

24 Port 10/100/1000 + 4 SFP + UPLINK Switch, 19", L2 + Features



Web Management User Manual

DN-80233

Directory

Get	tting Start	1
We	2b-based Switch Configuration	3
Cor	nsole Port Interface	4
1.	Switch basic configuration	5
	1.1. Switch basic configuration	5
	1.1.1. Login user configuration	5
	1.1.2. Login user authentication method configuration	5
	1.1.3. Login user Security IP management	6
	1.1.4. Basic configuration	6
	1.1.5. Save current running-configuration	7
	1.2. SNMP authentication	8
	1.2.1. SNMP authentication	8
	1.2.1.1. User	8
	1.2.1.2. Groups	9
	1.2.1.3. Views	9
	1.2.1.4. SNMP engineid configuration	10
	1.2.2. SNMP management	10
	1.2.3. Community managers	10
	1.2.4. Configure snmp manager security IP	11
	1.2.5. SNMP statistics	11
	1.3. SSH management	12
	1.3.1. Switch on-off SSH	12
	1.3.2. SSH management	12
	1.4. Firmware update	13
	1.4.1. TFTP service	13
	1.4.1.1. TFTP client service	13
	1.4.1.2. TFTP server service	13
	1.4.2. FTP service	14
	1.4.2.1. FTP client service	14
	1.4.2.2. FTP server service	14
	1.5. Telnet server configuration	15
	1.5.1. Telnet server state	15
	1.5.2. Max numbers of telnet access connection	15
	1.6. Maintenance and debugging command	16
	1.6.1. Debug command	16
	1.6.2. Show clock	16
	1.6.3. Show CPU usage	16
	1.6.4. Show memory usage	17
	1.6.5. Show flash	17
	1.6.6. Show running-config	17
	1.6.7. Show switchport interface	
	1.6.8. Show tcp	
	1.6.9. Show udp	
	1.6.10. Show telnet login	18

	1.6.11. Show version	19
2.	Module management	19
	2.1. Show boot-files	19
	2.2. Set Boot IMG and Startup-Config	19
3.	Port configuration	20
	3.1. Ethernet port configuration	20
	3.1.1. Port layer 1 attribution configuration	20
	3.1.2. Bandwidth control configuration	22
	3.1.3. Switchport description	23
	3.1.4. Port combo forced mode config	23
	3.1.5. Port scan mode	24
	3.2. VLAN interface configuration	24
	3.2.1. Add interface VLAN	24
	3.2.2. Interface IP address mode configuration	25
	3.3. SPAN configuration	25
	3.4. Loopback-detection configuration	27
	3.4.1. Port Loopback-detection mode configuration	27
	3.4.2. VLAN Loopback-detection configuration	28
	3.4.3. Loopback-detection interval-time configuration	29
	3.4.4. Loopback-detection control recovery configuration	29
	3.5. Isolate-port configuration	29
	3.5.1. Isolate-port group configuration	29
	3.5.2. Interface join group config	30
	3.5.3. Show Isolate-port group	30
	3.6. Port storm-control config	30
	3.6.1. Port storm-control config	30
	3.6.2. storm-control bypass configuration	31
	3.7. Port rate-violation config	32
	3.7.1. rate-violation configuration	32
	3.8. Port virtual-cable-test config	32
	3.8.1. virtual-cable-test configuration	32
	3.9. Port debug and maintenance	33
	3.9.1. Show port information	33
	3.9.2. Show entire traffic information	33
	3.9.3. Show rate violation port	33
	3.10. uldp configuration	34
	3.10.1. uldp enable config	34
	3.10.2. uldp Hello message config	35
	3.10.3. uldp recovery time config	35
	3.10.4. Show uldp configuration	35
	3.11. LLDP configuration	36
	3.11.1. LLDP configuration	36
	3.11.2. LLDP port status config	36
	3.11.3. LLDP tx-interval config	37
	3.11.4. LLDP msgTxHold config	37
	3.11.5. LLDP transmit delay config	38
	· •	

	3.11.6. LLDP notification interval config	
	3.11.7. LLDP neighbors max-num config	
	3.11.8. LLDP too mangy neighbors config	
	3.11.9. LLDP transmit optional tlv config	
	3.11.10. Show LLDP configuration	
	3.12. LED shutoff configuration	41
	3.12.1. Time Range configuration	41
	3.12.2. LED shutoff config	41
	3.13. Jumbo packet forwarding configuration	42
4.	MAC address table configuration	42
	4.1. MAC address table configuration	42
	4.1.1. MAC address aging-time configuration	42
	4.1.2. Configurate MAC address	43
	4.1.3. Delete MAC address	44
	4.1.4. MAC address query	44
5.	VLAN configuration	45
	5.1. VLAN configuration	45
	5.1.1. Create/Remove VLAN	45
	5.1.2. Assign ports for VLAN	46
	5.1.3. Port type configuration	47
	5.1.4. Hybrid port configuration	47
	5.1.5. Trunk port configuration	48
	5.1.6. Private-vlan configuration	49
	5.2. GVRP configuration	49
	5.2.1. Enable global GVRP	49
	5.2.2. Enable GVRP on port	50
	5.2.3. GARP configuration	50
	5.3. VLAN-translation configuration	51
	5.3.1. Enable/Disable VLAN-translation	51
	5.3.2. Add/Delete VLAN-translation	51
	5.3.3. VLAN-translation miss drop configuration	52
	5.3.4. Show VLAN-translation	52
	5.4. Dynamic VLAN configuration	53
	5.4.1. VLAN protocol configuration	53
	5.5. Dot1q tunnel configuration	53
	5.5.1. Enable dot1q tunnel	53
	5.5.2. dot1q tunnel tpid configuration	54
6.	IGMP Snooping configuration	54
	6.1. Switch on-off IGMP Snooping	54
	6.2. IGMP Snooping port enable	55
	6.3. IGMP Snooping configuration	55
	6.4. IGMP Snooping mrouter port configuration	56
	6.5. IGMP Snooping query configuration	56
7.	MLD Snooping configuration	57
	7.1. Switch on-off MLD Snooping	57
	7.2. MLD Snooping port enable	57

	7.3. MLD Snooping configuration	58
	7.4. MLD Snooping mrouter port configuration	58
	7.5. MLD Snooping query configuration	59
8.	Time Range configuration	59
	8.1. Time Range configuration	59
9.	ACL configuration	60
	9.1. Numeric ACL	60
	9.1.1. Standard numeric ACL	60
	9.1.1.1. IP standard ACL	60
	9.1.1.2. MAC standard ACL	61
	9.1.2. Extended numeric ACL	62
	9.1.2.1. IP extended ACL	62
	9.1.2.2. MAC-IP extended ACL	63
	9.1.3. Delete Numeric ACL	64
	9.2. Name ACL	65
	9.2.1. Standard name ACL	65
	9.2.1.1. IP standard ACL	65
	9.2.2. Extended name ACL	66
	9.2.2.1. IP extended ACL	66
	9.2.2.2. MAC extended ACL	67
	9.2.2.3. MAC-IP extended ACL	68
	9.2.3. Delete Name ACL	69
	9.3. Filter configuration	69
	9.3.1. Firewall configuration	69
	9.4. Show ACL configuration	70
	9.4.1. Show access list	70
	9.4.2. Show firewall	70
	9.4.3. Show time range	70
	9.5. ACL binding configuration	70
	9.5.1. Attach ACL to port	70
	9.5.2. Show access group	71
	9 5 3 Clear Pack Statistic	71
	9.5.4 Attach ACL to vlan	71
	9.5.5. Show yacl configuration	72
	9.5.6. Clear vlan acl statistic	72
10	IPv6 ACL configuration	, 2
10.	10.1 JPv6 standard access-list configuration	72
	10.2 IPv6 name access-list configuration	, 2
	10.3 Show IPv6 access list	, 5
	10.3. Attach IPv6 ACL to nort	75
	10.5 Attach IPv6 ACL to vlan	, 5
11	AM configuration	, 4 7/
±1.	11 1 AM global configuration	,4 7/
	11.1. The block configuration	,4 7/
	11.2 AM nort configuration	,4 71
	11.2. An port comparation	74 71
	בדיכידי בוומטוכן הואמטור אוויו אטו נ	/+

	11.2.2. AM IP-Pool configuration	75
	11.2.3. AM MAC-IP-Pool configuration	75
	11.3. Show AM port configuration	75
	11.3.1. Show AM port configuration	75
	11.3.2. Clear port AM Pool	76
12.	Port channel configuration	76
	12.1. LACP port group configuration	76
	12.2. Delete port group	77
	12.3. Show port group info	77
	12.4. Show interface port-channel	78
	12.5. Add member port	78
	12.6. Del member port	79
	12.7. Set lacp port priority	79
	12.8. Set lacp system priority	79
13.	DHCP configuration	80
	13.1. DHCP management	80
	13.1.1. Enable DHCP	80
	13.2. DHCP server configuration	80
	13.2.1. Dynamic pool configuration	80
	13.2.1.1. Dynamic address pool configuration	80
	13.2.1.2. Client's default gateway configuration	81
	13.2.1.3. Client DNS server configuration	82
	13.2.1.4. Client WINS server configuration	83
	13.2.1.5. DHCP file server address configuration	84
	13.2.1.6. DHCP network parameter configuration	85
	13.2.1.7. Excluded address configuration	86
	13.2.2. Manual DHCP IP pool configuration	86
	13.2.2.1. Static address pool configuration	86
	13.2.3. Address pool name configuration	87
	13.2.4. DHCP packet statistics	
	13.3. DHCP relay configuration	
	13.3.1. DHCP relay configuration	
	13.4. DHCP debugging	
	13.4.1. Delete record	
	13 4 1 1 Delete hinding log	89
	13.4.1.2. Delete conflict log	
	13.4.1.3. Delete DHCP server statistics log	
	13.4.2. Show IP-MAC binding	90
	13.4.3. Show conflict-logging	90
14.	DHCP Snooping configuration	91
	14.1. DHCP Snooping global configuration	
	14.1.1. Enable/Disable DHCP Snooping	
	14.1.2. DHCP Snooping binding configuration	
	14.1.3. DHCP Snooping binding user configuration	۹2 م
	14.1.4 DHCP Snooning action count config	 ۵۷
	14.1.5. DHCP Snooping limit-rata config	_ر مع

	14.1.6. DHCP Snooping helper-server config	93
	14.2. DHCP Snooping port configuration	94
	14.2.1. Enable/Disable DHCP Snooping binding dot1x	94
	14.2.2. Enable/Disable DHCP Snooping binding user	94
	14.2.3. Enable/Disable DHCP Snooping trust	95
	14.2.4. DHCP Snooping action config	96
	14.3. Show DHCP snooping configuration	96
	14.3.1. Show DHCP snooping configuration	96
15.	SNTP configuration	97
	15.1. SNTP server configuration	97
	15.2. Request interval configuration	
	15.3. Time difference configuration	
	15.4. Show sntp	
16.	NTP configuration	
	16.1. NTP global configuration	
	16.1.1. NTP global switch configuration	
	16.1.2. NTP server configuration	
	16.1.3. NTP broadcast or multicast address count configuration	99
	16.1.4. NTP access group configuration	
	16.1.5. NTP authenticate configuration	
	16.2. NTP interface configuration	
	16.2.1. NTP interface switch configuration	
	16.3. NTP configuration display	
	16.3.1. NTP status display	
17.	QOS configuration	
	17.1. QOS port configuration	
	17.1.1. QOS port trust state configuration	
	17.1.2. QOS port COS parameters configuration	
	17.1.3. OOS port select queue schedule algorithm configuration	
	17.1.4. OOS port wrr algorithm queue weight configuration	
	17.1.5. OOS port wdrr algorithm queue weight configuration	
	17.1.6. OOS service policy configuration	
	17.2. OOS class-map configuration	
	17.2.1. Class map-configuration	
	17.2.2. Classification criteria configuration	
	17.3. QoS policy configuration	
	17.3.1. OoS policy configuration	
	17.4. OOS policy-map configuration	
	17.4.1 nolicy-map configuration	110
	17.4.2 Class-man use to policy-man config	110
	17.5. OoS policy-class-map configuration	111
	17.5.1. Policy-class-map accounting configuration	
	17.5.2. Aggregate policy configuration	
	17.5.3. Policy-class-map policy configuration	
	17.5.4 Policy-class-map policy configuration	117
	17.6 OoS manning configuration	112 112

	17.6.1. COS-to-IntP mapping	113
	17.6.2. COS-to-DP mapping	114
	17.6.3. DSCP-to-DSCP mapping	115
	17.6.4. DSCP-to-IntP mapping	116
	17.6.5. DSCP-to-DP mapping	117
	17.6.6. EXP-to-IntP mapping	117
	17.6.7. EXP-to-DP mapping	118
	17.6.8. IntP-to-DSCP mapping	118
	17.6.9. IntP-to-EXP mapping	118
	17.7. QoS aggregate policy configuration	119
	17.8. QoS service policy configuration	119
18.	L3 forward configuration	120
	18.1. IP route Aggregation configuration	120
	18.1.1. Route aggregate configuration	120
	18.2. ARP configuration	120
	18.2.1. ARP configuration	120
	18.2.2. Clear ARP cache	121
	18.2.3. Show ARP	121
	18.3. Gratuitous Arp config	121
	18.3.1. gratuitous-arp interval time configuration	121
	18.3.2. Interface gratuitous-arp interval time configuration	121
	18.3.3. Show gratuitous-arp configuration	122
	18.4. ARP protection configration	122
	18.4.1. ARP GUARD configration	122
	18.4.1.1. ARP GUARD configration	122
	18.4.2. ANTI-ARPSCAN configration	123
	18.4.2.1. ANTI-ARPSCAN on-off configration	123
	18.4.2.2. ANTI-ARPSCAN port-based threshold configration	123
	18.4.2.3. ANTI-ARPSCAN IP-based threshold configration	124
	18.4.2.4. ANTI-ARPSCAN trust port configuration	124
	18.4.2.5. ANTI-ARPSCAN trust IP configuration	125
	18.4.2.6. ANTI-ARPSCAN recovery on-off configuration	125
	18.4.2.7. ANTI-ARPSCAN recovery time configration	125
	18.4.2.8. Show ANTI-ARPSCAN information	126
	18.5. Show IP Traffic	126
19.	Route configuration	127
	19.1. Policy based routing	127
	19.2. Static route configuration	127
	19.2.1. Static route configuration	127
20.	IPv6 Route configuration	128
	20.1. IPv6 configuration	128
	20.1.1. IPv6 basic configuration	128
	20.1.2. IPv6 ND configuration	129
	20.1.3. Show IPv6 neighbor	131
	20.2. Show IPv6 route	132
	20.2.1. Show IPv6 route database	132

	20.2.2. Show IPv6 NSM route	
	20.2.3. Show IPv6 FIB	
	20.2.4. Show IPv6 route statistics	
21.	DCSCM configuration	
	21.1. DCSCM Source-control enable/disable configuration	
	21.2. DCSCM destination-control enable/disable configuration	
	21.3. DCSCM Source-control access-group configuration	
	21.4. DCSCM destination-control access-group configuration	
	21.5. DCSCM destination-control access-group configuration (sip)	
	21.6. DCSCM destination-control access-group configuration (vMAC)	
	21.7. Multicast policy configuration	
	21.8. ACL multicast source control	
22.	Spanning-tree configuration	140
	22.1. Spanning-tree field configuration	140
	22.1.1. Instance configuration	140
	22.1.2. Field name configuration	141
	22.1.3. Revision-level configuration	141
	22.2. Spanning-tree Port configuration	
	22.2.1. PortFast configuration	
	22.2.2. Port priority configuration	
	22.2.3. Port cost configuration	143
	22.2.4. Spanning-tree port mode	143
	22.2.5. Link-type configuration	
	22.2.6. Spanning-tree agreement port configuration	
	22.3. Spanning-tree global configuration	145
	22.3.1. Spanning-tree global agreement port configuration	145
	22.3.2. Forward-time configuration	145
	22.3.3. Hello-time configuration	146
	22.3.4. Max age time configuration	146
	22.3.5. Max hop time configuration	147
	22.3.6. Spanning tree mode configuration	147
	22.3.7. Spanning tree cost-format configuration	148
	22.3.8. Priority configuration	148
	22.4. Show spanning-tree	148
	22.4.1. Instance information	148
	22.4.2. Revision-Level information	149
23.	MRPP configuration	149
	23.1. MRPP global configuration	149
	23.1.1. MRPP global switch configuration	149
	23.1.2. MRPP poll time configuration	150
	23.1.3. MRPP domain id configuration	150
	23.2. MRPP port configuration	151
	23.2.1. MRPP port property configuration	151
	23.3. MRPP domain configuration	151
	23.3.1. MRPP control vlan config	
	23.3.2. MRPP node mode config	

	23.3.3. MRPP hello timer config	153
	23.3.4. MRPP fail timer config	
	23.3.5. MRPP domain switch config	154
	23.4. MRPP configuration display	154
	23.4.1. MRPP display	154
	23.4.2. MRPP statistics display	
	23.4.3. Clear MRPP statistics	
24.	ULPP configuration	
	24.1. ULPP global configuration	
	24.1.1. ULPP group configuration	
	24.2. ULPP port configuration	
	24.2.1. ULPP port property configuration	156
	24.3. ULPP group configuration	
	24.3.1. ULPP group description configuration	156
	24.3.2. ULPP group property configuration	157
	24.4. ULPP configuration display	
	24.4.1. ULPP group configuration display	
	24.4.2. ULPP port statistics display	
	24.4.3. ULPP port property display	
	24.4.4. ULPP port statistics clear	
25.	ULSM configuration	159
	25.1. ULSM global configuration	159
	25.1.1. ULSM group configuration	159
	25.2. ULSM port configuration	159
	25.2.1. ULSM port property configuration	159
	25.3. ULSM configuration display	160
	25.3.1. ULSM display	
26.	Authentication configuration	
	26.1. RADIUS client configuration	
	26.1.1. RADIUS global configuration	161
	26.1.2. RADIUS authentication configuration	162
	26.1.3. RADIUS accounting configuration	162
	26.2. TACACS server configuration	163
	26.2.1. TACACS global configuration	163
	26.2.2. TACACS server host configuration	163
	26.3. 802.1x configuration	164
	26.3.1. 802.1x Global configuration	
	26.3.2. 802.1x port authentication configuration	
	26.3.3. 802.1x port MAC configuration	
	26.3.4. 802.1x port status list	
	26.4. MAB configuration	166
	26.4.1. MAB ENABLE configuration	166
	26.4.2. MAB Authentication configuration	
	26.4.3. MAB parameter configuration	
	26.4.4. MAB show	167
27.	DOS attack protection configration	

	27.1. Source IP equal destination IP DOS attack protection configration	168
	27.2. Source port equal destination port DOS attack protection configration	168
	27.3. TCP DOS attacks on invalid flags configration	168
	27.4. ICMP DOS attack protection configration	169
	27.5. ICMP packet-size configration	169
	27.6. First fragment IP packet DOS attack protection configration	169
28.	SSL config	170
	28.1. IP HTTP server configuration	170
	28.2. SSL global configuration	170
	28.3. SSL server monitor port configuration	170
	28.4. SSL secure-ciphersuite configuration	171
29.	sFlow configuration	171
	29.1. sFlow collector global address configuration	171
	29.2. sFlow collector port address configuration	172
	29.3. sFlow agent address configuration	172
	29.4. sFlow priority configuration	172
	29.5. sFlow header length configuration	173
	29.6. sFlow data length configuration	173
	29.7. sFlow rate configuration	173
	29.8. sFlow counter interval configuration	174
	29.9. sFlow analyzer configuration	174
30.	IPv6 security ra configuration	175
	30.1. IPv6 security ra global configuration	175
	30.2. IPv6 security ra port configuration	175
	30.3. Show IPv6 security ra	175
31.	Device log message	176
	31.1. Show device log message	176
	31.2. Clear logging in logbuff channel	176

Getting Start

This section provides an introduction to the web-based configuration utility, and covers the following topics:

- Powering on the device
- Connecting to the network
- Starting the web-based configuration utility

• Power

Connecting to Power



Power down and disconnect the power cord before servicing or wiring a switch.

Do not disconnect modules or cabling unless the power is first switched off. The device only supports the voltage outlined in the type plate. Do not use any other power components except those specifically designated for the switch.



Disconnect the power cord before installation or cable wiring.

The switch is powered by the AC 100-240 V 50/60Hz internal high-performance power supply. It is recommended to connect the switch with a single-phase three-wire power source with a neutral outlet, or a multifunctional computer professional source.

Connect the AC power connector on the back panel of the switch to the external power source with the included power cord, and check the power LED is on.



Rear View AC Power Socket

• Connecting to the Network

To connect the switch to the network:

- 1. Connect an Ethernet cable to the Ethernet port of a computer
- 2. Connect the other end of the Ethernet cable to one of the numbered Ethernet ports of the switch. The LED of the port lights if the device connected is active.
- 3. Repeat Step 1 and Step 2 for each device to connect to the switch.



We strongly recommend using CAT-5E or better cable to connect network devices. When connecting network devices, do not exceed the maximum cabling distance of 100 meters (328 feet). It can take up to one minute for attached devices or the LAN to be operational after it is connected. This is normal behavior.

Switch ports will automatically adjust to the characteristics (MDI/MDI-X, speed, duplex) of the device to which the switch is connected.

• Starting the Web-based Configuration Utility

This section describes how to navigate the web-based switch configuration utility. Be sure to disable any pop-up blocker.

Browser Restrictions

• If you are using older versions of Internet Explorer, you cannot directly use an IPv6 address to access the device. You can, however, use the DNS (Domain Name System) server to create a domain name that contains the IPv6 address, and then use that domain name in the address bar in place of the IPv6 address.

• If you have multiple IPv6 interfaces on your management station, use the IPv6 global address instead of the IPv6 link local address to access the device from your browser.

Launching the Configuration Utility

To open the web-based configuration utility:

1. Open a Web browser.

2. Enter the IP address of the device you are configuring in the address bar on the browser (factory default IP address is 192.168.2.1) and then press Enter.



When the device is using the factory default IP address, its power LED flashes continuously. When the device is using a DHCP assigned IP address or an administrator-configured static IP address, the power LED is lit a solid color. Your computer's IP address must be in the same subnet as the switch. For example, if the switch is using the factory default IP address, your computer's IP address can be in the following range: 192.168.2.x (whereas x is a number from 2 to 254).

After a successful connection, the login window displays.



Usemame	
Password	

Login Window

• Logging In

The default username is admin and the default password is admin. The first time that you log in with the default username and password, you are required to enter a new password.

To log in to the device configuration utility:

- 1. Enter the default user ID (admin) and the default password (admin).
- 2. If this is the first time that you logged on with the default user ID (admin) and the default password (admin) it is recommended that you change your password immediately.

When the login attempt is successful, the System Information window displays.



System Information

If you entered an incorrect username or password, an error message appears and the Login page remains displayed on the window. If you are having problems logging in, please see the Launching the Configuration Utility section in the Administration Guide for additional information.

• Logging Out

By default, the application logs out after ten minutes of inactivity.

To logout, click Logout in the top right corner of any page. The system logs out of the device. When a timeout occurs or you intentionally log out of the system, a message appears and the Login page appears, with a message indicating the logged-out state. After you log in, the application returns to the initial page.

Web-based Switch Configuration

The smart switch software provides rich Layer 2 functionality for switches in your networks. This chapter describes how to use the web-based management interface (Web UI) to configure the switch's features. For the purposes of this manual, the user interface is separated into four sections, as shown in the following figure:

	L D Down	
System IP address:192.168.2.1 Current sys	tem time: Sat Jan 2 00:02:38 2021 System description: Switch Exit Save & Exit	
Default	Cliant ID address 102 158 2 122	
Switch	WHEN IT WALLERS FOR TOUR TEST	
Switch basic configuration	System Version Information	
Module management	Device: Switch, sysLocation: Default.	
Port configuration	CPU MAC 00-13-e2-24-1c-3c	
MAC address table configuration	SoftWare Version V101591.8.3	
VLAN configuration	BootRom Version V1.00	
IGMP Snooping configuration	Serial No.:UN2021/022001	
MLD Snooping configuration	Last robort was cold reset	
Time Range configuration	Uptime is 0 weeks, 0 days, 23 hours, 57 minutes	
ACL configuration		
IPv6 ACL configuration		
AM configuration		
Port channel configuration		
DHCP configuration		
DHCP Snooping configuration		
SNTP configuration		
Implementation		
QoS configuration		
L3 forward configuration		
Route configuration		
IPv6 Route configuration		
DCSCM configuration		
Spanning-tree configuration		
MRPP configuration		
ULPP configuration		
ULSM configuration		
Authentication configuration		
DOS attack protection configration		
SSL config		
sFlow configuration		
IPv6 security ra configuration		
Device log message		

Console Port Interface

The smart switch has a monitor port (Console port). Rate 1200bps-115200bps, standard RJ45 plug. Use a dedicated monitoring cable to lead the port to the PC serial port connection, as follows:



The RJ45 connector used by the Console port is shown in the figure below, and the RJ45 plug corresponds to the RJ45 socket, from left to right numbered from 1 to 8.



This cable is used to connect the console port of the switch to the external monitoring terminal. One end of the RJ45 eight-pin plug, the other end is a 25-hole plug(DB25) and 9-hole plug(DB9), RJ45 head into the switch's console port socket, DB25 and DB9 can be used according to the requirements of the terminal serial port, the cable internal connection schematic as follows:

RJ45 <===> DB9	
RTS 1~~~8 CTS]
DTR 2~~~6 DSR]
TXD 3~~~2 RXD]
GND 4~~~5 GND]
GND 5~~~5 GND]
RXD 6~~~3 TXD]
DSR 7~~~4 DTR]
CTS 8~~~7 RTS]

1. Switch basic configuration

1.1. Switch basic configuration

1.1.1. Login user configuration

Login user management module, users in this module can add or delete user operations.

Login username and password configuration					
User					
Password	Encrypted 1				
Priority					
Operation	Remove 🗸				
			Apply		
Jser					
User name	e Password	State	Priority		
admin	admin	Plain text	15		

User	User name to operate ,1-32 characters		
Password	User password, choose the password encryption, otherwise no encryption of 1-32		
	characters		
Priority	Used to specify permission level, default level 15		
Operation	Add Create new users		
	Remove	Delete the specified user (password and priority cannot be entered)	

1.1.2. Login user authentication method configuration

Login user authentication method configuration module, the user can configure console.vty.web authentication method used in login, authentication method can be any one or combination of Local.RADIUS and TACACS.preferences from left to right when the login method is combined configuration. If the user has passed the authentication method, the authentication method of the lower preference is ignored. As long as you pass an authentication method, the user can log in.AAA functions and RADIUS servers should be configured before using RADIUS authentication. If local authentication is configured without configuring a local user, the user will be able to log on to the switch through the console method.

Login user authentication method configuration				
Login method	Console 🗸			
Authentication method1	None 🗸			
Authentication method2	None 🗸			
Authentication method3	None 🗸			
Apply	Default			

Login user authentication method						
Login method	Authentication method1	Authentication method2	Authentication method3			
console	None	None	None	None		
vty	local	None	None	None		
web	local	None	None	None		

Login mothod	Authentication	
Login method	method	
console	local	Authentication using the local user account database
vty	radius	Authentication using remote Radius server
web	tacacs	Authentication using remote Tacas server
Default Default console no authentication , vty and web local authentication		

1.1.3. Login user Security IP management

Login user security IP configuration module, where users can configure the security IP.IPv6 address for login switch, or configure access control list.

Login user Security IP Set						
Security IP address						
Operation	Add	~				
					Арр	ly
Login Access control list Set						
Ipv4 access control	list 🗸					
Operation	Add	~				

Login user Security IPv4 List		
end of security IPv4		
Login user Security IPv6 List		
end of security IPv6		
Login Ipv4 access control list		
end of ipv4 access list		
Login Ipv6 access control list		
end of ipv6 access list		

Security IP address	Fill in the specified security IP or IPv6 address (the access control list is valid until the IPv6 address is filled in)		
IPv4/IPv6access control list	Standard access control list number, scope 1-64		
Operation	Add	Add address or list number	
Operation	Remove	Delete address or list number	

1.1.4. Basic configuration

Basic configuration module, in which users can configure switch current time, exit privilege mode timeout and switch name respectively.

		Configure exec timeo	ut	
Basic clock confi	guration	Timeout(minute)		
HH:MM:SS		Timeout(second)		
YYYY.MM.DD		Operation	Configuration	~
Apply				Apply

Switch n	Switch name configuration				
Switch name					
Operation		Configuration \checkmark			
Apply					

HH:MM:SS	Current time, format hours: minutes: seconds				
YYYY.MM.DD	Current date, for	Current date, format year. Month. Day			
Timeout	Exit privilege mo	de timeout score 0-35791			
(minute)					
Timeout	seconds of exit p	rivilege mode timeout (not set separately),0-59 seconds			
(second)					
Operation	Configuration Configuration operations				
	Default Restore default (default timeout 10 minutes)				
Switch name	Fill in the new name of the switch to be changed, 1-64 characters				
Operation	Configuration Configuration operations				
	Default	Do recovery default (default name Switch)			

1.1.5. Save current running-configuration

Save the current configuration module, the user can save the current set configuration, can also leave the factory initial settings restart, but also choose whether to save the current set configuration before restart.

Save current running-configuration		
	Apply	
Reboot with the default configuration	on	
	Apply	
Save current configuration before r	eboot?	
	Apply	

1.2. SNMP authentication

1.2.1. SNMP authentication

1.2.1.1. User

SNMP user management module, users can add or delete SNMP user operations in this module.

Users	
SNMP username	
SNMP group	
Security level	noAuthNoPriv 🗸
Authentication protocol:	MD5 🗸
Authentication password:	
Privacy protocol:	DES 🗸
Privacy password:	
Ipv4 access control list	
Ipv6 access control list	
Operation	Add 🗸
	Apply

SNMP username	User name to operate ,1-32 characters		
SNMP group	User group to join ,1-32 characters		
Security level	noAuthNoPriv	Uncertified non-encrypted level	
	authNoPriv	Authentication but not encryption level	
	authpriv	Authentication and encryption level	
Authentication protocol:	MD5	HMAC MD5 algorithm for authentication	
	SHA	Authentication uses HMAC SHA algorithms	
Authentication password:	Password for authentication		
Privacy protocol:	DES Encryption DES algorithm		
	AES	Encryption AES algorithm	
	3DES Encryption with 3 DES algorithm		
Privacy password:	Password for encryption		
Ipv4 access	Standard IPv4 access control list number, range 1-64 characters		
control list			
lpv6 access	Standard IPv6 access control list number, range 1-64 characters		
control list			
Operation	Add Add SNMP users		
	Remove Delete SNMP users		

1.2.1.2. Groups

SNMP group management module in which users can add or delete SNMP group operations.

Groups	
SNMP group	
Security level	noAuthNoPriv 🗸
Read SNMP view	
Write SNMP view	
Notify SNMP view	
Operation	Add 🗸
	Apply

SNMP group	User group name to operate ,1-32 characters				
Security level	noAuthNoPriv Uncertified non-encrypted level				
	authNoPriv Authentication but not encryption level				
	authpriv Authentication and encryption level				
Read SNMP view	Name of readable view, including 1-32 characters				
Write SNMP view	Name of writable view, including 1-32 characters				
Notify SNMP view	Notice the name of the view, including 1-32 characters				
Operation	Add Add SNMP groups				
	Remove Delete SNMP groups				

1.2.1.3. Views

SNMP view management module in which users can add or delete SNMP view operations.

Views	
SNMP view	
OID	
Туре:	Include 🗸
Operation	Add 🗸
	Apply

SNMP view	OID	Туре
v1defaultviewname	1.0.	Include
v1defaultviewname	1.2.	Include
v1defaultviewname	1.3.	Include

SNMP view	User view name to operate, 1-32 characters			
OID	OID number to operate, decimal			
Туре:	Include Include this OID			
	Exclude	Exclude this OID		
Operation	Add	Add view		
	Remove	ve Delete View		

1.2.1.4. SNMP engineid configuration

SNMP Engineid configuration module, the user can configure SNMP Engineid operation in this module.

SNMP engineid configuration			
Engineid			
Operation	Configuration 🗸		
		Apply	
Engineid			
18c308c6b3c	91aab		

Engineid	Engine id,Hex ,1-32 characters		
Operation	configuration Configuration operations		
	Default	Restore default (default is company ID plus local MAC address)	

1.2.2. SNMP management

SNMP network management function switch module, users can enable or disable SNMP functions.

SNMP management	
SNMP Agent state	Open 🗸
RMON state	Open 🗸
Trap state	Open 🗸
Security IP state	Open 🗸
	Apply

1.2.3. Community managers

The group string management module where users can SNMP group string management and configure TRAP management settings.

			TRAP manager configuration	
			Trap receiver	
Community manage	ers		Community string	
Community string			Version	1 🗸
Access priority	Read only	>	Security level	noAuthNoPriv 🗸
Operation	Add 🗸		Operation	Add 🗸
		Apply		Apply

Community string	Community string name ,1-255 characters			
Access priority	Read only	Read-only permission level		
Access priority	Read and write	Read and write permission level		
Onoration	Add	Do Community string add operations		
Operation	Remove	Do Community string delete operations		
Trap receiver	Recipient IPv4/IPv6 address of Trap information			
Community string	Community string name, V1/V2 version :1-255 characters, V3 version :1-24			
Community string	characters			
Version	Three versions:V1/V2C/V3			

Security level	noAuthNoPriv	Uncertified non-encrypted level
(V3 version	authNoPriv	Authentication but not encryption level
support only)	authpriv	Authentication and encryption level
Oneration	Add	For Trap information receiver add operation
	Remove	For Trap information receiver remove operation

1.2.4. Configure snmp manager security IP

The administrator IP the address setting module, where the user can add or delete the SNMP manager's safe IP address.

