

8-Port Gigabit + 2-Port Gigabit SFP L2 Managed PoE Switch User's Manual

V1.0.0

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.

Поставщик систем безопасности TELECAMERA.RU

Cybersecurity Recommendations

Mandatory actions to be taken towards cybersecurity

1. Change Passwords and Use Strong Passwords:

The number one reason systems get "hacked" is due to having weak or default passwords. It is recommended to change default passwords immediately and choose a strong password whenever possible. A strong password should be made up of at least 8 characters and a combination of special characters, numbers, and upper and lower case letters.

2. Update Firmware

As is standard procedure in the tech-industry, we recommend keeping NVR, DVR, and IP camera firmware up-to-date to ensure the system is current with the latest security patches and fixes.

"Nice to have" recommendations to improve your network security

1. Change Passwords Regularly

Regularly change the credentials to your devices to help ensure that only authorized users are able to access the system.

2. Change Default HTTP and TCP Ports:

• Change default HTTP and TCP ports for systems. These are the two ports used to communicate and to view video feeds remotely.

• These ports can be changed to any set of numbers between 1025-65535. Avoiding the default ports reduces the risk of outsiders being able to guess which ports you are using.

3. Enable HTTPS/SSL:

Set up an SSL Certificate to enable HTTPS. This will encrypt all communication between your devices and recorder.

4. Enable IP Filter:

Enabling your IP filter will prevent everyone, except those with specified IP addresses, from accessing the system.

5. Change ONVIF Password:

On older IP Camera firmware, the ONVIF password does not change when you change the system's credentials. You will need to either update the camera's firmware to the latest revision or manually change the ONVIF password.

6. Forward Only Ports You Need:

• Only forward the HTTP and TCP ports that you need to use. Do not forward a huge range of numbers to the device. Do not DMZ the device's IP address.

• You do not need to forward any ports for individual cameras if they are all connected to a recorder on site; just the NVR is needed.

7. Disable Auto-Login on SmartPSS:

Those using SmartPSS to view their system and on a computer that is used by multiple people should disable auto-login. This adds a layer of security to prevent users without the appropriate credentials from accessing the system.

8. Use a Different Username and Password for SmartPSS:

In the event that your social media, bank, email, etc. account is compromised, you would not want someone collecting those passwords and trying them out on your video surveillance system. Using a different username and password for your security system will make it more difficult for someone to guess their way into your system.

9. Limit Features of Guest Accounts:

If your system is set up for multiple users, ensure that each user only has rights to features and functions they need to use to perform their job.

10. UPnP:

• UPnP will automatically try to forward ports in your router or modem. Normally this would be a good thing. However, if your system automatically forwards the ports and you leave the credentials defaulted, you may end up with unwanted visitors.

• If you manually forwarded the HTTP and TCP ports in your router/modem, this feature should be turned off regardless. Disabling UPnP is recommended when the function is not used in real applications.

11. SNMP:

Disable SNMP if you are not using it. If you are using SNMP, you should do so only temporarily, for tracing and testing purposes only.

12. Multicast:

Multicast is used to share video streams between two recorders. Currently there are no known issues involving Multicast, but if you are not using this feature, deactivation can enhance your network security.

13. Check the Log:

If you suspect that someone has gained unauthorized access to your system, you can check the system log. The system log will show you which IP addresses were used to login to your system and what was accessed.

14. Physically Lock Down the Device:

Ideally, you want to prevent any unauthorized physical access to your system. The best way to achieve this is to install the recorder in a lockbox, locking server rack, or in a room that is behind a lock and key.

Foreword

General

This user's manual introduces the functions and operations of 8-Port Gigabit + 2-Port Gigabit SFP L2 Managed PoE Switch devices.

Models

DH-PFS4210-8GT-150

Safety Instructions

The following categorized signal words with defined meaning might appear in the Manual.

Signal Words	Meaning
	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
	Indicates a potential risk which, if not avoided, could result in property damage, data loss, lower performance, or unpredictable result.
©TIPS	Provides methods to help you solve a problem or save you time.
	Provides additional information as the emphasis and supplement to the text.

Revision History

No.	Version	Revision Content	Release Time
1	V1.0.0	First Release.	June 1, 2018

Privacy Protection Notice

As the device user or data controller, you might collect personal data of others' such as face, fingerprints, car plate number, Email address, phone number, GPS and so on. You need to be in compliance with the local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures include but not limited to: providing clear and visible identification to inform data subject the existence of surveillance area and providing related contact.

About the Manual

- The Manual is for reference only. If there is inconsistency between the Manual and the actual product, the actual product shall govern.
- We are not liable for any loss caused by the operations that do not comply with the Manual.
- The Manual would be updated according to the latest laws and regulations of related regions. For detailed information, see the paper User's Manual, CD-ROM, QR code or our official website. If there is inconsistency between paper User's Manual and the electronic version, the electronic version shall prevail.
- All the designs and software are subject to change without prior written notice. The product updates might cause some differences between the actual product and the Manual. Please contact the customer service for the latest program and supplementary documentation.
- There still might be deviation in technical data, functions and operations description, or errors in print. If there is any doubt or dispute, please refer to our final explanation.
- Upgrade the reader software or try other mainstream reader software if the Guide (in PDF format) cannot be opened.
- All trademarks, registered trademarks and the company names in the Manual are the properties of their respective owners.
- Please visit our website, contact the supplier or customer service if there is any problem occurred when using the device.
- If there is any uncertainty or controversy, please refer to our final explanation.

Important Safeguards and Warnings

Electrical safety

- All installation and operation here should conform to your local electrical safety codes.
- The product must be grounded to reduce the risk of electric shock.
- We assume no liability or responsibility for all the fires or electrical shock caused by improper handling or installation.

Transportation security

Heavy stress, violent vibration or water splash are not allowed during transportation, storage and installation.

Installation

- Keep upwards. Handle with care.
- Do not apply power to the Device before completing installation.
- Do not place objects on the Device.

Qualified engineers needed

All the examination and repair work should be done by the qualified service engineers. We are not liable for any problems caused by unauthorized modifications or attempted repair.

Environment

The Device should be installed in a cool, dry place away from conditions such as direct sunlight, inflammable substances, and explosive substances.

Accessories

- Be sure to use all the accessories recommended by manufacturer.
- Before installation, please open the package and check all the components are included.
- Contact your local retailer ASAP if something is broken in your package.

Battery

- Improper battery use might result in fire, explosion, or personal injury.
- When replacing the battery, please make sure you are using the same type. Risk of explosion if battery is replaced by an incorrect type.
- Dispose of used batteries according to the instructions.
- Please make sure to use the same battery model if possible.
- We recommend replace battery regularly (such as one-year) to guarantee system time accuracy. Before replacement, please save the system setup, otherwise, you may lose the data completely.

Table of Contents

Cybersecurity Recommendations	I
Foreword	III
Important Safeguards and Warnings	V
1 Introduction	1
1.1 Overview	1
1.2 Features	1
1.3 External Component Description	2
1.3.1 Front Panel	2
1.3.2 Rear Panel	3
1.4 Package Contents	4
2 Installation and Connection	5
2.1 Installation	5
2.1.1 Desktop Installation	5
2.1.2 Rack-mountable Installation in 19-inch Cabinet	5
2.1.3 Power on the Switch	6
2.2 Connect Computer (NIC) to the Switch	6
2.3 Switch connection to the PD	7
3 Login to the Switch	8
3.1 Switch to End Node	8
3.2 Login the Switch	8
4 Switch Configuration	10
4.1 Quickly Setting	10
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 rate-limit	17
4.2.5 Storm control	18
4.2.6 Port isolation	20
4.2.7 Port information	21
4.3 VLAN	22
4.3.1 VLAN Settings	22
4.3.2 Access Port Settings	23
4.3.3 Trunk-port setting	24
4.3.4 Hybrid-port setting	25
4.4 Fault/Safety	28
4.4.1 Anti attack	28
4.4.2 Channel detection	33
4.4.3 ACL	36
4.5 PoE	
4.5.1 PoE Port Config	38

4.6 STP	39
4.6.1 MSTP region	40
4.6.2 STP bridge	41
4.7 DHCP relay	43
4.7.1 DHCP relay	44
4.7.2 0ption82	44
4.8 QoS	46
4.8.1 Queue config	46
4.8.2 Mapping the queue	
4.9 Addr table	51
4.9.1 MAC Management	52
4.9.2 MAC Learning and Aging	53
4.9.3 MAC Filter	55
4.10 SNMP	55
4.10.2 Snmp config	56
4.10.3 Rmon config	62
4.11 LACP	67
4.11.2 Lacp config	67
4.12 SYSTEM	70
4.12.2 System config	70
4.12.3 System upgrade	
4.12.4 Config management	77
4.12.5 Config save	80
4.12.6 Administrator privileges	80
4.12.7 Info collect	
Appendix 1 Technical Specifications	

Поставщик систем безопасности TELECAMERA.RU

Introduction

1.1 Overview

The Switch is a new generation designed for high security and high performance network the second layer switch. Provides eight 10/100/1000Mbps self-adaption RJ45 port, and two 100/1000Mbps SFP ports, all ports support wire-speed forwarding, can provide you with larger network flexibility. All ports support Auto MDI/MDIX function. The Switch with a low-cost, easy-to-use, high performance upgrade your old network to a 1000Mbps Gigabit network.

The Switch supports 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, easy to maintenance and management, meet the networking and access requirements of small and medium-sized enterprises, intelligent village, hotel, office network and campus network.

The Switch all UTP ports support PoE power supply function, support IEEE802.3at standard, 802.3af downward compatibility, power supply equipment for Ethernet, can automatically detect identification standard of electrical equipment, and through the cable for the power supply.

1.2 Features

- Comply with 802.3i, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3x, IEEE 802.3z, IEEE802.1Q, IEEE802.1p, IEEE802.3af, IEEE802.3at
- Supports PoE power up to 30W for each PoE port, total power up to 140W for all PoE ports
- 8 x 10/100/1000Mbps Auto MDI/MDI-X Ethernet port
- 2 x 100/1000Mbps SFP port
- 8K entry MAC address table of the switch with auto-learning and auto-aging
- Supports IEEE802.3x flow control for Full-duplex Mode and backpressure for Half-duplex Mode
- Support Web interface management
- supports QoS (quality of service), port mirror, Link aggregation protocol
- LED indicators for monitoring Power, System, link/activity/Speed, PoE

1.3 External Component Description

1.3.1 Front Panel

The front panel of the Switch consists of AC power connector, one marker, 1 x Reset button, a series of LED indicators, 8 x 10/100/1000Mbps RJ-45 ports, 2 x SFP ports and 1x Console port as shown as below.

Figure 1-1 Front panel



AC Power Connector:

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

Grounding Terminal:

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

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 (1~8):

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

SFP ports (9, 10):

Designed to install the SFP module and connect to the device with a bandwidth of 100Mbps or 1000Mbps. Each has a corresponding Link/Act/Speed LED.

