



16-Port Gigabit + 4-Port Gigabit SFP L2 Managed PoE Switch



User Manual

V1.1.2

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.

Copyright Statement

Our company reserves all copyrights of this document. Any reproduction, excerption, backup, modification, transmission, translation or commercial use of this document or any portion of this document, in any form or by any means, without the prior written consent of our company is prohibited.

Exemption Statement

This document is provided "as is". The contents of this document are subject to change without any notice. Please obtain the latest information through our company website. Our company endeavors to ensure content accuracy and will not shoulder any responsibility for losses and damages caused due to content omissions, inaccuracies or errors.

Table of Contents

1. Product Introduction.....	4
1.1. Product Overview	4
1.2. Features	4
1.3. External Component Description	5
1.3.1. Front Panel	5
1.3.2. Rear Panel	6
1.4. Package Contents	6
2. Installing and Connecting the Switch	7
2.1. Installation.....	7
2.1.1. Desktop Installation	7
2.1.2. Rack-mountable Installation in 19-inch Cabinet.....	7
2.1.3. Power on the Switch.....	8
2.2. Connect Computer (NIC) to the Switch.....	9
2.3. Switch connection to the PD.....	9
3. How to Log in the Switch.....	9
3.1. Switch to End Node	9
3.2. How to Login the Switch.....	9
4. Switch Configuration.....	10
4.1. Quickly Set	11
4.2. PORT	13
4.2.1. Basic Config.....	13
4.2.2. Port Aggregation	15
4.2.3. Port Mirroring.....	16
4.2.4. Port Limit.....	17
4.2.5. Storm Control	18
4.2.6. Port Isolation.....	19
4.2.7. Port Information.....	20
4.3. VLAN	21
4.3.1. VLAN Settings.....	21
4.3.2. Access Port Settings.....	22
4.3.3. Trunk Port Settings.....	23
4.3.4. Hybrid Port Settings.....	24
4.4. Fault/Safety	26

4.4.1.	Anti Attack.....	26
4.4.1.1.	DHCP.....	26
5.1.1.1.	DOS.....	28
5.1.1.2.	IP Source Guard.....	29
5.1.1.3.	IP/Mac/Port.....	30
5.1.2.	Channel Detection.....	31
5.1.2.1.	Ping.....	31
5.1.2.2.	Tracert.....	32
5.1.2.3.	Cable Test	33
5.1.3.	ACL	34
5.2.	PoE.....	35
5.2.1.	PoE Port Config.....	36
5.2.1.1.	Chip information	36
5.2.1.2.	Poe Port Config.....	36
5.3.	STP.....	37
5.3.1.	MSTP Region.....	37
5.3.2.	STP Bridge.....	38
5.4.	DHCP RELAY	41
5.4.1.	DHCP RELAY.....	41
5.4.2.	option82.....	41
5.5.	QOS.....	43
5.5.1.	Queue Config	43
5.5.2.	Mapping the Queue.....	44
5.5.2.1.	COS Queue Map	44
5.5.2.2.	DSCP COS Map	45
5.5.2.3.	Port COS Map.....	46
5.6.	Addr table.....	47
5.6.1.	MAC Management	48
5.6.2.	MAC Learning and Aging.....	49
5.6.3.	MAC Filter	50
5.7.	SNMP	51
5.7.1.	Snmp Config.....	51
5.7.1.1.	Snmp Config	51
5.7.1.2.	Community Config	51
5.7.1.3.	View Config	52
5.7.1.4.	Group Config	53
5.7.1.5.	User Config	54
5.7.1.6.	Trap Config	55
5.7.2.	Rmon Config.....	56
5.7.2.1.	Statistics Group.....	56
5.7.2.2.	History Group	57

5.7.2.3.	Event Group	58
5.7.2.4.	Alarm Group.....	59
5.8.	LACP	61
5.8.1.	Lacp Config	61
5.8.1.1.	LACP Setting	61
5.8.1.2.	LACP Display	63
5.9.	SYSTEM	63
5.9.1.	System Config	64
5.9.1.1.	System Settings	64
5.9.1.2.	System Restart.....	66
5.9.1.3.	EEE Enable.....	66
5.9.1.4.	Password.....	67
5.9.1.5.	SSH Login	68
5.9.1.6.	Telnet Login.....	68
5.9.1.7.	System Log	69
5.9.2.	System Upgrade	70
5.9.3.	Config Management.....	70
5.9.3.1.	Import/Export Config	70
5.9.3.2.	Restore Config	72
5.9.3.3.	Factory Reset.....	73
5.9.4.	Config Save	73
5.9.5.	Administrator Privileges.....	73
5.9.6.	Info collect.....	74

1. Product Introduction

Congratulations on your purchasing of the 16-Port Gigabit + 4-Port Gigabit SFP L2 Managed PoE Switch. Before you install and use this product, please read this manual carefully for full exploiting the functions of this product.

1.1. Product Overview

The Switch is high performance the second managed gigabit switch. Provides sixteen 10/100/1000Mbps self-adaption RJ45 ports, plus four Gigabit SFP port, it can be used to link bandwidth higher upstream equipment. Support VLAN ACL based on port, easily implement network monitoring, traffic regulation, priority tag and traffic control. Support traditional STP/RSTP/MSTP 2 link protection technology; greatly improve the ability of fault tolerance, redundancy backup to ensure the stable operation of the network. Support ACL control based on the time, easy control the access time accurately. Support 802.1x authentication based on the port and MAC, easily set user access. Perfect QoS strategy and plenty of VLAN function. PoE ports can automatically detect and supply power with those IEEE 802.3at/af compliant Powered Devices (PD). In this situation, the electrical power is transmitted along with data in one single cable allowing you to expand your network where there are no power lines or outlets, where you wish to fix devices such as AP, IP Cameras or IP Phones, etc.

1.2. Features

- Comply with IEEE802.3i, IEEE802.3u, IEEE802.3ab, IEEE802.3x, IEEE802.3z, IEEE802.3ad standards.
- Supports IEEE802.3at/af PoE standards.
- Supports PoE power up to 30W for each PoE port, total power up to 240 W for all PoE ports.
- Supports MAC address auto-learning and auto-aging.
- Store and forward mode operates.
- Support SNMP/RMON/TELENET.
- Support IEEE802.1q VLAN, 4K VLAN Table.
- Support IEEE802.1p Priority Queues.
- Support 2K+256-entry ingress and egress ACL.
- Support Storm Control.
- Support QoS, Port Mirroring, Link Aggregation Protocol.
- LED indicators for monitoring PSE, Link/Activity/Speed.
- Web-based Management Support.

1.3. External Component Description

1.3.1. Front Panel

The front panel of the Switch consists of a series of LED indicators, 1 x Reset button, 16 x 10/100/1000Mbps RJ-45 ports, 1x Console and 4 x SFP ports as shown as below.



Figure 1 - Front Panel

Reset button (Reset):

Keep the device powered on and push a paper clip into the hole. Press down the button for 5 seconds to restore the Switch to its original factory default settings.

10/100/1000Mbps RJ-45 ports (1~16):

Designed to connect to the device with a bandwidth of 10Mbps, 100Mbps or 1000Mbps. Each has a corresponding Link/Act/Speed and PoE indicator.

Console port (Console):

Designed to connect with the serial port of a computer or terminal for monitoring and configuring the Switch.

SFP ports (17-20):

Designed to install the SFP module and connect to the device with a bandwidth of 1000Mbps. Each has a corresponding Link/Act/Speed LED.

LED indicators:

The LED Indicators will allow you to monitor, diagnose and troubleshoot any potential problem with the Switch, connection or attached devices.

The following chart shows the LED indicators of the Switch along with explanation of each indicator.

LED Indicator	Faceplate Marker	Status	Indication
Power Indicator	PWR	Off	Power Off
		Solid green	Power On
System indicator	SYS	Off	System not started
		Blinking green	System is starting or the system starts successfully
10/100/1000 BASE-T	Link/Act	Off	The port is NOT connected.

adaptive Ethernet port indicators (1-16)	/Speed	Solid green	The port is connected at 1000Mbps.
		Solid orange	The port is connected at 100/10Mbps
		Blinking	The port is transmitting or receiving data.
SFP port indicators (17-20)	Link/Act /Speed	Off	The port is NOT connected.
		Solid green	The port is connected at 1000Mbps.
		Blinking	The port is transmitting or receiving data.
PoE status indicators (1-8)	PoE	Off	No PD is connected to the corresponding port, or no power is supplied according to the power limits of the port
		Solid yellow	A Powered Device is connected to the port, which supply power successfully.
		Blinking	The PoE power circuit may be in short or the power current may be overloaded

1.3.2. Rear Panel

The rear panel of the Switch contains one Grounding Terminal and AC power connector shown as below.



Figure 2 - Rear Panel

Grounding Terminal:

Located on the left side of the power supply connector, use wire grounding to lightning protection.

AC Power Connector:

Power is supplied through an external AC power adapter. It supports 100-240 VAC, 50/60 Hz.

1.4. Package Contents

Before installing the Switch, make sure that the following the "packing list" listed OK. If any part is lost and damaged, please contact your local agent immediately. In addition, make sure that you have the tools install

switches and cables by your hands.

- One PoE Web Smart Ethernet Switch.
- One Installation Component
- One AC power cord.
- One User Manual.

2. Installing and Connecting the Switch

This part describes how to install your PoE Ethernet Switch and make connections to it. Please read the following topics and perform the procedures in the order being presented.

2.1. Installation

Please follow the following instructions in avoid of incorrect installation causing device damage and security threat.

- Put the Switch on stable place or desktop in case of falling damage.
- Make sure the Switch works in the proper AC input range and matches the voltage labeled on the Switch.
- To keep the Switch free from lightning, do not open the Switch's shell even in power failure.
- Make sure that there is proper heat dissipation from and adequate ventilation around the Switch.
- Make sure the cabinet to enough back up the weight of the Switch and its accessories.

2.1.1. Desktop Installation

Sometimes users are not equipped with the 19-inch standard cabinet. So when installing the Switch on a desktop, please attach these cushioning rubber feet provided on the bottom at each corner of the Switch in case of the external vibration. Allow adequate space for ventilation between the device and the objects around it.

2.1.2. Rack-mountable Installation in 19-inch Cabinet

The Switch can be mounted in an EIA standard-sized, 19-inch rack, which can be placed in a wiring closet with other equipment. To install the Switch, please follow these steps:

- A. Attach the mounting brackets on the Switch's side panels (one on each side) and secure them with the screws provided.

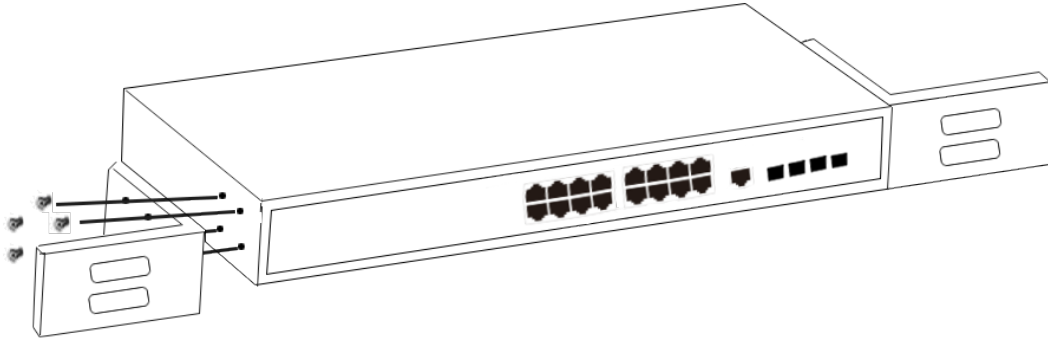


Figure 3 - Bracket Installation

- B. Use the screws provided with the equipment rack to mount the Switch on the rack and tighten it.

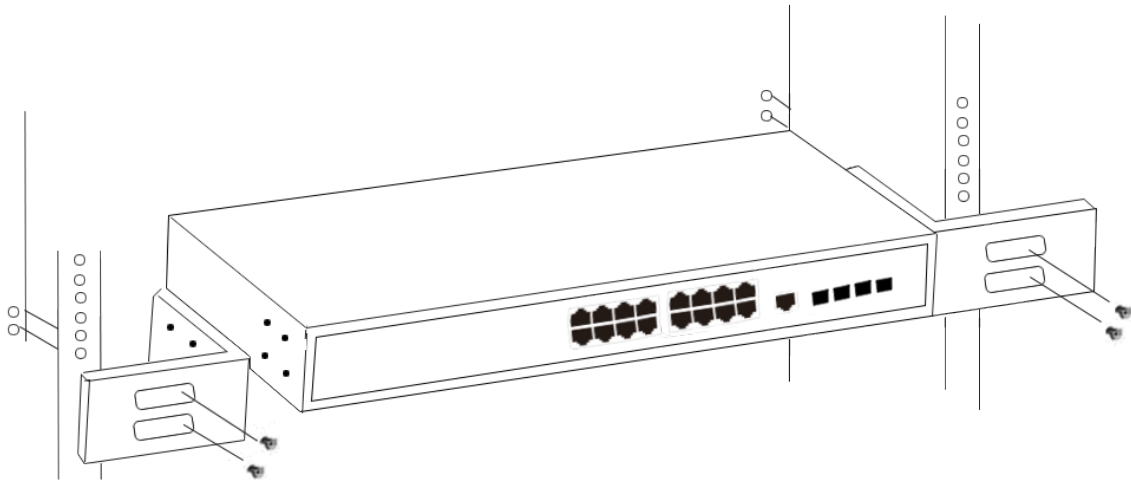


Figure 4 - Rack Installation

2.1.3. Power on the Switch

The Switch is powered on by the 100-240 VAC 50/60 Hz internal high-performance power supply. Please follow the next tips to connect:

AC Electrical Outlet:

It is recommended to use single-phase three-wire receptacle with neutral outlet or multifunctional computer professional receptacle. Please make sure to connect the metal ground connector to the grounding source on the outlet.

AC Power Cord Connection:

Connect the AC power connector in the back panel of the Switch to external receptacle with the included power cord, and check the power indicator is ON or not. When it is ON, it indicates the power connection is OK.

2.2. Connect Computer (NIC) to the Switch

Please insert the NIC into the computer, after installing network card driver, please connect one end of the twisted pair to RJ-45 jack of your computer, the other end will be connected to any RJ-45 port of the Switch, the distance between Switch and computer is around 100 meters. Once the connection is OK and the devices are power on normally, the LINK/ACT/Speed status indicator lights corresponding ports of the Switch.

2.3. Switch connection to the PD

1-16 ports of the Switch have PoE power supply function, the maximum output power up to 30W each port, it can make PD devices, such as internet phone, network camera, wireless access point work. You only need to connect the Switch PoE port directly connected to the PD port by network cable.

3. How to Log in the Switch

3.1. Switch to End Node

Use standard Cat.5/5e Ethernet cable (UTP/STP) to connect the Switch to end nodes as described below. Switch ports will automatically adjust to the characteristics (MDI/MDI-X, speed, duplex) of the device to which is connected.

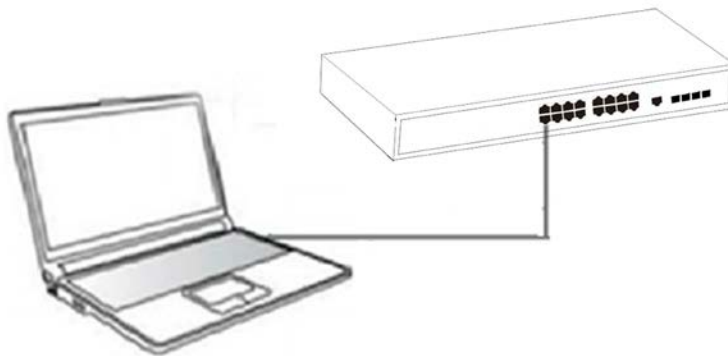


Figure 5 - Connect PC to Switch

Please refer to the LED Indicators. The LINK/ACT/Speed LEDs for each port lights on when the link is available.