Configure snmp manager security IP				
Security IP address				
Operation	Add	~		
			Apply	
Security IP address				

Security IP	SNMP Management Security IPv4/IPv6 Address		
address			
Operation	Add	Add a Security IP	
Operation	Remove	Remove a Security IP	

1.2.5. SNMP statistics

SNMP statistical information module, users in this module can view the SNMP function feedback information.

Information feedback window
SW1# show snmp
0 SNMP packets input
0 Bad SNMP version errors
0 Unknown community name
0 Illegal operation for community name supplied
0 Encoding errors
0 Number of requested variables
0 Number of altered variables
0 Get-request PDUs
0 Get-next PDUs
0 Set-request PDUs
0 SNMP packets output
0 Too big errors (Max packet size 1500)
0 No such name errors
0 Bad values errors
0 General errors
0 Get-response PDUs
0 SNMP trap PDUs

1.3. SSH management

1.3.1. Switch on-off SSH

SSH function switch module in which the user can enable or disable switches by SSH.

Switch on-off SSH			
Switch on-off SSH	Open	<	
		Apply	

1.3.2. SSH management

SSH management configuration module, the user can configure the SSH timeout, SSH authentication times and SSH RSA secret key modulus, and can also view the user login status of the SSH server.

SSH timeout management			SSH reauthentication management		
SSH timeout			SSH reauthentio	ation	
Operation	Configuration 🗸		Operation		Configuration 🗸
	Apply				Apply
Create SSH RSA	. key]	SSH timeout	SSH	reauthentication
SSH RSA key	1024		600	3	
	Apply				

Show SSH Server's State			
Num	Version	Status	SSH usename

SSH timeout	timeout of exit SSH login status ,10-600 seconds		
Operation	Configuration configuration operations		
	Default	recovery default (default 180 s)	
SSH reauthentication	SSH number of re-authentications when logged in,1-10		
Operation	Configuration configuration operations		
	Default Restore default (default re-authentication 3 times)		
SSH RSA key	A module for calculating Rsa keys, ranging from 768-2048, default 1024		

1.4. Firmware update

1.4.1. TFTP service

1.4.1.1. TFTP client service

TFTP client service module, the user can upload or download files by TFTP way, and can upgrade the firmware of the switch by this method.

	FTP client service	
e e	Gerver IP address	
	.ocal file name	
5	Server file name	
	Dperation type	Upload 🗸
E	ransmission type ि	binary 🗸
		Apply
Server IP address	TFTP address IP p	peer server, point decimal
Local file name	Name of destinat	tion file to upload or download ,1-100 characters
Server file name	Source name to upload or download, 1-100 characters	
Operation type	Upload	To upload files
	Download	To download files
Transmission type	binary	Transfer files in binary format (default)
	ascii	Transfer files in ascii format

1.4.1.2. TFTP server service

TFTP server-side service module, users can configure the TFTP server settings in this module.

TFTP server service			
Server state	Close 🗸		
TFTP Timeout	600		
TFTP Retransmit times	5		
Operation	Configuration 🗸		
	Apply		

Server state	Open	Enable TFTP server functionality	
	Close	Disable TFTP server functionality (default)	
TFTP Timeout	TFTP service exit timeout, range 5-3600 s (default 600 s)		
TFTP Retransmit times	TFTP number of retransmissions after transmission failure, range 1-		
	20(default 5)		
Operation	Configuration Configuration operations		
	Default	Restore default	

1.4.2. FTP service

1.4.2.1. FTP client service

FTP client service module, the user can upload or download files by FTP way, and can upgrade the firmware of the switch by this method.

FTP client service		
Server IP address		
User		
Password		
Local file name		
Server file name		
Operation type	Upload 🗸	
Transmission type	binary 🗸	
		Apply

Server IP address	FTP address IP peer server, point decimal			
User	FTP server-to	-server username ,1-100 characters		
Password	FTP server-sid	de user password 1-100 characters		
Local file name	Name of dest	ination file to upload or download ,1-100 characters		
Server file name	Source name	to upload or download ,1-100 characters		
Operation type	Upload To upload files			
	Download To download files			
Transmission type	binary Transfer files in binary format (default)			
	ascii	Transfer files in ascii format		

1.4.2.2. FTP server service

FTP server service module, the user can configure various settings of FTP server.

FTP server service					
FTP server State	Close	~			
FTP Timeout	600				
Operation	Config	gura	atio	n 🗸	
				Ap	ply
FTP user name and password setting					
FTP user name and p	asswor	٢d s	setti	ing	
FTP user name and p User	asswor	d s	setti	ing	
FTP user name and p User Password	asswor	d s	setti	ing	
FTP user name and p User Password State	asswor Plain	tex	etti	ing V	
FTP user name and p User Password State Operation type	asswor Plain · Add	tex	etti :t	ing V	

FTP server State	Open Enable FTP server functionality				
	Close	Disable FTP server functionality (default)			
FTP Timeout	FTP service exit timeout, range 5-3600s (default 600 s)				
Operation	Configuration Configuration operations				
	Default	Restore default			

User	FTP service username to operate ,1-32 characters					
Password	FTP service user pass	FTP service user password to operate ,1-16 characters				
State	Plain text	Plain text Do not encrypt FTP service password				
	Encrypted	Encrypted Encryption of FTP service passwords				
Operation type	Add	Add Add operations				
	Remove	Delete operations				

1.5. Telnet server configuration

1.5.1. Telnet server state

Telnet server status module, where users can enable or disable login switches by Telnet.

Telnet server state			
Telnet server state	0pen	~	
		Ap	ply

1.5.2. Max numbers of telnet access connection

Telnet connect the maximum number module, the user can configure the maximum number of connections to the switch by Telnet.

Max numbers of telnet access connection				
Telnet access connection number				
Operation	Configuration 🗸			
	Apply			
Information feedback window				
Telnet access connection number 5				

Telnet access	Maximum number of connections logged in by Telnet, range 1-16(default 5)			
connection number				
Operation	Configuration Operations			
	Default	Restore default		

1.6. Maintenance and debugging command

1.6.1. Debug command

Maintenance and debugging command module. The user can configure the mapping relationship between host and IP, also can run ping command and route tracking command.

Basic host con	guration	
Host name	PING	
IP address	Host na	ame
Operation	Add 🗸 IP add	ress
	Apply	Apply
	Traceroute	
	IP address	
	Host name	
	Hops	
	timeout	
		Apply

Host name	Host name for mapping ,1-64 characters		
IP address	IP address for mappi	ng, point decimal	
Operation	Add	Add operations	
	Remove	Delete operations	
Host name	To ping the host nam	e, configure the mapping relationship between the host and the IP	
IP address	IP address to ping, decimal		
IP address	IP address for routing tracing, point decimal		
Host name	Host name for routing tracing ,1-64 characters		
Hops	Number of hops, rou	te, range 1-255	
timeout	10, Tracking timeout	0-10000	

1.6.2. Show clock

This module is used to display the current system time and date.

Information feedback window		
SW1# show clock		
Current time: Wed Jan 01 01:03:21	2020	[UTC]

1.6.3. Show CPU usage

This module is used to display resource usage CPU current system.

Information feedback window						
SW1#	SW1# show cpu usage					
Last	5	second	CPU	IDLE:	83%	
Last	30	second	CPU	IDLE:	92%	
Last	5	minute	CPU	IDLE:	92%	
From	ru	unning	CPU	IDLE:	91%	

1.6.4. Show memory usage

This module is used to display the current system memory resource usage.

```
Information feedback window
SW1# show memory usage
The memory total 128 MB , free 68009984 bytes , usage is 49.33%
```

1.6.5. Show flash

This module is used to display the current system flash storage resource usage.

Information feedback window							
SW1# show f	SW1# show flash						
total 2278	9K						
-rw-	10817705	mantest.img					
-rw-	12514223	nos.img					
-rw-	1384	startup.cfg					
-rw-	1361	test1.cfg					
Drive : flash:							
Size:30.0M	Used:23.5M	Available:6.5M	Use:78%				

1.6.6. Show running-config

This module is used to display configuration information in the current system run.

```
Information feedback window

SW1# show run

!

no service password-encryption

!

hostname SW1

sysLocation Russia, Moscow, Ryabinovaya st, 26 bld 2

sysContact +7 (495)797-3311

!

username admin privilege 15 password 0 admin

!

!

ssh-server enable

ssh-server timeout 600

!

web language english

!

snmp-server enable

snmp-server enable

snmp-server enable traps

!
```

1.6.7. Show switchport interface

This module is used to display the port information of the current switch.

```
Information feedback window

SW1# show switchport interface

Ethernet1/0/1

Type :Universal

Mode :Trunk

Port VID :1

Trunk allowed Vlan: 1-4094

Ethernet1/0/2

Type :Universal

Mode :Trunk

Port VID :1

Trunk allowed Vlan: 1-4094
```

1.6.8. Show tcp

This module is used to display tcp connection information for the current switch.

Information feedback window							
SW1# show tcp							
LocalAddress	LocalPort	ForeignAddress	ForeignPort	State	IF	VRF	
192.168.2.1	80	192.168.2.200	54216	ESTABLISH	ED0	0	
127.0.0.1	2650	127.0.0.1	32785	ESTABLISH	ED0	0	
127.0.0.1	32785	127.0.0.1	2650	ESTABLISH	EDO	0	
0.0.0.0	80	0.0.0.0	0	LISTEN	0	0	
0.0.0.0	22	0.0.0.0	0	LISTEN	0	0	
0.0.0.0	23	0.0.0.0	0	LISTEN	0	0	
127.0.0.1	2650	0.0.0.0	0	LISTEN	0	0	

1.6.9. Show udp

This module is used to display udp connection information for the current switch.

Information feedback window					
SW1# show udp					
LocalAddress	LocalPort	ForeignAddress	ForeignPort	State	
0.0.0.0	161	0.0.0.0	0	CLOSE	
0.0.0.0	3071	0.0.0.0	0	CLOSE	

1.6.10. Show telnet login

This module is used to display the user information that is currently logged in to the switch by telnet.

Information feedback window
SW1# show telnet login
Authenticate login by local.
Login user:

1.6.11. Show version

This module is used to display the user information that is currently logged in to the switch by telnet.

System Version Information				
Device: Switch, sysLocation: Russia, Moscow, Ryabinovaya st, 26 bld 2.				
CPU MAC 08-c6-b3-c9-1a-ab				
VLAN MAC 08-c6-b3-c9-1a-ac				
SoftWare Version 8.101.30				
BootRom Version 2011.12.16				
HardWare Version 1.2				
CPLD Version N/A				
Serial No.:7135070820200001				
Last reboot was cold reset.				
Uptime is 0 weeks, 0 days, 1 hours, 9 minutes				

2. Module management

Client IP address: 192. 168. 2. 200

2.1. Show boot-files

This module is used to display system firmware and configuration files for the next restart of the switch.

Information feedback window					
Booted files on switch The primary img file at the next boot time: The backup img file at the next boot time: Current booted img file:	flash:/nos.img flash:/nos.img flash:/nos.img				
The startup-config file at the next boot time: Current booted startup-config file:	flash:/startup.cfg flash:/startup.cfg				

2.2. Set Boot IMG and Startup-Config

This module is used to configure the system firmware and configuration files for the next restart of the switch.

Set boot files in Active Master				
Primary IMG		Set		
Backup IMG		Set		
Startup-config		Set		

Primary IMG	System firmware first boot item when switch restarts
Backup IMG	System firmware second boot item when switch restarts
Startup-config	Start configuration file on switch restart

3. Port configuration

3.1. Ethernet port configuration

This chapter mainly configures the related port function of Ethernet port.

3.1.1. Port layer 1 attribution configuration

This page is mainly used to configure the basic properties of physical ports.

To display the "Port layer 1 attribution configuration" page, click Port configuration ->Ethernet port configuration->Port layer 1 attribution configuration, click "Apply" to configure.

Port configuration					
Port	Ethernet1/0/1 V				
mdi	auto 🗸				
Admin status	no shutdown 🗸				
Speed/Duplex status	Auto				
Module type	auto-detected V				
1000M Mode	```				
Fiber portMode	Auto				
Flow control status	Invalid flow control V				
Loopback	k no loopback V				
	Apply				

entry	describe			
Mdi	Invalid settings			
Admin status	Port status: Shutdown: enable			
	no shutdown: disable			
Speed/Duplex status	Port rate and Working mode			
Module type	Port types such as Ethernet port, Gigabit optical port, etc.			
1000M Mode	Mode configuration in Gigabit port configuration			
Fiber portMode	Invalid settings			
Flow control status	Port Flow Control			
Loopback	Port loop detection:			
	Loopback: enable			
	No Loopback: disable			
Port rate	Port rate:10: 10M			
	100: 100M, 1000: 1000M			
	Auto: Automatic negotiation rate			
Working mode	Working mode:			
	Auto: Automatic negotiation mode			
	Half: Half duplex mode			
	Full: Full duplex mode			

Port list								
Port	mdi	managementStatus	Speed	Mode	1000M Mode	Fiber portMode	Flow control	loopback
Ethernet1/0/1	auto	No Shutdown	10M	full	NULL	Auto	Non flow control status	no loopback
Ethernet1/0/2	auto	No Shutdown	auto	auto	NULL	Auto	Non flow control status	no loopback
Ethernet1/0/3	auto	No Shutdown	auto	auto	NULL	Auto	Non flow control status	no loopback
Ethernet1/0/4	auto	No Shutdown	auto	auto	NULL	Auto	Non flow control status	no loopback
Ethernet1/0/5	auto	No Shutdown	auto	auto	NULL	Auto	Non flow control status	no loopback
Ethernet1/0/6	auto	No Shutdown	auto	auto	NULL	Auto	Non flow control status	no loopback
Ethernet1/0/7	auto	No Shutdown	auto	auto	NULL	Auto	Non flow control status	no loopback
Ethernet1/0/8	auto	No Shutdown	auto	auto	NULL	Auto	Non flow control status	no loopback

entry	describe			
Mdi	Invalid settings			
managementStatus	Port enable status:			
	Shutdown: enable			
	no shutdown :disable			
Speed	Port rate:			
	10: 10M			
	100: 100M			
	1000: 1000M			
	Auto: Automatic negotiation rate			
Mode	Working mode:			
	Auto: Automatic negotiation mode			
	Half: Half duplex mode			
	Full: Full duplex mode			
1000M Mode	Mode configuration in Gigabit port configuration			
Fiber portMode	Invalid settings			
Flow control	Port Flow Control			
Loopback	Port loop detection:			
	Loopback: enable			
	No Loopback: disable			

3.1.2. Bandwidth control configuration

The page is configured for bandwidth control.

To display the "Bandwidth control configuration" page, click Port configuration ->Ethernet port configuration->Bandwidth control configuration, click "Apply" to configure.

Bandwidth control configuration					
Port	Bandwidth control level		Control type	Operation	
Ethernet1/0/1 V			Transmit 🗸	Configuration	~
					Apply

entry	describe	
Bandwidth control level	Bandwidth control rate in the range of Kbps 1-1000000	
Control type	Control type:	
	Transmit: send	
	receive : receive	
	Both: send and receive	
Operation	Configuration: User-defined configuration	
	Default: Restore default configuration	

Port list		
Port	Ingress bandwidth threshold(Kb)	Engress bandwidth threshold(Kb)
Ethernet1/0/1	1000000	1000000
Ethernet1/0/2	1000000	1000000
Ethernet1/0/3	1000000	1000000
Ethernet1/0/4	1000000	1000000
Ethernet1/0/5	1000000	1000000
Ethernet1/0/6	1000000	1000000
Ethernet1/0/7	1000000	1000000
Ethernet1/0/8	1000000	1000000

Port	Ethernet port name	
Ingress bandwidth threshold(Kb) Displays the current received data bandwidth limit		
	range of Kbps 1-1000000	
Engress bandwidth threshold(Kb)	Displays the bandwidth limit of the current sending data,	
	ranging from 1-1000000kbps	

3.1.3. Switchport description

This page can be used to set the port name.

To display the "Switchport description" page, click Port configuration ->Ethernet port configuration->Switchport description, click "Apply" to configure.

Switchport description		
Port	Ethernet1/0/1 V	
Description		
Operation	Configuration V	
	Apply	

Port	Ethernet port name
Description	Port description name, length 1-200 characters
Operation	Configuration: User-defined configuration
	Default: Restore default configuration

Port list			
Port	Description		
Ethernet1/0/1			
Ethernet1/0/2			
Ethernet1/0/3			
Ethernet1/0/4			
Ethernet1/0/5			
Ethernet1/0/6			
Ethernet1/0/7			
Ethernet1/0/8			

Port	Ethernet port name
Description	Port description name, length 1-200 characters

3.1.4. Port combo forced mode config

This page can be used to configure the combo port interface type to switch.

To display the "Port combo forced mode config" page, click Port configuration ->Ethernet port configuration->Port combo forced mode config, click "Apply" to configure.

Port combo forced mode config					
Port	Ethernet1/0/1	~			
forced mode	copper-forced			~	
					Apply

Port	Ethernet port name	
forced mode	Configure combo port current interface type:	
	Copper-forced: copper	
	Sfp-forced: fiber	
	sfp-preferred-auto: Automatic switching	

Information feedback window			
Port	forced mode		
Ethernet1/0/1	no support		
Ethernet1/0/2	no support		
Ethernet1/0/3	no support		
Ethernet1/0/4	no support		
Ethernet1/0/5	no support		
Ethernet1/0/6	no support		
Ethernet1/0/7	no support		
Ethernet1/0/8	no support		

Port	Ethernet port name
forced mode	Configure combo port current interface type:
	Copper-forced: copper
	Sfp-forced: fiber
	sfp-preferred-auto: Automatic switching

3.1.5. Port scan mode

This function switch is not supported for the time being.

3.2. VLAN interface configuration

This chapter mainly realizes the creation of VLAN interface and the configuration of interface address.

3.2.1. Add interface VLAN

This page is mainly used to create VLAN interfaces.

To display the "add interface VLAN" page, click Port configuration ->VLAN interface configuration->add interface VLAN, click "Apply" to configure.

Add interface VLAN			
VLAN ID	1 ~		
Operation	Add	~	
			Apply

entry	describe
VLAN ID	VLAN ID created
Operation	Action: Add/Remove

Vlan ID	State
Vlan1	Layer 3 interface
Vlan5	Non layer 3 interface

entry	describe
VLAN ID	VLAN ID added
State Is VLAN a layer 3 interface	

3.2.2. Interface IP address mode configuration

The page can be used to configure IP address and subnet mask for the VLAN interface. To display the "L3 interface IP address mode configuration" page, click Port configuration ->VLAN interface configuration->L3 interface IP address mode configuration, click "Apply" to configure.

L3 interface IP address mode configuration		
VLAN interface	Vlan1 🗸	
IP mode	Specify IP address ∽	
Interface IP address		
Interface network mask		
Operation	Add V	
	Apply	

entry	describe	
VLAN interface	VLAN ID of layer 3 interface created	
IP mode	Access to interface IP address:	
	bootp-client: bootp-clientAutomatic acquisition	
	dhcp-client: dhcp-client Automatic acquisition	
	Specify IP address: User self configuration	
Interface IP address	IP address, e.g. A.B.C D	
Interface network mask	Network mask: for example :255.255.255.0	
Operation	Action: Add/Remove	

3.3. SPAN configuration

This section can be used for port mirroring function configuration. To display the "SPAN configuration" page, click Port configuration ->VLAN interface configuration->SPAN configuration, click "Apply" to configure.

Destination port (SPAN) configuration			
Session	1 ~		
Destination port (SPAN)	1/0/1 🗸		
Operation	Add 🗸		
	Apply		

entry	describe
Session	Mirror Session
Destination port (SPAN)	Mirror destination port
Operation	Action: Add/Remove

	SPAN configuration		
Session Destination port (SPAN)			
	1	Ethernet1/0/1	

entry	describe	
Session	Mirror Session	
Destination port (SPAN)	Mirror destination port	
Source port (SPAN) configurati	on	
--------------------------------	---------	-----
Session	1 ~	
Source port (SPAN) list	1/0/1 🗸	
CPU to be used for source port		
Access list		
Mirror direction	both 🗸	
Operation	Add 🗸	
	Арр	oly

entry	describe			
Session	Mirror Session			
Source port (SPAN)	Mirror Source Port			
list				
CPU to be used for	CPU used as the source of data			
source port				
Access list	The access control list set for the mirror source port			
Mirror direction	What kind of data is needed to filter to the destination port:			
	Both: Sending and receiving			
	Rx: receive			
	Tx: send			
Operation	Add: Add configuration for the corresponding operation			
	Remove: Delete the corresponding configuration			

Rspan vlan configuration					
VLAN ID]	
Operation	Add	~			
					Apply

entry	describe		
VLAN ID	VLAN ID		
Operation	Add: Add configuration for the corresponding operation		
	Remove: Delete the corresponding configuration		

reflector port (SPAN) configuration			
Session	1 ~		
Port	Ethernet1/0/1 V		
Operation	Add 🗸		
	Apply		

entry	describe		
Session	Mirroring Session		
Port	Ethernet port number		
Operation	Add: Add configuration for the corresponding operation		
	Remove: Delete the corresponding configuration		

remote vlan configuration					
Session	1 ~				
VLAN ID					
Operation	Add	~			
					Apply

entry	describe	
Session	Mirroring Session	
VLAN ID	VLAN ID	
Operation	Add: Add configuration for the corresponding operation	
	Remove: Delete the corresponding configuration	

sample rate configuration				
Session	1 🗸			
rate				
		Apply		

entry	describe
Session	Mirroring Session
rate	It indicates how many packets are mirrored to the destination port

Source port (SPAN) list								
session 1 sea		session 2	session 2		session 3		session 4	
Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	

entry	describe		
Session	Mirroring Session		
Tx/Rx	Direction of source port mirror data		
Ethernet1/0/10	Mirror Source Port for Session		

3.4. Loopback-detection configuration

This chapter is mainly for port loop detection function configuration.

3.4.1. Port Loopback-detection mode configuration

The configuration of the page is used to set the loop detection control method.

To display the "Port Loopback-detection mode configuration" page, click Port configuration ->Port Loopback-detection configuration->Port Loopback-detection mode configuration, click "Apply" to configure.

Port Loopback-detection mode configuration		
Port	Ethernet1/0/1 V	
Loopback-detection mode	shutdown 🗸	
Operation	Add 🗸	
	Apply	

entry	describe		
Port	Ethernet port name		
Loopback-detection mode	Operation in case of loop:		
	Shutdown: Disable port		
	block : Block port		
Operation	Operation of loop detection function:		
	Add:		
	Open loop detection and configure control mode		
	Remove:		
	Disable loop detection		

Information feedback window		
Port	Loopback-detection mode	
Ethernet1/0/1	no control mode	
Ethernet1/0/2	no control mode	
Ethernet1/0/3	no control mode	
Ethernet1/0/4	no control mode	
Ethernet1/0/5	no control mode	
Ethernet1/0/6	no control mode	
Ethernet1/0/7	no control mode	
Ethernet1/0/8	no control mode	

entry	describe	
Port	Ethernet port name	
Loopback-detection mode	Shutdown: Disable port	
	block : Block port	
	no control mode :Disable port loop detection	

3.4.2. VLAN Loopback-detection configuration

This page can be used to configure VLAN loop detection function enabled or disabled. To display the "VLAN Loopback-detection configuration" page, click Port configuration ->Port Loopback-detection configuration->VLAN Loopback-detection configuration, click "Apply" to configure.

VLAN Loopback-detection configuration		
Port	Ethernet1/0/1 V	
VLAN ID		
Operation	Add 🗸	
	A	oply

entry	describe	
Port	Ethernet port name	
VLAN ID	VLAN ID, range 1-4094	
Operation	Add: Enable VLAN loop detection	
	Remove: Disable VLAN loop detection	

3.4.3. Loopback-detection interval-time configuration

This page can be used to configure the loop detection interval.

To display the "Loopback-detection interval-time configuration" page, click Port configuration ->Port Loopback-detection configuration->Loopback-detection interval-time configuration, click "Apply" to configure.

Loopback-detection interval-time co	nfiguration
Loopback-detection interval time	
no Loopback-detection interval time	
Operation	Configuration 🗸
	Apply

entry	describe	
Loopback-detection interval time	Interval time between loops, size 5-300 seconds	
no Loopback-detection interval time	No loop interval, size 1-30 seconds	
Operation	Configuration: Set the test time by yourself.	
	Default: Restore the default configuration, there is a loop	
	detection interval of 5 seconds, there is no loop detection	
	interval of 3 seconds.	

3.4.4. Loopback-detection control recovery configuration

This page is used to configure loop detection to automatically return to an uncontrolled state. To display the "Loopback-detection control recovery configuration" page, click Portconfiguration

-> PortLoopback-detection configuration -> Loopback-detection control recovery configuration, click "Apply" to configure.

Loopback-detection control recovery configuration		
Recovery switch timeout		
	Apply	

entry	describe	
Recovery switch timeout	When a port is disabled or blocked due to a loop, it automatically	
	recovers to an uncontrolled time, the size range is 0-3600 seconds.	
	When it is configured as 0, the auto recovery function is disabled.	

3.5. Isolate-port configuration

This section can set up port isolation related functions.

3.5.1. Isolate-port group configuration

This page can be used to add or delete isolated groups.

To display the "Isolate-port group configuration " page, click

Port configuration -> Isolate-port configuration -> Isolate-port group configuration , click "Apply" to configure.

Isolate-port	group	confi	guration	
Group name				
Operation	Add	~		
				Apply

entry	describe
Group name	Isolation group name, example: aaaa
Operation	Add: Create an isolation group
	Remove: Delete an isolation group

3.5.2. Interface join group config

This page can be used to add ports for isolation groups.

To display the "Interface join group config" page, click Port configuration ->Isolate-port configuration->Interface join group config, click "Apply" to configure.

Interface join group config			
Group name			
Port	Ethernet1/0/1 V		
Operation	Add V		
	Apply		

entry	describe
Group name	Created isolation group name, example: aaaa
Port	Ethernet port name
Operation	Add: Add ports to the isolation group
	Remove: Delete ports in isolation groups

3.5.3. Show Isolate-port group

This page is used to display isolation group information.

To display the "show Isolate-port group" page, click Port configuration ->Isolate-port configuration->show Isolate-port group, click "Apply" to view.

show Isolate-port group		
Group name		
	Apply	

entry	describe
Group name	Created isolation group name, example: aaaa

3.6. Port storm-control config

This chapter can set up storm control related functions.

3.6.1. Port storm-control config

This page can be configured for the storm control function of the port.

To display the "Port storm-control config" page, click Port configuration ->Port storm-control config->Port storm-control config, click "Apply" to configure.

storm-control configuration					
Port	Ethernet1/	0/1	v]	
storm-control type	broadcast	~			
storm-control value					
Operation	Add 🗸	•			
				Арр	bly

entry	describe	
Port	Ethernet port name	
storm-control type	Broadcast/Multicast/Unicast	
storm-control value	storm control rate, ranging from 1-1000000 kbps or pps 1-1488095	
Operation	Add: Turn on the storm control function and configure the speed limit	
	Remove: Disable Storm Control	

Information feedback window		
Port	storm-control type	
Ethernet1/0/1	None	
Ethernet1/0/2	None	
Ethernet1/0/3	None	
Ethernet1/0/4	None	
Ethernet1/0/5	None	
Ethernet1/0/6	None	
Ethernet1/0/7	None	
Ethernet1/0/8	None	

entry	describe
Port	Ethernet port name
storm-control type	Broadcast/Multicast/Unicast

3.6.2. storm-control bypass configuration

This page can configure storm control unit, filter protocol, filter protocol status and other functions. To display the "storm-control bypass configuration" page, click Port configuration ->Port storm-control config->storm-control bypass configuration, click "Apply" to configure.

storm-control configuration		
storm-control type:	bypass 🗸	
storm-control bypass protocol:	arp 🗸	
storm-control bypass protocol status: disab		
	Apply	

entry	describe	
storm-control type Bypass: Bypass Protocol		
	Kbps: Storm control rate units	
	pps: Storm control rate units	
storm-control bypass protocol	Broadcast Storm Filter Agreement	
storm-control bypass protocol status	rotocol status Disable: Disable protocol filtering	
	Enable: Enable protocol filtering	

3.7. Port rate-violation config

This chapter is mainly used for the configuration of rate limiting functions.

3.7.1. rate-violation configuration

This page is mainly used to configure the rate limit function.

To display the "rate-violation configuration" page, click Port configuration -> Port rate-violation config ->rate-violation configuration, click "Apply" to configure.

Port rate-violation config		
Port	Ethernet1/0/1	~
rate-violation type	all 🗸	
rate-violation value		
rate-violation sub type	shutdown	~
rate-violation recover time		
Operation	Add 🗸	
		Apply

entry	describe	
Port	Ethernet port name	
rate-violation type	Type of breach:	
	All/Broadcast/Multicast/Unicast/	
	Control: Operation violation	
rate-violation value	Limit rate, range 200-2000000	
rate-violation sub	Overspeed operation:	
type	Shutdown: Disable port	
	Block: Block port	
rate-violation	The time when the port overspeed is automatically resumed after it is	
recover time	disabled, if the size is 0-86400 seconds, configuring 0 seconds means no	
	automatic recovery	
Operation	Add: Function Enable	
	Remove: Function disabled	

3.8. Port virtual-cable-test config

This chapter can be used to detect port link lines.

3.8.1. virtual-cable-test configuration

This chapter can be used to detect port link lines.

To display the "virtual-cable-test configuration" page, click Port configuration ->Port virtual-cable-test configuration, click "Apply" to configure.

virtual-cable-test configuration				
Port	Ethernet1/0/1	~		
				Apply

Information feedback window					
Switch# virtual Interface Ether:	-cable-test intendent of the second sec	erface Ethernet1/0/14			
Cable pairs	Cable status	Length (meters)			
(1, 2)	well	13			
(3, 6)	well	13			
(4, 5)	well	13			
(7, 8)	well	13			

entry	describe
Port	Ethernet port name

3.9. Port debug and maintenance

This section is mainly used to view port, overall traffic statistics, port rate violation configuration and other information view.

3.9.1. Show port information

This page can be used to view port details.

To display the "Show port information" page, click Port configuration ->Port debug and maintenance->Show port information, click "Apply" to view.

```
Please select port: Ethernet1/0/1 ~
```

```
Information feedback window
Interface brief:
Ethernet1/0/1 is down, line protocol is down
Ethernet1/0/1 is layer 2 port, alias name is (null), index is 1
Hardware is Gigabit-TX, address is 00-1f-ce-10-b0-1b
PVID is 1
MTU 1500 bytes, BW 10000 Kbit
Time since last status change: 0w-0d-0h-36m-32s (2192 seconds)
Encapsulation ARPA, Loopback not set
Auto-duplex , Auto-speed
FlowControl is off, MDI type is auto
```

3.9.2. Show entire traffic information

This page can be used to view statistics of overall traffic.

To display the "Show entire traffic information" page, click Port configuration ->Port debug and maintenance->Show entire traffic information, click "Apply" to view.

Show entire tra	Show entire traffic information									
Dort		Receiving statistics			Transmitting statistics					
Porc	Total packets	Error packets	Dropped packets	5 minute rate(packets/sec)	Last 5 second rate(packets/sec)	Total packets	Error packets	Dropped packets	5 minute rate(packets/sec)	Last 5 second rate(packets/sec)
Ethernet1/0/1	0	0	0	0	0	0	0	0	0	0
Ethernet1/0/2	0	0	0	0	0	0	0	0	0	0
Ethernet1/0/3	0	0	0	0	0	0	0	0	0	0
Ethernet1/0/4	0	0	0	0	0	0	0	0	0	0
Ethernet1/0/5	0	0	0	0	0	0	0	0	0	0
Ethernet1/0/6	0	0	0	0	0	0	0	0	0	0
Ethernet1/0/7	0	0	0	0	0	0	0	0	0	0
Ethernet1/0/8	0	0	0	0	0	0	0	0	0	0

3.9.3. Show rate violation port

This page can be used to view port rate violation function configuration information. To display the "Show rate violation port" page, click Port configuration ->Port debug and maintenance->Show rate violation port, click "Apply" to view.

Rate-violation port state information				
Port	Port rate-violation control mode	Rate-violation port state		
Ethernet1/0/1	shutdown	down		

entry	describe
Port	Ethernet port name
Port rate-violation control mode	Shutdown: Disable port
	Block: Block port
Rate-violation port state	Status of current port:
	Down: Not connected
	Up: Connected
	Forwarding: forward
	Block: block

3.10. uldp configuration

This chapter is mainly used for the configuration of single link detection function.

3.10.1. uldp enable config

This page can be used to enable or disable single link detection protocols.

