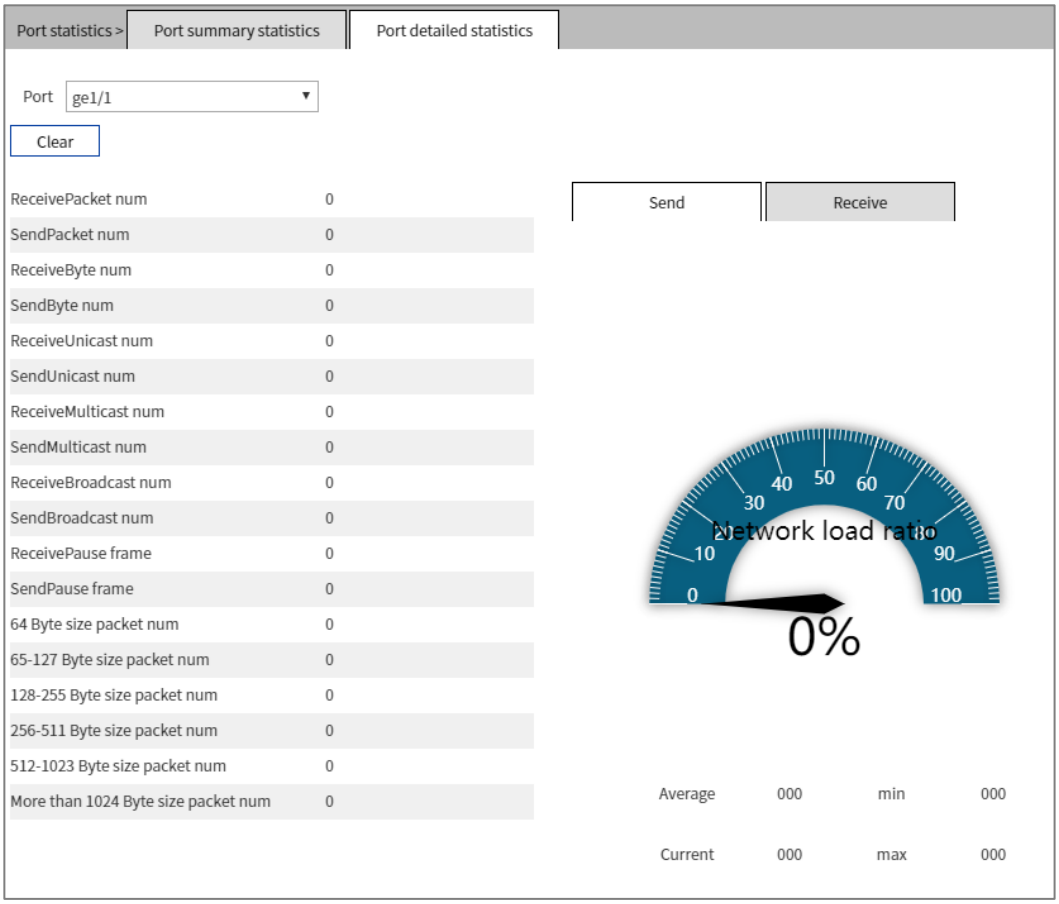
On the "Detail port stats" page, user can check the data sum and message size classified statistic that each port sends or receives, and network load diagrams for ports.

Operation Path

Open in order: "Port Config > Port statistics > Detail port stats".

Interface Description

Detail port stats interface as follows:



Copyright © 3onedata Co., Ltd.

4.8 Cable Test

Function Description

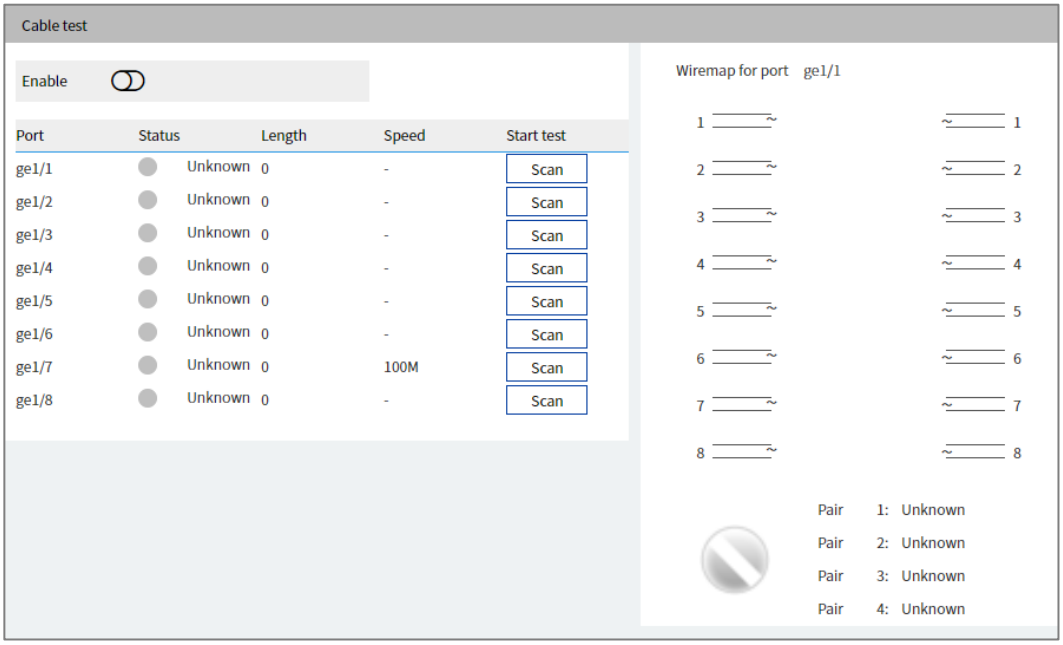
On the “Cable Test” page, user can check the physical status of network cable of Ethernet port.

Operation Path

Open in order: "Port Configuration > Cable Test".

Interface Description

Cable Test interface is as below:



The main element configuration description of the Cable Test interface:

Interface Element	Description
Enable	Check the cable enable switch button, and the status is as follows: • : Enable • : Shutdown
Port	The corresponding port name of the device Ethernet port. Note: This port will be rebooted when Cable Test is enabled.
Status	The Cable Test status could be divided into the following

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	types: • OK: Normal • Open: open circuit • Short: short circuit • Open/Short: open circuit or short circuit • Crosstalk • Unknow: Unknown
Length	The length of cable. Note: The length error range of test result: ±10m
Speed	Port transmission speed.
Start test	Click the "Scan" button to start detecting the port connection cable information.
Cable test result	Displays the cable status, the number of twisted pairs, and the status of each twisted pair.

Copyright © 3onedata Co., Ltd.

5 Layer 2 Configuration

5.1 VLAN Configuration

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, don’t need to change ports or connection; only needs to change the software 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 802.1Q

Function Description

On the VLAN 802.1Q page, users can add 802.1Q VLAN entries.

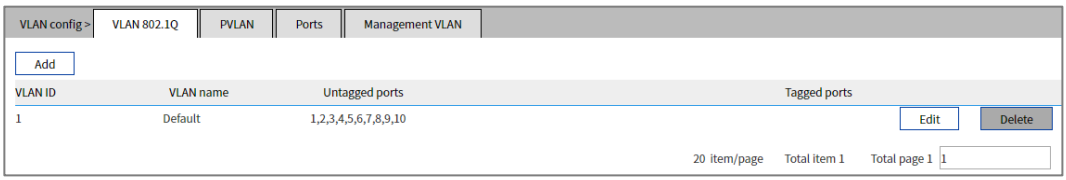
Operation Path

Open in order: "Layer 2 Configuration > VLAN Configuration > VLAN 802.1Q".

Copyright © 3onedata Co., Ltd.

Interface Description

VLAN 802.1Q interface as below:



Main elements configuration descriptions of VLAN 802.1Q interface:

Interface Element	Description
VLAN ID	VLAN ID number, value range is 1-4094.
VLAN name	VLAN name information.
Untagged ports	Untagged port member to conduct untagged process to sending data frame.
Tagged ports	Tag port member to conduct tagged process to sending data frame.

5.1.2 PVLAN

Function Description

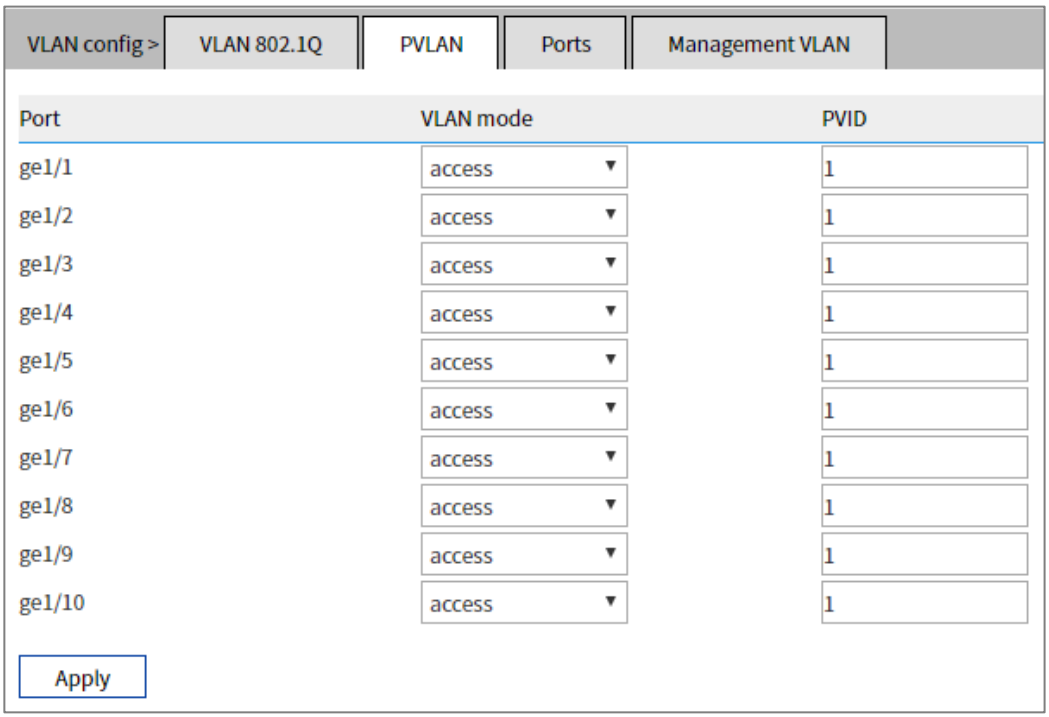
On the PVLAN page, users can configure the port type and port VLAN ID.

Operation Path

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

Interface Description

PVLAN interface as below:



Main elements configuration descriptions of PVLAN interface:

Interface Element	Description
Port	The corresponding port name of the device Ethernet port.
VLAN Mode	Port VLAN mode. Options are: • Access: The port can only belong to 1 VLAN (the default VLAN). When the Tag of the message received by the port is the same as the PVID, the message is received, otherwise it is discarded. Generally used to connect with terminal device. • Trunk: port can belong to multiple VLANs. When the Tag of the message received by the port is the VLAN ID to which the port belongs, the message is received; otherwise, it is discarded. Commonly used in the connection between network devices.
PVID	Default port VLAN ID number, value range is 1-4094. 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.

5.1.3 Port

Function Description

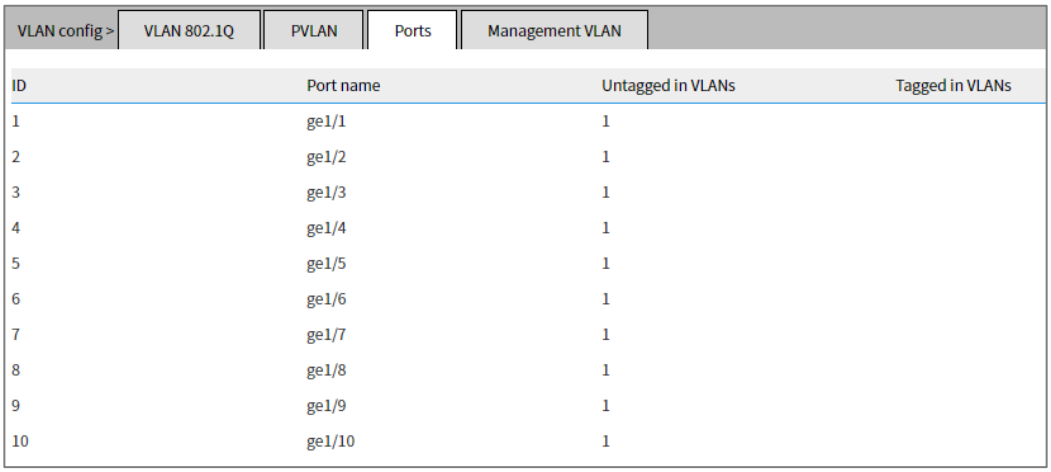
On the Port page, users can view the port VLAN configuration information.

Operation Path

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

Interface Description

Port interface as below:



The main element configuration description of port interface:

Interface Element	Description
ID	Port entry ID.
Port name	The corresponding port name of the device Ethernet port.
Untagged in VLANs	The VLAN ID number that the port allows to pass without tags.
Tagged in VLANs	The VLAN ID number that the port allows to pass with tags.

5.1.4 Manage VLAN

Function Description

On the "Management VLAN" page, users can configure the management VLAN ID, and members in the management VLAN can access the device WEB.

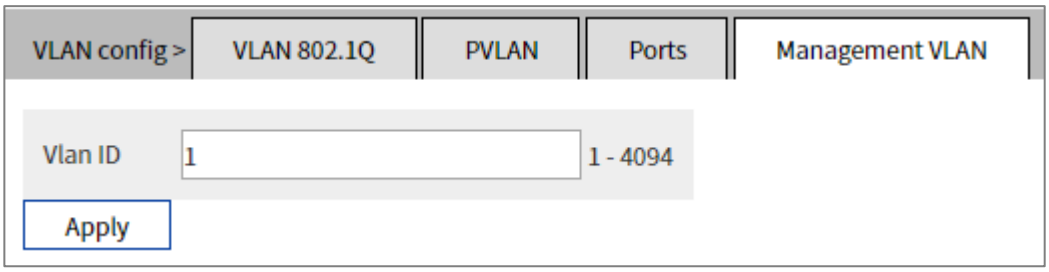
Copyright © 3onedata Co., Ltd.

Operation Path

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

Interface Description

Management VLAN interface as below:



Main element configuration descriptions of Management VLAN interface:

Interface Element	Description
Vlan ID	Users can login to the switch through the interface of manageVLAN to realize the centralized device management of network management. ManageVLAN ID, its value range is 1-4094.

5.2 MAC Configuration

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.

5.2.1 MAC Configuration

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

Copyright © 3onedata Co., Ltd.

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).

Function Description

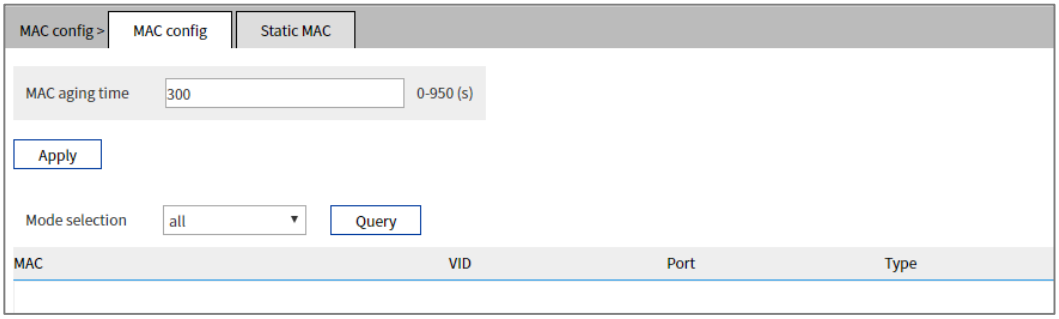
On the "MAC Config" page, user can configure the ageing time of dynamic MAC address and check static and dynamic MAC address information.

Operation Path

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

Interface Description

MAC configuration interface is as follows:



The main element configuration description of MAC configuration interface:

Interface Element	Description
MAC Aging Time	MAC address aging-time, unit is second, default value is 300, and range is 0~950.
Mode Selection	MAC table query mode, the options are as follows: • All • Vlan-Based • Port-Based • MAC-based
MAC	Access the device MAC address.
VID	VLAN ID number the data MAC address sending belongs to.
Port	Corresponding port number of the MAC address.
Type	MAC address type, dynamic MAC and static MAC address, display as follows: • Static;

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	• Dynamic.

5.2.2 Static MAC

Function Description

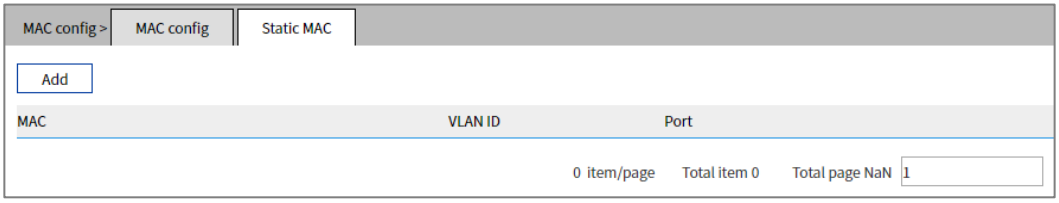
On the "Static Mac" page, user can manually configure the static MAC address and bind the source MAC address without aging.

Operation Path

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

Interface Description

Static MAC interface as follows:



The main element configuration description of static MAC interface:

Interface Element	Description
MAC	Static MAC address bound to the interface, for example: 0001-0001-0001.
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.
Port	Select the binding port number via the drop-down arrow.

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.

Copyright © 3onedata Co., Ltd.

- Please don't enter reserved MAC address, such as the local MAC address.

5.3 IGMP Snooping

IP host applies for joining (or leaving) multicast group to nearby routers through the Internet Group Management Protocol (IGMP). IGMP Snooping is a multicast suppression mechanism that manages and controls multicast group by listening and analyzing IGMP messages exchanged between host and multicast devices.

The working process of IGMP Snooping: The switch snoops the messages between user host and router, as well as tracking multicast information and the ports that have been applied for. When the switch intercepts the IGMP Report (request) sent by the host toward router, the switch adds the port to multicast forwarding table. When the switch intercepts the IGMP Leave message sent by the host, the router sends a Group-Specific Query message of the port. If other hosts need the multicast, they will respond with the IGMP Report message. If the router can't receive any response from the host, the switch deletes the port from the multicast forwarding table. The router sends IGMP Query message periodically. When switch receives IGMP Query message, it would delete this port from multicast table if it doesn’t receive IGMP Report message from the host in a given period time.

5.3.1 IGMP Snooping

Function Description

On the "IGMP-snooping" page, users can enable/disable IGMP and configure the host aging time.

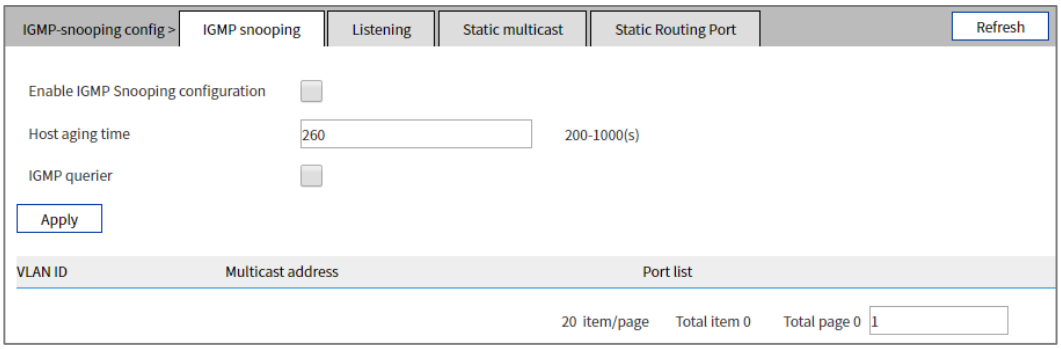
Operation Path

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

Interface Description

IGMP Snooping interface as below:

Copyright © 3onedata Co., Ltd.



