

HR-SWTG3424S

24-Gigabit Port + 4-10Gigabit SFP Port

Web Manual

Ver. 1.0

Revision history



Date	Version	Description
Feb. 24, 2021	V 1.0	The first edition



Contents

HR-SWTG3424S1
24-Gigabit Port + 4-10Gigabit SFP Port1
Web Manual1
Ver. 1.0 1
1 Foreword9
1.1 Target Audience9
1.2 Manual Convention
2 Web Page Login10
2.1 Log in the Network Management Client10
2.2 Constitution of Client Interface10
2.3 Navigation Bar on Web Interface11
3 Status
3.1 System Information18
3.2 Statistics
3.3 MAC Address Table
3.4 Reboot
3.5 Management IP Address21
4 Network 21
4.1 DNS
4.2 System Time
5 Port24
5.1 Port Setting24
5.2 Error Disabled25
5.3 Link Aggregation26
5.3.1 Group
5.3.2 Port Setting28
5.3.3 LACP
5.4 EEE
5.5 Jumbo Frame
5.6 Port Security

HRUÍ

5.7 Protected Port	
5.8 Storm Control	35
5.9 Mirroring	
6 VLAN	
6.1 VLAN	
6.1.1 Create VALN	
6.1.2 VLAN Configuration	40
6.1.3 Membership	
6.1.4 Port Setting	43
6.2 Voice VLAN	45
6.3 Protocol VLAN	50
6.4 MAC VLAN	54
6.5 Surveillance VLAN	57
6.6 GVRP	59
6.6.1 Property	60
6.6.2 Membership	61
6.6.3 Statistics	62
7 MAC Address Table	62
7.1 Dynamic Address	63
7.2 Static Address	64
7.3 Filtering Address	65
7.4 Port Security Address	65
8 Spanning Tree	66
8.1 Property	67
8.2 Port Setting	68
8.3 MST Instance	70
8.4 MST Port Setting	71
8.5 Statistics	75
9 Discovery	75
9.1 LLDP	76
9.2 Port Setting	77
9.3 MED Network Policy	

HRUI

9.4 MED Port Setting	80
9.5 Packet View	
9.6 Local Information	82
9.7 Neighbor	83
9.8 Statistics	
10 DHCP	84
10.1 Property	
10.2 IP Pool Setting	87
10.3 VLAN IF Address Group Setting	
10.4 Client List	
10.5 Client Static Binding Table	
11 Multicast	
11.1 General	
11.1.1 Property	
11.1.2 Group Address	90
11.1.3 Router Port	
11.1.4 Forward All	
11.1.5 Throttling	93
11.1.6 Filtering Profile	
11.2 IGMP Snooping	94
11.2.1 Property	94
11.2.2 Querier	96
11.2.3 Statistics	97
11.3 MLD Snooping	97
11.3.1 Property	
11.3.2 Statistics	
11.4 MVR	
11.4.1 Property	
11.4.2 Port Setting	
11.4.3 Group Address	
12 Routing	
12.1 IPv4 Management and Interfaces	

	12.1.1 IPv4 Interface	104	
	12.1.2 IPv4 Routes		
	12.1.3 ARP		
	12.2 IPv6 Management and Interfaces	107	
	12.2.1 IPv6 Interface	107	
	12.2.2 IPv6 Address		
	12.2.3 IPv6 Routes		
	12.2.4 Neighbors		
	12.3 Rip Routes Management	111	
	12.4 Ospf Routes Management		
1:	.3 Security	114	
	13.1 RADIUS	114	
	13.2 TACACS+		
	13.3 AAA	117	
	13.3.1 Method List	117	
	13.3.2 Login Authentication	118	
	13.4 Management Access	119	
	13.4.1 Management VLAN		
	13.4.2 Management Service	119	
	13.4.3 Management ACL		
	13.5 Authentication Manager	124	
	13.5.1 Property	124	
	13.5.2 Port Setting	126	
	13.5.3 MAC-Based Local Account		
	13.5.4 WEB-Based Local Account	127	
	13.5.5 Sessions	128	
	13.6 DoS	128	
	13.6.1 Property	128	
	13.6.2 Port Setting	129	
	13.7 Dynamic ARP Inspection		
	13.7.1 Property	130	
	13.7.2 Statistics		

HRUI

13.8 DHCP Snooping131	
13.8.1 Property	
13.8.2 Statistics	
13.8.3 Option82 Property134	
13.9 IP Source Guard	
13.9.1 Port Setting 139	
13.9.2 IMPV Binding140	
14 ACL	
14.1 MAC ACL 142	
14.2 IPv4 ACL145	
14.3 IPv6 ACL147	
14.4 ACL Binding150	
15 QoS	
15.1 General 153	
15.1.1 Property	
15.1.2 Queue Scheduling154	
15.1.3 CoS Mapping 154	
15.1.4 DSCP Mapping155	
15.1.5 IP Precedence Mapping157	
15.2 Rate limit157	
15.2.1 Ingress / Egress Port157	
15.2.2 Egress Queue	
16 Diagnostics	
16.1 Logging160	
16.2 Ping	
16.3 Traceroute	
16.4 Copper Test163	
16.5 Fiber Module163	
16.6 UDLD	
16.6.1 Property	
16.6.2 Neighbor 165	
17 Management	

HRUI

17.1 User Account
17.2 Firmware
17.3 Configuration167
17.3.1 Upgrade167
17.3.2 Save Configuration167
17.4 SNMP
17.4.1 View169
17.4.2 Group170
17.4.3 Community171
17.4.4 User
17.4.5 Engine ID 173
17.4.6 Trap Event174
17.4.7 Notification174
17.5 RMON
17.5.1 Statistics
17.5.2 History177
17.5.3 Event 178
17.5.4 Alarm



1 Foreword

1.1 Target Audience

This manual is prepared for the installers and system administrators who are responsible for network installation, configuration and maintenance. It assumes that the user has understood all network communication and management protocols, as well as the technical terms, theoretical principles, practical skills, and expertise of devices, protocols and interfaces related to networking. Work experience in Graphical User Interface (GUI), Command-line Interface, Simple Network Management Protocol (SNMP) and Web Explorer is also required.

1.2 Manual Convention

The following approaches should prevail.

GUI Convention	Description
Interpretation	Describe operations and add necessary information.
	Remind the user of cautions as improper operations will result
Caution	in data loss or equipment damage.



2 Web Page Login

2.1 Log in the Network Management Client

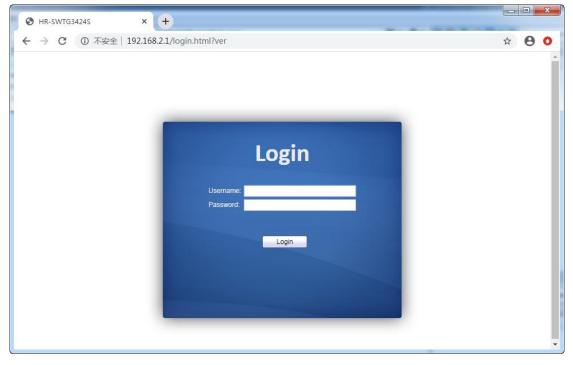
Type in the default switch address: http://192.168.2.1 and press "Enter".

Description:

Browser standards: superior to IE 9.0, Chrome 23.0 and Firefox 20.0

Keep the IP network segment of PC consistent with that of switch but differentiate the IP address as you log in. Set PC's IP address of **192.168.2.x** and the subnet mask of **255.255.255.0** for the first login ($1 < x \le 254$).

A login window appears as follows. Type in the default username of "**admin**" and the password of "**admin**". Click the "Log in" to see the switch system.



2.2 Constitution of Client Interface

The typical operation interface of Web network management system is as follows.



→ C ① 不安全 :	.92.168.2.1/home.html?ver					☆ \varTheta
HRUI						
	-			Save	Logout	Reboot Deb
	Status >> System I	nformation		System	n menu are	
Status		Port status area	1	cy occi	in mond and	
System Information			X			
Logging Message		1 3 5 7 9 11 13 15 17 19	9 21 23			
Port						
Link Aggregation						
MAC Address Table				26 27 28		
MAC Address Table letwork		2 4 6 8 10 12 14 16 18 20				
MAC Address Table letwork Port		2 4 6 8 10 12 14 16 18 20	0 22 24 25 :			1
MAC Address Table Network Port 1/AN	System Information	2 4 6 8 10 12 14 16 18 20 Ed	0 22 24 25 3			1
MAC Address Table Jetwork Port /LAN MAC Address Table	System Information Model		100%		CPU]
MAC Address Table letwork Port /LAN MAC Address Table spanning Tree	System Information Model	Ed HR-SWTG3424S	100% 90% 80%		CPU]
MAC Address Table leftwork Port ALAN AAC Address Table Bpanning Tree Discovery	System Information Model System Name	Ed HR-SWTG3424S Switch	100% 90% 80% 70%		CPU]
MAC Address Table letwork Vort ALAN MAC Address Table ganning Tree Discovery DHCP	System Information Model System Name System Location	Ed HR-SWT03424S Switch default	100% 90% 80% 70% 60%		CPU	
MAC Address Table letwork tort LAN MAC Address Table jascovery HCP Auticast	System Information Model System Name System Name	Ed HR-SWTG3424S Switch default default	at 100% 90% 80% 50% 50%		CPU	Informatio
MACAddress Table letwork Tort LAN AC Address Table panning Tree biscovery HCP HCP kulticast kouting	System Information Model System Name System Location System Contact	Ed HR-SWT03424S Switch default	100% 90% 80% 70% 60% 60% 60%			Informatio
MAC Address Table ketwork fort LAN AAC Address Table spanning Tree liscovery HCP Autitast kouting Security	System Information Model System Name System Location System Contact Serial Number	Ed HR-SWTG3424S Switch default default 0123456789	at 100% 90% 90% 80% 70% 60% 50% 40% 30%			Informatio show area
MAC Address Table letwork fort AAN AAC Address Table apanning Tree becovery bHCP Autilicast Routing Becurity NCL	System Information Model System Name System Location System Contact System Contact Serial Number	Ed HR-SWTG3424S Switch default default	8t 100% 90% 80% 80% 50% 50% 50% 20%			
MAC Address Table ketwork fort AAN AAC Address Table panning Tree panning Tree panning Tree panning htCP Autitaast kouting becurity kouting becurity bogs	System Information Model System Name System Location System Contact Serial Number MAC Address IPv4 Address	Ed HR-SWTG3424S Switch default default 0123456789	100% 90% 90% 80% 50% 50% 40% 30% 20%			
MAC Address Table ketwork fort LAN AAC Address Table spanning Tree liscovery HCP Autitast kouting Security	System Information Model System Name System Location System Contact Serial Number MAC Address	Ed HR-SWTG3424S Switch default default 0123456789 1C:2A:A3:00:34:24 192:168.2.1	8t 100% 90% 80% 80% 50% 50% 50% 20%	26 27 28	08:05:00	

2.3 Navigation Bar on Web Interface

Menu items such as State, Network, Port, VLAN, MAC Address Table, Spanning Tree, Discovery, DHCP, Multicast, Routing, Security, ACL, QoS, Diagnostics and Management are available on the web network management client. Each item contains submenus. Navigation bar is detailed as follows:

Menu Items	Submenus	Secondary	Description
		Submenus	
Status	System		Display the port state and product
	Information		info
	Logging		Display the device running and
	Message		operation logs
	Port	Statistics	Display the detailed port statistics
		Error Disabled	Display the faults occurring to ports
		Bandwidth	Display the bandwidth utilization per
		Utilization	unit time of all ports
	Link		Display the aggregation group state
	Aggregation		and members
	MAC Address		Display the MAC address table of
	Table		the current device
Network	IP Address		Configure and view the
			management IP address
	DNS		Configure and view the DNS and
			server setting
	Hosts		Configure and view the DNS Server
			and dynamic host mapping table
	System Time		Configure and view the current
			system time
Port	Port Setting		Configure and view all ports



		-	
	Error Disabled		Configure and view the port error disable protection
	Link Aggregation	Group	Configure and view the port & strategy balancing algorithms
	Aggregation		contained in LAG
		Port Setting	Configure and view the LAG
		LACP	Check LACP system priority and port
			configuration
	EEE		Configure and view the EEE state
			and information
	Jumbo Frame		Configure and view the length of the
			max message forwarded by system
	Port Security		Configure and view the rate limiting
	Protected Port		of port security, as well as port state Configure and view the port
	Protected Port		Configure and view the port isolation
	Storm Control		Configure and view the port storm
			policing
	Mirroring		Configure and view the port
			mirroring
VLAN	VLAN	Create VLAN	Configure and view the VLAN info of the device
		VLAN	Configure and view the VLAN
		Configuration	configuration of all ports
		Membership	Configure and view the port info of VLANs
		Port Setting	Configure and view the PVID and
			VLAN attributes of ports
	Voice VLAN	Property	Configure and view Voice-VLAN
			function and port status information
		Voice OUI	Configure and view Voice-VLAN
			OUI information
	Protocol VLAN	Protocol Group	Configure and view the protocol
			VLAN group
		Group Binding	Configure and view the protocol
			VLAN port and group binding.
	MAC VLA	MAC Group	Configure and view the MAC VLAN
		Group Binding	group Configure and view the MAC VLAN
			port and group binding
	Surveillance	Property	Configure and view
	VLAN		Surveillance-VLAN function and port
			status information



	1		
		Surveillance OUI	Configure and view
		Descent	Surveillance-VLAN OUI information
	GVRP	Property	Configure and view the functional
			global and port state
		Membership	Configure and view the VLANs
		Charlier	learned and the port members
		Statistics	Configure and view the message
			statistics related to ports
MAC Address	Dynamic		Configure and view the dynamic
Table	Address		MAC addresses and aging time of the device
	Static Address		Configure and view the static MAC
			address tables of the device
	Filtering Address		Configure and view the MAC
			address tables to be filtered
	Port Security		Configure and view the MAC
	Address		address table learned by port
			security
Spanning	Property		Configure and view the STP state
Tree			and attributes
	Port Setting		Configure and view the port
			attributions of STP
	MST Instance		Configure and view the instance
			attributes of STPs
	MST Port		Configure and view the instances
	Setting		(incl. port info) of STPs
	Statistics		Configure and view the STP
			message statistics of each port
Discovery	LLDP	Property	Configure and view the attributes
			related to LLDP
		Port Setting	Configure and view the transmitting
			& receiving state of LLDP at each
			port
		MED Network	Configure and view the MED
		Policy	network strategy table entry
		MED Port Setting	Configure and view the MED state at
			each port
		Packet View	Configure and view the detailed
			LLDP messages at each port
		Local Information	Configure and view the LLDP and
			LLDP-MED state
		Neighbor	Configure and view the LLDP
			neighbor info



Statistics	
5121131163	Configure and view the transmitting
	& receiving state of LLDP message
	at each port
	Configure and view DHCP service
	switches and port switches
ng	Configure and view DHCP server IP
	address pool
IF	Configure and view VLANIF and
pup	DHCP server group binding
	relationship
	View the list of DHCP clients
atic	Configure and view DHCP client
e	static binding table entries
Property	Configure and view the function
	configuration
Group Address	Configure and view the relevant
	static multicast info
Router Port	Configure and view the multicast
	routed port info
Forwarding All	Configure and view the multicast
	forwarding port info
Throttling	Configure and view the multicast
Thousang	limit at each port
Filtering Profile	Configure and view the multicast
Thering Frome	addresses filtered
Filtoring Pinding	Configure and view the binding info
Filtering binding	
Droporti /	related to filtering rule and ports
ig Property	Configure and view the switch,
Querier	version, etc.
	Configure and view the querier state
Statistics	Configure and view the protocol
	messages
g Property	Configure and view the protocol,
	switch, etc.
Statistics	Configure and view the protocol
	messages
Property	Configure and view the attribute info
	such as switch
Port Setting	Configure and view the state at each
	port
Group Address	Configure and view the function,
Group Address	Configure and view the function, VLAN and group address
	IF pup atic e Atic Atic Atic Atic Atic Atic Atic Atic



	Management		address information
	and Interfaces	IPv4 Routes	Configure and view IPv4 static routes
		ARP	Configure and view ARP table
	IPv6	IPv6 Interface	Configure and view VLANIF IPv6
	Management		interface information
	and Interfaces	IPv6 Address	Configure and view VLANIF IPv6
			address information
		IPv6 Routes	Configure and view IPv6 static
			routes
		IPv6 Neighbors	Configure and view IPv6 neighbors
			table
	Rip Routes	Rip Routes Setting	Configure and view RIP routes
	Management		
	Ospf Routes	Ospf Routes	Configure and view OSPF routes
	Management	Setting	
Security	RADIUS		Configure to view RADIUS server
			related information
	TACACS+		Configure to view TACACS+ server
			related information
	AAA	Method List	Configure and view the login authentication method
		Login	Configure and view the
		Authentication	authentication methods of terminals
	Management	Management VLAN	Configure and view management
	Access		VLAN
		Management	Configure and view the service
		Service	management mode and relevant
			attributes
		Management ACL	Configure and view the ACL aiming
			at management channels
		Management ACE	Configure and view the ACE
			configuration of management
			channels
	Authentication	Property	Configure and view the
	Management		authentication attributes
		Port Setting	Configure and view the
			authentication info at each port
		MAC Local Account	Configure and view the list of MAC
			local accounts
		Web Local Account	Configure and view the list of Web
			local accounts
		Sessions	Configure and view the info related



			to session authentication
	DoS	Property	Configure and view the switch option
		Port Setting	Configure and view the switch option at ports
	Dynamic ARP Inspection	Property	Configure and view the dynamic ARP inspection
		Statistics	Configure and view the messages statistics in APR inspection state at each port
	DHCP Snooping	Property	Configure and view the switch and state
		Statistics	Configure and view the DHCP message statistics received by each port
		Option82 Property	Configure and view the attributes related to Option 82
		Option82 Circuit ID	Configure and view the Circuit ID of Option 82
	IP Source Guard	Port Setting	Configure and view the state at ports
		IMPV Binding	Configure and view the binding tables of IP, MAC, Port and VLAN
		Save Database	Configure and view the storage and info of the binding table entry
ACL	MAC ACL		Configure and view the MAC ACL rules
	MAC ACE		Configure and view the MAC ACE table entries
	IPv4 ACL		Configure and view the IPv4 ACL rules
	IPv4 ACE		Configure and view the IPv4 ACE table entries
	IPv6 ACL		Configure and view the IPv6 ACL rules
	IPv6 ACE		Configure and view the IPv6 ACE table entries
	ACL Binding		Configure and view the ACL rules and the port binding application
QoS	General	Property	Configure and view the QoS switch and state
		Queue Scheduling	Configure and view the algorithm of queue scheduling



Anagement Cos Mapping Configure and view the priority and local queue mapping table DSCP Mapping Configure and view the priority and local queue mapping table IP Precedence Mapping Configure and view the priority and local queue mapping table Rate Limit Ingress/Egress Port Egress Queue Configure and view the priority and local queue mapping table Diagnostics Logging Property Configure and view the switch and state Ping Property Configure and view the switch and state Ping Network diagnostics by Ping Traceroute Network diagnostics by Ping Traceroute Network diagnostics by Ping Fiber Module Check the SFP module at optical interfaces UDLD Property Configure and view the neighbor state Management User Account Configure and view the user info supporting device running SNMP View Configure and view the SNMP function files Save Configuration Save the configuration files supporting device running SNMP View Configure and view the SNMP function files Source Configure and view the SNMP group Configure and view the SNMP f		-		
DSCP Mapping Configure and view the priority and local queue mapping table IP Precedence Mapping Configure and view the priority and local queue mapping table Rate Limit Ingress/Egress Port Configure and view the rate limiting configuration of port rate limiting configuration based on egress queue Diagnostics Logging Property Configure and view the switch and state Ping Network diagnostics by Ping Traceroute Configure and view the address of remote servers Ping Network diagnostics by Ping Traceroute Configure and view the switch and state Copper Test Electrical interface link diagnostics by VCT Electrical interface link diagnostics by VCT Fiber Module Check the SFP module at optical interfaces Neighbor Management User Account Configure and view the user info Firmware Upgrade Update configuration files SNMP View Configure and view the SNMP function view the SNMP group Community Configure and view the SNMP group Community User Configure and view the SNMP group Community User Configure and view the SNMP group Comm			CoS Mapping	Configure and view the priority and
Incal queue mapping table IP Precedence Configure and view the priority and local queue mapping table Rate Limit Ingress/Egress Port Configure and view the priority and local queue mapping table Diagnostics Logging Egress Queue Configure and view the switch and state Diagnostics Logging Property Configure and view the switch and state Ping Property Configure and view the address of remote servers Ping Network diagnostics by Ping Traceroute Network diagnostics by Ping Copper Test Electrical interface link diagnostics by VCT Fiber Module Check the SFP module at optical interfaces UDLD Property Configure and view the user info state Management User Account Configure and view the user info save configuration files SNMP View Configure and view the SNMP function view table entry Group Configure and view the SNMP propu- function view table entry Group Configure and view the SNMP propu- function view the SNMP propu- supporting device running SNMP View Configure and view the SNMP function view the SNMP propu- function view the SNMP pr				local queue mapping table
IP Precedence Mapping Configure and view the priority and local queue mapping table Rate Limit Ingress/Egress Port Configure and view the configuration of port rate limiting Egress Queue Configure and view the rate limiting configuration based on egress queue Diagnostics Logging Property Configure and view the switch and state Ping Network diagnostics by Ping Traceroute Network diagnostics by Ping Traceroute Network diagnostics by traceroute Copper Test Electrical interface link diagnostics by VCT Fiber Module Property Configure and view the switch and state State Management User Account Property Configure and view the switch and state Management User Account Configure and view the user info firmware Upgrade View Configure and view the SNMP function view table entry Save the configuration files SNMP View Configure and view the SNMP group Community Configure and view the SNMP ser attributes Configure and view the SNMP and remote Engine IDs SNMP View Configure and view the SNMP and remote Engine IDs Configure and view the SNMP and re			DSCP Mapping	Configure and view the priority and
Mapping local queue mapping table Rate Limit Ingress/Egress Port Configure and view the test limiting Egress Queue Configure and view the rate limiting configuration based on egress queue Configure and view the switch and state Diagnostics Logging Property Configure and view the switch and state Ping Network diagnostics by Ping Traceroute Network diagnostics by Ping Traceroute Network diagnostics by Varceroute Coper Test Electrical interface link diagnostics by VCT Fiber Module Check the SFP module at optical interfaces Nubbor Configure and view the switch and state Management User Account Configure and view the user info State Management User Account Configure and view the user info State SNMP View Configure and view the SNMP Save the configuration files SNMP View Configure and view the SNMP group Configure and view the SNMP group Community Configure and view the SNMP group Configure and view the SNMP group Community SNMP View Configure and view the SNMP group Configure and view t				local queue mapping table
Rate Limit Ingress/Egress Port Configure and view the configuration of port rate limiting Egress Queue Configure and view the rate limiting configuration based on egress queue Configure and view the switch and state Diagnostics Logging Property Configure and view the switch and state Ping Network diagnostics by Ping Traceroute Network diagnostics by Ping Traceroute Network diagnostics by Viraceroute Coper Test Electrical interface link diagnostics by VCT Fiber Module Check the SFP module at optical interfaces Network diagnostics by VCT UDLD Property Configure and view the switch and state Management User Account Configure and view the user info Firmware Upgrade Update software Configuration Save the configuration files Save Configure and view the SNMP Supporting device running SNMP View Configure and view the SNMP group Community Configure and view the SNMP user attributes Engine ID Configure and view the SNMP user attributes Engine ID Configure and view the SNMP and remote Engine IDs			IP Precedence	Configure and view the priority and
Image: Configuration of port rate limiting Egress Queue Configure and view the rate limiting configuration based on egress queue Diagnostics Logging Property Configure and view the switch and state Ping Remote Server Configure and view the address of remote servers Ping Network diagnostics by Ping Traceroute Network diagnostics by traceroute Copper Test Electrical interface link diagnostics by VCT Fiber Module Check the SFP module at optical interfaces UDLD Property Configure and view the switch and state Management User Account Configure and view the user info Firmware Upgrade Update software Configuration Save Configuration Save the configuration files Save Configuration Save the configuration files Supporting device running SNMP View Configure and view the SNMP group Community Configure and view the SNMP group Community Group Configure and view the SNMP group Configure and view the SNMP group Community User Configure and view the SNMP and remote Engine I			Mapping	local queue mapping table
Egress Queue Configure and view the rate limiting configuration based on egress queue Diagnostics Logging Property Configure and view the switch and state Remote Server Configure and view the address of remote servers Configure and view the address of remote servers Ping Network diagnostics by Ping Traceroute Network diagnostics by traceroute Copper Test Electrical interface link diagnostics by VCT Fiber Module Check the SFP module at optical interfaces UDLD Property Configure and view the switch and state Management User Account Configure and view the user info firmware Management User Account Configure and view the user info state Management User Account Configure and view the user info firmware SNMP View Configure and view the SNMP function view table entry Group Configure and view the SNMP group Community Configure and view the SNMP group Community Configure and view the SNMP user attributes Engine ID Configure and view the SNMP and remote Engine IDs Trap Event Configure and view the SNMP Trap switch an		Rate Limit	Ingress/Egress Port	Configure and view the
Diagnostics Logging Property Configure and view the switch and state Ping Remote Server Configure and view the address of remote servers Ping Network diagnostics by Ping Traceroute Network diagnostics by traceroute Copper Test Electrical interface link diagnostics by VCT Fiber Module Check the SFP module at optical interfaces UDLD Property Configure and view the switch and state Management User Account Configure and view the user info Firmware Upgrade Update configuration files Save Configuration Save the configuration files Save Configure and view the SNMP function wite the SNMP function view table entry Group Configure and view the SNMP group Community Configure and view the SNMP group Community User Configure and view the SNMP group Community User Configure and view the SNMP group				configuration of port rate limiting
Diagnostics Logging Property Configure and view the switch and state Remote Server Configure and view the address of remote servers Remote Server Configure and view the address of remote servers Ping Network diagnostics by Ping Traceroute Network diagnostics by traceroute Copper Test Electrical interface link diagnostics by VCT Electrical interfaces by VCT Fiber Module Property Configure and view the switch and state interfaces UDLD Property Configure and view the switch and state state Management User Account Configure and view the neighbor state Configure and view the switch and state Management User Account Upgrade Update configuration files Save Configuration Save the configuration files supporting device running SNMP View Configure and view the SNMP group Community Group Configure and view the SNMP group Community Configure and view the SNMP user attributes Engine ID Configure and view the SNMP user attributes Engine ID Configure and view the SNMP and remote Engine IDs <td></td> <td></td> <td>Egress Queue</td> <td>Configure and view the rate limiting</td>			Egress Queue	Configure and view the rate limiting
Diagnostics Logging Property Configure and view the switch and state Remote Server Configure and view the address of remote servers Ping Network diagnostics by Ping Traceroute Network diagnostics by traceroute Copper Test Electrical interface link diagnostics by VCT Fiber Module Check the SFP module at optical interfaces UDLD Property Configure and view the switch and state Management User Account Configure and view the user info Firmware Upgrade Update software Configuration Save Configure and view the user info SNMP View Configure and view the SNMP function view table entry Group Configure and view the SNMP group Community Configure and view the SNMP group Community User User Configure and view the SNMP group Community User Configure and view the SNMP group Community Configure and view the SNMP and remote Engine IDs Trap Event Configure and view the SNMP Trap switch and state				configuration based on egress
Management User Account Remote Server Configure and view the address of remote servers Ping Network diagnostics by Ping Traceroute Network diagnostics by traceroute Copper Test Electrical interface link diagnostics by VCT Fiber Module Check the SFP module at optical interfaces UDLD Property Configure and view the switch and state Management User Account Configure and view the user info Firmware Upgrade Update configuration files Save Configuration Save Configure and view the SNMP Group Configure and view the SNMP group Community Configure and view the SNMP group Tormunity User Configure and view the SNMP and remote Engine IDs Trap Event Trap Event Configure and view the SNMP Trap switch and state				queue
Pingremote serversPingNetwork diagnostics by PingTracerouteNetwork diagnostics by tracerouteCopper TestElectrical interface link diagnostics by VCTFiber ModuleCheck the SFP module at optical interfacesUDLDPropertyConfigure and view the switch and stateManagementUser AccountConfigure and view the neighbor stateManagementUser AccountConfigure and view the user info FirmwareFibm ModuleUpgradeUpdate configuration files supporting device runningSNMPViewConfigure and view the SNMP function view table entryGroupConfigure and view the SNMP group CommunityUserConfigure and view the SNMP group function view table entryGroupConfigure and view the SNMP group CommunityUserConfigure and view the SNMP group CommunityTrap EventConfigure and view the SNMP and remote Engine IDsTrap EventConfigure and view the SNMP Trap switch and state	Diagnostics	Logging	Property	
Traceroute Network diagnostics by traceroute Copper Test Electrical interface link diagnostics by VCT Fiber Module Check the SFP module at optical interfaces UDLD Property Configure and view the switch and state Management User Account Configure and view the user info Firmware Upgrade Update software Configuration Upgrade Update configuration files Save Configuration Save Configure and view the SNMP function view table entry Group Configure and view the SNMP group Community Configure and view the SNMP group Community Configure and view the SNMP group Trap Event Configure and view the SNMP Trap switch and state			Remote Server	
Traceroute Network diagnostics by traceroute Copper Test Electrical interface link diagnostics by VCT Fiber Module Check the SFP module at optical interfaces UDLD Property Configure and view the switch and state Management User Account Configure and view the user info Firmware Upgrade Update software Configuration Upgrade Update configuration files Save Configuration Save Configure and view the SNMP function view table entry Group Configure and view the SNMP group Community Configure and view the SNMP group Community Configure and view the SNMP group Trap Event Configure and view the SNMP Trap switch and state		Ping		Network diagnostics by Ping
Copper Test Electrical interface link diagnostics by VCT Fiber Module Check the SFP module at optical interfaces UDLD Property Configure and view the switch and state Management User Account Configure and view the user info Firmware Upgrade Update software Configuration Upgrade Update configuration files Save Configuration Save the configuration files SNMP View Configure and view the SNMP function view table entry Group Configure and view the SNMP group Community Configure and view the SNMP group Community User Configure and view the SNMP user attributes Engine ID Configure and view the SNMP and remote Engine IDs Trap Event Trap Event Configure and view the SNMP Trap switch and state				
Image: Simple service of the servic				
Image of the synthesis of the synt				-
UDLD Property Configure and view the switch and state Management User Account Configure and view the neighbor state Management User Account Configure and view the user info Firmware Upgrade Update software Configuration Upgrade Update configuration files Save Configuration Save the configuration files SNMP View Configure and view the SNMP function view table entry Group Configure and view the SNMP group Community User Configure and view the SNMP user attributes Engine ID Engine ID Configure and view the SNMP rap switch and state		Fiber Module		Check the SFP module at optical
Management User Account Configure and view the neighbor state Management User Account Configure and view the user info Firmware Upgrade Update software Configuration Upgrade Update configuration files Save Configuration Save the configuration files SNMP View Configure and view the SNMP function view table entry Group Configure and view the SNMP group Community Configure and view the SNMP user attributes Engine ID Configure and view the SNMP and remote Engine IDs Trap Event Configure and view the SNMP Trap switch and state				interfaces
ManagementUser AccountStateManagementUser AccountConfigure and view the user infoFirmwareUpgradeUpdate softwareConfigurationUpgradeUpdate configuration filesSave ConfigurationSave the configuration files supporting device runningSNMPViewConfigure and view the SNMP function view table entryGroupConfigure and view the SNMP group CommunityCommunityConfigure and view the SNMP user attributesEngine IDConfigure and view the SNMP and remote Engine IDsTrap EventConfigure and view the SNMP Trap switch and state		UDLD	Property	
Management User Account Configure and view the user info Firmware Upgrade Update software Configuration Upgrade Update configuration files Save Configuration Save the configuration files SNMP View Configure and view the SNMP function view table entry Group Configure and view the SNMP group Community User Configure and view the SNMP user attributes Engine ID Configure and view the SNMP and remote Engine IDs Trap Event Configure and view the SNMP Trap switch and state			Neighbor	
FirmwareUpgradeUpdate softwareConfigurationUpgradeUpdate configuration filesSave ConfigurationSave the configuration files supporting device runningSNMPViewConfigure and view the SNMP function view table entryGroupConfigure and view the SNMP group CommunityCommunityConfigure and view the SNMP user attributesEngine IDConfigure and view the SNMP and remote Engine IDsTrap EventConfigure and view the SNMP Trap switch and state	Management	Llser Account		
ConfigurationUpgradeUpdate configuration filesSave ConfigurationSave the configuration files supporting device runningSNMPViewConfigure and view the SNMP function view table entryGroupConfigure and view the SNMP group CommunityCommunityConfigure and view the SNMP user attributesEngine IDConfigure and view the SNMP and remote Engine IDsTrap EventConfigure and view the SNMP Trap switch and state	Management		Lingrada	
Save ConfigurationSave the configuration files supporting device runningSNMPViewConfigure and view the SNMP function view table entryGroupConfigure and view the SNMP group CommunityCommunityConfigure and view the SNMP user attributesEngine IDConfigure and view the SNMP and remote Engine IDsTrap EventConfigure and view the SNMP Trap switch and state				· ·
SNMPViewConfigure and view the SNMP function view table entryGroupConfigure and view the SNMP group CommunityCommunityConfigure and view the SNMP user attributesEngine IDConfigure and view the SNMP and remote Engine IDsTrap EventConfigure and view the SNMP Trap switch and state		Configuration		
GroupConfigure and view the SNMP groupCommunityConfigure and view the SNMP CommunityUserConfigure and view the SNMP user attributesEngine IDConfigure and view the SNMP and remote Engine IDsTrap EventConfigure and view the SNMP Trap switch and state			Save Configuration	u u u u u u u u u u u u u u u u u u u
GroupConfigure and view the SNMP groupCommunityConfigure and view the SNMP CommunityUserConfigure and view the SNMP user attributesEngine IDConfigure and view the SNMP and remote Engine IDsTrap EventConfigure and view the SNMP Trap switch and state		SNMP	View	Configure and view the SNMP
CommunityConfigure and view the SNMP CommunityUserConfigure and view the SNMP user attributesEngine IDConfigure and view the SNMP and remote Engine IDsTrap EventConfigure and view the SNMP Trap switch and state				function view table entry
CommunityUserConfigure and view the SNMP user attributesEngine IDConfigure and view the SNMP and remote Engine IDsTrap EventConfigure and view the SNMP Trap switch and state			Group	Configure and view the SNMP group
CommunityUserConfigure and view the SNMP user attributesEngine IDConfigure and view the SNMP and remote Engine IDsTrap EventConfigure and view the SNMP Trap switch and state			Community	Configure and view the SNMP
UserConfigure and view the SNMP user attributesEngine IDConfigure and view the SNMP and remote Engine IDsTrap EventConfigure and view the SNMP Trap switch and state				
Engine IDConfigure and view the SNMP and remote Engine IDsTrap EventConfigure and view the SNMP Trap switch and state			User	-
Trap EventConfigure and view the SNMP Trap switch and state			Engine ID	Configure and view the SNMP and
switch and state			Trap Event	
Notification Configure and view the SNMP				
			Notification	Configure and view the SNMP



