

Ruijie RG-S5300-E Series Switches

RG-5300-E_RGOS 12.5(4)B0701 Web-based Configuration Guide

Document Version: V1.3 Date: January 29th, 2023 Copyright © 2023 Ruijie Networks

Copyright

Copyright © 2023 Ruijie Networks

All rights are reserved in this document and this statement.

Any reproduction, excerption, backup, modification, transmission, translation or commercial use of this document or any portion of this document, in any form or by any means, without the prior written consent of Ruijie Networks is prohibited.



All other trademarks or registered trademarks mentioned in this document are owned by their respective owners.

Disclaimer

The products, services, or features you purchase are subject to commercial contracts and terms. Some or all of the products, services or features described in this document may not be within the scope of your purchase or use. Unless otherwise agreed in the contract, Ruijie Networks does not make any express or implied statement or guarantee for the content of this document.

Due to product version upgrades or other reasons, the content of this document will be updated from time to time. Ruijie Networks reserves the right to modify the content of the document without any notice or prompt.

This manual is for reference only. Ruijie Networks endeavors to ensure content accuracy and will not shoulder any responsibility for losses and damages caused due to content omissions, inaccuracies or errors.

Preface

Intended Audience

This document is intended for:

- 1) Network engineers
- 2) Technical support and servicing engineers
- 3) Network administrators

Technical Support

- 4) Ruijie Networks Website: <u>https://www.ruijienetworks.com/</u>
- 5) Technical Support Website: <u>https://ruijienetworks.com/support</u>
- 6) Case Portal: <u>https://caseportal.ruijienetworks.com</u>
- 7) Community: <u>https://community.ruijienetworks.com</u>
- 8) Technical Support Email: <u>service_rj@ruijienetworks.com</u>
- 9) Live Chat: https://www.ruijienetworks.com/rita

Conventions

1. Conversions

Convention	Description
Bold font	Commands, command options, and keywords are in bold font.
Italic font	Arguments for which you supply values are in <i>italic</i> font.
[]	Elements in square brackets are optional.
{ x y z }	Alternative keywords are grouped in braces and separated by vertical bars.
[x y z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
&<1-n>	The argument before the sign (&) can be input for consecutive 1- n times.
//	Double slashes at the beginning of a line of code indicate a comment line.

2. Signs

The signs used in this document are described as follows:

Warning

An alert that calls attention to important rules and information that if not understood or followed can result in data loss or equipment damage.

🛕 Caution

An alert that calls attention to essential information that if not understood or followed can result in function failure or performance degradation.

1 Note

An alert that contains additional or supplementary information that if not understood or followed will not lead to serious consequences.

Specification

An alert that contains a description of product or version support.

3. Note

The manual offers configuration information (including model, port type and command line interface) for indicative purpose only. In case of any discrepancy or inconsistency between the manual and the actual version, the actual version prevails.

1 Configuring Switch Eweb

1.1 Overview

Users can access the Web management system (that is, Eweb) of switches through a browser (such as Internet Explorer (IE)) to manage the switches.

Web management involves the Web server and Web client. The Web server, integrated into the switch, is used to receive and process requests from a client (reading Web files or executing commands), and return processing results to the client. The Web client is usually a Web browser, such as IE.

This document applies only to S5300-E and S5310-E series switches.

The Eweb and device cannot be configured in a hybrid manner. After the device is configured, the Eweb needs to be refreshed, for example, you can press F5 for refreshing.

1.2 Applications

Application	Description
Managing Devices by Using the	After switches are configured, you can access the Eweb through a browser.
<u>Eweb</u>	

1.2.1 Managing Devices by Using the Eweb

Scenario

As shown in the figure below, you can access the Eweb of an access switch or distribution switch through a browser to manage and configure the switch.



Remark	The device enclosed in the red rectangle in the figure above is the accessed switch. Ensure that the switch can
s	be pinged successfully from the PC. Then, you can access the Eweb of the switch.

Deployment

U Configuration Environment Requirements

Client requirements:

- Network administrators can log in to the Eweb graphical user interface (GUI) of a switch from a browser to manage the switch. Clients refer to PCs or other mobile terminals such as laptops.
- Browser: IE9–IE11, Google Chrome, and 360 Browser are supported. Exceptions such as garble or format error may
 occur if an unsupported browser is used.
- Resolution: You are advised to set the resolution to 1024 x 768, 1280 x 1024, 1440 x 960, or 1920 x 1080. If other resolutions are used, the page fonts and formats may not be aligned, the GUI is less artistic, or other exceptions may occur.
- Eweb configuration and command line interface (CLI) configuration can be performed at the same time. After CLI configuration is complete, enter the write command to save the configuration. If a Web page is opened, refresh the page to ensure synchronization between the Eweb configurations and CLI configurations.

Logging In to the Web Management Platform

Enter http://X.X.X.X (management IP address) in the browser and press **Enter** to open the login page, as shown in the figures below.



 Official Website
 Service Portal
 Service Mail
 Cookbook Download

 19/10/11 and Google Chrome browsers are recommended
 ©2000-2022 Ruijie Network



Enter the username and password and click Login. The following table provides the default username and password.

Default Username/Password	Permission Description
admin / admin	Super administrator with all permissions

The default username is displayed in output of the show running-config command only after its default password is changed.

After authentication is successful or the password is changed, the homepage of the Eweb is displayed, as shown in the figure below.

Ruíjie sw	표 @ Monitoring @ Config 왕 Diagnosis 🗙 Mainte	nance	Enter a search term Q S Config Wize	ard 📾 🗛 admin 🗎
😭 Favorites 🛛 🗿	S53E			O Refresh
SWITCH Overview	Model: SS300-48GT4XS-E	(a) 9.3% CPU Usage	B 48.2%	
Anti-loop Monitoring + IN DHCP + IV Other Monitoring +	SN: G1QC2N0000484 MAC Address: 5416.5156.6554 Firmware Version: 521 Hardsare Version: 1.21 Bostet on: 1707-0-101 000000 Uptime: 3 d 21 h 15 min 24 s System: Time: 1970-01-04 211522	90.7N	51.8N 48.2N	
	Selected 1 AD Port Up Shutdoon VEL Port Image: Selected 1 AD Port Image: Selected VEL Port Image: Selected 1 AD Port Image: Selected Image: Selected Image: Selected 1 AD Port Image: Selected Image: Selected Image: Selected Image: Selected 1 AD Port Image: Selected Image			Copper Fiber

For details about Eweb pages, see "Eweb Management System."

1.3 Eweb Management System

Basic Concepts

**** Icons and Buttons on the GUIs

Icon/Button	Description
Edit	Edit. Click this icon to edit the selected record.
Delete	Delete.
ON	Function enabling/disabling icon.
	Available port. After you click or select the icon, the port becomes selected.
	Shutdown port.
	Selected port.
20	Aggregate port. The digit in the port indicates the aggregate port number.
[]	Trunk port. It is displayed on the panel of the VLAN/VLAN Settings page.
	The port is powered on.
•	Virtual switching link (VSL) port.
	Bidirectional forwarding detection (BFD) port. It is displayed on the panel of the SWITCH
	Overview page.
	40G port.
-=	40G port that has been split.
Save	Save. Click it to submit and save input information.
+	Click it to add settings.
×	Click it to delete settings.
*	Required item. An input box marked with this symbol indicates a required item.
0	Note symbol.
	Caution symbol.

System Operations

Device panel

Selected 1 AG Port I Shutdown 🕑 VSL Port	Copper Eiber
2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 40 42 44 46 48 50 52	
Port Role: 🕜 Trunk Port 🐵 Routed Port	

Overview

The following table describes feature configurations of the second-level menu items in the left navigation tree of the Web GUI.

Feature	Description		
Config Wizard	Helps you build a network by using the devices.		
SWITCH Overview	Displays port information and overall device information.		
STP Status	Displays the Spanning Tree Protocol (STP) status and port roles.		
RLDP Status	Displays the Rapid Link Detection Protocol (RLDP) status and ports, on which RLDP is enabled.		
Client List	Displays addresses allocated by a switch address pool.		
Server Status	Displays the DHCP server and configured address pools.		
VSU Status	Displays the virtual switching unit (VSU) topology. It exists only when the device works in VSU mode.		
VLAN	Sets VLANs and trunk ports.		
Port	Configures basic information about ports, aggregate ports, port mirroring, and port rate limit.		
Routing	Sets routes.		
DHCP	Configures Dynamic Host Configuration Protocol (DHCP), allocates static addresses, ar displays the client list.		
VRRP	Sets Virtual Router Redundancy Protocol (VRRP).		
MAC Address	Sets static addresses and filter addresses.		
VSU Settings	Configures the standalone mode and VSU mode for the device for switching.		
STP	Configures STP global basic information and STP ports.		
RLDP Settings	Configures RLDP globally and port RLDP.		
ACL	Configures access control lists (ACLs) and ACL time, and applies ACLs.		
Port Security	Configures port security and security binding.		
Storm Control	Control storms.		
DHCP Snooping	Sets DHCP snooping.		
Gateway Anti-ARP-	Configures anti-ARP spoofing on the gateway, Address Resolution Protocol (ARP) check,		
Snooping	dynamic ARP inspection (DAI), and ARP entries.		
IP Source Guard	Configures ports and user binding.		
NFPP	Displays information related to Network Foundation Protection Policy (NFPP).		
IGMP Snooping	Sets Internet Group Management Protocol (IGMP) snooping.		

QOS	Configures classes, policies, and flows.
DHCP Relay	Sets the DHCP relay.
Authentication	Configures ePortal and advanced settings.
Ping	Detects the connectivity of an IP address or domain name.
Tracert	Uses tracert to detect an IP address or domain name.
One-click Collection	Collects information on the device in one-click mode.
Display System Log	Sets the syslog server and queries system logs.
Monitor System Log	Queries logs by level or module name.
Upgrade	Performs local upgrade.
Restart	Restarts the device.
Config MGMT	Backs up configurations, restores factory settings, and sets system character sets.
Systime	Sets the system time.
Syslog	Configures whether to enable the logging function on the device.
DNS	Sets domain name system (DNS).
Web	Configures the administrator password, basic settings, and administrator permissions.
Telnet	Configures the telnet and Secure Shell (SSH) functions, and password.
SNMP	Sets SNMPv2 and SNMPv3.

1.3.1 Config Wizard

표 🛛 Monitoring 🛛 👳 O		Enter a search term Q 🚔 Config Wizard 🛷 🗚 admin
S53E Model: S5300-48GT4XS-	e 8.1% couldage	Click Config Wizard. The Config Wizard window is discloved
SN: G1QC2N9000484	Config Wizard	x
MAC Address: 5416.5158.6554 Firmware Version: 55300E_RGOS 12 Hardware Version: 1.21	🚯 Device 🖂 Terminal Port 🔤 Bridge Port 🧼 🧭 Security	
Booted on: 2022-07-28 15:00:51	Config Mode: Layer 2 Layer 3	47.1%
Uptime: 0 d 20 h 53 min 34 s System Time: 2022-07-29 11:54:25	Management Port: MGMT Port OMGMT VLAN	
	Management Port: Mgmt 0 🗸	
	* IP Address: 172.26.147.230	
Selected 1 AG Port 💼 Up	* Submask: 255.255.255.0	Copper Fiber
	* Gateway: 172.26.147.1	
	DNS Server:	
Port Role: 🗊 Trunk Port 🛎 Routed		•
Traffic Commons Contra	Next	

Device

Config Wizard				×
Device	🗊 Terminal Port	🖾 Bridge Port	Security	~
Config Mode:	● Layer 2 ○ Layer 3			
Management Port:	● MGMT Port ○ MGMT VLAN	I		
Management Port:	Mgmt 0 🗸			
* IP Address:	172.26.147.183			
* Submask:	255.255.255.0			
* Gateway:	172.26.147.1			
DNS Server:				
Reset Time:	● PC Time ○ Custom			
Time Zone:	UTC+8(Beijing, CCT)			
* Charset:	Default 🗸			
		_		
* Submask: * Gateway: DNS Server: Reset Time: Time Zone: * Charset:	255.255.255.0 172.26.147.1 • PC Time • Custom UTC+8(Beijing, CCT) • Default •	Next		

The steps of configuring device management are as follows:

- 1) Configure **Config Mode**. This option is displayed for L3 devices.
- 2) Select **MGMT Port** and configure **Management Port**.
- 3) Configure **Submask**. A network segment that has been assigned to a port cannot be assigned to the port.
- 4) **DNS Server** is an incremental parameter.
- 5) Configure the system character set in **Charset**.
- 6) Click Next.
- Terminal Port

Config Wizard				×
O Device	Terminal Port 😁 🖻 E	iridge Port 🖻 Routed	Port 🖻 Gateway	🧿 Security 🗸
Note: Terminals include PCs, pri	nters, monitors and APs.			
Terminal Port				+ Add
Port ID Port S	tatus VLAN		Description	Action
Gi0/1 🗸 Ena	ble			Delete



The steps of configuring a terminal port are as follows:

- 1) Click **Add** to add a terminal port.
- 2) **Port ID** must be unique.
- 3) Click **Delete** to delete the terminal configuration.
- 4) Click **Next** after completing the configuration.
- Bridge Port

Device	nfig Wizard							
ote: The bridge port refers to the port used to access the switch. ridge Port Ort ID Port Status Allowed VLAN Native VLAN Description Action Gi0/1 Y Enable	Device	🕑 Termir	nal Port 🗵 Bridg	e Port 🚥 🖆	Routed Port	🖻 Gateway	🛛 Security	\
ridge Port Ort ID Port Status Allowed VLAN Native VLAN Description Action Gi0/1 Cliphic Cliphic Cliphic Cliphic Deleter	ote: The bridge	e port refers to the po	rt used to access the switch.					
Ort ID Port Status Allowed VLAN Native VLAN Description Action Gi0/1 III IIII IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	idge Port							+ %
	ort ID	Port Status	Allowed VLAN		Native VLAN	Description	Actio	n
	Gi0/1 🖌	🗹 Enable					Dele	ete
Previous				Previous	Next			

The steps of configuring a bridge port are as follows:

- 1) Click **Add** to add a bridge port.
- 2) **Port ID** must be unique.
- 3) Click **Delete** to delete the bridge port.
- 4) Click **Next** after completing the configuration as prompted.
- Routed Port

nfig Wizard					
Device	🥑 Termina	al Port 🛛 🕑 Bridge F	ort 🖪 Route	d Port 👘 Gateway	Security 🗸
lote: The routed	d port serves layer 3	interconnection.			
outed Port					+ 添
Port ID	Port Status	IPv4 Address	Submask:	Description	Action
Gi0/1 🖌	🗸 Enable				Delete
			Previous Next		

The steps of configuring a routed port are as follows:

- 1) Click **Add** to add a routed port.
- 2) **Port ID** must be unique.
- 3) Click **Delete** to delete the routed port.
- 4) Click **Next** after completing the configuration as prompted.
- Gateway

Config Wizard				×
⊘ Device ⊘	Terminal Port <table-cell></table-cell>) Bridge Port 🔗 Rou	Ited Port 🛅 Gateway	Security 🗸 🗸
Note: Gateway is a link betw	veen two VLANs at layer :	3. It is recommended to configure	a gateway for each VLAN.	
Gateway				+ 添加
Allowed VLAN	Gateway	IPv4 Address	Submask:	Action
	Enable			Delete

The steps of configuring a gateway are as follows:

- 1) Click **Add** to add a gateway.
- 2) Click **Delete** to delete the gateway.
- 3) Click **Next** after completing the configuration as prompted.
- Security

Config Wizard	×
Oevice	📀 Terminal Port 🛇 Bridge Port 🛇 Routed Port 🥥 Gateway 🧭 Security 🗸
Note: Default rou	ting is enabled by default. If there are multiple routed ports, priority will be assigned to these ports based on record ID.
Default Routing:	Z Enable
SPT:	✓ Enable
Port Fast:	✓ Enable
RLDP:	✓ Enable
	Previous Next

Select the functions to be enabled and click Next.

• Saving configurations

Config Wizard		×
Oevice	🕑 Terminal Port 🥥 Bridge Port 🧭 Routed Port 🥥 Gateway 🛇 Security 🥑	
Device		
Management Por	t: Mgmt 0	
IP/Submask:	172.26.147.183 / 255.255.255.0	
Gateway:	172.26.147.1	
DNS Server:		
Time Zone:	UTC+8(Beijing, CCT)	
Reset Time:	PC Time	
Charset:	Default	
Security		
Default Routing:	: Enable	
SPT:	Enable	
Port Fast:	Enable	
RLDP:	Enable	
	Previous Save	

Check the configurations and click **Save** to deliver configuration commands. After the configuration succeeds, the **Config Wizard** window automatically disappears. If you change the management IP address of the device, determine whether to redirect to the new management address and perform operations above.

1.3.2 Monitoring

Click Monitoring to open the level-2 menu, which includes SWITCH Overview, Anti-loop Monitoring, DHCP, and Other Monitoring.

1.3.2.1 SWITCH Overview

The **SWITCH Overview** page displays basic information about the device, including the device MAC address, device model, device running time, version information, device CPU and memory, port status, port traffic trend, and port bandwidth usage.

Standalone scenario



Traffic Su	Immary Gi0/1 • Kbps •	Select the port and unit and view tr	affic information in the traf	fic diagram.	
Kbps		-			● Tx Traffic ● Rx Traffic
35					
25					
15 10					
5					Time
13:35:23	13:35:30	13:36:00	13:36:30	13:37:00	13:37:18
Top5 Por	ts by Bandwidth Usage			Click More to display bandwidth information of a	all ports. 🔶 More
Port	Input Rate	Output Rate		Status(Port real speed)	
Gi0/1	0.010%	0.0	10%	Connected(1000M)	

For the Top 5 ports in bandwidth usage, click **More**. A dialog box will be displayed.

⇒ Back → Refresh	× Clear Selected × Clear All					
Interface	Rx Bandwidth Usage ≑	Tx Bandwidth Usage 💲	Status(Port real speed)	UnderSize/OverSize	CRC/FCS Error	Collision Count
Gi0/1	0.010	0.000	Connected(1000M)	0/0	0/0	0
Show No.: 10 🗸	Total Count:1			K First	< Pre (1) Next > Last	Н <mark>1 GO</mark>

1.3.2.2 Anti-loop Monitoring

The Anti-loop Monitoring page monitors the loop status based on the STP status and RLDP status.

1.3.2.2.1 STP Status

The STP Status tab page displays STP Status, STP Mode, Root Status, Instance, and port use status.

STP Status: C Enabled Configure STP	
STP Mode: MSTP	
Root Status: Root	
Instance: 0 •	
Select Port:	
🗋 Selected 🚹 AG Port 💼 up 💼 shutdown	Copper Fiber
Port Role: 🛞 Root Port 🐵 Designated Port 🛞 Alternate Port 🛞 Master Port STP Status: 🕏 Forwarding 🚭 Blocking 🕒 STP Enabled 🔹 Port Fast Enabled	

1.3.2.2.2 RLDP Status

 RLDP Status:

 • Enabled
 • Configure RLDP
 Local MAC: 541651586554
 Select Port:
 • Selected
 • Add Port
 • p
 • Plane
 • Plane

The RLDP Status tab page displays RLDP Status, Local MAC, handling method of port violation, and RLDP status.

1.3.2.3 DHCP

DHCP is monitored from the DHCP server status and DHCP client list.

1.3.2.3.1 Client List

				IP-based v Search
IP IP	MAC	Lease Time	Allocation Type	
			No Data Found	
Show No.: 1	īotal Count:0			K First < Pre Next > Last > 1 GO

The **Client List** tab page displays clients assigned IP addresses in the address pool on the switch.

1.3.2.3.2 Server Status

The Server Status tab page displays the DHCP server status and the usage of the address pool.

DHCP Settings	Static Address	Client Display				
+ Add DHCP × Dele	te Selected ⊘Excluded A	ddress Range DHCP: ON				
		3				
Name	IP Address Range	Default Gat	teway	Lease Time	DNS	Action
		N	o Data Found			
Show No.: 10 V To	otal Count:0			K First	< Pre Next >	Last X 1 GO

1.3.2.4 Other Monitoring

1.3.2.4.1 VSU Status

The device monitors the VSU status only when the device works in VSU mode. You can check the topology of the VSU composed of devices, BFD status, and the status of ports, on which bidirectional forwarding detection (BFD) is enabled.

1.3.3 Config

Click Config to open level-2 menu, which includes Network, Other, Security, and Advanced.

1.3.3.1 Network

1.3.3.1.1 VLAN

The VLAN page consists of VLAN Settings and Trunk Port.