The main element configuration description of IGMP Snooping interface:

Interface Element	Description
Enable IGMP-snooping configuration	Enable IGMP-snooping configuration checkbox.
Host aging time	Host aging time, value range is 200-1000s.
IGMP querier	Enable IGMP Querier, the device can join in IGMP Querier election. It would send query message and receive report message of the member to maintain the relationship of multicast group member.
VLAN ID	Port number VLAN ID number.
Multicast address	Multicast IP address.
Port list	The corresponding port name of the device Ethernet port.

5.3.2 IGMP Monitoring-VLAN

Function Description

On the page of "IGMP monitoring-VLAN", you can configure the basic functions of VLAN-based IGMP Snooping, and the device can establish and maintain the layer 2 multicast forwarding table to realize the on-demand distribution of multicast data messages in the data link layer.

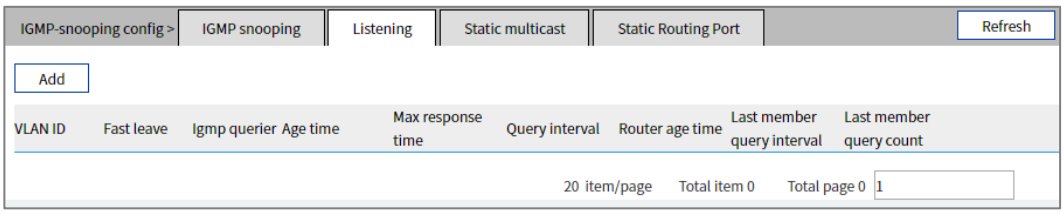
Operation Path

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

Interface Description

IGMP-snooping VLAN configuration interface as follows:

Copyright © 3onedata Co., Ltd.



The main element configuration description of IGMP-snooping-VLAN configuration interface:

Interface Element	Note (Click "Add" to add snooping entry)
VLAN ID	The VLAN ID monitored by IGMP, with a value of 1-4094.
Fast Leave	Fast Leave allows the member ports in VLAN to leave the multicast group quickly.
Igmp Querier	IGMP Snooping query function of VLAN.
Age time	Aging time of dynamic member ports in VLAN, in integer form, ranging from 1 to 255, and the unit is seconds.
MAX response time	The maximum response time of IGMP universal group query message in VLAN, an integer ranging from 1 to 25 in seconds. The default value is 10s.
Query interval	IGMP universal group query message sending time interval, in integer form, ranging from 2 to 300, and the unit is seconds.
Router age time	Dynamic router port aging time in VLAN, in integer form, ranging from 2 to 300, and the unit is seconds.
Last member query interval	The last member query time interval in VLAN, that is, the sending time interval of IGMP specific group query message, is in integer form, with the value range of 1-5 and the unit of seconds.
Last member query count	IGMP robustness coefficient, that is, the number of times Query messages are sent in integer form, and the value range is 1-255.

5.3.3 Static Multicast

Function Description

On the "Static multicast" page, user can add or delete static multicast.

Main function of static multicast: Add certain ports to a multicast group; these ports can receive data when data is sent to this multicast address.

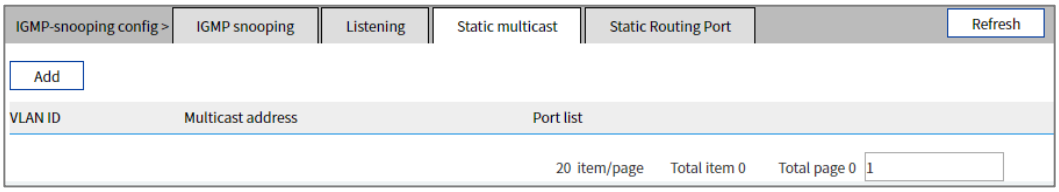
Copyright © 3onedata Co., Ltd.

Operation Path

Open in order: "Layer 2 Configuration > IGMP-snooping > Static Multicast".

Interface Description

Static multicast interface as follows:



The main element configuration description of static multicast interface:

Interface Element	Description
VLAN ID	VLAN ID number, value range is 1-4094.
Multicast address	Multicast IP address information, such as: 225.1.2.3.
Port list	The display device ports form multicast group.

5.3.4 Static Routing Port

Function Description

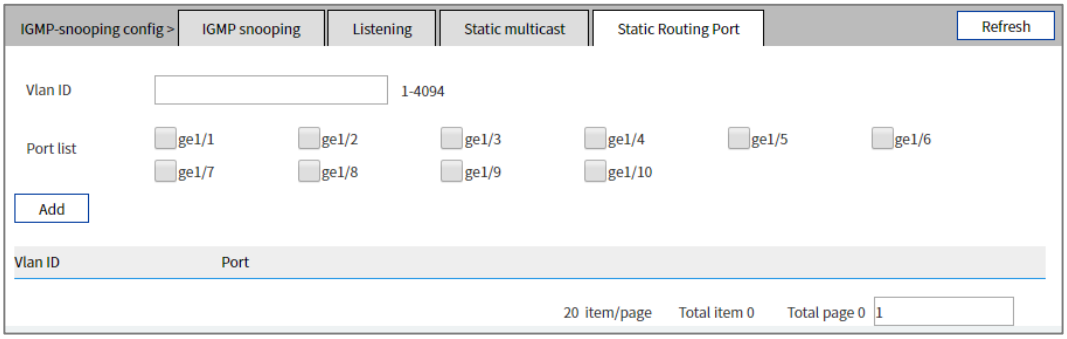
On the "Static Routing Port" page, user can configure the port of multicast router.

Operation Path

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

Interface Description

The static routing port interface as follows:



The main elements configuration description of static routing port configuration interface:

Copyright © 3onedata Co., Ltd.

Interface Element	Description
VLAN ID	VLAN ID number, value range is 1-4094.
Port	Check the checkbox of port list, select device port as the static router port that connects router.

5.4 Spanning-Tree Configuration

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.

5.4.1 Bridge Configuration

Function Description

On the "Bridge Configuration" page, user can configure relative parameters of spanning-tree.

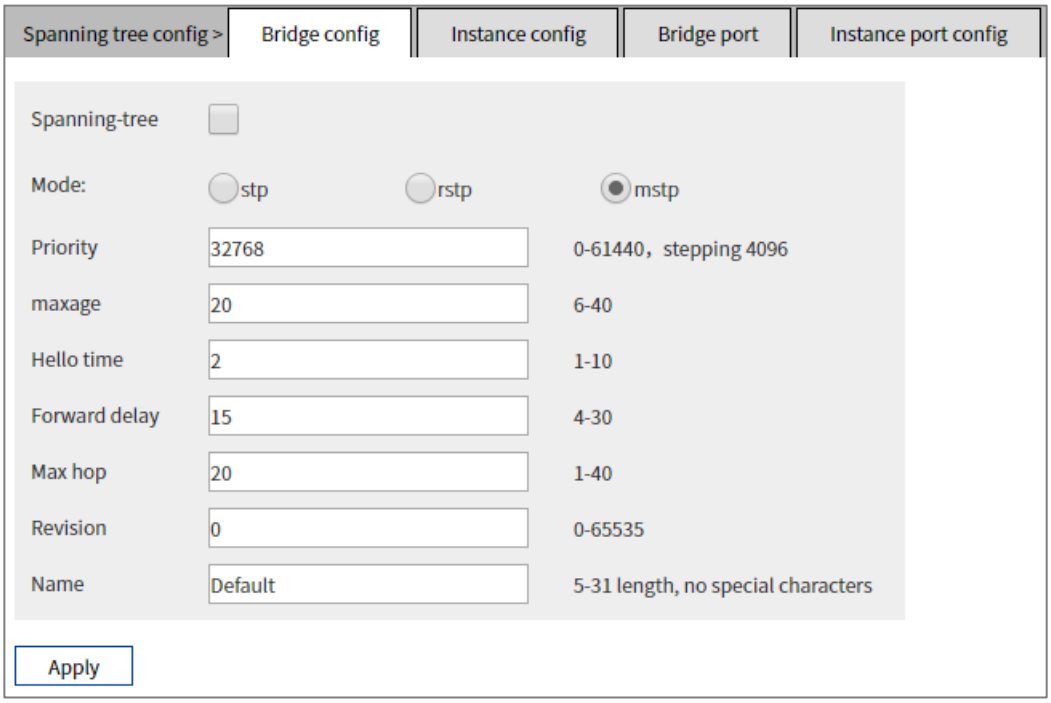
Operation Path

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

Interface Description

Bridge settings interface as follows:

Copyright © 3onedata Co., Ltd.



The main element configuration description of bridge settings interface:

Interface Element	Description
Spanning Tree	Check to enable Spanning-tree.
Mode	Three modes for spanning-tree protocol choice: • STP: Spanning-tree; • RSTP: Rapid spanning tree; • MSTP: Multiple spanning-trees.
Priority	Bridge priority level, value range is 0-61440. Note: Smaller the priority level value is, higher the priority level is.
Maxage	The maximum lifetime of the message in the device, range is 6-40. It's used to determine whether the configuration message times out.
Hello Time	Message sending cycle, value range is 1-10. Note: The spanning tree protocol sends configuration information every Hello time to check whether the link is faulty.
Forward delay	Port state transition delay, value range is 4-30.
Max Hop	The maximum hop in MST region, 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.
Revision	MSTP revision level, value range is 0-65535. Note:

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	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.
Name	MST domain name, up to 31 characters.

5.4.2 Instance Configuration

Function Description

On the "Instance Configuration" page, user can 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).

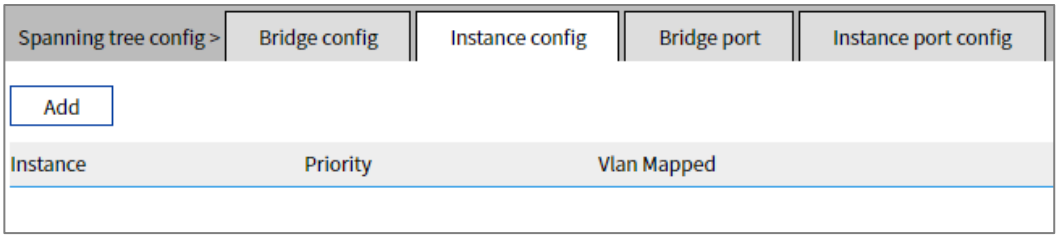
VLAN mapping table is an attribute of MST region, and it's used to describe the mapping relation between VLAN and MSTI.

Operation Path

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

Interface Description

Instance configuration interface as follows:



The main element configuration description of instance configuration interface:

Interface Element	Description
Instance	Multiple Spanning-tree instance ID number.
Priority	Device priority level, value range is 0-61440, default to 32769, step is 4096. Note: The priority of a device participates in spanning tree calculation. Its size determines whether the device can be selected as the root

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	bridge of a spanning tree.
VLAN Mapped	VLAN mapping table is separated by commas, such as: 4, 5, 6, 7; "-" represents range, such as: 4-7. 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.

5.4.3 Bridge Ports

Function Description

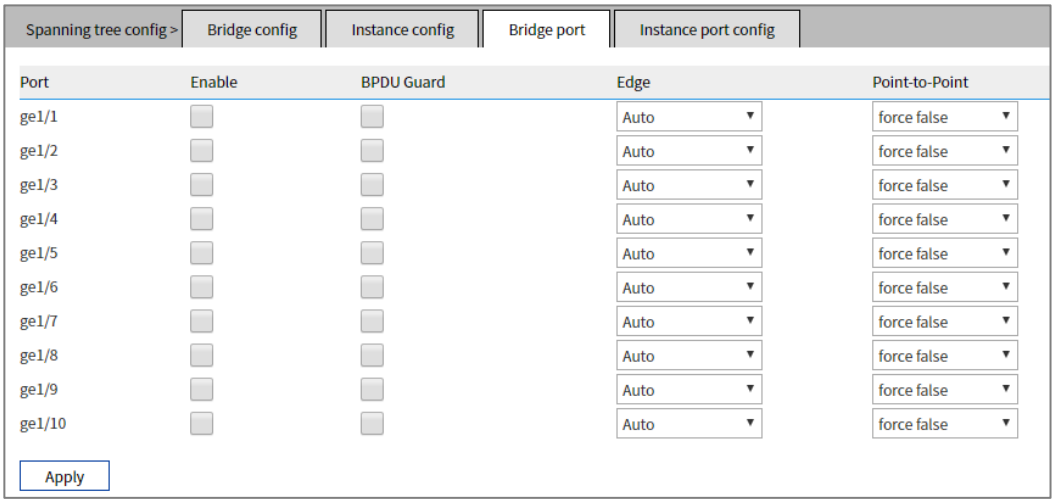
On the "Bridge Port" page, user can enable port to participate in spanning-tree and configure port type, link type and BPDU protection function.

Operation Path

Open in order: "Layer 2 Config > Spanning-tree > Bridge Ports".

Interface Description

Bridge ports interface as follows:



The main element configuration description of bridge ports interface:

Interface Element	Description
Port	The corresponding port name of the device Ethernet port.
Enable	Check to enable check box and participate in spanning-tree.
BPDU Guard	BPDU (Bridge Protocol Data Unit) protection function.
Edge	Configure port type:

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	• Auto: Automatic system detection; • Force true: edge port; • Force false: non-edge port.
Point-to-Point	Port link type: • Auto: Automatic system detection; • Force true: point-to-point link; • Force false: Non point-to-point link.

5.4.4 Instance Port Configuration

Function Description

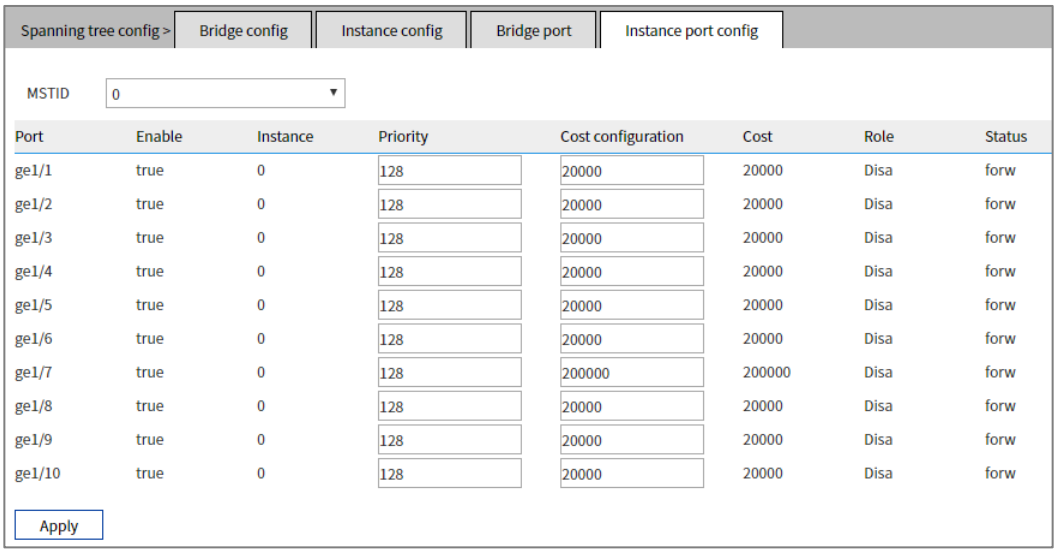
On the "Inst Port Config" page, user can configure port priority level and cost.

Operation Path

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

Interface Description

Instance port configuration interface as follows:



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:

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	• true: enable, participate in spanning-tree; • no: not enabled, not participate in spanning-tree.
Instance	Instance ID number port belongs to.
Priority	Port priority 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.
Cost configuration	The path cost from network bridge to root bridge.
Cost	Cost from current port to root bridge.
Role	Port role. • unkn: Unknown; • root: Root port; • desg: Designated port; • altn: Alternate port; • back: Backup port; • disa: Disable port.
Status	Port status in spanning-tree: • Disable: Port close status; • Blocking: Blocked state; • Listening: Monitoring state. • Learning: Learning state; • Forwarding: Forwarding state;

5.5 Ring Configuration

Ring provides automatic recovery and reconnection mechanism for the disconnected Ethernet network, which has link redundancy and self-recovery ability in case of network interruption or network failure.

The core of Ring technology adopt non-master station setting. In a multi-ring network of up to 250 switches, the network self-recovery time is less than 20 milliseconds. Each port in this device can be used as a ring port and connected with other devices. When an interruption occurs in the network connection, the Ring redundant mechanism enables the backup link to quickly recover the network communication.

Copyright © 3onedata Co., Ltd.

5.5.1 Global Configuration

Function Description

On the "Local Configuration" page, user can enable/disable the ring network.

Operation Path

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

Interface Description

Global configuration interface is as follows:



The main element configuration description of global configuration interface:

Interface Element	Description
Ring Configuration	Ring setting checkbox, enable Ring network function after checking.

5.5.2 Node Configuration

Function Description

On the "Node Configuration" page, user can configure ring network port and related parameters.

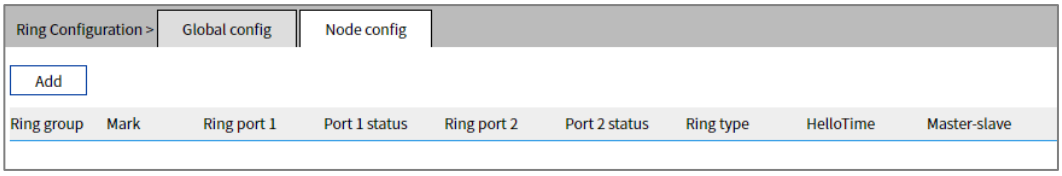
Operation Path

Open in order: "Layer 2 Config > Ring Config > Node Config".

Interface Description

Node configuration interface as follows:

Copyright © 3onedata Co., Ltd.



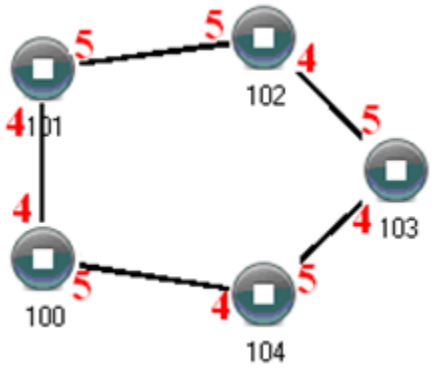
The main element configuration description of node configuration interface:

Interface Element	Description
Ring group	Support ring group 1-4, it can create 4 ring networks at the same time.
Mark	When multiple switches form a ring, the current ring ID would be network ID. Different ring network has different ID.
Ring Port1	The network port 1 on the switch device used to form a ring. Note: When the ring network type is "Couple", it displays "Coupled Port". Coupling port is the port that connects different network identities.
Port1 Status	Display the current state of ring port1 in the ring group.
Ring port2	The network port 2 on the switch used to form a ring. Note: When the ring network type is “Couple”, it displays “console port”. Console port is the port in the chain where two rings intersect.
Port2 Status	Display the current state of ring port2 in the ring group.
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. • 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 a device; users can carry the same device on two different networks or two different switching devices on the same 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.
Master-slave	Master-slave mode, options as follows: • Master: the master device of the ring network; • Slave: the slave device of the ring network; Note:

Interface Element	Description
	Single ring has master/slave device option. One-Master Multi-Slave mode is recommended in one single ring. 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.

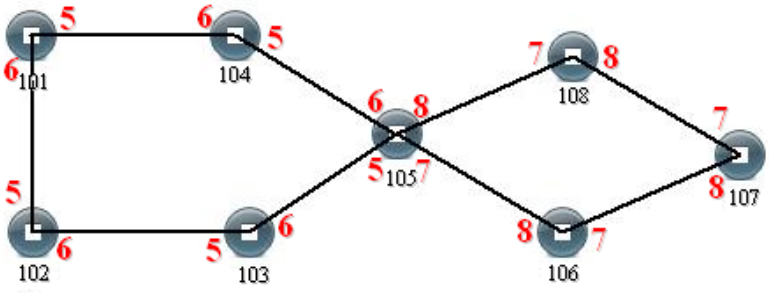
Single Ring Configuration

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:



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,

Copyright © 3onedata Co., Ltd.