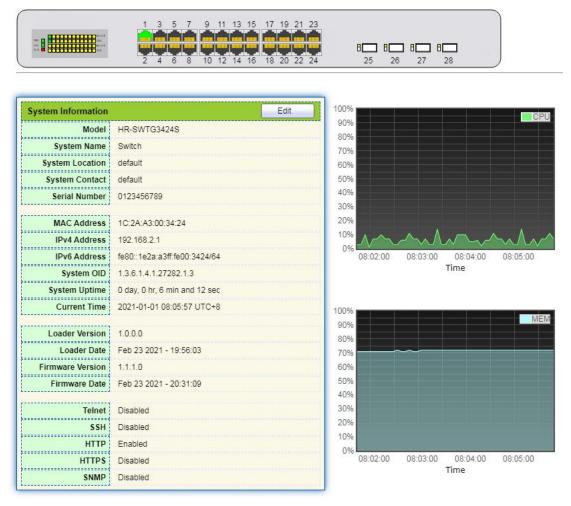
		Notification server state
RMON	Statistics	Configure and view the message
		statistics history of all ports
	History	Configure and view the history
		record state
	Event	Configure and view the event state
	Alarm	Configure and view the alarm state

3 Status

3.1 System Information

According to the switch connected, web network management panel directly displays the port and product info, incl.: number of ports, port states, product info, device states, function on-off states, etc. Instructions:

1. Click the "Status > System Information" in the navigation bar as follows:





Description:

Mouseover a port to check the port No., type, rate and state. "Edit" the "System Name", "Location" and "Contact" in the product info. "Apply" and finish.

3.2 Statistics

Introduce the detailed flow statistics at a port and the info to be refreshed or cleared manually by users.

1. Click the "Status > Port > Statistics" in the navigation bar as follows:

MIB Counter	NI nterface Etherlike RMON
Refresh Rate	None i sec O sec iO sec
Clear	
Interface	
ifInOctets	60938
ifInUcastPkts	210
ifInNUcastPkts	318
ifInDiscards	0
ifOutOctets	185965
ifOutUcastPkts	212
ifOutNUcastPkts	1422
ifOutDiscards	0
ifInMulticastPkts	160
ifInBroadcastPkts	158
ifOutMulticastPkts	770
ifOutBroadcastPkts	652

Description:

"Clear" the flow statistics at the current port and refresh the page.



3.3 MAC Address Table

View MAC address table information

Instructions:

1. Click the "Status > MAC Address Table" in the navigation bar as follows:

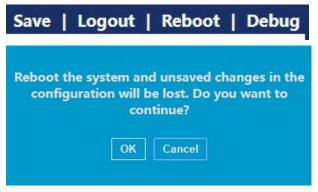
showing	All • entries	Showing 1 to	o 2 of 2 entr	ies	Q		
VLAN	MAC Address	Туре	Port				
1	1C:2A:A3:00:34:24	Management	CPU				
1	00:E0:4C:2E:2C:DD	Dynamic .	GE1				
				First	Previous	1 Next	Last

Interface data are as follows.

Query	Description
Items	
MAC	Destination MAC Address
VLAN	VLAN ID belonging to MAC address
Port	Message egress corresponding to MAC address
Туре	Dynamic MAC Address refers to the entry which will age with the set aging time. Switches can add entries based on the learning mechanism of MAC address or manual creation. Static MAC address refers to the specified table which is manually configured and won't age. Management MAC address refers to the address at the management port.

3.4 Reboot

1. Click the "Reboot" on the upper right as guided as follows.





3.5 Management IP Address

Change the management IP address on web interface.

Instructions:

1. Click the "Routing > IPv4 Management and Interfaces > IPv4 Interface" in the navigation bar to discover IPv4 address of **192.168.2.1/24** by default as follows:

IPv4 Interface Table

			Q	
Interface	IP Address Type	IP Address	Mask	Status
VLAN 1	Static	192.168.2.1	255.255.255.0	Valid
Add	Delete			

4 Network

4.1 DNS

DNS is short for Domain Name System to name computers and network services from units to domain hierarchies. A domain name consists of the dots separated by a series of words or abbreviations, each corresponding to a unique IP address. DNS is the server on the Internet that resolves domain names. Applicable to Internet and other TCP/IP networks, DNS name retrieves computers and services through user-friendly names. As one of the core Internet services, DNS is a distributed database that maps domain names and IP addresses mutually. Instructions:

1. Click on the "Network > DNS" in the navigation bar as follows.

DNS Configuration

DNS Status O Disabl	
DNS Default Name	(1 to 255 alphanumeric characters)
Apply	
IS Server Configuration	
IS Server Configuration	Q
S Server Configuration	Q
DNS Server Configuration Preference DNS Server	0 results found.



Interface data are as follows.

Configuration Items	Description
DNS State	DNS switch
DNS Default Name	Enter the DNS default name

2. "Add" to configure DNS server.

Pv4/IPv6 Address	114.114.114.114	
------------------	-----------------	--

3. "Apply" and finish as follows.

		Q
Preference	DNS Server	
1	114.114.114.114	

4.2 System Time

It is mainly used to configure the system time, and select the time source, daylight-saving time, etc. Instructions

1. Click on the "Network > System Time" in the navigation bar as follows.



Source	 SNTP From Computer Manual Time 		
Time Zone	UTC +8:00 V		
SNTP			
Address Type	 Hostname IPv4 		
Server Address			
Server Port	123	(1 - 65535, default 123)	
Manual Time			
Date	2019-01-01	YYYY-MM-DD	
Time	09:07:05	HH:MM:SS	
Daylight Saving Ti	me		
Туре	 None Recurring Non-recurring USA Europen 		
Offset	60	Min (1 - 1440, default 60)	
Recurring	From: Day Sun 🗸	Week First V Month Jan V Time	
	To: Day Sun 🗸	Week First 🗸 Month Jan 🗸 Time	
	From:	YYYY-MM-DD	HH:MM
Non-recurring	То:	YYYY-MM-DD	HH:MM
Operational Status			
Current Time	2019-01-01 09:07:05 UTC	C+8	

Apply

Interface data are as follows.

Configuration	Description
ltems	
Time Source	Select the time source in SNTP, PC or manual modes
Time Zone	Set the time zone
Address Type	Host name or IPv4 address (with time source set by SNTP)
Server Address	Server Address (with time source set by SNTP)
Server Port No.	Server Port No. (with time source set by SNTP)
Date	Date info: DD/MM/YYYY (with time source set in manual mode)
Time	Time info: SS/MM/HH (with time source set in manual mode)
Туре	Daylight-saving time types are divided into None, cyclic, non-cyclic, United States and Europe.



Reimbursed Time	Reimbursed Time of daylight-saving time
Cyclic Mode	Configure the cyclic mode of daylight-saving time
Non-cyclic Mode	Configure the non-cyclic mode of daylight-saving time

5 Port

5.1 Port Setting

Interfaces should be identified so that users can inquire and configure Ethernet interfaces as they want. Instructions:

1. Click the "Port > Port Setting" in the navigation bar:

Port Setting Table

								Q	
	Entry	Port	Туре	Description	State	Link Status	Speed	Duplex	Flow Control
D	1	GE1	1000M Copper		Enabled	Down	Auto	Auto	Disabled
	2	GE2	1000M Copper		Enabled	Down	Auto	Auto	Disabled
0	3	GE3	1000M Copper		Enabled	Down	Auto	Auto	Disabled
)	4	GE4	1000M Copper		Enabled	Down	Auto	Auto	Disabled
D	5	GE5	1000M Copper		Enabled	Down	Auto	Auto	Disabled
1	6	GE6	1000M Copper		Enabled	Down	Auto	Auto	Disabled
-	7	GE7	1000M Conner		Enabled	Down	Auto	Auto	Disabled

2. Select the port(s) to be configured, and "Edit" as follows:

Port	GE1-GE3				
Description					
State	Enable				
Speed		00	10M 100M 1000M 10G		
Duplex	Auto Full Half				
low Control	 Auto Enable Disable 				

Interface data are as follows

	Configuration	Description
--	---------------	-------------



ltems						
Port	Port list					
Description	Port alias					
State	Enable or disable port					
Speed	Configurable auto negotiation with mandatory 10 Mb, 100 Mb and 1,000 Mb states. Interface rates including 10 Mbit/s, 100 Mbit/s and 1,000 Mbit/s are available to Ethernet electrical interfaces and are optional as required.					
Duplex	Configurable auto negotiation with full or half duplexes.					
Flow Control	After it is enabled on both local network and opposite network devices, the local one will notify the other to stop transmitting messages in the presence of network congestion. The opposite one will execute the command temporarily to ensure zero message loss. Disable-Disabled reception and transmission of PAUSE frame; Enable-Enabled reception and transmission of PAUSE frame; Auto negotiation-Negotiate PAUSE frame with opposite network devices automatically.					

5.2 Error Disabled

In general, if the software of the switch detects some errors in the port, the port will be closed immediately. In other words, when the operating system of the switch detects some error events on the switch port, the switch will automatically close the port Instructions:

1. Click the "Port > Error Disabled" in the navigation bar to enable or disable configuration as follows:

Recovery Interval	300	Sec (30 - 86400)
BPDU Guard	Enable	
UDLD	Enable	
Self Loop	Enable	
Broadcast Flood	Enable	
Unknown Multicast Flood	Enable	
Unicast Flood	Enable	
ACL	Enable	
Port Security	Enable	
DHCP Rate Limit	Enable	
ARP Rate Limit	Enable	



5.3 Link Aggregation

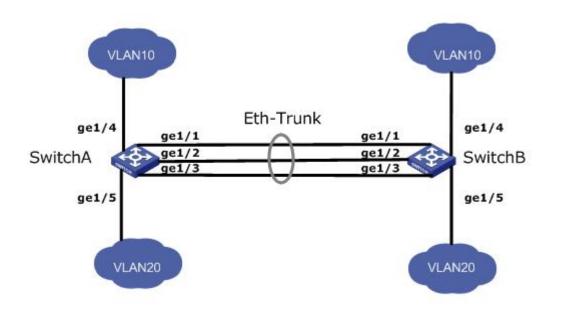
Link Aggregation broadens bandwidth and reliability by bundling a group of physical interfaces into a single logical interface.

LAG (Link Aggregation Group) is a logical link bundled by multiple Ethernet links (Eth-Trunk).

Ceaselessly expanding network size increases users' demands of link bandwidth and reliability. Traditionally, high-speed interface board or the compatible equipment is usually replaced to optimize bandwidth, which is expensive and inflexible.

Link Aggregation Technology bundles multiple physical interfaces into a single logical interface without upgrading hardware. Its backup mechanism not only improves reliability, but also shares the flow load on different physical links.

As shown below, Switch A is linked with Switch B through three Ethernet links which are bundled into an Eth-Trunk logical link. Its bandwidth equals to that of the three links in total, thus broadening the bandwidth. Meanwhile, these three links back up mutually to be more reliable.



Link Aggregation can meet the following demands:

- Insufficient bandwidth of two switches connected with one link.
- Insufficient reliability of two switches connected with one link.

Link Aggregation can be divided into Manual Mode and LACP Mode in accordance with Link Aggregation Control Protocol (LACP) state.

In the first mode, Eth-Trunk establishment, member interface access should be added manually without LACP. It is also called the Load-sharing Mode because all links are involved in data forwarding and load sharing. In case any active link fails, LAG will average load with the remaining ones. This mode is preferred under the circumstance that two directly connected devices require a larger link bandwidth but has no access to LACP.

5.3.1 Group

Instructions for adding a Static Link Aggregation:



1. Click the "Port > Link Aggregation > Group", select a load-balancing algorithm with a radio button. "Apply" and finish as follows:

Load Balance Algorithm	MAC Address IP-MAC Address
Apply	

Link Aggregation Table

							Q
	LAG	Name	Туре	Link Status	Active Member	Inactive Member	
С	LAG 1						
С	LAG 2		8 <u>000</u> 9				
0	LAG 3						
0	LAG 4		1000				
0	LAG 5						
0	LAG 6		1075				
0	LAG 7						
0	LAG 8		100.00	5.750.			

2. Select one of 8 LAGs available, "Edit" the configuration page as follows:

Edit Link Aggregation Group	oup
-----------------------------	-----

LAG	1	
Name		
Туре	StaticLACP	
Member	Available Port	elected Port

Interface data are as follows

Configuration Items	Description
LAG	There are 8 LAGs numbering from 1 to 8.
Name	Description of LAG, which can be modified as needed.
Туре	Select from the manual mode and the LACP mode.



Member

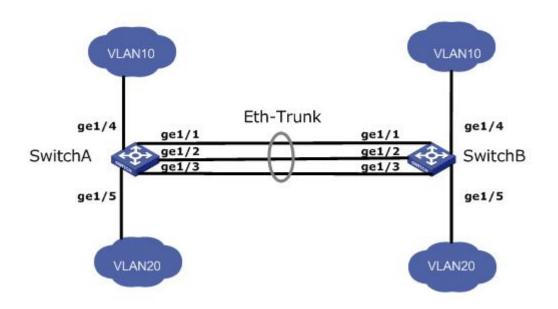
Up to 8 member ports are available in LAG.

Illustration:

As shown below, Switch A and Switch B connect VLAN 10 and 20 via Ethernet respectively, with large data flow between them.

Both Switch A and B are expected to provide superior link bandwidth for VLAN communication. Meanwhile, there should be the redundancy for reliable data transmission and links.

Networking diagram LAG in manual mode



Instructions:

1. Create the ETH trunk interface in SwitchA and add a member interface to increase the link bandwidth. The configuration of SwitchB is like that of SwitchA. Click the "Port > Link Aggregation > Group", choose "LAG 1" and port GE1, 2 and 3 and move them to the selected ports on the right. "Apply" and finish as follows.

						Q
	LAG	Name	Туре	Link Status	Active Member	Inactive Member
	LAG 1		Static	Up	GE3	GE1-GE2
0	LAG 2			223		
)	LAG 3					
D.	LAG 4					

5.3.2 Port Setting

Attribute configuration of aggregation group member port

1. Click the "Port > Link Aggregation > Port Setting", to enter the attribute configuration interface of aggregation group member port as follows:



Port Setting Table

	LAG	Туре	Description	State	Link Status	Speed	Duplex	Flow Control
1	LAG 1			Enabled	Down	Auto	Auto	Disabled
	LAG 2			Enabled	Down	Auto	Auto	Disabled
	LAG 3			Enabled	Down	Auto	Auto	Disabled
	LAG 4			Enabled	Down	Auto	Auto	Disabled
	LAG 5			Enabled	Down	Auto	Auto	Disabled
	LAG 6			Enabled	Down	Auto	Auto	Disabled
	LAG 7			Enabled	Down	Auto	Auto	Disabled
	LAG 8			Enabled	Down	Auto	Auto	Disabled

5.3.3 LACP

LACP (Link Aggregation Control Protocol), based on IEEE 802.3ad Standard, dynamically aggregates and disaggregates links. It exchanges info with the opposite network devices through LACPDU (Link Aggregation Control Protocol Data Unit).

After a port uses LACP, it will inform the opposite network device of system priority, system MAC, port priority and No., and operation Key by transmitting a LACPDU. The opposite device will compare such info with that saved by other ports after receiving it, thus reaching an agreement on port participation in or quitting from a dynamic aggregation.

Dynamic LACP aggregation is automatically created or deleted by system, that is, internal ports can be added or removed by themselves. Only the ports connected to a same device with the same rate, duplex, and basic configuration can be aggregated.

Instructions for adding a dynamic link aggregation:

1. Click the "Port > Link Aggregation > Group" in the navigation bar, select the LAG ID and LACP mode, "Edit" them as follows:



Edit Link Aggregation Group

2. Click the "Port >Link Aggregation > LACP" in the navigation bar to configure the LACP attributes such as system priority, port priority and timeout method as follows:

 1 - 65535, default	

LACP Port Setting Table

						Q
	Entry	Port	Port Priority	Timeout	-	
)	1	GE1	1	Long		
0	2	GE2	1	Long		
	3	GE3	1	Long		
0	4	GE4	1	Long		
3	5	GE5	1	Long		
	6	GE6	1	Long		
	7	GE7	1	Long		
	8	GE8	1	Long		

Interface data are as follows

Configuration	Description
Items	
System Priority	LACP determines the active and passive modes between two
	devices subject to priority standard.
Port	Port list
Port Priority	LACP determines the dynamic LAG member mode subject to the



	port priority with a superior system.
Timeout	It decides the transmission frequency of LACP messages.

Description:

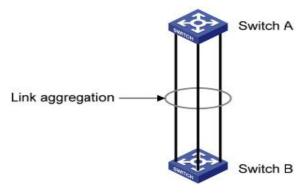
Please make sure there is no member interface accessing the Eth-Trunk before changing its work pattern, otherwise it fails.

Work pattern of the local network devices should be consistent with that of the opposite network devices.

Illustration

Ethernet Switch A aggregates 3 ports from GE1 to GE3 to Switch B, in order to share the load by each member port.

The following configurations are exampled by means of dynamic aggregation.



Description:

The following is the configuration of Switch A only, which should stay the same with that of Switch B for port aggregation.

Instructions:

1. Click the "Port > Link Aggregation > Group" in the navigation bar, "Edit" with LAG 2, select GE1-GE3 in LACP mode. "Apply" and finish as follows:



Edit Link Aggregation Group

LAG	2					
Name						
Typ <mark>e</mark>	 Static LACP 					
	Available Port		Selected	Port		
Member	GE4 GE5 GE6 GE7 GE8		GE1 GE2 GE3			
	GE0 GE9 GE10 GE11 -	<		Ψ.		

5.4 EEE

Port power will be turned down in case of zero or less flow

Instructions:

1. Click the "Port > EEE" in the navigation bar, select the port and "Edit" to enter the configuration interface as follows:

				Q
7	Entry	Port	State	
)	1	GE1	Disabled	
	2	GE2	Disabled	
	3	GE3	Disabled	
	4	GE4	Disabled	
3	5	GE5	Disabled	
	6	GE6	Disabled	
90	7	057	Burbled	

2. Set the port enable tag and "Apply" to complete the configuration as follows:



EEE Setting Table

- 11	Entre	Dent	Ctata	
	Entry	Port	State	
	1	GE1	Enabled	
	2	GE2	Enabled	
	3	GE3	Disabled	
D	4	GE4	Disabled	

5.5 Jumbo Frame

Set the MTU (Maximum Transmission Unit) of the port

Instructions:

1. Click the "Port > Jumbo Frame" in the navigation bar, enter Jumbo Frame configuration interface as follows:

Jumbo Frame	Enable	
	10000	Byte (1518 - 10000, default 1522)

5.6 Port Security

The port security feature records the Ethernet MAC address connected to the switch port through the MAC address table, and only one MAC address can communicate through this port. When packets sent by other MAC addresses pass through this port, port security features prevent it. Using port security features can prevent unauthorized devices from accessing the network and enhance security. In addition, port security features can also be used to prevent MAC address table from filling up due to MAC address flooding Instructions:

1. Click the "Port > Port Security" in the navigation bar, enter port security configuration interface as follows:

State	Enable		
Rate Limit	100	Packet / Sec (1 - 600, default 100)	

2. Click the "Port > Port Security" in the navigation bar, select the port and "Edit" to enter the port level configuration interface as follows:



Port Security Table

Q									
	Entry	Port	State	Address Limit	Total	Configured	Violate Number	Violate Action	Sticky
	1	GE1	Disabled	1	0	0	0	Protect	Disabled
	2	GE2	Disabled	1	0	0	0	Protect	Disabled
	3	GE3	Disabled	1	0	0	0	Protect	Disabled
	4	GE4	Disabled	1	0	0	0	Protect	Disabled
	5	GE5	Disabled	1	0	0	0	Protect	Disabled
	6	GE6	Disabled	1	0	0	0	Protect	Disabled
1	7	GE7	Disabled	1	0	0	0	Protect	Disabled

Edit Port Security

Port	GE1-GE2		
State	Enable		
Address Limit	1	(1 - 256, default 1)	
Violate Action	 Protect Restrict Shutdown 		
Sticky	Enable		
Apply Clo	ose		

5.7 Protected Port

Messages of broadcast, multicast, etc. will flood at each port even though the flow needs no mutual communication sometimes. Under this circumstance, port isolation can separate the messages between two ports.

Instructions:

1. Click the "Port > Protected Port" in the navigation bar, check the port(s) to be isolated, "Edit" to switch this function as follows:

Prot	tected	Port Ta	able	
				Q
	Entry	Port	State	
	1	GE1	Unprotected	
	2	GE2	Unprotected	
	3	GE3	Unprotected	
	4	GE4	Unprotected	
	5	GE5	Unprotected	
	6	GE6	Unprotected	
	7	GE7	Unprotected	



Edit Protected Port

•	GE1-GE4
State	Protected
Apply	Close

Instructions for achieve port isolation:

1. Click the "Port > Protected Port" in the navigation bar, check and "Edit" the GE1, 2 and 3 to be isolated. "Apply" and finish as follows:

Protected Port Table

			Q
Entry	Port	State	
1	GE1	Protected	
2	GE2	Protected	
3	GE3	Protected	
4	GE4	Unprotected	
5	GE5	Unprotected	

2. GE1, 2 and 3 fail to communicate mutually like other non-isolated ports.

5.8 Storm Control

Storms generated via broadcast, unknown multicast and unicast messages are prevented as follows. These messages will be suppressed subject to packet rates respectively. The average rate of the messages received by monitoring interfaces will be compared with the max threshold configured during an inspection interval. Configured storm policing will be performed at this interface if the average rate exceeds the max threshold.

When a L2 Ethernet interface receives the broadcast, unknown multicast or unicast messages, the device will forward them to other L2 interfaces in a same VLAN (Virtual Local Area Network) if the egress interface cannot be recognized according to destination MAC addresses. As a result, broadcast storm may occur to degrade device operation performance.

Three kinds of message flow can be controlled by storm policing characteristics to stay away from broadcast storms.

Instructions:

1. Click the "Port > Storm Control" in the navigation bar to configure the attributes related to storm policing such as mode as follows:



Mode	 Packet / Sec Kbits / Sec 	
IFG	 Exclude Include 	
Apply		

2. Select the appropriate port and "Edit" it by configuring the policing rates of broadcast, unknown multicast and unicast storms at each port.

									Q	
	Broadcast Unknown Multicast Unknown Unicast									
	Entry	Port	State	State	Rate (Kbps)	State	Rate (Kbps)	State	Rate (Kbps)	Action
	1	GE1	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
	2	GE2	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
	3	GE3	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
	4	GE4	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
	5	GE5	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
	6	GE6	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
	7	GE7	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
m	8	GE8	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop

3. Configure info such as storm switch and rate, "Apply" and finish as follows:

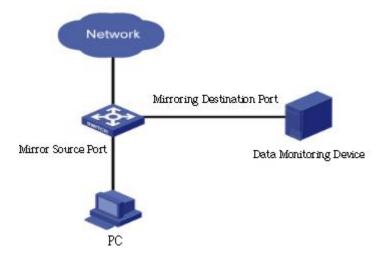
Port	GE1-GE3		
State	Enable		
Bard at	Enable		
Broadcast	10000	Kbps (16 - 1000000, default 10000)	
	Enable		
Unknown Multicast	10000	Kbps (16 - 1000000, default 10000)	
11-1	Enable		
Unknown Unicast	10000	Kbps (16 - 1000000, default 10000)	
Action	 Drop Shutdown 		

5.9 Mirroring

Port Mirroring copies the message of a specified switch port to the destination port. The copied port is the Source Port, and the copying port is the Destination Port. Destination Port accesses to data inspection devices so that users can analyze the messages received to monitor network and troubleshoot as follows:



Shenzhen Hongrui Optical Technology Co., Ltd.



Instance

PC1 and PC2 access Switch A through interface GE1 and GE2 respectively.

Users intend to monitor the messages transmitted from PC2 to PC1.

