

Models: S5860-20SQ; S5860-24XB-U



CONFIGURATION GUIDE

Contents

Web-Based Configuration 1
1.1 Overview 1
1.2 Application 1
1.2.1 Web-based Management 1
1.3 Web Management System
1.3.1 Quick Settings 6
1.3.2 Monitor 9
1.3.3 Configuration 13
1.3.4 Diagnosis 65
1.3.5 Maintain 68
1.3.6 Other Functions 72
1.4 Open WEB Server 75

Web-Based Configuration

1.1 Overview

A user accesses the Web-based management system of a switch by using a browser (for example, IE browser) to manage the switch. Web-based management involves two parts: Web server and Web client. A Web server is integrated onto a device to receive and process requests sent from a client (for example, read a Web file or execute a command request) and returns the processing result to the client. Generally, a Web client refers to a Web browser, for example, IE browser.

At present, this document is only applicable to S5860 series switches.

Note that the web cannot be mixed with the device side. After the device side is configured, the web needs to be refreshed, for example, press F5 to refresh.

1.2 Application

Application	Description
Web-based Management management	After finishing relevant configuration, a user can access the Web-based system through a browser.

1.2.1 Web-based

Management Scenario

As shown in the following figure, a user can access an access switch or aggregation switch through a browser on a PC to manage and configure the device.



NOTE: A user can access the Web-based management system of the switch in the red rectangle if this switch can be pinged from the PC.

Function Deployment

Configuration Environment Requirements

Requirements for Client

An administrator logs in to the Web-based management system by using the Web browser on a client to manage the switch. Generally, a client refers to a PC. It may also be other mobile terminal devices, for example, a laptop.

Browser: IE7.0, IE8.0, IE9.0, IE10.0, IE11.0, Google chrome, Firefox, and some IE kernel-based browsers (for example, 360 security browser) are all supported. Exceptions such as messy code and format error may occur when other browsers are used.

Resolution: It is recommended that the resolution be set to 1024*768, 1280*1024, or 1920*1080. Exceptions such as font alignment error and format error may occur when other resolutions are selected.

WEB configuration and command line configuration can be carried out at the same time. It should be noted that after the

command line configuration is completed, it is best to enter the "write" command to save the configuration; when you open the WEB page, please refresh the opened page. So as to ensure the synchronization of WEB configuration and command line configuration.

🖈 Login

6

You can type http://X.X.X.X (management IP address) in the address bar of a browser and press Enter to access the login page, as shown in the following figure.

	6	FS
WELCOME TO FS SWITCH		
Username	Terring Start	
$\mathcal{P}_{\mathbf{F}}$ Please enter the username		
Password		
Please enter the password		
Login		

After typing the username and password, click Login. The following table lists the default username and password.

Permission Description

admin / admin

Super administrator who possesses all permissions.

NOTE: The default username and password are not displayed by running the show running-config command.

When logging in with the default user name and password, the system will ask to change the password for security reasons;

After passing authentication, the home page of the Web-based management platform is displayed, as shown in the following figure.

S 55860-205Q	Monitoring > SWITCH Overview				Q Enter a search term	크는 Config Wizard 👌 admin 🗸
avorites 2						
Ionitoring >	Device Details			~	Device Usage	(Å)
onfig >		SN G1PC135000034 MAC Address 649d.99d0.70da	Booted on 2022-07-18 16:30:49 System Time 2022-07-21 12:28:53		CPU Usage	9.9 %
iagnosis > Iaintenance >	Model\$5860-205Q	Firmware Version SS860_FSOS 12.5(4)B0151, Release(09182801) Hardware Version 1.00	Uptime 2 d 19 h 58 min 03 s		Memory Usage	56.2%
	Device Port			S	elected 🔲 AG Port 📕 Up 🔳 Shi	utdown 🛛 VSL Port 🔲 BFD Port.
	FS NAME OF THE OWNER OWNE	0 4 7 4 7 0 4 7 4 7 4 7 4 7 4 7 4 7 4 7	17 A T B A T B B A T B	21 A ¥ 22 22 A ¥ 34 1 2 3 A ¥ A ¥ 256 400	4 40G Breakest 25 26	<u>55840 - 2050</u>
	Port Role (1) Trunk Port (2) Routed	Port			Copper 📕 Fit	er 40Gb 40Gb(Splited)
	Kbps 120 60 40 0					Tx Traffic Rx Traffic Time
	Ton5 Ports by Bandwidth Lis	1227:30 12:24	:00	12:28:30		12:29:00 12:29:07
	Port Input Rate	Outp	ut Rate		Status(Port real speed)	
			No Data Found	er Bosonaul		
			n wzooz-zozz rocowine. Ali Right	ur murur PEU.		

NOTE: For details about the Web page, see Web Management System.

1.3 Web Management System

Basic Concepts

Various Icons and Buttons on the GUI

lcon/Button	Note
	Edit, click this icon to edit the currently selected record
Delete	delete
	Status switch icon
	Optional port, click or frame selection can make the port become "selected port"
	Shutdown port

•	Select the port
0	Aggregation port, the number in the port represents the aggregation port number
0	Trunk port is reflected in the panel of VLAN management/VLAN setting page
•	The port is powered on
<u>v</u>	VSL port
В	BFD port, withdraw cash in the panel of the switch overview page
	40G port
-63	40G split port
Save	Save button to submit and save the entered information
+	Add settings
	Delete settings
*	Required item, if the symbol behind the input box indicates that the option is required
0	Description flag
0	Attention sign
0	Fail

System Operations

1) Standalone Device Panel

1▲▼2	3▲▼4	5▲▼6	7▲▼8	9▲▼10	11 ▲ ▼12 1	13▲▼14	15▲▼16	17▲▼1	8 19▲▼20	21▲▼	22 23▲▼24	25▲▼2	6			
A.Y.	A 7	A. Y	A.Y.	**	**	A.Y	A.¥	A.Y	A Y	A. 7	A Y	* * *				

≓ Panel operation

You can click the <port> on the panel or drag the mouse to select multiple <ports> to make the <port> become <selected port>, and then set the selected <port>, such as adding port description, port mirroring And port speed limit, etc.

Device panel selected port diagram

Feature

The following table describes the functions in the secondary menu on the left of the Web page.

Feature	Description
Quick Configuration	Simple network construction can be carried out on the equipment
Switch Overview	You can view port information and device overview
Spanning Tree State	Can view spanning tree status and port role information
RLDP Status	You can view the RLDP switch and the port information that enables RLDP detection
DHCP Client List	You can view the addresses assigned by the switch address pool
DHCP Server Status	Can view DHCP server and configured address pool
VSU Status	Only exists when the device is in stacking mode, you can view the topology diagram that composes the stacking
VLAN Management	You can set VLAN and Trunk port
Port Management	You can perform basic settings on the port, and set port aggregation, port mirroring, and port speed limit
Routing Settings	You can set up routing
DHCP Server	Can set up DHCP, static address assignment and client list
VRRP	Can set up VRRP
MAC Address	Can carry on static address setting and filtering address setting
VSU Configuration	The device can be configured for stand-alone and stacking mode conversion
SpanningTreeProtocol	You can set the global basic information of spanning tree and spanning tree port settings
RLDP settings	RLDP global configuration and port configuration
ACL	You can set the ACL list, ACL time, and apply ACL.
Port protection	Port protection can be set.
Port security	Port security settings and security binding can be performed.
Storm control	Can carry out storm control.
DHCP Snooping	You can set up DHCP Snooping.
Anti-ARP attack	You can set anti-gateway ARP spoofing, ARP inspection settings, DAI settings and ARP table entries.
IP Source Guard	You can set the interface and bind users.
NFPP	You can view NFPP anti-attack related content.
IGMP Snooping	You can set IGMP Snooping.
QOS	You can perform classification settings, policy settings, and stream settings.

DHCP relay	You can set up DHCP relay.
Online real-name authentication	Can carry out external web authentication and advanced configuration.
ping detection	Connectivity test for IP address or domain name
tracert detection	Tracert detection of IP address or domain name
One-click collection	Collect information on the device with one click
System log	You can set the syslog log server and view the system log.
System log monitoring	Log can be queried according to grade and module name
upgrade	Can be upgraded locally.
Reboot	Restart the device
Configuration management	Can perform configuration backup, restore factory settings and system character set settings
system time	Revise the system time
Log server	Set whether the log function is enabled on the device
DNS	Can set DNS
WEB configuration management	You can set the administrator password, basic configuration
Telnet	Set Telnet and SSH function and password
SNMP	Can set V2 and V3 version

1.3.1 Quick Settings

1	Device — 2 Terminal Port — 3 Br	idge Port — (4)	Routed Port — 5 Gateway — 6 Security — 7 Confirm	
Config Mode	◯ Layer 2			
Management Port	MGMT Port O MGMT VLAN			
Management Port	Mgmt 1/0 ~			
P Address *	10.36.1.111	Submask *	255.255.255.0	
Gateway *	10.36.1.254	DNS Server		
Reset Time	PC Time Custom			
Time Zone	UTC+8(Beijing, CCT)	Charset *	UTF-8 ~	

1. Equipment management

Configure the management VLAN ID, IP address, subnet mask, default gateway and DNS server settings, click "Next" to continue the configuration.

2. Terminal interface

onfig Wizard				
Device	2 Terminal Port	- 3 Bridge Port - 4	Bouted Port — 5 Gateway — 6 Security –	7 Confirm
Note: Terminals include PCs	, printers, monitors and APs.			
rminal Port				
rminal Port + Add				
rminal Port + Add Port ID	Port Status	VLAN	Description	Action

3. Connect switch interface

	vice — 🗸 Terminal Port — 3 Bridge Port — 4 Routed Port — 5 Gateway — 6 Security –	— 7 Confirm
Note: The bridge por	efers to the port used to access the switch.	X
ridge Port		
ridge Port + Add		
ridge Port + Add Port ID	Port Status Allowed VLAN Native VLAN Description	Actio

4. Router interface

Config Wizard					×
C Der	vice — 🗸 Te	erminal Port - 🖌 Bridge Po	rt — (4) Routed Port — (5) C	Sateway — 6 Security — 7 0	Confirm
Note: The routed port s	erves layer 3 interconnec	tion.			×
louted Port					
+ Add					
Port ID	Port Status	IPv4 Address	Submask:	Description	Action

5. Downlink port configuration

After the configuration is successful, the quick configuration pop-up window will automatically close. If you modify the managed IP address of the device, follow the prompts to choose whether to adjust to the new management address.

Lonng Wizard				
) Terminal Port — 🖉 Bi	ridge Port — 😧 Routed Port —	5 Gateway — 6 Security — 7 Confirm	
Note: Gateway is a link between two VLAN	vs at layer 3. It is recommended to config	ure a gateway for each VLAN.		
Gateway				
+ Add				
	Gateway	IPv4 Address	Submask:	Actio
Allowed VLAN	Gateway			

6. Security configuration

Johng VVIZa	d	
(Device — 🗘 Terminal Port — 🗘 Bridge Port — 🔷 Routed Port — 🗘 Gateway — 🌀 Security — 🤈 Confirm	
Note: Defaul	routing Is enabled by default. If there are multiple routed ports, priority will be assigned to these ports based on record ID.	×
• Hotel Delia		
• Hotel Belle		
Default Routing		
Default Routing		
Default Routing STP Port Fast		

7. Save configuration

After the configuration is successful, the quick configuration pop-up window will automatically close. If you modify the managed IP address of the device, follow the prompts to choose whether to adjust to the new management address.

1.3.2 Monitor

Through the first level menu "Commonly used", you can enter the second level menu. Including homepage, VLAN management, port management, POE settings, system restart.

Switch Overview

"Switch Overview" allows you to view the basic information of the device at a glance, such as device MAC address, device model, system running time, version information, device cpu and memory, various status of device ports, traffic trends of device interfaces and interface information Bandwidth utilization.

Stand-alone scene

Stacking scene

			Domain ID 100(100)			
			1(Active)			
BFD Set	tings					
Note:	BFD requires a direct link between th	vo devices and the ports on both end	s must be physical routing ports.			×
BFD Status BFD I Select /	CEnabled Device1 Slott	Configure BFD 9 55860-205Q t			Selected 🗉 AG Port 🔳 up	shutdown
1.	¥2 3▲¥4 5▲¥6 7▲¥8 5	AV10 11 AV12 13 AV14 15 AV1	5 17AV18 19AV20 21AV22 23AV	24 25▲▼26		
BFD Port Note: Click	Enabled Senabled. Port and hold the left button as you of and hold the left button as you of	is down. rag the pointer across the section	in to select multiple ports.	Сорре	r Fiber 40Gb 🞫 40	Gb(Splited)
e Details				^	Device Usage	
de \$5860-20\$Q	SN G1PC13S000034 MAC Address 649d.99 Firmware Version 5586 Release(09182801)	d0.70da 0_FSOS 12.5(4)B0151,	Booted on 2022-07-18 16:30:49 System Time 2022-07-22 14:56:38 Uptime 3 d 22 h 25 min 50 s		CPU Usage Memory Usage	8.3 %
	Hardware Version 1.00					
			Sele	ected 🔢 AG Po	rt 📕 Up 📕 Shutdown 💟 V	/SL Port 🔲 BFD Po
Port						

TOP5 interface bandwidth utilization, click on the "More" pop-up page

50			\wedge	
0		14:55:47		
0		No Data Available		
D	:55:30	14:56:00	14:56:30	14:57:00 14:57:1
p5 Ports by Ba	ndwidth Usage			More
Port Inp	ut Rate	Output Rate	Status	(Port real speed)

Anti-loop Monitoring

Anti-loop monitoring uses spanning tree status and RLDP status to monitor the loop status.