3.2. How to Login the Switch

As the Switch provides Web-based management login, you can configure your computer's IP address manually to log on to the Switch. The default settings of the Switch are shown below.

Parameter	Default Value
Default IP address	192.168.1.110
Default user name	admin
Default password	admin123

You can log on to the configuration window of the Switch through following steps:

1. Connect the Switch with the computer NIC interface.
2. Power on the Switch.
3. Check whether the IP address of the computer is within this network segment: 192.168.1.xxx ("xxx" ranges 0~254, except 110), for example, 192.168.1.100.
4. Open the browser, and enter http://192.168.1.110 and then press "Enter". The Switch login window appears, as shown below.

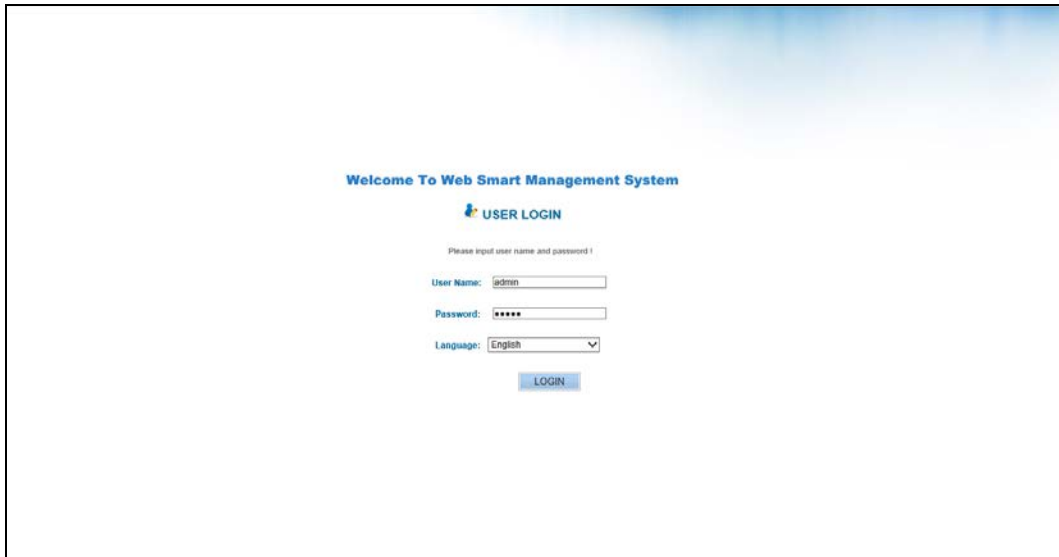
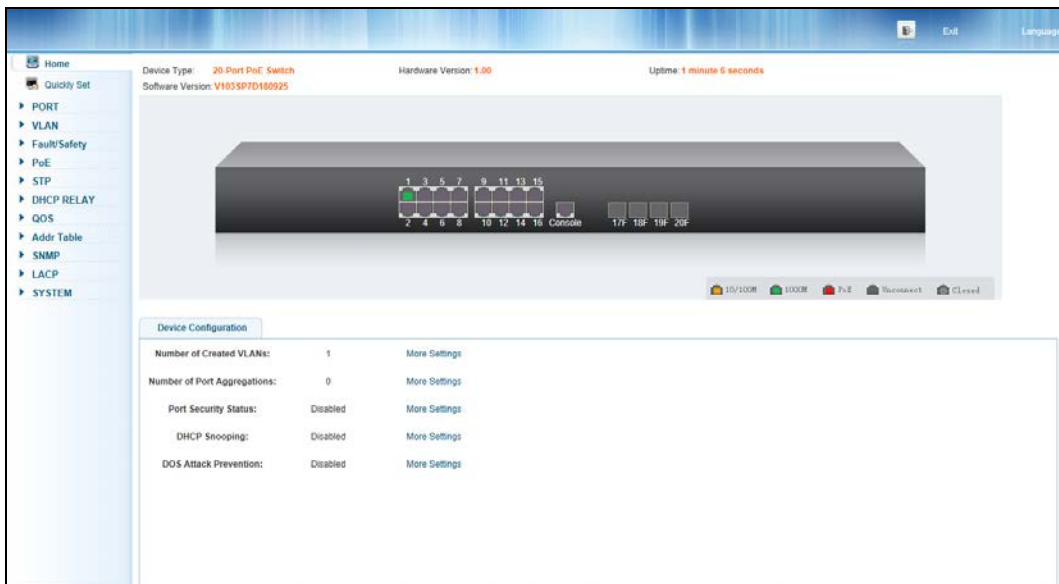


Figure 7- Login Windows

5. Switching language to English .Enter the Username and Password (The factory default Username is **admin** and Password is **admin123**), and then click "**LOGIN**" to log in to the Switch configuration window

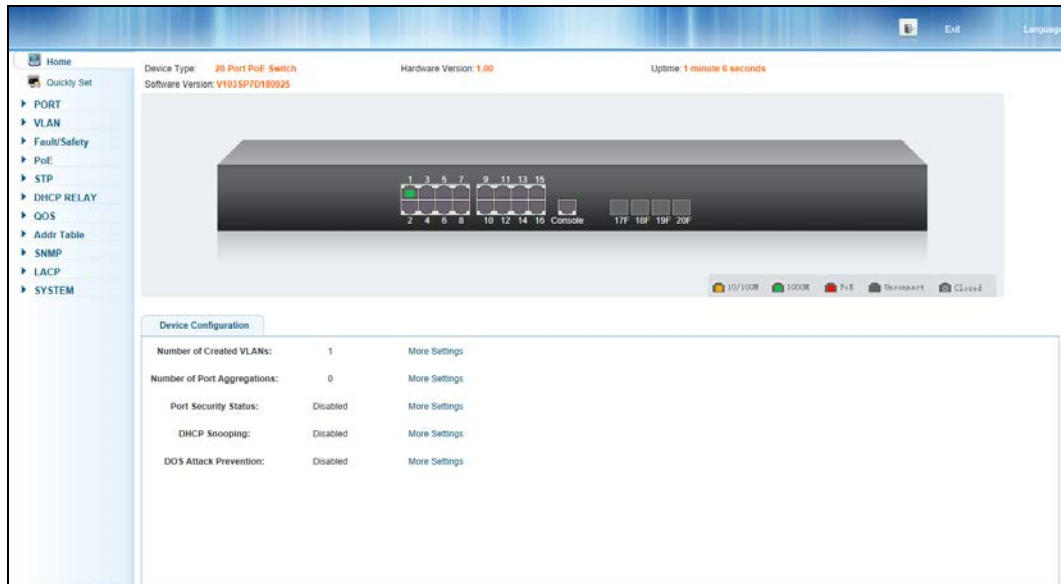


4. Switch Configuration

The Web Smart Ethernet Switch Managed switch software provides rich layer 2 functionality for switches in

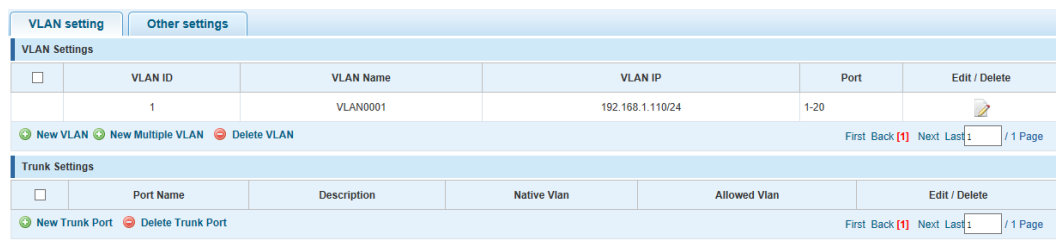
your networks. This chapter describes how to use Web-based management interface(Web UI) to this switch configure managed switch software features.

In the Web UI, the left column shows the configuration menu. Above you can see the information for switch system, such as memory, software version. The middle shows the switch's current link status. Green squares indicate the port link is up, while black squares indicate the port link is down. Below the switch panel, you can find a common toolbar to provide useful functions for users. The rest of the screen area displays the configuration settings.



4.1. Quickly Set

In the navigation bar to select "**Quickly Set**", can create a VLAN in this module, add the port in the VLAN, set the basic information and modify the switch login password. The following picture:



[Parameter description]

Parameter	Description
VLAN ID	VLAN number
VLAN Name	VLAN mark
VLAN IP	Manage the IP address of the VLAN
Management VLAN	Switch's management in use of the VLAN
Device Name	Switch name

[Instructions]

Native VLAN: as a Trunk, the mouth will belong to a Native VLAN. The so-called Native VLAN, is refers to UNTAG send or receive a message on the interface, is considered belongs to the VLAN. Obviously, the interface of the default VLAN ID (PVID) in the IEEE 802.1 Q VLAN ID is the Native VLAN. At the same time, send belong to Native VLAN frame on the Trunk, must adopt UNTAG way.

Allowed VLAN list: A Trunk can transport the equipment support by default all the VLAN traffic (1-4094). But, also can by setting the permission VLAN Trunk at the mouth of the list to limit the flow of some VLAN can't through the Trunk.

[Configuration example]

- 1) VLAN setting: such as create VLAN 2, Sets the port 8 to Trunk, Native VLAN 2.

New VLAN

VLAN ID(1~4094): *

VLAN Name(1-32):

☒ New VLAN ☐ New Multiple

Select ports to add to the vlan:

1	3	5	7	9	11	13	15	17	19
2	4	6	8	10	12	14	16	18	20

Optional Fixed port Selected Aggregation Trunk E

Tip: Click and drag cursor over ports to select multiple ports [Select all](#) [Select](#)

Save **Exit**

The screenshot displays the Ruijie Cloud Management System interface. The 'VLAN setting' tab is selected. In the 'VLAN Settings' section, the 'New Trunk Port' button is circled in red. A red arrow points from this button to the 'New Trunk port' configuration dialog. The dialog shows a grid of ports (1-20) with port 8 selected. A tip indicates that clicking and dragging over ports allows for selecting multiple ports. The 'Native VLAN(1-4094):' field is set to 2, and the 'Allowing VLAN(such as 3-5,8,10):' field is set to 1. The 'Save' button at the bottom of the dialog is also circled in red.

- 2) Click "next step" button, into other settings, such as: manage IP address set as 192.168.1.11, device name

set as switch-123, default gateway with the DNS server set as 172.16.1.241.

VLAN setting **Other settings**

Basic System Information

Management VLAN: 1

Management IP: 192.168.1.11 *

Subnet Mask: 255.255.255.0 *

Device Name: Switch-123 *

Default Gateway: 172.16.1.241

DNS Server: 172.16.1.241

Save **Delete** **Set Management VLAN**

Use 192.168.1.11 to log in, set a new password for 1234.

Change Administrator Password

Password type: Encrypted password

Old Password: ●●●●●●

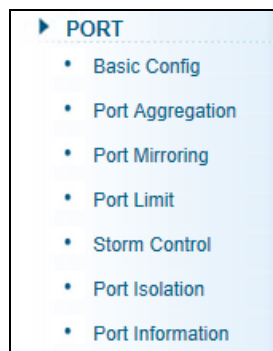
New Password: ●●●●●●

Confirm New Password: ●●●●●●

Back **Finish**

4.2. PORT

In the navigation bar to select "**PORT**", you may conduct **Basic Config**, **Port Aggregation**, **Port Mirroring**, **Port Limit**, **Storm Control**, **port Isolation** and **Port Information**.



4.2.1. Basic Config

In the navigation bar to select "**PORT>Basic Config**", For panel port to port described, port speed, port status, working mode, flow control, cross line order configuration, the following picture:

Basic settings

Optional ☐ Fixed port ☒ Selected ☐ Aggregation ☐ Trunk ☒ IP Source Enable Port

Tip: Click and drag cursor over ports to select multiple ports. Select all Select all others Cancel

Port Description(0-80 characters): Status:

Port Speed: Duplex Mode:

Flow Control: Cable Type Detection:

Port List

Port	Port Description	Port Status	Port Speed	Working Mode	Mega Frame	Cable Type Detection	Flow Control	Edit
Gi0/1		Enabled	Auto	Auto	1518	Auto	Off	
Gi0/2		Enabled	Auto	Auto	1518	Auto	Off	
Gi0/3		Enabled	1000M	Full	1518	Auto	Off	
Gi0/4		Enabled	Auto	Auto	1518	Auto	Off	
Gi0/5		Enabled	Auto	Auto	1518	Auto	Off	
Gi0/6		Enabled	Auto	Auto	1518	Auto	Off	
Gi0/7		Enabled	Auto	Auto	1518	Auto	Off	
Gi0/8		Enabled	Auto	Auto	1518	Auto	Off	
Gi0/9		Enabled	Auto	Auto	1518	Auto	Off	

[Parameter description]

Parameter	Description
Port	Select the current configuration port number
Port Description	The port is described
Status	Choose whether to close link port
Port Speed	It can choose the following kinds: Auto 10 M 100 M 1000 M
Duplex Mode	Can choose the following kinds: Auto Duplex Half duplex
Flow Control	Whether open flow control
Cable Type Detection	It can choose the following kinds: Auto MDI MDIX

[Instructions]

Open flow control should be negotiated will close, negotiated close is to set port speed rate and working mode. Set the port rate more than actual rate of port, the port will be up.

[Configuration example]

Such as: The port is set to 10 M, half duplex, open flow control and cross line sequence and port state.

Basic settings

1 3 5 7 9 11 13 15 17 19

2 4 6 8 10 12 14 16 18 20

☐ Optional ☒ Fixed port ☒ Selected ☐ Aggregation ☐ Trunk ☐ IP Source Enable Port

Tip: Click and drag cursor over ports to select multiple ports [Select all](#) [Select all others](#) [Cancel](#)

Port Description(0-80 characters):

Port Speed:

Flow Control:

Status:

Duplex Mode:

Cable Type Detection:

[Save](#)

4.2.2. Port Aggregation

In the navigation bar to select "**PORT>Port Aggregation**", In order to expand the port bandwidth or achieve the bandwidth of the redundancy backup. The following picture:

Load Balancing

Load Balancing method: [Save](#)

Port Aggregation

Aggregate Group Number(1-8):

Please select the port to join the Aggregate Group:

1 3 5 7 9 11 13 15 17 19

2 4 6 8 10 12 14 16 18 20

☐ Optional ☒ Fixed port ☒ Selected ☐ Aggregation ☐ Trunk ☐ IP Source Enable Port

Tip: Click and drag cursor over ports to select multiple ports [Select all](#) [Select all others](#) [Cancel](#)

[Save](#)

Port Aggregation List

Aggregation Group Number	Group Members	Edit / Delete

First [Back](#) [1](#) [Next](#) Last [1](#) / 1 Page

[Parameter description]

Parameter	Description
-----------	-------------

Aggregate Group Number	Switch can be set up 8 link trunk group, group_1 to group_8
Member port	For each of the members of the group and add your own port, and with members of other groups

[Instructions]

Open the port of the ARP check function, the port of the important device ARP, the port of the VLAN MAC function, and the monitor port in the port image cannot be added!

[Configuration example]

Such as: set the port 7, 8, for aggregation port 1, lets this aggregation port 1 connected to other switch aggregation port 1 to build switch links .

Load Balancing

Load Balancing method: Source MAC Save

Port Aggregation

Aggregate Group Number(1-8): 1 *

Please select the port to join the Aggregate Group:

1	3	5	7	9	11	13	15	17	19
2	4	6	8	10	12	14	16	18	20

☐ Optional
 ☐ Fixed port
 ☒ Selected
 ☒ Aggregation
 ☐ Trunk
 ☒ IP Source Enable Port

Tip: Click and drag cursor over ports to select multiple ports Select all Select all others Cancel

Save

4.2.3. Port Mirroring

In the navigation bar to select "**PORT>Port Mirroring**", Open port mirror feature, All packets on the source port are copied and forwarded to the destination port, Destination port is usually connected to a packet analyzer to analyze the source port, Multiple ports can be mirrored to a destination port, the following picture:

Port Mirroring

Mirror Group Number (1-4): 1 *

Please choose the source port:(Selecting multiple source ports can affect the device performance)

1	3	5	7	9	11	13	15	17	19
2	4	6	8	10	12	14	16	18	20

☐ Optional
 ☐ Fixed port
 ☒ Selected
 ☒ Aggregation
 ☐ Trunk
 ☒ IP Source Enable Port

Tip: Click and drag cursor over ports to select multiple ports Select all Select all others Cancel

Please choose the destination port:(Can only choose one port)

1	3	5	7	9	11	13	15	17	19
2	4	6	8	10	12	14	16	18	20

☐ Optional
 ☐ Fixed port
 ☒ Selected
 ☒ Aggregation
 ☐ Trunk
 ☒ IP Source Enable Port

Save

Port Mirror List

Mirror Group	Source Port	Destination Port	Edit/Delete

[Parameter description]

Parameter	Description
Source port	To monitor the port in and out of flow
Destination port	Set destination port, All packets on the source port are copied and forwarded to the destination port
Mirror group	Range: 1-4

[Instructions]

The port of the aggregate port cannot be used as a destination port and the source port, destination port and source port cannot be the same.