Instructions:

1. Click the "Port > Mirroring" in the navigation bar. 4 sets of flow mirroring rules can be configured as follows:

					Q
	Session ID	State	Monitor Port	Ingress Port	Egress Port
0	1	Disabled			
0	2	Disabled	8 9	()	2 717 8
0	3	Disabled			
0	4	Disabled	19 -22 -0	19 <u>00</u> 0	(111)

2. Select one session and "Edit" it in the mirroring group configuration interface:



124	8.43			
 IT	IVI I	ILL	огі	ng

Session ID	1
State	🖂 Enable
Monitor Port	GE1 Send or Receive Normal Packet
Ingress Port	Available Port Selected Port GE1 GE2 GE5 GE3 GE6 GE4 GE10 Image: Compare the second secon
Egress Port	Available PortSelected PortGE1GE2GE5GE3GE6GE4GE9Image: Comparison of the second

Interface data are as follows

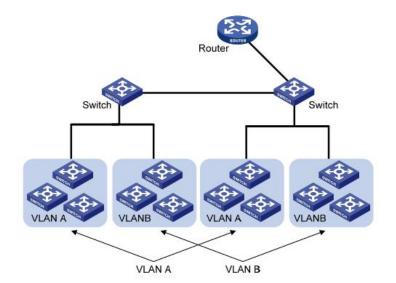
Configuration Items	Description					
Session ID	The switch has 4 session IDs by default.					
State	The mirroring group can be enabled or not.					
Monitor Port	Only one ordinary physical port can be selected, excluding link aggregation port and source port.					
Ingress Port	Any message received will be mirrored to the destination port.					
Egress Port	Any message transmitted will be mirrored to the destination port.					

6 VLAN

VLAN is formulated not restricted to physical locations, which means the hosts in a same VLAN can be placed at will. As shown below, each VLAN, as a broadcast domain, divides a physical LAN into logical LANs. Hosts can exchange messages by means of traditional communication. For the hosts in different VLANs, the device such as router or L3 switch is a must.



Shenzhen Hongrui Optical Technology Co., Ltd.



VLAN is superior to the traditional Ethernet in terms of:

- Broadcast domain coverage: the broadcast message in a LAN is limited in a VLAN to save the bandwidth and handle the network-related issues more efficiently.
- LAN security: VLAN hosts fail to communicate with each other since the messages are separated by the broadcast domain in the data link layer. They need a router or a Layer 3 switch for Layer 3 forwarding.
- Flexibility of creating a virtual working team: VLAN can create a virtual working team beyond the control of physical network. Users have access to the network without changing the configuration if their physical locations are moving within the scope. This management switch is compatible with VLAN types based on 802.1Q, protocols, MAC, and ports. For default configuration, 802.1Q VLAN mode should be adopted. Port VLAN is divided subject to a switch's interface No. Network administrator gives each switch interface a different PVID, namely a port default VLAN. If a data frame without a VLAN tag flows into a switch interface with a PVID, it will be marked with the same PVID, or it will get rid of an additional tag even though the interface has a PVID.
- The solution to a VLAN frame depends on the interface type, which eases member definition but re-configures VLAN in case of member mobility.

6.1 VLAN

6.1.1 Create VALN

Instructions for creating a new VLAN:

1. Click the "VLAN > VLAN > Create VLAN" to select a name in the valid VLAN box, move it to the VLAN creating box on the right (up to 256 VLANs can be created). "Apply" and finish as follows:



Available VLAN C	ted VLAN
AN VLAN 2 VLAN 3 VLAN 4 VLAN 5 VLAN 6 VLAN 7 VLAN 8 VLAN 9	N 1

Apply

VLAN Table

	VLAN	Name	Туре	VLAN Interface State					
0	1	default	Default	Disabled	7				
					First	Previous	1	Next	Last

2. The VLAN created will be displayed in the VLAN Table. Users can "Edit" the VLAN as follows: Edit VLAN Name

Name	VLAN0002	
Apply	Close	

Interface data are as follows.

Configuration Items	Description
VLAN ID	It is required to select an ID ranging from 1 to 4,094. For example, 1-3,5,7 and 9. LAN 1 is the default, which won't be repeated in another new VLAN.
Name	It is optional to modify the VLAN description as required.

6.1.2 VLAN Configuration

There are two methods. One is to add multiple ports under a single VLAN. The other is to add a port to multiple VLANs. They are configured according to different purposes.

Instructions for the first method to add the current port to a specified VLAN

1. Click the "VLAN > VLAN > VLAN Configuration" in the navigation bar, select the VLAN ID on the upper left,



and then click the port info as follows:

VLAN Configuration Table

VLAN default •

						Q	
Entry	Port	Mode		Membership		PVID	Forbidden
1	GE1	Trunk	Excluded	C Tagged	Untagged		
2	GE2	Trunk	Excluded	Tagged	Untagged	1	
3	GE3	Trunk	Excluded	Tagged	Untagged	1	
4	GE4	Trunk	Excluded	Tagged	Untagged	1	
5	GE5	Trunk	Excluded	Tagged	Untagged	1	
6	GE6	Trunk	Excluded	Tagged	Untagged	1	
7	GE7	Trunk	Excluded	Tagged	Untagged		
8	GE8	Trunk	Excluded	Tagged	Untagged	1	

Interface data are as follows.

Configuration Items	Description					
VLAN	VLAN ID to be configured					
Port	Port list					
Mode	VLAN mode of port					
Membership	Member roles at the VLAN port:					
	Excluded: the port is out of this VLAN					
	Tagged: the port is a tagged member of this VLAN					
	Untagged: the port is an untagged member of this VLAN					
PVID	Whether this VLAN is the port PVID					
Forbidden	Whether the VLAN message is forbidden to be forwarded at					
	this port					

6.1.3 Membership

Instructions for the second method to add the current port to a specified VLAN

1. Click the "VLAN > VLAN > Membership" in the navigation bar, select the port to be configured and "Edit" to configure its attributes:



Membership Table

				Q				
	Entry	Port	Mode	Administrative VLAN	Operational VLAN			
0	1	GE1	Trunk	1UP	1UP			
0	2	GE2	Trunk	1UP	1UP			
0	3	GE3	Trunk	1UP	1UP			
0	4	GE4	Trunk	1UP	1UP			
0	5	GE5	Trunk	1UP	1UP			
0	6	GE6	Trunk	1UP	1UP			
0	7	GE7	Trunk	1UP	1UP			

Edit Port Setting

Port	GE2
Mode	Trunk
Membership	10 1UP 2T 3T 4T 5T 6T 7T 8T Forbidden Excluded Tagged Untagged Untagged PVID

Interface data are as follows.

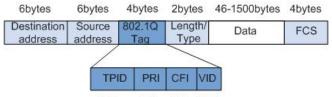
Configuration Items	Description
Port	Port list
Mode VLAN mode of port	
Membership	The port is the attribute of VLAN ID and VLAN: Forbidden: do not forward the VLAN message Excluded: the port out of the VLAN Tagged: The Tagged member of the VLAN Untagged: The Untagged member of the VLAN PVID: whether the VLAN is the port PVLAN



6.1.4 Port Setting

Trunk configuration. Connected with other switches, Trunk interfaces mainly connect trunk links to allow the VLAN frames to flow through. IEEE 802.1q is the encapsulation protocol of Trunk link and considers the formal standard for Virtual Bridged Local Area Networks. It changes the frame format of Ethernet by adding a 4-bit 802.1q Tag between the source MAC address field and the protocol field.

802.1q frame format



2bytes 3bits 1bit 12bits

Meanings of 802.1q tag fields

Field	Length	Name	Analysis
TPID	2 bytes	Tag Protocol Identifier to describe the frame type	It refers to the 802.1q Tag frame when the value is 0x8,100, which will be discarded if relevant equipment fails to receive it.
PRI	3 bits	Frame Priority	It ranges from 0 to 7, with the higher priority represented by larger number. Data frame with higher priority will be sent preferentially in case of switch congestion.
CFI	1 bit	Canonical Format Indicator to reveal whether the MAC address is classical or not.	MAC address is classical when CFI is 0 and non-classical when CFI is 1. It promotes the compatibility between Ethernet and token ring. CFI will be 0 in the Ethernet.
VID	12 bits	VLAN ID indicates the VLAN to which the frame belongs.	It ranges from 0 to 4,095, with 1 to 4,094 valid since 0 and 4,095 are the protocol retention values.

Packets sent by each switch supporting 802.1q protocol contain a VLAN ID to indicate the VLAN to which the switch belongs. Therefore, Ethernet frames are divided into two types as follows in a VLAN switching network:

- Tagged frame: it refers to the frame adding a 4-bit 802.1q Tag.
- Untagged frame: it refers to the original frame without a 4-bit 802.1q Tag.
 Connected with other switches, Trunk interfaces mainly connect trunk links to allow the VLAN frames to



flow through.

Instructions for trunk interface configuration:

1. Click the "VLAN > VLAN > Port Setting" in the navigation bar, select the port and "Edit" it to configure the attributes:

Port Setting Table

						Q		
	Entry	Port	Mode	PVID	Accept Frame Type	Ingress Filtering	Uplink	TPID
1	1	GE1	Trunk	1	All	Enabled	Disabled	0x8100
	2	GE2	Trunk	1	All	Enabled	Disabled	0x8100
	3	GE3	Trunk	1	All	Enabled	Disabled	0x8100
	4	GE4	Trunk	1	All	Enabled	Disabled	0x8100
	5	GE5	Trunk	1	All	Enabled	Disabled	0x8100
	6	GE6	Trunk	1	All	Enabled	Disabled	0x8100
	7	GE7	Trunk	1	All	Enabled	Disabled	0x8100
	8	GE8	Trunk	1	All	Enabled	Disabled	0x8100

Edit Port Setting

Port	GE4-GE8	
Mode	 Hybrid Access Trunk Tunnel 	
PVID	1	(1 - 4094)
Accept Frame Type	 All Tag Only Untag Only 	
Ingress Filtering	Enable	
Uplink	Enable	
TPID		

Interface data are as follows.

Configuration Items	Description
Port	Port No. to be configured
Mode	VLAN mode of port
	Hybrid: port in this mode serves as the member of
	Tagged and Untagged ports of VLANs
	Access: port in this mode serves as the only member of
	VLAN
	Trunk: port in this mode serves as the only Untagged



Shenzhen Hongrui Optical Technology Co., Ltd.

	member of PVID and the Tagged member of VLANs Tunnel: Port Q-in-Q VLAN
PVID	Port native VLAN
Accept Frame Type	Message types received by ports All: all messages Tag Only: only Tagged messages will be received Untag Only: only Untagged messages will be received
Ingress Filtering	A switch to decide to filter VLAN messages excluded at the port
Uplink	Whether in uplink mode or not
TPID	Identification No. of VLAN Tag

6.2 Voice VLAN

Traditionally, ACL (Access Control List) will be applied to distinguish Voice Data and QoS (Quality of Service) will be used to ensure transmission quality, thus enhancing the priority. In order to simplify user configuration and facilitate voice flow management, Voice VLAN emerges. Enabled interface judges whether it is Voice Data flow or not according to the source MAC address field accessing the interface data flow. The message in the source MAC address is the Voice Data flow, which confirms to the OUI (Organizationally Unique Identifier) of the voice devices that are configured by the system. The interfaces receiving Voice Data flow will automatically transmit to Voice VLAN, thus simplifying user configuration and Voice Data management.

OUI of Voice VLAN

OUI represents a MAC address field. Its address can be calculated based on the 48-bit MAC address and the corresponding bit of mask. The number of bits of ingress MAC address and matching OUI is determined by the length of the all "1"-bit in the mask. For example, if the MAC address is 1-1-1 and the mask is FFFF-FF00–0000, the result of execution and calculation of MAC address and corresponding mask, namely OUI, will be 0001–0000–0000.

If the first 24 bits of the ingress MAC address are matched with those of OUI, the enabled Voice VLAN interface identifies the data flow and the ingress device as the Voice Data flow and voice device respectively.

Voice VLAN is divided for user Voice Data flow. Voice VLANs are created to connect the interfaces linked with voice devices to transmit the Voice Data inside in a centralized way.

Voice Data and non-Voice Data often exist in the same network. Voice Data needs a higher priority than other business data during transmission to reduce the possible delay and packet loss.

1. Click the "VLAN > Voice VLAN > Property" in the navigation bar as follows.



State	Enable	
VLAN	None V	
	Enable	
CoS / 802.1p Remarking	6 🗸	
Aging Time	1440	Min (30 - 65536, default 1440)

Apply

Interface data are as follows.

Configuration	Description
Items	
State	Check and enable the Voice VLAN
VLAN	Specify the VLAN ID added ranging from 1 to 4,094, e.g. 1-3, 5, 7
	and 9, with VLAN 1 by default. Other VLANs must be added in an
	untagged way to the port needing links.
CoS / 802.1p	Whether to redefine the Voice VLAN message priority or not
Remarking	
Aging Time	Table aging time

Port Setting Table

						Q
	Entry	Port	State	Mode	QoS Policy	
	1	GE1	Disabled	Auto	Voice Packet	
	2	GE2	Disabled	Auto	Voice Packet	
	3	GE3	Disabled	Auto	Voice Packet	
	4	GE4	Disabled	Auto	Voice Packet	
	5	GE5	Disabled	Auto	Voice Packet	
	6	GE6	Disabled	Auto	Voice Packet	
m	7	GE7	Disabled	Auto	Voice Packet	

Edit Port Setting

Port	GE1
State	Enable
Mode	Auto
QoS Policy	Voice Packet All
Apply	Close



Interface data are as follows.

Configuration	Description
ltems	
Port	Enabled Voice VLAN port
State	Check and enable the Voice VLAN
Mode	Voice VLAN port can be operated in auto mode and manual mode.
QoS Policy	Select the message to be affected by QoS

2. Click the "VLAN > Voice VLAN > Voice OUI" in the navigation bar to configure the address segment of OUI of Voice VLAN as follows:

Void	e OUI Ta	ble					
Showing All ~ entries		Showing 1 to	Showing 1 to 8 of 8 entries		Q		
	OUI	Description					
	00:E0:BB	3COM					
	00:03:6B	Cisco					
	00:E0:75	Veritel					
	00:D0:1E	Pingtel					
	00:01:E3	Siemens					
	00:60:B9	NEC/Philips					
	00:0F:E2	H3C					
	00:09:6E	Avaya					
	Add	Edit	Delete		F	irst Previous	1 Next Last

Add Voice OUI

oui	_:_	_:_			 		 		
Description]					
Apply Close	se								

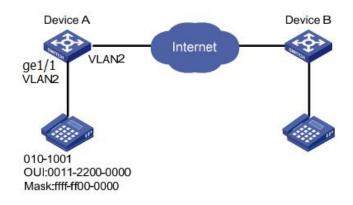
- 3. Fill in corresponding configuration items.
- 4. "Apply" and finish as follows.



Voice OUI Table

	OUI	Description				
m	00:E0:BB	3COM				
	00:03:6B	Cisco				
	00:E0:75	Veritel				
	00:D0:1E	Pingtel				
	00:01:E3	Siemens				
	00:60:B9	NEC/Philips				
	00:0F:E2	H3C				
	00:09:6E	Avaya				
	98:00:36	H7650				
				First	evious 1	Next Las
	Add	Edit	Delete			

For example, configure the Voice VLAN in manual mode so that the ports accessing IP telephony can ingress/egress the Voice VLAN and transmit voice flow within it. Create VLAN2 to operate Voice VLAN securely, which allows only Voice Data to flow through. IP telephony transmits Untagged voice flow to GE1, the ingress Trunk port. Users must customize an OUI (0011-2231-05e1) and configure the Voice VLAN networking diagram in automatic mode.



Instructions:

1. Create a VLAN to recognize the VLANs where employees belong. Click the "VLAN > VLAN > Create VLAN" in the navigation bar to add VLAN 2 to the VLAN list on the right. "Apply" and finish:



Edit

Delete

	VLAN	Available VL VLAN 3 VLAN 4 VLAN 5 VLAN 6 VLAN 7 VLAN 8 VLAN 9 VLAN 10	AN	Created VLAN VLAN 1 VLAN 2			
	Apply) le					
Show	ing All	\vee entries		Showing 1 to 2 of 2 e	ntries	Q	
	VLAN	Name	Туре	VLAN Interface State			
0	1	default	Default	Disabled			
0	2	VLAN0002	Static	Disabled			
_					(First Previous 1	Next Las

2. Configure the Ethernet interface GE1 of Switch A in Hybrid mode. Click the "VLAN > VLAN > Port Setting" in the navigation bar, "Edit" GE1 in Hybrid mode:

Port	Settin	g Tabl	e					
	Entry	Port	Mode	PVID	Accept Frame Type	Ingress Filtering	Uplink	TPID
	1	GE1	Hybrid	1	All	Enabled	Disabled	0x8100

 Click the "VLAN > Voice VLAN > Voice OUI" in the navigation bar to configure and add the range of OUI MAC address, and enter the first 24 bits of MAC address of voice device: 00:11:22. "Apply" and finish as follows:

	1					
Showing All 🗸	entries	Showing 1 to 1 of 1 entries		Q		
OUI	Description					
00:11:22	aaa					
Add	Edit	Delete	First	Previous 1	Next	Last

4. Enable the Voice VLAN of port GE1. Click the "VLAN > Voice VLAN > Property" in the navigation bar to enable the global configuration, select VLAN2. Select port GE1 in the configuration list, "Edit" and enable the auto mode. "Apply" and finish as follows:



VLAN	VLAN0002 V	
CoS / 802.1p Remarking	Enable	
	0 -	
Aging Time	1440 Min (30 - 65536, default 1440)	

Port Setting Table

					Q
Entry	Port	State	Mode	QoS Policy	
1	GE1	Enabled	Auto	Voice Packet	
2	GE2	Disabled	Auto	Voice Packet	



• With the auto mode enabled, ports will forward Voice VLAN messages even though there is no port in VLAN2.

6.3 Protocol VLAN

Protocol VLAN distributes different VLAN IDs according to the protocol (family) type and encapsulation format of the messages received by the interfaces.

Administrators should prepare the mapping scheme between the protocol domain of Ethernet frame and VLAN ID which will be added if untagged frames are received. Strength: Such division method will enhance the management and maintenance by binding the network services and VLANs. Shortcomings: Initial configuration of the mapping relation scheme is necessary. Address formats of protocols should be analyzed and converted, thus leading to a lower speed due to many resources consumed. Instructions:

1. Click the "VLAN > Protocol VLAN > Protocol Group" in the navigation bar as follows:

Protocol Group Table

Showing All 🗸	entries	Showing 1						
Group ID	Frame Type	Protocol Value						
1	Ethernet_II	0x8888			-			
Add	Edit	Delete		First	Previous	1	Next	Last



Add Protocol Group

Group ID	2 ~	
Frame Type Protocol Value	Ethernet_II V	(0x600 ~ 0xFFFE)

Interface data are as follows.

Configuration Items	Description
Group ID	Protocol VLAN Group
Frame Type	Frame types: Ether2, LLC, RFC 1042
Protocol Value	It ranges from 0x600 to 0xFFFE

- 2. Fill in corresponding configuration items.
- 3. "Apply" and finish.

Protocol Group Table

Show	ving All 🗸	entries	Showing 1		Q,				
	Group ID	Frame Type	Protocol Value						
	1	Ethernet_II	0x8888						
	2	RFC_1042	0x8889						
	Add	Edit	Delete		First	Previous	1	Next	Last

4. Click the "VLAN > Protocol VLAN > Group Binding" in the navigation bar to bind the protocol No., port No. and VLAN ID, to bring the configuration into effect as follows:

Gro	up Bi	nding Tal	ole					
Show	ving All	✓ entries		Showing 1 to 1 of 1 entries		Q		
	Port	Group ID	VLAN					
	GE1	1	10					
	Add	Edit		Delete	First	Previous	Next	Last

Description:

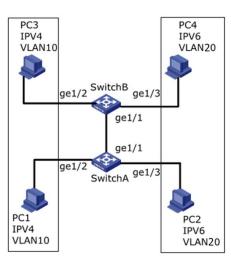
Configure the matching protocols IPv4 and IPv6, as well as the ARP protocol.

For example, PC1 and 3 can access mutually, with IPv4 communication protocol binding with VLAN10. PC2 and 4 can access mutually, with IPv6 communication protocol binding with VLAN20.

Networking diagram of protocol VLAN division



Shenzhen Hongrui Optical Technology Co., Ltd.



Instructions:

1. Create a VLAN to recognize the VLANs where employees belong. Click the "VLAN > VLAN > Create VLAN", add the VLAN10 and 20 to the VLAN Creating List on the right, "Apply" and finish:

Apply	e	<u> </u>		
	 ✓ entries 	Showing 1 to 3	of 3 entries	Q
VLAN	Name	Туре	VLAN Interface State	
	Name	Type Default	VLAN Interface State Disabled	
VLAN				

2. Configure GE2 and GE3 interfaces of Switch A in Hybrid mode. Click the "VLAN > VLAN > Port Setting", "Edit" the interfaces in Hybrid mode:

Q [

TPID

Port	t Settin	ng Tab	le			
	Entry	Port	Mode	PVID	Accept Frame Type	Ingress Filtering
	1	GE1	Trunk	1	All	Enabled
1 mm 10	2	050	Llubrid	1000	A 11	Enchlad

	1	GET	Trunk	1	All	Enabled Disabled 0x8100
	2	GE2	Hybrid	1	All	Enabled Disabled 0x8100
	3	GE3	Hybrid	1	All	Enabled Disabled 0x8100
	4	GE4	Trunk	1	All	Enabled Disabled 0x8100
	5	GE5	Trunk	1	All	Enabled Disabled 0x8100
-						

3. Add the Untagged GE2 and GE3 to VLAN10 and VLAN20 respectively. Click the "VLAN > VLAN > VLAN



Shenzhen Hongrui Optical Technology Co., Ltd.

Configuration", drop down the list to choose VLAN10 and the Untagged GE2 port. Following the same steps, add the untagged GE3 to VLAN20 as follows:

VLAN Configuration Table

LAN 🛛	/LAN001	10 ~					Q	
Entry	Port	Mode		Membership	C.	PVID	Forbidden	
1	GE1	Trunk	Excluded	○ Tagged	O Untagged			
2	GE2	Hybrid	O Excluded	○ Tagged	Untagged			
3	GE3	Hybrid	Excluded	○ Tagged	O Untagged			

VLAN Configuration Table

LAN 🛛	/LAN002	20 ~					
							Q
Entry	Port	Mode		Membership		PVID	Forbidden
1	GE1	Trunk	Excluded	○ Tagged	○ Untagged		
2	GE2	Hybrid	Excluded	○ Tagged	O Untagged		
3	GE3	Hybrid	O Excluded	○ Tagged	Untagged		
4	GE4	Trunk	Excluded	○ Tagged	○ Untagged		
			~	-	-		

- 4. Add the Untagged GE2 and GE3 interfaces of Switch B to VLAN whose ports need links. Steps are like step 2 and 3.
- 5. Add the Tagged GE1 interface of Switch A to VLAN10 and 20. Click the "VLAN > VLAN > VLAN Configuration", drop down the list to select VLAN10 and the Tagged member of GE1. Configure VLAN20 similarly.

VLAN	Config	juration	Table					
VLAN 🔽	/LAN001	0 ~						
							Q	
Entry	Port	Mode		Membership	0	PVID	Forbidden	
1	GE1	Trunk	O Excluded	Tagged	O Untagged			
		guration	Table					
VLAN []	/LAN002	20 ~					Q	
Entry	Port	Mode		Membership)	PVID	Forbidden	
1	GE1	Trunk	O Excluded	• Tagged	O Untagged			

6. Related protocol and VLAN. VLAN IDs are assigned according to the protocol (family) type and encapsulation format of the messages received by interfaces. Click the "VLAN > Protocol VLAN > Protocol Group" in the navigation bar to add 2 rules for protocol groups:



Protocol Group Table

Show	howing All 💛 entries		Showing	1 to 2 of 2 entries	Q
	Group ID	Frame Type	Protocol Value		
	1	Ethernet_II	0x0800		
	2	Ethernet_II	0x86DD		
	Add	Edit	Delete		First Previous 1 Next Last

7. Port, protocol group, and VLAN binding. Click the "VLAN > Protocol Group > Group Binding", "Add" to bind GE2 and binding group ID1 with VLAN10, and to bind GE3 and binding group ID2 with VLAN20:

howing All 🗸 entries				Showing 1 to 2 of 2 entries	Q			
	Port	Group ID	VLAN					
	GE2	1	10					
	GE3	2	20					

6.4 MAC VLAN

MAC-based VLANs are divided subject to the MAC addresses in the network card. Administrators will prepare the mapping scheme between MAC address and VLAN ID which will be added if the switch receives untagged frames.

Strength: There is no need to re-configure VLAN when the physical location of a terminal user changes, which ensures user security and access flexibility. Shortcoming: It applies to the scene where network card and simple network environment are infrequently replaced, with members defined in advance. Instructions:

1. Click the "VLAN > MAC VLAN > MAC Group" in the navigation bar, and "Add" a new MAC group as follows:

MAC Group	Table							
Showing All 🗸	entries S	Showing 1	to 1 of 1 entries		Q			
Group ID	MAC Address	Mask						
1	00:0A:5A:00:00:00	24	k =					
Add Edit	Delete			First	Previous	1	Next	ast



Add MAC Group

Group ID	2	(1 - 2147483647)	
AC Address	00:22:00:22:00:22		
Mask	48	× (9 - 48)	

Interface data are as follows.

Configuration	Description
Items	
Group ID	MAC VLAN Group ID
MAC Address	The MAC address to be bound with VLAN
Mask	It indicates the MAC address port. Enter 48 if it is an exact match. Others should be consistent with the masks of IP addresses.

For example, a company with high info security requirements allows its PCs only to access the internal network. As is shown, switch GE1 connects the uplink ports of Switch A while its downstream ports connect PC1, 2 and 3. As a result, PC1, 2 and 3 can access the internal network through Switch A and Switch, while other PCs can't.

Configuration logic: following steps are used to divide the VLAN based on MAC address.

- 1. Create a relevant VLAN.
- 2. Add Ethernet interfaces to the VLAN in a correct way.
- 3. Connect the VLAN with the MAC addresses of PC1, 2 and 3.

Data preparation: following data should be prepared for the configuration instance:

- Set GE1 PVID of 100 on the switch.
- Set GE1 to access VLAN10 in the Untagged way on the switch.
- Set GE2 to access VLAN10 in the Tagged way on the switch.
- Set the Switch A interface by default, namely all interfaces will be added to VLAN1 in an Untagged way.
- Connect the MAC addresses of PC1, 2 and 3 with VLAN10.

Draw a networking diagram for VLAN division based on MAC addresses:

Instructions:

1. Create a VLAN to recognize the VLANs where employees belong. Click the "VLAN > VLAN > Create VLAN" in the navigation bar, add VLAN10 to the VLAN Creating List on the right, "Apply" and finish as follows:



3

GE3

0

1UP

Trunk

MAC Group Table

VLAN Table

	VLAN	Name	Туре	VLAN Interface State					
0	1	default	Default	Disabled					
0	10	VLAN0010	Static	Disabled					
0	100	VLAN0100	Static	Disabled					
-		9 BB	415		First	Previous	1	Next	Las

2. Configure Switch's GE1 in Hybrid mode with PVID of 100 to serve as an Untagged member of VLAN10. Configure GE2 in Trunk mode to serve as a Tagged member of VLAN10.

ort	Settin	ng Tab	le						
								Q	
	Entry	Port	Mode	PVID	Accept Frame	Туре	Ingress Filtering	Uplink	TPID
	1	GE1	Hybrid	100	All		Enabled	Disabled	0x8100
	2	GE2	Trunk	1	All		Enabled	Disabled	0x8100
lem	bersh	ip Tab	le					Q	
	Entry	Port	Mode	Admin	istrative VLAN	Oper	ational VLAN		
С	1	GE1	Hybrid	1U, 10	U, 100P	1U, 1	0U, 100P		
	2	GE2	Trunk	1UP, 1	от	1UP,	10T		

1UP

 Configure the Switch A's interfaces by default, namely all interfaces access VLAN1 in an Untagged way. Connect the MAC addresses of PC1, 2 and 3 with VLAN10. Click the "VLAN > MAC VLAN > MAC Group" in the navigation bar, enter the MAC addresses of PC1 (0022-0022-0022), PC2 (0033-0033-0033) and PC3 (0044-0044-0044), with the mask of 48-bit exact match as follows:

howing All 🗸 entries			Show	1 to 3 of 3 entries	Q				
Gr	oup ID	MAC Address	Mask						
	1	00:22:00:22:00:22	48						
	2	00:33:00:33:00:33	48						
	3	00:44:00:44:00:44	48						
Add		Edit Dele		Fi	irst	Previous	1	Next)

4. Click the "VLAN > MAC VLAN > Group Binding" in the navigation bar, "Add" to select the Hybrid port only, MAC group ID to be bound, and specified VLAN ID. "Apply" and finish:



MAC Group Table

Group ID	MAC Address	Mask	
1	00:22:00:22:00:22	48	
2	00:33:00:33:00:33	48	
3	00:44:00:44:00:44	48	

5. Configuration verification

Only PC1, 2 and 3 have access to the internal network.

6.5 Surveillance VLAN

Surveillance VLAN is mainly used for video stream packets. In order to ensure the priority of such packets in the transmission process, it is higher than ordinary packets

Instructions:

1. Click the "VLAN > Surveillance VLAN > Property" in the navigation bar as follows.

State	Enable	
VLAN	None	\checkmark
CoS / 802.1p	Enable	
CoS / 802.1p Remarking	6 🗸	
Aging Time	1440	Min (30 - 65536, default 1440)

Apply

Configuration	Description
Items	
State	Check and enable the Surveillance VLAN
VLAN	Specify the VLAN ID added ranging from 1 to 4,094, e.g. 1-3, 5, 7
	and 9, with VLAN 1 by default. Other VLANs must be added in an
	untagged way to the port needing links.
CoS / 802.1p	Whether to redefine the Voice VLAN message priority or not
Remarking	
Aging Time	Table aging time



Port Setting Table

Entry	Port	State	Mode	QoS Policy
1	GE1	Disabled	Auto	Video Packet
2	GE2	Disabled	Auto	Video Packet
3	GE3	Disabled	Auto	Video Packet
4	GE4	Disabled	Auto	Video Packet
5	GE5	Disabled	Auto	Video Packet
6	GE6	Disabled	Auto	Video Packet
7	GE7	Disabled	Auto	Video Packet

Edit Port Setting

	GE1-GE2
State	Enable
Mode	 Auto Manual
QoS Policy	Video Packet All

Interface data are as follows.

