Managed Switches

SL-SWTG3DE48A6S

Web Management Manual

Version: 1.0

Contents

Revision Record

Date	Version	Description
Apr 13 2023	V 1.0	First Version

1 Preface

1.1 Intended Audience

This manual is intended for installers and system administrators who are responsible for installing, configuring, or maintaining networks. This manual assumes that you understand all transport and management protocols used by the network.

This manual also assumes that you are familiar with the terminology, theoretical principles, practical skills, and specific expertise of network devices, protocols, and interfaces related to networking. You must also have experience working with graphical user interfaces, command line interfaces, simple network management protocols, and Web browsers.

1.2 Conventions of this book

The following conventions are used in this manual.

GUI Conventions	Description
📖 Description	The description of the operation content, make necessary additions and explanations.
⚠ Note	Reminds of the precautions to be taken during operation, improper operation may lead to data loss or equipment damage.

2 Logging in to the Web Page

2.1 Logging in to Web Network Management Client

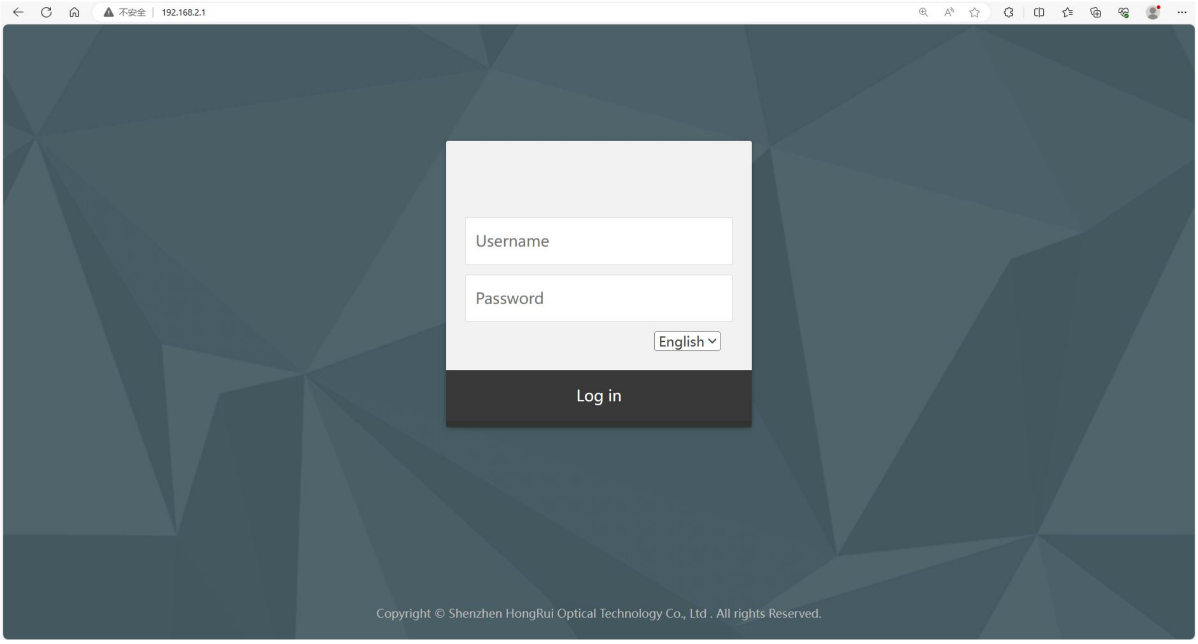
Users can open a Web browser and enter the switch default address: http://192.168.2.1 and press Enter.

📖 Instructions:

The device supports browsers: IE9.0 or above, Chrome23.0 or above, Firefox20.0 or above

When logging into the switch, you should make the IP network segment of the PC and the switch network segment consistent. When logging in for the first time, set the IP address of PC to 192.168.2.x (x stands for 1~254, except 1), and set the subnet mask to 255.255.255.0, but the IP address of PC can not be the same as that of switch, i.e., it can not be 192.168.2.1.

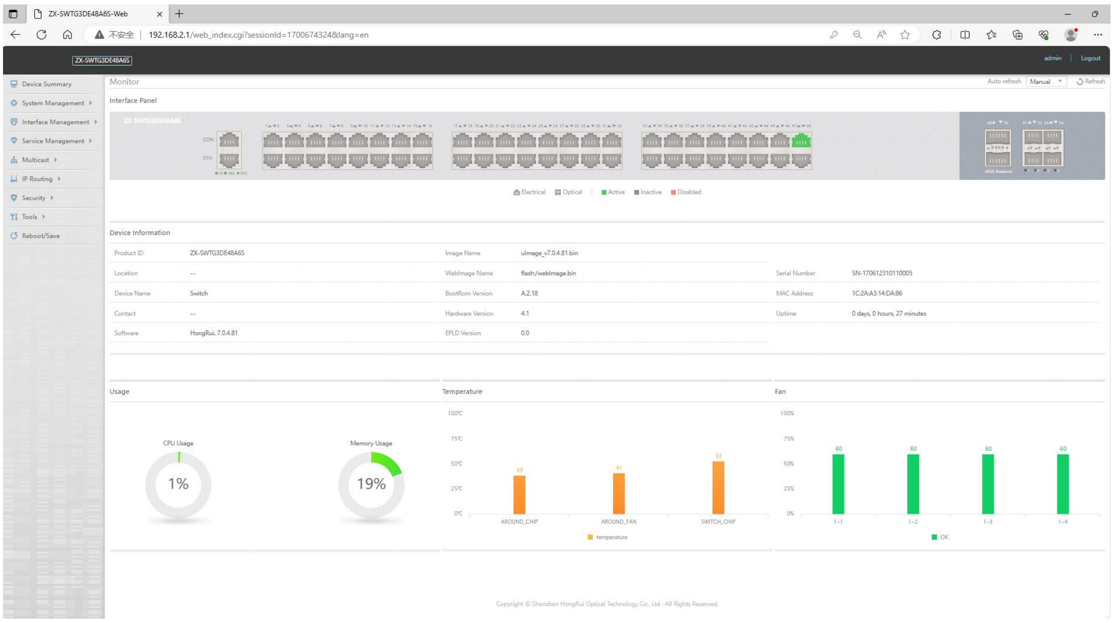
At this time, the login window appears, as shown in the figure below. Enter the default user name: admin and password: admin. Click the <Login> button and you will see the switch system information.



Copyright © Shenzhen HongRui Optical Technology Co., Ltd . All rights Reserved.

2.2 Client Interface Composition

The typical operating interface of the Web-based network management system is described in the following figure.



Device Information

Product ID	ZX-SWTG3DE48A6S	Image Name	uImage_v7.0.4.81.bin		
Location	--	WebImage Name	flash:/webImage.bin	Serial Number	SN-170612310110005
Device Name	Switch	BootRom Version	A.2.18	MAC Address	1C:2A:A3:14:DA:86
Contact	--	Hardware Version	4.1	Uptime	0 days, 0 hours, 27 minutes
Software	HongRui, 7.0.4.81	EPLD Version	0.0		

Copyright © Shenzhen HongRui Optical Technology Co., Ltd . All Rights Reserved.

2.3 Web interface navigation tree

The Web Webmaster's menu mainly provides menu items such as Device Overview, System Management, Ports, Service Management, Multicast, IP Routing, Security, Tools, and Reboot/Save. There are submenus under each menu option. The detailed navigation tree information is as follows:

Menu Item	Submenu	Secondary submenu	Description
System Status			Displays port status and product information
System management	Document management		Configure to view the current device's memory usage and files
	System Configuration		Configure to view base settings, temperature, basic information, time and date, time zone, etc.
	Loading Configuration		Configuration loading
	Log Management		Configure to view log messages
	SNMP Configuration		Configure to view basic configuration and group configuration
	SNMP Trap Configuration		Configuration to view basic configuration and Trap target host configuration
Ports	Port Status		Configure to view information about all ports on the device
	Port Statistics		Configure to view port packet data
	Link Aggregation	Global Configuration	Configure to view the global configuration (load sharing mode)
		Port Configuration	Configure to view port configuration information
	Storm Control		Configure to view storm control information
	Flow Control		Configure to view flow control information

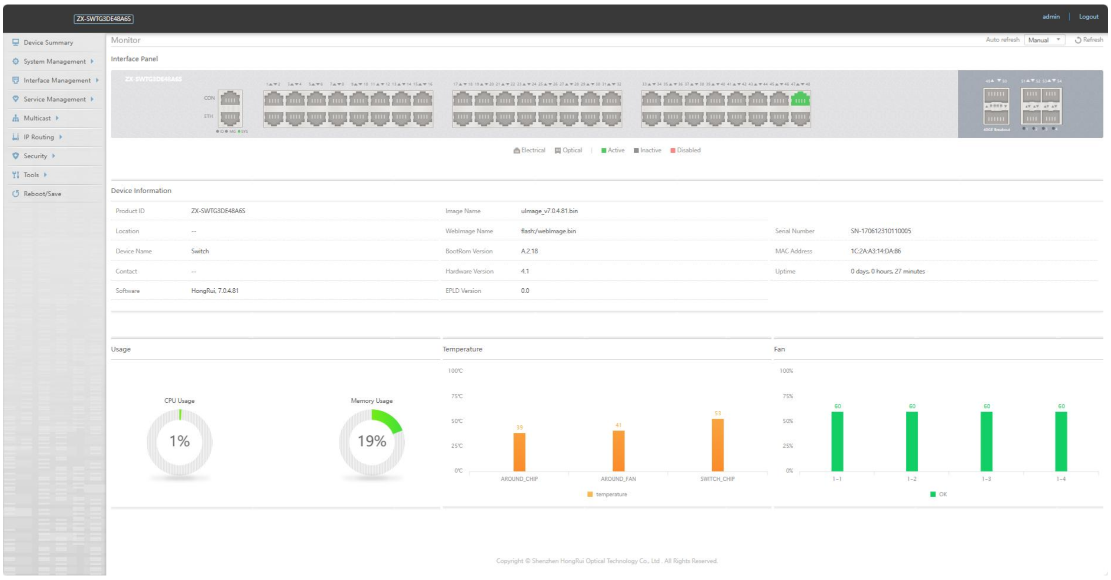
	Port Isolation	Global Configuration	Configuring to View Global Configuration Port Isolation Information
		Port Configuration	Configure to view optional port isolation information
	Port Mirroring	Overview	Configure to view mirrored port information
		Global Configuration	Configure to view Dest port normal forwarding information
		Mirroring Configuration	Configure to view information on adding mirrors to a port
		Remote Mirror MAC Escape	Configure to view the information of remote mirror MAC Escape.
	Port Monitoring		Configure to view parameter configuration and monitoring configuration information
Service Management	VLAN	VLAN Status	Configure to view VLAN status information
		VLAN Add/Remove	Configure to view VLAN add/remove configuration
		VLANIF Ports	Configure to view VLANIF port information
		Access/Trunk Ports	Configure to view Access/Trunk port information.
	VLAN Classification	Status	Configure to view VLAN classification rules, VLAN classification groups, and VLAN classification usage information.
		Rules	Configure to view VLAN classification rule settings
		Groups	Configure to view VLAN classification group settings
		Application	Configure to view VLAN classification application information
	MAC	MAC Address Table	Configure to view MAC address table information
		MAC Global Configuration	Configure to view MAC global configuration information
		MAC Learning	Configure to view MAC learning information
		Static MAC Address Table	Configure to view static MAC address table information

		Blackhole MAC Address Table	Configure to view black hole MAC address table information
		Port Security	Configure to view port security information
		Static Secure MAC Address Table	Configure to view static secure MAC address table information
	Spanning Tree	Spanning Tree Information	Configuring to View Spanning Tree Information
		Global Configuration	Configure to view global configuration, advanced configuration, and instance configuration information
		Spanning Tree Ports	Configure to view spanning tree port status information
		MST Domain	Configure to view MST domain information
	ERPS	ERPS Configuration	Configuring to View ERPS Configuration Information
		ERPS Status	Configure to view ERPS status information
IGMP Snooping	IGMP Snooping Features		Configuring to View IGMP Snooping Function Information
	IGMP Snooping Information		Configure to View IGMP Snooping Information
IP Routing	IPv4 Routing Table		Configure to view IPv4 routing table information
	IPv4 Static Routes		Configuring to View IPv4 Static Route Information
Security	Worm Attack Protection		Configure to view worm attack protection information
	DDoS Attack Protection		Configure to view DDoS attack protection information
	ARP Attack Protection		Configure to view ARP attack protection information
	Current Session		Configure to view current session information
	User Management		Configure to view user management information
Artifact	Ping		Configuring to View Ping Information
	Traceroute		Configuring to View Traceroute Information

Reboot/Save	Basic Functions	Function Configuration	Configure to view multicast feature configuration information

3 Equipment Overview

As shown：



Device Information

Product ID	ZX-SWTG3DE48A6S	Image Name	uImage_v7.0.4.81.bin		
Location	--	WebImage Name	flash:/webImage.bin	Serial Number	SN-170612310110005
Device Name	Switch	BootRom Version	A.2.18	MAC Address	1C:2A:A3:14:DA:86
Contact	--	Hardware Version	4.1	Uptime	0 days, 0 hours, 27 minutes
Software	HongRui, 7.0.4.81	EPLD Version	0.0		

Copyright © Shenzhen HongRui Optical Technology Co., Ltd . All Rights Reserved.

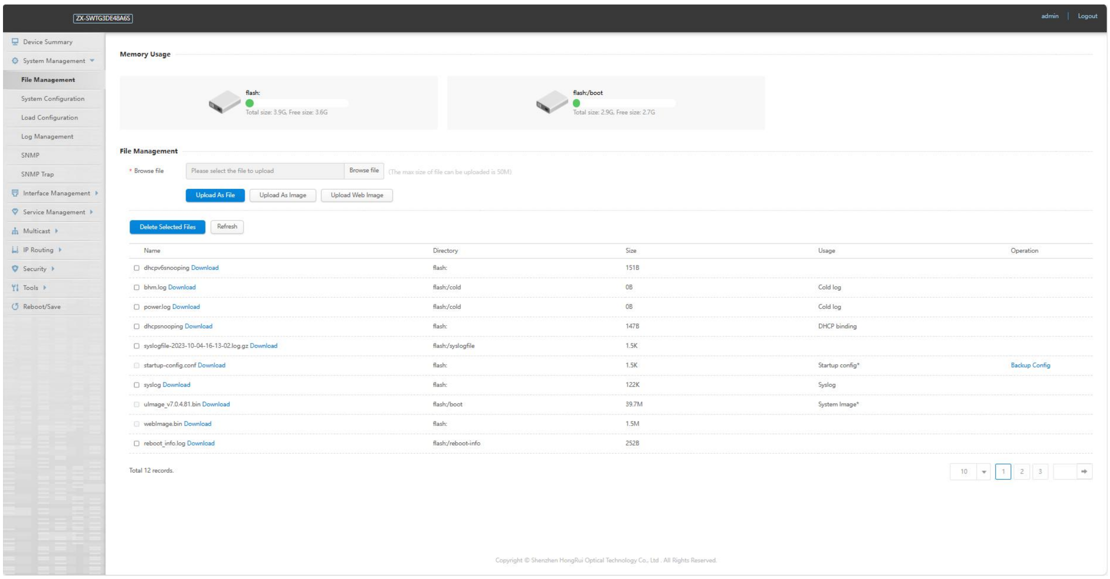
4 System Management

4.1 File Management

In the file management, there are memory usage status size flash and flash/boot, real-time view to understand the memory usage, and in the file management, you can choose to upload files, upload images, upgrade the Web Image, and download the application files, and so on.

Operation steps:

1. Click the "System Management > File Management" menu in the navigation tree to enter the system information view interface, as shown in the following figure:



Memory Usage

flash:
Total size: 3.9G, Free size: 3.6G

flash:/boot
Total size: 2.9G, Free size: 2.7G

File Management

* Browse file: Please select the file to upload [Browse file] (The max size of file can be uploaded is 50M)

[Upload As File] [Upload As Image] [Upload Web Image]

[Delete Selected Files] [Refresh]

	Name	Directory	Size	Usage	Operation
□	dhcpv6snooping Download	flash:	151B		
□	bhm.log Download	flash:/cold	0B	Cold log	
□	power.log Download	flash:/cold	0B	Cold log	
□	dhcpsnooping Download	flash:	147B	DHCP binding	
□	syslogfile-2023-10-04-16-13-02.log.gz Download	flash:/syslogfile	1.5K		
□	startup-config.conf Download	flash:	1.5K	Startup config*	Backup Config
□	syslog Download	flash:	122K	Syslog	
□	uImage_v7.0.4.81.bin Download	flash:/boot	39.7M	System Image*	
□	webImage.bin Download	flash:	1.5M		
□	reboot_info.log Download	flash:/reboot-info	252B		

Total 12 records.

10 ▾ 1 2 3 →

Copyright © Shenzhen HongRui Optical Technology Co., Ltd . All Rights Reserved.

Description:

Page has status information about memory usage.

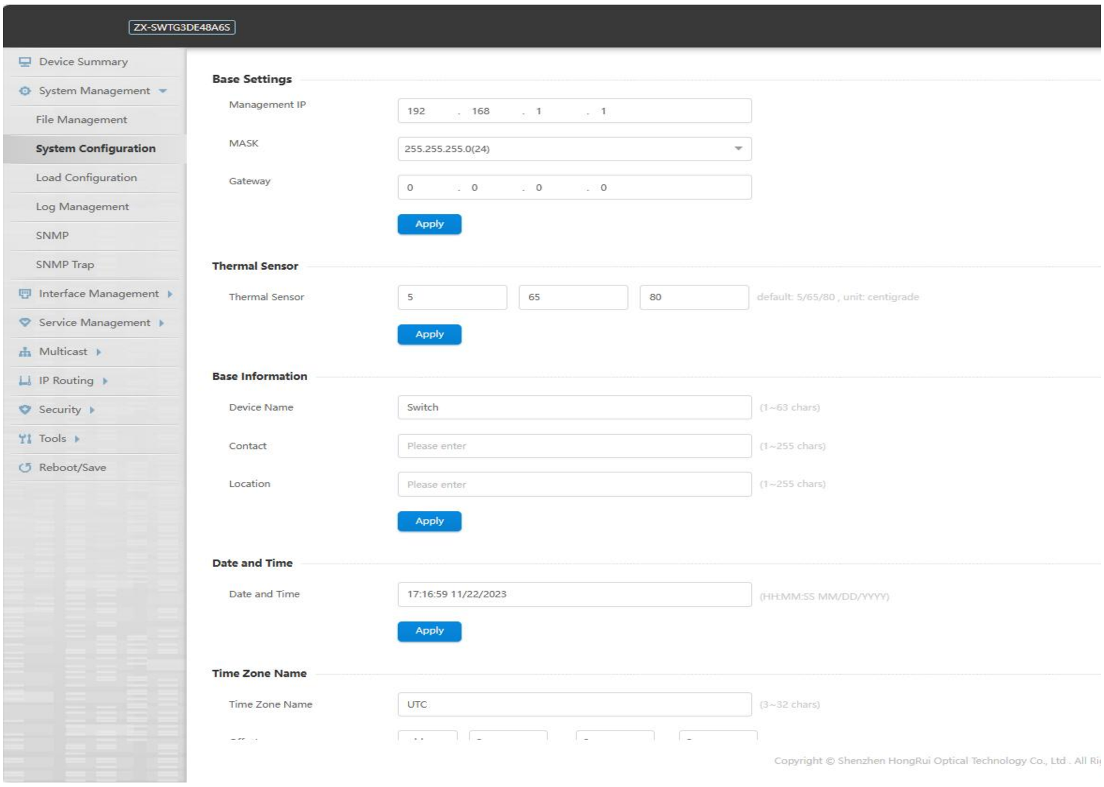
File management allows uploading files, uploading images and upgrade operations. The bottom has function to download the installation package.

