3onedata



IES618 Series
Managed Industrial Ethernet Switch
User Manual

Document Version: 01

Issue Date: 05/20/2025

Copyright © 2025 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 trademarks owned by 3onedata Co., Ltd. And other trademarks mentioned in this manual belong to their corresponding companies.

Notice

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 is only for usage guide, all statement, information, and suggestion in this document won't constitute any warranty.

3onedata



3onedata Co., Ltd.

Headquarter address:	3/B, Zone 1, Baiwangxin High Technology Industrial park, Nanshan District, Shenzhen, 518108 China
Technology support:	tech-support@3onedata.com
Service hotline:	+86 -880-4496
E-mail:	sales@3onedata.com
Fax:	+86 -0755-26703485
Website:	http://www.3onedata.com

Preface

Managed Industrial Ethernet Switch User Manual has introduced this series of switches:

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

Audience

This manual applies to the following engineers:

- Network administrators responsible for network configuration and maintenance
- On-site technical support and maintenance personnel
- Network engineer

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’.

Symbols

Format	Description
Notice	Remind the announcements in the operation, improper operation may result in data loss or equipment damage.

Copyright © 3onedata Co., Ltd.

Format	Description
Warning	Pay attention to the notes on the mark, improper operation may cause personal injury.
Note	Conduct necessary supplements and explanations for the description of operation content.
Key	Configuration, operation, or tips for device usage.
Tips	Pay attention to the operation or information to ensure success device configuration or normal working.

Button Operation Convention

Format	Description
Logout	There is a logout button in the upper right corner of the webpage. After clicking it, the webpage returns to the login page.
Reboot	There is a restart button in the upper right corner of the webpage. After clicking, a restart confirmation box pops up. After confirmation, the device will restart.
Save	There is a Save button in the upper right corner of the webpage. Click it to save the current device configuration.
Add	Click the Add button to add a line of configuration. Note that repeated configuration may result in data overwrite.
Delete	Check the line to be deleted, and then click the Delete button to delete the configuration.
Config	Check the line to be configured, and then click the configure button to enter the configuration page.
	Click the right side of the switch to enable the function, as shown in figure:  . Click the left side of the switch to disable the function, as shown in the figure:  .
Apply	Click the Set button to submit the current configuration.

Copyright © 3onedata Co., Ltd.

Revision Record

Version No.	Revision Date	Revision Note
01	05/20/2025	Product release

Copyright © 3onedata Co., Ltd.

Contents

PREFACE 1
CONTENTS I
1 LOGIN TO THE WEB INTERFACE 1
1.1 SYSTEM REQUIREMENTS FOR WEB BROWSING 1
1.2 SET THE IP ADDRESS OF PC 1
1.3 LOGIN TO THE WEB CONFIGURATION INTERFACE 3
2 SYSTEM INFORMATION 4
3 LOGIN CONFIGURATION 7
3.1 IP ADDRESS CONFIGURATION 7
3.2 USER CONFIGURATION 8
3.3 PROTOCOL AUTHORIZATION 10
4 PORT CONFIGURATION 12
4.1 PORT SETTINGS 12
4.2 LINK AGGREGATION 13
4.3 PORT SPEED LIMIT 15
4.4 STORM CONTROL 16
4.5 PORT MIRRORING 18
4.6 PORT STATISTICS 19
4.6.1 Port Statistics-Overview 19
4.6.2 Port Statistics-Port 20
5 LAYER 2 CONFIGURATION 21
5.1 VLAN CONFIGURATION 21
5.1.1 Global Configuration 22
5.1.2 VLAN Configuration 24
5.2 MAC CONFIGURATION 26
5.2.1 MAC Address Table 27
5.2.2 Static MAC 28
5.3 SPANNING TREE 29
5.3.1 Global Configuration 29
5.3.2 Port Configuration 31
5.3.3 State Information of Spanning Tree 32
5.4 RING 34
5.4.1 Instance: create single ring 37
5.5 IGMP SNOOPING CONFIGURATION 38

Copyright © 3onedata Co., Ltd.

5.5.1 Global Configuration 38
5.5.2 Static Multicast MAC 40
5.6 PORT LOOPBACK DETECTION 41
5.7 ERPS 42
5.7.1 Timer Configuration 42
5.7.2 Ring Configuration 44
5.7.3 Instance Configuration 45
6 NETWORK MANAGEMENT 49
6.1 SNMP CONFIGURATION 49
6.1.1 View 49
6.1.2 Community 50
6.1.3 SNMP Group 51
6.1.4 V3 User 52
6.1.5 Trap Alarm 55
6.2 LLDP CONFIGURATION 56
6.2.1 Global Configuration 56
6.2.2 Port Configuration 57
6.2.3 Neighbor Information 59
6.3 DHCP-SERVER 59
6.3.1 DHCP Switch 60
6.3.2 Lease and Gateway Configuration 60
6.3.3 DNS server 61
6.3.4 Port Binding 62
6.4 ACCESS CONTROL 63
6.4.1 Port Authentication 63
6.4.2 Authentication Database 65
6.5 QOS 66
6.5.1 QoS Classification 66
6.5.2 CoS Mapping 69
6.5.3 ToS Mapping 70
6.6 MODBUS_TCP 71
7 SYSTEM MAINTENANCE 77
7.1 NETWORK DIAGNOSIS 77
7.1.1 Ping 77
7.2 TIME 78
7.2.1 NTP Configuration 78
7.2.2 Time Zone Configuration 79
7.3 ALARM CONFIGURATION 80
7.3.1 Relay Setting 80
7.3.2 Port Alarm 81
7.3.3 Power Alarm 82
7.3.4 Utilization Alarm 83
7.3.5 Mail Alarm 84

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

7.4 CONFIGURATION FILE MANAGEMENT 86
7.4.1 Configuration File Update 86
7.4.2 Restore Factory Settings 87
7.5 UPGRADE 87
7.6 LOG INFORMATION 88
7.6.1 Log Information 88
7.6.2 Syslog Server 89
8 FAQ 91
8.1 SIGN IN PROBLEMS 91
8.2 CONFIGURATION PROBLEM 91
8.3 ALARM PROBLEM 92
8.4 INDICATOR PROBLEM 92
9 MAINTENANCE AND SERVICE 95
9.1 INTERNET SERVICE 95
9.2 SERVICE HOTLINE 95
9.3 PRODUCT REPAIR OR REPLACEMENT 96

Copyright © 3onedata Co., Ltd.

1 Login to the WEB Interface

1.1 System Requirements for WEB Browsing

Using the industrial Ethernet switch, the system should meet the following conditions.

Hardware and Software	System Requirements
CPU	Above Pentium 586
Memory	Above 128MB
Resolution	Above 1024x768
Color	256 colors or above
Browser	Internet Explorer 6.0 or above
Operating system	Windows XP Windows 7

1.2 Set the IP Address of PC

The switch default management is as follows:

IP Settings	Default Value
IP address	192.168.1.254
Subnet mask	255.255.255.0

While configuring the switch via Web:

- Before remote configuration, please make sure the route between computer and switch is reachable.
- Before local configuration, please make sure the IP address of the computer is on

Copyright © 3onedata Co., Ltd.

the same subnet to the one of switch.

Note:
While first configuring the switch, if it is a local configuration mode, please make sure that the network segment of current PC is 1.

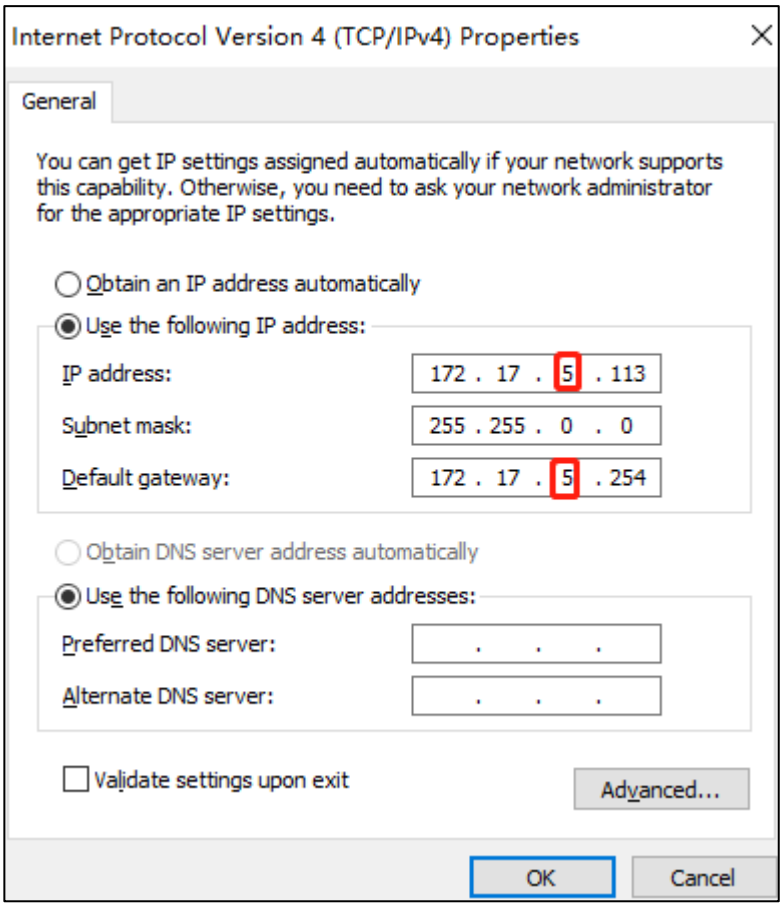
Eg: Assume that the IP address of the current PC is 192.168.5.60, change the network segment "5" of the IP address to "1".

Operation Steps

Amendment steps are as follows:

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

Step 2 Change the "5" selected by the red frame in the figure to "1".



Step 3 Click "OK", modification is successful.

Step 4 End.

Copyright © 3onedata Co., Ltd.

1.3 Login to the WEB Configuration Interface

Operation Steps

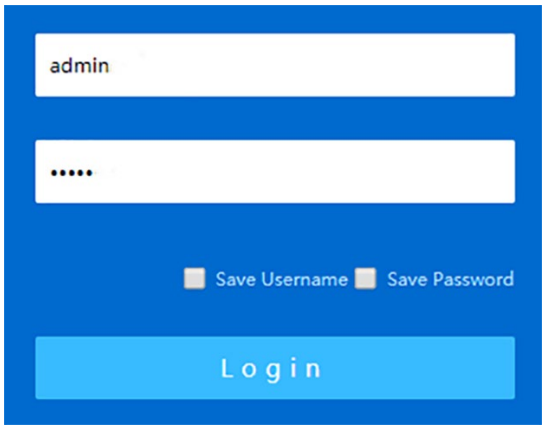
Log in to the WEB configuration interface as follows:

Step 1 Run the computer browser.

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

Step 3 Click the Enter key.

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



Note:

- The default username and password for the switch are "admin", which is strictly case-sensitive when typing.
- The default user password is with administrator privileges.
- WebServer will provide 3 opportunities to enter username and password. If you enter the error 3 times in succession, the browser will display "Access denied" to deny access to the information. Please refresh the page and try again.

Step 5 Click "Login".

Step 6 End.

After login successfully, user can configure relative parameters and information of WEB interface according to demands.

Note:

After logging in to the device, you can modify the IP address of the switch for ease of use.

Copyright © 3onedata Co., Ltd.

2 System Information

Function Description

View port status such as port type and connection status.

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

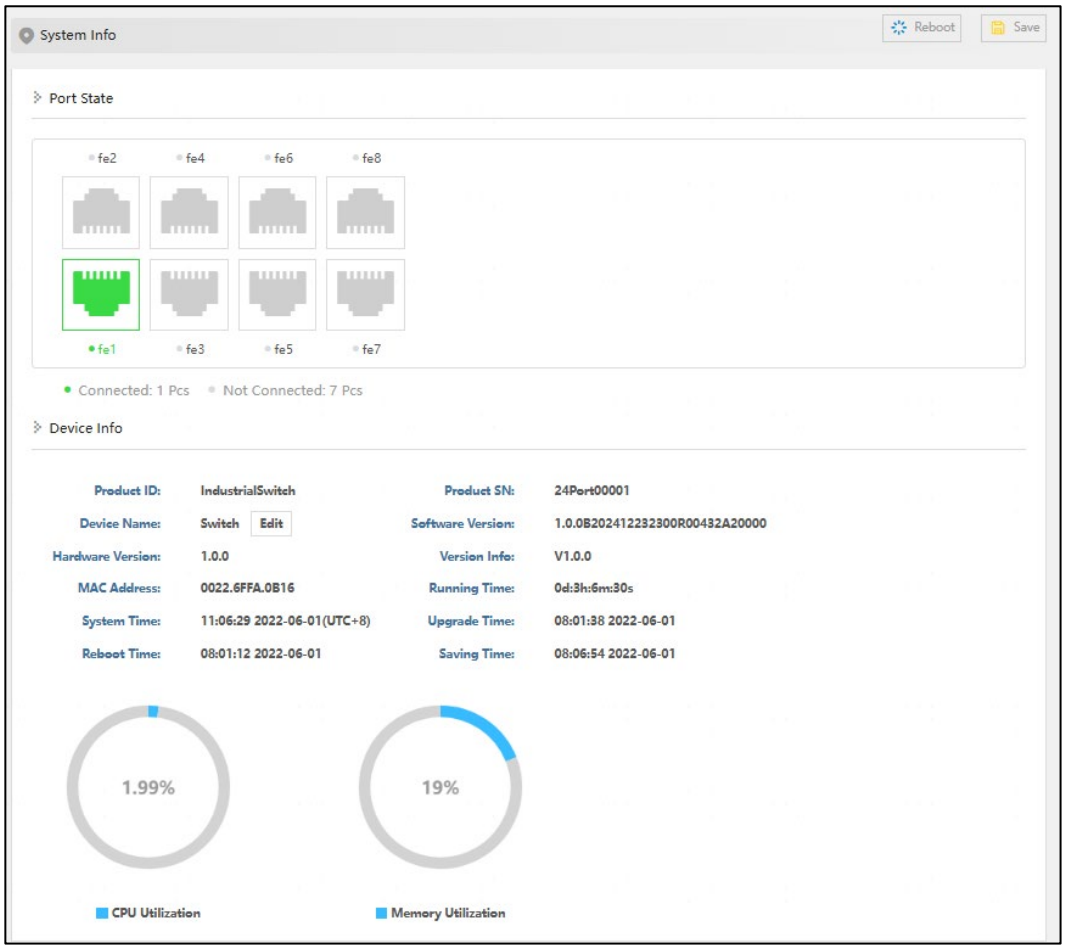
Operation Path

Open in the navigation bar: “System Info”.

Interface Description

System information interface screenshot:

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



The main element configuration description of system information interface:

Interface Element	Description
Port State	Display port icon and port connection status of the device: • Copper port icon, grayed out indicates that the device is not connected. •  Copper port icon, highlighting indicates that the device is connected. •  Copper port icon, grayed out indicates that the device is not connected. •  Fiber port icon, highlighting indicates that the device is connected. Note: The number of fiber ports and copper ports displayed on the interface varies depending on the device.

Copyright © 3onedata Co., Ltd.

Interface Element	Description
Device Info	Basic information of software, hardware, and operation of the device. • Product ID • Device Name • Hardware Version • MAC Address • System Time • Reboot Time • Product SN • Software Version • Version Info • Running Time • Upgrade Time • Saving Time • CPU Utilization • Memory Utilization

Copyright © 3onedata Co., Ltd.

3 Login Configuration

3.1 IP Address Configuration

Function Description

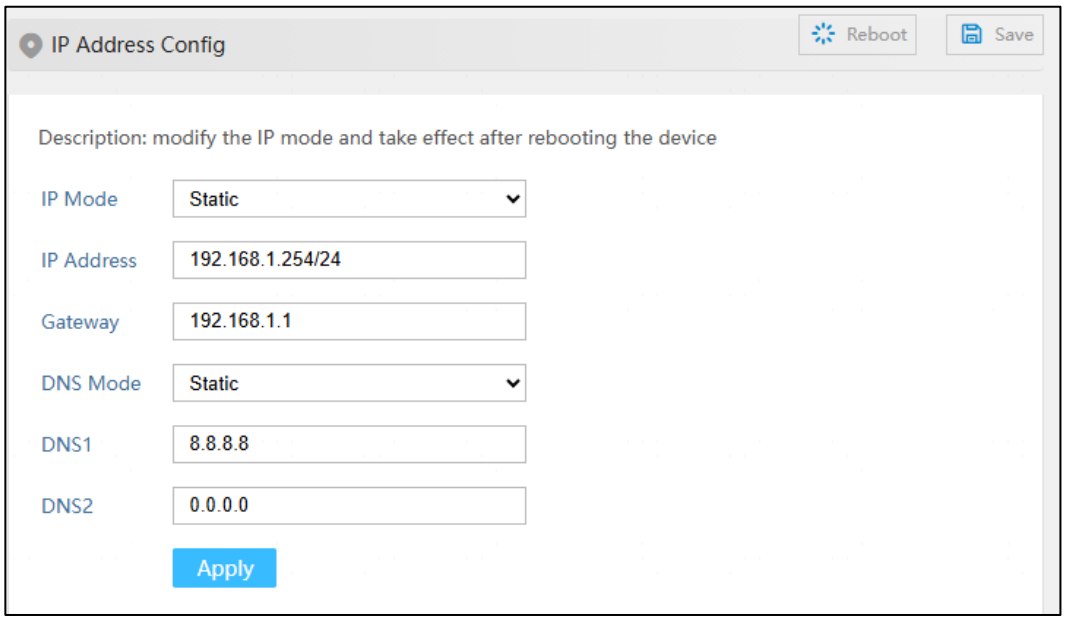
Configure the static or dynamic IP address.

Operation Path

Open on the navigation bar: "Login Config > IP Address ".

Interface Description

Interface screenshot of IP address configuration:



The main elements configuration description of IP address configuration interface:

Copyright © 3onedata Co., Ltd.

Interface Element	Description
IP Mode	Set the IP address acquisition mode, which can be set to: • Static: System IP address configured by default or manually. • Dynamic: system automatically acquired IP address of the device. Note: Default configured IP address is 192.168.1.254/24.
IP Address	Display the IP address of the device.
Gateway	Display the gateway address of the device.
DNS Mode	Set the DNS acquisition mode, which can be set to: • Static: DNS that is either system default configuration or manually set. • Dynamic: system automatically acquired DNS of the device. Note: The default DNS1/DNS2 configuration is 8.8.8.8/0.0.0.0.
DNS1	Display device DNS1.
DNS2	Display device DNS2.

3.2 User Configuration

Function Description

Add/delete users accessing the network management system.

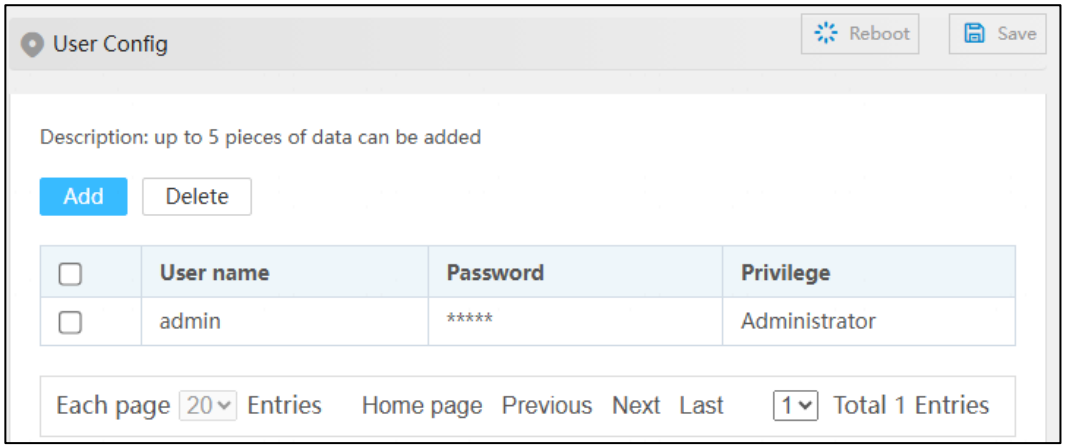
Operation Path

Open in the navigation bar: “Login Config > User”.

Interface Description

The screenshot of user configuration interface:

Copyright © 3onedata Co., Ltd.



The main element configuration description of user configuration interface:

Interface Element	Description
User name	User name for accessing the network management system. Note: • The user name is a combination of letters, numbers and symbols not more than 20 bytes. Please be case-sensitive. • Up to 5 groups of users are supported.
Password	User name for accessing the network management system. Note: The password is a combination of letters, numbers and symbols not more than 20 bytes. Please be case-sensitive.
Privilege	• Observer: The configuration information of the device can be viewed, but the configuration of the device cannot be modified. • Administrator: User has all privileges of the device, including downloading, uploading, rebooting, modifying device information and other other operations. Notice: • Users can view, delete, or add other users whose priority does not exceed their own. • If the added user name already exists, the original user information will be overwritten.