Console port (Console):

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

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	PWR	Off	Power Off
Indicator		Solid green	Power On

Table 1-	1 Front	panel
----------	---------	-------

LED Indicator	Faceplate Marker	Status	Indication
System		Off	System not started
indicator	SYS	Blinking green	System is starting or the system starts successfully
10/100/10		Off	The port is NOT connected.
00 BASE-T		Solid green	The port is connected at 1000Mbps.
adaptive Ethernet	Link/Act	Solid orange	The port is connected at 100/10Mbps
port indicators (1-8)	/Speed	Blinking	The port is transmitting or receiving data.
		Off	The port is NOT connected.
SFP port	Link/Act /Speed	Solid green	The port is connected at 1000Mbps.
indicators (9-10)		Solid orange	The port is connected at 100Mbps
(0.10)		Blinking	The port is transmitting or receiving data.
PoE		Off	No PD is connected to the corresponding port, or no power is supplied according to the power limits of the port
status indicators (1-8)	PoE	Solid orange	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 Heat vent shown as below. Figure 1-2 Real panel



Heat vent:

The Heat vent is located in the middle position of the rear panel of the switch. It is used for heat dissipation and ventilation. Do not cover it.

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's Manual

Installation and Connection

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:

<u>Step 1</u> Attach the mounting brackets on the Switch's side panels (one on each side) and secure them with the screws provided.

Figure 2-1 Bracket installation



<u>Step 2</u> Use the screws provided with the equipment rack to mount the Switch on the rack and tighten it.

Figure 2-2 Rack installation



2.1.3 Power on the Switch

The Switch is powered on by the AC 100-240V 50/60Hz 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

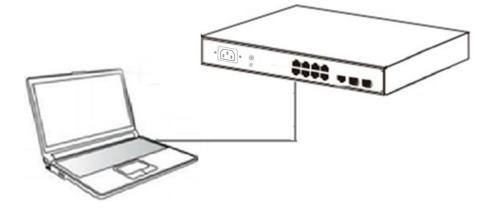
1-8 ports of the Switch have PoE power supply function, the maximum output power up to 30W each port, it can make PD devices, such as internet phone, network camera, wireless access point work. You only need to connect the Switch PoE port directly connected to the PD port by network cable.

Login to 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 3-1 Connect PC to switch



3.2 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. Table 3-1 Default value

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:

- Step 1 Connect the Switch with the computer NIC interface.
- <u>Step 2</u> Power on the Switch.
- <u>Step 3</u> 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.
- <u>Step 4</u> Open the browser, and enter http://192.168.1.110 and then press "Enter". The Switch login window appears, as shown below.

Figure 3-2 Login windows

Welcome To Web Smart Management System
k USER LOGIN
Please input user name and password ! User Name: admin
Password:
Language: English V
LOGIN

<u>Step 5</u> 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.

Figure 3-3 Switch configuration window

	Cu	irrent username: admin					E E	
😸 Home	Device Type: 8-Port	PoE Switch	Hardware Version: 1.00		2 hours 29 minutes 41			
SQuickly Set	Software Version: V103S			Upti	me: seconds			
PORT								
VLAN								
Fault/Safety								
PoE		í			_			
STP				1 3 5 7				
DHCP RELAY			Console	98	105			
QOS			-	2468				
Addr Table								
SNMP								
LACP								
SYSTEM					100M	💼 1000H 💼 PoE	Unconnect 👔	Closed
	Port Information	Device Configuration P	Port Statistics					
		Device Configuration F umber or port descriptio Search						
				Output Flow(Bps)	Port Status	Port Connection	VLAN	Trunk Port
	Keyword Input port m	umber or port descriptio Searc	h 🗹 Refresh	Output Flow(Bps)	Port Status ON	Port Connection	VLAN 1	Trunk Port No
	Keyword Input port n	umber or port descriptio Searc	h Refresh					
	Keyword Input port m Port = Gi 0/1	umber or port descriptio Searc	h Refresh Input Flow(Bps)	0.00K	ON	Source Disconnected	1	
	Keyword Input port m Port A Gi 0/1 Gi 0/2	umber or port descriptio Searc	h	0.00K	ON ON	State Disconnected State Disconnected	1	No
	Keyword Input port m Port A Gi 0/1 Gi 0/2 Gi 0/3	umber or port descriptio Searc	h Imput Flow(Bps) 0.00K 0.00K 0.00K 0.00K 0.00K 0.00K	0.00K 0.00K 0.14K	ON ON ON	State State State State State State State State State State	1 1 1	No No No
	Keyword Input port m Port m Gi 0/1 Gi 0/2 Gi 0/2 Gi 0/3 Gi 0/3 Gi 0/4 Gi 0/4	umber or port descriptio Searc	Imput Flow(Bps) 0.00K 0.00K 0.00K 0.00K 0.00K	0.00K 0.00K 0.14K 0.00K	ON ON ON ON	State State State State State State State State State State State State	1 1 1 1	No No No No
	Keyword Input port m Port ▲ Gi 0/1 Gi 0/2 Gi 0/3 Gi 0/4 Gi 0/5	umber or port descriptio Searc	Input Flow(Bps) 0.00K 0.00K 0.00K 0.00K 0.00K 0.00K 0.00K	0.00K 0.00K 0.14K 0.00K 0.00K	ON ON ON ON	State Disconnected Disconnected Connected Disconnected Disconnected Disconnected Disconnected	1 1 1 1 1	No No No No No

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. Figure 4-1 Switch configuration window

	c	urrent username: admin					B D	cit Langua
🖪 Home	Device Type: 8-Por	rt PoE Switch	Hardware Version: 1.00		2 hours 29 minutes 41	1		
uickly Set	Software Version: V103	SP2D180118		Upt	seconds			
PORT								
VLAN								
Fault/Safety								
PoE								
STP DHCP RELAY			Console	1 3 5 7 9S	105			
QOS					105			
Addr Table				2 4 6 8				
SNMP								
LACP								
SYSTEM					💼 100M	💼 1000M 🛛 💼 PoE	💼 Unconnect 🛛 👩	Closed
	Port Information Keyword Input port	Device Configuration Pennumber or port descriptio Search	Refresh					
	Porta	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	S Disconnected	1	No
	Gi 0/3		0.00K	0.14K	ON	💛 Connected	1	No
	Gi 0/4		0.00K	0.00K	ON	Bisconnected	1	No
	Gi 0/5		0.00K	0.00K	ON	😽 Disconnected	1	No
			0.00K			Disconnected	1	No
	Gi 0/6		0.00K	0.00K	ON	Disconnected	1.1.1	INO
	Gi 0/6 Gi 0/7		0.00K	0.00K	ON	 Disconnected Disconnected 	1	No

4.1 Quickly Setting

In the navigation bar to select "**quickly setting**", 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:

Figure 4-2 Quickly setting

VLAN setting Other settings									
VLAN Settings									
VLAN ID VLAN Name VLAN IP Port Edit / Delete									
	1 VLAN0001 192.168.1.110/24 1-10								
🔘 New V	/LAN 😳 New Multiple VLAN 🤤 De	elete VLAN				First Back [*] Next Last 1 / 1	Page	
Trunk Se	ttings								
Port Name Description Allowed Vian Edit / Delete									
🗿 New T	runk Port 🤤 Delete Trunk Port					First Back [] Next Last 1 / 1	Page	

[Parameter Description]

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

[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]

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

Figure 4-3 VLAN setting I

VLAN setting Other	settings
VLAN Settings	
VLAN ID	VI AN Name VI AN IS
1	New VLAN
	VLAN ID(1~4094): 2 *
New VLAN O New Multiple W	VLAN Name(1-31): VLAN0002
Trunk Settings	Select the ports to modify the
Port	VLAN:
New Trunk Port O Delete Tr	
	C Optional T Fixed port Selected C Aggregation C Trunk
	Tip: Click and drag cursor over ports to select multiple ports Select all Select all others Cancel
	<
	Save Exit
	→ Next

Figure 4-4 VLAN setting II

VLAN setting Other s	settings
VLAN Settings	
VLAN ID	VLAN Name VLAN ID New Trunk Port
1	Please select port to configure:
2 New VLAN O New Multiple V Trunk Settings	$ \begin{array}{cccccccccccccccccccccccccccccccccccc$
Port	Optional Fixed port Selected Aggregation Control Select all scheme of the select multiple parts Select all scheme of the select multiple parts Select all scheme of the select multiple parts
New Trunk Port Delete Tr	Tip: Click and drag cursor over ports to select multiple ports Select all Select all others Cancel Native VLAN(1-4094):
	Allowing VLAN(such as 3-5,8,10): 1
	Save Exit
	Next

Step 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.

Figure 4-5 Save

VLAN setting Other settings	
Basic System Information	
-	
Management VLAN: 1	Device Name: Spitch-123 *
Management IP: 192. 168. 1. 11 *	Default Gateway: 172. 16. 1. 241
Subnet Mask: 255. 255. 0 *	DNS Server: 172.16.1.241
Save Delete Set Management VLAN	

Step 3 Use 192.168.1.11 to log in, set a new password for admin1234.

⊢ıgure	4-6	Finish	

	Change Administrator Password						
	Password type:	Encrypted passwo 🗸	,				
	Old Password:	•••••					
	New Password:	••••					
	Comfirm New Password:	••••					
				E	Back		Finish
_)	

4.2 Port

In the navigation bar to select "**PORT**", you may conduct **Basic config**, **Port aggregation**, **Port mirroring**, **Port limit** and **port isolation**.

Figure 4-7 Port



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:

Figure 4-8 Basic settings I

Basic settin	Basic settings							
① Optional 💼 Fixed port 💼 Selected 11 Aggregation 그 Trunk 과 IP Source Enable Port								
Tip: Click and drag cursor over ports to select multiple ports Select all others Cancel								
Port Description(0-80 characters): Status: Enabled								
Port Speed: Auto v Duplex Mode: Auto v								
Flow Control: Off Cable Type Detection: Auto Save								
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	
					1518		Off	
Gi0/3		Enabled	1000M	Duplex		Auto		
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	2
Gi0/8		Enabled	Auto	Auto	1518	Auto	Off	2
Gi0/9		Enabled	1000M	Duplex	1518	Auto	Off	
Gi0/10		Enabled	100014	Duploy	1510	Auto	0#	

[Parameter Description]

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

Figure 4-9 Basic settings I	Figure	4-9	Basic	settings	II
-----------------------------	--------	-----	-------	----------	----

Basic settings				
C 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				
Port Description(0-80 characters): Status:	Enabled	\sim		
Port Speed: 10M V Duplex Mode:	Half Duplex	\sim		
Flow Control: On Cable Type Detection:	Auto	\sim		
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: Figure 4-10 Port aggregation

Load Balancing		
Load Balancing method: Source MAC V		
Port Aggregation		
Aggregate Group Number(1-8): *		
Please select the port to join the Aggregate Group:		
C Optional T Fixed port Selected Aggregation C Trunk E 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
Aggregation 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.