Spanning Tree State

Show spanning tree status and mode, port role and STP usage status

RLDP Status

Display RLDP status, port application mode, violation handling method and status.

DHCP

DHCP monitoring is monitored in two dimensions: DHCP service status and DHCP client list.

DHCP Client List

Display the users assigned by the address pool on the switch.

Bind MAC to Dynam	nic IP		IP-Based	V Q Search
□ IP	MAC	Lease Time	Allocation Type	Action

DHCP Server Status

Display the status of the DHCP server and the usage of the address pool.

1.3.3 Configuration

Through the first level menu "configuration", you can enter the second level menu, network, advanced configuration, security, advanced configuration.

Network

VLAN Management

The VLAN management page contains two parts: "VLAN Settings" and "Trunk Port Settings".

☆ VLAN settings

1. Add VLAN

Add VEAN	Add VLAN	×
	VLAN ID + Range (1-4094) VLAN Name	
	Select Port	
1	☑ Select All \$\frac{12}{16}\$ Invert Imes Deselect	Selected AG Port Trunk Port
7 2 item(s)	1472 3474 5476 7478 94710 114712 134714 154716 174718 194720 214722 23474	25.4*26
	Note: Click and hold the left button as you drag the pointer across the section to select multiple ports.	Fiber 40Gb - 40Gb(Splited)

To set a VLAN, you must fill in the VLAN ID, and other information is optional. After clicking "Finish Configuration" and prompting "Setup successful", it will be displayed in the VLAN list.

2. Edit VLAN

+ Add VLAN + Batch Add VLAN	Edit VLAN	×	
VLANID +	VLAN ID * 1		Action
1	VLAN Name VLAN0001	,	21-
7			C D
2 item(s)			
		Cancel Save	

Click the <Edit> button under the operation column of the last column of "VLAN List", the page will display the VLAN information. After editing the information, click <Complete Configuration> to prompt "Setup Successful".

3. Delete VLAN

	VI AN Name	VI AN Status	Port	Action
	Note	× LAN Status	Te1/0/4-8,Te1/0/13-18,TF1/0/	/21-
1	V Are you sure you	want to delete the VLAN?	24,Fo1/0/25-26	Ø
	• • • • • • • • • • • • • • • • • • • •		AG: Ag2	
7	v		Te1/0/5-6,Te1/0/17	C d
al 2 item(s)	Items per page:	Cancel		

1) Select multiple records in "VLAN List" and click "Delete Selected VLAN" to delete data in batches.

2) Click the <Delete> icon under the operation column of the last column of "VLAN List", and prompt "OK to delete the selected vlan", click OK and prompt "Delete successfully" to complete the deletion. VLAN 1 is the default VLAN and cannot be deleted.

VLAN1 is the default VLAN, the page only provides modification functions and cannot be deleted.

$\stackrel{\wedge}{\mathcal{T}}$ Trunk port settings

1. Add Trunk port

6

VLAN Settings	Trunk Port							
() Note: If a port allow	rs multiple VLAN packets to go through, configure i	as a trunk port. It is recommended t	to configure the port connect	ed to the network device	e as a trunk port.			×
Select All X Der Te1/0/5	select All 🔋 Batch Delete Te1/0/6							
Native VLAN *								
Allowed VLAN 1	-4094							
Select Port	vert 🗵 Deselect				Selected	AG Port	Up Shutdow	n 🛛 VSL P
1 • • 2 3 • • • • • • • • • • • • • • • •	54¥6 74¥8 94¥10 114¥12 134¥1 V V X X X X X X X X X X X X X X X X X X	15 A ¥16 17 A ¥18 19 A ¥20	21 • • 22 23 • • 24	25▲▼26				
Note: Click and hold the	e left button as you drag the pointer across t	e section to select multiple po	rts.		Copper	Fiber	40Gb -1	40Gb(Splited)
Edit	Cancel							

Select the panel port, fill in the Native Vlan and allowed VLAN (such as 3-5, 8, 10), click "Save Settings" to prompt "Setup Successful" to complete the adding operation, the added Trunk will be displayed in the Trunk Port List.

2. Edit Trunk Port

VLAN Settings	Trunk Port					
Note: If a port allow:	s multiple VLAN packets to go through, configure it as a tr	unk port. It is recommended to configure the po	t connected to the network device as	a trunk port.		×
Select All 🛛 Des	elect All 🗻 Batch Delete					
Te1/0/5	Te1/0/6 Te1/0/17					
Native VLAN * 1						
Allowed VLAN 1	4094					
Select Port						
🔄 Select All 🛛 😨 Inv	ert 🗵 Deselect			Selected II AG I	Port 📕 Up 📕 Shutdown	VSL Port
1 * 2 3 * 4	54¥6 74¥8 94¥10 114¥12 134¥14 154¥ V V V AV AV AV AV AV AV	16 17 * ¥18 19 * ¥20 21 * ¥22 23	▲▼24 25▲▼26			
Note: Click and hold the	left button as you drag the pointer across the sec	ion to select multiple ports.		Copper F	iber 🚺 40Gb 🧮 40	IGb(Splited)
Edit	Cancel					

Click on a Trunk port in the "Trunk Port List", the page will display the Trunk port information, after editing and modifying the information, click <Edit Settings> to prompt "Setup successful".

3. Delete Trunk Port

Select All 🗵 Deselect All 🔯 Batch Delete				
Te1/0/5 Te1/0/6 Te1/0/17				
ative VLAN * 1	Note	×		
lowed VLAN 1-4094	 Are you sure you want to de 	elete the trunk port?		
lect Port J Select All 답 invert 또 Deselect		Cancel	Selected 🔲 AG Port 📕 Up 🔳 St	nutdown 🔲 VSL
1 ** 2 3 ** 4 5 ** 6 7 ** 8 9 ** 10 11 ** V V ** ** ** ** ** **	2 13 A ¥14 15 A ¥16 17 A ¥18 19 A ¥	20 21▲▼22 23▲▼24 25▲▼26		
ote: Click and hold the left button as you drag the points	er across the section to select multiple	ports.	Copper 📰 Fiber 🔜 40Gb	40Gb(Splited
Edit Cancel				

In the "Trunk Port List", move the mouse to a Trunk port, select the <Delete> icon, and prompt "Are you sure you want to delete this Trunk port?", click OK and prompt "Delete successfully" to complete the deletion.

4. Delete Trunk Ports in batch

Note: If a port allows multiple VLAN packets to go through, c	onfigure it as a trunk port. It is recomn	nended to configure the port connected	to the network device as	a trunk port.	×
Select All Deselect All Batch Delete Te1/0/5 Te1/0/6 Te1/0/17					
Native VLAN * 1	Note		×		
Allowed VLAN 1-4094	 Are you sure you want t 	o delete the trunk port?			
Select Port 데 Select All 답 Invert 또 Deselect	[Cancel Confirm	n	Selected II AG Port	Up 📕 Shutdown 🗳 VSL P
14¥2 34¥4 54¥6 74¥8 94¥10 114¥12 4¥ 4¥ 4¥ 4¥ 4¥ 4¥ 4¥ 4¥ 4¥ 4¥ 4¥	134¥14 154¥16 174¥18 1	94720 214722 234724	25▲▼26		
Note: Click and hold the left button as you drag the pointer	across the section to select mult	iple ports.		Copper Fiber	40Gb 40Gb(Splited)
Edit Cancel					

Select the Trunk port to be deleted in the "Trunk Port List", select the <Batch Delete> icon, and prompt "Are you sure you want to delete the Trunk Port?", click OK and prompt "Delete successfully" to complete the deletion.

Port Management

"Port Management" can perform basic port settings, port aggregation, port mirroring, and port speed limit settings.

Port Settings	Aggregate port	Port Mirroring	Rate Limiting				
+ Batch Add	+ Add SVI						
L3 Port							
Port	Status	IP	Mask		IPv6	Description	Ac
Te1/0/1	Up						C
Te1/0/2	Up						C
Te1/0/3	Up						2
Te1/0/19	Up						e
Te1/0/20	Up						Z
L2 Port							
L2 Port Port	Status	Port Type	Access VLAN	Native VLAN	Permit VLAN	Description	Actio
L2 Port Port Te1/0/4	Status Up	Port Type Access	Access VLAN	Native VLAN	Permit VLAN	Description	Actio
L2 Port Port Te1/0/4 Te1/0/5	Status Up Up	Port Type Access Trunk	Access VLAN 1 1	Native VLAN 1	Permit VLAN 1-4094	Description	Actio
L2 Port Port Te1/0/4 Te1/0/5 Te1/0/6	Status Up Up Up	Port Type Access Trunk Trunk	Access VLAN 1 1	Native VLAN 1 1 1	Permit VLAN 1-4094 1-4094	Description	Actio
L2 Port Port Te1/0/4 Te1/0/5 Te1/0/6 Te1/0/7	Status Up Up Up	Port Type Access Trunk Trunk Access	Access VLAN 1 1 1 1	Native VLAN 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Permit VLAN 1-4094 1-4094	Description	Actio
L2 Port Port Te1/0/4 Te1/0/5 Te1/0/7 Te1/0/7	Status Up Up Up Up	Port Type Access Trunk Trunk Access Access	Access VLAN 1 1 1 1 1 1 1	Native VLAN 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Permit VLAN 1-4094 1-4094	Description	Action
L2 Port Port Te1/0/5 Te1/0/6 Te1/0/7 Te1/0/8 Te1/0/9	Status Up Up Up Up Up Up	Port Type Access Trunk Trunk Access Access	Access VLAN 1 1 1 1 1 1	Native VLAN 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Permit VLAN 1-4094 1-4094	Description	Action C C C C C
L2 Port Port Te1/0/6 Te1/0/6 Te1/0/7 Te1/0/9 Te1/0/9	Status Up Up Up Up Up Up	Port Type Access Trunk Trunk Access Access	Access VLAN 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Native VLAN 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Permit VLAN 1-4094 1-4094	Description	Activ
L2 Port Port Te1/0/4 Te1/0/5 Te1/0/7 Te1/0/8 Te1/0/10 Te1/0/10	Status Up Up Up Up Up Up Up	Port Type Access Trunk Trunk Access Access	Access VLAN 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Native VLAN 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Permit VLAN 1-4094 1-4094	Description	Activ
L2 Port Port Te1/0/4 Te1/0/7 Te1/0/7 Te1/0/7 Te1/0/1 Te1/0/11 Te1/0/11	Status Up Up Up Up Up Up Up Up	Port Type Access Trunk Trunk Access Access	Access VLAN 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Native VLAN 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Permit VLAN 1-4094 1-4094	Description	Activ

1. Set Ports in batch

t Settings	Aggregate port	Port Mirroring	Rate Limiting		
Batch A	٨dd				
Status	Кеер	~	Description		
Port Mode	Access Port	~	Access VLAN *	Range (1-4094)	
Advanced	Settings				
Select Port	t :All 🐺 invert 💌 Desel	ect			Selected 💵 AG P
1	xv2 3 x v4 5 x v6 7 x v8	9×10 11×12 13×14 15×16	17 × 18 19 × 20 21 × 22 2:	▲▼24 25▲¥26	
Note: Click	< and hold the left button as you	drag the pointer across the section to a	elect multiple ports.	in Coppe	r Fiber 40Gb 💷 40Gb(Splited)
					Cancel Save
Te1/0/6	Up	Trunk	1 1	1-4094	Cancel Save

First select the port that needs to be configured, and then select the port status, speed, mode, etc., among which "no modification" means to keep the original configuration. In batch setting, you can set only one or two items in batch by setting "no modification".

2. Edit port

Port Te1/0/	1				>
Status	Up	~	Description		
Port Mode	L3 Port	~	IPv4 *		
Mask *			IPv6/Mask	/	
Medium Type	Fiber				
Advanced Setting	5				

In the "Port List", the <Edit> icon under the operation bar in the last column will display the information of the port on the page. After editing the information, click <Complete Configuration> to prompt "Setup Successful".

☆ Port aggregation

1. Add polymerization port

Enter the aggregate port number and select the member port and press "Add Setting", and the message "Setup successful" is displayed to complete the adding operation of the aggregate port. After the addition is successful, the panel will display <Aggregation Port>.

2. Edit aggregation port

AG2				
Aggregate Port ID *	Range: 1-128			
Port Type	L2 Port(Switching Port) U L3 Interfac	e(Routed Interface)		
Open LACP	🔿 Yes (No			
Select Port				
Select Port	Invert 🗶 Deselect		Selected	🛙 AG Port 📕 Up 📕 Shutdown 🗳 VSL P
Select Port	Invert 🔄 Deselect	▼16 17▲▼18 19▲▼20 21▲▼22 23▲▼	Selected 24 25▲▼26	AG Port Up Shutdown VSL P
Select Port	Invert Deselect	×1 6 17 ×1 8 19 ×7 20 21 ×7 2 23 ×7	Selected 25▲▼26	AG Port Up Shutdown VSL P
Select Port	Invert Deselect	×1 6 17 × ¥18 19 × ¥20 21 × ¥2 23 × ¥	24 25▲▼26	🔲 AG Port 📕 Up 📓 Shutdown 🔳 VSL P

The aggregation port displayed on the panel is <unselectable port>. If you want to edit and modify them, you can click an aggregation port in the "Port Aggregation List", then the "Member Port" will become selected, click on the port You can uncheck it, and then click "Edit Settings" to modify the aggregation port.

3. Delete aggregation port

52	Note	×		
gregate Port ID * Range: 1-128	 Are you sure you want to de 	lete the selected aggregate port(s)?		
rt Type	rt)			
ien LACP 🔷 Yes 💿 No		Cancel Confirm		
ect Port				
Select All 📫 Invert 🗵 Deselect			Selected 🚺 AG	Port 📕 Up 🔳 Shutdown 🔲 VSL P
ect Port Select All 🛗 Invert 🗵 Deselect			Selected D AG	Port 📕 Up 📕 Shutdoy

In the "Port Aggregation List", move the mouse to the aggregation port, click the <Delete> icon, and a confirmation box will prompt whether to delete the aggregation port. Click OK to delete the aggregation port. After deletion, the panel will be deleted. Aggregate port> becomes <optional port>.