[Configuration example]

Such as: set a mirror group for port 3 regulatory port 4, 5, 6 on and out flow conditions.

Port Mirroring

Mirror Group Number (1-4):

Please choose the source port: (Selecting multiple source ports can affect the device performance)

1	3	5	7	9	11	13	15	17	19
2	4	6	8	10	12	14	16	18	20

Optional Fixed port Selected 1 Aggregation Trunk E IP Source Enable Port

Tip: Click and drag cursor over ports to select multiple ports Select all Select all others Cancel

Please choose the destination port: (Can only choose one port)

1	3	5	7	9	11	13	15	17	19
2	4	6	8	10	12	14	16	18	20

Optional Fixed port Selected 1 Aggregation Trunk E IP Source Enable Port

Save

4.2.4. Port Limit

In the navigation bar to select "**PORT>Port Limit**", to port output, input speed limit, the following picture:

Port Speed Limit



Optional ☐ Fixed port ☒ Selected ☐ Aggregation ☐ Trunk ☐ IP Source Enable Port

Tip: Click and drag cursor over ports to select multiple ports [Select all](#) [Select all others](#) [Cancel](#)

Input Speed Limit(multiple of 16): * 0,16-1,000,000Kb/s

Output Speed Limit(multiple of 16): * 0,16-1,000,000Kb/s

[Save](#)

Port Speed Limit list

Ports	Input Speed Limit	Output Speeds Limit	Edit
1	1000Mb/s	1000Mb/s	
2	1000Mb/s	1000Mb/s	
3	1000Mb/s	1000Mb/s	
4	1000Mb/s	1000Mb/s	
5	1000Mb/s	1000Mb/s	
6	1000Mb/s	1000Mb/s	
7	1000Mb/s	1000Mb/s	
8	1000Mb/s	1000Mb/s	
9	1000Mb/s	1000Mb/s	
10	1000Mb/s	1000Mb/s	

[Parameter description]

Parameter	Description
Input speed limit	Set port input speed
Output speed limit	Set port output speed

[Instructions]

1 Mbit/s = 1000 Kbit/s = 1000 / 8 KB/s = 125 KB/s . That is, the theoretical rate of 1M bandwidth is 125KB/s .

[Configuration example]

Such as: the port 5 input rate is set to 6400 KB/s, the output rate is set to 3200 KB/s.

Port Speed Limit



Optional ☐ Fixed port ☒ Selected ☐ Aggregation ☐ Trunk ☐ IP Source Enable Port

Tip: Click and drag cursor over ports to select multiple ports [Select all](#) [Select all others](#) [Cancel](#)

Input Speed Limit(multiple of 16): * 0,16-1,000,000Kb/s

Output Speed Limit(multiple of 16): * 0,16-1,000,000Kb/s

[Save](#)

4.2.5. Storm Control

In the navigation bar to select "**PORT>Storm Control**", to port storm control config, the following picture:

Broadcast Control

Counting mode: pps

Save

1 3 5 7 9 11 13 15 17 19
2 4 6 8 10 12 14 16 18 20

Optional Fixed port Selected Aggregation Trunk IP Source Enable Port

Tip: Click and drag cursor over ports to select multiple ports Select all Select all others Cancel

Broadcast Limit: * 0-262143
Multicast Limit: * 0-262143
Unicast Limit: * 0-262143

Save

Broadcast Control List

Ports	Broadcast Limit	Multicast Limit	Unicast Limit	Edit
1	0 (OFF)	0 (OFF)	0 (OFF)	
2	0 (OFF)	0 (OFF)	0 (OFF)	
3	0 (OFF)	0 (OFF)	0 (OFF)	
4	0 (OFF)	0 (OFF)	0 (OFF)	
5	0 (OFF)	0 (OFF)	0 (OFF)	
6	0 (OFF)	0 (OFF)	0 (OFF)	
7	0 (OFF)	0 (OFF)	0 (OFF)	
8	0 (OFF)	0 (OFF)	0 (OFF)	
9	0 (OFF)	0 (OFF)	0 (OFF)	

[Parameter description]

Parameter	Description
Broadcast Limit	Storm suppression value of the broadcast packets
Multicast Limit	Storm suppression value of the multicast packets
Unicast Limit	Storm suppression value of the unicast packets

[Instructions]

1 Mbit/s = 1000 Kbit/s = 1000 / 8 KB/s = 125 KB/s. That is, the theoretical rate of 1M bandwidth is 125KB/s.

[Configuration example]

Such as: should be forwarded to the port 1-8 of all kinds of packet forwarding rate is 5000 KB/s .

Broadcast Control

Counting mode: pps

Save

1 3 5 7 9 11 13 15 17 19
2 4 6 8 10 12 14 16 18 20

Optional Fixed port Selected Aggregation Trunk IP Source Enable Port

Tip: Click and drag cursor over ports to select multiple ports Select all Select all others Cancel

Broadcast Limit: 5000 * pps:0-262143 bps:0,16-4194288(Kbps)
Multicast Limit: 5000 * pps:0-262143 bps:0,16-4194288(Kbps)
Unicast Limit: 5000 * pps:0-262143 bps:0,16-4194288(Kbps)

Save

4.2.6. Port Isolation

In the navigation bar to select "PORT>Port Isolation ", ports are isolated. The following picture:

Port Isolation

Please select two or more ports to configure:

1	3	5	7	9	11	13	15	17	19
2	4	6	8	10	12	14	16	18	20

☐ Optional
 ☐ Fixed port
 ☒ Selected
 ☐ Aggregation
 ☐ Trunk
 ☒ IP Source Enable Port

Tip: Click and drag cursor over ports to select multiple ports [Select all](#) [Select all others](#) [Cancel](#)

[Save](#)

Port Isolation List

Source Port	Isolate Port	Delete

First Back [1](#) Next Last [1](#) / 1 Page

[Parameter description]

Parameter	Description
Source port	Choose a port, to configure the isolated port
Isolated port	Port will be isolated

[Instructions]

Open port isolation function, all packets on the source port are not forwarded from the isolated port, the selected ports are isolated.

Ports that have been added to the aggregate port aren't also capable of being a destination port and source port, destination port and source port cannot be the same.

[Configuration example]

Such as: the port 3, 4, 5, and 6 ports isolated.

Port Isolation

Please select two or more ports to configure:

1	3	5	7	9	11	13	15	17	19
2	4	6	8	10	12	14	16	18	20

☐ Optional
 ☐ Fixed port
 ☒ Selected
 ☐ Aggregation
 ☐ Trunk
 ☒ IP Source Enable Port

Tip: Click and drag cursor over ports to select multiple ports [Select all](#) [Select all others](#) [Cancel](#)

[Save](#)

Port Isolation List

Source Port	Isolate Port	Delete
3	4 5 6	×
4	3 5 6	×
5	3 4 6	×
6	3 4 5	×

First Back [1](#) Next Last [1](#) / 1 Page

4.2.7. Port Information

In the navigation bar to select “**PORT>Port Information**”, the following picture:

Port information							
Keyword Input port number or port description		Search	☒ Refresh				
Port▲	Description	Input Flow(bps)	Output Flow(bps)	Port Status	Port Connection	VLAN	Trunk Port
Gi 0/1		0.00K	0.00K	ON	Disconnected	1	No
Gi 0/2		0.00K	0.00K	ON	Disconnected	1	No
Gi 0/3		0.00K	0.00K	ON	Connected	1	No
Gi 0/4		0.00K	0.00K	ON	Disconnected	1	No
Gi 0/5		0.00K	0.00K	ON	Disconnected	1	No
Gi 0/6		0.00K	0.00K	ON	Disconnected	1	No
Gi 0/7		0.00K	0.00K	ON	Disconnected	1	No
Gi 0/8		0.00K	0.00K	ON	Disconnected	1	No
Gi 0/9		0.00K	0.00K	ON	Disconnected	1	No
Gi 0/10		0.00K	0.00K	ON	Disconnected	1	No

First Back **[1]** [2] Next Last / 2 Page

[Parameter description]

Parameter	Description
Input Flow	Port input flow statistics
Output Flow	Port output flow statistics

[Instructions]

Show port input and output streams information port connection status, belongs to VLAN.

[Configuration Example]

Enter port number 8 for the query.

Port information							
Keyword 8		Search	☒ Refresh				
Port▲	Description	Input Flow(bps)	Output Flow(bps)	Port Status	Port Connection	VLAN	Trunk Port
Gi 0/8		0.00K	0.00K	ON	Disconnected	1	No
Gi 0/18		0.00K	0.00K	ON	Disconnected	1	No

First Back **[1]** Next Last / 1 Page

4.3. VLAN

In the navigation bar to select "**VLAN**", You can manage the **VLAN Settings**, **Access Port Settings**, **Trunk Port Settings** and **Hybrid Port Settings**, the following picture:

VLAN Settings		Access Port Settings		Trunk Port Settings		Hybrid Port Settings	
VLAN IDs							
☐	VLAN ID	VLAN Name	VLAN IP	Port	Edit / Delete		
	1	VLAN0001	192.168.1.110/24	1-10			
New VLAN New Multiple VLAN Delete VLAN First Back1Next Last1/1 Page							

4.3.1. VLAN Settings

In the navigation bar to select "**VLAN config>VLAN Settings**", Vlan can be created and set the port to the VLAN (port default state for the access mode) , the following picture:

VLAN Settings		Access Port Settings	Trunk Port Settings	Hybrid Port Settings	
VLAN IDs					
☐	VLAN ID	VLAN Name	VLAN IP	Port	Edit / Delete
	1	VLAN0001	192.168.1.110/24	1-20	
New VLAN New Multiple VLAN Delete VLAN First Back [1] Next Last 1 / 1 Page					

[Parameter description]

Parameter	Description
VLAN ID	VLAN number
VLAN Name	VLAN mark
VLAN IP address	Manage switch IP address

[Instructions]

Management VLAN, the default VLAN cannot be deleted. Add ports to access port, port access mode can only be a member of the VLAN.

[Configuration example]

Such as: connect switches pc1, pc2 couldn't ping each other, will be one of the PC connection port belongs to a VLAN 2.

The screenshot shows the 'New VLAN' configuration window. The 'VLAN ID (2~4094)' field is set to 2, and the 'VLAN Name (1-32 character)' field is set to VLAN0002. Below these fields is a grid of ports to select. The grid shows ports 1 through 20. Port 8 is selected, indicated by a blue icon. Below the grid, there are checkboxes for 'Optional', 'Fixed port', 'Selected', 'Aggregation', 'Trunk', and 'IP Source Enable Port'. A tip at the bottom says: 'Tip: Click and drag cursor over ports to select multiple ports'. The 'Save' button is circled in red.

4.3.2. Access Port Settings

In the navigation bar to select "**VLAN config>Access Port Settings**", it can set port to Access port, the following picture:

The screenshot shows the 'Access Port Settings' window. The 'Access port list' table has the following data:

Port	Port description	Native VLAN	Operation
1		1	[Edit]
2		1	[Edit]
3		1	[Edit]
4		1	[Edit]
5		1	[Edit]
6		1	[Edit]
7		1	[Edit]
8		1	[Edit]
9		1	[Edit]
10		1	[Edit]

At the bottom, there is a 'New Access port' button and a pagination bar showing 'First Back [1] [2] Next Last 1 / 2 Page'.

[Parameter description]

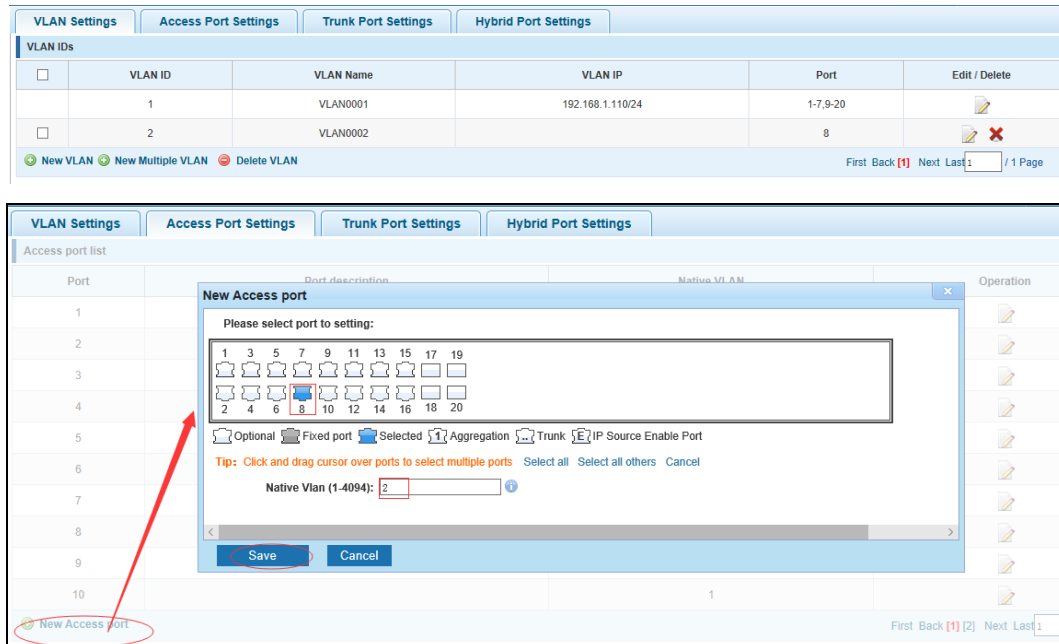
Parameter	Description
Native VLAN	Only set one

[Instructions]

Native VLAN: Refers to the default Access VLAN, must be the same as the end of the VLAN Native port, otherwise it can't work.

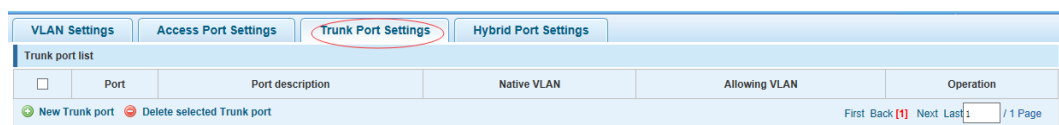
[Configuration Example]

Such as: Port 8, Access VLAN2.



4.3.3. Trunk Port Settings

In the navigation bar to select "**VLAN config>Trunk Port Setting**", it can set port to Trunk port, the following picture:



[Parameter description]

Parameter	Description
Native VLAN	Only set one
Allowing VLAN	Can set up multiple

[Instructions]

Native VLAN: as a Trunk, the mouth will belong to a Native VLAN. The so-called Native VLAN, is refers to UNTAG send or receive a message on the interface, is considered belongs to the VLAN. Obviously, the interface of the default VLAN ID (PVID) in the IEEE 802.1 Q VLAN ID is the Native VLAN. At the same time, send belong to Native VLAN frame on the Trunk, must adopt UNTAG way.

Allowed VLAN list: a Trunk can transport the equipment support by default all the VLAN traffic (1-4094). But, also can by setting the permission VLAN Trunk at the mouth of the list to limit the flow of some VLAN can't through the Trunk.