Figure 4-11 Configuration example

Load Balancing
Load Balancing method: Source MAC V Save
Port Aggregation
Aggregate Group Number(1-8): 1 * Please select the port to join the Aggregate Group:
$ \begin{array}{cccccccccccccccccccccccccccccccccccc$
C Optional 🚍 Fixed port 🚍 Selected 1 Aggregation 1 Trunk 1 Pource Enable Port
Tip: Click and drag cursor over ports to select multiple ports Select all Select all others Cancel

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:

		-		
Figure	4-12	Port	mirro	nina
iguic	- 1 L	I OIL	THUR	лшg

Port Mirroring			
Mirror Group Number (1-4): * Please choose the source port:(Selecting multiple source ports can affect the device performance)			
C Optional 💼 Fixed port 💼 Selected ① Aggregation C Trunk [관] IP Source Enable Port			
Tip: Click and drag cursor over ports to select multiple ports Select all others Cancel Please choose the destination port:(Can only choose one port)			
2 4 6 8 10 10 1 10 10 10 13 5 7 9 1 3 5 7 9 1 3 5 7 9 COptional Served port Selected 512 Aggregation 5_2 Trunk 5 [2] 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

Parameter	Description
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. Figure 4-13 Configuration example

Port Mirroring
Mirror Group Number (1-4): 1 * Please choose the source port:(Selecting multiple source ports can affect the device performance)
Prease choose the source point Generality multiple source points can anext the device performance)
COptional 🕎 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)
COptional 🚍 Fixed port 🚍 Selected 1 Aggregation S Trunk E IP Source Enable Port
Save

4.2.4 Port rate-limit

In the navigation bar to select "**PORT**>**port rate-limit** ", to port output, input speed limit. The following picture:

Figure 4-14 Port rate-limit

Port Speed Limit				
Optional E Fixed port Selected	1 Aggregation . Trunk E IP Source Enable Port			
	elect 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 Spees 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	2	
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	2	

[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 is125KB/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.

Figure 4-15 Configuration example

_		
	Port Speed Limit	
	ر	
	Tip: Click and drag cursor over ports to select multiple ports Select all Select all others Cancel	
	Input Speed Limit(multiple of 16): 6400 * 0,16-1,000,000Kb/s	
	Output Speed Limit(multiple of 16): 3200 * 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:

Figure 4-16 Storm control

Broadcast Control				
Counting mode pps V				
Save				
2 4 6 8 10 1 1 1 1 1 1 1 1 1 3 5 7 9 9 1				
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 Linnt	broadcast packets
Multicast Limit	Storm suppression value of the
	multicast packets
Unicast Limit	Storm suppression value of the
Unicast Eimit	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.

Figure 4-17 Configuration example

Broadcast Control
Counting mode pps V
Save
2 4 6 8 10 1 3 5 7 9
COptional 🚍 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
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: Figure 4-18 Port isolation

Port Isolation						
Please select two or more ports to configure:						
2 4 6 8 10 1 1 1 1 1 1 1 1 3 5 7 9						
C Optional E Fixed port Selected Aggregation C True	Ink <u>∑E</u>]IP Source Enable Port					
Tip: Click and drag cursor over ports to select multiple ports Select	t all Select all others Cancel					
Save						
Port Isolation List						
Source Port	Isolate Port	Delete				

[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.

Figure 4-19 Configuration example I

Port Isolation
Please select two or more ports to configure:
$ \begin{array}{cccccccccccccccccccccccccccccccccccc$
COptional 🕎 Fixed port 💼 Selected 11 Aggregation 1. Trunk 12 IP Source Enable Port
Tip: Click and drag cursor over ports to select multiple ports Select all Select all others Cancel
Save

Figure 4-20 Configuration example II

Port isolation list				
Source port	Isolated port	Opretion		
3	456	×		
4	356	×		
5	346	×		
6	345	×		
	frist page prev page [1]	next page last page 1		

4.2.7 Port information

In the navigation bar to select "**PORT>Port Information**", the following picture: Figure 4-21 Port information

Home	Port information							
Quickly Set	Keyword Input port num	mber or port descriptio Search	Refresh					
ORT Basic Config	Port▲	Description	Input Flow(Bps)	Output Flow(Bps)	Port Status	Port Connection	VLAN	Trunk Port
Port Aggregation	Gi 0/1		0.00K	0.00K	ON	😽 Disconnected	1	No
Port Mirroring	Gi 0/2		0.00K	0.00K	ON	😽 Disconnected	1	No
Port Limit	Gi 0/3		0.00K	0.06K	ON	💛 Connected	1	No
Storm Control Port Isolation	Gi 0/4		0.00K	0.00K	ON	😽 Disconnected	1	No
Port Isolation	Gi 0/5		0.00К	0.00K	ON	😽 Disconnected	1	No
LAN	Gi 0/6		0.00K	0.00K	ON	😽 Disconnected	1	No
ault/Safety	Gi 0/7		0.00K	0.00K	ON	😽 Disconnected	1	No
oE TP	Gi 0/8		0.00K	0.00K	ON	😽 Disconnected	1	No
HCP RELAY	Gi 0/9		0.00K	0.00K	ON	😽 Disconnected	1	No
os	Gi 0/10		0.00K	0.00K	ON	😽 Disconnected	1	No
ddr Table NMP						F	irst Back [1] Next L	.ast 1 / 1 Pa
ACP								

[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.

Figure 4-22 Configuration example

Port information	1						
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
						First Back [1] Next La	ast 1 / 1 Page

4.3 VLAN

In the navigation bar to select "VLAN", you can manage the VLAN config, Trunk Settings and Hybrid Settings, the following picture:

Figure 4-23 VLAN settings

VLAN	VLAN Settings Access Port Settings Trunk Port Settings Hybrid Port Settings						
VLAN ID	VLAN IDS						
	VLAN ID	VLAN Name	VLAN IP	Port	Edit / Delete		
	1	VLAN0001	192.168.1.110/24	1-10			
O New 1	S New VLAN S New Multiple VLAN S Delete VLAN						

4.3.1 VLAN Settings

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

Figure 4-24 VLAN settings

VLAN Settings Access Port Settings Trunk Port Settings VLAN IDS VLAN IDS Hybrid Port Settings						
	VLAN ID	VLAN Name	VLAN IP	Port	Edit / Delete	
1 VLAN0001 192.168.1.110/24 1-10						
O New	🕲 New VLAN 🕲 New Multiple VLAN 🤤 Delete VLAN					

[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.

Figure 4-25 Configuration example

VLAN Settings Acces	ss Port Settings Trunk Port Settings Hybrid Port Settings
VLAN IDs	
VLAN ID	VI AN Name VI AN ID
1	New VLAN
New VLAN 😵 New Multiple V	VLAN ID (2~4094): 2 *
New VLAN & New multiple vi	VLAN Name (1-31 character): VLAN0002
	Select ports to add to a VLAN:
	$ \begin{array}{cccccccccccccccccccccccccccccccccccc$
	C Optional E Fixed port Selected Aggregation C Trunk C I Pource Enable Port
	Tip: Click and drag cursor over ports to select multiple ports Select all Select all others Cancel
	(Save) Cancel

4.3.2 Access Port Settings

In the navigation bar to select "VLAN config>Access-port setting", can set port to Access port, the following picture:

Figure 4-26 Access port settings

VLAN Settings	Access Port Settings Trunk Port Settings	Hybrid Port Setting	IS		
Access port list					
Port	Port description		Native VLAN	Operation	
1			1	2	
2			1		
3			1		
4			1		
5			1		
6			1		
7			1		
8			1		
9			1		
10			1		
New Access port				First Back [1] Next Last 1 / 1 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.

Figure 4-27 Configuration example I

VLAN Settings Access Port Settings Trunk Port Settings Hybrid Port Settings							
VLANIDs							
	VLAN ID	VLAN Name	VLAN IP	Port	Edit / Delete		
	1	VLAN0001	192.168.2.1/24	1-7,9-10			
	2	VLAN0002		8			
📀 New	🔉 New VLAN 😮 New Multiple VLAN 🤤 Delete VLAN 😜 Delete VLAN /1 Page						

Figure 4-28 Configuration example II

VLAN Settings	Access Port Settings Trunk Port Settings Hybrid Port Settings	
Access port list		
Port	Dort description Native VI AN	Or X
1	New Access port Please select port to setting:	
2		
3		
4		
5	COptional Exced port Selected Aggregation COTTURE Selected STRAGGEREATION SET IP Source Enable Port	
6	Tip : Click and drag cursor over ports to select multiple ports Select all Select all others Cancel	
7	Native Vlan (1-4094): 2	
8	<	Þ
9	Save Cancel	
10	1	
Q New Access port	First	Back [1] Ne

4.3.3 Trunk-port setting

In the navigation bar to select "VLAN config>trunk-port setting", can set port to Trunk port, the following picture:

Figure 4-29 Trunk port

VLAN Settings Access Port Settings Hybrid Port Settings								
Trunk por	Trunk port list							
	Port	Port description	Native VLAN	Allowing VLAN	Operation			
O New T	3 New Trunk port 3 Delete selected Trunk port							

[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

Figure 4-30 Configuration example I

VLAN Settings Access Port Settings Trunk Port Settings Hybrid Port Settings						
VLAN IDS						
VLAN ID VLAN Name		VLAN Name	VLAN IP	Port	Edit / Delete	
	1	VLAN0001	192.168.1.110/24	1-10		
	2	VLAN0002			📄 🗶	
😮 New VLAN 😮 New Multiple VLAN 🤤 Delete VLAN First Back [1] Next Las 1 / 1 Page						

Figure 4-31 Configuration example II

Port Settings Trunk Port Settings Hybrid Port Settings
Port description Native VLAN Allowing VLAN W Trunk port
2 4 6 8 10
Fip: Click and drag cursor over ports to select multiple ports Select all Select all others Cancel Native Vian (1.4094):
Native Vlan (1-4094): 2 6 Allowing VLAN(such as 3-5,8,10): 2 2
Save settings Cancel

4.3.4 Hybrid-port setting

In the navigation bar to select "VLAN config>hybrid-port setting", Can set the port to take the tag and without the tag, the following picture:

Figure 4-32 Hybrid port settings

VLA	N Settings	Access Port Settin	gs Trunk Port Setting	s Hybrid Port Settings			
Hybrid	Port List						
	Port	Port Name	Native VLAN	Added VLAN TAG	Removed VLAN TAG	Edit / Delete	
O New	O New Hybrid Port O Delete Selected Hybrid Port						

[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:

<u>Step 1</u> Determine the VLAN in this port attributes (disp interface can see the port to which VLAN untag, which VLAN tag).

<u>Step 2</u> 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.

Figure 4-33 Configuration example I

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				
	10	VLAN0010			in 😥 🗶			
	20	VLAN0020			in 😥 🗙			
🔇 New VLAN 🔇 New Multiple VLAN 🤤 Delete VLAN First Back [1] Next Last 1 / 1 Page								

Figure 4-34 Configuration example II

VLAN Settings Ac	cess Port Settings Trunk Port Settings Hybrid Port Settings
Hybrid Port List	
Port F	New Hybrid Port
S New Hybrid Port S Delet	A structure of the s
	<
	Save Cancel

Figure 4-35 Configuration example III

VLAN Settings Acces	ss Port Settings Trunk Port Settings Hybrid Port Settings
Hybrid Port List Port Port New Hybrid Port Delete S	
	Image: Contract of the second seco
	Tip: Click and drag cursor over ports to select multiple ports Select all Select all others Cancel Native Vlan(1-4094):
	VLAN TAG (3-5,8,10): 1 Go to VLAN's TAG (such as 3-5,8,10): 10, 20
	Save Cancel

Figure 4-36 Configuration example IV

VLAN Settings Access Port Settings Trunk Port Settings Hybrid Port Settings								
Hybrid Port List								
	Port	Port Name	Native VLAN	Added VLAN TAG	Removed VLAN TAG	Edit / Delete		
	1		10	1	10,20	📄 🗙		
	2		20	1	10,20	📝 🗙		
New Hybrid Port Delete Selected Hybrid Port First Back [1] Next Las[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.