4.2 System Configuration

Introduces system information, as well as temperature time and date information.

Operational Steps:

1. Click the "System Management > System Configuration" menu in the navigation tree to enter the Port Statistics interface, as shown in the following figure:



Base Settings

Management IP: 192 . 168 . 1 . 1

MASK: 255.255.255.0(24)

Gateway: 0 . 0 . 0 . 0

Thermal Sensor

Thermal Sensor: 5 | 65 | 80 default: 5/65/80 , unit: centigrade

Base Information

Device Name: Switch (1~63 chars)

Contact: Please enter (1~255 chars)

Location: Please enter (1~255 chars)

Date and Time

Date and Time: 17:16:59 11/22/2023 (HH:MM:SS MM/DD/YYYY)

Time Zone Name

Time Zone Name: UTC (3~32 chars)

Copyright © Shenzhen HongRui Optical Technology Co., Ltd . All Ri

📖 Description:

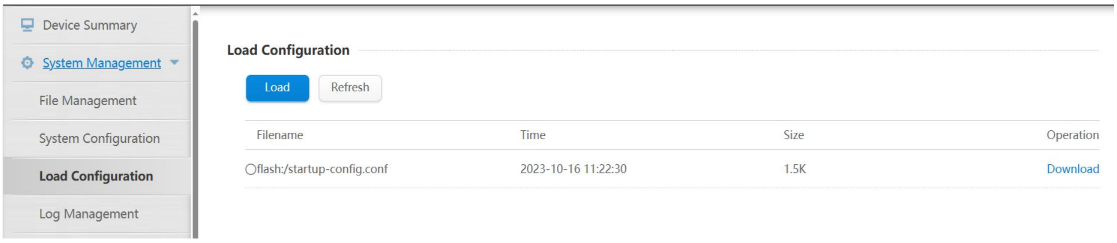
Click "Apply" after configuring, you need to save it to take effect.

4.3 Loading Configuration

Loading an application file

Operational Steps:

1. Click "System Management > Load Configuration" menu in the navigation tree to enter the Port Statistics interface, as shown in the following figure:

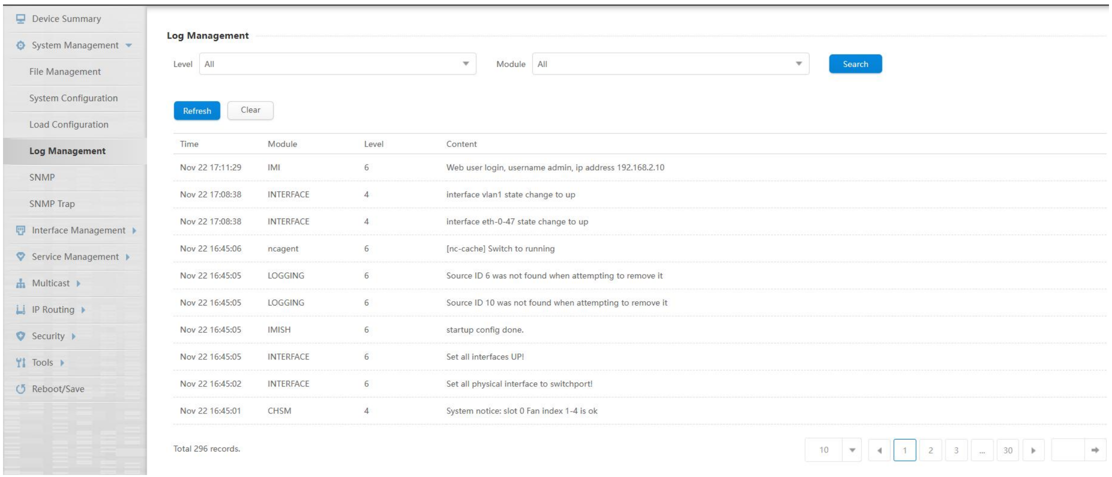


Load Configuration

Filename	Time	Size	Operation
○flash:/startup-config.conf	2023-10-16 11:22:30	1.5K	Download

4.4 Log Management

Viewing the system logs provides a clear understanding of the device status information, as shown in the following figure.



Log Management

Level: All Module: All

Time	Module	Level	Content
Nov 22 17:11:29	IMI	6	Web user login, username admin, ip address 192.168.2.10
Nov 22 17:08:38	INTERFACE	4	interface vlan1 state change to up
Nov 22 17:08:38	INTERFACE	4	interface eth-0-47 state change to up
Nov 22 16:45:06	ncagent	6	[nc-cache] Switch to running
Nov 22 16:45:05	LOGGING	6	Source ID 6 was not found when attempting to remove it
Nov 22 16:45:05	LOGGING	6	Source ID 10 was not found when attempting to remove it
Nov 22 16:45:05	IMISH	6	startup config done.
Nov 22 16:45:05	INTERFACE	6	Set all interfaces UP!
Nov 22 16:45:02	INTERFACE	6	Set all physical interface to switchport!
Nov 22 16:45:01	CHSM	4	System notice: slot 0 Fan index 1-4 is ok

Total 296 records.

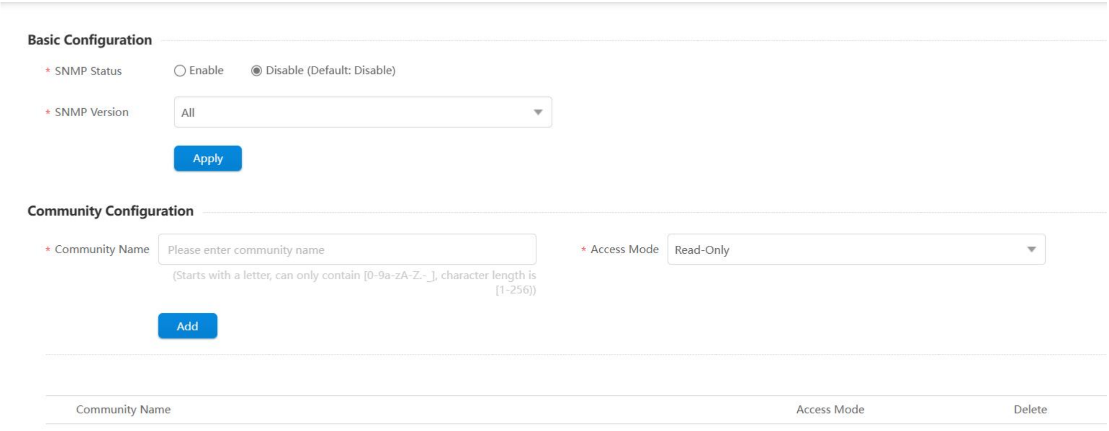
10 ◀ 1 2 3 ... 30 ▶

4.5 SNMP Configuration

You can perform basic SNMP configuration and group configuration.

Operation steps:

1. Click the "System Management > SNMP Configuration" menu in the navigation bar, you can see the SNMP information, as shown below



Basic Configuration

* SNMP Status ○ Enable ● Disable (Default: Disable)

* SNMP Version All

Community Configuration

* Community Name Please enter community name (Starts with a letter, can only contain [0-9a-zA-Z-_], character length is [1-256])

* Access Mode Read-Only

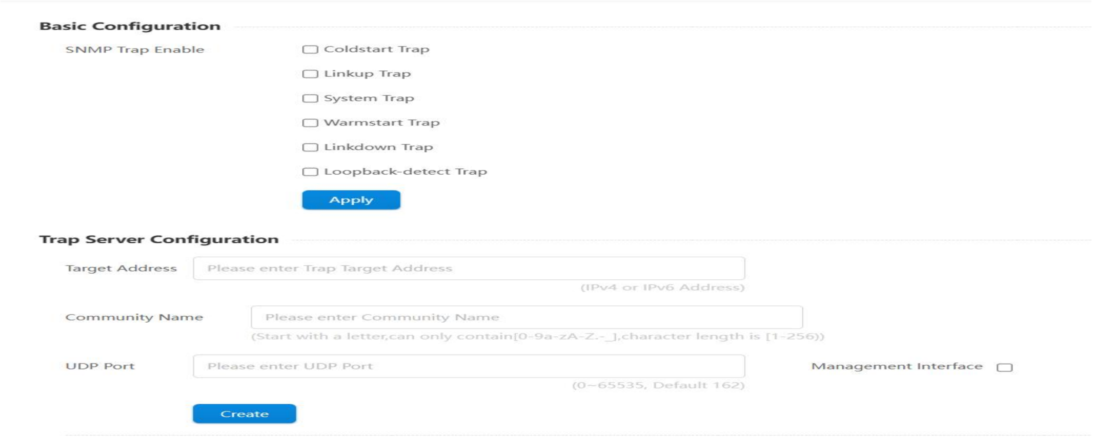
Community Name	Access Mode	Delete

4.5 SNMP Trap Configuration

You can perform basic SNMP Trap configuration and Trap target host configuration.

Operational Steps:

1. Click "System Management > SNMP Trap Configuration" in the navigation bar, you can see the information of SNMP Trap, as shown in the following figure.



Basic Configuration

SNMP Trap Enable
☐ Coldstart Trap
☐ Linkup Trap
☐ System Trap
☐ Warmstart Trap
☐ Linkdown Trap
☐ Loopback-detect Trap

Trap Server Configuration

Target Address: Please enter Trap Target Address
(IPv4 or IPv6 Address)

Community Name: Please enter Community Name
(Start with a letter,can only contain[0-9a-zA-Z.-_],character length is [1-256])

UDP Port: Please enter UDP Port
(0~65535, Default 162)

Management Interface ☐

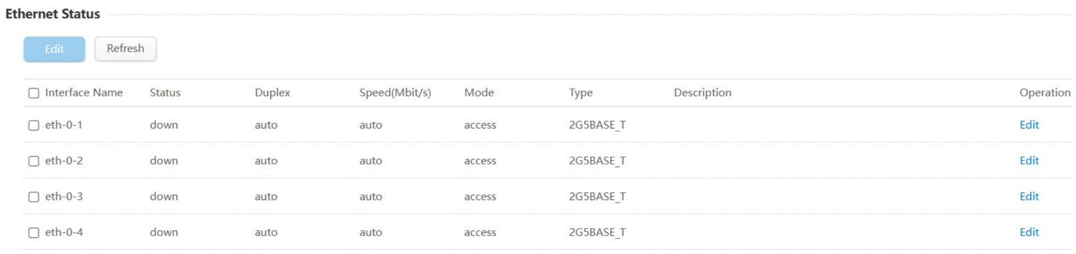
5 Port

5.1 Port Status

You can view the port status, duplex mode, rate, etc.

Operational Steps:

1. Click "Port > Port Status" menu in the navigation tree, as shown in the following figure.



Ethernet Status

☐ Interface Name	Status	Duplex	Speed(Mbit/s)	Mode	Type	Description	Operation
☐ eth-0-1	down	auto	auto	access	2G5BASE_T		Edit
☐ eth-0-2	down	auto	auto	access	2G5BASE_T		Edit
☐ eth-0-3	down	auto	auto	access	2G5BASE_T		Edit
☐ eth-0-4	down	auto	auto	access	2G5BASE_T		Edit

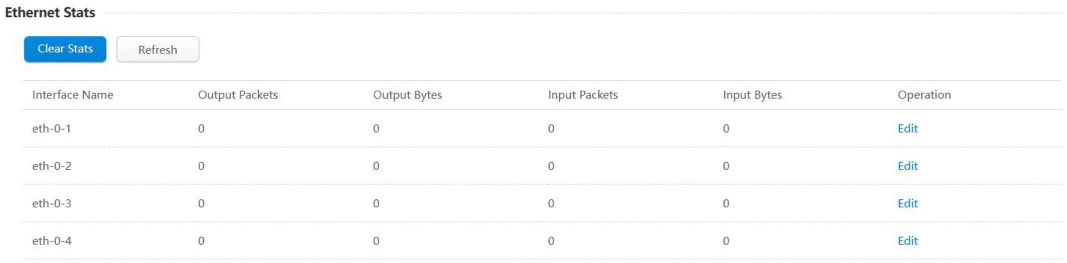
The meaning of the interface is shown in the table below

Configuration item	Description
Edit	Edits the configuration port
Refresh	Refreshes the state of the port

5.2 Port Statistics

Port statistics include statistics of egress data messages and bytes, and statistics of ingress data messages and bytes.

1. Click the "Port > Port Statistics" menu in the navigation tree to enter the "Port Statistics" interface, as shown in the following figure.



Ethernet Stats

Interface Name	Output Packets	Output Bytes	Input Packets	Input Bytes	Operation
eth-0-1	0	0	0	0	Edit
eth-0-2	0	0	0	0	Edit
eth-0-3	0	0	0	0	Edit
eth-0-4	0	0	0	0	Edit

The meaning of the interface is shown in the table below

Configuration item	Description
Clear Statistics	Clear all statistics
Refresh	Update incoming and outgoing data messages and byte statistics

5.3 Link Aggregation

Link Aggregation is a method of bundling a group of physical interfaces together as a logical interface to increase bandwidth and reliability.

Link Aggregation Group (LAG) is a logical link formed by bundling several Ethernet links together, abbreviated as Eth-Trunk.

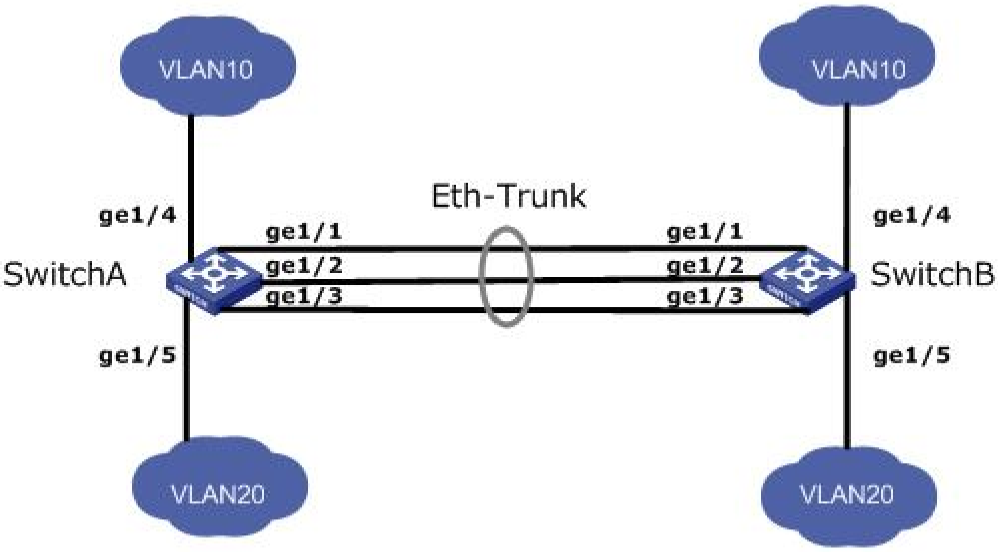
With the continuous expansion of network size, users have higher and higher requirements for link bandwidth and reliability. In traditional technology, it is common to increase the bandwidth by replacing the interface boards with high speed or by replacing the equipment that supports the interface boards with high speed, but this solution requires high cost and is not flexible enough.

The use of link aggregation technology can achieve the purpose of increasing link bandwidth by bundling multiple physical interfaces into a single logical interface without hardware upgrades. The backup mechanism of link aggregation can effectively improve reliability, and at the same time, it can also realise the load sharing of traffic on different physical links.

As shown in the figure below, SwitchA and SwitchB are connected by three Ethernet physical links, and by bundling these three links together, they become an Eth-Trunk logical link, and the bandwidth of this logical link is equal to the sum of the bandwidths of the original three Ethernet physical links, which achieves the purpose of increasing the bandwidth of the link; at the same time, these three Ethernet physical links are backed up to each other, which effectively improves the reliability of the link. At the same time, these three Ethernet physical links back up each other, which effectively

improves the reliability of the

links.



This can be achieved by configuring link aggregation when there is a need for the following:

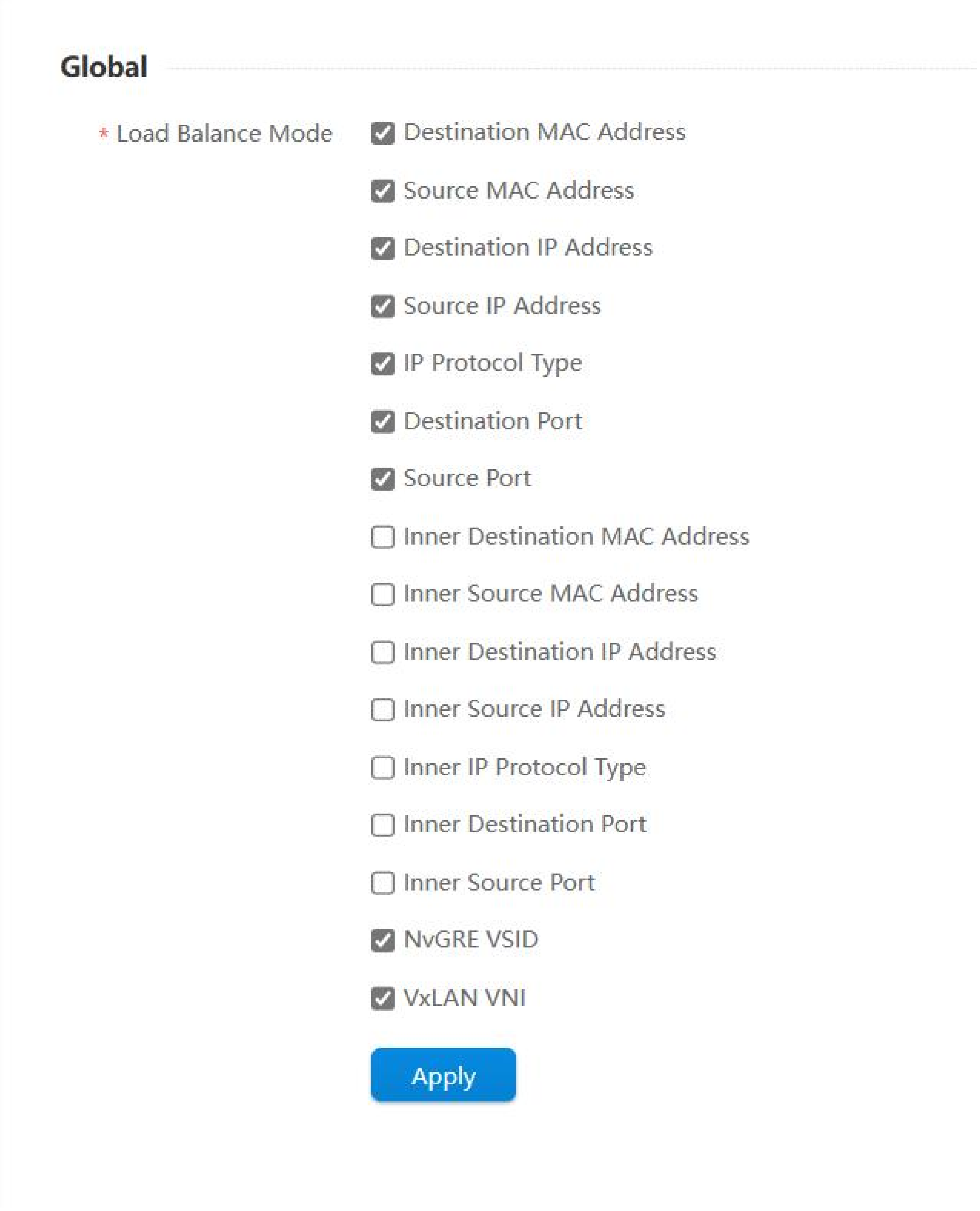
- when there is insufficient bandwidth between two switch devices connected by a single link.
- When the reliability of the connection between two switch devices over a single link does not meet the requirements.