4. Batch delete aggregation ports

AG2	Note	×		
Aggregate Port ID * Range: 1-12	8 O Are you sure you want	to delete the selected aggregate port(s)?		
Port Type	(Switching Port)			
Open LACP O Yes	No	Cancel Confirm		
Select Port				
🗐 Select All 🔡 Invert 🗵	Deselect		Selected 🔲 AG Port 📕 Up	Shutdown SVSL

In the "Port Aggregation List", select the aggregation port to be deleted, click the <Batch Delete> icon, a confirmation box will be prompted whether to delete the aggregation port, click OK to delete the aggregation port, and the panel will be deleted after deletion The <aggregation port> becomes <optional port>.

Ports with ARP inspection function enabled, ports for ARP spoofing of important devices, ports with MAC VLAN function and monitoring ports in port mirroring cannot be added to the aggregation, and the panel displays as <unavailable port>, put the mouse on <unavailable port> It will prompt that these functions are enabled on the port and cannot be selected.

\bigstar Port mirroring

Port Settings	Aggregate port	Port Mirroring	Rate Limiting						
 Note: Port mirroring is A source port car 	the capability to send a copy of net not be a destination port.	twork packets seen on the source	port to the destination port for a	alysis by a networ	k analyzer. Traffic on	multiple source ports can be	e mirrored to one sinj	gle destination port	
Select All 🗵 De	eselect All 🛛 🗟 Batch Delete	2							
No Data									
ession ID *	Range (1-4)								
Ionitor Packets	All Packets	×							
elect Source Port 🥥	Device1 Slot0 S586	0-205Q v						Selected	d 🔳 Ad
1472 3474	54¥6 74¥8 94¥10 1	14 12 134 14 154 16	17 × 18 19 × 20 21 × 1	22 23▲▼24	25▲▼26				
ote: Click and hold th	e left button as you drag the p	pointer across the section to	select multiple ports.			Сорр	er Fiber	40Gb 44)Gb(Splite
elect Destination Por	Device1 Slot0 S586	0-205Q v						Selected	d 🔳 A
1472 3474	54¥6 74¥8 94¥10 1		17A¥18 19A¥20 21A¥	22 23 • ¥24	25▲▼26				
						Сорр	er 📕 Fiber	40Gb 11 44)Gb(Splite

The port mirroring page is initialized to edit status, because multiple mirroring ports are allowed to be set on the web. There are two panels on the page. The port selected in the upper panel will be the source port (mirrored port, multiple selections are available), and only one port can be selected as the destination port (mirrored port) in the lower panel. After selecting or modifying the port on the panel, click the <Configuration Mirror> button to prompt "Setup successful!".

- The current port mirroring status displayed on the panel is in the editing state. After the user has modified the port, but does not want to edit it, he can click the <Refresh> button to restore the panel to display the current port mirroring configuration status.
- The member port that has been added to the aggregation port cannot be used as the destination port and source port, and the destination port and source port cannot be the same.

0

0

$\stackrel{}{\not\propto}$ Port speed limit

ort Settings	Aggregate port	Port Mirroring	Rate Limiting			
+ Batch Add	Batch Delete					
Port		Input Rate-L	mit (KBps)	Output Rate-Limit (KBps)	Action	
			-			
			Ŷ			
			No Data I	Found		

1.Add speed limit port

+ ва Е	Batch Add					×
S	Select Port 회 Select All 다 Invert 💌 De	eselect		Selected	🖬 AG Port 📕 Up 🔳 S	ihutdown 📓 VSL Port
al Olt	14¥2 34¥4 54¥6 741	▼8 9▲▼10 11▲▼12 13▲▼14 15↓ ∨ ∨ ∨ ∨ ∨ ∨	▼16 17▲▼18 19▲▼20	21 A V 22 23 A V 24 25 A V 26		
n o n Ir	Note: Click and hold the left button as input Rate-Limit Range(64-10000	you drag the pointer across the se	ction to select multiple ports.	Copper	Fiber 40Gb	40Gb(Splited)
c	Output Rate-Limit Range(64-10000	00) KBps				

To set the speed limit port, you must fill in one of the input speed limit and output speed limit. Click "Save configuration" to prompt "Set successfully" and it will be displayed in the port speed limit list.

2.Edit rate limit port

Port	PortTe1/0/7	חר ×
otal 1 item(s)	Input Rate-Limit 6000 Ite Output Rate-Limit Range(64-1000000) KBps	
	c	ancel

Click the <Edit> icon under the operation column of the last column of "Port Speed Limit List", the page will display the port speed limit information, after editing the information, click <Save Configuration> to prompt "Setup successful".

3. Delete rate limit port

Port Settings Aggregate	port Port Mirroring Rate Limi	ting	
+ Batch Add	te		
Port	Input Rate-Limit (KBps)	Output Rate-Limit (KBps)	Action
✓ Te1/0/7	Note	×	C D
iotal 1 item(s)	Items per page: O Are you sure you want to delete	the port configuration?	
	Car	Confirm	

1) Select multiple records in the "Port Rate Limit List", and click "Delete Rate Limit Ports in Batch" to delete data in batches.

2) Click the <Delete> icon under the operation column of the last column of "Port Speed Limit List", and prompt "Are you sure to delete the selected port configuration?", click OK and prompt "Delete Successful" to complete the deletion.

Routing settings

"Route Settings" can manage routing.

1.Add static route

louting	Add Static Route		×	
Note: Routing includes a primary route and backup re	ІР Туре	IPv4 IPv6		ince 1 has higher priority than the Backup Route-2. \qquad \qquad
+ Add Static Route + Add Default	Destination Subnet *			
	Subnet Mask *			
Destination Subnet Subnet	Egress Port	Please Select v		Action
	Next Hop Address *			
	Administrative Distance *	1		
al O item(s)				
		c	ancel Save	

Set static route, select IP type, destination network segment, destination network segment mask and next hop address are require fields, click "Complete configuration" and prompt "Setup successful", it will be displayed in the routing list.

2. Edit routing

Note: Routing includes a primary route	and backup re	Edit Static Route			×	nce 1 has higher priority than the E	Jackup Route-2.
+ Add Static Route + Ad	ld Default	IP Туре	● IPv4 ○ IPv6				
		Destination Subnet *	0.0.0.0				
Destination Subnet	Subne	Subnet Mask *	0.0.0.0			Act	ion
al 1 item(s)	Items per (Egress Port	Please Select	~			
		Next Hop Address *	1.1.1.1				
		Administrative Distance *	1				

Click the <Edit> icon under the operation bar in the last column of "Route List", the page will display the information of the route, after editing the information, click <Complete Configuration> to prompt "Setup successful".

3. Delete route

Destination Subnet Subset						
	ubnet Mas	Are you sure you want to delete the route?		Administrative Distance	Туре	Action
0.0.0.0 0.	.0.0.0			1	Default	0
I 1 item(s)	ns per page:	Cancel	Confirm			

1) Select multiple records in "Route List" and click "Delete Selected Route" to delete data in batches.

2) Click the <Delete> icon under the operation column of the last column of "Route List", and prompt "OK to delete?", click OK and prompt "Delete successfully" to complete the deletion.

4. Add default route

Routing	Add Default Route		×		
Note: Routing includes a primary route and backup re	ІР Туре	IPv4 IPv6		ince 1 has higher priority	r than the Backup Route-2. $ imes$
+ Add Static Route + Add Default	Egress Port	Please Select V			
	Next Hop Address *				
Destination Subnet Subnet	Administrative Distance *	1			Action
0.0.0.0 0.0.0.0				ault	c d
Total 1 item(s)					
		Cancel	Save		

Set the default route, select the IP type, the next hop address is a required field, click "complete configuration" to prompt "setup successful", it will be displayed in the routing list.

Route selection is divided into main route and backup route. When the main route fails to take effect, the backup route will be used. The backup route follows the configured priority. The priority of backup route 1 is higher than the priority of backup route 2.

DHCP server

0

"DHCP server" can perform DHCP configuration, static address assignment and client list.

$\stackrel{}{\mathcal{M}}$ DHCP configuration

Note: If you want to d	elete a static address converted	I from a dynamic address, please go to the SI	atic Address page.			
列 Bind MAC to Dyr	namic IP			IP-Based	 ✓ Q Search 	
IP		MAC	Lease Time	Allocation Type	Action	
			-			
			Y			

1.Add DHCP

DHCP Settings	Static Address	Client Display		
рнср				
+ Add DHCP	Ø Excluded Address Ra	Add DHCP	×	
Name	IP A	Pool Name *		Action
		Туре	IPv4 IPv6	
		Advanced Settings		
		Address Range *	eg:192.168.1 1 to 254	
Total O Item(s)	> Items per page: 1	Default Gateway *		1
		Lease Time *	8 Hour(s) v	
			Cancel Save	

Set the address pool name, IP allocation network segment, mask, default gateway, and lease time, and click "Complete configuration" to prompt "Setup successful", it will be displayed in the DHCP list.

2.Edit DHCP

DHCP Settings	Static Address	Client Display		
рнср				
+ Add DHCP	Excluded Address Ra	Edit DHCP	×	
□ Name	IPA	Pool Name *	001	Action
001	1.1.:	Туре	IPv4 O IPv6	0 0
Total 1 item(s)	1 > Items per pa	Advanced Settings		
		Address Range *	1.1.1 1 to 254	
		Default Gateway *	1.1.1.1	
		Lease Time *	8 Hour(s) v	
			Cancel	

Click the <Edit> icon under the operation column of the last column of "DHCP List", the page will display the DHCP information, after editing the information, click <Complete Configuration> to prompt "Setup successful".

3. Remove DHCP

DHCP Settings	Static Address	Client Display			
DHCP					
+ Add DHCP Ø E	xcluded Address Range	Batch Delete			
Name	IP Add	Note	×	DNS	Action
001 Total 1 item(s) < 1	1.1.1.1-	Please retain at least one DHCP service. Are you sure you want to	address pool for the DCHP o delete the address pool?		C D
		Car	icel Confirm		

1) Select multiple records in the "DHCP List" and click "Delete Selected DHCP" to delete data in batches.

2) Click the <Delete> icon under the operation column of the last column of "DHCP List", and prompt "Are you sure to delete the selected DHCP?", click OK and prompt "Delete successfully" to complete the deletion.

4. Turn on DHCP

DHCP Settings	Static Address	Client Display				
+ Add DHCP	Ø Excluded Address Ra	ange 🗑 Batch Delet	e			
Name	IP A	Address Range	Default Gateway	Lease Time	DNS	Action
Name 001	IP A	Address Range	Default Gateway	Lease Time 8 Hour(s)	DNS	Action

Click <DHCP Service Switch> to enable DHCP service.

\bigstar Static address allocation

The static address allocation page is as follows:

DHCP Settings	Static Address	Client Display				
+ Add Static Addres	s 🗊 Batch Delete					
Client Name	Client IP	Mask	Gateway Address	Client MAC	DNS Server	Action
			No Data Found			
otal 0 item(s)	> Items per page: 10	~ 1 GO				

1.Add static address

DHCP Settings Static Address	Client Display
+ Add Static Address	Add Static Address ×
Client Name Client IF	Client Name *
	Client IP *
	Mask
	Client MAC *
tal O item(s)	Gateway Address *
	DNS *
	Cancel Save

Set the client name, client IP, and client MAC address are mandatory, other configurations are optional, click "complete configuration" to prompt "setup successful", it will be displayed in the static address list.

2. Edit static address

r Add Statt: Address	a batti Delete	Edit Static Addres	55	1	×	
Client Name	Client IP	Client Name *	net1		IS Server	Action
net1	1.1.1.1	Client IP *	1.1.1.1]	.1.254	0
al 1 item(s) < 1	> Items per pa	Mask	255.255.255.0]		
		Client MAC *	0002.0002.0002]		
		Gateway Address *	1.1.1.254]		
		DNS *	1.1.1.254]		
				ancel		

Click the <Edit> icon under the operation column of the last column of "Static Address List", the page will display the information of the static address. After editing the information, click <Complete Configuration> to prompt "Setup successful".

3. Delete static address

DHCP Settings	Static Address	Client Display				
+ Add Static Address	Batch Delete					
Client Name	Client IP	Mask	Gateway Address	Client MAC	DNS Server	Action
net1	1.1.1.1	Note	×	0002.0002.0002	1.1.1.254	0
Total 1 item(s) 🤇 🚺	Items per page:	 Are you sure you want to 	delete the static address?			
			Cancel Confirm			

1) Select multiple records in the "Static Address List" and click "Delete Selected Address" to delete data in batches.

2) Click the <Delete> icon in the operation column of the last column of "Static Address List", and prompt "Are you sure to delete this static address?", click OK and prompt "Delete successfully" to complete the deletion.

DHCP Settings	Static Address	Client Display			
1 Note: If you want to de	lete a static address converted	from a dynamic address, please go to the	Static Address page.		
Bind MAC to Dyna	amic IP			IP-Based	V Q Search
🗆 IP		MAC	Lease Time	Allocation Type	Action
			Ŷ		
			No Data Found		

The client list page is as follows:

1.Query IP address

Bind MAC to Dy	mamic IP			IP-Based	V Q Search	
🗆 IP		MAC	Lease Time	Allocation Type	Action	
				, and a down type	Action	

Enter the IP address in the search box to query.