[Configuration example]

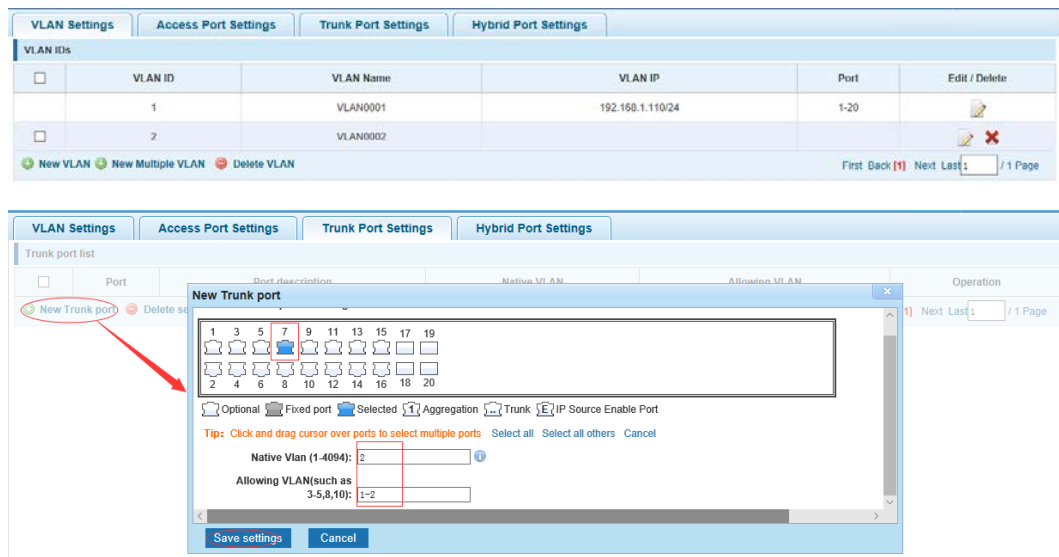
Such as: PVID=VLAN2

PC1:192.168.1.122, port 8, access VLAN2

PC2:192.168.1.123, port 7, Trunk allowed VLAN 1-2

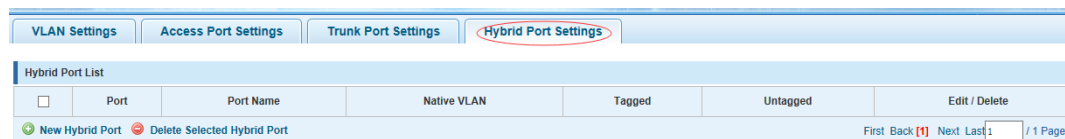
PC3:192.168.1.124, port 6, access VLAN1(The default port belongs to VLAN1)

Can let the PC2 PING PC1, cannot PING PC3



4.3.4. Hybrid Port Settings

In the navigation bar to select "**VLAN config>Hybrid Port Settings**", it Can set the port to take the tag and without the tag , the following picture:



[Instructions]

Hybrid port to packet:

Receives a packet, judge whether there is a VLAN information: if there is no play in port PVID, exchanged and forwarding, if have, whether the Hybrid port allows the VLAN data into: if can be forwarded, or discarded (untag on port configuration is not considered, untag configuration only work when to send it a message)

Hybrid port to send packet:

1, determine the VLAN in this port attributes (disp interface can see the port to which VLAN untag, which VLAN tag)

2, if it is untag stripping VLAN information, send again, if the tag is sent directly

[Configuration example]

Such as: create vlans 10, 20, VLAN sets the Native VLAN port 1 to 10, to tag VLAN for 10, 20, sets the Native VLAN port 2 to 20, to tag VLAN for 10, 20 .

VLAN Settings Access Port Settings Trunk Port Settings Hybrid Port Settings

VLAN IDs

☐	VLAN ID	VLAN Name	VLAN IP	Port	Edit / Delete
☐	1	VLAN0001	192.168.1.110/24	1-20	
☐	10	VLAN0010			
☐	20	VLAN0020			

New VLAN New Multiple VLAN Delete VLAN

First Back **1** Next Last **1** / 1 Page

VLAN Settings Access Port Settings Trunk Port Settings Hybrid Port Settings

Hybrid Port List

☐	Port	
☐		

New Hybrid Port Delete Selected Hybrid Port

New Hybrid Port

☒	1	☐	3	☐	5	☐	7	☐	9	☐	11	☐	13	☐	15	☐	17	☐	19
☐	2	☐	4	☐	6	☐	8	☐	10	☐	12	☐	14	☐	16	☐	18	☐	20

☐ Optional
 ☐ Fixed port
 ☒ Selected
 ☐ Aggregation
 ☐ Trunk
 ☐ IP Source Enable Port

Tip: Click and drag cursor over ports to select multiple ports [Select all](#) [Select all others](#) [Cancel](#)

Native Vlan(1-4094):

Tagged vlan(3-5,8,10):

Untagged vlan(such as 3-5,8,10):

[Save](#) [Cancel](#)

VLAN Settings Access Port Settings Trunk Port Settings Hybrid Port Settings

Hybrid Port List

☐	Port	
☐	1	

New Hybrid Port Delete Selected Hybrid Port

New Hybrid Port

☐	1	☐	3	☐	5	☐	7	☐	9	☐	11	☐	13	☐	15	☐	17	☐	19
☒	2	☐	4	☐	6	☐	8	☐	10	☐	12	☐	14	☐	16	☐	18	☐	20

☐ Optional
 ☐ Fixed port
 ☒ Selected
 ☐ Aggregation
 ☐ Trunk
 ☐ IP Source Enable Port

Tip: Click and drag cursor over ports to select multiple ports [Select all](#) [Select all others](#) [Cancel](#)

Native Vlan(1-4094):

Tagged vlan(3-5,8,10):

Untagged vlan(such as 3-5,8,10):

[Save](#) [Cancel](#)

VLAN Settings Access Port Settings Trunk Port Settings Hybrid Port Settings

Hybrid Port List

☐	Port	Port Name	Native VLAN	Tagged	Untagged	Edit / Delete
☐	1		10	1	10,20	
☐	2		20	1	10,20	

New Hybrid Port Delete Selected Hybrid Port

First Back **1** Next Last **1** / 1 Page

This system e0/1 and the receive system e0/2 PC can be exchanged, but when each data taken from a VLAN is different.

Data from the pc1, by inter0/1 pvid VLAN10 encapsulation VLAN10 labeled into switches, switch found system e0/2 allows 10 data through the VLAN, so the data is forwarded to the system e0/2, because the system e0/2 VLAN is untagged 10, then switches at this time to remove packet VLAN10 tag, in the form of ordinary package sent to pc2, pc1 -> pc2 is VLAN10 walking at this time

Again to analyze pc2 gave pc1 package process, data from the pc2, by inter0/2 pvid VLAN20 encapsulation VLAN20 labeled into switch, switch found system e0/1 allows VLAN by 20 data, so the data is forwarded to the system e0/1, because the system e0/1 on the VLAN is untagged 20, then switches remove packets on VLAN20 tag at this time, in the form of ordinary package sent to pc1, pc2 at this time - > pc1 is VLAN 20.

4.4. Fault/Safety

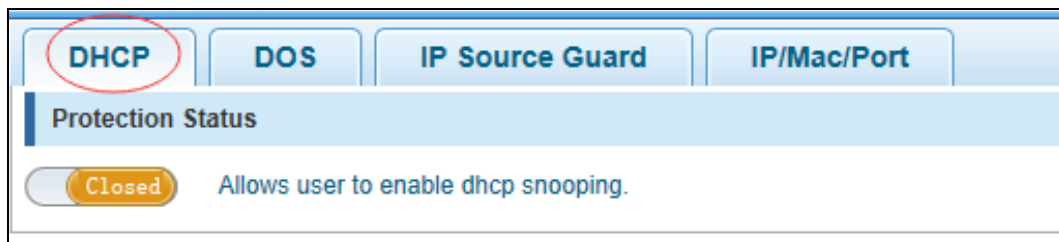
In the navigation bar to select "**Fault/Safety**", you can set **Anti attack**, **Channel Detection** and **ACL configuration**.



4.4.1. Anti Attack

4.4.1.1. DHCP

In the navigation bar to select "**Fault/safety>Anti Attack>DHCP**", Open the DHCP anti-attack function, intercepting counterfeit DHCP server and address depletion attack packets ban kangaroo DHCP server, the following picture:



[Instructions]

DHCP trusted port configuration, select the port as a trusted port. Prohibit DHCP for address, select the port and save, you can disable this feature for the port.

Open DHCP attack prevention function, need to set the DHCP protective vlan simultaneously, other functions to take effect.

[Configuration example]

Such as: 1.dhcp snooping open



2. Setting dhcp snooping vlan

DHCP configuration

DHCP Trusted Port DHCP Restricted Port Option82 Binding Table **Other Configuration**

Dhcp Snooping Vlan: *

Add

3. Set the connection router 8 ports for trust, then 6 port is set to the prohibit.

DHCP configuration

DHCP Trusted Port DHCP Restricted Port Option82 Binding Table Other Configuration

DHCP trusted port:

1	3	5	7	9	11	13	15	17	19
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
2	4	6	8	10	12	14	16	18	20
☐	☐	☐	☒	☐	☐	☐	☐	☐	☐

☐ Optional
☒ Fixed port
☒ Selected
 Aggregation
☐ Trunk
☒ IP Source Enable Port

Tip: Click and drag cursor over ports to select multiple ports Select all Select all others Cancel

Save

DHCP Trusted Ports List

Port list

DHCP configuration

DHCP Trusted Port **DHCP Restricted Port** Option82 Binding Table Other Configuration

Prohibit DHCP port:

1	3	5	7	9	11	13	15	17	19
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
2	4	6	8	10	12	14	16	18	20
☐	☐	☒	☐	☐	☐	☐	☐	☐	☐

☐ Optional
☒ Fixed port
☒ Selected
 Aggregation
☐ Trunk
☒ IP Source Enable Port

Tip: Click and drag cursor over ports to select multiple ports Select all Select all others Cancel

Save

4. Set option82 information

DHCP configuration

DHCP Trusted Port DHCP Restricted Port **Option82** Binding Table Other Configuration

Option82 Enable: ☒

Client Option82 Enable: ☒

Circuit control Remote Agent IP address

Circuit Name: *

VLAN ID: *

Add

No.	Circuit Control Name	Circuit Control ID	VLAN ID	Operations
First Back 1 Next Last 1 / 1 Page				

DHCP configuration

DHCP Trusted Port DHCP Restricted Port Option82 Binding Table Other Configuration

Option82 Enable: ☒
 Client Option82 Enable: ☒

Circuit control Remote Agent IP address

Remote Name: *
 VLAN ID: *

No.	Remote Agent Name	Remote Agent ID	VLAN ID	Operations
First Back [1] Next Last 1 / 1 Page				

DHCP configuration

DHCP Trusted Port DHCP Restricted Port Option82 Binding Table Other Configuration

Option82 Enable: ☒
 Client Option82 Enable: ☒

Circuit control Remote Agent IP address

IP Address: *
 VLAN ID: *

5. The port 7 for binding

DHCP configuration

DHCP Trusted Port DHCP Restricted Port Option82 Binding Table Other Configuration

MAC Address: *
 VLAN ID: *
 Port Number: ✓

Dhcp Snooping Binding Table

Index	Mac Address	Port Number	Vlan ID	IP Address	Lease	Status	Operations
First Back [1] Next Last 1 / 1 Page							

5.1.1.1. DOS

In the navigation bar to select "**Fault/Safety>Anti Attack>DOS**", Open the anti DOS attack function, intercept Land attack packets, illegal TCP packets, to ensure that the device or server to provide normal service to legitimate users, the following picture:

DHCP DOS IP Source Guard IP/Mac/Port

DOS Attack Protection

[Instructions]

Open the anti DOS attack function, intercept Land attack packets, illegal TCP packets, to ensure that the device or server to provide normal service to legitimate users.

[Configuration example]

Such as: Open the anti DOS attack function

DHCP **DOS** IP Source Guard IP/Mac/Port

DoS Attack Protection

5.1.1.2. IP Source Guard

In the navigation bar to select "**Fault/Safety>Anti Attack>IP Source Guard**", Through the source port security is enabled, on port forwarding the packet filter control, prevent illegal message through the port, thereby limiting the illegal use of network resources, improve the safety of the port, the following picture:

IP source protection port enable configuration

Please select a source port:

1	3	5	7	9	11	13	15	17	19
2	4	6	8	10	12	14	16	18	20

Optional Fixed port Selected Aggregation Trunk IP Source Enable Port

Tip: Click and drag cursor over ports to select multiple ports

If do not select the port, the configuration of the port will be removed. If do not select this option, the configuration of all the ports will be removed.

Save

Index	Source IP Address	Source MAC Address	Port	VLAN ID	Status	Delete
New Security Port						

First Back [1] Next Last 1 / 1 Page

[Instructions]

Add the port that is currently being used as a IP source protection enable port, the port will not be able to use.

[Configuration example]

Such as: to open source IP protection enabled port first, then to binding.

IP source protection port enable configuration

Please select a source port:

1	3	5	7	9	11	13	15	17	19
2	4	6	8	10	12	14	16	18	20

Optional Fixed port Selected Aggregation Trunk IP Source Enable Port

Tip: Click and drag cursor over ports to select multiple ports

If do not select the port, the configuration of the port will be removed. If do not select this option, the configuration of all the ports will be removed.

Save

IP source protection port enable configuration

Please select a source port:

1 3 5 7 9 11 13
2 4 6 8 10 12 14

Optional Fixed port Selected

Tip: Click and drag cursor over port icon
If do not select the port, the port will be disabled.

Save

Manual IP Source Protection List

Index

New Security Port

VLAN ID: 1 *

Source IP Address: 192.168.1.30 *

Source MAC Address *

3 5 7 9 11 13 15 17 19
2 4 6 8 10 12 14 16 18 20

Optional Fixed port Selected 1 Aggregation Trunk IP Source Enable Port

Save Exit

5.1.1.3. IP/Mac/Port

In the navigation bar to select "**Fault/safety>Anti Attack>IP/Mac/Port**", automatically detect the port based IP address, MAC address of the mapping relationship, and then realize the function of a key binding, the following picture:

DHCP DOS IP Source Guard IP/Mac/Port

Test List

Binding Enable ☒

	MAC Address	IP Address	Port Number
☐			

First Back [1] Next Last 1 / 1 Page

Scanning Binding

Application List

	MAC Address	IP Address	Port Number
☐			

Delete First Back [1] Next Last 1 / 1 Page

[Instructions]

A bond must be bound before the binding to enable the switch to open. And if you want to access shall be binding and switch the IP address of the same network segment.

[Configuration example]

Such as: the binding to make first can open, must be a key bindings port 7.

Binding Enable ☒

☐	
--------------------------	--

Scanning Binding

Binding enable ☒

	mac address	ip address	Port number
☐			10
☐			10
☐			10
☒			10
☐			4

first page prev page **11** next page last page 1 / 1 page

Scanning Binding

Application List

	mac address	ip address	Port number
☐		192.168.2.11	10

Delete option first page prev page **11** next page last page 1 / 1 page

Can check the delete option.

5.1.2. Channel Detection

5.1.2.1. Ping

In the navigation bar to select "**Fault/Safety> Channel Detection>Ping**", Use ping function to test internet connect and host whether to arrive. The following picture:

Ping Tracert Cable Test

Destination IP Address: *

Timeout in Seconds (1-10):

Ping Count (1-100):

Start

[Parameter description]

Parameter	Description
Destination IP address	Fill in the IP address of the need to detect
Timeout in Seconds	Range of 1 to 10
Ping Count	Testing number

[Instructions]

Use ping function to test internet connect and host whether to arrive.

[Configuration example]

Such as: PING connect the IP address of the PC .