Figure 4-37 Fault/safety



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:

Figure 4-38 DHCP

DHCP	DOS	IP Source Guard	IP/Mac/Port	
Protection S	tatus			
Closed	Allows user to	configure custom DHCP trus	ted ports.	

[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】

Step 1 DHCP snooping open

Figure 4-39 Snooping open

DHCP DOS IP Source Guard IP/Mac/Port					
Protection Suite					
Open Allows user to configure custom DHCP trusted ports.					

Step 2 Setting DHCP snooping vlan

Figure 4-40 Set DHCP snooping vlan

DHCP configuration									
DHCP Trusted Port DHCP Restricted Ports MAC Verification Option82 Binding Table Other Configuration									
Dhcp Snooping Vlan:									

<u>Step 3</u> Set the connection router 8 ports for trust, then 6 port is set to the prohibit. Figure 4-41 Set trusted router

DHCP configuration					
DHCP Trusted Port	DHCP Restricted Ports	MAC Verification	Option82	Binding Table	Other Configuration
DHCP truste	d ports:				
Optional E Fixed po	rt <u> </u>	n 57 Trunk 5E7 IP Sourc	e Enable Port]
Tip: Click and drag curso	r over ports to select multiple po	rts Select all Select all ot	hers Cancel		
Save					

Figure 4-42 Set restricted ports

DHCP configuration					
DHCP Trusted Port	DHCP Restricted Ports	MAC Verification	Option82	Binding Table	Other Configuration
Prohibit D	HCP port:				
2 4 6 8 10 1 3 5 7 9]				
Optional E Fixed	port <u> </u> Selected <u>1</u> Aggregation	Trunk EIP Source	ce Enable Port		
Tip: Click and drag curs	sor over ports to select multiple ports	Select all Select all of	thers Cancel		
Save					

<u>Step 4</u> Verify source mac F0:DE:F1:12:98:D2, set server ip address to 192.168.1.110. Figure 4-43 Verify MAC address

DHCP configuration						
DHCP Trusted Port DHCP Restricted F	Ports MAC Verification	Option82	Binding Table	Other Configuration		
MAC Verification Enable : MAC Address : F0:DE:F1: Save	2:98:D2					
MAC Verification List						
No.	MAC Address			Status		Delete
				first page	prev page [1] next page last pa	ge 1 / 1 page

Step 5 Set option82 information

Figure 4-44 Set option82 information

DHCP configuration								
DHCP Trusted Port	DHCP Restricted Ports	MAC Verification	Option82 Binding Table	Other Configuration				
Option82 Enable: Client Option82 Enable: Circuit control Remote Agent IP address								
Circuit Name: 122 * VLAN ID: 1 *								
No. Circuit Control Name Circuit Control ID VLAN ID Operations								
First Back [1] Next Last / 1 Page								

Figure 4-45 IP address

DHCP configuration									
DHCP Trusted Port	DHCP Restricted Ports	MAC Verification	Option82	Binding Table	Other Configuration				
Option82 Enable: 🗹 Client Option82 Enable: 🗹									
Circuit control	Remote Agent IP addr	ess							
IP Address: 192.168.1.37 * VLAN ID: 1 *									
No.		IP Address			VL	AN ID	Operations		
	First Back 1 Next Last / 1 Page								

Step 6 The port 7 for binding.

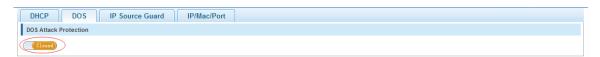
Figure 4-46 Binding table

DHCP configuration					
DHCP Trusted Port	DHCP Restricted Port	MAC Verification	Option82	Binding Table	Other Configuration
	C Address: 00:01:15:09:3 VLAN ID: 1 rt Number: 7	*			

4.4.1.2 OS

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:

Figure 4-47 DOS



[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

Figure 4-48 Configuration example

DHCP DOS	IP Source Guard	IP/Mac/Port		
DoS Attack Protection				
Open				

4.4.1.3 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:

Figure 4-49 IP source guard

IP source protection port enable configuration Please select a source port: 2 4 6 8 10 2 2 7 9 1 3 5 7 9 1 3 5 7 9 1 Selected fill Aggregation fill P Source Enable Port Tip: Click and drag cursor over ports to select multiple ports	DHCP DOS OP Source Guard IP/Mac/Port				
2 4 6 8 10 1 1 1 1 1 1 1 1 3 5 7 9 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	IP source protection port enable configuration				
Image: Contract of the selected of the select multiple ports	Please select a source port:				
	Image: Control in the second secon		Ê ☐ IP Source Enable Port		
Index Source IP Address Source MAC Address Port	New Security Port				

[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.

Figure 4-50 Configuration example I

DHCP DOS IP Source Guard IP/Mac/Port	
IP source protection port enable configuration	
Please select a source port:	
C Optional E Fixed port Selected Aggregation C Trunk E IP Source Enable Port	
Tip: Click and drag cursor over ports to select multiple ports	
Save	

Figure 4-51 Configuration example II

DHCP DOS IP	Source Guard IP/Mac/Port
IP source protection port enable of	configuration
Please select a source port	
2 4 6 8 10 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	VLAN ID: 1 * Source IP Address: 192.168.1.30 * Source MAC Address 00:01:16:09:35:37 *
Coptional Fixed port So Tip: Click and drag cursor over po Save	
Manual IP Source Protection List Index New Security Port	Optional 📃 Fixed port 📃 Selected 🚹 Aggregation 🛄 Trunk 🔁 IP Source Enable Port
	Save Exit

4.4.1.4 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:

Figure	4-52	IP/Mac/Port	
--------	------	-------------	--

DHCP DOS	S 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	9		
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 Figure 4-53 Configuration example I

Binding Enab	le 🗹	
Scanning	Binding	

Figure 4-54 Configuration example II

	mac address	ip address	Port number
	3C:97:0E:4F:57:F2	10.10.111	10
	3C:97:0E:4F:57:F2	192.168.1.112	10
	3C:97:0E:4F:57:F2	192.168.168.22	10
V	3C:97:0E:4F:57:F2	192.168.2.11	10
	00:01:15:09:37:35	169.254.131.107	4
		frist pag	e prev page [1] next page last page 1 / 1pag

Figure 4-55 Configuration example IV

Application List			
	mac address	ip address	Port number
	3C:97:0E:4F:57:F2	192.168.2.11	10
Delete option		frist pag	e prev page [1] next page last page1 / 1page

Can check the delete option.

4.4.2 Channel detection

4.4.2.1 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:

Figure 4-56 Ping

Ping Tracert Cable	Test
Destination IP Address:	*
Timeout in Seconds (1-10): 2	
Ping Count (1-100): 5	
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 connects the IP address of the PC.

Figure 4-57 Configuration example

Ping Tracert	Cable Test
Destination IP Address:	192.188.1.110
Timeout in Seconds (1-10):	
Ping Count (1-100):	5
Start	
Result	
PING 192.168.1.110 (192.168.1.110 64 bytes from 192.168.1.110: icmp_ 64 bytes from 192.168.1.110: icmp_ 64 bytes from 192.168.1.110: icmp_ 64 bytes from 192.168.1.110: icmp_ 64 bytes from 192.168.1.110: icmp_	seq=0 tht=64 time=0 0 ms seq=2 tht=64 time=0 0 ms seq=2 tht=64 time=0 0 ms seq=2 tht=64 time=0 0 ms
192.168.1.110 ping statistics 5 packets transmitted, 5 packets rec round-trip min/avg/max = 0.0/0.0/0.0	

4.4.2.2 tracert

In the navigation bar to select "**fault/safety**> **channel detection**>**tracert**". Tracert detection can detect to the destination through the .The following picture:

Figure 4-58 Tracert

Ping Tracert Cable Test		
Destination IP Address:		
Desunation IP Address:		
Start		
Result		

[Parameter Description]

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

Parameter	Description		
Destination IP address	Fill in the IP address of the need to detect		
Timeout period	Range of 1 to 10		

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.

Figure 4-59 Configuration example

Ping Tracert Cable Test	
Destination IP Address: 192. 168. 1. 110 *	
Result	
Tracing the route to 192.168.1.110 1 192.168.1.110 <10 ms <10 ms	

4.4.2.3 Cable test

In the navigation bar to select "fault/safety> channel detection>cable test", Can detect connection device status, the following picture:

Figure 4-60 Cable test

Ping Tracert Cable Test	
Please select port to configure:	
C Optional 🚍 Fixed port 💼 Selected 51 Aggregation 5 Trunk 52 IP Source Enable Port	
Start	

【Configuration Example】

Figure 4-61 Configuration example

Ping Tracert Cable Test	
Please select port to configure:	
C Optional 🚍 Fixed port 🚍 Selected 1 Aggregation . Trunk E IP Source Enable Port	
Start	

4.4.3 ACL

In the navigation bar to select "**fault/safety**>**ACL**", can be applied to port ACL rules and Settings to take effect in time.

Figure 4-62 ACL

Timetable ACL Apply ACL								
Time Name:	Time Name:							
Day Selection: 🗌 Monday 🗌 Tuesday 🗌	🗌 Wednesday 🔲 Thursda	ay 🗌 Friday 🗌 Saturday 🗌 Sunday						
Time Interval:	-	+						
Save								
Time Name	Time Name Day Time Interval Edit / Delete							
First Back [1] Next Las 1 / 1 Page								

[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:

- Step 1 According to the order, as long as there is a meet, will not continue to find.
- <u>Step 2</u> Implied refused, if don't match, so must match the final implied refused entry, cisco default.
- <u>Step 3</u> Any only under the condition of the minimum permissions to the user can satisfy their demand.

<u>Step 4</u> 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 .

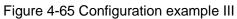
steps: building ACL time - building ACL rules - is applied to the port.