107 and 108 switches as the ring ports and the ring group 2;

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

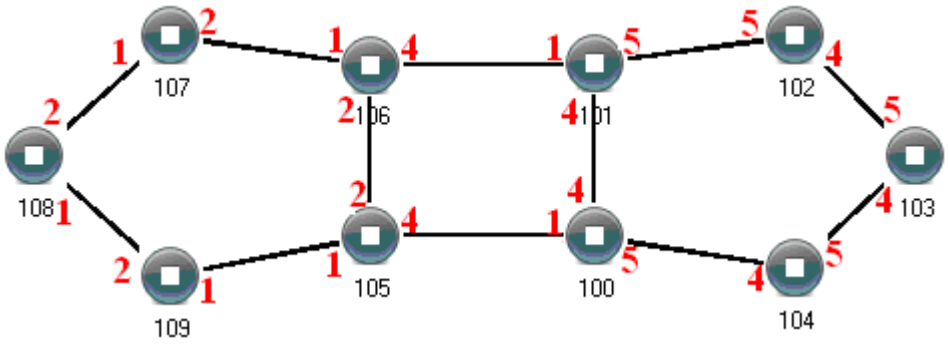
Step 4 Adopt network cable to connect the ring group 2;

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:



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,

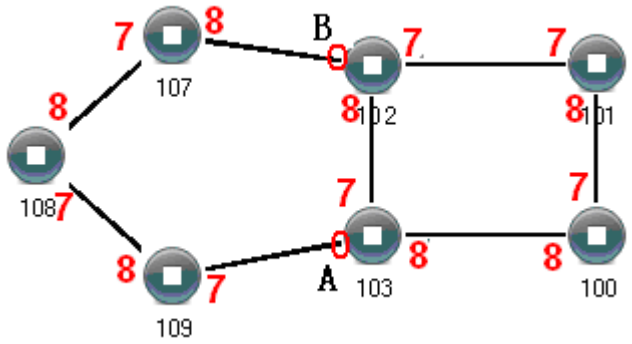
Copyright © 3onedata Co., Ltd.

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:



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.

Copyright © 3onedata Co., Ltd.

5.6 ERPS Configuration

Ethernet Ring Protection Switching (ERPS) is the Ethernet Ring Network Link Layer Technology with high reliability and stability. 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

Function Description

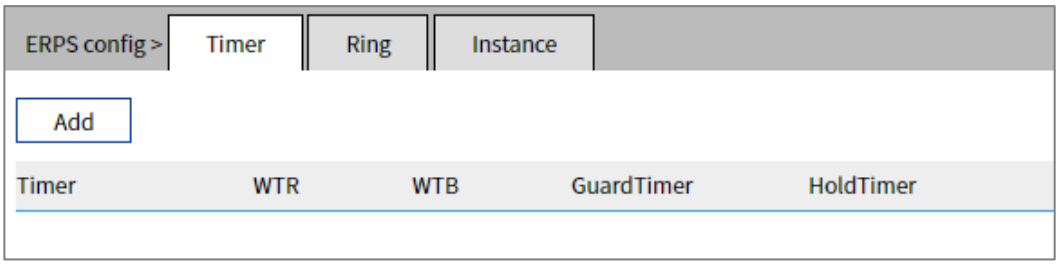
On the “Timer” page, users can configure the parameters of the ring network timer.

Operation Path

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

Interface Description

Timer configuration interface is as follows:



Main elements configuration description of timer interface:

Interface Element	Description
Timer	The default name of timer is timer, which is up to 32 bytes.
WTR	WTR(Wait To Restore)timer, its value range is 1-12 minutes. Under revertive mode, the timer starts when the owner node in protection state receives NR packet. The owner node blocks the RPL port and unblocks the fault port after the timer expires.
WTB	WTB (Wait To Block) timer, its value range is 1-12 minutes. Under revertive mode, when the owner node is in MS (Manual Switch) or FS (Forced Switch) status, WTB timer will start if

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	user carries out clean command on the owner node. After the timer expires, the owner node will block the RPL port and unblock temporary blocking port.
GuardTimer	Guard timer, its value range is 10-2000ms. The timer starts when the port detects the link restoration, before the timer expires, the port won't deal with R-APS (Ring Automatic Protection Switching) packet.
HoldTimer	Hold timer, its value range is 0-10s. The timer starts when the port detects the link restoration, delay the fault report speed. When the link fails, the timer should report the fault if it exists after Hold timer expires.

5.6.2 Loop

Function Description

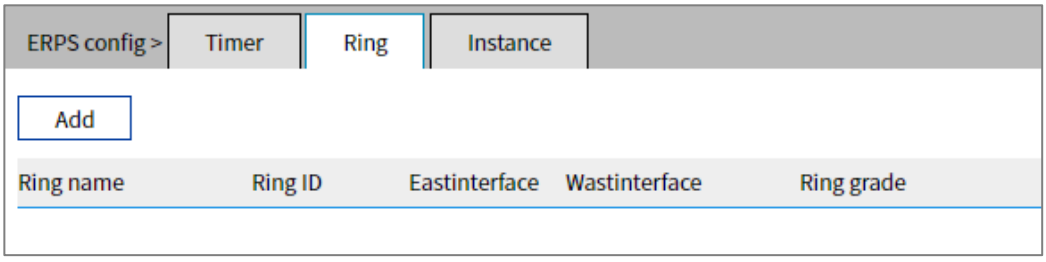
On the "Ring" page, user could configure the ID, interface and level of the ring network.

Operation Path

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

Interface Description

Ring interface as follows:



Configuration description of main elements of the Ring interface:

Interface Element	Description
Ring Name	The default name of ring network is ring, which is up to 32 bytes.
Ring ID	The ID of ring network, its value range is 1-255.
East Interface	Ring port1.

Copyright © 3onedata Co., Ltd.

Interface Element	Description
West Interface	Ring port2.
Ring grade	The higher the ring network level is, the greater the value is, its value range is 1-7.

5.6.3 Instance Configuration

Function Description

On the "Instance" page, user could configure instance.

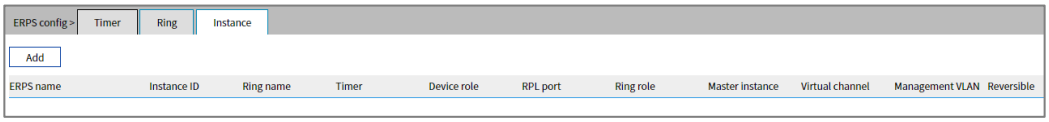
An Ethernet network topology connected in ring is called a ERPS Ring. ERPS ring could be divided into main ring and subring. Each device in ERPS ring is called a node. The main node is in charge of blocking and opening ports on this node, preventing loops from forming.

Operation Path

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

Interface Description

Instance interface as follows:



The main element configuration description of instance interface:

Interface Element	Description
ERPS name	The default name of ERPS is ERP, which is up to 32 bytes
Instance ID	The ID of instance, its value range is 0-63
Ring Name	The default name of ring network is the ring name that has been added in the ring network list.
Timer	The default name of timer is the name that has been added in the timer list.
Device Role	Each device in ERPS ring is called a node. The node role is decided by user configuration, they are divided into following types: • rpl-owner: owner node is responsible for blocking and unblocking the port in RPL of the node to prevent loop

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	forming and conduct link switching. • rpl-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 switching. • interconnection: interconnected node is the node to connect multiple rings in the multi-loop model, it belongs to the subring, and the primary ring has no interconnected node. In the link protocol packet upload mode between the two subring interconnected nodes, the subring protocol packet ends in the interconnected node, but the data packet won't end. • other: normal node is the other node in addition to the above three nodes. Normal node is responsible for receiving and forwarding the protocol packet and data packet in the link.
RPL-Port	RPL (Ring Protection Link) port is the appointed ring network port for Owner node to establish RPL. • East-ifindex • West-ifindex
Ring Role	Options of Ring Role drop-down box: • Major-ring: main ring network • Sub-ring: subring network
Master Instance	The major instance name could be set and need to be set as ERPS instance name only when the ring role is Sub-ring
Virtual Channel	After enable virtual channel, the subring protocol packet could transmit across the primary ring; otherwise, the subring protocol packet can only transmit in the ring. Options: • enable • disable
Management VLAN	The VLAN channel of protocol packet, its value range is 1-4094.
Reversible	Options: • Enable: In revertive mode, WTR timer starts when the owner node receives the link recovery packet after the clearing of fault. The timer will change from fault link protection status to idle status after expiring. • disable: Irreversible mode: Owner node doesn't conduct any action after receiving the link recovery packet and

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	keeps the port status set before.

5.7 Loop 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.

5.7.1 Global Configuration

Function Description

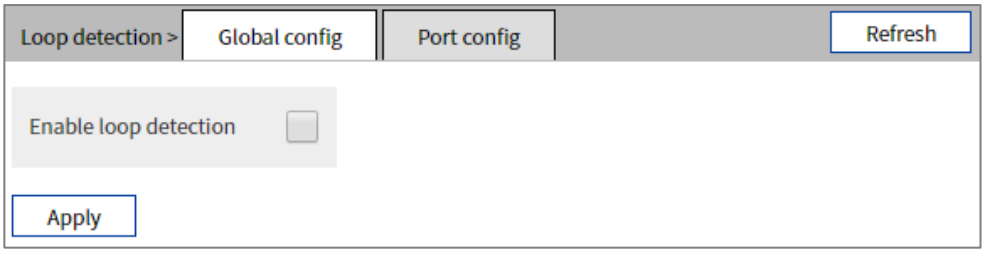
On the "Global config" page, user can enable loop-detect configuration.

Operation Path

Open in order: "Layer 2 Config > Loop-detect > Global Config".

Interface Description

Global configuration interface is as follows:



The main element configuration description of global configuration interface:

Interface Element	Description
Enable loop detection	Enable the loop detection check box, which can enable loop detection function after being checked.

Copyright © 3onedata Co., Ltd.

5.7.2 Port Configuration

Function Description

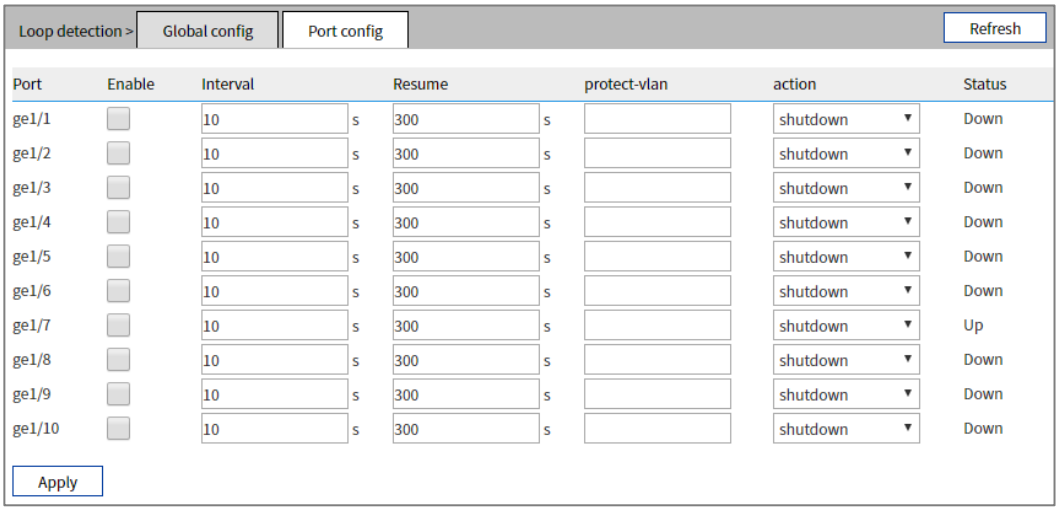
On the "Port config" page, user can implement relevant configuration of port loop detection.

Operation Path

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

Interface Description

Check port configuration interface as below:



The main element configuration description of port configuration interface:

Interface Element	Description
Port	The corresponding port number of this device's Ethernet port.
Enable	Check the box to enable the loop detection configuration of this port
Interval	The interval time of loop detection data packet sending, value range: 10-300, its unit is second.
Resume	The resume time after the action of detecting loop, value range: 300-600, its unit is second.
Protect VLAN	The VLAN ID of loop protection. It is None by default. The value range: 1-4094, the number of VLAN ID is ≤5 Note: This parameter must be configured, otherwise there would be errors in down sending the data.

Copyright © 3onedata Co., Ltd.

Interface Element	Description
Action	The selected action after detecting a loop, options are: • Log: log • Shutdown: the port is closed
Status	The status of this port, displayed items are: • Down: the port is physically disconnected • Up: the port is connected • Shutdown: the port is closed • No Shutdown: the port is not closed

Copyright © 3onedata Co., Ltd.

6 Network Security

6.1 Access Control

Function Description

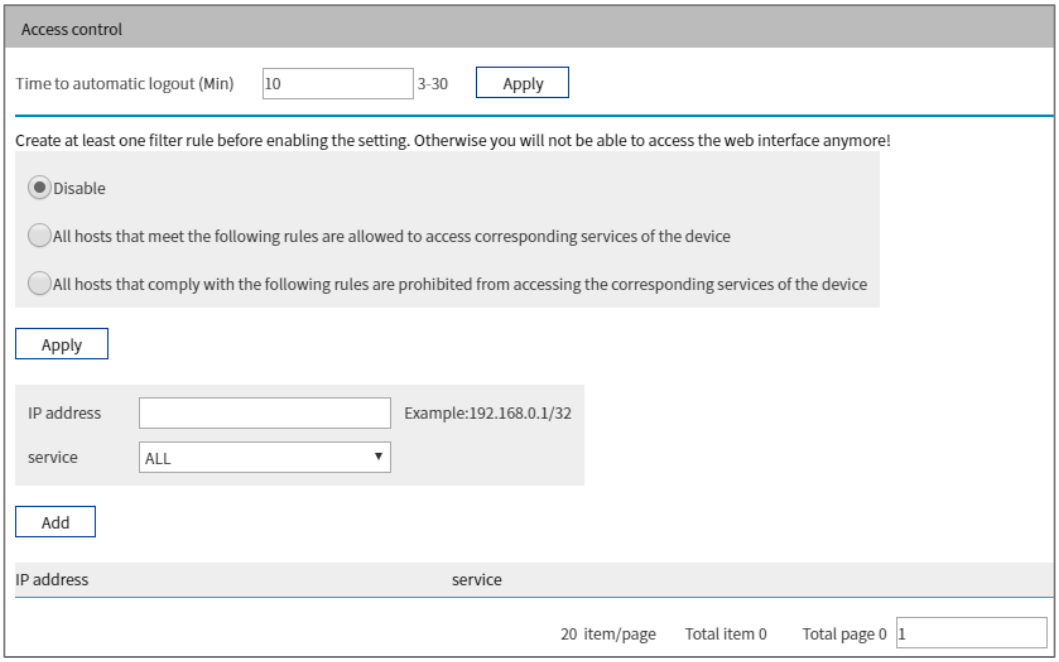
On the "Access Control" page, user can configure access rules and filtering rule.

Operation Path

Open in order: "Network Security > Access Control".

Interface Description

Access control interface as follows:



The main element configuration description of access control interface:

Interface Element	Description

Copyright © 3onedata Co., Ltd.

Interface Element	Description
Time to automatic logout (Min)	Set the time of automatic logout, unit: minutes, default value: 10, value range: 3-30.
Filtering rule	Set filtering rule, default to disable, that is disable access filtering function. Options as follows: • Disable; • All hosts that meet the following rules are allowed to access corresponding service of the device; • All hosts that comply with the following rules are prohibited from accessing corresponding service of the device.
IP Address	Enable/disable device to access the device IP address.
Service	Methods of enabling/disabling device to access the device. Options as follows: • ALL: support HTTP, TELNET, SSH and SNMP access management; • HTTP: Support WEB interface access; • TELNET: Support Telnet client command line access; • SSH: Support SSH client access; • SNMP: Support SNMP network management.

Notice

Please first add the client list, and then set the access rules, otherwise it may cause the current web can't be accessed.

6.2 802.1X Configuration

IEEE 802.1X protocol is a port-based network access control protocol, that is, the accessed user device is authenticated on the port of LAN access device, so that the user device can control the access to network resources.

In the authentication architecture of IEEE 802.1x, the logical functions of "controllable port" and "uncontrollable port" are adopted to realize the separation of service and authentication. After the user is authenticated, the service flow is separated from the

Copyright © 3onedata Co., Ltd.

authentication flow, and there is no special requirement for subsequent data packet processing. The service can be very flexible, especially in broadband multicast and other services, and all services are not restricted by authentication methods.

802.1x structure mainly consists of three parts:

- Supplicant: Users or customers who want to be authenticated;
- Authentication server:Typical example is RADIUS server;
- Authenticator:End-to-end devices, such as wireless access points, switches, etc.

6.2.1 Global Configuration

Function Description

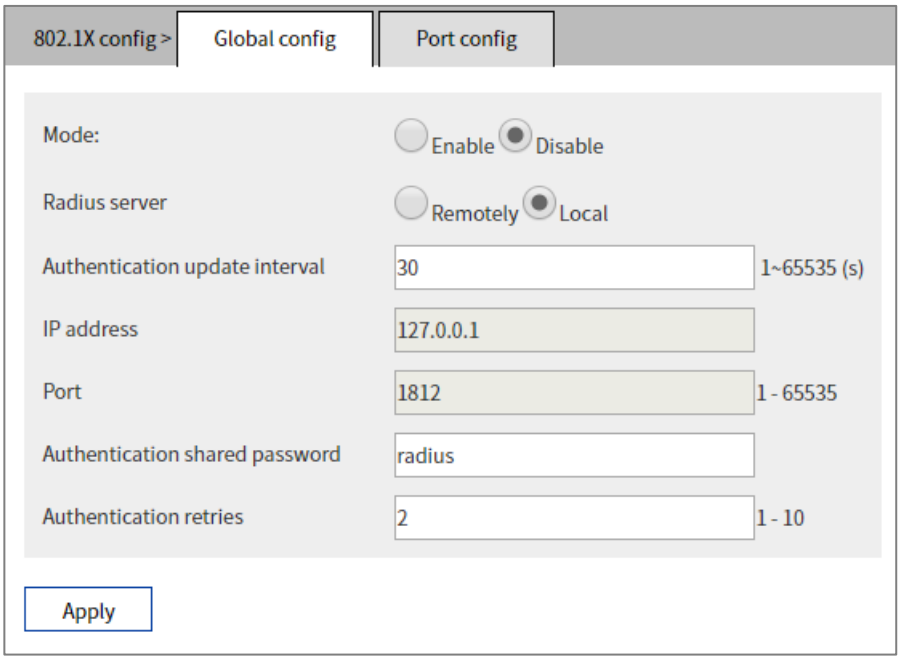
On the "Global Config" page, user can configure 802.1x authentication and Radius server parameters.

Operation Path

Open in order: " Network Security > 802.1X Configuration".

Interface Description

Global configuration interface is as follows:



The main element configuration description of global configuration interface:

Copyright © 3onedata Co., Ltd.

Interface Element	Description
Mode	IEEE802.1X authentication status settings: • Enable; • Disable.
Radius Server	Local internal Radius server and external Radius server configuration: • Local: built-in Radius server, if choosing internal Radius server, the applicant will only use the username and password of internal Radius database. • Remote: fill in the IP address and port number of the authentication server if using external Radius server.
Authentication upgrade interval	The range of authentication upgrade interval is 1~65535, unit: second. The reauthentication interval of 802.1x used for strengthening the security of authentication.
IP address	IP address of Radius server
Port	The port number of the remote Radius server. The default is 1812, value range is 1-65535.
Authentication Shared Password	The shared password character string used for device accessing authentication server.
Authentication Retries	The number of retries allowed for authentication ranges from 1 to 10.

6.2.2 Port Configuration

Function Description

On the "Port Config" page, user can enable 802.1X Port Authentication.