Link aggregation is classified into static mode and LACP mode according to whether or not the Link Aggregation Control Protocol LACP is enabled. In static mode, the establishment of Eth-Trunk and the joining of member interfaces are configured manually, and there is no link aggregation control protocol involved. All active links in this mode participate in the forwarding of data and share the traffic equally, so it is called load-sharing mode. If an active link fails, the link aggregation group automatically shares the traffic equally among the remaining active links. Static mode can be used when a larger link bandwidth needs to be provided between two directly connected devices and the device does not support the LACP protocol.

5.3.1 Global configuration

Add Static Link Aggregation Procedure:

1. Click the "Port > Link Aggregation > Global Configuration" menu in the navigation bar to enter the link aggregation global configuration interface and select the load sharing mode, as shown in the following figure:



Global

* Load Balance Mode

☑ Destination MAC Address

☑ Source MAC Address

☑ Destination IP Address

☑ Source IP Address

☑ IP Protocol Type

☑ Destination Port

☑ Source Port

□ Inner Destination MAC Address

□ Inner Source MAC Address

□ Inner Destination IP Address

□ Inner Source IP Address

□ Inner IP Protocol Type

□ Inner Destination Port

□ Inner Source Port

☑ NvGRE VSID

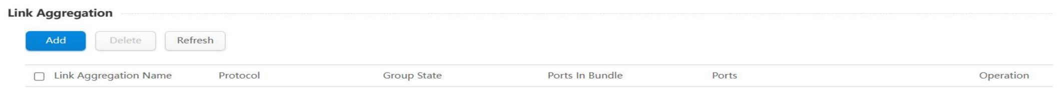
☑ VxLAN VNI

5.3.2 Port Configuration

Add Static Link Aggregation Procedure:

1. Click "Port > Link Aggregation > Port Configuration" in the navigation bar to enter the Link Aggregation Port Configuration interface, select the aggregation group and the aggregation group port members, and then click Apply to save the

configuration, as shown in the following figure:

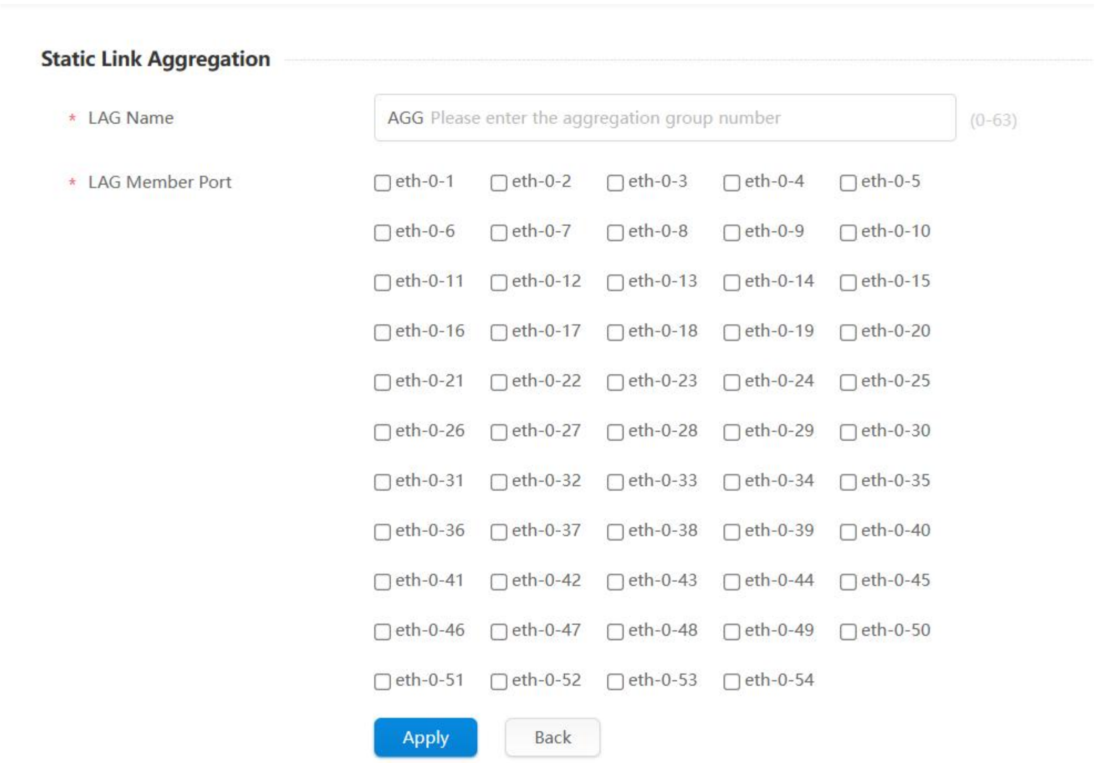


Link Aggregation

Add | Delete | Refresh

□ Link Aggregation Name	Protocol	Group State	Ports In Bundle	Ports	Operation

1. click Add to enter the static link aggregation configuration.



Static Link Aggregation

* LAG Name: AGG Please enter the aggregation group number (0-63)

* LAG Member Port:

□ eth-0-1 □ eth-0-2 □ eth-0-3 □ eth-0-4 □ eth-0-5
□ eth-0-6 □ eth-0-7 □ eth-0-8 □ eth-0-9 □ eth-0-10
□ eth-0-11 □ eth-0-12 □ eth-0-13 □ eth-0-14 □ eth-0-15
□ eth-0-16 □ eth-0-17 □ eth-0-18 □ eth-0-19 □ eth-0-20
□ eth-0-21 □ eth-0-22 □ eth-0-23 □ eth-0-24 □ eth-0-25
□ eth-0-26 □ eth-0-27 □ eth-0-28 □ eth-0-29 □ eth-0-30
□ eth-0-31 □ eth-0-32 □ eth-0-33 □ eth-0-34 □ eth-0-35
□ eth-0-36 □ eth-0-37 □ eth-0-38 □ eth-0-39 □ eth-0-40
□ eth-0-41 □ eth-0-42 □ eth-0-43 □ eth-0-44 □ eth-0-45
□ eth-0-46 □ eth-0-47 □ eth-0-48 □ eth-0-49 □ eth-0-50
□ eth-0-51 □ eth-0-52 □ eth-0-53 □ eth-0-54

Apply | Back

The meaning of the interface information is shown in the following table:

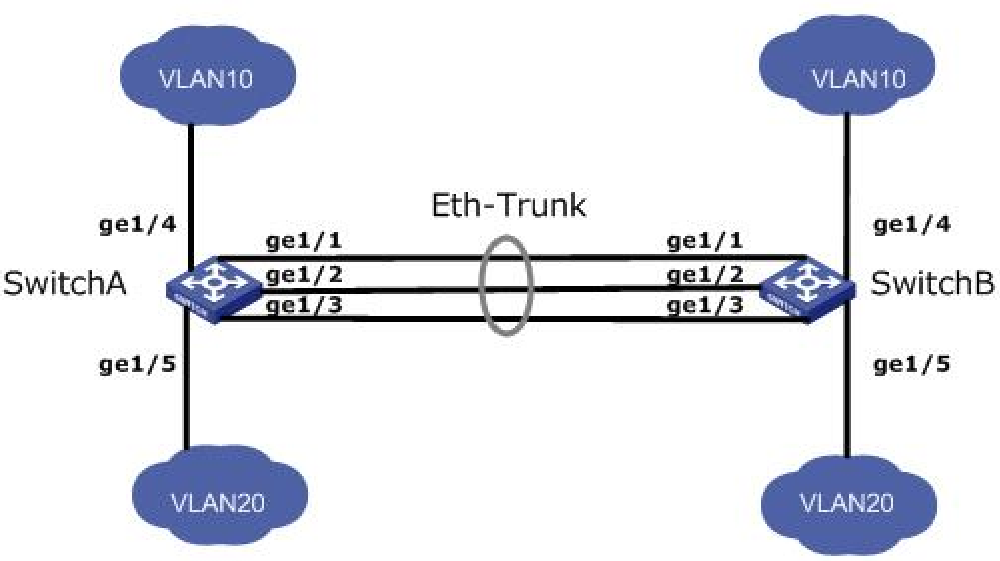
Configuration item	Description
Aggregation Group	Link aggregation group ID, there are 0 ~ 63
Aggregation group member port	Ports can be selected for aggregation binding, effective after applying.

Example:

As shown in the figure below, SwitchA and SwitchB are both connected to the network

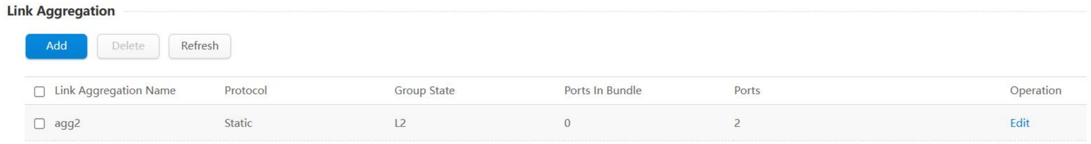
in VLAN 10 and VLAN 20, respectively, via Ethernet links, and there is a large amount of data traffic between SwitchA and SwitchB.

The user wants to provide a larger link bandwidth between SwitchA and SwitchB to enable the same VLANs to communicate with each other. The user also wants to provide some redundancy to ensure data transmission and link reliability.



Operation steps:

1. Create an Eth-Trunk interface in SwitchA and add member interfaces to increase the link bandwidth, and the configuration of SwitchB is similar to that of SwitchA. Click "Port > Link Aggregation > Port Configuration" in the navigation bar, click Add to enter the static link aggregation configuration interface, select the group "AGG 1", select the ports ge1, ge2 and ge3 that need to be aggregated, click the right arrow to move to the selected ports, click "Add", and then click "Add". selected ports, click "Apply" to take effect, as shown in the following figure.



Link Aggregation

☐ Link Aggregation Name	Protocol	Group State	Ports In Bundle	Ports	Operation
☐ agg2	Static	L2	0	2	Edit

5.4 Storm control

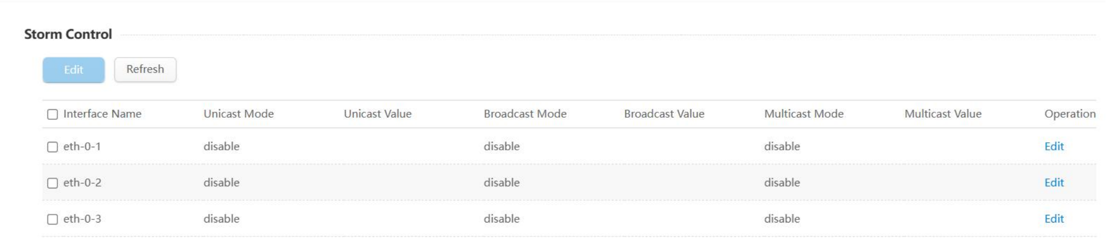
Storm control prevents broadcast, unknown multicast, and unknown unicast messages from generating broadcast storms in the following forms. The device supports storm control by packet rate for each of these three types of messages under the interface. During a detection interval, the device monitors the average rate of the three types of messages received under an interface and compares it with the configured maximum threshold; when the message rate is greater than the configured maximum threshold, the device performs storm control on the interface and executes the configured storm control actions.

When a Layer 2 Ethernet interface receives a broadcast, multicast, or unknown unicast message, if the device cannot specify the outgoing interface of the message based on the destination MAC address of the message, the device forwards the message to other Layer 2 Ethernet interfaces within the same VLAN (Virtual Local Area Network), which may result in a broadcast storm and reduce the forwarding performance of the device.

Introducing the storm suppression feature can control the traffic of these three types of messages and prevent broadcast storms.

Operational Steps:

1. Click the "Port > Storm Control" menu in the navigation tree to enter the interface, as shown in the following figure:

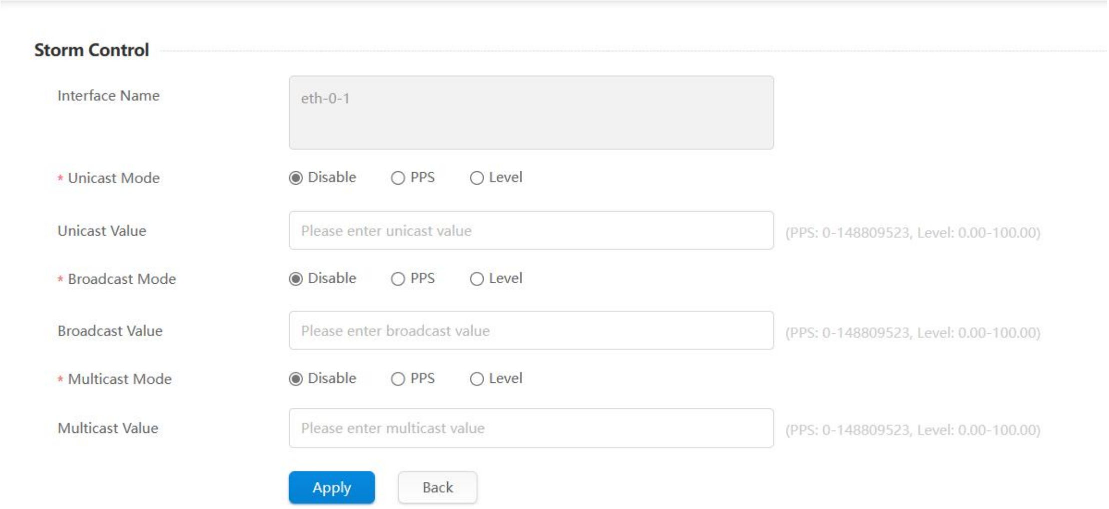


Storm Control

Edit Refresh

□ Interface Name	Unicast Mode	Unicast Value	Broadcast Mode	Broadcast Value	Multicast Mode	Multicast Value	Operation
□ eth-0-1	disable		disable		disable		Edit
□ eth-0-2	disable		disable		disable		Edit
□ eth-0-3	disable		disable		disable		Edit

2. Select the port list and click "Edit" to configure the control switch as shown in the figure below:



Storm Control

Interface Name: eth-0-1

* Unicast Mode: ● Disable ○ PPS ○ Level

Unicast Value: Please enter unicast value (PPS: 0-148809523, Level: 0.00-100.00)

* Broadcast Mode: ● Disable ○ PPS ○ Level

Broadcast Value: Please enter broadcast value (PPS: 0-148809523, Level: 0.00-100.00)

* Multicast Mode: ● Disable ○ PPS ○ Level

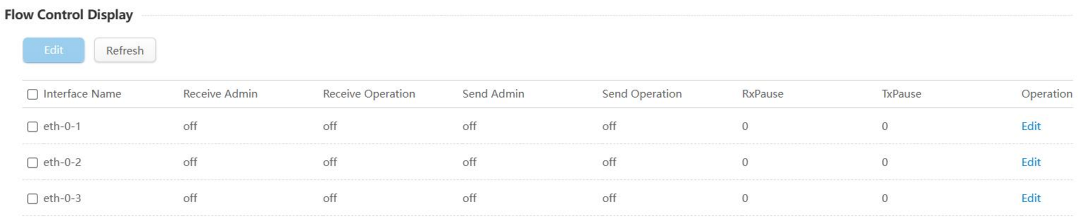
Multicast Value: Please enter multicast value (PPS: 0-148809523, Level: 0.00-100.00)

Apply Back

5.5 Flow control

Operational Steps:

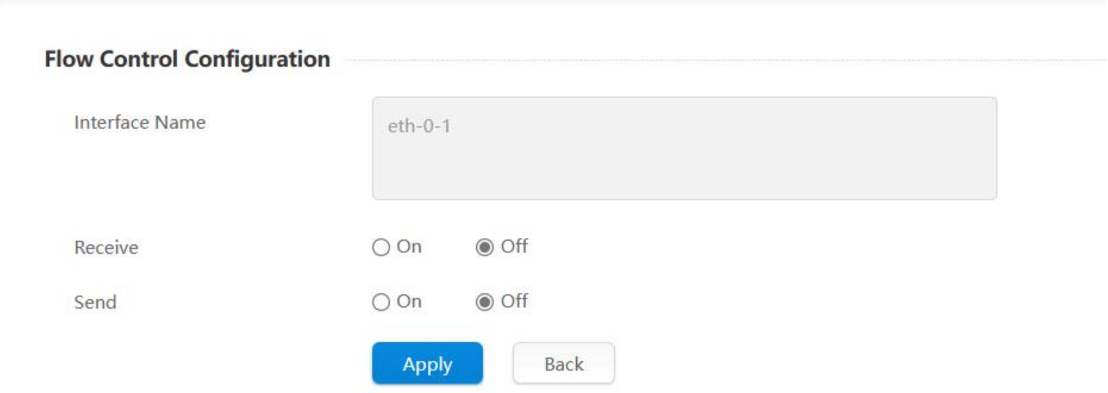
1. Click "Port > Flow Control" menu in the navigation tree to enter the interface, as shown in the following figure:



Flow Control Display

□ Interface Name	Receive Admin	Receive Operation	Send Admin	Send Operation	RxPause	TxPause	Operation
□ eth-0-1	off	off	off	off	0	0	Edit
□ eth-0-2	off	off	off	off	0	0	Edit
□ eth-0-3	off	off	off	off	0	0	Edit

2. Select the port list and click "Edit" to configure the control switch as shown in the figure below:



Flow Control Configuration

Interface Name: eth-0-1

Receive: ○ On ● Off

Send: ○ On ● Off

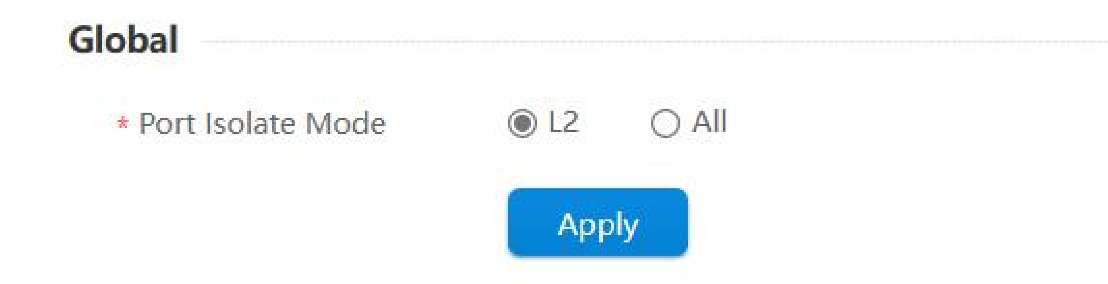
5.6 Port isolation

Sometimes port traffic does not need to communicate with each other, but broadcast, multicast and other messages will flood to each port, this time you can use the port isolation function to achieve port to port message isolation.