Configuration	Description
Items	
Port	Enabled Voice VLAN port
State	Check and enable the Surveillance VLAN
Mode	Surveillance VLAN port can be operated in auto mode and manual mode.
QoS Policy	Select the message to be affected by QoS

2. Click the "VLAN > Surveillance VLAN > Surveillance OUI" in the navigation bar to configure the address segment of OUI of Surveillance VLAN as follows:

Showing All entries	Showing 0 to 0 of 0	entries	Q			
OUI Description						
	0 results fou	nd.				_
		First	Previous	1	Next	Last



Add Voice OUI

oui	:_		 		
Description					
Apply	lose				

- 3. Fill in corresponding configuration items.
- 4. "Apply" and finish as follows.

Surveillance OUI Table

	ving All ▼	entrico	Showing 1 to 1 of 1	enuies	a			
	OUI	Description						
	98: <mark>00:</mark> 36	H7650	-					
				First	Previous	1	Next	Last
j.	Add	Edit	Delete					

6.6 GVRP

GVRP VLAN registration protocol is an application of general attribute registration protocol, which provides 802.1Q compatible VLAN pruning function and dynamic VLAN establishment on 802.1Q trunk port trunk port.

GVRP switches can exchange VLAN configuration information with each other, cut unnecessary broadcast and unknown unicast traffic, and create and manage VLAN dynamically on switches connected through 802.1Q trunk.

GID and GIP are used in GVRP, which provide the general state mechanism description and information dissemination mechanism for GARP based applications respectively. GVRP only runs on 802.1Q trunk links. GVRP cuts off the trunk link so that only the active VLAN is transmitted on the trunk connection. Before GVRP adds a VLAN to the trunk line, it first receives the join information from the switch. GVRP update information and timer can be changed. The GVRP ports have a variety of operating modes to control how they tailor VLANs. GVRP can dynamically add and manage VLAN for VLAN database

GVRP supports the propagation of VLAN information between devices. In GVRP, the VLAN information of a switch can be configured manually, and all other switches in the network can dynamically understand the VLANs. The terminal node can access any switch and connect to the required VLAN. In order to use GVRP, a GVRP compatible network interface card (NIC) should be installed. GVRP compatible NIC can be configured to join the required VLAN, and then access to a GVRP enabled switch. The communication connection between NIC and switch is established, and VLAN connectivity is realized between NIC and switch.



6.6.1 Property

Global and port configuration

Instructions:

1. Click the "VLAN > GVRP > Property" in the navigation bar as follows.

perational	Timeout		
Join	20	cs (2 - 16375, default 20)	
Leave	60	cs (45 - 32760, default 60)	
LeaveAll	1000	cs (65 - 32765, default 1000)	

Interface data are as follows.

Configuration	Description
Items	
State	The GVRP feature is globally enabled by setting
Join	A value in the range of 2-16375cs, i.e. in units of one hundredth
	of a second. The default value is 20cs.
leave	a value in the range of 45-32760cs, i.e. in units of one hundredth
	of a second. The default is 60cs.
LeaveAll	a value in the range of 65-32765cs, i.e. in units of one
	hundredth of a second. The default is 1000cs.

2. Click the "VLAN > GVRP > Property" in the navigation bar, select the port and "Edit" to enter the configuration interface as follows.

Port Setting Table

						Q	
	Entry	Port	State	VLAN Creation	Registration		
	1	GE1	Disabled	Enabled	Normal		
	2	GE2	Disabled	Enabled	Normal		
	3	GE3	Disabled	Enabled	Normal		
	4	GE4	Disabled	Enabled	Normal		
	5	GE5	Disabled	Enabled	Normal		
	6	GE6	Disabled	Enabled	Normal		
	7	GE7	Disabled	Enabled	Normal		
-	8	GE8	Disabled	Enabled	Normal		



Edit Port Setting

State	Enable
/LAN Creation	Enable
Registration	 Normal Fixed Forbidden

Interface data are as follows.

Configuration Items	Description
Port	Port list
State	Enable or disable the GVRP function of the port
VLAN Creation	Enable or disable to create VLAN automatically
Registration	Three registration modes of GVRP Normal: Allow dynamic VLAN to register on the port, and send declaration messages of static VLAN and dynamic VLAN at the same time Fixed: Dynamic VLAN is not allowed to register on the port, only static VLAN declaration messages are sent Forbidden: Dynamic VLAN is not allowed to register on the port. At the same time, all VLANs except vlan1 on the port are deleted, and only vlan1 declaration message is sent

6.6.2 Membership

View GVRP dynamic member information

Instructions:

1. Click the "VLAN > GVRP > Membership" in the navigation bar as follows.

Mem	bers	hip	Table
	_		

Showing	All	• er	ntries	Showing	g 0 to 0 of	0 entries	Q				
VLAN	Mer	nber	Dynam	ic Member	Туре						
				C) results f	ound.					
						First	Pre	vious	1	Next	Last



6.6.3 Statistics

View port GVRP message statistics

Instructions:

1. Click the "VLAN > GVRP > Statistics" in the navigation bar as follows.

Port	GE1 V
Statistics	 All Receive Transmit Error
Refresh Rate	 None 5 sec 10 sec 30 sec
Clear	
	0
Receive	0 0
Receive Join empty	
Receive Join empty Empty	0
Receive Join empty Empty Leave Empty	0 0

7 MAC Address Table

Ethernet switches are mainly innovated to forward according to the purposes in the data link layer. That is, MAC address will transmit the messages to corresponding ports according to the purposes. MAC address forwarding table is a L2 table illustrating MAC addresses and forwarding ports, which is the basis of fast forwarding of L2 messages.

MAC address forwarding table contains following data:

- Destination MAC Address
- VLAN ID belonging to port
- Forwarding ingress No. of this device

There are two message forwarding types according to MAC address table info:

- Unicast mode: the switch directly transmits the messages from the table's egress when MAC address forwarding table contains corresponding entries with the destination MAC address.
- Broadcast mode: When the switch receives the messages with the destination address full of F-bits, or



Shenzhen Hongrui Optical Technology Co., Ltd.

there is no entry corresponding to the MAC destination address in the forwarding table, the switch will forward the messages to all ports excluding the receiving port in this way.

7.1 Dynamic Address

Aging time and table info of MAC addresses can be configured and checked on this page.

MAC address table needs constant updates to cater to network changes. It automatically generates entries that are limited by their lifetime (i.e. aging time). Those entries not refreshed after expiration will be deleted. The aging time of an entry will be recalculated if its record is refreshed before expiration.

Proper aging time helps to achieve the aging target of MAC address. Shortage of aging time may lead many switches broadcast to discover the packets of destination MAC addresses, thus influencing the switch performance.

Aging too long can cause the switch to save outdated MAC address entries, thus exhausting the forwarding resources and failing to update the forwarding table based on network changes.

The switch may remove valid MAC address table entries due to too short aging time, thus reducing forwarding efficiency. In general, the aging time recommended is 300 seconds by default.

Instructions for aging time setting:

1. Click the "MAC Address Table > Dynamic Address" in the navigation bar to the configuration and view interface:

VL/	AN	MAC Address	Port	
	1	00:0B:0E:0F:00:ED	GE3	
	1	00:CF:E0:52:B0:4F	GE3	
	1	00:CF:E0:52:B0:8B	GE3	
	1	00:E0:4C:00:53:35	GE3	
	1	00:E0:4C:2E:2C:B3	GE3	
	1	00:E0:4C:2E:2C:DD	GE7	
	1	00:E0:4C:2E:2D:4C	GE3	
	1	00:E0:4C:93:C3:00	GE3	
	1	00:E0:4D:36:99:E4	GE3	
	1	00:E0:66:70:A6:CB	GE3	

Dynamic Address Table

Interface data are as follows

Configuration Items	Description
---------------------	-------------



MAC Aging Time Enter the aging time of MAC address

- 2. Fill in corresponding configuration items.
- 3. "Apply" and finish.

MAC Table stores the MAC address, VLAN No., Ingress/Egress info, etc. that are learned by switches. When forwarding data, it will fast locate the device egress in accordance with the destination MAC address and VLAN No. query table of Ethernet frames.

To check the MAC address table, see Section 3.3 of Chapter 3

7.2 Static Address

Static table is manually configured by users and distributed to each interface board, which won't age. Instructions:

1. Click the "MAC Address Table > Static Address" as follows:

Static Add	ress Table						
Showing All	 ✓ entries 		Showing 1 to 1 of 1 entries		Q		
VLAN	MAC Address	Port					
1	00:00:11:11:22:22	GE3					
Add	Edit	Delet	e	First	Previous 1	Next	Last

Add Static Address

MAC Address	00:00:11:11:22:22	2	
VLAN	10	× (1 - 4094)	
Port	GE1 V		

Interface data are as follows.

Configurati	Description
on Items	
MAC	Required. Enter the new MAC address e.g.: HH:HH:HH:HH:HH:HH
VLAN	Required. Specify the VLAN ID
Port	Required. Select the interface type and enter the interface name
	Description: it must be the member port of the configured VLANs.

2. Fill in corresponding configuration items.

3. "Apply" and finish.



7.3 Filtering Address

The switch discards the matched data frame by configuration

Instructions:

1. Click the "MAC Address Table > Filtering Address" as follows:

Showing All entries	Showing 0 to 0 of 0 entries	Q	
VLAN MAC Address			
	0 results found.		
Add Edit Delete		First Previous 1	Next

Add Filtering Address

MAC Address		
VLAN	(1 - 4094)	
pply Close		

Interface data are as follows.

Configuration Items	Description
MAC Address	MAC address to be filtered
VLAN	VLAN of MAC address

7.4 Port Security Address

If the MAC address is set to secure Mac, the port only allows the data frames of the secure Mac to pass through forever, and the others will be discarded

Instructions:

1. Click the "MAC Address Table > Port Security Address" as follows:

Port Security Address Table

Show	ing All	entries	5	Showing	o 0 of 0 entries	Q
	VLAN	MAC Address	Туре	Port		
					esults found.	
A	dd)	Edit	elete		First	t Previous 1 Next Last



Add Port Security Address

MAC Address			
VLAN		(1 - 4094)	
Port	GE1 🔻		
Port	GE1 V		

Interface data are as follows.

Configuration Items	Description
MAC Address	MAC address for security
VLAN	VLAN of MAC address
Port	Port ID that enables port security

8 Spanning Tree

Redundant links are often used for link backup and network reliability in the Ethernet switching network. However, such links will generate loops on the switching network, leading to broadcast storm, unstable MAC address list and other faults, thus worsening users' communication quality, or even interrupting the communication. As a result, STP (Spanning Tree Protocol) appears.

Same with the development of other protocols, from the original STP defined in IEEE 802.1D, to RSTP (Rapid Spanning Tree Protocol) defined in IEEE 802.1W and to MSTP (Multiple Spanning Tree Protocol) defined in IEEE 802.1S, STP keeps upgrading.

MSTP is compatible with RSTP and STP while RSTP is compatible with STP. The contrast among these 3 protocols is shown in the table.

The contrast among 3 protocols

STP	Characteristic	Application				
STP	A tree rid of loops as the solution to	All VLANs can be shared				
	broadcast storms and redundant backups.	without discrimination in user				
	It converges slowly.	or business flow.				
RSTP	A tree rid of loops as the solution to					
	broadcast storms and redundant backups.					
	It converges rapidly.					
MSTP	A tree rid of loops as the solution to	Distinguish the user and				
	broadcast storms and redundant backups.	business flow for load sharing.				
	It converges rapidly.	Different VLANs forward the				
	Spanning trees balance the load among	flow through separate				
	VLANs. Flow of different VLANs will be	spanning trees.				
	forwarded subject to paths.					



Shenzhen Hongrui Optical Technology Co., Ltd.

After STP is deployed, the following objectives can be achieved by calculating the loops with topology:

- Loop elimination: eliminate possible communication loops by blocking redundant links.
- Link backups: activate redundant links to restore network connectivity if the active path fails.

8.1 Property

Configure STP global parameters. In specific network environment, STP parameters of some devices must be adjusted to achieve the best performance.

Instructions:

1. Click the "Spanning Tree > Property" in the navigation bar as follows:

State	Enable			
Operation Mode	 STP RSTP MSTP 			
Path Cost	 Long Short 			
BPDU Handling	FilteringFlooding			
Priority	32768	(0 - 61440, default 32768)		
Hello Time	2	Sec (1 - 10, default 2)		
Max Age	20	Sec (6 - 40, default 20)		
Forward Delay	15	Sec (4 - 30, default 15)		
Tx Hold Count	6	(1 - 10, default 6)		
Region Name	1C:2A:A3:00:34:24			
Revision	0	(0 - 65535, default 0)		
Max Hop	20	(1 - 40, default 20)		

Interface data are as follows.

Configuration	Description
Items	
State	It is checked by default to enable the spanning tree on behalf of switches.
Operation Mode	3 modes are available, namely STP, RSTP and MSTP.
Path Cost	In Long mode and Short mode
BPDU Handling	The method to handle the BPDU messages received by the device
Priority	Port priority



Hello Time	Intervals between Hello messages
	Intervals between richo messages
Max Age	Max aging time
Forward Delay	Forward delay time
Tx Hold Count	Specify the Tx-hold-count used to limit the maximum numbers
	of packets transmission per second
Region Name	MST domain name. Switch master board sets the MAC address
	by default.
	Together with the VLAN mapping table of MST domain and the
	revision level of MSTP, switch domain name will jointly determine
	the domain to which it belongs.
Revision	The MSTP revision number
Мах Нор	Specify the number of hops in an MSTP region before the BPDU
	is discarded

2. Fill in corresponding configuration items.

3. "Apply" and finish.

8.2 Port Setting

In specific network environment, STP parameters of some devices need to be adjusted for the best performance.

1. Click the "Spanning Tree > Port Setting" in the navigation bar, select the port and "Edit" to configure its attributes:

													Q	
	Entry	Port	State	Path Cost	Priority	BPDU Filter	BPDU Guard	Operational Edge	Operational Point-to-Point	Port Role	Port State	Designated Bridge	Designated Port ID	Designated Cost
	1	GE1	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-1	20000
	2	GE2	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-2	20000
	3	GE3	Enabled	200000	128	Disabled	Disabled	Disabled	Enabled	Disabled	Forwarding	0-00:00:00:00:00:00	128-3	200000
	4	GE4	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-4	20000
	5	GE5	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-5	20000
	6	GE6	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-6	20000
	7	GE7	Enabled	200000	128	Disabled	Disabled	Disabled	Enabled	Disabled	Forwarding	0-00:00:00:00:00:00	128-7	200000
-	0	GEO	Enabled	20000	100	Disabled	Disabled	Disabled	Displied	Disabled	Disabled	0.00.00.00.00.00	100.0	20000



Edit Port Setting

Port	GE1
State	🔽 Enable
Path Cost	0 (0 - 20000000) (0 = Auto)
Priority	128 🗨
Edge Port	🔄 Enable
BPDU Filter	📄 Enable
BPDU Guard	📄 Enable
Point-to-Point	 Auto Enable Disable
Port State	Disabled
Designated Bridge	0-00:00:00:00:00
Designated Port ID	128-1
Designated Cost	20000
Operational Edge	False
Operational Point-to-Point	False

.....

Interface data are as follows.

Configuration	Description
Configuration	Description
ltems	
Port	The port No. to configure attributes
State	Enable STP or not
Path Cost	Enter the path cost value of the interface Use IEEE 802.1t Standard with the value ranging from 0 to 200,000,000
Priority	 Select the port priority with smaller value representing higher priority. Interface priority affects the role of the interface on the specified MSTI. On different MSTI, users can configure the priorities for a same interface. As a result, flow of different VLANs can be forwarded along physical links to achieve VLAN load sharing. Description: MSTP will recalculate the interface role and migrate its state when its priority changes.
Edge Port	Rather than another switch or network segment, the edge port should be connected directly to user terminals. It can quickly transit to the forward state since topology changes create no loops. An edge port under configuration can be quickly transitioned to forward state by STP. To achieve this, it is recommended that Ethernet ports connected directly to user terminals should be



	configured as edge ports.
BPDU Filter	Enable BPDU Filter or not
BPDU Guard	Enable BPDU Guard or not. Unchecked by default. If BPDU Guard is enabled, the device will shut down the interfaces receiving BPDU and notify the NMS. Such interfaces can only be restored manually by network administrators.
Point-to-Point	Select enabled, shutdown, and auto modes. Auto mode: it indicates the connect state between the default auto inspection and point-to-point links. Enabled mode: it indicates the specific port is connected to the point-to-point links. Shutdown mode: it indicates the specific port fails to connect the point-to-point links.

- 2. Fill in corresponding configuration items.
- 3. "Apply" and finish.

8.3 MST Instance

A switching network is divided into multiple domains by MSTP, with independent spanning trees formed within each domain. Each Spanning Tree is called a MSTI (Multiple Spanning Tree Instance), and each domain is called a MST Region: Multiple Spanning Tree Region).

Description:

An instance is a group of VLANs that reduces communication cost and resource utilization rate. Each instance, independently calculated with topology, can balance the load. VLANs with the same topology can be mapped to a same instance, and they are forwarded according to the port state in corresponding MSTP instances.

In simple terms, mapped to the specified MST instance, one or more VLANs are distributed to a spanning tree at a time.

Instructions:

1. Click the "Spanning Tree > MST Instance" in the navigation bar, "Edit" the selected spanning tree instances to be configured as follows:

MST Instance Table

							Q	
	MSTI	Priority	Bridge Identifiter	Designated Root Bridge	Root Port	Root Path Cost	Remaining Hop	VLAN
D	0	32768	32768-1C:2A:A3:00:34:24	0-00:00:00:00:00	N/A	0	0	1-4094
0	1	32768	32768-1C:2A:A3:00:34:24	0-00:00:00:00:00:00	N/A	0	0	
0	2	32768	32768-1C:2A:A3:00:34:24	0-00:00:00:00:00:00	N/A	0	0	
0	3	32768	32768-1C:2A:A3:00:34:24	0-00:00:00:00:00:00	N/A	0	0	
0	4	32768	32768-1C:2A:A3:00:34:24	0-00:00:00:00:00:00	N/A	0	0	
0	5	32768	32768-1C:2A:A3:00:34:24	0-00.00.00.00.00.00	N/A	0	0	



Edit MST Instance Setting

Priority	32768	(0 - 61440, default 32768)
Bridge Identifiter	32768-1C:2A:A3:	00:34:24
Designated Root Bridge	0-00:00:00:00:00:	00
Root Port		
Root Path Cost	0	
Remaining Hop	0	

Interface data are as follows.

Configuration	Description
Items	
MSTI	Instance No. of spanning trees ranges from 0 to 15
VLAN	VLAN No. mapped from instances
Priority	Set the priority of a multiple of 4,096 for the specified instance,
	ranging from 0 to 65,535 with 32,768 as default.

- 2. Fill in corresponding configuration items.
- 3. "Apply" and finish as follows.

8.4 MST Port Setting

Instructions:

1. Click the "Spanning Tree > MST Port Setting" in the navigation bar, check the port to be modified from the list of all ports of the device, "Edit" to enter the detailed configuration interface as follows:

1511	0 •											
_											Q	
	Entry	Port	Path Cost	Priority	Port Role	Port State	Mode	Туре	Designated Bridge	Designated Port ID	Designated Cost	Remaining Hop
	1	GE1	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-1	0	20
	2	GE2	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-2	0	20
	3	GE3	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-3	0	20
	4	GE4	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-4	0	20
	5	GE5	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-5	0	20
	6	GE6	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-6	0	20
	7	GE7	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-7	0	20
	8	GE8	20000	128	Disabled	Forwarding	RSTP	Boundary	0-00:00:00:00:00:00	128-8	0	20
	9	GE9	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-9	0	20



Edit MST Port Setting

MSTI Port	GE1-GE2	
Path Cost	0	(0 - 200000000) (0 = Auto)
Priority	128 💌	
Port Role	Disabled	
Port State	Disabled	
Mode	RSTP	
Type	Boundary	
Designated Bridge	0-00:00:00:00:00:00	
Designated Port ID	128-1	
Designated Cost	20000	
Remaining Hop	20	

Interface data are as follows.

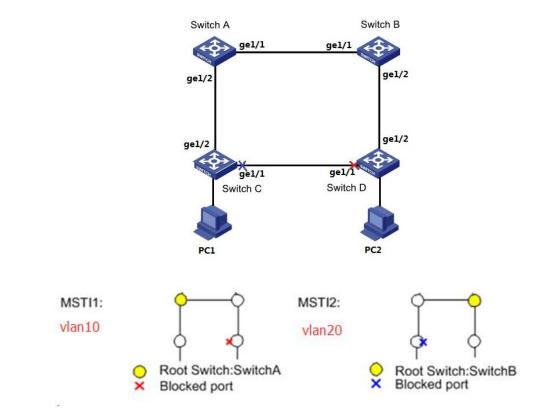
Configuration	Description
MSTI	Select the instance for configuration through the drop-down box in the upper left.
Port	Select the port to be configured by users
Path Cost	Enter the path cost value of the interface Use IEEE 802.1t Standard with the value ranging from 0 to 200,000,000
Priority	Select the port priority with smaller value representing higher priority. Interface priority affects the role of the interface on the specified MSTI. On different MSTI, users can configure the priorities for a same interface. As a result, flow of different VLANs can be forwarded along physical links to achieve VLAN load sharing. Description: MSTP will recalculate the interface role and migrate its state when its priority changes.
Port Role	3 types of root ports, namely specified port, backup port and disabled port.
Port State	Including 3 states, namely Discarding, Forwarding and Disabled
Mode	Current STP mode
Туре	The port types in the instance contain boundary and internal ports

- 2. Fill in corresponding configuration items.
- 3. "Apply" and finish.

Example of MSTP function configuration:



Switch A, B, C and D all run MSTP which introduces instances to share the load of VLAN10 and 20. MSTP can set up the VLAN mapping table to associate VLANs with spanning tree instances, and to map VLAN10 from instance 1 and VLAN20 from instance 2.



Instructions:

 Switch A, B, C and D create VLAN10 and 20 to configure the L2 forwarding function of the devices on the Ring. Click the "VLAN > VLAN > Create VLAN" in the navigation bar, fill in the corresponding configurations. "Apply" and finish as follows.

VLAN 2 VLAN 1 VLAN 3 VLAN 10 VLAN 5 VLAN 6 VLAN 7 VLAN 8 VLAN 9 VLAN 9	VLAN Tabl	e ∽ entries	Showing 1 to 3 of 3 entries	Q
		VLAN 3 VLAN 4 VLAN 5 VLAN 6 VLAN 7 VLAN 8	VLAN 10 VLAN 20	

	VLAN	Name	Туре	VLAN Interface State
0	1	default	Default	Disabled
0	10	VLAN0010	Static	Disabled
0	20	VLAN0020	Static	Disabled
		ar - 12		
E	Edit	Delete		



2. VLANs are added to the switch ports ingress loops. Click the "VLAN > VLAN > Membership" in the navigation bar, select the ring port to be configured, move VLAN10 and 20 to the right box and mark them with "Tagged". "Apply" and finish:

Edit Port Setting

	Trunk	
Membership	10 20 IUP IUP Forbidden Excluded Tagged Untagged PVID	

3. Click the "Spanning Tree > Property" in the navigation bar, and choose MSTP mode as follows:

State	Enable	
Operation Mode	 STP RSTP MSTP 	
Path Cost	 Long Short 	
BPDU Handling	FilteringFlooding	
Priority	32768	(0 - 61440, default 32768)
Hello Time	2	Sec (1 - 10, default 2)
Max Age	20	Sec (6 - 40, default 20)
Forward Delay	15	Sec (4 - 30, default 15)
Tx Hold Count	6	(1 - 10, default 6)
Region Name	1C:2A:A3:00:34:24	
Revision	0	(0 - 65535, default 0)
Max Hop	20	(1 - 40, default 20)

4. Configure the VLAN mapping between instance MSTI1 and MSTI2. Click the "Spanning Tree > MST



Instance" to fill in corresponding parameters, and "Add" them as follows:

MST Instance Table

							Q	
1	MSTI	Priority	Bridge Identifiter	Designated Root Bridge	Root Port	Root Path Cost	Remaining Hop	VLAN
)	0	32768	32768-1C:2A:A3:00:34:24	0-00:00:00:00:00:00	N/A	0	0	1-9,11-19,21-4094
)	1	32768	32768-1C:2A:A3:00:34:24	0-00:00:00:00:00:00	N/A	0	0	10
)	2	32768	32768-1C:2A:A3:00:34:24	0-00:00:00:00:00:00	N/A	0	0	20
)	3	32768	32768-1C:2A:A3:00:34:24	0-00:00:00:00:00:00	N/A	0	0	
	10	00700				-		



- Set the priority of MSTI1 to 0 and MSTI2 to 4,096 before configuring Switch A.
- Set the priority of MSTI1 to 4,096 and MSTI2 to 0 before configuring Switch B.
- The priority must be a multiple of 4,096.
- 5. Switch B serves as the root bridge of MSTI2 and the backup root bridge of MSTI1 in the domain. Please refer to 5 for instructions.
- 6. The tree-shaped network will eliminate loops.

8.5 Statistics

Instructions:

1. Click the "Spanning Tree > Statistics" in the navigation bar, entry port statistics as follows:

stat	istics	Table								
efre	sh Rate	0 🔻	sec						0	
		-	Rec	eive BF	DU	Tran	smit Bl	PDU	q	
-	Entry	Port	Config	TCN	MSTP	Config	TCN	MSTP		
	1	GE1	0	0	0	0	0	0		
	2	GE2	0	0	0	0	0	0		
	3	GE3	0	0	0	0	0	0		
0	4	GE4	0	0	0	0	0	0		
	5	GE5	0	0	0	0	0	0		
	6	GE6	0	0	0	0	0	0		
-	7	057	1.00							

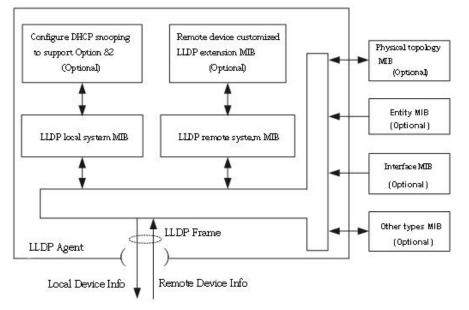
9 Discovery

LLDP (Link Layer Discovery Protocol) is defined in IEEE 802.1ab. It is a standard L2 discovery method which integrates the info such as management addresses, device and interface identifications of local network devices and transmits to the neighbor devices. After receiving the info, they will save it in form of standard MIB (Management Information Base) for NMS query and link communication judgment.



It can also integrate the info and transmit to its own remote devices. The info received by the local network device will be kept in the form of MIB. The following shows how it works.

Block diagram of LLDP principles



LLDP is realized based on:

- LLDP module updates its local system MIB, as well as the customized extension MIB, through the interaction between LLDP agent and MIBs of physical topology, entity, interface and other types.
- Encapsulate the info of local network device into LLDP frames and transmit to the remote device.
- Receive the LLDP frame sent by the remote device to update LLDP remote system MIB and customized extension MIB.
- Master the info of remote device such as connection interface and MAC address through the transmitting & receiving function of LLDP agent.
- The local system MIB stores local device info, including device and interface IDs, system name and description, interface description, network management address, etc.
- The remote system MIB stores local device info, including device and interface IDs, system name and description, interface description, network management address, etc.

Based on **LLDP**, **LLDP-MED** allows other units to expand. The info checked by network devices facilitates fault analysis and deepens the accurate understanding of network topology by management system.

9.1 LLDP

Instructions:

1. Click the "Discovery > LLDP > Property" in the navigation bar as follows.



State	Enable	
LLDP Handling	FilteringBridgingFlooding	
TLV Advertise Interval	30	Sec (5 - 32767, default 30)
Hold Multiplier	4	(2 - 10, default 4)
Reinitializing Delay	2	Sec (1 - 10, default 2)
Transmit Delay	2	Sec (1 - 8191, default 2)
P-MED		
ast Start Repeat Count	3	(1 - 10, default 3)

Interface data are as follows.

Configuration	Description
ltems	
State	Enable or disable the LLDP
LLDP Handling	LLDP messages will be processed by means of "Filtering", "Bridging" and "Flooding" when disabling the LLDP.
TLV Advertise Interval	30s by default ranging from 5 to 32,768s.
Hold Multiplier	Transmission period product with 4 by default ranges from 2 to 10. Transmission period * product should be no more than 65,535.
Reinitializing Delay	2s by default ranging from:1 to 10s.
Transmit Delay	2s by default ranging from:1 to 8,191s.
Fast Start Repeat Count	3s by default of the LLDP-MED port ranging from 1 to 10s.

Ethernet message encapsulated with LLDPDU (LLDP Data Unit) are recognized as LLDP message. Each TLV is a unit of LLDPDU carried with specified info.

2. Fill in corresponding configuration items

3. "Apply" and finish.

9.2 Port Setting

Instructions

1. Click the "Discovery > LLDP > Port Setting" in the navigation bar as follows.



Port Setting Table

Entry	Port	Mode	Selected TLV	
1	GE1	Normal	802.1 PVID	
2	GE2	Normal	802.1 PVID	
3	GE3	Normal	802.1 PVID	
4	GE4	Normal	802.1 PVID	

Interface data are as follows.

Configuration Items	Description
Port	Port list
Mode	LLDP mode include: Transmit, Receive, Normal, Disable, the default is Normal Transmit: transmit LLDP messages only; Receive: receive LLDP messages only; Normal: transmit and receive LLDP messages; Disable: neither transmit nor receive LLDP messages.
Selected TLV	Info of selected TLV and VLAN

LLDP can work in 4 patterns: Transmit: transmit LLDP messages only; Receive: receive LLDP messages only; Normal: transmit and receive LLDP messages; Disable: neither transmit nor receive LLDP messages. 2. Check corresponding port and "Edit" the port configuration. "Apply" and finish as follows.