To display the "uldp enable config" page, click Port configuration -> uldp configuration->uldp enable config, click "Apply" to configure.

uldp global enable configuration			
uldp global enable type	uldp enable	~	
Operation	Enable 🗸		
		Apply	

entry	describe
uldp global	uldp enable: Turn on the ULDP function of all ports that support ULDP functions.
enable type	uldp aggressive-mode: Configure all ports ULDP working mode for positive mode.
	uldp manual shutdown: global close auto disable port, switch to manual close port.
Operation	Enable: Function Enable
	Disable: Function Disable

uldp port enable configuration			
Port	Ethernet1/0/1 V		
uldp port enable type	uldp port enable	~	
Operation	Enable 🗸		
		Apply	

entry	describe		
Port	Ethernet port name		
uldp port enable type	Uldp port enable: Turn on the ULDP function of the specified port.		
	mode to positive mode.		
Operation	Enable: Function Enable		
	Disable: Function Disable		

3.10.2. uldp Hello message config

This page is used to Hello the message sending interval.

To display the "uldp Hello message config" page, click Port configuration -> uldp configuration->uldp Hello message config, click "Apply" to configure.

uldp Hello message confi	g	
uldp Hello message time		
Operation	Configuration	~
		Apply

entry	describe
uldp Hello message time	Message sending interval, range 5-100 seconds
Operation	Configuration: User self-configuration
	Default: Restore the default configuration, the default configuration is
	10 seconds.

3.10.3. uldp recovery time config

This page can be used to configure ULDP auto recovery time.

To display the "uldp recovery time config" page, click Port configuration -> uldp configuration->uldp recovery time config, click "Apply" to configure.

uldp recovery time config			
uldp Hello message time			
Operation	Configuration V		
	Apply		

entry	describe	
uldp Hello message	Automatic recovery time after the port is disabled, ranging from 30-86400	
time	seconds to 0 seconds without automatic recovery	
Operation	Configuration: User self-configuration	
	Default: Restore default configuration, default configuration is 0 seconds.	

3.10.4. Show uldp configuration

This page can be used to view port ULDP configuration information.

To display the "uldp recovery time config" page, click Port configuration -> uldp configuration->uldp recovery time config, click "Apply" to view.

show uldp configuration				
Port	Port all 🗸			
			Apply	

```
Information feedback window
Switch# show uldp
uldp enable
uldp hello interval is
                        10
uldp shut down mode is
                       AUTO
uldp global work mode is
                      NORMAL
the total number of the port is
                       4
     _____
 PortName PhyLink LineProto WorkMode
                                 PortState NeighborNum
_____
Ethernet1/0/25 UP
                   DOWN NORMAL
                                             0
                                   INACTIVE
Ethernet1/0/26 UP
                  DOWN
                         NORMAL
                                   INACTIVE
                                             0
Ethernet1/0/27 UP
Ethernet1/0/28 UP
                  DOWN
                         NORMAL
                                   INACTIVE
                                             0
                   DOWN
                                   INACTIVE
                                             0
                         NORMAL
 _____
```

3.11. LLDP configuration

This chapter can be used to configure LLDP related functions.

3.11.1. LLDP configuration

This page can be configured to enable or disable LLDP functionality.

To display the "LLDP configuration" page, click Port configuration ->LLDP configuration->LLDP configuration, click "Apply" to configure.

LLDP global enable configuration				
IIdp enable Enable V				
				Apply

entry	describe
lldp enable	Enable: Global On LLDP Function
	Disable: Global Off LLDP Function

LLDP port enable configuration				
Port	Ethernet1/0/1 V			
LLDP port enable type	LLDP port enable 🛛 🗸			
Operation	Enable 🗸			
	Apply			

entry	describe
Port	Ethernet port name
LLDP port enable type	Enable or disable LLDP functions
Operation	Turn on or off LLDP function

3.11.2. LLDP port status config

This page can configure port status.

To display the "LLDP port status config" page, click Port configuration ->LLDP configuration->LLDP port status config, click "Apply" to configure.

LLDP port status config				
Port	Ethernet1/0/1 V			
LLDP port status	send 🗸			
	Apply			

entry	describe	
Port	Ethernet port name	
LLDP port status	Send: Send only data	
	Receive: Receive only data	
	Both: Sending and receiving data simultaneously	
	Disable: Both sending and receiving are prohibited	

3.11.3. LLDP tx-interval config

This page can configure the interval between sending updates.

To display the "LLDP tx-interval config" page, click Port configuration ->LLDP configuration->LLDP tx-interval config, click "Apply" to configure.

LLDP tx-interval config		
LLDP Hello message time		
Operation	Configuration V]
	A	pply

entry	describe
LLDP Hello	Update message sending interval between 5-32768 seconds
message time	
Operation	Configuration: User self-configuration
	Default: Restore the default configuration, the default configuration is 30 seconds.

3.11.4. LLDP msgTxHold config

This page can configure the value of the message aging time multiplier.

To display the "LLDP msgTxHold config" page, click Port configuration ->LLDP configuration->LLDP msgTxHold config, click "Apply" to configure.

LLDP msgTxHold config		
LLDP msgTxHold value		
Operation	Configuration	~
		Apply

entry	describe	
LLDP msgTxHold value	Numerical magnitude between 2-10	
Operation	Configuration: User self-configuration	
	Default: Restore default configuration, default configuration is 4	

3.11.5. LLDP transmit delay config

This page can configure the sending delay time of the update message.

To display the "LLDP transmit delay config" page, click Port configuration ->LLDP configuration->LLDP transmit delay config, click "Apply" to configure.

LLDP transmit delay config	J	
LLDP transmit delay value		
Operation	Configuration ~	
	Appl	у

entry	describe	
LLDP transmit delay value	Value between 1-8192 seconds	
Operation Configuration: User self-configuration		
	Default: Restore default configuration for 2 seconds	

3.11.6. LLDP notification interval config

This page can configure the interval between sending Trap messages. To display the "LLDP notification interval config" page, click Port configuration ->LLDP configuration->LLDP notification interval config, click "Apply" to configure.

LLDP notification interval config			
LLDP notification interval value			
Operation	Configuration ~		
	A	pply	

entry	describe	
LLDP notification interval value	Value between 5 and 3600 seconds	
Operation Configuration: User self-configuration		
	Default: Restore default configuration for 5 seconds	

3.11.7. LLDP neighbors max-num config

This page can be used to Remote Table the settings for save entries. To display the "LLDP notification interval config" page, click Port configuration ->LLDP configuration->LLDP notification interval config, click "Apply" to configure.

LLDP neighbors max-num config		
Port	Ethernet1/0/1 V	
LLDP neighbors max-num value		
Operation	Configuration ~	
	Apply	

entry	describe		
Port	Ethernet port name		
LLDP neighbors max-num value	Remote table maximum save entry size 5-500		
Operation	Configuration: User self-configuration		
	Default: Restore default configuration, default configuration is 100		

3.11.8. LLDP too mangy neighbors config

This page can be used to set up operations after Remote Table is full. To display the "LLDP too mangy neighbors config" page, click Port configuration ->LLDP configuration->LLDP too mangy neighbors config, click "Apply" to configure.

LLDP too mangy neighbors config			
Port	Ethernet1/0/1 V		
LLDP too mangy neighbors value	discard V		
	Apply		

entry	describe	
Port	Ethernet port name	
LLDP too mangy	Discard: Discard new neighbor information	
neighbors value	Delete: Delete the neighbor information with the least aging time in the	
	remore table, and then add new neighbor information	

3.11.9. LLDP transmit optional tlv config

This page can configure port TLV properties.

To display the "LLDP transmit optional tlv config" page, click Port configuration ->LLDP configuration->LLDP transmit optional tlv config, click "Apply" to configure.

LLDP transmit optional tlv config			
Port	Ethernet1/0/1 V		
LLDP Port description			
LLDP System capability			
LLDP System description			
LLDP System name			
	Apply		

entry	describe
Port	Ethernet port name
LLDP Port description	Port description name information needs to be configured
LLDP System capability	Information describing system capabilities
LLDP System description	Message describing the system
LLDP System name	System name information

3.11.10. Show LLDP configuration

This page can be used to view LLDP configuration messages.

To display the "show LLDP configuration" page, click Port configuration ->LLDP configuration->show LLDP configuration, click "Apply" to view.

show LLDP configuration			
LLDP too mangy neighbors value	show LLDP		~
Port	all	~	
		A	oply

Information feedback window				
Switch# show lldp				
LLDP GLOBAL INFORMATIONS				
LLDP has been disabled globally.				
LLDP enabled port : NULL				
LLDP interval :30				
LLDP txTTL :120				
LLDP NotificationInterval :5				
LLDP txDelay :2				
LLDP-MED FastStart Repeat Count :4				
ENDEND				

show LLDP configuration		
LLDP too mangy neighbors value	show LLDP port	~
Port	Ethernet1/0/14 ~	·]
		Apply

Information feedback window

```
Switch# show lldp
-----LLDP GLOBAL INFORMATIONS-----
LLDP has been disabled globally.
LLDP enabled port : NULL
LLDP interval :30
LLDP txTTL :120
LLDP txTTL :120
LLDP NotificationInterval :5
LLDP txDelay :2
LLDP-MED FastStart Repeat Count :4
------END------
```

show LLDP configuration				
LLDP too mangy neighbors value	show LLDP		~	
Port	all	~		
			Apply	

Information feedback v	window						
Switch# show lldp t	raffic						
PortName	Ageouts	FramesDiscarded	FramesInErrors	FramesIn	FramesOut	TLVsDiscarded	TLVsUnrecognized
Ethernet1/0/14	0	0	0	0	0	0	0

show LLDP configuration				
LLDP too mangy neighbors value	show LLDP		~	
Port	all	~		
			Apply	

3.12. LED shutoff configuration

This chapter can be used to set the timing of led lights out.

3.12.1. Time Range configuration

This page can be used to set the time range for led lights to go out.

To display the "Time Range configuration" page, click Port configuration ->LED shutoff configuration->Time Range configuration, click "Apply" to configure.

Time range configuration				
Time range name				
Time range type	absolute 🗸 🗌			
Start Time				
Week				
Time				
Date				
End Time				
Week				
Time				
Date				
Operation type	Add V			
	Apply			

entry	describe	
Time range name	Time range name, length 1-64 characters	
Time range type	Absolute: Absolute time range, date required	
	Absolute-periodic: Absolute cycle time range	
	Periodic: Period Time Range	
Week	Range :1-7	
Time	Time format :14:00	
Date	Date Scope: 2001.1.1-2038.12.31	

3.12.2. LED shutoff config

This page can be used for LED timing extinguishing configuration.

To display the "LED shutoff config" page, click Port configuration ->LED shutoff configuration->LED shutoff config, click "Apply" to configure.

LED shutoff configuration				
Time range name		~		
LED state	Open 🗸			
Operation	Configuration ~			
		Apply		

entry	describe	
Time range name	With the configured time range name	
LED state	LED lamp status	
Operation	Configuration: User self-configuration	
	Default: Function disabled	

3.13. Jumbo packet forwarding configuration

This section can be used for the configuration of super packet forwarding. To display the "LED shutoff config" page, click Port configuration ->LED shutoff configuration->LED shutoff config, click "Apply" to configure.

Jumbo packet forwarding configuration				
Jumbo packet size				
Operation	Configuration ~			
		Apply		

entry	describe	
Jumbo packet size	Range :1500-12270	
Operation	Configuration: User self-configuration	
	Default: Function disabled	

4. MAC address table configuration

4.1. MAC address table configuration

4.1.1. MAC address aging-time configuration

Each time the switch learns a MAC address, it will store the address and set the aging time. When the time is over, the address will be removed from the switch.

MAC address aging-time configuration				
MAC address aging-time				
Operation	Configuration 🗸			
		Apply		

MAC address aging-time	The aging time range is 10-1000000, 0 means no aging		
Operation	Configuration	Set the aging time into the switch	
	Default	Restore the aging time of the switch to the default state	

MAC address aging-time
300

Display the current MAC address aging time

4.1.2. Configurate MAC address

Configure static or Blackhole MAC addresses, and establish the mapping relationship between MAC addresses and ports and VLANs.

Configurate static MAC address		
MAC address		
VLAN ID	1 🗸	
Port list	Ethernet1/0/1 🗸	
Operation	Add 🗸	
	Apply	

MAC address	Hexadecimal MAC address, the format is xx-xx-xx-xx-xx-xx		
VLAN ID	Created VLAN ID		
Port list	Mapped port		
Operation	Add	The mapping relationship between MAC address and port and	
		VLAN will be added	
	Remove	Delete the mapping relationship of the specified MAC address,	
		VLAN, and port	

Configurate blackhole MAC address		
MAC address		
VLAN ID	1 🗸	
Blackhole based type	~	
Operation	Add 🗸	
	Apply	

MAC address	Hexadecimal MAC address, the format is xx-xx-xx-xx-xx, packets with this address will be discarded and will not be forwarded to the network by		
	the switch		
VLAN ID	Created VLAN ID		
Blackhole based type	source Source based on source address filter		
	destination	Target based on target address filter	
	both	Both are based on source address and destination address	
		filters, the default value is both	
Operation	Add	The mapping relationship between MAC address and port	
		and VLAN will be added	
	Remove	Delete the mapping relationship of the specified MAC	
	address, VLAN, and port		

MAC address	VLAN ID	Port
00-11-22-cc-bb-dd	1	Ethernet1/0/1
00-11-55-cc-bb-df	1	Blackhole

Display current existing MAC address, port, and VALN mapping relationship

4.1.3. Delete MAC address

Quickly delete the MAC address in the switch.

Delete MAC address		
Port status	Static 🗸	
Delete by VLAN ID	1 🗸	Select
Delete by MAC		Select
Delete by port	Ethernet1/0/1 V	Select
		Delete

Port status	Static	User-created and assigned MAC address
	Dynamic	The MAC address automatically learned by the switch through
		the message
	Blackhole	The user creates the assigned MAC address, but the packet of
		this address will not be forwarded by the switch
Delete by VLAN ID	The created VLA	N ID, delete the selected address type in the VLAN
Delete by MAC	Hexadecimal MAC address, the format is xx-xx-xx-xx-xx-xx	
Delete by port	Delete all MAC addresses under the port	

MAC address	VLAN ID	Status
00-1a-33-44-de-fd	1	Ethernet1/0/1
10-55-df-98-77-55	1	Blackhole

Display the current mapping relationship between MAC address, VLAN ID, and port

4.1.4. MAC address query

Quickly query the MAC address in the switch.

MAC address query		
Port status	Static 🗸	Select
Query by MAC		Select
Query by VLAN ID	1 🗸	Select
Query by port	Ethernet1/0/1 V	Select
		Apply

Port status	Static	User-created and assigned MAC address
	Dynamic	The MAC address automatically learned by the switch through
		the message
	Blackhole	The user creates the assigned MAC address, but the packet of
		this address will not be forwarded by the switch
Query by MAC	Hexadecimal N	IAC address, the format is xx-xx-xx-xx-xx
Query by VLAN ID	The created VL	AN ID, showing the address in the VLAN
Query by port	Find the MAC a	ddress by port

Note: Check the small box at the back to make the condition take effect. By default, there is no condition. When there is no condition, all MAC address information will be displayed.

Read Vlan	mac address table Mac Address	Туре	Creator	Ports
1 1	00-0e-c6-c7-93-15 10-f0-13-f1-72-3a	STATIC STATIC	App System	Ethernet1/0/8 CPU
2	00-11-33-55-88-66	STATIC	: User	Ethernet1/0/4

Display the results of the query

5. VLAN configuration

5.1. VLAN configuration

5.1.1. Create/Remove VLAN

VLAN configuration function module, users add or delete VLANs in this module .

VLAN ID configuration			
VLAN ID			
VLAN Name			
VLAN Type			~
Operation	Add	~]
			Apply

VLAN ID	The serial number of the VLAN, range: 2-4094			
VLAN name	By default, the default is VLAN plus four-digit serial number, range: 1-64 characters.			
VLAN type	Private vlan (isolated). Private vlan (comm There are three dedicated VLANs in the P and Community VLAN can communicate Community VLAN related to this Primary isolated from each other and are only rela communicate with each other; the ports with each other or with the related Prima between the ports in the Community VLA is no communication between the ports i	unity).Private vlan (primary).universal vlan; rimary port: Primary VLAN, Isolated VLAN with the ports of the Isolated VLAN and VLAN; the ports in the Isolated VLAN are ated to it. The ports in the Primary VLAN in the Community VLAN can communicate ary VLAN ports; there is no communication N and the ports in the Isolated VLAN. There in the Community VLAN and the ports in the		
Operation	Add Add VLAN			
	Remove Remove VLAN			

VLAN ID information				
VLAN ID	VLAN Name	VLAN Type		
1	default	universal vlan		

5.1.2. Assign ports for VLAN

Assign ports to the VLAN, and users add and remove ports in the VLAN in this module.

Assign ports for VLAN			
VLAN ID	1~		
Port	Ethernet1/0/1 🗸		
Operation	Add 🗸		
	Apply		

VLAN ID	Created VLAN	
Port	Port name	
Operation	Add Add port to VLAN	
	Remove	Remove the port from the VLAN port list

LAN	Name	Туре	Media	Ports	
1	default	Static	ENET		
				Ethernet1/0/3	Ethernet1/0/4
				Ethernet1/0/5	Ethernet1/0/6(T)
				Ethernet1/0/7	Ethernet1/0/8
				Ethernet1/0/9	Ethernet1/0/10
				Ethernet1/0/11	
				Ethernet1/0/13	Ethernet1/0/14
				Ethernet1/0/15	Ethernet1/0/16
				Ethernet1/0/17	Ethernet1/0/18
				Ethernet1/0/19	Ethernet1/0/20
				Ethernet1/0/21	Ethernet1/0/22
				Ethernet1/0/23	Ethernet1/0/24
				Ethernet1/0/25	Ethernet1/0/26
				Ethernet1/0/27	Ethernet1/0/28
Priva	ate vlan:				
/LAN	Name	Type	Asso VLAN	Ports	
2	test	Primary	4		
		_		Ethernet1/0/18(T)	Ethernet1/0/20(T)
				Ethernet1/0/22(T)	
1	R&D	Isolate	2	Ethernet1/0/2(T)	Ethernet1/0/5
				Ethernet1/0/6(T)	Ethernet1/0/18(T)
				Ethernet1/0/20(T)	Ethernet1/0/22(T)

5.1.3. Port type configuration

Switch port type setting, the user can change the switch port type in this module.

Port mo	Port mode configuration		
Port	Ethernet1/0/1 V		
Туре	access 🗸		
State	Enable VLAN ingress check 🗸		
	Apply		

Port	Port name		
Туре	access		
	trunk		
	hybrid		
State Enable VLAN When a data packet enters the switch, the		When a data packet enters the switch, the VLAN ingress filter	
	ingress check checks whether the ingress port of the data packet belor		
	given (forwarded) VLAN		
	Disable VLAN	When a data packet enters the switch, the VLAN ingress filter	
	ingress check does not check whether the ingress port of the data packet		
		belongs to the given (forwarded) VLAN	

Port mode configuration			
Port	Туре	State	
Ethernet1/0/1	access	Open	
Ethernet1/0/2	access	Open	
Ethernet1/0/3	access	Open	
Ethernet1/0/4	access	Open	
Ethernet1/0/5	access	Open	
Ethernet1/0/6	access	Open	
Ethernet1/0/7	access	Open	
Ethernet1/0/8	access	Open	

5.1.4. Hybrid port configuration

Switch Hybrid port VLAN configuration, the user changes the attributes of the switch's Hybrid port type in this module

Set hybrid native VLAN		
Port	Ethernet1/0/4 V	
Hybrid native VLAN		
Operation	Add 🗸	
	Apply	

Port	Port name		
Hybrid native VLAN	PVID of the port, VLAN TAG tag when the port is sending and		
	receiving data frames		
Operation	Add Add port to VLAN		
	Remove Remove the port from the VLAN port list		

Set hybrid allow VLAN		
Port	Ethernet1/0/4 🗸	
Hybrid allowed VLAN list		
Operation	Add all 🗸	
Tagged	Untag 🗸	
	Apply	

Port	Port name		
Hybrid allowed	List of allowed VLANs, connected with "-" and ";"		
VLAN list			
Operation	Add all Add port to all VLANs, 1-4094		
	Add Add a VLAN to the list of existing passed VLANs		
	Except add Add the port to all VLANs outside the specified VLAN		
	Cover add Clear the original passed VLAN list, and then add the specified		
	VLAN list to the VLAN list		
	Remove Remove the specified VLAN list from the existing passed VLAN list		
Tagged	Untag method to join		
	Tag way to joir	1	

Port	Hybrid native VLAN	Hybrid Tagged allowed VLAN list	Hybrid UnTagged allowed VLAN list
Ethernet1/0/4	1		

Display detailed information of Hybrid port

5.1.5. Trunk port configuration

Switch trunk port VLAN configuration, the user can change the attributes of the trunk port type of the switch in this module.

Set trunk native VLAN		
Port	Ethernet1/0/6 V	
Trunk native VLAN		
Operation	Add 🗸	
	Apply	

Port	Port name	
Trunk native VLAN	PVID of the po	rt, VLAN TAG tag when the port is sending and receiving
	data frames	
Operation	Add Add port to VLAN	
	Remove	Remove the port from the VLAN port list

Set trunk allow VLAN		
Port	Ethernet1/0/6 ¥	
Trunk allowed VLAN list		
Operation	Add all 🗸	
	Apply	

Port	Port name	
Trunk allowed VLAN list	List of allowed VLANs, connected with "-" and ";"	
Operation	Add all Add port to all VLANs, 1-4094	
	Add a VLAN to the list of existing passed VLANs	
	Except add Add the port to all VLANs outside the specified VLAN	
	Cover add Clear the original passed VLAN list, and then add the	
	specified VLAN list to the VLAN list	
	Remove Remove the specified VLAN list from the existing	
	passed VLAN list	

Port	Trunk native VLAN	Trunk allowed VLAN list
Ethernet1/0/6	1	1-4094

Display the detailed information of the trunk port

5.1.6. Private-vlan configuration

Switch Private-vlan binding operation, the user binds the private-vlan relationship in this module.

Private-vlan association		
Designate Primary-vlan	▼	
Association VLAN list		
Operation	Configuration V	
	Apply	

Designate Primary-vlan	Created Primary-vlan		
Association VLAN list	The secondary VLAN associated with the Primary-vlan, the secondary VLAN		
	includes private vlan (isolated), private vlan (community)		
Operation	Configuration Associate the secondary VLAN with the primary VLAN		
	Default Clear the primary-vlan association		

Primary-vlan	Association VLAN list
2	4

Display the related information of Primary-vlan

5.2. GVRP configuration

5.2.1. Enable global GVRP

The switch starts the global GVRP setting, and the user turns on or off the global GVRP.

Enable global GVRP	
Enable/Disable global GVRP	Disable 🗸
	Apply

Enable/Disable global GVRP	Enable	Start the global GVRP module function
	Disable	Disable the global GVRP module function

Enable global GVRP	
GVRP status	Disable

5.2.2. Enable GVRP on port

The switch port starts GVRP settings, and the user opens or closes the port GVRP.

Enable GVRP on port	
Port	Ethernet1/0/4 V
Enable/Disable GVRP	Enable 🗸
	Apply

Port	Port name	
Enable/Disable GVRP	Enable	Start the port GVRP module function
	Disable	Disable the port GVRP module function

Port	GVRP Status
Ethernet1/0/4	Disable
Ethernet1/0/6	Disable

Display the GVRP status of each port

5.2.3. GARP configuration

The switch configures GARP parameters, and the user sets the value of various timers to manage GARP.

GARP parameters configuration		
Join timer	200	
Leave timer	600	
Leaveall timer	10000	
Operation	Configuration 🗸	
	Apply	

Join timer	200-500ms	
Leave timer	500-1200ms	
Leaveall timer	500-60000ms	
Operation	configuration	Modify the value of the timer
	default	Restore the timer value to the default configuration

5.3. VLAN-translation configuration

5.3.1. Enable/Disable VLAN-translation

The switch port starts the VLAN-translation setting, and the user opens or closes the port VLAN-translation.

Enable/Disable VLAN-translation	
Port	Ethernet1/0/1 V
Enable/Disable VLAN-translation	Enable 🗸
	Apply

Port	Port name	
Enable/Disable VLAN-	Enable	Enable the VLAN-translation function of the port
translation	Disable	Disable the VLAN-translation function of the port

Port	VLAN-translation Status
Ethernet1/0/1	Disable
Ethernet1/0/2	Disable
Ethernet1/0/3	Disable
Ethernet1/0/4	Disable
Ethernet1/0/5	Disable
Ethernet1/0/6	Disable
Ethernet1/0/7	Disable
Ethernet1/0/8	Disable

Display the VLAN-translation status of each port

5.3.2. Add/Delete VLAN-translation

Switch VLAN-translation conversion settings, the user sets the VLAN-translation conversion relationship.

Add/Delete VLAN-translation		
Port	Ethernet1/0/1 V	
source vlan ID	Vlan1 🗸	
destination vlan ID	Vlan1 🗸	
dirction	in 🗸	
Operation	Add 🗸	
	Apply	

Port	Port name		
Source vlan ID	Configured VLAN		
Destination vlan ID	Configured VLAN		
direction	in	Configure the conversion direction of VLAN-translation as the ingress conversion function	
	out	Configure the conversion direction of VLAN-translation as the egress conversion function	
Operation	Add	Add VLAN-translation conversion relationship	
	Remove	Remove VLAN-translation conversion relationship	

5.3.3. VLAN-translation miss drop configuration

When the switch VLAN-translation fails to find the translation relationship, the packet loss settings are set. The user sets the direction of the packet loss configuration when the VLAN-translation finds the translation relationship.

VLAN-translation miss drop configuration		
Port	Ethernet1/0/1 V	
dirction	both 🗸	
Operation	Configuration 🗸	
	Apply	

Port	Port name	
direction	both The port performs VLAN-translation search and translation relatio	
		configuration for packet loss at both the egress and the ingress
	in	Packet loss configuration when the port performs VLAN-translation
		lookup translation relationship at the ingress
	out	Packet loss configuration when the port performs VLAN-translation
		lookup translation relationship at the egress
Operation	Configuration	Add VLAN-translation to find the packet loss configuration when
		searching for translation relations
	Cancel	Delete the configuration of packet loss when searching for translation
		relationship in VLAN-translation

5.3.4. Show VLAN-translation

The display of switch VLAN-translation related configuration, the user can check the switch VLAN-translation configuration.



Apply

Confirm that you want to view VLAN-translation related configuration information

Information feedback window					
Switch# show vlan-translation					
Interface Ethernet1/0/1:					
vlan-translation is enable,	miss	drop	is	not	set

Display VLAN-translation related configuration information

5.4. Dynamic VLAN configuration

5.4.1. VLAN protocol configuration

Switch VLAN protocol table entry configuration, user configuration protocol VLAN parameters to generate VLAN.

protocol vlan mode configuration		
VLAN interface	Vlan1 🗸	
protocol mode	ethernetll 🗸	
protocol mode ID		
SSAP ID		
priority ID		
Operation	Configuration V	
	Apply	

VLAN interface	Created VLAN		
Protocol mode	ethernetll	VLAN is divided according to data packets in ethernetII format	
	snap	VLAN is divided according to data packets in snap format	
	llc	VLAN is divided according to data packets in the LLC format	
	all	Used when cancel operation, restore all protocol VLAN to static VLAN	
Protocol mode ID	The ID range of ethernetII and snap is 1536-65535, and the ID range of Ilc is 0-255		
SSAP ID	It is only set in the llc protocol, range: 0-255		
Priority ID	Queue priority, range: 0-7		
Operation	configuration	Modify VLAN parameters and configure to dynamic protocol	
		VLAN	
	cancel	Restore VLAN from dynamic VLAN to static	

<mark>Information feedback window</mark> Switch# config Switch(config)# protocol-vlan mode ethernetII etype 1536 vlan 1 priority 0

Display configuration info

5.5. Dot1q tunnel configuration

5.5.1. Enable dot1q tunnel

Switch dot1q tunnel configuration, the user configures the port to enable the dot1q tunnel function.

Enable dot1q tunnel		
Port	Ethernet1/0/1 🗸	
Operation	Enable 🗸	
	Apply	

Port	Port name	
Operation	Enable	Enable dot1q tunnel
	Disable	Disable dot1q tunnel

Information feedback window
Switch# config
Switch(config)# interface Ethernet1/0/1
Switch(config-if-ethernet1/0/1)# dot1q-tunnel enable

Display the execution process and results

5.5.2. dot1q tunnel tpid configuration

Switch port dot1q tunnel tpid configuration, users configure port dot1q tunnel tpid parameters.

Dot1q tunnel tpid configuration		
Port	Ethernet1/0/1 V	
protocol	0x8100 V	
protocol ID		
	Apply	

Port	Port name	
Protocol	0x8100	Set the outer TPID to 0x8100
	0x9100	Set the outer TPID to 0x9100
	0x9200	Set the outer TPID to 0x9200
	protocol ID	Set a custom TPID
Protocol ID	The value of the custom TPID	
Information feedba	ck window	
Switch# config		
Switch(config)# interface Ethernet1/0/1		
Switch(config-if-ethernet1/0/1)# dot1q-tunnel tpid 0x8100		
QinQ enabled in Ethernet1/0/1, please disable it first!		
ERROR: set dot1q	-tunnel tpid on Ethernet1/0/1 err	or

Display the execution process and results

6. IGMP Snooping configuration

6.1. Switch on-off IGMP Snooping

Switch IGMP Snooping global switch, snooping IGMP messages

Switch on-off IGMP Snooping	
Switch on-off IGMP Snooping	Close 🗸
	Apply

Switch on-off IGMP	Open	Turn on the global switch of IGMP Snooping on the switch
Snooping	Close	Turn off the global switch of IGMP Snooping on the switch

Switch on-off IGMP Snooping
Switch on-off IGMP Snooping
Close

Display the current global status of IGMP Snooping

6.2. IGMP Snooping port enable

Configure IGMP Snooping port switch.

IGMP Snooping VLAN config				
VLAN ID	vlan 1 🗸			
Operation type	Open 🗸			
	Apply			

VLAN ID	Created VLAN ID		
Operation type	Open	Open VLAN interface IGMP Snooping	
	Close	Close VLAN interface IGMP Snooping	

IGMP Snooping VLAN config		
VLAN ID	Operation type	
1	OPEN	

Display the current existing VLAN interface and the running status of IGMP Snooping under the VLAN interface

6.3. IGMP Snooping configuration

Configure IGMP Snooping based on VLAN interface.

Igmp Snooping Configuration		
VLAN ID	N ID vlan 1 🗸	
Immediate leave configuration	immediate leave 🗸	
L2-general-querier configuration L2-general-querier 🗸		
Group number		
Source table number		
Operation	Configuration 🗸	
	App	ly

VI AN ID	Created VLAN ID				
Immediate leave	IGNP fast leave function	in VLAN			
configuration					
L2-general-querier	Used to send regular que	ries regularly to help switches in this			
configuration	network segment learn t	he mrouter port			
Group number	The upper limit of the tot	al number of groups. When the number of			
	joined groups reaches the	e limit, the newly joined groups will be			
	rejected to prevent hostile attacks. The default is 50, and the range:				
	1-65535.				
Source table number	The maximum number of	f source entries in each group, including			
	include sources and exclu	de sources. The default is 40. and the			
	range: 1-65535.	,			
Operation	Configuration Configure the checked parameters into the				
-	selected VLAN				
	Default Restore the checked parameters to the				
	default state				

Note: Whether it is to configure parameters or restore the default state, it is required to check the box at the back to take effect. The group number and the number of source table entries are unified functions, so the two function parameters will take effect together (when one parameter is set, the other will be set to the default value).

VLAN ID	Immediate leave configuration	L2-general-querier configuration	Group number	Source table number
1	Disable	Disable	50	40

Display the configuration parameters of the existing VLAN

6.4. IGMP Snooping mrouter port configuration

IGMP Snooping mrouter port parameter configuration.

IGMP Snooping mrouter port configuration					1
VLAN ID	vlan 1	~			
Mrouter port	Etherne	t1/0)/1	<	
MRouter port alive time					
Operation type	Add	~			
				App:	ly

VLAN ID	Created VLAN ID			
Mrouter port	Port name	Port name		
Mrouter port alive time	Time to live	of the port, range: 1-65535		
Operation type	Add Add the mrouter port parameter configuration checke			
	under the selected VLAN			
	Remove Delete the mrouter port parameter configuration che			
		under the selected VLAN		

VLAN ID	Mrouter port	MRouter port alive time
1		255

Display current configuration information

6.5. IGMP Snooping query configuration

IGMP Snooping query parameter configuration.

IGMP Snooping query configuration			
VLAN ID	vlan 1	~]
Query-Interval			\circ
Query-mrsp configuration			0
Query-robustness configuration			$ \circ $
Suppression-query-time configuration			0
Operation type	Add	~]
		Арр	oly

VLAN ID	Created VLAN ID		
Query-Interval	IGMP Snooping query interval, range: 1-65535		
Query-mrsp configuration	Maximum response time for group query		
Query-robustness configuration	IGMP Snooping robustness, range: 2-10		
Suppression-query-time configuration	Prohibited query time, range: 1-65535		
Operation type	Add	Add the mrouter port parameter configuration	
		checked under the selected VLAN	
	Remove Delete the mrouter port parameter		
	configuration checked under the selected VLAN		

VLAN ID	Query-Interval	Query-mrsp configuration	Query-robustness configuration	Suppression-query-time configuration
1	125	10	2	255

Display current configuration information

7. MLD Snooping configuration

7.1. Switch on-off MLD Snooping

Configure MLD Snooping global status switch

Switch on-off MLD Snooping	
Switch on-off MLD Snooping	Open 🗸
	Apply

Switch on-off MLD	Open	Turn on the global switch of the switch MLD Snooping
Snooping	Close	Turn off the global switch of the switch MLD Snooping

7.2. MLD Snooping port enable

Configure MLD Snooping port switch.