VLAN Settings

VLAN Settings Trunk Po	rt			
J. Dateb Add VI AN J. Add VI AN	M Delete Celected			
	Contraction Contraction			
VLAN ID 🗘	VLAN name	VLAN Status	Port	Action
. 1	VLAN0001	STATIC	Gi0/3,Gi0/7-48,Te0/49-52	Edit
□ 3	VLAN0003	STATIC	Gi0/1	Edit Delete
□ 10	VLAN0010	STATIC		Edit Delete
Show No.: 10 V Total Count:3				K First < Pre 1 Next > Last > 1 GO

Bulk adding VLANs

VLAN Settings Irunk Por	rt			
+ Batch Add VLAN + Add VLAN	× Delete Selected			
□ VLAN ID \$	VLAN name	VLAN Status	Port	Action
. 1	VLAN0001	STATIC	Gi0/3,Gi0/7-48,Te0/49-52	Edit
3	VLAN0003	STATIC	Gi0/1	Edit Delete
□ 10	VLAN0010	STATIC		Edit Delete
Show No.: 10 V Total Count:3		Batch Add VLAN	>	K First < Pre 1 Next > Last > 1 GO
		VLAN ID: 10-20	• Range: 3-5,20	
			Cancel	

The steps of bulk adding VLANs are as follows:

- 1) Click Batch Add VLAN.
- 2) Enter VLAN IDs or ranges, which can be separated by commas (,).
- 3) Click Save. The message "Add Succeeded" is displayed and the added VLANs are displayed in the list.
- Adding a VLAN

VLAN Settings	Trunk Port						
+ Batch Add VLAN +	Add VLAN 🗙 Delete Selec	cted					
ULAN ID 🗘	VLAN	l name VL	AN Status	Port		Action	
. 1	VLAN	Add VLAN			×	Edit	
□ 3	VLAN					Edit Delete	
18	VLAN	VLAN ID:	* Range: 1-4094			Edit Delete	
19	VLAN	VLAN name:				Edit Delete	
□ 20	VLAN	Salact Part				Edit Delete	
Show No.: 10 - Tot	tal Count:5	Selected 1 AG Port 1 Tru	nk Port		Copper Fiber	st < Pre 🚺 N	lext > Last > 1 GO
		1 3 5 7 0 11 2 4 6 8 10 12 4 All Invert Deselect	13 15 17 19 21 23 14 15 17 19 21 24 14 16 18 20 22 24 Note:Click and hold	$\begin{array}{cccccccccccccccccccccccccccccccccccc$	37 39 41 43 45 47 30 40 42 44 46 48 , across the section to select multiple ports.		
			Cancel	Save			

The steps of adding a VLAN are as follows:

- 1) Click Add VLAN.
- 2) (Required) Enter the VLAN ID.
- 3) (Optional) Enter the VLAN name.
- 4) (Optional) Select ports.
- 5) Click Save. The message "Add Succeeded" is displayed and the added VLAN is displayed in the list.
- Editing a VLAN

VLAN	Settings	Trunk Port				
🕂 Batch		Add VI AN 🗙 Dele	te Selected			
1 Daten	Add VEAR					
	VLAN ID 🗘	VI	AN name	VLAN Status	Port	
	Edit VLAN					×
						A
	VLAN	ID: 21	* Range: 1-4094			
	VLAN nam	ne:				
	Select Po	ort:				
	Selected	AG Port Trun	k Port		Copper Fiber	
Show		5 7 9 11 ~~		25 27 29 31 33 35 [^_][^][^][^][^][^]	37 39 41 43 45 47 [^_][^][^][^]	
	2 4	6 8 10 12	14 16 18 20 22 24	26 28 30 32 34 36	38 40 42 44 46 48	
						-
			Cance	Save		

The steps of editing a VLAN are as follows:

- 1) Click **Edit** in the **Action** column for a VLAN to be edited. Information about the VLAN is displayed in the pop-up dialog box.
- 2) Change the VLAN name.
- 3) Select ports.
- 4) Click **Save**. The message "Edit Succeeded" is displayed, indicating the editing is successful.
- Deleting a VLAN

+ Batch Add VLAN + Add VLAN × Delete Selected VLAN ID : VLAN name VLAN Status Port Action 1 VLAN 0001 STATIC Gi0/3,Gi0/7-20,Gi0/22-48,Te0/49-52 Edit 3 VLAN003 STATIC Gi0/1 Edit Delete 18 VLAN018 STATIC Gi0/1 Edit Delete 19 VLAN019 STATIC Edit Delete 20 VLAN020 STATIC Edit Delete 21 VLAN0021 STATIC Edit Delete Shorw No: [10] Total Count5 K First < Pre Next > Last > 1 G	VLAN Settings	Trunk Port			
VLAN ID * VLAN name VLAN Status Port Action 1 VLAN0001 STATIC Gi0/3,Gi0/7-20,Gi0/22-48,Te0/49-52 Edit Edit	+ Batch Add VLAN + Add	VLAN X Delete Selected			
1 VLAN0001 STATIC Gi0/3,Gi0/7-20,Gi0/22-48,te0/49-52 Edit 3 VLAN0013 STATIC Gi0/1 Edit Delete 18 VLAN0018 STATIC Gi0/1 Edit Delete 19 VLAN0019 STATIC Edit Delete 20 VLAN0020 STATIC Edit Delete 21 VLAN0021 STATIC Edit Delete Show No.: 10 V Total Count/S K First < Pre ① Next > Last 》 1 GO Cancel OK	ULAN ID 🗘	VLAN name	VLAN Status	Port	Action
3 VLAN0003 STATIC Gi0/1 Edits Delete 18 VLAN018 STATIC Gi0/1 Edits Delete 19 VLAN019 STAT Gid Delete 20 VLAN0020 STAT Gid Delete 21 VLAN0021 STAT Gid Delete Show No: Total Counts/ K First < Pre ① Next > Last > 1 Gid	□ 1	VLAN0001	STATIC	Gi0/3,Gi0/7-20,Gi0/22-48,Te0/49-52	Edit
18 VLAN0018 STATC 19 VLAN0019 STAT 20 VLAN0020 STAT 21 VLAN0021 STAT Show No: Total Count/5 K First < Pre ① Next > Last > 1 GB	3	VLAN0003	STATIC	Gi0/1	Edit Delete
19 VLAN0019 STAT X 20 VLAN0020 STAT X 21 VLAN0021 STAT Show No.: 10 v Total Count/5 Cancel OK	18	VLAN0018	STATIC		Edit Delete
20 VLAN0020 STAT 21 VLAN0021 STAT Show No.: 10 Total Count.6 Cancel OK	19	VLAN0019	STAT	×	Edit Delete
21 VLAN0021 STAT Show No:: 10 v< Total Count.6 Cancel OK	20	VLAN0020	STAT		Edit Delete
Show No.: 10 V Total Count.6 K First < Pre 1 Next > Last X 1 GO	21	VLAN0021	STAT The	you sure you want to delete VLAN?	Edit Delete
	Show No.: 10 🗸 Total Co	unt6		Cancel OK	K First < Pre (1) Next > Last > 1 GO

The steps of deleting a VLAN are as follows:

- 1) In the VLAN list, select multiple records and click **Delete Selected** to bulk delete the records.
- 2) In the VLAN list, click **Delete** in the **Action** column for a VLAN to be deleted. The message "Are you sure you want to delete the VLAN?" is displayed. Click **OK**. The message "Delete Succeeded" is displayed and the VLAN is deleted.

(i) VLAN1 is the default VLAN. It can be only modified but cannot be deleted.

I Trunk Port

VLAN Settings	Trunk Port	
Note: If a port allows mul	+ VLAN packets to go through, configure it as a trunk port. It is recommended to configure the port connected to the network device as a trunk port.	
Native VLA	1 * Ranger 1-4094	
Allowed VL/	1-4994 Example(3-5,200)	
Select Po		
Selected 1 AG P	Up 📩 Shutdown 💽 VSL Port	Copper Fit
] [], [], [], [], [], [], [], [], [], []	
All Invert Deselect	Note:Click and hold the left button as you drag	the pointer across the section to select multiple po
	Save	

Adding a trunk port

VLAN Settings	Trunk Port	
Note: If a port allows mi	ultiple VLAN packets to go	through, configure it as a trunk port. It is recommended to configure the port connected to the network device as a trunk port.
🔁 Select All 🛛 🛅 Desel	ect All 🍵 Batch Dele	e
Gi0/9		
Native VI	LAN: 1	* Range: 1-4094
Allowed VI	LAN: 1-4094	Example(3-5,200)
Select I	Port:	
Selected 1 AG	Port 🛑 Up 💼 Shut	lown 🕑 VSL Port
		17 19 21 23 25 27 29 31 33 35 37 39 41 43 45 47 49 51
	10 12 14 16	Image: Constraint of the
All Invert Deselect		Note:Click and hold the left button as you drag the pointer across the section to select multiple ports.
	Save	Cancel

The steps of adding a trunk port are as follows:

- 1) Select a port on the panel.
- 2) Set Native VLAN and Allowed VLAN. Native VLAN is required and Allowed VLAN is optional. You can enter a range or a specific VLAN ID.
- 3) Click **Save**. The message "Configuration Succeeded" is displayed and the add operation is completed. The added trunk port is displayed in the trunk port list.
- Editing a trunk port

VI AN Settings	Trunk Port				
VEAN Settings	ITUIK POIL				
Note: If a port allows m	ultiple VLAN packets to go	through, configure it as a trunk port. It is recommended to a	onfigure the port connected to the netwo	k device as a trunk	port.
🔁 Select All 🛛 🗂 Desel	lect All 🝵 Batch Dele	te			
Gi0/9 Gi	i0/12 Gi0/17				
Native V	'LAN: 20	* Range: 1-4094			
Allowed V	'LAN: 20	Example(3-5,200)			
Select	Port:				
Selected 1 AG	Port 📩 Up 🛄 Shut	tdown 💽 VSL Port			Copper Fiber
			5 37 39 41 43 45 47	49 51	
		1 -	6 38 40 42 44 46 48	50 52	
All Invert Deselect					Note: Click and hold the left button as you drag the pointer across the section to select multiple ports.
	Edit	Cancel			

The steps of editing a trunk port are as follows:

- 1) In the trunk port list, click a trunk port to be edited.
- Edit Native VLAN and Allowed VLAN. Native VLAN is required and Allowed VLAN is optional. You can enter a range or a specific VLAN ID.
- 3) Change the selected port.
- 4) After editing information about the trunk port, click **Edit**. The message "Configuration Succeeded" is displayed, indicating that the edit operation is completed.

• Deleting a trunk port

VLAN Setting	s	Trunk Port					
Note: If a port a	lows multiple	VLAN packets to go through, c	onfigure it as a trunk port. It is r	recommended to configure the port connected to	the netwo	k device as a trunk p	ort.
🔁 Select All 🛛 🖺	Deselect A	II 🝵 Batch Delete					
Gi0/9	Gi0/12	Gi0/17					
Ni	itive VLAN:	1	* Range: 1-4094				
Allo	wed VLAN:	1-4094	Example(3-5,200)		×		
	Select Port:			Are you sure you want to delet the trunk port?	ete		
Selected [1 AG Port	Up 💼 Shutdown 💽	VSL Port				Copper D Fiber
				取消 确定		49 51	
				ل لے الے الے الے الے الے الے الے الے الے	لے الے 46 48	50 52	
All Invert De	select						Note:Click and hold the left button as you drag the pointer across the section to select multiple ports.
		Save Ca	ncel				

The steps of deleting a trunk port are as follows:

- 1) In the trunk port list, move the cursor over a trunk port to be deleted. The 🛞 icon appears. Click this icon to delete the trunk port.
- 2) The message "Are you sure you want to delete the trunk port?" is displayed. Click **OK**. The message "Delete Succeeded" is displayed.
- Bulk deleting trunk ports

VLAN Settings	Trunk Port				
Note: If a port allows mu	ltiple VLAN packets to go thr	ough, configure it as a trunk port. It is n	ecommended to configure the port connected to the netwo	rk device as a trunk	port.
🔁 Select All 🛛 📋 Desele	ect All 🝵 Batch Delete				
Gi0/9 Gi0	/12				
Native VL	AN: 7	* Range: 1-4094			
Allowed VL	AN: 7	Example(3-5,200)	×		
Select F	'ort:		Are you sure you want to delete the trunk port?		
Selected AG	Port 📕 Up 🛄 Shutdow	/n 🚺 VSL Port			Copper Fiber
			取消	49 51	
			ل لے الے الے الے الے الے الے الے الے الے	50 52	
All Invert Deselect					Note:Click and hold the left button as you drag the pointer across the section to select multiple ports.
	Edit	Cancel			

The steps of bulk deleting trunk ports are as follows:

- 1) In the trunk port list, select trunk ports to be deleted and click **Batch Delete**.
- 2) The message "Are you sure you want to delete the trunk port?" is displayed. Click **OK**. The message "Delete Succeeded" is displayed, indicating that the deletion operation is completed.

1.3.3.1.2 Port

The **Port** page allows you to configure basic information about ports, and configure aggregate ports, port mirroring, and port rate limit.

V Port Settings

Port Settings	Aggregate port	Port Mirroring	Rate Limiting					
+ Batch Add + Ad	dd SVI							
L3 Port								
Port	Status	IP		Mask	IPv	6 1	Description	Action
Gi0/5	Up	192.168.1.2		255.255.255.0				Edit Delete
Gi0/6	Up	192.168.28.1		255.255.255.0				Edit Delete
Vlan 1	Up							Edit Delete
显示 10 🗸 条共	\$3条						K 首页 く 上一页 (1) 下	—页〉末页 〉 1 确定
12 Port								
Port		-						
	Status Port	Type Acces	s VLAN	Native VLAN	Permit VLAN	Descri	ption Action	n
Gi0/1	Up ACCE	Type Access	s VLAN	Native VLAN	Permit VLAN	Descri	ption Action	Details
Gi0/1 Gi0/2	Up ACCE Up ACCE	Type Access SS 3 SS 1	s VLAN	Native VLAN 1 1	Permit VLAN	Descri	ption Actio Edit	Details Details
Gi0/1 Gi0/2 Gi0/3	Up ACCE Up ACCE Up ACCE	Type Access SS 3 SS 1 SS 1	s VLAN	Native VLAN 1 1 1 1	Permit VLAN	Descri	ption Actio Edit Edit	Details Details Details
Gi0/1 Gi0/2 Gi0/3 Gi0/4	Up ACCE Up ACCE Up ACCE Up ACCE	Type Acces: SS 3 SS 1 SS 1 SS 1	s VLAN	Native VLAN 1 1 1 1 1 1	Permit VLAN	Descri	ption Action Edit Edit Edit Edit	Details Details Details Details Details
Gi0/1 Gi0/2 Gi0/3 Gi0/4 Gi0/7	Up ACCE Up ACCE Up ACCE Down ACCE Up ACCE	Type Acces: SS 3 SS 1 SS 1 SS 1 SS 1 SS 1	s VLAN	Native VLAN 1 1 1 1 1 1 1	Permit VLAN	Descri	ption Actio Edit Edit Edit Edit Edit	Details Details Details Details Details Details Details
Gi0/1 Gi0/2 Gi0/3 Gi0/4 Gi0/7 Gi0/8	Status Port Up Acces Up Acces Up Acces Down Acces Up Acces	Type Acces: SS 3 SS 1	s VLAN	Native VLAN 1 1 1 1 1 1 1 1 1 1 1	Permit VLAN	Descri	ption Action Edit Edit Edit Edit Edit Edit	
Gi0/1 Gi0/2 Gi0/3 Gi0/4 Gi0/7 Gi0/8 Gi0/8	Status Port Up Acce	Type Access SS 3 SSS 1	s VLAN	Native VLAN 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Permit VLAN	Descri	ption Action Edit Edit Edit Edit Edit Edit Edit	
Gi0/1 Gi0/2 Gi0/3 Gi0/4 Gi0/7 Gi0/8 Gi0/9 Gi0/10	Status Port Up Acce Up Acce	Type Access SS 3 SSS 1 SSS 1	s VLAN	Native VLAN	Permit VLAN	Descri	ption Action Edit Edit Edit Edit Edit Edit Edit Edit	

Bulk setting ports

Port Settings	Aggrega	ite port P	fort Mirroring Rate Limiting	
+ Batch Add +	- Add SVI			
13 Port			Batch Add ×	
Loron				
Port	Statu	IS	Status: Up 🗸	ion Action
Gi0/5	Up		Description:	Edit Delete
Gi0/6	Up			Edit Delete
Vlan 1	Up		Port Mode: Access Port	Edit Delete
显示 10 🗸	景共3条		Access VLAN: * Range: 1-4094	く 上一页 (1) 下一页 > 末页 > 1 確定
L2 Port				
Port	Status	Port Type	Speed: Keep 🗸	Action
Gi0/1	Up	ACCESS	Working Mode: Keep 🗸	Edit Details
Gi0/2	Up	ACCESS	Salart Port	Edit Details
Gi0/3	Up	ACCESS	Capper Fiber	Edit Details
Gi0/4	Down	ACCESS	1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43	Edit Details
Gi0/7	Up	ACCESS		Edit Details
Gi0/8	Up	ACCESS		Edit Details
Gi0/9	Up	TRUNK	All Invert Deselect Note:Click and hold the left button as you drag the pointer across the section to select multiple ports.	Edit Details
Gi0/10	Up	ACCESS		Edit Details
Gi0/11	Up	ACCESS		Edit Details
Gi0/12	Up 网易有道词典	TRUNK	Cancel Save	Edit Details

The steps of bulk setting ports are as follows:

1) Click **Batch Add**. The **Batch Add** dialog box is displayed.

- 2) Set Access VLAN, Speed, and Working Mode. Access VLAN is a required field. Speed and Working Mode are set to Keep, which does not need to be modified.
- 3) Select ports.
- 4) After setting, click **Save**. The message "Configuration Succeeded" is displayed and the ports are displayed in the list, indicating that the batch setting of the ports is completed.
- Editing a port

+ Batch Add + Ad	dd SVI								
L3 Port									
Port	Status		IP		Mask		IPv6	Description	Action
Gi0/5	Up		192.168.1.2		255.255.255.0				Edit Delete
Gi0/6	Up		192.168.28.1	Edit SVI Vlan 1			×		Edit Delete
Vlan 1	Up			(Edit Delete
显示 10 🗸 条共	43条			Status:	Up .			└ 首页 └ 上──页	1 下一页 〉 末页 丬 1 确定
				VLAN ID:	1	* Range: 1-4094			
L2 Port				IPv4地址:		*			
Port	Status	Port Type	Acce			ך ר		Description	Action
Gi0/1	Up	ACCESS	3	子网掩码:					Edit Details
Gi0/2	Up	ACCESS	1	IPv6/Mask:					Edit Details
Gi0/3	Up	ACCESS	1						Edit Details
Gi0/4	Down	ACCESS	1						Edit Details
Gi0/7	Up	ACCESS	1						Edit Details
Gi0/8	Up	ACCESS	1		Cancel Save				Edit Details

The steps of editing a port are as follows:

- 1) In the port list, click **Edit** in the **Action** column for a port to be edited. Information about the port is displayed.
- 2) Edit information. VLAN ID, IPv4 Address, and Mask are required fields.
- After editing, click Save. The message "Configuration Succeeded" is displayed and relevant configuration is displayed in the list, indicating that port editing is completed.

Aggregate Port

Port Settings	Aggregate port	Port Mirroring	Rate Limiting					
Global Configuration								
Note:the aggregate por	t is used to perform traffic alloc	ation according to the selected	load-balance algorithm.					
Load-balan	Load-balance Enhanced Profile							
	Save	Default Settings						
Aggregation Port	Settings							
In order to provide incr	eased bandwidth and redundan	cy, multiple physical ports (mem	ber ports) are combined into	one logical port (aggregate port). An aggregate port contains up to eight member ports, and the aggregate port load balances traffic across these physical ports.				
Aggregate Po	rt ID:	* Range: 1-128						
Port	Type: L2 Port(Switching F	ort) OL3 Interface(Route	d Interface)					
Open I	ACP: 🔿 Yes 💿 No							
Select	Port							
Selected 1 A	S Port 💼 Up 💼 Shutdow	n 🚺 VSL Port		Copper E Fiber				
		7 19 21 23 25	27 29 31 33 35	37 39 41 43 45 47 49 51				
All Invert Deselect				Note:Click and hold the left button as you drag the pointer across the section to select multiple ports.				
	Add	Cancel						

Adding an aggregate port

| Aggregation Port Settings

rder to provide increased bandwidth and redundancy, multiple physical ports (member ports) are combined into one logical port (aggregate port). An aggregate port contains up to eight member ports, and the aggregate port load balances traffic across these physical ports.	
Aggregate Port ID: 10 * Ranger 1-128	
Port Type: L2 Port(Switching Port) O L3 Interface(Routed Interface)	
Open LACP: O Yes 🛞 No	
Select Port:	
] selected 👔 AG Port 💼 Up 🛅 Shuddown 🕑 YSL Port	er
1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43 45 47 49 51 ■□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□	
invert Deselect NoteClick and hold the left button as you drag the pointer across the section to select multiple po	ts.
Add	

The steps of adding an aggregate port are as follows:

- 1) Set Aggregate Port ID.
- 2) Set Port Type to L2 Port (Switch Port) or L3 Interface (Routed Interface).
- 3) Select whether to enable LACP.
- 4) Select ports.
- 5) After configuration, click **Add**. The message "Configuration Succeeded" is displayed, indicating that the aggregate port is added. The port panel displays the successfully added aggregate port.
- Editing an aggregate port

Aggregation Port Settings	
In order to provide increased bandwidth and redundancy, multiple physical ports, imember ports) are combined into one logical port (aggregate port). An aggregate port contains up to eight member ports, and the aggregate port load balances traffic across these physical ports.	
업 Select All ① Deselect All	
AG10 AG15 C	
Aggregate Port ID: 15 * Range: 1-128 Port Type: L2 Port(Switching Port) OL3 Interface(Routed Interface)	
Open LACP: O Yes 💿 No	
Select Port:	Copper Fiber
1 3 5 7 9 11 13 15 17 19 21 22 25 27 28 31 33 35 37 38 41 43 45 47 49 51 ■ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	
All Invert Deselect Note:Click and hold the left button as you drag the pointer across the	section to select multiple ports.
Edit Cancel	

The steps of editing an aggregate port are as follows:

- Aggregate ports displayed on the panel cannot be selected. To edit an aggregate port, click the aggregate port in the aggregate port list. Its member ports become selected. Click a port to deselect it and then click Edit to modify the aggregate port.
- 2) Modify **Port Type** and **Open LACP**.
- 3) You can click a selected member port to deselect it.
- 4) After editing, click **Edit** to complete the editing of the aggregate port.