Figure 4-63 Configuration example I

Timetable ACL Apply ACL			
Time Name: Workday			
Day Selection: 🗹 Monday 🗹 Tuesday	Wednesday 🗹 Thursda	ay 🗹 Friday 🔲 Saturday 🗌 Sunday	
Time Interval: 9:00	- 18:00	+	
Save			
Time Name	Day	Time Interval	Edit / Delete
			First Back [1] Next Last 1 / 1 Page

Figure 4-64 Configuration example II

Timetable ACL App	bly ACL		
Create ACL			
Priority Acl Permission	Index Protocol Source IP / M	ask Source	Destination IP / Mask Destination Timetable
number	new ACL access rule		· · · · · · · · · · · · · · · · · · ·
	ACL Number: 100		Protocol Type: TCP ~
	Permission: Deny	*	Protocol Type: TCP ACL Name: Workday
	Any src IP Address:		
	Any source port:		
	Any dst IP Address:		
	Any dst Port:		
	Single dst Port(0-65535):	80	
	Save		



Timeta	able ACL Apply ACL		
Create A			
Priority	The new ACL access rule	×	Ti
1	ACL Number: 100 Permission: Permit		v
	Any src IP Address:		
	Any dst IP Address:		
	Save		

Figure 4-66 Configuration example IV

Timetab	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 Las 1 / 1 Page										

Figure 4-67 Configuration example V

	CL		
2 4 6 8 10 1 3 5 7 9 Coptional Ericed port Estimation (1)	Aggregation 5Trunk 5€71P Source Enable Port		
Tip: Click and drag cursor over ports to select n ACL Number: 100 Filtering Direction: Receive m Save			
Access Control List ACL Number	Port	Filtering Direction	Edit / Delete

4.5 PoE

In the navigation bar to select "**PoE**", you can set the **PoE Port Config** configuration. Figure 4-68 PoE



4.5.1 PoE Port Config

4.5.1.1 Poe Port Config

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

System Max power: 140W								
Current system power: 0.000W								
2 4 6	8							
ćċċ	. Ċ							
Optional	📄 Fixed port 📄 Se	lected 1 Aggre	egation 🛄 Trunk	E IP Source Enable Port				
Tip: Click an			e ports Select all	Select all others Cancel				
	port enabled:	·	•	Power supply priority: Id	▼ WC			
	threshold:	7.5mA	¥	Port power: 30)			
Save	threshold:	7.5mA	T	Port power: 3)			
Save PoE config	threshold:	7.5mA	T	Port power: 3				
	threshold:	7.5mA Status	T Max power	Port power: 3	Current(mA)	Voltage(V)	Limit Current	Priori
PoE config				· _		Voltage(V) 0.000	Limit Current 7.5mA	Priori
PoE config Ports	Enable Control	Status	Max power	CurrentPower(W)	Current(mA)			
PoE config Ports Gi01	Enable Control ON	Status OFF	Max power 30	CurrentPower(W)	Current(mA) 0	0.000	7.5mA	Low
PoE config Ports Gi01 Gi02	Enable Control ON ON	Status OFF OFF	Max power 30 30	CurrentPower(W) 0.000 0.000	Current(mA) 0 0	0.000	7.5mA 7.5mA	Lov

Figure 4-69 Poe port Config

[Parameter Description]

Parameter Description

Parameter	Description
port enabled	You can enable or disable PoE function
Power supply priority	Configure port priority, when the load exceeds the maximum power POE, low priority port equipment will be dropped
threshold	You can specify threshold
Port power	You can configure max power of port

【Configuration Example】

Such as: The PoE function of port 8 can be enabled, the maximum Port power is 23 W, threshold is 15mA, and the Power supply priority is high.

Figure 4-70 Configuration example

Poe Port Config	Temperature Distribution	
System Max Current system		
$ \begin{array}{cccccccccccccccccccccccccccccccccccc$		
Optional 📑 Fixed port	Selected 517 Aggregation 57 Trunk 527 IP Source Enable Port	
Tip: Click and drag cursor	rer ports to select multiple ports Select all Select all others Cancel	
port e	abled: Enabled Power supply priority: high	
thr	shold: 15mA Port power: 23	
Save		

4.5.1.2 Temperature distribution

In the navigation bar to select "POE>POE port Config>Temperature distribution", you can view temperature distribution, As follows.

Figure 4-71 Temperature distribution

Poe Port Config Temperature Distribution					
List	InputVoltage(v)	Temperature(c)			
1	52.989	38			
2	52.926	36			
		First Back [1] Next Last / 1 Page			

4.6 STP

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

Figure 4-72 STP						
► ST	ГР					
•	MSTP Region					
STP Bridge						
:	-					

4.6.1 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.

Figure 4-73 MSTP region

MSTP Configuration		
Region Name : 00E0	4C000002 * (1 to 32 characters)	
Revision Level: 0	* (0 to 65535,default 0)	
Save		
Instance Mapping		
Instance ID: 1	•	
VLAN ID :	* For example : 1,3,5,7-10	
Save Delete		
Mapping List		
Instance ID	Mapping VLAN	Edit
0	1-4094	Ø
	first name prev name [1] next name	last nace 1 / 1 nace

[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.

Figure 4-74 Configuration example I

MSTP Configuration							
Region Name:	DEADBEEF0102	*	(1 to 32 characters)				
Revision Level:	123	*	(0 to 65535,default 0)				
Save							

Figure 4-75 Configuration example II

Instance Mapping	
Instance ID:	4 ~
VLAN ID:	2 * For example: 1,3,5,7-10
Save Delete	

4.6.2 STP bridge

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

STP Bridge Config							
Instance Priority:							
Instance ID :)	-		Priority : 3276	8 🚽		
Enable: O ON OFF Mode: OSTP ORSTP MSTP						ISTP	
Hello Time : 2		* (1-10	s)	MAX Age: 10		*	(6-40s)
Forward Delay : 1	0	* (4-30	s)	MAX Hops: 10		*	(1-40)
Save Show Bridge	Info						
STP port config							
Instance :	0	~		Priority :	128		* (0-240,step 16)
Port Fast :	ON 🔘	OFF		Path Cost :	auto		* (auto or 1-20000000)
Auto Edge :	ON	OFF		Point to Point :	ON C	OFF	Auto
BPDU Guard :	O ON	OFF		Compatibility			
BPDU Filter :	O ON	OFF		Root Guarde:	🖲 🤂 🗑	Refe	
TC Guard :	O ON	OFF		TC Ignore :	🔘 ON 🧕	OFF	
1 3 5 7 9 2 4 6 8 10							
Optional 🚍 Fixed po	ort 📃 Sel	ected 🖸 Aggrega	ation 🗔 Trunk 🗹	[] IP Source Enable	Port		
Save Show Curren	nt Port						

Figure 4-76 STP bridge

[Parameter Description]

Parameter	Description	
Instance Priority	Whether open instance priority	

Parameter	Description	
	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	

<u>Step 1</u> (hello_time+1)×2<=max_age<=(f_delay-1)×2, enable the switch to set instance priority.

<u>Step 2</u> Enable STP or switch mode would spend 2 times of the forward delay time.

【Configuration Example】

<u>Step 1</u> Open the STP, configuration has to create an instance of the priority, configuration time parameters, set the pattern to MSTP.

Figure 4-77 Configuration example I

inst :	4	-		priority: 128 * (0-240,step
port-fast :	© off	on		path-cost: auto * (auto or 1-20
auto-edge :	© off	🖲 on		point-to-point: 🔘 off 🔘 on 💿 auto
bpdu-guard :	© off	on		compatible : 💿 off 💿 on
bpdu-filter :	off	◎ on		rootguard : 💿 none 💿 root
tc-guard :	off	© on		tc-ignore : 💿 off 💿 on
	7 9 2			
Coptional	Not optio	onal 📃 S	Selecte	ed 🚹 Aggregation 🛄 Trunk 🕅 ip source enable port
show of	current p	ort		
Show	currenc p		1 70	8 Configuration example II
		riguie	4-70	
				Mstp Port Information [Gi0/4]
Mstp Port Config[Gi0/4]				
Tips: Config mstp and show informat PortAdminPortFast: enable PortOperPortFast: disable PortAdminAutoEdge: enable				
in	st: 0			PortOperAutoEdge: disable
port-fa		off 🍥	on	PortAdminLinkType: auto PortOperLinkType: point-to-point
	_			PortBPDUGuard: enable PortBPDUFilter: disable
auto-edg			on	PortTCGuard: disable
bpdu-gua	rd : 🔘	off 🧕	on	instance[0]
bpdu-filt	er: 🍥	off 🔘	on	VlanMap: 2-4094 PortState: down
tc-gua	rd : 🍥	off 🔘	on	PortPriority: 128
1 3 5		9 10 t optional	1	PortDesignatedRoot: 32768 - 40:97:0e:4f:57:55 PortDesignatedCost: 0 PortDesignatedBridge: 32768 - 40:97:0e:4f:57:55 PortDesignatedPortPriority: 128 PortDesignatedPort: 4 PortAdminPathCost: auto PortOperPathCost: 5000000 PortRole: disabled
save	iow curr	ent pop		quit

<u>Step 2</u> 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)

4.7 DHCP relay

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

Figure 4-79 DHCP relay

DHCP RELAY
Dhcp Relay
option82

4.7.1 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. Figure 4-80 Enable

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

Figure 4-81 Configuration example

DHCP Relay Enabl	e				
DHCP Relay Enable: 🗹 DHCP Option Trust Field Enable: 🗹					
DHCP Relay Config	9				
Save	HCP Server IP: 192.168.1.22 × •				
Number	IP Address	Status	Edit		
1	0.0.0.0	invalid	×		
		First Back [*	I] Next Last 1 / 1 Page		

4.7.2 Option82

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

Figure 4-82 Option82

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] nex	kt page last page 1 / 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.

Figure 4-83 Configuration example I

Circuit control Pr	roxy remote IP a	ddress		
Circuit control: 123	*	١	/LAN ID	*
Serial number	Circuit	control name		Circuit control ID
	Figure 4-84 Con	-	-	
Proxy remote: In general, an	access layer switch for th	e MAC information is i	nserted into the option82.	
Circuit control Pro	oxy remote IP add	dress		
Proxy remote: swet	*	VLA		*
Serial number	Proxy rer	note name		Proxy remote ID
	Figure 4-85 Cont	figuration exam	ple III	
Circuit control	Proxy remote	IP address		
IP address: 192. 14	68. 2. 35 *		VLAN ID: 1	*
Serial number			IP addre	SS

4.8 QoS

In the navigation bar to select "QoS", you can set to the Remark, queue config and mapping the queue.

Figure 4-86 QoS

•	Q	05
	•	Queue Config
	•	Mapping the Queue

4.8.1 Queue config

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

Figure 4-87 Queue config

Queue setting	
Queue mode:	WFQ ~
Byte weight (0~127):	1 2 3 4 5 6 7 8
Apply	

[Parameter Description]

Parameter	Description	
	Can choose four kinds of modes:	
	RR round-robin scheduling	
Scheduling strategy	SP absolute priority scheduling	
Soliciality strategy	WRR weighted round-robin scheduling	
	WFQ weighted fair scheduling	
WRR-weights	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: Byte weight(0~127):	

4.8.2 Mapping the queue

4.8.2.1 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.

Figure 4-89 COS queue map

COS Que	COS Queue Map DSCP COS Map Port COS Map								
Mapping Que	Mapping Queue Status Information								
Server ID	0	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.

Figure 4-90 Configuration example I

COS Quei	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	eID 0 1 2 7 7 4 5 6 7 7								
Save									

Figure 4-91 Configuration example II

Queue setting	
Queue mode: Byte weight (0~127): Apply	WRR

4.8.2.2 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:

Figure 4-92 DSCP COS map

COS Queu	COS Queue Map DSCP COS Map Port COS Map															
Differential se	fferential 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.

Figure 4-93 Configuration example

COS Queu	COS Queue Map DSCP COS Map Port COS Map															
Differential se	fferential 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																

4.8.2.3 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:

Figure 4-94 Port COS map

COS Queue Ma	p DSCP CC	OS Map Por	t COS Map						
Port CoS mapping									
Port:	1	\sim							
Server ID:	0	~							
Trust									
Mode:	COS	\checkmark							
Apply									
Control list									
Port				Serv	ver ID				Trust Mode
	0	1	2	3	4	5	6	7	
1	т								
2	т								
3	т								
4	т								
5	т								
6	т								
7	т								

[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.