Notice

Please keep the modified login name and password in mind. If you forget it, you can restore it to factory setting via DIP switch. Default login name and password of logging in to the WEB configuration interface are “admin”.

Copyright © 3onedata Co., Ltd.

3.3 Protocol Authorization

Function Description

Open the access security protocols Telnet and SSH for the remote login service.

The full English name of SSH is Secure Shell. SSH is the security protocol based on the application layer and transport 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. After SSH function is enabled, users can enter the command line configuration interface to manage devices.

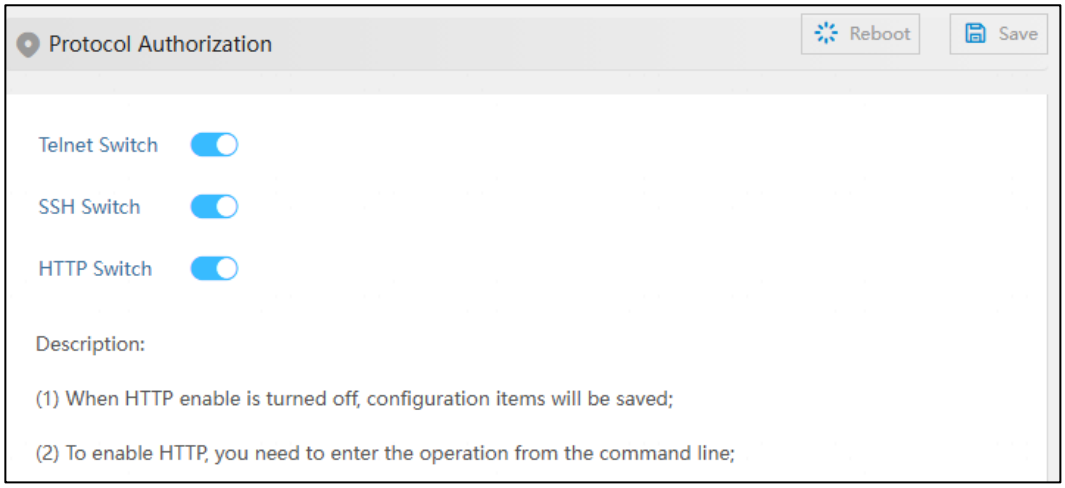
Telnet is the standard protocol and main mode of Internet remote login service. It provides users with the ability to complete the remote host work on the local computer. After the TELNET function is enabled, users can enter the command line configuration interface to manage devices.

Operation Path

Open in the navigation bar: “Login Config > Protocol Authorization”.

Interface Description

Screenshot of protocol authorization interface:



Configuration description of main elements of the protocol interface:

Copyright © 3onedata Co., Ltd.

Interface Element	Description
Telnet Switch	After opening, users can access the command line configuration interface through Ethernet port.
SSH Switch	After opening, users can access the command line configuration interface through Ethernet port.
HTTP Switch	After enabling, users can access the WEB configuration interface via the web page. After being disabled, the WEB configuration interface becomes inaccessible, but it can be re-enabled via the command line.

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

4 Port Configuration

4.1 Port Settings

Function Description

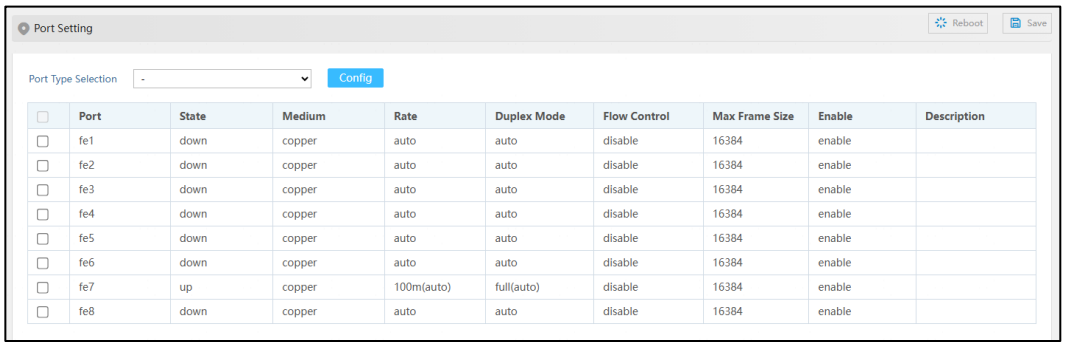
Set port parameters individually or in batches.

Operation Path

Open in order: "Main Menu > Port Config > Port Setting".

Interface Description

Port setting interface is 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: • down: represent the port is disconnected; • up: represent the port is connected.
Medium	Ethernet port connection type, display medium as follows:

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	• copper: copper port • fiber: fiber port
Rate	Ethernet port working speed, optional speed as follows: • auto • 10m • 100m
Duplex Mode	Under current Ethernet working mode, optional mode as follows: • Auto: Auto-negotiation • Full: full duplex • Half: half-duplex
Flow Control	Port flow control status, options as follows: • disable • enable
Max Frame Size	Display the maximum data frame length that the Ethernet port transmitted.
Enable	Enable Ethernet port. Notice: If “disable” is selected, the port won't be connected to use.
Description	Support entering port description of no more than 31 characters.

4.2 Link Aggregation

The link aggregation technology can increase link bandwidth by bundling multiple physical interfaces into one logical interface without hardware upgrade. While increasing the bandwidth, link aggregation adopts the mechanism of backup link, which can effectively improve the reliability of link between devices.

Link aggregation technology has the following three advantages:

- Increase bandwidth

  The maximum bandwidth of link aggregation interface can reach the sum of the bandwidth of each member interface.
- Improve the reliability

  When an active link fails, traffic can be switched to other available member links, thus improving the reliability of link aggregation interface.
- Load sharing

Copyright © 3onedata Co., Ltd.

Within a link aggregation group, load sharing can be achieved on the active links of each member.

Function Description

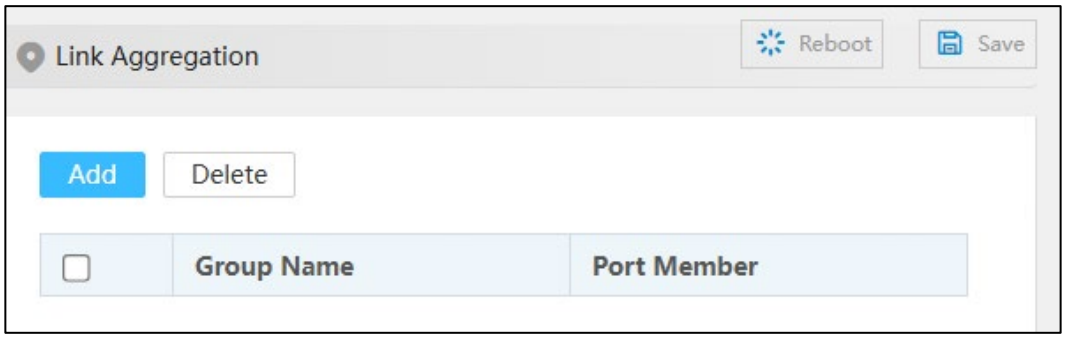
Binding multiple physical ports into one logical channel.

Operation Path

Open in order: “Main Menu > Port Config > Link Aggregation".

Interface Description

Screenshot of Link Aggregation interface:



The main element configuration description of Link Aggregation interface:

Interface Element	Description
Group Name	Aggregation group number, supports two aggregation groups.
Port Member	Ports that join the trunking group.

Note

- The attributes of all member ports in trunking group should be the same, including medium, rate and duplex mode, etc.
- Setting one port as both ring network port and trunking port is not supported.
- One port can only join a trunking group.

Copyright © 3onedata Co., Ltd.

4.3 Port Speed Limit

Function Description

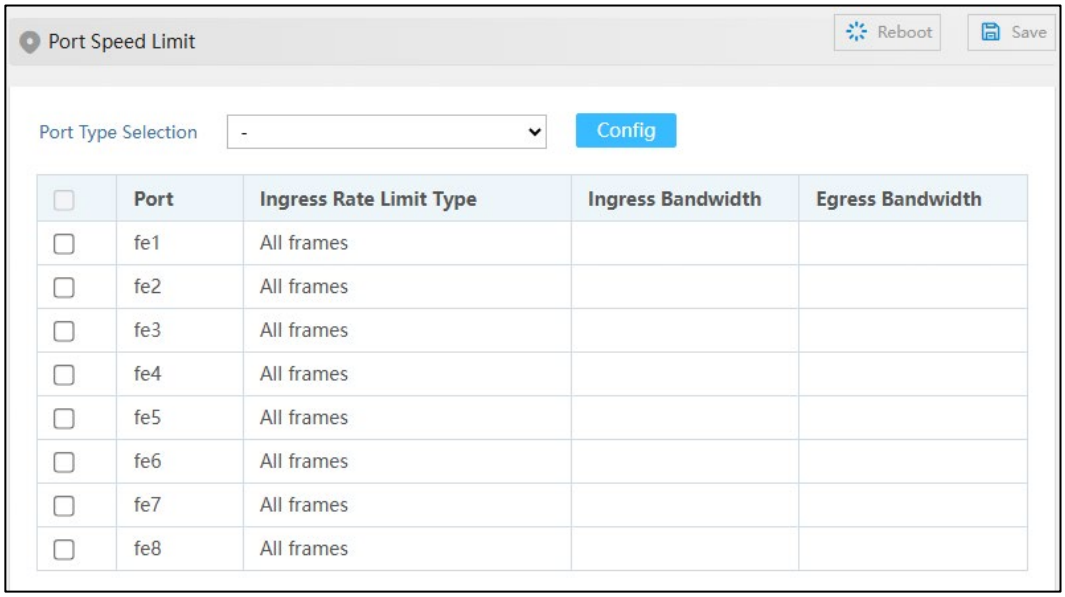
Single or batch limit the ingress bandwidth and egress bandwidth of broadcast, multicast and unicast received by the port.

Operation Path

Open in order: "Main Menu > Port Config > Port Speed Limit".

Interface Description

Port speed limit interface is as follows.



Main elements configuration description of bandwidth management interface:

Interface Element	Description
Port Type Selection	Select the port type, and check the ports of the same type in batches: • 100M port (fe) • 100M fiber port (fx)
☐	Check box, you can check multiple ports for simultaneous configuration.
Port	Port number of the device.
Ingress Rate Limit Type	The data packets type of receiving bandwidth needs to be limited, options of drop-down list as follows: • All frames: all kinds of data packets;

Copyright © 3onedata Co., Ltd.

Ingress Bandwidth	Limit the transmission rate of all ingress data, and select the rate range: • 128/256/512Kbps • 1/2/4/8/16/32/64Mbps
Egress Bandwidth	Limit the transmission rate of all egress data, and select the rate range: • 128/256/512Kbps • 1/2/4/8/16/32/64Mbps


Note

Port speed limit has high requirements on network cable quality. If the cable quality is not up to the standard, lots of conflict packets and broken packet would appear.

4.4 Storm Control

Function Description

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

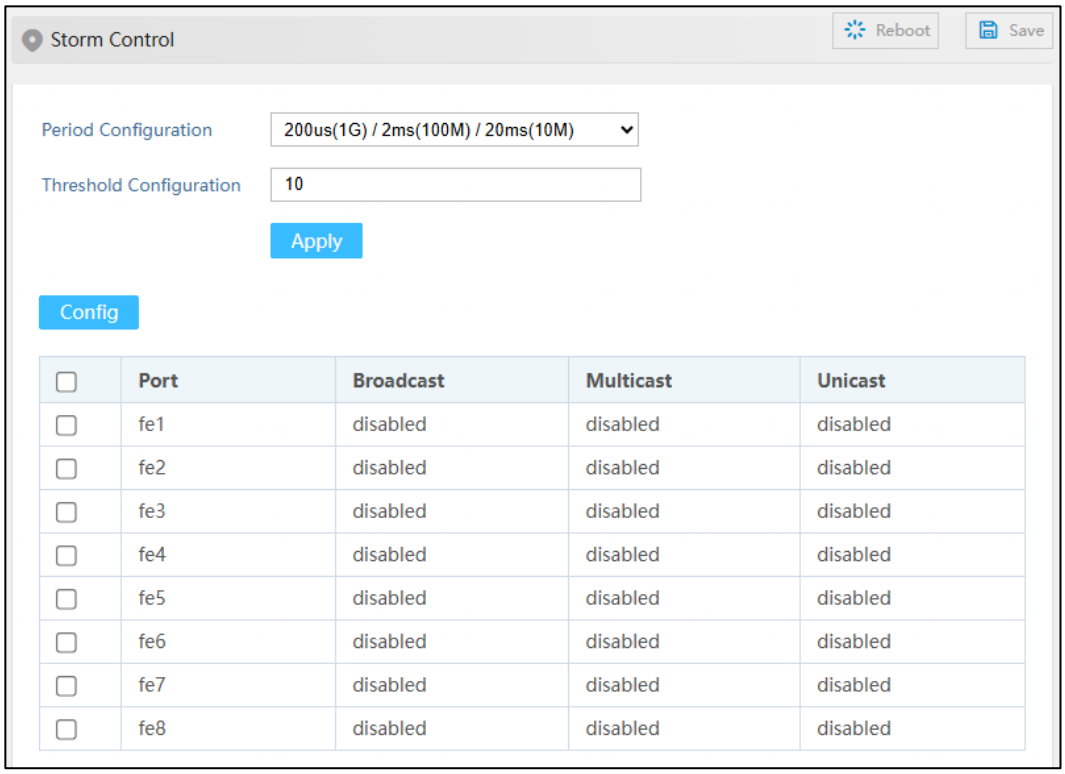
Operation Path

Open in order: "Port Config > Storm Control".

Interface Description

Storm control interface is as follows:

Copyright © 3onedata Co., Ltd.



Main elements configuration description of storm control interface:

Interface Element	Description
Period Configuration	The detection period of different bandwidth ports for broadcasting, unknown multicast or unknown unicast can be selected as follows: • 200us (1G) / 2ms (100M) / 20ms (10M) • 1ms (1G) / 10ms (100M) / 100ms (10M) • 10ms (1G) / 10ms (100M) / 10ms (10M) • 100ms (1G) / 100ms (100M) / 100ms (10M)
Threshold Configuration	The limit number of detected broadcasts, unknown multicasts or unknown unicasts in a specified period, with a value range of 1-255; When the storm suppression threshold is exceeded, the exceeded message will be discarded.
Port	Port number.
Broadcast	Enabled state of broadcast suppression. • enable • disabled
Multicast	Enabled state of unknown multicast suppression. • enable • disabled

Copyright © 3onedata Co., Ltd.

Interface Element	Description
Unicast	Enabled state of unknown unicast suppression. • enable • disabled

4.5 Port Mirroring

Function Description

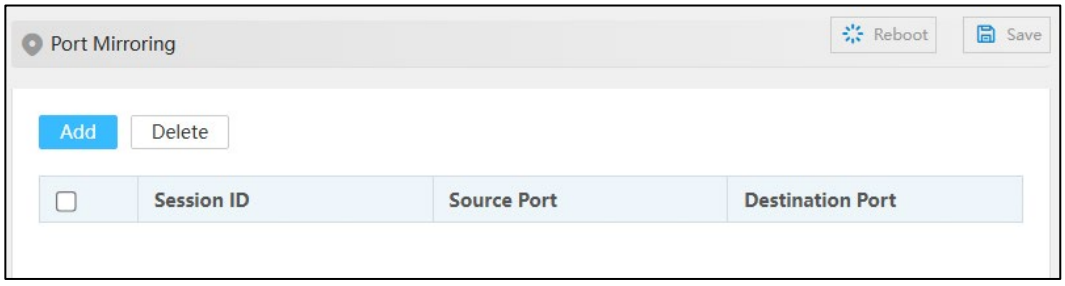
Copy the data from the source port to the appointed port for analysis and monitoring.

Operation Path

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

Interface Description

Port mirroring interface is as follows:



The main element configuration description of port mirror interface:

Interface Element	Description
Session ID	Device mirror ID number, value is 1. Note: Support only 1 mirror session. If mirroring is configured multiple times, only the data of the last configuration will be retained.
Source Port	Monitored ports, from which the device will collect input or output messages. There can be one or more mirror ports.
Destination Port	Monitoring port, used to copy and analyze messages from source port.
Add	Click “Add” to reconfigure the mirror and configure the data direction of the mirror. Data direction options are as follows:

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	• transmit tx: egress data, the message sent by the source port will be mirrored to the destination port; • receive rx: ingress data, the message received by the source port will be mirrored to the destination port; • Both: all data, mirror the source port receiving and sending packets at the same time.

4.6 Port Statistics

4.6.1 Port Statistics-Overview

Function Description

Check the data information of each port:

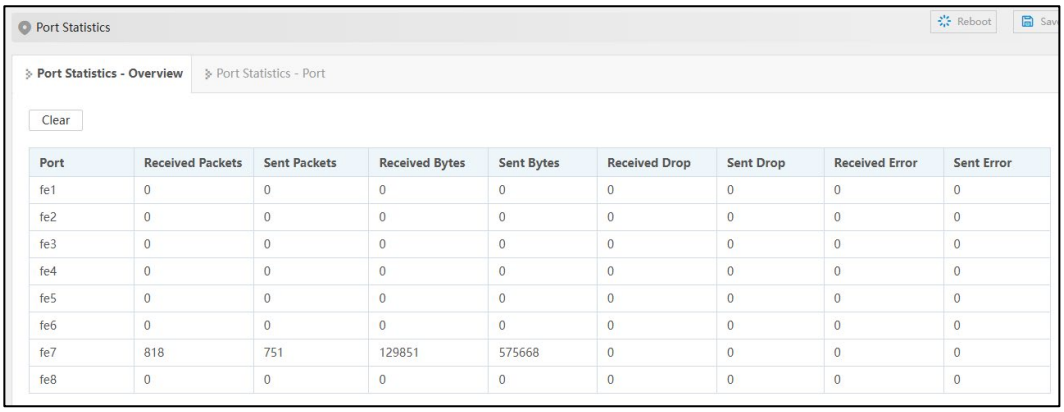
- Number of messages sent and received and number of message bytes
- Number of dropped and error messages

Operation Path

Open in order: "Port Config > Port Statistics > Port Statistics-Overview".

Interface Description

Port Statistics-Overview interface is as follows:



Port	Received Packets	Sent Packets	Received Bytes	Sent Bytes	Received Drop	Sent Drop	Received Error	Sent Error
fe1	0	0	0	0	0	0	0	0
fe2	0	0	0	0	0	0	0	0
fe3	0	0	0	0	0	0	0	0
fe4	0	0	0	0	0	0	0	0
fe5	0	0	0	0	0	0	0	0
fe6	0	0	0	0	0	0	0	0
fe7	818	751	129851	575668	0	0	0	0
fe8	0	0	0	0	0	0	0	0

Copyright © 3onedata Co., Ltd.