Edit Port Setting

Port	GE1		
Mode	 Transmit Receive Normal Disable 		
	Available TLV	Selected TLV	
Optional TLV	Port Description System Name System Description System Capabilities 802.3 MAC-PHY	802.1 PVID	
	Available VLAN	Selected VLAN	
02.1 VL <mark>AN Name</mark>	VLAN 1		^
		~ <	~

Interface data are as follows.

Configuration	Description
ltems	
Port	Port list
Mode	LLDP mode include: Transmit, Receive, Normal, Disable, the default is Normal Transmit: transmit LLDP messages only; Receive: receive LLDP messages only; Normal: transmit and receive LLDP messages; Disable: neither transmit nor receive LLDP messages.
Optional TLV	Select the info of TLV and VLAN
802.1 VLAN Name	Select the VLAN name

9.3 MED Network Policy

MED is based on IEEE 802.1ab. LLDP is the neighbor discovery protocol of IEEE, which can be extended by other organizations. Information identified from network devices, such as switches and wireless access points, can help with fault analysis and allow management systems to accurately understand the network topology. Instructions

1. Click the "Discovery > LLDP > MED Network Policy" in the navigation bar as follows.



MED Network Policy Table

Show	ring <mark>All</mark> v	entries	S	Showing 0 to 0	of 0 entrie	s		Q			
-	Policy ID	Application	VLAN	VLAN Tag	Priority	DSCP					
				0 res	sults found.	ke die					
-	Add	Edit	Delete)			First	Previous	1	Next	Last

Add MED Network Policy

Application	Voice		
VLAN		Range (0 - 4095)	
VLAN Tag	 Tagged Untagged 		
Priority	0 •		
DSCP	0 •		

Interface data are as follows.

Configuration	Description
ltems	
Policy ID	Policy ID number
Application	Configure and publish network policy TLV
VLAN	VLAN number
VLAN Tag	VLAN Mode, optional Tagged or Untagged
Priority	CoS for services
DSCP	DSCP for services

9.4 MED Port Setting

Instructions

1. Click the "Discovery > LLDP > MED Port Setting" in the navigation bar as follows.



MED Port Setting Table

	Entry	Dent	Charles	Netw	ork Policy	1	
	Entry	Port	State	Active	Application	Location	Inventory
)	1	GE1	Enabled	Yes		No	No
	2	GE2	Enabled	Yes		No	No
ð	3	GE3	Enabled	Yes		No	No
	4	GE4	Enabled	Yes		No	No
	5	GE5	Enabled	Yes		No	No
	6	GE6	Enabled	Yes		No	No
ä	7	GE7	Enabled	Voc		No	No

Edit MED Port Setting

Port	GE1-GE2		
State	Enable		
	Available TLV	Selected TLV	
Optional TLV	Location Inventory	Network Polic	CY A
Network policy	Available Policy	Selected Polic	cy
			<u> </u>
Location			
Coordinate		(16 pairs of hexadecimal characters)
		(6 - 160 pairs of hexadecimal characte
Civic			

Interface data are as follows.

Configuration	Description
ltems	
Entry	Serial No. of MED port setting
Port	Port list
State	Port enable status
Network Policy	Configure and publish network policy TLV
Location	Configure and publish location TLV



Inventory

Configure and publish inventory TLV

9.5 Packet View

Instructions

1. Click the "Discovery > LLDP > Packet View" in the navigation bar as follows.

```
Packet View Table
```

				Q				
	Entry	Port	In-Use (Bytes)	Available (Bytes)	Operational Status			
9	1	GE1	38	1450	Not Overloading			
0	2	GE2	38	1450	Not Overloading			
0	3	GE3	38	1450	Not Overloading			
0	4	GE4	38	1450	Not Overloading			
0	5	GE5	38	1450	Not Overloading			
0	6	GE6	38	1450	Not Overloading			
0	7	GE7	38	1450	Not Overloading			
0	0	050	20	1450	Not Overlanding			

9.6 Local Information

Instructions for device summary:

1. Click the "Discovery > LLDP > Local Information" in the navigation bar as follows.

Device Summary

Chassis ID Subtype	MAC address	
Chassis ID	1C:2A:A3:00:34:24	
System Name	Switch	
System Description	HR-SWTG3424S	
Supported Capabilities	Bridge, Router	
Enabled Capabilities	Bridge, Router	
Port ID Subtype	Local	

Instructions for port status table:

2. Click the "Discovery > LLDP > Local Information" in the navigation bar as follows.



Port Status Table

			Q					
	Entry	Port	LLDP State	LLDP-MED State				
0	1	GE1	Normal	Enabled				
0	2	GE2	Normal	Enabled				
0	3	GE3	Normal	Enabled				
0	4	GE4	Normal	Enabled				
0	5	GE5	Normal	Enabled				
0	6	GES	Normal	Enabled				

9.7 Neighbor

Instructions for LLDP neighbor displaying

1. Click the "Discovery > LLDP > Neighbor" in the navigation bar as follows.

Local Port Chassis ID Subtype Chassis ID Port ID Subtype Port ID System Name Time to	
	Live
GE9 MAC address 00:E0:41:00:00:02 Local gi13	118

9.8 Statistics

Instructions:

1. Click the "Discovery > LLDP > Statistics" in the navigation bar as follows.



Global Statistics

Insertions	11	
Deletions	7	
Drops	0	
AgeOuts	0	

Statistics Table

		Q								
	Fata	-	Transmit Frame	R	Receive Frame		Receive TLV		Neighbor	
Ч.	Entry	Port	Total	Total	Discard	Error	Discard	Unrecognized	Timeout	
	1	GE1	0	0	0	0	0	0	0	
	2	GE2	0	0	0	0	0	0	0	
	3	GE3	278	29	0	0	0	0	0	
	4	GE4	0	0	0	0	0	0	0	
	5	GE5	0	0	0	0	0	0	0	
	6	GE6	0	0	0	0	0	0	0	

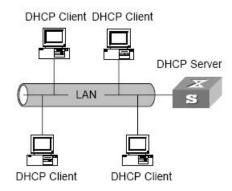
10 DHCP

DHCP Server brief introduction

With the expansion of network scale and the improvement of network complexity, network configuration is becoming more and more complex. Computer location changes (such as portable computer or wireless network) and the number of computers exceeds the IP address that can be allocated.

Dynamic Host Configuration Protocol (DHCP) is developed to meet these requirements. The DHCP protocol works in the client / server mode. The DHCP client requests the configuration information from the DHCP server dynamically, and the DHCP server returns the corresponding configuration information according to the policy.

In a typical application of DHCP, it generally includes a DHCP server and multiple clients (such as PC and laptop), as shown in Figure 1-1.





IP address assignment of DHCP

IP address allocation strategy

According to the different needs of clients, DHCP provides three IP address allocation strategies

- Manual address assignment: the administrator binds the fixed IP address for a few specific clients (such as WWW server). Send the configured fixed IP address to the client through DHCP.
- Automatic address assignment: DHCP assigns IP addresses with unlimited lease term to clients.
- Dynamic address assignment: DHCP assigns IP address with valid period to client, and client needs to re-apply for address after expiration of service life. Most clients get this dynamic address assignment.

Dynamic IP address acquisition process

The message interaction process between DHCP client and DHCP server is shown in Figure 2-1.

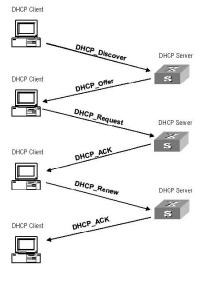


Figure 2-1. Interaction process

In order to obtain the legal dynamic IP address, the DHCP client interacts different information with the server at different stages. Generally, there are three modes as follows:

(1) DHCP client logs in to the network for the first time

When the DHCP client logs in to the network for the first time, it mainly establishes contact with the DHCP server through four stages

- The discovery phase: the stage in which the DHCP client looks for the DHCP server. The client sends the DHCP discover message in broadcast mode, and only the DHCP server will respond.
- The stage of providing IP address: that is, the stage when the DHCP server provides IP address. After receiving the DHCP discover message from the client, the DHCP server selects an unassigned IP address from the IP address pool and assigns it to the client, and sends the DHCP offer message containing the leased IP address and other settings to the client.
- The selection stage: the stage in which the DHCP client selects the IP address. If more than one DHCP



server sends a DHCP offer message to the client, the client only accepts the first received DHCP offer message, and then responds to the DHCP request message by broadcasting to each DHCP server. The information contains the content of requesting IP address from the selected DHCP server.

• The confirmation stage: the stage in which the DHCP server confirms the IP address provided. When the DHCP server receives the DHCP request message answered by the DHCP client, it will send the dhcp-ack confirmation message containing the IP address and other settings provided by the client; otherwise, it will return the dhcp-nak message, indicating that the address cannot be assigned to the client. After receiving the dhcp-ack confirmation message returned by the server, the client will send ARP (the destination address is the address to which it is assigned) in broadcast mode for address detection. If no response is received within the specified time, the client will use this address.

(2) The DHCP client logs on to the network again

When the DHCP client logs in to the network again, it mainly establishes contact with the DHCP server through the following steps.

- After the DHCP client logs in to the network correctly for the first time and then logs in to the network again, it only needs to broadcast the DHCP request message containing the IP address assigned last time, and it is not necessary to send the DHCP discover message again.
- After receiving the DHCP request message, if the address requested by the client is not assigned, the dhcp-ack confirmation message will be returned to notify the DHCP client to continue using the original IP address.
- If the IP address cannot be assigned to the DHCP client (for example, it has been assigned to other clients), the DHCP server will return a dhcp-nak message. After receiving the message, the client sends the DHCP discover message again to request a new IP address.

(3) DHCP client extends lease validity of IP address

The dynamic IP address assigned by the DHCP server to the client usually has a certain lease term. After the expiration, the server will take back the IP address. If the DHCP client wants to continue using the address, the IP lease needs to be updated.

In practice, the DHCP client sends a DHCP request message to the DHCP server by default when the IP address lease term reaches half to complete the IP lease update. If the IP address is valid, the DHCP server will respond to the dhcp-ack message to inform the DHCP client that a new lease has been obtained.

10.1 Property

DHCP global and static binding configuration Instructions:

1. Click the "DHCP > Property" in the navigation bar as follows.



State	Enable
Static Binding First	Enable

Apply

DHCP Port Setting Table

			Q
Entry	Port	State	
1	GE1	Enabled	
2	GE2	Disabled	
3	GE3	Disabled	
4	GE4	Disabled	
5	GE5	Disabled	
6	GE6	Disabled	

Instructions for port DHCP configuration:

2. Click the "DHCP > Property", and select the port and click "Edit" as follows.

Port	GE1-GE2	
State	Enable	

ANote:

• Enable DHCP server or DHCP relay mode, port needs to enable this function

10.2 IP Pool Setting

DHCP IP pool configuration

Instructions:

1. Click the "DHCP > IP Pool Setting", Click "Add" to add IP pool as follows.

nowing All	• entries	3	Sho	owing 0 to 0	of 0 entri	es	c	2
Pool	Section		Gateway	Mask	DNS Primary Server	DNS Second Server Lease time		
Pool	Section	Start Address	End Address	Galeway	WIdSK	Divis Primary Server	DNS Second Server Lease time	Lease unie
					0 results	found.		



IP Pool Table

Pool		(1 to 32 alphanumeric characters)
Gateway		
Mask		
IP Address Section	Section Start Address End Address	
DNS Primary Server	Enable	
DNS Second Server	Enable	
Lease time	1 Day	0 V Hour 00 V Minute

ANote:

• The start address and end address cannot be configured or contain a gateway address

10.3 VLAN IF Address Group Setting

Server group configuration

Instructions:

1. Click the "DHCP > VLAN IF Address Group Setting", enter the DHCP Server Group Table and click "Add" to configure the server group as follows.

			Q
Group ID	Group IP Address	Bind VLAN Interface	
		0 results found.	



DHCP Server Group Table

DHCP Se	erver Group	1	•		
Group	IP Address				
)		 	
ppiy	Close				

VLAN interface and server group binding configuration

Instructions:

1. Click the "DHCP > VLAN IF Address Group Setting", enter the VLAN Interface Address Pool Table, select the interface and server group, and then click "Apply" as follows.

Interface	MGMT VLAN	۲
DHCP Server Group	1	•

10.4 Client List

Client list information

Instructions:

1. Click the "DHCP > Client List", enter DHCP Client list as follows.

nowing All entries	Showing	g 0 to 0 of	f 0 entries	Q	
MAC Address Table	IPv4 Address	VLAN	Hostname		
1.	5	0 results	found.		
				First Previous	s 1 Next

10.5 Client Static Binding Table

Static IP address assignment configuration Instructions:

1. Click the "DHCP > Client Static Binding Table", enter Static Binding Table, and click "Add" as follows.



Static Binding Table

owing All v entries	Showing	g 0 to 0 of	f 0 entries		Q			
MAC Address Table	IPv4 Address	VLAN	User Name					
		0 results	found.		_			
Add Delete				First	Previous	1	Next	Las

• The IP configuration of static binding is required to be within the scope of IP address assignment.

11 Multicast

11.1 General

11.1.1 Property

Instructions:

1. Click the "Multicast > General > Property" in the navigation bar as follows.

Unknown Multicast Action	Flood Drop Forward to Router Port
ulticast Forward Me	thod
IPv4	DMAC-VID DIP-VID
IPv6	DMAC-VID DIP-VID

11.1.2 Group Address

According to the previous request mode of multicast, the multicast router will copy and forward data to each VLAN containing receivers when users in different VLANs request the same multicast group, which wastes a great deal of bandwidth. IGMP Snooping configures multicast VLAN by connecting the different users of switch ports to a same multicast VLAN to receive multicast data. In this way, multicast flow can only be transmitted within a multicast VLAN, thus saving bandwidth. In addition, security and bandwidth are



guaranteed because multicast VLANs are completely isolated from user VLANs.

Instructions

1. Click the "Multicast > Group Address", "Add" a new static multicast item, and "Edit" the existing ones as follows:

Gro	up Add	tress Table								
IP Ve	ersion IF	Pv4 ▼								
Show	ving All	▼ entries	Sho	wing 0 t	o 0 of 0 entries		a			
	VLAN	Group Address	Member	Туре	Life (Sec)					
				0	results found.					
	Add	Edit	Delete	F	Refresh	First	Previous	1	Next	Last

Add Group Address

VLAN		
IP Version	IPv4 🗸	
iroup Address		
Member	Available Port Selected Port	

Apply Close

Interface data are as follows.

Configuration	Description
ltems	
VLAN	VLAN ID to which the multicast group belongs. Drop down to
	select an existing VLAN.
IP Version	Whether v4 or v6 is the version of multicast IP address
Multicast Address	Enter the multicast address
Member	Add multicast member(s)

- 2. Fill in corresponding configuration items.
- 3. "Apply" and finish as follows.



Group Address Table

IP Version IP	v4 \sim						
Showing All	 ✓ entries 	Sh	owing 1	to 1 of 1 entries		Q	
VLAN	Group Address	Member	Туре	Life (Sec)			
1	224.1.1.111	GE1-GE8	Static				
Add	Edit Delete	Refrest	1		First	Previous 1	Next Last

11.1.3 Router Port

Configure and view multicast router port

Instructions:

1. Click the "Multicast > General > Router Port" in the navigation bar as follows.

Router Port Table								
IP Version IPv4 V								
Showing All entries		Showing 0 to 0 of	0 entries		a			
VLAN Member	Static Port	Forbidden Port	Life (Sec)					
		0 results	s found.					
Add Edit	Refresh			First	Previous	1	Next	Last

11.1.4 Forward All

Configure and view multicast forward port

Instructions:

1. Click the "Multicast > General > Forward All" in the navigation bar as follows.

Forward All Table					
IP Version IPv4 ▼					
Showing All 🔻 entries	Showin	ng 0 to 0 o <mark>f 0 en</mark> tries		Q	
VLAN Static Port	Forbidden Port				
		0 results found.			
Add Edit	Delete		First	Previous 1	Next Last



11.1.5 Throttling

Configure and view port multicast group restrictions

Instructions:

1. Click the "Multicast > General > Throttling" in the navigation bar as follows

/ei	rsion IF	°v4 ▼				
					0	
	Entry	Port	Max Group	Exceed Action	4	
3	1	GE1	256	Deny		
0	2	GE2	256	Deny		
1	3	GE3	256	Deny		
	4	GE4	256	Deny		
3	5	GE5	256	Deny		
	6	GES	256	Denv		

11.1.6 Filtering Profile

Configure and view port multicast filtering profile

Instructions:

1. Click the "Multicast > General > Filtering Profile" in the navigation bar as follows.

Filte	ring Profi	le Table				
IP Ver	rsion IPv4 •	•				
Show	ing <mark>All ▼</mark> e	ntries	Showing 0 to 0 of	0 entries	Q	
	Profile ID	Start Address	End Address	Action		
			0 results	found.		
	Add	Edit	Delete		First Previous	s 1 Next Last

Configure and view multicast filtering profile and port binding relationship

2. Click the "Multicast > General > Filtering Binding" in the navigation bar as follows.



Filtering Binding Table

IP Version IPv4 ▼

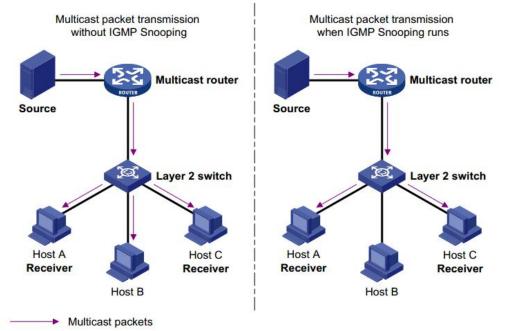
				Q
	Entry	Port	Profile ID	
	1	GE1		
	2	GE2		
	3	GE3		
	4	GE4		
	5	GE5		
1731	0	050		

11.2 IGMP Snooping

IGMP Snooping (Internet Group Management Protocol Snooping) is a constraint mechanism on L2 devices to manage and control multicast groups.

By analyzing the IGMP messages received, L2 devices establish a mapping between ports and MAC multicast addresses and forward the multicast data accordingly.

As shown below, multicast data are transmitted on L2 without IGMP snooping. When IGMP snooping runs, known multicast group data are transmitted to specified receivers while unknown multicast data are still on Layer 2.



11.2.1 Property

IGMP Snooping is on the L2 switch between the multicast routers and the user hosts, applicable to deploy



IPv4 networks. It is configured in a VLAN to snoop the IGMP/MLD messages transmitted between routers and hosts, and to establish a L2 forwarding table for multicast data, in order to manage and control the multicast data forwarding in L2 network.

Global IGMP Snooping function should be enabled since it is disabled by default.

Instructions:

1. Click the "Multicast > IGMP Snooping > Property", select the VLAN to be configured from the created VLAN info, and "Edit" the details as follows:

State	Enable	
Version	 IGMPv2 IGMPv3 	
Report Suppression	Enable	

Apply

VLAN Setting Table

Q									
	VLAN	Operational Status	Router Port Auto Learn	Query Robustness	Query Interval	Query Max Response Interval	Last Member Query Counter	Last Member Query Interval	Immediate Leave
	1	Disabled	Enabled	2	125	10	2	1	Disabled
	10	Disabled	Enabled	2	125	10	2	1	Disabled
	20	Disabled	Enabled	2	125	10	2	1	Disabled

Edit

Edit VLAN Setting

VLAN	20	
State	Enable	
Router Port Auto Learn	Enable	
Immediate leave	Enable	
Query Robustness	2	(1 - 7, default 2)
Query Interval	125	Sec (30 - 18000, default 125)
Query Max Response Interval	10	Sec (5 - 20, default 10)
Last Member Query Counter	2	(1 - 7, default 2)
Last Member Query Interval	1	Sec (1 - 25, default 1)
Operational Status		
Status	Disabled	
Query Robustness	2	
Query Interval	125 (Sec)	
Query Max Response Interval	10 (Sec)	
Last Member Query Counter	2	
Last Member Query Interval	1 (Sec)	

Apply

Close



Interface data are as follows.

Configuration Items	Description
VLAN	VLAN ID to be configured
State	Enable or disable the IGMP Snooping in this VLAN
Router Port Auto Learn	Enable or disable route port automatic learning
Immediate leave	Multicast members leave quickly
Query Robustness	The Robustness Variable allows tuning for the expected packet loss on a network
Query Interval	The interval between message queries
Query Max Response Interval	Timeout (over the max response time) of a query message
Last Member Query Counter	Max number of queries for a specified group
Last Member Query Interval	The interval between message queries for a specified group

- 2. Fill in corresponding configuration items.
- 3. "Apply" and finish.

11.2.2 Querier

Configure and view IGMP snooping Querier

Instructions:

1. Click the "Multicast > IGMP Snooping > Querier" in the navigation bar as follows.

Querier Table

VLAN	State	Operational Status	Version	Querier Address
1	Disabled	Disabled		

Interface data are as follows.

Configuration Items	Description
VLAN	Multicast VLAN
State	Enable or disable IGMP snooping querier
Operational Status	IGMP snooping querier running status
Version	Version for querier
Querier Address	Multicast address for querier



11.2.3 Statistics

Configure and view IGMP snooping statistics Instructions:

1. Click the "Multicast > IGMP Snooping > statistics" in the navigation bar as follows.

Total	0
Valid	0
InValid	0
Other	D
Leave	0
Report	0
General Query	0
Special Group Query	0
Source-specific Group Query	0
ransmit Packet	
Leave	0
Report	0
General Query	0
Special Group Query	0
special oroup query	
Source-specific Group Query	0

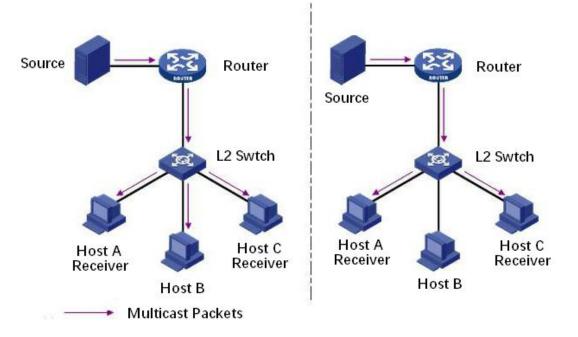
11.3 MLD Snooping

MLD snooping is the abbreviation of multicast Listener Discovery snooping. It is an IPv6 Multicast constraint mechanism running on layer 2 devices, which is used to manage and control IPv6 Multicast Groups.

The second layer device running MLD snooping establishes a mapping relationship between port and MAC multicast address by analyzing the received MLD message, and forwards IPv6 multicast data according to the mapping relationship

As shown in the figure below, when the layer 2 device does not run MLD snooping, the IPv6 multicast data packets are broadcast at layer 2; when the layer 2 device runs MLD snooping, the multicast data packets of known IPv6 Multicast groups will not be broadcast at layer 2, but will be multicast to the designated receivers at layer 2.





MLD snooping can only forward information to the receivers in need through layer 2 multicast, which can bring the following benefits:

- Reduce the broadcast packets in the layer 2 network and save the network bandwidth;
- Enhance the security of IPv6 Multicast information;
- It is convenient to charge each host separately.

11.3.1 Property

Global MLD Snooping function should be enabled since it is disabled by default. Instructions:

1. Click the "Multicast > MLD Snooping > Property", select the VLAN to be configured from the created VLAN info, and "Edit" the details as follows:

State	Enable Enable
Version	 MLDv1 MLDv2
Report Suppression	Enable

VLAN Setting Table

1	VLAN	Operational Status	Router Port Auto Learn	Query Robustness	Query Interval	Query Max Response Interval	Last Member Query Counter	Last Member Query Interval	Immediate Leave
)	1	Disabled	Enabled	2	125	10	2	1	Disabled



Edit VLAN Setting

VLAN	1	
State	Enable	
Router Port Auto Learn	Enable	
Immediate leave	Enable	
Query Robustness	2	(1 - 7, default 2)
Query Interval	125	Sec (30 - 18000, default 125)
Query Max Response Interval	10	Sec (5 - 20, default 10)
Last Member Query Counter	2	(1 - 7, default 2)
Last Member Query Interval	1	Sec (1 - 25, default 1)
perational Status		
Status	Disabled	
Query Robustness	2	
Query Interval	125 (Sec)	
Query Max Response Interval	10 (Sec)	
Last Member Query Counter	2	
Last Member Query Interval	1 (Sec)	

Interface data are as follows.

Configuration Items	Description
VLAN	VLAN ID to be configured
State	Enable or disable the IGMP Snooping in this VLAN
Router Port Auto Learn	Enable or disable route port automatic learning
Immediate leave	Multicast members leave quickly
Query Robustness	The Robustness Variable allows tuning for the expected packet loss on a network
Query Interval	The interval between message queries
Query Max Response Interval	Timeout (over the max response time) of a query message
Last Member Query Counter	Max number of queries for a specified group
Last Member Query Interval	The interval between message queries for a specified group

2. Fill in corresponding configuration items.



3. "Apply" and finish.

11.3.2 Statistics

Configure and view MLD snooping statistics

Instructions:

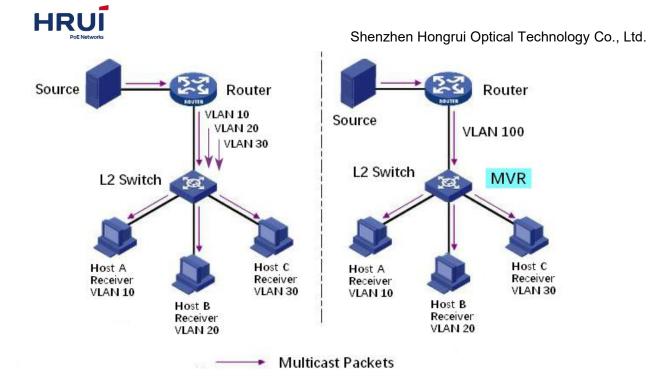
1. Click the "Multicast > MLD Snooping > statistics" in the navigation bar as follows.

Receive Packet	
Total	0
Valid	0
InValid	0
Other	0
Leave	0
Report	0
General Query	0
Special Group Query	0
Source-specific Group Query	0
Transmit Packet	
Leave	0
Report	D
	0
General Query	5
General Query Special Group Query	0

11.4 MVR

In order to solve the problem of multicast traffic broadcast based on VLAN in layer 2 network, we use IGMP snooping protocol to control the receiver, that is, only the receiver can receive the multicast traffic normally.

However, IGMP snooping can only effectively control the traffic of the same multicast VLAN, but not the cross VLAN traffic. As a result, the efficiency of multiple replication of the same multicast in different VLANs still exists. In order to solve the flooding problem of cross VLAN, we adopt the dedicated multicast VLAN of multicast source traffic, as shown in the figure below



11.4.1 Property

Global MVR function should be enabled since it is disabled by default.

Instructions:

1. Click the "Multicast > MVR > Property", enter the MVR global configuration interface as follows:

State	Enable	
VLAN	1.1	
Mode	 Compatible Dynamic 	
Group Start	0.0.0.0	
Group Count	1	(1 - 128)
Query Time	1	Sec (1 - 10)
Operational Grou	ıp	
Maximum	128	
Current	0	

Apply

Interface data are as follows.

Configuration Items	Description
State	Enable or disable MVR
VLAN	VLAN ID to be configured

HRUÍ
PoE Networks

Mode	Compatible: The CPU of MVR switch normally forwards the
	query message of router and the join message of client to
	form the multicast forwarding table of dynamic learning.
	However, the CPU will not forward the join message to the
	router port, so the upper router will not receive the following
	join message, resulting in the router data cannot be
	forwarded to the switch normally. In this mode, it is necessary
	to configure the router manually Multicast forwarding table
	forwards data to switch
	Dynamic: The only difference between the dynamic mode
	and the compatible mode is that the CPU can forward the
	join message to the router port in the dynamic mode, so the
	upper layer router can learn the multicast forwarding table
	dynamically, and there is no need to manually configure the
	multicast forwarding table of the router to forward the data
	to the switch
Group Start	The starting address of the multicast group
Group Count	Number of multicast group addresses
Query Time	Multicast group query time

- 2. Fill in corresponding configuration items.
- 3. "Apply" and finish.

11.4.2 Port Setting

Instructions:

1. Click the "Multicast > MVR > Port Setting", enter the MVR port setting interface as follows:

Port Setting Table

	Q						
	Entry	Port	Role	Immediate Leave			
	1	GE1	None	Disabled			
	2	GE2	None	Disabled			
	3	GE3	None	Disabled			
	4	GE4	None	Disabled			
	5	GE5	None	Disabled			
613	6	GE6	None	Disabled			



Edit Port Setting

Port	GE1
Role	 None Receiver Source
Immediate Leave	Enable

Interface data are as follows.

Configuration Items	Description
Port	Port list
Role	Port mode
	Receiver: Represents the port of the switch to which the
	multicast host is connected, which is used to receive the
	multicast stream
	Source: Source port refers to the source port of multicast flow
	of upper layer equipment, that is, multicast source access port
Immediate Leave	Multicast members leave quickly

11.4.3 Group Address

Instructions:

1. Click the "Multicast > MVR > Group Address", view multicast group information as follows:

Group Address Table

Showing All	▼ entries	Showing () to 0 of	0 entries	Q	
VLAN	Group Address	Member	Туре	Life (Sec)		
		01	results fo	ound.		
Add	Edit	Delete	F	First Refresh	Previous	1 Next Last



Add Group Address

Group Address		(0	.0.0.0 - 0.0.0.0)	
Member	Available Port	Selecte	d Port	
ply Clos		<	*	

Interface data are as follows.