5.6.1 Global configuration

Operational Steps:

1. Click "Port > Port Isolation > Global Configuration" in the navigation tree to enter the interface, as shown in the following figure:

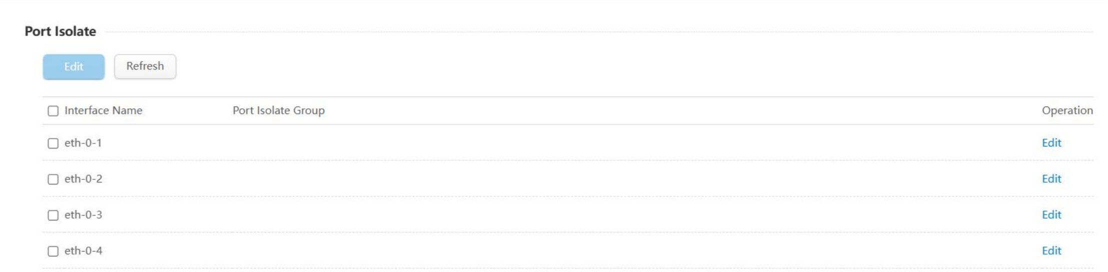


Global

* Port Isolate Mode ● L2 ○ All

5.6.2 Port Configuration

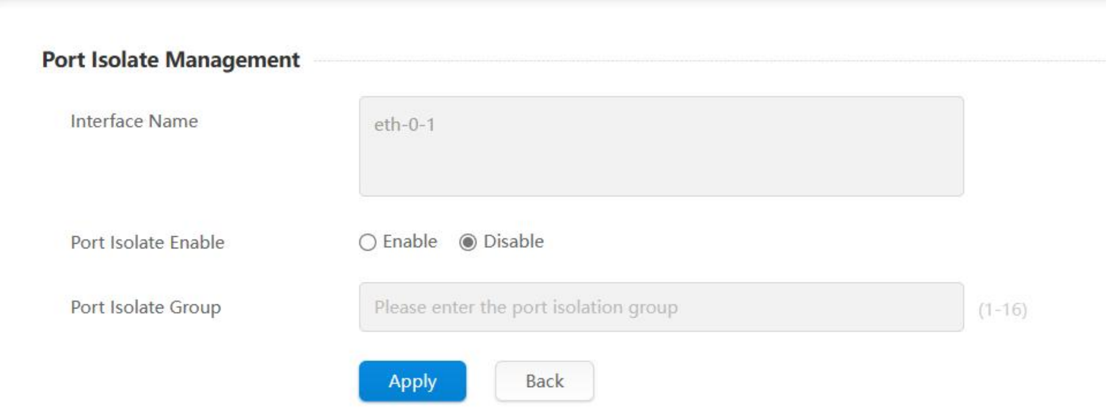
1. Click "Port > Port Isolation > Port Configuration" in the navigation tree to enter the interface, as shown in the following figure:



Port Isolate

□ Interface Name	Port Isolate Group	Operation
□ eth-0-1		Edit
□ eth-0-2		Edit
□ eth-0-3		Edit
□ eth-0-4		Edit

2. Select a port and click Edit to enter the port isolation management interface, as shown in the following figure:



Port Isolate Management

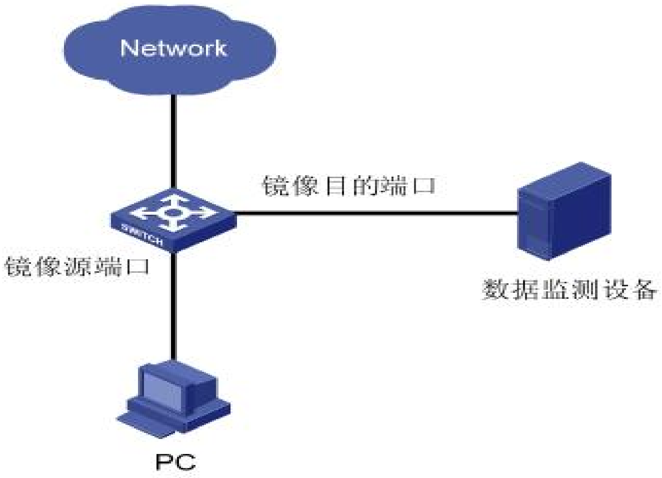
Interface Name: eth-0-1

Port Isolate Enable: ○ Enable ● Disable

Port Isolate Group: Please enter the port isolation group (1-16)

5.7 Port mirroring

Port mirroring is the copying of messages from a specified port of a switch to a destination port; where the port being copied is called the source port and the copied port is called the destination port. The destination port will have access to data inspection devices, which users use to analyse the messages received on the destination port for network monitoring and troubleshooting. This is shown in the figure below:



Configuration Example

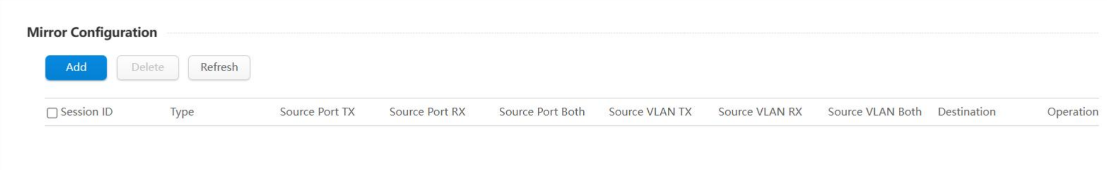
PC1 is connected to SwitchA through interface ge1. PC2 is directly connected to the ge2 interface of SwitchA.

The user wants to monitor the messages sent by PC1 through the monitoring device PC2.

5.7.1 Profile

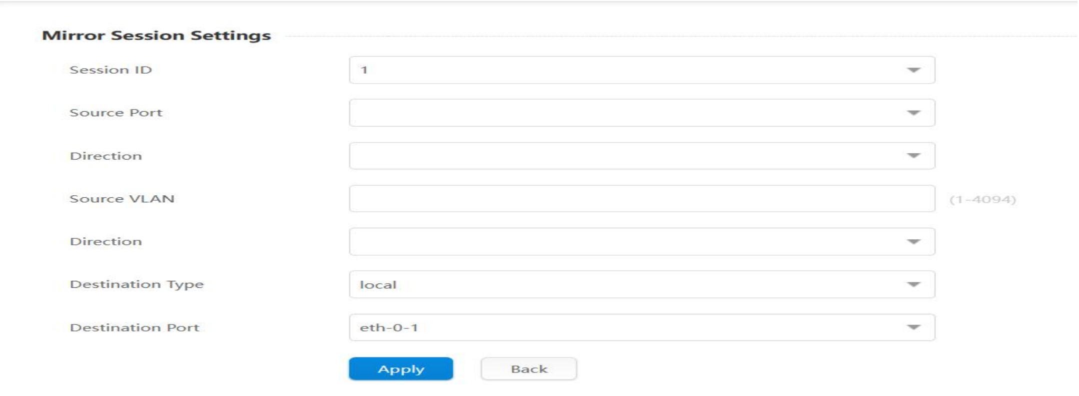
1. Operational Steps:

Click "Port > Port Mirroring > Overview" in the navigation bar to enter the Port Mirroring Configuration page. You can configure three groups of flow mirroring rules on this page, and the interface is as follows:



□ Session ID	Type	Source Port TX	Source Port RX	Source Port Both	Source VLAN TX	Source VLAN RX	Source VLAN Both	Destination	Operation

1. Select one of the mirror sessions and click the Modify button to enter the mirror group configuration interface:



Mirror Session Settings

Session ID	1
Source Port	
Direction	
Source VLAN	(1-4094)
Direction	
Destination Type	local
Destination Port	eth-0-1

The meaning of the interface information is shown in the table below

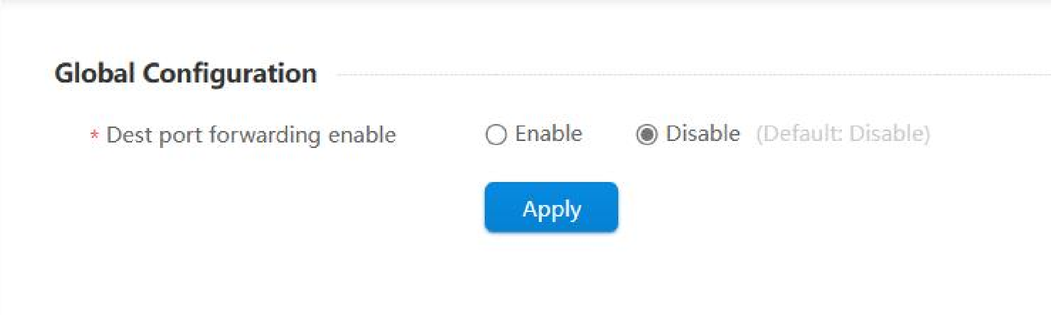
configuration item	Clarification
Session ID	The switch has three mirrored session IDs by default
Source Port	Any transmit packets on this port are mirrored to the destination port.
Direction	Optionally receive or transmit, any receive or transmit packets on this port are mirrored to the destination port
Source VLAN	About the port's VLAN
Direction	Optionally, any incoming or outgoing packets on this port are mirrored to the destination port.
Destination Type	Selectable destination type, local/remote

Destination Port	Cannot be a link aggregation port, only a normal physical port can be selected as the destination port, and cannot be selected as the source port at the same time.

5.7.2 Global configuration

Operational Steps:

Click the "Port > Port Mirroring > Global Configuration" menu in the navigation bar to enter the Port Mirroring Global Configuration page. The interface is as follows:



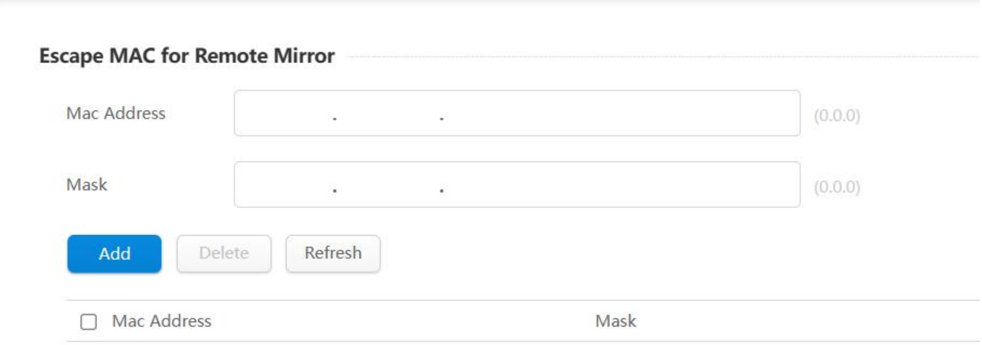
Global Configuration

* Dest port forwarding enable ○ Enable ● Disable (Default: Disable)

5.7.3 Remote Mirror MAC Escape

Operational Steps:

Click "Port > Port Mirroring > Remote Mirror MAC Escape" menu in the navigation bar to enter the Port Mirroring global configuration page. The interface is as follows:



Escape MAC for Remote Mirror

Mac Address . . (0.0.0)

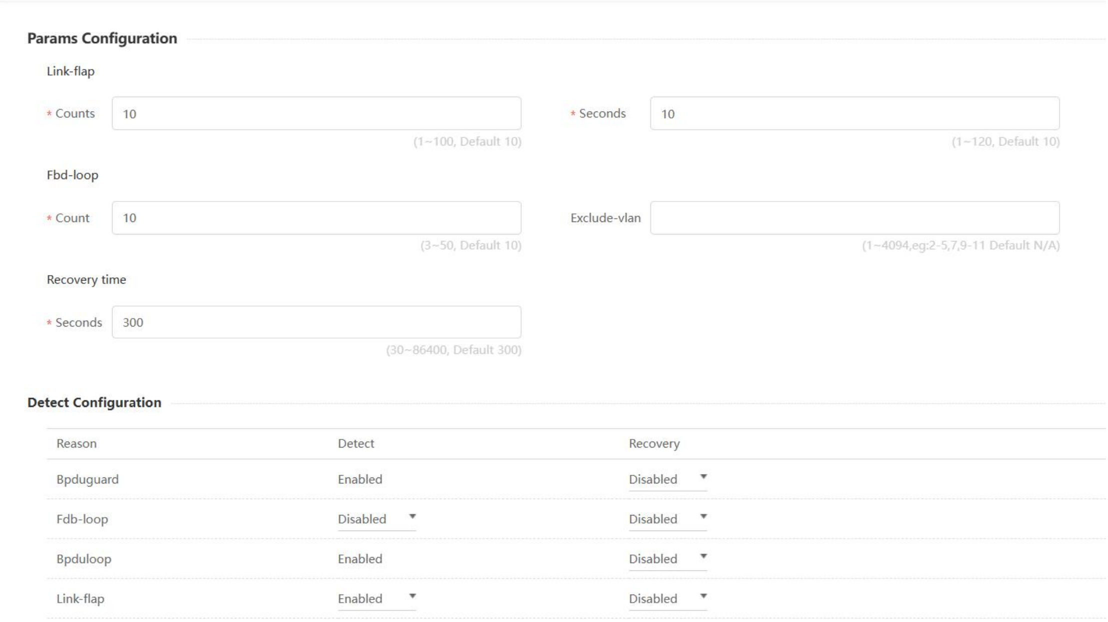
Mask . . (0.0.0)

□ Mac Address	Mask

5.8 Port Monitoring

Operational Steps:

Click the "Port > Port Monitoring" menu in the navigation bar to enter the Port Mirroring Global Configuration page. The interface is as follows:



Params Configuration

Link-flap

* Counts 10 (1~100, Default 10)

* Seconds 10 (1~120, Default 10)

Fbd-loop

* Count 10 (3~50, Default 10)

Exclude-vlan (1~4094,eg:2-5,7,9-11 Default N/A)

Recovery time

* Seconds 300 (30~86400, Default 300)

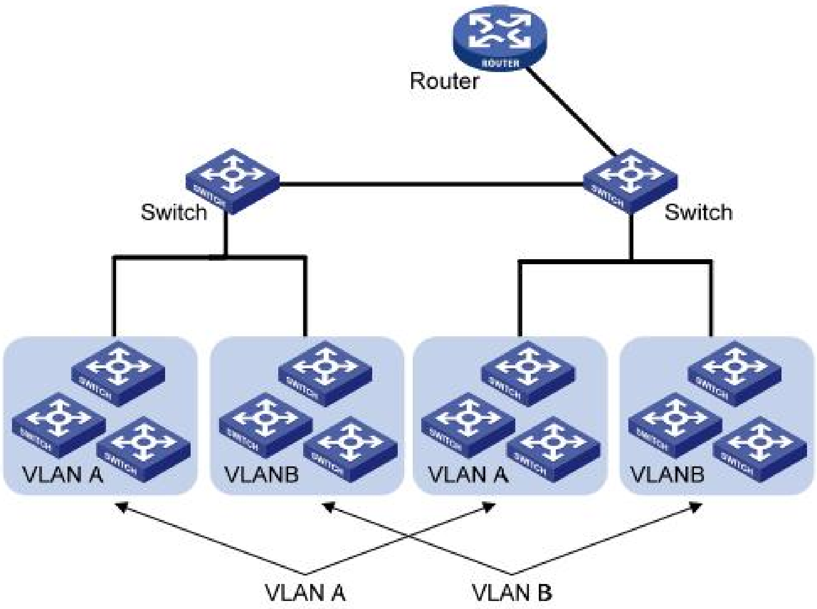
Detect Configuration

Reason	Detect	Recovery
Bpduguard	Enabled	Disabled ▾
Fdb-loop	Disabled ▾	Disabled ▾
Bpduloop	Enabled	Disabled ▾
Link-flap	Enabled ▾	Disabled ▾

6 Service management

6.1 VLAN

The composition of VLANs is not limited by physical location, so hosts within a VLAN do not need to be placed in the same physical space. As shown in the figure below, a VLAN divides a physical LAN into multiple logical LANs, each of which is a broadcast domain. hosts within a VLAN can interact with each other by using traditional Ethernet communications, while hosts in different VLANs must communicate with each other through network layer devices such as routers or Layer 3 switches.



VLANs offer the following advantages over traditional Ethernet:

- Controlling the range of broadcast domains: broadcast messages in the LAN are limited to one VLAN, saving bandwidth and improving network processing power.
- Enhanced LAN security: Because messages are isolated at the data link layer by the broadcast domain delineated by VLANs, hosts within each VLAN cannot communicate directly with each other, and need to forward the messages at Layer 3 through network layer devices such as routers or Layer 3 switches.
- Flexible creation of virtual workgroups: VLANs can be used to create virtual workgroups across physical network ranges, allowing users to access the network without changing network configurations when their physical location

is moved within the virtual workgroup range.

This managed switch supports 802.1Q VLANs, protocol-based VLANs, MAC-based VLANs, and port-based VLANs.In the default configuration, the VLAN is in 802.1Q VLAN mode.

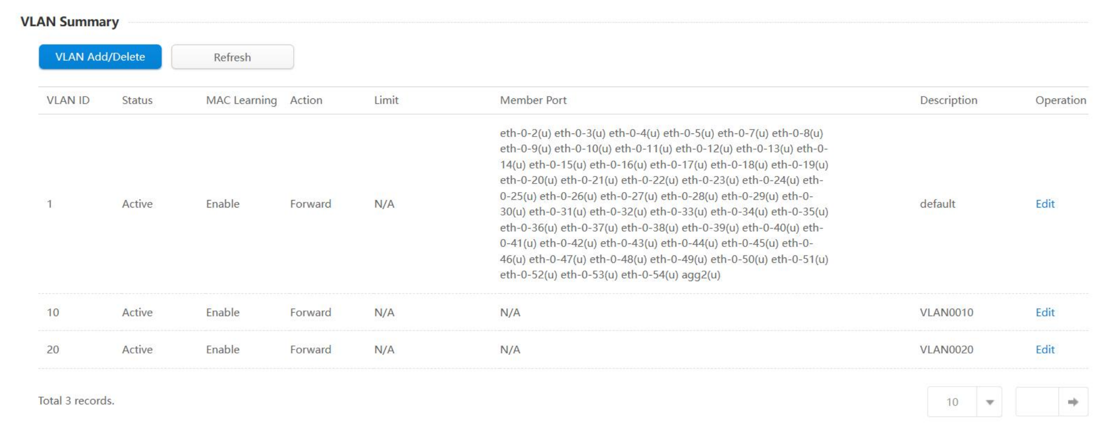
Port-based VLANs, which works by dividing VLANs based on the interface number of the switching device.The network administrator configures each interface of the switch with a different PVID, which is the VLAN to which an interface belongs by default.When a data frame enters a switch interface, if it does not come with a VLAN tag, and if a PVID is configured on the interface, then the frame is tagged with the interface's PVID.If the incoming frame is already VLAN-tagged, the switch does not add a VLAN tag, even if the interface is configured with a PVID.