4.6.2 Port Statistics-Port

Function Description

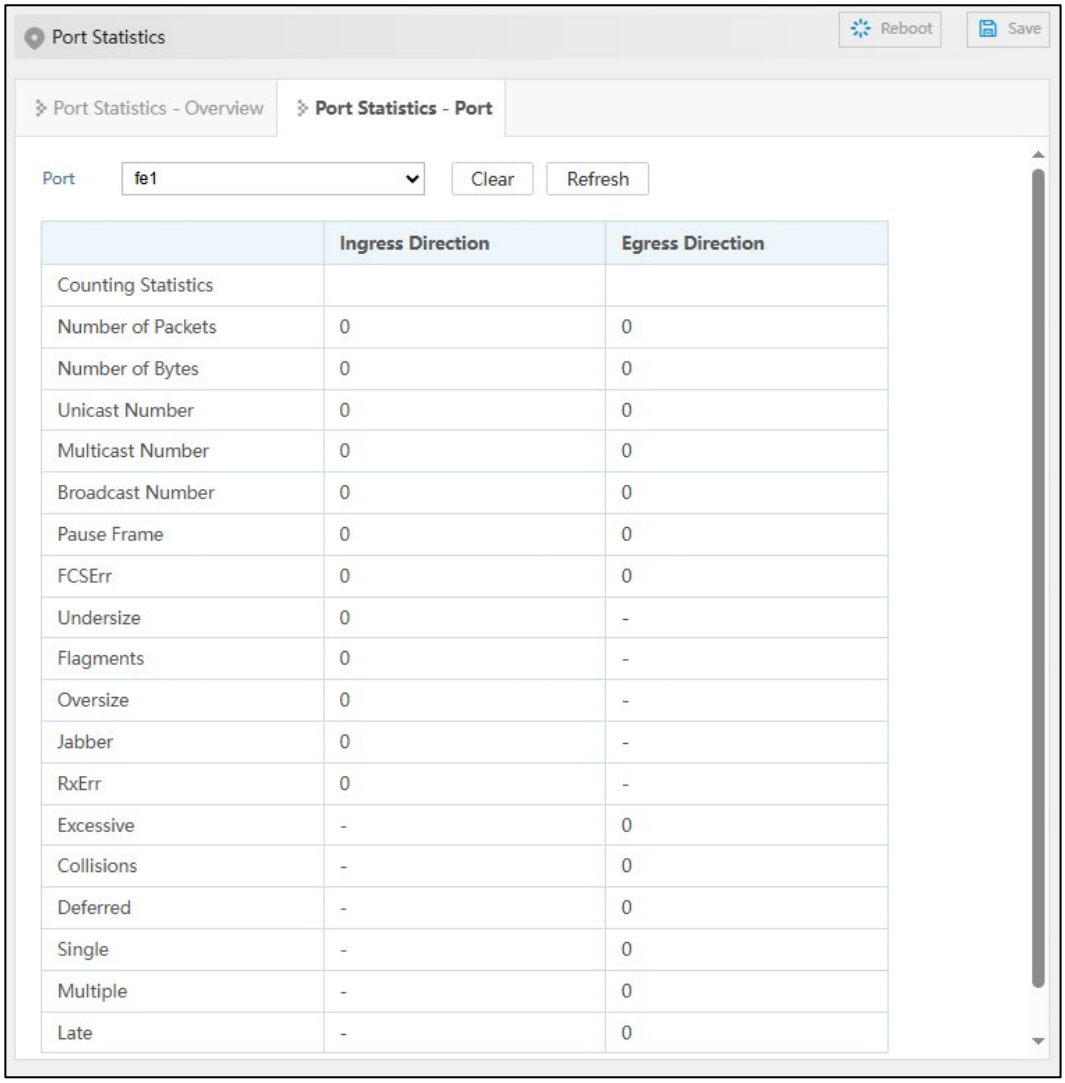
Check the classification statistics of the total number of messages sent and received by the designated port and the number of bytes of messages.

Operation Path

Open in order: "Port Config > Port Statistics > Port Statistics-Port".

Interface Description

Port Statistics-Port interface is as follows:



	Ingress Direction	Egress Direction
Counting Statistics		
Number of Packets	0	0
Number of Bytes	0	0
Unicast Number	0	0
Multicast Number	0	0
Broadcast Number	0	0
Pause Frame	0	0
FCSErr	0	0
Undersize	0	-
Flagments	0	-
Oversize	0	-
Jabber	0	-
RxErr	0	-
Excessive	-	0
Collisions	-	0
Deferred	-	0
Single	-	0
Multiple	-	0
Late	-	0

Copyright © 3onedata Co., Ltd.

5 Layer 2 Configuration

5.1 VLAN Configuration

VLAN (Virtual Local Area Network) is a communication technology that logically divides a physical LAN into multiple broadcast domains. Hosts in VLAN can directly communicate with each other, but two VLAN can't directly communicate with each other, which can limit the broadcast message in a VLAN. Using VLAN can bring following benefits to users.

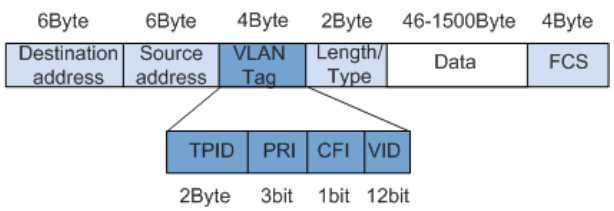
- Limit the broadcast domain;
- Increase the security of LAN;
- Improve the network stability;
- Flexiblely construct virtual working team.

Port VLAN

Port VLAN adopts different identifications to distinguish different VLAN. Adopting the same ID identification will cause internal member groups being replaced, new ID identification will establish new forwarding rules, and all ports must belong to one or more VLAN.

IEEE802.1Q VLAN

Under the provisions of IEEE 802.1Q protocol, the device can add 4 bytes VLAN tag (Tag for short) between Source address and Length/Type fields of Ethernet data frame, identifying the VLAN information. As the picture below.



Copyright © 3onedata Co., Ltd.

- TPID: Tag Protocol Identifier represents the data frame type, when the value is 0x8100, it represents the VLAN data frame of IEEE 802.1Q.
- PRI: Priority represents the 802.1p priority of data frame. The value ranges from 0 to 7. A larger value indicates a higher priority. During network congestion, the switch will preferentially send data frame with higher priority.
- CFI: Canonical Format Indicator represents whether MAC address is packaged in standard format in different transmission media. 0 represents that MAC address is packaged in standard format.
- VID: VLAN ID represents the VLAN number of the data frame. The value range of VLAN ID is 0-4095. 0 and 4095 are reserved values of the protocol, so the valid value range of VLAN ID is 1-4094.

5.1.1 Global Configuration

Function Description

Global Configuration could realize:

- Set VLAN type
- Set the PVID of CUP
- Set the default PVID of the port
- Set port type

Operation Path

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

Interface Description 1: Port-based VLAN

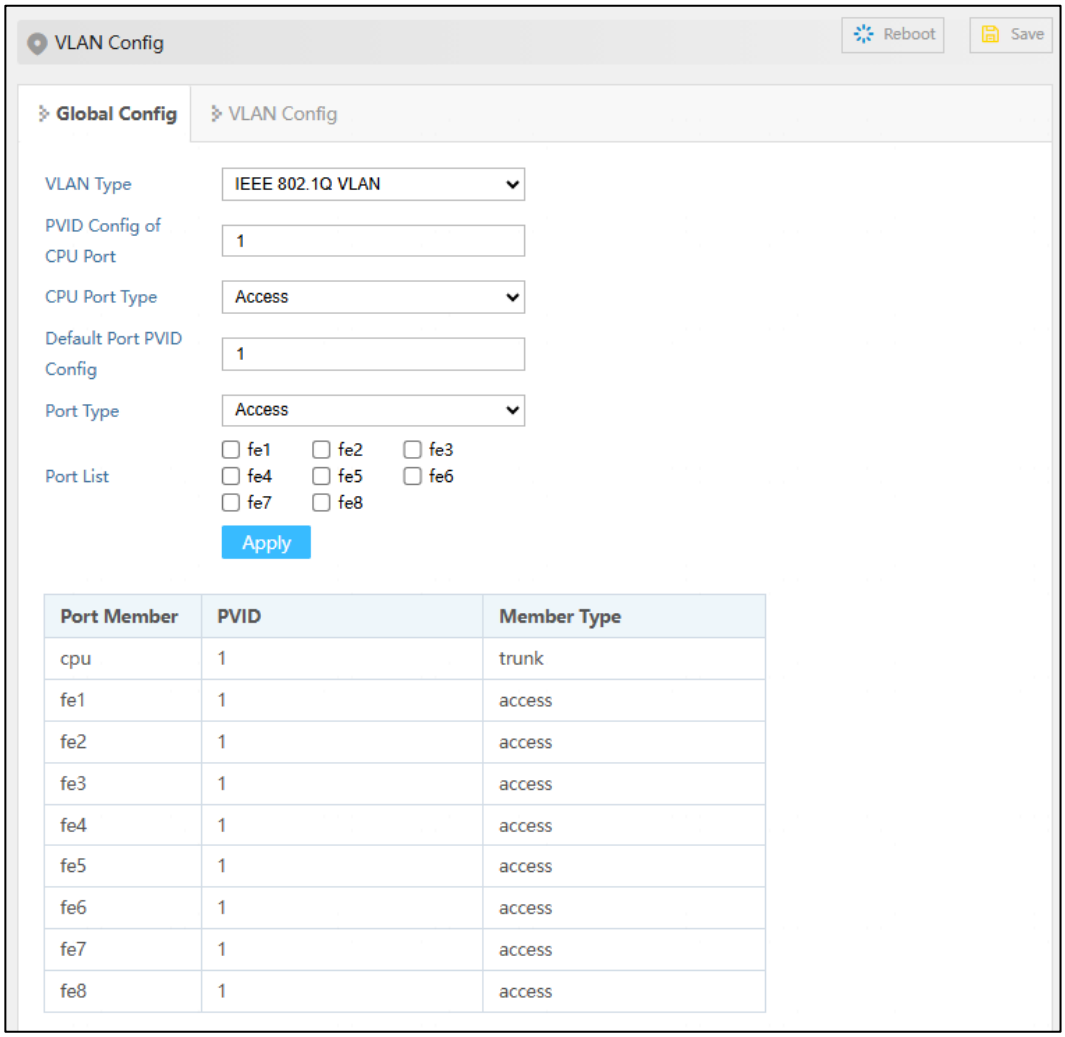
Port-based VLAN interface is as follows:



Interface Description: 802.1Q VLAN

Interface screenshot of 802.1Q VLAN:

Copyright © 3onedata Co., Ltd.



The main element configuration description of global configuration interface:

Interface Element	Description
VLAN Type	VLAN can be configured in two types: • Port-based VLAN • 802.1Q VLAN
PVID Config of CPU port	The default configuration is 1, and the optional range is 1-4094.
CPU Port Type	Configure the link type of CPU port, there are two types as follows: • Access: The message entering the switch from the Access port, which is forced to use the PVID of the port as the VLAN ID. • Trunk: the message entering the switch from Trunk port. If there is already a VLAN TAG, use the VLAN ID in the VLAN TAG of the message;

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	Otherwise, use the PVID of this port as VLAN ID.
Default Port PVID Config	The default configuration is 1, and the optional range is 1-4094.
Port Type	Configure the link type of port, there are two types as follows: • Access: The message entering the switch from the Access port, which is forced to use the PVID of the port as the VLAN ID. • Trunk: the message entering the switch from Trunk port. If there is already a VLAN TAG, use the VLAN ID in the VLAN TAG of the message; Otherwise, use the PVID of this port as VLAN ID.
Port List	Device port number check box to configure the port type of the selected port in batch.

5.1.2 VLAN Configuration

Function Description

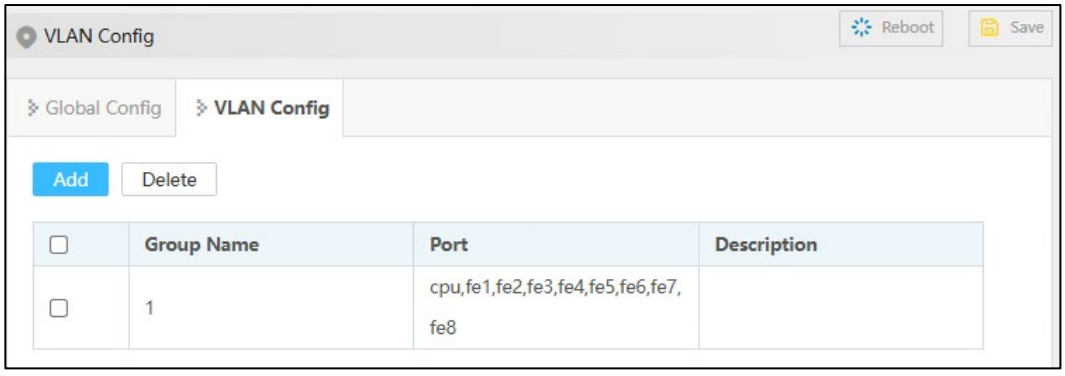
Add VLAN based on port or 802.1Q.

Operation Path

Open in order: "Layer 2 Config > VLAN > VLAN Config".

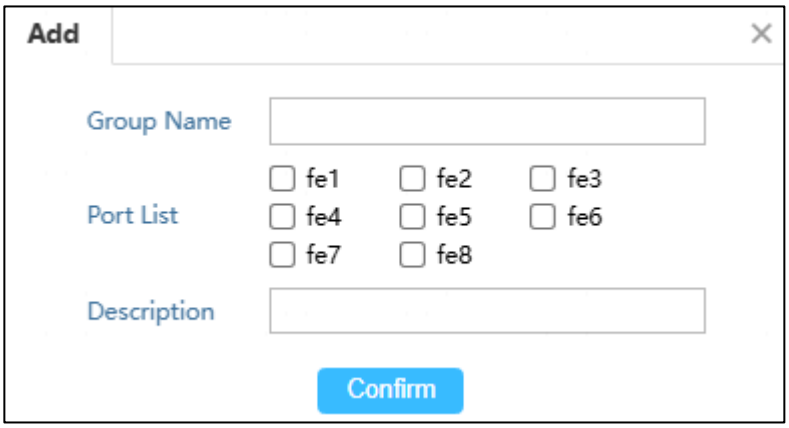
Interface Description: View VLAN Configuration

View port-based VLAN interface screenshot:



Copyright © 3onedata Co., Ltd.

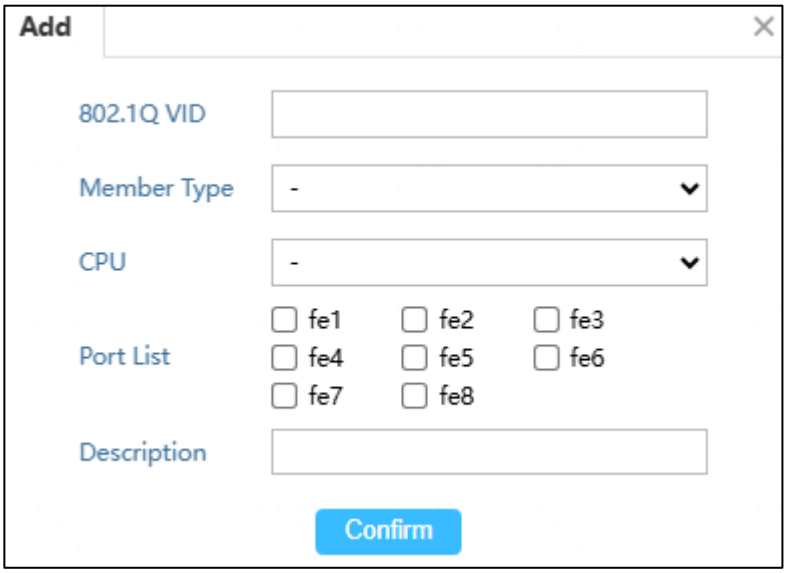
Interface Description: Add Port-based VLAN



Configuration instructions for adding port-based VLAN key elements:

Interface Element	Description
Group Name	VLAN group name, ranging from 1 to 4094 bytes.
Port List	The device port number check box can be used to configure the port type of the selected port in batch.
Description	Support entering a VLAN description with a maximum of 31 characters.

Interface Description: Add 802.1Q-based VLAN



The main element configuration description of Add 802.1Q-based VLAN interface:

Copyright © 3onedata Co., Ltd.

Interface Element	Description
802.1Q VID	Enter the ID to add the VALN. Note: If the VLAN ID already exists, the original VLAN ID configuration will be overwritten after saving.
Member Type	There are three types of “VLAN ID” for data frames sent out by the port: • Unmodified: when the data frame is sent out from the port, it will recover the “VLAN ID” of accessing to the switch. • Untagged: remove the “VLAN ID” fields when the data frame is sent out from the port, • Tagged: reserve “VLAN ID” fields when the data frame is sent out from the port.
CPU	There are three types of “VLAN ID” for data frames sent out by CPU: • Unmodified: when the data frame is sent to CPU, it will recover the “VLAN ID” of accessing to the switch. • Untagged: remove the “VLAN ID” fields when the data frame is sent to CPU, • Tagged: reserve “VLAN ID” fields when the data frame is sent to CPU.
Port List	The device port number check box can be used to configure the port type of the selected port in batch.
Description	Support entering a VLAN description with a maximum of 31 characters.

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.

Copyright © 3onedata Co., Ltd.

5.2.1 MAC Address Table

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

Function Description

View the MAC address, including:

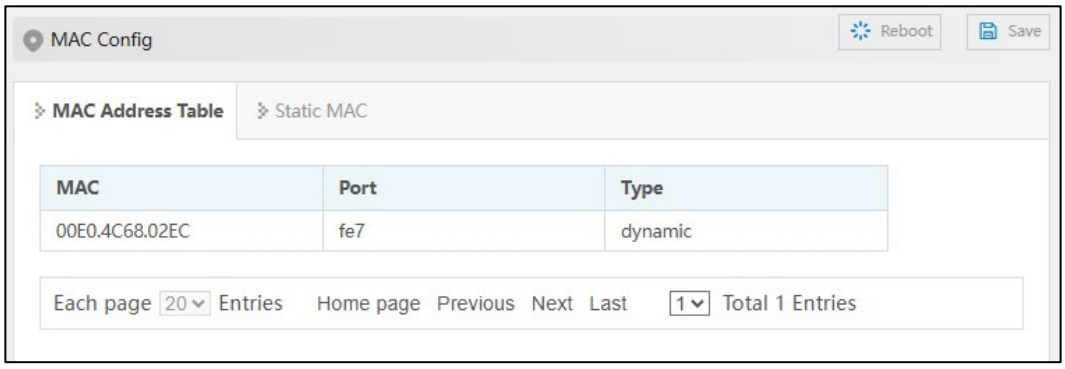
- The data source MAC of the access device learned by the device
- Static unicast MAC

Operation Path

Open in order: "Layer-2 Config > MAC > MAC Address Table".

Interface Description

MAC address table interface is as follows:



Main elements configuration description of MAC address table interface:

Interface Element	Description
MAC	The dynamic MAC that the device has learned or the static unicast or multicast MAC that user has configured.
Port	Access the port number of the source data of the corresponding MAC address.
Type	The type of MAC address, it displays as follows:

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	• Dynamic: dynamic MAC address; • Static: static MAC address.

5.2.2 Static MAC

Function Description

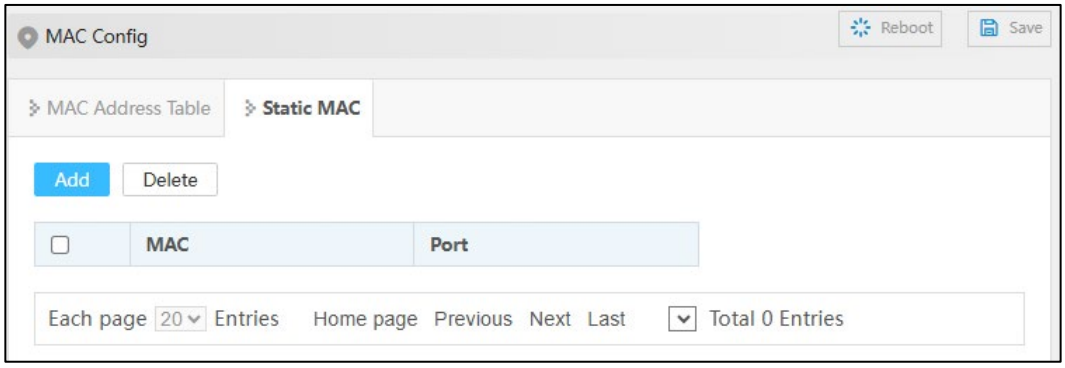
Support manual binding of unicast MAC addresses. The unicast address after binding is static MAC, which will not age.

Operation Path

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

Interface Description

Static MAC interface is as follows:



The main element configuration description of static MAC interface:

Interface Element	Description
MAC	Fill in the unicast MAC address that needs to bind the interface, such as 0001.0001.0001.
Port	The Binding Port Number.

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;

Copyright © 3onedata Co., Ltd.

- Please don't adopt multicast address as the entering address;
- Please don't enter reserved MAC address, such as the local MAC address.

5.3 Spanning Tree

Notice

Spanning tree and Ring cannot be enabled at the same time. Please disable the enable switch of the Ring before setting the spanning tree.

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

- STP (Spanning Tree Protocol)
- RSTP (Rapid Spanning Tree Protocol);

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.

5.3.1 Global Configuration

Function Description

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

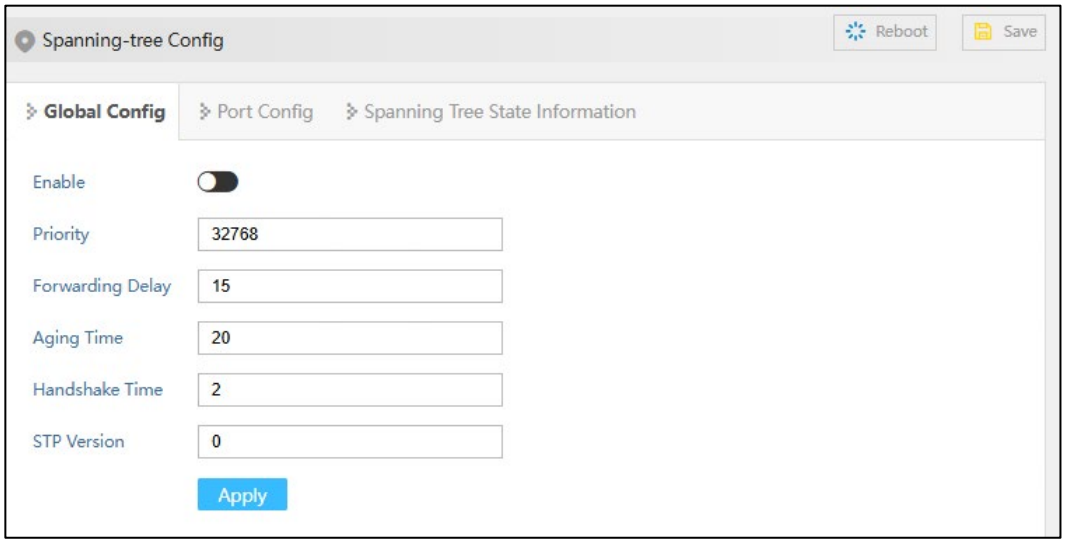
Operation Path

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

Interface Description

Global configuration interface is as follows:

Copyright © 3onedata Co., Ltd.