Ping **Tracert** Cable Test

Destination IP Address: *

Timeout in Seconds (1-10):

Ping Count (1-100):

Start

Result

```
PING 192.168.1.110 (192.168.1.110): 56 data bytes
64 bytes from 192.168.1.110: icmp_seq=0 ttl=64 time=0.0 ms
64 bytes from 192.168.1.110: icmp_seq=1 ttl=64 time=0.0 ms
64 bytes from 192.168.1.110: icmp_seq=2 ttl=64 time=0.0 ms
64 bytes from 192.168.1.110: icmp_seq=3 ttl=64 time=0.0 ms
64 bytes from 192.168.1.110: icmp_seq=4 ttl=64 time=0.0 ms
--- 192.168.1.110 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

5.1.2.2. Tracert

In the navigation bar to select "**Fault/Safety> Channel Detection>Tracert**", Tracert detection can detect to the destination through. The following picture:

Ping **Tracert** Cable Test

Destination IP Address:

Start

Result

[Parameter description]

Parameter	Description
Destination IP address	Fill in the IP address of the need to detect

[Instruction]

The function is used to detect more is up to and reach the destination path. If a destination unreachable, diagnose problems.

[Configuration example]

Such as: Tracert connect the IP address of the PC.

Ping Tracert **Cable Test**

Destination IP Address: 192.168.1.110 *

Start

Result

Tracing the route to 192.168.1.110

1	192.168.1.110	<10 ms	<10 ms	<10 ms
---	---------------	--------	--------	--------

5.1.2.3. Cable Test

In the navigation bar to select "**Fault/Safety> Channel Detection>Cable Test**", Can detect connection device status. The following picture:

Ping Tracert **Cable Test**

Please select port to configure:

1	3	5	7	9	11	13	15	17	19
2	4	6	8	10	12	14	16	18	20

Optional Fixed port Selected Aggregation Trunk IP Source Enable Port

Start

[Configuration example]

Ping Tracert **Cable Test**

Please select port to configure:

1	3	5	7	9	11	13	15	17	19
2	4	6	8	10	12	14	16	18	20

Optional Fixed port Selected Aggregation Trunk IP Source Enable Port

Start

Result

Port	Length(m)	Status
8	1	Circuit Breaker

First Back [1] Next Last 1 / 1 Page

5.1.3. ACL

In the navigation bar to select "**Fault/Safety>ACL**", Can be applied to port ACL rules and Settings to take effect in time.

[Instruction]

The ACL rules are sequenced, row in front of the match will be priority rule. Many, if the strategy items operating time is relatively longer.

Basic principles:

- 1, according to the order, as long as there is a meet, will not continue to find.
- 2, implied refused, if don't match, so must match the final implied refused entry, cisco default.
- 3, any only under the condition of the minimum permissions to the user can satisfy their demand.
- 4, don't forget to apply the ACL to the port.

[Configuration example]

Such as: test time is every Monday to Friday 9 to 18 points, set port 1-6 cannot access the network.

Steps: building ACL time - building ACL rules - is applied to the port.

Timetable ACL Apply ACL

Create ACL

The new ACL access rule

Priority 1

ACL Number: 100 * Protocol Type: IP

Permission: Permit ACL Name:

Any src IP Address: ☒ Any dst IP Address: ☒

Save

Timetable ACL Apply ACL

Create ACL

Priority	Acl number	Permission	Index	Protocol	Source IP / Mask	Source Port	Destination IP / Mask	Destination Port	Timetable Name	Status	Delete
1	100	deny	10	tcp	any/any	any	any/any	80	Workday	active	✖
1	100	permit	20	ip	any/any	any	any/any	any	none	active	✖

First Back 1 Next Last 1 / 1 Page

Timetable ACL Apply ACL

1 3 5 7 9 11 13 15 17 19

2 4 6 8 10 12 14 16 18 20

Optional Fixed port Selected 1 Aggregation Trunk IP Source Enable Port

Tip: Click and drag cursor over ports to select multiple ports

ACL Number: 100

Filtering Direction: Receive message

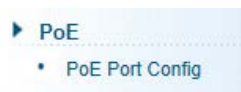
Save

Access Control List

ACL Number	Port
------------	------

5.2. PoE

In the navigation bar to select "PoE", you can set to the **PoE Port Config** configuration.



5.2.1. PoE Port Config

5.2.1.1. Chip information

In the navigation bar to select "**PoE>PoE Port Config>Chip information**", you can view chip information.

Chip information		
The total power of the system: 240(W) The current system consumes: 0.00(W)		
List	InputVoltage(v)	Temperature(c)
1	53.00	40.00
2	53.00	39.00

First Back **1** Next Last 1 / 1 Page

5.2.1.2. Poe Port Config

In the navigation bar to select "**PoE>PoE Port Config>Poe Port Config**", you can set Poe Port , As follows.

Chip information

Poe Port Config

Select ports to setting:

1 3 5 7 9 11 13 15

2 4 6 8 10 12 14 16

Optional

Fixed port

Selected

Aggregation

Trunk

IP Source Enable Port

Tip: Click and drag cursor over ports to select multiple ports

Select all

Select all others

Cancel

port enabled: Enabled

Port power(W): 30

Port Priority: Low

Save

PoE config

Ports	Enable Control	Status	Priority	Max power	CurrentPower(W)	Class
GI1	Enable	Disable	Low	30	0.0	Unknown
GI2	Enable	Disable	Low	30	0.0	Unknown
GI3	Enable	Disable	Low	30	0.0	Unknown
GI4	Enable	Disable	Low	30	0.0	Unknown
GI5	Enable	Disable	Low	30	0.0	Unknown
GI6	Enable	Disable	Low	30	0.0	Unknown
GI7	Enable	Disable	Low	30	0.0	Unknown
GI8	Enable	Disable	Low	30	0.0	Unknown
GI9	Enable	Disable	Low	30	0.0	Unknown
GI10	Enable	Disable	Low	30	0.0	Unknown

First Back **1** **2** Next Last 1 / 2 Page

[Parameter description]

Parameter	Description
port enabled	You can enable or disable PoE function
Port power	You can configure max power of port
Port Priority	You can configure Port Priority

[Configuration example]

Such as: The PoE function of port 8 can be enabled, the maximum Port power is 23 W, and the Power supply priority is high.

5.3. STP

In the navigation bar to select "STP", you can set to the **MSTP region** and **STP bridge** configuration.



5.3.1. MSTP Region

In the navigation bar to select "**STP>MSTP Region**", Can modify the domain and domain name, add instance is mapped to a VLAN. the following picture.

Instance ID	Mapping VLAN	Edit
0	1-4094	

[Parameter description]

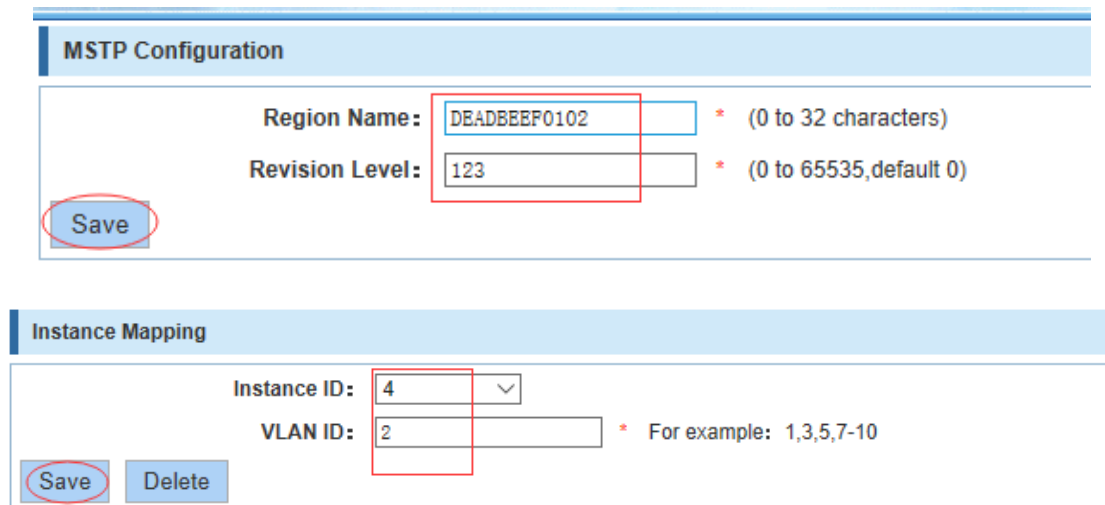
Parameter	Description
Region Name	Configure the region name
Revision Level	Parameter configuration revision level
Instance ID	Select configuration instance ID
VLAN ID	Mapping of the VLAN configuration instance

[Instruction]

An instance can only be mapped to a VLAN, instance and VLAN is a one-to-one relationship.

[Configuration example]

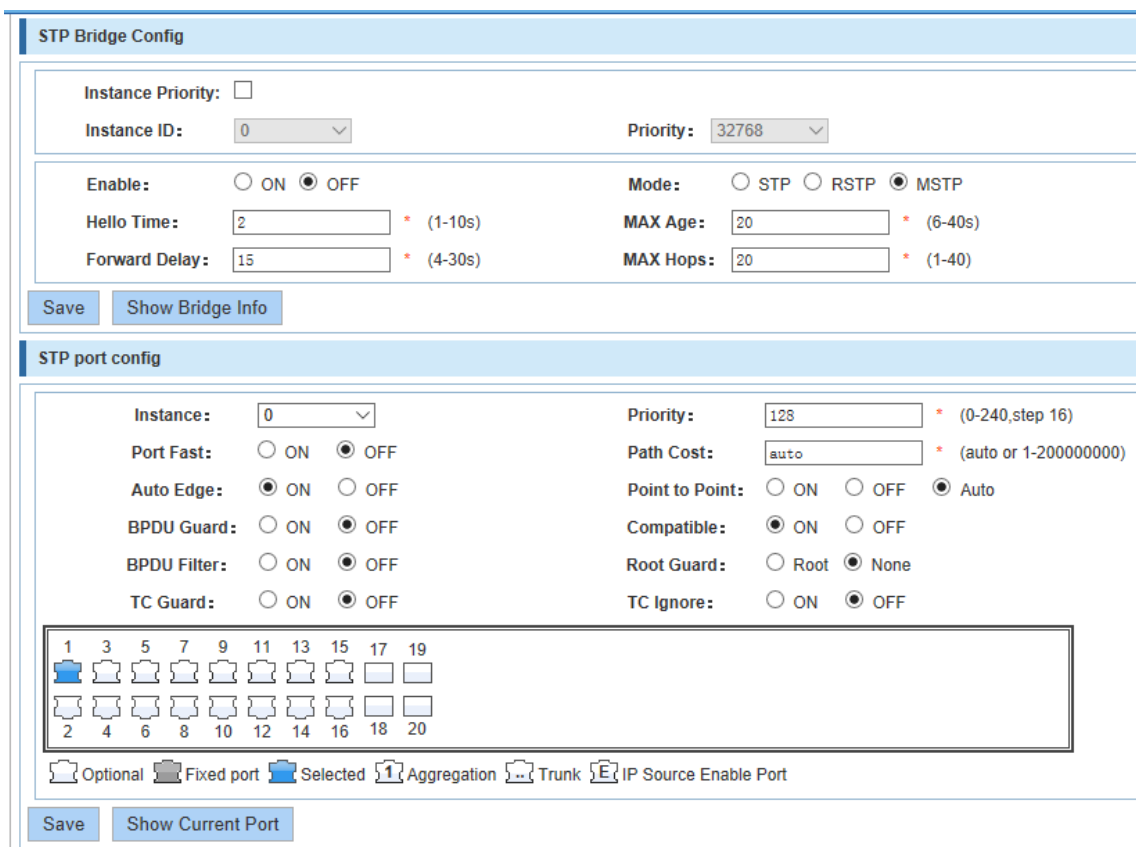
Such as: change the region to DEADBEEF0102, region name is 123, instance 4 is mapped to a VLAN 2, in the first need to create a VLAN 2.



The image shows two screenshots from a network configuration interface. The top screenshot is titled "MSTP Configuration" and contains two input fields: "Region Name" with the value "DEADBEEF0102" and "Revision Level" with the value "123". Both fields are highlighted with red boxes. A "Save" button is circled in red. The bottom screenshot is titled "Instance Mapping" and contains two input fields: "Instance ID" with the value "4" and "VLAN ID" with the value "2". Both fields are highlighted with red boxes. "Save" and "Delete" buttons are visible at the bottom left.

5.3.2. STP Bridge

In the navigation bar to select "**STP>STP Bridge**", Can be related to bridge, port configuration, and the following picture:



The image shows two screenshots from a network configuration interface. The top screenshot is titled "STP Bridge Config" and contains several configuration options: "Instance Priority" (checkbox), "Instance ID" (0), "Priority" (32768), "Enable" (ON/OFF), "Mode" (STP/RSTP/MSTP), "Hello Time" (2), "MAX Age" (20), "Forward Delay" (15), and "MAX Hops" (20). The bottom screenshot is titled "STP port config" and contains several configuration options: "Instance" (0), "Port Fast" (ON/OFF), "Auto Edge" (ON/OFF), "BPDU Guard" (ON/OFF), "BPDU Filter" (ON/OFF), "TC Guard" (ON/OFF), "Priority" (128), "Path Cost" (auto), "Point to Point" (ON/OFF/Auto), "Compatible" (ON/OFF), "Root Guard" (Root/None), and "TC Ignore" (ON/OFF). Below these options is a grid of 20 port icons, with port 1 highlighted in blue. A legend at the bottom indicates port types: Optional, Fixed port, Selected, Aggregation, Trunk, and IP Source Enable Port.

[Parameter description]

Parameter	Description
-----------	-------------

Instance Priority	Whether open instance priority setting
Instance ID	Select the created instance id is configured
Bridge Priority	Priority setting bridge example, the default instance bridge priority for 32768
Enable	Whether to open the STP bridge function
Mode	The model is divided into: the STP, RSTP, MSTP
Hello Time	Switches sends bpdu in packet interval
Max Age	Ports are not yet received a message in the time, will initiate topology changes
Forward Delay	The state of the port switch time
Port Priority	Set port instance priority, defaults to 128, you must enter multiple of 16, the range of 0-240
Path Cost	Configure port costs
Port Fast	Select configuration state
Auto Edge	Select configuration state
Point to Point	Select configuration state
BPDU Guard	Select configuration state
BPDU Filter	Select configuration state
Compatible	Select configuration state
Root Guard	Select configuration state
TC Guard	Select configuration state
TC Ignore	Select configuration state

[Instruction]

- (1) $(\text{hello_time}+1) \times 2 \leq \text{max_age} \leq (\text{f_delay}-1) \times 2$, enable the switch to set instance priority.
(2) Enable STP or switch mode would spend 2 times of the forward delay time.

[Configuration example]

Such as: 1) Open the STP, configuration has to create an instance of the priority, configuration time parameters, set the pattern to MSTP.

STP port config

Instance: Priority: * (0-240, step 16)

Port Fast: ☒ ON ☐ OFF Path Cost: * (auto or 1-200000000)

Auto Edge: ☒ ON ☐ OFF Point to Point: ☐ ON ☐ OFF ☒ Auto

BPDU Guard: ☒ ON ☐ OFF Compatible: ☐ ON ☒ OFF

BPDU Filter: ☐ ON ☒ OFF Root Guard: ☐ Root ☒ None

TC Guard: ☐ ON ☒ OFF TC Ignore: ☐ ON ☒ OFF

1 3 5 7 9 11 13 15 17 19
2 4 6 8 10 12 14 16 18 20

☐ Optional ☒ Fixed port ☒ Selected ☐ Aggregation ☐ Trunk ☐ IP Source Enable Port

Save **Show Current Port**

STP Bridge Config

Instance Priority: ☐ Instance ID:

Enable: ☐ ON ☒ OFF

Hello Time: Forward Delay:

Save **Show Bridge Info**

STP port config

Instance: Port Fast: ☒ ON ☐ OFF

Auto Edge: ☒ ON ☐ OFF BPDU Guard: ☒ ON ☐ OFF

BPDU Filter: ☐ ON ☒ OFF TC Guard: ☐ ON ☒ OFF

1 3 5 7 9 11 13 15
2 4 6 8 10 12 14 16 18 20

☐ Optional ☒ Fixed port ☒ Selected ☐ Aggregation ☐ Trunk ☐ IP Source Enable Port

Save **Show Current Port**

STP Port Information [Gi0/4]

-----[Gi0/4]-----

PortAdminPortFast: enable
PortOperPortFast: disable
PortAdminAutoEdge: enable
PortOperAutoEdge: disable
PortAdminLinkType: auto
PortOperLinkType: share
PortBPDUGuard: enable
PortBPDUFilter: disable
PortTCGuard: disable

instance[0]
VlanMap: 1,3-4094
PortState: down
PortPriority: 128
PortDesignatedRoot: 32768 - 00:e0:4c:00:00:00
PortDesignatedCost: 0
PortDesignatedBridge: 32768 - 00:e0:4c:00:00:00
PortDesignatedPortPriority: 0
PortDesignatedPort: 0
PortAdminPathCost: auto
PortOperPathCost: 200000000
PortRole: disabled

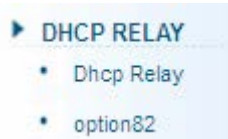
instance[4]
VlanMap: 1,3-4094

Exit

2) Set MSTP has launched port configuration, select the created instance, set priority (port configuration is not online, on-line configuration will only take effect, can click on the "view the current configuration" button to view the configured completed)

5.4. DHCP RELAY

In the navigation bar to select "**DHCP RELAY**", you can set to the **Dhcp relay** and **option82**.



5.4.1. DHCP RELAY

In the navigation bar to select "**DHCP RELAY>Dhcp relay**", Open the DHCP relay function, set up and view the relay server IP address and its status. the following picture.

DHCP Relay Enable	
DHCP Relay Enable:	☐
DHCP Option Trust Field Enable:	☒

[Parameter description]

Parameter	Description
IP address	DHCP server address
status	Invalid and valid

[Instruction]

If open the function of relay agent, then receives the broadcast DHCP message, to be delivered in the form of unicast to configure on the server. The DHCP server to IP and switches in the same network segment will only take effect.

[Configuration example]

Such as: setting DHCP server ip for 192.168.1.22

DHCP Relay Enable			
DHCP Relay Enable: ☒			
DHCP Option Trust Field Enable: ☒			
DHCP Relay Config			
DHCP Server IP: 192.168.1.22 *			
Save			
Number	IP Address	Status	Edit
1	0.0.0.0	invalid	<input checked="" type="button" value="✖"/>
First Back 1 Next Last 1 / 1 Page			

5.4.2. option82

In the navigation bar to select "**Dhcp relay>option82**", can set to OPTION82 circuit control, proxy remote, IP address. The following picture:

Option82 Config

Circuit Control Proxy Remote IP Address