The handling of VLAN frames is determined by the interface type. The advantage is the simplicity of defining members. The disadvantage is that VLAN reconfiguration is required for member movement.

6.1.1 VLAN status

Operational Steps:

Click the "Service Management > VLAN > VLAN Status" menu in the navigation tree to enter the VLAN Status interface to view the VLAN ID, status, MAC learning, actions, MAC learning maximum entries, member ports, and other information. As shown in the figure:



VLAN Summary

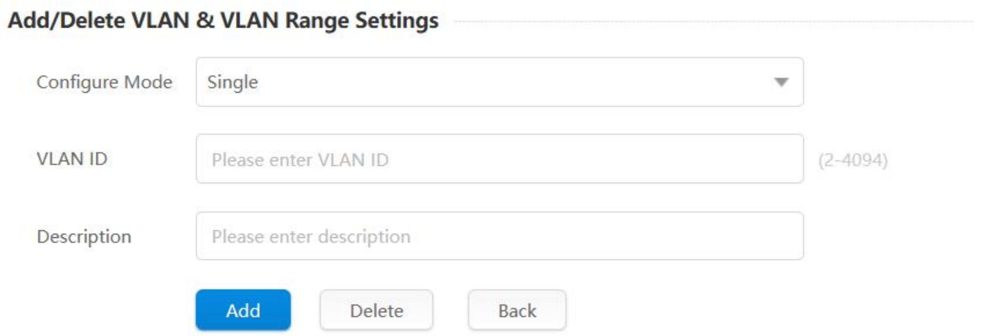
VLAN ID	Status	MAC Learning	Action	Limit	Member Port	Description	Operation
1	Active	Enable	Forward	N/A	eth-0-2(u) eth-0-3(u) eth-0-4(u) eth-0-5(u) eth-0-7(u) eth-0-8(u) eth-0-9(u) eth-0-10(u) eth-0-11(u) eth-0-12(u) eth-0-13(u) eth-0-14(u) eth-0-15(u) eth-0-16(u) eth-0-17(u) eth-0-18(u) eth-0-19(u) eth-0-20(u) eth-0-21(u) eth-0-22(u) eth-0-23(u) eth-0-24(u) eth-0-25(u) eth-0-26(u) eth-0-27(u) eth-0-28(u) eth-0-29(u) eth-0-30(u) eth-0-31(u) eth-0-32(u) eth-0-33(u) eth-0-34(u) eth-0-35(u) eth-0-36(u) eth-0-37(u) eth-0-38(u) eth-0-39(u) eth-0-40(u) eth-0-41(u) eth-0-42(u) eth-0-43(u) eth-0-44(u) eth-0-45(u) eth-0-46(u) eth-0-47(u) eth-0-48(u) eth-0-49(u) eth-0-50(u) eth-0-51(u) eth-0-52(u) eth-0-53(u) eth-0-54(u) agg2(u)	default	Edit
10	Active	Enable	Forward	N/A	N/A	VLAN0010	Edit
20	Active	Enable	Forward	N/A	N/A	VLAN0020	Edit

Total 3 records.

6.1.2 VLAN 添加/删除

Operational Steps:

1. Click "Service Management > VLAN > VLAN Add/Remove" menu in the navigation tree to enter the VLAN add/remove interface, you can choose single or range in the configuration mode, and enter a number in the range of 2-4094 for VLAN ID (you can create up to 256 VLANs), click "Add" to save and take effect. Click "Add" to save and take effect, as shown in the following figure:

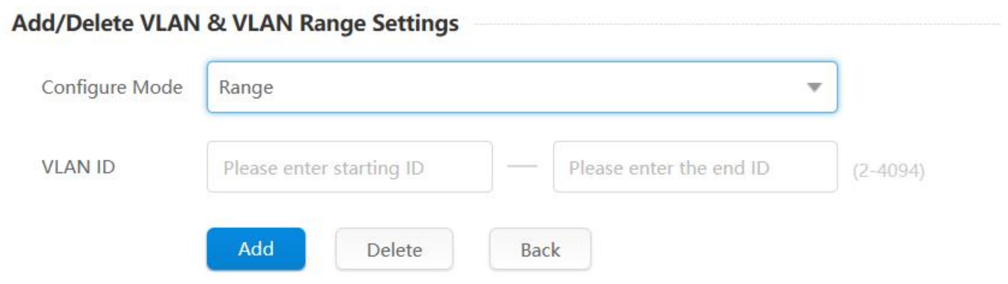


Add/Delete VLAN & VLAN Range Settings

Configure Mode: Single

VLAN ID: Please enter VLAN ID (2-4094)

Description: Please enter description



Add/Delete VLAN & VLAN Range Settings

Configure Mode: Range

VLAN ID: Please enter starting ID — Please enter the end ID (2-4094)

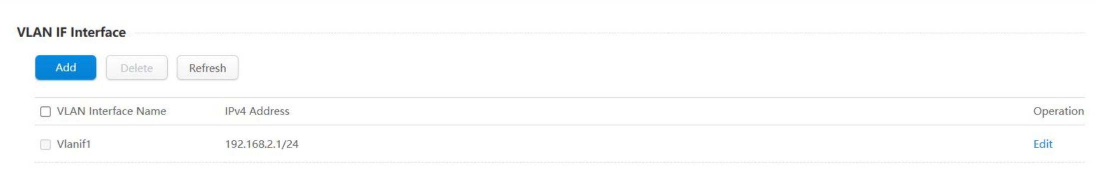
The meaning of the interface information is shown in the following table.

Configuration item	Description
Configuration Mode	Single or range can be selected
VLAN ID	Required, specify the join VLAN ID number, the value range is 1~4094. e.g. 1-3, 5, 7, 9. where VLAN 1 is the default, VLAN 1 will not be recreated when you create a new one.
Description	Optional, the specific description of the VLAN, which can be modified as needed.

6.1.3 VLANIF port

Operational Steps:

Click "Service Management > VLAN > VLANIF Port" menu in the navigation tree to enter the VLANIF Port interface and view the VLANIF port information. As shown in the figure:



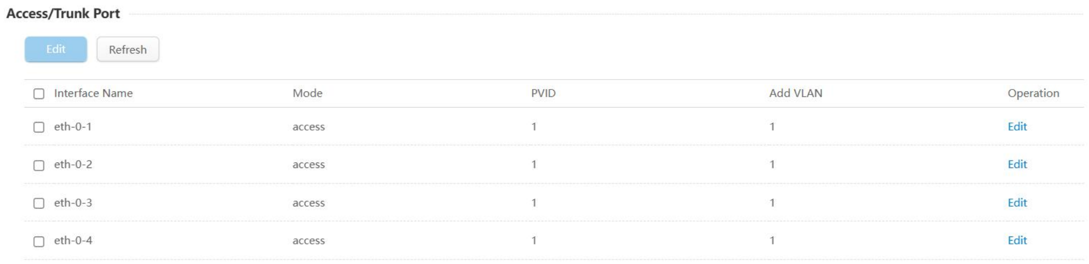
VLAN IF Interface

□ VLAN Interface Name	IPv4 Address	Operation
□ Vlanif1	192.168.2.1/24	Edit

6.1.4 Access/Trunk port

Operational Steps:

Click "Service Management > VLAN > Access/Trunk Ports" menu in the navigation tree to enter the Access/Trunk Ports interface and view the Access/Trunk port information. As shown in the figure:



Access/Trunk Port

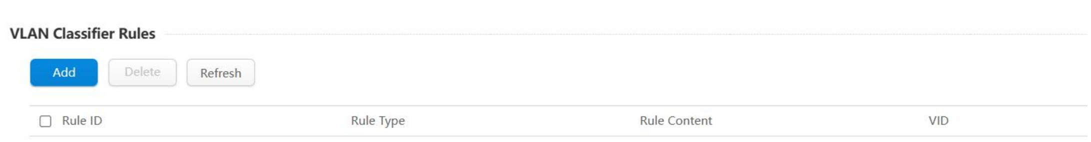
□ Interface Name	Mode	PVID	Add VLAN	Operation
□ eth-0-1	access	1	1	Edit
□ eth-0-2	access	1	1	Edit
□ eth-0-3	access	1	1	Edit
□ eth-0-4	access	1	1	Edit

6.2 VLAN Classification

6.2.1 State of affairs

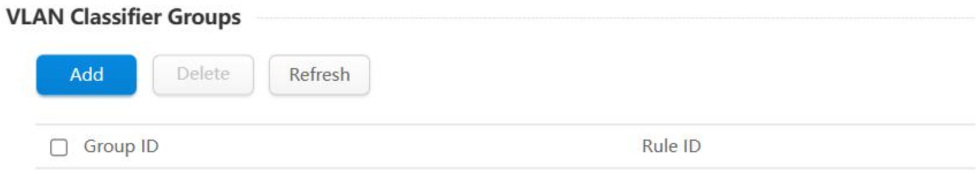
Operational Steps:

Click the "Service Management > VLAN Classification > Status" menu in the navigation tree to enter the Status interface and view the VLAN classification rules, VLAN classification groups, VLAN classification usage and other information. As shown in the figure:



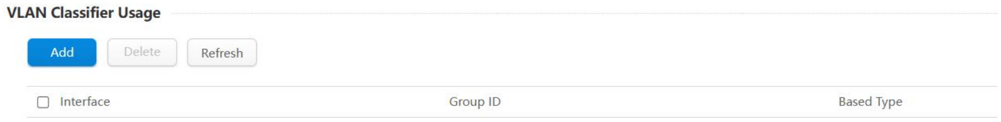
VLAN Classifier Rules

□ Rule ID	Rule Type	Rule Content	VID



VLAN Classifier Groups

□ Group ID	Rule ID



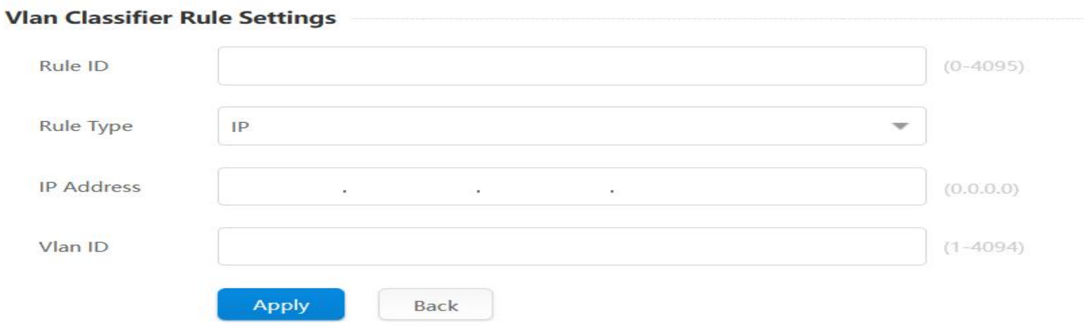
VLAN Classifier Usage

□ Interface	Group ID	Based Type

6.2.2 VLAN Rule Setting

Operational Steps:

Click "Service Management > VLAN Classification > VLAN Rule Setting" menu in the navigation tree to enter the VLAN Rule Setting interface, as shown in the figure:



Vlan Classifier Rule Settings

Rule ID (0-4095)

Rule Type: IP

IP Address . . . (0.0.0.0)

Vlan ID (1-4094)

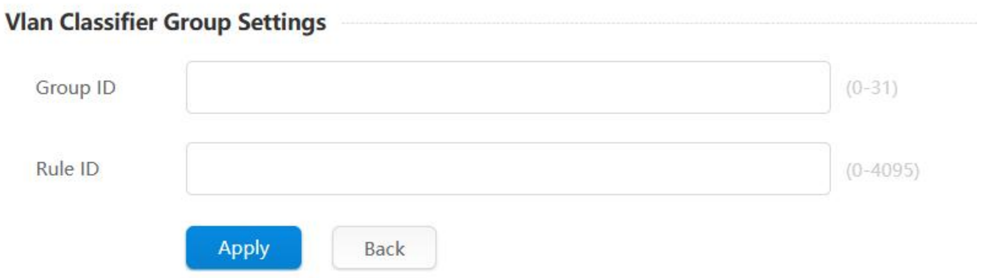
The meaning of the interface information is shown in the following table.

Configuration item	Description
Rule ID	Rule number 0-4095
Rule Type	Optional IP, MAC, Protocol
VLAN ID	VLAN created

6.2.3 VLAN Classification Group Settings

Operational Steps:

Click "Service Management > VLAN Classification > VLAN Classification Group Setting" menu in the navigation tree to enter the VLAN Classification Group Setting interface, as shown in the figure:


Vlan Classifier Group Settings

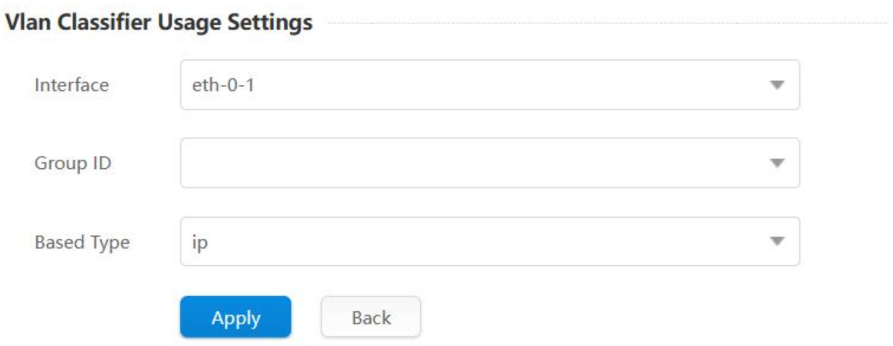
Group ID (0-31)

Rule ID (0-4095)

6.2.4 VLAN Classification Purpose Setting

Operational Steps:

Click "Service Management > VLAN Classification > VLAN Classification Purpose Setting" menu in the navigation tree to enter the VLAN Classification Purpose Setting interface, as shown in the figure:


Vlan Classifier Usage Settings

Interface: eth-0-1

Group ID:

Based Type: ip

6.3 MAC

6.3.1 MAC address table

The main function of an Ethernet switch is to forward messages at the data link layer, that is, to output the messages to the corresponding ports according to the destination MAC addresses of the messages. The MAC address forwarding table is a Layer 2 forwarding table that contains the correspondence between MAC addresses and forwarding ports, and it is the basis for Ethernet switches to realize fast forwarding of Layer 2 messages.

The table entries of the MAC address forwarding table contain the following information:

- destination MAC address
- VLAN ID to which the port belongs
- Forwarding port number on this device

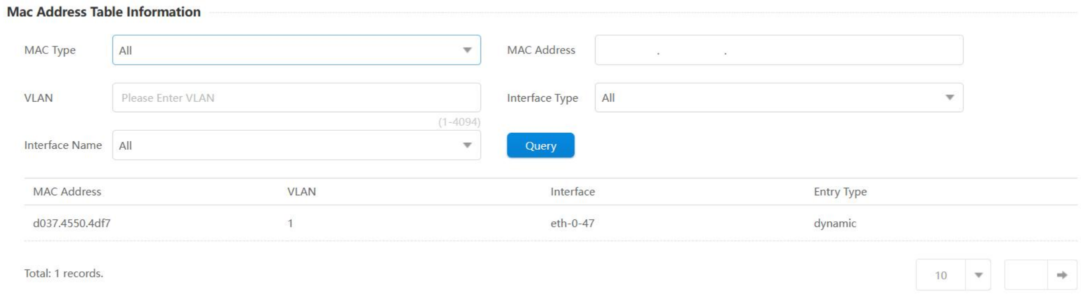
When forwarding a message, the Ethernet switch takes the following two forwarding methods according to the MAC address table entry information:

- Unicast mode: when the MAC address forwarding table contains a table entry corresponding to the destination MAC address of the message, the switch sends the message directly from the forwarding port in that table entry.
- Broadcast method: when the switch receives a message with destination address of all F, or the MAC address forwarding table does not contain a table entry corresponding to the destination MAC address of the message, the

switch will take the broadcast method to forward the message to all ports except the receiving port.

Operational Steps:

Click "Service Management > MAC > MAC Address Table" menu in the navigation tree to enter the MAC Address Table interface, as shown in the figure:



Mac Address Table Information

MAC Type: All

MAC Address: . .

VLAN: Please Enter VLAN (1-4094)

Interface Type: All

Interface Name: All

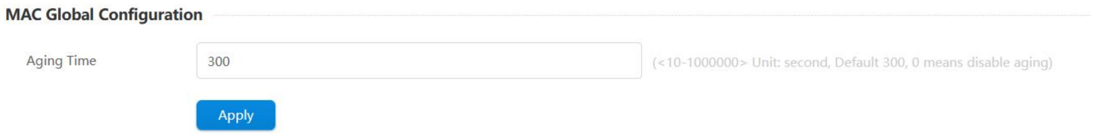
MAC Address	VLAN	Interface	Entry Type
d037.4550.4df7	1	eth-0-47	dynamic

Total: 1 records.