The main element configuration description of global configuration interface:

Interface Element	Description
Enable	Spanning-tree enable switch. Disable by default
Priority	Bridge priority level, defaults to 32768, value range is 0-61440. Note: Smaller the priority level value is, higher the priority level is.
Forwarding Delay	Port state transition delay, defaults to 15S, the value range is 4-30.
Aging Time	The maximum lifetime of the message in the device, defaults to 20S, the value range is 6-40. It's used to determine whether the configuration message times out.
Handshake Time	Message sending cycle, defaults to 2S, the value range is 1-10. Note: The spanning tree protocol sends configuration information every Hello time to check whether the link is faulty.
STP version	STP revision level, defaults to 0, the value range is 0-1. • 0 means STP Spanning Tree Protocol. • 1 means RSTP (Rapid Spanning Tree Protocol)

Copyright © 3onedata Co., Ltd.

5.3.2 Port Configuration

Function Description

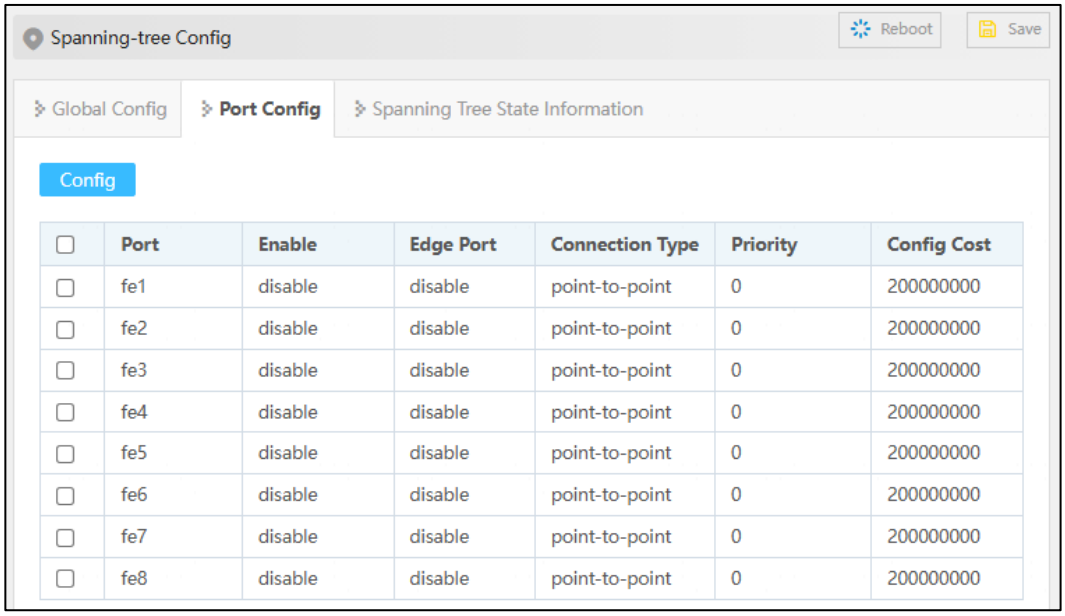
On the "Port Configuration" page, users can enable ports to participate in spanning tree and configure port connection type, path cost, priority, and other attributes.

Operation Path

Open in order: "Layer 2 Configuration > Spanning-tree > 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.
Enable	Status of participating in spanning tree enable switch.
Edge Port	Remote port enable switch: • Enable: participate in spanning-tree; • Disable: not participate in spanning-tree.
Connection Type	Select port link type: • Auto: Automatic system detection • Point-to-point: Point-to-point link is the connection

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	between switches. • Shared: Non-point-to-point link is the connection between switch and hub.
Priority	Port priority, optional values are: 0/16/32/48/64/80/96/112/128/144/160/176/192/208/224/240. Note: Port priority level in bridge, port priority level is higher when the value is smaller. The higher the priority of the port, the more likely it is to be a root port.
Config Cost	The path cost from network bridge to root bridge, defaults to 200000000. Value range: 1-200000000.

5.3.3 State Information of Spanning Tree

Function Description

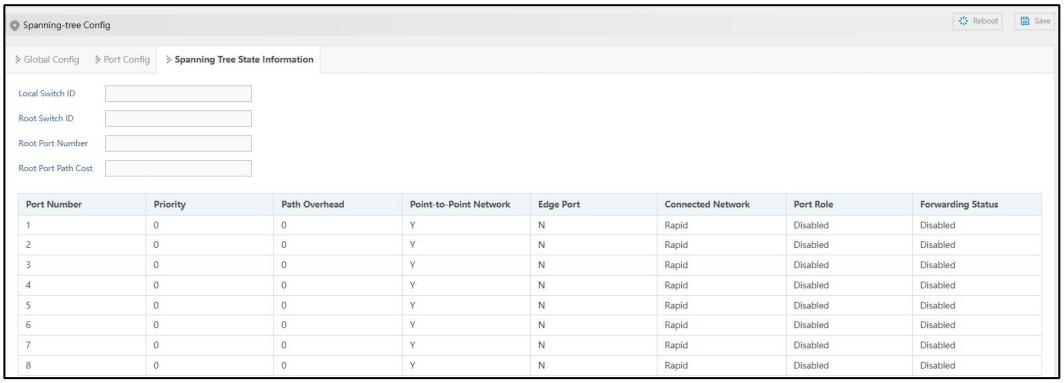
Display information about the root switch and this switch in the spanning tree.

Operation Path

Open in order: "Layer-2 Config > Spanning-tree > Spanning Tree State Information".

Interface Description

The State Information of Spanning Tree interface is as follows:



The main element configuration description of RSTP status interface:

Interface Element	Description
Local Switch ID	It displays the priority of this switch and MAC address information ID.
Root Switch ID	It displays the priority of the root switch and MAC address

Copyright © 3onedata Co., Ltd.

	information ID.
Root Port Number	The port of the switch, which is not in the root bridge but nearest to it, oversees communicating with the root bridge. The path cost from this port to the root bridge is the lowest. When the path costs of multiple ports are the same, the one with the highest priority would be the root port.
Root Port Path Cost	The root cost of a switch is the sum of root port cost and the root cost that data packet goes through all switches. The root cost of root bridge is zero.
Port Number	Display the device port number.
Priority	The priority of ports in network bridge. The values range from 0 to 240. The smaller the value, the higher the port priority. The higher the priority of the port, the more likely it is to be a root port.
Path Overhead	The path cost from network bridge to root bridge.
Point-to-Point Network	The directly connected switch port.
Edge Port	The port that directly connects to terminal instead of other switches.
Connected Network	It displays the network protocol of devices with connected ports.
Port Role	Root port, specified port, Alternate port and Backup port.
Forwarding Status	It is divided by whether the port forwards user flow and learns MAC address. • Discarding: neither forward user flow nor learn MAC address; • Learning: doesn't forward user flow but learn MAC address; • Forwarding: forward user flow and learn MAC address; • Listening: neither forward user flow nor learn MAC address; but can receive and send configuration message; • Blocking: port only receives and processes BPDU, doesn't forward user flow; • Disabled: blocked or physically disconnected.

Copyright © 3onedata Co., Ltd.

5.4 Ring

Notice

Spanning tree and Ring cannot be enabled at the same time. Please disable the enable switch of spanning tree before setting the Ring.

Ring is an Ethernet Ring network algorithm developed and designed by the company for highly reliable industrial control network applications that require link redundancy backup. Features in Ethernet link redundancy, fast automatic recovery. Ring adopts no master station design. In a multi-ring network of up to 250 switches, the network self-recovery time is less than 20 milliseconds. Each port in this series of switches can be used as a ring port and connected with other switches. When an interruption occurs in the network connection, the SW-Ring redundant mechanism enables the backup link to quickly recover the network communication.

Function Description

Quickly configure Ring network.

Operation Path

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

Interface Description

Ring config interface is as follows:



The main element configuration description of Ring config interface:

Interface Element	Description
Enable	Enable switch, slide to the right to enable the Ring ring network function.
Ring Group	Support ring group 1/2, it can create 2 ring networks at the

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	same time.
Ring ID	When multiple switches form a ring, the current ring ID would be network ID. Different ring network has different ID. Value range is 0-255. Note: The ring network identification must remain the same in one ring network.
Ring Port 1	The network port 1 on the switch device used to form the ring network. Note: When the ring network type is "Couple", port 1 is the "Coupled Port". Coupling port is the port that connects different network identities.
Port1 Status	The current state of Port 1. • block • forward
Ring Port 2	The network port 2 on the switch device used to form the ring network. Note: • When the ring network type is “Couple”, port 2 is the “console port”. Console port is the port in the chain where two rings intersect. • “Port 1” and “Port 2” cannot be set to the same port, and the port number it sets must be the same as it connects without sequential order.
Port2 Status	The current state of Port 2. • block • forward
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: Two adjacent rings share a switch; users can carry the same switch 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

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	the ring port, CPU sends query packet to adjacent device for confirming the connection is normal or not. Input range is 0~100. Note: When the Hello Time value is 0, it means that no inquiry packet is sent.
Master-slave	Single loop network supports no-master station structure and one-master multi-slave structure. • When all the single-loop devices are slave stations, the single-loop structure is no-master station. • When a single ring device is a master and multiple slave station, one device can be designated as the master device and the other devices as the slave device. One end of the main device of the ring network is the backup link. When the ring network fails, the backup link is enabled from the master station to ensure the normal operation of the network.
Heartbeat	Heartbeat detection mechanism. When this configuration is enabled, the network association will periodically send heartbeat messages to detect whether the corresponding devices are in live state, thus enhancing the reliability of the network. Configurable: • Enable • Disable

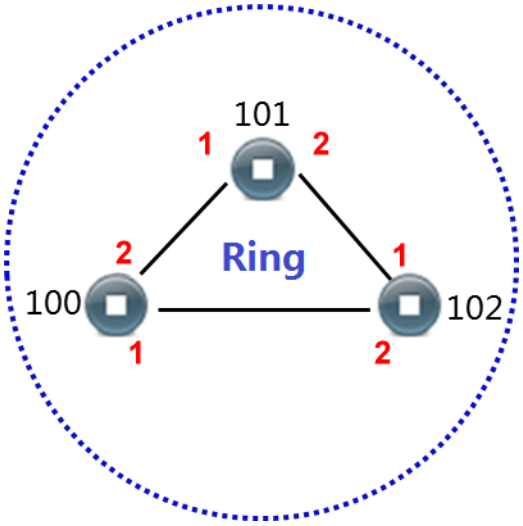
Notice

- The port that has been set to port trunking could not be set as rapid ring port. One port can't belong to multiple ring networks.
- The ID in the same single ring must be the same; otherwise, it cannot form a ring and achieve normal communication.
- To ensure the communication of ring network, it's recommended to set the "Type" of ports that have already been set as ring network to "Trunk" and "member relationship" to "Tagged".
- When forming complicated ring networks like tangent ring, please make sure the ID conforms to the unity of single ring network ID. Network ID of different single ring must be different.

Copyright © 3onedata Co., Ltd.

5.4.1 Instance: create single ring

For example: create the following single ring:



Instance Analysis

The ring ports of Device 100, 101, and 102 are port 1 and port 2. Therefore, creating single ring is viable. Port 1 and port 2 are set as the ring ports of each device.

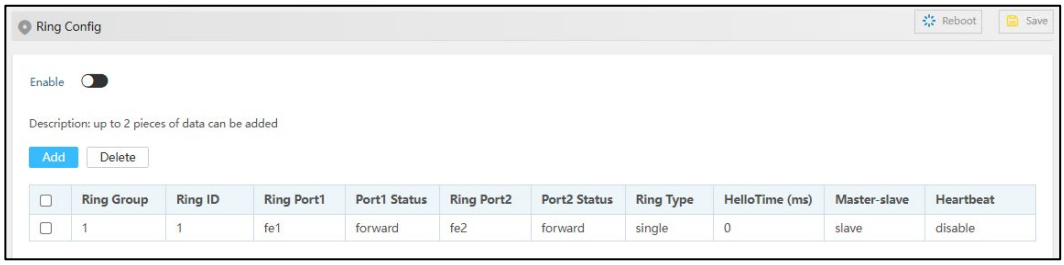
Operation Steps

Configuring Device 100, 101 and 102 in the following steps:

Step 1 Select “Layer 2 Config > Ring Configuration”.

Step 2 Turn on the “Enable switch”.

Step 3 Enter “1” into the “ID” textbox of “Group 1”.



Step 4 Set “Port 1” as “fe1” and “Port 2” as “fe2” separately.

Note:

“Port 1” and “Port 2” cannot be set to the same port.

Step 5 Choose “Single” in the drop-down list of “Type” of “Group 1”.

Step 6 Enter “0” into the “HelloTime” textbox of “Group 1”.

Copyright © 3onedata Co., Ltd.

Step 7 (For Device 100 and 101) Choose “Slave” in the drop-down list of “Master-slave” of “Group 1”.

Step 8 (For Device 102) Choose “Master” in the drop-down list of “Master-slave” of “Group 1”.

Step 9 Click “OK”.

Step 10 End.

5.5 IGMP Snooping Configuration

IGMP Snooping (Internet Group Management Protocol Snooping) is a kind of IPv4 layer-2 multicast protocol. It maintains the outgoing information of multicast messages by snooping the multicast protocol messages transmitted between layer 3 multicast device and user host, to manage and control the forwarding of multicast data messages in data link layer.

After configuring IGMP Snooping, layer 2 multicast device can snoop and analyze the IGMP message between multicast user and upstream router, and create layer 2 multicast forwarding entries based on this information to control multicast data message forwarding. This prevents multicast data from being broadcast in the layer 2 network.

The ways of IGMP Snooping processing different messages:

- IGMP universal group query message: IGMP universal group query message is sent periodically to all hosts and routers in the local network segment to query which multicast group members are in the network segment.
- IGMP report message: the member receives the IGMP universal group query message and responds by the IGMP report message. The member actively sends an IGMP report message to the IGMP query to declare joining the multicast group.
- IGMP leave message: a member running IGMPv2 sends an IGMP leave message to notify the IGMP query that it has left a multicast group.

5.5.1 Global Configuration

Function Description

Enable/disable IGMP Snooping.

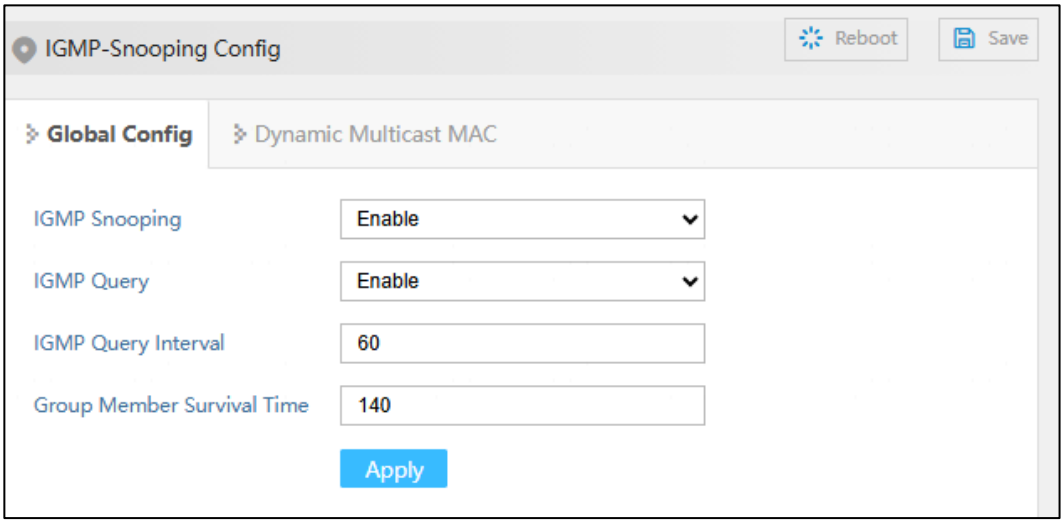
Copyright © 3onedata Co., Ltd.

Operation Path

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

Interface Description

Global configuration interface is as follows:



The main element configuration description of IGMP Snooping interface:

Interface Element	Description
IGMP Snooping	The switch of IGMP snooping function, options are: • Enable; • Disable. Note: IGMP snooping means snooping the messages between user host and router, as well as tracking multicast information and the ports that have been applied for.
IGMP Query	The switch of IGMP query, options are: • Enable; • Disable. Note: IGMP query means that router inquiring all hosts in subnet if they join some multicast groups.
IGMP Query Interval	IGMP query interval, unit: second. Note: The time range that can be entered is 60~300s.
Group Member Survival Time	The maximum time that multicast members in device can survive from existence to not receiving any response. Unit: second. Note:

Copyright © 3onedata Co., Ltd.

	• IGMP snooping needs to be enabled before using this function. • The time range of group survival that can be set is 140-8960s, a multiple of 70.

Note

- You need to set multicast source and port in one VLAN first to enable IGMP Snooping function.
- Multiple IGMP inquirers should be avoided in network lest cause waste of resources. Please choose all ports if the forwarding relationship of unknown multicast group is uncertain.

5.5.2 Static Multicast MAC

Function Description

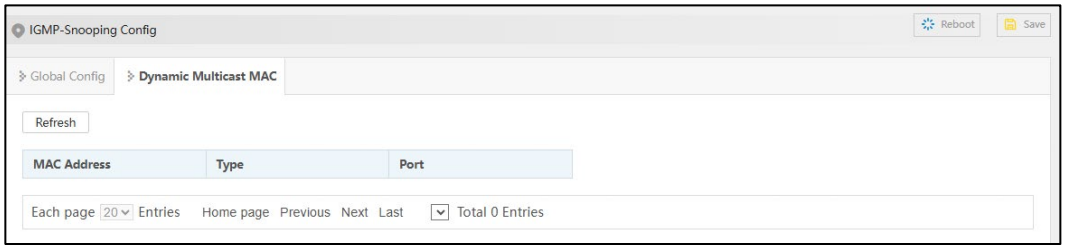
Display the dynamic multicast information received by the device interface.

Operation Path

Open in order: "Layer-2 Config > IGMP-Snooping > Dynamic Multicast MAC".

Interface Description

The Dynamic Multicast MAC interface is as follows:



Main element configuration description of multicast group information interface:

Interface Element	Description
MAC Address	The multicast address received by the interface.
Type	Multicast type:

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	• dynamic • static
Port	Ethernet port.

5.6 Port Loopback Detection

Function Description

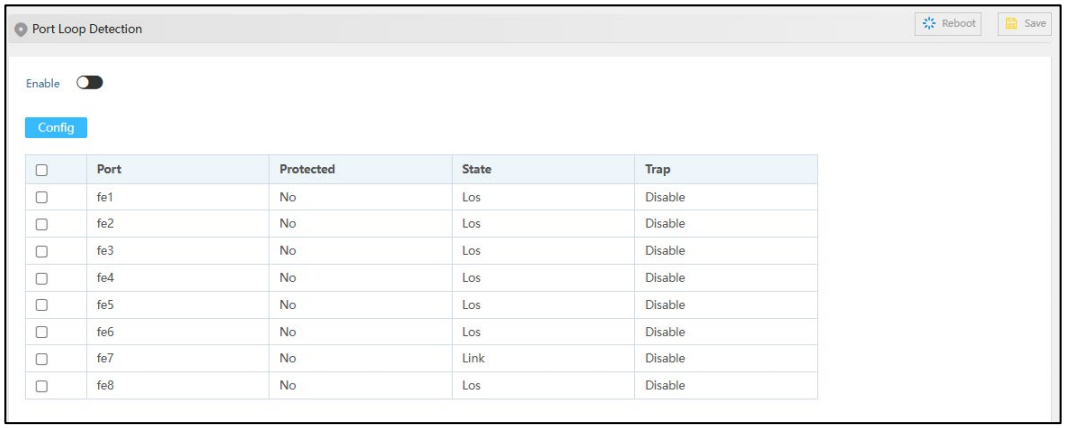
Loop protection can be configured to avoid ring network storm.