MLD Snooping VLAN config				
VLAN ID	vlan 1 🗸			
Operation type	Open 🗸			
	Apply			

VLAN ID	Created VLAN ID	
Operation type	Open	Open VLAN interface MLD Snooping
	Close	Close VLAN interface MLD Snooping

7.3. MLD Snooping configuration

MLD Snooping configuration based on VLAN interface.

MLD Snooping Configuration					
VLAN ID	vlan 1 🗸				
Immediate leave configuration	immediate leave 🗸				
L2-general-querier configuration	L2-general-querier 🗸				
Group number					
Source table number					
Operation	Configuration 🗸				
	App	ly			

VLAN ID	Create VLAN ID			
Immediate leave	MLD fast leave f	MLD fast leave function in VLAN		
configuration				
L2-general-querier	Used to send reg	gular queries regularly to help switches in this network		
configuration	segment learn th	ne mrouter port		
Group number	The upper limit of the total number of groups. When the number of joined			
	groups reaches the limit, the newly joined groups will be rejected to prevent			
	hostile attacks. The default is 50, and the range: 1-65535.			
Source table number	The maximum number of source entries in each group, including include			
	sources and exclude sources. The default is 40, and the range: 1-65535.			
Operation	Configuration	Configure the checked parameters into the selected VLAN		
	Default	Restore the checked parameters to the default state		

Note: Whether it is to configure parameters or restore the default state, it is required to check the box at the back to take effect. The group number and the number of source table entries are unified functions, so the two function parameters will take effect together (when one parameter is set, the other will be set to the default value).

7.4. MLD Snooping mrouter port configuration

MLD Snooping MRouter port parameter configuration.

MLD Snooping mrouter port configuration						
VLAN ID	vlan	$1 \vee$				
Mrouter port	Ether	net1	/0	/1	~	
MRouter port alive time						
Operation type	Add	~				
					App:	ly

VLAN ID	Created VLAN ID		
Mrouter port	Port name		
MRouter port alive time	Time to live of the port, range: 1-65535		
Operation type	Add Add the mrouter port parameter configuratio under the selected VLAN		
	RemoveDelete the mrouter port parameter configurationchecked under the selected VLAN		

7.5. MLD Snooping query configuration

MLD Snooping query parameter configuration.

MLD Snooping query configuration					
VLAN ID	vlan 1 🗸]			
Query-Interval		\circ			
Query-mrsp configuration		0			
Query-robustness configuration		\circ			
Suppression-query-time configuration		0			
Operation type	Add 🗸]			
	App	oly			

VLAN ID	Created VLAN ID			
Query-Interval	MLD Snoopin	MLD Snooping query interval, range: 1-65535		
Query-mrsp configuration	Maximum response time for group query			
Query-robustness	MLD Snooping robustness, range: 2-10			
configuration				
Suppression-query-time	Prohibited query time, range: 1-65535			
configuration				
Operation type	Add Add the mrouter port parameter configuration checked			
	under the selected VLAN			
	Remove Delete the mrouter port parameter configuration			
		checked under the selected VLAN		

8. Time Range configuration

8.1. Time Range configuration

Time Range configuration module, the user can add or delete the operation of in this module, which can be applied to various ACL.

In the absolute mode you must input the start-time, end-time is not necessary.

You must input the weeks, start-time and end-time, but need not input the date including start and end time in the absolute-periodic.

You must input the weeks, start-time and end-time, but need not input the date including start and end time, and may input multi-week values, separate them with ",", such as:1-7: Monday-Sunday; 31: daily; 96: weekdays; 127: weekend.

Input date format: YYYY.MM.DD. Input week format: number (1: Monday etc.), if input multi-week values, separate them with ",", such as:1,2 identify Monday Tuesday. Input time format: HH:MM: SS.

Time range configu	ration	
Time range name		
Time range type	absolute	< □
Start Time		
Week		
Time		
Date		
End Time		
Week		
Time		
Date		
Operation type	Add 🗸	
		Apply

Time range name	Time period names must begin with alphabetic or numeric characters ,1-64		
	characters		
Time range type	absolute Absolutely		
	absolute-periodic	Absolute-periodic	
	periodic periodic		
Week	Start or end weeks, "1-7":"monday-sunday";		
	"31":"daily"; "96":"weekdays"; "127":"weekend"		
Time	Start or end time, HH:MM:SS		
Date	Start or end date, YYYY.MM.DD, range2001.1.1-2038.12.31		
Operation type	Add Add operations		
	Remove	Delete operations	

9. ACL configuration

9.1. Numeric ACL

9.1.1. Standard numeric ACL

9.1.1.1. IP standard ACL

The digital standard IP access list configuration module, where users can create or modify parameters for the digital standard IP access list.

IP standard ACL(Number)		
List name		
Rule	permit 🗸	
Source address type	Any IP 🗸	
Source IP		
Reverse network mask		
tpid		
VLANID		
VLANID mask		
dscp		
	Apply	

List name	Digital Standard IP Access List Number 1-99	
Rule	permit	Rule permit
	deny	Rule deny
Source address type	Any IP	Match any IP address
	Specified IP	Match IP specified address
	Host IP	Match the specified host IP
Source IP	Source IP address, decimal point	
Reverse network mask	Source IP address mask, decimal point	
tpid	Label Protocol Identification ,0-65535	
VLANID	VLAN ID,1-4094	
VLANID mask	VLAN mask, 0-4095	
dcsp	IP message priority ,0-63	

9.1.1.2. MAC standard ACL

The digital standard MAC access list configuration module, where users can create or modify parameters for the digital standard MAC access list.

MAC standard ACL(Number)			
List name			
Rule	permit 🗸		
Source address type	Any MAC	\sim	
Source MAC			
Reverse network mask			
		Apply	

List name	Digital Standard MAC Access List Number 700-799	
Rule	permit	Rule permit
	deny	Rule deny
Source address type	Any MAC	Match any MAC address
	Specified MAC	Match MAC specified address
	Host MAC	Match the specified host MAC
Source MAC	Source MAC address	
Reverse network mask	source MAC address inverse mask	
9.1.2. Extended numeric ACL

9.1.2.1. IP extended ACL

Digital extension IP access list configuration module, where users can create or modify parameters for digital extension IP access list.

IP extended ACL(Number)				
Operation type	ICMP		~		
List name					
Rule	permit 🗸				
Fragment packet					
Source address type	Any IP	\sim			
Source IP					
Reverse network mask					
Destination address type	Any IP	\sim			
Destination IP					
Reverse network mask				ICMP extended	
IP precedence				ICMP type	
TOS				ICMP code	
Time range name			~		App

Operation type	Extended operation type:			
	ICMP.IGMP.TCP.UDP.EIGRP.GRE.IGRP.IPINIP.OSPF.IP.or			
	Specified_protocol			
List name	Digital extensions IP	access list numbers ,100-199		
Rule	permit	Rule permit		
	deny	Rule deny		
Fragment packet	Optional whether lo	ng messages are transmitted in pieces		
Source address type	Any IP	Match any IP address		
	Specified IP	Match IP specified address		
	Host IP	Match the specified host IP		
Source IP	Source IP address, decimal point			
Reverse network mask	Source IP address mask, decimal point			
Destination address type	Any IP Match any IP address			
	Specified IP	Match IP specified address		
	Host IP	Match the specified host IP		
Destination IP	Destination IP, decimal points			
Reverse network mask	Destination IP address mask, decimal point			
IP precedence	IP priority ,0-7			
TOS	Service type ,0-15			
Time range name	Time period names t	o be applied must begin with alphabetic or		
	numeric characters, 1-64 characters			
ICMP type	ICMP message type ,0-255			
ICMP code	ICMP message code	,0-255		

9.1.2.2. MAC-IP extended ACL

Digital extension MAC-IP access list configuration module, where users can create or modify parameters for digital extension MAC-IP access list.

MAC-IP extended ACL(Nu	mber)	
Operation type	ICMP	\checkmark
List name		
Rule	permit 🗸	
Source address type	Any MAC 🗸	
Source MAC		
Reverse network mask		
Destination address type	Any MAC 🗸	
Destination MAC		
Reverse network mask		
Source address type	Any IP 🗸	
Source IP		
Reverse network mask		
Destination address type	Any IP 🗸	
Destination IP		
Reverse network mask		
tpid		
VLANID		
VLANID mask		
dscp		
IP precedence		
тоѕ		
Time range name		
ICMP extended		
ICMP type		
ICMP code		
	App	ly

Operation type	Extension operation type:			
	ICMP.IGMP.TCP.UDP.EIGRP.GRE.IGRP.IPINIP.OSPF.IP.or Specified_protocol			
List name	3100-3199, Digital Extension MAC-IP Access List Number			
Rule	permit	Rule permit		
	deny	Rule deny		
Source address type	Any MAC	Match any MAC address		
	Specified MAC	Match MAC specified address		
	Host MAC	Match the specified host MAC		
Source MAC	Source MAC addr	ess		
Reverse network mask	source MAC addre	ess inverse mask		
Destination address	Any MAC	Match any MAC address		
type	Specified MAC	Match MAC specified address		
	Host MAC	Match the specified host MAC		
Destination MAC	Destination MAC address			
Reverse network mask	Destination MAC address inverse mask			
Source address type	Any IP	Match any IP address		
	Specified IP Match IP specified address			
	Host IP	Match the specified host IP		
Source IP	Source IP address, decimal point			
Reverse network mask	Source IP address mask, decimal point			
Destination address	Any IP	Match any IP address		
type	Specified IP	Match IP specified address		
	Host IP	Match the specified host IP		
Destination IP	Destination IP, d	ecimal points		
Reverse network mask	Destination IP add	dress mask, decimal point		
tpid	Label Protocol Identification ,0-65535			
VLANID	VLAN ID, 1-4094			
VLANID mask	VLAN mask, 0-4095			
dcsp	IP message priority 0-63			
IP precedence	IP priority ,0-7			
TOS	Service type ,0-15			
Time range name	Time period names to be applied must begin with alphabetic or numeric			
	characters ,1-64 c	haracters		
ICMP type	ICMP message typ	ICMP message type ,0-255		
ICMP code	ICMP message code ,0-255			

9.1.3. Delete Numeric ACL

Delete the digital access list module, where the user can delete the specified digital access list.

Delete Numeric ACL			
List name			
		Apply	

List name	1-3199, specify numeric access list numbers

9.2. Name ACL

9.2.1. Standard name ACL

9.2.1.1. IP standard ACL

Naming standard IP access list configuration module, where users can create or modify parameters for naming standard IP access list.

IP standard ACL	
List name	
Rule	permit 🗸
Source address type	Any IP 🗸
Source IP	
Reverse network mask	
tpid	
VLANID	
VLANID mask	
dscp	
	Apply

List name	-1, Nomenclature criteria IP access list names, strings must start with letters			
	64 characters			
Rule	permit	Rule permit		
	deny	Rule deny		
Source address type	Any IP Match any IP address			
	Specified IP	Match IP specified address		
	Host IP	Match the specified host IP		
Source IP	Source IP address, decimal point			
Reverse network mask	Source IP address mask, decimal point			
tpid	Label Protocol Identification ,0-65535			
VLANID	VLAN ID, 1-4094			
VLANID mask	VLAN mask, 0-4095			
dcsp	IP message priority 0-63	IP message priority 0-63		

9.2.2. Extended name ACL

9.2.2.1. IP extended ACL

Name extension IP access list configuration module, where users can create or modify parameters for named extension IP access list.

IP extended ACL			
Operation type	ICMP	~	
List name			
Rule	permit 🗸		
Source address type	Any IP 🗸		
Source IP			
Reverse network mask			
Destination address type	Any IP 🗸		
Destination IP			
Reverse network mask			ICMP extended
IP precedence			ICMP type
TOS			ICMP code
Time range name			Appl

Operation type	Extension operation type:			
	ICMP.IGMP.TCP.UDP.EIGRP.GRE.IGRP.IPINIP.OSPF.IP.or Specified_protocol			
List name	Name extensions IP access list names, strings must start with letters ,1-64			
	characters			
Rule	permit	Rule permit		
	deny	Rule deny		
Fragment packet	Optional whether long	messages are transmitted in pieces		
Source address type	Any IP	Match any IP address		
	Specified IP	Match IP specified address		
	Host IP	Match the specified host IP		
Source IP	Source IP address, decimal point			
Reverse network mask	Source IP address mask, decimal point			
Destination address	Any IP Match any IP address			
type	Specified IP	Match IP specified address		
	Host IP	Match the specified host IP		
Destination IP	Destination IP, decimal points			
Reverse network mask	Destination IP address mask, decimal point			
IP precedence	IP priority ,0-7			
TOS	Service type ,0-15			
Time range name	Time period names to be applied must begin with alphabetic or numeric			
	characters ,1-64 charac	characters ,1-64 characters		
ICMP type	ICMP message type ,0-255			

9.2.2.2. MAC extended ACL

Name extension MAC access list configuration module, where users can create or modify parameters for named extension MAC access list.

MAC extended ACL				
List name				
Rule	permit 🗸			
Source address type	Any MAC	~		
Source MAC				
Reverse network mask				
Destination address type	Any MAC	~		
Destination MAC				
Reverse network mask				
Packet type	none	~		
cos				
cos mask				
VLANID				
VLANID mask				
etherType				
etherType mask				
		Apply		

List name	Digital Extension MAC-IP Access List Number ,3100-3199		
Rule	permit	Rule permit	
	deny	Rule deny	
Source address type	Any MAC	Match any MAC address	
	Specified MAC	Match MAC specified address	
	Host MAC	Match the specified host MAC	
Source MAC	Source MAC address		
Reverse network mask	source MAC address invers	se mask	
Destination address	Any MAC	Match any MAC address	
type	Specified MAC	Match MAC specified address	
	Host MAC	Match the specified host MAC	
Destination MAC	Destination MAC address		
Reverse network mask	Destination MAC address inverse mask		
Packet type	none	none	
	tagged-802-3	Format of marked Ethernet 802-3 packets	
	tagged-eth2	Format of marked Ethernet II packets	
	untagged-802-3	Format of unmarked Ethernet 802-3 packets	
	untagged-eth2	Format of unmarked Ethernet II packets	
COS	cos, 0-7		
cos mask	cos mask, 0-7		
VLANID	VLAN ID,1-4094		
VLANID mask	VLAN mask, 0-4095		
etherType	Ethernet type field value, 1536-65535		
etherType mask	Ethernet type field value mask, 0-65535		

9.2.2.3. MAC-IP extended ACL

Name extension MAC-IP access list configuration module, where users can create or modify parameters for named extension MAC-IP access list.

MAC-IP extended ACL			
Operation type	ICMP		<
List name			
Rule	permit 🗸		
Source address type	Any MAC	~	
Source MAC			
Reverse network mask			
Destination address type	Any MAC	~	
Destination MAC			
Reverse network mask			
Source address type	Any IP	\sim	
Source IP			
Reverse network mask			
Destination address type	Any IP	\sim	
Destination IP			
Reverse network mask			
tpid			
VLANID			
VLANID mask]
dscp			
IP precedence			
тоѕ			
Time range name			

Operation type	Extension operation type:				
	ICMP.IGMP.TCP.UDP.EIGRP.GRE.IGRP.IPINIP.OSPF.IP.or Specified_protocol				
List name	Digital Extension MAC-IP Access List Number ,3100-3199				
Rule	permit	ermit Rule permit			
	deny	Rule deny			
Source address type	Any MAC	Match any MAC address			
	Specified MAC	Match MAC specified address			
	Host MAC	Match the specified host MAC			
Source MAC	Source MAC address				
Reverse network mask	source MAC address inverse mask				
Destination address	Any MAC Match any MAC address				
type	Specified MAC	Match MAC specified address			
	Host MAC	Match the specified host MAC			
Destination MAC	Destination MAC address				
Reverse network mask	Destination MAC address inverse mask				
Source address type	Any IP	Match any IP address			
	Specified IP	Match IP specified address			
	Host IP	Match the specified host IP			

Source IP	Source IP address, decimal point				
Reverse network mask	Source IP address mask, decimal point				
Destination address	Any IP Match any IP address				
type	Specified IP Match IP specified address				
	Host IP Match the specified host IP				
Destination IP	Destination IP, decimal points				
Reverse network mask	Destination IP address mask, decimal point				
tpid	Label Protocol Identification ,0-65535				
VLANID	VLAN ID,1-4094				
VLANID mask	VLAN mask, 0-4095				
dcsp	IP message priority 0-63				
IP precedence	IP priority ,0-7				
TOS	Service type ,0-15				
Time range name	Time period names to be applied must begin with alphabetic or numeric				
	characters, 1-64 characters				
ICMP type	ICMP message type ,0-255				
ICMP code	ICMP message code ,0-255				

9.2.3. Delete Name ACL

Delete the named access list module, where users can delete the specified named access list.

Delete Name ACL				
List name				
		Apply		

LIST Hame String must start with a letter, 1-04 characters

9.3. Filter configuration

9.3.1. Firewall configuration

Firewall ACL configuration module in which users can operate switch firewall configuration.

Switch firewall configuration			
Packet filtering		~	
Firewall default action		it 🗸	
			oly

Packet filtering	open	open
	close	close
Firewall default action	permit	Rule permit
	deny	Rule deny

9.4. Show ACL configuration

9.4.1. Show access list

The access control list module is displayed in which the user can display ACL specified information or all ACL information.

Show access list				
Access list	ALL			
		Apply		

Access list	Specify the ACL name or number to display ALL display all ACL
-------------	---------------------------------------------------------------

9.4.2. Show firewall

Display packet filtering function configuration information module, user in this module can display firewall status information.

Show firewall	
	Refresh

9.4.3. Show time range

Display time range function configuration information module, where users can display configured custom time information.

Show time range				
Time-range name	ALL			
		Apply		

Time-range name Specifies the time period name to display, ALL displays all time period information

9.5. ACL binding configuration

9.5.1. Attach ACL to port

ACL port binding module, the user can bind and delete the access list of the specified port.

Attach ACL to port					
Port	Ethe	rnet1	/0/1	~	
ACL type	IP	~			
List name					
ACL Attached Direction	in				~
Operation type	Add	~			
					Apply

Port	Designated port number				
ACL type	IP IP type				
	MAC	MAC type			
	MAC-IP	MAC-IP type			
List name	Specify access list name ,1-64 characters				
ACL Attached	in Application ACL only				
Direction	in and traffic-statistics Application ACL and flow monitoring				
Operation type	Add Add operations				
	Remove	Delete operations			

9.5.2. Show access group

The configuration information module on ACL display port, where the user can display the ACL binding information of the specified port or all ports.

Show access group					
Port	ALL	~			
ACL Attached Direction	in 🗸				
		Apply			

Port	Specifies the port number to display the information ALL displays all port information				
ACL Attached	in Application ACL only				
Direction	in and traffic-statistics	Application ACL and flow monitoring			

9.5.3. Clear Pacl Statistic

The statistical information module ACL the port, where the user can clear the ACL statistics of the specified port.

Clear Pacl Statistic				
Port or Interface name	Ethernet1/0/1 💙			
ACL Attached Direction	in 🗸			
	Apply			

Port or Interface name	Specifies the port number to clear statistics				
ACL Attached Direction	in Application ACL only				
	in and traffic-statistics	Application ACL and flow monitoring			

9.5.4. Attach ACL to vlan

ACL vlan binding module, where users can bind and delete access lists to specified VLAN.

Attach ACL to vlan				
VLAN interface	Vlan1	~	•	
ACL type	IP	\sim		
List name				
ACL Attached Direction	in			~
Operation type	Add	$\mathbf{\mathbf{v}}$		
				Apply

VLAN interface	Specifies the VLAN number to operate on			
ACL type	Specifies the type of ACL to bind: IP.MAC.MAC-IP			
List name	Specify access list name ,1-64 ch	Specify access list name ,1-64 characters		
ACL Attached	in Application ACL only			
Direction	in and traffic-statistics Application ACL and flow monitoring			
Operation type	Add	Add operations		
	Remove Delete operations			

9.5.5. Show vacl configuration

The vlan acl configuration information module is displayed in which the user can display ACL binding information for the specified VLAN or all VLAN.

show vacl configuration				
VLAN interface	Vlan1	~		
ACL Attached Direction in 🗸				
Apply				

9.5.6. Clear vlan acl statistic

Clear the VLAN acl statistical information module, where the user can clear the ACL statistics of the specified VLAN.

clear vlan acl statistic				
VLAN interface	Vlan1	~		
ACL Attached Direction	in 🗸			
				Apply

VLAN interface	Specifies the VLAN number to clear statistics				
ACL Attached	in Application ACL only				
Direction	in and traffic-statistics	Application ACL and flow monitoring			

10.IPv6 ACL configuration

10.1. IPv6 standard access-list configuration

IPv6 standard access list configuration module, users can create, delete or modify parameters for digital standard IPv6 access lists.

IPv6 standard access-list configuration					
Access list number					
Rule	permi	t 🗸			
Source address type	host-source 🗸				
IPv6 address					
Operation	Add	~			
					Apply

Access list number	Digital Standard IPv6 Access I	ist Number ,500-599		
Rule	permit Rule permit			
	deny	Rule deny		
Source address type	Specifies IPv6 source host	Matches IPv6 specified source host		
	All IPv6 source hosts	Match any IPv6 source host		
	IPv6 source address	Match IPv6 specified source address		
IPv6 address	IPv6 address to operate			
Operation	Add Add operations			
	Remove Delete operations			

10.2. IPv6 name access-list configuration

IPv6 named access table configuration module, the user can create, delete, or modify parameters on the named standard IPv6 access list.

IPv6 name access-list	configurat	ion		
IPv6 name access-list				
Rule	~			
Source address type	host-sourc	e 🗸		
IPv6 address				
Operation	Add 🗸			
				Apply

IPv6 name access-list	Name of access list		
Rule	permit	Rule permit	
	deny	Rule deny	
Source address type	Specifies IPv6 source host	Matches IPv6 specified source host	
	All IPv6 source hosts Match any IPv6 source host		
	IPv6 source address	Match IPv6 specified source address	
IPv6 address	IPv6 address to operate		
Operation	Add	Add operations	
	Remove	Delete operations	

10.3. Show IPv6 access list

Show IPv6 access control list module where users can display IPv6 access list to create, delete, or modify parameters.

Show IPv6 access list			
List name			
		Apply	

List name

Specifies the ACL name or number to display ,0-64 characters

10.4. Attach IPv6 ACL to port

IPv6ACL port binding module, the user can bind and delete the IPv6 access list on the specified port.

Attach IPv6 ACL to port					
Port	Ether	net1	/0/1	~	
List name					
ACL Attached Direction	in				~
Operation type	Add	~			
					Apply

Port	Designated port number		
List name	Specify access list name ,1-64 characters		
ACL Attached	in Application ACL only		
Direction	in and traffic-statistics	Application ACL and flow monitoring	
Operation type	Add	Add operations	
	Remove	Delete operations	

10.5. Attach IPv6 ACL to vlan

IPv6ACL VLAN binding module, the user can bind and delete the IPv6 access list to the specified VLAN.

Attach IPv6 ACL to vlan				
VLAN interface	Vlan1	~		
List name]	
ACL Attached Direction	on in 💊		~	
Operation type	Add 🗸			
				Apply

VLAN interface	VLAN number specified		
List name	Specify access list name ,1-64 characters		
ACL Attached	in Application ACL only		
Direction	in and traffic-statistics	Application ACL and flow monitoring	
Operation type	Add	Add operations	
	Remove	Delete operations	

11.AM configuration

11.1. AM global configuration

11.1.1. Enable/Disable AM

AM switch configuration module, the user can start or close the global AM function in this module.

Enable/Disable AM				
AM status	Enable 🗸		Information feedb	ack window
		Apply	AM status	Enable

11.2. AM port configuration

11.2.1. Enable/Disable AM port

AM port switch configuration module, where the user can start or close the AM function of the specified port.

		Information fee	nformation feedback window			
		Port	AM port status			
Enable/Disable AM port		Ethernet1/0/1	Disable			
Port	AM port status	Ethernet1/0/2	Disable			
Ethernet1/0/1 V	Enable 🗸	Ethernet1/0/3	Disable			
	Apply	Ethernet1/0/4	Disable			

Port	Specifies the port number	
AM port status	enable or disable	

11.2.2. AM IP-Pool configuration

AM IP-Pool configuration module, the user can set up a AM IP segment on the specified port, allowing / rejecting messages from within the segment to be forwarded through the port.

AM IP-Pool configuration				
Port	Ethernet1/0/1 🗸			
IP address				
Count				
Operation	Add 🗸			
	Apply			

Port	Designated port number		
IP address	Beginning IP address, decimal point		
Count	Number of consecutive addresses after starting IP address, 1-32		
Operation	Add Add operations		
	Remove	Delete operations	

11.2.3. AM MAC-IP-Pool configuration

AM MAC-IP-Pool configuration module, the user can set up a AM MAC-IP segment on the specified port, allowing / rejecting messages from within the segment to be forwarded through the port.

AM MAC-IP-Pool configuration						
Port	Ether	net1	/0/1	\sim	'	
IP address						
MAC address						
Operation	Add	~				
						Apply

Port	Designated port	number	
IP address	Beginning IP address, decimal point		
MAC address	Source MAC address		
Operation	Add Add operations		
	Remove	Delete operations	

11.3. Show AM port configuration

11.3.1. Show AM port configuration

The AM port configuration module is displayed in which the user can display the AM function configuration information of the specified port.

Show AM port configuration				
Port	~			
		Apply		

Designated port number

11.3.2. Clear port AM Pool

AM Pool address pool cleanup module, where users can configure the specified AM Pool to clear.

Clear port AM Pool				
Operation	all	~		
				Apply

Operation	all	Clear all AM Pool
ip-pool		Clear ip-pool only
	mac-ip-pool	Clear mac-ip-pool only

12. Port channel configuration

Configure port related features settings using the Port Channel configuration page.

12.1. LACP port group configuration

This section can be used to create convergent groups.

To display the "LACP port group configuration" page, click Port channel configuration->LACP port group configuration, click "Apply" to configure.

LACP port group configuration				
Group number				
Load balance mode src-mac 🛛 🗸				~
	set		Reset	

entry	describe		
Group number	Range :1-128		
Load balance mode	src-mac: Execute load balancing according to source MAC		
	dst-mac: Execute load balancing according to target MAC		
	dst-src-mac: Execute load balancing based on source and target MAC		
	src-ip: Execute load balancing according to source IP		
	dst-ip: Execute load balancing according to target IP		
	dst-src-ip: Execute load balancing according to target IP source		
	dst-src-mac-ip: Perform load balancing based on target and source Mac and		
	source IP		

Port group table					
Group number	Group member size	Load balance	Operation		
1	0	src-mac	Add member	<u>Remove member</u>	Show interface

entry	describe		
Group number	Convergence group created, size range :1-128		
Group member size	Number of members in convergent groups		
Load balance mode	src-mac: Execute load balancing according to source MAC		
	dst-mac: Execute load balancing according to target MAC		
	dst-src-mac: Execute load balancing based on source and target MAC		
	src-ip: Execute load balancing according to source IP		
	dst-ip: Execute load balancing according to target IP		
	dst-src-ip: Execute load balancing according to target IP source		

	dst-src-mac-ip: Perform load balancing based on target and source Mac and source IP
Operation	Click on the entry in the corresponding action bar and jump to the corresponding settings page

12.2. Delete port group

This page can be used to delete created convergent groups.

To display the "Delete port group" page, click Port channel configuration->Delete port group, click "Apply" to configure.

Port group table			
Group number	Group member size	Load balance	Operation
1	0	src-mac	<u>Delete</u>

entry	describe						
Group number	Range :1-128						
Group member	Number of members in convergent groups						
size							
Load balance	src-mac: Execute load balancing according to source MAC						
	dst-mac: Execute load balancing according to target MAC						
	dst-src-mac: Execute load balancing based on source and target MAC						
	src-ip: Execute load balancing according to source IP						
	dst-ip: Execute load balancing according to target IP						
	dst-src-ip: Execute load balancing according to target IP source						
	dst-src-mac-ip: Perform load balancing based on target and source Mac and						
	source IP						

12.3. Show port group info

This page can view the information of the convergent group configuration.

To display the "Show port group info" page, click Port channel configuration->Show port group info, click "Apply" to view.

```
Information feedback window
Switch# config
Switch(config)# show port-group brief
ID: port group number; Mode: port group mode such as on active or passive;
Ports: different types of port number of a port group,
     the first is selected ports number, the second is standby ports number, and
     the third is unselected ports number.
ID Mode Partner ID
                               Ports
                                            Load-balance
                                             src-mac
Switch(config)# show port-group detail
Flags: A -- LACP_Activity, B -- LACP_timeout, C -- Aggregation,
      D -- Synchronization, E -- Collecting, F -- Distributing,
      G -- Defaulted, H -- Expired
Port-group number: 1, Mode: ,
                           Load-balance: src-mac
Port-group detail information:
System ID: 0x8000,00-1f-ce-10-b0-1b
Local:
 Port
              Status
                        Priority Oper-Key Flag
 _____
Remote:
              Partner Priority Oper-Key SystemID
                                                             Flag
 Actor
 _____
```

12.4. Show interface port-channel

This page can view the information of the convergent group port. To display the "Show interface port-channel" page, click Port channel configuration->Show interface port-channel, click "Apply" to view.

```
Information feedback window
Switch# show interface port-channel 1
Interface brief:
 Port-Channell is down, line protocol is down
 Port-Channell is layer 2 port, alias name is (null), index is 53
 Port-Channell is LAG port, member is :
     Hardware is EtherChannel, address is 00-1f-ce-10-b0-1b
 PVID is 1
 MTU 1500 bytes, BW 10000 Kbit
 Time since last status change:0w-0d-3h-21m-9s (12069 seconds)
 Encapsulation ARPA, Loopback not set
 Force half-duplex, Auto-speed
 FlowControl is off, MDI type is auto
Statistics:
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
 The last 5 second input rate 0 bits/sec, 0 packets/sec
 The last 5 second output rate 0 bits/sec, 0 packets/sec
 Input packets statistics:
    0 input packets, 0 bytes, 0 no buffer
   0 unicast packets, 0 multicast packets, 0 broadcast packets
   0 input errors, 0 CRC, 0 frame alignment, 0 overrun, 0 ignored,
   0 abort, 0 length error, 0 undersize 0 jabber, 0 fragments, 0 pause frame
 Output packets statistics:
   0 output packets, 0 bytes, 0 underruns
    0 unicast packets, 0 multicast packets, 0 broadcast packets
    0 output errors, 0 collisions, 0 late collisions, 0 pause frame
```

12.5. Add member port

This page can be used to add port members to a convergence group. To display the "Add member port" page, click Port channel configuration->Add member port, click "Apply" to configure.

Port group add port					
Group nu	mber	1 ~			
Port list		Ethernet1/0/1			~
mode		on		~	
	Add			Reset	

entry	describe
Group number	To create a convergent group number
Port list	Ethernet port name
mode	On: force port to join port channel without LACP. enabled
	Active: Enable the LACP on the port and set it to Active mode;
	Passive: Enable LACP on the port and set it to passive mode

Port group port list	
Index	Port Name
1	Ethernet1/0/1

entry	describe
Index	To create a convergent group numb
Port Name	Ethernet port name added to convergence group

12.6. Del member port

This page can be used to delete port members within the convergence group. To display the "Del member port" page, click Port channel configuration->Del member port, click "Apply" to configure.

Port group remove port					
Group number 1 🗸					
Port list		Ethe	rnet1	/0/1	~
	Remove]	Reset	

entry	describe
Group number	To create a convergent group number
Port list	Ethernet port name

12.7. Set lacp port priority

This page is available with setting port priority.

To display the "Set lacp port priority" page, click Port channel configuration->Set lacp port priority, Click set "to set, click Reset" to restore default settings.

Set lacp port priority					
Group number 1		1 ~			
Port list		Ethe	ernet	1/0/1	~
Lacp port priority					
	set			Reset	

entry	describe
Group number	To create a convergent group number
Port list	Ethernet port name added to convergence group
Lacp port priority	Range :0-65535

12.8. Set lacp system priority

This page is available with setting system priorities.

To display the "Set lacp system priority" page, click Port channel configuration->Set lacp system priority, Click set "to set, click Reset" to restore default settings.

Set lacp system priority					
Lacp system	n priority				
	set		Reset		

entry	describe
Lacp system priority	Range :0-65535

13. DHCP configuration

13.1. DHCP management

13.1.1. Enable DHCP

DHCP status configuration and query, the user configures the DHCP server status and address conflict log status in this module, and checks the DHCP server status and address conflict log status.

Enable DHCP		
DHCP server status	Clo	ose 🗸
Conflict logging status	Ope	en 🗸
		Apply

DHCP server status	Close Close DHCP server		
	Open	Open DHCP server	
Conflict logging status	Close address conflict logging		
	Open	Open address conflict logging	
Apply	Apply the currently selected configuration to the switch to make the		
	configuration effective		

Information feedback window				
DHCP server status	Conflict logging status			
Close	Open			

DHCP server status	Close	se The current DHCP server is off		
	Open	The current DHCP server is on		
Conflict logging status	Close	The current address conflict log is off		
	Open	The current address conflict log is open		

13.2. DHCP server configuration

13.2.1. Dynamic pool configuration

13.2.1.1. Dynamic address pool configuration

Switch DHCP address pool configuration, the user configures the DHCP address pool parameters.