Figure 4-95 Configuration example I

COS Queue Map		DSCP C	OS Map	Port COS Map	
Port CoS mapping					
Port: Server ID: Trust Mode:	4 4 COS		Y Y		

Figure 4-96 Configuration example II

COS Queue Map	DSCP COS Map	Port COS Map
Port CoS mapping		
Port: Server ID: Trust Mode:	5 ~ 5 ~ cos ~	

Figure 4-97 Configuration example III

COS Que	ue Map		DSCP	COS Maj	p	Port	COS Map	2
Port CoS m	apping							
	Port: Server	6		\sim				
	ID: Trust	6		~				
	Mode:	COS		\sim				
Apply								

Figure 4-98 Configuration example IV

Control list	Control list								
Port	Server ID						Trust Mode		
	0	0 1 2 3 4 5 6 7							
1	т								
2	т								
3	т								
4					т				cos
5						т			cos
6							т		COS
7	т								
8	т								
	First Back [1] [2] Next Last 1 / 2 Pag						ast 1 / 2 Page		

4.9 Addr table

In the navigation bar to select "Address table", you can set to MAC Management, MAC learning and Aging and MAC Filter.

Figure 4-99 MAC management

Address Table Config						
MAC Management MAC Learning and Aging MAC Filter						
Clear MAC: Clear appoint MAC VLAN: 1 MAC Address : Valid Range (1 to 4094) Save Save						
	2 4 6 8 10 1 1 2 1 1 3 5 7 9					
	ed port 🚞 Selected 🚹 Aggregation 🛄 Trunk					
VLAN: MAC Add	I Valid Range (1 to 40	94)				
Save						
MAC	MAC Address List: All					
Number	MAC Address	VLAN ID	Address Type	Port		
1	00:0A:6A:00:03:EE	1	dynamic	5		
	first page prev page [1] next page last page 1 / 1 page					

4.9.1 MAC Management

In the navigation bar to select "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: Figure 4-100 MAC management

Address Table Config						
MAC Management MAC Learning and Aging MAC Filter						
Clear MAC: Clear appoint MAC: VLAN: 1 Valid Range (1 to 4094) MAC Address : Image: Clear appoint MAC:						
2 4 6 8 10 \square \square \square \square \square \square \square \square \square \square 1 3 5 7 9						
Optional 🚍 Fix	ed port 💼 Selected 🚹 Aggregation 🛄 Trunk					
VLAN:	1 Valid Range (1 to 40	94)				
MAC Ad	dress :					
Save						
MAC Address List: All						
Number	MAC Address	VLAN ID	Address Type	Port		
1	00:0A:6A:00:03:EE	1	dynamic	5		
first page prev page [1] next page 1 / 1 page						

[Parameter Description]

Parameter	Description
Clear Mac	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

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

【Configuration Example】

Step 1 The port 6 Mac set to static Mac.

Figure 4-101 Configuration example I

2 4 6 8 10 2 5 5 5 5 5 10 1 3 5 7 9	
C Optional E Fixed port	Selected 17 Aggregation Trunk
VLAN:	1 Valid Range (1 to 4094)
MAC Address :	3C:97:0E:4F:57:F2
Save	

<u>Step 2</u> Clear port 6 static Mac addresses.

Figure 4-102 Configuration example II

Address Table Config	
MAC Management	MAC Learning and Aging MAC Filter
Clear MAC: VLAN: MAC Address	Clear appoint MAC : Valid Range (1 to 4094) 1 Valid Range (1 to 4094) 3C:97:0B:4F:57:F2 Valid Range (1 to 4094)

4.9.2 MAC Learning and Aging

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

Figure 4-103 MAC learning and aging

Address Table Config				
MAC Management MAC Learning	and Aging MAC Filter			
I				
1 3 5 7 9				
Optional Exception Fixed port Exception Selected Tip: Click and drag cursor over ports to se				
MAC Learning Limit: 8191				
Save				
MAC Address Aging Time: 300	(0 indicates no aging, <u>10-1000000</u> second)			
Save	(o inductor no aging <u>, o robobio</u> boond)			
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] Next Last / 2 Page		

[Parameter Description]

Parameter	Description
Mac address	Range 0-8191, default 8191
Mac address study limit	Default 300

[【]Configuration Example】

Step 1 Setting port 2, 3, 4, 5 address study limit for 2000.

Figure 4-104 Configuration example I

Address Table Config
MAC Management MAC Learning and Aging MAC Filter
Copional 💼 Fixed port 💼 Selected 🔐 Aggregation 🛄 Trunk
Tip: Click and drag cursor over ports to select multiple ports
MAC Learning Limit 2000 (Learning Range 0-8191)
MAC Address Aging Time: 300 (0 indicates no aging.10-1000000 second)
Save

<u>Step 2</u> Will be dropped or learn the Mac address of the port equipment after 2 minutes disappear automatically from the Mac address table.

Figure 4-105 Configuration example II

Suve	
Mac address Aging time: 120	(0 indicates not aging,10-1000000 second)
save	

4.9.3 MAC Filter

In the navigation bar to select "address table>MAC Filter", Can be filtered according to the condition does not need the Mac address. The following picture: Figure 4-106 MAC filter

Address Table Config						
MAC Management MAC Learning and Aging MAC Filter						
MAC Address: VLAN: Valid Range (1 to 4094) Save						
MAC Address VLAN ID Address Type Delete						
first page prev page [1] next page last page 1 / 1 page						

[Parameter Description]

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

【Configuration Example】

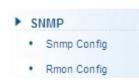
Such as: the Mac address for 00:20:15:09:12:12 added to the filter in the table. Figure 4-107 Configuration example I

Address Table Config						
MAC Management MAC Learning and Aging MAC Filter						
MAC Address: 00:20:15:09:12:12 VLAN: 1 Save	ilid Range (1 to 4094)					
MAC Address VLAN ID Address Type Delete						
first page prev page [1] next page last page 1 / 1 page						

4.10 SNMP

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

Figure 4-108 SNMP



4.10.2 Snmp config

4.10.2.1 Snmp config

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

Figure 4-109 SNMP Config

	5		5		
SNMP Config	Community Config	Group Config	User Config	Trap Config	View Config
SNMP Config					
Closed					

[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.



SNMP Config	Community Config	Group Config	User Config	Trap Config	View Config
SNMP Config					
Open					

4.10.2.2 Community config

In the navigation bar to select "Snmp >Snmp config>community config", Can specify group access. The following picture.

Figure 4-111 Community Config

SNMP Config Community Config Group Config User Config Trap Config View Config						
SNMP Community List						
Community Name Access Authority Edit / Delete						
New community Delete Selected Community First Back [1] Next Last 1 / 1 Page						

[Parameter Description]

Parameter	Description
group	Community string, is equal to the NMS and Snmp agent

Parameter	Description
	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

The upper limit of the number of groups is 8.

【Configuration Example】

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

Figure 4-112 Configuration example

SNMP Config Comm	unity Config Group Config User Config Trap Config View Config
SNMP Community List	
	Community Name Access Authority SNMP Community Configuration
New community Solution Delete S	Community Name public * String Length (1-16) Access Authority : Read Write
	Save Exit

4.10.2.3 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. Figure 4-113 View Config

SNMP Config Community Config Group Config User Config Trap Config View Config							
View Name * String length[1-16]							
New view							
View Rule List Delete View							
Rule MIB Subtree OID Subtree Mask Edit / Delete							
New View Rule Delete Selected View Rule First Back [1] Next Last					First Back [1] Next Last 1 / 1 Page		

[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

Parameter	Description		
MIB Subtree OID	View the associated MIB object, is a number of MIB		
Subtree mask	MIB OID mask		

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. Figure 4-114 Configuration example I

SNMP Config Community Config		Group Config	User Config	Trap Config	View Config
View Name 123	* String le	ngth[1-16]			
New view					

Figure 4-115 Configuration example II

SNMP Config	Community Config	Group Config User Config Trap Config View Config
View Name	* String ler	ngth[1-16]
New view	Edit Vie	ew Rule
View Rule List 123	Rule Delete Selected Vie OID :	Excluded applies to a subset of the included content.Exclusive use does not take effect. Rule : Include Exclude Subtree 1.3.6.1 * String length[1-64]
		ee Mask : * String length[1-31]

4.10.2.4 Group config

In the navigation bar to select "Snmp>Snmp config>group config", setting Snmp group. The following picture.

Figure 4-116 group Config

SNN	IP Config Community	Config Group Config	User Config	Trap Config View Config		
SNMP	Group					
	Group Name	Security Level	Read View	Read and Write View	Notify View	Edit / Delete
🗿 Nev	S New Group O Delete Selected Group First Back [1] Next Las 1 / 1 Page					

[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

Parameter	Description
	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

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.

Figure 4-117 Configuration example I

View rule list 123 delete view						
	rule	MIB subtree OID	subtree mask	operation		
	included	.1.3.6.1		2 🗙		
O New view rule 😑 Delete select View rule frist page prev page [1] next page last page 1						

Figure 4-118 Configuration example II

SNM	P Config Community	Config Group C	onfig Us	er Config	Trap Config View Config	J
SNMP	Group					
Nev	Group Name	New group	R	load View	Read and Write View	
		Group Name : Security Level : Read View : Read and Write View : Notify View:	group1 Authentication a none none none		Length (1-16)	
		Save	Exit	-		

4.10.2.5 User config

In the navigation bar to select "Snmp>Snmp config>user config", setting Snmp user. The following picture:

Figure 4-119 User Config

SN	MP Config	Community Conf	ig Group C	onfig User Config	Trap Config View Config	3		
SNM	P User							
	User Name	Security Level	Group Name	Authentication Mode	Authentication Password	Encrypt Mode	Encrypt password	Edit / Delete
😳 Ne	ew User 🤤 Dele	te Select User					First Back [1] Next Las	at 1 / 1 Page

[Parameter Description]

Parameter	Description
User Name	User name, range 1-16
	Attestation not only encryption: this group of users transmission of the message need to verify the data don't need to confidential
Security Level	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 user1.

Figure 4-120 Configuration example

SNMP Config	Community Config Grou	up Config User Con	fig Trap Config	View Config	
SNMP User					
User Name	Edit SNMP user	Authontication Mod	do Authontication	Daseword Epon	rst Mod
New User C Delet	User Name : Security Level :	user1 * Str	ing Length (1-16)		
	Group Name : Authentication Mode :	group1 ~ MD5 ~			
	Authentication Password : Confirm Authentication	12345678 * Stri	ing Length (8-60)		
	Password : Encrypt Mode :	12345678 * DES V			
	Encrypted Password :	* Str	ing Length (8-60)		
	Confirm Encrypted Password :				
	Save				
	Save Exit				

4.10.2.6 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: Figure 4-121 Trap Config

SNMP	Config Community Config Group	Config User Config	Trap Config View Config			
Trap Des	stination Host					
	Destination IP Address	Security Name	UDP Port Number	Security Mode	Edit / Delete	
🔘 New T	🔇 New Trap 🤤 Delete Selected Trap					

[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 hoset 192.168.1.30 receives trap information.

Figure 4-122 Configuration example

SNMP Config Community Config	g Group Co	nfig User Co	onfig	Trap Config	View Config	
Trap Destination Host						
	ew Trap	Security Name			f Number	
	Destination IP Address : Security Name : JDP Port Number : Security Mode :	192.168.1.30 user1 162 v1	*			
	Save E	xit				

4.10.3 Rmon config

4.10.3.1 Statistics group

In the navigation bar to select "Snmp>Rmon config>statistics group", Set an Ethernet interface statistics .the following picture:

Figure 4-123 Statistics group

Statistics Gr	oup History Group	Alarm Group Event Group		
Statistics Group	p List			
	Index	Interface Name	Owner	Edit / Delete
O New Count (Group 🤤 Delete Selected Co	unt Group	first page	prev page [1] next page last page 1 / 1 pa

[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.