Operation Path

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

Interface Description

Screenshot of Port Loopback Detection interface:



Main elements configuration descriptions of Loop Protection interface:

Interface Element	Description
Enable	Enable or disable port loop detection.
Port	Displays the port number of the device.
Protected	The state of the port protected by a loop. After enabled, when there is a port self-loop or a port loop, the loop can be quickly disconnected, and the port status can be set to blocking or forwarding to avoid network storms. Notice: The loop port cannot be set as a loop detection port.

Copyright © 3onedata Co., Ltd.

State	The connection status of this port, values are: • Los: the port is physically disconnected • Link: The port is not looped and the port is connected. • Block: The port is enabled with loop protection function, and the loop has been detected, so it has entered the protection state. • Forward: The port is connected; loop protection is enabled and no loop is detected.
Trap	The Trap switch is used to send or not send Trap information when the port loop is detected. The options are: • Enable • Disable

5.7 ERPS

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

5.7.1 Timer Configuration

Function Description

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

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

- WTR timer

Copyright © 3onedata Co., Ltd.

If an RPL owner port is unblocked due to a link or node fault, the involved port may not go Up immediately after the link or node recovers. Blocking the RPL owner port may cause network flapping. To prevent this problem, the node where the RPL owner port resides starts the wait to restore (WTR) timer after receiving a RAPS (NR) message. The WTR Timer will be turned off if SF (Signal Fail) RAPS messages are received from other ports before the timer expires. If the node does not receive any RAPS (SF) message before the timer expires, it blocks the RPL owner port when the timer expires and sends NR-RB (RPL Block, RPL) RAPS message. After receiving this RAPS (NR, RB) message, the nodes set their recovered ports on the ring to the Forwarding state.

- Guard timer

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

- Hold Timer

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

Operation Path

Open in order: "Layer-2 Config > ERPS > Timer Config".

Interface Description

Timer configuration interface is as follows:

Copyright © 3onedata Co., Ltd.



Main elements configuration description of timer configuration interface:

Interface Element	Description
Timer Name	The name of ERPS timer, which supports 1-31 characters and consists of uppercase letters, lowercase letters, numbers, or special characters (! @ _-).
WTR	WTR timer, value range is 1-12, unit: minute.
WTB	WTB timer, value range is 1-12, unit: minute.
Guard timer	Guard timer, its value range is 10-200, unit: ms.
Hold Timer	Hold timer, value range is 0-10, unit: minute.
Reversible	ERPS reversible mode status, options as follows: • enable If the failed link recovers, the RPL owner port will be blocked again after waiting for WTR time. Blocked links are switched back to RPL. • disable If the failed link recovers, the WTR timer is not started, and the original faulty link is still blocked and will be switched to RPL.

5.7.2 Ring Configuration

Function Description

Configure ERPS ring port.

Operation Path

Open in order: "Layer-2 Config > ERPS > Ring Network Config".

Interface Description

Ring configuration interface is as follows:

Copyright © 3onedata Co., Ltd.



The main element configuration description of ring configuration interface:

Interface Element	Description
Ring Name	The name of ERPS ring network, which supports 1-32 characters, consists of uppercase letters, lowercase letters, numbers, or special characters (! @ _-).
eastinterface	ERPS ring port.
westinterface	ERPS ring port. Notice: • ERPS ring ports can be normal physical ports. • ERPS ring ports cannot be enabled with other Layer 2 ring network protocols at the same time. • ERPS ring ports can't be the same ports. • ERPS ring ports must be trunk ports and allow the ring instance VLAN to pass.

5.7.3 Instance Configuration

Function Description

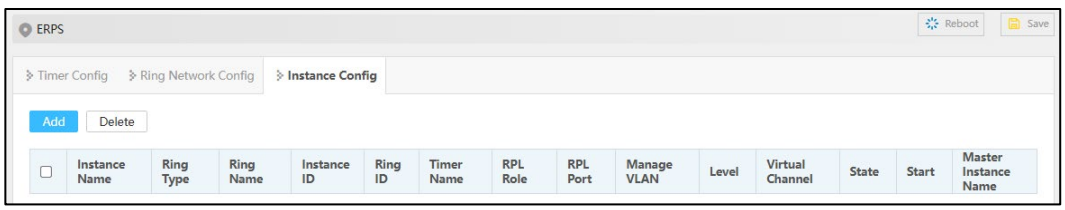
Configure ERPS ring network instance.

Operation Path

Open in order: "Layer-2 Config >ERPS > Instance Config".

Interface Description

Instance configuration interface is as follows:



Copyright © 3onedata Co., Ltd.

The main element configuration description of instance configuration interface:

Interface Element	Description
Instance Name	The name of the ERPS instance, which supports 1-32 characters, consists of uppercase letters, lowercase letters, numbers, or special characters (! @ _-).
Ring Type	ERPS instance ring network type, the options are as follows: • Major-ring: main ring, closed ring. • Sub-ring: a sub-ring, an unclosed ring, forms a multi-ring network such as an intersecting ring with the main ring.
Ring Name	ERPS Ring Name. Note: The ring name should be created in advance in ERPS "Ring Network Configuration", and the ring network port should be specified.
Instance ID	ID of the ERPS protection instance, and the default value is 0. Note: All VLANs are mapped to Instance 0.
Ring ID	The ID of ERPS ring network, its value range is 1-239. The ring ID is used to uniquely identify an ERPS ring, and all nodes on the same ERPS ring should be configured with the same ring ID. Note: ERPS ring ID will be the last byte of the MAC destination of the RAPS message.
Timer Name	The name of the timer, which supports the default parameter timer or customization in the timer configuration.
RPL Role	Each device in ERPS ring is called a node. The node role is decided by user configuration, they are divided into following types: • RPL-OWNER: owner node is responsible for blocking and unblocking the port in RPL of the node to prevent loop 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

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	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	Port connected by RPL link; the options are as follows: • EAST_PORT • WEST_PORT
Manage VLAN	The VLAN channel of protocol packet, its value range is 1-4094.
Level	ERPS ring network level, the value range is 0-7. The higher the ring network level, the greater the value. When the R-APS message needs to be transmitted across the ring, it can only be crossed by the ring with high rank to low rank.
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: • VIRTUAL CHANNEL: virtual channel status; • NON_VIRTUAL CHANNEL: non-virtual channel state;
State	The instance statuses of ERPS are as follows: • ERPS_INIT: initial state, which is the initialized state when the protocol starts. • ERPS__IDLE: idle state, it would enter this state when the ring topology is complete; • ERPS_FS: force-switch state, it would enter this state when force-switch command is implemented. • ERPS_MS: manual-switch state, it would enter this state when manual-switch command is implemented. • ERPS_PROTECTION: protection state, it would enter this state when the ring link has failure. • ERPS_PENDING: pending state, it would enter this state when the ring link has recovered from failure.
Start	ERPS instance startup status: • start • stop
Master Instance	The ERPS primary instance name is the instance name of the

Copyright © 3onedata Co., Ltd.

Interface Element	Description
Name	Sub-ring-associated primary ring. When the ring network role is sub-ring and the RPL role is Interconnection, the primary instance name can only be set, and it needs to be set as the erps instance name.

Copyright © 3onedata Co., Ltd.

6 Network Management

6.1 SNMP Configuration

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.

6.1.1 View

Function Description

Add/delete SNMP view.

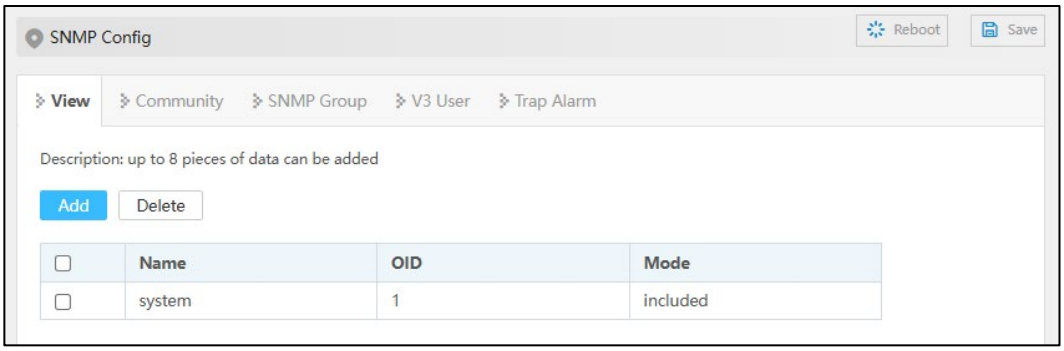
Operation Path

Open in order: “Network Config > SNMP > View”.

Interface Description

View interface is as below:

Copyright © 3onedata Co., Ltd.



The main element configuration description of view interface:

Interface Element	Description
Name	SNMP view name definition, support 32 characters input including a-z and 0-9.
OID	Node location information of MIB tree where the device resides. Note: • OID object identifier, a component node of MIB, uniquely identified by a string of numbers that represent the path. • The information of OID could be viewed via the third-party software MG-SOFT MIB Browser.
Mode	Node OID dealing method, options as below: • Included: It contains all objects under the node subtree; • Excluded: Eliminate all objects beyond the node subtree.

6.1.2 Community

Function Description

Add SNMP community, and define MIB view that community can access, set MIB object access privilege of community as write privilege or read privilege.

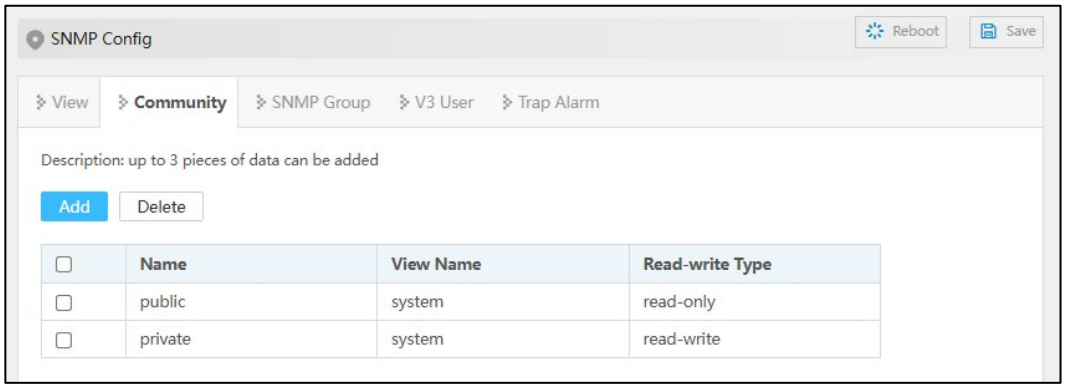
Operation Path

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

Interface Description

Community interface is as below:

Copyright © 3onedata Co., Ltd.



The main element configuration description of community interface:

Interface Element	Description
Name	Group name, including numbers or letters, with a length of no more than 32 characters.
View Name	SNMP view name definition, which has been configured in the View page.
Read-write Type	Read-write privilege view name selection, options: • Read-only • write-only • Read-write

6.1.3 SNMP Group

Function Description

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

Operation Path

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

Interface Description

SNMP Group interface is as follows:

Copyright © 3onedata Co., Ltd.



Main elements configuration description of SNMP Group interface:

Interface Element	Description
Name	SNMP group name, ranging from 1 to 32 bytes.
Encryption Mode	Whether to authenticate and encrypt the message, values: • noauth: indicates that the message is neither authenticated nor encrypted; • auth: indicates that the message is authenticated but not encrypted; • priv: indicates that the message is authenticated and encrypted.
Read View	Specify the read view of the group. Note: The view must be configured in the View interface.
Write View	Specify the write and read view of the group Note: The view can be matched or not. To configure, the view must be configured by the View interface.
Notification View	Specify the notification view of the group. Note: The view can be matched or not. To configure, the view must be the view configured in the View interface.

6.1.4 V3 User

Function Description

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

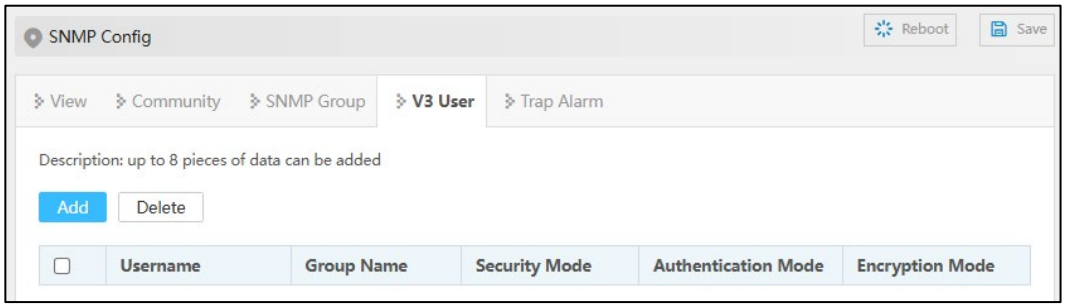
Copyright © 3onedata Co., Ltd.

Operation Path

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

Interface Description

V3 user interface is as follows:

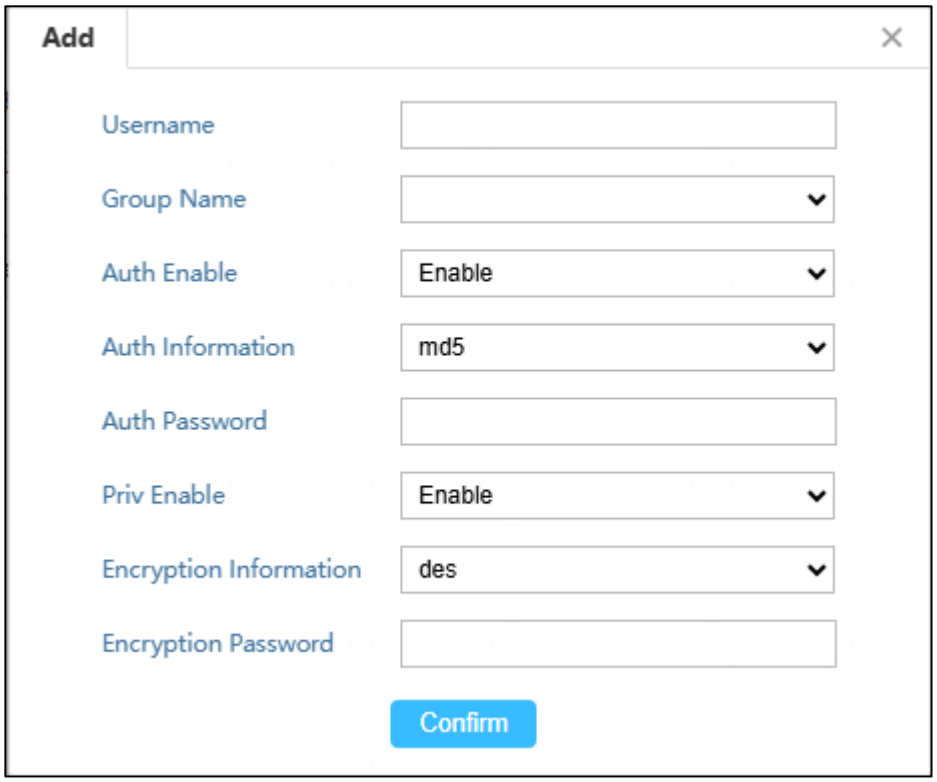


The main element configuration description of V3 user interface:

Interface Element	Description
User name	SNMP v3 user name definition, can only contain numbers, letters, or @_! , no longer than 32 characters.
Group Name	Group name, ranging from 1 to 32 bytes. Note: Group name must be created snmp group, and only created group can create SNMP v3 users.
Security Mode	Whether to authenticate and encrypt the message, values: • auth: indicates that the message is authenticated but not encrypted; • noauth: indicates that the message is neither authenticated nor encrypted; • priv: indicates that the message is authenticated and encrypted.
Authentication Mode	Authentication mode type, acceptable value: • Md5: Information abstract algorithm 5; • Sha: Secure hash algorithm.
Encryption Mode	V3 user data encryption algorithm, options as follows: • Des: Adopt data encryption algorithm; • Aes: Adopt advanced encryption standard.

Copyright © 3onedata Co., Ltd.

V3 User: “Add” Interface Description



The main element configuration description of V3 user “add” interface:

Interface Element	Description
User name	SNMP v3 user name definition, can only contain numbers, letters, or @_! , no longer than 32 characters.
Group Name	The drop-down list of SNMP group name.
Auth Enable	Indicate that security mode requires authentication. If “disable” is selected, the default is no authentication, no encryption mode.
Auth Information	Authentication information type, acceptable values: • Md5: Information abstract algorithm 5; • Sha: Secure hash algorithm.
Auth Password	Authentication password, character string, length greater than or equal to 8 bytes.
Priv Enable	Indicate that security mode requires encryption.
Encryption Information	V3 user data encryption algorithm, options as follows: • Des: Adopt data encryption algorithm; • Aes: Adopt advanced encryption standard.
Encryption Password	Encrypted password, character string, length greater than or equal to 8 bytes.

Copyright © 3onedata Co., Ltd.

6.1.5 Trap Alarm

Function Description

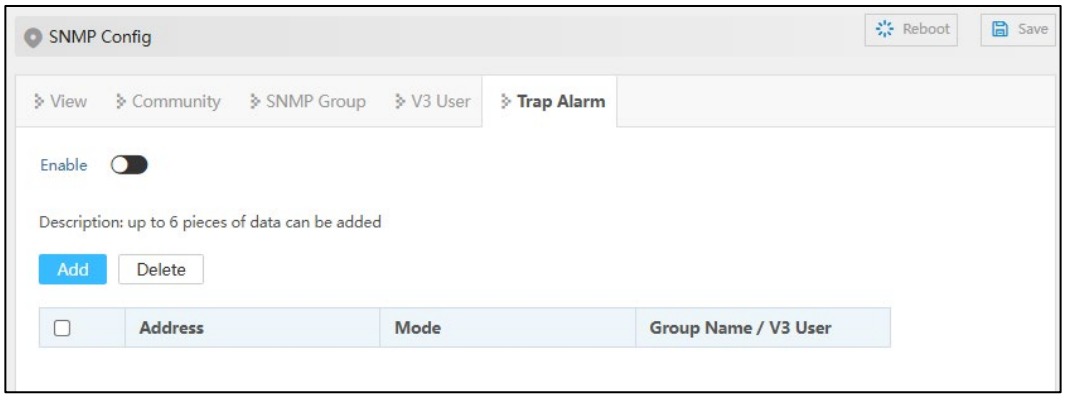
Base on TCP/IP protocol, SNMP usually adopts UDP port 161 (SNMP) and 162 (SNMP-traps), SNMP protocol agent exists in the network device and adopts information specific to the device (MIBs) as the device interface; these network devices can be monitored or controlled via Agent. When a trap event occurs,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

Operation Path

Open in order: "Network Config > SNMP Config > Trap Alarm".

Interface Description

Trap alarm interface is as follows:



The main element configuration description of Trap alarm interface:

Interface Element	Description
Address	IP address of SNMP management device, used for receiving alarm information, such as PC.
Mode	Managed device that sends an active alert to the NMS. After the inform alarm is sent out, it will wait for the confirmation message from NMS, and if no confirmation message is received, it will resend the Inform message; Trap message has no confirmation process. The types of

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	alarm messages include: • trapV1: send snmpV1 trap • trapV2c: send snmpV2c trap • trapV3: send snmpV3 trap • informV2c: send snmpv2 inform • informV3: send snmpV3 inform
Group Name/V3 User	Community name or snmpv3 user name.

6.2 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.

6.2.1 Global Configuration

Function Description

Enable LLDP and configuration.

Operation Path

Open in order: "Network Config > LLDP > Global Config".

Interface Description

Global configuration interface is as follows:

Copyright © 3onedata Co., Ltd.



Main elements configuration description of the global configuration interface:

Interface Element	Description
Enable	The radio box of LLDP function status, check to enable.
Send Period	LLDP transmission period, range 5-32769, unit: second, default: 30 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.
Apply	Click "Apply" button to operate.

6.2.2 Port Configuration

Function Description

Configure the LLDP work mode of the port.