DHCP IP address pool co	nfiguration	
DHCP pool name	~	
DHCP pool domain name		
Address range	IP address:	
	Network mask:	
DHCP client node type	b-node 🗸	
	○Infinite	
	Day:	
Address lease timeout	Hour:	
	Minute:	
Operation	Add 🗸	
	Apply	

DHCP pool name	The name of the created address pool		
DHCP pool domain name	The domain name of the currently selected address pool. After configuration, you need to tick the box at the back to apply the domain name to the switch		
	ID addross Notwork number of the addross need		
Address range	IP address	Network number of the address pool	
	Network mask	Netmask of the address pool	
DHCP client node	b-node	Broadcast node	
type	p-node	For point-to-point nodes	
	m-node	Used for hybrid nodes to perform point-to-point	
		communication after broadcasting	
	h-node	Hybrid nodes that broadcast after peer-to-peer	
		communication	
	Designate	Hexadecimal node type, from 0 to 255	
Address lease	Infinite	The lease period of the address is unlimited, and the number	
timeout		of days/hours/minutes below do not need to be filled in	
	Specified	There is a time limit for the lease of the address. You can rent it	
	-	according to the lease time filled in below, and it will be	
		automatically recovered if the time is exceeded	
Operation	add	Add the above four parameters with check boxes to the switch,	
		the parameters without check boxes will not be operated	
	remove	Restore the four parameters with check boxes to the default	
		configuration, and the parameters without check boxes will not	
		be operated	

Information feedback window	
Switch# show ip dhcp pool config	
dhcp pool 1	
Lease day:1, hour: 0, minute	:0

Information display of the currently configured address pool

13.2.1.2. Client's default gateway configuration

The switch DHCP client default gateway configuration, the user configures the gateway parameters of the DHCP address pool.

Client's default gatew	ay co	onfigu	ırati	on	
DHCP pool name	1 🗸				
Gateway 0					
Gateway 1					
Gateway 2					
Gateway 3					
Gateway 4					
Gateway 5					
Gateway 6					
Gateway 7					
Operation	Add	~			
				Ag	oply

DHCP pool name	The name of the create	d address pool
Gateway0-7	Gateway IP address in dotted decimal format. Gateway 0 has the highest priority. The smaller the number, the higher the priority. The gateway can be set to zero or more, but the setting must start with 0 and no vacancies can appear in the middle, otherwise the gateway will be Ignore the following parameters, such as setting gateway 0-1 and gateway 7 only gateway 0-1 takes effect	
Operation	Add Remove	Add the gateway effectively set above to the currently selected DHCP address pool Clear all gateways and restore to the default state

```
Information feedback window
Switch# config t
Switch(config)# ip dhcp pool 1
Switch(dhcp-1-config)# default-router 1.1.1.1
```

Information display after application

13.2.1.3. Client DNS server configuration

The switch DHCP client DNS server configuration, the user configures the DNS server parameters of the DHCP address pool.

Client DNS server con	figura	ation		
DHCP pool name	1 🗸			
DNS server 0	1.1.1	. 1		
DNS server 1				
DNS server 2				
DNS server 3				
DNS server 4				
DNS server 5				
DNS server 6				
DNS server 7				
Operation	Add	~		
			Ar	oply

DHCP pool name	The name of th	ne created address pool	
DNS server 0-7	For the IP addr priority. The sn set to zero or n vacancies in the will be ignored server 0-1 take	For the IP address in dotted decimal format, DNS server 0 has the highest priority. The smaller the number, the higher the priority. The DNS server can be set to zero or more, but the setting must start from 0 and there can be no vacancies in the middle, otherwise the DNS server The following parameters will be ignored, such as setting DNS server 0-1 and DNS server 7, only DNS	
Operation	Add Remove	Add the DNS server effectively set above to the currently selected DHCP address pool Clear all DNS servers and restore to the default state	

```
Information feedback window
Switch# config t
Switch(config)# ip dhcp pool 1
Switch(dhcp-1-config)# dns-server 1.1.1.1
```

```
Information display after application
```

13.2.1.4. Client WINS server configuration

The switch DHCP client WINS server configuration, the user configures the WINS server parameters of the DHCP address pool.

Client WINS server co	nfigu	Iratio	n		
DHCP pool name	1 🗸				
WINS server 0					
WINS server 1					
WINS server 2					
WINS server 3					
WINS server 4					
WINS server 5					
WINS server 6					
WINS server 7					
Operation	Add	~			
				Ap	oply

DHCP pool name	The name of th	ne created address pool	
WINS server 0-7	The WINS serve highest priority can be set to ze vacancies in the parameters, su 0-1 takes effect	The WINS server IP address in dotted decimal format. WINS server 0 has the highest priority. The smaller the number, the higher the priority. The WINS server can be set to zero or more, but the setting must start from 0 and there can be no vacancies in the middle, otherwise WINS server will ignore the following parameters, such as setting WINS server 0-1 and WINS server 7, only WINS server 0.1 teles affect	
Operation	Add	Add the WINS server effectively set above to the currently selected DHCP address pool	
	Remove	Clear all WINS servers and restore them to the default state	

Information feedback window Switch# config t Switch(config)# ip dhcp pool 1 Switch(dhcp-1-config)# netbios-name-server 1.1.1.1

Information display after application

13.2.1.5. DHCP file server address configuration

The switch client import file stores the address configuration, and the user configures the parameters of the DHCP address pool client import file.

DHCP file server address o	onfig	juratior	ı	
DHCP pool name	1 🗸			
DHCP client bootfile name	123.	cfg		
File server 0	1.1.	1.1		
File server 1				
File server 2				
File server 3				
File server 4				
File server 5				
File server 6				
File server 7				
Operation	Add			~
			Ap	oply

DHCP pool name	The name o	of the created address pool		
DHCP client	Specify the	name of the file to be imported for the client. Usually used for		
bootfile name	diskless wor	kstations, these workstations need to download configuration files		
	from the se	rver at startup.		
File server 0-7	The IP address in dotted decimal format has the highest priority for importing			
	file server 0. The smaller the number, the higher the priority. The importing file			
	server can be set to zero or more, but the setting must start from 0 and there			
	should be n	be no vacancies in the middle, otherwise Importing file server will ignore		
	the followin	ng parameters, such as setting import file server 0-1 and import file		
	server 7, on	nly import file server 0-1 takes effect		
Operation	Add	Add the imported file server effectively set above to the currently		
		selected DHCP address pool		
	Remove	Clear all imported file servers and restore to the default state		

Information feedback window
Switch# config t
Switch(config)# ip dhcp pool 1
Switch(dhcp-1-config) # bootfile 123.cfg
Switch# config t
Switch(config)# ip dhcp pool 1
Switch(dhcp-1-config) # next-server 1.1.1.1

Information display after application

13.2.1.6. DHCP network parameter configuration

Switch network parameter configuration, the user configures the network parameters of the DHCP address pool.

DHCP network parameter configuration				
DHCP pool name	1 🗸	'		
Code				
Network parameter value type	IP ADDRESS 🗸			
Network parameter value(ASCII,HEX or IP)				
Operation type	Add	~		
			Apply	

DHCP pool name	The name of	the created address pool		
Code	The code range of network parameters is 0-254, and each code corresponds to a different function in DHCP. The definition of option codes is described in detail in RFC2123.			
Network parameter	There are three types of network parameter values: ASCII, HEX, and IP			
value type	ADDRESS.			
Network parameter	ASCII string, up to 255 characters;			
value (ASCII, HEX	Hexadecimal value, not greater than 510, and must be an even number;			
or IP)	IP address in decimal format, up to 63 IP addresses can be configured.			
Operation	Add	Add the network parameters of the selected address pool to		
		the switch		
	Remove	Clear the network parameters filled in the selected address		
		pool (delete according to the code of the network parameter)		

```
Information feedback window
Switch# config t
Switch(config)# ip dhcp pool 1
Switch(dhcp-1-config)# option 82 ip 192.168.2.1
DHCPD: Option 82 has been added to pool 1
```

Information display after application

13.2.1.7. Excluded address configuration

Excluding the dynamic allocation address configuration, the user configures the addresses that are not used for dynamic allocation

Address allocation configuration			
Starting address			
Ending address			
Operation type	Add	~	
			Apply

Starting address	Start address not used for dynamic allocation		
Ending address	End address not used for dynamic allocation		
Operation type	Add	Add the address range that is not used and dynamically allocated to the switch	
	Remove	Delete the address range that is not used and dynamically allocated from the switch	

Address list	
Starting address	Ending address
1.1.1.1	1.1.1.25
end o	f list

Display the address range currently not used for dynamic allocation

13.2.2. Manual DHCP IP pool configuration

13.2.2.1. Static address pool configuration

Switch static address pool configuration, and manually bind client parameters.

Hardware address	
DHCP pool name	1 🗸
Parameter choose	ethernet 🗸
Hardware address	00-11-22-33-44-55
Operation	Add 🗸
	Apply

DHCP pool name	The name o	The name of the created address pool		
Parameter choose	The protocol type used by the client is rfc\ethernet\ieee802.			
	RFC ID: RFC	RFC ID: RFC protocol number, valid range is 1-255.		
Hardware address	Hardware address			
Operation	Add Add manually bound hardware address and protocol type			
	Remove Remove the manually bound hardware address and protocol type			

Client pool configuration			
Client pool configuration	1		
Client IP address			
Client network mask			
Operation	Add	~	
			Apply

Client pool	The name of the created address pool (modify the selection through the		
configuration	address pool name of the user's hardware address)		
Client IP address	IP address assigned by the DHCP server to the client		
Client network mask	The subnet mask assigned by the DHCP server to the client IP		
Operation	Add Add manually bound IP address and subnet mask		
	Remove Delete the manually bound IP address and subnet mask		

User name						
DHCP pool name	1					
User						
Client identifier						
Operation	Add	~				
				Appl	у	

DHCP pool name	The name of the created address pool (modify the selection through the					
	address pool	address pool name of the user's hardware address)				
user	Client user na	ime				
Client identifier	The identifier of the client, for example: 44-11-22-33-44-55 (MAC address)					
Operation	Add Add manually bound client identifier and user name					
	Remove	Delete the manually bound client identifier and user name				

13.2.3. Address pool name configuration

DHCP server address pool name configuration, user settings add and delete the address pool name.

Address pool name configuration					
DHCP pool name					
Operation type	Add pool 🗸 🗸				
	Apply				

DHCP pool name	The name of the created address pool				
Operation type	Add pool Add the address pool of the DHCP server				
	Remove poolDelete the address pool of the DHCP server				

Info	Information feedback window							
Swit	Switch# show ip dhcp pool config							
dhcp	dhcp pool 1							
	Leas	e d	ay:1,	hou	1 r: (0, m	inute	:0

Display the address pool of the current DHCP server

13.2.4. DHCP packet statistics

DHCP server data packet statistics, users can view DHCP data packets.

DHCP packet statistics							
Address poo	l numbe	r			1		
Proxy datab	xy database						
Dynamical a	Dynamical assignment address						
Manual bind	ed addre	ess			0		
Address con	flict				0		
Binding exce	eeding le	as	e time		0		
Errors					0		
Received DH	ICP pack	et	statistics	;			
Received					0		
DHCP DISCOVER					0		
DHCP REQUEST					0		
DHCP DECLINE					0		
DHCP RELEA		0					
DHCP INFORM					0		
Transmitted DHCP packet statistics							
Transmitted					0		
DHCP OFFE	ર				0		
DHCP АСК					0		
DHCP NAK					0		
DHCP RELAY					0		
DHCP FORWARD 0					0		
Clear Show							

It can be viewed in real time by clicking "Clear" and "Show"

13.3. DHCP relay configuration

13.3.1. DHCP relay configuration

The switch DHCP relay configuration, the user configures the port range, and the switch sends UDP broadcast messages to the port.

DHCP forward UDP configuration			Port
Range			67
Operation	Add 🗸		
		Apply	

Range	Port used by DHCP to forward UDP packets				
Operation	Add Add the port used by DHCP to forward UDP packets				
	Remove	Delete the port through which DHCP forwards UDP packets			

DHCP help-address configuration						
IP address						
L3 Interface	Vlan1 🗸					
Operation	Add 🗸					
	Apply					

IP address	L3 Interface		
192.168.2.1	Vlan1		

IP address	IP addres	IP address of the Layer 3 interface				
L3 Interface	Establish	Established Layer 3 interface				
Operation	Add	Add a Layer 3 interface for DHCP to forward UDP packets				
	Remove	Delete the Layer 3 interface through which DHCP forwards UDP packets				

13.4. DHCP debugging

13.4.1. Delete record

13.4.1.1. Delete binding log

DHCP binding record deletion, users can delete all binding records or delete specified binding records, static binding records need to be deleted in the static address pool configuration.

Delete DHCP binding log								
Delete binding area	Delete	all	binding	lo	g 🗸			
IP Address								
					Apply			

Delete binding area	Delete all	Delete all binding records, no need to fill in the IP
	binding log	address below
	Delete specify	Delete the specified binding record, fill in the deleted IP
	binding log	in the IP address below
IP Address	IP address in dotted decimal notation	

13.4.1.2. Delete conflict log

The DHCP conflict record is deleted, and the user can delete all conflict records or delete the specified conflict record.

Delete conflict log					
Delete conflict address area	Delete	all	conflict	lo	g 🗸
IP Address					
					Apply

Delete conflict log	Delete all conflict log	Delete all conflict records, no need to fill in the IP address below
	Delete specify binding log	Delete the specified conflict record, fill in the deleted IP in the IP address below
IP Address	IP address in dotted decimal no	otation

13.4.1.3. Delete DHCP server statistics log

Deleting the statistics records of the DHCP server, the user can delete all the statistics records of the DHCP server.

Delete DHCP server statistics log
Apply

After deleting the statistical record of the DHCP server, the statistical information of the DHCP packet will be cleared

13.4.2. Show IP-MAC binding

The DHCP server's IP and MAC binding status, the user can view the binding entries and the relationship between the bound IP and MAC.

```
Information feedback window
Switch# clear ip dhcp server statistics
Switch# show ip dhcp binding
Total dhcp binding items: 0, the matched: 0
IP address Hardware address Lease expiration Type
```

IP address	Client's IP address		
Hardware address	The hardware address or MAC address of the client		
Lease expiration	Client IP expiration time		
Туре	Manual Manual binding		
	Dynamic Dynamic allocation		

13.4.3. Show conflict-logging

The conflict record of the DHCP server, the user can view the conflict situation.

```
Information feedback window
Switch# show ip dhcp conflict
IP Address Detection method Detection Time
```

Display info	Description
IP Address	Conflicting IP address.
Detection method	The conflicting method was detected.
Detection Time	The time when the conflict was detected.

14. DHCP Snooping configuration

14.1. DHCP Snooping global configuration

14.1.1. Enable/Disable DHCP Snooping

With the enabling and disabling of the DHCP Snooping module, users can view and operate the status of DHCP Snooping.

Enable/Disable DHCP Snooping				
DHCP Snooping status Disable 🗸				
		Арр	ly	

DHCP Snooping	Disable	Disable DHCP Snooping
status	Enable	Enable DHCP Snooping

Information feedback window	
DHCP Snooping status	Enable

Display the current DHCP Snooping status

14.1.2. DHCP Snooping binding configuration

When DHCP Snooping binding is enabled and disabled, users can view and operate the status of DHCP Snooping. When configuring this binding, users must ensure that the binding status is in the on state.

Enable/Disable DHCP Snooping binding				
DHCP Snooping binding status Disable 🗸				
		Apply		

DHCP Snooping	Disable	Disable DHCP Snooping binding function
binding status	Enable	Enable DHCP Snooping binding function

Information feedback window
DHCP Snooping binding status
Disable

Shows whether the current DHCP Snooping binding status function is enabled.

14.1.3. DHCP Snooping binding user configuration

When DHCP Snooping binding is enabled and disabled, users can view and operate the status of DHCP Snooping. When configuring this binding, users must ensure that the binding status is in the on state.

DHCP Snooping binding user configuration				
MAC address				
User IP address				
User mask				
VLAN ID				
Port	Ethernet1	/0/1	~	
Operation	Add 🗸			
			Apply	

MAC address	The MAC address of the statically bound user is the only index of the bound user		
User IP address	Statically bind the user's IP address		
User mask	Statically bind the user's subnet mask		
VLAN ID	Statically bind the VLAN ID of the user		
Port	Bind the user's access port statically, the port is associated with the VLAN ID, and		
	the port is required to allow the VLAN to pass		
Operation	Add Add DHCP Snooping binding user relationship		
	Remove Delete DHCP Snooping binding user relationship		

Information feedback window	
Switch# config t	
Switch(config)# no Ip dhcp snooping binding user 00-22-33-44-55-66 interface Ethernet1/0/1 vlar	1
Please enable dhcp snooping binding in global first!	

Display the process and error messages or results generated during application execution

14.1.4. DHCP Snooping action count config

DHCP Snooping defense action number configuration, if the number of alarm messages is greater than the set number, it will force the restoration of the earliest defense measures to send new defense measures.

DHCP Snooping action count config				
DHCP Snooping action count				
Operation	Add	\sim		
			Apply	

DHCP Snooping	Set the maximum number of defense actions to avoid exhaustion of switch			
action count	resources caused by attacks.			
Operation	Add	Configure the number of defense actions filled in above		
	Remove	Reduce the number of defense actions to 10		

Information feedback window	
DHCP Snooping action count	10

Display the current number of DHCP Snooping defense actions

14.1.5. DHCP Snooping limit-rata config

DHCP Snooping packet receiving rate limit sets the number of DHCP messages sent per second.

DHCP Snooping limit-rate config				
Packet per second				
Operation	Add	~		
				Apply

Packet per second	Range: 0-100			
Operation	Add Configure the number of packets per second			
	Remove	Restore the default number of packets per second, the default is 100		

Information feedback window Packet per second 100

Display the number of packets per second configured for the current DHCP Snooping.

14.1.6. DHCP Snooping helper-server config

DHCP SNOOPING will send the monitored binding information to HELPER SERVER for storage. If the switch starts abnormally, you can recover the bound data from the HELPER SERVER

DHCP Snooping helper-server config				
Helper-server address				
Helper-server UDP port				
Local IP address				
Second address			\sim	•
Operation	Add	~		
				Apply

Helper-server address	HELPER server address		
Helper-server UDP port	DHCP SNOOPING and HELPER SERVER use UDP protocol for		
	communicatio	on, the port range is 1-65535.	
Local IP address	The effective	management IP address of the switch	
Second address	Two HELPER s	server addresses are allowed, DHCP SNOOPING will first try	
	to connect to	the PRIMARY server. Only when the PRIMARY server	
	cannot be accessed, the switch HELPER server will connect to the		
	SECONDARY server. Set the PRIMARY server before setting up the		
	SECONDARY server.		
Operation	Add Add HELPER server address		
	Remove Delete the HELPER server address, you can leave it blank		
		when deleting	

Information feedback window	
Switch# config t	
Switch(config)# no ip user helper-address	

Display the process and error messages or results generated during application execution

14.2. DHCP Snooping port configuration

14.2.1. Enable/Disable DHCP Snooping binding dot1x

DHCP SNOOPING will notify the DOT1X module of the binding information captured by the user controlled by the DOT1X. DHCP Snooping port binding dot1x function needs to enable DHCP Snooping binding configuration first.

Enable/Disable DHCP Snooping binding dot1x			
Port DHCP Snooping binding dot1x status			Lx status
Ethernet1/0/1 🗸	Enable 🗸		
			Apply

Port	Port name	
DHCP Snooping	Enable	Enable the dot1x status of DHCP Snooping port binding
binding dot1x status	Disable	Disable the dot1x binding status of the DHCP Snooping port

Information feedback window				
Port	DHCP Snooping binding dot1x status			
Ethernet1/0/1	Disable			
Ethernet1/0/2	Disable			
Ethernet1/0/3	Disable			
Ethernet1/0/4	Disable			
Ethernet1/0/5	Disable			
Ethernet1/0/6	Disable			
Ethernet1/0/7	Disable			
Ethernet1/0/8	Disable			

Display the dot1x binding status of each DHCP Snooping port of the switch

14.2.2. Enable/Disable DHCP Snooping binding user

When this function is enabled on the port, DHCP SNOOPING will treat the captured binding information as a trusted user who is allowed to access all resources. The DHCP Snooping port binding user status function needs to enable the DHCP Snooping binding configuration first.

Enable/Disable DHCP Snooping binding user						
Port	DHCP Snooping binding user status					
Ethernet1/0/1 🗸	Enable 🗸					
					Apply	

Port	Port name	
DHCP Snooping	Enable	Enable DHCP Snooping port binding user status
binding user status	Disable	Disable DHCP Snooping port binding user status

Information fee	Information feedback window					
Port	DHCP Snooping binding user status					
Ethernet1/0/1	Disable					
Ethernet1/0/2	Disable					
Ethernet1/0/3	Disable					
Ethernet1/0/4	Disable					
Ethernet1/0/5	Disable					
Ethernet1/0/6	Disable					
Ethernet1/0/7	Disable					
Ethernet1/0/8	Disable					

Display the status of users bound to each DHCP Snooping port of the switch

14.2.3. Enable/Disable DHCP Snooping trust

When a port changes from an untrusted port to a trusted port, the original defense action of the port will be automatically deleted; all security history records will be cleared.

Enable/Disable DHCP Snooping trust					
Port	DHCP Snooping binding trust status				
Ethernet1/0/1 🗸	Enable 🗸]			
					Apply

Port	Port name	
DHCP Snooping	Enable	Enable DHCP Snooping port trust attribute status
binding trust status	Disable	Disable the trust attribute status of the DHCP Snooping port

Information feedback window					
Port	DHCP Snooping binding trust status				
Ethernet1/0/1	Disable				
Ethernet1/0/2	Disable				
Ethernet1/0/3	Disable				
Ethernet1/0/4	Disable				
Ethernet1/0/5	Disable				
Ethernet1/0/6	Disable				
Ethernet1/0/7	Disable				
Ethernet1/0/8	Disable				

Display the trust attribute status of each DHCP Snooping port of the switch

14.2.4. DHCP Snooping action config

Automatic port defense action, the port will detect the fake DHCP server, and the trusted port will not detect the fake DHCP server, so the corresponding defense action will never be triggered. When a port changes from an untrusted port to a trusted port, the original defense action of the port will be automatically deleted;

DHCP Snooping action config					
Port	Etherne	et1	/0/1 🗸		
DHCP Snooping action	shutdown 🗸				
DHCP Snooping recovery time					
Operation	Add	\sim			
			Apply		

Port	Port name	
DHCP Snooping	shutdown	Automatically close the port
action	blackhole	Block traffic from fake DHCP server based on MAC
DHCP Snooping	The user can set	the recovery after performing automatic defense operations
recovery time		
Operation	Add	Add DHCP Snooping port automatic defense configuration
	Remove	Delete DHCP Snooping port automatic defense configuration

Information feedback window					
Port	DHCP Snooping action	DHCP Snooping recovery time			
Ethernet1/0/1	none	0			
Ethernet1/0/2	none	0			
Ethernet1/0/3	none	0			
Ethernet1/0/4	none	0			
Ethernet1/0/5	none	0			
Ethernet1/0/6	none	0			
Ethernet1/0/7	none	0			
Ethernet1/0/8	none	0			

Display the automatic defense configuration of each DHCP Snooping port

14.3. Show DHCP snooping configuration

14.3.1. Show DHCP snooping configuration

Display detailed configuration of DHCP Snooping

Show DHCP Snooping configuration	
DHCP Snooping show object	~
	Apply

DHCP Snooping All		All ports are displayed
show object	Ethernet1/0/1-28	Only display information about one port

Information feedback window Switch# show ip dhcp snooping interface Ethernet1/0/1 interface Ethernet1/0/1 user config: trust attribute: untrust action: none binding dot1x: disabled binding user: disabled binding mab guard: disabled recovery interval:0(s) Driver user number 0 : Max user number 1024 Alarm info: 0 Binding info: 0 Static Binding info: 0 Static Binding info from shell: 0 Static Binding info from server: 0 flag: D - Dynamic ; U - already upload server ; S - static binding info from shell; R - static binding info from server; O - dhcp ack has option82; X - notify dot1x ok; L - notify driver ok; E - notify dot1x error P - binding protect; Expired Binding: 0 Request Binding: 0

Select Ethernet1/0/1, only display the DHCP Snooping information of Ethernet1/0/1

15. SNTP configuration

15.1. SNTP server configuration

SNTP the server settings module, the user can add or delete the specified time server as the clock source.

SNTP server and version configuration						
Server address						
Version						
Operation	Add	~				
					Ар	ply

Information feedback window		
SW1# config t		
SW1(config) # show sntp		
server address	version	last receive

Server address	The specified time server address decimal point		
Version	Version number, range 1-4, default 4		
Operation	Add	Add operations	
	Remove	Delete operations	
15.2. Request interval configuration

Send request interval setting module, where the user can set the interval SNTP the client sends a request to the NTP/SNTP. By default, the interval is 64 seconds.

Request interval from SNTP client to SNTP serve					
Interval					
Operation	Configurati	on 🗸			
			Apply		
Interval					
Interval		64			

Interval	Duration value, range 16-16284 s	
Operation	Configuration Configuration operations	
	Default Do recovery default (default 64 s)	

15.3. Time difference configuration

SNTP the time zone and UTC time difference setting module where the client is located, the user can set the switch's current time zone and name it.

Time difference configuration				
Time zone				
Time difference	● After-utc ○ Before	-utc		
Time value				
Operation	Add 🗸			
			Apply	

Time zone	Time zone name ,1-16 characters	
Time	Add	Increased time zone behavior
difference	reduce	Reduced time zone behavior
Time value	Time zone specific change hours 0-23	Time zone specific change minute value 0-59
Operation	Add	Add operations
	Remove	Delete operations

15.4. Show sntp

Display SNTP module, where users can view the current information status SNTP the switch.

Information feedback window		
SW1# config t		
SW1(config) # show sntp		
server address	version	last receive

16. NTP configuration

16.1. NTP global configuration

16.1.1. NTP global switch configuration

NTP service global switch configuration module, user can NTP service global switch operation.

NTP global switch co	nfiguration			
Operation	Disable 🗸		NTP global switch configuration	
		Apply	NTP global configuration	disable

Operation	Disable	Close operation
	Enable	Start (default)

16.1.2. NTP server configuration

NTP the server configuration module, the user can configure the specified time server of the switch time source in this module.

NTP server and v	ersion configuration
Server address	
Version	
Key	Information feedback window
Operation	Add V SW1# config t
	Apply ntp peer doesn't exist!

Server address	The specified time server address decimal point		
Version	Version number, range 1-4, default 4		
Кеу	Secret key value, range 1-4294967295		
Operation	Add Add operations		
	Remove Delete operations		

16.1.3. NTP broadcast or multicast address count configuration

NTP service address number configuration module, the user can configure the maximum number of broadcast or multicast servers supported by the switch NTP client.

NTP broadcast or multicast address count configuration					
Address max count					
Operation	Add	~			
					Apply
Address max count					
Address max count			50		

Address max count	Maximum number of broadcast or multicast servers supported			
	NTP clients ,1-100(default 50)			
Operation	Add Add operations			
	Remove Delete operations			

16.1.4. NTP access group configuration

NTP access control list configuration module, where users can configure switch NTP access control list.

NTP access group configuration					
Access list					
Operation	Add	~			
		Apply			

Access list	IPv4:1-99; IPv6: 50-599		
Operation	Add Add operations		
	Remove	Delete operations	

16.1.5. NTP authenticate configuration

NTP verification configuration module, the user can configure the switch NTP authentication related items.

NTP authenticate configuration				
NTP authenticate switch	Disable 🗸			
Key type	none	~		
Кеу				
MD5				
Operation	Add 🗸			
		Apply		

NTP authenticate	Disable	Close NTP validation (default)		
switch	Enable	Enable NTP validation		
Key type	none	none		
	authentication-key	Authentication secret key		
	trusted-key	Trust key		
Кеу	Secret key value, range	ey value, range 1-4294967295		
Md5	The MD5 value of the secret key, which ranges from 1-16 of ascii code			
Operation	Add	Add operations		
	Remove	Delete operations		

16.2. NTP interface configuration

16.2.1. NTP interface switch configuration

NTP service interface switch configuration module, the user can specify the NTP service interface switch operation.

NTP interface configuration				
VLAN interface	Vlan1 🗸			
NTP interface configuration	Disable 🗸			
NTP interface client	none	~		
		Apply		

VLAN interface	VLAN1	VLAN interface for current switch configurable		
NTP interface	Disable	Close operation		
configuration	Enable	Start-up operation		
NTP interface client	none			
	broadcast			
	no broadcast			
	multicast	Interface NTP client type		
	no multicast			
	ipv6 multicast			
	no ipv6 multicast			

16.3. NTP configuration display

16.3.1. NTP status display

NTP status display module, where users can view NTP service current status information.



17. QOS configuration

17.1. QOS port configuration

17.1.1. QOS port trust state configuration

Configure port trust rules

QoS port trust state configuration						
Port	Ethernet1/0/1 🗸					
Packet class rule	COS	~				
Operation Add 🗸						
						Apply

Port	To configure the port name, click to expand the remaining ports			
Packet class rule	COS	COS Cos to int mapping based on intp field		
	DSCP Intp field based on dscp to intp mapping			
Operation	add	Add a trust rule for the port		
	Remove Remove a trust rule for the port			

Information feedback window				
Port	Trust class			
Ethernet1/0/1	cos			
Ethernet1/0/2	COS			
Ethernet1/0/3	COS			
Ethernet1/0/4	COS			
Ethernet1/0/5	COS			
Ethernet1/0/6	COS			
Ethernet1/0/7	COS			
Ethernet1/0/8	COS			

17.1.2. QOS port COS parameters configuration

Configure the COS value of the port, regardless of whether the trust rule of the current port is trusted

QoS port cos parameters configuration					
Port	Ether	net1	/0/1	~	
Port related COS value					
Operation	Add	~			
				Арр	ly

Port	To configure the port name, click to expand the remaining ports		
Port related COS value	The default COS value of the port, range: 0-7		
Operation	Add Add the COS value of the port		
	Remove Delete the COS value of the port and restore it to 0		

Information feedback window					
Port	Port related COS value				
Ethernet1/0/1	0				
Ethernet1/0/2	0				
Ethernet1/0/3	0				
Ethernet1/0/4	0				
Ethernet1/0/5	0				
Ethernet1/0/6	0				
Ethernet1/0/7	0				
Ethernet1/0/8	0				

17.1.3. QOS port select queue schedule algorithm configuration

Configure the port to process the priority of packets according to different queue scheduling algorithms

QoS port select queue schedule algorithm configuration				
Port	Ethernet1/0/1 🗸			
Queue schedule algorithm	sp 🗸			
	Apply			

Port	To configure the port name, click to expand the remaining ports			
Queue	sp	Strict queuing priority, packet transmission in order of priority.		
schedule	wrr	vrr Weighted round-robin scheduling. Rotate scheduling between queues to		
algorithm		ensure that each queue gets a certain amount of service time		

۱. ۱	wdrr	Weighted difference round-robin scheduling, based on message length
		transmission, based on the combined effect of weight and K value to
		generate the length of transmission in the message queue

Information feedback window			
Port	Trust class		
Ethernet1/0/1	sp		
Ethernet1/0/2	wdrr		
Ethernet1/0/3	wrr		
Ethernet1/0/4	wrr		
Ethernet1/0/5	wrr		
Ethernet1/0/6	wrr		
Ethernet1/0/7	wrr		
Ethernet1/0/8	wrr		

Display the queue scheduling algorithm trusted by the current port

17.1.4. QOS port wrr algorithm queue weight configuration

Configure the weight value of the eight queues of each port, and allocate the number of packets according to the weight value

QoS port wrr algor	QoS port wrr algorithm queue weight configuratior				
Port	Ethernet1	/0/1 🗸			
Weight1					
Weight2					
Weight3					
Weight4					
Weight5					
Weight6					
Weight7					
Weight8					
Operation	Add 🗸				
				Apply	

Port	To configure the port name, click to expand the remaining ports			
Weight1	The weight value of queue 1, the range is 0-127			
Weight2	The weight value of queue 2, the range is 0-127			
Weight3	The weight value of queue 3, the range is 0-127			
Weight4	The weight value of que	eue 4, the range is 0-127		
Weight5	The weight value of queue 5, the range is 0-127			
Weight6	The weight value of queue 6, the range is 0-127			
Weight7	The weight value of queue 7, the range is 0-127			
Weight8	The weight value of queue 8, the range is 0-127			
	۸dd	Add the weight of each queue to the port, and fill in all		
Owenetien	Add	the weights of each queue before adding		
Operation	Pomovo	To restore the weight of each queue of the port to the		
	Reniove	default, you need to add the value of eight queues		

Information feedback window				
Port	Queue weight			
Ethernet1/0/1	1 2 3 4 5 6 7 8			
Ethernet1/0/2	12345678			
Ethernet1/0/3	12345678			
Ethernet1/0/4	1 2 3 4 5 6 7 8			
Ethernet1/0/5	12345678			
Ethernet1/0/6	1 2 3 4 5 6 7 8			
Ethernet1/0/7	1 2 3 4 5 6 7 8			
Ethernet1/0/8	12345678			

Information feedback window

17.1.5. QOS port wdrr algorithm queue weight configuration

Configure the weight value of the eight queues of each port, transmit based on the length of the message, and generate the transmission length in the message queue based on the combined action of the weight and the K value

QoS port v	wrr algorith	m qu	eue	weight	config	guration
Port	Ethernet1/0	/1 ~]			
Weight1						
Weight2						
Weight3						
Weight4						
Weight5						
Weight6]		
Weight7						
Weight8						
Operation	Add 🗸					
						Apply

Port	To configure the port name, click to expand the remaining ports			
Weight1	The weight val	The weight value of queue 1, the range is 0-32767		
Weight2	The weight val	ue of queue 2, the range is 0-32767		
Weight3	The weight val	ue of queue 3, the range is 0-32767		
Weight4	The weight val	ue of queue 4, the range is 0-32767		
Weight5	The weight val	ue of queue 5, the range is 0-32767		
Weight6	The weight value of queue 6, the range is 0-32767			
Weight7	The weight value of queue 7, the range is 0-32767			
Weight8	The weight value of queue 8, the range is 0-32767			
Operation	Add Add the weight of each queue to the port, and fill in all the weights of			
		each queue before adding		
	Remove	To restore the weight of each queue of the port to the default, you		
		need to add the value of eight queues		

17.1.6. QOS service policy configuration

Configure the port's policy table, and the port will process packets according to the rules of the classification table in the policy table.