6.3.2 MAC Global Configuration

Operational Steps:

Click "Service Management > MAC > MAC Global Configuration" menu in the navigation tree to enter the MAC Global Configuration interface, as shown in the figure:



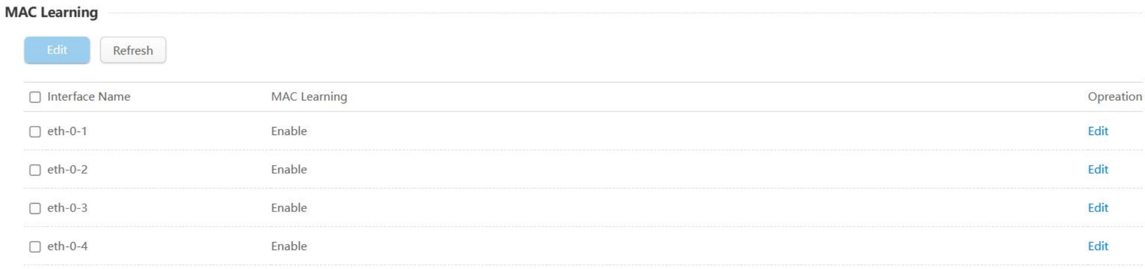
MAC Global Configuration

Aging Time: 300 (<10-1000000> Unit: second, Default 300, 0 means disable aging)

6.3.3 MAC Learning

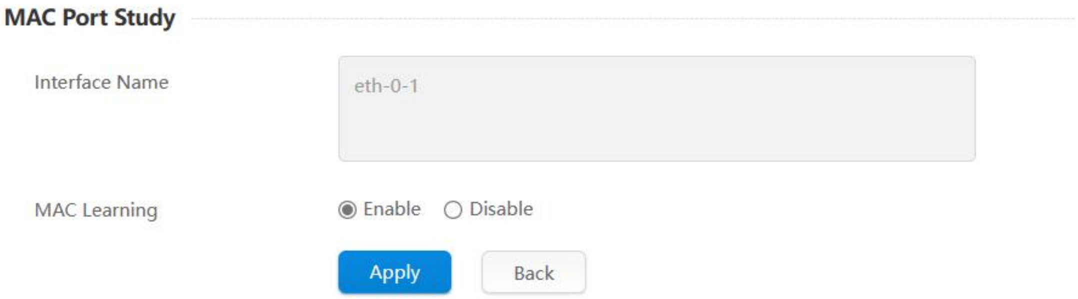
Operational Steps:

Click "Service Management > MAC > MAC Learning" menu in the navigation tree to enter the MAC Learning interface, as shown in the figure:



MAC Learning

□ Interface Name	MAC Learning	Opreation
□ eth-0-1	Enable	Edit
□ eth-0-2	Enable	Edit
□ eth-0-3	Enable	Edit
□ eth-0-4	Enable	Edit



MAC Port Study

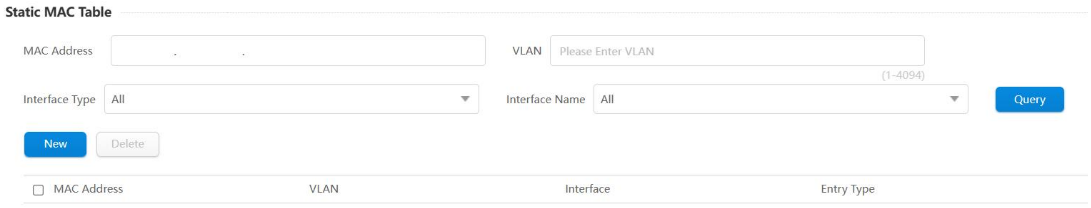
Interface Name: eth-0-1

MAC Learning: ● Enable ○ Disable

6.3.4 Static MAC address table

Operational Steps:

Click the "Service Management > MAC > Static MAC Address Table" menu in the navigation tree to enter the Static MAC Address Table interface, as shown in the figure:



Static MAC Table

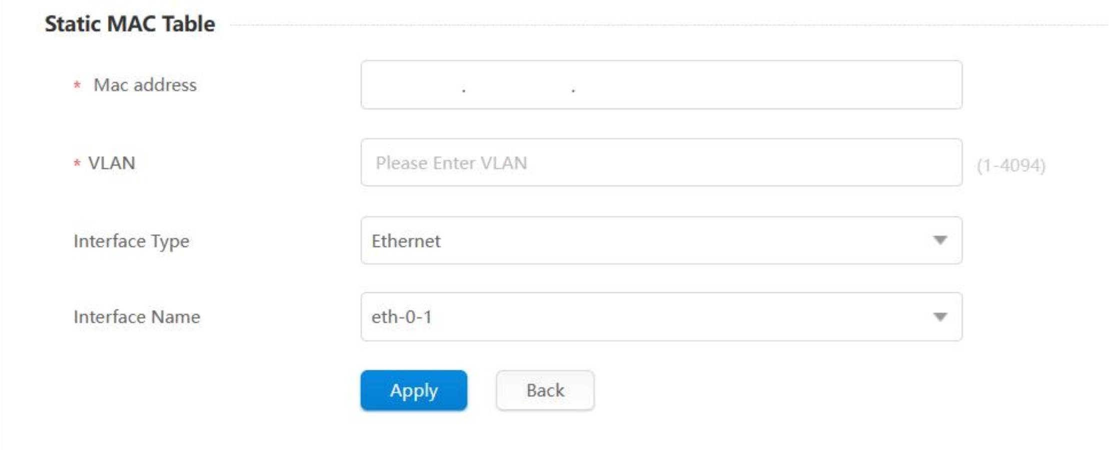
MAC Address: . .

VLAN: Please Enter VLAN (1-4094)

Interface Type: All

Interface Name: All

□ MAC Address	VLAN	Interface	Entry Type



Static MAC Table

* Mac address: . .

* VLAN: Please Enter VLAN (1-4094)

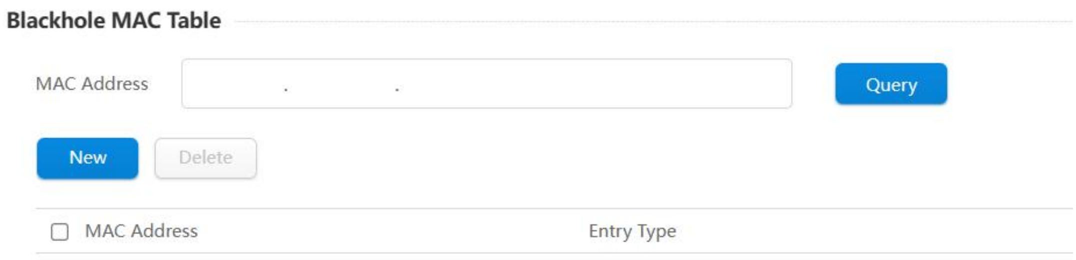
Interface Type: Ethernet

Interface Name: eth-0-1

6.3.5 Blackhole MAC address table

Operational Steps:

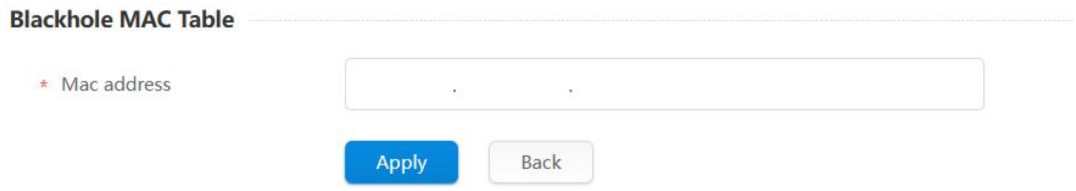
Click "Service Management > MAC > Blackhole MAC Address Table" menu in the navigation tree to enter the Blackhole MAC Address Table interface, as shown in the figure:



Blackhole MAC Table

MAC Address: . .

□ MAC Address	Entry Type



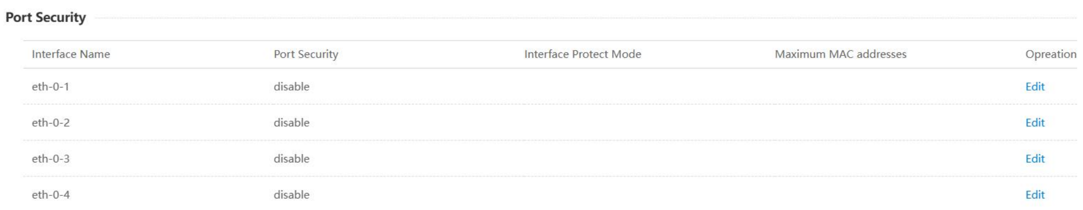
Blackhole MAC Table

* Mac address: . .

6.3.6 Port security

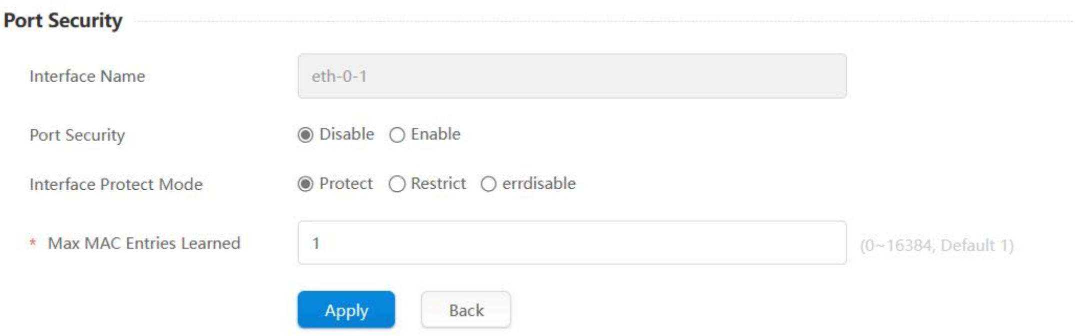
Operational Steps:

Click the "Service Management > MAC > Port Security" menu in the navigation tree to enter the Port Security interface, as shown in the figure:



Port Security

Interface Name	Port Security	Interface Protect Mode	Maximum MAC addresses	Opreation
eth-0-1	disable			Edit
eth-0-2	disable			Edit
eth-0-3	disable			Edit
eth-0-4	disable			Edit



Port Security

Interface Name: eth-0-1

Port Security: ● Disable ○ Enable

Interface Protect Mode: ● Protect ○ Restrict ○ errdisable

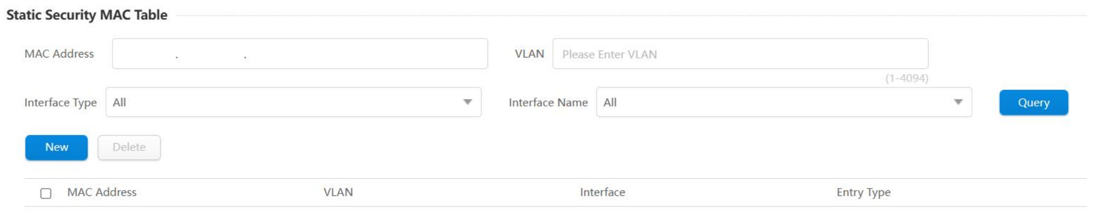
* Max MAC Entries Learned: 1 (0~16384, Default 1)

6.3.7 Static Secure MAC Address Table

Static table entries are manually configured by the user and distributed to each interface board, and the table entries are not aged. If the MAC address is set to Secure MAC, the port will only allow data frames with secure MAC to pass through permanently, and other data frames will be discarded

Operational Steps:

Click the "Service Management > MAC > Static Secure MAC Address Table" menu in the navigation tree to enter the Static Secure MAC Address Table interface, as shown in the figure:



Static Security MAC Table

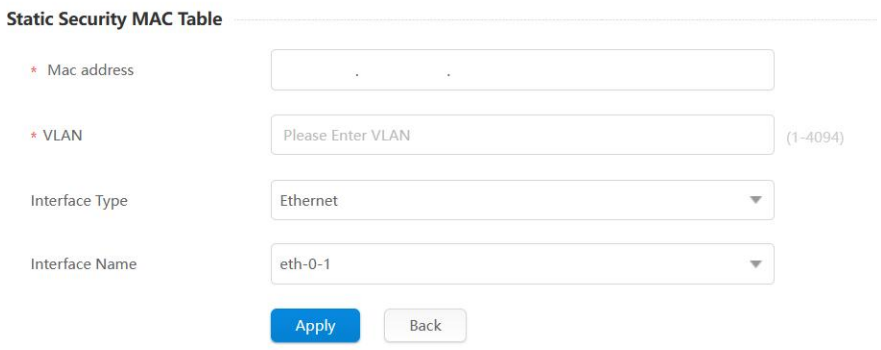
MAC Address . .

VLAN Please Enter VLAN (1-4094)

Interface Type All

Interface Name All

☐	MAC Address	VLAN	Interface	Entry Type



Static Security MAC Table

* Mac address . .

* VLAN Please Enter VLAN (1-4094)

Interface Type Ethernet

Interface Name eth-0-1

6.4 Spanning tree

Redundant links are often used in Ethernet switched networks for link backup and to improve network reliability. However, the use of redundant links creates loops in the switched network, causing broadcast storms and failures such as unstable MAC address tables, which leads to poor user communication quality and even communication interruption. To solve the problem of loops in switched networks, the Spanning Tree Protocol (STP) is proposed.

Like the development of many protocols, the Spanning Tree Protocol has been continuously updated with the development of the network, from the initial STP defined in IEEE 802.1D, to the Rapid Spanning Tree Protocol (RSTP) defined in IEEE

802.1W, to the latest Multiple Spanning Tree Protocol (MSTP) defined in IEEE 802.1S. Spanning Tree Protocol (MSTP) defined in the latest IEEE 802.1S.

In Spanning Tree Protocol, MSTP is compatible with RSTP and STP, and RSTP is compatible with STP.The comparison of the three Spanning Tree Protocols is shown in the table.

Comparison of three spanning tree protocols

Spanning Tree Protocol	Characteristics	Application Scenarios
STP	Forms a loop-free tree, resolves broadcast storms and enables redundant backups. Convergence is slow.	There is no need to distinguish between user or service traffic. all VLANs share a spanning tree.
RSTP	Forms a loop-free tree, resolves broadcast storms and enables redundant backups. Fast convergence.	
MSTP	Forms a loop-free tree, resolves broadcast storms and enables redundant backups. Fast convergence. Multiple spanning trees achieve load balancing among VLANs, and traffic from different VLANs is forwarded according to different paths.	There is a need to differentiate between user or business traffic and to achieve load sharing. Different VLANs forward traffic through different spanning trees, each of which is independent of the other.

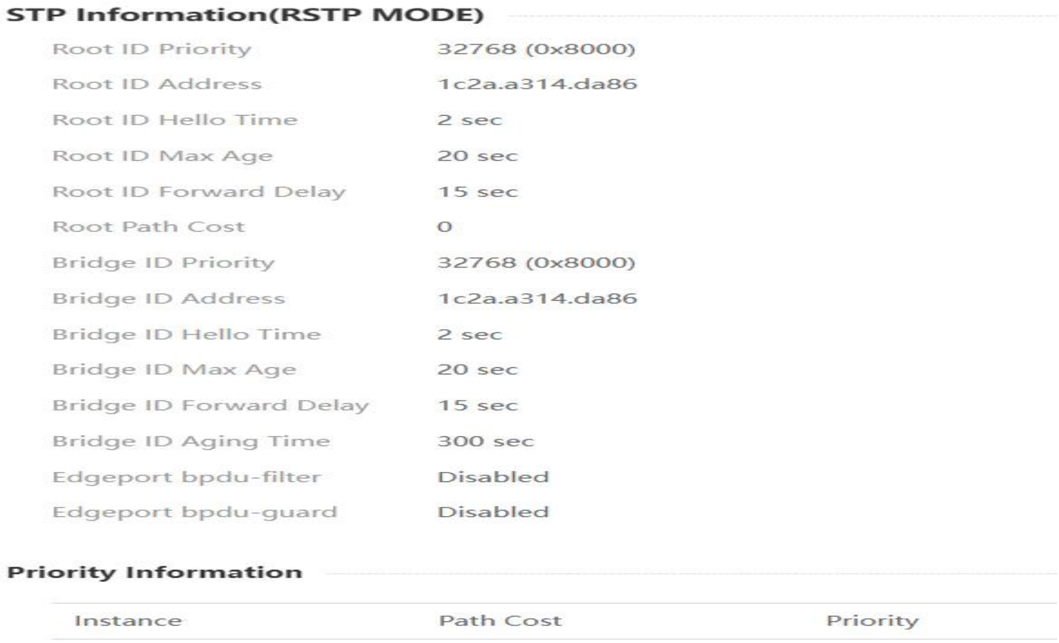
After deploying the Spanning Tree Protocol in an Ethernet switched network, if a loop occurs in the network, the Spanning Tree Protocol can be realized by topology calculation:

- Loop Elimination: Eliminates network communication loops that may exist in the network by blocking redundant links.
- Link Backup: In case of failure of the currently active path, activate redundant backup links to restore network connectivity.

6.4.1 Spanning Tree Information

Operational Steps:

Click "Service Management > Spanning Tree > Spanning Tree Information" menu in the navigation tree to enter the Spanning Tree Information interface, as shown in the figure:



STP Information(RSTP MODE)

Root ID Priority	32768 (0x8000)
Root ID Address	1c2a.a314.da86
Root ID Hello Time	2 sec
Root ID Max Age	20 sec
Root ID Forward Delay	15 sec
Root Path Cost	0
Bridge ID Priority	32768 (0x8000)
Bridge ID Address	1c2a.a314.da86
Bridge ID Hello Time	2 sec
Bridge ID Max Age	20 sec
Bridge ID Forward Delay	15 sec
Bridge ID Aging Time	300 sec
Edgeport bpdu-filter	Disabled
Edgeport bpdu-guard	Disabled

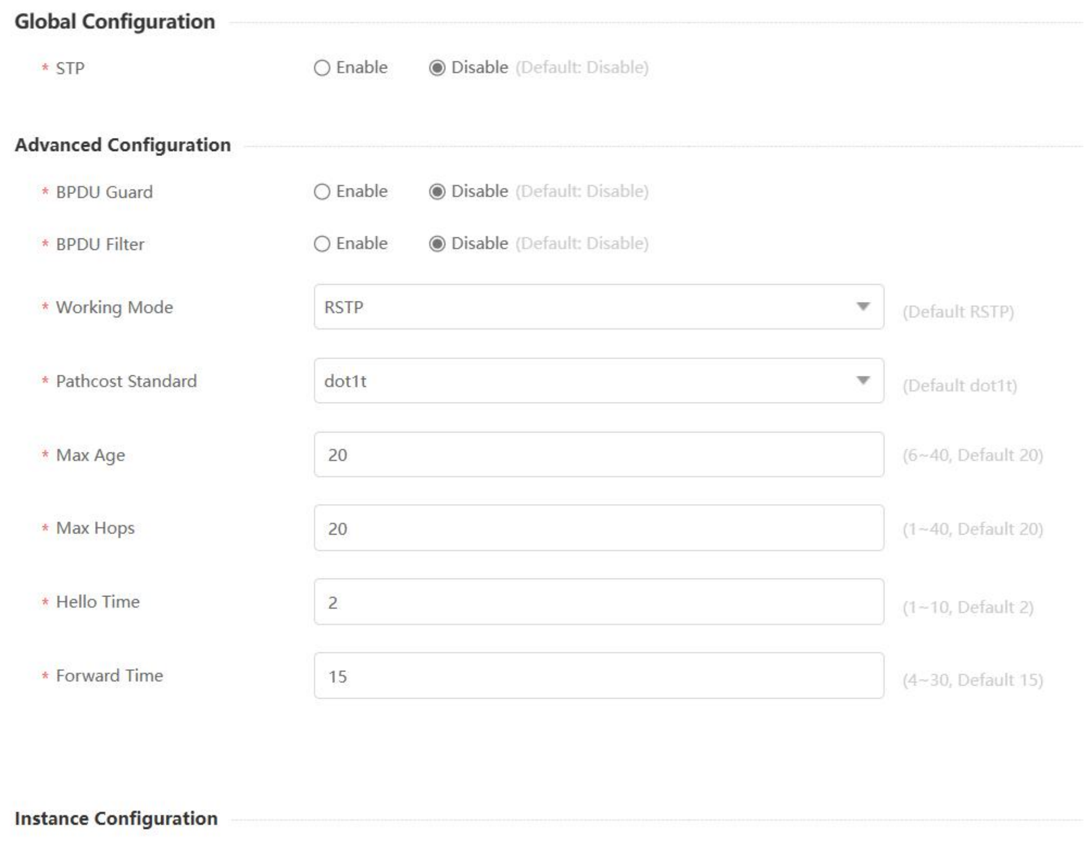
Priority Information

Instance	Path Cost	Priority

6.4.2 Global configuration

Operational Steps:

Click the "Service Management > Spanning Tree > Global Configuration" menu in the navigation tree to enter the Global Configuration interface, as shown in the figure:



Global Configuration

* STP	○ Enable ● Disable	(Default: Disable)