VRRP configuration

+ Add VRRP					
VRRP Group No.	VRRP Port	VRRP Group IP	VRRP Priority	Action	
1	Te1/0/1	1.1.1.1	100	C D	
2	Te1/0/2	1.1.1.2	100		
	Te1/0/3	1.1.1.3	100		

1.Add VRRP

	Add VRRP		×	
VRRP Group No.	Dort	T-4 /0/4		Action
□ 1	Port	le1/0/1 V		
2	VRRP Group Number *	Range (1-255)		
3	IP *	Please enter a VRRP group IP address.		0
stal 3 item(s) < 1 > Items per	Priority *	100		
		Cancel	Save	

Set the VRRP interface, VRRP group number, and VRRP group IP are mandatory, and other configurations are optional. Click "Complete Configuration" and prompt "Setup Successfully" and it will be displayed in the VRRP list.

2. Delete VRRP in batches

VRRP Group No.	VRRP Port	VRRP Group IP	VRRP Priority	Action
□ 1	Te Note	×	100	0
2	Te	want to delete the item?	100	
3	Te	want to delete the item:	100	
3 item(s) < 1 > it	tems per page:	Cancel Confirm		

1) Select multiple records in the "VRRP list" and click "Delete selected VRRP" to delete the data in batches.

2) Click the <Delete> icon under the operation column of the last column of "VRRP List", and prompt "Are you sure you want to delete?", click OK and prompt "Delete successful" to complete the deletion.

3.Edit VRRP

	Edit VRRP		×	
VRRP Group No.	Port	Te1/0/1 v		Action
1				0 D
2	VRRP Group Number *	1		
3	IP *	1.1.1.1		
3 item(s)	Priority *	100		
-				
		Can	Save	

Click the <Edit> icon under the operation column of the last column of "VRRP List", the page will display the VRRP information, after editing the information, click <Complete Configuration> to prompt "Setup successful".

MAC address

The MAC address management page contains three parts: "Dynamic Address Table", "Static Address Setting" and "Filtering Address Setting".

Dynamic Address Table	Static Address Settings	Filtering Address Settings		
			Select Query Condi v	Sea
MAC Address		VLAN ID	Interface	
		No Data Found		
		No Data Found		

$\overset{}{\cancel{}}$ Dynamic address table

1. Query dynamic addresses according to conditions

Dynamic Address Table	Static Address Settings	Filtering Address Settings	
			Select Query Condi v Q Search S
MAC Address		VLAN ID	Interface
MAC Address		VLAN ID	Interface
		Ŷ	
		No Data Found	

Query by MAC, Query by VLAN, Query by interface

1) Select multiple records in the "Static Address List" and click "Delete Selected Static Address" to delete data in batches.

2) Click the <Delete> icon under the operation column of the last column of "Static Address List", and prompt "OK to delete the selected static address", click OK and prompt "Delete Successfully" to complete the deletion.

☆ Filter address settings

1. Add filter address

Dynamic Address Table	Static Address Settings	Filtering Address Settings		
Note: The switch forwards data configuring a filter address the set	according the MAC address inside the data me as the MAC address of ARP packets.	frame. If a switch receives a packet with the source/destination MAC a	ddress which is configured as a filter address, it di	scards the packet. You can prevent the ARP attack by
+ Add Filter Address	Batch Delete	dd Filter Address	×	
	M	AC Address *		Action
4422.6622.8866	VL	AN ID * Please enter a VLAN ID		
tal 1 item(s) < 1	Items per page: 10			
	-			
		Cancel	Save	

To set the filter address, you must fill in the MAC address and VLAN ID, click "Save Configuration" and prompt "Setup Successfully", it will be displayed in the static address list.

2. Edit filter address

		Edit Filter Ad	dress	×	
+ Add Filter Address	🗑 Batch Delete				
		MAC Address *	4422.6622.8866		
MAC Address		VI AN ID *	1		Action
4422.6622.8866				_	
otal 1 item(s)	> items per page: 10				
			Consel	- Contraction of the second	
				511/45	

Click the <Edit> icon under the operation column of the last column of "Filtered Address List", the page will display the information of the filtered address, after editing the information, click <Save Configuration> to prompt "Setup successful".

🖈 VSU mode

The Stacking mode page is as follows:

landalone mode.	
Domain ID 100(100)	
	Domain ID 100(100)

Se	Device 1 Cor	nfig		×
polo	VSU Set	tings		
	Device Mode	Standalone VSU		
	Device ID 🕗	1		
	Domain ID *	100		
	Priority *	100		
	Descriptor			
	VSL 📀	Device1 Slot0 S5860-20SQ v		
	🔄 Select All	invert 🗙 Deselect	Selected	AG Port
		A V 4 5 A V 6 7 A V 8 9 A V 10 11 A V 12 13 A V 14 15 A V 16 17 A V 18 19 A V 20 21 A V 22 21	3▲¥24 25▲¥26	

Click the icon to configure a single device, switch device mode, revise device ID, domain ID, priority, device description and VSL port. Dual host detection in stacking scenario

					9 6.3v	use the provident outling por	and the ports on boar ends in	ik between two bevic	requires a uncer m	
								D		D Status
							205Q ~	evice1 Slot0 S5860	De	D
🛛 AG Port 🔳 up 🔳 shut	AG Port	Selected						X Deselect	땹 Invert [Select All
				25▲▼26	21 • • 22 23 • • 24		. • • 12 13 • • • 14 15 • • 16		3474 5476	1472
40Gb 40Gb(Splite	40Gb	Fiber	Copper					nabled. Port is dow	Enabled 🙁 Er	D Port
					s.	o select multiple ports:	ointer across the section f	on as you drag the	hold the left butt	ote: Click and
40Gb - 🖼	40Gb	Fiber	Copper		s.	to select multiple ports	wointer across the section	nabled. Port is dow on as you drag the	Enabled 📀 Er	ED Port

Spanning Tree Protocol

"Spanning Tree Protocol" can set the global parameters of the spanning tree and the port settings of the spanning tree.

STP Global	Settings	STP Port Settings			
Global Co	nfiguration				
STP					
Priority	8		Hello Time	2	
Aging Time	20		Forward Delay	15	
STP Mode	MSTP	~			
MST Name	1		MST Version	1	

The global parameters of the spanning tree can be configured. When the spanning tree mode is selected as "MSTP", the MST instance can be set.

1.Add instance

To set an instance, you must fill in the instance value and VLAN range, and other information is optional. After clicking "Complete Configuration" and prompting "Setup Successful", it will be displayed in the instance list.

2. Fdit	exam	nle
2. Luit	CAUTT	pic

Global Co	nfiguration					
TP						
Priority	8	Hello Time	2			
ging Time	20	Forward Delay	15			
TP Mode	MSTP v					
/IST Name	1	Edit Instance	ſ]	×		
	Save	Instance Number *	0			
AST Cont	figuration	VLAN Range *	1-2,4-4094			
1 Note: It i	s recommended to disable STP before configuring an insta	Priority	8			
+ Add In	stance Batch Delete					
🗌 Ins	tance Number		Cancel	Save	Action	
0					Ø	
		3	8		口面	

Click the <Edit> icon under the operation column of the last column of "Instance List", the page will display the information of the instance, after editing the information, click <Complete Configuration> to prompt "Setup Successful".

3. Delete instance

Priority	8	Hello Lime	2		
Aging Time	20	Forward Delay	15		
STP Mode	MSTP ~				
MST Name	1	MST Version	1		
	Save	Note	×		
MST Confi	guration	Are you sure you want to delete	ete the instance?		
Note: It is	recommended to disable STP before configuring a		Cancel Confirm	ence of network topology.	
+ Add Ins	tance Batch Delete				
🗌 Insta	ance Number	VLAN	Priority	Action	
0		1-2,4-4094	8	ß	
□ 1		3	8	C 1	1
Total 2 item(s)	< 1 > Items per page: 10	0 v 1 GO			

1) Select multiple records in the "Instance List" and click "Delete Selected Instances" to delete data in batches.

2) Select and click the <Delete> icon under the operation column of the last column of "Instance List", and prompt "Are you sure to delete the selected instance?", click OK and prompt "Delete successfully" to complete the deletion. Instance 0 is the default instance that cannot be deleted.

\bigstar Spanning tree portsettings

TP Global Settings	STP Port Settings						
1 Note: It is recommended	to enable Port Fast on the port connec	cted to the PC.					×
+ Batch Add							
Port	Status	Port Fast	BPDU Guard	Protection Mode	Connection Mode	Instance Cost Priority	Acti
Te1/0/4	Down	Enabled	Disabled	Null	Auto	0 0 128 1 0 128	Ø
Te1/0/5	Down	Disabled	Enabled	Null	Auto	0 0 16 1 0 32	Ø
Te1/0/6	Down	Enabled	Disabled	Null	Auto	0 0 128 1 0 128	
Te1/0/7	Down	Enabled	Disabled	Null	Auto	0 0 128 1 0 128	Ø
Te1/0/8	Down	Enabled	Enabled	Null	Auto	0 0 128 1 0 128	
Te1/0/13	Down	Enabled	Disabled	Null	Auto	0 0 128 1 0 128	Ø
Te1/0/14	Down	Enabled	Disabled	Null	Auto	0 0 128 1 0 128	Ø
Te1/0/15	Down	Enabled	Disabled	Null	Auto	0 0 128 1 0 128	Ø
Te1/0/16	Down	Enabled	Disabled	Null	Auto	0 0 128 1 0 128	
Te1/0/17	Down	Enabled	Disabled	Null	Auto	0 2000 128 1 2000 128	Ø
al 18 item(s)	1 2) Items per pa	age: 10 v					

1. Batch settings Select the protection mode, Port Fast, BPDU filter, connection type, port priority, etc., and select the port for batch setting.

FS

2.Edit settings

Note: It is recon	Port Te1/0/4	×
- Batch Add	Protection Mode Null v Port Fast Lenabled v	
Port	BPDU Guard Connection Mode Auto ~	l Acti
Te1/0/4	Port Priority + Add	C.
Te1/0/5	Instance Number 0 v Priority * 128	Ø.
Te1/0/6	Instance Number 1 v Priority * 128	ß
Te1/0/7		Ø
Te1/0/8		
Te1/0/13		
Te1/0/14		Ø
Te1/0/15		
Te1/0/16		Ø
Te1/0/17	Cancel	Save

In the "Spanning Tree Port List", the <Edit> icon under the operation column of the last column will display the information of the port on the page. After editing the information, click <Complete Configuration> to prompt "Setup successful".

RLDP settings

Note: RLDP enables you to detect link failure quickly, RLDP can run on the port only after it	
	enabled globality. X
RLDP	
Detection Interval	etection Count 2
rrdisable	
Range(30-86400s)	
Save	
Port Configuration	
1.RLDP global settings

Global configura	ation			
1 Note: RLDP enable	es you to detect link failure quickly. RLDP can run on the po	rt only after it is enabled globally.		×
RLDP				
Detection Interval	1	Detection Count	2	
Errdisable				
Recovery Interval	Range(30-86400s)			
	Save			

Click the RLDP switch button to enable or disable the RLDP function. Configure the detection interval, detection times and recovery period when it is turned on, and click the <Save Settings> button to prompt "Setup successful"

- 2. Port RLDP settings
- 3. Add RLDP detection port

Batch Add					×
Detection Mode					
Unidirectional Link Detectio	Warning	Bidirectional Link detection	Warning	~	
Loop Detection	Warning				
Select Port					
Select All E Invert	Deselect Tave 9av10 11av12 13av14 15av16 V V V V V V V V V V V V	8 19▲▼20 21▲▼22 23▲▼24 25▲▼2	Selected AG Port	Up Shutdown	VSL Port

Select "Detection Type", "Troubleshooting" and the port and then press "Add Setting", it prompts "Set successfully" to complete the RLDP detection port addition operation. After successful addition, it will be displayed in "RLDP Detection PortList".

4. Edit RLDP detection port

Erre	PortTe1/0/1		×
Rec	Detection Mode		
Po	Unidirectional Link Detection Warning Loop Detection Warning	Bidirectional Link detection Warning	~
			Cancel Save

Click the <Edit> icon under the operation column of the last column of "RLDP Detection Port List", the page will display the information of the RLDP detection port. After editing the information, click <Complete Configuration> to prompt "Setup successful".

5. Delete RLDP detection port

RLDP						
Detection Interval	1	Detecti	on Count 2			
Errdisable						
Recovery Interval						
	Save	Note		×		
Port Configurati	ion	 Are you sure you want t 	o delete the item?			
Note: 1. Enabling RLDP o 2. Unidirectional/B 3.An aggregate por	on the port can avoid broadcast storm cau- idirectional link detection requires the po- t can only be configured with port violatic	[Cancel	ənfirm	o monitor the link between two switches;	×
+ Add Port						
Port		Dete	tion Type:Troubleshootir:	ng	Action	
Te1/0/1		Unidir	ectional Link Detection:Block	¢	C D	
Total 1 item(s)	1 > Items per page:	10 v 1 GO				

1) Select multiple records in the "RLDP detection port list" and click "Delete RLDP detection ports in batch" to delete data in batches.

2) Click the <Delete> icon under the operation column of the last column of "RLDP Detection Port List", and prompt "Are you sure to delete the selected data?", click OK and prompt "Delete successfully" to complete the deletion.

Safety

ACL

Input ACL When the device interface receives a packet, check whether the packet matches an ACE of the interface's input ACL; output ACL When the device is ready to output a packet from an interface, check whether the packet matches the interface output ACL Match one of the ACEs.

When formulating different filtering rules, multiple rules may be applied at the same time, or only a few of them may be applied. As long as it conforms to a certain ACE, the packet (Permit or Deny) is processed according to the ACE definition.