Figure 4-124 Configuration example I

Statistics Group	History Group	Alarm Group Event Group	
count group list			
	index	statistical group configuration	owner status
e new count group	uciele aciect count group		1-65535]
			string length[1-30]
		csave quit	

Figure 4-125 Configuration example II

Statist	ics Group	History Gro	up Alai	m Group	Event Group				
count gro	oup list								
	index			interface na Statistica	l information	owner	etatue	×	operation
new control	77 ount group 🥥 d	lelete select coun	t group		Number of Packet D Number o	iscarding Events : f Received Bytes :	0 989395	,	rst page prev page [1] next page la
				N	Number of Re umber of Received Broad	ceived Packets :L casting Packets :	9813 4164		
				Number o	Number of Received N f Received Packets With		5222		
				Number of	Received Packets Small	: er Than 64 Bytes :	0 312		
				Quit	ber of Received Packets	Larger Than 1518		-	

4.10.3.2 History group

In the navigation bar to select "**Snmp>Rmon config>history group**", Record the history of an Ethernet interface information. The following picture.

Figure 4-126 History group

<u>Statis</u>	tics Group	History Group Alarm G	roup Event Group				
history	proup list						
	index	interface name	maximum number of samples	sample period	owner	status	operation
🗿 new	history group	🤤 delete select history group			frist page prev pa	ge <mark>(1)</mark> next page la:	st page 1 / 1 page

[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

Parameter	Description
	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.

Figure 4-127 Configuration example

Statistics Group	History Group A	arm Group Event Group	
history group list			
index	interface name delete select history group	history group configuration	noriod X
non motory group	, and a construction of group	index: 222 * [1-65535] interface name: interface Gi0/4 + * Maximum number/of	E
		samples: 2222 * [1-65535] sample period 23 * second	•

4.10.3.3 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.

Figure 4-128 Event group

Statistics Gr	oup History Group	Alarm Group Event Grou								
event group list										
	index	description	owner	action	status	operation				
🗿 new event gro	oup 🤤 delete select event gro	e delete select event group frist page prev page [1] next page last page 1 / 1p								

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,

Parameter	Description
	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. Figure 4-129 Configuration example

Statistics Group History Group	Alarm Group Event Group	
event group list		
index	description event group configuration	ownor action statys
ew event group	index: 345	* [1-65535]
	description 212	* string length[1-30]
	owner: Coco	* string length[1-30]
	action: 🗷 Log 🖉 Trap	
	save quit	

4.10.3.4 Alarm group

In the navigation bar to select" **Snmp>Rmon config>alarm group**", define alarm group. The following picture.

Figure 4-130 Alarm group

Sta	Statistics Group History Group Event Group											
Alam	Alarm Group List											
🗆 Ind	lex Statis		Sampling Time Interval	Sample Type	Last Sample Count	Upper Alarm Threshold Limit	Upper Alarm Threshold Limit Events	Lower Alarm Threshold Limit	Lower Alarm Threshold Limit Events	Ower	Status	Edit / Delete
🗿 Ne	New Alarm Group Delete Selected Alarm Group First Back [1] Next Last / / 1 Page											

[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:CRCAlignErrors. 9:UndersizePkts. 10:OversizePkts. 11:Fragments. 12:Jabbers. 12:Collisions. 14:Pkts64Octets.

-	5:Pkts65to127Octets.
I I I I I I I I I I I I I I I I I I I	
-	6:Pkts128to255Octets.
	7:Pkts256to511Octets.
	3:Pkts512to1023Octets.
19	9:Pkts1024to1518Octets
Se	et up the corresponding
atistical Group Index	atistics statistical index number,
de	ecided to statistics to monitor the
pc	ort number
Sa Sa	ampling time interval, the scope
mpling Time Interval for	r 5 ~ 65535, the unit for seconds
Sa	ample types for the absolute
	alue of sampling, the sampling
tin	me arrived directly extracting the
va	alue of a variable
Sa	ampling type for change value
	ampling, extraction of the arrival
•	the sampling time is variable in
	e change of the sampling
int	terval value
per Alarm threshold Limit	et the upper limit the Parameter
va	alues
wer Alarm threshold Limit	et the lower limit Parameter
	alues
per Alarm/Lower Alarm	pper/lower limit reached, for
eshold Limit Events ea	ach event
vner	et the table creator, ownername
fo	r 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.

Figure 4-131 Configuration example

The current user name: admin	
Statistics Group History Group Alarm Group E	Event Group
alarm group list	
note: Configure the alarm group before you configure the statistical group construction of the statistical g	
index static Statistical group and table index in	index: 123 * [1-65535]
e new alarm group delete select alarm group Statistical group Statistical group	ic table: DropEvents
Sausucargiou Sampling time i	
Samp	wer; Coco * string length 1-30]
The alarm thresho	
Events that exc thresho	eed the Md limit: 345 🗸
Alarm thresho	
Events below the th	limit: 345 -
Save quit	

4.11 LACP

In the navigation bar to select "LACP", you can set to the lacp config. Figure 4-132 LACP



4.11.2 Lacp config

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

Figure 4-133 LACP settings

LACP Setting LACP Display
LACP status
Open LACP:
Apply
LACP public parameter settings
System priority 1 (1-65535)
Apply
LACP activation port parameter settings
choose port to set up:
2 4 6 8 10 立立立立
Image:
C Optional E Fixed port Selected Aggregation C Trunk C IP Source Enable Port
Tip: Click and drag cursor over ports to select multiple ports Select all Select all others Cancel
Port priority: 1 (0-65535)
Aggregate port number: 1
Aggregate model: active V
Apply

4.11.2.2 LACP Setting

In the navigation bar to select "LACP>Lacp config>LACP settings" the following picture: Figure 4-134 LACP settings

LACP Setting LACP Display			
LACP status			
Open LACP: Apply			
LACP public parameter settings			
System priority 1 (1-65535)			
Apply			
LACP activation port parameter settings			
choose port to set up:			
$ \begin{array}{cccccccccccccccccccccccccccccccccccc$			
C Optional E Fixed port Selected Aggregation C Trunk E IP Source Enable Port			
Tip: Click and drag cursor over ports to select multiple ports Select all Select all others Cancel			
Port priority: 1 (0-65535)			
Aggregate port number: 1 Aggregate model: active			
Apply			

LACP status

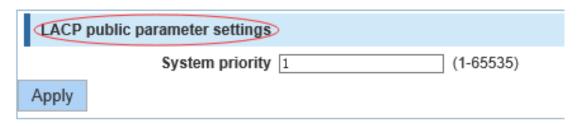
Figure 4-135 LACP status

LACP status	
	Open LACP:
Apply	

Open or close LACP.

LACP public parameter settings

Figure 4-136 LACP public parameter settings



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

LACP activation port parameter settings

Figure 4-137 LACP activation port parameter settings

LACP activation port parameter settings				
choose port to set up:				
$ \begin{array}{cccccccccccccccccccccccccccccccccccc$				
Coptional 🚍 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: 1 (0-65535)				
Aggregate port number: 1				
Aggregate model: active				
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.

4.11.2.3 LACP Display

In the navigation bar to select "LACP>Lacp config>LACP Display", You can see the table of lacp. The following picture:

Figure 4-138 LACP display

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

4.12 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.

Figure 4-139 System



4.12.2 System config

4.12.2.1 System settings

In the navigation bar to select "SYSTEM>system config>System settings", Basic information set switch. The following picture:

Figure 4-140 System settings

System Settings System Restart	Password EEE Enable SSH Login Telnet Login System Log
Basic System Information	
Management VLAN: 1 ×	Device MAC: 00:E0:4C:00:00:00
Management IP: 192. 168. 1. 110 *	lpv6 Address:
Subnet Mask: 255. 255. 255. 0 *	Device Name: Switch
Default Gateway: 0. 0. 0. 0	Device Location:
Jumbo Frame: 1518 (1518-9216)	Contacts(include
DNS Server: 0.0.0.0	mailbox):
Login Timeout	
(Minutes): 30	
Save Delete Set Management VLAN	
System Time	
Current System Time: 2000-01-01 01:59:10	
Set Time:	
NTP Server	
Save	

[Parameter Description]

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

【Configuration Example】

<u>Step 1</u> 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.

Figure 4-141 Configuration example I

VLAN	VLAN Settings Access Port Settings Trunk Port Settings Hybrid Port Settings					
VLAN ID	VLAN IDs					
	VLAN ID VLAN Name VLAN IP Port Edit / Delete					
	1 VLAN0001		192.168.1.110/24	1-10		
	2 VLAN0002					
🕲 New VLAN 🎱 New Multiple VLAN 👄 Delete VLAN						

Figure 4-142 Configuration example II

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	

Figure 4-143 Configuration example III

System Settings	System R	estart	Password EEE En	able SSH L	ogin	Telnet Login	System Log
Basic System Inform	nation						
Management VLAN:	2	*	Device MAC:	00:E0:4C:00:00:00			
Management IP:	192. 168. 1. 110	*	Ipv6 Address:				
Subnet Mask:	255. 255. 255. 0	*	Device Name:	Switch			
Default Gateway:	0. 0. 0. 0]	Device Location:				
Jumbo Frame:	1518	(1518-9216)	Contacts(include				
DNS Server:	0. 0. 0. 0]	mailbox):				
Login Timeout							
(Minutes):	30]					
Save Cancel s	ettings						

<u>Step 2</u> 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.

Figure	1-111	Config	uration	avami	مام	۱\/
FIGULE	4-144	Coming	uralion	exam	pie	IV

System settings System restart	Password change ssh login
system basic information	
Manage VLAN: 2 🗸	Device MAC: da:ad:12:34:56:78
Manage IP: 192. 168. 2. 12 *	Device name: yoyo
Mask: 255. 255. 255. 0 *	Device position:
Default gateway: 0. 0. 0. 0	Contacts:
Jumboframe 5000 (1518-9216)	Contact
DNS server: 0. 0. 0. 0	information:
Login	
timeout(minute): 20	
Save settings Set management vlan	

<u>Step 3</u> Use 192.168.2.12 logging in, sets the system time. Figure 4-145 Configuration example V

system time	system time										
current system time: 2000year01month01dayMorning07:53:25											
Reset time:											
🔲 Automati	-	I N	ov	201	5	•	₩				
save settii	Sun	Mon	Tue	Wed	Thu	Fri	Sat				
\sim	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 🗘		e)				
		(Clear	Too	lay	0	K				

4.12.2.2 System restart

In the navigation bar to select "SYSTEM>system config>system restart", equipment can be restarted. The following picture:

Figure 4-146 System restart

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.<u>http://192.168.2.1/system/sysreload.htm?1448508984027</u>

[Configuration Example]

Such as: click "restart" button.

Figure 4-147 Configuration example

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

4.12.2.3 EEE Enable

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

Figure 4-148 EEE enable

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

[Instruction]

Energy Efficient Ethernet, Open the EEE features by default.