• Deleting an aggregate port

Aggregation Port Settings		
In order to provide increased bandwidth and redundancy, multiple physical ports (member ports) are combined	into one logical port (aggregate port). An aggregate port con	ains up to eight member ports, and the aggregate port load balances traffic across these physical ports.
Select All 🗈 Deselect All 🕆 Batch Delete	×	
AG10 AG15	Are you sure you want to delete the selected aggregate port(s)?	
Aggregate Port ID: 15 * Range: 1-128	Cancel OK	
Port Type:		
Open LACP: 🔿 Yes 💿 No		
Select Port:		
Selected 1 AG Port 💼 Up 💼 Shutdown 💽 VSL Port		Copper Eiber
1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 3 רקריקריקריקריקריקריקריקריקריקריקריקריקרי	יד 37 39 41 43 45 47 49 51 רא ראר גער 143 15 47 15 1	
	J J	
All Invert Deselect		Note: Click and hold the left button as you drag the pointer across the section to select multiple ports.
Edit Cancel		

In the aggregate port list, move the cursor over an aggregate port and click \bigotimes . The message "Are you sure you want to delete the selected aggregate port(s)?" is displayed. Click **OK** to delete the aggregate port.

• Bulk deleting aggregate ports

Aggregation Port Settings		
In order to provide increased bandwidth and redundancy, multiple physical ports (member ports) are combined	into one logical port (aggregate port). An aggregate port contains up to eight member ports, and the a	ggregate port load balances traffic across these physical ports.
🔁 Select All 🛛 Deselect All 🖀 Batch Delete	×	
AG10 AG15 AG20	? Are you sure you want to delete the selected aggregate port(s)?	
Aggregate Port ID: * Range: 7–128	Cancel OK	
Port Type:		
Open LACP: 🔿 Yes 💿 No		
Select Port:		
Selected 🚺 AG Port 💼 Up 💼 Shutdown 💽 VSL Port		Copper Eiber
	35 37 39 41 43 45 47 49 51	
	Ji Ji<	
All Invert Deselect	Na	texClick and hold the left button as you drag the pointer across the section to select multiple ports.
Add		

In the aggregate port list, select aggregate ports to be deleted and click **Batch Delete**. The message "Are you sure you want to delete the selected aggregate port(s)?" is displayed. Click **OK** to delete the aggregate ports.

Ports with the ARP check function, anti-ARP spoofing, or the MAC VLAN function enabled and monitored ports in port mirroring cannot be added to an aggregate port, and these ports are unavailable on the panel. When you move the cursor over an unavailable port, a message is displayed, indicating that the functions are enabled on the port and the port cannot be selected.

V Port Mirroring

Port Settings	Aggregate port	Port Mirroring	Rate Limiting				
Note: Port mirroring is Tip: A source port can	s the capability to send a copy of not be a destination port.	network packets seen on the s	ource port to the destination po	t for analysis by a network analyzer. Traffic on multi	ele source ports can be mirrored to one sing	le destination port.	
Ses	ssion ID:	* Range(1-4)					
Monitor	Packets: All Packets	~					
Select Sour	rce Port: (You can select multip	le ports, but it may affect devic	ce performance.)				
Selected AG F	Port						Copper Fiber
				39 41 43 45 47 49 51			
2 4 6 8	10 12 14 16 18	20 22 24 26 28	یا لے یا لے یا لے یا لے یا لے 8 30 32 34 36 3	40 42 44 46 48 50 52			
All Invert Deselect						Note:Click and hold the left button as you drag the pointer	across the section to select multiple ports
Select Dest	ination Port: (You can select o	nly one port.)					
Selected AG	Port						Copper Fiber
	9 11 13 15 17 1 1 10			39 41 43 45 47 49 51			
2 4 6 8	LULU LULU 10 12 14 16 18	لوں لیا لیا لیا ل 20 22 24 26 26	بالريالريالريالريا لر 8 30 32 34 36 3	40 42 44 46 48 50 52			
	Save	cancel					

The steps of configuring port mirroring are as follows:

- 1) Enter the session ID.
- 2) Select a source port.
- 3) Select a destination port.
- 4) Click Save. The message "Configuration Succeeded" is displayed. The configured session is displayed on the GUI.
- The panel displays the current port mirroring status, and both the source and destination ports can be edited. If you want to abandon a modification to port information, click **Refresh** to restore the panel to the current port mirroring status.

A member port of an aggregate port cannot be configured as the source or destination port, and the source and destination ports cannot be the same.

Nate Limiting

Port Settings	Aggregate port	Port Mirroring	Rate Limiting		
+ Batch Add × Bat	h Delete				
		1.000			
Port	Input Rate-Li	imit (KBps)		Output Rate-Limit (RBps)	Action
Gi0/11	0			100000	Edit Delete
Show No.: 10 V	tal Count:1				K First < Pre 1 Next > Last > 1 GO

• Adding a rate-limited port

	egate port Port Mirror	ing Rate Limiting	
+ Batch Add × Batch Delete			
Port	Input Rate-Limit (KBps)	Output Rate-Limit (KBps)	Action
🗆 Gi0/11	0	100000	Edit Delete
Show No.: 10 V Total Count:			K First < Pre 1 Next > Last > 1 GO
		Batch Add X	
		Select Port: Select Port: Se	
		Cancel	

The steps of adding a rate-limited port are as follows:

- 1) Click Batch Add.
- 2) Select a port.
- 3) Set the input rate limit and output rate limit.
- 4) After configuration, click **Save**. The message "Configuration Succeeded" is displayed, indicating that the rate-limited port is added. The port is displayed in the port rate limit list.
- Editing a rate-limited port

Port Settings Aggregate port Port Mirror	ing Rate Limiting	
+ Batch Add X Batch Delete		
Port Input Rate-Limit (KBps)	Output Rate-Limit (KB;	ps) Action
Gi0/11 1000000	100000	Edit Delete
Show No.: 10 V Total Count:1		K First < Pre (1) Next > Last > 1 GO
	PortGI0/11	x
		·
	Input Rate-Limit: 1000000	Range: 64-1000000KBps
	(Rate-limit value varies with)	port type.)
	Output Rate-Limit: 100000	Range: 64-1000000/KBps
	(Rate-limit value varies with)	port (ype)
	Cancel Save	

The steps of editing a rate-limited port are as follows:

- 1) In the port rate limit list, click Edit in the Action column for a port. Rate limits of the port are displayed.
- 2) Edit Input Rate-Limit and Output Rate-Limit.
- After editing, click Save. The message "Configuration Succeeded" is displayed, indicating that the rate-limited port is edited successfully.
- Deleting a rate-limited port

tch Add 🗙 Batch	Delete		
Port	Input Rate-Limit (KBps)	Output Rate-Limit (KBps)	Action
Gi0/11	1000000	1000000	Edit Delete
w No.: 10 🗸 Tota	al Count:1		K First < Pre 1 Next > Last > 1
		×	
		Are you sure you want to delete	
		X Are you sure you want to delete the port configuration?	

The steps of deleting a rate-limited port are as follows:

- 1) Select multiple records in the port rate limit list and click **Batch Delete** to bulk delete the records.
- 2) In the port rate limit list, click **Delete** in the **Action** column for a port. The message "Are you sure you want to delete the port configuration?" is displayed. Click **OK**. The message "Delete Succeeded" is displayed, indicating that the deletion operation is completed.

1.3.3.1.3 Routing

The **Routing** page allows you to manage routes.

Note	Note: Routing includes a primary route and backup routes. When the primary route does not work, a backup route takes effect in accordance with the priority level. The Backup Route-1 has higher priority than the Backup Route-2.								
+ Add	+ Add Static Route + Add Default Route × Deleted								
0	Destination Subnet	Subnet Mask	Next Hop Address	Egress Port	Administrative Distance	Туре	Action		
	0.0.0.0	0.0.0.0	172.26.147.1		1	Default Route	Edit Delete		
Show	Show No: 10 Total Count1 K First < Pre () Next > Last X () (6)								

• Adding a static route

Week transforming includes a permay note does not work, a backup note take effect a accordance with the priority level. The Backup Roote -1 lass lighter periority than the Backup Roote -1 lass lighter Periority Distance Type Action • Add Default Roote Subnet Mask Next Hop Address Egress Port Add Ininitizative Distance Type Action • Ono No. • On No. • Ono No. • Or No. • First < First • No. * Or * O							
+ Add Static Route + Add Static Route Subset Mask Next Hop Address Egress Port Administrative Distance Type Action 0.00.0 0.00.0 17226.147.1 1 Default Route Edit Duelee show No: 1000 0.00.0 17226.147.1 1 Default Route Edit Duelee show No: 1000 10206 Thirty I Program Add Static Route X X I Program X First I Program Next X Static X I I IIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	Note: Routing includes a primary route and backup ro	outes. When the primary route does n	ot work, a backup route takes effect in accordanc	e with the priority level. The Backu	p Route-1 has higher priority than the Backup R	oute-2.	
Sectination Solubet Submet Mask Next Hop Address Egress Port Administrative Distance Type Action 0.0.00 0.0.00 122.65.147.1 1 Default Route Cell Cell Default Route Cell Cell Default Route Cell Cell Default Route Cell Default Route Cell Default Route Cell Default Route Cell Cell Default Route Cell Cell Default Route Cell <td>+ Add Static Route + Add Default Route ></td> <td>Collete Selected</td> <td></td> <td></td> <td></td> <td></td> <td></td>	+ Add Static Route + Add Default Route >	Collete Selected					
0.0.0 0.0.0 17226.147.1 1 Default Route It is in the initial is initial it initial is initial it initial is initial it initial is initial it initial it initial is initial it initialitial it initial it initial it initial it initial it initial it i	Destination Subnet	Subnet Mask	Next Hop Address	Egress Port	Administrative Distance	Туре	Action
Show No: 10 total Count:1 K Hext < Pre 1 Next > Last > 1 GO Add Static Route x IP Type: IP4 O IP46 Destination Subnet * Subnet Mask: * Egress Port * Administrative Distance: * Cancel Save	0.0.0.0	0.0.0.0	172.26.147.1		1	Default Route	Edit Delete
	Show No.: 10 Total Count:1		Add Static Route IP Type: • IP4 Destination Subnet Subnet Mask: Egress Port: Select Next Hop Address: Administrative Distance: 1	Port Annual Save Save	× e 1-255	K first <	Pre (1) Next > Last > (1) GO

The steps of adding a static route are as follows:

1) Click Add Static Route.

- Configure IP Type, Destination Subnet, Subnet Mask, Egress Port, Next Hop Address, and Administrative Distance.
 Destination Subnet, Subnet Mask, Next Hop Address, and Administrative Distance fields are required fields.
- 3) After configuring parameters, click **Save**. The message "Configuration Succeeded" is displayed, indicating that the static route is added successfully. The static route is displayed in the route list.
- Editing a route

Note: Bouting includes a primary route and backup routes. When the primary route does not work, a backup route takes effect in accordance with the priority level. The Backup Route-1 has higher priority than the Backup Route-2.									
+ Add Static Route + Add Default Route	× Delete Selected								
Destination Subnet	Subnet Mask	Next Hop Address	Egress Port	Administrative Distance		Туре	Action		
□ 0.0.0.0	0.0.0	172.26.147.1		1		Default Route	Edit Delete		
Show No.: 10 - Total Count:1		_				K First	Pre (1) Next > Last > (1) GO		
		Edit Default Route			×				
		IP Type: 🖲 I	Pv4 O IPv6						
		Egress Port: S	elect Port 🗸						
		Next Hop Address: 17	2.26.147.1	*					
		Administrative Distance: 1		*Range: 1-255					
					-				
			Cancel	ave					

The steps of editing a route are as follows:

- 1) In the route list, click **Edit** in the **Action** column for a route. Information about the route is displayed.
- Configure IP Type, Egress Port, Next Hop Address, and Administrative Distance. Next Hop Address and Administrative Distance fields are required fields.
- 3) After editing, click **Save**. The message "Configuration Succeeded" is displayed.
- Deleting a route

Note: Routing includes a primary route and b	ackup routes. When the primary route do	es not work, a backup route takes effect in acc	ordance with the priority level. The Back	up Route-1 has higher priority than the Backup I	Route-2.	
Add Static Route + Add Default Rou	ute X Delete Selected					
Destination Subnet	Subnet Mask	Next Hop Address	Egress Port	Administrative Distance	Туре	Action
0.0.0.0	0.0.0	172.26.147.1		1	Default Route	Edit Delete
w No.: 10 V Total Count:1					K First K	Pre 1 Next > Last > 1
			×			
		Are y the n	ou sure you want to delete oute?			
			ancel OK			

The steps of deleting a route are as follows:

- 1) Select multiple records in the route list and click **Delete Selected** to bulk delete the records.
- 2) In the route list, click **Delete** in the **Action** column for a route. The message "Are you sure you want to delete the route?" is displayed. Click **OK**. The message "Delete Succeeded" is displayed, indicating that the deletion operation is completed.
- Adding a default route

Note: Routing includes a primary route and backup routes. When the primary route does not work, a backup noute takes effect in accordance with the priority level. The Backup Route-1 has higher priority than the Backup Route-2.										
+ Add Static Route + Add Default Route ×	Delete Selected									
Destination Subnet	Subnet Mask	Next Hop Address	Egress Port	Administrative Distance		Туре	Action			
0.0.0.0	0.0.0.0	172.26.147.1		1		Default Route	Edit Delete			
Show No.: 10 V Total Count:1						K First	<pre> Pre 1 Next > Last > 1 GO </pre>			
		Add Default Route			×					
		IP Type: 💿 IPv4	⊖ IPv6							
		Egress Port: Select F	Port 🗸							
		Next Hop Address:	*							
		Administrative Distance: 1	*Rang	ie: 1-255						
			Cancel Save							

The steps of adding a default route are as follows:

- 1) Click Add Default Route.
- 2) Configure IP Type, Egress Port, Next Hop Address, and Administrative Distance. Next Hop Address and Administrative Distance are required fields.
- After configuration, click Save. The message "Configuration Succeeded" is displayed, indicating that the default route is added successfully. The default route is displayed in the route list.
- Routes are classified into primary and backup routes. When a primary route becomes invalid, a backup route takes over services. Backup routes are selected based on their priorities. The priority of backup route 1 is higher than that of backup route 2.

1.3.3.1.4 DHCP

The **DHCP** page allows you to configure DHCP and allocate static addresses, and displays the client list.

DHCP Settings

DHCP Settings	Static Address Client Display									
+ Add DHCP X Delete Selected Ø Excluded Address Range DHCP; (VI)										
Name	IP Address Range	Default Gateway	Lease Time	DNS	Action					
	No Data Found									
Show No.: 10 ▼ To	tal Count:0			K First K Pre N	lext > Last > 1 GO					

• Adding a DHCP address pool

DHCP Settings	Static Address Client Display			
+ Add DHCP × Delete Sele	ected Ø Excluded Address Range DHC	2 ⁰⁰		
Name	IP Address Range	Default Gateway	Lease Time	DNS Action
		No Data Found		
Show No.: 10 V Total Co				K First 〈 Pre Next 〉 Last 〉 1 GO
		Add DHCP	×	
		Pool Name:	İ	
		Type: ● IPv4 ○ IPv6		
		Address Range: 1 to 254 *		
		Pefault Gateway: *		
		Lease Time: 8 hour(s) 💙		
		Cancel Save		

The steps of adding a DHCP address pool are as follows:

- 1) Click Add DHCP.
- Configure Pool Name, Type, Address Range, Default Gateway, and Lease Time. Pool Name, Type, Address Range, Default Gateway, and Lease Time are required fields.
- 3) After configuration, click **Save**. The message "Configuration Succeeded" is displayed. The added DHCP address pool is displayed in the DHCP list.
- Editing a DHCP address pool

DHCP Settings	Static Address	Client Display					
+ Add DHCP × Dele	te Selected Ø Excluded /	Address Range DHCP:	34 				
Name	IP Address R	ange	Default Gateway	Lease Time	DNS	Action	
□ RG-001	192.168.1.1-1	92.168.1.254	192.168.1.1	8 hour(s)		Edit Delete	
Show No.: 10 V	tal Count:1					K First K Pre 1 Next > Last X 1	
			Edit DHCP		×		
			Pool Name: RG-001 * Type: • IPv4 _ O IPv6 Address Range: 192.168.1 1 to 254 * Default Gateway: 192.168.1.1 * Lease Time: 8 hour(s) * * Cancel Swe				

The steps of editing a DHCP address pool are as follows:

- 1) In the DHCP list, click **Edit** in the **Action** column for a DHCP address pool. Information about the DHCP address pool is displayed.
- 2) Modify fields. Pool Name, Type, Address Range, Default Gateway, and Lease Time are required fields.
- 3) After editing, click **Save**. The message "Configuration Succeeded" is displayed.
- Deleting a DHCP address pool

DHCP Settings	Static Address Client Display			
+ Add DHCP × Delete S	Selected Ø Excluded Address Range DHCP: ON			
Name	IP Address Range	Default Gateway	Lease Time	DNS Action
□ RG-002	192.168.2.101-192.168.2.200	192.168.1.2	8 hour(s)	Edit Delete
🗆 RG-001	192.168.1.1-192.168.1.100	192.168.1.1	8 hour(s)	Edit Delete
Show No.: 10 🗸 Total	Count:2			K First < Pre 1 Next > Last > 1 GO
		Are you surre you want to delete the selected address pool? Crcel Crcel Crcel		

The steps of deleting a DHCP address pool are as follows:

- 1) In the DHCP list, select multiple records and click **Delete Selected** to bulk delete the records.
- 2) In the DHCP list, click **Delete** in the **Action** column for a DHCP address pool. The message "Are you sure you want to delete the selected address pool?" is displayed. Click **OK**. The message "Delete Succeeded" is displayed, indicating that the deletion operation is completed.
- Enabling DHCP

DHCP Settings	Static Address	Client Display									
DHCP: OFF	DHCP: \bigcirc or \rightarrow Click DHCP to enable the DHCP service.										
Diter		renable the brick s	ervice.								

Static Address

The figure below shows the **Static Address** tab page.

DHCP Settings	Static Address	Client Display								
+ Add Static Address	+ Add Static Address X Delete Selected									
Client Name		Client IP	Mask	Gateway Address	Client	MAC DNS Server	Action			
No Data Found										
Show No.: 10 V Tota	Show No. 10 Total CountD K First < Pre Next > Last X 1 00									

• Adding a static address

Configuring Guide

DHCP Settings Static Add	dress Client Display				
+ Add Static Address - X Delete Select	ad				
T Add Static Address - A Derete Selecti	eu				
Client Name	Client IP	Mask Gateway Address	Client MAC	DNS Server	Action
		No Data i	Found		
Show No.: 10 V Total Count:0		Add Static Address	×	K First <	Pre Next > Last > 1 GC
		Client Name:	×		
		Client IP:	*		
		Mask:			
		Client MAC:	×		
		Gateway Address:	×		
		DIN3.			
			_		
		Cancel	Save		

The steps of adding a static address are as follows:

- 1) Click Add Static Address.
- Configure Client Name, Client IP, Mask, Client MAC, Gateway Address, and DNS. Client Name, Client IP, Client MAC, Gateway Address, and DNS are required fields.
- After configuration, click Save. The message "Configuration Succeeded" is displayed. The added static address is displayed in the static address list.
- Editing a static address

DHCP Settings	Static Address	Client Display										
+ Add Static Address 🛛 🗙	Collete Selected											
Client Name	Client	t IP	Mask	G	iateway Address		Client MAC		DNS Server	Action		
TEST	192.1	68.1.5	255.255.2	255.0 1	92.155.1.2		0002.0002.0002		192.155.1.3	Edit	Delete	
Show No.: 10 V Tota	l Count:1									K First K Pre (1)	Next > Last	Я 1 GO
				Edit Static Address				×				
				Client Name:	TEST	*						
				Client IP:	192.168.1.5	*						
				Mask:	255.255.255.0							
				Client MAC:	0002.0002.0002	*						
				Gateway Address:	192.155.1.2	*						
				DNS:	192.155.1.3	*						
						_		-				
					Cancel	ive						

The steps of editing a static address are as follows:

- 1) In the static address list, click **Edit** in the **Action** column for a static address. Information about the static address is displayed.
- 2) Edit parameters. Client Name, Client IP, Client MAC, Gateway Address, and DNS are required fields.
- 3) After editing, click Save. The message "Edit Succeeded" is displayed.
- Deleting a static address

DHC	P Settings Static Addre	Client Display					
+ Add S	Static Address × Delete Selected						
	Client Name	Client IP	Mask	Gateway Address	Client MAC	DNS Server	Action
	TEST	192.168.1.5	255.255.255.0	192.155.1.2	0002.0002.0002	192.155.1.3	Edit Delete
Show	No.: 10 🗸 Total Count:1					K Firs	t < Pre 1 Next > Last > 1 GO
				×			
			0	Are you sure you want to delete			
				the static address?			
				Cancel OK			

The steps of deleting a static address are as follows:

- 1) Select multiple records in the static address list and click **Delete Selected** to bulk delete the records.
- 2) In the static address list, click **Delete** in the **Action** column for a static address. The message "Are you sure you want to delete the static address?" is displayed. Click **OK**. The message "Delete Succeeded" is displayed, indicating that the deletion operation is completed.

U Client Display

The figure below shows the **Client Display** tab page.

Note: If you want to delete a static address converted from a dynamic address, please go to the Static Address page. OP Bind MAC to Dynamic IP Image: Constraint of the static address please go to the Static Address page.	IP-based v Search
Bind MAC to Dynamic IP IP MAC Lease Time Allocation Type	IP-based v Search
IP MAC Lease Time Allocation Type	Action
No Data Found	
Show No.: 1 Total Count0	K First < Pre Next > Last > 1 GO

Querying an IP address

DHCP Settings Note: If you want to dele	Static Address	Client Display	Enter an IP add query the IP ad	dress in the search box and click Search to ddress
Ø Bind MAC to Dynam	ic IP			IP-based v 192.168.1.1 Search
□ IP	MAC	Lease Time	Allocation Type	Action
			No Data Found	
Show No.: 1 V Tota	il Count:0			K First < Pre Next > Last > 1 GO

Binding a MAC address and a dynamic IP address

DHCP Settings	Static Address	Client Display		
Note: If you want to dele	te a static address converted fr	rom a dynamic address, please go to the Static Address pag	λ	
Ø Bind MAC to Dynam	ic IP			IP-based V 192.168.1.1 Search
D IP	MAC	Lease Time	Allocation Type	Action
			No Data Found	

The steps of binding a MAC address and a dynamic IP address are as follows:

- 1) Select an IP address in the client list.
- 2) Click **Bind MAC to Dynamic IP** to bind the IP address to the current MAC address.