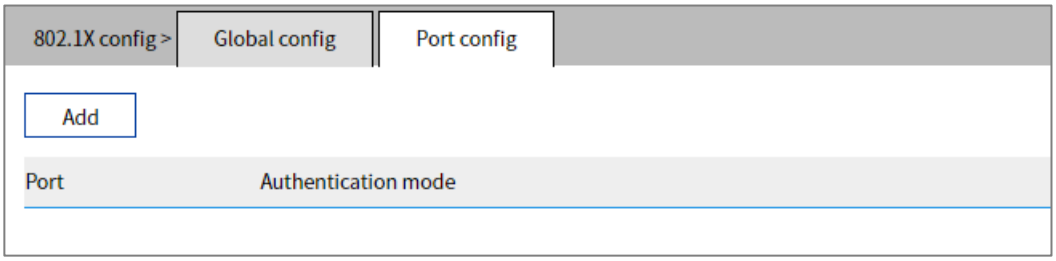
Operation Path

Open in order: " Network Security > 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	Device Ethernet port No.
Authentication mode	802.1x port authentication mode: • Auto: normal authentication; • Forced authentication passing: Force the interface to become the authenticated state directly; • Forced authentication non-passing: Force the interface to become the unauthenticated state directly.

7 Advanced Configuration

7.1 QOS Configuration

Quality of Service (QoS) is the service quality. As for network business, service quality includes transmission bandwidth, transfer delay, data packet loss rate and so on. In network, user can improve the service quality by ensuring the transmission bandwidth, reducing transfer delay, data packet loss rate, delay jitter and other measures.

Network resources are always limited, as long as there exists the case of snatching network resources, there will be service quality requirements. Quality of service is relative to the network business, while ensuring the service quality of a certain type of business; it may damage the service quality of other businesses. For example, in the case of total network bandwidth is fixed, if a type of business occupies more bandwidth, other businesses will be able to use less bandwidth, which may influence the usage of other businesses. Therefore, network managers need to make rational planning and distribution of network resources according to the characteristics of various businesses, so that network resources can be efficiently utilized.

QoS function provides 8 internal queues, each queue supports 8 different levels traffic, High-priority data packets stay on the device for a short period of time, and some latency-sensitive traffic supports lower latency. According to 802.1p priority level tag, IP TOS, the device can classify packets to a certain level.

Function Description

On the “QoS Configuration” page, you can configure QoS mode, priority mode, etc.

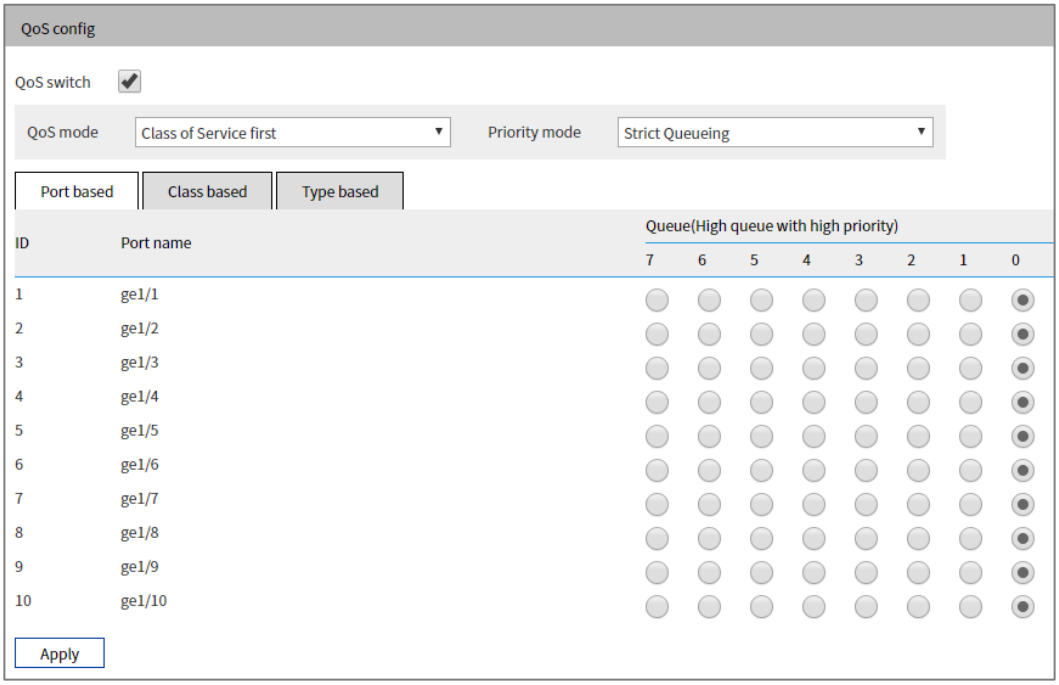
Operation Path

Open in order: "Advanced Configuration > QoS Configuration".

Copyright © 3onedata Co., Ltd.

Interface Description 1: Port-based

Check QoS-Port-based configuration interface as below:



The main element configuration description of QoS-Port-based configuration interface:

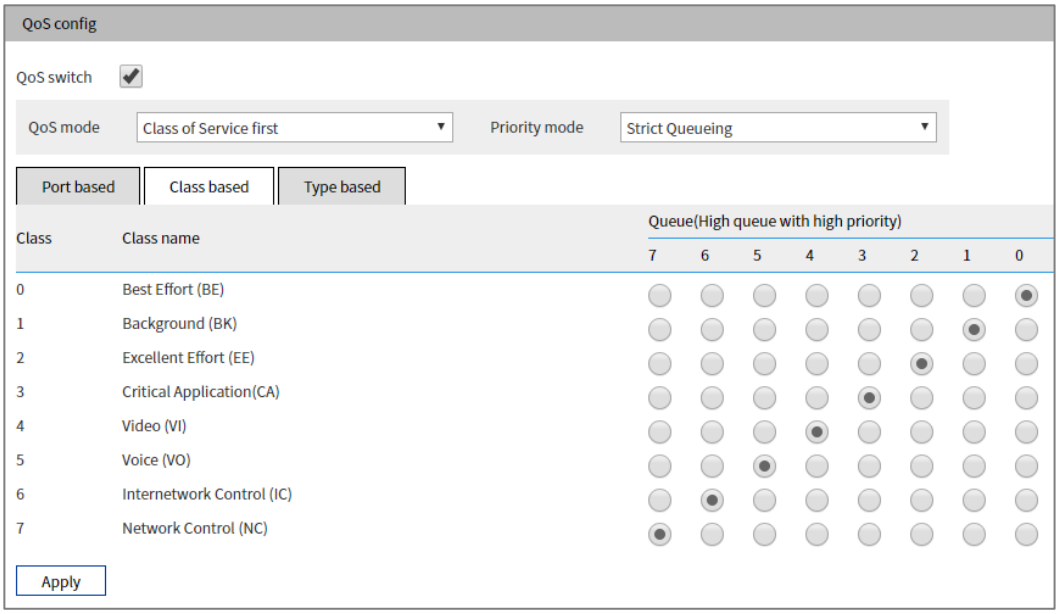
Interface Element	Description
QoS switch	Check to enable QoS function
QoS mode	The drop-down box of QoS mode: • Port-based only • Service level only • Service type only • CoS first • ToS first
Priority mode	The drop-down box of priority mode: • Strict Queueing: sends the higher-priority queues strictly according to the priority level from high to low. Queue 7 has the highest priority level and queue 0 has the lowest priority level. • 3-25-17-12-6-3-2-1 weighted fair queening. Each queue is configured with a weighted value of 33-25-17-12-6-3-2-1, and how many messages are dispatched by each queue can be configured, and the

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	queues are scheduled in turn, thus avoiding the disadvantage that messages in low priority queues may not be served for a long time when strict priority queues are adopted.
Port-Based	**Port-Based Configuration bar** Note: This function can only be configured when port-based only, CoS first or ToS first is selected in QoS mode.
ID	Port-based ID number.
Port name	The corresponding port name of the device Ethernet port.
Queue (High queue with high priority)	Mapping relationship between ports and queues. Note: By default, device would use port priority in place of the 802.1p priority the port comes with when receiving message to control the quality of service the messages deserve. The range of priority is 0-7. By default, the port priority is 0. The higher the value, the higher the priority.

Interface Description: Class based

QoS Config-class-based interface is as follows:



The main element configuration description of QoS Config-class-based interface:

Interface Element	Description
QoS switch	Check to enable Qos function
QoS mode	The drop-down box of QoS mode: • Port-based only

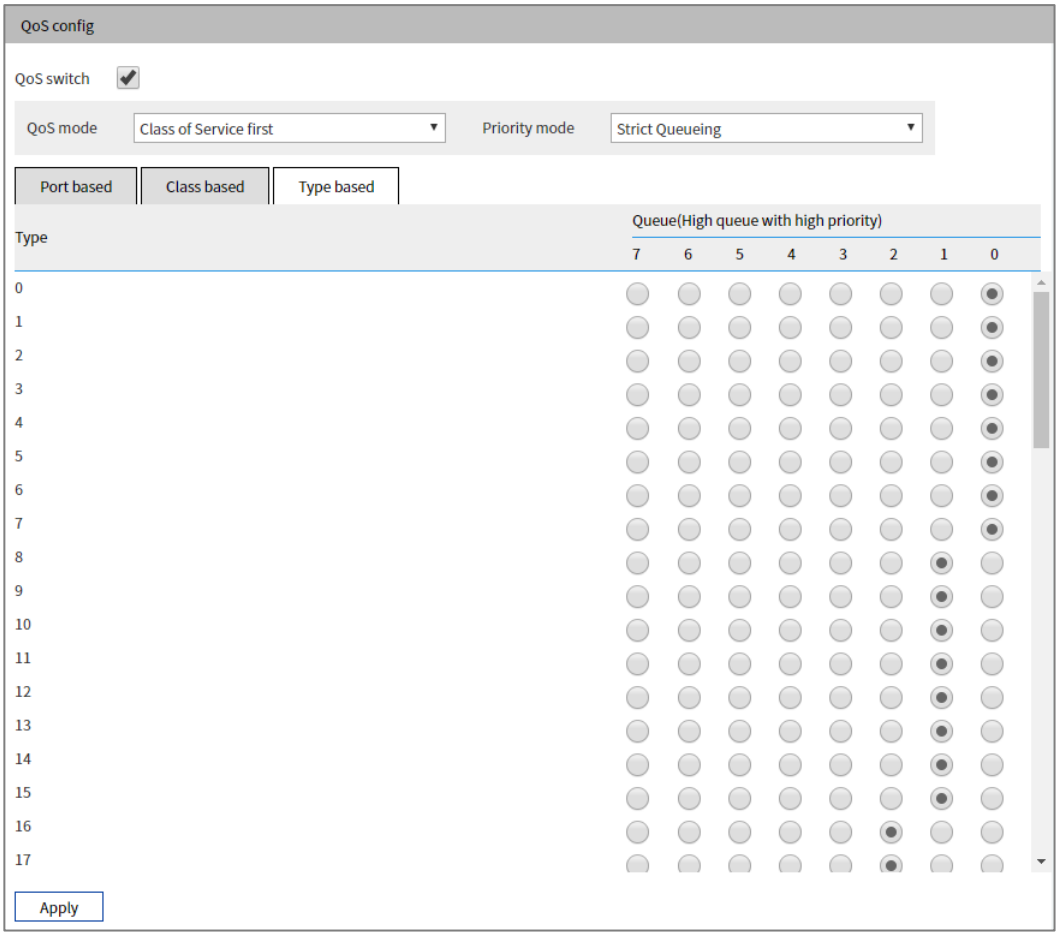
Copyright © 3onedata Co., Ltd.

Interface Element	Description
	• Service level only • Service type only • CoS first • ToS first
Priority mode	The drop-down box of priority mode: • Strict Queueing: sends the higher-priority queues strictly according to the priority level from high to low. Queue 7 has the highest priority level and queue 0 has the lowest priority level. • 3-25-17-12-6-3-2-1 weighted fair queening. Each queue is configured with a weighted value of 33-25-17-12-6-3-2-1, and how many messages are dispatched by each queue can be configured, and the queues are scheduled in turn, thus avoiding the disadvantage that messages in low priority queues may not be served for a long time when strict priority queues are adopted.
Class-based	**Class-based configuration bar** Note: This function can only be configured when CoS only, CoS first or ToS first is selected in QoS mode.
Class	802.1Q CoS business service level.
Class name	Class name corresponding to service class: • Best Effort (BE) • Background (BK) • Excellent Effort (EE) • Critical Application(CA) • Video (VI) • Voice (VO) • Internetwork Control (IC) • Network Control (NC)
Queue (High queue with high priority)	Mapping relationship between service class and queues.

Copyright © 3onedata Co., Ltd.

Interface Description: Type based

QoS Config-class-based configuration interface is as follows:



The main element configuration description of QoS Config-class-based interface:

Interface Element	Description
QoS switch	Check to enable QoS function
QoS mode	The drop-down box of QoS mode: • Port-based only • Service level only • Service type only • CoS first • ToS first
Priority mode	The drop-down box of priority mode: • Strict Queueing: sends the higher-priority queues strictly according to the priority level from high to low. Queue 7 has the highest priority level and queue 0 has the lowest priority level.

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	• 3-25-17-12-6-3-2-1 weighted fair queening. Each queue is configured with a weighted value of 33-25-17-12-6-3-2-1, and how many messages are dispatched by each queue can be configured, and the queues are scheduled in turn, thus avoiding the disadvantage that messages in low priority queues may not be served for a long time when strict priority queues are adopted.
Type-based	**Class-based Configuration** Note: This function can only be configured when ToS only, CoS first or ToS first is selected in QoS mode.
Type	IP DSCP value is 0-63, 63 is the highest priority level, 0 is the lowest priority level.
Queue (High queue with high priority)	Mapping relationship between DSCP and queues.

7.2 LLDP Configuration

LLDP is a layer 2 topology discovery protocol, its basic principle is: Devices in network send the status information message to adjacent device, and each port in the device stores its own information, if there is change in the status of local device, it can also send updated information to the adjacent device directly connected to it. Adjacent devices will store the information in standard SNMP MIB bank. The network management system could inquiry the connection status of current layer 2 from SNMP MIB bank. It should be noted that LLDP is only a remote device status information discovery protocol, which cannot complete the network device configuration, port control and other functions.

7.2.1 Global Configuration

Function Description

On the "Global Config" page, user can configure the relevant parameters of LLDP.

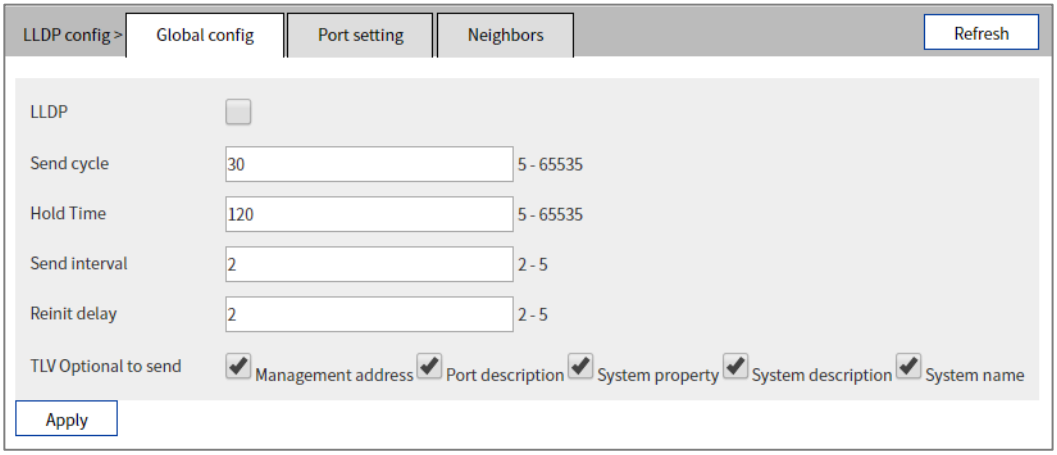
Copyright © 3onedata Co., Ltd.

Operation Path

Open in order: "Advanced Configuration > LLDP Configuration > Global Configuration".

Interface Description

The global configuration interface is as follows:



Main elements configuration description of the global configuration interface:

Interface Element	Description
LLDP	The check box of LLDP function status, check to enable LLDP function.
Send Cycle	LLDP send cycle, range 5-65535. Note: When no device status changes, the device periodically sends LLDP packets to its adjacent nodes. The interval is called the period for sending LLDP packets.
Hold Time	LLDP hold time, range 5-65535. Note: Hold time can control the aging time of this device information on neighboring device.
Send Interval	The LLDP send interval, range 2-5, that is, the delay time of LLDP continuous message transmission.
Reinit delay	Reinit delay time, range 2-5. Note: When the working mode of LLDP on the port changes, the port will initialize the protocol state machine. By configuring the reinit delay time, the interface can be prevented from being initialized constantly due to the frequent change of working mode.
TLV Optional to Send	TLV sends information, with the following options: • Management address;

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	• Port description; • System property; • System description; • System name. Note: TLV is the unit of LLDPDU, each TLV represents a message, and LLDPDU is the data unit encapsulated in the data part of LLDP message.

7.2.2 Port Setting

Function Description

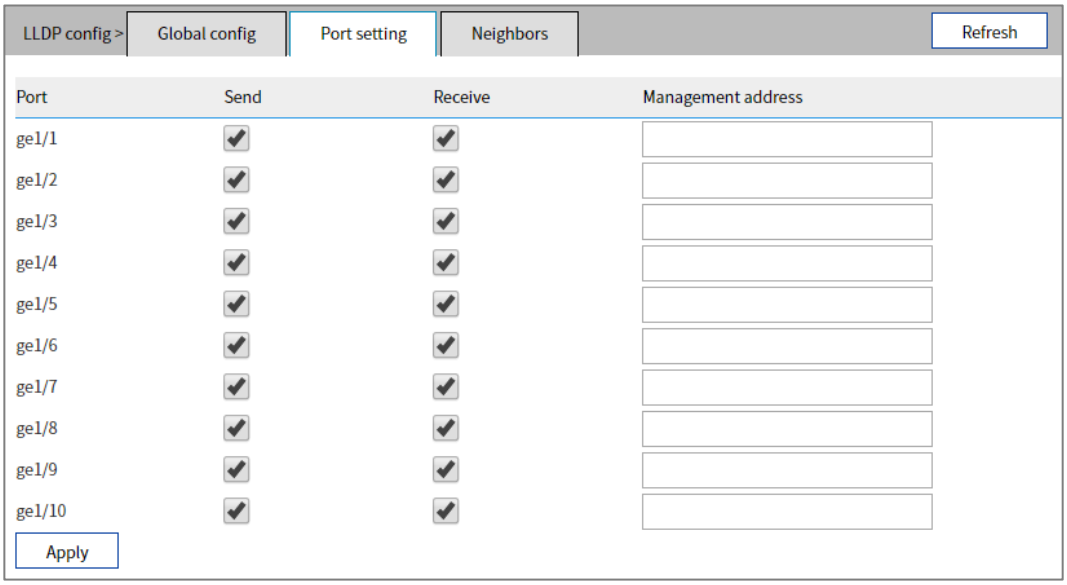
On the "Port Setting" page, user can configure the sending and receiving mode and management address of the port.

Operation Path

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

Interface Description

Check port setting interface as below:



The main element configuration description of port configuration interface:

Copyright © 3onedata Co., Ltd.

Interface Element	Description
Port	The corresponding port name of the device Ethernet port.
Send	This device only transmits LLDP message and not receive it from neighbors.
Receive	This device will not transmits LLDP message, but receive it from neighbor devices to analyse it.
Management Address	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.

7.2.3 Neighbors

Function Description

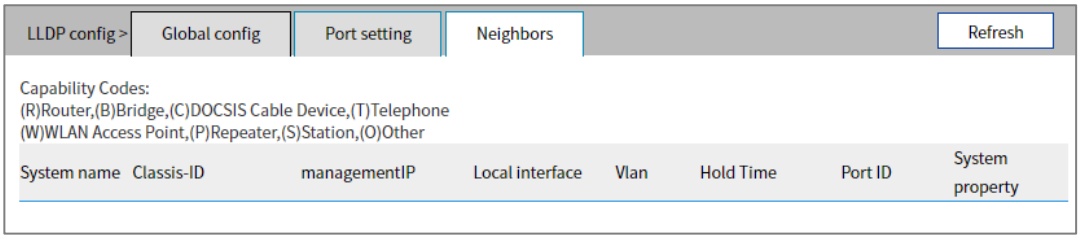
On the "Neighbors" page, user can look over the relative information of neighbors.