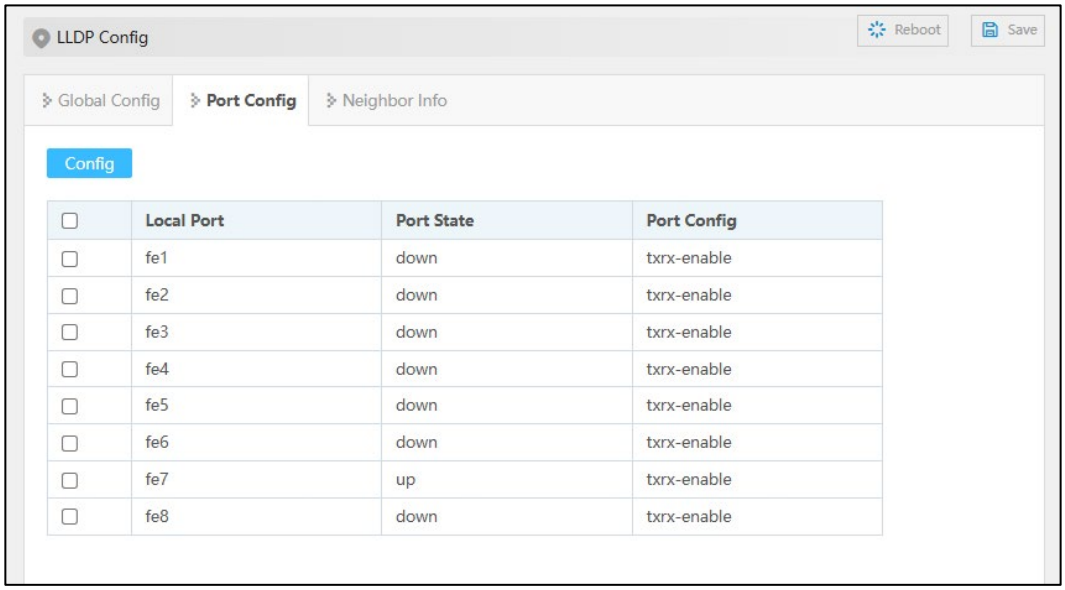
Operation Path

Open in order: "Network Config > LLDP > Port Config".

Interface Description

Check port configuration interface is as below:

Copyright © 3onedata Co., Ltd.



The main element configuration description of port configuration interface:

Interface Element	Description
Local Port	The corresponding port name of the device Ethernet port.
Port State	Port connection status: • UP • down
Port Config	The options of LLDP working modes of device port are as follows: • tx-enable: working mode is Tx, only sending and not receiving LLDP message. • rx-enable: working mode Rx, only receiving, and not sending LLDP message. • txrx-enable: working mode is TxRx, both sending and receiving LLDP message. • disable: working mode Disable, neither receiving nor sending LLDP message. Note: By default, the working mode of LLDP is TxRx when global LLDP is enabled.

Copyright © 3onedata Co., Ltd.

6.2.3 Neighbor Information

Function Description

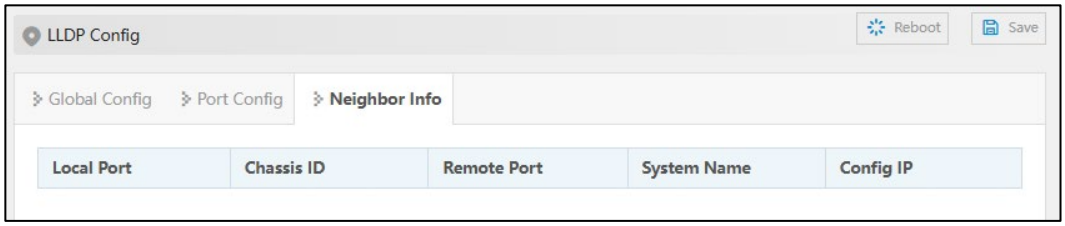
On the "Neighbors Information" page, user can look over the relative information of neighbors.

Operation Path

Open in order: " Network Config > LLDP > Neighbor Info".

Interface Description

Neighbor information interface is as follows:



Main elements configuration description of neighbor information interface:

Interface Element	Description
Local Port	Local port number of local switch connected to adjacent devices.
Chassis ID	Bridge MAC address of neighbor device or port.
Remote Port	Port number of neighbor device.
System Name	System name of the neighbor device.
Config IP	Management IP address of neighbor device or port.

6.3 DHCP-Server

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

Copyright © 3onedata Co., Ltd.

6.3.1 DHCP Switch

Function Description

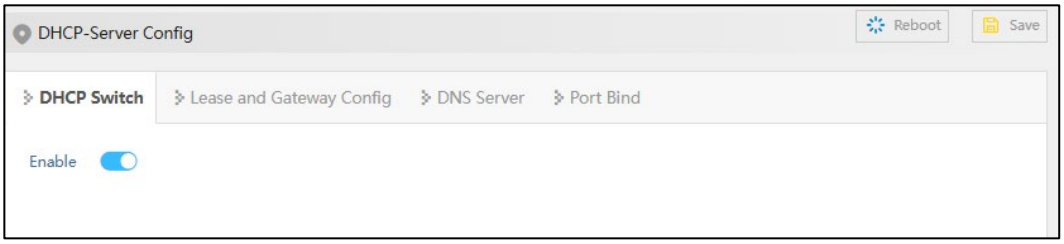
On the "DHCP Switch" page, user can enable/disable DHCP.

Operation Path

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

Interface Description

DHCP switch interface is as follows:



The main element configuration description of DHCP switch configuration interface.

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

6.3.2 Lease and Gateway Configuration

Function Description

Set the valid time and default gateway for the IP address of the client.

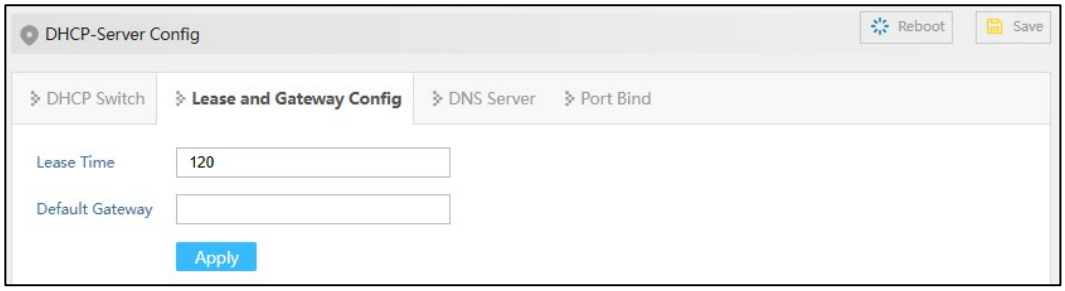
Operation Path

Open in order: "Network Config > DHCP-Server > Lease and Gateway Config".

Interface Description

The Lease and Gateway Configuration interface is as follows:

Copyright © 3onedata Co., Ltd.



The main element configuration description of Lease and Gateway Configuration interface:

Interface Element	Description
Lease Time	The IP address of the client is valid for use. The default value is 120, the unit is min, and the value range is 1-65535. Note: When the time of ip address obtained by dhcp client reaches the lease time, it needs to renew it otherwise the ip address would be invalid and dhcp client needs to request ip address again.
Default Gateway	Default client gateway address, example: 255.255.255.0.

6.3.3 DNS server

Function Description

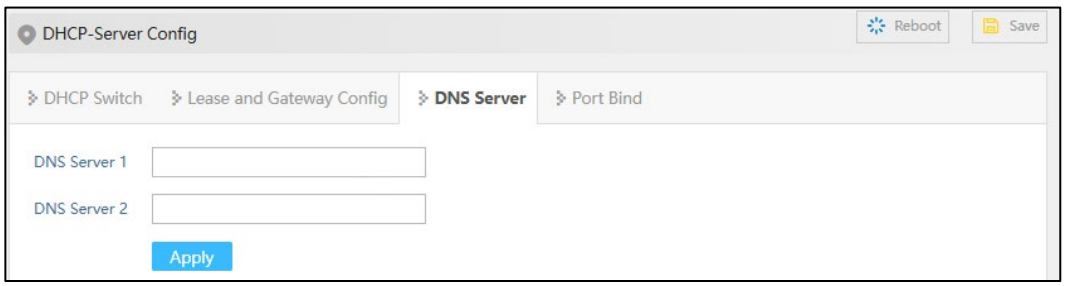
Configure the DNS server address. Parse the domain name to be visited to an IP address, realizing domain name access network.

Operation Path

Open in order: "Network Config > DHCP-Server > DNS Server".

Interface Description

Server configuration interface is as follows:



Copyright © 3onedata Co., Ltd.

The main element configuration description of server configuration interface:

Interface Element	Description
DNS Server 1	IP address of domain name resolution server 1.
DNS Server 2	IP address of domain name resolution server 2.

6.3.4 Port Binding

Function Description

Bind the relationship of IP addresses assigned by ports.

Take Device A and Device B as examples.

If DHCP Server function is enable on Device A and two static address allocation tables are set:

- 192.168.1.19 corresponds to Port 1;
- 192.168.1.20 corresponds to Port 2.

After the function of automatically obtaining the IP address is enabled on Device B,

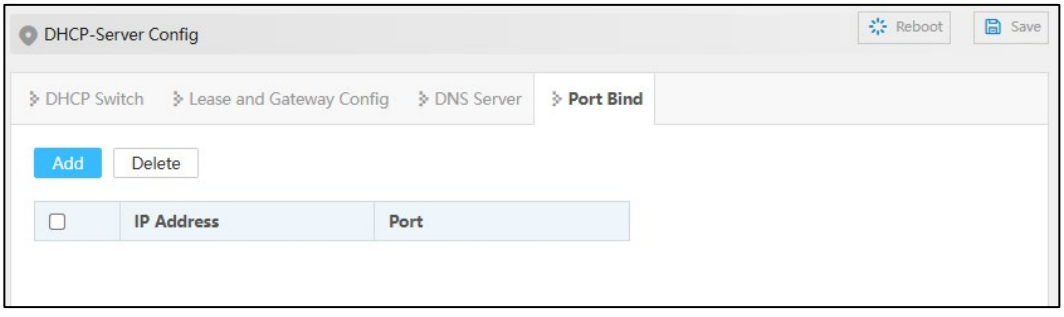
- If Device A is connected to Device B through port 1, Device B can automatically obtain the IP address of 192.168.1.19;
- If Device A is connected to Device B through port 2, Device B can automatically obtain the IP address of 192.168.1.20.

Operation Path

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

Interface Description

Port Bind configuration interface is as follows:



Copyright © 3onedata Co., Ltd.

The main element configuration description of port binding interface:

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

6.4 Access Control

6.4.1 Port Authentication

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

IEEE 802.1x adopts the logic functions of "controllable port" and "uncontrollable port" in the authentication architecture, thus realizing the separation of business and authentication. After the user passes the authentication, the business flow and the authentication flow realize the separation. It has no special request to the subsequent packet processing, the service can be very flexible, and has a great advantage in business especially in carrying out broadband multicast, all services are not restricted by the authentication method.

802.1X structure mainly consists of three parts:

- Supplicant: user or client that wants to get the authentication;
- authentication server: typical example is RADIUS server;
- Authentication system Authenticator: access devices, such as wireless access points, switches, etc

Function Description

Enable and configure 802.1X Authentication parameter.

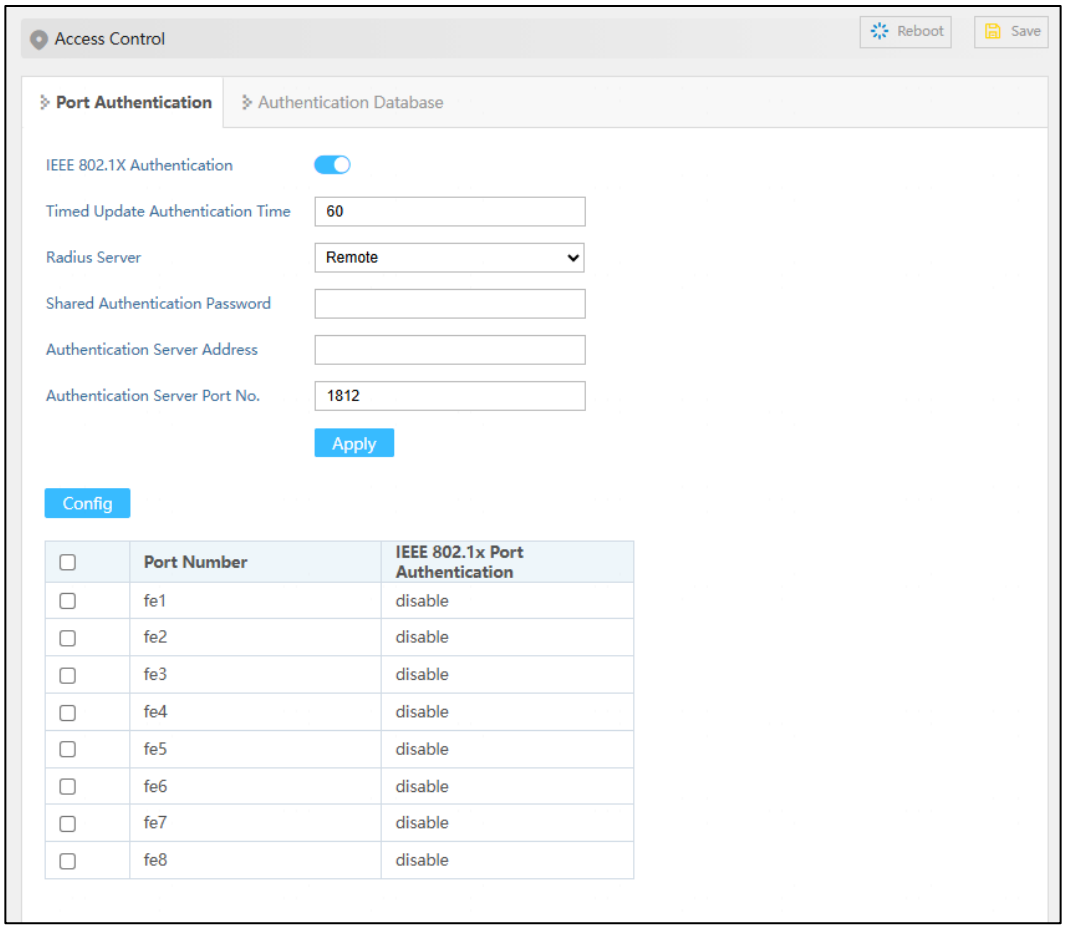
Operation Path

Open in order: "Network Config > Access Control > Port Authentication".

Copyright © 3onedata Co., Ltd.

Interface Description

The screenshot of Port Authentication interface is as follows:



The main element configuration description of port authentication interface:

Interface Element	Description
IEEE802.1X Authentication	Enable/disable IEEE802.1X authentication.
Timed Update Authentication Time	The time range of authentication upgrade interval is 60~4095, unit: second. The reauthentication interval of 802.1x used for strengthening the security of authentication.
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.

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	• Remote: fill in the IP address, port number and shared password for authentication of the authentication server if using external Radius server.
Shared Authentication Password	The shared password character string used for device accessing Radius server. Supports combinations of letters, numbers, and symbols with a length of no more than 33 characters.
Authentication Server Address	IP address of Radius server
Authentication Server Port No.	The port number of the Radius server. The default is 1812, value range is 1-65535.
Port Number	Switch port number.
IEEE802.1x Port Authentication	IEEE802.1X authentication state of the port: • Enable; • Disable.

6.4.2 Authentication Database

Function Description

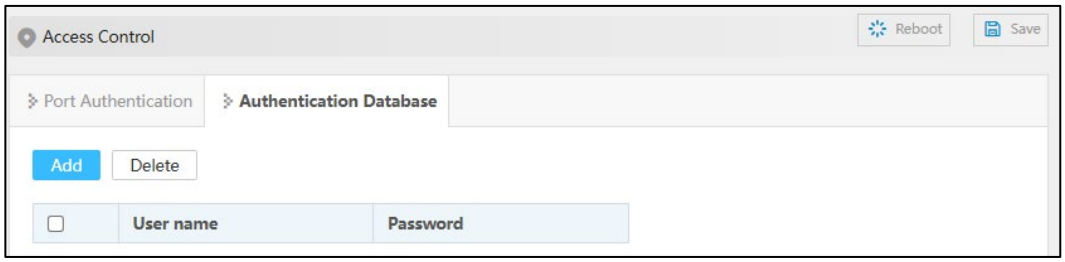
Set the username and password locally authenticated by 802.1X, and add, delete, and save users.

Operation Path

Open in order: “Network Config > Access Control > Authentication Database”.

Interface Description

Screenshot of authentication database interface:



Copyright © 3onedata Co., Ltd.

The main element configuration description of database authentication interface:

Interface Element	Description
User name	Username of logging into local authentication.
Password	Password of logging into local authentication

6.5 QoS

6.5.1 QoS Classification

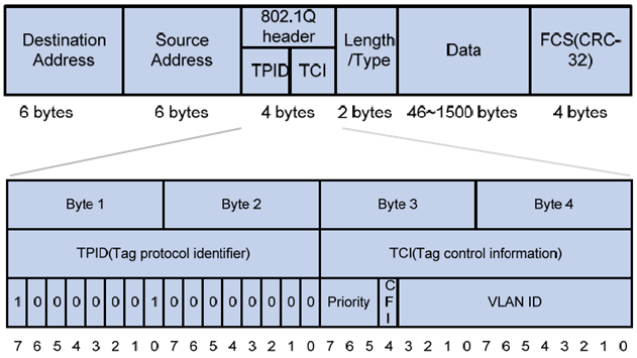
QoS (Quality of Service) is used to evaluate the ability of the service provider to meet the service needs of customers. As for network business, service quality includes transmission bandwidth, transfer delay, data packet loss rate and so on.

The service quality issues that traditional network faces are caused by network congestion. The so-called congestion refers to the phenomenon that the forwarding rate decreases and extra delays are introduced due to the relative shortage of supply resources, thus leading to the decline of service quality. As for congestion management, queue technology is generally adopted. It uses a queue algorithm to classify flow, then uses some priority algorithm to send this flow.

Priority is used to tag the priority of message transmission.

- CoS

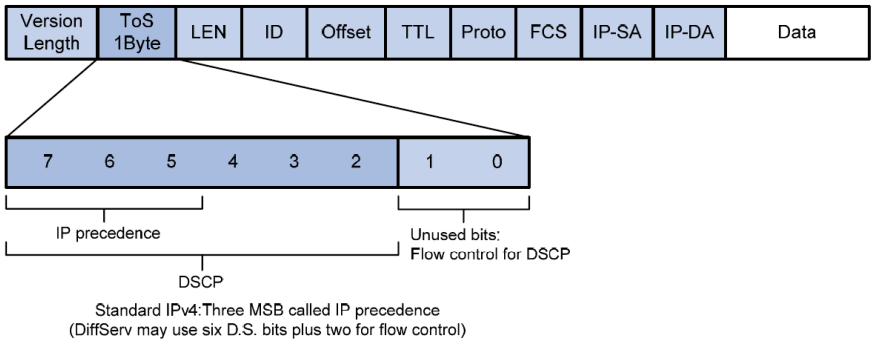
  Ethernet defines 8 business priorities (CoS, Class of Service) in the VLAN TAG of Ethernet frame head. The 802.1Q label head of 4 bytes has included 2-byte TPID （Tag Protocol Identifier) and 2-byte TCI （Tag Control Information), TPID's is 0x8100, the following graph has displayed the details of 802.1Q label head, priority field is 802.1p priority.



Copyright © 3onedata Co., Ltd.

- ToS

  The ToS (Type of Service) domain in the head of IP message is called DS (differential Services) domain, in which the priority of DSCP is represented by the first 6 digits (0 ~ 5 digits) of this domain, with a value range of 0-63, and the last 2 digits (6 and 7 digits) are reserved. The greater the priority level value, the higher the priority level.



Function Description

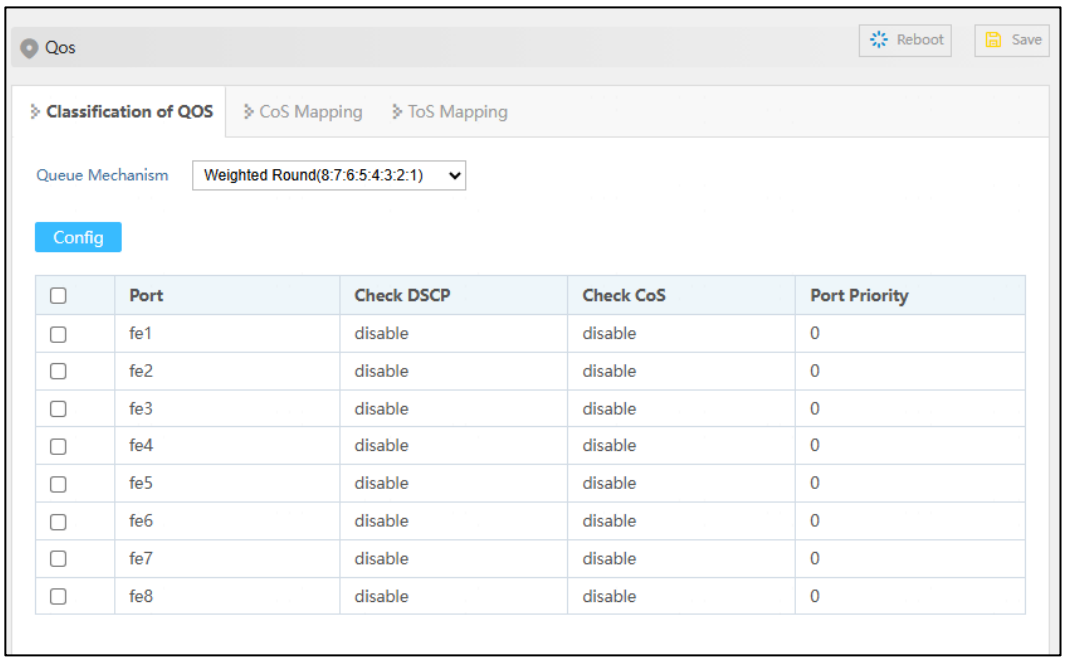
Set the queue mechanism of the device and the priority parameters of each port.