1.3.3.1.5 VRRP

+ Add VRRP X Delete Selected				
VRRP Group No.	VRRP Port	VRRP Group IP	VRRP Priority	Action
		No Data Found		
Show No.: 10 V Total Count:0				K First K Pre Next > Last > 1 GO

• Adding a VRRP group

+ Add VRRP X Delete Selected				
U VRRP Group No. VR	RP Port	VRRP Group IP	VRRP Priority	Action
		No Data Found		
Show No.: 10 V Total Count:0				K First K Pre Next > Last > 1 GO
	Add VRRP		×	
	Port:	Gi0/1 🗸		
	VRRP Group Number:	* (Range: 1-255)		
	IP: Prioriter	* 100 * (Danner 1,254)		
		rungie i acey		
		Cancel Save		

The steps of adding a VRRP group are as follows:

- 1) Click Add VRRP.
- 2) Configure Port, VRRP Group Number, IP, and Priority. VRRP Group Number, IP, and Priority are required fields.
- After configuration, click Save. The message "Add Succeeded" is displayed. The added VRRP group is displayed in the VRRP list.
- Deleting a VRRP group

+ Add VRRP X Delete Selected				
VRRP Group No.	VRRP Port	VRRP Group IP	VRRP Priority	Action
□ 10	Gi0/1	192.145.1.1	100	Edit Delete
□ 20	Gi0/1	192.148.1.2	90	Edit Delete
Show No.: 10 V Total Count:2				K First K Pre 1 Next > Last > 1 GO
	Ć	X Are you sure you want to delete the item? Cancel OK		

The steps of deleting a VRRP group are as follows:

- 1) Select multiple records in the VRRP list and click **Delete Selected** to bulk delete the records.
- 2) In the VRRP list, click **Delete** in the **Action** column for a VRRP group. The message "Are you sure you want to delete the item?" is displayed. Click **OK**. The message "Delete Succeeded" is displayed, indicating that the deletion operation is completed.
- Editing a VRRP group

+ Add VRRP × Delete Selected								
U VRRP Group No.	VRRP Port	VR	RP Group IP		VRRP Priority	Action		
□ 10	Gi0/1	192	2.145.1.1		100	Edit Delete		
□ 20	Gi0/1	192	2.148.1.2		90	Edit Delete		
Show No.: 10 V Total Count:2						K First K Pre	1 Next > Last >	1 GO
		Edit VRRP			×			
		Port:	Gi0/1 ~					
		VRRP Group Number:	10	* (Range: 1-255)				
		IP:	192.145.1.1	*				
		Priority:	100	* (Range: 1-254)				
			Cancel	ave				

The steps of editing a VRRP group are as follows:

- 1) In the VRRP list, click **Edit** in the **Action** column for a VRRP group. Information about the VRRP group is displayed.
- 2) Edit parameters. VRRP Group Number, IP, and Priority are required fields.
- 3) After editing, click **Save**. The message "Configuration Succeeded" is displayed.

1.3.3.1.6 MAC Address

The MAC Address page includes the Dynamic Address Table, Static Address Settings, and Filtering Address Settings tab pages.

Dynamic Address Table

Dynamic Address Table	Static Address Settings	Filtering Address Settings				
					Select Query Condition 🗸	Search
MAC Address			VLAN ID	Interface		
			No Data Found			
Show No.: 10 V Total Count	:0				K First K Pre Next > L	ast X 1 GO
Show No.: 10 V Total Count	:0				K First K Pre Next > L	ast X 1 GO

• Querying dynamic addresses by conditions

Dynamic Address Table	Static Address Settings	Filtering Address Settings			Select Query Condition Select Query Condition
MAC Address			VLAN ID	Interface	Query By MAC Query By VLAN Query By Interface
			No Data Found		
Show No.: 10 V Total Count	0				K First < Pre Next > Last > 1 G

Query conditions include Select Query Condition, Query By MAC, Query By VLAN, and Query By Interface.

Static Address Settings

Dynamic Address Table	Static Address Settings	Filtering Address Settings		
Note: The switch forwards data ac you can implement authentication	cording the MAC address inside the data exemption by binding MAC address with	frame. If you configure MAC-port binding on a network device manua port.	By after you add a static address, the switch that receives the packet with	the same destination address forwards it to the specified port. With 802.1X authentication enable
Add Static Address X Dele	te Static Address			
Port	MAC Address		VLAN ID	Action
			No Data Found	
Show No.: 10 ♥ Total Coun	нo			K First < Pro Next > Last > 1

• Adding a static address

Add Static Address X Delete	Static Address				
Port	MAC Address		VLAN ID		Action
			No Data Found		
		Add Static Address		×	
how No.: 10 V Total Count:		MAC Address:	•	•	K First < Pre Next > Last > 1
		VLAN ID:	*		
		Select Port:			
		Selected 1 AG Port 💼 Up 📄 Shutdown 🕞	VSL Port Copper	Fiber	
				47	
		2 4 6 8 10 12 14 16 18 20	22 24 26 28 30 32 34 36 38 40 42 44 46	48	
		4		· ·	
			Cancel Save		

The steps of adding a static address are as follows:

1) Click Add Static Address.

- 2) Configure a static address. MAC Address, VLAN ID, and port are required fields.
- After configuration, click Save. The message "Configuration Succeeded" is displayed. The added static address is displayed in the static address list.

• Deleting a static address

Cyrianie, Pouress lable	Static Address Settings Filtering A	dress Settings	
Note: The switch forwards data aco you can implement authentication e	cording the MAC address inside the data frame. If you config exemption by binding MAC address with port.	re MAC-port binding on a network device manually, after you add a static address, the switch that receives the p	acket with the same destination address forwards it to the specified port. With 802.1X authentication enabled
Add Static Address 🗙 Delet	te Static Address		
Port	MAC Address	VLAN ID	Action
) Gi0/12	0003.0003.0003	10	Delete
how No. 10 V Total Count:			K First < Pre (1) Next > Last > 1 GO
		X Are you sure you want to delete the static address? Cancel CK	

The steps of deleting a static address are as follows:

- 1) Select multiple records in the static address list and click **Delete Static Address** to bulk delete the records.
- 2) In the static address list, click **Delete** in the **Action** column for a static address. The message "Are you sure you want to delete the static address?" is displayed. Click **OK**. The message "Delete Succeeded" is displayed, indicating that the deletion operation is completed.

**** Filtering Address Settings

Dynamic Address Table	Static Address Settings	Filtering Address Settings		
Note: The switch forwards data acc packets.	ording the MAC address inside the data fra	me. If a switch receives a packet with the source/de	istination MAC address which is configured as a filter address, it discards the packet. You can p	prevent the ARP attack by configuring a filter address the same as the MAC address of ARP
+ Add Filter Address × Delet	e Filter Address			
MAC Address			VLAN ID	Action
			No Data Found	
Show No.: 10 - Total Count	:0			K First K Pre Next > Last > 1 GO

• Adding a filter address

Dynamic Address Table Static Address Settings Filtering Address Settings		
Note: The switch forwards data according the MAC address inside the data frame. If a switch receives a packet with packets.	the source/destination MAC address which is configured as a filter address, it discards	he packet. You can prevent the ARP attack by configuring a filter address the same as the MAC address of ARP
+ Add Filter Address × Delete Filter Address		
MAC Address	VLAN ID	Action
	No Data Found	
Show No. 10 Total Count:0	Add Filter Address ×	K First < Pre Next > Last > 1 GO
	MAC Address:	
	VLAN ID: *	
	Cancel	

The steps of adding a filter address are as follows:

- 1) Click Add Filter Address.
- 2) Configure a filter address. **MAC Address** and **VLAN ID** are required fields.
- After configuration, click Save. The message "Configuration Succeeded" is displayed. The added filter address is displayed in the filter address list.
- Editing a filter address

Dynamic Address Table	Static Address Settings	Filtering Address Settings			
Note: The switch forwards data acc packets.	cording the MAC address inside the data	frame. If a switch receives a packet with the s	ource/destination MAC address which is configured as a filter address, it di	scards the packet. You can prever	t the ARP attack by configuring a filter address the same as the MAC address of ARP
+ Add Filter Address × Delet	e Filter Address				
MAC Address			VLAN ID		Action
0003.0003.0003			35		Edit Delete
Show No.: 10 V Total Count					K First < Pre 1 Next > Last > 1 GO
		3	dit Filter Address MAC Address VLAN ID: 35 Cancel Save	X	

The steps of editing a filter address are as follows:

- 1) In the filter address list, click Edit in the Action column for a filter address. Information about the filter address is displayed.
- 2) Edit parameters. MAC Address and VLAN ID are required fields.
- 3) After editing, click Save. The message "Configuration Succeeded" is displayed.
- Deleting a filter address

Dynamic Address Table	Static Address Settings	Filtering Address Settings		
Note: The switch forwards data ac packets.	cording the MAC address inside the data	frame. If a switch receives a packet with the source/d	stination MAC address which is configured as a filter address, it discards the packet. You can prevent t	the ARP attack by configuring a filter address the same as the MAC address of \ensuremath{ARP}
- Add Filter Address 🗙 Delet	te Filter Address			
MAC Address			VLAN ID	Action
0003.0003.0003			35	Edit Delete
Show No.: 10 V Total Coun	e1			K First K Pre 1 Next > Last > 1 GO
		۰	× r you sure you want to delete filter address? Cancel CK	

The steps of deleting a filter address are as follows:

- 1) Select multiple records in the filter address list and click **Delete Filter Address** to bulk delete the records.
- 2) In the filter address list, click **Delete** in the Action column for a filter address. The message "Are you sure you want to delete the filter address?" is displayed. Click **OK**. The message "Delete Succeeded" is displayed, indicating that the deletion operation is completed.

1.3.3.2 Other

1.3.3.2.1 VSU Settings

For devices supporting the VSU mode, the **VSU Settings** page in standalone mode is different from that in VSU mode. The domain IDs of devices composing the VSU must be the same. Device IDs must be unique in a VSU and the device with the highest priority is the master device.

Standalone Mode

The figure below shows the VSU Settings page in standalone mode.

VSU Settings	
Device ID	2: 1 * Ranger 1- 4 (2)
Domain IE	2: 100 * Range 1-255
Priority	y: 100 * Range 1-255
Descripto	
VSI	t 0
Selected 1 AG Por	t Copper 🗔 Fiber
All Invert Deselect	Note:Click and hold the left button as you drag the pointer across the section to select multiple ports.
	Save Change to VSU clear

In VSU standalone mode, Device ID, Domain ID, and Priority are required fields.

1.3.3.2.2 STP

The **STP** page allows you to configure STP global parameters and STP ports.

STP Global Settings

STP Global Settings	STP Port Settings				
Global Configuration					
STP: ON					
Priority: 8	Range(0-15), default 8	Hello Time 2	Range(1-10s), default 2		
Aging Time: 20	Range(6-40s), default 20	Forward Delay: 15	Range(4-30s), default 15		
STP Mode: MSTP	~				
MST Name:	String less than 32-byte	MST Version: 0	Range(0-65535), default 0		
Save					
MST Configuration					
Note: It is recommended to disable ST	P before configuring an instance and e	nable STP again after configuration,	so as to ensure the stability and convergence of network	k topology.	
+ Add Instance × Delete Selecte	d				
 Instance Number 			VLAN	Priority	Action
O			ALL	8	Edit
Show No.: 10 V Total Count:1					K First < Pre (1) Next > Last > (1) GO

You can configure STP global parameters. When **STP Mode** is set to **MSTP**, you can configure an MST instance.

• Adding an instance

STP Global Settings STP Port Settings		
Global Configuration STP: CP Priority: B Respector 15), default 8 Aging Time: 20 Respector 40b, default 80 Forward Delay: 15 STP Mode: MSTP V V V V	Range(1-10s), default 2 Range(4-30s), default 15	
MST Name: String less than 32-byte MST Version: 0 Save MST Configuration Note: It is recommended to disable STP before configuring an instance and enable STP again after configuring	Add Instance X Instance Number: * VLAN Range: * Prioriter Proventi 10. defende #	
+ Add Instance × Delete Selected	Filongy	Antine
0	Cancel Save	Edit
Show No. 10 V Total Count:1		K First K Pre (1) Next > Last > (1) GO

The steps of adding an instance are as follows:

- 1) Click Add Instance.
- 2) Configure an instance. Instance Number and VLAN Range are required fields and other fields are optional.
- 3) After configuration, click **Save**. The message "Configuration Succeeded" is displayed. The added instance is displayed in the instance list.

• Editing an instance

Global Configuration				
STP: ON				
Priority: 8 Range(0-15), default 8 Hello Time 2	Range(1-10s), default 2			
Aging Time: 20 Range(6-40s), default 20 Forward Delay: 15	Range(4-30s), default 15			
STP Mode: MSTP V				
MST Name: String less than 32-byte MST Version: 0	Edit Instance	×		
Save	Instance Number: 10]•		
MST Configuration	VLAN Range: 1-10).		
Note: It is recommended to disable STP before configuring an instance and enable STP again after configu	Delasitua 7			
+ Add Instance X Delete Selected	rionty. /	Kangelu-15), delault o		
Instance Number		A	ction	
· 0	Cancel Save		Edit	
D 10	1-10 7		Edit Delete	
Show No.: 10 V Total Count:2			K First K Pr	e (1) Next > Last > 1 GO

The steps of editing an instance are as follows:

- 1) In the instance list, click **Edit** in the **Action** column for an instance. Information about the instance is displayed.
- 2) Edit instance information. Instance Number and VLAN Range are required fields and other fields are optional.
- 3) After editing, click Save. The message "Configuration Succeeded" is displayed.
- Deleting an instance

STP Global Settings STP Port Settings				
Global Configuration				
STP: ON				
Priority: 8 Range(0-15); default 8 Hello Time 2	Range(1-10s), default 2			
Aging Time: 20 Range(6-40s), default 20 Forward Delay: 15	Range(4-30s), default 15			
STP Mode: MSTP 👻				
MST Name: String less than 32-byte MST Version: 0	Range(0-65535), default 0	_		
Care		×		
Juve	Are you sure you want to delete			
MST Configuration	the instance?			
Note: It is recommended to disable STP before configuring an instance and enable STP again after configuratio	Cancel OK	xology.		
+ Ard Instance X Delate Selected				
1 Pour Insurree - A benete Selecteu				
Instance Number	VLAN	Priority	Action	
0	11-4094	8	Edit	
ID 10	1-10	7	Edit Delete	
Show No. 10 V Total Count:2				K First < Pre 1 Next > Last > 1 GO

The steps of deleting an instance are as follows:

- 1) Select multiple records in the instance list and click **Delete Selected** to bulk delete the records.
- 2) In the instance list, click **Delete** in the **Action** column for an instance. The message "Are you sure you want to delete the instance?" is displayed. Click **OK**. The message "Delete Succeeded" is displayed, indicating that the deletion operation is completed. Instance 0 is the default instance and cannot be deleted.

STP Port Settings

STP Global Settings	STP Port Settings						
Note: It is recommended to ena	able Port Fast on the port connected to t	he PC.					
+ Batch Add							
Port	Status	Port Fast	BPDU Guard	Protection Mode	Connection Mode	Instance Cost Priority	Action
GigabitEthernet0/2	Up	Enabled	Disabled	Null	Auto	0 0 128 10 0 128	Edit
GigabitEthernet0/3	Up	Enabled	Disabled	Null	Auto	0 0 128 10 0 128	Edit
GigabitEthernet0/4	Up	Enabled	Disabled	Null	Auto	0 0 128 10 0 128	Edit
GigabitEthernet0/7	Up	Enabled	Disabled	Null	Auto	0 0 128 10 0 128	Edit
GigabitEthernet0/8	Up	Enabled	Disabled	Null	Auto	0 0 128 10 0 128	Edit
GigabitEthemet0/9	Up	Enabled	Disabled	Null	Auto	0 0 128 10 0 128	Edit
GigabitEthernet0/10	Up	Enabled	Disabled	Null	Auto	0 0 128 10 0 128	Edit
GigabitEthernet0/11	Up	Enabled	Disabled	Null	Auto	0 0 128 10 0 128	Edit
GigabitEthernet0/12	Up	Enabled	Disabled	Null	Auto	0 0 128 10 0 128	Edit
GigabitEthernet0/13	Up	Enabled	Disabled	Null	Auto	0 0 128 10 0 128	Edit
Show No.: 10 V Total Con	unt:48					K First < Pre 1 2 3 4 5 Next >	Last X 1 GO

Bulk setting STP ports

Note: It is recommended to enable Port Fast on th	ne port connected to the F	¢.		
+ Batch Add				
Port	Status	Batch Add ×	Instance Cost Priority	Action
GigabitEthernet0/2	Up	Protection Mode: Null	0 0 128 10 0 128	Edit
GigabitEthernet0/3	Up	NUII V	0 0 128 10 0 128	Edit
GigabitEthernet0/4	Up	Port Fast: Disabled	0 0 128 10 0 128	Edit
GigabitEthernet0/7	Up	BPDU Guard: Enabled	0 0 128 10 0 128	Edit
GigabitEthernet0/8	Up	Connection Mode: Auto 🗸	0 0 128 10 0 128	Edit
GigabitEthernet0/9	Up	Port Priority	0 0 128 10 0 128	Edit
GigabitEthernet0/10	Up	+ Add	0 0 128 10 0 128	Edit
GigabitEthernet0/11	Up	Select Port:	0 0 128 10 0 128	Edit
GigabitEthernet0/12	Up	Selected 1 AG Port Dup Shutdown VSL Port Copper Fiber	0 0 128 10 0 128	Edit
GigabitEthernet0/13	Up		0 0 128 10 0 128	Edit
Show No.: 10 V Total Count:48			irst < Pre 1 2 3 4 5 Next > Last > [1 GO
		()		
		All Invert Deselect Note:Click and hold the left button as you drag the pointer across the section to select multiple ports.		
		Cancel		

The steps of bulk setting STP ports are as follows:

- 1) Click Batch Add.
- 2) Configure Protection Mode, Port Fast, BPDU Guard, Connection Mode, and Port Priority, and select ports.
- Editing an STP port

Note: It is recommended to enable Port Fast on the	port connected to the	PC.							
+ Batch Add									
Port	Status	Port Fast	BPDU Guard	Protection M	ode	Connection Mod	e	Instance Cost Priority	Action
GigabitEthernet0/2	Up	Enabled	Disabled	Null		Auto		0 0 128 10 0 128	Edit
GigabitEthernet0/3	Up	Enabled	Disabled	Null		Auto		0 0 128 10 0 128	Edit
GigabitEthernet0/4	Up	Enabled	PortGigabitEthernet0/2				×	0 0 128 10 0 128	Edit
GigabitEthernet0/7	Up	Enabled	Protection Mode:	Null 🗸				0 0 128 10 0 128	Edit
GigabitEthernet0/8	Up	Enabled	Port Fast:	Enabled ¥				0 0 128 10 0 128	Edit
GigabitEthernet0/9	Up	Enabled						0 0 128 10 0 128	Edit
GigabitEthernet0/10	Up	Enabled	BPDU Guard:	Disabled V				0 0 128 10 0 128	Edit
GigabitEthernet0/11	Up	Enabled	Connection Mode:	Auto 🗸				0 0 128 10 0 128	Edit
GigabitEthernet0/12	Up	Enabled	Port Priority:) +	0 0 128 10 0 128	Edit
GigabitEthernet0/13	Up	Enabled		Instance Number: 0 V	Priority: 128	*Range(0-240) ×	Ad	0 0 128 10 0 128	Edit
Show No.: 10 V Total Count:48					Priority: 128	_*Kange(0-240) ×	d K	First < Pre 1 2 3 4 5 1	Next > Last > 1 GO
				Cancel	Save		Ţ		

The steps of editing an STP port are as follows:

- 1) In the STP port list, click **Edit** in the **Action** column for an STP port. Information about the port is displayed.
- 2) Configure parameters.
- 3) After editing, click **Save**. The message "Configuration Succeeded" is displayed.