Circuit Control: *

VLAN ID:

Save

Number	Circuit Name	Circuit ID	VLAN ID	Edit / Delete
first page prev page 1 next page last page: / 1 page				

[Parameter description]

Parameter	Description
VLAN ID	the DHCP request message in the VLAN, value range is 1 ~ 4094
Circuit Control	Circuit ID to populate the user custom content, scope of string length is 3 ~ 63
Proxy Remote	Configuration ASCII remote id string value, the length of the range of 1 ~ 63
IP Address	Decimal IP address

[Instruction]

Switches, relay information to the DHCP server will take option82, VLAN ID must be configured to DHCP message taken VLAN can bring option82 information.

[Configuration example]

Such as: add circuit control, proxy remote, ip address information.

Option82 Config

Circuit Control Proxy Remote IP Address

Circuit Control: *

Circuit ID: *

VLAN ID: *

Save

Number	Circuit Name	Circuit ID	VLAN ID
--------	--------------	------------	---------

Option82 Config

Circuit Control Proxy Remote IP Address

Proxy Remote: *

Proxy Remote ID: *

VLAN ID: *

Save

Number	Proxy Remote Name	Proxy Remote ID
--------	-------------------	-----------------

The screenshot shows the 'Option82 Config' window with three tabs: 'Circuit Control', 'Proxy Remote', and 'IP Address'. The 'IP Address' tab is active. It contains two input fields: 'IP Address' with the value '192.168.1.35' and 'VLAN ID' with the value '1'. Both fields have a red asterisk to their right. A 'Save' button is located below the 'VLAN ID' field. At the bottom, there is a table with two columns: 'Number' and 'IP Address'.

5.5. QOS

In the navigation bar to select "QOS", you can set to the **Queue Config** and **Mapping the Queue**.



5.5.1. Queue Config

In the navigation bar to select "QoS>Queue Config", Can be set up queue scheduling policy. The following picture:

The screenshot shows the 'Queue setting' window. It has a 'Queue mode' dropdown menu set to 'WFQ'. Below it, there is a 'Byte weight (0~127):' section with eight input boxes numbered 1 through 8. An 'Apply' button is located at the bottom left.

[Parameter description]

Parameter	Description
Queue mode	Can choose four kinds of modes: RR round-robin scheduling SP absolute priority scheduling WRR weighted round-robin scheduling WFQ weighted fair scheduling
Byte weight	Set the weights of each queue, they will be in proportion to occupy the bandwidth to send data

[Instruction]

Queue 7 cannot for 0.

[Configuration example]

Such as: set the scheduling strategy for WRR, weight value respectively, 10, 11, 12, 12, 14, 15, 16, 17.

Queue setting

Scheduling strategy: WRR

Byte weight(0~127): 10 11 12 13 14 15 16 17

Apply

5.5.2. Mapping the Queue

5.5.2.1. COS Queue Map

In the navigation bar to select "**QoS>Mapping the Queue>COS Queue Map**", Service category can be mapped to the corresponding queue. The following picture:

COS Queue Map **DSCP COS Map** **Port COS Map**

Mapping Queue Status Information

Server ID	0	1	2	3	4	5	6	7
Queue ID	0	1	2	3	4	5	6	7

Save

[Parameter description]

Parameter	Description
Server ID	COS the VLAN priority fields (0 to 7)
Queue ID	Set each cosine value mapping queue number (0 to 7)

[Configuration example]

Such as: cos 3 mapping to the queue 7, set the queue weight 7 to 10.

COS Queue Map **DSCP COS Map** **Port COS Map**

Mapping Queue Status Information

Server ID	0	1	2	3	4	5	6	7
Queue ID	0	1	2	7	4	5	6	7

Save

Queue setting

Queue mode:

WRR

Byte weight (0~127):

0

0

0

0

0

0

0

10

Apply

5.5.2.2. DSCP COS Map

In the navigation bar to select "QoS>Mapping the Queue>DSCP COS Map", Differential service can be mapped to the corresponding service categories. The following picture:

COS Queue Map

DSCP COS Map

Port COS Map

Differential service code point mapping team list

Server ID	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Server List 1	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
Server ID	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Server List 2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3
Server ID	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
Server List 3	4	4	4	4	4	4	4	4	5	5	5	5	5	5	5	5
Server ID	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
Server List 4	6	6	6	6	6	6	6	6	7	7	7	7	7	7	7	7

Save

[Parameter description]

Parameter	Description
Server list	DSCP field has seven (0-63) is divided into four tables
Server ID	Map the DSCP to COS fields (0 to 7), based on the cosine is mapped to a queue

[Instruction]

Cos priority is greater than the DSCP, DSCP priority is greater than the port.

[Configuration example]

Such as: the DSCP value of 3, 12, 23 mapping to cos 5.

COS Queue Map		DSCP COS Map		Port COS Map												
Differential service code point mapping team list																
Server ID	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Server List 1	0	0	0	5	0	0	0	0	1	1	1	1	1	5	1	1
Server ID	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Server List 2	2	2	2	2	2	2	2	5	3	3	3	3	3	3	3	3
Server ID	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
Server List 3	4	4	4	4	4	4	4	4	5	5	5	5	5	5	5	5
Server ID	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
Server List 4	6	6	6	6	6	6	6	6	7	7	7	7	7	7	7	7
Save																

5.5.2.3. Port COS Map

In the navigation bar to select "**QoS>Mapping the Queue>Port COS Map**". Port can be mapped to the corresponding service categories. The following picture:

COS Queue Map		DSCP COS Map		Port COS Map					
Port CoS mapping									
Port:	1								
Server ID:	0								
Trust Mode:	none								
Apply									
Control list									
Port	Server ID							Trust Mode	
	0	1	2	3	4	5	6	7	
1	T								
2	T								
3	T								
4	T								
5	T								
6	T								
7	T								
8	T								
First Back [1] [2] [3] Next Last 1 / 3 Page									

[Parameter description]

Parameter	Description
Port	Select the port number (1-10)
Service ID	Mapped to the service ID, and then according to the service ID into the queue

[Instruction]

Cos priority is greater than the DSCP, DSCP priority is greater than the port.

[Configuration example]

Such as: port 4, 5, 6 respectively cos4,cos5,cos6.

COS Queue Map DSCP COS Map Port COS Map

Port CoS mapping

Port: 4
 Server ID: 4
 Trust Mode: COS

Apply

COS Queue Map DSCP COS Map Port COS Map

Port CoS mapping

Port: 5
 Server ID: 5
 Trust Mode: COS

Apply

COS Queue Map DSCP COS Map Port COS Map

Port CoS mapping

Port: 6
 Server ID: 6
 Trust Mode: COS

Apply

Control list									
Port	Server ID							Trust Mode	
	0	1	2	3	4	5	6	7	
1	T								
2	T								
3	T								
4					T				COS
5						T			COS
6							T		COS
7	T								
8	T								

First Back 1 2 3 Next Last 1 / 3 Page

5.6. Addr table

In the navigation bar to select "**Addr table**", you can set to **Address Table**.

Address Table Config

MAC Management MAC Learning and Aging MAC Filter

Clear MAC:

VLAN: Valid Range (1 to 4094)

MAC Address:

☐ Optional
☐ Fixed port
☒ Selected
 Aggregation
☐ Trunk
☒ IP Source Enable Port

VLAN: Valid Range (1 to 4094)

MAC Address:

MAC Address List:

Number	MAC Address	VLAN ID	Address Type	Port
1	00:0E:C8:D6:21:5C	1	dynamic	5

first page prev page **1** next page last page 1 / 1 page

5.6.1. MAC Management

In the navigation bar to select **"Addr Table > Address table > MAC Management"**. You can add static Mac and delete Mac and view to the current of the Mac address table. The following picture:

Address Table Config

MAC Management MAC Learning and Aging MAC Filter

Clear MAC:

VLAN: Valid Range (1 to 4094)

MAC Address:

☐ Optional
☐ Fixed port
☒ Selected
 Aggregation
☐ Trunk
☒ IP Source Enable Port

VLAN: Valid Range (1 to 4094)

MAC Address:

MAC Address List:

Number	MAC Address	VLAN ID	Address Type	Port
1	00:0E:C8:D6:21:5C	1	dynamic	5

first page prev page **1** next page last page 1 / 1 page

[Parameter description]

Parameter	Description
MAC Address	Can choose to clear the multicast Mac address, clear dynamic unicast Mac address, clear static unicast Mac address, clear the specified Mac address, Mac address table
VLAN	Fill in the need to add or delete VLAN id, not create VLAN to create can only take effect

[Instruction]

According to different conditions to clear Mac address, view/add/learn the Mac address, Mac address filtering.

[Configuration example]

Such as: 1) the port 6 Mac set to static Mac.

1 3 5 7 9 11 13 15 17 19
2 4 6 8 10 12 14 16 18 20

Optional Fixed port Selected Aggregation Trunk IP Source Enable Port

VLAN: 1 Valid Range (1 to 4094)

MAC Address :

Save

2) Clear port 6 static Mac addresses.

1 3 5 7 9 11 13 15 17 19
2 4 6 8 10 12 14 16 18 20

Optional Fixed port Selected Aggregation Trunk IP Source Enable Port

VLAN: 1 Valid Range (1 to 4094)

MAC Address :

Save

5.6.2. MAC Learning and Aging

In the navigation bar to select **Addr Table>Address table>MAC Learning and Aging**, Can be set up port Mac address study limit and Mac address aging time. The following picture:

Address Table Config

MAC Management MAC Learning and Aging MAC Filter

1 3 5 7 9 11 13 15 17 19
2 4 6 8 10 12 14 16 18 20

Optional Fixed port Selected Aggregation Trunk IP Source Enable Port

MAC Learning Limit: 8191 (Learning Range 0-8191)

Save

MAC Address Aging Time: 300 (0 indicates no aging 10-1000000 second)

Save

Number	Port	MAC Learning Limit Number
1	Gi0/1	8191
2	Gi0/2	8191
3	Gi0/3	8191
4	Gi0/4	8191
5	Gi0/5	8191
6	Gi0/6	8191
7	Gi0/7	8191
8	Gi0/8	8191

First Back 1 2 3 Next Last 1 / 3 Page

[Parameter description]

Parameter	Description
MAC Learning Limit	Range 0-8191,default 8191

MAC Address Aging Time	Default 300
------------------------	-------------

[Configuration example]

Such as: 1) setting port 2 address study limit for 2000.

2) Will be dropped or learn the Mac address of the port equipment after 2 minutes disappear automatically from the Mac address table

5.6.3. MAC Filter

In the navigation bar to select "**Addr Table > Address table > MAC Filter**", Can be filtered according to the condition does not need the Mac address. the following picture:

[Parameter description]

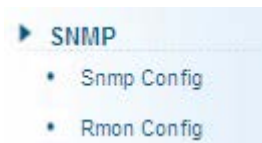
Parameter	Description
MAC address	Can't add multicast Mac address
VLAN	VLAN number

[Configuration example]

Such as: the Mac address for 00:20:15:09:12:12 added to the filter in the table.

5.7. SNMP

In the navigation bar to select **"SNMP"**, you can set to the **Snmp Config** and **Rmon Config**.



5.7.1. Snmp Config

5.7.1.1. Snmp Config

In the navigation bar to select **"SNMP > Snmp Config > SNMP Config"**, you can Snmp function enable. The following picture:

[instruction]

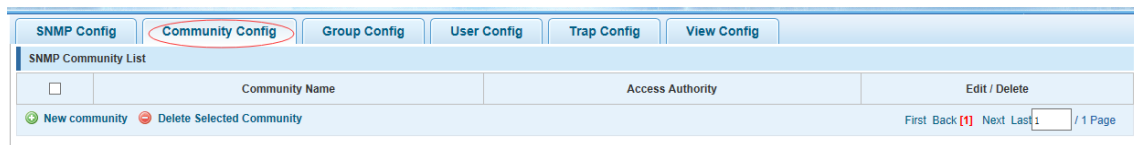
The SNMP function must be turned on in the configuration RMON, otherwise it will be configured to fail.

[Configuration example]

Such as: open Snmp.

5.7.1.2. Community Config

In the navigation bar to select **"SNMP > Snmp Config > Community Config"**, Can specify group access. the following picture.



[Parameter description]

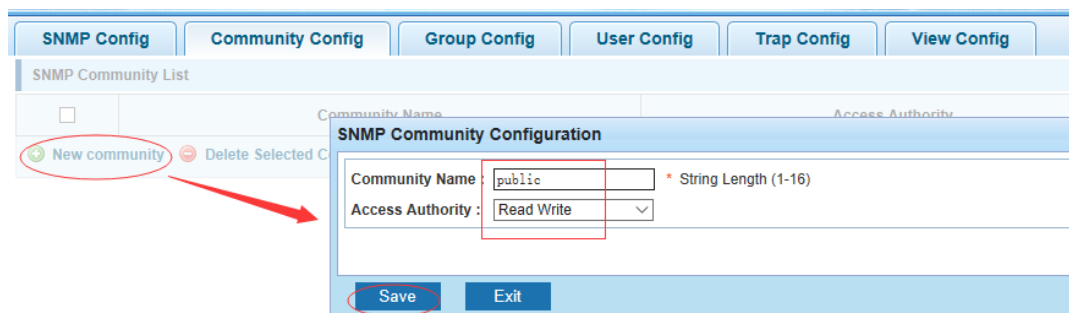
Parameter	Description
group	Community string, is equal to the NMS and Snmp agent communication between the password
Access authority	Read-only: specify the NMS (Snmp host) of MIB variables can only be read, cannot be modified Read-only can write: specify the NMS (Snmp host) of MIB variables can only read, can also be modified

[Instruction]

The upper limit of the number of groups is 8.

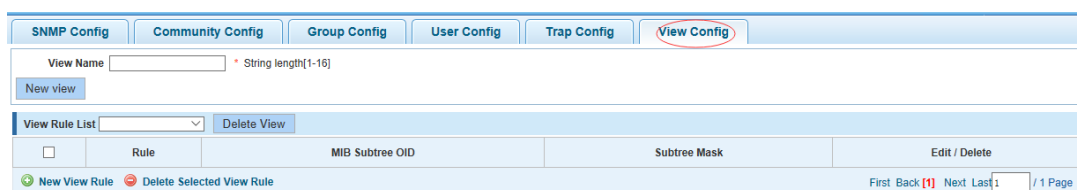
[Configuration example]

Such as: add a read-write group called public...



5.7.1.3. View Config

In the navigation bar to select **"SNMP>Snmp Config>View Config"**, Set the view the rules to allow or disable access to some of the MIB object. the following picture.



[Parameter description]

Parameter	Description
View name	View name
include	Indicate the MIB object number contained within the view

exclude	Indicate the MIB object son number was left out of view
MIB Subtree OID	View the associated MIB object, is a number of MIB
Subtree mask	MIB OID mask

[Instruction]

Each view is best to configure a view rule, otherwise it will affect the SNMP function.

[Configuration example]

such as: establish a view 123 , MIB subtree oid .1.3.6.1 contain among them.

5.7.1.4. Group Config

In the navigation bar to select **"Snmpp>Snmpp Config>Group Config"**, setting Snmp group. The following picture:

[Parameter description]

Parameter	Description
Group name	Group name
Security level	Attestation not only encryption: this group of users transmission of the message need to verify the data don't need to confidential No authentication encryption: this group of users' messages don't need to verify data transmission also does not need to be kept secret