Operation Path

Open in order: "Advanced Configuration > LLDP Configuration > Neighbors ".

Interface Description

Neighbors interface as follows:



Main elements configuration description of neighbors interface:

Interface Element	Description
System Name	System name of the neighbor device.
Chassis-ID	Bridge MAC address of neighbor device or port.
management IP	Management IP address of neighbor device or port.

Copyright © 3onedata Co., Ltd.

Interface Element	Description
Local Interface	Local port number of local switch connected to adjacent devices.
Vlan	The local switch port VLAN PVID number.
Hold Time	Neighbor LLDP retransmission time.
Port ID	Neighbor port ID number.
System Property	System property, the shorthand codes are as follows: • R: Router; • B: Bridge; • C: DOCSIS Cable Device; • T: Telephone; • W: WLAN Access Point; • P: Repeater; • S: Station; • O: Other.

7.3 SNMP Configuration

SNMP Introduction

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.

SNMP Working Mechanism

SNMP is divided into NMS and Agent:

- Network Management Station (NMS) is the work station that runs client procedure, at present, common network management platforms include Quid View, Sun Net Manager and IBM Net View. Agent is the server software that runs in network device.

Copyright © 3onedata Co., Ltd.

- NMS can send Get Request, Get Next Request and Set Request messages to Agent, after receiving these request messages from NMS, Agent will conduct Read or Write operation, generate Response message and return messages to NMS according to the message type. When the device appears abnormal situation or the state changes (such as device resets), Agent will forwardly send Trap message to NMS and report occurred event to NMS.

SNMP supports three basic operations:

- Get operation: manager adopts the operation to inquire a variable value of Agent;
- Set operation: manager adopts the operation to set a variable value of Agent;
- Trap operation: Agent adopts the operation to send abnormal alarm information to manager.

SNMP Protocol Version

At present, SNMP Agent in the device supports SNMP V1 version, SNMP V2C and SNMP V3 version. SNMP V1, SNMP V2C adopt community name authentication, SNMP message of community name without device authentication will be discarded. SNMP community name is used for defining the relationship of SNMP, NMS and SNMP Agent. Community name plays a role similar to password, and can limit SNMP NMS to access SNMP Agent in device. User can choose and appoint one or more characters relative to community name:

- Define MIB view that community name can access.
- Configure MIB object access privilege of community name as read-write privilege or read-only privilege. Community name with read-only privilege can only inquire the device information; community name with read-write privilege can configure the device.
- Set the basic access control list appointed by community name.

7.3.1 Global Configuration

Function Description

On the "Global Configuration" page, user can 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.

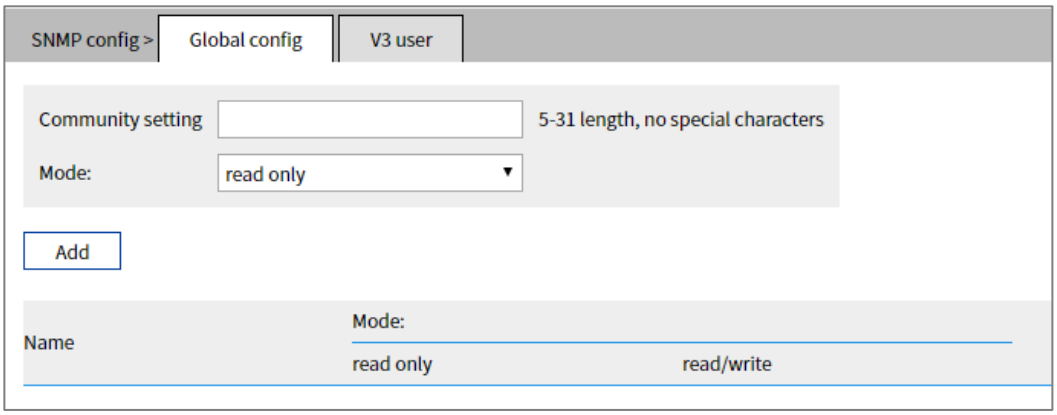
Operation Path

Open in order: "Advanced Configuration > SNMP Configuration > Global Configuration".

Copyright © 3onedata Co., Ltd.

Interface Description

Global configuration interface is as follows:



The main element configuration description of global configuration interface:

Interface Element	Description
Community settings	SNMP community name definition, support 31 characters input.
Mode	Community mode setting, the options are as follows: • Read-only: Read-only mode community. • Read-write: Read-write mode community.
Name	Display community name.
Mode-read only	Display community read-only mode.
Mode-read/write	Display the community read-write mode.

7.3.2 V3 User

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.

Function Description

On the "V3 User" page, user can configure SNMP V3 user information.

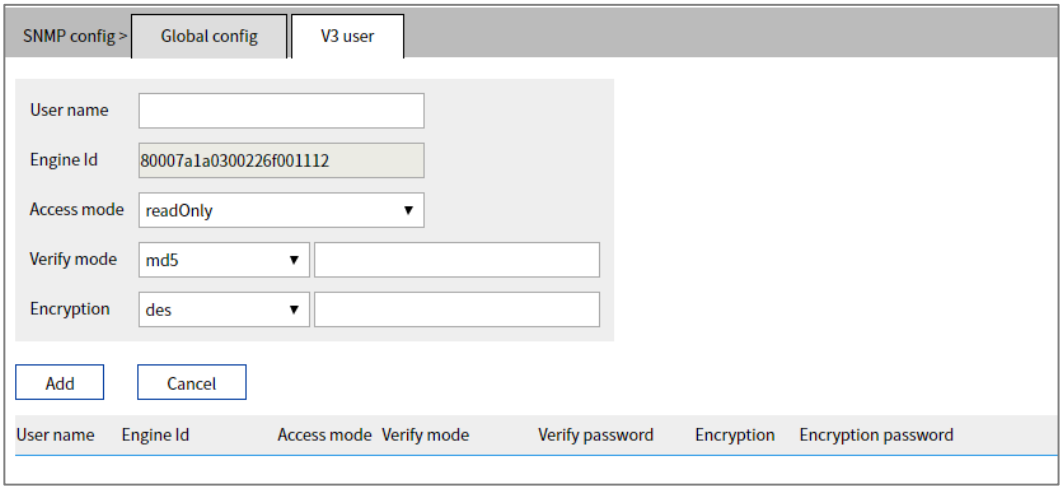
Copyright © 3onedata Co., Ltd.

Operation Path

Open in order: "Advanced Config > SNMP Config > V3 User".

Interface Description

V3 user interface as follows:



The main element configuration description of V3 user interface:

Interface Element	Description
User name	SNMP v3 version user name definition, combination of letters and numbers, and support 48 characters input.
Engine ID	SNMP protocol engine identification. There is a one-to-one correspondence between the engine identification and SNMP entity. It is in charge of SNMP protocol operation, providing service for each type of SNMP applications. Note: The main function of SNMP engine includes: send and receive message, authenticate and encrypt message, control access toward managed object.
Zugriff Mode	Access mode, options as follows: • ReadOnly: Read-only mode. • ReadWrite: ReadWrite mode.
Authentifizieren Mode	Authentication method and authentication password information, two authentication methods are optional: • Md5: Information abstract algorithm 5; • Sha: Secure hash algorithm.
Verschlüsselung Mode	V3 user data encryption algorithm and encryption password information, encryption algorithm options are

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	as follows: • Des: Adopt data encryption algorithm; • Aes: Adopt advanced encryption standard; • None: No encryption.

7.4 DHCP Server Configuration

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.

7.4.1 DHCP Server

Function Description

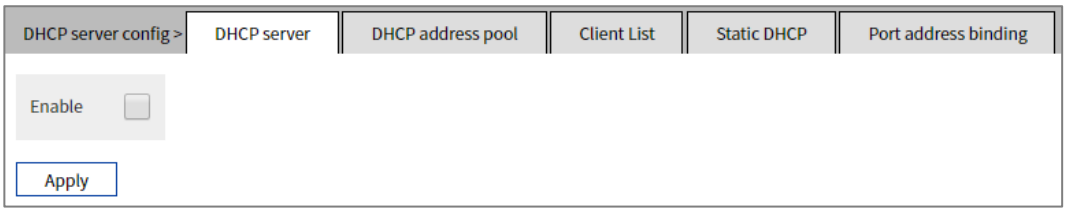
On the "DHCP Server" page, user can enable/disable DHCP Server.

Operation Path

Open in order: "Advanced Configuration > DHCP Server Configuration > DHCP Server".

Interface Description

The DHCP server interface as follows:



DHCP server interface main elements configuration instructions:

Interface Element	Description
Enable	After enabling DHCP Server function, the device will distribute address as a DHCP server by setting static allocation address table, the device can distribute IP address to devices connected to it.

Copyright © 3onedata Co., Ltd.

7.4.2 DHCP Address Pool

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.

DHCP server chooses and distributes IP address and other relative parameters for client from address pool.

DHCP server adopts tree structure: Tree root is the address pool of natural network segment. Branch is the subnet address pool of the network segment. Leaf node is the manually binding client address. The order of address pool at the same level is decided by the configuration order. This kind of tree structure has realized the inheritance of configuration, that is, subnet configuration inherits the configuration of natural network segment, and client configuration inherits the subnet configuration. Therefore, as for some common parameters (such as DNS server address), user only needs to configure in the natural network segment or subnet. Specific inheritance situation as follows:

1. When the parent-child relationship is established, sub address pool will inherit the existing configuration of parent address pool.
2. After the parent-child relationship is established, parent address pool is configured, sub-address pool will inherit or not, two situations as follows:
   - If the child address pool doesn't include the configuration, it will inherit the configuration of parent address pool;
   - If the child address pool has included the configuration, it won't inherit the configuration of parent address pool.

Function Description

On the "DHCP Pool Address" page, user can add, delete the address pool and look over the configuration information of address pool.

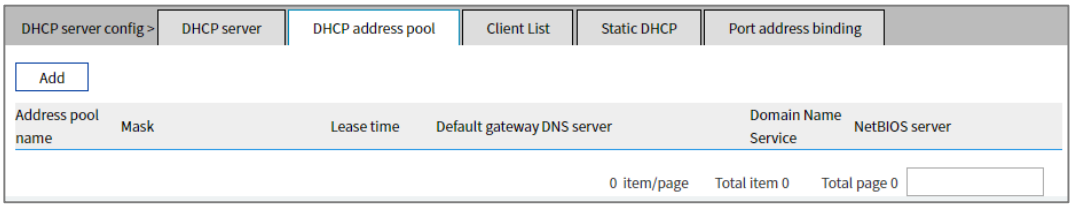
Operation Path

Open in order: "Advanced Configuration > DHCP Server Configuration > DHCP Address Pool".

Copyright © 3onedata Co., Ltd.

Interface Description

DHCP address pool interface as follow:



The main elements configuration description of DHCP address pool interface:

Interface Element	Description
Address pool name	Address pool name, length range is 1-48.
Mask	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, range is 0-999 days.
Default gateway DNS server	Default gateway address of client.
DNS server	DNS server IP address of client.
Domain name server	DNS server domain address of client.
NetBIOS Server	NetBIOS server IP address of client.

7.4.3 Client List

Function Description

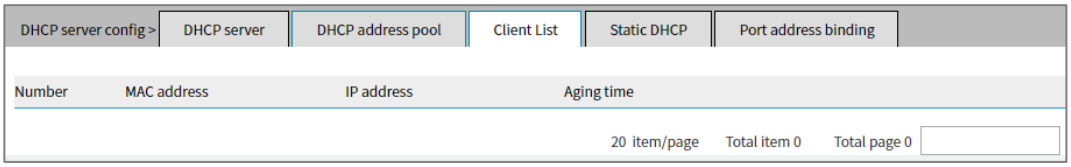
On the "Client List" page, user can look over the information of DHCP client.

Operation Path

Open in order: "Advanced Configuration > DHCP Server Configuration > 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
Number	Serial number name of DHCP client.
MAC Address	MAC address of DHCP client device.
IP Address	IP address of DHCP client-side device.
Aging Time	Ageing time of the client address.

7.4.4 Static DHCP

Function Description

On the page of "Static DHCP", user can add, delete, and view the configuration information of static clients.

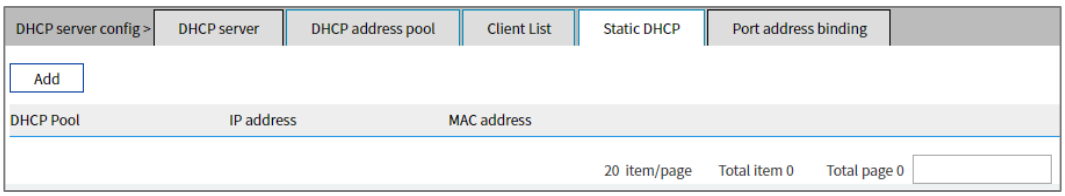
The client MAC address is bound to the address assigned by DHCP server; therefore, each address obtained by the client from server is a binding IP address.

Operation Path

Open in order: "Advanced Configuration > DHCP Server Configuration > Static DHCP".

Interface Description

Static DHCP interface as follows:



The main elements configuration description of static DHCP interface:

Interface Element	Description
DHCP pool	Corresponding list name of DHCP address pool.
IP Address	IP address that DHCP address pool distributes, client needs to gain the static IP address.
MAC Address	MAC address of DHCP client.

Copyright © 3onedata Co., Ltd.

7.4.5 Port Address Binding

Function Description

On the “Port Address Binding” page, users can bind the relationship of IP addresses assigned by ports.

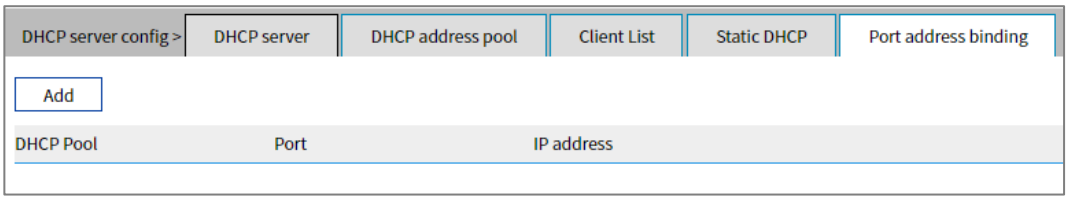
Device A enables DHCP Server function and sets 2 static distribution address tables: 192.168.1.19 corresponding port is 1; 192.168.1.20 corresponding port is 2. After device B enables IP address automated acquisition function, if device A is connected to device B via port 1, device B can automatically obtain IP address 192.168.1.19; If device A is connected to device B via port 2, device B can automatically gain IP address 192.168.1.20.

Operation Path

Open in order: "Advanced Configuration > DHCP Server Configuration > Port Address Binding".

Interface Description

Port address binding interface as follows:



The main element configuration description of port binding interface:

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

7.5 DHCP-Snooping Configuration

DHCP Snooping is layer 2 snooping function of DHCP service, after enable DHCP Snooping function, the device can extract and record IP address and MAC address information from received DHCP-ACK and DHCP-REQUEST messages.

Copyright © 3onedata Co., Ltd.

7.5.1 Global Configuration

Function Description

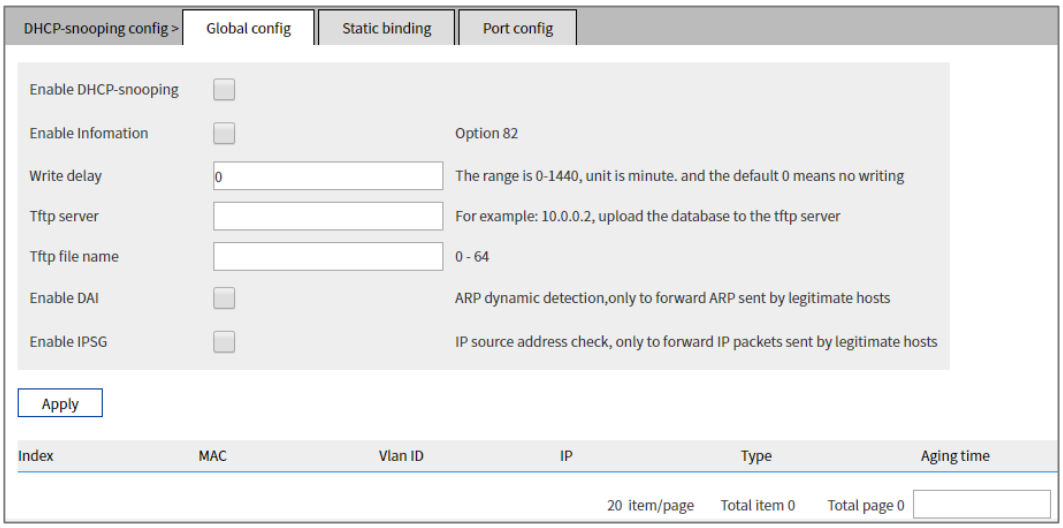
On the "Global Config" page, user can configure DHCP-Snooping parameters information.

Operation Path

Open in order: "Advanced Configuration > DHCP-Snooping Configuration > Global Configuration".

Interface Description

Global configuration interface is as follows:



The main element configuration description of global configuration interface:

Interface Element	Description
Enable DHCP-snooping	Enable DHCP-Snooping function checkbox.
Enable Information	Enable information function checkbox, after checking; enable Option 82 relay agent function which records the location information of DHCP client.
Write Delay	Writing delay range is 1-1440; unit is minute, default to 0, which represents not writing.
Tftp Server	Upload database to IP address of TFTP server, for example 10.0.0.2.
Tftp File name	Folder name of database uploading to TFTP server.
Enable DAI	ARP dynamic detection, after checking, forward ARP sent by

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	legitimate host according to DHCP Snooping table items.
Enable IPSG	IP source address check, after checking, forward IP message sent by legitimate host via dynamically gaining DHCP Snooping table items.

7.5.2 Static Binding

Function Description

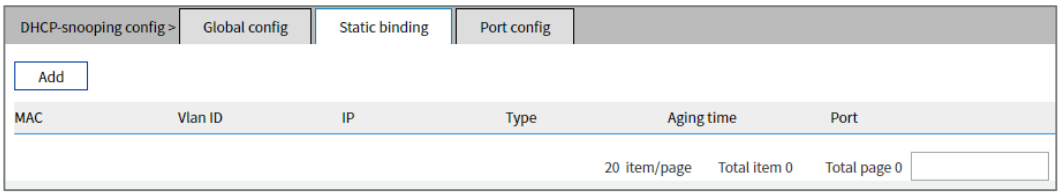
On the "Static Binding" page, user can bind static MAC and port.

Operation Path

Open in order: "Advanced Config > DHCP-snooping > Static Binding".

Interface Description

Static binding interface as follows:



The main element configuration description of static binding interface:

Interface Element	Description
MAC	Binding MAC address, for example: 0001-0001-0001.
Vlan ID	Binding VLAN ID information, for example: 1-4096.
IP	Binding IP address, for example: 192.168.1.1.
Type	IP address type.
Aging time	IP address aging-time.
Port	The corresponding port name of the device Ethernet port.

Copyright © 3onedata Co., Ltd.

7.5.3 Port Configuration

Function Description

On the "Port Config" page, user can configure DHCP Snooping port information. The trust function of DHCP Snooping can control the source of the DHCP server reply message to prevent any forged or illegal DHCP server from distributing IP address and other configuration information to other hosts.