Advanced Configuration

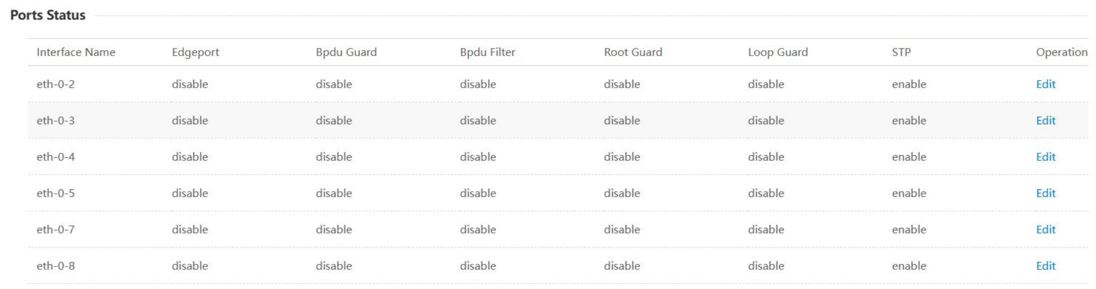
* BPDU Guard	○ Enable ● Disable	(Default: Disable)
* BPDU Filter	○ Enable ● Disable	(Default: Disable)
* Working Mode	RSTP	(Default RSTP)
* Pathcost Standard	dot1t	(Default dot1t)
* Max Age	20	(6~40, Default 20)
* Max Hops	20	(1~40, Default 20)
* Hello Time	2	(1~10, Default 2)
* Forward Time	15	(4~30, Default 15)

Instance Configuration

6.4.3 Spanning tree port

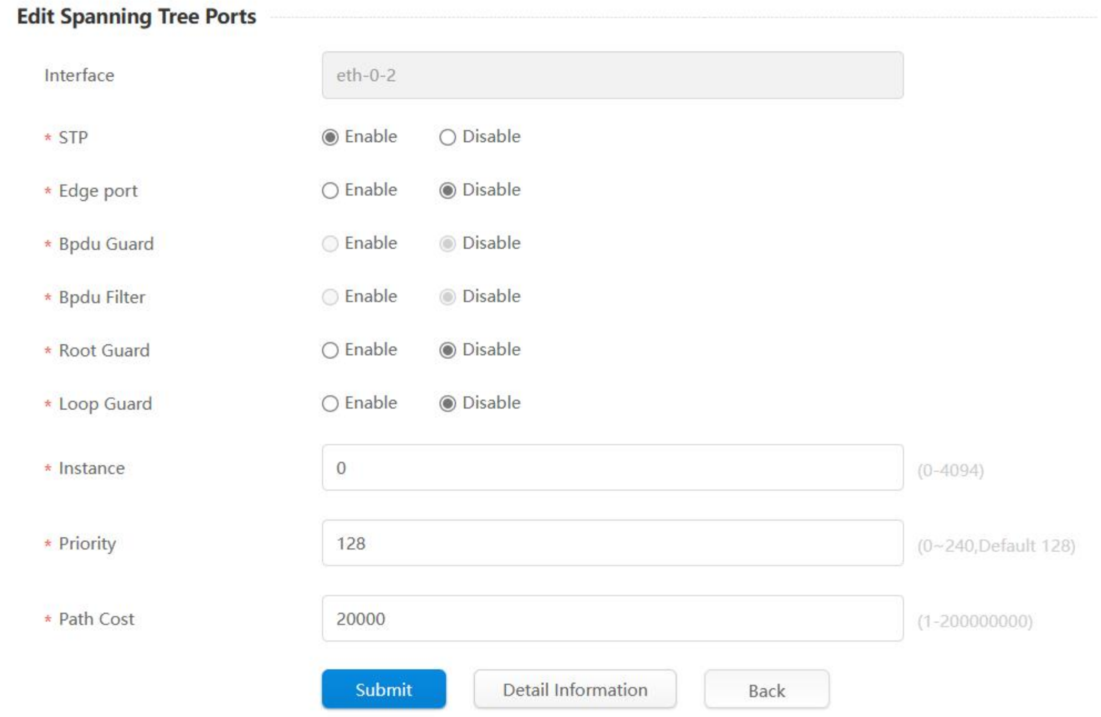
Operational Steps:

Click the "Service Management > Spanning Tree > Spanning Tree Ports" menu in the navigation tree to enter the Spanning Tree Ports interface, as shown in the figure:



Ports Status

Interface Name	Edgeport	Bpdu Guard	Bpdu Filter	Root Guard	Loop Guard	STP	Operation
eth-0-2	disable	disable	disable	disable	disable	enable	Edit
eth-0-3	disable	disable	disable	disable	disable	enable	Edit
eth-0-4	disable	disable	disable	disable	disable	enable	Edit
eth-0-5	disable	disable	disable	disable	disable	enable	Edit
eth-0-7	disable	disable	disable	disable	disable	enable	Edit
eth-0-8	disable	disable	disable	disable	disable	enable	Edit



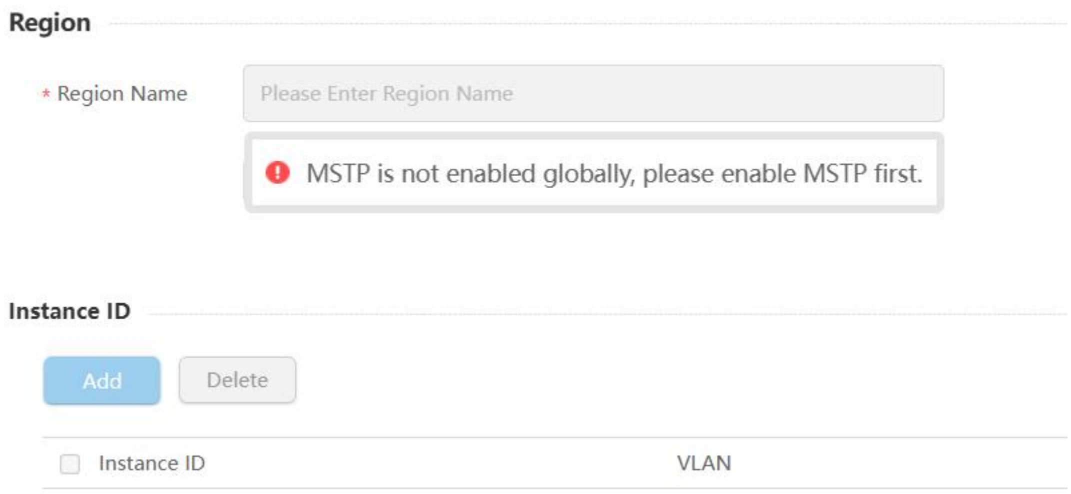
Edit Spanning Tree Ports

Interface	eth-0-2
* STP	● Enable ○ Disable
* Edge port	○ Enable ● Disable
* Bpdu Guard	○ Enable ● Disable
* Bpdu Filter	○ Enable ● Disable
* Root Guard	○ Enable ● Disable
* Loop Guard	○ Enable ● Disable
* Instance	0 (0-4094)
* Priority	128 (0~240,Default 128)
* Path Cost	20000 (1-200000000)

6.4.4 MST 域

Operational Steps:

Click the "Service Management > Spanning Tree > MST Domain" menu in the navigation tree to enter the MST Domain interface, as shown in the figure:



Region

* Region Name: Please Enter Region Name

MSTP is not enabled globally, please enable MSTP first.

Instance ID

Add Delete

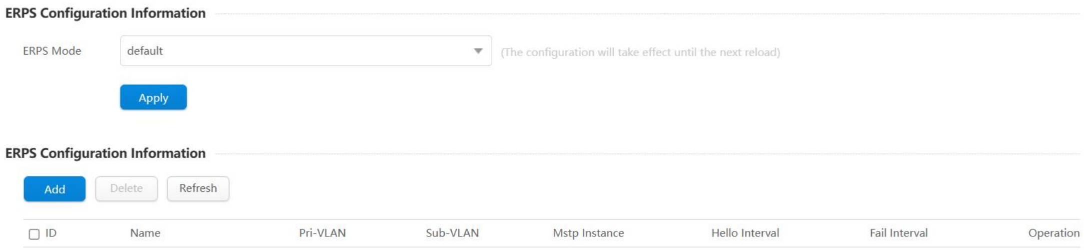
□ Instance ID	VLAN

6.5 ERPS

6.5.1 ERPS Configuration

Operational Steps:

Click "Service Management > ERPS > ERPS Configuration" menu in the navigation tree to enter the ERPS configuration interface, as shown in the figure:



ERPS Configuration Information

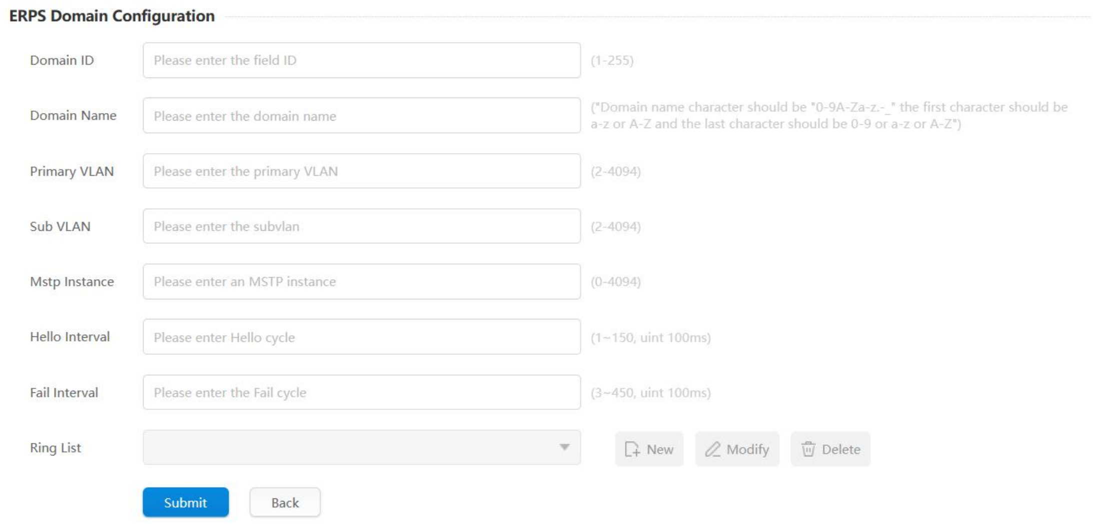
ERPS Mode: default (The configuration will take effect until the next reload)

Apply

ERPS Configuration Information

Add Delete Refresh

□ ID	Name	Pri-VLAN	Sub-VLAN	Mstp Instance	Hello Interval	Fail Interval	Operation



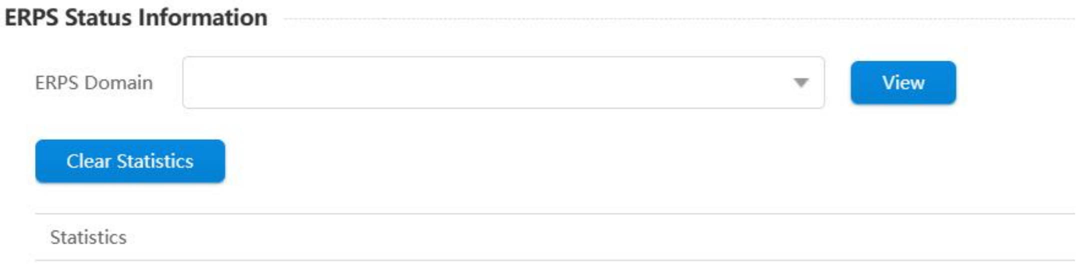
ERPS Domain Configuration

Domain ID	Please enter the field ID	(1-255)
Domain Name	Please enter the domain name	("Domain name character should be "0-9A-Za-z.-_" the first character should be a-z or A-Z and the last character should be 0-9 or a-z or A-Z")
Primary VLAN	Please enter the primary VLAN	(2-4094)
Sub VLAN	Please enter the subvlan	(2-4094)
Mstp Instance	Please enter an MSTP instance	(0-4094)
Hello Interval	Please enter Hello cycle	(1~150, uint 100ms)
Fail Interval	Please enter the Fail cycle	(3~450, uint 100ms)
Ring List		New Modify Delete

6.5.2 ERPS Status

Operational Steps:

Click the "Service Management > ERPS > ERPS Status" menu in the navigation tree to enter the ERPS status interface, as shown in the figure:



ERPS Status Information

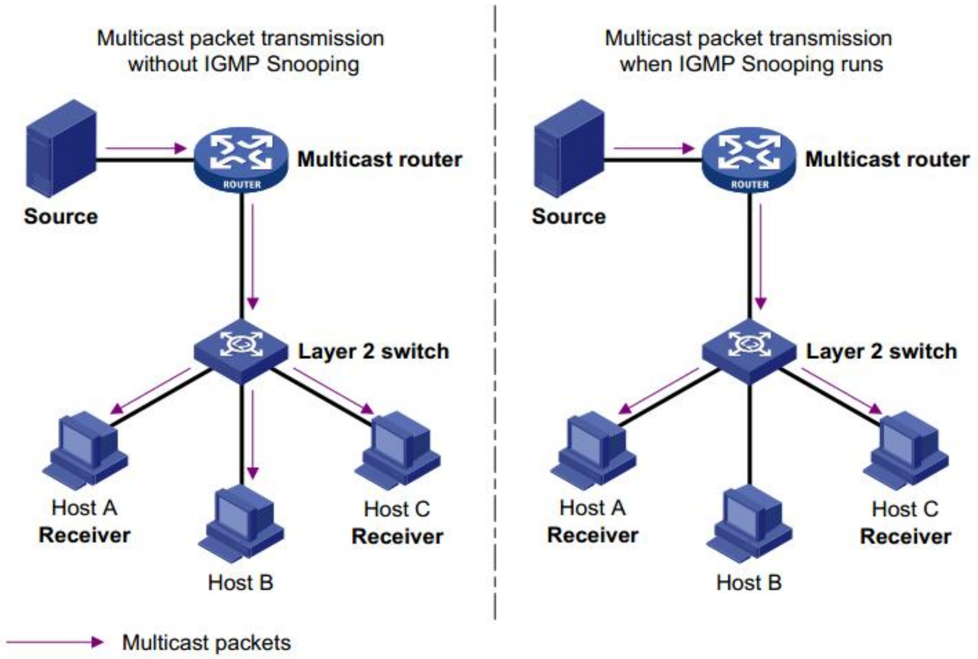
ERPS Domain

7 Multicast

IGMP snooping (Internet Group Management Protocol Snooping) is a multicast constraint mechanism running on Layer 2 devices to manage and control multicast groups.

A Layer 2 device running IGMP snooping analyzes received IGMP messages to establish a mapping relationship between ports and MAC multicast addresses and forwards multicast data according to this mapping relationship.

As shown in the following figure, when a Layer 2 device is not running IGMP snooping, multicast data is broadcast at Layer 2; when a Layer 2 device is running IGMP snooping, the multicast data of a known multicast group will not be broadcast at Layer 2 but will be multicast at Layer 2 to the specified receivers, but the unknown multicast data will still be broadcast at Layer 2.



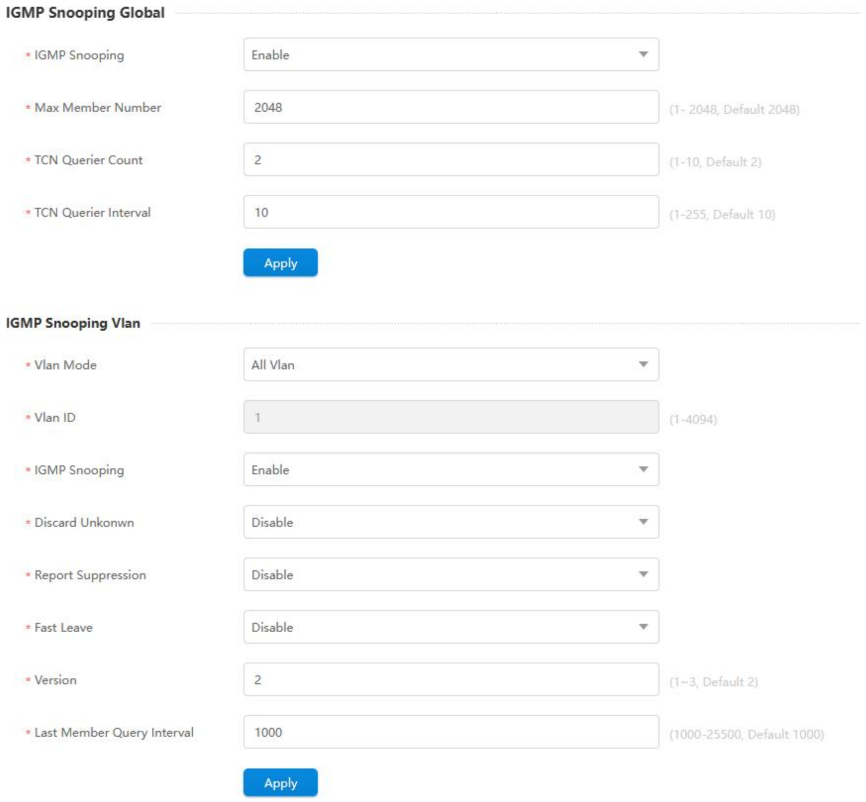
7.1 IGMP Snooping Features

IGMP Snooping, used in IPv4 networks, is deployed on Layer 2 switches between multicast routers and user hosts, configured in VLANs, and serves to listen to IGMP/MLD packets sent between routers and hosts to establish a Layer 2 forwarding table for multicast data, and thus manages and controls the forwarding of multicast data in the Layer 2 network.

By default, the IGMP Snooping function of the switch is in the de-enable state, so you need to enable the global IGMP Snooping function of the switch.