	Both authentication and encryption: this group of users need to verify the news of transmission and transmission of data need to be kept secret
Read view, read and write view ,study view	The associated view name

[Instruction]

Before the cap on the number set of configuration of 8, the new group needs a new view to create a group.

[Configuration example]

Such as: firstly, new view 123, then new group of goup1.

The screenshot displays the 'View rule list' table with the following data:

rule	MIB subtree OID	subtree mask	operation
included	.1.3.6.1		

Below the table, there are buttons for 'New view rule' and 'Delete select View rule'. The 'SNMP Group' configuration page is shown with a 'New Group' dialog box open. The dialog box contains the following fields:

- Group Name : group1
- Security Level : Authentication and r
- Read View : none
- Write View : none
- Notify View : none

The 'Save' button is highlighted with a red circle, and a red arrow points to it from the 'New Group' button in the background.

5.7.1.5. User Config

In the navigation bar to select **"Snm>Snm Config>User Config"**, setting Snmp user. The following picture:

The screenshot displays the 'User Config' page. The navigation bar at the top shows 'SNMP Config', 'Community Config', 'Group Config', 'User Config' (highlighted with a red circle), 'Trap Config', and 'View Config'. Below, the 'SNMP User' configuration page is shown with a table for user configuration. The table has columns for User Name, Security Level, Group Name, Authentication Mode, Authentication Password, Encrypt Mode, Encrypt password, and Edit / Delete. The 'New User' button is highlighted with a red circle.

[Parameter description]

Parameter	Description
User Name	User name, range 1-16
Security Level	Attestation not only encryption: this group of users transmission of the message need to verify the data don't need to confidential No authentication encryption: this group of users' messages don't need to verify data transmission also does not need to be kept secret

	Both authentication and encryption: this group of users need to verify the news of transmission and transmission of data need to be kept secret
Authentication Mode	Specified use MD5 authentication protocol or SHA authentication protocol
Authentication Password	Range 8-10
Encrypt Mode	Specified using AES encryption protocol or DES encryption protocol
Group Name	A user group name
Encrypt Password	Range 8-60

[Instruction]

Cap on the number configuration of 8, users need a new view and group to use, the user's security level must be consistent with the group level of security. Add a user authentication and encryption, and configure belong to groups of users, the user will be used for Snmpv3 connection.

[Configuration example]

Such as: new view 123, the newly built group group1, new user user1.

5.7.1.6. Trap Config

In the navigation bar to select "**Snmp>Snmp Config>Trap Config**", Can specify sent the trap messages to Snmp host (NMS). the following picture:

[Parameter description]

Parameter	Description
Destination IP address	Snmp host ipv4 address
Security name	Snmp user name
version	V1,V2,V3
Security mode	Specified using AES encryption protocol or DES encryption protocol
Group name	User group name

[Instruction]

The Trap cap on the number configuration of 8, you can configure a number of different Snmp Trap host used to receive messages. Trigger the trap message time: port Linkup/LinkDown, equipment of cold - start (restart when power supply drop)/warm - start (a warm restart), and Rmon set port statistical fluctuation threshold.

[Configuration example]

Such as: setting host 192.168.1.30 receive trap information.

The screenshot shows the 'SNMP Config' tab selected. Below it, the 'Trap Destination Host' section has a 'New Trap' button circled in red. A red arrow points from this button to a 'New Trap' dialog box. The dialog box contains the following fields: 'Destination IP Address' with the value '192.168.1.30', 'Security Name' with the value 'user1', 'UDP Port Number' with the value '162', and 'Security Mode' with the value 'v1'. The 'Save' button at the bottom of the dialog is also circled in red.

5.7.2. Rmon Config

5.7.2.1. Statistics Group

In the navigation bar to select **"SNMP>Rmon Config>Statistics Group"**, Set an Ethernet interface statistics .the following picture:

The screenshot shows the 'Statistics Group' tab selected. Below it, the 'Statistics Group List' table is shown with columns: Index, Interface Name, Owner, and Edit / Delete. The 'New Count Group' button is highlighted with a red circle.

[Parameter description]

Parameter	Description
-----------	-------------

Index	The index number, the value range of statistical information table is 1 ~ 65535
Interface Name	To monitor the source port
owner	Set the table creator, range: 1 ~ 30 characters of a string

[Instruction]

At the time of configuration Rmon Snmp functions must be open, otherwise the prompt dialog box will appear.

[Configuration example]

Such as: set up monitoring Ethernet port after 4 to check the data.

The first screenshot shows the 'Statistics Group' configuration page. A red circle highlights the 'new count group' button, with a red arrow pointing to the 'statistical group configuration' dialog box. In this dialog, the 'index' is set to 77, 'interface name' is 'interface Gi0/4', and 'owner' is 'Coco'. The 'save' button is highlighted with a red circle.

The second screenshot shows the 'Statistics Group' configuration page with the 'index' 77 selected. A red circle highlights the 'new count group' button, with a red arrow pointing to the 'Statistical information' dialog box. This dialog displays various statistics for the selected group, including 'Number of Packet Discarding Events', 'Number of Received Bytes', 'Number of Received Packets', 'Number of Received Broadcasting Packets', 'Number of Received Multicast Packets', 'Number of Received Packets With CRC Check Failed', 'Number of Received Packets Smaller Than 64 Bytes', and 'Number of Received Packets Larger Than 1518'. The 'quit' button is highlighted with a red circle.

5.7.2.2. History Group

In the navigation bar to select **"SNMP>Rmon Config>History Group"**, Record the history of an Ethernet interface information. the following picture.

The screenshot shows the 'History Group' configuration page. The 'History Group' tab is selected and highlighted with a red circle. Below the tabs, there is a 'history group list' table with columns: index, interface name, maximum number of samples, sample period, owner, status, and operation. The 'new history group' button is highlighted with a red circle. At the bottom right, there are pagination controls: 'first page', 'prev page [1]', 'next page', 'last page 1', and '/1page'.

[Parameter description]

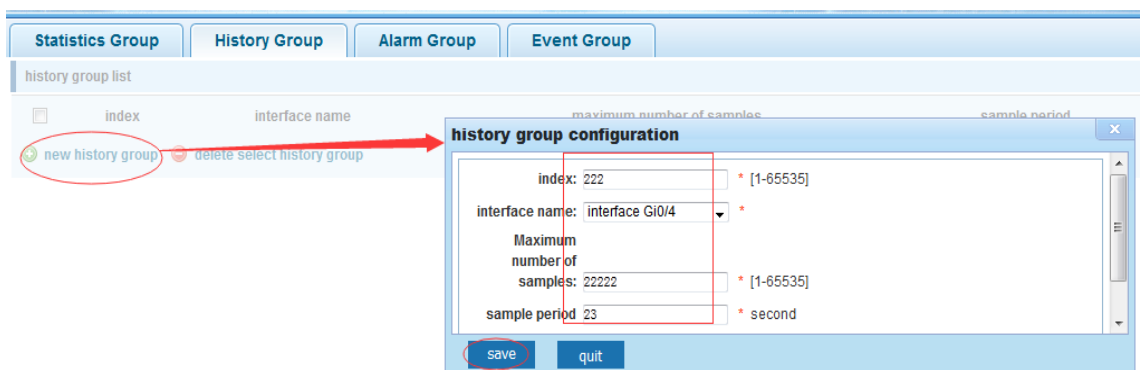
Parameter	Description
Index	Historical control table item index number, value range is 1 ~ 65535
Interface Name	To record the Ethernet interface
Maximum Number of Samples	Set the history control table item of the corresponding table capacity, namely the Max for number of records the history table, value range is 1 ~ 65535
Sample Period	Set up the statistical period, scope for 5 ~ 3600, the unit is in seconds
Owner	Set the table creator, range: 1 ~ 30 characters of a string

[Instruction]

At the time of configuration Rmon Snmp functions must be open, otherwise the prompt dialog box will appear.

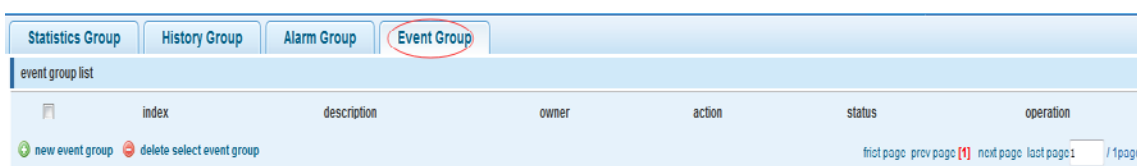
[Configuration example]

Such as: monitor Ethernet port 4 historical information.



5.7.2.3. Event Group

In the navigation bar to select “**SNMP>Rmon Config>Event Group**”, The way in which define events trigger and record them. the following picture.



[Parameter description]

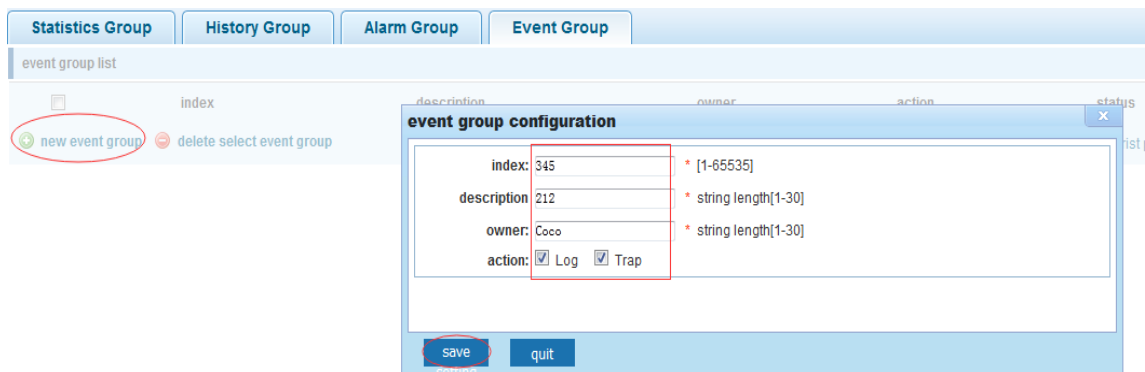
Parameter	Description
Index	The index number, the value range of the event table is 1 ~ 65535
Description	The Trap events, when the event is triggered, the system will send the Trap message, Log events, when the event is triggered, the system will log
Owner	Set the table creator, ownername for 1 ~ 30 characters of a string

[Instruction]

At the time of configuration Rmon Snmp functions must be open, otherwise the prompt dialog box will appear.

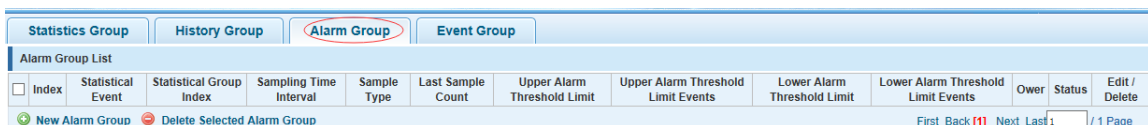
[Configuration example]

Such as: create an event to trigger 345, the system sends the trap message and log .



5.7.2.4. Alarm Group

In the navigation bar to select " **SNMP>Rmon Config>Alarm Group**", define alarm group. The following picture:



[Parameter description]

Parameter	Description
Index	The alarm list items index number, value range is 1 ~ 65535
Static Event	Statistical type values :3:DropEvents. 4:Octets. 5:Pkts. 6:BroadcastPkts. 7:MulticastPkts. 8:CRCAAlignErrors. 9:UndersizePkts. 10:OversizePkts. 11:Fragments. 12:Jabbers. 12:Collisions. 14:Pkts64Octets. 15:Pkts65to127Octets. 16:Pkts128to255Octets. 17:Pkts256to511Octets. 18:Pkts512to1023Octets. 19:Pkts1024to1518Octets

Statistical Group Index	Set up the corresponding statistics statistical index number, decided to statistics to monitor the port number
Sampling Time Interval	Sampling time interval, the scope for 5 ~ 65535, the unit for seconds
Sampling Type	Sample types for the absolute value of sampling, the sampling time arrived directly extracting the value of a variable
Last Sample Count	Sampling type for change value sampling, extraction of the arrival of the sampling time is variable in the change of the sampling interval value
Upper Alarm threshold Limit	Set the upper limit the Parameter values
Lower Alarm threshold Limit	Set the lower limit Parameter values
Upper Alarm/Lower Alarm threshold Limit Events	Upper/lower limit reached, for each event
Owner	Set the table creator, ownername for 1 ~ 30 characters of a string

[Instruction]

At the time of configuration Rmon Snmp functions must be open, otherwise the prompt dialog box will appear. This configuration needs to configure statistics groups and events.

[Configuration example]

Such as: new statistics group of 77 and the event group 345, set up more than 12 and below the lower limit 3 , Beyond the scope of alarm .

The screenshot shows the 'statistical group configuration' dialog box. The fields are as follows:

- index: 123 (range: [1-65535])
- Static table: DropEvents
- Statistical group index: 77
- Sampling time interval: 123 (unit: second)
- Sample type: Absolute
- owner: Coco (string length: [1-30])
- The alarm threshold limit: 12 (range: [0-2147483647])
- Events that exceed the threshold limit: 345
- Alarm threshold limit: 3 (range: [0-2147483647])
- Events below the threshold limit: 345

Buttons at the bottom: save, quit.

5.8. LACP

In the navigation bar to select "**LACP**", you can set to the **Lacp Config**.



5.8.1. Lacp Config

In the navigation bar to select "**LACP>Lacp Config**" the following picture:

5.8.1.1. LACP Setting

In the navigation bar to select "**LACP>Lacp Config>LACP Setting**", the following picture:

LACP Setting | LACP Display

LACP status

Open LACP: ☐

Apply

LACP public parameter settings

System priority: (1-65535)

Apply

LACP activation port parameter settings

choose port to set up:

1	3	5	7	9	11	13	15	17	19
2	4	6	8	10	12	14	16	18	20

☐ Optional
 ☐ Fixed port
 ☒ Selected
 ☐ Aggregation
 ☐ Trunk
 ☐ IP Source Enable Port

Tip: Click and drag cursor over ports to select multiple ports [Select all](#) [Select all others](#) [Cancel](#)

Port priority: (0-65535)

Aggregate port number:

Aggregate model:

Apply

LACP status

LACP status

Open LACP: ☐

Apply

Open or close LACP.

LACP public parameter settings

LACP public parameter settings

System priority: (1-65535)

Apply

You can set to System settings, range 1-65535.

LACP activation port parameter settings

LACP activation port parameter settings

choose port to set up:

1	3	5	7	9	11	13	15	17	19
2	4	6	8	10	12	14	16	18	20

☐ Optional
 ☒ Fixed port
 ☒ Selected
 ☒ 1 Aggregation
 ☐ Trunk
 ☐ IP Source Enable Port

Tip: Click and drag cursor over ports to select multiple ports [Select all](#) [Select all others](#) [Cancel](#)

Port priority: (0-65535)
 Aggregate port number:
 Aggregate model:

[Apply](#)

Port priority: You can set to Port priority. Rang 1-65535

Aggregate port number: You can select the Aggregate port number.

Aggregate model: You can select the Aggregate port number. Include active and passive.

5.8.1.2. LACP Display

In the navigation bar to select "**LACP>Lacp config>LACP Display**". You can see the table of lacp.

LACP Setting		LACP Display							
LACP list									