QoS service policy configuration				
Port	Ethernet1/0/1 🗸			
Policy map name				
Operation	Add 🗸			
		Apply		

Port	To configure the port name, click to expand the remaining ports			
Policy map name	The name of the policy table, added by the policy table configuration			
Operation	Add policy for adding ports			
	Remove Delete port policy			

17.2. QOS class-map configuration

17.2.1. Class map-configuration

Create and delete classification tables, view the currently configured classification tables

Class map-configuration				
Class-map name				
Operation	Add	~		
				Apply

Class-map name	Class-map name, range:1-64 character			
Operation	Add	Add Class-map		
	Remove	Remove Class-map		

Information feedback window	
Class-map name	1

Display the currently created class-map name

17.2.2. Classification criteria configuration

Set the rules and corresponding parameters for classification matching

Classification criteria configuration							
Classification criteria rule	e access-group 🗸 🗸						
Class-map name	1 🗸						
ACL list name							
Operation	Add	``	~				
					App	ply	

Classification	accesss-group	Sss-group Match the specified IP ACL, MAC ACL or IPv6 standard			
criteria rule		ACL or MAC-IP ACL			
Class-map name	The name of the creat	The name of the created class-matching table, select by clicking the drop-down			
ACL list name	Created ACL name, 1-0	Created ACL name, 1-64 characters			
Operation	Add	Add matching rules			
	Remove	Remove matching rules			

Classification criteria conf	fig	ura	ati	on		
Classification criteria rule	i	p d	sc	p	\sim	
Class-map name	1	\sim				
IP dscp0						
IP dscp1						
IP dscp2						
IP dscp3						
IP dscp4						
IP dscp5						
IP dscp6						
IP dscp7						
Operation	A	dd		\sim		
					Ap	ply

Classification	ip dscp	Match the specified DSCP value, this parameter is				
criteria rule	the DSCP list					
Class-map name	The name of the created c	ass-matching table, select by clicking the drop-down				
IP dscp0-7	One or more DSCP values can be set, up to 8 DSCP values can be set, the range is					
	0~63;					
Operation	Add	Add matching rules				
	Remove	Remove matching rules				

Classification criteria conf	Classification criteria configuration							
Classification criteria rule	ip p	preced	lence	~				
Class-map name	1 🗸							
IP precedence0								
IP precedence1								
IP precedence2								
IP precedence3								
IP precedence4								
IP precedence5								
IP precedence6								
IP precedence7								
Operation	Add	~						
				App	oly			

Classification	ip precedence	Match the specified ip priority, this parameter is the IP					
criteria rule		priority list					
Class-map name	The name of the cr	The name of the created class-matching table, select by clicking the drop-down					
IP precedence0-7	One or more ip priority values can be set, the list contains up to 8 IP priority						
	values, and the valid range is 0~7;						
Operation	Add	Add matching rules					
	Remove	Remove matching rules					

Classification criteria conf	Classification criteria configuration						
Classification criteria rule	vlan				`	/	
Class-map name	1 🗸						
Vlan0							
Vlan1							
Vlan2							
Vlan3							
Vlan4							
Vlan5							
Vlan6							
Vlan7							
Operation	Add	`	~				
					A	pp	ly

Classification criteria rule	vlan	Match the specified vlan, this parameter is a list of vlan id				
Class-map name	The name o	f the created class-matching table, select by clicking the drop-				
	down	own				
Vlan0-7	One or more	One or more VLAN IDs can be set, including 8 VLAN IDs at most, ranging				
	from 1 to 40)94				
Operation	Add	Add matching rules				
	Remove	Remove matching rules				

Classification criteria configuration							
Classification criteria rule	cos			~			
Class-map name	1 🗸						
Cos0							
Cos1							
Cos2							
Cos3							
Cos4							
Cos5							
Cos6							
Cos7							
Operation	Add	~					
				App	oly		

Classification	COS	Match the specified CoS value, this parameter is a list of vlan id					
criteria rule							
Class-map name	The name of th	ne created class-matching table, select by clicking the drop-down					
Cos 0-7	One or more co	One or more cos values can be set, the parameter is a CoS list composed of up					
	to 8 CoS, the ra	to 8 CoS, the range is 0~7;					
Operation	Add	Add matching rules					
	Remove	Remove matching rules					

Classification criteria conf	Classification criteria configuration						
Classification criteria rule	ipv6	dscp		~			
Class-map name	1 🗸						
IPv6 dscp0							
IPv6 dscp1							
IPv6 dscp2							
IPv6 dscp3							
IPv6 dscp4							
IPv6 dscp5							
IPv6 dscp6							
IPv6 dscp7							
Operation	Add	~					
				App	ly		

Classification	ipv6 dscp Match the specified ipv6 DSCP value, this parameter			
criteria rule	is the ipv6 DSCP list			
Class-map name	The name of the created class-matching table, select by clicking the drop-down			
IPv6 dscp0-7	One or more ipv6 DSCP values can be set, up to 8 DSCP values can be set, the			
	range is 0~63;			
Operation	Add Matching rules			
	Remove Remove matching rules			

Classification criteria configuration					
Classification criteria rule	ipv6	flow	label	· ~	
Class-map name	1 🗸				
IPv6 flowlabel0					
IPv6 flowlabel1					
IPv6 flowlabel2					
IPv6 flowlabel3					
IPv6 flowlabel4					
IPv6 flowlabel5					
IPv6 flowlabel6					
IPv6 flowlabel7					
Operation	Add	~			
				App	ly

Classification criteria	ipv6 flowlabel Match the specified IPv6 flow label, this parameter is		
rule		the value of the IPv6 flow label DSCP list	
Class-map name	The name of the created class-matching table, select by clicking the drop-		
	down		
IPv6 flowlabel0-7	One or more IPv6 flowlabel values can be set, ranging from 0 to 1048575;		
Operation	Add	Add matching rules	
	Remove	Remove matching rules	

```
Switch# config t
Switch(config)# class-map c1
Switch(config-classmap-c1)# match access-group 1
```

Display configuration application execution process and return result

17.3. QoS policy configuration

17.3.1. QoS policy configuration

Configure the policy table burst-group, provide the policy class-map to use

policy configuration			
policy burst id configuration:	1	\sim	
policy burst size configuration			
			Apply

Policy burst id configuration	There are only two IDs, 1 and 2
Policy burst size configuration	The default is 1024, the range that can be set: 1-8192

17.4. QOS policy-map configuration

17.4.1. policy-map configuration

Create and delete policy tables, and collaborate with classification tables to create packet in and out rules

Policy-map configuration				
Policy-map name				
Operation	Add	~		
				Apply

Policy-map name	Policy-map name, range:1-64 character		
Operation	Add Add policy-map		
	Remove Remove policy-map		

Information feedback window Policy-map name p1

Display the currently created policy-map.

17.4.2. Class-map use to policy-map config

Apply the class-map to the policy-map.

Class-map use to policy-map configuration				
Policy-map name	p1 🗸			
Class-map name				
Inserted before the class-map name				
Operation	Add	~		
			Apply	

policy-map name	The name of the created policy-map			
class-map name	The name of the classification table created by the classification matching			
	table, this table will be applied to the policy -map			
Inserted before the	Prior to the	Prior to the insertion of the classification matching table, the name of the		
class-map name	classification table that has been applied to the strategy table, and the			
	priority of the newly applied classification matching table is increased			
Operation	Add	Add an association between the strategy table and the		
	classification table			
	Remove Remove an association between the strategy table and the			
		classification table		

Information feedback window					
Policy-map name	Class-map name				
p1	1				

Display the association between the created policy table and the classification matching table

17.5. QoS policy-class-map configuration

17.5.1. Policy-class-map accounting configuration

Configure the statistics switch of the strategy table and the classification matching table, and display the association between the strategy table and the classification matching table.

Policy-class-map accounting configuration				
Policy-map name	p1 🗸			
Class-map name	c1 🗸			
Accounting switch	Disable	$\mathbf{\mathbf{v}}$		
		Apply		

Policy-map name	The name of the policy-map that has been created	
class-map name	The name of the classification matching table that has been created	
accounting switch	disable	Disable the traffic statistics function associated with the policy-map and class-map, and automatically establish an association if there is no association
	enabled	Start the traffic statistics function associated with the policy-map and class-map, and automatically establish an association if there is no association

Information feedback window						
Policy-map name	Class-map	name	Accounting	switch		
p1	c1		Enable			

Display the traffic statistics switch information of the associated policy-map and class-map table

17.5.2. Aggregate policy configuration

Configure the set strategy of the associated policy table and classification matching table. The policy mapping refers to the aggregation policy, and the aggregation policy is applied to the classified traffic. The same policy set can be referenced by different policy class mappings.

Aggregate policy configuration						
Policy-map name	p1	\sim				
Class-map name	c1	\sim				
Aggregate policy name						
Operation	Add	1	~			
					Арр	oly

Policy-map name	Name of the	created policy table				
Class-map name	Classification	Classification match table created				
Aggregate policy name	The name of	The name of the aggregation strategy, 1-64 characters in length				
operation	add	Start the set strategy associated with the strategy table and the classification matching table, and automatically establish the association if there is no associated strategy table and the classification matching table				
	remove	Close the set strategy associated with the strategy table and the classification matching table, and automatically establish the association between the strategy table and the classification matching table without association				

Information feedback window							
Policy-map name	Class-map	name	Aggregate	policy	name		
p1	c1		a1				

Display the set policy information of the associated policy table and the classification matching table

17.5.3. Policy-class-map policy configuration

Configure the information rate in the policy mapping configuration mode.

Policy-class-map policy configuration							
Policy-map name	p1 🗸	·					
Class-map name	c1 🗸	•					
Committed information rate							
Committed burst id:	1 🗸						
Operation	Add	`	~				
			1	Apply			

Policy-map name	Name of t	he created policy table			
Class-map name	Classification match table created				
Committed	Committed Information Rate-CIR (Committed Information Rate), in Kbps,				
information rate	ranging from 1 to 10,000,000;				
Committed burst ID	The burst ID range is 1 and 2, and the main commitment is the burst size				
	add	Add the strategy information rate and burst size associated with the strategy table and the classification matching table, and automatically establish the association if there is no associated strategy table and the classification matching table			
operation	remove	Delete the policy information rate and burst size associated with the policy table and the classification matching table, and automatically establish the association if there is no associated policy table and the classification matching table			

17.5.4. Policy-class-map set configuration

Configure the priority of packets in the policy mapping configuration mode. Assign a new DSCP and IP priority to the classified traffic. Only the classified traffic that meets the matching criteria will be assigned a new value.

Classification criteria configuration						
Classification criteria rule	ip dscp	~				
Policy-map name	p1 🗸					
Class-map name	c1 🗸					
DSCP						
Operation	Add 🗸					
		Apply				

Classification	ip dscp	Set the DSCP value again according to the rules defined in the				
criteria rule		policy-map and class-map				
	ip precedence	Set the IP priority again according to the rules defined in the				
		policy-map and class-map				
	drop-precedence	Set the discarding priority again according to the rules				
		defined in the policy-map and class-map				
	internal-priority	Set the internal priority again according to the rules defined				
		by the policy-map and class-map				
	cos	Set the COS value again according to the rules defined by the				
		policy table and the classification matching table				
	ipv6 default	Set the default next hop address again according to the rules				
	nexthop vrf	defined in the policy table and classification matching table				
Policy-map name	The name of the created policy table					
Class-map name	Created classification match table					
DSCP	DSCP value, range	: 0-63				
Precedence	IP priority, range	:0-7				
Drop-precedence	drop priority, rang	e: 0-2				
Internal-priority	internal priority, ra	ange: 0-7				
COS	COS value, range:	0-7				
Vrf	Vrf value, range: 0	-252				
IPv6 Address	IPv6 default next h	nop address				
(X:X::X:X)						
Operation	add	Add the priority and queue value associated with the strategy				
		table and the classification matching table				
	remove	Remove the priority and queue value associated with the				
		strategy table and the classification matching table				

17.6. QoS mapping configuration

17.6.1. COS-to-IntP mapping

Configure the value mapped from the COS value to the internal priority (queue).

CoS-to-IntP mapping								
CoS value	0	1	2	3	4	5	6	7
IntP value	0	1	2	3	4	5	6	7
Operation type Configuration 🗸								
Apply								

CoS value	The COS value carried in the message or the default COS value assigned when				
	entering				
IntP value	The value of the internal priority (queue) to which the COS value will be mapped				
Operation type	Configuration Configure the value of COS to IntP				
	Default Restore the mapping relationship to the default state				

Display the execution process and the current mapping relationship

17.6.2. COS-to-DP mapping

Configure the value mapped from the COS value to the drop priority (queue).

CoS-to-DP mapping								
CoS value	0	1	2	3	4	5	6	7
DP value	0	0	0	0	0	0	0	0
Operation type Configuration 🗸								
Apply								

CoS value	The COS value carried in the message or the default COS value assigned when entering				
IntP value	The value of the drop priority (queue) to which the COS value will be mapped				
Operation	Configuration Configure COS to drop priority value				
type	default	default Restore the mapping relationship to the default state			

ingress C	OS-TO-D	rop-1	Prece	denc	e mar	p:	
:OS: 0	1 2	3	4	5	6	7	
)P: 0	0	0	0	0	0	0	0

Display the execution process and the current mapping relationship

17.6.3. DSCP-to-DSCP mapping

Configure the mapping from DSCP value to DSCP value.

DSCP-to-DSCP mapping		
DSCP value1		
DSCP value2(optional)		
DSCP value3(optional)		
DSCP value4(optional)		
DSCP value5(optional)		
DSCP value6(optional)		
DSCP value7(optional)		
DSCP value8(optional)		
DSCP value		
Operation type	Configurat	ion 🗸
		Apply

DSCP value1-DSCP	Up to eight DSCP va	alues can be configured to the new DSCP value, among				
value8(optional)	which DSCP value1 is required, DSCP valuce2-8 is optional, range: 0-63					
DSCP value	New DSCP value, range: 0-63					
Operation type	Configuration Configure DSCP to DSCP value					
	default	Restore the mapping relationship to the default state				

Sw: Sw:	itch itch	confi confi	ig t .g) ‡ :	mls q	os map	dscp	-dscj	p 63	60		to	1
In	gress	DSCP	-TO-	DSCP :	map:							
d1	: d2	2 0	1	2	34	5	6	7	8	9		
0:		0	1	2	3	4	5		6	7	8	9
1:		10	11	12	13	14	15	1	6	17	18	19
2:		20	21	22	23	24	25	2	6	27	28	29
3:		30	31	32	33	34	35	3	6	37	38	39
4:		40	41	42	43	44	45	4	6	47	48	49
5:		50	51	52	53	54	55	5	6	57	58	59
6:		1	61	62	1							

Shows the execution process and the current mapping relationship. The vertical d1 represents the tens digit of DSCP, and the horizontal d2 represents the single digit of DSCP. The value of the intersection of the two is the mapping value.

17.6.4. DSCP-to-IntP mapping

Configure the value mapped from the DSCP value to the IntP value.

DSCP-to-IntP mapping		
DSCP value1		
DSCP value2(optional)		
DSCP value3(optional)		
DSCP value4(optional)		
DSCP value5(optional)		
DSCP value6(optional)		
DSCP value7(optional)		
DSCP value8(optional)		
IntP value		
Operation type	Configurat	ion 🗸
		Apply

DSCP value1-DSCP	Up to eight DSCP va	alues can be configured to the new IntP value, among					
value8(optional)	which DSCP value1 is required, DSCP valuce2-8 is optional, range: 0-63						
IntP value	New IntP value, range: 0-7						
Operation type	Configuration Configure DSCP to IntP value						
	default	Restore the mapping relationship to the default state					

Switch Switch	h# conf h(confi	ig t .g) # m	ls qos	map	dscp	-intp	60 5	0 31	t	:0 2	
Ingres	ss DSCP	-то-і	nterna	1-Pri	iorit	y map	:				
d1 : (d2 0	1	2 3	4	5	6	7 8	9			
0:	0	0	0	0	0	0	0	0	1	1	
1:	1	1	1	1	1	1	2	2	2	2	
2:	2	2	2	2	3	3	3	3	3	3	
3:	3	2	4	4	4	4	4	4	4	4	
4:	5	5	5	5	5	5	5	5	6	6	
5:	2	6	6	6	6	6	7	7	7	7	
6 -	2	7	7	7	-	-				-	
	-										

Shows the execution process and the current mapping relationship. The vertical d1 represents the tens digit of DSCP, and the horizontal d2 represents the single digit of DSCP. The value of the intersection of the two is the mapping value.

17.6.5. DSCP-to-DP mapping

Configure the value mapped from the DSCP value to the DP value.

DSCP-to-DP mapping		
DSCP value1		
DSCP value2(optional)		
DSCP value3(optional)		
DSCP value4(optional)		
DSCP value5(optional)		
DSCP value6(optional)		
DSCP value7(optional)		
DSCP value8(optional)		
DP value		
Operation type	Configurat	ion 🗸
		Apply

DSCP value1-DSCP	Up to eight DSCP val	Up to eight DSCP values can be configured to the new DP value, among						
value8(optional)	which DSCP value1 is required, DSCP valuce2-8 is optional, range: 0-63							
DP value	New DP value, range: 0-2							
Operation type	Configuration Configure DSCP to DP value							
	default	Restore the mapping relationship to the default state						

- · · · ·	ress	DSCP	-10-1	Drop-Fr	ecea	ence	map:						
d1	: d2	0	1	2 3	4	5	6	7	8	9			
0:		0	0	0	0	0	0	(D	0	0	0	
1:		0	0	0	0	0	0	(D	0	0	0	
2:		0	0	0	0	0	0	(D	0	0	0	
3:		0	0	0	0	0	0	(D	0	0	0	
4:		0	0	0	0	0	0	(D	0	0	0	
5:		0	0	0	0	0	0	(D	0	0	0	
6:		0	0	0	0								

Shows the execution process and the current mapping relationship. The vertical d1 represents the tens digit of DSCP, and the horizontal d2 represents the single digit of DSCP. The value of the intersection of the two is the mapping value.

17.6.6. EXP-to-IntP mapping

Configure the value mapped from EXP value to IntP.

EXP-to-IntP ma	EXP-to-IntP mapping							
EXP value	0	1	2	3	4	5	6	7
IntP value	0	1	2	3	4	5	6	7
Operation type Configuration 🗸								
							Ap	oply

EXP value	EXP value carried in th	EXP value carried in the message, range: 0-7						
IntP value	New IntP value, range	Jew IntP value, range: 0-7						
Operation type	Configuration	Configure DSCP to IntP value						
	default	Restore the mapping relationship to the default state						

17.6.7. EXP-to-DP mapping

Configure the value mapped from EXP value to DP.

EXP-to-DP mapping								
EXP value	0	1	2	3	4	5	6	7
DP value	0	0	0	0	0	0	0	0
Operation type Configuration 🗸								
							Ap	oply

EXP value	EXP value carried in the message, range: 0-7				
DP value	New DP value, range	: 0-2			
Operation type	Configuration	Configure EXP to DP value			
	default	Restore the mapping relationship to the default state			

17.6.8. IntP-to-DSCP mapping

Configure the value mapped from IntP value to DSCP.

IntP-to-DSCP mapping								
IntP value	0	1	2	3	4	5	6	7
DSCP value	0	8	16	24	32	40	48	56
Operation type Configuration 🗸								
							Ap	oply

IntP value	The value of the internal priority of the message, range: 0-7					
DSCP value	New DSCP value, ra	New DSCP value, range: 0-63				
Operation type	Configuration	Configure IntP to DSCP value				
	default	Restore the mapping relationship to the default state				

17.6.9. IntP-to-EXP mapping

Configure the value mapped from IntP value to EXP.

IntP-to-EXP mapping								
IntP value	0	1	2	3	4	5	6	7
EXP value	0	1	2	3	4	5	6	7
Operation type Configuration 🗸								
							Αp	oply

IntP value	The value of the internal priority of the message, range: 0-7				
EXP value	New EXP value, range	e: 0-7			
Operation type	Configuration	Configure IntP to EXP value			
	default	Restore the mapping relationship to the default state			

17.7. QoS aggregate policy configuration

Configure the new aggregation strategy and the information rate and burst id of the aggregation strategy.

QoS aggregate policy configuration						
Aggregate policer name						
Committed Information Rate						
policy burst id configuration:	1 🗸					
Operation	Add	`	/			
						Apply

Aggregate policer name	New aggregate policer name, range: 1-64 character.			
Committed Information Rate	Information Rate, range: 1-10000000kbit/s			
Policy burst id configuration	Burst id configuration, range: 1-2			
Operation	Add Add aggregate policer			
	Remove Remove aggregate policer			

Information feedback window	
Switch# config t	
Switch(config) # mls qos aggregate-policy	y agg1 10000 burst-group 1

Display the configuration process and results, no error will be reported after normal configuration

17.8. QoS service policy configuration

Configure VLAN Association Policy.

QoS service policy configuration						
Policy-map name	p1 🗸]				
Vlan List						
Operation	Add	~				
					Apply	

Policy-map name	The name of the created strategy, select by clicking the drop-down				
VLAN List	VLAN ID, range: 1-4094				
Operation	add Add VLAN-based policy				
	remove remove VLAN-based policy				

Switch# config t Switch(config)# service-policy input p1 vlan 2

Display the configuration process and results, no error will be reported after normal configuration

18. L3 forward configuration

18.1. IP route Aggregation configuration

18.1.1. Route aggregate configuration

This page is used for enabled or disabled configuration of routing aggregation $_{\circ}$

To display the "Route aggregate configuration" page, click L3 forward configuration->IP route Aggregation configuration->Route aggregate configuration, click "Apply" to configure.

Enable route aggregation		
Enable route aggregation	Disable 🗸	
		Apply

entry	describe
Enable route aggregation	Enable: Enable routing aggregation
	Disable: Disable routing aggregation

Route aggregation status Route aggregation status disable

entry	describe
Routing aggregation state	enable: Enable routing aggregation
	disable: Disable routing aggregation

18.2. ARP configuration

18.2.1. ARP configuration

This page is used to configure ARP static entries.

To display the "ARP configuration" page, click L3 forward configuration->ARP configuration->ARP configuration, click "Apply" to configure.

ARP configuration	n
IP address	
MAC address	
Operation type	Add 🗸
VLAN interface	Vlan1 🗸
Port	Ethernet1/0/1 V
	Apply

entry	describe	
IP address	IP address, e.g .1.1.1.1	
MAC address	MAC address	
Operation type	add: Apply the above settings	
	Remove: Delete the above	
VLAN interface	VLAN id created	
Port	Ethernet port name	

18.2.2. Clear ARP cache

This page is used to clear ARP statistics.

To display the "Clear ARP cache" page, click L3 forward configuration->ARP configuration->Clear ARP cache, click "Apply" to configure.

Clear ARP cache	
	Apply

18.2.3. Show ARP

This page is used to view the information of the ARP table.

To display the "Clear ARP cache" page, click L3 forward configuration->ARP configuration->Clear ARP cache.

ARP list					
Binding IP	Binding MAC	Interface	Port	flag	
192.168.2.74 00-0e-c6-bf-ad-7a Vlan1 Ethernet1/0/14 dynar					
Number of ARP er	ntry				
Number of ARP er	ntry		1		
				Refresh	

18.3. Gratuitous Arp config

18.3.1. gratuitous-arp interval time configuration

This page is used to configure the global free ARP send time interval. To display the "gratuitous-arp interval time configuration" page, click L3 forward configuration->Gratuitous arp config->gratuitous-arp interval time configuration, click "Apply" to configure.

gratuitous-arp interval time configuration					
interval time					
Operation	Add	~			
				Apply	

entry	describe
interval time	Range :5-1200 seconds
Operation	Add: Apply the above settings
	Remove: Recovery default interval 300 seconds

18.3.2. Interface gratuitous-arp interval time configuration

This page is used to set vlan interface free ARP send interval configuration. To display the "interface gratuitous-arp interval time configuration" page, click L3 forward configuration->Gratuitous arp config->interface gratuitous-arp interval time configuration, click "Apply" to configure.

interface gratuitous-arp interval time configuration					
Vlan ID	1 ~				
interval time					
Operation	Add V				
	Apply				

entry	describe		
VLAN ID	vlan ID created		
interval time	Range :5-1200 seconds		
Operation	Add: Apply the above settings		
	Remove: Recovery default interval 300 seconds		

18.3.3. Show gratuitous-arp configuration

This page is used to view ARP free configuration information.

To display the "show gratuitous-arp configuration" page, click L3 forward configuration->Gratuitous arp config->show gratuitous-arp configuration, click "Apply" to view.

	gratuito	us-ar	p interval t	ime con	figuı	ration	
	Vlan ID			~			
						Apply	
Informat	ion feedl	back w	/indow				
Switch#	show ip	o grat	cuitous-ar	р			
Gratuito	ous ARP	send	is Global	disabl	.ed		
Gratuito	ous ARP	send	enabled i	nterfac	e vl	lan inf	ormation:
Name		Int	cerval-Tim	e (secon	ds)		

18.4. ARP protection configration

18.4.1. ARP GUARD configration

18.4.1.1. ARP GUARD configration

This page is used for ARP GUARD configuration.

To display the "ARP GUARD configration" page, click L3 forward configuration->ARP protection configration->ARP GUARD configration->ARP GUARD configration, click "Apply" to configure.

ARP GUARD configration				
Port	Ethernet1/0/1	~		
IP address				
Operation	Add 🗸			
			Apply	

entry	describe	
Port	Ethernet port name	
IP address	IP address, e.g. 1.1.1.1	
Operation	Add: Apply the above settings	
	Remove: Delete the above	

18.4.2. ANTI-ARPSCAN configration

18.4.2.1. ANTI-ARPSCAN on-off configration

This page is used to configure the anti ARP scan function switch.

To display the "ARP GUARD configration" page, click L3 forward configuration->ARP protection configration->ANTI-ARPSCAN configration->ANTI-ARPSCAN on-off configration, click "Apply" to configure.

ANTI-ARPSCAN on-off configration	
ANTI-ARPSCAN on-off status Disable 🗸	
	Apply
ANTI-ARPSCAN on-off status	
ANTI-ARPSCAN on-off status	Disable

entry	describe
ANTI-ARPSCAN on-off status	Enable: Function Enable
	Disable: Function disabled

18.4.2.2. ANTI-ARPSCAN port-based threshold configration

This page is available for port-based configuration of anti-scan ARP thresholds. To display the "ANTI-ARPSCAN port-based threshold configration" page, click L3 forward configuration->ARP protection configration->ANTI-ARPSCAN configration->ANTI-ARPSCAN port-based threshold configration, click "Apply" to configure.

ANTI-ARPSCAN port-based threshold configration	
Range of threshold	
Operation	Configuration ~
	Apply

entry	describe	
Range of threshold	Size range :2-200, unit pack/s	
Operation	Configuration: Application settings	
	Default: Restore default 10 packs/s	

ANTI-ARPSCAN port-based threshold configration Range of threshold 16

entry	describe
Range of threshold	Current configured threshold, size range :
	2-200, unit pack/second

18.4.2.3. ANTI-ARPSCAN IP-based threshold configration

This page is used to configure the IP-based anti ARP scan threshold. To display the "ANTI-ARPSCAN IPbased threshold configration" page, click L3 forward configuration->ARP protection configration-> ANTI-ARPSCAN configration->ANTI-ARPSCAN IP-based threshold configration, click "Apply" to configure.

ANTI-ARPSCAN IP-based threshold configratior	
Range of threshold	
Operation	Configuration ~
	Apply

entry	describe
Range of threshold	Size range :2-200, unit pack/s
Operation	Configuration: Application settings
	Default: Restore default 6 packs/s

ANTI-ARPSCAN IP-based threshold configra	tion
Range of threshold	8

entry	describe
Range of threshold	Current configured threshold, size range :
	2-200, unit pack/second

18.4.2.4. ANTI-ARPSCAN trust port configuration

This page is used to set the port to anti ARP scan trust port.

To display the "ANTI-ARPSCAN trust port configration" page, click L3 forward configuration->ARP protection configration->ANTI-ARPSCAN configration->ANTI-ARPSCAN trust port configration, click "Apply" to configure.

ANTI-ARPSCAN trust port configration		
Port	Ethernet1/0/1	~
Port trust status	trust-port	~
Operation	Add 🗸	
		Apply

entry	describe
Port	Ethernet port name
Port trust status	trust-port: Trust port
	supertrust-port: Super trust port
	iptrust-port: IP trust port
Operation	Add: Application settings
	Remove: Delete the corresponding settings

18.4.2.5. ANTI-ARPSCAN trust IP configuration

This page can be used to prevent ARP scanning trust IP configuration.

To display the "ANTI-ARPSCAN trust IP configuration" page, click L3 forward configuration->ARP protection configration->ANTI-ARPSCAN configration->ANTI-ARPSCAN trust ip configration, click "Apply" to configure.

ANTI-ARPSCAN trust IP configration						
IP address						
Network mask						
Operation	Add	``	~			
					Appl	у

entry	describe	
IP address	IP address, e.g .1.1.1.1	
Network mask	Corresponding IP address mask	
Operation	Add: Application settings	
	Remove: Delete the corresponding settings	

18.4.2.6. ANTI-ARPSCAN recovery on-off configuration

This page can be used to prevent ARP scanning automatic recovery switch configuration. To display the "ANTI-ARPSCAN recovery on-off configuration" page, clickL3 forward configuration->ARP protection configration -> ANTI-ARPSCAN configration->ANTI-ARPSCAN recovery on-off configration, click "Apply" to configure.

ANTI-ARPSCAN recovery on-off configration
ANTI-ARPSCAN recovery on-off status Enable 🗸
Apply
ANTI-ARPSCAN recovery on-off status
ANTI-ARPSCAN recovery on-off status Enable

entry	describe
ANTI-ARPSCAN recovery	Enable: Enable automatic recovery function
on-off status	Disable: Disable automatic recovery function

18.4.2.7. ANTI-ARPSCAN recovery time configration

This page can be used to configure the automatic recovery time against ARP scanning. To display the "ANTI-ARPSCAN recovery time configuration" page, click L3 forward configuration->ARP protection configration -> ANTI-ARPSCAN configration->ANTI-ARPSCAN recovery time configration, click "Apply" to configure.

ANTI-ARPSCAN recovery time configration					
Recovery time					
Operation	Configuration ~				
		Apply			
ANTI-ARPSCAN recovery time configration					
Recovery time		300			

entry	describe	
Recovery time	Size range :5-86400 per second	
Operation	Configuration: Apply the above settings	
	Default: Recovery default auto recovery 300 seconds	

18.4.2.8. Show ANTI-ARPSCAN information

This page is used to view anti ARP scan run information.

To display the "Show ANTI-ARPSCAN information" page, click L3 forward configuration->ARP protection configration -> ANTI-ARPSCAN configration->Show ANTI-ARPSCAN information, click "Apply" to view.

Information feedback window						
Switch# show an	ti-arpscan					
Total port: 28						
Name	Port-property	beShut	shutTime(seconds)			
Ethernet1/0/1	untrust	N	0			
Ethernet1/0/2	untrust	N	0			
Ethernet1/0/3	untrust	N	0			
Ethernet1/0/4	untrust	N	0			
Ethernet1/0/5	untrust	N	0			
Ethernet1/0/6	untrust	N	0			
Ethernet1/0/7	untrust	N	0			
Ethernet1/0/8	untrust	Ν	0			

18.5. Show IP Traffic

This page can be used to view statistics for IP packets.