🖈 ACL list

Y + Add ACL 🗊 De	lete ACL			
Batch Delete				
escription Src IP/Wildcard	Source Port Access Control	Protocol Dest IP/Wildcard	Dest Port Time Period	Status Action
	escription Src IP/Wildcard	Pescription Src Source Port Access Control	escription Src Source Port Access Protocol Dest IP/Wildcard	Batch Delete rescription Src IP/Wildcard Source Port Access Control Protocol Dest IP/Wildcard Dest Port Time Period

1.Add ACL

Click the "Add ACL" button and set the content in the pop-up box. The ACL list is a required field. Click "OK" to prompt "Setup successful". You can see the added ACL in the ACL list drop-down box.

ACL List: a 🗸 🕇	Add ACL 🔀 Delete ACL	
	Add ACL >>	<
Add Access Rule Batch Del NO. Description	ACL Type	Period Status Action
ntal () item/s)	Cancel Confirm No Data Found	

2. Remove ACL

Select the ACL to be deleted in the ACL list drop-down box, click the "Delete ACL" button, and prompt "Delete successfully".

ACL List: a	Add ACL AC	Delete ACL				
Access Rule		Note	×			
+ Add Access Rule	Batch Delete	• Are you sure you want to delete the ACL?	_			
□ NO.	Description Src IP/W	Cancel	Confirm t	Icard Dest Port	Time Period Status	Action
			•			

3.Add ACE rules

Add Ac	cess Rule							×
ACL Type	Extended A	CL (Flow-based Control)						
ACL Name	а							
Access Cor	itrol 💿 Permit	O Deny						
Description	1							
Protocol	IP		~ 1	Time Period	~	Time managemen	nt	
Any Source	IP 🗌							
	Single IP		~ I	P				
Any Dest. I	P 🗌							

4. Edit ACE rules

Edit Access F	Rule					×
Access Control	Permit O Deny					
Description						
Protocol	lb	~	Time	Period	Time management	
Any Source IP						
	Mask Configuration	~	IP	1.1.1.2		
Any Dest. IP						
	Single IP	~	IP	1.1.1.3		

5. Delete ACE rules

	Y Add ACL							
Access Rule		Note		×				
+ Add Access Rule	Batch Delete	Are you sure you want t	to delete the access rule?					
NO.	Description Src IP/W		Cancel	nfirm ^t Vildc	ard Dest Port	Time Period	Status	Action
V 1	1.1.1. 0		· · · · · · · · · · · ·	0	0.0.	All Time	Active	0 1
otal 1 item(s)	> Items per page:	0 v 1 GO						

ACL effective time

ACL List ACL Time	ACL Application			
Note: The ACL active time must be periodic.				×
+ Add Time Object	elete			
+ Add Time Object	Day	Time Period	Action	
Add Time Object Batch De Time Object 1	Day Everyday	Time Period 2:00-7:00	Action	

You can make ACLs run based on time, for example, make ACLs take effect during certain periods of a week. To meet this requirement, you must first configure a time object.

1.Add time object

CL List	ACL Time	ACL /	plication			_
+ Add Time	Object 🗑 Batc	h Delete	Add Time Object		×	
Time C	Object		Object Name *			Action
1 tal 1 item(s)		Items per p	Time Period + Add	0		
			Ca	incel Save		

2. Batch delete time objects

ACL List ACL Time ACL App	lication			
• Note: The ACL active time must be periodic.				×
+ Add Time Object	Note	×		
Time Object1	O Are you sure you want to delete the time object	12	Action	
Total 1 item(s) < 1 > Items per page:	Cancel	Confirm		

3. Edit time object

+ Add Time Object	Edit Time Period ×	
Time Object	Object Name * 1	Action
1	Time Period + Add Monday,Tuesday,Wednesday ~ 2:00	
	Cancel Save	

4. Delete time object

ACL List ACL Time ACL Appl	ication			
Note: The ACL active time must be periodic.				×
+ Add Time Object Batch Delete	Noto			
Time Object	Note		Action	
V 1	O Are you sure you want to delete the	time object?	2 1	
Total 1 item(s) < 1 > Items per page:	Cancel	Confirm		

ACL application

It is by configuring ACL rules and applying them to the corresponding ports or VLANs to restrict specific user access or restrict users from accessing specific networks.

0

After ACL is applied to the port, there may be no way to echo it immediately, you need to refresh the page to echo

ACL List	ACL Time	ACL Application	n			
1 Note: If the o	configuration takes effect bu	ut is not displayed properly on	n the page, please refresh the page.			
+ Add Port	Batch Delete	e				
+ Add Port	Batch Delete	8				
ACL	Batch Delete	8	Port	Direction	Action	
ACL a(IP)	Batch Delete	8	Port Te1/0/20	Direction	Action	
Add Port ACL a(IP)	Batch Delete	8	Port Te1/0/20	Direction	Action ে ি	

1. Add ACL application

• Note: If the configu	Add Port ×	
+ Add Port	ACLList v Direction Input v	
ACL	Select Port	
al 1 item(s)		
	Note: Citica and float the feet fullion as your orag the pointer actors the section to select initiative p Copper Fiber Hock Hock Layer 3 Port Te1/0/1 Te1/0/2 Te1/0/3 Te1/0/19 Te1/0/20	

2. Delete ACLs in batch

ACL List ACI	Time ACL Appli	cation				
Note: If the configuration	takes effect but is not displayed pro	perly on the page, please refresh the page.				×
+ Add Port	atch Delete	Note		×		
a(IP)		 Are you sure you want to del 	lete the ACL application?		Action	
Total 1 item(s)	> Items per page:		Cancel Confirm			

3.Edit ACL application

+ Add Port Batch Delete	PortTe1/	0/20	×	
ACL	ACL List	a(IP)		Action
a(IP)	Direction	Input ~		0
tal 1 item(s)	tems per page: 10			
tal 1 item(s)	tems per page: 10			

4. Delete ACL application

		operly on the page, please refresh the page.	onfiguration takes effect but is not displayed p	1 Note: If the con
	×	Note	Batch Delete	+ Add Port
Action				ACL
C D	he item?	Are you sure you want to delete the iter		a(IP)
			< 1 > Items per page:	otal 1 item(s)
	cel Confirm	Cancel		
Action	the item?	Note Are you sure you want to delete the iter Cancel	Batch Delete	Add Port ACL a(IP) atal 1 item(s)

Port security

\bigstar basic settings

1.Add a security port

Max Secure Add	ress * 128			Aging Time *	0				
Security Action	Protectio	n	Ý						
Select Port	C Invert I D	eselect				Selecte	d 🔲 AG Port	Lin Shutdowr	VSI Po
1472	3▲▼4 5▲▼6 7▲	▼8 9▲▼10 11▲▼	2 13▲▼14 15▲▼16	17▲▼18 19▲▼20	21▲▼22 23▲▼24	25▲▼26			
**			** **	**	A.V. A.V.	****			
Note: Click and I	nold the left button as	you drag the point	er across the section t	o select multiple ports.		Cop	er Fiber	40Gb 4	0Gb(Splited)

2. Edit security port

avoid attacks caused by MAC a •If the configuration takes e	iddress depletion. ffect but is not displayed properly on the page, p	please refresh the page.			
- Add Port	h Delete	Edit - TF2/0/21		×	
Port	Max Secure Address			ction	Action
] TF2/0/21	128	Max Secure Address*	128		C D
tal 1 item(s) 🛛 🔍 🚺	> Items per page: 10 ~	Aging Time*	0		
		Security Action	Protection ~		

Click the <Edit> icon under the operation column of the last column of "User Security Port List", the page will display the information bound to the user, after editing the information, click <Complete Configuration> to prompt "Setup successful".

3. Delete security port

 It is generally applied to the on the console port to avoid a If the configuration takes eff 	e scenario where the accessed user has valid IP and attacks caused by MAC address depletion. fect but is not displayed properly on the page, plea	d MAC address or where the user accesses the net ase refresh the page.	work through a fixed por	t instead of changing IP/MAC address or p	port number, or limits the number of MAC addresses
	Note		×		
- Add Port	Are yo	ou sure you want to delete the security port	2		
Port	N			Security Action	Action
Te1/0/5	1.	Cancel	Confirm	Protection	
Te1/0/7	1			Protection	C D
al 2 item(s)	> Items per page: 10	1 GO			

1) Select multiple records in the "Security Port List" and click "Delete Selected Security Ports" to delete data in batches.

2) Click the <Delete> icon under the operation column of the last column of "Security Port List", and prompt "Are you sure to delete the selected security port?", click OK and prompt "Delete successfully" to complete the deletion.

☆ Secure binding

1. Add secure binding address

'	Add Address	>
I	IP * MAC	
١	VLAN ID	
5	Select Port	
		Selected AG Port Up Shutdown VSL Port
	1442 3444 5446 7448 94410 114412 134414 154416 174418 19442	20 21 • 722 23 • 724 25 • 726
		AV AV VVVV
	V V	
		Copper Fiber 40Gb Fig 40Gb(Splited)

Set the security binding address, the IP address is required, others are optional, click "complete configuration" and prompt "setup successful", it will be displayed in the security binding address list.

2. Edit security port

Port Securit Settings	Security Binding			
A Made Deal Counting in such that	Here and the second state of the second state			
Note: Port Security is used to	allow only the packet whose source MAC	address is consistent with the secure address to enter the switch.		
+ Add Address		Edit - TF1/0/21	×	
-		IP * 1.1.1.1		
U Port	IP			Action
TF1/0/21	1.1.1.1	MAC		
tal 1 item(s)	> Items per page: 10	VLAN ID		
		Cancel	Save	

Click the <Edit> icon under the operation column of the last column of "Security Binding Address List", the page will display the user's binding information, after editing the information, click <Complete Configuration> to prompt "Setup successful". 3.Delete the secure binding address list

+ Add Address	Batch Delete	Note	×		
Port	IF			VLAN ID	Action
TF1/0/21	1.	Are you sure you want to delete the port? Cancel	Confirm	-	

1) Select multiple records in the "Security binding address list", and click "Delete selected security binding ports" to delete data in batches.

2) Click the <Delete> icon under the operation column of the last column of "Security Binding Address List", prompt "Are you sure you want to delete the selected security binding port?", click OK and prompt "Delete Successful" to complete the deletion.

DHCP Snooping

The DHCP Snooping page is as follows:

DHCP Snooping	
 Note: DHCP snooping is used to filter DHCP packets received on an untrusted port from outside the network or firewall. The DHCP request packet is forwarded to the trus The port connected to the DHCP server is configured as a trusted port generally. 	\times sted port. The DHCP reply packet is forwarded only if it is from a trusted port.
DHCP Snooping	
☑ Select All 🔛 Invert 🗷 Deselect	Selected AG Port Up Shutdown VSL Port
14¥2 34¥4 54¥6 74¥8 94¥10 114¥12 134¥14 154¥16 174¥18 194¥20 214¥22 234¥24 254¥26 V V V 4¥ 4¥ 4¥ 4¥ 4¥ 4¥ 4¥ 4¥ 4¥ 4¥ 4¥ 4¥ 4¥	
Trusted Port 🥝	Copper Fiber 40Gb 🚭 40Gb(Splited)
Note: Click and hold the left button as you drag the pointer across the section to select multiple ports.	
Save Display DHCP Snooping Trusted Port	

The port connected by the DHCP SERVER needs to be set as a DHCP trusted port, and the DHCP SERVER on the untrusted port cannot work normally. The currently configured trusted port means that the DHCP trusted port is enabled on the port. The user can directly select the port on the panel and click the <Save Settings> button.

Anti-ARP attack

"Anti-ARP Attack" can be used to prevent gateway ARP spoofing settings, ARP inspection settings, DAI settings and ARP table entries.

Anti-Gateway ARP Spoofing

1.Add filtering port:

Add Port							×
Gateway *							
Select Port							
I Select All 및	Invert 💌 Deselect				Selected	🖪 AG Port 📕 Up	Shutdown VSL Port
Note: Click and hol	d the left button as you drag	g the pointer across the sectior	to select multiple ports	5.	Coppe	r Fiber 4	40Gb 40Gb(Splited)

To set the filter port, you must fill in the IP address, click "complete configuration" and prompt "setting successful", it will be displayed in the filter port list.

2. Edit filter port

Note: It is configured on only the port connected to the client to prevent ARP sponfing. Add Port Filtering Port PortTe1/0/5 Total 1 Item(s) I > Items per page: 10 Cancel Save			ARP Entries	DAI Settings	ARP Check	Anti-ARP-Spoofing
Add Port Batch Delete PortTe1/0/5 × Action Te1/0/5 cateway * 192.168.1254 Cancel Sive	×		-	ient to prevent ARP spoofing.	ly the port connected to the c	Note: It is configured on or
Filtering Port PortTe1/0/5 Cateway * Gateway * Interms per page: Cancel Save:						+ Add Port
□ Te1/0/5 Gateway * 192.168.1.254 total 1 item(s) < 1 Image: Cancel Save Save	Action	×	ortTe1/0/5	Po		Filtering Port
Cancel Save	C ti		ateway * 192.168.1.254	Gat	> Items per page	Te1/0/5
			Cancel			

Click the <Edit> icon under the operation column of the last column of "Filter Port List", and the page will display the information of the filtered port. After editing the information, click <Complete Configuration> to prompt "Setup successful".

3. Delete filter port

	ARP Check	DAI Settings	ARP Entries		
1 Note: It is configured on only the	e port connected to the c	lient to prevent ARP spoofing.			
+ Add Port		Note		×	
Filtering Port					Action
Te1/0/5		 Are you sure yo 	ou want to delete the port?		c d
Fotal 1 item(s)	Items per page				
			Cancel	Confirm	

1) Select multiple records in the "Filter Port List", and click "Delete Selected Filter Port" to delete data in batches.