1.3.3.2.3 RLDP Settings

Global configuration			
Note: RLDP enables you to detect link fai	lure quickly. RLDP can run on the port only after it is enabled globally.		
RLDP: ON			
Detection Interval: 3	Runge(2-15)		
Detection Count: 2	Range(2-10)		
errdisable recovery:	Range(30-66400a)		
Save			
Port Configuration			
Note: 1. Enabling RLDP on the port can a 2. Unidirectional/Bidirectional link 3.An aggregate port can only be o	wold broadsat storm cuand by loogs. It is recommended to anable RLP or the port convected to the PC; is Rubertion require the point on both ends of the kins be available with RLP is a recommended to configure RLP to monitor the link between two writches; onfigured with port violation or alarm; Loog detection on a member port will be genchronized to other member ports.		
+ Add Port X Delete Port			
Port	Detection Type:Troubleshooting	Action	
Gi0/1	Loop Detection:Warning	Edit Delete	
Show No.: 10 V Total Count:1			K First < Pre (1) Next > Last > (1) GO

1. RLDP global configuration

Note: RLDP enables you to o	detect link failure quickly. RLDP ca	n run on the port only after it is enabled globally.
RLDP:		
Detection Interval:	3	Range(2-15)
Detection Count:	2	Range(2-10)
errdisable recovery:		Range(30-86400s)
	Save	

The steps of configuring RLDP globally are as follows:

- 1) Click **RLDP** to enable/disable the RLDP function.
- 2) If RLDP is enabled, configure **Detection Interval**, **Detection Count**, and **errdisable recovery**, and click **Save**. The message "Configuration Succeeded" is displayed.
- 2. Port RLDP configuration
- Adding an RLDP port

Global configuration	
Note: RLDP enables you to detect link failure quickly. RLDP can run on the po	t only after it is enabled globally.
RLDP: ON	
Detection Interval: 3 Range(2-15	
Detection Count: 2 Range(2-10	Batch Add X
errdisable recovery:	Detection Mode: □ Unidirectional Link Detection Warning
Save	Bidirectional Link detection Warning
Port Configuration	Loop Detection Warning
Note: 1. Enabling RLDP on the port can avoid broadcast storm caused by loo 2. Unidirectional/Bidirectional link detection requires the ports on both 3.An aggregate port can only be configured with port violation or alarr	Select Port:
+ Add Port X Delete Port	O selected ① AG Port © top ○ Selected ○ Copper □ Filer 1 3 5 7 9 11 31 15 77 9 14 44
Port Detection Type:Troublest	
Gi0/1 Loop Detection:Warning	< B
Show No.: 10 V Total Count:1	All invert Deselect Note:Click and hold the left button as you drag the pointer across the section to select multiple ports.
	Cancel Save

The steps of adding an RLDP port are as follows:

- 1) Click Add Port.
- 2) Configure parameters.

- After configuration, click Save. The message "Configuration Succeeded" is displayed, indicating that the RLDP port is added. The added RLDP port is displayed in the RLDP port list.
- Editing an RLDP port

Global configuration			
Note: RLDP enables you to detect link failure quickly. RLDP can run on the po	t only after it is enabled globally.		
RLDP: ON			
Detection Interval: 3 Range(2-15			
Detection Count: 2 Range(2-10			
errdisable recovery:	00:)		
Save	PortGi0/1	×	
Port Configuration	Detection Mode: Unidirectional Link Detection Warning v		
Note: 1. Enabling RLDP on the port can avoid broadcast storm caused by loo 2. Unidirectional/Bidirectional link detection requires the ports on both 3.An aggregate port can only be configured with port violation or alarr	Bidirectional Link detection Warning v		
+ Add Port X Delete Port	Loop Detection Warning		
Port Detection Type:Troublesh			
Gi0/1 Loop Detection:Warning	Cancel Save	te	
Show No.: 10 V Total Count:1		K First K Pre 1 Next > Last	X 1 GO

The steps of editing an RLDP port are as follows:

- 1) In the RLDP port list, click **Edit** in the **Action** column for an RLDP port. Information about the RLDP port is displayed.
- 2) Edit parameters.
- 3) After editing, click **Save**. The message "Configuration Succeeded" is displayed.
- Deleting an RLDP port

Global configuration		
Note: RLDP enables you to detect link failure quickly RLDP can run on the port only after it is enabled globally.		
RLDP. CON		
Detection Interval: 3 Range(2-15)		
Detection Count: 2 Range(2-10)		
errdisable recovery:		
Save	*	
Port Configuration	Are you sure you want to delete	
Note: 1 Enabling #LIDP on the port can avoid broadcast storm caused by loops. It is recommended to enable ful 2. Undirectional/Bidirectional link detection requires the ports on both ends of the link to be enabled wit 3.An aggregate port can only be configured with port violation or alarm. Loop detection on a member po	the Item? Ink between two switches;	
+ Add Port X Delete Port	Cancel	
Port Detection Type: Troubleshooting		Action
Gi0/1 Loop Detection:Warning		Edit Delete
Show No. 10 V Total Count:1		K First K Pre (1) Next > Last > (1) GO

The steps of deleting an RLDP port are as follows:

- 1) Select multiple records in RLDP port list and click **Delete Port** to bulk delete the records.
- 2) In the RLDP port list, click **Delete** in the **Action** column for an RLDP port. The message "Are you sure you want to delete the item?" is displayed. Click **OK**. The message "Delete Succeeded" is displayed, indicating that the deletion operation is completed.

1.3.3.3 Security

1.3.3.3.1 ACL

When receiving a packet, a device port, on which an input ACL is configured, checks whether the packet matches an access control entry (ACE) in the input ACL. When sending out a packet, a device port, on which an output ACL is configured, checks whether the packet matches an ACE in the output ACL.

After different ACEs are configured, multiple ACEs may be applied at the same time or only a few ACEs are applied. Packets matching an ACE are processed (permitted or denied) according to the ACE.

ACL List

ACL List	ACL Time	ACL Application									
ACL List:	▼ Add ACL	Delete ACL + Add A	ccess Rule X Delete Select	ted							
D NO. D	Description	Src IP/Wildcard	Source Port	Access Control	Protocol	Dest IP/Wildcard	Dest Port	Time Period	Status	Action	
	No Data Found										
Show No.: 10	Show No. 10 Total Count.0 K First < Pre Next > Last X 1 GO										

• Adding an ACL

ACL I	ist ACL Time	ACL Application								
ACL List:	✓ Add ACL	Delete ACL + Ad	d Access Rule 🛛 🗙 Delete Selecte	d						
	NO. Description	Src IP/Wildcard	Source Port	Access Control	Protocol	Dest IP/Wildcard	Dest Port	Time Period	Status	Action
					No Data Found					
Show I	No.: 10 V Total Count:0							K First	< Pre Next ≻ Last ≯	1 GO
			Add ACL				×			
			ACI	L Type: Standard ACL (Sour C Extended ACL (Flow MAC-based Extended Name: 1300-1900.	ce-address-based Contro based Control) ed ACL(Flow-based Contr * Please enter let	0 01) ters or numbers in the range of 1-99 i	nd			
					Cancel					

The steps of adding an ACL are as follows:

- 1) Click Add ACL.
- 2) Configure parameters in the displayed dialog box. **ACL Name** is a required field.
- After configuration, click OK. The message "Configuration Succeeded" is displayed. The added ACL is displayed in the ACL List drop-down list.
- Deleting an ACL

ACL List	ACL Time	ACL Application								
ACL List: 104	✓ Add ACL	Delete ACL + Add	Access Rule × Delete Selecter	đ						
NO.	Description	Src IP/Wildcard	Source Port	Access Control	Protocol	Dest IP/Wildcard	Dest Port	Time Period	Status	Action
					No Data Found					
Show No.: 1	0 ✔ Total Count:0							K First 🛛 K	're Next > Last >	1 GO
				Are you sure you v the ACL2 Cancel	X want to delete					

The steps of deleting an ACL are as follows:

- 1) Select an ACL to be deleted from the ACL List drop-down list.
- Click Delete ACL. The message "Are you sure you want to delete the ACL?" is displayed. Click OK. The message "Delete Succeeded" is displayed.
- Adding an ACE

ACL List ACL Time ACL Application							
ACL List: 104 Add ACL Delete ACL + Add A	ccess Rule X Delete Selected						
NO. Description Src IP/Wildcard	Source Port Access Contro	Protocol	Dest IP/Wildcard	Dest Port	Time Period	Status	Action
		No Data Found					
Show No. 10 V Total Count0	Add Access Rule ACL Name: 104 Access Rule Settings Access Control: Permit Description: Protocol: P Single IP Any Destinat	y Time Period:Select (The role is applied to any source P add T P: P: P: P:	[Time management] resect;)	×	K fina <	Pre Nest > Last X	1 @

The steps of adding an ACE are as follows:

- 1) Select an ACL, to which ACEs need to be added, from the ACL List drop-down list.
- 2) Click Add Access Rule.
- 3) In the displayed dialog box, set parameters.
- 4) Click **OK**. The message "Configuration Succeeded" is displayed. The added ACE is displayed in the ACE list.
- Editing an ACE

101 H									
ACL List ACL Time	ACL Application								
ACL List: 104 V Add ACL	Delete ACL + Add Acc	ess Rule × Delete Selected	i						
NO. Description	Src IP/Wildcard	Source Port	Access Control	Protocol	Dest IP/Wildcard	Dest Port	Time Period	Status	Action
0 1	192.147.14.3/0.0.0.0		Permit	ip	192.147.14.4/0.0.0.0		All Time	Active	Edit Move
Show No.: 10 V Total Count:1							K First	< Pre 1	Next > Last > 1 GO
		Edit Access Rule				×			
		ACL Type ACL Name Access Rule Setting Access Control	Estended ACL (Plow-ba 104 Permit O Deny Description: Protocol: [P] ~ Any Source IP (rite Single IP	sed Control) Time Period:Select rule: is applied to any source IP: 192:147.14.3 Cancel OK	(Time management)				

The steps of editing an ACE are as follows:

- 1) In the ACE list, click **Edit** in the **Action** column for an ACE.
- 2) The displayed dialog box displays information about the ACE. Edit the ACE information.
- After editing, click OK. The message "Configuration Succeeded" is displayed, indicating that the editing operation is completed.
- Deleting an ACE

	ACL Lis	t ACL Time	ACL Application								
AC	L List: (104 V Add ACL	Delete ACL + Add Access R	ule X Delete Selected							
	2 N	O. Description	Src IP/Wildcard	Source Port	Access Control	Protocol	Dest IP/Wildcard	Dest Port	Time Period	Status	Action
	a 1		192.147.14.3/0.0.0.0		Permit	ip	192.147.14.4/0.0.0.0		All Time	Active	Edit Move
	2 2		192.148.1.3/0.0.0.0		Permit	ip	192.148.1.5/0.0.0.0		All Time	Active	Edit Move
	how No	o.: 10 ✔ Total Count:2							K First	< Pre 1	Next > Last > 1 GO
					Are you sure you war the access rule? Cancel OK	× In to delete					

The steps of deleting an ACE are as follows:

- 1) Select one or more records in the ACE list.
- 2) Click **Delete Selected**. The message "Are you sure you want to delete the access rule?" is displayed. Click **OK** to complete the deletion operation.

ACL Time

You can make an ACL available based on time, for example, make an ACL take effect in some time ranges of a week. For this, you need to first configure a time object.

ACL List	ACL Time	ACL Application							
Nete: The ACL active time must be periodic.									
+ Add Time Obje	+ Add Time Object X Delete Selected								
 Time Obj 	ect		Day	Time Period	Action				
No Data Found									
Show No.: 10	✔ Total Count:0				K First < Pre Next > Last > 1 GO				

• Adding a time object

Nete: The ACL active time must be periodic.	
LAN Tex Office V Delay Friend	
T Adu Ime (dijet) A Lenete seet.teu	
Day Time Daje Action	
No Data Sarand	
No Sala Found	
Show No: 10 Total Count:0 K First < F	Pre Next > Last > 1 GO
Add Time Object X	
Object Name: *	
Time Period.	
V Visit time - Und time X	
Cancel Save	

The steps of adding a time object are as follows:

- 1) Click Add Time Object.
- 2) In the displayed dialog box, set parameters.
- After configuration, click Save. The message "Configuration Succeeded" is displayed, indicating that the operation is completed.
- Bulk deleting time objects

ACL List ACL Time	ACL Application			
Note: The ACL active time must be periodic.				
+ Add Time Object × Delete Selected				
Time Object	Day	Time Period	Action	
001	Tuesday	7:00-18:00	Edit Delete	
Show No.: 10 V Total Count:1				K First K Pre 1 Next > Last > 1 GO
		X Are you sure you want to delete the time object? Gancel GK		

The steps of bulk deleting time objects are as follows:

- 1) Select time objects to be deleted in the list.
- 2) Click **Delete Selected**. The message "Are you sure you want to delete the time object?" is displayed. Click **OK** to complete the deletion operation.

• Editing a time object

ACL List	ACL Time	ACL Application											
Note: The ACL ac	tive time must be periodic												
+ Add Time Obje	ect X Delete Selected												
Time Ob	ject		Day		Time Period		A	ction					
001			Tuesday		7:00-18:00			Edit	Delete				
Show No.: 10	✓ Total Count:1									K First	Pre 1 Next	> Last >	1 GO
				Edit Time Period			×						
				Object Name: 00	M *								
				Time Period:			+ Add						
					luesday V 7:00	- 18:00 ×							
					Cancel Save								
					Cuncer	1							

The steps of editing a time object are as follows:

- 1) Click **Edit** in the **Action** column for a time object in the list.
- 2) The displayed dialog box displays information about the time object. Edit the information.
- After editing, click Save. The message "Configuration Succeeded" is displayed, indicating that the editing operation is completed.
- Deleting a time object

ACL List ACL Time ACL Application				
Note: The ACL active time must be periodic.				
+ Add Time Object × Delete Selected				
Time Object	Day	Time Period	Action	
□ 001	Tuesday	7:00-18:00	Edit Delete	
Show No. 10 V Total Count:1				K First K Pre 1 Next > Last X 1 GO
		×		
		Are you sure you want to delete		
		the time object?		
		Cancel CK		

The steps of deleting time objects are as follows:

- 1) Click **Delete** in the **Action** column for a time object in the list.
- The message "Are you sure you want to delete the time object?" is displayed. Click OK. The message "Delete Succeeded" is displayed.

ACL Application

You can configure ACEs and apply them to ports or VLANs to restrict the access of specific users or allow users to access specific networks.

'L List ACL Time	ACL Application			
If the configuration takes effect but is	not displayed properly on the page, please refresh the	page.		
Add Port X Delete Port				
ACL	Port	Direction	Action	
		No Data Found		

• Adding an ACL application

ACL List	ACL Time	ACL Application			
Note: If the conf	iguration takes effect but	is not displayed properly on the p	age, please refresh the page.		
+ Add Port 🗙	Delete Port				
ACL		Port	Direction	Action	
			Add Port	×	
Show No.: 10	▼ Total Count:0		ACL List:		K First ≺ Pre Next ≻ Last ౫ 1 GO
			Direction: Input ~		
			Select Port:		
			Selected 🚹 AG Port 💼 Up 💼 Shutdown 💽 VSL Port	iber	
				5	
				2	
			All Invert Deselect Note:Click and hold the left button as you drag the pointer across the section to select multiple p	orts.	
				-	
			Cancel Save		

The steps of adding an ACL application are as follows:

- 1) Click Add Port.
- 2) The **Add Port** dialog box is displayed. Set parameters.
- After configuration, click Save. The message "Configuration Succeeded" is displayed. The added ACL application is displayed in the ACL list.
- Bulk deleting ACL applications

ACL List ACL Time AC	L Application			
Note: If the configuration takes effect but is not disp	layed property on the page, please refresh the page.			
+ Add Port X Delete Port				
ACL	Port	Direction	Action	
🖬 104(IP)	Gi0/11	in	Edit Delete	
🖸 104(IP)	Gi0/11	out	Edit Delete	
2 701(MAC)	Gi0/24	in	Edit Delete	
Show No: 10 V Total Count:3				K First < Pre (1) Next > Last > 1 GO
		Are you sure you want to delete the ACL application? Cancel OK		

The steps of bulk deleting ACL applications are as follows:

- 1) Select one or more records in the ACL application list.
- Click Delete Port. The message "Are you sure you want to delete the ACL application?" is displayed. Click OK. The message "Delete Succeeded" is displayed, indicating that deletion operation is completed.
- Editing an ACL application

ACL	List ACL Time	ACL Application					
			1. () N				
Note:	If the configuration takes effect but	is not displayed properly on the page,	please refresh the page.				
+ Add	Port 🗙 Delete Port						
	ACL		Port	Direction	Actio	on	
	104(IP)		Gi0/11	in	Edi	Delete	
	104(IP)		Gi0/11	out	Edi	Delete	
	701(MAC)		Gi0/24	in	Edi	Delete	
Show	No.: 10 🗸 Total Count:3		PortGi0/11		×	K Firs	t < Pre 1 Next > Last > 1 GO
			ACL Li	t: 104(IP) 🗸			
			Directio	i Input 🗸			
				Cancel Save			
					•		

The steps of editing an ACL application are as follows:

- 1) In the ACL application list, click Edit in the Action column for an ACL application.
- 2) The displayed dialog box displays information about the ACL application. Edit the information.
- After editing, click Save. The message "Configuration Succeeded" is displayed, indicating that the editing operation is completed.
- Deleting an ACL application

ACL List ACL Time A	CL Application			
Note: If the configuration takes effect but is not dis	played properly on the page, please refresh the page.			
+ Add Port X Delete Port				
C ACL	Port	Direction	Action	
104(IP)	Gi0/11	in	Edit Delete	
104(IP)	Gi0/11	out	Edit Delete	
701(MAC)	Gi0/24	in	Edit Delete	
Show No: 10 V Total Count:3				K First K Pre (1) Next > Last > (1) GO
		Are you sure you want to delete the item?		

The steps of deleting an ACL application are as follows:

- 1) In the ACL application list, click **Delete** in the **Action** column for an ACL application.
- 2) The message "Are you sure you want to delete the item?" is displayed. Click OK. The message "Delete Succeeded" is displayed, indicating that the deletion operation is deleted.

1.3.3.3.2 Port Security

Dert Security Settings

• Adding a security port

t Securit Settings	Security Binding			
: It is generally applied tion.	to the scenario where the accessed user hi	s valid IP and MAC address or where the user accesses the network through a fixed port instead of ch	hanging IP/MAC address or port number, or limits the number of MAC addresse	s on the console port to avoid attacks caused by MAC add
: If the configuration ta	akes effect but is not displayed properly on	the page, please refresh the page.		
i Port 🗙 Delete S	elected			
Port	Max Secure Address	Aging Time	Security Action	Action
		Add Port	×	
			<u>^</u>	
		Max Secure Address: 128 *		
No.: 10 🗸 Total	Count:0	Arias Terry 0		K First K Pre Next > Last > 1
		Aging time.		
		Security Action: Protection		
		Select Port:		
		Selected 1 AG Port 💼 Up 💼 Shutdown 💽 VSL Port	Copper Fiber	
			30 32 34 36 38 40 42 44 46 48	
			· · · · · · · · · · · · · · · · · · ·	
		All invert Deselect Notesclick and hold the left button as y	you arag the pointer across the section to select multiple ports.	
		Cancel Save		
		Current Current Current		

The steps of adding a security port are as follows:

- 1) Click Add Port.
- 2) (Required) Configure Max Secure Address. The maximum value of this parameter is 128.
- 3) (Required) Configure **Aging Time**. The value range of this parameter is 0 to 1440.
- 4) Select one port at least.

5) After configuration, click **Save**. The message "Configuration Succeeded" is displayed, indicating that the adding operation is completed.

• Editing a security port

Port Securit Settings	Security Binding			
Note: It is generally applied to depletion. Note: If the configuration take	the scenario where the accessed user has valid IP and MAC es effect but is not displayed properly on the page, please rel	address or where the user accesses the network through a fixed port instead resh the page.	of changing IP/MAC address or port number, or limits th	ne number of MAC addresses on the console port to avoid attacks caused by MAC address
+ Add Port X Delete Sele	ected			
D Port	Max Secure Address	Aging Time	Security Action	Action
Gi0/11	50	40	Protection	Edit Delete
Show No.: 10 V Total Co	punt:1			K First < Pre (1) Next > Last > (1) GO
		Edit - Gi0/11	×	
		May Serune Address: 50	*	
		Julia Scene Andress		
		Aging Time: 40	*	
		Security Action: Protection	~	
		Cancel	ve	

- 1) In the user security port list, click **Edit** in the **Action** column for a security port. Information about the security port is displayed.
- 2) Edit information.
- 3) After editing, click **Save**. The message "Configuration Succeeded" is displayed.
- Deleting a security port

Port Securit Settings	Security Binding			
Note: It is generally applied to depiction. Note: If the configuration take + Add Port X Delete Seld	o the scenario where the accessed user has valid IP and MAC es effect but is not displayed property on the page, please ref ected	address or where the user accesses the network through a fixed port instead resh the page.	of changing IP/MAC address or port number; or limits th	te number of MAC addresses on the consiste port to avoid attacks caused by MAC address
Port	Max Secure Address	Aging Time	Security Action	Action
Gi0/11	50	40	Protection	Edit Delete
Show No.: 10 - Total G	ount:1			K First K Pre (1) Next > Last > 1 GO
		 Are you sure you want to delete the security port? Cancel CK 	×	

The steps of deleting a security port are as follows:

- 1) Select multiple records in the security port list and click **Delete Selected** to bulk delete the records.
- 2) In the security port list, click **Delete** in the Action column for a security port. The message "Are you sure you want to delete the security port?" is displayed. Click **OK**. The message "Delete Succeeded" is displayed, indicating that the deletion operation is completed.
- **Security Binding**
- Adding a security address to be bound

Port Securit Settings	Security Binding				
Neter Port Security is used to all	ou only the packet where course MAC a	deers is consistent with the secure address to enter the	cuitch		
+ Add Address 🗙 Delete Se	elected				
Port	IP	MAC	VLAN ID		Action
		Add Address		×	
Show No.: 10 V Total Cou		IP:	*	<u>^</u>	K First 〈 Pre Next 〉 Last 〉 1 GO
		MAC:			
		VLAN ID:			
		Select Port:			
		Selected 1 AG Port 🛑 Up 🛄 Shu	tdown 💽 VSL Port	Copper Fiber	
			5 17 19 21 23 25 27 29 31 33 35 37 10 10 10 11 11 11 11 11 11 11 11 11 11 1		
			Image: Constraint of the state of		
		•		· · ·	
			Cancel Save		

The steps of adding a security address to be bound are as follows:

- 3) Click Add Address.
- 4) Configure the security address to be bound. **IP** is required and other parameters are optional. Select a port.
- 5) After configuration, click **Save**. The message "Configuration Succeeded" is displayed. The added security address is displayed in the list of bound security addresses.
- Editing a bound security address

Port Securit Settings	Security Binding						
Note: Port Security is used to all	ow only the packet whose source MAC address is consistent w	ith the secure address to enter the switch.					
+ Add Address 🗙 Delete Se	lected						
Port	IP	MAC	VLAN ID	Ac	tion		
🗆 Gi0/15	147.156.89.1			E	idit Delete		
□ Gi0/13	192.147.2.5				dit Delete		
Show No.: 10 V Total Cou	nt:2					K First K Pre (1)	Next > Last > 1 GO
		Edit - Gi0/15		×			
		IP: 147.1	*				
		MAC:					
		VLAN ID:					
		Can	Save				

- 1) In the list of bound security addresses, click **Edit** in the **Action** column for a bound security address. Information about the security address is displayed.
- 2) Edit information.
- 3) After editing, click **Save**. The message "Configuration Succeeded" is displayed.
- Deleting a bound security address

Port Securit Settings	Security Binding				
Note: Port Security is used to	o allow only the packet whose source MAC address is consistent wi	th the secure address to enter the switch.			
+ Add Address X Delete	e Selected				
Port	IP	MAC	VLAN ID	Action	
🗇 Gi0/15	147.156.89.1			Edit Delete	
🗇 Gi0/13	192.147.2.5			Edit Delete	
Show No.: 10 V Total C	Count:2			K First < Pre (1) Next > Last >	1 60
		Are you sure you we the port? Cancel O	X ant to delete		

The steps of deleting a bound security address are as follows:

- 1) Select multiple records in the list of bound security addresses and click **Delete Selected** to bulk delete the records.
- 2) In the list of bound security addresses, click **Delete** in the **Action** column for a bound address. The message "Are you sure you want to delete the port?" is displayed. Click **OK**. The message "Delete Succeeded" is displayed, indicating that the deletion operation is completed.