Configuration	Description
Items	
VLAN	VLAN ID for multicast
Group Address	Enter the multicast address
Member	Add multicast member(s)

12 Routing

The switch provides three layers of VLAN interface, which is used to communicate with network layer devices. VLANIF interface is a network layer interface, which can be configured with IP address. Before creating VLANIF interface, the corresponding VLAN should be created first. With the help of VLANIF interface, switches can communicate with other network layer devices.

12.1 IPv4 Management and Interfaces

12.1.1 IPv4 Interface

Instructions:

1. Click the "Routing > IPv4 Management and Interfaces > IPv4 Interface", enter IPv4 layer 3 interface configuration as follows:



IPv4 Interface Table

				Q	
1	Interface	IP Address Type	IP Address	Mask	Status
0	VLAN 1	Static	192.168.2.1	255.255.255.0	Valid

Add IPv4 Interface

Interface	Loopback		
Address Type	 Dynamic Static 		
IP Address			
Mask	Network Mask		
Mask	O Prefix Length	(8 - 30)	

Interface data are as follows.

Configuration Items	Description
VLAN	VLAN ID to be configured
Loopback	Loopback interface
Address Type	Dynamic: The IP address of the interface is obtained by DHCP
	Static: The IP address of the interface is configured manually
IP Address	The IP address of the interface
Mask	The IP address mask of the interface

12.1.2 IPv4 Routes

Instructions:

1. Click the "Routing > IPv4 Management and Interfaces > IPv4 Routes", enter IPv4 static route interface configuration as follows:

						Q	
1	Destination IP Prefix	Prefix Length	Route Type	Next Hop Router IP Address	Metric	Administrative Distance	Outgoing Interfac
3	192.168.2.0	24	Directly Connected				MGMT VLAN*



.....

Add IPv4 Static Route

IP Address		
NA1-	Network Mask	
Mask	O Prefix Length	(0 - 32)
Next Hop Router IP Address		
Metric	1	(1 - 255, default 1)

Interface data are as follows.

Configuration Items	Description
IP Address	Destination IP address segment
Mask	Destination IP address mask
Next Hop Router IP	The next hop IP address needs to be in the same network
Address	segment as the interface gateway
Metric	Network hops

12.1.3 ARP

Instructions:

1. Click the "Routing > IPv4 Management and Interfaces > ARP", configure and view ARP table entries as follows:

ARP Entry Age Out	1200	Sec (15 - 21600, default 1200)		
Clear ARP Table Entries	 All Dynamic Static Normal Age Out 			

ARP Table

				Q
Interface	IP Address	MAC Address	Status	
VLAN 1	192.168.0.20	00:e0:4c:2e:2c:dd	Dynamic	
VLAN 1	192.168.1.15	00:e0:4c:2e:2c:dd	Dynamic	
VLAN 1	192.168.1.71	04:d4:c4:49:63:fb	Dynamic	
VLAN 1	192.168.1.80	b0:6e:bf:c6:dc:1a	Dynamic	



Add ARP

Interface	VLAN 1
	Note: Only interfaces with an valid IPv4 address are available for selection
IP Address	
MAC Address	

Interface data are as follows.

Configuration Items	Description
Interface	VLANIF interface
IP Address	IP address of the same network segment as the interface
	gateway
MAC Address	MAC address corresponding to IP address

12.2 IPv6 Management and Interfaces

12.2.1 IPv6 Interface

Instructions:

1. Click the "Routing > IPv6 Management and Interfaces > IPv6 Interface", enter IPv6 layer 3 interface configuration as follows:

IPv6 Uni	icast Routing	Enable	 	 	
Apply	Cancel)			

IPv6 Interface Table

					Q	
	DHCPv6 Client					
Interface	Stateless	Information Refresh Time	Minimum Information Refresh Time	Auto Configuration	DAD Attempts	
			0 results fou	und.		
Add	Edit	Delete				



Add IPv6 Interface

Interface	Loopback	
Auto Configuration	Enable	
DAD Attempts	1	(0 - 600, default 1)
HCPv6 Client		
Stateless	Enable	
Information Refresh Time	86400	(86400 - 4294967294, default 86400)

Interface data are as follows.

Configuration Items	Description
VLAN	VLAN ID to be configured
Loopback	Loopback interface
Auto Configuration	Auto configuration switch
DAD Attempts	Configure the number of times neighbor request messages are sent for duplicate address detection
Stateless	Stateless auto configuration
Information Refresh Time	Auto configuration refresh Time
Minimum Information Refresh Time	Minimum refresh time for auto configuration

12.2.2 IPv6 Address

Instructions:

1. Click the "Routing > IPv6 Management and Interfaces > IPv6 Address", enter the IPv6 address configuration interface as follows:



Interface VLAN 5 V

Π	IPv6 Address Type	IPv6 Address	IPv6 Prefix Length	DAD Status
Ľ	Link Local	fe80::1e2a:a3ff:fe00:24	64	Tentative
	Multicast	ff02::1		
	Multicast	ff01::1		

Add IPv6 Interface

IPv6 Address Type	 Global Link Local 	
IPv6 Address		
Prefix Length	(3 - 128)	
EUI-64	Enable	

Interface data are as follows.

Configuration Items	Description
Interface	VLANIF interface
IPv6 Address Type	Global: Global IPv6 address
	Link Local: Local IPv6 address
IPv6 Address	IPv6 address
Prefix Length	Prefix of IPv6 address
EUI-64	Enable or disable the address derived from the IEEE802
	address

12.2.3 IPv6 Routes

Instructions:

1. Click the "Routing > IPv6 Management and Interfaces > IPv6 Routes", enter IPv6 static route interface configuration as follows:

IPv6 Routing Table

					Q	
Destination IP Prefix	Prefix Length	Route Type	Next Hop Router IP Address	Metric	Administrative Distance	Outgoing Interface
			0 results found.			
Add Edit	Delete]				



Add IPv6 Static Route

IPv6 Prefix			
IPv6 Prefix Length	-	(0 - 128)	
Next Hop Router IP Address	-		
Metric	1	(1 - 255, default 1)	

Interface data are as follows.

Configuration Items	Description
IPv6 Prefix	Destination IPv6 address segment
IPv6 Prefix Length	Destination IPv6 address prefix
Next Hop Router IP	The next hop IPv6 address needs to be in the same network
Address	segment as the interface gateway
Metric	Network hops

12.2.4 Neighbors

Instructions:

1. Click the "Routing > IPv6 Management and Interfaces > Neighbors", configure and view IPv6 neighbor table entries as follows:

Clear Neighbor Table	 All Dynamic Static N/A
Apply Cancel]

IPv6 Neighbor Table

						Q	
ø	Interface	IPv6 Address	MAC Address	Status	Router		
		A	0 res	ults found	-		
	Add	Edit	Delete				



Add Neighbor

IP Address			
MAC Address			

Interface data are as follows.

Configuration Items	Description
Interface	VLANIF interface
IP Address	IPv6 address of the same network segment as the interface
	gateway
MAC Address	MAC address corresponding to IPv6 address

12.3 Rip Routes Management

The routing information protocol (RIP) is a relatively outdated but still widely used internal gateway protocol (IGP), which is mainly used in the smaller homogeneous networks. RIP is a classical distance vector routing protocol, which appears in RFC 1058, and presents an improved RIP-2 among RFC1388, and was revised in RFC 1723 and RFC 2453.

RIP uses Bellman-For algorithm currently RIP IPv4 has two versions, RIPv1 and RIPv2. RIP has the following main features:

RIP is a typical distance vector routing protocol.

RIP messages sent by the broadcast address 255.255.255.255, RIPv2 send messages by using multicast address 224.0.0.9, both using the port 520 of UDP

RIP takes the minimum hop count to the destination network as the routing metric, rather than the bandwidth and delay of the link.

RIP is designed for small networks. The number of hops is limited to 15 hops, and the 16 hop is not reachable.

RIP-1 is a kind of class routing protocol, does not supporting discontinuous subnet design.

RIP-2 support CIDR and VLSM variable subnet mask, which make it supports the discontinuous subnet mask design

RIP periodic full routing updating, make the routing table broadcast to the neighbor router, broadcast cycle default 30 seconds.

RIP protocol management distance is 120.

For small networks, in terms of occupied bandwidth, RIP is small cost and easy to configure, manage, and implement, and RIP is still in use. But RIP also has obvious shortcomings. When there is more than one network will appear loop problem. In order to solve the loop problem, IETF proposed a split-Horizon method, the routing information received at this interface will no longer go out from the interface. The scope of the division



Shenzhen Hongrui Optical Technology Co., Ltd.

solves the routing loop problem between two routers, but can't prevent the problem which is the loop mainly formed by delay factor because of large scale network. The trigger update requires the router to transmit its routing table immediately when the link changes. These speeds up the convergence of the network, but prone to broadcast flooding. In short, the solution of the loop problem needs to consume a certain amount of time and bandwidth. If the RIP protocol is adopted, the number of links in the network can't exceed 15, which makes the RIP protocol is not suitable for large networks.

RIP Working principle

RIP is a distributed type routing protocol based on distance vector, which is the standard protocol of the Internet. Its biggest advantage is simple. The RIP protocol requires that each router in the network maintain a distance record from itself to each other destination network. The RIP protocol defines "distance" as: the distance of a router directly connected network defines as 1.the distance of a router not directly connected network defines as pass each router plus 1. "Distance" is also called "hops". RIP allows one path contain up to 15 routers, so distance equal to 16 is unreachable. So RIP protocol only applies to small Internet.

RIP 2 comes from RIP and is a supplementary protocol for RIP. It is mainly used to increase the number of loaded useful information and increase its security performance. RIPv1 and RIPv2 are UDP-based protocols. Under RIP2, each host or router sends and receives packets from UDP port 520 through the routing select process. The default routing update period for RIP protocol is 30S. Instructions

1. Click on the "Routing > Rip Routes Management > Rip Routes Setting" in the navigation tree as follows.

Rip Routes Info

Rip Routes status	Enable	
Apply		

2. Network Setting table, click "Add" enter the configuration interface as follows.

Network Setting table

Network Ipv4 Address	Network Mask	
441 (4) (1) (1) (1) (1) (1)	0 results four	nd.
		First Previous 1 Next L
Add Delete		
work Setting table		
work Setting table		
Network Ipv4 Address		



Notice:

Before configuring and publishing the network, please configure the interface IP and ensure that the IP protocol and physical state of the interface are up

12.4 Ospf Routes Management

OSPF (Open Shortest Path First) is an Interior Gateway Protocol (IGP) for routing decisions within a single autonomous system (AS). It is an implementation of the link state routing protocol, under the internal gateway protocol (IGP). It is operating within the autonomous system. The shortest path is calculated using the Dixdale algorithm.

OSPF is IGP routing protocols developed by IETF's OSPF workgroup OSPF designed for IP networks support IP subnet and external routing information marking, also allows authentication of message and supports IP multicast

OSPF routing protocol is a typical link state routing protocol, which is generally used in the same routing domain. Here, routing domain refers to an autonomous system (as), which refers to a group of networks that exchange routing information through a unified routing policy or routing protocol. In this as, all OSPF routers maintain the same database describing the as structure, which stores the state information of the corresponding links in the routing domain. It is through this database that OSPF routers calculate their OSPF routing tables

As a link state routing protocol, OSPF transmits link state multicast data LSA (link state advertisement) to all routers in a certain area, which is different from distance vector routing protocol. The router running distance vector routing protocol passes part or all of the routing tables to its neighboring routers

As for the security of information exchange, OSPF stipulates that any information exchange between routers can be authenticated when necessary, so as to ensure that only trusted routers can transmit routing information. OSPF supports a variety of authentication mechanisms, and allows different authentication mechanisms to be used among different regions. OSPF optimizes the application of link state algorithm in broadcast network (such as Ethernet) in order to make full use of hardware broadcast ability to transmit link state messages. Usually, in the topology of link state algorithm, a node represents a router. If all k routers are connected to the Ethernet, when the link state is broadcast, the packets about these K routers will reach the square of K. Therefore, OSPF allows a node to represent a broadcast network in the topology diagram. All routers in each broadcast network send link status messages to report the link status of routers in the network Instructions

1. Click on the "Routing > Ospf Routes Management > Ospf Routes Setting" in the navigation tree as follows.

OSPF Routes Info

OSPF Routes status	Enable	

2. Area Network Setting, click "Add" enter the configuration interface as follows.



Area Network Setting table

Area Id	Network Ipv4 Address	Network Mask	
		0 results found.	
Add	Delete		First Previous 1 Next La
1 100			
a Network	Setting table		
a Network	Setting table		
a Network			
a Network	Setting table Area Id	A.B.C.D	
	Area Id	A.B.C.D	
Network	Area Id	A.B.C.D	
Network	Area Id	A.B.C.D	
Network	Area Id	A.B.C.D	

Notice:

Before configuring and publishing the network, please configure the interface IP and ensure that the IP protocol and physical state of the interface are up

13 Security

13.1 RADIUS

Instructions: 1. Click the "Security > RADIUS", enter RADIUS interface as follows:



Retry	3	(1 - 10, default 3)
Timeout	3	Sec (1 - 30, default 3)
Key String		

Apply

RADIUS Table

Show	ving All • entries	5	Showing 0 t	:0 0 of 0 e	entries		Q			
	Server Address	Server Port	Priority	Retry	Timeout	Usage				
			01	results fo	und.					
A	dd Edit	Delete				First	Previous	1	Next	Last

Add RADIUS Server

Address Type	 Hostname IPv4 IPv6 	
Server Address		
Server Port	1812	(0 - 65535, default 1812)
Priority		(0 - 65535)
Key String	Use Default	
Retry	Use Default	(1 - 10, default 3)
Timeout	Use Default	Sec (1 - 30, default 3)
Usage	 Login 802.1X All 	

Interface data are as follows.

Configuration Items	Description
Address Type	Depending on the type, you can choose Hostname, IPv4, IPv6
Server Address	Server's IP address
Server Port	Service's port
Priority	Service's priority
Key String	The secret key, shared between the RADIUS server and the



	switch
Retry	Retransmit is the number of times
Timeout	to wait for a reply from a RADIUS server before retransmitting the request
Usage	Usage scenarios

13.2 TACACS+

Instructions:

1. Click the "Security > TACACS+", enter TACACS+ interface as follows:

Jse Default Para	ameter
	5 Sec (1 - 30, default 5)
Key String	
Apply	
CACS+ Table	
CACS+ TADIe	
wing All 🔻 enti	tries Showing 0 to 0 of 0 entries Q
Server Addres	ss Server Port Priority Timeout
	Descently forward
	0 results found.
	First Previous 1 Next
	Edit Delete
d TACACS+ Serve	Edit Delete
Address Type Server Address	First Previous 1 Next Edit Delete
Address Type Server Address Server Port	First Previous 1 Next Edit Delete 1 Next er 1 Next 1 IPv4 1Pv6 1 1 49 (0 - 65535, default 49) 1 1
Address Type Server Address Server Port	First Previous 1 Next Edit Delete 0 0 0 er 0 1 Next 0 IPv4 0 1 1 Next 49 (0 - 65535, default 49) 0 0 65535)
Address Type Server Address Server Port Priority Key String	First Previous 1 Next Edit Delete 1 Next 1 er IPv4 1 1 1 IPv4 1 1 1 1 49 (0 - 65535, default 49) 1 1 1 Image: Use Default Image: Use Default 1 1 1
Address Type Server Address Server Port Priority	First Previous 1 Next Edit Delete 1 Next 1 er IPv4 1 1 1 IPv4 1 1 1 1 49 (0 - 65535, default 49) 1 1 1 Image: Use Default Image: Use Default 1 1 1



Interface data are as follows.

Configuration Items	Description
Address Type	Depending on the type, you can choose Hostname, IPv4, IPv6
Server Address	Server's IP address
Server Port	Service's port
Priority	Service's priority
Key String	The secret key, shared between the RADIUS server and the switch
Retry	Retransmit is the number of times
Timeout	to wait for a reply from a RADIUS server before retransmitting the request

13.3 AAA

13.3.1 Method List

Instructions:

1. Click the "Security > AAA > Method List", enter method list interface as follows:

Showing All	▼ entries	Showing 1 t	o 1 of 1 entries	Q		
Name	Sequence					
📄 default	(1) Local					
			Fin	st Previo	ous 1	Next Las



.....

Add Method List

Name		
Method 1	Empty None Local Enable RADIUS TACACS+	
Method 2	 Empty None Local Enable RADIUS TACACS+ 	
Method 3	Empty None Local Enable RADIUS TACACS+	
Method 4	 Empty None Local Enable RADIUS TACACS+ 	
Apply	Close	

Interface data are as follows.

Configuration Items	Description
Name	Method name
Method 1-4	Empty: Method is disable
	None: Do nothing and just make user to be authenticated
	Local: Use local user account database to authenticate
	Enable: Use local enable password database to authenticate
	RADIUS: Use remote Radius server to authenticate
	TACACS+: Use remote TACACS+ server to authenticate

13.3.2 Login Authentication

Instructions:

1. Click the "Security > AAA > Login Authentication", enter login authentication interface as follows:



Telnet	default 🔻	(1) Local		
SSH	default 🔻	(1) Local		
нттр	default 🔻	(1) Local		
HTTPS	default 🔻	(1) Local		

13.4 Management Access

13.4.1 Management VLAN

Instructions:

1. Click the "Security > Management Access > Management VLAN", enter management VLAN interface as follows:

Management VLAN	1 - default	
management vLAN	Note: Change Management VLAN may cause connection interrupt	ted

13.4.2 Management Service

Instructions for Telnet:

1. Click the "Security > Management Access > Management Service", enter management service interface as follows:



lanagemer	nt Service	
Telnet	Enable	
SSH	Enable	
HTTP	Enable	
HTTPS	Enable	
SNMP	Enable	
Session Tin	neout	
	r	Min (0 - 65535, default 10)
Console Telnet	10	Min (0 - 65535, default 10) Min (0 - 65535, default 10)
Console	10	
Console Telnet	10	Min (0 - 65535, default 10)

Instructions for SSH:

2. Click the "Security > Management Access > Management Service", enter management service interface as follows:

anagemen	t Service	
Telnet	📄 Enable	
SSH	Enable	
HTTP	C Enable	
HTTPS	Enable	
SNMP	Enable	
ession Tim Console	eout	Min (0 - 65535, default 10)
ession Tim Console Telnet	20200000000000000000000000000000000000	Min (0 - 65535, default 10) Min (0 - 65535, default 10)

Instructions for HTTPS:

3. Click the "Security > Management Access > Management Service", enter management service interface as follows:



anagemen	it Service	
Telnet	Enable	
SSH	Enable	
HTTP	Imable	
HTTPS	Imable Enable	
SNMP	Enable	
ssion Tin	neout	
ession Tin Console	10	Min (0 - 65535, default 10)
		Min (0 - 65535, default 10) Min (0 - 65535, default 10)
Console Teinet SSH	10	
Console Telnet	10 10	Min (0 - 65535, default 10)

Instructions for SNMP:

4. Click the "Security > Management Access > Management Service", enter management service interface as follows:

Telnet	Enable
S SH	Enable
HTTP	C Enable
HTTPS	Enable
SNMP	Enable

13.4.3 Management ACL

ACLS applied to management

Instructions:

1. Click the "Security > Management Access > Management ACL", enter management ALC interface as follows:



ACL Name			
Apply			
Management A	ACL Ta	ble	
Showing All	ntries	S	Showing 0 to 0 of 0 entries Q
ACL Name	State	Rule	
	A		0 results found.
Active	Deactive		First Previous 1 Next Last

2. Click the "Security > Management Access > Management ACE", enter management ACE interface as follows:

nagemen	TACE Ia	able			
Name Nor	entries	S	howing () to 0 of 0 entries	Q
Priority	Action	Service	Port	Address / Mask	
			0	results found.	
				1	First Previous 1 Next



Add Managemet ACE

ACL Name	а					
Priority	1	(1 - 655	35)			
Service	 All Http Https Snmp SSH Telnet 					
Action	PermitDeny	t				
	Available I	Port	Select	ed Port		
Port	GE1 GE2 GE3 GE4 GE5 GE6 GE7 GE8		<	*		
IP Version	 All IPv4 IPv6 					
IPv4				12	55.255.255.255	
IPv6				/ 1	28	(1 - 128)

Interface data are as follows.

Configuration Items	Description
ACL Name	ACL name
Priority	ACL Priority
Service	Type of service used
Action	Match action
Port	The port on which this ACL is applied
IP Version	Manage the version of the IP address
IPv4	IPv4 address
IPv6	IPv6 address



13.5 Authentication Manager

13.5.1 Property

Enable the global setting of 802.1x/MAC/WEB authentication network access control Instructions:

1. Click the "Security > Management Manager > Property", enter global interface as follows:

Authentication Type	MAC-Based
	WEB-Based
	Enable
Guest VLAN	1 *
MAC-Based User ID Format	XXXXXXXXXXXXXX

Port Mode Table

	Q									
_	Fata	Port	Authentication Type			11	Order	Mathad	C	MAN Assign Mode
-	Entry	Pon	802.1x	MAC-Based	WEB-Based	Host Mode	Host Mode Order	Method	Guest VLAN	VLAN Assign Mode
	1	GE1	Enabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
	2	GE2	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
	3	GE3	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
	4	GE4	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
	5	GE5	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
	6	GE6	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
	7	GE7	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static



Edit Port Mode

Port	GE1		
	802.1x		
Authentication Type	MAC-Based		
	WEB-Based		
Host Mode	 Multiple Authentica Multiple Hosts Single Host 	ation	
	Available Type	Select Type	
Order	MAC-Based A WEB-Based	802.1x	
	<		
	Available Method	Select Method	
Method	Local	RADIUS	
Guest VLAN	Enable		
VLAN Assign Mode	 Disable Reject Static 		

Interface data are as follows.

Configuration Items	Description
Port	Port list
Authentication Type	Port authentication type
Host Mode	Multiple Authentication: In this mode, every client needs to pass authenticate procedure individually. Multiple Hosts: In this mode, only one client need to be authenticated and other clients will get the same access accessibility. Single Host: In this mode, only one host can be authenticated. It is the same as multi-auth mode with max hosts number configure to be 1
Order	Match action
Method	Port authentication method order
Guest VLAN	Guest VLAN
VLAN Assign Mode	Port RADIUS VLAN assign mode Reject: If get VLAN authorized information, just use it.



Shenzhen Hongrui Optical Technology Co., Ltd.

host.
is no VLAN authorized information, keep original VLAN of
Static: If get VLAN authorized information, just use it. If there
the host and make it unauthorized
However, if there is no VLAN authorized information, reject

13.5.2 Port Setting

Instructions:

1. Click the "Security > Management Manager > Port Setting", enter port setting interface as follows:

Port Setting Table

	Entry	Entry Port Port Control	Dant Dant Court					Dort Control	t Port Control	Port Dort Control	David David Comford	Deputhentiantion	Max Hosts	Commo	n Timer			802.1x Pa	rameters		Web-Based Parameters
	Entry		Control Reauthentication M		Reauthentication	Inactive	Quiet	TX Period	Supplicant Timeout	Server Timeout	Max Request	Max Login									
	1	GE1	Disabled	Disabled	256	3600	60	60	30	30	30	2	3								
D	2	GE2	Disabled	Disabled	256	3600	60	60	30	30	30	2	3								
D	3	GE3	Disabled	Disabled	256	3600	60	60	30	30	30	2	3								
	4	GE4	Disabled	Disabled	256	3600	60	60	30	30	30	2	3								
8	5	GE5	Disabled	Disabled	256	3600	60	60	30	30	30	2	3								
	6	GE6	Disabled	Disabled	256	3600	60	60	30	30	30	2	3								
D	7	GE7	Disabled	Disabled	256	3600	60	60	30	30	30	2	3								
553	0	OE0	Disabled	Disabled	256	0030	60	60	20	nc	20	2	3								

Edit Port Setting

Port	GE1-GE2	
Port Control	 Disabled Force Authorized Force Unauthorized Auto 	6
Reauthentication	Enable	
Max Hosts	256	(1 - 256, default 256)
ommon Timer		
Reauthentication	3600	Sec (300 - 2147483647, default 3600)
Inactive	60	Sec (60 - 65535, default 60)
Quiet	60	Sec (0 - 65535, default 60)
2.1x Parameters		
TX Period	30	Sec (1 - 65535, default 30)
Supplicant Timeout	30	Sec (1 - 65535, default 30)
Server Timeout	30	Sec (1 - 65535, default 30)
Max Request	2	(1 - 10, default 2)
eb-Based Parameter	S	
	📄 Infinite	
Max Login	3	(3 - 10, default 3)
Apply Close		



Interface data are as follows.

Configuration Items	Description
Port	Port list
Port Control	Force Authorized: Port is force authorized and all clients have network accessibility.
	Force Unauthorized: Port is force unauthorized and all clients
	Auto: Need passing authentication procedure to get network accessibility
Reauthentication	Enable the port reauthentication
Max Hosts	The port max hosts number for multi-auth mode
Reauthentication	The port reauthentication period value with unit second if the reauthentication time is not assigned by local database or remote authentication server
Inactive	The port inactive timeout value
Quiet	the port quiet period value
TX Period	The port 802.1x EAP TX period value
Supplicant Timeout	The port supplicant timeout value
Server Timeout	The port 802.1x server timeout value
Max Request	The port 802.1x max EAP request value
Max Login	The port WEB authentication max login attempt number

13.5.3 MAC-Based Local Account

Instructions:

1. Click the "Security > Management Manager > MAC-Based Local Account", enter configuration interface as follows:

MAC Address Control VLAN Timeout (Sec) Reauthentication Inactive	
0 results found.	

13.5.4 WEB-Based Local Account

Instructions:

1. Click the "Security > Management Manager > WEB-Based Local Account", enter configuration interface as follows:



WEB-Based Local Account Table

	Username	VLAN	Timeout (S	ec)			
-	Usemaine	VLAN	Reauthentication	Inactive			
				0 results found.			

13.5.5 Sessions

Instructions:

1. Click the "Security > Management Manager > Sessions", view sessions interface as follows:

0.	ring All ▼ e	ntries		Show	ng 0 to 0	or o entrie	.5				q	
						(Operationa	I Information	i		Authorized Informat	ion
Session IE	Session ID	D Port MAC Address		Current Type	Status	VLAN	Session Time	Inactived Time	Quiet Time	VLAN	Reauthentication Period	Inactive Timeout
						0 results	found.					
										F	irst Previous 1	Next La

13.6 DoS

13.6.1 Property

Enable the Attack Resistance option to make the switch more secure.