To display the "Show IP Traffic" page, click L3 forward configuration->ARP protection configration -> Show IP Traffic, click "Apply" to view.

```
Information feedback window
Switch# show ip traffic
IP statistics:
        134947 total, 135005 local destination
 Rcvd:
         0 header errors, 0 address errors
         0 unknown protocol, 0 discards
  Frags: 0 reassembled, 0 timeouts
         0 fragment rcvd, 0 fragment dropped
         0 fragmented, 0 couldn't fragment, 0 fragment sent
  Sent: 138810 generated, 0 forwarded
         0 dropped, 0 no route
ICMP statistics:
 Rcvd: 0 total 0 errors 0 time exceeded
         0 redirects, 0 unreachable, 0 echo, 0 echo replies
         0 mask requests, 0 mask replies, 0 quench
         0 parameter, 0 timestamp, 0 timestamp replies
 Sent: 0 total 0 errors 0 time exceeded
         0 redirects, 0 unreachable, 0 echo, 0 echo replies
         0 mask requests, 0 mask replies, 0 quench
         0 parameter, 0 timestamp, 0 timestamp replies
TCP statistics:
 TcpActiveOpens
                           6, TcpAttemptFails
                                                        0
                           3, TcpEstabResets
 TcpCurrEstab
                                                        3
                          0, TcpInSegs
 TcpInErrs
                                                   135005
                  264, TcpOutRsts
138868, TcpPassiveOpens
167, TcpRtoAlgorithm
120000, TcpRtoMin
 TcpMaxConn
TcpOutSegs
                                                        0
                                                     1738
  TcpRetransSegs
                                                        1
                                                      200
  TcpRtoMax
UDP statistics:
                           0, UdpInErrors
                                                        0
 UdpInDatagrams
  UdpNoPorts
                           0, UdpOutDatagrams
                                                        0
```

19. Route configuration

19.1. Policy based routing

The directory function is to be developed.

19.2. Static route configuration

19.2.1. Static route configuration

This page can be used for the basic configuration of static routing.

To display the "Static route configuration" page, click Route configuration ->Static route configuration, click "Apply" to configure.

Static IP route configuration					
Destination IP address					
Network mask or prefix-length					
Nexthop or Interface null0					
preference(optional)					
Operation type	Add	~	•		
					Apply

entry	describe	
Destination IP address	IP address, format :10.10.11.11	
Network mask or prefix-length	Subnet mask in the following format :255.255.255.0; or mask length	
Nexthop or Interface null0	IP address, format: 10.10.11.11. or null0	
preference(optional)	Range :1-255	
Operation type	Add: Add the above settings	
	Remove: Delete the above	

20. IPv6 Route configuration

20.1. IPv6 configuration

20.1.1. IPv6 basic configuration

This page is used to vlan the ipv6 address of the interface and the configuration of ipv6 routing. If you want to display the "IPV6 Basic Configuration" page, Click IPv6 Route configuration->IPv6 configuration, Click "Apply" to configure.

IPv6 basic configuration	
command	ipv6 address ∨
VLAN interface	Vlan1 🗸
IPv6 address(X:X::X:X/M)	
EUI-64	~
Operation	Configuration ~
	Apply

entry	describe
IPV6 address	vlan interface ipv6 address configuration
VLAN interface	vlan created
IPv6 address	example: 2001:3f:ed8::99/64
EUI-64	IPv6 address is automatically generated based on the eui64 interface
	identifier of the interface
Operation	Configure: User self-configuration
	Default: Restore default configuration

IPv6 basic configuration	
command	ipv6 route 🗸
IPv6 Destination address(X:X::X:X/M)	
IPv6 nexthop address(X:X::X:X)	
VLAN interface	~
IPv6 tunnel number	
Precedence	
Operation	Configuration ~
	Apply

Note: the switch does not support ipv6 routing configuration, the configuration of this page is not effective.

20.1.2. IPv6 ND configuration

This page is used for settings that can be used for neighbor discovery related functions. If you display the "IPv6 ND Configuration" page, click IPv6 Route configuration->IPv6 configuration, click "Apply" to configure.

IPv6 ND configuration		
command	dad attempts V	
VLAN interface	Vlan1 🗸	
IPv6 dad-attemps		
Operation	Configuration 🗸	
	Apply	

entry	describe
Data attempts	During duplicate address detection, the neighbor request message
	number continuously sent by the interface is set
VLAN interface	vlan created
IPv6 dad-attemps	Range :0-10
Operation	Configuration: Apply the above settings
	Default: Default request message number is 1

IPv6 ND configuration		
command	ns-interval V	
VLAN interface	Vlan1 🗸	
IPv6 ns-interval		
Operation	Configuration V	
	Apply	

entry	describe
ns-interval	Time interval setting for neighbor request messages
VLAN interface	vlan created
IPv6 ns-interval	Size range :1-3600 ,per second
Operation	Configuration: Apply the above settings
	Default: Default request message number is 1 second

IPv6 ND configuration	
command	neighbor V
VLAN interface	Vlan1 🗸
IPv6 address	
MAC address	
Port	Ethernet1/0/1 V
Operation	Configuration V
	Apply

entry	describe
Neighbor	Set the Static Neighbor Table Item
VLAN interface	vlan created
IPv6 address	Static Neighbor IPv6 Address
MAC address	Static Neighbor MAC Address
Port	Ethernet port name
Operation	Configuration: Apply the above settings
	Default: delete the corresponding static neighbor table item

IPv6 ND configuration	
command	clear ipv6 neighbors ∨
Operation	Configuration V
	Apply

entry	describe
Clear ipv6 neighbor	Clear neighbor table items, but cannot delete static neighbor table items
Operation	Configuration: Delete neighbor table item
	Default: Delete Neighbor Table Item

20.1.3. Show IPv6 neighbor

This page is used to view ipv6 neighbor information.

To display the "Show IPv6 neighbor" page, click IPv6 Route configuration->IPv6 configuration->Show IPv6 neighbor, click "Apply" to view.

Show IPv6 neighbor		
Parameter choose	Address 🗸	
IPv6 address		
		Apply

entry	describe
Address	Based on address
IPV6 address	Ipv6 address

Show IPv6 neighbor	
Parameter choose	Count 🗸
	Apply

entry	describe
Count	Display counter information

Show IPv6 neighbor			
Parameter choose	Vlan	~	
VLAN ID			
			Apply

entry		describe				
Vlan		vlan Based	l Interface			
Vlan id		vlan id created				
	Show I	Pv6 neighbo	or			
	Parame	eter choose	Ethernet 🗸			
	Etherne	et port				
			<u>.</u>		Apply	

entry	describe
ethernet	Based on Ethernet port
Ethernet port	Physical Port Name

20.2. Show IPv6 route

20.2.1. Show IPv6 route database

This page is used to view IPv6 routing table database information. To display the "Show IPv6 route database" page, click IPv6 Route configuration->Show IPv6 route->Show IPv6 route database, click "Apply" to view.

Show IPv6 route database				
Parameter choose	destination \checkmark			
IPv6 address				
		Apply		

entry	describe
Destination	Based on ipv6 address
IPv6 address	ipv6 address in the routing table

Show IPv6 route database			
Parameter choose	prefix	~	
IPv6 address(X:X::X:X/M)			
			Apply

entry	describe
Prefix	Based on ipv6 address
IPv6 address	ipv6 address in the routing table

Show IPv6 route database				
Parameter choose database 🗸				
		Apply		

entry	describe
database	Routing table database information

20.2.2. Show IPv6 NSM route

This page is used to view IPV6 NSM routing table information.

To display the "Show IPv6 NSM route" page, click IPv6 Route configuration->Show IPv6 route->Show IPv6 NSM route, click "Apply" to view.

	Show IPv6 route databas		
	Parameter choose 🗸 🗸 🗸		
		Apply	
Information feedba	ick window		
Switch# show ipv	6 route database		
IPv6 Routing Tab	le		
Codes: K - kerne I - IS-IS	l route, C - connected , B - BGP	l, S – static, R	- RIP, O - OSPF,
> - selec	ted route, * - FIB rou	ite, p – stale i	nfo
Timers: Uptime			
C*> ::1/128 via	::, Loopback, 03:55:41	. tag:0	

entry	describe
connected	IPv6 routing table information from NSM

	Show IPv6 NSM route		
	Parameter choose	database 🗸]
	Parameter choose	connected ~	
		Apply	
Information feedback	(window		
Switch# show ipv6 route nsm database connected IPv6 Routing Table			
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF, I - IS-IS, B - BGP			
> - selected route, * - FIB route, p - stale info			
Timers: Uptime			
C*> ::1/128 via ::	, Loopback, 03:57:50	tag:0	

entry	describe	
database	IPv6 Routing Table Database	
connected	Route table information	

20.2.3. Show IPv6 FIB

This page is used to view IPv6 forward information.

To display the "Show IPv6 FIB" page, click IPv6 Route configuration->Show IPv6 route->Show IPv6 FIB, click "Apply" to view.

Show IPv6 FIB	
Parameter choose	
Apply	
Information feedback window	
Switch# show ipv6 route fib	
Total IPv6 routes: 2 entries	
Codes: C - connected, L - Local, S -	static, R - RIP, O - OSPF,
I - IS-IS, B - BGP	
C fe80::/64 via ::, Vlan1 0	
C ff00::/8 via ::, Vlan1 0	

entry	describe
Blank parameters	Forwarding Information Database

Show IPv6 FIB			
Parameter choose	local	~	
		Apply	
Information feedback window			
Switch# show ipv6 route fib	local		
Total IPv6 routes: 3 entries	s		
::1/128 via ::, Loopl	back		
			- 1 1

entry	describe	
Local	Local table	
Show IPv6 FIB		
----------------------------------------------	--	--
Parameter choose vrf 🗸		
VRF ID(0-255)		
Apply		
Switch# show ipv6 route fib vrf 0 statistics		
Route statistics:		
Total routes are : 4 item(s)		
Total unspec routes are : 0 item(s)		
Total boot routes are : 2 item(s)		
Total kernel routes are : 2 item(s)		
Total connected routes are : 0 item(s)		
Total static routes are : 0 item(s)		
Total rip routes are : 0 item(s)		
Total bgp routes are : 0 item(s)		
Total ospf routes are : 0 item(s)		
Total ospf external routes are : 0 item(s)		
Total dvmrp routes are : 0 item(s)		
Total unknown routes are : 0 item(s)		

entry	describe		
Vrf	Virtual routing transponder		
VRF ID(0-255)	Virtual Route Forwarder Number		

Show IPv6 FIB		
Parameter choose	statistics 🗸	
	/	Apply

Information feedback window			
Switch#	show ipv6 route fib statistics		
Route s	statistics:		
Total r	coutes are : 4 item(s)		
Total u	inspec routes are : 0 item(s)		
Total b	poot routes are : 2 item(s)		
Total k	cernel routes are : 2 item(s)		
Total c	connected routes are : 0 item(s)		
Total s	static routes are : 0 item(s)		
Total r	rip routes are : 0 item(s)		
Total b	ogp routes are : 0 item(s)		
Total c	ospf routes are : 0 item(s)		
Total c	ospf external routes are : 0 item(s)		
Total c	dvmrp routes are : 0 item(s)		
Total u	unknown routes are : 0 item(s)		

entry	describe	
statistics	Routing table statistics	

20.2.4. Show IPv6 route statistics

This page is used to view IPv6 routing statistics.

To display the "Show IPv6 route statistics" page, click IPv6 Route configuration->Show IPv6 route->Show IPv6 route statistics "Apply" to view.

Show IPv6 route statistics	
Parameter choose	~
	Apply

Information feedback window		
Switch# show ipv6 route statistics		
Route statistics:		
Total routes are : 1 item(s)		
Total default routes are : 0 item(s)		
Total kernel routes are : 0 item(s)		
Total connected routes are : 1 item(s)		
Total static routes are : 0 item(s)		
Total rip routes are : 0 item(s)		
Total bgp routes are : 0 item(s)		
Total ospf routes are : 0 item(s)		
Total ospf intra area routes are : 0 item(s)		
Total ospf inter area routes are : 0 item(s)		
Total ospf nssa type 1 routes are : 0 item(s)		
Total ospf nssa type 2 routes are : 0 item(s)		
Total ospf external type 1 routes are : 0 item(s		
Total ospf external type 2 routes are : 0 item(s		

Note: the corresponding function of parameter vrf has not been realized.

21. DCSCM configuration

21.1. DCSCM Source-control enable/disable configuration

Configure Dcscm multicast source control configuration and view the configuration status.

DCSCM Source-control enable/disable configuration		
DCSCM Source-control enable/disable configuration	Enable	~
	Appl	ly

Dcscm Source-control	Enable	Enable dcscm multicast source control configuration
enable/disable configuration	Disable	Disable dcscm multicast source control configuration

DCSCM S	ource-control state		
DCSCM S	ource-control state	Disable	

Display the current configuration status

21.2. DCSCM destination-control enable/disable configuration

Configure Dcscm multicast destination control configuration and view configuration status.

DCSCM destination-control enable/disable configuration		
DCSCM destination-control enable/disable configuration	nable	$\overline{}$
	Appl	у

Dcscm destination-control	Enable	Enable dcscm multicast destination control configuration
enable/disable configuration	Disable	Disable dcscm multicast destination control configuration

DCSCM destination-control enable/disable state DCSCM destination-control enable/disable state Disable

Display the current configuration status

21.3. DCSCM Source-control access-group configuration

Configure Dcscm multicast source control list configuration and view the configuration status of the configuration list.

DCSCM Source-control access-group configuration					
Port	Ethernet1/0/1 🗸				
DCSCM Source-control access-group number					
Operation	Add	~			
				App	ly

Port	Port name	Port name			
DCSCM destination-	Match the multicast data message imported from the interface according to				
control access-group	the configured source control list number. The source control list number is				
number	derived from the ACL multicast source control configuration of ACL				
	multicast control, range: 5000-5099				
Operation	Add Add source control list number under port				
	Remove Delete the source control list from the port				

DCSCM Source-control access-group				
Port	DCSCM Source-control access-group i	number		
Ethernet1/0/1	5000			

Display the currently configured port and the corresponding source control list number (there is no port configured by default)

21.4. DCSCM destination-control access-group configuration

Configure Dcscm multicast destination control list configuration and view configuration list configuration status.

DCSCM destination-control access-group configuration					
Port	Ether	net1,	/0/1	\sim	
DCSCM destination-control access-group number					
Operation	Add	~			
				Appl	ly

Port	Port name			
DCSCM destination-	Match the	Natch the multicast data message imported from the interface according to		
control access-	the configu	ne configured destination control list number. The destination control list		
group number	number is derived from the ACL multicast destination control configuration of			
	ACL multicast control, range: 6000-7999			
Operation	Add Add the destination control list number under the port			
	Remove Delete the destination control list from the port			

DCSCM destination-control access-group					
Port	DCSCM destination-control access-group numb	er			
Ethernet1/0/1	6000				

Display the currently configured port and the corresponding destination control list number (there is no port configured by default)

21.5. DCSCM destination-control access-group configuration (sip)

Configure the IP-based Dcscm port multicast destination control list configuration and view the configuration list configuration status.

DCSCM destination-control access-group configuration(sip)				
DCSCM destination-control IP-address/mask				
DCSCM destination-control access-group number				
Operation	Add	~		
				Apply

DCSCM destination- control IP- address/mask	Determine the members of the multicast group according to the specified network end and mask. When the multicast group member matches the control list number, the interface can be added, otherwise the interface is not added				
DCSCM destination-	Match the multicast data	message imported from the specified network			
control access-group	according to the configur	ed destination control list number. The destination			
number	control list number is configured from the ACL multicast destination control				
	configuration of ACL multicast control, range: 6000-7999				
Operation	Add Add the destination control list number under the				
	designated network terminal				
	Remove Delete the destination control list from the				
		specified network segment			

DCSCM destination-control access-group(sip)	
DCSCM destination-control IP-address/mask	DCSCM destination-control access-group number
10.0.0/24	6000

Display the current configured destination IP address and the corresponding destination control list number (there is no configured port by default)

21.6. DCSCM destination-control access-group configuration (vMAC)

Configure VLAN-MAC based Dcscm multicast source control list configuration and view the configuration list configuration status.

DCSCM destination-control access-group configuration(vMAC)				
VLAN interface	Vlan1	\sim		
MAC address				
DCSCM destination-control access-group number				
Operation	Add	~		
				Apply

VLAN interface	VLAN interface		
MAC address	Transmit the source MAC address of IGMP-REPORT, the format is "xx-xx-xx-		
DCSCM destination-	Match the multicast data message imported from the interface according		
control access-group	to the config	gured destination control list number. The destination control	
number	list number is derived from the ACL multicast destination control		
	configuration of ACL multicast control, range: 6000-7999		
Operation	Add	Add the destination control list number to the host	
	corresponding to the MAC address in the VLAN		
	Remove Delete the destination control list from the corresponding		
		MAC address host under the VLAN	

DCSCM destination-control access-group(vMAC)					
VLAN interface	MAC address	DCSCM destination-control access-group number			
1	01-00-22-33-44-55	6000			

Display the mac host and the corresponding destination control list number under the currently configured vlan (there is no configured port by default)

21.7. Multicast policy configuration

Configure multicast policy and view configuration status.

Multicast policy configuration					
Source IP-address/mask					
Destination IP-address/mask					
DCSCM priority					
Operation	Add	~			
				App	ly

Source IP-address/mask	The source IP address range of multicast data packets, format:		
	192.168.2.0/24		
Destination IP-	The destination IP address range of multicast data packets, format:		
address/mask	224.0.0.0/8		
DCSCM priority	Specify priority, range: 0-7		
Operation	Add	Configure the switch matching priority of multicast data packets in a specified range to be modified to a specified value, and TOS is also specified to the same value	
Remove		Delete the priority policy of multicast data in the specified range	

Multicast policy	
ip multicast-policy	192.168.2.0/24 224.168.2.0/24 cos 1

Display the currently configured multicast policy

21.8. ACL multicast source control

Configure ACL access rules and view the configuration status of the configuration list.

ACL multicast source control	
ACL number	
Rule	permit 🗸
Source address type	Any IP 🗸 🗸
Multicast source address	
Multcast source wildcard	
Source address type	Any IP 🗸 🗸
Multicast destination address	
Multicast destination wildcard	
Operation type	Add 🗸
	Apply

ACL number	ACL number, range	ACL number, range: 5000-5099		
Rule	permit	Allow the following rules to pass		
	deny	Reject the following rules to pass		
Source address type	Specified address	An address range determined by IP addresses and address		
		wildcards		
	Any IP	Any host address		
	Host Address	A specified address (set in the multicast		
		source/destination IP address)		
Multicast	The address type is the host address and the IP address set when specifying			
source/destination	the address, for example: 10.1.1.0 or 192.168.5.1			
address				
Multcast	The address type is	e address type is the wildcard set when specifying the address, for example:		
source/destination	0.0.0.255	.255		
wildcard				
Operation type	Add	Add the set rules to the ACL number, and other functions		
		use the source control list number to use these rules		
	Remove	Delete the rule of ACL number		

ACL multicast destination con	trol
ACL number	
Rule	permit 🗸
Source address type	Any IP 🗸 🗸
Multicast source address	
Multcast source wildcard	
Source address type	Any IP 🗸
Multicast destination address	
Multicast destination wildcard	
Operation type	Add 🗸
	Apply

ACL number	ACL number, range: 5000-5099			
Rule	permit	Allow the following rules to pass		
	deny	Reject the following rules to pass		
Source address type	Specified address	An address range determined by IP addresses		
		and address wildcards		
	Any IP	Any host address		
	Host Address	A specified address (set in the multicast		
		source/destination IP address)		
Multicast source/destination	The address type is the host address and the IP address set when			
address	specifying the address, for example: 10.1.1.0 or 192.168.5.1			
Multcast source/destination	The address type is the wildcard set when specifying the address, for			
wildcard	example: 0.0.0.255			
Operation type	Add	Add the set rules to the ACL number, and other		
		functions use the ACL number to use these rules		
	Remove	Delete the rule of ACL number		

Information feedback window
Switch# show ip multicast source-control access-list
access-list 5000 permit ip any-source any-destination
access-list 5093 permit ip any-source any-destination
Switch# show ip multicast destination-control access-list
access-list 6000 permit ip any-source any-destination

Display the currently configured multicast source control list number and multicast destination control list number rules

22. Spanning-tree configuration

22.1. Spanning-tree field configuration

22.1.1. Instance configuration

This page can be used to configure the mapping relationship between the spanning tree instance and the VLAN.

To display the "Instance configuration" page, click Spanning-tree configuration ->Spanning-tree field configuration->Instance configuration, click "Apply" to configure.

Instance configuration			
Instance name			
VLAN name			
Operation	Add	~	
			Apply

entry	describe	
Instance name	Generating tree instance ID, range 0-64	
VLAN name	VLAN ID, range : 1-4094	
Operation	Add: Add the above configuration information	
	Remove: Delete the above configuration information	

Instance configuration	
Instance name	VLAN name
0	1-4094

entry	describe
Instance name	Generating tree instance ID, size range 0-64
VLAN name	VLAN ID, range : 1-4094

22.1.2. Field name configuration

This page can be used to configure MSTP domain name.

To display the "Instance configuration" page, click Spanning-tree configuration ->Spanning-tree field configuration->Field name configuration, click "Apply" to configure.

Field name configuration		
Field name		
Operation	Configuration V	
		Apply
Field name		
Field name	name	

entry	describe	
Field name	MSTP domain name, the length is 1-32 characters	
Operation	Configuration: Use the above configuration	
	Default: Default does not match domain name	

22.1.3. Revision-level configuration

This page can be used to configure MSTP revision level.

To display the "Instance configuration" page, click Spanning-tree configuration ->Spanning-tree field configuration->Revision-level configuration, click "Apply" to configure.

Revision-level configuration			
Revision-level			
Operation	Default	~	
			Apply

entry	describe
Revision-level	Range :0-65535
Operation	Configuration: Use the above configuration
	Default: Restore default configuration 0

Revision-level	
Revision-level	0

entry	describe
Revision-level	MSTP revision level with configuration, size range :0-65535

22.2. Spanning-tree Port configuration

22.2.1. PortFast configuration

This page can be used for the configuration of edge ports.

To display the "PortFast configuration" page, click Spanning-tree configuration ->Spanning-tree Port configuration->PortFast configuration, click "Apply" to configure.

PortFast configuration	
Port	Ethernet1/0/1 V
Operation	Add V
	Apply

entry	describe	
Port	Ethernet port name	
Operation	Add: Configure the above port type to an edge port	
	Remove: Configure the above port type to be a non-edge port	

PortFast configuration		
Port	PortType(1/0)	
Ethernet1/0/1	0	
Ethernet1/0/2	0	
Ethernet1/0/3	0	
Ethernet1/0/4	0	
Ethernet1/0/5	0	
Ethernet1/0/6	0	
Ethernet1/0/7	0	
Ethernet1/0/8	0	

entry	describe
Port	Ethernet port name
PortType(1/0)	1: Represents an edge port
	0: Represents a non-edge port

22.2.2. Port priority configuration

This page can be used for configuration of instance port priority. To display the "PortFast configuration" page, click Spanning-tree configuration ->Spanning-tree Port configuration->Port priority configuration, click "Apply" to configure.

Port priority configuration		
Port	Ethernet1/0/1 V	
Instance name		
Priority		
Operation	Default V	
	Apply	

entry	describe
Port	Ethernet port name
Instance name	Generate tree instance name

Priority	The size range is :0-240, multiple of 16
Operation	Configuration: Apply the above configuration
	Default: Restore default priority 32768

Port priority configuration

Ethernet1/0/1 of Instance 0 Operation port path cost 20000, Port priority 32, Port Identifier 032.001

22.2.3. Port cost configuration

This page can be used to configure port path costs.

To display the "Port cost configuration" page, click Spanning-tree configuration ->Spanning-tree Port configuration, click "Apply" to configure.

Port cost configuration			
Port	Ethernet1/0/1 V		
Instance name			
Cost			
Operation	Default 🗸		
	Apply		

entry	describe	
Port	Ethernet port name	
Instance name	Generate tree instance name	
Cost	Size range :0-20000000	
Operation	Configuration: Apply the above configuration	
	Default: Recovery port default path cost	

22.2.4. Spanning-tree port mode

This page can be used to configure the spanning tree running mode where the port is located. To display the "Spanning-tree port mode" page, click Spanning-tree configuration ->Spanning-tree Port configuration->Spanning-tree port mode, click "Apply" to configure.

Spanning-tree port mode			
Port Ethernet1/0/1 V			
		Apply	

entry	describe
Port	Ethernet port name

22.2.5. Link-type configuration

This page can be used to configure port link types.

To display the "Link-type configuration" page, click Spanning-tree configuration ->Spanning-tree Port configuration->Link-type configuration, click "Apply" to configure.

Link-type configuration	
Port	Ethernet1/0/1 V
Link type	auto 🗸
Operation	Default 🗸
	Apply

entry	describe	
Port	Ethernet port name	
Link type	Auto: Automatic consultations	
	Force-true: Point-to-point type	
	Force-false: Non-point-to-point type	
Operation	Configuration: Apply the above configuration	
	Default: Auto is the default link type for the recovery port	

Link-type configuration			
Port	Link type		
Ethernet1/0/1	auto		
Ethernet1/0/2	auto		
Ethernet1/0/3	auto		
Ethernet1/0/4	auto		
Ethernet1/0/5	auto		
Ethernet1/0/6	auto		
Ethernet1/0/7	auto		
Ethernet1/0/8	auto		

entry	describe	
Port	Ethernet port name	
Link type	Auto: Automatic consultations	
	Force-true: Point-to-point type	
	Force-false: Non-point-to-point type	

22.2.6. Spanning-tree agreement port configuration

This page can be used to configure enable or disable the tree generation function under the port. To display the "Spanning-tree agreement port configuration" page, click Spanning-tree configuration -> Spanning-tree Port configuration -> Spanning-tree agreement port configuration, click "Apply" to configure.

Spanning-tree agreement port configuration			
Port	Ethernet1/0/1 🗸		
Operation	Disable V		
	Apply		

entry	describe
Port	Ethernet port name
Operation	Enable: Port enable spanning tree function
	Disable: Port disables spanning tree functionality

22.3. Spanning-tree global configuration

22.3.1. Spanning-tree global agreement port configuration

This page uses the build tree function with global enable.

To display the "Spanning-tree global agreement port configuration" page, click Spanning-tree configuration -> Spanning-tree global configuration -> Spanning-tree global agreement port configuration, click "Apply" to configure.

Spanning-tree global agreement port configuration			
Operation Disable 🗸			
			Apply

entry	describe
Operation	Enable: enable spanning tree function
	Disable: disables spanning tree functionality

22.3.2. Forward-time configuration

This page can be used to configure forwarding delay time.

To display the "Forward-time configuration" page, click Spanning-tree configuration -> Spanning-tree global configuration -> Forward-time configuration, click "Apply" to configure.

Forward-time configuration			
Forward-time			
Operation	Default	~	
			Apply

entry	describe		
Forward-time	Size range :4-30, in seconds, the following conditions shall be met:		
	2 * (Bridge_Forward_Delay - 1.0 seconds) >= Bridge_Max_Age		
	Bridge_Max_Age >= 2 * (Bridge_Hello_Time + 1.0 seconds)		
Operation	configuration: Configure the above settings		
	Default: Restore default 15s		

Forward-time configuration	
Forward-time configuration	15

entry	describe
Forward-time configuration	Configuration of current forwarding delay time

22.3.3. Hello-time configuration

This page can be used to bpdu the configuration of the sending interval.

To display the "Hello-time configuration" page, click Spanning-tree configuration -> Spanning-tree global configuration -> Hello-time configuration, click "Apply" to configure.

Hello-time configuration			
Bridge hello time			
Operation	Default	~	
			Apply

entry	describe	
Bridge hello	Size range :1-10, in seconds, the following conditions shall be met:	
time	2 * (Bridge_Forward_Delay - 1.0 seconds) >= Bridge_Max_Age	
	Bridge_Max_Age >= 2 * (Bridge_Hello_Time + 1.0 seconds)	
Operation	configuration: Configure the above settings	
	Default: Restore default 2s	

Hello-time configuration	
Bridge hello time	2

entry	describe
Bridge hello time	Current HELLO Maximum Survival Time Configuration

22.3.4. Max age time configuration

This page can be used to configure the maximum aging time of BPDU messages.

To display the "Max age time configuration" page, click Spanning-tree configuration -> Spanning-tree global configuration -> Max age time configuration, click "Apply" to configure.

Max age time configuration			
Max age time			
Operation	Default	~	
			Apply

entry	describe	
Max age time	Size range :6-40, in seconds, the following conditions shall be met:	
	2 * (Bridge_Forward_Delay - 1.0 seconds) >= Bridge_Max_Age	
	Bridge_Max_Age >= 2 * (Bridge_Hello_Time + 1.0 seconds)	
Operation	configuration: Configure the above settings	
	Default: Restore default 20s	

Max age time configuration	
Max age time	20

entry	describe
Max age time	Configuration of current maximum ageing time

22.3.5. Max hop time configuration

This page can be used to BPDU the maximum number of hops that packets are forwarded in the spanning tree domain.

To display the "Max hop time configuration" page, click Spanning-tree configuration -> Spanning-tree global configuration -> Max hop time configuration, click "Apply" to configure.

Max hop time configuration				
Max hop time				
Operation	Default	~		
			Apply	

entry	describe
Max hop time	Numerical range :1-40
Operation	configuration: Configure the above settings
	Default: Restore default 20s

Max hop time configuration	
Max hop time	20

entry	describe
Max hop time	Maximum number of hops currently configured

22.3.6. Spanning tree mode configuration

This page is used to set the running mode of the switch spanning tree.

To display the "Spanning tree mode configuration" page, click Spanning-tree configuration -> Spanning tree global configuration -> Spanning tree mode configuration, click "Apply" to configure.

Spanning tree mode configuration				
Mode	Mstp 🗸			
Operation	Default	~		
		A	pply	

entry	describe
Mode	Generating tree protocol type: Mstp.Stp.Rstp
Operation	Configuration: Configure the above settings
	Default: Restore default configuration mode to mstp

Spanning tree mode	configuration
Mode	mstp

entry	describe
Mode	Current run spanning tree protocol type

22.3.7. Spanning tree cost-format configuration

This page is used to set the global configuration path cost format.

To display the "Spanning tree cost-format configuration" page, click Spanning-tree configuration -> Spanning-tree global configuration -> Spanning tree cost-format configuration, click "Apply" to configure.

Spanning tree cost-format configuration				
Mode	dot1t	~]	
				Apply

entry	describe
Mode	Path cost format:Dot1t.Dot1d

22.3.8. Priority configuration

This page is used to set the bridge priority of the spanning tree instance.

To display the "Priority configuration" page, click Spanning-tree configuration -> Spanning-tree global configuration -> Priority configuration, click "Apply" to configure.

Priority configuration				
Instance name				
Priority				
Operation	Default	~		
			Apply	

entry	describe
Instance name	Generate tree instance name
Priority	Numerical range :0-61440, and an integer multiple of 4096
Operation	Configuration: Configure the above settings
	Default: Restore default configuration priority 32768

22.4. Show spanning-tree

22.4.1. Instance information

This page can be used to view information for the specified instance.

To display the "Instance information" page, click Spanning-tree configuration -> Show spanning-tree -> Instance information, click "Apply" to view.

Instance informa	tion
Instance name	
	Apply

entry	describe
Instance name	Generate tree instance name

22.4.2. Revision-Level information

This page can be used to view configuration information for the spanning tree domain.

To display the "Revision-Level information" page, click Spanning-tree configuration -> Show spanning-tree -> Revision-Level information, click "Apply" to view.

Information feedback window			
Switch# show	spanning-tree mst config		
Name	name		
Revision	0		
Instance	Vlans Mapped		
00	1-4094		

23. MRPP configuration

23.1. MRPP global configuration

23.1.1. MRPP global switch configuration

This page is used to enable or disable MRPP protocols.

To display the "MRPP global switch configuration" page, click MRPP configuration->MRPP global configuration, click "Apply" to configure.

MRPP global switch configuration		
Operation	Disable 🗸	
		Apply

entry	describe
Operation	Enable: Enable MRPP protocol functionality
	Disable: Close MRPP Protocol Function

MRPP global switch configuration	
MRPP global configuration	disable

entry	describe
MRPP global	disable: Current mrpp protocol status is closed
configuration	enable: Current mrpp protocol status opens

23.1.2. MRPP poll time configuration

This page can be used to configure MRPP query time.

To display the "MRPP poll time configuration" page, click MRPP configuration->MRPP global configuration->MRPP poll time configuration, click "Apply" to configure.

MRPP poll time configuration			
MRPP poll time			
Operation	Default	~	
			Apply

entry	describe	
MRPP poll time	range: 20-200, unit milliseconds	
Operation	Configuration: Apply the above settings	
	Default: Restore default ms 100	

MRPP poll time configuration	
MRPP poll time	100

entry	describe
MRPP poll time	Current configured query time

23.1.3. MRPP domain id configuration

This page is used to set the ID number of the MRPP domain.

To display the "MRPP domain id configuration" page, click MRPP configuration->MRPP global configuration->MRPP domain id configuration, click "Apply" to configure.

MRPP domain id configuration			
MRPP domain			
Operation	Remove	~	
			Apply

entry	describe
MRPP domain	ID range :1-4096
Operation	Configuration: Apply the above settings
	Remove: Delete configured domain ID

MRPP domain id configuration		
Index	Domain ID	

entry	describe
Domain ID	Domain ID range :1-4096

23.2. MRPP port configuration

23.2.1. MRPP port property configuration

This page can be used to configure the primary and secondary ports of the MRPP ring. To display the "MRPP port property configuration" page, click MRPP configuration->MRPP port configuration->MRPP port property configuration, click "Apply" to configure.