Operation Path

Open in order: “Network Config > QoS > Classification of QOS”.

Interface Description

Screenshot of QoS Classification interface:



Copyright © 3onedata Co., Ltd.

The main element configuration description of QoS classification interface:

Interface Element	Description
Queue Mechanism	Queuing scheduling setting, options are: • Weighted Fair (8:7:6:5:4:3:2:1): according to the queue's weighted value 8:7:6:5:4:3:2:1, weighted round-robin queue scheduling algorithm would schedule queues in turn to ensure that each queue can get some service time. • Strict (Strict Priority): Strict priority queue scheduling algorithm includes 4 queues and schedules in the decreasing order of priority. When the queue with high priority is empty, then it would send groupings of queue with low priority.
Port	The switch port number.
Check DSCP	After checking the checkbox, the priority of ToS would be inspected during queue scheduling.
Check CoS	After checking the checkbox, the priority of CoS would be inspected during queue scheduling.
Port Priority	Configure "Port Priority" for ports without ToS and Cos priority enabled. The valid range is 0-7, with higher values indicating higher priority. Note: By default, switch 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.

Note

- When the ToS and CoS are not enabled, queuing and scheduling are in the order of port priority.
- When the ToS or CoS are enabled, queuing, and scheduling according to ToS or CoS instead of considering port priority.
- If the ToS and CoS are enabled at the same time, queuing according to ToS priority. When the ToS values are the same, queuing according to CoS priority.

Copyright © 3onedata Co., Ltd.

6.5.2 CoS Mapping

Function Description

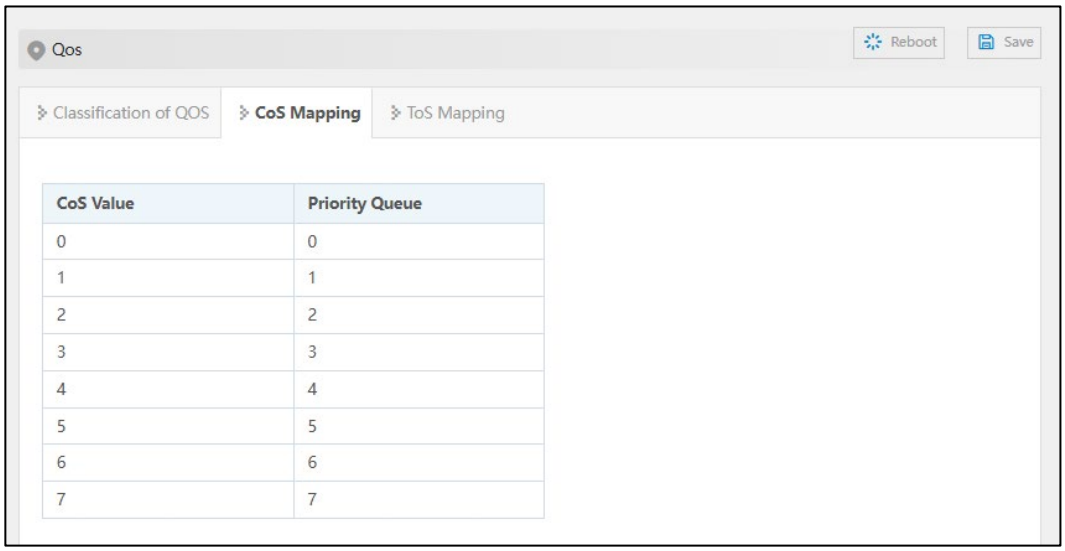
On the page of “CoS Mapping”, user can configure mapping between CoS value and priority queues.

Operation Path

Open in order: “Network Config > QoS > CoS Mapping”.

Interface Description

Screenshot of CoS Mapping interface:



The main element configuration description of CoS mapping interface:

Interface Element	Description
CoS Value	Display CoS value.
Priority Queue	Mapping between CoS value and priority queue.

Copyright © 3onedata Co., Ltd.

6.5.3 ToS Mapping

Function Description

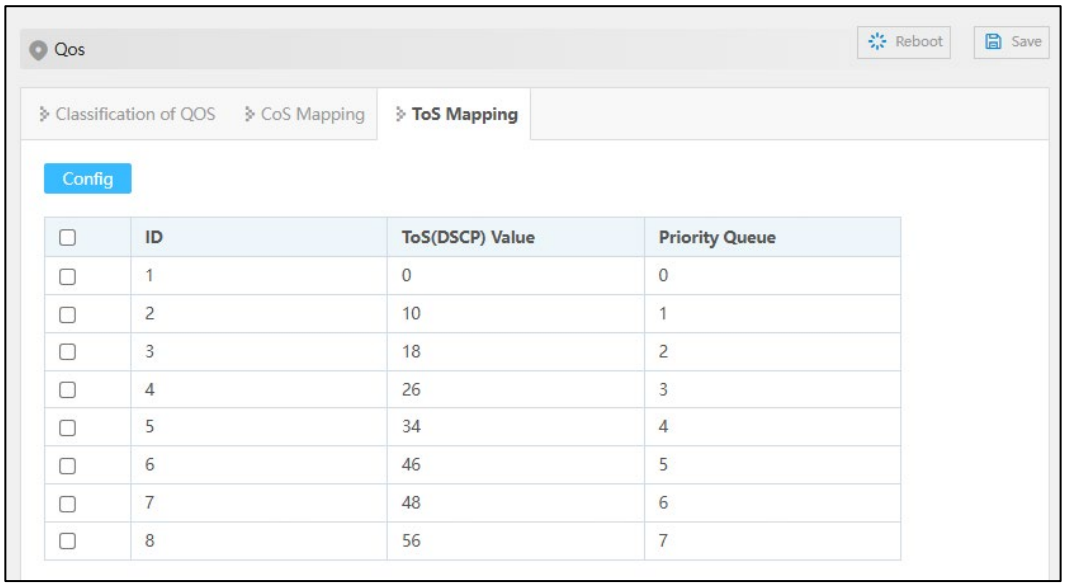
On the page of “ToS Mapping”, user can configure mapping between CoS value and priority queue.

Operation Path

Open in order: “Network Config > QoS > ToS Mapping”.

Interface Description

Screenshot of ToS Mapping interface:



The main element configuration description of ToS mapping interface:

Interface Element	Description
ToS (DSCP) Value	It displays ToS (DSCP) in hexadecimal and decimal format simultaneously. The value in the bracket is decimal.
Priority Queue	Mapping between ToS value and priority queue.

Copyright © 3onedata Co., Ltd.

6.6 Modbus_TCP

Function Description

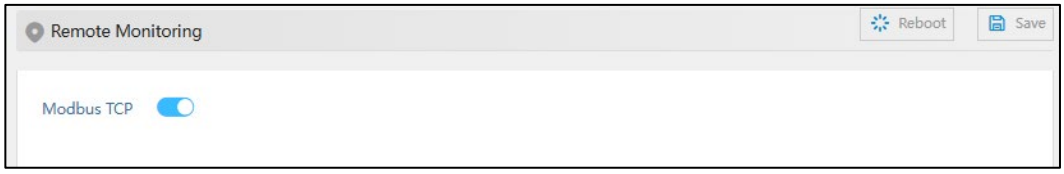
Modbus TCP monitoring function can be enabled. Client can read the switch system, port, ring network, frame statistics and other parameters information via Modbus TCP protocol, which are convenient for various integrated systems to monitor and manage the device.

Operation Path

Open in order: "Network Config > Modbus TCP".

Interface Description

Modbus_TCP screenshot:



The main element configuration description of Modbus_TCP interface:

Interface Element	Description
Modbus TCP	Modbus TCP monitoring enable switch, which is disabled by default. After enabling Modbus TCP monitoring function, client can read the switch device information via function code 4.

Modbus_TCP Data Sheet

Switch read-only register (support function code 4) address information and stored device information, as the table below:

Note

The following table address is hexadecimal format, please convert it into suitable format according to the demands of current debugging tool.

Copyright © 3onedata Co., Ltd.

Information Type	Address (HEX)	Data Type	Description
System Information	0x0000	2 Words	Device ID (reserved)
	0x0002	16 Words	Name (ASCII display)
	0x0012	16 Words	Description (ASCII display)
	0x0022	3 Words	MAC Address (HEX display)
	0x0025	2 Words	IP address
	0x0027	16 Words	Contact Information
	0x0037	16 Words	Firmware Ver (ASCII display)
	0x0047	16 Words	Hardware Ver (ASCII display)
	0x0057	16 Words	Serial No.
	0x0067	1 Word	Power supply 1 status: • 0x0000: OFF • 0x0001: ON
	0x0068	1 Word	Power supply 2 status: • 0x0000: OFF • 0x0001: ON
Port Information	0x1000-0x101B	1 Word	Port connection status: • 0x0000: Link down • 0x0001: Link up • 0x0002: Disable • 0xFFFF: No port
	0x101D-0x1038	1 Word	Port operating mode: • 0x0000: 10M-Half • 0x0001: 10M-Full • 0x0002: 100M-Half • 0x0003: 100M-Full • 0x0004: 1G-Half • 0x0005: 1G-Full • 0xFFFF: No port
	0x1039-0x1054	1 Word	Port flow control status: • 0x0000: OFF • 0x0001: ON • 0xFFFF: No port
	0x1056-0x1071	1 Word	Port interface type: • 0x0000: Copper port

Copyright © 3onedata Co., Ltd.

Information Type	Address (HEX)	Data Type	Description
			• 0x0001: Fiber port • 0x0002: Combo port • 0xFFFF: No port

Example: MODBUS_TCP Configuration

Acquire the switch device name information via DebugTool analogue client, the switch information is as follows:

- Switch default IP address: 192.168.1.254;
- Address of switch register that stores the device name information: 0x002;
- Number of switch register that stores the device name information: 16 words.

Operation Steps

First, configure the switch Modbus_TCP monitoring enable.

Step 1 Log into Web configuration interface.

Step 2 Select "Network Config > Remote Monitoring > Modbus_TCP".

Step 3 Slide on the "Modbus_TCP" enable switch, as shown in the figure below.



Step 4 End.

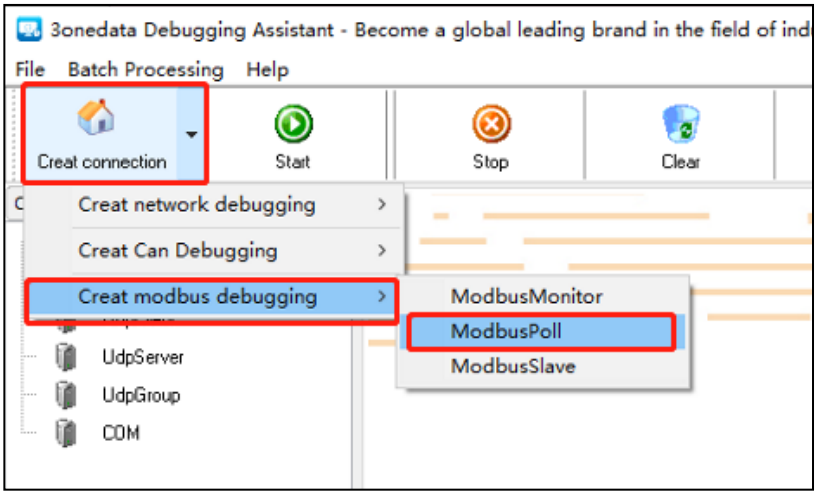
Then, run the debug tool software to acquire the device parameters.

Step 1 Open "Debug Tool".

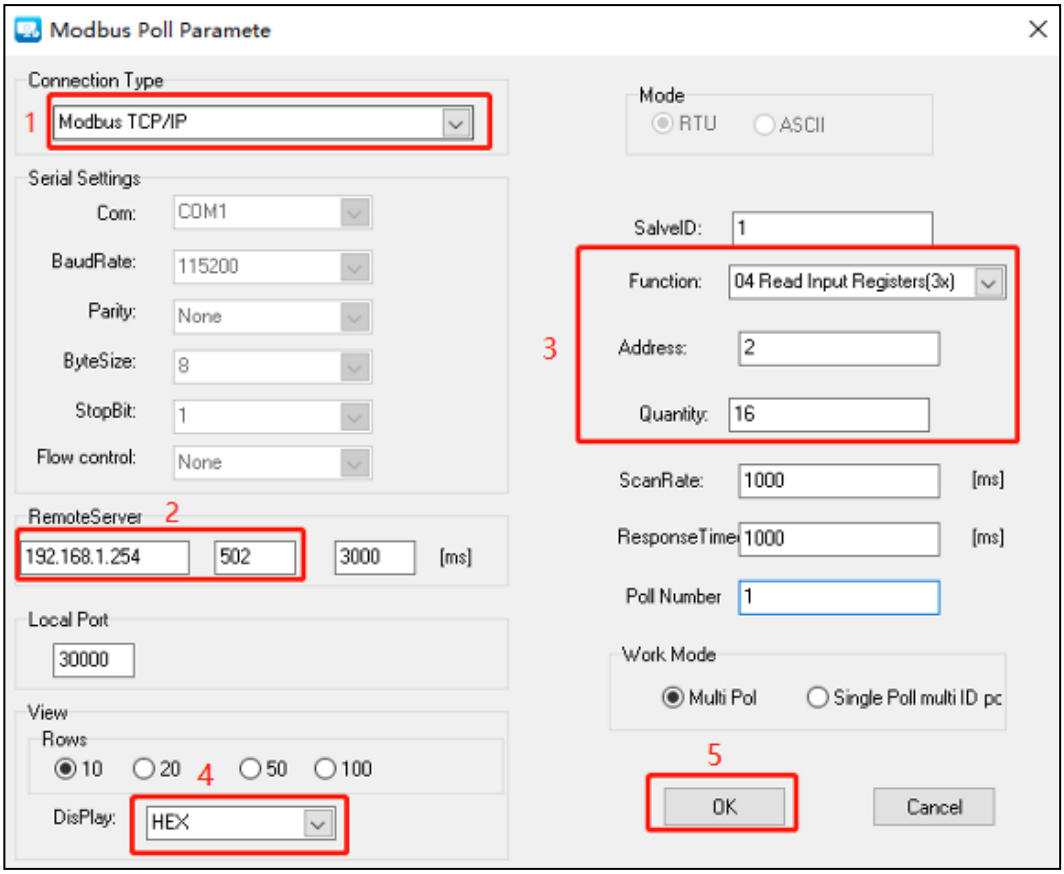
Step 2 Click the drop-down list of "Create connection".

Step 3 Select "Create Modbus debugging > ModbusPoll", as the picture below.

Copyright © 3onedata Co., Ltd.



Step 4 Configuration window of ModbusPoll parameters pops up, the configuration as the picture below:



1 On the drop-down list of "Connection Type", select "Modbus TCP/IP";

2 Enter the switch IP address "192.168.1.254" and port number "502" on the column of "Remote Server";

3 Select "04 Read Input Registers (3x)" on the drop-down list of "Function";

4 Enter decimal device name register address "2" on the text box of "Address";

Notice:

Copyright © 3onedata Co., Ltd.

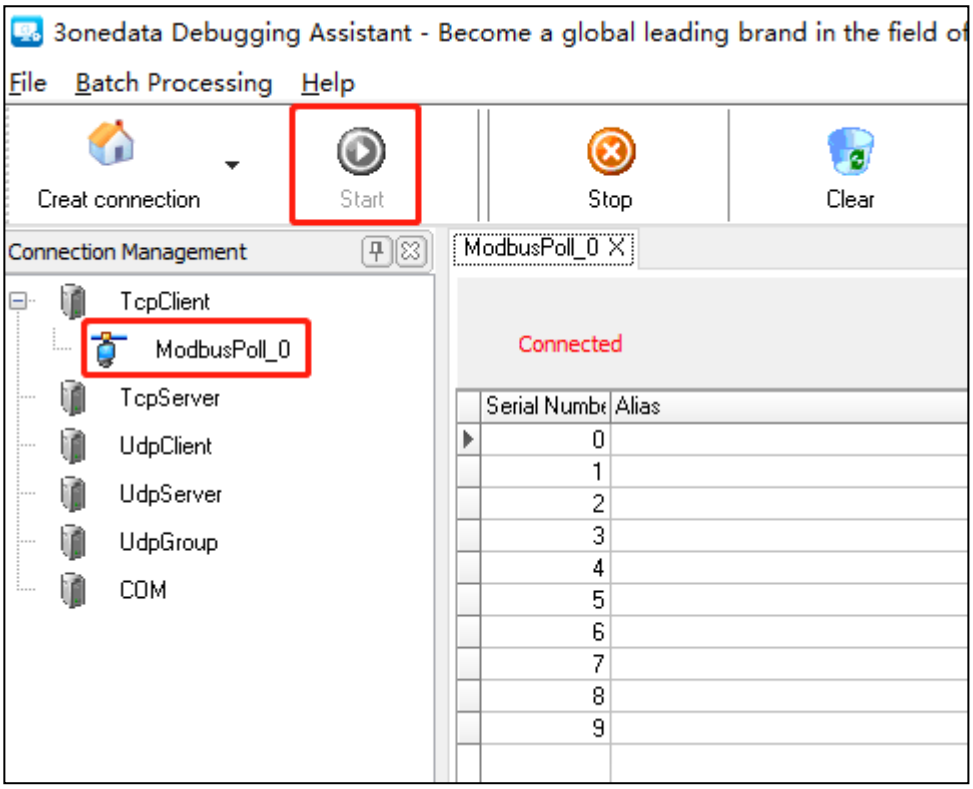
Here the start address is decimal format, so hexadecimal register address should be converted into decimal format.

5 Enter the register amount "16" on the text box of "Quantity";

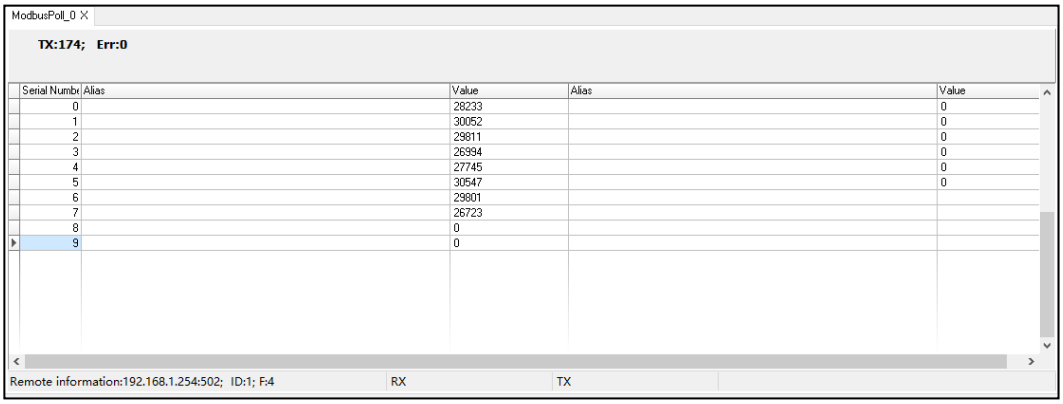
6 Select "HEX" on the drop-down list of "Display";

7 Click "OK".

Step 5 On the page of Debug Tool, select created ModbusPoll, and then click "Start";



Step 6 Check responsive data, and convert the hexadecimal value read by register into ASCII code, displayed as "Industrial Switch";



Step 7 End.

Copyright © 3onedata Co., Ltd.

Note

- Switch can establish 4 Modbus TCP monitoring connections at the same time.
- Switch Port Information, Frame Statistics and PoE Information. It supports the sequential read of port parameters of multiple registers. For example, address range of the register that stores port connection status information is 0x1000-0x101B, each register data is 1 word; when the start address of register is 0x1000, the register number is 1, it will read port 1 status; If the register quantity is 10, it will read the status from Port 1 to Port 10; If the port doesn't exist, then the read data will be 0xFFFF.

Copyright © 3onedata Co., Ltd.

7 System Maintenance

7.1 Network Diagnosis

7.1.1 Ping

Function Description

Ping is used to check whether the network is open or network connection speed. The Ping command uses the uniqueness of the IP addresses of the machines on the network to send a packet to the target IP address, and then asks the opposite end to return a packet with the same size to determine the connection status and delay value of the two network devices.