Aggregate ID	Port ID	Port status flag	Port state	Priority	Port operation key	Port number	Lacp Protocol state	Lacp Partner State	Operation
First Back 1 Next Last 1 / 1 Page									

5.9. SYSTEM

In the navigation bar to select "**SYSTEM**", you can set to the **System Config, System Update, Config Management, Config Save, Administor Privileges** and **Info Collect**.



5.9.1. System Config

5.9.1.1. System Settings

In the navigation bar to select "**SYSTEM>System Config>System Settings**", Basic information set switch. the following picture:

[Parameter description]

Parameter	Description
Device Name	Switch name
Management VLAN	Switches use VLAN management
Management IP	Switch IP address management
Login Timeout	Don't use more than login timeout after login to log in again

[Configuration example]

Such as: 1) set up the VLAN 2 is management VLAN, should first created vlan 2 the VLAN Settings, and set a free port in the VLAN 2.

System Settings **System Restart**

Basic System Information

Management VLAN: 1 *

Management IP: 192.168.1.110 *

Subnet Mask: 255.255.255.0 *

Default Gateway: 0.0.0.0

Jumbo Frame: 1518 (1518-9216)

DNS Server: 0.0.0.0

Login Timeout (Minutes): 30

Save Delete **Set Management VLAN**

System Settings **System Restart** **Password** **EEE Enable** **SSH Login** **Telnet Login** **System Log**

Basic System Information

Management VLAN: 2 *

Management IP: 192.168.2.12 *

Subnet Mask: 255.255.255.0 *

Default Gateway: 0.0.0.0

Jumbo Frame: 1518 (1518-9216)

DNS Server: 0.0.0.0

Login Timeout (Minutes): 30

Device MAC: 00:B0:4C:00:00:00

Ipv6 Address:

Device Name: Switch

Device Location:

Contacts(include mailbox):

Save Cancel settings

2) Insert the PC interface 9 or 10 ports, set up the management IP for 192.168.2.12, device name is yoyo, timeout for 20 minutes, Jumbo frame for 5000.

System settings **System restart** **Password change** **ssh login**

system basic information

Manage VLAN: 2 *

Manage IP: 192.168.2.12 *

Mask: 255.255.255.0 *

Default gateway: 0.0.0.0

Jumboframe: 5000 (1518-9216)

DNS server: 0.0.0.0

Login timeout(minute): 20

Device MAC: da:ad:12:34:56:78

Device name: yoyo

Device position:

Contacts:

Contact information:

Save settings Set management vlan

3) use 192.168.2.12 logging in, sets the system time .

system time

current system time: 2000year01month01dayMorning07:53:25

Reset time:

☐ Automatic

save settings

Nov 2015

Sun	Mon	Tue	Wed	Thu	Fri	Sat
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	1	2	3	4	5
6	7	8	9	10	11	12

Time 16:51:25

Clear Today OK

5.9.1.2. System Restart

In the navigation bar to select **"SYSTEM>System Config>System Restart"**, equipment can be restarted. The following picture:

System Settings **System Restart** Password EEE Enable SSH Login Telnet Login System Log

System reboot

Restart

[instruction]

Click the button to restart the switch. The restart process may take 1 minute. Please wait patiently. The page will be refreshed automatically after device restart.

[Configuration example]

Such as: click "restart" button.

System Settings System Restart Password EEE Enable SSH Login Telnet Login System Log

System reboot

Restart

5.9.1.3. EEE Enable

In the navigation bar to select **"SYSTEM>System Config>EEE Enable"**, The password change to equipment. The following picture:

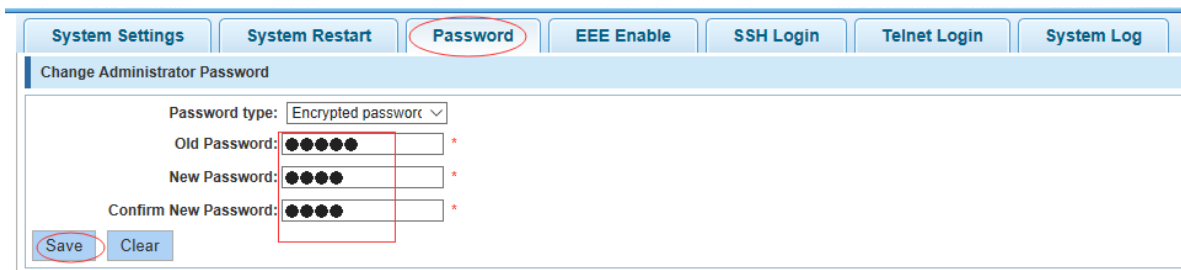


[Instruction]

Energy Efficient Ethernet, Open the EEE features by default.

5.9.1.4. Password

In the navigation bar to select "**SYSTEM>System Config>Password**", The password change to equipment. The following picture:



[Instruction]

1. If you set a new Web login password, then log in again after setting the new password.
2. Password cannot contain Chinese, full-width characters, question marks and spaces.
3. If forget the password reset, can be reset in the console.

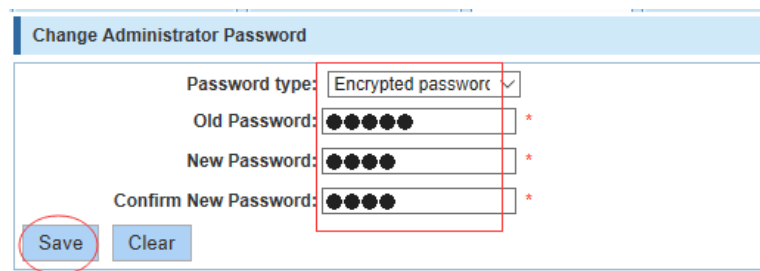
Switch (config)# password admin

New Password: 3456

Confirm Password: 3456

[Configuration example]

Such as: amend the password to 1234.



5.9.1.5. SSH Login

In the navigation bar to select "**SYSTEM>System Config>SSH Login**", SSH open. The following picture:

[Instruction]

Configure the user to be able to switch through the SSH login device.

[Configuration example]

Such as: SSH open, you can CRT to log in.

5.9.1.6. Telnet Login

In the navigation bar to select "**SYSTEM>System Config>Telnet Login**", Telnet open. The following picture:

[Instruction]

Configure the user to be able to switch through the Telnet login device.

[Configuration example]

Such as: Telnet open, PC Telnet function open, you can log in.

5.9.1.7. System Log

In the navigation bar to select "**SYSTEM>System Config>System Log**", to view the log and set up the log server. The following picture:

[Parameter description]

Parameter	Description
Log switch	Open and close
Server IP	Appoint to server address
Send Log Level	0-7
Keyword	Enter the required query of characters

[Instruction]

Open log switch, set up the syslog server, system log will automatically be pushed to the server.

[Configuration example]

Such as: 1) the error log information in 192.168.1.110 pushed to the server

2) Input the Mac keywords, click "query" button, click on the "clear log" button, can clear the log .

current log information

Syslog logging: enabled

Console logging: disabled

Monitor logging: level debugging, 0 messages logged

Buffer logging: level debugging, 444 messages logged

Timestamp debug messages: datetime

Timestamp log messages: datetime

Sequence-number log messages: disable

Sysname log messages: disable

Trap logging: level informational, 444 message lines logged, 0 fail

Log Buffer (Total 4096 Bytes):

Jan 01 00:00:22 %CLI-Errors-CLIERRINFO: CLI load config excute cmd error: vlan-filter enable

Jan 01 00:00:22 %CLI-Errors-CLIERRINFO: CLI load config excute cmd error: mac-vlan enable

Jan 01 00:00:22 %CLI-Errors-CLIERRINFO: CLI load config excute cmd error: subnet-vlan enable

Jan 01 00:00:22 %PORTMANAGE-Informational-PORT: set port 26 flow control off.

Jan 01 00:00:22 %CLI-Errors-CLIERRINFO: CLI load config excute cmd error: rate-limit input 262143

Jan 01 00:00:22 %CLI-Errors-CLIERRINFO: CLI load config excute cmd error: rate-limit output 262143

Jan 01 00:00:22 %CLI-Errors-CLIERRINFO: CLI load config excute cmd error: cvlan-trusted enable

Jan 01 00:00:22 %CLI-Errors-CLIERRINFO: CLI load config excute cmd error: vlan-translation ingress disable

Jan 01 00:00:22 %CLI-Errors-CLIERRINFO: CLI load config excute cmd error: vlan-translation egress disable

Jan 01 00:00:22 %CLI-Errors-CLIERRINFO: CLI load config excute cmd error: vlan-filter enable

Jan 01 00:00:22 %CLI-Errors-CLIERRINFO: CLI load config excute cmd error: mac-vlan enable

5.9.2. System Upgrade

In the navigation bar to select **"SYSTEM>System Upgrade"**, Optional upgrade file to upgrade. The following picture:

System Upgrade

Current Software Version: V103SP7D180809

File Name:

[Instruction]

- 1 please confirm that the upgraded version of the same model and the same model.
- 2 in the upgrade process, you may encounter flash to make the page is temporarily unable to respond to the page, this time cannot power off or restart the device, until prompted to upgrade successfully!

5.9.3. Config Management

5.9.3.1. Import/Export Config

In the navigation bar to select **"SYSTEM>Config Management>Import/Export Config"**, can import and export configuration files, the backup file. the following picture:

Import/Export Config	Restore Config	Factory Reset
Show Current Config Export Config		
☒ Backup ☐ Import Configuration		
File Name: .conf		
Confirm Backup		
Backup File List		
Name		Size
1234.conf		3.49K

[Instruction]

Import process cannot be closed or refresh the page, or import will fail!

After the introduction of configuration, to enable the new configuration, please in this page Restart device
Otherwise configuration does not take effect.

[Configuration example]

Such as: 1) in the configuration first save the page, click save configuration to save the current configuration, and then export the configuration.

Import/Export Config	Restore Config	Factory Reset
Show Current Config Export Config		
☒ Backup ☐ Import Configuration		
File Name: 111 .conf		
Confirm Backup		
Backup File List		
Name		Size
123.conf		2.86K
		00:07:46 2000-01-01

2) Import configuration.

Import/Export Config	Restore Config	Factory Reset
Show Current Config Export Config		
☐ Backup ☒ Import Configuration		
Do not refresh or close the page during the import Prompt: After the introduction of configuration, to enable the new		
File Name: Browse... Import config		
Backup File List		
Name		
123.conf		

Save As

Desktop

Organize New folder

Desktop Downloads Recent places

Homegroup This PC Network

Test Libraries New Rich Text Document
Rich Text Document
7 bytes

File name:

Save as type: All Files

Import/Export Config Restore Config Factory Reset

Show Current Config Export Config

☐ Backup ☒ Import Configuration

Do not refresh or close the page during the import
 Prompt: After the introduction of configuration, to enable the new configuration, please in this page, [Restart device](#). Otherwise configuration does not take effect

File Name: 浏览... Import configuration

Backup File List

Name	Size	Time Stamp
2345.conf	2.19K	03:05:51 2000-01-01

3) backup.

Import/Export Config Restore Config Factory Reset

Show Current Config Export Config

☒ Backup ☐ Import Configuration

File Name: .conf

Confirm Backup

5.9.3.2. Restore Config

In the navigation bar to select **"SYSTEM>Config Management>Restore Config"**, you can configure backup file. The following picture:

Import/Export Config **Restore Config** Factory Reset

Name	Size	Time Stamp
☒ 2345.conf	2.19K	03:05:51 2000-01-01
☐ 123456.conf	1.99K	02:35:53 2000-01-01

☒ Restore Backup ☐ Delete Backup ☐ Save Backup ☐ Rename Backup

Confirm Recovery

[Instruction]

Operating this page should be in the current configuration page first, the backup file.

[Configuration example]

Such as: restore backup.

Import/Export Config **Restore Config** Factory Reset

Name	Size	Time Stamp
☒ 2345.conf	2.19K	03:05:51 2000-01-01
☐ 123456.conf	1.99K	02:35:53 2000-01-01

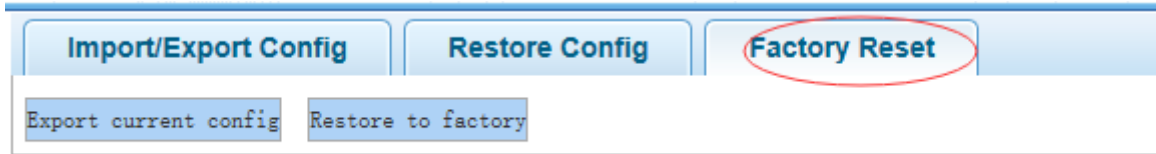
☐ Restore Backup ☐ Delete Backup ☐ Save Backup ☒ Rename Backup

Rename: .conf

Confirm Rename

5.9.3.3. Factory Reset

In the navigation bar to select "**SYSTEM>Config Management> Factory Reset**", Can export the current configuration and restore factory configuration. The following picture:

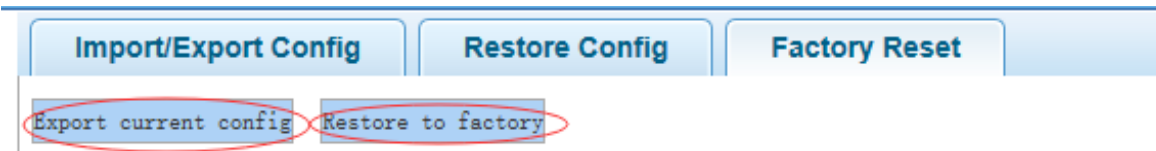


[Instruction]

Restore the factory configuration, will delete all the current configuration. If you have any useful configuration, the current system can lead the factory configuration again after the current configuration.

[Configuration example]

Such as: restore configuration can be the guide before they leave the current configuration.



5.9.4. Config Save

In the navigation bar to select "**SYSTEM>Config Save**", you can save current configuration. The following picture:



[Instruction]

Save settings will delete all default configurations. If there are useful configurations, click backup Configurations before save the settings.

[Configuration example]

Such as: click "save settings" button.



5.9.5. Administrator Privileges

In the navigation bar to select "**SYSTEM>Administrator Privileges**", Configurable ordinary users. The following picture:

Administrator Settings

Password type: Encrypted password ▾

User Name: *

New Password: *

Confirm Password: *

User List

User Name	Edit / Delete
user	
admin	

First [Back](#) [1](#) Next Last [1](#) / 1 Page

[Instruction]

Only the admin of the super administrator can access this page is used to manage users and visitors. The user can log in the Web management system of equipment for routine maintenance. In addition to the admin and user, add up to five users. Ordinary users can only access information system home page.

[Configuration example]

Such as:

Administrator Settings

Password type: Encrypted password ▾

User Name: *

New Password: *

Confirm Password: *

5.9.6. Info collect

In the navigation bar to select **"SYSTEM>Info collect"**, you can collect to the system debug information. The following picture:

[Instruction]

Collect useful infomation, it may take a few moment.

[Configuration example]

Such as: click on "collect" button.

ENABLING A SAFER SOCIETY AND SMARTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.

Address: No. 1399, Binxing Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Postcode: 310053

Email: dhoverseas@dhvisiontech.com | Tel: +86-571-87688888 28933188