MRPP port property configuration			
Port	Ethernet1/0/1	~	
MRPP domain			
MRPP port property	primary 🗸		
Operation	Remove	~	
			Apply

entry	describe
Port	Ethernet port name
MRPP domain	MRPP domain ID, range :1-4096
MRPP port property	Primary: Main port
	Secondary: Secondary port
Operation	Configuration: Apply the above configuration
	Remove: Delete the above configuration

MRPP port property configuration
Index Domain ID Port Name Property

entry	describe	
Domain ID	MRPP domain ID, range :1-4096	
Port Name	Ethernet port	
Property	Primary: Main port	
	Secondary: Secondary port	

23.3. MRPP domain configuration

23.3.1. MRPP control vlan config

This page can be used to configure control VLAN for MRPP rings

To display the "MRPP control vlan configuration" page, click MRPP configuration->MRPP domain configuration->MRPP control vlan configuration, click "Apply" to configure.

MRPP control vlan config			
MRPP domain	~		
VLAN ID			
Operation	Remove	~	
			Apply

entry	describe
MRPP domain	MRPP domain ID, range created :1-4096
VLAN ID	VLAN ID, range :1-4094
Operation	Configuration: Apply the above configuration
	Remove: Delete the above configuration

MRPP control vlan config Index Domain ID Control-VLAN

entry	describe
Domain ID	MRPP domain ID, range :1-4096
Control-VLAN	Scope of control VLAN, for current MRPP domain configuration :1-4094

23.3.2. MRPP node mode config

This page can be used to configure MRPP nodes.

To display the "MRPP node mode configuration" page, click MRPP configuration->MRPP domain configuration->MRPP node mode configuration, click "Apply" to configure.

MRPP node mode config			
MRPP domain	~		
MRPP node mode	ma	ster 🔊	/
			Apply

entry	describe	
MRPP domain	MRPP domain ID, range :1-4096	
MRPP node mode	master: Master node	
	transit: Transmission node	

MRPP no	de mode config	
Index	Domain ID	Node mode

entry	describe
Domain ID	MRPP domain ID, range :1-4096
Node mode	master: Master node
	transit: Transmission node

23.3.3. MRPP hello timer config

This page can be used to MRPP Hello the configuration of message sending intervals. To display the "MRPP hello timer configuration" page, click MRPP configuration->MRPP domain configuration->MRPP hello timer configuration, click "Apply" to configure.

MRPP hello timer config			
MRPP domain	~		
MRPP hello timer range			
Operation	Remove	~	
			Apply

entry	describe	
MRPP domain	MRPP domain ID range :1-4096	
MRPP hello timer range	Interval time range :1-100 seconds	
Operation	Configuration: Apply the above configuration	
	Remove: Delete the above configuration and restore the default	
	configuration to 1 second	

MRPP he	llo timer config	
Index	Domain ID	Hello-Timer

entry	describe
Domain ID	MRPP domain ID range :1-4096
Hello-Timer	Hello message sending interval when the current configuration takes effect

23.3.4. MRPP fail timer config

This page is used MRPP configure the health message receive timeout. To display the "MRPP fail timer configuration" page, click MRPP configuration->MRPP domain configuration->MRPP fail timer configuration, click "Apply" to configure.

MRPP fail timer config			
MRPP domain	~		
MRPP fail timer range			
Operation	Remove	~	
			Apply

entry	describe	
MRPP domain	MRPP domain ID range : 1-4096	
MRPP fail timer range	Interval time range :1-300 seconds	
Operation	Configuration: Apply the above configuration	
	Remove: Delete the above configuration and restore the default	
	configuration to 3 second	

MRPP fail timer config Index Domain ID FAIL-Timer

entry	describe
Domain ID	MRPP domain ID range :1-4096
FAIL-Timer	Receive timeout when the current configuration takes effect

23.3.5. MRPP domain switch config

This page can be used to enable or disable MRPP rings.

To display the "MRPP domain switch config" page, click MRPP configuration->MRPP domain configuration->MRPP domain switch config, click "Apply" to configure.

MRPP domain switch config		
MRPP domain	~	
Operation	Disable 🗸	
		Apply

entry	describe
MRPP domain	MRPP domain ID range :1-4096
Operation	Enable: Enable the corresponding MRPP ring
	Disable: Disable the corresponding MRPP ring

MRPP domai	in switch configuration	
Index	Domain ID	Flag

entry	describe	
Domain ID	MRPP domain ID range :1-4096	
Flag	The enable state disable or enable of the currently configured active MRPP domain	

23.4. MRPP configuration display

23.4.1. MRPP display

This page can be used to view configuration information for MRPP domains. To display the "MRPP display" page, click MRPP configuration->MRPP domain configuration->MRPP

display, click "Apply" to view.

MRPP display		
MRPP domain	all 🗸	
Apr		Apply
Information feedback wi	ndow	
Switch# show mrpp		
Poll time : 100 (ms)		

entry	describe	
Domain ID	MRPP domain ID range :1-4096	

23.4.2. MRPP statistics display

This page can be used to view statistics of MRPP domain data and status changes. To display the "MRPP statistics display" page, click MRPP configuration->MRPP domain configuration->MRPP statistics display, click "Apply" to view.



entry	describe	
Domain ID	MRPP domain ID range :1-4096	

23.4.3. Clear MRPP statistics

This page can be used to clear statistics for MRPP domains.

To display the "Clear MRPP statistics" page, click MRPP configuration->MRPP domain configuration->Clear MRPP statistics, click "Apply" to configure.

Clear MRPP statistics		
MRPP domain	all 🗸	
		Apply

24. ULPP configuration

24.1. ULPP global configuration

24.1.1. ULPP group configuration

This page can be used to add or delete ULPP groups.

To display the "ULPP group configuration" page, ULPP configuration ->ULPP global configuration->ULPP group configuration, click "Apply" to configure.

ULPP group configuration			
ULPP group			
Operation	Add	~	
			Apply

entry	describe	
ULPP group	Group ID size range :1-48	
Operation	Add: Add ULPP groups	
	Remove: Delete ULPP groups	

ULPP group configuration	
ULPP group	1

entry	describe	
ULPP group	ULPP groups created	

24.2. ULPP port configuration

24.2.1. ULPP port property configuration

This page can be used to set the port as the master-slave port of the ulpp group. It can also enable or disable receiving MAC address and ARP update packets, can also configure a control VLAN for the port. To display the "ULPP port prperty configuration" page, ULPP configuration ->ULPP port configuration, click "Apply" to configure.

ULPP port property configuration			
Port	Ethernet	1/0/1 🗸	
ULPP port flush mode mac 🗸			
ULPP port control vlan			
ULPP group	1 ~]
ULPP port mode	master ~	·	
Operation	Remove	~]
		Apply	

entry	describe	
Port	Ethernet port name	
ULPP port flush mode	mac: Receive mac update packets	
	arp: Receive arp more packets	
ULPP port control vlan	vlan created	
ULPP group	ULPP groups created	
ULPP port mode	master: Main port	
	slave: Slave port	
Operation	Configuration: Apply the above configuration	
	Remove: Delete the above configuration	

24.3. ULPP group configuration

24.3.1. ULPP group description configuration

This page can be used to configure the description name for ULPP group.

To display the "ULPP group description configuration" page, ULPP configuration ->ULPP group configuration->ULPP group description configuration, click "Apply" to configure.

ULPP group description configuration		
ULPP group	1 ~	
ULPP group description		
Operation	Remove V	
	Apply	

entry	describe	
ULPP group	ULPP groups created	
ULPP group description	1-128 characters in length	
Operation	Configuration: Apply the above configuration	
	Remove: Delete the above configuration	

ULPP group description configuration		
ULPP group	ULPP group description	
1		

entry	describe
ULPP group	ULPP groups created
ULPP group description	Description of ULPP groups currently set

24.3.2. ULPP group property configuration

This page can be used to configure the ulpp group properties of preemption mode, preemption delay, protection VLAN, control VLAN, flush mode, etc.

To display the "ULPP group description configuration" page, ULPP configuration ->ULPP group configuration, click "Apply" to configure.

ULPP group property configura	ation		
ULPP group	1 ~]
ULPP group preemption mode	on 🗸		
ULPP group preemption delay			
ULPP group control vlan			
ULPP group protect vlan			
ULPP group flush mode	mac 🗸		
Operation	Remove	• v	
		Apply	

entry	describe	
ULPP group	ULPP groups created	
ULPP group preemption mode	on: Preemptive mode enabled	
	off: Disable Preemptive Mode	
ULPP group preemption delay	Delay time range :1-600, per second	
ULPP group control vlan	Created VLAN,VLAN ID between 1-4094	
ULPP group protect vlan	MSTP instance list, value range: 1-4094	
ULPP group flush mode	mac: Send mac update packet	
	arp: Send arp update packet	
Operation	Configuration: Apply the above configuration	
	Remove: Delete the above configuration	

 ULPP group property configuration

 ULPP group ULPP group preemption mode
 ULPP group preemption delay

 1
 OFF

 30
 1

entry	describe	
ULPP group	Ulpp group created	
ULPP group preemption mode	on: Preemptive mode enabled	
	off: Disable Preemptive Mode	
ULPP group preemption delay	Delay time for current configuration	
ULPP group control vlan	ULPP group control VLAN currently set	
ULPP group flush mode	mac: Send mac update packet	
	arp: Send arp update packet	
	ALL: Send mac and arp update packet	

24.4. ULPP configuration display

24.4.1. ULPP group configuration display

This page can be used to view configuration information for ULPP groups. To display the "ULPP group description configuration" page, ULPP configuration ->ULPP configuration display->ULPP group configuration display, click "Apply" to view.

	ULPP group co	nfiguration	display		
	ULPP group		all 🗸		
				Apply	
Information f	eedback window				
Switch# show	w ulpp group				
ULPP group :	1 information:				
Description	:				
Preemption 1	mode: OFF				
Preemption (delay: 30s				
Control VLA	N: 1				
Flush packet	t: MAC ARP				
Protected VI	LAN: Reference	Instance			
Member	Role	State	Trac	k-cfm-leve	el

24.4.2. ULPP port statistics display

This page can be used to view ULPP port statistics.

To display the "ULPP group description configuration" page, ULPP configuration ->ULPP configuration display->ULPP port statistics display, click "Apply" to view.

ULPP port statistics display		
Port	Ethernet1/0/1	~
		Apply

24.4.3. ULPP port property display

This page can be used to view ULPP port configuration information.

To display the "ULPP group description configuration" page, ULPP configuration ->ULPP configuration display->ULPP port property display, click "Apply" to view.

Information fe	edback window	
Switch# show	ulpp flush-rec	eive-port •
Portname	Туре	Control Vlan

24.4.4. ULPP port statistics clear

This page can be used to clear statistics of ULPP related data on the port.

To display the "ULPP group description configuration" page, ULPP configuration ->ULPP configuration display->ULPP port statistics clear, click "Apply" to view.

ULPP port statistics clear		
Port	Ethernet1/0/	1 🗸
		Apply

25. ULSM configuration

25.1. ULSM global configuration

25.1.1. ULSM group configuration

This page can be used to create or delete ULSM groups.

To display the "ULSM group configuration" page, click ULSM configuration ->ULSM global configuration->ULSM group configuration, click "Apply" to configure.

ULSM group config	juration	I	
ULSM group			
Operation	Add	~	
			Apply

entry	describe	
ULSM group	Group ID range :1-32	
Operation	Add: Create a ULSM group	
	Remove: Removing ULSM groups of corresponding ID	

ULSM group configuration	
ULSM group	1

entry	describe
ULSM group	ULSM groups created

25.2. ULSM port configuration

25.2.1. ULSM port property configuration

This page can be used to add uplink or downlink ports for ULSM groups that have been created. To display the "ULSM group configuration" page, click ULSM configuration ->ULSM port configuration, click "Apply" to configure.

ULSM port property configuration			
Port	Ethernet1/0/1 V		
ULSM group	1 ~		
ULSM port property	downlink 🗸		
Operation	Remove ~		
	Apply		

entry	describe	
Port	Ethernet port name	
ULSM group	ULSM groups created	
ULSM port property	uplink: Uplink port	
	downlink: Downlink port	
Operation	Configuration: Apply the above settings	
	Remove: Delete the above	

ULSM port property					
Port	ULSM	group	ULSM	port	property
Ethernet1/0/1	1		uplink		

entry	describe
Port	Ethernet port name
ULSM group	ULSM groups created
ULSM port property	Current ULSM groups correspond to configured upper and lower ports uplink: Uplink port downlink: Downlink port

25.3. ULSM configuration display

25.3.1. ULSM display

This page can be used to view the current status of the ULSM group and the status of the upper and lower ports within the group.

To display the "ULSM group configuration" page, click ULSM configuration ->ULSM port configuration, click "Apply" to view.

	ULSM display		
	ULSM group	all 🗸	
		Apply	·
Information feedbac	k window		
Switch# show ulsm ULSM group 1 stat	e: Down		
Port	Role	State	ShutDown-by-ULSM
Ethernet1/0/	1 UpLink	Down	

26. Authentication configuration

26.1. RADIUS client configuration

26.1.1. RADIUS global configuration

RADIUS global configuration module, users in this module can configure the global RADIUS function services.

RADIUS configuration	
Authentication status	Disable ~
Accounting	Disable V
Radius key operation	~
RADIUS key	
System recovery time	5
RADIUS Retransmit times	3
RADIUS server timeout	3
	Apply

AAA server status					
the status of the aaa	disable				
the status of the radius accounting	disable				
radius-server timeout	3				
radius-server retransmit	3				
radius-server dead-time	5				
radius-server authentication host	192.168.2.200 port:23 primary				

Authentication status	Enable Enable RADIUS certification services		
	Disable	Disabling RADIUS certification services	
Accounting	Enable	Enable RADIUS billing services	
	Disable	Disabling RADIUS billing services	
Radius key operation	Add	Add RADIUS key	
	Remove	Delete RADIUS key	
RADIUS key	Key string ,1-64 characters		
System recovery time	Radius service recovery time from downtime to accessibility, 1-255 minutes		
RADIUS Retransmit	Radius authentication packet retransmission time, 1-100 seconds		
times			
RADIUS server timeout	The corresponding time of the radius server, 1-100 seconds		

26.1.2. RADIUS authentication configuration

RADIUS authentication configuration module, users in this module can configure the RADIUS authentication server.

RADIUS authentication server configuration							
Authentication s	erver IP						
Authentication s	erver port(optional)						
Primary authent	ication server	Primary authentication server V		~			
Operation		Add	~				
						A	pply
ADIUS server co	onfiguration list						
erver IP	Port num		Prima	rv s	erver		

Authentication server IP	The address of IPv4 or IPv6 of the radius authentication server				
Authentication server	Port number of radius authentication server(optional),0-65535				
port					
	Primary authentication	Specify radius server as primary			
Primary authentication	server	authentication server			
erver Non-Primary		Specify radius server as non-primary			
	authentication server	authentication server			
Organistica	Add	Add operations			
Operation	Remove	Delete operations			

26.1.3. RADIUS accounting configuration

Radius authentication and accounting module, users in this module can configure the RADIUS billing server.

RADIUS accounting server configuration						
Accounting server IP						
Accounting server port(optional)						
Primary accounting server	Primary accounting server ~					
Operation	Add	~				
						Apply
RADIUS accounting server config	uratior	ı list				
Server IP Port num		Prir	mary serve	r		

Accounting server IP	Radius authentication server IPv4 or IPv6 address			
Accounting server port	Radius authentication serv	Radius authentication server port number (optional),0-65535		
Primary accounting	Primary accounting	Specify radius server as primary accounting		
server	server	server		
	Non-Primary accounting	Specify radius server as non-primary		
	server	accounting server		
Operation	Add	Add operations		
	Remove	Delete operations		

26.2. TACACS server configuration

26.2.1. TACACS global configuration

TACACS global configuration module, users in this module can configure the global TACACS function services.

TACACS configuration				
TACACS key				
TACACS server timeout	3			
Operation	Remove	~		
				Apply
TACACS server status				
the status of the tacacs				
tacacs-server timeout				3

TACACS key	TACACS authentication key ,1-16 characters		
TACACS server timeout	TACACS authentication timeout ,1-60 seconds, default 3 seconds		
Operation	Add Add operations		
	Remove	Delete operations	

26.2.2. TACACS server host configuration

TACACS server configuration module, users in this module can configure the TACACS authentication server.

TACACS server configuration						
Authentication server IP						
Authentication server port(optional)						
Primary authentication server	Primary authentication server		~			
Operation	Add	~				
					Ар	ply

Authentication server IP	TACACS authentication ser	TACACS authentication server IPv4 address, decimal point			
Authentication server port	TACACS authentication server port number (optional),0-65535				
Primary authentication	Primary accounting	Specify TACACS server as primary			
server	server	accounting server			
	Non-Primary accounting	Specify TACACS server as non-primary			
	server	accounting server			
Operation	Add	Add operations			
	Remove	Delete operations			

26.3. 802.1x configuration

26.3.1. 802.1x Global configuration

802.1 x Global Configuration Module, users in this module can configure the global 802.1 x function services.

802.1x configuration		
802.1x status	Disable 🗸	
Maximum retransmission times of EAP-request/identiry	2	
Reauthenticate client periodically	Disable 🗸	
Holddown time for authentication failure	10	
Reauthenticate client interval	3600	
Resending EAP-request/identity interval	30	
EAP relay authentication mode	forbid 🗸	
Private client	forbid 🗸	
MAC filtering	forbid 🗸	
802.1x unicast	Disable 🗸	
		Apply

802.1x status	Boot or turn off 802.1 x function
Maximum retransmission times of EAP-	Scope 1-10
request/identiry	
Reauthenticate client periodically	Start or close periodic recertification
Holddown time for authentication failure	Range 1-65535 seconds, default 10 seconds
Reauthenticate client interval	Range 1-65535 seconds, default 3600 seconds
Resending EAP-request/identity interval	Range 1-65535 seconds, default 30 seconds
EAP relay authentication mode	Ban or permit EAP relay authentication
Private client	Prohibit or allow private clients
MAC filtering	Ban or permit MAC address filtering
802.1x unicast	Disable or enable 802.1 x unicast teleport function

26.3.2. 802.1x port authentication configuration

802.1 x port authentication configuration module, in this module, users can configure the 802.1x function of the specified port

802.1x port configuration	
Port	Ethernet1/0/1 V
802.1x status	Disable V
Authentication type	force-unauthorized V
Authentication mode	Port-based V
Port maximum user	1
Guest VLAN ID	0
	Apply

Port	Designated port number			
802.1x status	Boot or close 802.1 x on	3oot or close 802.1 x on this port		
Authentication type	force-unauthorized	orce-unauthorized Mandatory Unauthorized		
	force-authorized	Mandatory authorization		
	Auto(802.1x) automatism (802.1x authorization)			
Authentication	Port-based	Based on port		
mode	Mac-based	Based on MAC		
Port maximum user	Maximum number of users allowed to connect to ports ,1-256, default 1			
Guest VLAN ID	Guest VLAN ,0-4094, default 0			

26.3.3. 802.1x port MAC configuration

802.1x port MAC configuration module, users in this module can add or delete port 802.1 x functions MAC specified ports.

802.1x port MAC configuration				
Port	Ethernet1/0/1 V			
Mac				
Operation	Add MAC filter entry	~		
			Apply	

Port	Specifies the port number
MAC	MAC address to operate
Operation	Add or delete port MAC address filter table items

26.3.4. 802.1x port status list

802.1x port MAC status list, the user can view 802.1 status information on x specified port and authenticate 802.1 x in this module.

802.1x port status list			
Port	Ethernet1/0/1 V		
802.1x status	Disable		
Authentication type	NULL		
Authentication status	Unauthenticated		
Authentication mode	No authentication mode		
	Reauthenticate		

26.4. MAB configuration

26.4.1. MAB ENABLE configuration

MAB enable configuration module, users in this module can MAB the function of global enable and specified port enable operation.

MAB global enable configuration					
MAB global enable Enab		ble	~		
Appl					pply
MAB port enable confi	MAB port enable configuration				
Port	Etherr	net1/	0/1	~]
MAB port enable	Enable	e 🗸			
				1	Apply

MAB global enable	Global enable or disable MAB function	
Port	Specifies the port number	
MAB port enable	Function on or off MAC specified port	

26.4.2. MAB Authentication configuration

MAB user authentication configuration module, users in this module can configure the MAB user authentication mode.

MAB Authentication configuration			
MAB Authentication TYPE MAC address ~			
username			
password			
	Apply		

МАВ	Mac address	Authentication based on MAC address		
Authentication	Username and	Authentication based on username and password (to be		
ТҮРЕ	password	configured)		
username	user name for authentication ,1-32 characters			
password	password for authentication ,1-32 characters			

26.4.3. MAB parameter configuration

MAB parameter configuration module, users in this module can configure the parameters of the MAB function.

MAB parameter configuration					
Port	Ethernet1/0/1 V				
parameter type	guest vlan range	~			
value					
Enable 🗸					
			Apply		

Port	Specify port name		
parameter type	guest vlan range	VLAN operation for guest	
	Max binding value	Operation of maximum binding on ports	
value	After the parameter type is selected, the corresponding parameter value range		
	can be set		
Enable Disable	Boot or close port MAB p	parameter configuration	

MAB parameter configuration				
parameter type	reauth-period 🗸			
value				
Enable 🗸				
			Apply	

parameter	reauth period	MAB time interval for re-authentication after failed authentication			
type	Offline-detect	Detect the scan time of each port online status, 0 does not detect			
	Quiet-period	onfigure the silence time after mAb authentication failure			
	Stale-period	onfigure the time to delete bound users after the mAb port is			
		closed			
	Linkup-period	Configure the restart time range after mAb port shutdown			
value	After the parameter type is selected, the corresponding parameter value can be set				
Enable Disable	Boot or close global MAB parameter configuration				

authentication mab		
check type	radius 🗸	
Enable 🗸		
		Apply

Check type	MAC address authentication uses radius or none to verify user login
Enable Disable	Start or close validation mode configuration

spoofing-garp-check			
spoofing-garp-check	Enable	~	
	(Ap	oply

spoofing-garp-check	Activate or close check fake free ARP configuration
---------------------	-----------------------------------------------------

26.4.4. MAB show

MAB display module, users can display mAb status of specified port or all ports in this module

	MAB show	I				
	Port all	~				
					Apply	
Informa	tion feedba	ck window				
Switch	# show mac	-authentic	ation-b	ypass		
The Nu	umber of a	ll binding	fis O			
MAC		Inter	:Iace	LV 	.an 1D	State

Displays information MAB the specified port or all ports

27. DOS attack protection configration

27.1. Source IP equal destination IP DOS attack protection configration

Source IP equal to destination IP anti DoS attack configuration module, the user can start or turn off the DOS attack function IP equal to the destination in this module.

S	Source IP equal destination IP DOS attack protection configration				
C	OOS attack protection status)isable 🗸		
				Apply	
	DOS attack protection status				
	DOS attack protection status	Disable			
Inforr	nation feedback window				
Swite	h# config t				
Swite	ch(config)# no dosattack-check :	srcip-eq	qual-dst	ip enab	

27.2. Source port equal destination port DOS attack protection configration

Source port equal to destination port anti DoS attack configuration module, users in this module can start or close the source port equal to the destination port DOS attack function.

Sour	Source port equal destination port DOS attack protection configration				
DOS	attack protection status	Disable 🗸			
			Apply		
	DOS attack protection status				
	DOS attack protection status Disable	e			
Informat	nformation feedback window				
Switch#	config t				
Switch(config)# no dosattack-check srcport-e	qual-dstp	ort enable		

27.3. TCP DOS attacks on invalid flags configration

TCP DoS attack invalid flag bit configuration module, users in this module can start or close the DOS attack function to check unauthorized TCP tags.



27.4. ICMP DOS attack protection configration

ICMP anti DoS attack configuration module, the user can start or turn off the DOS attack check function of the anti- ICMP fragment in this module.

ICMP DOS attack protect	ion configra	tion
DOS attack protection st	atus Ena	able 🗸
		Apply
L		
DOS attack protection st	atus	
DOS attack protection st	atus E	nable
Information feedback window		
Switch# config t		
Switch(config)# dosattack-che	ck icmp-at	tacking

27.5. ICMP packet-size configration

The maximum ICMP message configuration module is allowed, users can configure the maximum net length of icmpv4 packets in this module

Packet-size 64		
	Apply	
Packet-size		1
Packet-Size		
Packet-size	64	
		_
Information feedback wir	ndow	
Switch# config t		
Switch (config) # dosat	tack-check icmpV4-si	70 (

Packet-size Maximum net length of allowed ICMPv4 packets,64-1023, Default 512

27.6. First fragment IP packet DOS attack protection configration

The first IP packet fragment anti DoS attack configuration module, the user can start or turn off the DOS attack function against the first IP message fragment in this module.

First fragment IP packet DOS attack protection configration				
DOS attack protection status	Enable 🗸			
	Apply			

DOS attack protection status		
DOS attack protection status	Enable	

```
Information feedback window
Switch# config t
Switch(config) # dosattack-check ipv4-first-fragment enable
```
28. SSL config

28.1. IP HTTP server configuration

HTTP server configuration module, the user can start or stop the HTTP service of the switch by using this module again

IP HTTP server configuration	n
IP HTTP server status	Enable 🗸
	Apply
<u>.</u>	
Information feedback wind	ow
IP HTTP server status	Enable
Information feedback wind	ow
Switch# config t	
Switch(config)# ip http	p server
web server has worked	

28.2. SSL global configuration

SSL function switch configuration module, users in this module can start or close the switch SSL service function.

SSL global configuration		
SSL status	Enable 🗸	
	Apply	

Information feedback	window	
SSL status	Enable	
Information feedback	window	
Switch# config t Switch(config)# ip web server is on	http secure-server	

28.3. SSL server monitor port configuration

SSL server monitor port number start configuration module, users can configure SSL server listening port number in this module

SSL server monitor port configuration			
port number			
Operation	Add	~	
			Apply

Information feedback window	
port number	443

Port	Specifies the port number	
Operation	Add	Add operations
	Remove	Delete operations

28.4. SSL secure-ciphersuite configuration

SSL encryption suite configuration module, users can configure the encryption suite type of SSL service in this module.

secure-ciphersuite configuration			
secure-ciphersuite type	aes25	6-sha	~
Operation	Add	~	
			Apply

Information feedback window ip http secure-ciphersuite aes256-sha

secure-ciphersuite	aes256-sha	aes256-sha encryption is used
type	ecdhe-rsa-aes256-sha	ecdhe-rsa-aes256-sha encryption is used
Operation	Add	Add operations
	Remove	Delete operations

29. sFlow configuration

29.1. sFlow collector global address configuration

This page can be used to configure the global sFlow analyzer address.

To display the "sFlow collector global address configuration" page, sFlow configuration->sFlow collector global address configuration, click "Apply" to configure.

sFlow collector global address configuration	
IP address	
destination port NO.	
Operation	Configuration ~
	Apply

entry	describe
IP address	sFlow Analyzer Address
Destination port NO.	Range between 1025 and 65535
Operation	Configuration: User self-configuration
	Default: Restore default configuration

29.2. sFlow collector port address configuration

This page can be used to configure port sFlow analyzer address.

To display the "sFlow collector port address configuration" page, sFlow configuration->sFlow collector port address configuration, click "Apply" to configure.

sFlow collector port address configuration		
Port	Ethernet1/0/1 V	
IP address		
destination port NO.		
Operation	Configuration ~	
	Apply	

entry	describe
Port	Ethernet port number
IP address	sFlow Analyzer Address
Destination port NO.	Range between 1025 and 65535
Operation	Configuration: User self-configuration
	Default: Restore default configuration

29.3. sFlow agent address configuration

This page can be used for sFlow agent configuration.

To display the "sFlow agent address configuration" page, sFlow configuration->sFlow agent address configuration, click "Apply" to configure.

sFlow agent address configuration		
IP address		
Operation	Configuration ~	
	Apply	

entry	describe	
IP address	sFlow agent address	
Operation	Configuration: User self-configuration	
	Default: Restore default configuration	

29.4. sFlow priority configuration

This command is used to set the priority of the sample message. To display the "sFlow priority configuration" page, sFlow configuration->sFlow priority configuration, click "Apply" to configure.

sFlow priority configuration		
agent priority value		
Operation	Configuration ~	
	Apply	,

entry	describe	
agent priority value	Range :0-3	
Operation	Configuration: User self-configuration	
	Default: Restore default configuration	

29.5. sFlow header length configuration

This page can be used to configure the length of header packets copied in sFlow data sampling. To display the "sFlow header lengh configuration" page, sFlow configuration->sFlow header lengh configuration, click "Apply" to configure.

sFlow header length configuration	
Port	Ethernet1/0/1 V
header length	
Operation	Configuration ~
	Apply

entry	describe	
Port	Ethernet port name	
header length	Length range :32-256	
Operation	Configuration: User self-configuration	
	Default: Restore default configuration	

29.6. sFlow data length configuration

This page is used to configure sflow packet length.

To display the "sFlow header lengh configuration" page, sFlow configuration->sFlow data lengh configuration, click "Apply" to configure.

sFlow data length configuration	
Port	Ethernet1/0/1 V
data length	
Operation	Configuration ~
	Apply

entry	describe
Port	Ethernet port name
data length	Length range :500-1470
Operation	Configuration: User self-configuration
	Default: restore default configuration, default value is 1400

29.7. sFlow rate configuration

This page can be used to configure port hardware sampling rates.

To display the "sFlow rate configuration" page, sFlow configuration->sFlow rate configuration, click "Apply" to configure.

sFlow rate configuration		
Port	Ethernet1/0/1 V	
direction	input 🗸	
rate value		
Operation	Configuration ~	
	Apply	

entry	describe
Port	Ethernet port name
direction	Input: receive data
	Output: send data
rate value	Rate range :1000-16383500
Operation	Configuration: User self-configuration
	Default: Restore default configuration

29.8. sFlow counter interval configuration

This page can be used to configure sFlow statistical sampling intervals. To display the "sFlow counter interval configuration" page, sFlow configuration->sFlow counter interval configuration, click "Apply" to configure.

sFlow counter interval configuration	
Port	Ethernet1/0/1 V
counter interval	
Operation	Configuration ~
	Apply

entry	describe
Port	Ethernet port name
counter interval	Sampling interval range :20-120
Operation	Configuration: User self-configuration
	Default: Restore default configuration

29.9. sFlow analyzer configuration

This page can be used for globally enabled sFlow analyzers. To display the "sFlow analyzer configuration" page, sFlow configuration->sFlow analyzer configuration, click "Apply" to configure.

sFlow analyzer configuration		
Operation	Configuration ~	
		Apply

entry	describe
Operation	Configuration: Function Enable
	Remote: Function disabled

30. IPv6 security ra configuration

30.1. IPv6 security ra global configuration

Launch the global IPv6 security RA module, the user can start or close the global IPv6 security RA function in this module.

IPv6 security ra global configuration					
Operation	Enable V				
	Apply				
Information feedback window					
Switch# config					
Switch(config)#	ipv6 security-ra enable				

30.2. IPv6 security ra port configuration

Start port IPv6 security RA module, the user can start or close the security RA function IPv6 the specified port in this module.

	IPv6 security ra port configuration				
	Port	Ethernet1/0/1	~		
	Operation	Enable 🗸			
			Apply		
Information f	eedback windo	w			
Switch# con:	fig				
Switch(conf:	ig)# interfac	e Ethernet	1/0/1		
Switch(conf:	ig-if-etherne	et1/0/1)# ip	pv6 securi	ty-ra	enable

Port	Specifies the port number		
Operation	Enable	Start operation	
	Disable	Close operation	

30.3. Show IPv6 security ra

Show IPv6 security RA configuration module, the user can display the specified port or global IPv6 security RA function configuration information in this module.

	-				_
	show IPv6 security ra				
	Port	Ethernet1/0/	/1 🗸]
				Apply]
Information feed	lback wir	ldow			
Switch# config	1				
Switch(config)	# show	ipv6 secu:	rity-ra	interface	Ethernet1/0/1
IPv6 security	RA info	rmation:			
Global IPv6 Security RA State: enabled					
IPv6 Security RA State: Yes					
Switch# config	1				
- Switch(config)	# show	ipv6 secu:	rity-ra	interface	Ethernet1/0/1
IPv6 security RA information:					
Global IPv6 Se	ecurity	RA State:	enable	d	
IPv6 Security	RA Stat	e: Yes			

Port Specifies the port number ALL represents all

31. Device log message

31.1. Show device log message

View device log information module, where users can view system key logs and warning logs.

Show device log message			
Level	critical	~	
Begin			
End			
			Apply

Level	critical Key-level log information		
	warnings	Warning Level Log Information	
Begin	To see where the log information starts		
End	To see the end location of the log information		

31.2. Clear logging in logbuff channel

Clears all log message modules in the buffer, users in this module can clear all log messages in the buffer.



CE Mark Warning: This is a Class A product. In home environment, this product may cause radio interference. In this case, the user may be required to take appropriate measures.

Hereby Assmann Electronic GmbH, declares that the Declaration of Conformity is part of the shipping content. If the Declaration of Conformity is missing, you can request it by post under the below mentioned manufacturer address.

www.assmann.com Assmann Electronic GmbH Auf dem Schüffel 3 58513 Lüdenscheid Germany