4.12.2.4 Password

In the navigation bar to select "**SYSTEM**>**system config**>**password**", The password change to equipment. The following picture:

Figure 4-149 Password

System Settings Sys	tem Restart	Password	EEE Enable	SSH Logi	n	Telnet Login		System Log	
Change Administrator Password									
Password type:	Encrypted passwo	orc 🗸							
Old Password	•••••	*							
New Password	••••	*							
Confirm New Password	••••	*							
Save Clear									

[Instruction]

<u>Step 4</u> If you set a new Web login password, then log in again after seting the new password.

<u>Step 5</u> Password cannot contain Chinese, full-width characters, question marks and spaces.

<u>Step 6</u> 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.

Figure 4-150 Configuration example

Change Administrator Password		
Password type:	Encrypted passwore ~	·
Old Password:	•••••	*
New Password:	••••	*
Confirm New Password:	••••	*
Save Clear		

4.12.2.5 SSH login

In the navigation bar to select "SYSTEM>system config>ssh login", SSH open. The following picture:

Figure 4-151 SSH login

System Settings	System Restart	Password	EEE Enable	SSH Login	Telnet Login	System Log
SSH Config						
Open						
SSH Timeout: 5	*					

[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.

Figure 4-152 Configuration example

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

4.12.2.6 Telnet login

In the navigation bar to select "**SYSTEM**>**system config**>**Telnet login**", Telnet open. The following picture:

Figure 4-153 Telnet login

System Settings	System Restart	Password	EEE Enable	SSH Login	Telnet Login	System Log
Telnet Config						
Open						
Telnet Timeout: 5	2					

[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.

Figure 4-154 Configuration example

1	System Settings	System Restart	Password	EEE Enable	SSH Login	Telnet Login	System Log
	Telnet Config						
<	Open						

4.12.2.7 System log

In the navigation bar to select "SYSTEM>password change>system log", to view the log and set up the log server. the following picture:

Figure 4-155 System log

System Settings	System Restart	Password	EEE Enable	SSH Login	Telnet Login	System Log		
Log Config								
Log Switch:	Open							
Server IP:								
Send Log Level:	Informational(6) V							
Save settings								
Current Log Information								
Keyword Search Clear Syslog								
Syslog logging: envel informational, 2 messages logged Monitor logging: level informational, 0 messages logged Buffer logging: level informational, 2 messages logged Timestamp log messages: datelime Sequence-number log messages: disable Sysname log messages: disable Trap logging: level informational, 2 message lines logged, 0 fail Log Buffer (Total 16384 Bytes): Jan 01 00:00:22 %PORTMANAGE-Notifications-UPDOWN: interface gigabitethernet 5, changed state to up Jan 01 00:00:30 %COMMON-Informational-SYSTEM-REBOOT: system cold reboot								

[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】

Step 1 The error log information in 192.168.1.110 pushed to the server

Fig	lure	4-1	156
110	iuie	– –	100

System Settings	System Restart Password
Log Config	
Log Switch:	Open
Server IP:	192. 168. 1. 110
Send Log Level:	Informational(6)
(Save settings)	

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

Figure 4-157							
current log information							
key ac clear log							
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: subnet-vlan enable Jan 01 00:00:22 %CLI-Errors-CLIERRINFO: CLI load config excute cmd error: subnet-vlan enable							

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

4.12.3 System upgrade

In the navigation bar to select "SYSTEM>system upgrade", Optional upgrade file to upgrade. The following picture.

System Upgrade				
Current Software Version:	V103SP2D180118			
File Name:		浏览	Start Upgrade	

[Instruction]

<u>Step 1</u> Please confirm that the upgraded version of the same model and the same model.

Step 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!

4.12.4 Config management

4.12.4.1 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:

Figure 4-159

Import/Export Config Restore Config Factory Reset								
how Current Config Export Config								
Backup OImport Configuration File Name:conf								
Confirm Backup								
Backup File List	Backup File List							
Name	Size	Time Stamp						
2345.conf	2.19K	03:05:51 2000-01-01						

[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】

<u>Step 1</u> In the configuration first save the page, click save configuration to save the current configuration, then export the configuration.

Figure 4-160 Configuration example I

Import/Export Config Restore Config Factory Reset									
Show Current Config Export Config									
O Backup Import Configuration									
Do not refresh or close the page during the import Prompr: After the introduction of configuration, to enable the new configuration, please in the	Do not refresh or close the page during the import Prompr: After the introduction of configuration, to enable the new configuration, please in this page Restart device Otherwise configuration does not take effect								
File Name: 潮览 Import configuration	File Name: 浏览 Import configuration								
Backup File List									
Name	Size	Time Stamp							
2345.conf	2.19К	03:05:51 2000-01-01							

你想怎么处理 switch.conf? 发件人: 192.168.1.110	打开	保存	取消	×

<u>Step 2</u> Import configuration.

Import/Export Config Restore Co	n 后。 打开	n Deer	•			
Show Current Config Export Config	← → * ↑	> 此	(电脑 > 桌面)		∨ ひ 搜	索"
O Backup Import Configuration	组织 ▼ 新建	文件夹				
Do not refresh or close the page during the import Prompr: After the introduction of configuration, to	🔹 📌 快速访问	^	名称	1	廖改日期	
The Marcola Mar	■ 桌面	*	FR-S3010PEGMF-G 用户	□手册 (大华客… 2	2018/4/21星	期
File Name:浏览	, ■ == == == == == == == == == == == = = =	*	截图	2	2018/4/21星	期
			用户手册	2	2018/4/20星	期
Backup File List	🔮 文档	*	🔂 1	2	2018/4/19 星	期
	▶ 图片	*	🥵 360安全浏览器	2	2018/1/30星	期
Name	File		🔒 360安全卫士	2	2018/1/30星	期
2045	FR-S3010F	PEGIN	💦 360软件管家	2	2018/4/21星	期
2345.conf			🗾 360桌面助手	2	2018/1/31星	期
	截图		Adobe Illustrator CS4	精简版 2	2018/4/18 星	期
				/c/ nto	0010/1/01 日	ĦĦ
		*				
		文件(봅(N):		~ 所	行 有3
						打

Figure 4-161 Configuration example II

Figure 4-162 Configuration example III

Import/Export Config Restore Config Factory Reset				
Show Current Config Export Config				
O Backup Import Configuration				
Do not refresh or close the page during the import Prompr: After the introduction of configuration, to enable the new configuration, please in this page (Restart device) Otherwise configuration does not take effect				
File Name: NMC Import configuration				
Backup File List				
Name Size Time Stamp				
2345.conf 2.19K 03.05.51 2000-01-01				

Step 3 Backup.

Figure 4-163 Configuration example IV

Import/Export Config Restore Config Factory Reset	
Show Current Config Export Config	
Backup Import Configuration	
File Name: 123456 .conf	
Confirm Backup	

4.12.4.2 Restore Config

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

Figure 4-164 Restore Config

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

[Instruction]

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

【Configuration Example】

Such as: restore backup.

Figure 4-165 Configuration example

Import/Export Config Factory Reset				
	Name	Size	Time Stamp	
۲	2345.conf	2.19K	03:05:51 2000-01-01	
0	123456.conf	1.99K	02:35:53 2000-01-01	

4.12.4.3 Factory Reset

In the navigation bar to select "SYSTEM>config management> Factory configura", Can export the current configuration and restore factory configuration .the following picture: Figure 4-166 Factory reset

Import/Export Config	Restore Config	Factory Reset	
Export current config Restore	to factory		

[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.

Figure 4-167 Configuration example

	Import/Export Config	Restore Config	Factory Reset	
<	Export current config Restore to factory			

4.12.5 Config save

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

Figure 4-168 Config save

Save Settings			
[Instruction]			

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

【Configuration Example】

Such as: click "save settings" button.

Figure 4-169 Configuration example



4.12.6 Administrator privileges

In the navigation bar to select "**SYSTEM**>administrator privileges", Configurable ordinary users. The following picture.

Figure 4-170 Administrator settings

Administrator Settings	
Password type: Encrypted passwort V	
User Name: *	
New Password: *	
Confirm Password:	
Add User	
User List	
User Name	Edit / Delete
user	
admin	Ø
	First Back [1] Next Last 1 / 1 Pag

[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, can add up to five users. Ordinary users can only access information system home page.

【Configuration Example】

Such as:

Figure 4-171 Configuration example

Administrator Settings		
Password type:	Encrypted passworc 🗸	
User Name:	1234	¢r
New Password:	••••	*
Confirm		
Password:	••••	*
Add User		-

4.12.7 Info collect

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

Figure 4-172 Info collect



[Instruction]

Collect useful infomation, it may take a few moment.

【Configuration Example】

Such as: click on "collect" button.

Appendix 1 Technical Specifications

The abbreviations in this glossary are related to the Manual.

Hardware Specifications				
Standards and Protocols		IEEE 802.3i, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3x, IEEE 802.3z, IEEE802.1Q , IEEE802.1p, IEEE802.3af, IEEE802.3at		
Interface		8 x 10/100/1000Mbps Auto-Negotiation ports 2 x 100/1000Mbps SFP port 1 x Console port 1 x AC Power Connector		
Network M	ledia	10BASE-T: UTP category 3,4 cable (maximum 100m) 100BASE-TX: UTP category 5,5e cable (maximum 100m) 1000Base-T: UTP category 5, 5e,6 cable (maximum 100m) 1000Base-X:MMF,SMF		
Transfer M	lethod	Store-and-Forward		
MAC Addr	ess Table	8K		
Switching	Capacity	20Gbps		
Packet Forwarding Rate		14.88Mbps		
Packet Bu	ffer	4.1Mbit		
Jumbo Fra	ame	10kBytes		
PoE Ports	(RJ45)	8* PoE ports compliant with 802.3at/af		
Power Pin Assignme		1/2(+),3/6(-)		
PoE Budg	et	140W		
Indicator	Per Device	Power(Green), System(Green)		
s Per Port		Link/Act/Speed: Green(1000Mbps)/Amber(100/10Mbps) ,PoE(Orange)		
Dimensions (LxWxH)		340*200*44mm		
		Operating Temperature: -0°C - 45°C		
Environment		Storage Temperature: -40°C - 70°C Operating Humidity: 5%~95% non-condensing Storage humidity: 5%~95% non-condensing		

Software Specification			
Basic function	Three layers of functional	The security policy	
Ethernet Setup	 The ARP deception, the network cheating 	 ACE capacity 	

Software Specification				
STP/RSTP/MSTP	• Filtering the IP port	ACL		
Storm-control	• Static binding IP and	• QoS		
Port Monitor	MACArp trust port	• DAI		
 Port rate-limit 	 Static routing capacity 			
MAC filtering				
	Ping and Traceroute			
VLAN	Safety features	Application protocol		
Port based VLAN	Radius	DHCP Relay		
• 802.1Q VLAN	• Tacacs+	DHCP snooping		
	 Preventing DOS attacks 	DHCP Client		
	• dot1x	• FTP/TFTP		
	 The gateway ARP deception 			
Management	Other function	POE Management		
HTTP WEB	• LLDP	POE Status		
Telnet	IGMP Snooping	Power supply		
• SSH	• SNMPV1,V2c,V3	management mode(auto/energy/stati		
Console	• RMON (1,2,3,9)	c)		
		• The port priority		