Operational Steps:

Click the "Multicast > IGMP Snooping Function" menu in the navigation tree to enter the IGMP Snooping function interface, as shown in the figure:



IGMP Snooping Global

* IGMP Snooping: Enable
* Max Member Number: 2048 (1- 2048, Default 2048)
* TCN Querier Count: 2 (1-10, Default 2)
* TCN Querier Interval: 10 (1-255, Default 10)

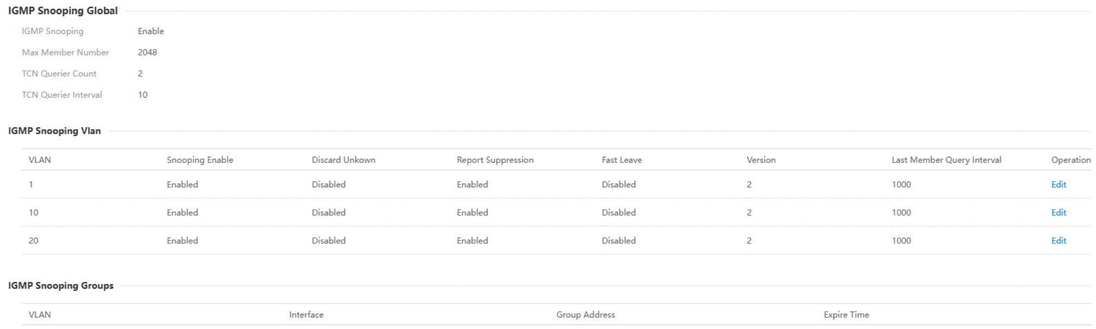
IGMP Snooping Vlan

* Vlan Mode: All Vlan
* Vlan ID: 1 (1-4094)
* IGMP Snooping: Enable
* Discard Unkonwn: Disable
* Report Suppression: Disable
* Fast Leave: Disable
* Version: 2 (1~3, Default 2)
* Last Member Query Interval: 1000 (1000-25500, Default 1000)

7.2 IGMP Snooping Information

Operational Steps:

Click the "Multicast > IGMP Snooping Information" menu in the navigation tree to enter the IGMP Snooping Information interface, as shown in Figure :



IGMP Snooping Global

IGMP Snooping	Enable
Max Member Number	2048
TCN Querier Count	2
TCN Querier Interval	10

IGMP Snooping Vlan

VLAN	Snooping Enable	Discard Unkown	Report Suppression	Fast Leave	Version	Last Member Query Interval	Operation
1	Enabled	Disabled	Enabled	Disabled	2	1000	Edit
10	Enabled	Disabled	Enabled	Disabled	2	1000	Edit
20	Enabled	Disabled	Enabled	Disabled	2	1000	Edit

IGMP Snooping Groups

VLAN	Interface	Group Address	Expire Time

8 IP Routing

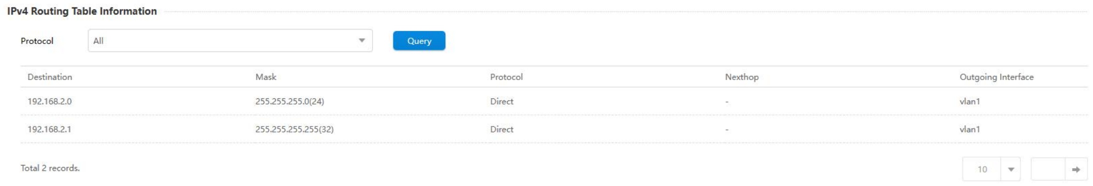
The switch provides three layers of VLAN interfaces for communicating with network layer devices. the VLANIF interface is a network layer interface with configurable IP address. Before creating a VLANIF interface, first create the corresponding VLAN. through the VLANIF interface, the switch can communicate with other network layer devices.

8.1 IPv4 Routing table

The system will be shipped with the interface address of VLAN1: 192.168.2.1, which is used for the WEB login of the switch.

Operational Steps:

Click the "IP Routing > IPv4 Routing Table" menu in the navigation tree to enter the IPv4 Routing Table interface, as shown in the figure:



IPv4 Routing Table Information

Protocol: All

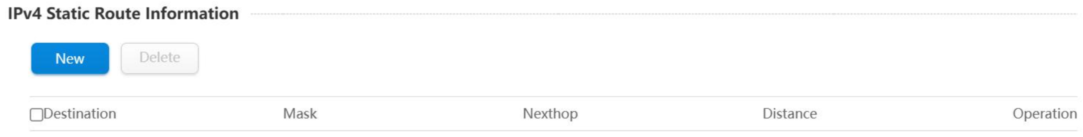
Destination	Mask	Protocol	Nexthop	Outgoing Interface
192.168.2.0	255.255.255.0(24)	Direct	-	vlan1
192.168.2.1	255.255.255.255(32)	Direct	-	vlan1

Total 2 records.

8.2 IPv4 Static Routes

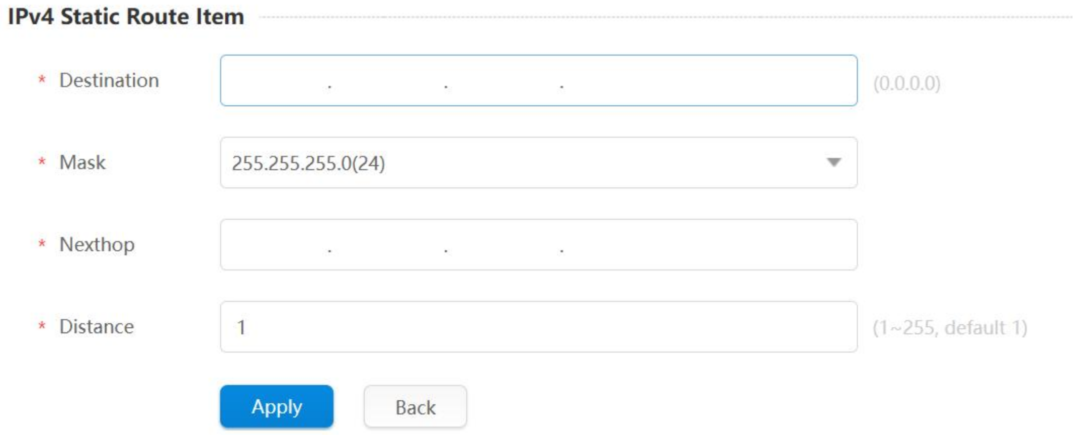
Operational Steps:

Click the "IP Routing > IPv4 Static Route" menu in the navigation tree to enter the IPv4 Static Route interface, as shown in the figure:



IPv4 Static Route Information

□Destination	Mask	Nexthop	Distance	Operation



IPv4 Static Route Item

* Destination: . . . (0.0.0.0)

* Mask: 255.255.255.0(24)

* Nexthop: . . .

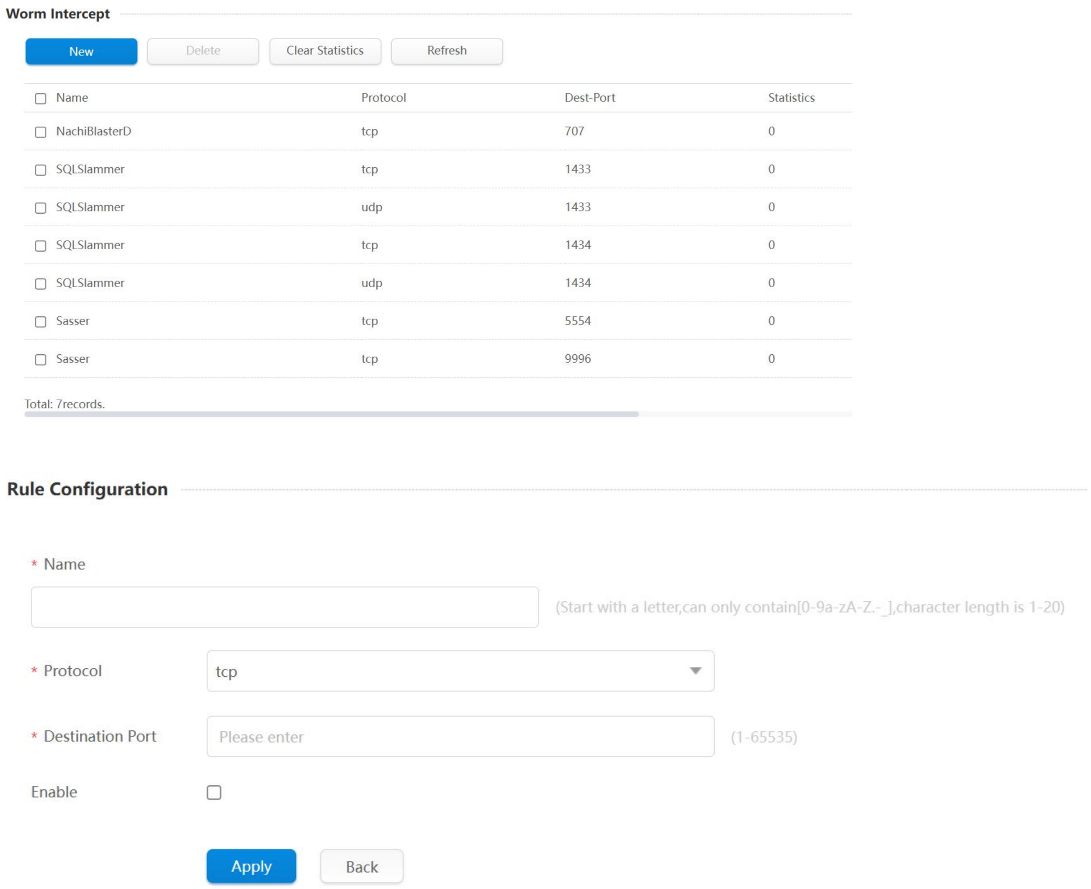
* Distance: 1 (1~255, default 1)

9 Surety

9.1 Worm Attack Protection

Operational Steps:

Click the "Security > Worm Attack Protection" menu in the navigation tree to enter the Worm Attack Protection interface, as shown in the figure:



□ Name	Protocol	Dest-Port	Statistics
□ NachiBlasterD	tcp	707	0
□ SQLSlammer	tcp	1433	0
□ SQLSlammer	udp	1433	0
□ SQLSlammer	tcp	1434	0
□ SQLSlammer	udp	1434	0
□ Sasser	tcp	5554	0
□ Sasser	tcp	9996	0

Total: 7records.

Rule Configuration

* Name (Start with a letter,can only contain[0-9a-zA-Z.-_],character length is 1-20)

* Protocol: tcp

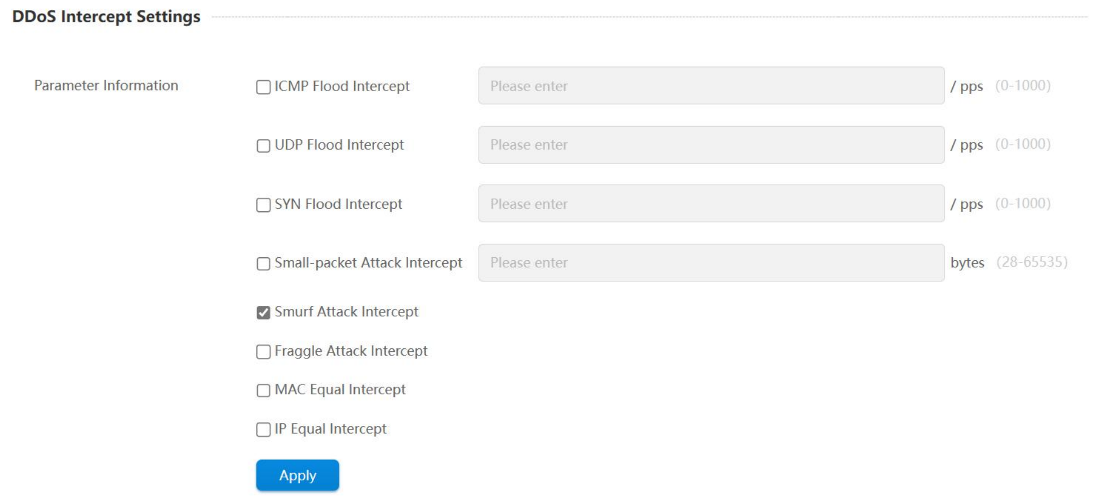
* Destination Port: Please enter (1-65535)

Enable □

9.2 DDoS Attack Protection

Operational Steps:

Click the "Security > DDoS Attack Protection" menu in the navigation tree to enter the DDoS Attack Protection interface, as shown in Figure :



DDoS Intercept Settings

Parameter Information

☐ ICMP Flood Intercept — Please enter / pps (0-1000)

☐ UDP Flood Intercept — Please enter / pps (0-1000)

☐ SYN Flood Intercept — Please enter / pps (0-1000)

☐ Small-packet Attack Intercept — Please enter bytes (28-65535)

☑ Smurf Attack Intercept

☐ Fraggle Attack Intercept

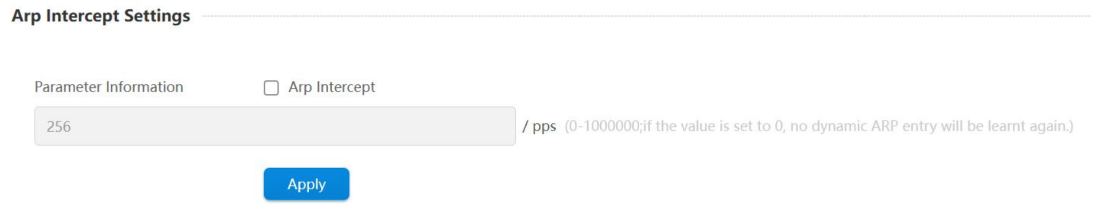
☐ MAC Equal Intercept

☐ IP Equal Intercept

9.3 ARP Attack Protection

Operational Steps:

Click the "Security > ARP Attack Protection" menu in the navigation tree to enter the ARP Attack Protection interface, as shown in the figure:



Arp Intercept Settings

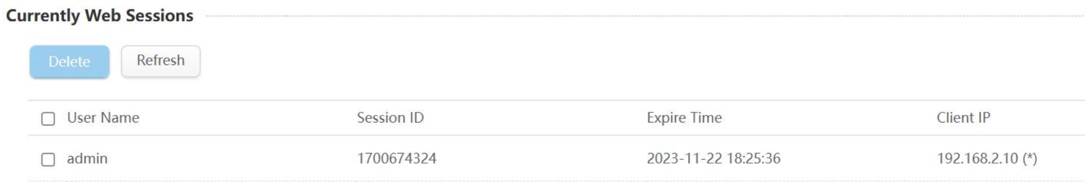
Parameter Information ☐ Arp Intercept

256 / pps (0-1000000;if the value is set to 0, no dynamic ARP entry will be learnt again.)

9.4 Current session

Operational Steps:

Click the "Security > Current Session" menu in the navigation tree to enter the Current Session screen, as shown in the figure:



Currently Web Sessions

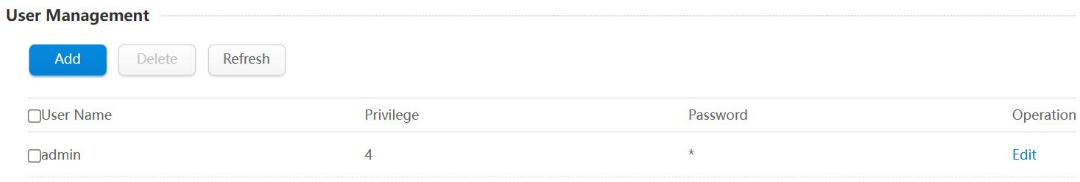
□ User Name	Session ID	Expire Time	Client IP
□ admin	1700674324	2023-11-22 18:25:36	192.168.2.10 (*)

9.5 User management

Users can view the current user name, password, and permissions of the switch, and users can modify the user name, password, and permissions.

Operational Steps:

Click the "Security > User Management" menu in the navigation tree to enter the user management interface, as shown in the figure:



User Management

□User Name	Privilege	Password	Operation
□admin	4	*	Edit

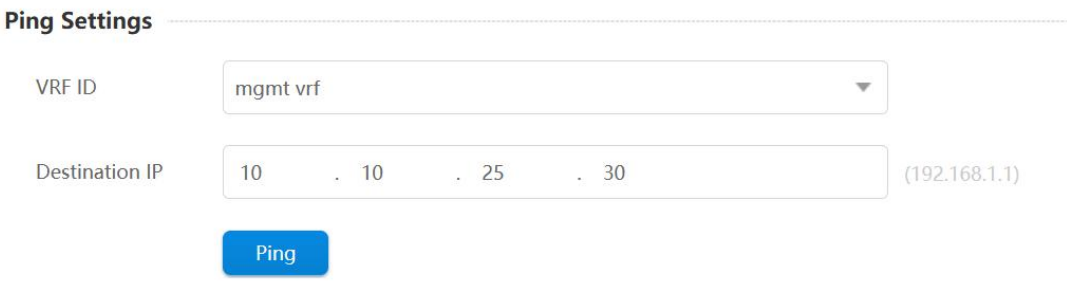
10 Artifact

10.1 Ping

The Ping command is used to check whether the specified IP address and host name are reachable and output the corresponding statistics.

Operational Steps:

Click the Tools > Ping menu in the navigation tree to enter the Ping interface, as shown in the figure:



Ping Settings

VRF ID: mgmt vrf

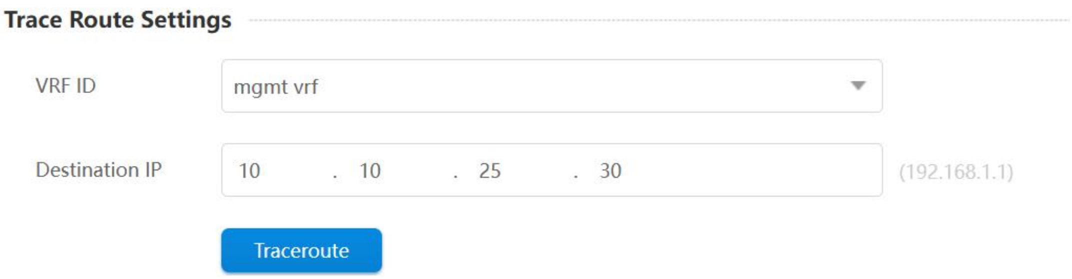
Destination IP: 10 . 10 . 25 . 30 (192.168.1.1)

10.2 Traceroute

Traceroute measures how long it takes by sending small packets to the destination device until it returns.

Operational Steps:

Click the Tools > Traceroute menu in the navigation tree to enter the Traceroute interface, as shown in Figure :



Trace Route Settings

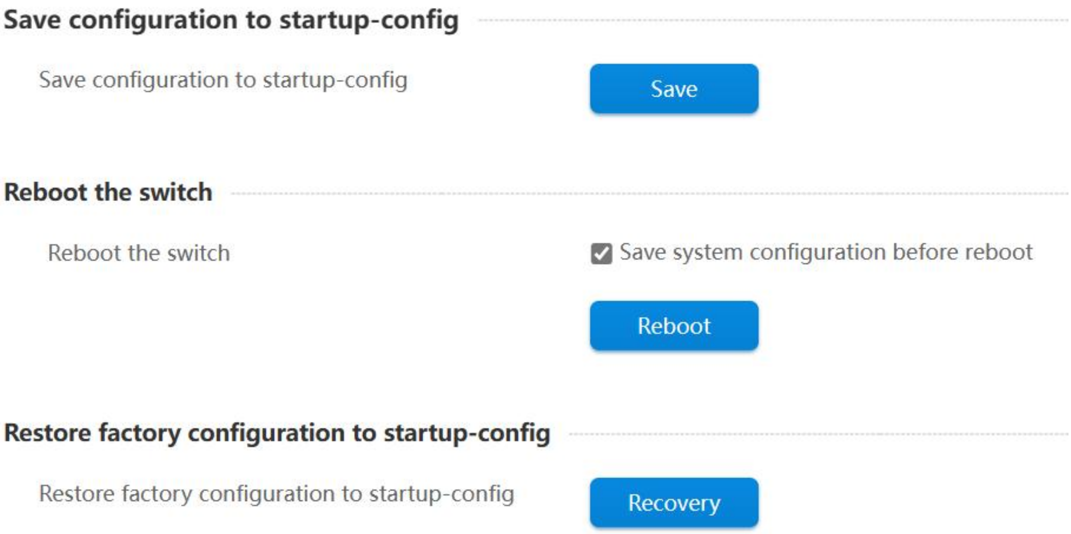
VRF ID: mgmt vrf

Destination IP: 10 . 10 . 25 . 30 (192.168.1.1)

10 Reboot/Save

Operational Steps:

Click the "Reboot/Save" menu in the navigation tree to enter the Reboot/Save interface, as shown in the figure:



Save configuration to startup-config

Save configuration to startup-config

Reboot the switch

Reboot the switch

☑ Save system configuration before reboot

Restore factory configuration to startup-config

Restore factory configuration to startup-config