2) Click the <Delete> icon under the operation column of the last column of "Filtered Port List", and prompt "Are you sure to delete the selected filtered port data?", click OK and prompt "Delete Successfully" to complete the deletion.

ARP inspection settings

Note: ARP Check is used to								
	filter all ARP packets on the I	ogical port and discard invalid.	ARP packets. It can effectively prever	t ARP Spoofing and improve	network stability. A DHCP Snoopin	g trusted port cannot be ena	bled with ARP Check.	×
elect Port	Deselect				Selected	🖪 AG Port 📕 Up	Shutdown	🔽 VSL F
		▼12 13▲▼14 15▲▼16	17▲▼18 19▲▼20 21▲▼22 :	3▲▼24 25▲▼26				
	vv							

The current port displayed on the panel has opened the ARP inspection setting state and is in the editing state. After the user has modified the port, but does not want to edit it, he can click the <Display Current ARP Inspection Port> button to restore the panel to display the current ARP inspection configuration state.

The port of the DHCP Snooping trusted port cannot enable ARP inspection.

☆ DAI settings

0

a

1.VLAN DAI setting added

Note: The untrusted and corresponding to the	DAL applied VI AN intercents all ADD request and expluses/arts	to discord involid ADD postote	
	Add VLAN DAI	u uistaiu invaiu Ann packets.	
Select All Deselect All Batch VID2 VID3	Delete VLAN Range *		
isted Port		Cancel	
Note: Packets received on the trusted port skip	o DAI Inspection as valid ARP packets.		

2.VLAN DAI delete

Add VLAN DAI Select All Deselect All Batch Delete VID2 VID3			
Trusted Port	Note	×	
Note: Packets received on the trusted port skip DAI Inspecti	Are you sure you want to d	elete the VLAN?	×
☑ Select All ☑ Invert ☑ Deselect 1▲¥2 3▲¥4 5▲¥6 7▲¥8 9▲¥10 11▲¥1 ▲¥ ▲¥ ▲¥ ↓ ↓ ↓ ▲¥ ▲¥ ▲¥ ▲¥ ↓ ↓		Cancel Confirm	Selected AG Port Up Shutdown VSL Po
Trusted Port 📀 Note: Click and hold the left button as you drag the pointer	across the section to select multiple	ports.	Copper Tiber 40Gb 📑 40Gb(Splited)
Save Display Trusted Port			

3.DAI confidence

Trusted Port	
O Note: Packets received on the trusted port skip DAI Inspection as valid ARP packets.	×
리 Select All 뚀 Invert I Deselect	Selected 🛛 AG Port 🔳 Up 📕 Shutdown 🖉 VSL Port
1 a v 3 a v 4 5 a v 6 7 a v 8 9 a v 10 11 a v 12 13 a v 14 15 a v 16 17 a v 18 19 a v 20 21 a v 22 23 a v 24 25 a v 26 a 	
Trusted Port 🧇 Note: Click and hold the left button as you drag the pointer across the section to select multiple ports.	Copper Fiber 40Gb 40Gb(Splited)
Save Display Trusted Port	

🕕 The setting status of the currently opened DAI trusted port displayed on the panel is in the editing state. After the user has

modified the port, but does not want to edit it, he can click the <Show current DAI trusted port> button to restore the panel to display the current DAI trusted port configuration status.



1.Dynamic >> Static binding

				ID Record
Dynamic Binding > St	atic Binding	MAC	Type	Action
		MAC	Туре	Action
			Ĩ.	

1) You can select multiple pieces of dynamic data in the "ARP table entry list" to batch setas static binding data.

2) Click the <dynamic to static binding> icon under the operation column of the last column of "ARP entry list" to prompt "Setup successful".

2. Manual binding

Anti-ARP-Spoofing	ARP Check	DAI Settings ARP Entries		
Dynamic Binding > S	Static Binding	Batch Delete 8 Manual Binding		IP-Based Q: Search
🗆 IP		MAC	Туре	Action
		Manual Binding	×	
		IP *		
		MAC *		
iotal 0 item(s)	Items per page: 10	~		
			Cancel Save	

Set static binding data, IP address and MAC address are required fields, click "OK" to prompt "Setup successful", it will be displayed in

"ARP table entry list".

IP Source Guard

"IP Source Guard" can carry out interface configuration and user binding.

☆ Interface configuration

1. Add IP Source Guard port

	Add Port	×
Add Port	Filter Type IP 🗸	
Port	Select Port ② Select All 단 Invert 로 Deselect	Selected 🗈 AG Port 🔳 Up 🔳 Shutdown 💷 VSL Port
	14¥2 34¥4 54¥6 74¥8 94¥10 114¥12 134¥14 154¥16 174¥18 194¥20 V V V 4¥ 4¥ 4¥ 4¥ 4¥ 4¥ 4¥ 4¥ 4¥ 4¥	214¥22 234¥24 254¥26
0 item(s)	Note: Click and hold the left button as you drag the pointer across the section to select multiple por	rts. 💼 Copper 🔜 Fiber 🔜 40Gb 📑 40Gb(Splited)

Set to enable the IP Source Guard port, select the filter type and port, click "Finish configuration" and prompt "Setup successful", it will be displayed in the IP Source Guard port list.

2. Delete IP Source Guard port list

ort settings	User binding					
Note: IP Source Guard i	s applied in combination with DHCP S	nooping, Port-based IP Source Guard takes effect on only the untri	usted port enabled wit	h DHCP Snooping. Othe	rwise, IP Source Guard does not take e	ffect.
+ Add Port						
		Note	×			
Port	Filter Type			MAC	VLAN ID	Action
Te1/0/5	IP-ONLY	Are you sure you want to delete the item?				0
tal 1 item(s)	1 > Items per page:			-		
		Cancel	Confirm			

Select multiple records in "IP Source Guard Port List", click "Delete Selected IP Source Guard Port List" to delete data in batches.
 Click the <Delete> icon under the operation column of the last column of "IP Source Guard Port List", and prompt "Are you sure to delete the selected data?", click OK and prompt "Delete successfully" to complete the deletion.

☆ User binding

1.Add user binding

Set user binding, MAC address, IP address, VLAN ID are required, click "complete configuration" and prompt "setup successful", it will be displayed in the user binding list.

2. Edit user binding

Port Settings	User Binding	
1 Note:		×
 1. The IP Source Gu 2. If the port is co 	dienabled port filters all non-DHCP1P packets. After configured with the static IP address, the port allows specified IP packets to pass through. PortTe1/0/5	×
+ Add Binding	MAC * 66586.6658.7788 IP * 192.168.1.1	
MAC	VLAN ID *	
6688.6688.7		
Total 1 item(s)		
	Cancel	Save

Click the <Edit> icon under the operation column of the last column of "User Bound Port List", the page will display the user's binding information, after editing the information, click <Complete Configuration> to prompt "Setup successful".

3. Delete user binding list

ort Settings	User Binding						
 Note: 1. The IP Source G 2. If the port is con 	uard-enabled port filters all non-D ifigured as a DHCP Snooping truste	HCP IP packets. After configured with the door, the configuration on this port ta	e static IP address, the port allows sp kes effect but it will not filter packets.	pecified IP packets to pa	ass through.		
+ Add Binding		Note		×			
П мас		IF O Are you sure you w	ant to delete the binding?		Port	Action	
6688.6688.77	788	1			Te1/0/5	6	
tal 1 item(s)	1 > Items per pa	age:	Cancel	Confirm			

1) Select multiple records in the "User Binding List" and click "Delete Selected Binding" to delete data in batches.

2) Click the <Delete> icon under the operation column of the last column of "User Binding List", and prompt "Are you sure to delete the binding?", click OK and prompt "Delete successfully" to complete the deletion.

NFPP

The NFPP page is as follows:

NFPP Set	tings
ARP-guard 📀	ARP-guard List
IP-guard 📀	IP-guard List
ICMP-guard 📀	ICMP-guard List
DHCP-guard 📀	DHCP-guard List
DHCPv6-guard 📀	DHCPv6-guard List
ND-guard 📀	ND-guard List
Display NFPP Log	Display NEPP Log
	Save Restore Default Settings

You can turn on or off each anti-attack function, click "Save Settings" to prompt "Setup successful", when you want to restore the default settings, click the "Restore Default Settings" button

advanced

IGMP Snooping

The page of IGMP settings is as follows:

On layer 2 devices, multicast frames	s are flooded to all ports, causing storm and consuming much ban	width.		
IGMP Snooping is used to find out o	on which port there is an IGMP subscriber and only send IGMP tra	ffic to the port, so as to save bandwidth.		
Snooping				
Add Profile	Delete			
Add Profile Batch D	Delete Multicast Address	Policy Action	Application Port	Action
Add Profile Batch D	Delete Multicast Address	Policy Action	Application Port	Action

1.Add group policy

To set a group policy, you must fill in the group policy identifier and the multicast address range, and other information is optional. After clicking "Save Configuration" and prompting "Setup successful", it will be displayed in the group policy list.

	Add Profile	×
 Note: On layer 2 di IGMP Snoop 	Profile ID * Range(1-1024)	
	Multicast Range * eg: 224.0.0.0-239.255.255.255 - eg: 224.0.0.0-239.255.255.255	
4P Snooping	Policy Action Permit Deny	
+ Add Profile	Select Port	ort
Profile	1442 3444 5446 7448 94410 114412 134414 154416 174418 194420 214422 234424 254426	on
2		۵
2 al 1 item(s)		
2	Note: Click and hold the left button as you drag the pointer across the section to select multiple ports.	

2. Edit Group Policy

IMP SI	Edit Profile ×	
Note: • On layer 2 di • IGMP Snoop	Profile ID * 2	
	Multicast Range * 224.0.0.1 - 224.0.0.8	
P Snooping	Policy Action Permit Deny	
Add Profile	Select Port	
	🖸 Select All 🤮 Invert 🗵 Deselect 🔲 Selected 🔳 AG Port 📕 Up 🔳 Shutdown 🔲 VSL Port	
Profile 2	1 A Y 3 A V 5 A V 6 7 A V 8 9 A V 10 11 A V 12 13 A V 14 15 A V 16 17 A V 18 19 A V 20 21 A V 22 3 A V 24 25 A V 26 A V 25 A V 26 A V 27 A V 47 A V	on fil
1 item(s)		
	Note: Click and hold the left button as you drag the pointer across the section to select multiple ports.	

Click the <Edit> icon under the operation column of the last column of "Group Policy List", the page will display the information of the group policy, after editing the information, click <Save Configuration> to prompt "Setup successful".

3. Delete Group Policy

1) Select multiple records in the "Group Policy List" and click "Delete Selected Group Policy" to delete data in batches.

2) Click the <Delete> icon under the operation column in the last column of "Group Policy List", and prompt "Are you sure you want to delete this selection?", click OK and prompt "Delete successfully" to complete the deletion.

QOS

\bigstar Classification settings

The category setting page is as follows:

Class Settings	Policy Settings	Flow Settings		
1 Note: Classificatio	on is used to identify and mark certa	ain data flows that match the ACL rule.		
+ Add Class	Batch Delete			
Class Nam	le		ACL	Action
Class Nam	le		ACL	Action

1.add category

Class Settings	Policy Settings	Flow Settings			
Note: Classification i	is used to identify and mark cert	ain data flows that match the ACL rule.			×
+ Add Class		Add Class		×	
Class Name	·	Class Name * (1-31) Bytes			Action
2	1 > Items per	ACL List a	 ACL List 		
			Cancel	Save	

category, the category name is required, select the ACL list, click "Save configuration" and prompt "Setup successful", it will be displayed in the category list.

2. Edit category

Click the <Edit> icon under the operation bar in the last column of "Category List", the page will display the information of the category, after editing the information, click <Save Configuration> to prompt "Setup successful".

Note: Classification is used to identif	iy and mark certain data flows that match the ACL rule.		
+ Add Class	Edit Class	×	
Class Name	Class Name * 2		Action
2	ACL List	✓ ACL List	2 0
iotal 1 item(s)	Items per		
		Cancel Save	

3. Delete category

1) Select multiple records in the "Category List", click "Delete Selected Categories" to delete data in batches.

2) Click the <Delete> icon in the operation column of the last column of "Category List", and prompt "Are you sure to delete this item?", click OK and prompt "Delete successfully" to complete the deletion.

Class Settings	Policy Settings	Flow Settings		
1 Note: Classification	n is used to identify and mark certa	in data flows that match the ACL rule.		
+ Add Class				
		Note	×	
Class Name	e			Action
2		 Are you sure you want to de 	elete the item?	C 🗇
otal 1 item(s)	1 S items per p	age:	Cancel Confirm	

☆ Policy setting

The policy setting page is as follows:

1.Add strategy

Set the strategy, the name of the strategy is required, click "complete configuration" and prompt "setup successful", it will be displayed in the strategy list.

Class Settings Policy Settings	Flow Settings			
 Note: The policy is used to constrain the bandwidth tha If the configuration takes effect but is not displayed 	: the classified data flow consumes. d properly on the page, please refresh the page			×
Policy Settings	Add Policy		×	
Policy List as · · · ·	Policy Name * (1-31) Bytes			
Policy Rule			_	
+ Add Policy Rule			Cancel Save	
Class Name	Bandwidth (KBps)	Burst Traffic (KBytes)	Bandwidth Violation Disposal	Action
2	88	8	Drop	
Total 1 item(s) < 1 > items per	page: 10 v 1 GO			

2. Delete strategy

Select a policy in the "Policy List", click the <Delete Policy> icon, and prompt "Are you sure you want to delete this item?", click OK and prompt "Delete successfully" to complete the deletion

3.Add policy rules

Set policy rules. Bandwidth and burst traffic are mandatory, and other configurations are optional. After clicking "Finish configuration" and prompting "Setup successful", it will be displayed in the list of policy rules.