The DHCP Snooping trust function divides ports into trust ports and non-trust ports:

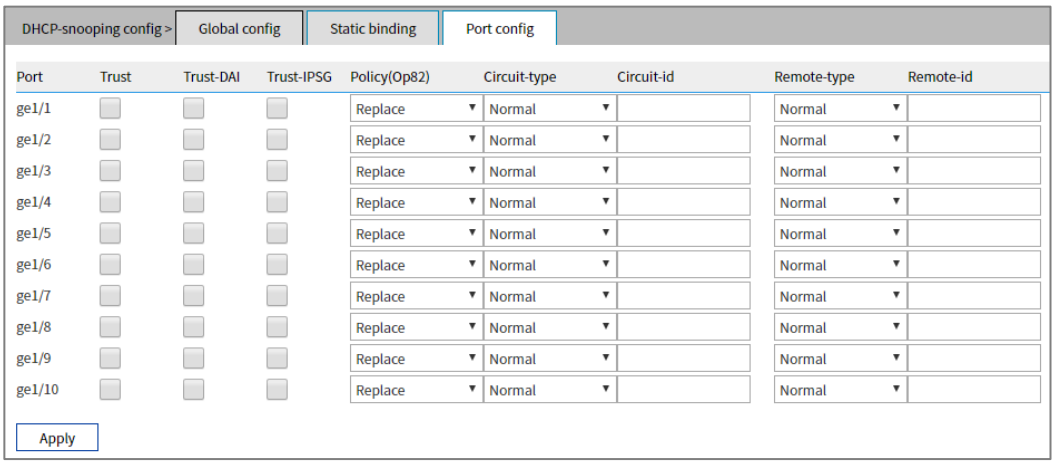
- Trust port is the port that is directly or indirectly connected to legitimate DHCP server. Trust port normally forwards received DHCP messages to ensure that DHCP client can gain correct IP address.
- Distrustful port is the port that isn't connected to legitimate DHCP server. The DHCP-ACK, DHCP-NAK, and DHCP-OFFER packets that receive DHCP server responses from untrusted ports will be discarded, preventing the DHCP client from obtaining the wrong IP address.

Operation Path

Open in order: "Advanced Configuration > DHCP-Snooping Configuration > 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.
Trust	Trust checkbox, trust port.

Copyright © 3onedata Co., Ltd.

Interface Element	Description
Trust-DAI	Trust-DAI checkbox, trust port ARP dynamic snooping.
Trust-IPSG	Trust-IPSG checkbox, source address examination of trust port IP .
Policy（Op82）	Option 82 dealing strategy, options as follows: • Replace: Keep Option 82 in messages unchanged and forward. • Keep: Adopt different modes to fill Option 82, replace prime Option 82 in message and forward, filling modes will be described as below. • Drop: Discard messages.
Circuit-type	Circuit ID sub-option filling type, options as follows: • Normal: Normal mode; • String: Detailed mode.
Circuit-id	Circuit ID sub-option filling content, support ASCII and HEX mode.
Remote-type	Remote ID sub-option filling type, options as follows: • Normal: Normal mode; • Sysname: Directly adopt device system name to fill Option 82; • String: Detailed mode.
Remote-id	Remote ID sub-option filling content, support ASCII and HEX mode.

7.6 DNS Settings

DNS, full Name Domain Name System. DNS helps users find paths in the Internet. Every computer on the Internet has a unique address called an "IP address" (Internet protocol address). Because IP addresses (a string of Numbers) are hard to remember, DNS allows users to replace them with a common string of letters (" Domain Names ").

DNS refers to the Domain Name Server. On the Internet, there is a one-to-one correspondence between domain names and IP addresses. Although domain names are easy for people to remember, machines can only know each other's IP addresses. The conversion between them is called domain name resolution which needs to be

Copyright © 3onedata Co., Ltd.

done by a dedicated domain name resolution server, DNS is the server for domain name resolution.

Function Description

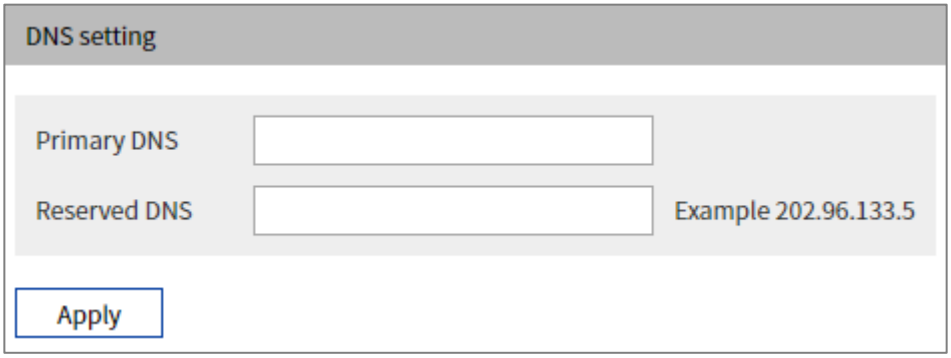
On the DNS Settings page, you can configure main DNS and backup DNS.

Operation Path

Open in order: "Advanced Configuration > DNS Configuration".

Interface Description

DNS setting interface as follows:



DNS settings interface main element configuration instructions

Interface Element	Description
Primary DNS	DNS Sever IP address, for example: 202.96.133.5.
Reserved DNS	DNS Sever backup IP address, for example: 202.96.133.5.

7.7 NTP Configuration

The full name of NTP protocol is 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 can be confirmed by the encrypted way to prevent malicious protocol attacks.

Function Description

On the "NTP Config" page, user can configure the device time and NTP server information.

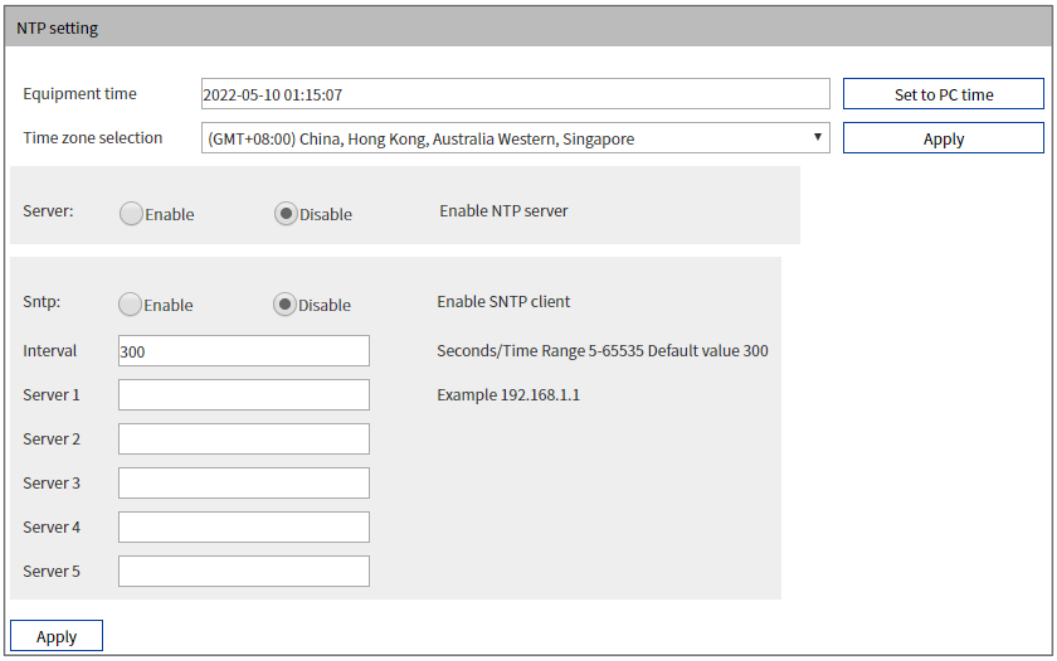
Copyright © 3onedata Co., Ltd.

Operation Path

Open in order: "Advanced Configuration > NTP Configuration".

Interface Description

NTP configuration interface as follows:



The main element configuration description of NTP configuration interface:

Interface Element	Description
Equipment time	The device own time, which can be synchronized to current computer time.
Timezone selection	Time standard of different global regions.
Server	The enable status of device as NTP server, the options are as follows: • Enable; • Disable.
Sntp	The enable status of device as NTP server, the options are as follows: • Enable; • Disable.
Interval	Time hack interval, values range from 5 to 65535, the default value is 300 seconds/time.
Server1	IP address of NTP-sync server 1, for example: 192.168.1.1.

Copyright © 3onedata Co., Ltd.

Interface Element	Description
Server2	IP address of NTP-sync server 2, for example: 192.168.1.1.
Server3	IP address of NTP-sync server 3, for example: 192.168.1.1.
Server4	IP address of NTP-sync server 4, for example: 192.168.1.1.
Server5	IP address of NTP-sync server 5, for example: 192.168.1.1.

7.8 PTP Configuration

PTP(Precision Time Protocol) is a time synchronization protocol, which can be used for high-precision time synchronization and frequency synchronization between devices. The time synchronization accuracy of PTP is sub-microsecond. IEEE 1588 standard of precision clock synchronization protocol for network measurement and control system is the basic protocol of PTP. It specifies the principle of high-precision clock synchronization in the network and the specification of message interaction processing. It was first applied to industrial automation, and now it is mainly used to bridge local area networks. Therefore, PTP is also called IEEE 1588, which is abbreviated as 1588. 1588 is divided into two versions: 1588v1 and 158v2. The 1588v1 can only achieve sub-millisecond time synchronization accuracy, while the 1588v2 can achieve sub-microsecond synchronization accuracy. It can realize phase synchronization and frequency synchronization at the same time. Based on IEEE 1588, PTP has derived IEEE 802.1AS, ITU-T G.8275.1, ITU-T G.8275.2, SMPTE ST2059-2, AES67-2015 and other protocols. Different PTP protocols have different functions in different usage scenarios, but their principles are basically the same.

The basic principle of PTP synchronization is as follows:

After confirming the master-slave relationship between clocks, the master and slave clocks exchange PTP protocol messages and record the sending and receiving time of messages, and calculate the total round-trip delay between master and slave clocks by calculating the round-trip time difference of PTP protocol messages. If the transmission delay in both directions is the same, half of the total round-trip delay is one-way delay. The slave clock calculates the time offset according to this one-way delay, the sending time of Sync message on the master clock and the time difference of receiving Sync message from the slave clock, and the slave clock adjusts the local time according to this time offset, so that the slave clock can synchronize with the master clock.

Copyright © 3onedata Co., Ltd.

Function Description

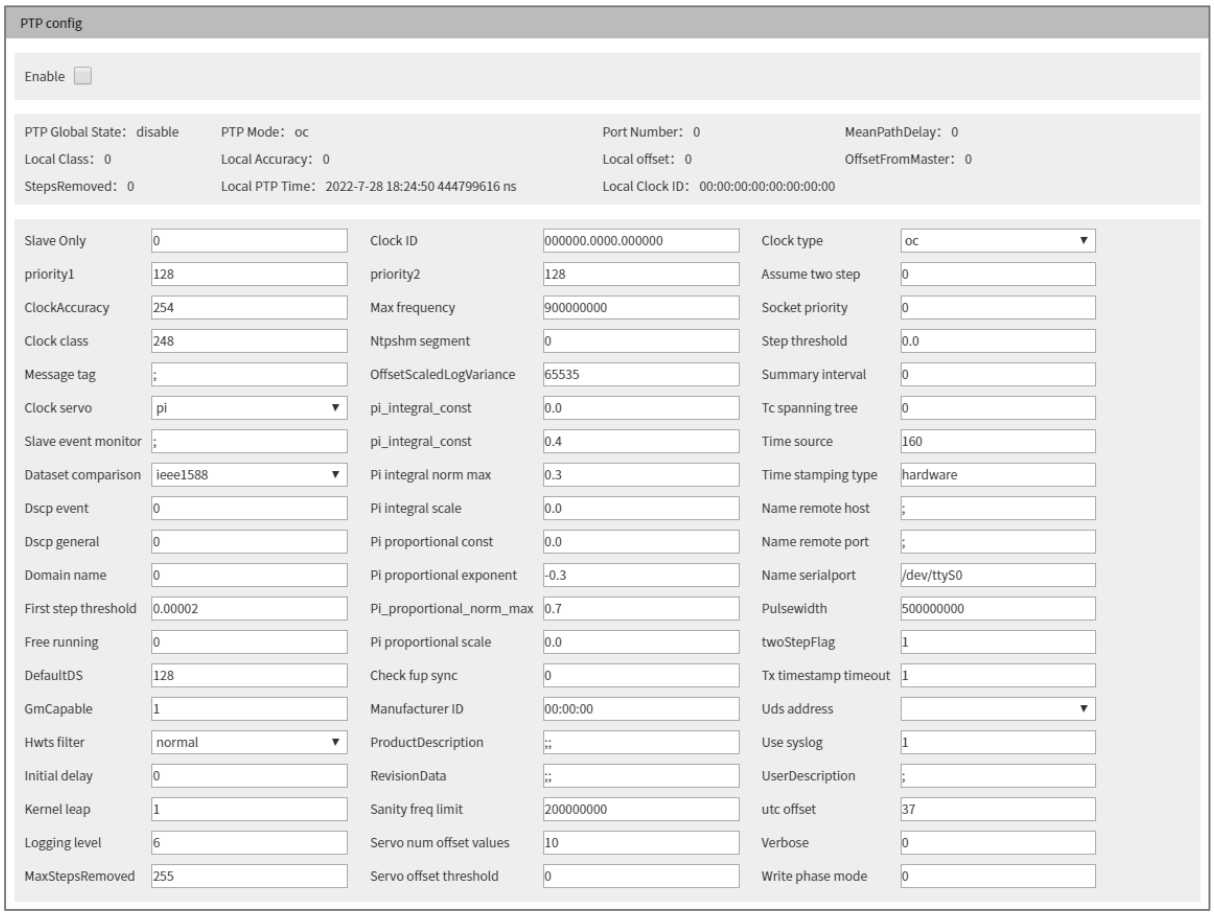
On the "PTP Config" page, user can configure the relevant parameters of PTP.

Operation Path

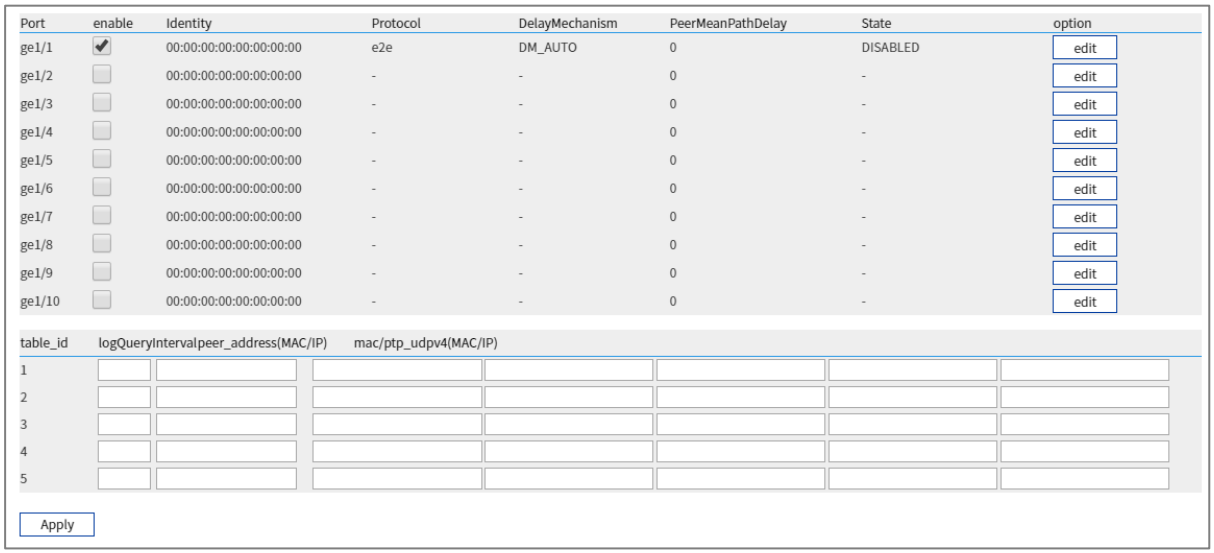
Open in order: "Advanced Config > PTP Config".

Interface Description

PTP configuration interface is as follows:



Copyright © 3onedata Co., Ltd.



The main element configuration description of PTP configuration interface:

Interface Element	Description
Enable	PTP Enable Configuration
PTP Global State	Display PTP enable status.
Local Class	Display the time level value of the clock on this device.
StepsRemoved	Display the number of hops from the optimal clock to the local clock node.
PTP Mode	Display the PTP clock node type.
Local Accuracy	Display the time precision value of the clock on this device.
Local PTP Time	Display the local PTP time.
Port Number	Display the number of interfaces with PTP enabled.
Local offset	Display the clock offset measure of the local clock source.
Local Clock ID	Display the local clock ID.
MeanPathDelay	Display the average path delay.
OffsetFromMaster	Display the clock offset from the master node.
Slave-only	Configure the working mode of OC. If enabled, the local clock is only a slave clock. The default value is 0 (disabled), and 1 means enabled.
Priority 1	Priority1 property of local clock, the value range is 0-255. It is used for the best main selection algorithm, and the lower value takes precedence.

Copyright © 3onedata Co., Ltd.

Interface Element	Description
ClockAccuracy	Configure the time accuracy of the clock, it ranges from 0 to 255. The smaller the value, the higher the accuracy.
Clock class	Configure the time level of the clock, it ranges from 0 to 255. The smaller the value, the higher the level.
Message tag	The tag which is added to all messages printed to the standard output or system log. The default is an empty string (which cannot be set in the configuration file as the option requires an argument).
Servo	The servo which is used to synchronize the local clock.
Slave event monitor	Specifies the address of a UNIX domain socket for slave event monitoring. The default is the empty string (disabled).
Dataset comparison	Specifies the method to be used when comparing data sets during the Best Master Clock Algorithm. The default is "ieee1588".
Dscp event	Defines the Differentiated Services Codepoint (DSCP) to be used for PTP event messages. The default is 0.
Dscp general	Defines the Differentiated Services Codepoint (DSCP) to be used for PTP general messages. The default is 0.
Domain Name	Configure the PTP domain to which the devices belong. In the same PTP domain, all devices follow a common rule to ensure the stable communication between devices. Devices in different domains cannot directly interact with each other. The value of PTP domain ranges from 0 to 127. When the standard of PTP protocol is IEEE1588v2, PTP devices belong to domain 0 by default.
First step threshold	The maximum offset the servo will correct by changing the clock frequency instead of stepping the clock. The default is 0.00002 (20 microseconds).

Copyright © 3onedata Co., Ltd.

Interface Element	Description
Free running	Don't adjust the local clock if enabled. The default is 0 (disabled).
DefaultDS	The Telecom Profiles (ITU-T G.8275.1 and G.8275.2) specify an alternate Best Master Clock Algorithm (BMCA) with a unique data set comparison algorithm. The default value is 128.
GmCapable	The local clock can be the master clock, with values ranging from 0-1, 0 means disabled and 1 means enabled. This only applies to the 802.1AS clock, and has no effect on the 1588 clock.
Hwts Filter	Select the hardware time stamp filter setting mode. Possible values are normal, check, full.
Initial delay	Use E2E or P2P delay mechanism to measure the initial path delay (in nanoseconds) of the clock used for clock synchronization before the delay. If it is set to 0, the clock will not be updated before the delay is measured.
Kernel leap	let the kernel apply it by stepping the clock instead of correcting the one-second offset with servo. The default is 1 (enabled).
Logging level	The maximum logging level of messages which should be printed. The default is 6 (LOG_INFO).
MaxStepsRemoved	Configure the maximum hop count of time synchronization device. In a PTP domain, if the step size of PTP synchronization clock path is too large, it will affect the accuracy of time synchronization due to the path delay. The value range is 0-255.
Clock id	Configure the clock ID of the GM clock. The format is XXXXXX.XXXX.XXXXXX. X represents a hexadecimal number, which cannot be all 0s.
Priority 2	Priority2 property of local clock, the value range is 0-255. It is used for the optimal main selection algorithm, and the lower value takes precedence.
Max frequency	The maximum allowed frequency adjustment of the clock in parts per billion (ppb). The default is

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	900000000 (90%).
Ntpshm segment	The number of the SHM segment used by ntpshm servo. The default is 0.
OffsetScaledLogVariance	The clock offset measure of the clock source, with the range of 0-65535.
Pi integral constant	The integral constant of the PI controller. The default is 0.0.
Pi integral index	The ki_exponent constant in the formula used to set the integral constant of the PI controller from the sync interval. The default is 0.4.
Pi integral norm max	The ki_norm_max constant in the formula used to set the integral constant of the PI controller from the sync interval. The default is 0.3.
Pi integral scale	The ki_scale constant in the formula used to set the integral constant of the PI controller from the sync interval. The default is 0.0.
Pi proportional const	The proportional constant of the PI controller. The default is 0.0.
Pi proportional exponent	The kp_exponent constant in the formula used to set the proportional constant of the PI controller from the sync interval. The default is -0.3.
Pi_proportional_norm_max	The kp_norm_max constant in the formula used to set the proportional constant of the PI controller from the sync interval. The default is 0.7.
Pi proportional scale	The kp_scale constant in the formula used to set the proportional constant of the PI controller from the sync interval. The default is 0.0.
Check fup sync	This option adds an additional check using the software time stamps from the networking stack to verify that the sync message did arrive first. This option is only useful if you do not trust the sequence IDs generated by the master. The default is 0 (disabled).
Manufacturer id	The manufacturer id which should be an OUI owned by the manufacturer. The default is 00:00:00.