1.3.3.3.3 Storm Control

• Adding a storm control port

+ Add Port X Delete Selected					
D Port	Broadcast	Multicast	Unicast	Action	
🗆 Gi0/1		Add Port		×	te
□ Gi0/2		Select Port:			te
□ Gi0/3		Selected 1 AG Port 🛑 Up 🛄 Shutdown 💽 VSL Por	rt	Copper Fiber	te
□ Gi0/4			23 25 27 29 31 33 35	37 39 41 43 45 47	te
□ Gi0/5					te
□ Gi0/6		2 4 6 8 10 12 14 16 18 20 22	24 26 28 30 32 34 36	38 40 42 44 46 48	te
□ Gi0/7		All Invert Deselect Note:Click and	hold the left button as you drag the pointer	r across the section to select multiple ports.	te
Gi0/8					te
□ Gi0/9		Type: 🖲 Bandwidth Usage 🔿 Packets	⊖ Kilobits		te
Gi0/10		Broadcast: %			te
Show No.: 10 V Total Count:51		Multicast: %			irst < Pre (1) 2 3 4 5 Next > Last > 1 GO
		Unicast: %			
		C	ancel Save		

The steps of adding a storm control port are as follows:

- 1) Click Add Port.
- 2) Set a storm control port. Set one of the Broadcast, Multicast, and Unicast parameters.
- After configuration, click Save. The message "Configuration Succeeded" is displayed. The added storm control port is displayed in the storm control port list.

• Editing a storm control port

+ Ad	i Port X Delete Selected					
	Port	Broadcast	Multicast	Unicast		Action
	Gi0/25					Edit Delete
	Gi0/26					Edit Delete
	Gi0/27		-	-		Edit Delete
	Gi0/28		-			Edit Delete
	Gi0/29	100%	Edit Port - Gi0/29		×	Edit Delete
	Gi0/30					Edit Delete
	GI0/31		lype: 💿 l	Bandwidth Usage 🔿 Packets 🔿 Kilobits		Edit Delete
	Gi0/32		Broadcast: 1	00 %		Edit Delete
	Gi0/33		Multicast:	%		Edit Delete
	GI0/34			~		Edit Delete
Sho	v No.: 10 🗸 Total Count:51		Unicast	76		K First < Pre 1 2 (3) 4 5 Next > Last > 3 GO
					-	
				Cancel Save		

The steps of editing a storm control port are as follows:

- 1) In the storm control port list, click **Edit** in the **Action** column for a storm control port. Information about the storm control port is displayed.
- 2) Edit information.
- 3) After editing, click **Save**. The message "Configuration Succeeded" is displayed.
- Deleting a storm control port

+ Add Port X Delete Selected				
Port	Broadcast	Multicast	Unicast	Action
Gi0/25				Edit Delete
Gi0/26				Edit Delete
Gi0/27				Edit Delete
□ Gi0/28				Edit Delete
□ Gi0/29	100%			Edit Delete
Gi0/30				Edit Delete
Gi0/31		×		Edit Delete
Gi0/32		Are you sure you want to delete		Edit Delete
Gi0/33		the port?	·	Edit Delete
□ Gi0/34		Cancel	•	Edit Delete
Show No.: 10 V Total Count:51				K First ≤ Pre 1 2 (3) 4 5 Next > Last > 3 GO

The steps of deleting a storm control port are as follows:

- 1) Select multiple records in the storm control port list and click **Delete Selected** to bulk delete the records.
- 2) In the storm control port list, click **Delete** in the **Action** column for a storm control port. The message "Are you sure you want to delete the port?" is displayed. Click **OK**. The message "Delete Succeeded" is displayed, indicating that the deletion operation is completed.

1.3.3.3.4 DHCP Snooping

The figure below shows the **DHCP Snooping** page.

Figure 1-1 Setting DHCP Snooping

Note: DHCP incoping is used to filter DHCP packets received on an uninuted port from outside the network or firewall. The DHCP request packet is forwarded to the trusted port. The DHCP reply packet Nete: The port connected to the DHCP inner is configured as a trusted port generally.	is forwarded only if it is from a trusted port.
DHCP Snooping: COL	
Select Port:	
🗂 Selected 🚹 AG Port 💼 Up 💼 Shutdown 💽 VSL Port	Copper Fiber
All Invert Deselect	Note:Click and hold the left button as you drag the pointer across the section to select multiple ports.
Trusted Port: 📀	
Save Display DHCP Snooping Trusted Port	

The steps of setting DHCP snooping are as follows:

- 1) Click **DHCP Snooping** to enable it.
- 2) Select the port to be configured.

3) Click **Save** to save the configuration. Click **Display DHCP Snooping Trusted Port** to display the configured ports.

The port connecting to a DHCP server needs to be configured as a DHCP trusted port. The DHCP server connecting to a nontrusted port cannot work properly. A configured trusted port indicates that the DHCP trusted port is enabled on the port. You can select ports on the panel and click **Save**.

1.3.3.3.5 Gateway Anti-ARP-Snooping

The Gateway Anti-ARP-Snooping page allows you to configure anti-ARP spoofing, ARP check, DAI settings, and ARP entries.

Anti-ARP Spoofing

• Adding a filter port

Anti-ARP-Spoofing	ARP Check	DAI Settings	ARP Entries				
Note: It is configured on only	the port connected to the	client to prevent ARP spoofi	ng.				
+ Add Port X Delete Sele	ected						
Filtering Port					IP		Action
				No Data Found			
Show No.: 10 V Total C	ount:0	Add	l Port			×	K First K Pre Next > Last > 1 GO
			Gateway:	*			
			Select Port:	Up 🗍 Shutdown 🚺 VSL Port	Copper Fiber	1	
				1 13 15 17 19 21 23 25 27 29 31 33 1 1 16	35 37 39 41 43 45 47 1 1 1 1 1 1 1 1 1 1 1 1 1 2 1 1 1 1 1 36 38 40 42 44 46 48		
		All	Invert Deselect	Note:Click and hold the left button as you drag the point	nter across the section to select multiple ports.		
				Cancel			

The steps of adding a filter port are as follows:

- 1) Click Add Port.
- 2) Set a filter port. Gateway is a required field. Select at least one filter port.

- 3) After configuration, click **Save**. The message "Configuration Succeeded" is displayed. The added filter port is displayed in the filter port list.
- Editing a filter port

Anti-ARP-Spoofing	ARP Check	DAI Settings	ARP Entries		
Note: It is configured on only the	he port connected to the	client to prevent ARP spoofi	1g.		
+ Add Port X Delete Selec	cted				
Filtering Port				IP	Action
□ Gi0/8				174.15.120.1	Edit Delete
🗆 Gi0/25				176.14.12.2	Edit Delete
Show No.: 10 V Total Co	unt:2				K First < Pre (1) Next > Last > (1) GO
				PortGi0/8 × Gateway: 174.15.120.1 · Cancel Save	

The steps of editing a filter port are as follows:

- 1) In the filter port list, click **Edit** in the **Action** column for a filter port. Information about the filter port is displayed.
- 2) Edit information.
- 3) After editing, click **Save**. The message "Configuration Succeeded" is displayed.
- Deleting a filter port

Anti-ARP-Spoofing	ARP Check	DAI Settings	ARP Entries		
Note: It is configured on only	the port connected to the	client to prevent ARP spoofi	ng.		
+ Add Port X Delete Sel	ected				
Filtering Port				IP	Action
GI0/8				174.15.120.1	Edit
□ GI0/25				176.14.12.2	Edit Delete
Show No. 10 V Total C	ount:2				K First C Pre (1) Next > Last > 1 GO
				Are you sure you want to delete the port? Cancel CK	

The steps of deleting a filter port are as follows:

- 1) Select multiple records in the filter port list and click **Delete Selected** to bulk delete the records.
- 2) In the filter port list, click **Delete** in the **Action** column for a filter port. The message "Are you sure you want to delete the port?" is displayed. Click **OK**. The message "Delete Succeeded" is displayed, indicating that the deletion operation is completed.
- ARP Check

Anti-ARP-Spoofing	ARP Check	DAI Settings	ARP Entries								
Note: ARP Check is used to fil	iter all ARP packets on the I	ogical port and discard invali	I ARP packets. It can effectively	r prevent ARP Spoofing and improve ne	twork stability. A DHCP	Snooping trusted p	port cannot be enabled wit	h ARP Check.			
Select Port:											
Selected 1 AG Port	Up Shutdown	VSL Port									Copper Fiber
	11 13 15 17 10 10 1 12 14 16 18	19 21 23 25 27 10 10 10 10 10 20 22 24 26 28	29 31 33 35 30 32 34 36	$\begin{array}{cccccccccccccccccccccccccccccccccccc$	9 51 						
All Invert Deselect							Notes	Click and hold the left butt	on as you drag the pointe	r across the section to	o select multiple ports.
ARP-check Port: 🥏	Save	isplay ARP Check Port									

The steps of configuring ARP check are as follows:

- 1) Ports, on which ARP check is enabled, are displayed on the page.
- 2) Select a port, on which ARP check needs to be enabled and click Save. The page displays the latest configuration.
- 3) Click **Display ARP Check Port** to display ports, on which ARP check is enabled.

The panel displays ports with the ARP check function enabled and the ports can be edited. If you want to abandon the modification to a port, click **Display ARP Check Port** to display the current ARP-check ports on the panel.

A The ARP check function cannot be enabled on DHCP snooping trusted ports.

DAI Settings

1. Configuring VLAN DAI

Anti-ARP-Spoofing	ARP Check	DAI Settings	ARP Entries						
VLAN DAI Configurati	on								
Note: The untrusted port corre	sponding to the DAI-enabl	ed VLAN intercepts all ARP r	request and reply packets	to discard invalid ARP	packets				
+ Add VLAN DAI									
Trusted Port			Add VI	AN DAI			×		
Note: Packets received on the	trusted port skip DAI Inspe	ction as valid ARP packets.		VLAN Range:		* The VLAN range is formatte	ted as 3-5,100.		
		_							
Selected AG Port	Up Shutdown	VSL Port	7 29 31		Cancel	Save			Copper Fibe
		ĩão đó	ìòò			-			
2 4 6 8 10	ل ل ا 15 ل ا 12 14 16 18	20	لے لیے لیے لیے لیے لیے 8 30 32 34 36	L.J.L.J.L.J 38 40 42	44 46 48 50 52]			
All Invert Deselect							,	Note:Click and hold the left button as you drag the	pointer across the section to select multiple ports
Trusted Port: 🤨									
	Save	isplay Trusted Port							

The steps of configuring VLAN DAI are as follows:

- 1) Click Add VLAN DAI. The Add VLAN DAI dialog box is displayed.
- 2) Enter the VLAN range.
- 3) Click **Save**. The list configuration is refreshed.
- 2. Removing the VLAN DAI configuration

Anti-ARP-Spoofing	ARP Check	DAI Settings	ARP Entries	
VLAN DAI Configuration	on			
Note: The untrusted port corre	sponding to the DAI-enabl	ed VLAN intercepts all ARP r	equest and reply packets to	discard invalid ARP packets
+ Add VLAN DAI 🛛 🖻 Selec	t All 🛛 Deselect All	î Batch Delete		
VID4 VID5	⊗ VID6			

The steps of removing the VLAN DAI configuration are as follows:

- 1) Select the required VLAN DAI configuration or click Select All, and click Batch Delete.
- 2) Click the deletion icon in the upper right corner to delete the VLAN DAI configuration.

Trusted Port						
Note: Packets received on the truste	d port skip DAI Inspection as valid ARI	packets.				
Claimer Change III	El dura Alverna					
Selected 1 AG Port	Shutdown VSL Port					Copper Piber
	ה'ה'ה'ה'ה'ה'	ññññññ		49 51	DAL Trusted Port	
					DAI Husted Port	
2 4 6 8 10 12	14 16 18 20 22 24	26 28 30 32 34 36	38 40 42 44 46 48	50 52		
All Invert Deselect					Note:Click and hold the left button as you o	Irag the pointer across the section to select multiple ports
Trusted Port: 🥑						
	Save Display Trusted I	Port				

The steps of configuring a DAI trusted port are as follows:

- 1) Select a port to be configured as a DAI trusted port and click **Save**. The latest configuration is displayed.
- 2) Click **Display Trusted Port** to display configured DAI trusted ports.
- The panel displays DAI trusted ports and the ports can be edited. If you want to abandon the modification to a port, click Display Trusted Port to display current DAI trusted ports on the panel.

ARP Entries

• Dynamic binding>>static binding

i-ARP-Spoofing	ARP Check	DAI Settings	ARP Entries		
namic Binding>>Stati	c Binding 🛛 🖓 Delete Se	lected 🛛 🕭 Manual Bind	ing		IP-based:
IP	MAC	Туре		Action	
1.1.1.1	4e54.3800.000	2 Static	Binding	Static Binding>>Dy	namic Binding
192.168.1.200	5416.5158.655	5 Local	ARP Entry	Dynamic Binding>>	Static Binding
v No.: 10 - Total Co	ount: 2			K First	< Pre 🟹 Next >
	i-ARP-Spoofing namic Binding>>Station IP 1.1.1.1 192.168.1.200 v No.: 10 Total Co	i-ARP-SpoofingARP Checknamic Binding>>Static Binding © Delete SelIPMAC1.1.1.14e54.3800.000192.168.1.2005416.5158.655v No.: 10 v Total Count: 2	ii-ARP-Spoofing ARP Check DAI Settings namic Binding>>Static Binding ◇ Delete Selected & Manual Bind IP MAC Type 1.1.1.1 4e54.3800.000 Static 192.168.1.200 5416.5158.655 Local v No.: 10 v Total Count: 2	i-ARP-Spoofing ARP Check DAI Settings ARP Entries Inamic Binding>>Static Binding & Delete Selected & Manual Binding IP MAC Type 11.1.1 4e54.3800.000 Static Binding 192.168.1.200 5416.5158.655 Local ARP Entry No.: 10 ~ Total Court: 2	ARP -Spoofing ARP Check DAI Settings ARP Entries namic Binding>>Static Binding Pelete Selected Manual Binding IP MAC Type Action 1.1.1.1 4e54.3800.0002 Static Binding Static Binding>>Dy 192.168.1.200 5416.5158.6555 Local ARP Entry Dynamic Binding> v No: 10 v< Total Count: 2

The steps of converting a dynamic binding into a static binding are as follows:

- Select dynamic binding entries and click Dynamic Binding>>Static Binding to bulk convert the dynamic binding entries into static binding entries.
- In the ARP entry list, click Dynamic Binding>>Static Binding in the Action column for an ARP entry. The message "Configuration succeeded!" is displayed.
- Deleting static bindings

🧭 Dynamic Binding>>Static Binding 🔗 Delete Selected 🐁 Manual Binding	
	IP-based:
IP MAC Type Action	
Image: 1.1.1 4e54.3800.0002 Static Binding	>>Dynamic Binding
192.168.1.200 5416.5158.6555 Local ARP Entry Dynamic Bindi	ng>>Static Binding
Show No.: 10 - Total Count: 2 K F	First < Pre 🏹 Next 🕽

The steps of deleting static bindings are as follows:

- 1) Select static binding entries and click **Delete Selected** to bulk delete the static binding entries.
- In the ARP entry list, click Static Binding>>Dynamic Binding in the Action column for a static binding entry. The message "Configuration Succeeded" is displayed.

Manual binding

An	ti-ARP-Spoofing	ARP Check	DAI Settings	ARP Entries						
æ Dy	namic Binding>>Stati	c Binding 🖓 Delete S	elected 👌 Manual Bindi	ing					IP-based:	Search
	IP		MAC		Туре	Action				
	172.162.1.7		0002.0002.0003		Manual Binding		× c Binding	2		
	172.168.4.2		0002.0003.0003		10.		c Binding			
Sho	w No.: 10 ∨ Total C	ount: 2			1P:			K Fi	irst < Pre 1 Next >	Last X 1 GO
					MAC:	*				
						OK Cancel				

The steps of performing manual binding are as follows:

1) Click Manual Binding.

- 2) Configure static binding data. **IP** and **MAC** are required fields.
- After configuration, click **OK**. The message "Configuration Succeeded" is displayed. The added static binding entry is displayed in the ARP entry list.

1.3.3.3.6 IP Source Guard

The IP Source Guard page allows you configure ports and bind users.

Port Settings

• Adding an IP Source Guard port

Port Settings	User Binding					
Note: IP Source Guard	I is applied in combination with DHCP Snooping.	Port-based IP Source Guard takes effect on only the untrusted port enabled	with DHCP Snooping. Otherwise, IP Sc	ource Guard does not take ef	lfect.	
+ Add Port X Dele	ete Selected					
Port	Filter Type	Filter Mode	IP	MAC	VLAN ID	Action
			No Data Found			
Show No.: 10 🗸 1	Total Count:0	Add Port			×	K First K Pre Next > Last X 1 GO
		Filter Type: IP			*	
		Selected AG Port Up Shutdown VSL	Port 1 23 25 27 29 31 3	3 35 37 39 41	Copper Fiber	
			Cancel Save			

The steps of adding an IP Source Guard port are as follows:

1) Click **Add Port**. The **Add Port** dialog box is displayed.

- 2) Set **Filter Type** and select ports.
- 3) After configuration, click **Save**. The message "Configuration Succeeded" is displayed. The added IP Source Guard port is displayed in the IP Source Guard port list.

• Deleting an IP Source Guard port

Por	t Settings	User Binding					
Note	s IP Source Guard is app	alied in combination with DHCP Snooping. Port	based IP Source Guard takes effect on only the untruste	d port enabled with DHCP Snooping. Otherwise, IP S	ource Guard does not take effect.		
+ Ad	d Port 🗙 Delete Se	lected					
	Port	Filter Type	Filter Mode	IP	MAC	VLAN ID	Action
	Gi0/13	IP-ONLY	Active	Deny-All			Delete
	Gi0/27	IP+MAC	Active	Deny-All			Delete
	v No.: 10 V Total (Sount:2					K First K Pre (1) Next > Last > (1) GO
			Are the	X you sure you want to delete tem? Cancel			

The steps of deleting an IP Source Guard port are as follows:

- 1) Select multiple records in the IP Source Guard port list and click **Delete Selected** to bulk delete the records.
- 2) In the IP Source Guard port list, click **Delete** in the **Action** column for an IP Source Guard port. The message "Are you sure you want to delete the item?" is displayed. Click **OK**. The message "Delete Succeeded" is displayed, indicating that the deletion operation is completed.

User Binding

• Adding a user binding

Port Settings	User Binding					
Note: 1. The IP Source (Note: 2. If the port is co	Guard-enabled port filters all nor onfigured as a DHCP Snooping tr	n-DHCP IP packets. A usted port, the config	ter configured with the static IP address, the port allows specifie uration on this port takes effect but it will not filter packets.	IP packets to pass through.		
+ Add Binding X D	Delete Selected					
MAC		IP	VLAN ID	Port		Action
			Add Binding		×	
Show No.2 10 T	otal Count®		MAC: IP: VLAN ID: Select Port: Select Port: 1 3 5 7 9 11 13 15 17 13 2 4 6 8 10 12 14 16 18 20 2 4 6 8 10 12 14 16 18 20	2000er Fiber 43 45 47 14 46 45 14 46 45	K First < Pre Next > Last X 1 60

The steps of adding a user binding are as follows:

- 1) Click Add Binding.
- 2) Configure the user binding. MAC, IP, and VLAN ID are required fields.