Operation Path

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

Interface Description

The Network diagnosis interface is as follows:



The main element configuration description of Ping interface:

Copyright © 3onedata Co., Ltd.

Interface Element	Description
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.

7.2 Time

7.2.1 NTP Configuration

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

Function Description

Enable and configure NTP server.

Operation Path

Open in order: "System Config > NTP > NTP Config".

Interface Description

The NTP configuration interface is as follows:



Main element configuration description of NTP configuration interface:

Copyright © 3onedata Co., Ltd.

Interface Element	Description
Enable	Enable/Disable NTP configuration.
NTP Server	IP address of NTP server, for example: 192.168.1.1. Note: As NTP client, the system will synchronize time with NTP server every 11 minutes.
Synchronization period	Set the time synchronization cycle, with a range of 10-72000 (s).

7.2.2 Time Zone Configuration

Function Description

Configure the device time zone.

Operation Path

Open in order: "System Config > NTP > Time Zone Config".

Interface Description

Time Zone Configuration interface is as follows:



Main elements configuration description of time zone configuration interface:

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

Copyright © 3onedata Co., Ltd.

7.3 Alarm Configuration

After enabling alarm, when the device port is in an abnormal state, the administrator can be informed in time, and the device state can be quickly repaired to avoid excessive loss.

7.3.1 Relay Setting

Function Description

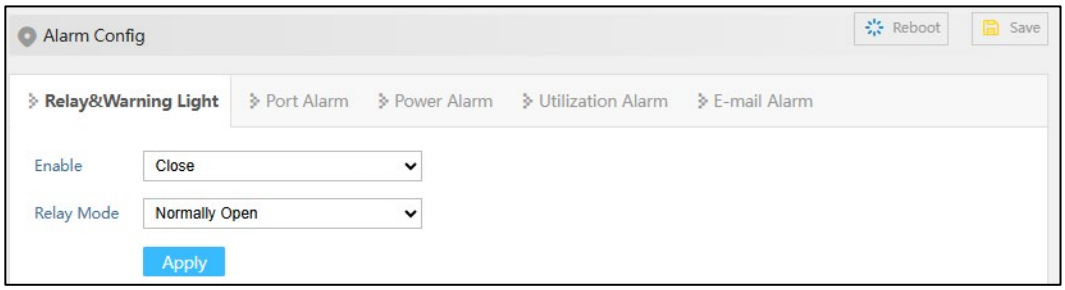
Set the enable and circuit mode of the relay.

Operation Path

Open in order: "System Config > Alarm > Relay&Warning Light".

Interface Description

The Relay&Warning Light configuration interface is as follows:



Main elements configuration description of Relay&Warning Light configuration interface:

Interface Element	Description
Enable	Enable/disable Relay&Warning Light.
Relay Mode	Set the circuit state of the relay: • Normally closed: when the relay is normal without alarm, it is in closed status; when alarm occurs, the relay is in open status; • Normally open: when the relay is normal without alarm, it is in open status; when alarm occurs, the relay is in closed status.

Copyright © 3onedata Co., Ltd.

7.3.2 Port Alarm

Function Description

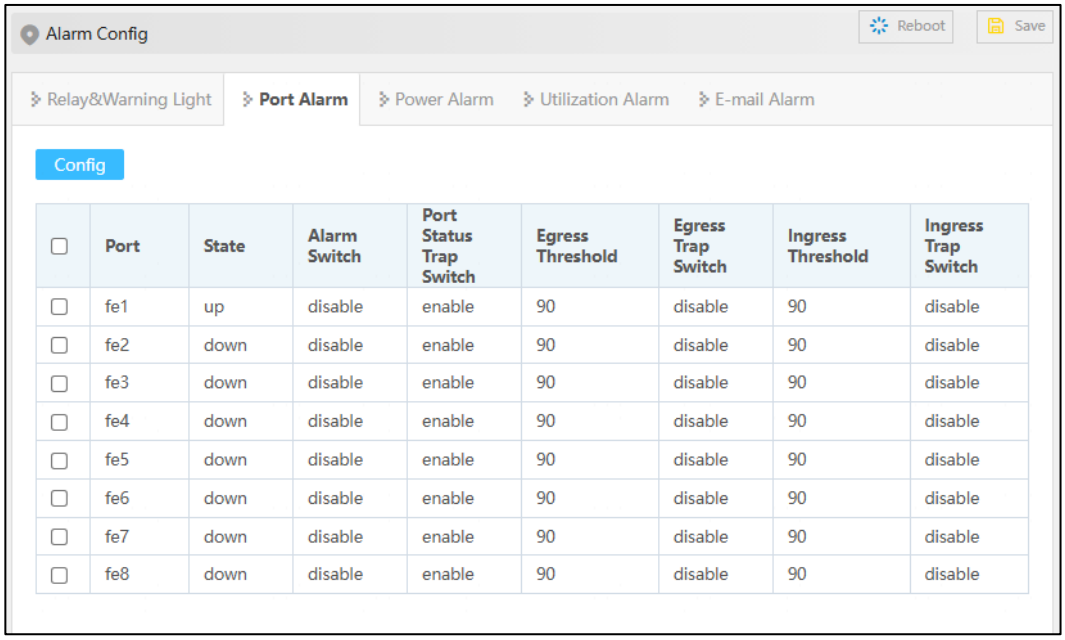
After enabling alarm, when the device port is in an abnormal state, the administrator can be informed in time, and the device state can be quickly repaired to avoid excessive loss.

Operation Path

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

Interface Description

Port alarm interface is as below:



The main element configuration description of port alarm interface:

Interface Element	Description
Port	The corresponding port name of the device Ethernet port.
State	Port link status, display items as follows: • up • down
Alarm Switch	Port alarm function status, options as follows: • Enable • Disable

Copyright © 3onedata Co., Ltd.

Interface Element	Description
Port Status Trap Switch	Port status Trap switch, options: • Enable • Disable
Egress Threshold	When the egress port reaches the threshold, NMS software prompts an alarm.
Egress Trap Switch	Enable the egress Trap switch. Send Trap information when the threshold is reached. Egress Trap switch, options: • Enable • Disable
Ingress Threshold	When the ingress port reaches the threshold, NMS software prompts an alarm.
Ingress Trap Switch	Enable the ingress Trap switch. Send Trap information when the threshold is reached. Ingress Trap switch, options: • Enable • Disable

7.3.3 Power Alarm

Function Description

Enable/disable the power alarm function.

Note

Only DC dual power supply supports power alarm, and AC current does not support power alarm.

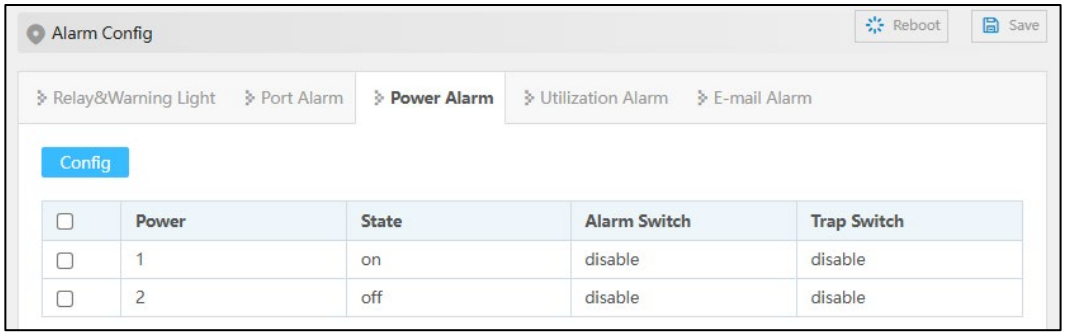
Operation Path

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

Interface Description

Power alarm interface is as below:

Copyright © 3onedata Co., Ltd.



Main elements configuration description of power alarm interface:

Interface Element	Description
Power	The corresponding name of this device's power supply
State	Device power link status, display items as follows: • On: connected • Off: disconnected
Alarm Switch	Port alarm function status, options are as follows: • Enable: alarm has been enabled. • Disable: the alarm is not enabled
Trap Switch	• When the power alarm is enabled or disabled, select "Enable" to send Trap information. • When the power alarm is enabled or disabled, select "Disable" to not send Trap information.

7.3.4 Utilization Alarm

Function Description

On the "Utilization Alarm" page, you can set CPU utilization and memory utilization alarm events. When the alarm event parameter value exceeds the set threshold, the device will continuously send out Trap information to inform relevant personnel. When the alarm event parameter value drops below the set threshold, the device will send out a Trap message to inform the relevant personnel.

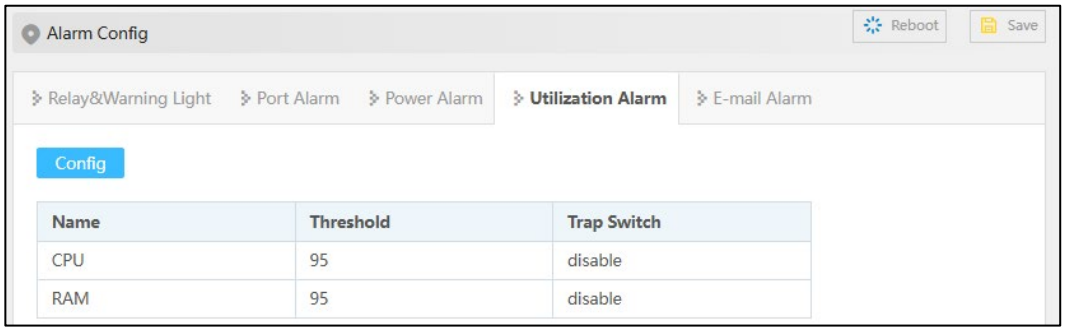
Operation Path

Open in order: "System Config > Alarm > Utilization Alarm".

Copyright © 3onedata Co., Ltd.

Interface Description

Utilization Alarm interface is as below:



The main element configuration description of utilization alarm interface:

Interface Element	Description
CPU Threshold	CPU utilization threshold, when the CPU utilization reaches the threshold, an alarm will be generated.
CPU Trap Switch	Enable the CPU Trap switch, and send Trap information when the CPU utilization reaches the threshold. CPU Trap status, options: • Enable • Disable
RAM Threshold	Memory utilization threshold, when the memory utilization reaches the threshold, an alarm will be generated.
RAM Trap switch	Enable the memory Trap switch, and send Trap information when the memory utilization reaches the threshold. Memory Trap status, options: • Enable • Disable

7.3.5 Mail Alarm

Function Description

On the page of "E-mail Alarm", user can enable remote alarm.

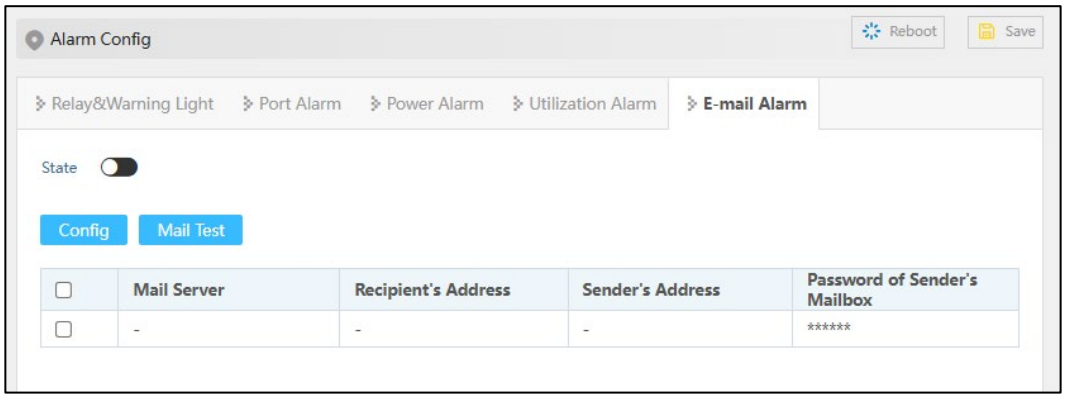
Operation Path

Open in order: "System Config > Alarm > E-mail Alarm".

Copyright © 3onedata Co., Ltd.

Interface Description

E-mail Alarm interface is as follows:



Main element configuration description of E-mail Alarm interface:

Interface Element	Description
State	Enable/disable E-mail alarm.
Mail Server	Server address of used E-mail should be filled according to the account of used E-mail address. The host IP address or used host name that provides E-mail delivery service for the device.
Recipient's Address	E-mail address used by abnormal event receiver.
Sender's Address	E-mail address of sender, account name used for logging in to the E-mail server.
Password of Sender's Mailbox	E-mail password of sender, corresponding password used for logging in to the E-mail account.

Notice

While using E-mail alarm, user must ensure that the switch is connected to network normally and the gateway of switch is same to the one of LAN.

Copyright © 3onedata Co., Ltd.

7.4 Configuration File Management

7.4.1 Configuration File Update

Function Description

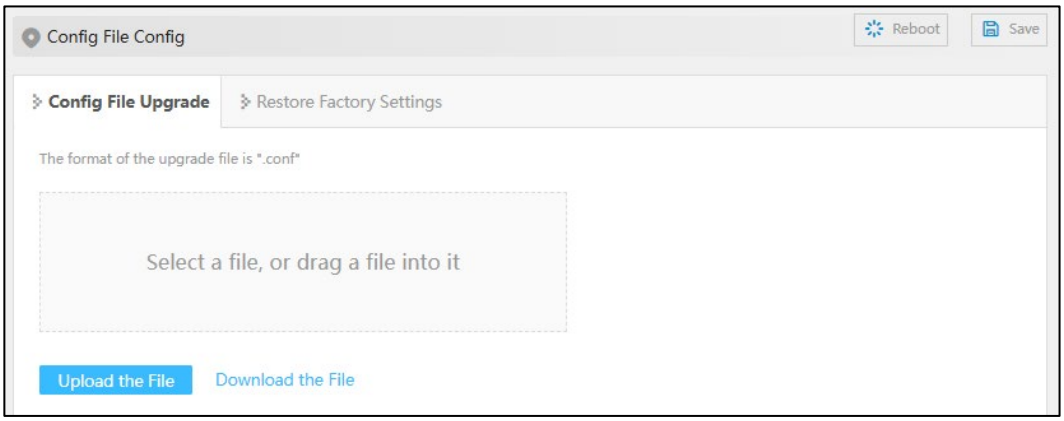
Upload and download configuration files

Operation Path

Open in order: "System Config > Config File Config > Config File Upgrade".

Interface Description

Configuration file upgrade interface is as follows:



The main element configuration description of System File interface:

Interface Element	Description
Download the File	Download the configuration information files of current switch. Tips: Downloaded configuration files can be uploaded to other homogeneous devices, achieving repeated usage after one-time configuration.
Upload the File	The format of the configuration file is ".conf". Drag the profile into the upgrade box, or click "Click Upload" to select the profile.

Notice

Copyright © 3onedata Co., Ltd.

In the process of uploading configuration files or upgrading software, please don't click or configure other WEB page of the switch, not even reboot the switch; otherwise, it will lead to failure of configuration files uploading or software upgrading, or even cause system breakdown of the switch.

7.4.2 Restore Factory Settings

Function Description

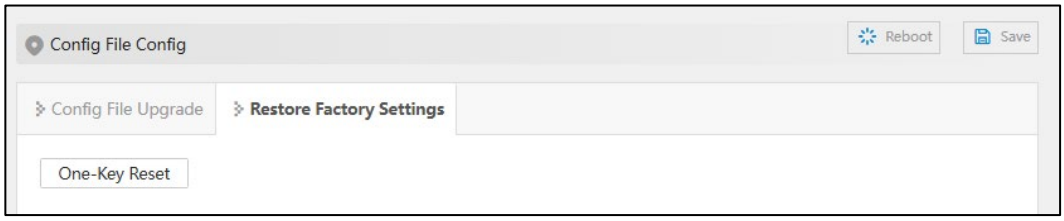
Restore the device firmware to the factory configuration.

Operation Path

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

Interface Description

The Restore Factory Settings interface is as follows.



The main element configuration description of configuration file management interface:

Interface Element	Description
One-Key Reset	Restore factory defaults of the switch. Note: Restore factory defaults will cause all devices to be in the factory status, default IP address is "192.168.1.254".

7.5 Upgrade

Function Description

Update and upgrade the device program via web.

Copyright © 3onedata Co., Ltd.

Operation Path

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

Interface Description

The software upgrade interface is as follows:



The main elements configuration description of software update interface:

Interface Element	Description
Upgrade	Drag the upgrade file into the upgrade box or click "Click Upload" to select the upgraded file in the format of ".bin".

7.6 Log Information

7.6.1 Log Information

Function Description

On the page of “Log information”, user can check the log information of the device. Log information mainly records user operation, system failure, system safety and other information, including user log, security log and diagnostic log.

- User log: records user operations and system operation information.
- Security log: records information including account management, protocol, anti-attack, and status.
- Diagnostic log: records information that assists in problem identification.

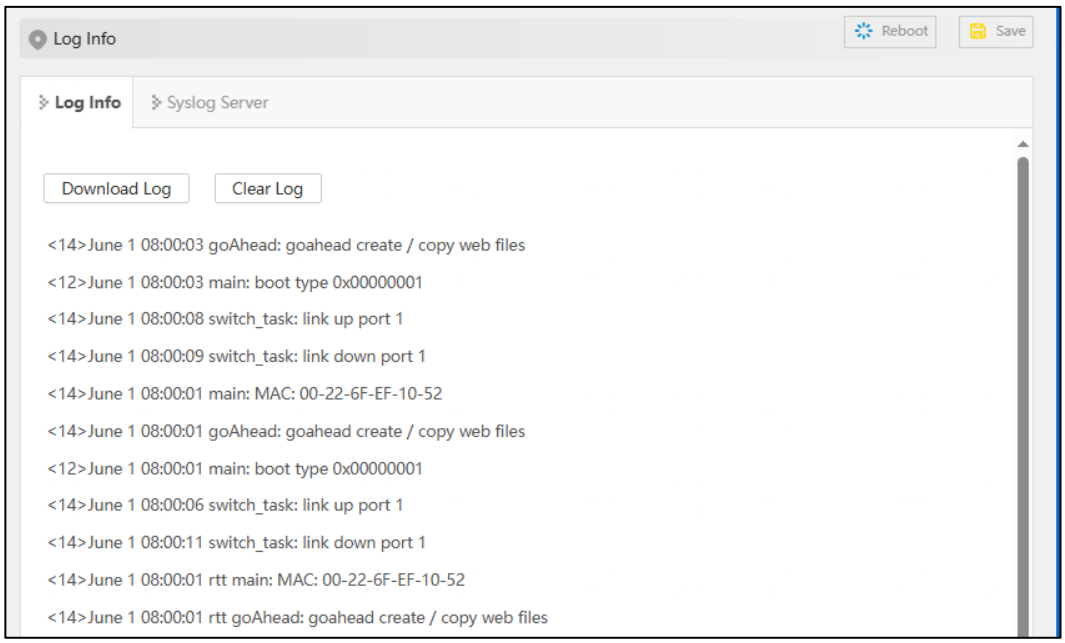
Operation Path

Open in order: "System Config > Log Info > Log Info".

Copyright © 3onedata Co., Ltd.

Interface Description

The Log Information interface is as follows:



Main elements configuration description of log information interface:

Interface Element	Description
Download Log	Click the "Download Log" button to download the current log information to the local.
Clear Log	Click the “Clear Log” button to clear the current log information record.

7.6.2 Syslog Server

Function Description

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

Operation Path

Open in order: "System Config > Log Info > Syslog Server".

Copyright © 3onedata Co., Ltd.

Interface Description

The Syslog server interface is as follows:



Syslog server interface main elements configuration instructions:

Interface Element	Description
Syslog Server	IP address of Syslog server
Port Number	Port number of Syslog server.

Copyright © 3onedata Co., Ltd.

8 FAQ

8.1 Sign in Problems

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

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

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

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

3. **Is configuring via WEB browser same to configuring via BlueEyes_Ⅱ software?**
   Both configurations are the same, without conflict.

8.2 Configuration Problem

1. **How to configure the device restore default setting via DIP switch?**

   Turn the DIP switch 2 to ON position, and restore default setting after power on again.

Copyright © 3onedata Co., Ltd.

2. **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.

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

8.3 Alarm Problem

1. **When the device alarms, except BlueEyes_II software nether alarm information display area will display alarm information, is there any other way to notify technical staffs?**

   When the device alarms, monitoring host computer buzzer will continue to emit alarm sounds.

8.4 Indicator Problem

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

Copyright © 3onedata Co., Ltd.

Possible reasons include:

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

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

Possible reasons include:

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

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.

Copyright © 3onedata Co., Ltd.

- 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.

9 Maintenance and Service

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

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

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

9.1 Internet Service

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

9.2 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.

9.3 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.

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

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