Copyright © 3onedata Co., Ltd.

Interface Element	Description
ProductDescription	The product description string. The default is ";;".
RevisionData	The revision description string which contains the revisions for node hardware (HW), firmware (FW), and software (SW). The default is an ";;".
Sanity freq limit	The maximum allowed frequency offset between uncorrected clock and the system monotonic clock in parts per billion (ppb). The default is 200000000 (20%).
Servo num offset values	The number of offset values considered in order to transition from the SERVO_LOCKED to the SERVO_LOCKED_STABLE state. The default value is 10.
Servo offset threshold	The offset threshold used in order to transition from the SERVO_LOCKED to the SERVO_LOCKED_STABLE state. The transition occurs once the last The default value of offset_threshold is 0 (disabled).
Clock Type	Configure the device clock node type, specify the type of PTP clock. • oc: Ordinary Clock. • bc: Boundary Clock. • p2p_tc: Peer-to-peer transparent clock. • e2e_tc: End-to-End transparent clock.
Assume two step	One-step response is regarded as two steps, with values ranging from 0-1, 0 means disabled and 1 means enabled. It is used to solve the problem of 802.1AS switch.
Socket priority	Configure the SO_PRIORITY of sockets. The default is 0.
Step threshold	The servo system will correct the maximum offset by changing the clock frequency instead of stepping the clock. When set to 0.0, the servo will never step the clock, except at startup. It is specified in seconds. This option was once called pi_offset_const.
Summary interval	The time interval in which are printed summary

Copyright © 3onedata Co., Ltd.

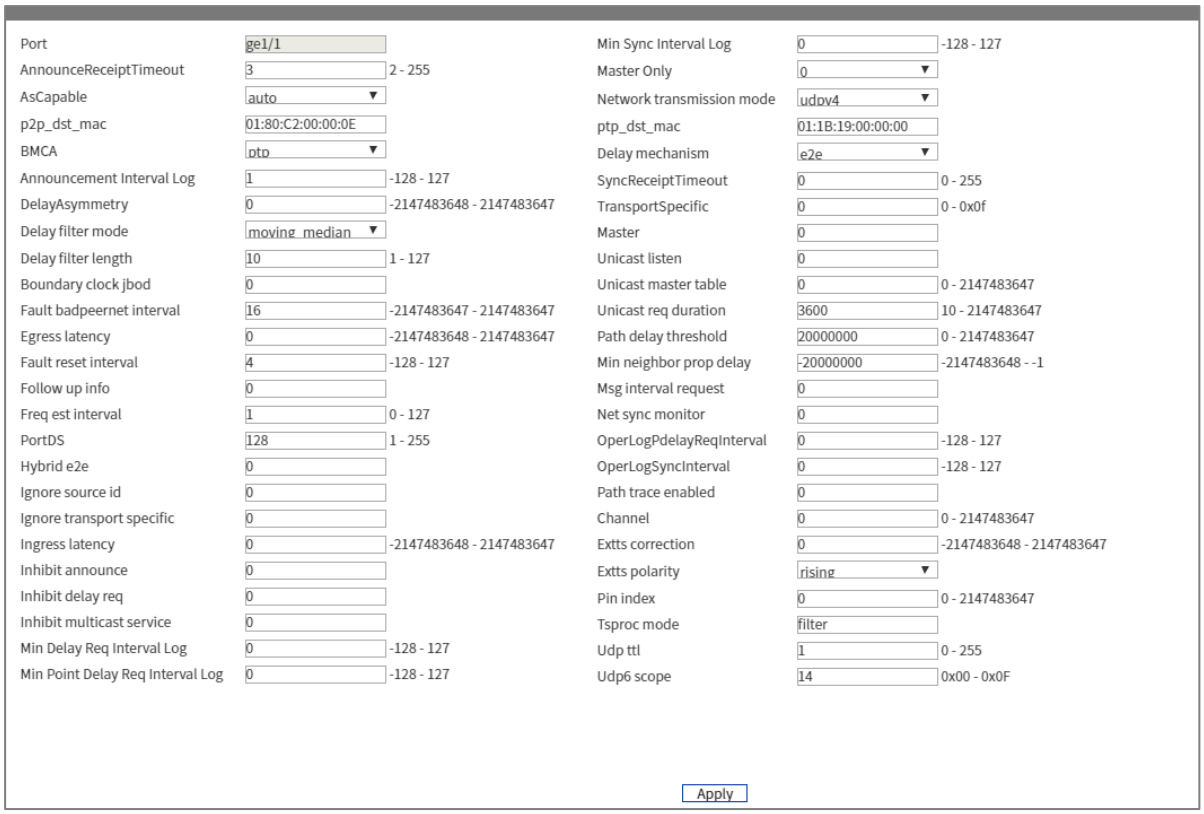
Interface Element	Description
	statistics of the clock. The default is 0 (1 second).
Tc spanning tree	When running as a Transparent Clock, increment the "stepsRemoved" field of Announce messages that pass through the switch.
Time source	The attribute of the clock. The corresponding parameter values are configured according to which type of time source is connected to the device, with values ranging from 16 to 254.
Timestamp type	The time stamping method. The allowed values are hardware, software and legacy. The default is hardware. • hardware • legacy • onestep • p2p1step • software
Name remote host	ts2phc.nmea_remote_host.
Name remote port	ts2phc.nmea_remote_port.
Name serialport	ts2phc.nmea_serialport.
Pulsewidth	ts2phc.pulsewidth. <1000000-999000000>
Two-step clock flag	Enable two-step mode for sync messages. One-step mode can be used only with hardware time stamping. The default is 1 (enabled).
Tx timestamp timeout	The number of milliseconds to poll waiting for the tx time stamp from the kernel when a message has recently been sent. The default is 1.
Uds address	Specifies the address of the UNIX domain socket for receiving local management messages. The default is /var/run/ptp4l.
Use syslog	Print messages to the system log if enabled. The default is 1 (enabled).
UserDescription	The user description string. Allowed values are of the form name; location and contain at most 128 utf8 symbols. The default is an empty string.
utc offset	The current offset between TAI and UTC. The

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	default is 37.
Verbose	Print messages to the standard output if enabled. The default is 0 (disabled).
Write phase mode	This option enables using the "write phase" feature of a PTP Hardware Clock. The default value is 0 (disabled).
Port	The Ethernet port number of the device.
Enable	Port PTP Enable Configuration
Identity	Display port transmission ID.
Protocol	Display port PTP protocol type.
DelayMechanism	Display the delay measurement mechanism of the port.
PeerMeanPathDelay	Display the average path delay between port and peer port.
State	Display port state.
Operation	Click "Edit" button to configure PTP interface.
Master table id.	Address table entry.
Request interval	It is specified as a power of two in seconds. The default is 0 (1 second).
Point delay address	peer address for delay packets(IPv4/MAC).
mac/dupv4 address (MAC/IP)	Configure the destination IP address of unicast PTP message in IPv4 UDP encapsulation format or the destination MAC address of PTP unicast message.

Click "Edit" button to configure PTP port, and the editing interface is shown below.

Copyright © 3onedata Co., Ltd.



Configuration description of main elements of the Edit interface:

Interface Element	Description
Port	Current Ethernet port number.
AnnounceReceiptTimeout	The number of missed Announce messages before the last Announce message expires, ranging from 2 to 255.
AsCapable	If it is set to "true", all checks that can unset the asCapable variable will be skipped. If it is set to "auto", asCapable will be initialized to "false" and set to "true" after the relevant checks pass.
Point delay destination mac address	MAC address to which the peer-to-peer delay message should be sent, which is only related to L2 transmission. The default value is 01:80:C2:00:00:0E.
BMCA	This option enables use of static roles for master and slave devices instead of running the best master clock algorithm (BMCA) described in 1588 profile. This is useful when you know the roles of the devices in advance. When set to ´noop', the

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	traditional BMCA algorithm used by 1588 is skipped. masterOnly and slaveOnly will be used to determine master or slave role for the device. In a bridge, slaveOnly (which is a global option) can be set to make all ports assume the slave role. masterOnly (which is a per-port config option) can then be used to set individual ports to take master role. BMCA is used in the Automotive profile to speed up the start time for grand master and slaves.
Announce interval logarithm	The mean time interval between Announce messages. A shorter interval makes ptp4l react faster to the changes in the master-slave hierarchy. The interval should be the same in the whole domain. It's specified as a power of two in seconds. The default is 1 (2 seconds).
DelayAsymmetry	The default is 0 nanoseconds.
Delay Filter Mode	• moving_average • Moving_median
Delay filter length	The default is 10.
Boundary clock jbod	The default is 0 (disabled).
Fault badpeernet interval	The default is 16 seconds.
Egress Latency	The default is 0.
Fault reset interval	The default is 4 (16 seconds).
Follow up info	If enabled, 802.1AS data will be included in the Follow_Up message. The range of values is 0-1, 0 means disabled and 1 means enabled.
Freq est interval	Estimate the time interval of local and peer clock frequency ratio. It is specified as a power of 2 in seconds.
PortDS	The default value is 128.
Hybrid e2e	The default is 0 (disabled).
Ignore source id	This will disable the source port identity check of Sync and Follow_Up messages. This is useful when the notification message is disabled in the master server and the slave server has no way to know its

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	identity.
Ignore transport specific	By default, if the transportSpecific field of the incoming message does not match the configured value, the incoming message will be discarded. However, many transports specified in the 1588 standard ignore this field. In addition, some devices are known to set the reserved bit. Configuring this option to 1 will cause this field to be completely ignored when receiving. The default value is 0.
Ingress latency	The default is 0.
Inhibit announce	This will disable the timer of the announcement message (i.e. FD_MANNO_TIMER) and the timeout timer of the announcement message (i.e. FD_ANNOUNCE_TIMER). This is used by the automotive profile as part of switching to static BMCA. If this option is enabled, ignore_source_id must be enabled in the slave, because it cannot identify the master identity in Sync and Follow_Up messages. The default value is 0 (disabled).
Inhibit delay req	Don't send any delay request. This requires the asCapable configuration option to be set to "true". This is useful when running as a designated master station that doesn't need to calculate the slave station offset. The default value is 0 (disabled).
Inhibit multicast service	Some unicast mode profiles insist on not transmitting multicast messages. Setting this option will prohibit multicast transmission. The default value is 0 (multicast enabled).
Minimum end delay request interval logarithm	The default is 0 (1 second).
Minimum point delay request interval logarithm	The minimum average time interval allowed between Delay_Req messages. A shorter interval makes ptp4l react faster to the change of path delay. It is specified as a power of 2 in seconds. The default value is 0(1 second).

Copyright © 3onedata Co., Ltd.

Interface Element	Description
Minimum synchronization interval logarithm	Average time interval between synchronous messages. A shorter interval can improve the accuracy of the local clock. It is specified as a power of 2 in seconds. The default value is 0(1 second).
Master Only	Set this option to 1 to prevent the port from entering the SLAVE state. In addition, the local clock will ignore the Announce message received by this port. The intended purpose of this option is to support telecom profiles that conform to ITU-TG.8265.1, G.8275.1 and G.8275.2.
Network transmission mode	Select network transmission. Possible values are UDPv4 and L2.
Master clock synchronization destination mac address	MAC address to which the PTP message should be sent, which is only related to L2 transmission. The default value is 01:1B:19:00:00:00.
Delay mechanism	Select the delay mechanism. Possible values are E2E, P2P and Auto.
SyncReceiptTimeout	The number of synchronization/follow-up messages that may be lost before the best master clock election is triggered. This option is used to run in gPTP mode according to the 802.1AS-2011 standard. Setting this option to zero will disable synchronization message timeout.
TransportSpecific	Transport-specific field. Must be in the range of 0 to 255.
Master	ts2phc.master
Unicast listen	The default is 0 (disabled).
Unicast master table	The default is 0 (unicast discovery disabled).
Unicast req duration	The default is 3600 seconds or one hour.
Path delay threshold	The upper limit of peer-to-peer delay (in nanoseconds). If the estimated peer-to-peer delay is greater than this value, the port is marked as not supporting 802.1AS
Min neighbor prop delay	The lower limit of peer-to-peer delay (in nanoseconds). If the estimated peer-to-peer delay is

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	smaller than this value, the port is marked as not supporting 802.1AS
Msg interval request	This option, when set, will trigger an adjustment to the Sync and peer delay request message intervals when the clock servo transitions into the SERVO_LOCKED_STABLE state. The Sync interval will be adjusted via the signaling mechanism while the pdelay request interval is simply adjusted locally. The values to use for the new Sync and peer delay request intervals are specified by the operLogSyncInterval and operLogPdelayReqInterval options, respectively. The default value of msg_interval_request is 0 (disabled).
Net sync monitor	The default is 0 (disabled).
OperLogPdelayReqInterval	The Pdelay Request messages interval to be used once the clock enters the SERVO_LOCKED_STABLE state. If the 'msg_interval_request' option is set, then the local slave port will adopt this rate when the local clock enters the "locked stable" state. This option is specified as a power of two in seconds, and the default value is 0 (1 second).
OperLogSyncInterval	The Sync message interval to be requested once the clock enters the SERVO_LOCKED_STABLE state. If the 'msg_interval_request' option is set, then the local slave port will request the remote master to switch to the given message rate via a signaling message containing a Message interval request TLV. This option is specified as a power of two in seconds, and default value is 0 (1 second).
Path trace enabled	Enables the mechanism for tracking the route of Announce messages. The default value is 0 (Disabled).
Channel	ts2phc.channel
Extts correction	ts2phc.extts_correction

Copyright © 3onedata Co., Ltd.

Interface Element	Description
Extts polarity	ts2phc.extts_polarity
Pin index	ts2phc.pin_index
Tsproc mode	• filter • filter_weight • raw • raw_weight
Udp ttl	The default is 1 to restrict the messages sent by ptp4l to the same subnet.
Udp6 scope	The default is 0x0E for the global scope.

7.9 TSN Configuration

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 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 standard mainly includes clock synchronization, flow control, reliability and security.

7.9.1 802.1Qav Configuration

Function Description

On the “Qav Configuration” page, you can configure TSN standard IEEE 802.1Qav forwarding and queue enhancement functions.

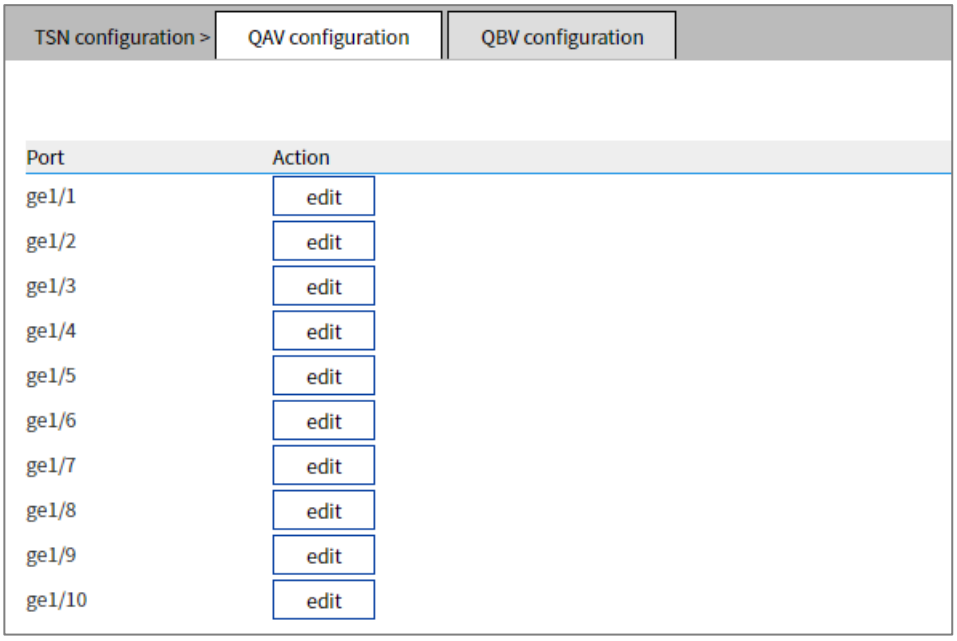
Operation Path

Open in order: "Advanced Config > TSN Configuration> Qav Config".

Interface Description

Qav Config interface is as follows:

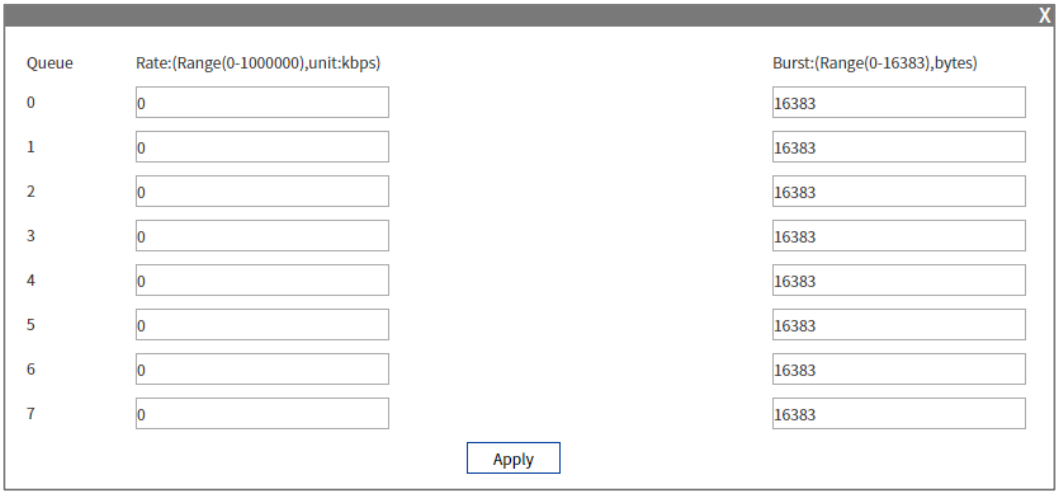
Copyright © 3onedata Co., Ltd.



Main elements configuration description of Qav Config interface:

Interface Element	Description
Port	The Ethernet port number of the device.
Action	Click “Edit” to edit the restriction parameters of the forwarding queue.

Click the “Edit” button, and the editing interface is shown below.



Configuration description of main elements of the Edit interface:

Interface Element	Description
Queue	Each interface has 8 forwarding queues, with queue numbers from 0 to 7.
Rate	Qav is based on the speed limit of the port/queue, and its

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	value range is 0-1,000,000, unit: kbps.
Burst	Qav is based on the burst byte limit of the port/queue, and its value range is 0-16383, unit: byte.

7.9.2 802.1Qbv Configuration

Function Description

On the “Qbv Configuration” page, you can configure TSN standard IEEE 802.1Qbv queuing scheduled traffic enhancement functions.