- After configuration, click Save. The message "Configuration Succeeded" is displayed. The added user binding is displayed in the user binding list.
- Editing a user binding

Port Settings	User Binding					
Note: 1. The IP Source G Note: 2. If the port is co	uard-enabled port filters all nfigured as a DHCP Snoopir	non-DHCP IP packets. After configured with the static IP addres ig trusted port, the configuration on this port takes effect but it i	, the port allows specified IP packets to pass through. vill not filter packets.			
+ Add Binding × De	elete Selected					
MAC		IP	VLAN ID	Port	Action	
0003.0001.000	2	192.168.1.1	4	Gi0/27	Edit Delete	
0001.0003.000	3	192.145.1.2	7	Gi0/39	Edit Delete	
Show No.: 10 V	tal Count:2		PortGI0/27 MAC: 0003.0001.0002 IP: 192.168.1.1 VLAN ID: 4 Cancel Save	×	K first 〈 Pre ① Nest 〉 Last X 1	

The steps of editing a user binding are as follows:

- 1) In the user binding list, click **Edit** in the **Action** column for a user binding. Information about the user binding is displayed.
- 2) Edit information about the user binding.
- 3) After editing, click **Save**. The message "Configuration Succeeded" is displayed.
- Deleting a user binding

Port Settings	User Binding					
Note: 1. The IP Source Note: 2. If the port is a	e Guard-enabled port filters al configured as a DHCP Snoopi	non-DHCP IP packets. After configured with the static IP address, the ing trusted port, the configuration on this port takes effect but it will no	port allows specified IP packets to pass through it filter packets.			
+ Add Binding X	Delete Selected					
D MAC		IP	VLAN ID	Port	Action	
0003.0001.00	02	192.168.1.1	-4	Gi0/27	Edit Delete	
0001.0003.00	008	192.145.1.2	7	Gi0/39	Edit Delete	
Show No: 10 -	Total Count:2				K First K Pro (1) N	Next > Last > 1 GO
			Are you sure you want to delete the binding?			

The steps of deleting a user binding are as follows:

- 1) Select multiple records in the user binding list and click **Delete Selected** to bulk delete the records.
- 2) In the user binding list, click **Delete** in the **Action** column for a user binding. The message "Are you sure you want to delete the binding?" is displayed. Click **OK**. The message "Delete Succeeded" is displayed, indicating that the deletion operation is completed.

1.3.3.3.7 NFPP

The figure below shows the **NFPP** page.

ARP-guard: 🗾 Enable ARP-guard, so as to prevent a large number of invalid ARP packets from attacking the device.
[ARP-guard List] Select a required guard list to display the guard list.
IP-guard: 😰 Enable IP-guard, so as to prevent hackers from scanning the entire network and consuming bandwidth.
ICMP-guard: 🗹 Enable ICMP-guard, so as to prevent a large number of invalid ICMP packets from consuming bandwidth and CPU resources.
DHCP-guard: Z Enable DHCP-guard, so as to prevent malicious requests from exhausting DHCP pools and leaving legitimate users unable to access the Internet.
DHCPv6-guard: Z Enable DHCPV6-guard, so as to prevent malicious requests from exhausting DHCPv6 pools and leaving legitimate users unable to access the Internet.
ND-guard: 🛃 Enable ND-guard, so as to prevent Neighbor Discovery packets from consuming bandwidth.
Display NFPP Log: [Display NFPP Log]
Save Restore Default Settings

You can enable/disable the attack guard function and click **Save**. The message "Configuration Succeeded" is displayed. To restore default settings, click **Restore Default Settings**.

1.3.3.4 Advanced

1.3.3.4.1 IGMP Snooping

The figure below shows the **IGMP Snooping** page.

Figure 1-2 Configuring IGMP Snooping

Profile ID	Multicast Address	Policy Action	Application Port	Action
		No Data Found		
nu Na 1011 Tatal Causto				K Root of Deer March X Last X
ivition 10 + iotal counco				K HISC K FIG NEWL Z LUSC ZI

• Adding a profile

Note: On layer 2 devices, multicast frames are flood	led to all ports, causing storm and consuming much ban	dwidth. IGMP Snooping is used to find out on which port there is an IGMP	subscriber and only send IGMP traffic to the port, so as to save bar	dwidth.
+ Add Profile × Delete Selected IGMP Sno	poping: ON			
Profile ID	Multicast Address	Policy Action	Application Port	Action
	Add Profile		\$	<
Show No.: 10 V Total Count:0	Profile ID:	* Range (1-1024)		K FQ < Pre Next > Last > 1 GO
	Multicast Range:	*-		
	Policy Action: PERN	11T O DENY		
	Select Port:			
	Selected AG Port Up	Shutdown 🚺 VSL Port	Copper Fiber	
	$\begin{array}{c}1\\1\\2\\4\\4\\6\\8\\10\\12\end{array}$	$\begin{matrix} 13 & 15 & 17 & 19 & 21 & 23 \\ \hline & \bullet & \bullet & \bullet & \bullet \\ \hline \bullet & \bullet & \bullet & \bullet & \bullet \\ 14 & 16 & 18 & 20 & 22 & 24 \end{matrix} \qquad \begin{array}{c} 25 & 27 & 29 & 31 & 33 & 35 \\ \hline & \bullet & \bullet & \bullet & \bullet \\ 26 & 28 & 50 & 51 & - \\ 26 & 28 & 50 & 52 & 24 & 36 \\ \hline \end{array}$	37 39 41 43 45 47 49 51	
	All Invert Deselect	NotesClick and hold the left button	as you drag the pointer across the section to select multiple ports	
		Cancel Save		

The steps of adding a profile are as follows:

- 1) Click Add Profile.
- 2) Configure a profile. The **Profile ID** and **Multicast Range** fields are required and other fields are optional.
- After configuration, click Save. The message "Configuration Succeeded" is displayed. The added profile is displayed in the profile list.
- Editing a profile

Note: On layer 2 devices, multicast frames are flood	ded to all ports, causing storm and consuming much bandwidth. IGMP Snooping	g is used to find out on which port there is an IGMP subscriber ar	nd only send IGMP traffic to the port, so as to sa	we bandwidth.
+ Add Profile × Delete Selected IGMP Sno	ooping: ON			
Profile ID	Multicast Address	Policy Action	Application Port	Action
□ 10 2i	224.0.0.1 239.123.4.1	PERMIT	Gi0/33	Edit Delete
□ 15 2 ²	239.255.1.4 239.2 ⁱ Edit Profile		×	Edit Delete
Show No.: 10 V Total Count:2	Profile ID: 10 Multicast Range: 2240.0.1 Policy Action: • PERMIT O C Select Port: Select Port: 1 3 5 7 9 11 1 13 2 4 6 8 10 12 14 16 All Invert: Decelect	* Range (1-1024) * - 233.123.4.1 CENY down * VSL Port 10 29 21 22 21 25 27 29 31 33 35 10 29 21 22 24 26 28 35 32 24 46 Note:Click and hold the left button as you drag the pointer Cancel Save	Copper Fiber 7 99 41 43 45 47 3 90 41 43 45 47 3 90 42 44 46 40 2 2 44 46 40 2 2 2 44 46 40	K First < Pre (1) Next > Last > 1 GO

The steps of editing a profile are as follows:

- 1) In the profile list, click **Edit** in the **Action** column for a profile. Information about the profile is displayed.
- 2) Edit the profile.
- 3) After editing, click **Save**. The message "Configuration Succeeded" is displayed.
- Deleting a profile

dd Profile X Delete Sele	cted IGMP Snooping:				
Profile ID	Multicast Address		Policy Action	Application Port	Action
10	224.0.0.1 239.123.4.1		PERMIT	Gi0/33	Edit De
15	239.255.1.4 239.255.255.4		PERMIT	Gi0/31,	Edit De
w No.: 10 🗸 Total Cour	nt:2			K	First < Pre (1) Next > Last > [1
		Are you sure you want to de the profile?	×		

The steps of deleting a profile are as follows:

- 1) Select multiple records in the profile list and click **Delete Selected** to bulk delete records.
- 2) In the profile list, click **Delete** in the **Action** column for a profile. The message "Are you sure you want to delete the profile?" is displayed. Click **OK**. The message "Delete Succeeded" is displayed, indicating that the deletion operation is completed.

1.3.3.4.2 QOS

**** Class Settings

The figure below shows the **Class Settings** tab page.

Figure 1-3 Class Settings

Class Settings Policy Settings Flow Settings				
Note: Classification is used to identify and mark certain data flows that match the ACL rule.				
+ Add Class X Delete Selected				
Class Name	ACL	Action		
No I	Pata Found			
Show No.: 10 V Total Count0		K First K Pre Next > Last > 1 GO		

Adding a class
Class Settings	Policy Settings	Flow Settings					
Note: Classification is u	ed to identify and mark certai	n data flows that match the A	CL rule.				
+ Add Class 🗙 Dele	te Selected						
Class Name						ACL	Action
				No	Data Found		
Show No.: 10 V To	tal Count:0						K First 〈 Pre Next 〉 Last 〉 1 GO
				Add Class		×	
				Class Name:	* (1-31) Bytes		
				ACL List: 104	✓ [ACL List]		
				Can	save		

The steps of adding a class are as follows:

- 1) Click Add Class.
- 2) Configure a class. Class Name is a required field. Select an ACL.
- After configuration, click Save. The message "Configuration Succeeded" is displayed. The added class is displayed in the class list.
- Editing a class

Class Settings	Policy Settings	Flow Settings						
Note: Classification is u	used to identify and mark certai	n data flows that match the AC	L rule.					
+ Add Class 🗙 Del	ete Selected							
Class Name						ACL		Action
C RG001						104		Edit Delete
□ RG002						104		Edit Delete
Show No.: 10 V	otal Count:2						K First	< Pre 1 Next > Last > 1 GO
			Edit Clas	is .		×		
				Class Name: RG001	* (1-31) Bytes			
				ACI List 104	IACI Liet			
				104	• [Not tist]			
						_		
				Cancel	Save			
						_		

The steps of editing a class are as follows:

- 1) In the class list, click **Edit** in the **Action** column for a class. Information about the class is displayed.
- 2) Edit information about the class.
- 3) After editing, click **Save**. The message "Configuration Succeeded" is displayed.
- Deleting a class

Class Settings Policy Settings Flow Settings			
Note: Classification is used to identify and mark certain data flows that match the ACL rule.			
+ Add Class X Delete Selected			
Class Name		ACL	Action
□ RG001		104	Edit Delete
□ RG002		104	Edit Delete
Show No.: 10 V Total Count:2			K First K Pre (1) Next > Last X 1 GO
	Xe you sure you want to delete the term?		

The steps of deleting a class are as follows:

- 1) Select multiple records in the class list and click **Delete Selected** to bulk delete the records.
- 2) In the class list, click **Delete** in the **Action** column for a class. The message "Are you sure you want to delete the item?" is displayed. Click **OK**. The message "Delete Succeeded" is displayed, indicating that the deletion operation is completed.

V Policy Settings

The figure below shows the **Policy Settings** tab page.

Figure 1-4 Policy Settings

Class Settings Pol	licy Settings Flow Settings			
Note: The policy is used to constra Note: If the configuration takes eff	ain the bandwidth that the classified data flow consumes. fect but is not displayed properly on the page, please refresh	the page.		
Policy List:	Add Policy Delete Policy + Add Policy Ru	le 🗙 Delete Selected		
Class Name	Bandwidth (KBps)	Burst Traffic (KBytes)	Bandwidth Violation Disposal	Action
		No Data Found	1	
	10			K Einst (Dog News) Last N 1 CO

Adding a policy

Note: The policy is used to constrain the ba Note: If the configuration takes effect but is	indwidth that the classified data flow consumes. s not displayed properly on the page, please refre	sh the page.		
Policy List: Add Po	Delete Policy + Add Policy	Rule × Delete Selected		
Class Name	Bandwidth (KBps)	Burst Traffic (KBytes)	Bandwidth Violation Disposal	Action
		No Data Fo	und	
Show No.: 10 Y Total Count:0				K First K Pre Next > Last > 1 GO
		Add Policy	×	
		Policy Name:	(1-31) Bytes Chinese and Chinese characters are not	
		Cancel	Save 2	

The steps of adding a policy are as follows:

1) Click Add Policy.

- 2) Configure a policy. Policy Name is a required field.
- After configuration, click Save. The message "Configuration Succeeded" is displayed. The added policy is displayed in the policy list.
- Deleting a policy

Class Settings Police	cy Settings Flow Settings			
Note: The policy is used to constrain Note: If the configuration takes effe	in the bandwidth that the classified data flow consumes. act but is not displayed properly on the page, please refres	h the page.		
Policy List: test1 🗸	Add Policy Delete Policy + Add Policy R	ule 🗙 Delete Selected		
Class Name	Bandwidth (KBps)	Burst Traffic (KBytes)	Bandwidth Violation Disposal	Action
Show No. 10 V Total Counts		No Data Found		Kfirst (Pre Next) 1act) 1
		Are you sure you want to delete the item?		
		Cancel		

The steps of deleting a policy are as follows:

- 1) Select a policy in the policy list and click **Delete Policy**.
- 2) The message "Are you sure you want to delete the item?" is displayed. Click OK. The message "Delete Succeeded" is displayed, indicating that the deletion operation is completed.
- Adding a policy rule

Class Settings Policy Settings File	low Settings				
Note: The policy is used to constrain the bandwidth that the class Note: If the configuration takes effect but is not displayed prope	assified data flow consumes. erly on the page, please refresh the page.				
Policy List: test1 Add Policy Delete Po	Policy + Add Policy Rule × D	elete Selected			
Class Name Bandwidth	h (KBps)	Burst Traffic (KBytes)	Bandwidth V	iolation Disposal	Action
		No Data F	ound		
		Add Policy Rule	×		
Show No.: 10 V Total Count:0		Dellas Manag	1 // 2010 / v	ŀ	<pre>< First < Pre Next > Last > 1 GO</pre>
		Policy Name: test1	* (1-31) Bytes		
		Bandwidth:	* (64-33554432) KBps		
		Burst Traffic:	* (4-8192)KBytes		
		Limit Violation Disposal:			
		Class List: RG001	~		
		Cancel	Save		

The steps of adding a policy rule are as follows:

- 1) Click Add Policy Rule.
- 2) Configure a policy rule. Bandwidth and Burst Traffic are required and other fields are optional.
- 3) After configuration, click **Save**. The message "Configuration Succeeded" is displayed. The added policy rule is displayed in the policy rule list.
- Editing a policy rule

Class Settings	Policy Settings Flow Settings			
Note: The policy is used to cons Note: If the configuration takes	strain the bandwidth that the classified data flow consumes. effect but is not displayed properly on the page, please refr	esh the page.		
Policy List: test1 🗸	Add Policy Delete Policy + Add Policy	Rule 🗙 Delete Selected		
Class Name	Bandwidth (KBps)	Burst Traffic (KBytes)	Bandwidth Violation Disposal	Action
🗆 RG001	3000000	4	Drop	Edit Delete
Show No.: 10 V Total Con	unt:1			K First K Pre (1) Next > Last > (1) GO
		Edit Policy Rule	×	
		Policy Name: test1	* (1-31) Bytes	
		Bandwidth: 3000000	★ (64-33554432) KBps	
		Burst Traffic: 4	* (4-8192)KBytes	
		Limit Violation Disposal: () Drop		
		Class List: RG001	~	
		Cancel	Save	

The steps of editing a policy rule are as follows:

- 1) In the policy rule list, click **Edit** in the **Action** column for a policy rule. Information about the policy rule is displayed.
- 2) Edit the policy rule.
- 3) After editing, click **Save**. The message "Configuration Succeeded" is displayed.
- Deleting a policy rule

Class Settings	Policy Settings	Flow Settings			
Note: The policy is used Note: If the configuration Policy List: test1	d to constrain the bandwidth th on takes effect but is not displa	hat the classified data flow con yed properly on the page, ple Delete Policy + Add	names. Ise refrech the page. Policy Rule X Delete Selected		
Class Name	Bandy	width (KBps)	Burst Traffic (KBytes)	Bandwidth Violation Disposal	Action
🗆 RG001	30000	00	4	Drop	Edit Delete
Show No.: 10 V To	otal Count:1				K First 《 Pre ① Next > Last > 1 GO
			Are you sure you want the item? Cancel CK	X to delete	

The steps of deleting a policy rule are as follows:

1) Select multiple records in the policy rule list and click **Delete Selected** to bulk delete records.

2) In the policy rule list, click **Delete** in the **Action** column for a policy rule. The message "Are you sure you want to delete the item?" is displayed. Click **OK**. The message "Delete Succeeded" is displayed, indicating that the deletion operation is completed.

V Flow Settings

The figure below shows the **Flow Settings** page.

Figure 1-5 Flow Settings

Class Settings	Policy Settings	Flow Settings			
Note: The policy is use Note: If the configurati	d to constrain input and output on takes effect but is not displa	flows (Input and output flows of one port yed properly on the page, please refresh t	. must be in the same trust mode but they can be config he page.	gured with different policies)	
+ Add Port X Dele	te Selected				
Port	Directio	n	Policy Name	Trust Mode	Action
			N	lo Data Found	
Show No.: 10 V	otal Count:0				K First K Pre Next > Last > 1 GO

• Adding a policy application port

Class Settings	Policy Settings	Flow Settings				
Note: The policy is used Note: If the configuration	to constrain input and output on takes effect but is not displa	flows (Input and output flows yed properly on the page, plea	of one port must be in the same trust mode but they can be c se refresh the page.	onfigured with different policies)		
+ Add Port X Delet	e Selected					
Port	Direction	n	Policy Name	Trust Mode		Action
		Add Port			×	
Show No.: 10 V To	otal Count:0	Rate-limitir	ng Direction: Input 🗸	Trust Mode: Untrusted 🗸		K First K Pre Next > Last > 1 GO
			Policy List: test1 ~			
			Select Port:			
		Selected	🚹 AG Port 💼 Up 💼 Shutdown 💽 VSL Port		Copper Fiber	
		1	5 7 9 11 13 15 17 19 21 23 ^ 1 () () () () () () () () () (25 27 29 31 33 35 37 39 41 43 45	47 49 51	
		2 4	6 8 10 12 14 16 18 20 22 24	26 28 30 32 34 36 38 40 42 44 46	48 50 52	
		All Invert D	eselect N	totesClick and hold the left button as you drag the pointer across the se	ction to select multiple ports.	
				Cancel Save		

The steps of adding a policy application port are as follows:

- 1) Click Add Port.
- 2) Configure a policy application port. Set Rate-limiting Direction, Trust Mode, Policy List, and Port.
- 3) After configuration, click **Save**. The message "Configuration Succeeded" is displayed. The added policy application port is displayed in the policy application port list.
- Deleting a policy application port

Class Settings	Policy Settings	Flow Settings			
Note: The policy is used Note: If the configuration	I to constrain input and output on takes effect but is not displa	flows (input and output flows of one port ryed properly on the page, please refresh t	must be in the same trust mode but they can be configured with differ he page.	ent policies).	
+ Add Port X Delet	e Selected				
Port	c	Direction	Policy Name	Trust Mode	Action
Gi0/13	h	nput	test1	Untrusted	Delete
Show No. 10 V	stal Count:1				K First < Pre 1 Next > Last > 1 GO
			2 Are you sure you want to delete the item?	¢	

The steps of deleting a policy application port are as follows:

1) Select multiple records in the policy application port list and click **Delete Selected** to bulk delete records.

2) In the policy application port list, click **Delete** in the **Action** column for a policy application port. The message "Are you sure you want to delete the item?" is displayed. Click **OK**. The message "Delete Succeeded" is displayed, indicating that the deletion operation is completed.

1.3.3.4.3 DHCP Relay

The figure below shows the **DHCP Relay** page.

Figure 1-6 Setting DHCP Relay

DHCP relay IPV4 configuration
Note: DHCP relay can centrally manage IP address assignment for large number of subscribers in different subnets. The DHCP relay agent forwards client-originated DHCP packets to a DHCP sener and then forwards the sener-to-client regit to the client.
DHCP Relay: COL
DHCP Server Address: + Add DHCP Server
Save DHCPv6 relay configuration

Enable/Disable DHCP Relay. When DHCP Relay is enabled, you can set multiple DHCP server addresses.

DHCP relay IPV4 configuration
Note: DHCP relay can centrally manage IP address assignment for large number of subscribers in different subnets. The DHCP relay agent forwards client-originated DHCP packets to a DHCP server and then forwards the server-to-client reply to the client.
DHCP Relay: ON
DHCP Server Address: + Add DHCP Server
Save DHCPv6 relay configuration
DHCPv6 relay configuration
Select Layer 3 interface: Gi0/1 🗸
DHCPv6 server address: *
Save

The steps of configuring DHCP Relay are as follows:

- 1) Enable DHCP Relay.
- 2) Set a DHCP server address.
- 3) You can enable DHCPv6 Relay.
- 4) Click **Save**. The DHCP Relay configuration is displayed on the page.

1.3.3.4.4 Authentication

The Authentication page allows you to configure ePortal and advanced settings.

b ePortal

The figure below shows the **ePortal** tab page.

ePortalv2		
Note: Authentication is b	sed on Web to control users' access to the network. It requires no authentication firmware on the client. Instead you can perform authentication on common browsers.	
Eportal Type	: ○ ePortalv1	
Portal Server IP		
Redirection URL		
Portal Key		
Authentication Server	All Servers (Radius Server Settings)	
Accounting Server	All Servers	
SNMP Server	: [SNMP Server] *	
Port		
Selected 1 AG Port	up 💼 Shutdown 💽 VSL Port	Copper Fiber
	11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43 45 47 49 51 ריין רייןרארארארארארארארארארארארארארארארארארא	
All Invert Deselect		Note:Click and hold the left button as you drag the pointer across the section to select multiple ports.
Authentication Port: 🥑		
	·· » Advanced Settings	
	Sove	

The steps of configuring ePortal are as follows:

- 1) Set **Eportal Type** to **ePortalv2**.
- 2) Configure parameters. Portal Server IP, Redirection URL, Portal Key, and SNMP Server are required fields.
- 3) Select a port.
- 4) After configuration, click **Save**. The message "Configuration Succeeded" is displayed.

**** Advanced Settings

The figure below shows the **Advanced Settings** page.

Figure 1-7 Advanced Settings

Advanced Settings				
Redirection HTTP Port:	80, 443	(Range: 1-65535) Please	use ',' to separat	e port numbers. You can configure up to 10 port numbers.
Whitelisted Network Resource:	All users(including unauthorized us	ers) can access the server l	P address. You c	an configure up to 50 IP addresses.
	IP: Ma	isk:	×	+Add
Whitelisted User IP:	The user can access the network wi	thout authentication. You o	an configure up	to 50 IP addresses.
	IP: Ma	isk:	×	+Add
	Save			

The steps of configuring advanced settings are as follows:

1) Click Add.