1 Note:		11					>
The policy is used If the configuration	to constrain the bandwidth that P takes effect but is not displayed	Add Policy Rule			×		
Policy Settings		Policy Name *	35				
Policy List as	× + A	Bandwidth *	(64-33554432) KBps				
,		Burst Traffic *	(4-8192)KBytes				
Policy Rule		Limit Violation Disposal	Drop OSCP				
+ Add Policy Rule	Batch Delete	Class List	2	v .			
Class Name	1				Sa	I Action	
2				Cancel	Save	0	
otal 1 item(s)	1 > Items per p	age: 10 v 1	GO				

4. Edit policy rules

Click the <Edit> icon under the operation column of the last column of "Policy Rule List", the page will display the information of the policy rule. After editing the information, click <Complete Configuration> to prompt "Setup successful".

A Note:							
The policy is used If the configuratio	to constrain the bandwidth that P	Edit Policy Rule			×		
		Later one) rate					
olicy Settings		Policy Name *	as				
as	× + A	Bandwidth *	88				
		Burst Traffic *	8				
olicy Rule		Limit Violation Disposal	Drop OSCP				
+ Add Policy Rule	Batch Delete	Class List	2	~	_		
Class Name	2				osal	Action	
2				Cancel	Save		

5. Delete policy rule

1) Select multiple records in the "Policy Rule List" and click "Delete Selected Rule" to delete data in batches.

2) Click the <Delete> icon under the operation column in the last column of "Policy Rule List", and prompt "Are you sure to delete this item?", click OK and prompt "Delete successfully" to complete the deletion.

 Note: The policy is used to constrain If the configuration takes effect 	the bandwidth that the cl t but is not displayed prop	assified data flow consumes. erly on the page, please refresh the pa	je.		
Policy Settings		Note	×		
olicy List as	× + Add P	• Are you sure you war	t to delete the item?		
Policy Rule			Cancel		
+ Add Policy Rule					
Class Name		Bandwidth (KBps)	Burst Traffic (KBytes)	Bandwidth Violation Disposal	Action
2		88	8	Drop	C D

☆ Stream settings

The page of flow settings is as follows:

iass settings	Policy Settings	Flow Settings				
1 Note:						
The policy is used	to constrain input and output flo	ws (Input and output flows of one por	t must be in the same trust mode but they can be co	nfigured with different policies)		
 If the configuration 	takes effect but is not displayed	properly on the page, please refresh t	he page.			
+ Add Port	🗑 Delete Port					
+ Add Port	Tolete Port					
+ Add Port	Tolete Port	Direction	Policy Name	Trust Mode	Action	
+ Add Port	🗑 Delete Port	Direction	Policy Name	Trust Mode	Action	
+ Add Port Port Te1/0/13	🗑 Delete Port	Direction	Policy Name	Trust Mode Untrusted	Action	
+ Add Port Port Te1/0/13	Telete Port	Direction	Policy Name	Trust Mode Untrusted	Action	

1.Add application policy port

Set the application policy port, select the speed limit direction, trust mode, policy list and port, click "Save configuration" and prompt "Setup successful", it will be displayed in the application policy port list.

• The policy is	Add Port	×
If the configu	Rate-limiting Direction Input ~	Trust Mode Untrusted ~
Add Port	Policy List as v	
Port Te1/0/1:	Select Port	Selected AG Port Up Shutdown VSL Port
1 item(s)	14V2 34V4 54V6 74V8 94V10 114V12 134V14 154V1 V V V V V V V V	5 17av18 19av20 21av22 23av24 25av26
	Note: Click and hold the left button as you drag the pointer across the section	n to select multiple ports. 💼 Copper 📰 Fiber 🔜 40Gb 📑 40Gb(Splited)

2. Delete application policy port

1) Select multiple records in the "Application Policy Port List" and click < Delete Selected Application Policy> to delete data in batches.

2) Click the <Delete> icon in the operation column of the last column of "Apply Policy Port List", and prompt "Are you sure to delete this item?", click OK and prompt "Delete successfully" to complete the deletion.

Class Settings	Policy Settings	Flow Settings				
 Note: The policy is used 	to constrain input and output flows (I	iput and output flows of one port must be in the same t	trust mode but they can be configured v	with different policies)		
If the configuration	takes effect but is not displayed prop	Note	×			
+ Add Port						
Port		C Are you sure you want to delete the	tem?	Trust Mode	Action	
Te1/0/13		0		Untrusted	Ū	
īotal 1 item(s)	1 > Items per page	Cancel	Confirm			
Fotal 1 item(s) <	1 > Items per page	Cancel	Confirm			

DHCP relay

The DHCP relay page is as follows:

DHCP relay	/			
 Note: DHCP relay can ce The DHCP relay ag 	ntrally manage IP address assignment for large nu gent forwards client-originated DHCP packets to	mber of subscribers in different subnets. I DHCP server and then forwards the server-t	o-client reply to the client.	×
DHCP Relay				
DHCP Server Address		G		
	Save			

Turn on or turn off the DHCP relay. When turned on, you can set multiple DHCP server addresses

DHCP relay can central The DHCP relay agent 1	rmanage IP address assignment for large number of subscribers in different subnets. Invards client-originated DHCP packets to a DHCP server and then forwards the server-to-client reply to the client.
DHCP Relay	
DHCP relay IPV4 cc	nfiguration
DHCP Server Address	•
DHCPv6 relay confi	guration All 🔀 Batch Delete
DHCPv6 relay confi Select All Deselec	guration All 🔞 Batch Delete

authentication

"Internet real-name authentication" can carry out external web authentication and advanced settings.

☆ External web authentication

The page for external web authentication is as follows:

ePortalv2	ePortalv Advanced Settings					
1 Note: Authentio	cation is based on Web to control users' access t	the network. It requires no authentica	ition firmware on the client. Inste	ad, you can perform authentication on commo	n browsers.	×
portal Type 🕐	ePortalv1 ePortalv2					
Portal Server IP *		Redirec	tion URL *			
Portal Key *		Authen	tication Server All Se	ervers v	Radius Server Settings	
Accounting Server	All Servers	✓ SNMP	Server * SNN	AP Server		
Port						
] Select All B	Invert 🗙 Deselect			Sele	cted 🔳 AG Port 📕 Up 🔳 Shute	down 🔟 VSL P
1472 34	v4 5av6 7av8 9av10 11av12 11 v v v v v v v av av av av av v v v v v v	AV14 15AV16 17AV18 19A	▼20 21▲▼22 23▲▼24	25 • • 26		
Authentication Port:	: •			e c	opper 📕 Fiber 📕 40Gb 📑	40Gb(Splited)
Note: Click and hold	I the left button as you drag the pointer ac	ross the section to select multiple	e ports.			
Save	Clear					

Server IP address, redirect homepage is required, click "Save Settings" to prompt the setting is successful.

☆ ePortalv Advanced Settings

ePortaiv2 ePortaiv	/ Advanced Settings		
Redirection HTTP Port: 80,	443		
Whitelisted Network Resource 📀			
+ Add			
IP:	Mask:		
Whitelisted User IP 📀			
+ Add			
IP:	Mask:	⊗	

Authentication-free network resources and authentication-free users can set multiple values. Under other configuration settings, click the "Save Settings" icon to prompt that the settings are successful

1.3.4 Diagnosis

Through the first level menu "Security", you can enter the second level menu. Including DHCP Snooping, ARP attack prevention, IP Source Guard, port security, NFPP, storm control.

Network diagnosis

PING detection

Ping			
Ping Type 📀	Not Via Management Port	Dest IP/Domain Name *	eg:192.168.1.1/www.google.com
Timeout Interval(s)	2	Repeat Times	5
Packet Size(Bytes)	100		
Fragment			
	Test		
Test Results			

PING method

Set to use out-of-band channels. It is only supported on devices that support MGMT. When the MGMT port is designated as the source interface, the management port must be selected, otherwise, the non-management port must be selected.

Destination IP address or domain name

The address or domain name to be pinged.

overtime time

Specify the timeout period.

repeat times

Specify the number of data packets sent.

Packet size

Specify the length of the data padding segment of the sent packet.

Allow fragmentation

Set the DF flag of the IP. When the DF bit is set to 1, it means that the packet will not be segmented. The default DF bit is 0.

tracert detection

Tracert			
Tracert Type	Not Via Management Port	Dest IP/Domain Name *	eg: 192.168.1.1/www.google.com
Timeout Interval(s)	2		
	Test Stop		
Test Results			

Tracert method

Set to use out-of-band channels. It is only supported on devices that support MGMT. When the MGMT port is designated as the source interface, the management port must be selected, otherwise, the non-management port must be selected.

Destination IP address domain name

Tracert's destination address or domain name address.

overtime time

The specified timeout period.

One-click collection

One-click collection will collect equipment fault information, which is convenient for troubleshooting equipment faults.

Note: One-Click Collection is used to collect fault information for	troubleshooting.
One-Click Collection	
One-Click Collection	

Log

System log

Configure the syslog log to help customers locate problems in after-sales and R&D.

Display System Log	
Enable Syslog Logging	
inable Syslog Logging C Export Log	
iystem Log (show log)	
Update Log	
Suite leaving applied	I
-y ang Ngg Ng N	
Monitor logging: level debugging, 0 messages logged	
Buffer logging: level debugging, 473 messages logged	
File logging: level informational, 473 messages logged	
File namesyslog.txt, size 128 Kbytes, the 2 file is currently being written	
Standard format:false	
Timestamp debug messages: datetime	
Timestamp log messages: datetime	
Sequence-number log messages: disable	
Sysname log messages: disable	

System log monitoring

The log can be queried according to the level and module for customer assistance in after-sales and R&D positioning problems.

Refresh		Severity Level All Levels	Search by Module	
Severity Level	Module	Mnemonic	Description	Time
(4)Warnings	DEV_MONITOR	POWER_STATUS_FAIL	The power status of 1/1 is fail, please check whether the power cord is plugged!	2022-07-23 10:07:06
(4)Warnings	DEV_MONITOR	POWER_STATUS_FAIL	The power status of 1/1 is fail, please check whether the power cord is plugged!	2022-07-23 10:06:06
(4)Warnings	DEV_MONITOR	POWER_STATUS_FAIL	The power status of 1/1 is fail, please check whether the power cord is plugged!	2022-07-23 10:05:06
(6)Informational	SNMP	AUTHSUCC	Authentication success for SNMP req from host 10.36.5.1	2022-07-23 09:44:45
(5)Notifications	HTTPD	LOGIN	User (admin@10.36.113.96) login from FS.	2022-07-23 09:33:36
(4)Warnings	DEV_MONITOR	POWER_STATUS_FAIL	The power status of 1/1 is fail, please check whether the power cord is plugged!	2022-07-23 09:04:06
(4)Warnings	DEV_MONITOR	POWER_STATUS_FAIL	The power status of 1/1 is fail, please check whether the power cord is plugged!	2022-07-23 09:03:06
(4)Warnings	DEV_MONITOR	POWER_STATUS_FAIL	The power status of 1/1 is fail, please check whether the power cord is plugged!	2022-07-23 09:02:06
(4)Warnings	DEV_MONITOR	POWER_STATUS_FAIL	The power status of 1/1 is fail, please check whether the power cord is plugged!	2022-07-23 08:01:05
(4)Warnings	DEV_MONITOR	POWER_STATUS_FAIL	The power status of 1/1 is fail, please check whether the power cord is	2022-07-23 08:00:05

1.3.5 Maintain

Switch management

upgrade

Upgrade		
 Note: Please download the co Make sure that the firmware The page may have no response 	responding firmware version from the official website, and then upgrade the device with the following tips. version (main program or Web package) matches the device model. rse during upgrade. Please do not power off or restart the device until an upgrade succeeded message is displayed.	×
ile Name	Browse File	

Click Browse, select the bin file saved locally, and then click the <Start Upgrade> button to implement the local upgrade operation.

Configuration management

\bigstar Configuration backup

Back up the configuration files on the device, import and export the configuration, and perform batch operations on the configuration, which is more convenient for users to operate.

Backup	Restore	Charset		
Note: Please	e don't close or update th	he page during import, or in	port will fail. If you want to apply the new settings, please restart the device on this page, or the settings will not take effect.	×
File Name			Browse File	
		Export Current Settin		
		Export Current Settin	5. 7	

	Restore	Charset			
1 Note: After	the device is reset to the	e factory default settings, all settings	be cleared. Please export current settings bef	fore resetting the device.	
Restore Facto	ry Settings Ex	port Current Settings			
Dicplay	Current S	ottings			
Jispiay	Current 5	ettings			
Display Curre	nt Settings				
Display Curre	nt Settings				
Display Curren	nt Settings	, Release(09182801)			
Display Current version S5860	nt Settings)_FSOS 12.5(4)B0151	, Release(09182801)			
Display Current version S5860 ! aggregateport	D_FSOS 12.5(4)B0151	, Release(09182801)			
Display Curren version S5860 ! aggregateport voice vlan agir	nt Settings D_FSOS 12.5(4)B0151 I load-balance dst-ip ng 1550	, Release(09182801)			
Display Curren version S5860 ! aggregateport voice vlan agir no voice vlan agir	nt Settings D_FSOS 12.5(4)B0151 : load-balance dst-ip ng 1550 security enable	, Release(09182801)			
Display Curren version 55860 ! aggregateport voice vlan agir no voice vlan agir voice vlan mac	nt Settings D_FSOS 12.5(4)B0151 : load-balance dst-ip ng 1550 security enable c-address 4422.6622	, Release(09182801) 0000 mask ffff.ffff.0000			
Display Curren version S5860 ! aggregateport voice vlan agin no voice vlan agin voice vlan mac mac-address-1	nt Settings)_FSOS 12.5(4)B0151 : load-balance dst-lp ng 1550 security enable c-address 4422.6622 table filtering 4422.6	, Release(09182801) 0000 mask ffff.ffff.0000 222.8866 vlan 1			
Display Curren version S5860 ! aggregateport voice vlan agir no voice vlan agir mac-address-1 spanning-tree	nt Settings 2_FSOS 12.5(4)B0151 : load-balance dst-lp ng 1550 security enable c-address 4422.6622 able fittering 4422.60 mst configuration	. Release(09182801) 0000 mask fff.fff.0000 522.8866 vlan 1			

Clear the configuration information and restore to the original state. Need to use the factory setting ip to revisit the WEB.