The workflow of IEEE 802.1Qbv is:

- The system time reaches the basic time, and the 802.1Qbv function is enabled.
- Classify the messages received by the interface according to the flow characteristics, and enter the corresponding forwarding queue according to the configured CoS value.
- According to the queue switch state in each node of the control link list, the opening and closing of the queue and the duration of the queue switch state are controlled, and the traffic in each queue is sent or prohibited, as well as the sending and prohibiting time.
- Execute the loop control link list, and send the TSN stream according to the rules.

TSN technology is based on time synchronization. Through network planning, all devices in TSN network can achieve microsecond time synchronization at first, and then the same 802.1Qbv configuration is deployed on each device, so that TSN traffic enters the same queue on all TSN devices, and the switch state and switch time of the queue are the same, thus achieving the effect that TSN flow can be linearly forwarded in TSN network.

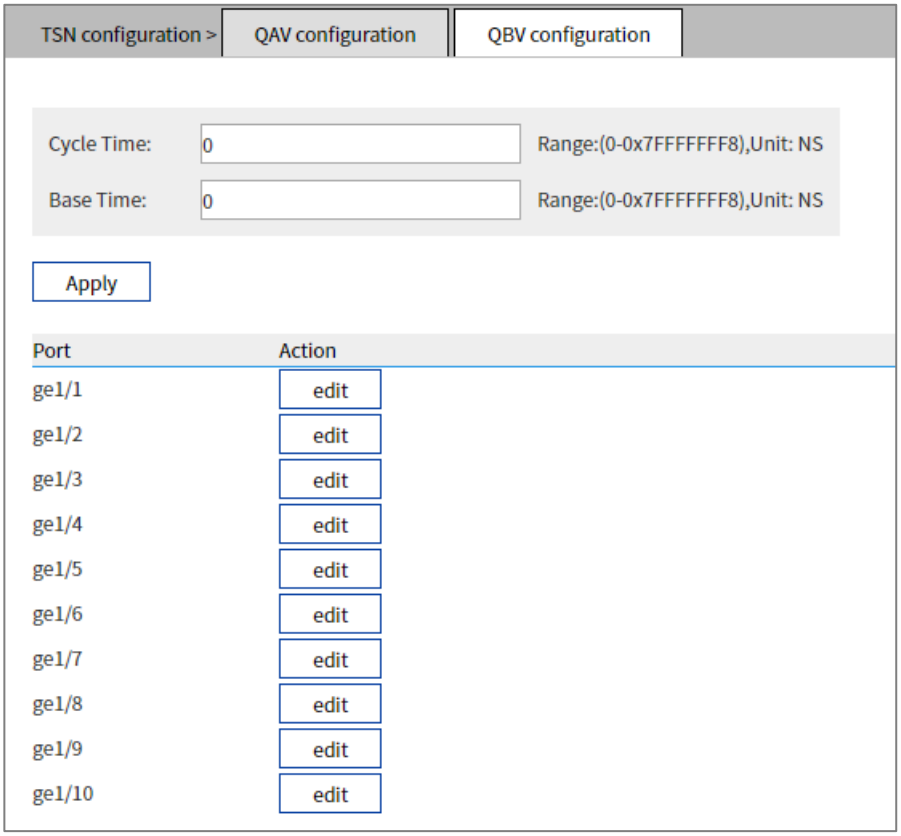
Operation Path

Open in order: "Advanced Config > TSN Configuration> Qbv Config".

Interface Description

Qbv Config interface is as follows:

Copyright © 3onedata Co., Ltd.

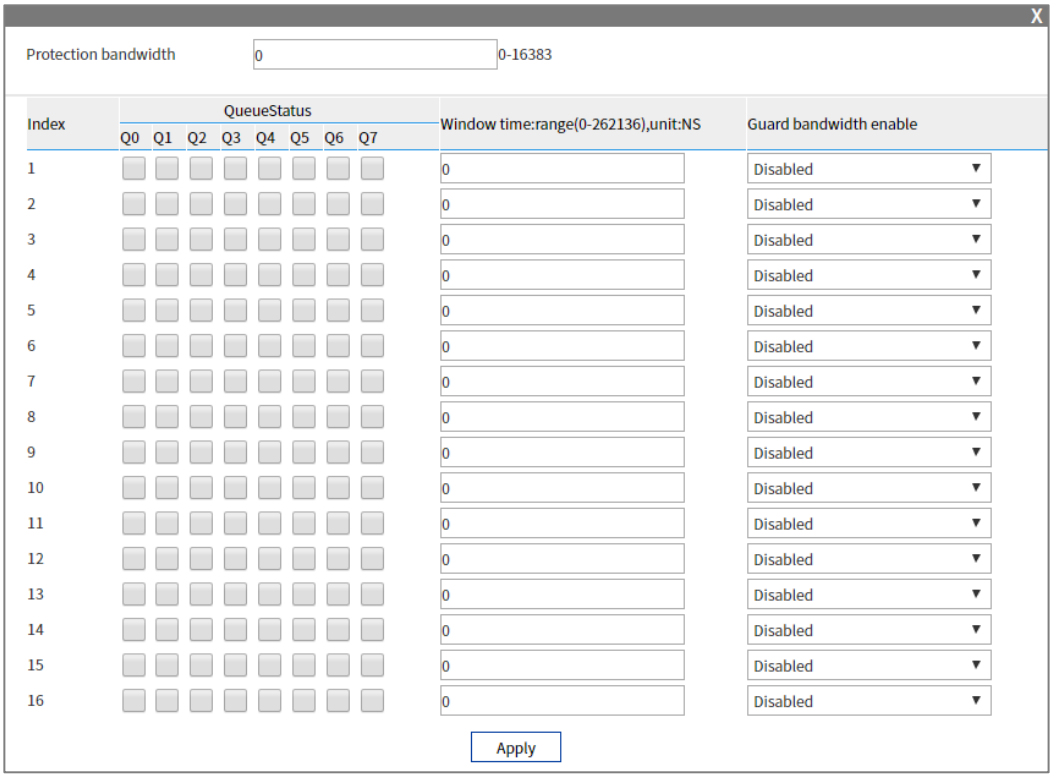


Main elements configuration description of Qbv Config interface:

Interface Element	Description
Cycle Time	802.1Qbv executes the control linked list periodically, and the cycle time is the time for the system to execute the control link list once. The cycle time range is 0-0x7FFFFFF8, unit: ns.
Base Time	The time when the interface starts to execute the 802.1Qbv forwarding queue scheduling policy. The basic time range is 0-0x7FFFFFF8, and the unit is ns.
Port	The Ethernet port number of the device.
Action	Click “Edit” to edit the restriction parameters of the forwarding queue.

Click the “Edit” button, and the editing interface is shown below.

Copyright © 3onedata Co., Ltd.



Configuration description of main elements of the Edit Config interface:

Interface Element	Description
Protection bandwidth	The 802.1Qbv protection band is the buffer time between two gate operations in TSN forwarding scheduling gating list, with a value range of 0-16383.
Index	Index entry.
Queue status	Qbv is based on the queue bitmap of port/time slice, that is, the switch state of forwarding queue. When checked, it is on, and when unchecked, it is off.
Window time	Qbv is based on the window time of the port/time slice, and the duration of each switch state. The value range is 0-262136, and the unit is ns.
Guard bandwidth enable	Qbv enables the protection bandwidth based on port/time slice, and the options are as follows: • Disabed: When the interface is forwarding the 802.1Qbv feature stream, a data frame is sent in half, and the duration of the forwarding queue gate state reaches, the 802.1Qbv will immediately perform the next gate operation. • Enable: When the interface is forwarding the 802.1Qbv feature stream, a data frame is sent in half, and the

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	duration of the forwarding queue gate state reaches, then the 802.1Qbv will send the rest of the data frame before performing the next gate operation.

Copyright © 3onedata Co., Ltd.

8 System Maintenance

8.1 Configure File Management

8.1.1 Global Configuration

Function Description

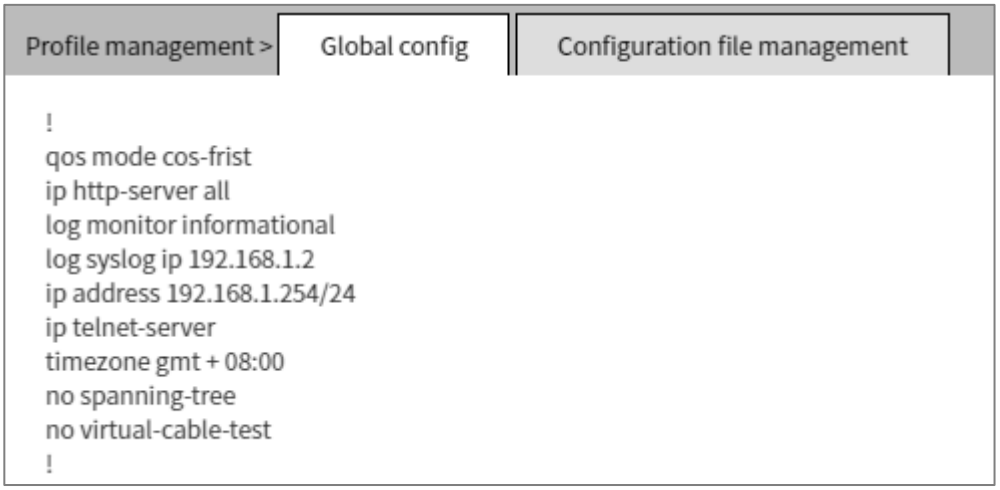
On the "Global Configuration" page, user can view current configuration information.

Operation Path

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

Interface Description

Global configuration interface is as follows:



Copyright © 3onedata Co., Ltd.

8.1.2 Manage Configuration File

Function Description

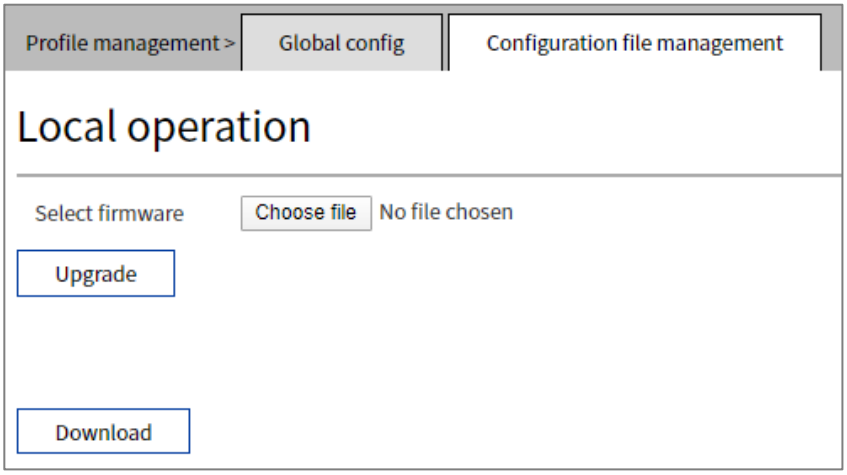
On the "Manage Configuration File" page, user can download and upload configuration file.

Operation Path

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

Interface Description

Configuration file management interface is as follows:



The main elements configuration description of configure file management interface:

Interface Element	Description
Local operation	**Local operation configuration bar**
Select Firmware	Click the "Select File" button to select the configuration upgrade file locally.
Upgrade	Click the "Upload" button to upload the configuration file.
Download	Download the configuration file of current device to the local PC, format: .conf.

Note

After finishing update, the device will automatically open a new page to "System State", and uploading configuration file will be valid after the device is reset.

Copyright © 3onedata Co., Ltd.

8.2 Restore Factory Defaults

Function Description

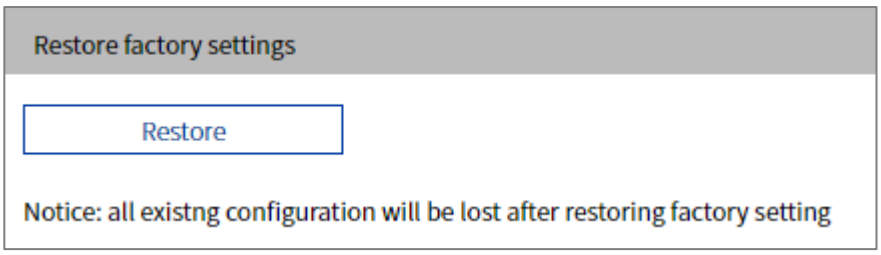
On the "Restore" page, user can restore the device to default settings.

Operation Path

Open in order: "System management > Restore".

Interface Description

Restore Factory Settings interface is as follows:



The main element configuration description of restore factory settings interface:

Interface Element	Description
Restore	Click this button and the device will lose all existing configurations and reverts to factory settings.

8.3 Upgrade

8.3.1 TFTP

Function Description

On the "TFTP" page, user can update and upgrade the device procedure via TFTP server.

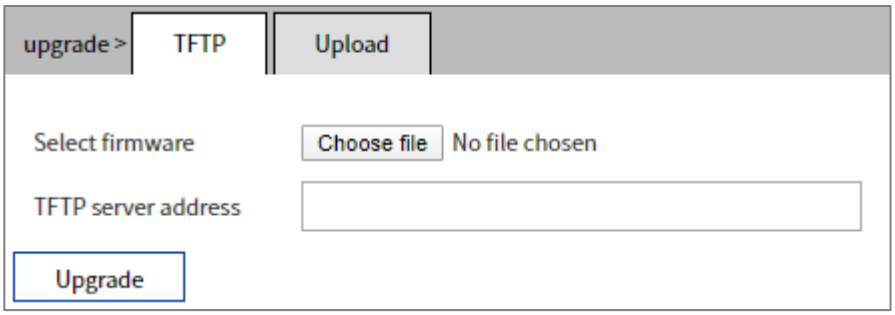
Operation Path

Open in order: "System Maintenance > Upgrade> TFTP".

Interface Description

TFTP interface as below:

Copyright © 3onedata Co., Ltd.



Main elements configuration descriptions of TFTP interface:

Interface Element	Description
Select firmware	The name of the TFTP server to store the upgrade file.
TFTP server address	The IP addresses of TFTP server that stores upgrade files.

8.3.2 Upload

Function Description

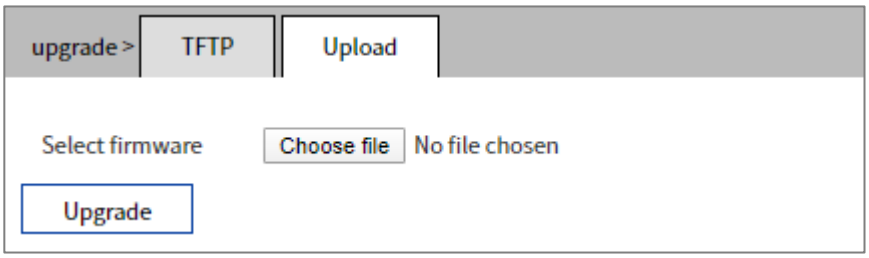
On the "Upload" page, user can update and upgrade the device procedure via local browser.

Operation Path

Open in order: “System Maintenance > Upgrade> Upload”.

Interface Description

Upload interface is as below:



Configuration description of main elements of the Upload interface:

Interface Element	Description
Select Firmware	Select update file stored in the local host by clicking “select file” button. After clicking “upgrade” button, it starts updating firmware.

Copyright © 3onedata Co., Ltd.

Warning

Do not click on or configure other WEB pages of the device or restart the switch when uploading configuration files or upgrading software. Otherwise, the configuration file upload or software update will fail, or the device system will crash.

9 FAQ

9.1 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_□ 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.

9.2 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.

Copyright © 3onedata Co., Ltd.

2. **What's the difference between RING V2 and RING V3?**

   RING V2 and RING V3 are our company's ring patents. RING V2 only supports single ring and coupling ring. RING V3 supports single ring, coupling ring, chain and Dual_homing, and Hello_Time can be set to detect port connection status.

3. **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 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.

4. **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 from high to low, connect automatically in supported highest speed.

9.3 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.

Copyright © 3onedata Co., Ltd.

- Power supply voltage can't meet the device requirements; troubleshooting, configure the power supply voltage according to the device manual.

2. **Why is the Link/Act indicator off?**

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.

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.

Copyright © 3onedata Co., Ltd.

10 Maintenance and Service

Since the date of product delivery, our company provides five-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 wireless AP, consumers can get help and solutions in the following ways:

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

10.1 Internet Service

More useful information and tips are available via our company website.

Website: http://www.3onedata.com

10.2 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

Copyright © 3onedata Co., Ltd.

10.3 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. 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.

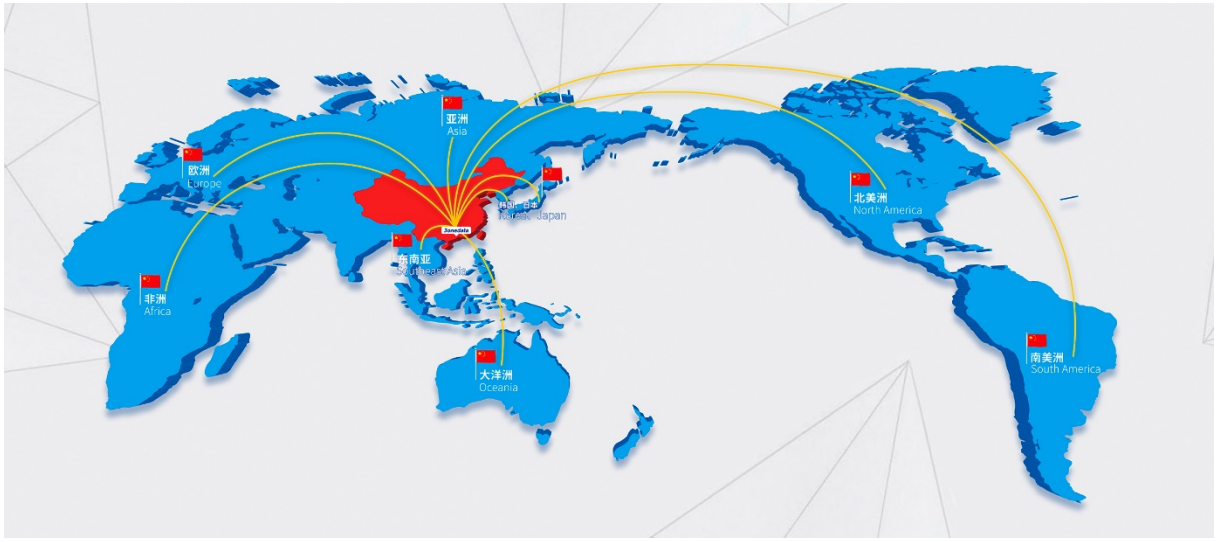
11 Appendix: Description of Log ID

The detailed description and corresponding level of the code are as follows:

ID	Note	Level
1	Power Alarming	False
2	Port Alarming	False
3	Temperature Alarming	False
4	Mrp Alarming!ring state open.	False
5	Leakage Current Alarming	False
6	Netload Alarming	False
7	Warning Neigborhood Alarming	False
8	Sdcard Alarming!SD card can not detect. Alarming	False
9	DSP warning!	False
10	AR Disconnect!	False
11	Upgrade form Web TFTP mode	Notice
12	Upgrade form Web HTTP mode	Notice
13	Upgrade form sdCard	Notice
14	Download configuration to Web TFTP mode	Notice
15	Download configuration to SD card	Notice
16	Upgrade configuration by Web TFTP mode	Notice
17	Upgrade configuration by SD card	Notice
18	System reboot	Notice
19	System restore	Notice
20	Save running configuration	Notice
21	AR Connect	Notice
22	Time sync form server	Notice
23	User log clear	Notice
24	Test Mail send failed	Notice

ID	Note	Level
25	Netload reset	Notice
26	Leakage current reset	Notice
27	DSP self-Saving	Notice
28	Dhcp server offering.	Notice
29	Dhcp server no offering.	Notice
30	Function Port mirror enable	Information
31	Function IGMP-Snooping enable	Information
32	Function STP enable	Information
33	Function MRP enable	Information
34	Function ACL enable	Information
35	Function NTP enable	Information
36	Function NTP disble	Information
37	Function NTP server enable	Information
38	Function NTP server disable	Information
39	Port Up	Information
40	Port Download	Information
41	Power on	Information
42	Power off	Information

3onedata



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