2) Configure Whitelisted Network Resource and Whitelisted User IP.

3) After configuration, click **Save**. The message "Configuration Succeeded" is displayed.

1.3.4 Diagnosis

Click Diagnosis to open the level-2 menu, which includes Network Diagnosis, One-Click Collection, and Syslog.

1.3.4.1 Network Diagnosis

1.3.4.1.1 Ping

Ping Type:	Not Via Management Por 🗸	0
Dest IP/Domain Name:		*
Timeout Interval(s):	2	Range: 1-10
Repeat Times:	5	Range: 1-100
Packet Size(Bytes):	100	Range: 36-18024
Fragment:	Z Enable	
	Test	

PING Type

Uses the out-of-band channel. The parameter is supported only on MGMT-supported devices. When a MGMT port is configured as a source port, set the parameter to **Via Management Port**. Otherwise, set it to **Not Via Management Port**.

Dest IP/Domain Name

Indicates the address or domain name to be pinged.

Timeout Interval(s)

Indicates the timeout interval.

Repeat Times

Indicates the number of data packets to be sent.

Package Size(Bytes)

Indicates the length of the data padding section in a data packet to be transmitted.

Fragment

Indicates the DF flag bit of an IP address. When the DF flag bit is set to 1, data packets are not fragmented. The default DF flag bit is **0**.

1.3.4.1.2 Tracert

Tracert Type:	Not Via Management Por 🗸	
Dest IP/Domain Name:	•	
Timeout Interval(s):	2	
	Test Stop	

Tracert Type

Uses the out-of-band channel. The parameter is supported only on MGMT-supported devices. When a MGMT port is configured as a source port, set the parameter to Via Management Port. Otherwise, set it to Not Via Management Port.

Dest IP/Domain Name

Indicates the Tracert destination address or domain name address.

Timeout Interval(s)

Indicates the timeout interval.

1.3.4.2 One-Click Collection

The one-click collection function collects device fault information for troubleshooting.

One-Click Collection	

1.3.4.3 Syslog

1.3.4.3.1 Display System Log

You can configure the syslog function to help customers' after-sales and R&D personnel locate problems.

Enable Syslog Logging: 🕐	
Enable Syslog Logging: 🕐 🔵 🖞 Export Log	
System Log (show log)	
O Update Log	Background Color: 🔲 🔳 📕
Syslog logging: disabled	A
Console logging: level debugging, 12 messages logged	
Monitor logging: level debugging, 0 messages logged	
Buffer logging: level debugging, 12 messages logged	
Standard format.false	
Timestamp debug messages: datetime	
Timestamp log messages: datetime	
Sequence-number log messages: disable	
Sysname log messages: disable	
Count log messages: disable	
Trap logging: level informational, 12 message lines logged,0 fail	
Log Buffer (Total 1048576 Bytes): have written 1114	
*Jan 1 00:00:29: %CLI-6-STARTUP: Cli server process startup.	
*Jan 1 00:00:29: %LOCAL_DP-5-LC_PROB: Board information in this chassis has been collected.	
*Jan 1 00:00:29: %DP-6-MASTER: Module in slot 0 has translated to master.	
*Jan 1 00:00:29: %SWITCH-6-INSTALL: Install chassis S5300-48GT4XS-E on switch 1	
*Jan 1 00:00:29: %DP-5-PROB: Board probing has completed.	
*Jan 1 00:00:29: %SYSMON-5-COLDSTART: System coldstart.	
*Jan 1 00:00:29: %REDUNDANCY-6-ROLE_STATES_CHANGE: Redundancy role or state changed: control role active, management role master, state alone.	
*Jan 1 00:00:29: %REDUNDANCY-6-STATES_CHANGE: Redundancy states changed: role master, state alone.	*

Click Enable Syslog Logging to enable/disable syslog. After syslog is enabled, you can export system logs.

1.3.4.3.2 Monitor System Log

You can query logs by level or module to help customers' after-sales and R&D personnel locate problems.

Severity Level: All	Levels 🗸		Search by Module 🗸 Please en	ter a module Search
Severity Level	Module	Mnemonic	Description	Time
(5)Notifications	DEV_MONITOR	CARD_POWER_ON	The power enough, card in slot 0 will be controlled to power on automatically.	1970-01-01 00:00:29
(6)Informational	DP	FAN_OK	Fan 1/1 OK.	1970-01-01 00:00:29
(6)Informational	DP	POWER_OK	Power 1 OK.	1970-01-01 00:00:29
(6)Informational	REDUNDANCY	ROLE_STATES_CHANGE	Redundancy role or state changed: control role active, management role master, state realtime.	1970-01-01 00:00:29
(6)Informational	REDUNDANCY	STATES_CHANGE	Redundancy states changed: role master, state alone.	1970-01-01 00:00:29
(6)Informational	REDUNDANCY	ROLE_STATES_CHANGE	Redundancy role or state changed: control role active, management role master, state alone.	1970-01-01 00:00:29
(5)Notifications	SYSMON	COLDSTART	System coldstart.	1970-01-01 00:00:29
(5)Notifications	DP	PROB	Board probing has completed.	1970-01-01 00:00:29
(6)Informational	SWITCH	INSTALL	Install chassis S5300-48GT4XS-E on switch 1	1970-01-01 00:00:29
(6)Informational	DP	MASTER	Module in slot 0 has translated to master.	1970-01-01 00:00:29
			Load More Refresh	

1.3.5 Maintenance

1.3.5.1 SWITCH

1.3.5.1.1 Upgrade

Note: Please download the c	omsponding firmsare version from the official vehicles and then upgrade the device with the following tips:
Tips: 1. Make sure that the fir	more version (main program or Web package) methods the device wide A. The page may have no reasons being upgrade Please do not power off or restart the device with an upgrade succeeded message is displayed.
File Name:	Browse Upprade Cancel

Click Browse, select a local bin file, and then click Upgrade to upgrade the device locally.

1.3.5.1.2 Config MGMT

Backup

You can back up the configuration file on the device, and import or export configurations to bulk perform operations on the configurations, thereby facilitating user operations.

Backup	Restore	Charset							
Note: Please do	i't close or update the	page during import, or i	import will fail. If you want to apply th	new settings, please restart the	device on this page, or the settin	gs will not take effect.			
Fi	e Name:		Browse Import	Export Current Settings					

N Restore

Backup	Restore	Charset	
Notes After the	device is reset to the fa	ctory default settings.	all settings will be cleared. Please Equipar Current Settings before resetting the device.
Restore Facto	bry settings		
Display Current	Settings		

You can clear the configurations to restore the system to the initial state. You need to use the IP address in the factory settings to access the Eweb.

N	C	harset	t		
Backu	ip	Restore	Charset		
Note: 1	he current	charset is the defaul	t charset. Please set the	t of terminal tool (e.g., SecureCRT) to be the same.	
Selecte	d Charset	t: Default	♥ Save		

Selected Charset can be set to **GBK**, **UTF-8** or **Default**. You are advised to use **UTF-8** for the Eweb and keep the system character set on SecureCRT or other terminal tools to be consistent with that on the Eweb. Otherwise, garble may occur.

1.3.5.1.3 Systime

You can set the system time of the time zone where the device is located so that the device information is accurate.

Current Time:	2022-7-12-13:50:41
Reset Time:	2022-07-12 13:50
Time Zone:	UTC+0(GMT)
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 displays the current system time. You can set the system time manually or select **Automatically synchronize with** an Internet time server.

Click Save. The message "Configuration Succeeded" is displayed, indicating that the operation is completed.

1.3.5.1.4 Syslog

The device can be configured to send local logs to the server for storage for the ease of query.

Local Logging: 🧿	🚺 → Enable/I	Disable the logging f	unction.	
Server IP:				
Logging Level:	formational(6)			
	Save			

Set Server IP and Logging Level. After configuration, the device will send system logs to the server.

1.3.5.1.5 DNS

Domain names can be dynamically parsed only after a DNS server is configured.

D	DNS Server 1:		+
		Save	

1.3.5.2 System

1.3.5.2.1 Web

**** Admin Password

To enhance the system security and information interaction security, you need to change the default password of the system.

Admin Password	Basic Settings	
Username:	admin	
Old Password:		*
New Password:		*
Confirm Password:		×
	Save	

The steps of changing the default password of the system are as follows:

- 1) To change a Web user password, enter the old password in **Old Password**, enter the new password in **New Password**, and enter the new password again in **Confirm Password**.
- 2) If the entered old password is incorrect, the message "Incorrect old password" in red font is displayed. You are required to enter the correct old password and click **Save** to complete the password change.
- The enable password is changed by default when the password of the Eweb is changed.

Basic Settings

You can configure the device location to better inspect the device and facilitate device management. Set **Login Timeout**. When you do not perform operations on the system for long, the Eweb automatically exits to ensure your system security.

Admin Password	Basic Settings	
Web Access Port:	443	* (Range: 443,1025-65535)
Login Timeout:	30 min 🗸	
Device Location:		
Access Redirection:	□ HTTP Redirection to HTTPS	In NAT scenario, redirection may cause HTTP access failure.
	Save	

The steps of configuring basic settings are as follows:

- 1) Set **Web Access Port**. You need to append the port ID when accessing the Eweb from a browser.
- 2) Set Login Timeout.
- 3) Set **Device Location** to facilitate management.

1.3.5.2.2 Telnet

To enhance the system security and information interaction security, you need to configure the Telnet function.

Telnet Service: ON	
SSH Service: OFF	
New Password:	*
Confirm Password:	*
Save	

To change the telnet password, you do not need to enter the old password but need to enter the new password in **New Password** and enter the new password again in **Confirm Password**. Other operations are the same as those of changing the password of the super administrator.

1.3.5.2.3 SNMP

The Simple Network Management Protocol (SNMP) provides a method for collecting network management information from devices on the network. It can be used to manage a large number of network devices.

Copper Fibe

Note: Either SNMPv2 or SNI	her SNMPv2 or SNMPv3 is supported						
SNMP Version:	⊙v2 ⊖v3 → The	fields to be configured vary with the SNMP version.					
Device Location:							
SNMP Community:		*					
Trap Community:		The Trap Community must be the same as the SNMP Community.					
Trap Receiver Address:		* You can configure up to 10 Trap receivers. Please use ',' or press the Enter key to separate addresses.					
	Save						

The steps of configuring SNMP are as follows:

- Set Device Location, SNMP Community, Trap Community, and Trap Receiver Address. The SNMP Community and Trap Receiver Address fields are required and other fields are optional.
- 2) After configuration, click Save. The message "Configuration Succeeded" is displayed.

1.3.6 Other Functions

1.3.6.1 Favorites

After you add frequently configured functions to favorites, you can click menu items in the favorites and configure the functions rapidly next time.

🕕 Curre	rently, a maximum of 10 menu items can be added to favorites.					
Addii	ng to favorites					
Ruijie sw	프 @Monitoring @Config % Diagnosis 및 Maintenance		Enter a search term. 🔾 🐧	i Config Wizard 🛷 🎗 admin		
Favorites O SWITCH Overview	(iii) \$538 Model: 55300-486T4VS-E	8.3% Of Ubare	48.5%	O Refresh		
Anti-loop Monitoring HOHCP	SH: G1G2H960044 M/G Advess: S41631588554 Firmware Venice: S300E (RGOS 12.5/480701		- news j suge			
Other Monitoring +	Hardware Version: 1.21 Booted on: 2022-07-07 12:28:7 Uptime: 5 d 01 h 49 min 22 s	91.5%	51.5% 44.5%			
	System Time: 2022-07-12 14:17:28					

Select a menu item and drag it to Favorites.

Canceling favorites

ted 1 AG

Ruijie sw	표 에 Monitoring @ Config & Diagnosis 및 Maintenance		Enter a search term 🔾 🖄 Config Wizard 💩 A admir
Favorites Client List X Vor. ora dag and drep the memot 5 Favorite Monitoring DECP Client List Server Status Other Monitoring	SSSE Vic 01220902044 Mick Associate Visionis 50020, 8020 15040001 Handram Visionis 15020, 8020 15040001 Handram Visionis 15020, 8020 15040001 Handram Visionis 15020, 8020 15040001 Handram Visionis 121 Bendram Visionis 2020, 8020 1504001 Sprimers Table 2020, 802 1504001 Sprimers Table 2020, 802 1504001	S 9.1 s CUUlage	Charlesh Menory Usay
	Sected ① Al Prot 10		Copper 🗖 Rae

In Favorites, select a menu item and click \times

to remove the menu item from the favorites.

1.3.6.2 Fast Query Menu

There are increasing functions in the system. The fast query menu helps users rapidly search for required functions.

Ruijie sw	☲ 🕼 Monitoring 🛞 Config 🗞 Diagnosis 🛪 Maintenance		DHCP Q	書 Config Wizard 🚿 凡 admin ・
Cient List	553E Mode: 5500-407405-E	(6) 8.5%	DHCP Settings DHCP Settings DHCP Settings DHCP Settings DHCP Settings	O Refresh
SWITCH Overview Anti-loop Monitoring • E DHCP • Client List Server Status • Image: Comparison of the Monitoring •	SYL CNGCMMM MAC Address: 5518,5554 Sincer 5518,5554 Sincer 5518,5554 Sincer 5518,5554 Sincer 5518,5554 Sincer 5518 Sincer 518,552 Sincer 518,55 Si	91.5%	51.3 K	

Enter a search condition in the search box. A list of records meeting the search condition are rapidly displayed. Click a function to redirect to the function page.

1.3.6.3 More Functions of the System

• Displaying the current account

Ruíjie sw	표 @ Monitoring @ Config & Diagnosis 🗙 Mainter	nance	Enter a search term Q 至 Config Wizard Ø A	admin
🕞 Favorites 🕚	Duille		The current account is adm	iin. esh
SWITCH Overview	Model: \$5300-48GT4XS-E	7.7% CPU Usage	e 46.7% Memory Usage	
Anti-loop + Monitoring	SN: G1QC2N9000484 MAC Address: 5416.5158.6554			
IE DHCP >	Firmware Version: \$5300E_RGOS 12.5(4)80701			
Other Monitoring +	Hardware Version: 1.21 Booted or: 2022-07-28 15:00-51		53.3% 46.7%	
	Uptime: 0 d 23 h 01 min 46 s	92.3%		
	System Time: 2022-07-29 14:02:37			
	Selected 🚺 AG Port 💼 Up 💼 Shutdown 🕩 VSL Port		Copper [] F	Fiber
		30 32 34 36 38 40 42 44 46 48 50 52		
	nunde Artini Antini			_

Online Service

Ruijie sw	표 @Monitoring @Config 및 Diagnosis X Maintenance		Enter a search term	🛛 A admin 🝷
C2 Favorites		1	On	line Service
	S53E		Sim	plified Chinese
SWITCH Overview	Model: 55300-48GT4XS-E	8.7%	48.9% Log	pout
Anti-loop Monitoring DHCP Other Monitoring	O1: G16221000044 MAIC Advances 544835184854 Finances Vesion: 54028 G00513 554880701 Finances Vesion: 54028 G00513 554880701 Finances 74282 757 52387 Gystem: 5ee 2022 677-12 3437 Spratem: Trave: 2022 677-12 343744	51N	12.15 Arms	

To seek help, click Online Service.

Ruijie sw	표 (아Monitoring) ⓒ Config 한 Diagnosis 및 Maintenance		Enter a search term 🔾 🛎 Coefig Wiczwel 🕳	A admin 🔹
Client List	353E Model 55305-4627405-E	8.6% Ølilære	e 49.0s	Refresh
SWITCH Overview Anti-loop Monitoring	SN: 61Q239600494 MACAdonu: S115358.654 Firmson Vanice: 55300E,802512.5(480701			
DHCP - Client List Server Status	Headwaw Wenkini, 1.21 Biostani oru, 2022-07.07 12:287 Uptimu: 5 dol h. 35 min 15 a Syntam Timu: 2022-07-12 14:28:20	\$1.4%	51.0% etca.	
③ Other Monitoring →				

Click the RITA icon on the page to redirect to the online customer consulting page or move the cursor over the icon and scan the QR code for access.

• Language switching

Ruíjie sw	표 ତ Monitoring		Enter a search term 🔘 🕿 Config Wizard	
😭 Favorites 🛛 🔒				Online Service
	S53E		1	Simplified Chinese
Client List	Model: \$5300-48GT4XS-E	6 8.5%	(a) 49.0%	Logout
SWITCH Overview		CPU Usage	Memory Usage	
Anti-loop , Monitoring	Sk & 01CC/H900044 MAC Addws: \$416.5158.6554 Fremsanv Venior: \$5308_R50C5 12.5(480701			
H DHCP .	Hardware Version: 1.21			
Client List Server Status	Bosted ov. 2022-07-07 12-28:7 Uptime: 54 01 h 59 min 34 s System Time: 2022-07-12 14:27:39	91.5%	510%	
③ Other Monitoring →				

Click **Simplified Chinese** to switch to the Chinese version.

The language switching item is displayed based on actual requirements. It is displayed only when both Chinese and English are supported.

Logging out of the system

Ruijie sw	표 @Monitoring @Config 및 Diagnosis 및 Maintenance		Enter a search term 🔾 🛣 Config Wicard 🕷	🗸 A admin 🔸
😭 Favorites 🛛 🌒	C (2)E		Ori Sim	line Service nplified Chinese
Client List	Model: 55300-48GT4KS-E	8.4%	(=) 49.0% Log	gout
SWITCH Overview Monitoring Monitoring DHCP Client List	O1: C102/060044 MAC Address: S416/S138855 Firmers: Interior: S5058/RGC61/S14480701 Headman Views: 120 Totalar 2002/0712387 Totalar 2002/0712387		510% 4 0%	
Server Status	System Time: 2022-07-12 14/29/42	91.6%		
③ Other Monitoring •				

Click Logout to log out of the system.

1.3.6.4 Help Information

When you are unfamiliar with system functions and need help information, click the cookbook to query required information.

Ruijie sw	표 ③ Monitoring		Enter a search term 🕜 🖹 Cotifig Wizzerd 🗖 R. admin •
😭 Favorites 🛛 🌖	C 575		O Refresh
SWITCH Overview	Model: 55300-48GT4XS-E	8.9% (PUUsan)	48.8% Manage Usage
 Anti-loop , Monitoring , DHCP , ☑ Other Monitoring , 	19. GIG20000944 106.758.0594 Termanar Yunion 1900.6093 130480701 Hendmark Winion 1.21 Enstration 2002.0707 12827 Ljoinnes 5-423.104-ten 19-5 Synteen Tenae 2002.071.12143.200	T.M.	31.2%

Click to view the cookbook.

1.4 Enabling the Web Server

The Web service is enabled when the switch is delivered. The default IP address is 192.168.1.200. The following describes how to enable the Web service on the CLI.

Configuration	Description and Command		
	enable service web-server	Enables the Web service.	
Configuring the Web Server	ip address	(Optional) Configures an IP address.	
Configuring the web Server		(Optional) Configures the username and	
	webmaster level username password	password for logging in to the Eweb.	

Configuration Steps

- **L** Enabling the Web Service
- Mandatory.
- Complete the configuration on the switch.
- **\U** Configuring an IP Address
- Optional.
- **U** Configuring the Username and Password for Logging In to the Eweb
- Optional.
- When the Web service is enabled, the administrator account/password (**admin/admin**) are created by default. The account and password can be changed. Users can also create other Eweb accounts.

Verification

Log in to the Eweb by using the configured IP address, Eweb account, and password to check whether the login is successful.

Related Commands

L Enabling the Web Service

Command	enable service web-server [http https all]
Parameter	http https all: Enables a service. Http enables the HTTP service, https enables the HTTPS service,
Description	and all enables both HTTP and HTTPS services. Both HTTP and HTTPS services are enabled by default.
Command	Global configuration mode
Mode	

**** Configuring an IP Address

Command	ip address ip-address ip-mask
Parameter	<i>ip-address</i> : IP address.
Description	<i>ip-mask:</i> Network mask.
Command	Interface configuration mode
Mode	

D Configuring the Username and Password for Logging In to the Eweb

Command	webmaster level privilege-level username name password { password [0 7] encrypted-passw
Parameter	privilege-level: User binding permission level, which includes level 0, level 1, and level 2. The default super
Description	administrator account (admin) has level 0 permissions and other accounts created manually have level 1
	permissions.
	name: Username.
	password: Password text.
	0 7: Indicates the password encryption type. 0 indicates no encryption, and 7 indicates simple encryption.
	The default value is 0 .
	encrypted-password: Encrypted password text.
Command	Global configuration mode
Mode	
Usage Guide	N/A

Configuration Example

**** Configuring the Web Server

Configuratio	 Enable the Web service. Configure a management IP address for the device. The default management VLAN is VLAN 1.
n Steps	Configure an IP address for VLAN 1 and ensure that users can ping the management IP address successfully from their PCs.
	Hostname> enable Hostname# configure terminal Hostname(config)#enable service web-server

	Hostname(config)# webmaster level 0 username test password test
	Hostname(config)#interface vlan 1
	Hostname(config-if-VLAN 1)#ip address 192.168.1.200 255.255.255.0
	Hostname(config) # end
Verification	Run the show running-config command to display related commands.
	Hostname(config)#show running-config
	Building configuration
	Current configuration : 6312 bytes
	1
	hostname ruijie
	1
	!
	webmaster level 0 username test password test //Username and password for Eweb
	authentication. The displayed password is encrypted.
	http update mode auto-detect
	1
	1
	interface VLAN 1
	ip address 192.168.1.200 255.255.255.0 //Management IP address of
	the device
	no shutdown
	!
	line con O
	line vty 0 4
	login
	1
	!
	End