☆ System character set

Note: The current charset is the default charset. Diese set the charset of terminal tool (e.g. SecureCRT) to be the same

System character set, GBK, UTF-8, default, web recommends to configure UTF-8 encoding, use SecureCRT and other terminal tools, it is recommended to keep the same, otherwise there will be garbled codes.

system time

Set the system time through the area where the device is located to make the device information accurate and clear.

Systime	
Current Time	2022-7-23-10:42:46
Reset Time *	2022-07-23 10:42
Time Zone	UTC+0(GMT) v
Time Synchronization	Automatically synchronize with an Internet time server(Please set DNS Server, first, otherwise the system time will not be synchronized.)
	Save

The page shows the current system time. You can manually set the current system time, or you can set the time by checking "Automatically synchronize with the Internet time server". Choose one of the two for configuration. Finally, click the <Save Settings> button to prompt "Save Settings Successfully" to complete the configuration.

Log server

The local log of the device is sent to the corresponding server for storage, and the history is saved for easy reference.

Syslog		
1 Note: Loggi	g is rated on 8 different levels: 0-Emergency, 1-Alert, 2-Critical, 3-Error, 4-Warning, 5-Notification, 6-Informational, 7-Debugging. The smaller the number, the higher the level.	×
Local Logging		
Server IP	192.168.1.3	
Logging Level	Informational(6) v	
	Save	

Set the IP address of the system log server and the log level parameters to be sent. After the setting is completed, the device will send the SYSLOG log to the corresponding server.

DNS

The DNS server is configured to perform dynamic domain name resolution.

0

DNS		
DNS Server 1		
1	Save	

Network management configuration

WEB configuration management

🛠 Administrator password

In order to improve system security and make information interaction more secure, please modify the system default password.

Admin Password	Basic Settings	Permissions
Admin Pas	ssword	
Username	admin	
Old Password *		Sec
New Password *		- See

Web user password modification requires the old password and the new password twice. When the old password is entered incorrectly, the red text "The original password entered is incorrect" will be prompted after the input box. You need to enter the correct old password and click the <Save Configuration> button to complete the modification.



The enable password is also changed by default when changing the web network management password.

\bigstar Basic configuration

Admin Password	Basic Settings	Permissions
Web Access Port *	443	
Login Timeout	1 hour	~
Device Location		
ccess Redirection	HTTP Redirection to HTT	PS(In NAT scenario, redire
	Save	

Basic configuration In order to facilitate the management of the device, configure the device to check the device with a better location. Set the timeout time, and the WEB will automatically exit after leaving for a long time to ensure the safety of your system.

Telnet

In order to improve system security and make information interaction more secure, please configure the telnet function.

Felnet			
elnet Service			
SH Service			
iew Password *	×		
onfirm Deceword			

To modify the telnet password, you do not need to enter the old password, just enter the same new password twice, and the other operations are the same as modifying the super user password.

SNMP

SNMP simple network management protocol, they provide a method to collect network management information from devices on the network, and can manage many network devices.

SNMP		
Note: Either SNMPv2 or St	MPv3 is supported	×
SNMP Version		
Device Location		
SNMP Community *		
Trap Community 💿	•••••	
Trap Receiver Address 🌍 *	10.36.1.54	
	Save	

Select the SNMP version, the device ID, SNMP password and Trap receiving host are mandatory, other settings are optional, click <Save Settings> to prompt "Setup Successful".

1.3.6 Other Functions

Menu favorites

When users want to collect frequently configured functions, they can quickly click the menu and configure next time.

To ensure the meaning of favorites, currently only 10 menus can be favorited

1.Add to favorites

FS 55860-205Q	Monitoring > SWITCH Overview				earch term	😤 Config Wizard 🐥 ad
Favorites 2	Voice Vlan					
Monitoring	- VLAN			^	Device Usage	^
🔂 Config >		5N G1PC135000034	Booted on 2022-07-18 16:30:49		CPU Usage	10.1 %
🔁 Diagnosis >	Model\$5860-205Q	MAC Address 649d.99d0.70da Firmware Version 55860_FSOS 12.5(4)B0151, Release(09182801)	System Time 2022-07-23 10:46:07 Uptime 4 d 18 h 15 min 19 s		Memory Usage	55.9%
🛱 Maintenance 🔸		Hardware Version 1.00			-	-
	Device Port			Selected	🛾 AG Port 🔳 Up 🔳 Shutdov	vn 📑 VSL Port 📑 BFD Por
	FS MART	0 4 7 0 4 7	NA¥12 DA¥16 DA¥16 V A¥ V V V X X X X X X X X X X X X X	19 A ¥ 20 B B B A ¥ B	2 22 A ¥ 24 1 2 3 4 400 Brake A ¥ 20 400 Brake 20 40 40 20 20	NS.
	Port Role (1) Trunk Port (1) Rou	ted Port			Copper 📕 Fiber	40Gb 40Gb(Split
	Traffic Summary	0_IP manage v Kbps v				

3. Unfavorite

🕞 FS 55860-205Q \Xi	Monitoring > SWITCH Overview		🗄 Config Wizard 👌 adm
Favorites 📀			
Monitoring	Device Details	Device Usage	
Config >	SH GJPC135000034 Booted on 2022-07-18 16-30 MAC Address 64949903.70da System Time 2022-07-28 10-	cPU Usage	10.1 %
 ➡ Diagnosis → ➡ Maintenance → 	Model \$5860-2050 Filmware Version \$5840. ECIC 4.9 CALIFORM 4.4 CALIFOR	X Memory Usage	55.9%
	Device Port	s? Selected 🗈 AG Port 🔳 Up 🔳 Shutdown	SU VSL Port BFD Port
		1 1 4 720 11 4 720 11 4 720 11 4 720 11 4 720 11 4 720 11 2 3 4 400 Breator 10 4 70 10 4 70 1	
	Port Role () Trunk Port () Routed Port	Copper 📰 Fiber	40Gb 40Gb(Splited)
	Traffic Summary Mg1/0_IP manage v Khps v		
	Kops 300 -		🛢 Tx Traffic 🍵 Rx Traffic

Quick query menu

The system has more and more functions, and the quick query menu is convenient for users to quickly find the functions they want.

FS 55860-205Q	Monitoring > SWITCH Overview	Q DHCP Relay	🗄 Config Wizard 🐥 admin
Favorites 2		DHCP Settings	
Monitoring	Device Details	DHCP Relay	^
ि Config →	SN G1PC135000034 Booted on 2022-07-1816-30-49	CPU Usage	10.5 %
🔄 Diagnosis 🔷	Model/S5640-205Q Fritmante Version 5586/5051254(80151, Release(09182001) Uptime 4 d 18 h 16 min 12 s Handwer Version 5580/5051254(80151, Release(09182001) Uptime 4 d 18 h 16 min 12 s	Memory Usage	55.9%
A Maintenance			
	Device Port	Selected 🔟 AG Port 📕 Up 📕 Shutd	own 🔲 VSL Port 📑 BFD Port
		20 21 x ¥22 21 x ¥34 1 2 3 4 400 Be	aland
	Port Role (1) Trunk Port (1) Routed Port	Copper 📰 Fiber	40Gb 40Gb(Splited)
	Traffic Summary Mg1/0_IP manage v Kbps v		a sint
	10ps		Tx Traffic

More functions of the system

1. Show current account

e	FS		osq 🚹	Monitoring > SWITCH Overview				search term	🗄 Config Wizard 🐥 admin 🗸
•		:5 📿							
	Monitor	ring	>	Device Details			^	Device Usage	~
6	Config		5		SN G1PC135000034	Booted on 2022-07-18 16:30:49		CPU Usage	10.5 %
₿			>	Model55860-205Q	Firmware Version 55860_FSO5 12.5(4)B0151, Release(09182801)	Uptime 4 d 18 h 16 min 40 s		Memory Usage	56.0%
R	Mainter	nance	X		Hardware Version 1.00				

2. online service

Click on the online customer service on the page to jump to the online customer consultation question

€FS 55860-205Q .	Monitoring > SWITCH Overview	Q Enter a search term	🗄 Config Wizard 👌 admin 🗠
Favorites 2			Online Service Logout
Monitoring	Device Details	O Device Usage	
Config >	SN GIPC135000034 Booted on 2022-07-18 16:30:49 MCC Address 4494(9940.704a System Time 2022-07-23 10:47:51	CPU Usage	9.1 %
🔁 Diagnosis 🔷	Model55860-205Q Firmware Version 55860_FS06 12.5(4)80151, Release(09182801) Uptime 4 d 18 h 17 min 03 s	Memory Usage	56.0%
🛱 Maintenance >	Hardware Version 1.00		
	Device Port	Selected 🔳 AG Port 🔳 Up 🔳 Shutdo	wn 🔲 VSL Port 🔲 BFD Port
		12 31 ± ¥ 22 22 ± ¥ ¥ ¥ 1 2 3 4 405 Brak Y A ¥ A ¥ Y Y Y Z5 20 400 400 400 25	ad
	Port Role	Copper 📰 Fiber	40Gb 40Gb(Splited)
	Traffic Summary Mg1/0_IP manage v Kbps v		
			Tv Traffle Rv Traffle

3. Exit system

FS 55860-205Q	C Enter a search term	🗄 Config Wizard 📍 admin 🗡
Favorites 2		 Online Service Logout
Monitoring	Device Details ^ Devi	ce Usage
Config →	SN G1PC135000034 Booted on 2022-07-18 16:30:49 MAC Address 649419901 20da System Time 2022-07-23 10:48:30	Isage 9.1 %
🔁 Diagnosis >	ModelS5860-20SQ Firmware Version 55860_FSOS 12.5(4)B0151, Release(09182801) Uptime 4 d 18 h 17 min 42 s Memory	ry Usage 56.1%
🛱 Maintenance >	Hardware Version 1.00	
	Device Port Selected AG Port	: Up 🖬 Shutdown 🗊 VSL Port 📑 BFD Port
		1 2 3 4 40G Breakout 25 40G
	Port Role 0 Trunk Port 0 Routed Port	Copper Fiber 40Gb 🕂 40Gb(Splited)
	Traffic Summary Mg1/0_IP manage v Kbps v	

1.4 Open WEB Server

When the switch leaves the factory, the WEB service is turned on, and the default IP: 192.168.1.1

The following describes how to open it under CLI when the WEB service is closed.

Configuration item	Related commands		
	enable service web-server	Open WEB service	
www.fs.com		75	
Configure WEB server	ip address	Optional configuration IP address	
----------------------	-----------------------------------	--	
	webmaster level username password	Optional configuration, login account password	
		information for WEB management	

Configuration method

☆ Open WEB service

- ≓ Must be configured.
- \Rightarrow Configure on the switch.

☆ Configure IP address

 \Rightarrow Optional.

 $\stackrel{\scriptstyle }{
m M}$ Configure the account and password information for logging in to WEB management

≓ Optional.

÷ When the WEB service is turned on, the default administrator account admin/admin is created. The account password can be

modified.

Testing method

Log in to the WEB interface through the set IP address and the account password of WEB management to check whether you can log in

normally.

Related commands

☆ Start WEB service

[Command format]	enable service web-server [http https all]
[Parameter Description]	http https all: Open the corresponding service. http is to open HTTP service, https is to open HTTPS service, all is to open HTTP and HTTPS service at the same time. The default is to enable both HTTP and HTTPS services.
[Command Mode]	Global mode

☆ Configure IP address

[Command format]	ip address ip-address ip-mask
[Parameter Description]	<i>ip-address :</i> ip address <i>ip-mask :</i> Netmask
[Command Mode]	Interface mode

\bigstar Configure the account and password information for logging in to WEB management

[Command format]	webmaster level privilege-level username name password { password [0 7] encrypted-passw
[Parameter Description]	privilege-level: User binding privilege level, divided into three levels: 0/1/2. The default super
	administrator account admin corresponds to level 0 permissions, and other manually created accounts correspond to level 1.
	name: The address of the static RP.
	password: Use ACL to limit the group address range of the static RP service. The default is to serve all
	groups.
	$0 \mid 7$: The encryption type of the password, 0 is no encryption, 7 is simple encryption. The default is 0.
	encrypted-password: password text.
[Command Mode]	Global mode
[User guides]	-

Configuration example

[Configuration method]	Open WEB service
	• Configure the device management IP. The default management VLAN is VLAN 1. Configure the IP
	of VLAN 1. Ensure that the user PC can ping the management IP.
	FS# configure terminal
	FS(config)#enable service web-server
	FS(config)# webmaster level 0 username test password test
	FS(config)#interface vlan 1
	FS(config-if-VLAN 1)#ip address 192.168.1.200 255.255.255.0
	FS(config)# end
[Testing method]	View related commands through show running-config.
	FS(config)#show running-config
	Building configuration
	Current configuration : 6312 bytes
	!
	hostname FS
	1
	!
	webmaster level 0 username test password test //WEB management authentication user name and
	password, password encryption display
	http update mode auto-detect
	!
	interface VLAN 1
	ip address 192.168.1.200 255.255.255.0 //Device management IP
	no shutdown
	!
	line con 0
	line vtv 0.4
	login
	1
	!
	End