Instructions

1. Click the "Security > DoS > Property" to the "DoS Global Configuration" interface as follows.



Land ☑ Enable UDP Blat ☑ Enable TCP Blat ☑ Enable DMAC = SMAC ☑ Enable DMAC = SMAC ☑ Enable Mull Scan Attack ☑ Enable X-Mas Scan Attack ☑ Enable TCP SYN-FIN Attack ☑ Enable TCP SYN-RST Attack ☑ Enable ICMP Fragment ☑ Enable TCP-SYN ☑ Enable Note: Source Port < 1024 ☑ Enable Note: Offset = 1 ☑ Enable Note: Offset = 1 ☑ Enable IPv4 Ping Max Size ☑ Enable IPv4 IPv6 Min Fragment ☑ Enable IQU Byte (0 - 65535, default 1240) IPv6 Enable IQU IPv6 Im Fragment I	POD	Imable
TCP Blat Enable DMAC = SMAC Enable Null Scan Attack Enable X-Mas Scan Attack Enable TCP SYN-FIN Attack Enable CMP Fragment Enable TCP-SYN Enable Note: Source Port < 1024 Enable Note: Offset = 1 Enable Note: Offset = 1 Enable Ping Max Size Enable IPv4 Enable IPv6 512 Stale IPv6 512 Stale IPv6 512 IPv6 Min Fragment Enable I240 Byte (0 - 65535, default 512) Enable I240 Byte (0 - 65535, default 1240) Enable I240	Land	C Enable
TCP Blat ✓ Enable DMAC = SMAC ✓ Enable Null Scan Attack ✓ Enable X-Mas Scan Attack ✓ Enable TCP SYN-FIN Attack ✓ Enable TCP SYN-FIN Attack ✓ Enable ICMP Fragment ✓ Enable TCP-SYN ✓ Enable Note: Source Port < 1024 ✓ Enable Note: Offset = 1 ✓ Note: Offset = 1 ✓ Ping Max Size ✓ Enable ICP Min Hdr size ✓ IPv6 Min Fragment ✓ I240 Byte (0 - 65535, default 512) ✓ Enable IPv6 Min Fragment Í240 Byte (0 - 65535, default 1240) ✓ IPv6 Min Fragment Í240 I240 Byte (0 - 31, default 20)		Inable
Null Scan Attack Enable X-Mas Scan Attack Enable TCP SYN-FIN Attack Enable TCP SYN-RST Attack Enable ICMP Fragment Enable TCP-SYN Enable TCP-SYN Enable TCP-SYN Enable TCP-SYN Enable TCP-SYN Enable Note: Source Port < 1024 Enable Note: Offset = 1 Enable Note: Offset = 1 Enable IPv4 Enable IPv6 Enable IPv6 512 Byte (0 - 65535, default 512) Y Enable IPv6 Min Fragment Enable Smurf Attack Enable 0 Enable		C Enable
Null Scan Attack Enable Enable Enable TCP SYN-FIN Attack Enable Enable TCP SYN-RST Attack Enable Mote: Source Port < 1024 Enable Note: Offset = 1 Prog Max Size Enable IPv4 Enable IPv6 [12 Byte (0 - 65535, default 512) Enable Enable Enable Byte (0 - 31, default 20) Enable En		Enable
X-Mas Scan Attack Image: Enable TCP SYN-FIN Attack Enable TCP SYN-RST Attack Image: Enable ICMP Fragment Image: Enable TCP-SYN Enable TCP-SYN Enable TCP-SYN Enable TCP-SYN Image: Enable Note: Source Port < 1024 Image: Enable Note: Offset = 1 Image: Enable Note: Offset = 1 Image: Enable Pring Max Size Image: Enable Image: Enable IPv4 Image: Enable Image: Enable IPv6 Image: Enab	Null Scan Attack	Enable
TCP SYN-RIN Attack Image: Composition of the synthetic of the	X-Mas Scan Attack	Enable
ICMP Fragment ☑ Enable TCP-SYN ☑ Enable Note: Source Port < 1024 ☑ Enable Note: Offset = 1 ☑ Enable IPv4 ☑ Enable IPv6 ☑ 512 ☑ Enable ICP Min Hdr size ☑ Enable IPv6 Min Fragment IPv6 Min Fragment ☑ Enable IPv6 Min Fragment I 240 Byte (0 - 65535, default 1240) ☑ Enable I 240 Byte (0 - 65535, default 1240) ☑ Enable I 240		✓ Enable
ICMP Fragment ☑ Enable TCP-SYN ☑ Enable Note: Source Port < 1024 ☑ Enable Note: Offset = 1 ☑ Enable IPv4 ☑ Enable IPv6 ☑ 512 ☑ Enable ICP Min Hdr size ☑ Enable IPv6 Min Fragment IPv6 Min Fragment ☑ Enable IPv6 Min Fragment I 240 Byte (0 - 65535, default 1240) ☑ Enable I 240 Byte (0 - 65535, default 1240) ☑ Enable I 240		
TCP-SYN Image: Constraint of the state of the sta		
TCP-SYN Note: Source Port < 1024 Note: Source Port < 1024 ✓ Enable Note: Offset = 1 Note: Offset = 1 Ping Max Size ✓ Enable IPv4 Y Enable IPv6 512 Byte (0 - 65535, default 512) Y Enable TCP Min Hdr size ✓ Enable 20 Byte (0 - 31, default 20) Y Enable IPv6 Min Fragment I240 Smurf Attack 0 Netmask Length (0 - 32, default 0)		
Image: CP Fragment Image: CP Fragment Note: Offset = 1 Note: Offset = 1 Image: CP Fragment Image: CP Fragment Image: CP Fragment Image: CP Fragment <t< th=""><th>TCP-SYN</th><th></th></t<>	TCP-SYN	
Note: Offset = 1 Ping Max Size Ping Max Size Enable IPv4 Enable IPv6 512 Byte (0 - 65535, default 512) Enable 20 Byte (0 - 31, default 20) Enable 1240 Byte (0 - 65535, default 1240) Enable 1240 Byte (0 - 65535, default 1240) Enable 0 Netmask Length (0 - 32, default 0)		Enable
Ping Max Size Image: Display state Image: Display state <	TCP Fragment	Note: Offset = 1
Ping Max Size Image: Display state Image: Display state <		
Image: index of 20 Image: index of 20 TCP Min Hdr size Image: index of 20 20 Byte (0 - 31, default 20) Image: index of 20 Image: index of 20 Image: index of 20		
TCP Min Hdr size 20 Byte (0 - 31, default 20) IPv6 Min Fragment 1240 Byte (0 - 65535, default 1240) Image: Smurf Attack 0	Ping Max Size	
TCP Min Hdr size 20 Byte (0 - 31, default 20) IPv6 Min Fragment I Enable 1240 Byte (0 - 65535, default 1240) Smurf Attack Image: Comparison of the state of the s		512 Byte (0 - 65535, default 512)
IPv6 Min Fragment 20 Byte (0 - 31, default 20) IPv6 Min Fragment I240 Byte (0 - 65535, default 1240) Smurf Attack Image: Contract of the second	TCP Min Hdr size	Enable
IPv6 Min Fragment		20 Byte (0 - 31, default 20)
Interference Interference<		Imable
Smurf Attack 0 Netmask Length (0 - 32, default 0)	IPV6 Min Fragment	1240 Byte (0 - 65535, default 1240)
Netmask Length (0 - 32, default 0)	Curry und Adda - It	C Enable
	Smuri Attack	0 Netmask Length (0 - 32, default 0)
America	Apply	

13.6.2 Port Setting

DoS attack resistance is enabled based on ports. Instructions

1. Click the "Security > DoS > Port Setting" as follows:

Port Setting Table

			Q
Entry	Port	State	
1	GE1	Disabled	
2	GE2	Disabled	
3	GE3	Disabled	
2	GE4	Disabled	

2. Select and "Edit" the port to enable or disable the DoS attack resistance function as follows.



Port	GE1		
State	Enable		
Apply	Close		

13.7 Dynamic ARP Inspection

13.7.1 Property

Instructions

1. Click the "Security > Dynamic ARP Inspection > Property" enter global configuration interface as follows:

	Available VI	LAN	Selected VLAN	
<mark>/L</mark> AN	VLAN 1 VLAN 5			
		-	-	

2. Select the port and "Edit" to enter the port configuration interface as follows:

						Q	
7	Entry	Port	Trust	Source MAC Address	Destination MAC Address	IP Address	Rate Limit
Ň	1	GE1	Disabled	Disabled	Disabled	Disabled	Unlimited
)	2	GE2	Disabled	Disabled	Disabled	Disabled	Unlimited
)	3	GE3	Disabled	Disabled	Disabled	Disabled	Unlimited
1	4	GE4	Disabled	Disabled	Disabled	Disabled	Unlimited
<u>ו</u>	5	GE5	Disabled	Disabled	Disabled	Disabled	Unlimited
1	6	GE6	Disabled	Disabled	Disabled	Disabled	Unlimited



Edit Port Setting

Port	GE1-GE2		
Trust	Enable		
Source MAC Address	Enable		
Destination MAC Address	Enable		
IP Address	Enable		
IF Address	Allow Z	ero (0.0.0.0)	
Rate Limit	0	pps (1 - 50, default 0), 0 is Unlimited	

13.7.2 Statistics

Instructions

1. Click the "Security > Dynamic ARP Inspection > Statistics" view DAI statistics as follows:

Statistics Table

							Q	
-	Entry	Port	Forward	Source MAC Failure	Destination MAC Failure	Source IP Validation Failure	Destination IP Validation Failure	IP-MAC Mismatch Failure
	1	GE1	0	0	0	0	0	0
	2	GE2	0	0	0	0	0	0
	3	GE3	0	0	0	0	0	0
	4	GE4	0	0	0	0	0	0
	5	GE5	0	0	0	0	0	0
	6	GE6	0	0	0	0	0	0
	7	GE7	0	0	0	0	0	0
100	0	059	0	0	0	n	0	n

13.8 DHCP Snooping

For sake of security, the network administrator may need to record the IP address of a user surfing the Internet and to confirm the correspondence between the IP address obtained from DHCP Server and the host's MAC address.

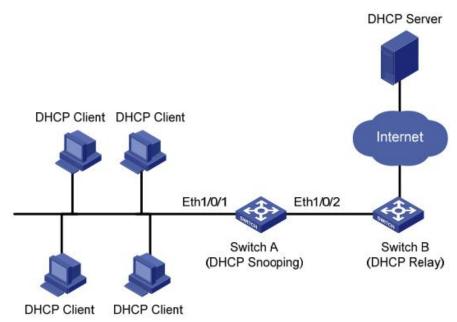
Switch can record the user's IP address through the secure DHCP relay at the network layer.

Switch can monitor DHCP messages and record the user's IP address through DHCP Snooping at the data link layer. In addition, private DHCP Server in the network may lead to wrong IP address for the user. To ensure that users obtain IP addresses through legal DHCP Server, the DHCP Snooping security mechanism divides the ports into Trust Port and Untrust Port.

Trust Port directly or indirectly connects legal DHCP Server. It forwards the DHCP messages received to ensure the correct IP address for DHCP Client. Untrust Port connects illegal DHCP Server. DHCPACK and DHCPOFFER messages received from the DHCP Server on the Untrust Port will be discarded to prevent incorrect IP addresses.



Shenzhen Hongrui Optical Technology Co., Ltd.



Typical Networking of DHCP Snooping

The following methods are used to obtain the IP address and user MAC address from DHCP Server:

- Snooping the DHCPREQUEST message
- Snooping the DHCPACK message

13.8.1 Property

Enable DHCP Snooping

Instructions:

1. Click the "Security > DHCP Snooping > Property". DHCP Snooping interface is divided into global configuration and port configuration. Select the port to be modified in the port configuration and "Edit" the details as follows:

	Available VL	AN	Selected VLAN	
/LAN	VLAN 1 VLAN 10 VLAN 100	•		
		<		
		÷	-	



Port Setting Table

				Q	
Entry	Port	Trust	Verify Chaddr	Rate Limit	
1	GE1	Disabled	Disabled	Unlimited	
2	GE2	Disabled	Disabled	Unlimited	
3	GE3	Disabled	Disabled	Unlimited	
4	GE4	Disabled	Disabled	Unlimited	
5	GE5	Disabled	Disabled	Unlimited	
6	GE6	Disabled	Disabled	Unlimited	
7	GE7	Disabled	Disabled	Unlimited	
8	GE8	Disabled	Disabled	Unlimited	

Edit Port Setting

Port	GE1-GE2	
Trust	Enable	
Verify Chaddr	Enable	
Rate Limit	0	pps (1 - 300, default 0), 0 is Unlimited

Apply Close

Interface data are as follows.

Configuration	n Items	Description
State		Enable and disable the DHCP Snooping
VLAN		Valid VLAN No. of DHCP Snooping
Port		Configure the port No. of DHCP Snooping
Trust		Whether the port is a Trust Port
Client	Address	Whether the consistency inspection for Client addresses is
Inspection		enabled
Rate Limit		Whether the port enables rate limit and configures the
		value

- 2. Fill in corresponding configuration items.
- 3. "Apply" and finish as follows.



					Q
Entry	Port	Trust	Verify Chaddr	Rate Limit	
1	GE1	Enabled	Enabled	100	
2	GE2	Enabled	Enabled	100	
3	GE3	Disabled	Disabled	Unlimited	
4	GE4	Disabled	Disabled	Unlimited	

13.8.2 Statistics

Statistics Table

Instructions

1. Click the "Security > Dynamic ARP Inspection > Statistics" view DHCP Snooping statistics as follows:

Q Untrust Port **Chaddr Check** Untrust Port Invalid Forward with Option82 Entry Port Drop Drop Drop Drop 1 GE1 0 0 0 0 0 2 GE2 0 0 0 0 0 3 GE3 0 0 0 0 0 0 4 GE4 0 0 0 0 0 0 0 0 5 0 GE5 6 GE6 0 0 0 0 0 0 0 0 0 0 7 GE7

13.8.3 Option82 Property

Private DHCP Servers in the network may lead to wrong IP addresses obtained by users. DHCP Snooping security mechanism based on PS7024 Ethernet switch divides the ports into Trust Port and Untrust Port in order to provide the IP addresses through legal DHCP Servers.

- Trust Port directly or indirectly connects legal DHCP Server. It ensures the correct IP address for DHCP Client by forwarding the DHCP messages received.
- Untrust Port connects illegal DHCP servers. DHCP ACK and DHCPOFFER messages responded by DHCP Server on untrusted ports will be discarded to prevent incorrect IP addresses.

Option 82 is the Relay Agent Information Option in DHCP messages, which records the location of DHCP Client. When the DHCP relay (or DHCP Snooping device) receives the request, message sent from DHCP Client to DHCP Server, administrators can add the Option 82 to locate the DHCP Client and control the security, cost, etc. More flexible approaches to address allocation are created by the servers supporting Option 82 in line with the IP addresses and other parameters allocation policies.



Shenzhen Hongrui Optical Technology Co., Ltd.

Up to 255 sub-options are contained in the Option 82. At least one sub-option should be defined if Option 82 is defined. The current device supports 2 sub-options: Circuit ID Sub-option and Remote ID Sub-option

Manufacturers usually fill options as needed since RFC 3046 fails to uniform the Option 82 options. As the DHCP relay device, Ethernet switch supports the extended padding formats for Option 82 sub-options and the padding defaults are as follows:

- Sub-option 1: VLAN No. and port index (port physical number minuses 1) of the port receiving the Request message sent by DHCP Client.
- Sub-option 2: bridge MAC address of DHCP relay device receiving the DHCP Client Request message.
 Sub-option 1: VLAN No. and port index (port physical number minuses 1) of the port receiving the Request

message sent by DHCP Client as follows.

0	7	15	23	31
Sub-option Type (0x01)	Length (0x06)		Circuit ID Type (0x00)	Circuit ID Length (0x04)
VL	AN ID		Port	Index

Sub-option 2: bridge MAC address of DHCP relay device receiving the DHCPREQUEST message of DHCP Client.

0	7		15	23	31
Sub-option Type (0x0)	2)	Length (0x08)	Remote ID Type (0x00) Remo	te ID Length (0x06)
		MAC	Address		

DHCP Relay Supporting Mechanism of Option 82

The processes of DHCP Client acquiring IP address from DHCP Server through DHCP relay is basically the same as that directly from DHCP Server. Steps of discovery, provision, selection, and validation are essential. The supporting mechanism of DHCP relay is introduced as follows:

(1) DHCP relay will check the Option 82 in the DHCPREQUEST message received and handle it accordingly.

- For existing Option 82 messages, DHCP relay will process according to the configuration policies (discarding, replacing with relay Option 82, or maintaining original Option 82), and then forward to DHCP Server.
- For messages without Option 82, DHCP relay will add and forward the new messages to DHCP Server.

(2) DHCP relay will peel off Option 82 from the response message received from DHCP Server, and then forward the message with DHCP configuration info to DHCP Client.

Description:

DHCP Client transmits a DHCPDISCOVERY message and a DHCPREQUEST message. DHCP relay will add Option 82 to both messages due to different processing mechanisms of DHCP Servers of manufacturers for Request message. Some devices handle Option 82 in the DHCPDISCOVERY message, while others handle it in the DHCPREQUEST message.

A switch configured with DHCP Snooping and Option 82 functions receives DHCPREQUEST messages with Option 82 sent by DHCP Clients. DHCP Snooping takes different processing mechanisms according to different configuration processing strategies and sub-option contents. Instructions:



Shenzhen Hongrui Optical Technology Co., Ltd.

1. Click the "Security > DHCP Snooping > Option82 Property". Global and port configurations are contained. Select the port to be configured and "Edit" the details as follows:

Operational Status	
Remote ID 1c:2a	a:a3:00:34:24 (Switch Mac in Byte Order)

Port Setting Table

					Q
	Entry	Port	State	Allow Untrust	
	1	GE1	Disabled	Drop	
	2	GE2	Disabled	Drop	
0	3	GE3	Disabled	Drop	
	4	GE <mark>4</mark>	Disabled	Drop	
	5	GE5	Disabled	Drop	
	6	GE6	Disabled	Drop	
	7	GE7	Disabled	Drop	

Edit Port Setting

State	Enable	
) Keep Drop Replace	

Interface data are as follows.

Configuration Items	Description					
Remote ID	Fill in the Remote ID fields in Option 82 (such as					
	user-defined XXXX)					
Port	Whether the port No. of Option 82 is enabled					
Untrust Port Access	Untrust Port processes messages with Option 82 enabled:					
	Maintaining: leave Option 82 in the message unchanged and					
	forward it					
	Discarding: discard the message					
	Replacing: replace and forward the Option 82 field in the					
	message according to the Circuit ID configuration					



Description:

Option 82 field independently configures Circuit ID or Remote ID sub-options.

It can be configured individually or simultaneously in no specific order.

DHCP Option 82 must be configured in the user bar, otherwise DHCP messages sent to DHCP Server won't carry Option 82.

When receiving the DHCP response message from DHCP Server, the message containing Option 82 will be forwarded after deleting the field, or forwarded directly if the message contains no Option 82.

2. Fill in corresponding configuration items.

3. "Apply" and finish as follows.

Remote ID	User Defined	annon an
	aaaaa	
orational C	tatua	
erational S	atus	
	aaaaa	
Remote ID		

Port Setting Table

				Q
Entry	Port	State	Allow Untrust	
1	GE1	Enabled	Replace	
2	GE2	Enabled	Replace	
3	GE3	Enabled	Replace	
4	GE4	Disabled	Drop	
5	GE5	Disabled	Drop	

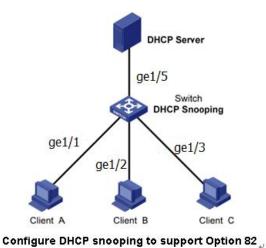
Illustration of DHCP Snooping Typical Configuration

As shown below, Switch port GE1-5 is connected to DHCP Server, and ports GE1-1, 2 and 3 are connected to DHCP Client A, B and C respectively.

- Enable the DHCP Snooping on the switch.
- Set the GE1-5 as the trust port of DHCP Snooping.
- Enable the Option 82 supporting function on the switch. For GE1-3 message flowing through the port, fill in the Option 82 according to the default configuration of Circuit ID and Remote ID.



Network Diagram



Instructions:

1. Enable the DHCP Snooping of switch. Click the "Security > DHCP Snooping > Property" in the navigation bar to enable the function as follows:

Avai	lable VLAN	Selected VL	.AN	
/LAN		VLAN 1 VLAN 10 VLAN 20	*	
	÷		-	

2. Set the GE1-5 as the trust port of DHCP Snooping, fill in corresponding configurations and "Edit" as follows:

Port Setting Table							
						Q	
	Entry	Port	Trust	Verify Chaddr	Rate Limit		
	1	GE1	Enabled	Disabled	Unlimited		
0	2	GE2	Enabled	Disabled	Unlimited		
	3	GE3	Enabled	Disabled	Unlimited		
	4	GE4	Enabled	Disabled	Unlimited		
	5	GE5	Enabled	Disabled	Unlimited		

3. Configure on the port GE3 so that user defined remote ID can be set by Option 82. Click the "Security > DHCP Snooping > Option82 Property", check and configure the port. "Apply" and finish as follows:



Remote ID	aaaaa	
erational S	aaaaa	
Remote ID		

Port Setting Table

Entry	Port	State	Allow Untrust
1	GE1	Disabled	Drop
2	GE2	Disabled	Drop
3	GE3	Enabled	Replace
4	GE4	Disabled	Drop
5	GE5	Disabled	Drop

4. Configure on the port GE3 so that the circuit ID can be set by Option 82. Click the "Security > DHCP Snooping > Option82 Circuit ID" to configure the port. "Apply" and finish as follows:

Showing All	entri	ies	Showing 1 to 1 of 1 entries		Q		
Port V	/LAN	Circuit ID					
GE3	1	ge1/3					
Add	E		lete	First	Previous 1	Next	Last

13.9 IP Source Guard

IP source guard (IPSG) is a port traffic filtering technology based on IP / Mac, which can prevent IP address spoofing attacks in LAN. IPSG can ensure that the IP address of the terminal device in the layer 2 network will not be hijacked, and it can also ensure that the unauthorized device cannot access the network or attack the network through its own specified IP address, resulting in network crash and paralysis

13.9.1 Port Setting

Instructions

1. Click the "Security > IP Source Guard > Port Setting" enter port configuration interface as follows:



Port Setting Table

	1 GE1	a second a s	Verify Source	Current Entry	Max Entry
	I OEI	Disabled	IP	0	Unlimited
	2 GE2	Disabled	IP	0	Unlimited
]	3 GE3	Disabled	IP	0	Unlimited
)	4 GE4	Disabled	IP	0	Unlimited
)	5 GE5	Disabled	IP	0	Unlimited
)	6 GE6	Disabled	IP	0	Unlimited
)	7 GE7	Disabled	IP	0	Unlimited
11 - 3	8 GF8	Disabled	IP	0	Unlimited
Port Set		E1-GE2 Enable			

Close

Interface data are as follows.

Apply

Configuration Items	Description
Port	Port list
State	Enable or disable IPSG
Verify Source	Default IP Source Guard filter source IP address. The "IP-MAC" filters not only source IP address but also source MAC address
Max Entry	Maximum number of ports allowed

13.9.2 IMPV Binding

In DHCP network, users (non-DHCP users) obtaining IP addresses statically may attack the network by imitating DHCP Server, constructing DHCP Request message, etc. Legal DHCP users may suffer from security risks when using the network normally.

Enabling the static MAC entries based on the interface generated by DHCP Snooping binding table can prevent such attacks. The device then, based on the DHCP Snooping binding table corresponding to all DHCP users, automatically executes the command to generate static MAC entries and disable the interface's learning ability of dynamic entries. Only messages that match the source MAC and static MAC entries can flow through



Shenzhen Hongrui Optical Technology Co., Ltd.

the interface. Therefore, for non-DHCP users, only the messages of static MAC entries that are manually configured by the administrators can flow through, while others will be discarded.

Instructions:

1. Click the "Security > IP Source Guard > IMPV Binding", "Add" a new binding group of IP-MAC-Port-VLAN as follows:

IP-N	IAC-P	ort-VL	AN Binding 1	Table						
Show	ing All	 ✓ entr 	ies Sh	lowing 0 to 0 of	0 entries		Q,			
	Port	VLAN	MAC Address	IP Address	Binding	Туре	Lease Tir	ne		
		h/		0 results	found.					
						First	Previous	1	Next	Last
	Add		Edit D	elete						

Add IP-MAC-Port-VLAN Binding

VLAN		(1 - 4094)
Binding	IP-MAC-Port-VLAN IP-Port-VLAN	-
MAC Address		1 255.255.255.255

Interface data are as follows.

Configuration	Description
Items	
Port	The port No. of binding group
VLAN	VLAN ID bound
Binding	Select the binding relation from IPMV and IPV
MAC Address	MAC address bound
IP Address	IP address bound

2. Fill in corresponding configuration items.

3. "Apply" and finish as follows.

IP-MAC-Port-VLAN Binding Table

Showing All V entries			ies	Showing 1 to 1 of 1 entries	Q		
	Port	VLAN	MAC Address	IP Address	Binding	Туре	Lease Time
	GE1	1	00:00:11:11:22:22	192.168.1.123 / 255.255.255.255	IP-MAC-Port-VLAN	Static	N/A
	Add		Edit Dele	te	First Pre	vious	1 Next Last



Shenzhen Hongrui Optical Technology Co., Ltd.

4. Click the "Security > IP Source Guard > Save Database" enter database interface as follows:

Type	 None Flash TFTP 	
Filename		
Address Type	 Hostname IPv4 	
Server Address		
Write Delay	300	Sec (15 - 86400, default 300)
Timeout	300	Sec (0 - 86400, default 300)

14 ACL

Expanding network scale and mounting flow strengthen the position of network security control and bandwidth allocation. Packet filtering prevents illegal users from accessing, control flow and saves network resources. ACL (Access Control List) filters packets by configuring the message matching rules and processing methods.

The switch port receiving messages analyzes the field according to the current ACL rules. Once a specific message is identified, it will be allowed or forbidden to flow through according to predetermined policies.

The packet matching rules defined by ACL can also be referenced by other functions requiring flow distinction such as the definition of QoS flow classification rules.

ACL can filter packets by setting matching rules and processing methods. ACL is a collection of permission and denial conditions applicable to packets. When the interface receives the packets, the switch compares the fields and ACL to determine the permitted and denied packets subject to specified standards. ACL classifies packets by matching conditions, which can be the source/destination MAC address, source/destination IP address, port No. and so on. ACL classifies packets by matching conditions, which can be following categories according to application purposes:

Basic IP ACL formulates rules based only on the source IP address of packets. ACL ID ranges from 100 to 999. Advanced IP ACL prepares rules according to packets' source/destination IP address, protocol types carried by IP, and Layer 3 or 4 info such as protocol characteristics. ACL ID ranges from 100 to 999.

L2 ACL: Rules are made according to the packets' source/destination MAC address, 802.1p priority, and L2 info such as protocol type. ACL ID ranges from 1 to 99.

14.1 MAC ACL

L2 ACL: Rules are made according to source/destination MAC address, VLAN priority, and L2 info such as protocol type.



Instructions:

1. Click on the "ACL > MAC ACL" in the navigation bar as follows.

ACL Name]	
Apply		

Interface data are as follows.

Configuration Items	Description
ACL Name	Name the MAC ACL Rules

2. Click on the "ACL > MAC ACE" in the navigation bar, "Add" the ACL name as follows:

CE Table										
CL Name 🛛 a 🗸										
howing All 🖂 e	entries		Showin	ng 0 to 0 of 0	entries		С	2		
	Action	Source MAC Destination MAC		on MAC	FHf		802.1p			
Sequence	Action	Address	Mask	Address	Mask	Ethertype	VLAN	Value	Mask	
				0 results	found.					
Add	Edit	Delet	e			F	irst Pr	evious	1 Next	t) [I

Interface data are as follows.

Configuration Items	Description
ACL Name	ACL rule list is prepared based on MAC ACL configuration.

3. Fill in corresponding configuration items.



Add ACE

ACL Name	а		
Sequence	1	(1 - 2147483647)	
Action	 Permit Deny Shutdown 		
	Any		
Source MAC	00:00:00:00:20:00	/ FF:FF:FF:FF:FF:00	(Address / Mask)
	Any Any		
Destination MAC	00:00:00:00:10:00	/ FF:FF:FF:FF:FF:00 ×	(Address / Mask)
	🖂 Any		
Ethertype	0x	(0x600 ~ 0xFFFF)	
	🖂 Any		
VLAN	(1 - 4094)		
	🖂 Any		
802.1p			(Value / Mask) (0 - 7

Interface data are as follows.

Configuration Items	Description
ACL Name	ACL rule list is prepared based on MAC ACL configuration.
Sequence	MAC ACL ranges from 1 to 2,147,483,647
Action	ACL actions are divided into "Permit" or "Deny", as well as "Shutdown".
Source MAC	Enter the source MAC address and mask of ACL rules with the format of H.H.H.H.H.H. Select "Any" to represent any MAC address
Destination MAC	Enter the destination MAC address and mask of ACL rules with the format of H.H.H.H.H.H. Select "Any" to represent any MAC address
EtherType	Enter the Ethernet type of ACL rules ranging from 0 x 600 to 0 x FFFF, select "Any" to represent any type.
VLAN	Enter the VLAN of ACL rules ranging from 1 to 4,094, select "Any" to represent any VLAN
802.1p	Enter the VLAN priority and mask of ACL rules ranging from 1 to 7, select "Any" to represent any VLAN priority

4. "Apply" and finish as follows.



802.1p

Value Mas

Any Any First Previous 1 Next Last

QI

Any

Ethertype VLAN

Any

ACE	able					
ACL	Name a 🗸					
Show	ring All 🖂 e	entries		Showing 1 to 1 c	of 1 entries	
	Sequence	Action	Source	ce MAC	Destina	tion MAC
	Sequence	Action	Address	Mask	Address	Mask
	1	Pormit	00.00.00.00.20.00	EE-EE-EE-EE-00	00.00.00.00.10.00	EE.EE.EE.EE.EE.00

Delete

14.2 IPv4 ACL

Edit

Add

IPv4-based ACL (Basic IP ACL) formulates rules as per the source IP address of packets only. ACL ID ranges from 100 to 999.

Advanced IP ACL Rules are made according to the packets' source/destination IP address, protocol type carried by IP, and Layer 3 or 4 info such as protocol characteristics. ACL ID ranges from 100 to 999. Instructions

1. Click on the "ACL > IPv4 ACL" in the navigation bar as follows.

ACL Name	
Apply	

Interface data are as follows.

Configuration Items	Description
ACL Name	Name the IPv4 ACL rules

2. Click on the "ACL > IPv4 ACE" in the navigation bar, "Add" the ACL Name as follows:

AC	E Table													
ACL	Name B 🗸													
Show	ving <mark>All ∨</mark> e	entries				Showing 0	to 0 of 0	entries				Q		
	Sequence	Action	Protocol	Sourc	e IP	Destinat	ion IP	Source Port	Destination Port	TCP Flags	Тур	e of Service	IC	MP
	Sequence	Action	FIOLOCOI	Address	Mask	Address	Mask	Source Fort	Destination Fort	ICF Flags	DSCP	IP Precedence	Туре	Code
								0 results found.						
	Add	Edit	De	lete							(First Previous	1 N	lext Last

Interface data are as follows.

Configuration Items	Description
ACL Name	ACL rule list is made based on IPv4 ACL configuration.

3. Fill in corresponding configuration items.



Add ACE

ACL Name	В		
Sequence	100 (1 - 21474	83647)	
Action	 Permit Deny Shutdown 		
Protocol	Any Select ICMP		
	O Define	(0 - 255)	
	🖂 Any		
Source IP	/		(Address / Mask)
	🖂 Any		
Destination IP	/		(Address / Mask)
	Any		
Type of Service	O DSCP	(0 - 63)	
	O IP Precedence	(0 - 7)	
	Any		
Source Port	O Single	(0 - 65535)	
	O Range	-	(0 - 65535
	Any		
Destination Port	O Single	(0 - 65535)	
	Range	-	(0 - 65535
	Urg: O Set O Unset Don't care		
	Ack: O Set O Unset Don't care		
TCP Flags	Psh: 🔿 Set 🔿 Unset 💿 Don't care		
ICF Flags	Rst: O Set O Unset Don't care		
	Syn: O Set O Unset Don't care		
	Fin: O Set O Unset Don't care		
	Any		
ICMP Type		<u>~</u>]	
	O Define	(0 - 255)	
ICMP Code	Any		
	O Define	(0 - 255)	

Interface data are as follows.

Configuration Items	Description
ACL Name	ACL rule list is made based on IPv4 ACL configuration.
Sequence	IPv4 ACL ranges from 1 to 2,147,483,647.
Action	ACL actions are divided into "Permit" or "Deny", as well as "Shutdown".
Protocol	It is required to select the protocol type such as ICMP, TCP and UDP. Select "Any" to represent any protocol.



Shenzhen Hongru Optical Technolog
Enter the source IP and mask of ACL rules. Select "Any" to
represent any source IP.
Enter the destination IP and mask of ACL rules. Select "Any" to
represent any destination IP.
Enter the service type of ACL rules, such as DSCP (0-63) and IP
priority (0-7). Select "Any" to represent any service type.
Enter the source port of ACL rules, such as single port No. or
range segment (0-65,535). Select "Any" to represent any source
port.
Enter the destination port of ACL rules, such as single port No. or
range segment (0-65,535). Select "Any" to represent any
destination port.
Enter the TCP flags of ACL rules, such as URG, ACK, PSH, RST,
SYN, FIN, with the actions such as "Set", "Unset" and "Don't care".
Enter the ICMP message type of ACL rules. Select "Any" to
represent any ICMP type.
Enter the ICMP Code value of ACL rules. Select "Any" to
represent any field value.

3. "Apply" and finish as follows.

N	lame 🛛 🗸													
wi	ng All 🗸 e	entries				Showing 1	to 1 of 1	entries				Q		
	Sequence A	Action	n Protocol -	Source IP Destination IP Source Port Destination Port TCP Address Mask Address Mask Source Port Destination Port TCP	Destination IP		Course Dant	Destination Dest	TOD FLORE	Type of Service		ICMP		
					TCP Flags	DSCP	IP Precedence	Туре	Cod					
	100	Permit	Any (IP)	Any	Any	Any	Any		6		Any	Anv		

14.3 IPv6 ACL

Instructions

1. Click the "ACL > IPv6 ACL" in the navigation bar as follows.

ACL Name			

Apply

Interface data are as follows.

Configuration Items	Description
ACL Name	Name the IPv6 ACL rules

2. Click the "ACL > IPv6 ACE" in the navigation bar, "Add" the ACL Name as follows:



ACE Table

NOW	ing All 🗸 e	entries				Showing 0	to 0 of 0	entries				Q		
_	0	A ation	Destand	Source IP	Source IP Destin		Destinat	ation IP Source Port	Destination Port	TOD Flame	Тур	be of Service	ICMP	
	Sequence	Action	Protocol	Address	Prefix	Address	Prefix	Source Port	Destination Port	ICP Flags	DSCP	IP Precedence	Туре	Code
								0 results found.						

Interface data are as follows.

Configuration Items	Description
ACL Name	ACL rule list is made based on IPv6 ACL configuration.

3. Fill in corresponding configuration items



Add ACE

ACL Name	b		
Sequence	100	(1 - 2147483647)	
Action	 Permit Deny Shutdown 		
Protocol	Any Select TCP		
Source IP	Define Any	(0 - 255)	(Address / Prefix (0 - 128))
Destination IP	Any	1	(Address / Prefix (0 - 128))
Type of Service	Any DSCP IP Precedence	(0 - 63)	
Source Port	Any Single	(0 - 65535)	······
	Range Any	-]	(0 - 65535)
Destination Port	Single Range	(0 - 65535)	(0 - 65535)
TCP Flags	Urg: Set Unset Ack: Set Unset Psh: Set Unset Rst: Set Unset Syn: Set Unset Fin: Set Unset	 Don't care Don't care Don't care Don't care Don't care 	
ІСМР Туре	 Any Select Destination U Define 		
ICMP Code	Any Define	(0 - 255)	

Interface data are as follows.

Configuration Items	Description
ACL Name	ACL rule list is made based on IPv6 ACL configuration.
Sequence	IPv6 ACL ranges from 1 to 2,147,483,647.
Action	ACL actions are divided into "Permit" or "Deny", as well as "Shutdown".
Protocol	It is required to select the protocol type such as ICMP, TCP and UDP. Select "Any" to represent any protocol.
Source IP	Enter the source IP and mask of ACL rules. Select "Any" to represent any source IP.



Destination IP	Enter the destination IP and mask of ACL rules. Select "Any" to
	represent any destination IP.
Type of Service	Enter the service type of ACL rules, such as DSCP (0-63) and IP
	priority (0-7). Select "Any" to represent any service type.
Source Port	Enter the source port of ACL rules, such as single port No. or
	range segment (0-65,535). Select "Any" to represent any source
	port.
Destination Port	Enter the destination port of ACL rules, such as single port No. or
	range segment (0-65,535). Select "Any" to represent any
	destination port.
TCP Flags	Enter the TCP flags of ACL rules, such as URG, ACK, PSH, RST,
	SYN, FIN, with the actions such as "Set", "Unset" and "Don't care".
ICMP Type	Enter the ICMP message type of ACL rules. Select "Any" to
	represent any ICMP type.
ICMP Code	Enter the ICMP code value of ACL rules. Select "Any" to represent
	any field value.

4. "Apply" and finish as follows.

W	ing All 🗸 e	entries				Showing 1	to 1 of 1	entries				Q		
	Comucine	Action	Protocol	Sourc	e IP	Destinat	tion IP	Source Port	Destination Port		Тур	e of Service	IC	MP
	Sequence	Action	Protocol	Address	Prefix	Address	Prefix	Source Port	Desunation Port	ICF Flags	DSCP	IP Precedence	Туре	Cod
٦Î	100	Permit	Any (IP)	Any	Any	Any	Any				Any	Any		1

14.4 ACL Binding

Once the list is created, it must be bound to each required interface.

Instructions:

1. Click the "ACL > ACL Binding" in the navigation bar as follows.

ACL Binding Table

					Q
Entry	Port	MAC ACL	IPv4 ACL	IPv6 ACL	
1	GE1	d			
2	GE2				
3	GE3				
4	GE4				

Interface data are as follows.

Configuration	Description
Items	



MAC ACL	MAC ACL name bound to the port
IPv4 ACL	IPv4 ACL name bound to the port (mutually exclusive with IPv6 ACL)
IPv6 ACL	IPv6 ACL name bound to the port (mutually exclusive with IPv4 ACL)

2. Fill in corresponding configuration items, taking the created MAC ACL a, IPv4 ACL b, IPv6 ACL c as examples.

3. "Apply" and finish as follows.

Add ACL Binding	nding	Bir	ACL	Add
-----------------	-------	-----	-----	-----

Port	GE3
1 011	Note: ACL without any rules cannot be bound
MAC ACL	a
IPv4 ACL	b v
IPv6 ACL	None ~

15 QoS

QoS (Quality of Service) assesses the ability of service providers to meet customer needs and the ability of transmitting packets over the Internet. Diversified services can be assessed based on different aspects. QoS usually refers to the evaluation of service capabilities that support core requirements such as bandwidth, delay, delay variation, and packet loss rate during delivery. Bandwidth, also known as throughput, refers to the average business flow within a certain period of time, with the unit of Kbit/s. Delay refers to the average time required for business flowing through the network. For a network device, the followings are general levels of delay requirements. There are two delay levels, that is, the high-priority business can be served as soon as possible by scheduling method of priority queue, while the low-priority business gets services after that. Delay variation refers to the time change of business flowing through the network. As modern transmission systems are very reliable, information is often lost in network congestion. Packet loss due to queue overflow is the most common situation.

All messages in a traditional IP network are treated equally. Every network device processes the messages on a FIFO basis, and makes every effort to transmit them to destinations without guaranteeing reliability, transfer delay, or other performance.

Network service quality is constantly improved as new applications keep springing up in the rapidly changing IP network. For example, VoIP, video and other delay-sensitive services have set higher standards on message transmission delay. Message transmission in a short period has been the common trend. In order to support voice, video and data services with different requirements, the network needs to identify business types and provide corresponding services.

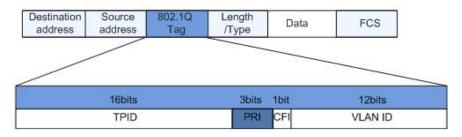


The ability to distinguish business types is the prerequisite to provide corresponding services, so the traditional best-effort service no longer meets the application needs. Therefore, QoS comes into being. It regulates the network flow to avoid and handle network congestion and reduce packet loss rate. Meanwhile, users can enjoy dedicated bandwidths while business can improve service quality, thus perfecting the network service capacity.

QoS priorities vary with message types. For instance, the VLAN message uses 802.1p, also known as the CoS (Class of Service) field, while the IP message uses DSCP. To maintain the priority, these fields need to be mapped at the gateway connected with various networks when messages flow through the network. 802.1p priority in the VLAN frame header

Typically, VLAN frames are interacted between Layer 2 devices. The PRI field (i.e. 802.1p priority), or CoS field, in the VLAN frame header identifies the quality of service requirements according to the definitions in IEEE 802.1Q.

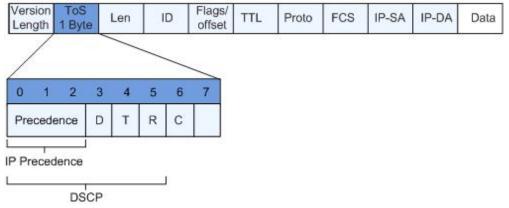
802.1p priority in the VLAN frame



The 802.1Q header contains 3-bit PRI fields. PRI field defines 8 CoS of business priority ranging from 7 to 0 from high to low.

IP Precedence/DSCP Field

According to RFC791 definition, ToS (Type of Service) domain in the IP message header is composed of 8 bits. Among them, the 3-bit long Precedence field, as located in the following, identifies the IP message priority. IP Precedence/DSCP Field



0 to 2 bits are Precedence fields representing the 8 priorities of message transmission ranging from 7 to 0 from high to low, with either Level 7 or 6 as the highest priority that is generally reserved for routing or updating network control communication. User-level applications only have access to Level 0 to 5.

ToS domain, in addition to Precedence fields, also includes D, T and R bits: D-bit represents the Delay requirement (0 for normal delay and 1 for low delay). T-bit represents the throughput (0 for normal throughput and 1 for high throughput). R-bit represents the reliability (0 for normal reliability and 1 for high reliability). ToS domain reserves the 6 and 7 bits.

RFC1349 redefines the ToS domain by adding a C-bit to represent the Monetary Cost. The IETF DiffServ group then redefines the 0 to 5 bits of ToS domain in the IPv4 message header of RFC2474 as DSCP and



renames it as DS (Differentiated Service) byte as shown in the figure above.

The first 6 bits (0-5 bits) of DS field distinguish the DSCP (DS Code Point), and the higher 2 bits (6-7 bits) are reserved. The lower 3 bits (0-2 bits) are CSCP (Class Selector Code Point), with the same CSCP value representing the DSCP of the same class. DS nodes select corresponding PHB (Per-Hop Behavior) according to DSCP values.

15.1 General

15.1.1 Property

Network congestion resulting from the competition for resource use rights among messages at the same time is usually solved by queue scheduling, thus avoiding intermittent congestions. Queue scheduling technologies include SP (Strict-Priority), WFQ (Weighted Fair Queue), WRR (Weighted Round Robin), and DRR (Deficit Round Robin, which is also expanded from RR technology).

Instructions for global and port scheduling configuration

1. Click the "QoS > General > Property" in the navigation bar as follows.

CoS DSCP CoS-DSCP IP Precedence	
	DSCP

Port Setting Table

						Q	
Entry	Entry Port CoS Trust Remarking						
Enay	Polt	COS	must	CoS	DSCP	IP Precedence	
1	GE1	0	Enabled	Disabled	Disabled	Disabled	
2	GE2	0	Enabled	Disabled	Disabled	Disabled	
3	GE3	0	Enabled	Disabled	Disabled	Disabled	
4	GE4	0	Enabled	Disabled	Disabled	Disabled	

Interface data of global configuration are as follows.

Configuration	Description
ltems	
State	Switch of global QoS function
Trust Mode	It can be divided into CoS, DSCP, CoS-DSCP and IP priority

Interface data of port configuration are as follows.



Configuration	Description
Items	
CoS	Ranging from 0 to 7
Port Trust Mode	Switch of port QoS function
CoS	Mark the CoS field
DSCP	Mark the DSCP field
IP Priority	Mark the IP Priority field

15.1.2 Queue Scheduling

1. Click the "QoS > General > Queue Scheduling". "Apply" and finish as follows. **Queue Scheduling Table**

Queue					
	Strict Priority	WRR	Weight	WRR Bandwidth (%)	
1	۲	0	1		
2	۲	\odot	2		
3	۲	0	3		
4	۲	0	4		
5	۲	0	5		
6	۲	0	9		
7	۲	0	13		
8	۲	0	15		

Interface data are as follows.

Configuration	Description
ltems	
Strict Priority	SP mode
WRR	WRR mode
Weight	Bandwidth percentage of WRR accounted for by Queue

15.1.3 CoS Mapping

1. Click the "QoS > General > CoS Mapping" in the navigation bar. "Apply" and finish as follows.



CoS to Queue Mapping

CoS	Queue	
0	1 •	
1	2 🔻	
2	3 🔻	
3	4 🔻	
4	5 🔻	
5	6 🔻	
6	7 •	
7	8 🔻	

Queue to CoS Mapping

Queue	CoS
1	0 •
2	1 •
3	2 🔻
4	3 🔻
5	4 🔻
6	5 🔻
7	6 🔻
8	7 🕶

Interface data are as follows.

Configuration	Description
ltems	
CoS	802.1p priority
Queue	Port queue

15.1.4 DSCP Mapping

1. Click the "QoS > General > DSCP Mapping". "Apply" and finish as follows.



DSCP to Queue Mapping

DSCP	Queue	DSCP	Queue	DSCP	Queue	DSCP	Queue
0 [CS0]	1 •	16 [CS2]	3 🔻	32 [CS4]	5 🔻	48 [CS6]	7 🔻
1	1 🔻	17	3 🔻	33	5 🔻	49	7 🔻
2	1 .	18 [AF21]	3 🔻	34 [AF41]	5 🔻	50	7 🔻
3	1 🔻	19	3 🔻	35	5 🔻	51	7 🔻
4	1 •	20 [AF22]	3 🔻	36 [AF42]	5 🔻	52	7 🔻
5	1 🔻	21	3 🔻	37	5 🔻	53	7 🔻
6	1 •	22 [AF23]	3 🔻	38 [AF43]	5 🔻	54	7 🔻
7	1 🔻	23	3 🔻	39	5 🔻	55	7 🔻
8 [CS1]	2 🔻	24 [CS3]	4 🔻	40 [CS5]	6 🔻	56 [CS7]	8 🔻
9	2 🔻	25	4 🔻	41	6 🔻	57	8 🔻
10 [AF11]	2 🔻	26 [AF31]	4 🔻	42	6 🔻	58	8 🔻
11	2 🔻	27	4 ▼	43	6 🔻	59	8 🔻
12 [AF12]	2 🔻	28 [AF32]	4 🔻	44	6 🔻	60	8 🔻
13	2 🔻	29	4 🔻	45	6 🔻	61	8 🔻
14 [AF13]	2 🔻	30 [AF33]	4 🔻	46 [EF]	6 🔻	62	8 🔻
15	2 -	31	4 🔻	47	6 🔻	63	8 -

Apply

Queue to DSCP Mapping

Queue	DSCP	
1	0 [CS0]	•
2	8 [CS1]	•
3	16 [CS2]	•
4	24 [CS3]	•
5	32 [CS4]	•
6	40 [CS5]	•
7	48 [CS6]	•
8	56 [CS7]	•

Interface data are as follows.

Configuration	Description
ltems	
DSCP	Value of IP DHCP domain priority
Queue	Port queue



15.1.5 IP Precedence Mapping

1. Click the "QoS > General > IP Precedence Mapping", enter this page and click "Apply", finish as follows.

IP Precedence to Queue Mapping

IP Precedence	Queue	
0	1 🔻	
1	2 🔻	
2	3 🔻	
3	4 🔻	
4	5 🔻	
5	6 🔻	
6	7 🔻	
7	8 •	

Queue to IP Precedence Mapping

Queue	IP Precedence	
1	0 •	
2	1 🔻	
3	2 🔻	
4	3 🔻	
5	4 🔻	
6	5 🔻	
7	6 🔻	
8	7 🔻	

Interface data are as follows.

Configuration	Description
ltems	
IP Precedence	Value of IP TOS domain priority
Queue	Port queue

15.2 Rate limit

15.2.1 Ingress / Egress Port

It refers to the rate restriction on transmitting and receiving data at physical interfaces.



Restrict the rate limiting at the egress before transmitting flow, thus controlling all outgoing message flow; Restrict the rate limiting at the ingress before receiving flow, thus controlling all incoming message flow;

- Instructions:
- 1. Click the "QoS > Rate Limit > Ingress / Egress Port" in the navigation bar to choose a rate-limiting port and check the current configuration as follows:

Ingress / Egress Port Table

	Entry	Dert	Dert	In	gress	E	gress
	Entry	Port	State	Rate (Kbps)	State	Rate (Kbps)	
0	1	GE1	Disabled		Disabled	1.e	
	2	GE2	Disabled		Disabled		
	3	GE3	Disabled		Disabled		
j.	4	GE4	Disabled		Disabled		
1	5	GE5	Disabled		Disabled		
D	6	GE6	Disabled		Disabled		
i	7	GE7	Disabled		Disabled		

2. Select the port (s) for rate limiting, "Edit" it at the bottom to switch the function and specify the rate. "Apply" and finish as follows:

Edit Ingress / Egress Port

	GE1-GE3		
	🕑 Enable		
Ingress	1000000	Kbps (16 - 1000000)	
-	Enable		
Egress	1000000	Kbps (16 - 1000000)	

Interface data are as follows.

Configuration	ltems	Description
Ingress	Enabled	Rate limiting switch
	Rate	Rate ranges from 16 to 1,000,000 Kbps
Egress	Enabled	Rate limiting switch
	Rate	Rate ranges from 16 to 1,000,000 Kbps



15.2.2 Egress Queue

Instructions for egress queue configuration

1. Click the "QoS > Rate Limit > Egress Queue" in the navigation bar as follows. Egress Queue Table

															C	2	
Entry Port		Qu	Queue 1 Que		Queue 2 Queue 3		Queue 4 Que		Queue 5 Qu		Queue 6 Q		Queue 7 Qu		ueue 8		
Entry	Port	State	CIR (Kbps)	State	CIR (Kbps)	State	CIR (Kbps)	State	CIR (Kbps)	State	CIR (Kbps)	State	CIR (Kbps)	State	CIR (Kbps)	State	CIR (Kbps)
1	GE1	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
2	GE2	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
3	GE3	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
4	GE4	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
5	GE5	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
6	GE6	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
7	GE7	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
8	GE8	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	

2. Select the port and "Edit" to enter the port configuration interface as follows.

Edit Egress Queue

Port	GE1-GE2	
0	Enable	
Queue 1	1000000	Kbps (16 - 1000000)
	Enable	
Queue 2	1000000	Kbps (16 - 1000000)
	Enable	
Queue 3	1000000	Kbps (16 - 1000000)
Queue 4	Enable	
	1000000	Kbps (16 - 1000000)
o	Enable	
Queue 5	1000000	Kbps (16 - 1000000)
0	Enable	
Queue 6	1000000	Kbps (16 - 1000000)
Queue 7	Enable	
Queue /	1000000	Kbps (16 - 1000000)
0	📄 Enable	
Queue 8	1000000	Kbps (16 - 1000000)



16 Diagnostics

16.1 Logging

It configures log switch, info integration, aging time and configuration level. It also uploads the switch's work logs to the TFTP Server.

Instructions:

1. Click the "Diagnostics > Logging > Property" in the navigation bar to switch logs enable/disable, select the egress terminal, configure the severity level, etc. as follows:

State	Enable				
Aggregation	🖂 Enable				
Aging Time	300	Sec (15 - 3600, default 300)			
onsole Loggi	ng				
State	🗹 Enable				
Minimum	Notice ~				
Severity	Note: Emergency, Alert, Critical, Error, Warning, Notice				
AM Logging State	🗹 Enable				
State	 ✓ Enable Notice 				
State	Notice V	t, Critical, Error, Warning, Notice			
State Minimum	Notice V	t, Critical, Error, Warning, Notice			
State Minimum Severity ash Logging State	Notice V	t, Critical, Error, Warning, Notice			
State Minimum Severity ash Logging	Notice	t, Critical, Error, Warning, Notice			

2. Click the "Diagnostics > Logging > Remote Server" in the navigation bar to add and view the server configuration as follows:

Ren	note Se	erver Table					
						Q	
	Entry	Server Address	Server Port	Facility	Minimum Severity		
		1		0 resu	ilts found.		
	Add	Edit	Delete				

3. "Add" a new remote log server and "Edit" the selected configuration. "Apply" and finish as follows:



Add Remote Server

Address Type	 Hostname IPv4 IPv6 		
Server Address			
Server Port	514	(1 - 65535, default 514)	
Facility	Local 7 🗸		
Minimum	Notice ~		
Severity	Note: Emergency	y, Alert, Critical, Error, Warning, Notice	
Severity			

16.2 Ping

Ping command checks the availability of specified IP addresses and host names and transmits statistics accordingly.

Instructions:

1. Click the "Diagnostics > Ping" in the navigation bar to enter a host name or an IP address, as well as the number of tests as follows:

Address Type	 Hostname IPv4 IPv6 	
Server Address	192.168.1.111	
Count	4	(1 - 65535)

2. Click the "Ping" to accept the packet-transmitting test from system to verify address validity, and output the result as follows:



Ping Result

cket Status	
Status	Success.
Transmit Packet	4
Receive Packet	4
Packet Lost	0 %
und Trin Time	
ound Trip Time	
Min	0 ms
Max	0 ms

16.3 Traceroute

Traceroute measures the duration from transmitting a small packet to receiving it back from the target device.

Instructions:

1. Click the "Diagnostics > Traceroute" in the navigation bar to enter a host name or IP address to define the message existence time as follows:

Address Type		
Server Address	192.168.1.122	
_	User Defined	
Time to Live	30	(2 - 255, default 30)

2. "Apply" to test and output the result as follows:

Traceroute Result

aceroute to 192.168.1.12				
192.168.1.122 (192.16	8.1.122) 0.000 ms	0.000 ms 0.000 ms	5	



16.4 Copper Test

Copper test evaluates the ingress cable state and locates the faults (about 5 m by error) according to the reflected voltage strength

Instructions:

1. Click the "Diagnostics > Copper Test" in the navigation bar to select a port for test as follows:

Port	GE1 V			
Copper Tes	st			

2. Click the "Copper Test" and output the result as follows:

Copper Test Result

Port	GE1
	Open Cable
Length	2.92 M

16.5 Fiber Module

Can be used to view optical module DDM information

Instructions:

1. Click the "Diagnostics > Fiber Module" in the navigation bar to select a port for test as follows:

Fiber Module Table

	Port	Temperature (C)	Voltage (V)	Current (mA)	Output Power (mW)	Input Power (mW)	OE Present	Loss of Signal
)	TE1	N/S	N/S	N/S	N/S	N/S	Remove	Loss
D	TE2	N/S	N/S	N/S	N/S	N/S	Remove	Loss
0	TE3	N/S	N/S	N/S	N/S	N/S	Remove	Loss
0	TE4	N/S	N/S	N/S	N/S	N/S	Remove	Loss

16.6 UDLD

UDLD (Unidirectional Link Detection): it is a Cisco private layer-2 protocol, which is used to monitor the physical configuration of Ethernet link connected by optical fiber or twisted pair. When one-way link appears (it can only transmit to one direction, for example, I can send data to you, you can also receive it, but I can't receive the data you sent to me), UDLD can detect this situation, close the corresponding interface and send it Warning message. One-way links may cause many problems, especially spanning trees, which may cause loopback. Note: UDLD needs to be supported by devices at both ends of the link to run normally.

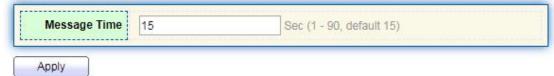


16.6.1 Property

Global and port switch configuration

Instructions:

1. Click the "Diagnostics > UDLD > Property" in the navigation bar to select a port for test as follows:



Port Setting Table

					Q	
	Entry	Port	Mode	Bidirectional State	Operational Status	Neighbor
	1	GE1	Disabled	Unknown		0
	2	GE2	Disabled	Unknown		0
0	3	GE3	Disabled	Unknown		0
0	4	GE4	Disabled	Unknown		0
0	5	GE5	Disabled	Unknown		0
n.	6	GER	Disabled	Hoknown		0

2. Select the port and click "Edit" to enter the Edit interface as follows:

Edit Port Setting

Port	GE1	
Mode	 Disabled Normal Aggressive 	

Interface data are as follows.

Configuration	Description
Items	
Port	Port id
Mode	UDLD port mode
	Disabled: Disable port function
	Normal: UDLD can detect one-way links and mark the port as
	undetermined to generate system logs
	Aggressive: UDLD can detect the unidirectional link. It will try to
	rebuild the link and send UDLD messages for 8 seconds
	continuously. If there is no UDLD echo response, the port will be
	placed in the errdisable state



16.6.2 Neighbor

UDLD periodically sends hello packets (also known as advertisement or probe probe) on each active interface.

When the Hello packet is received by the switch, the message is stored until the aging time is expired. When Hello is received again before the expiration of the aging time, the aging time is refreshed.

When a new neighbor or a neighbor requests to resynchronize the cache, a series of UDLD probe / echo (Hello) packets are sent.

Instructions:

1. Click the "Diagnostics > UDLD > Neighbor" in the navigation bar to select a port for test as follows:

Neighbor Table

Entry	Expiration Time	Current Neighbor State	Device ID	Device Name	Port ID	Message Interval	Timeout Interval
	,		0 results fou	nd.	-		

Interface data are as follows.

Configuration Items	Description
Entry	Serial No. of neighbor
Expiration Time	Remaining aging time
Current Neighbor State	Status of neighbors
Device ID	Device id of neighbors
Device Name	Device name of neighbors
Port ID	The ID of the connected interface
Message Interval	Message interval for neighbors
Timeout Interval	Timeout interval for neighbors

17 Management

17.1 User Account

Users can check and modify the current username, password and authority of the switch. Instructions:

1. Click the "Management > User Account" in the navigation bar to discover the username of "admin" and the privilege of "Admin" by default as follows:



User Account

Show	ing All ∨ e	entries	Showing 1 to 1 of 1 entries		Q			
	Username	Privilege						
	admin	Admin						
	Add	Edit	Delete	First	Previous	1	Next	Last

2. "Add" a new user account and "Edit" the selected user attribute as follows:

Add User Account

Password		
Confirm Password		
Privilege	 Admin User 	

Edit User Account

Username	admin
Password	
onfirm Password	
Privilege	Admin User
Privilege	

17.2 Firmware

System version firmware upgrade

Instructions:

1. Click the "Management > Firmware > Upgrade" in the navigation bar as follows:





17.3 Configuration

17.3.1 Upgrade

System configuration upgrade or backup

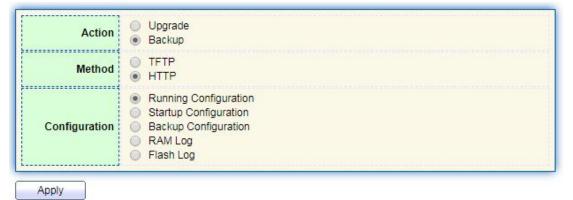
Instructions for configuration file upgrade:

1. Click the "Management > Configuration > Upgrade" click the "Upgrade" in mode of "TFTP" or "HTTP", select the corresponding files to be upgraded (servers should be illustrated in TFTP mode). "Apply" and finish as follows:

Action	 Upgrade Backup
Method	○ TFTP● HTTP
Configuration	 Running Configuration Startup Configuration Backup Configuration RAM Log Flash Log
Filename	Select File No files selected

Instructions for file backup configuration:

2. click the "Backup" in mode of "TFTP" or "HTTP", select the files or logs to be upgraded (servers should be illustrated in TFTP mode). "Apply" and finish as follows.



17.3.2 Save Configuration

Save system configuration or restore configuration to factory default Instructions:



1. Click the "Management > Configuration > Save Configuration" in the navigation bar as follows:

Source File	 Running Configuration Startup Configuration Backup Configuration 	
Destination File	 Startup Configuration Backup Configuration 	



• Click the "Factory Reset" and "Device Restart" to restore factory settings.

Save the "Running Configuration" as the "Start Configuration" (which can be saved as "Backup Configuration" or "Running Configuration") and the "Backup Configuration" (which can be saved as the "Start Configuration" or "Running Configuration").

Instructions for the second method of system preservation:

2. Click the "Save" on the upper right to save the running configuration as the start configuration as follows.

Save	Logout	Reboot	Debug
Save	e running con	Figuration	a to startun
	guration. Do y		
	ОК	Cancel	

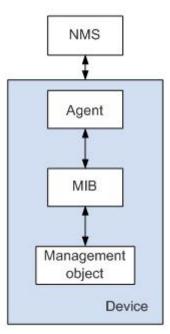
17.4 SNMP

SNMP (Simple Network Management Protocol) is widely used in TCP/IP network. It manages devices by the central computer which operates network management software (i.e. network management workstation). SNMP is:

- Simple: The polling-driving SNMP has the fundamental functionality set that is applicable to small-scale environment with fast speed and low cost. Besides, UDP-driven SNMP is compatible with most devices. Powerful: SNMP aims to ensure the management info transmission between two nodes so that administrators can retrieve, modify and troubleshoot the info easily. There are 3 common versions, namely SNMPv1, v2c and v3. Its system contains NMS (Network Management System), Agent, Management object and MIB (Management Information Base).
- NMS, as the management center, will manage all devices. Each device under management includes the resident Agent, MIB and management objects. NMS interacts with the Agent running on the management object which will operate the MIB to execute NMS orders.

SNMP management model





NMS

• As the network administrator, NMS manages/monitors network devices by SNMP on its server. It can request the Agent to inquire or modify specified parameter(s). NMS can receive the Trap actively sent by the Agent to be updated with the states of the managed devices.

Agent

• As an agent process of the managed devices, it maintains device data and responds to the NMS requests by reporting management data. Agent will fulfill relevant orders through MIB Table and transmit the results back to NMS after receiving its request. Devices will take the initiative to transmit info related to the current statues of devices to NMS through Agent once a fault or another event occurs.

Management object

• It refers to the object under management. Each device may have more than one objects, including a piece of hardware (e.g. an interface board), partial hardware and software (e.g. routing protocol), as well as other configuration item sets

MIB

 MIB is a database specifying the variables maintained by the management object (i.e. the info that can be inquired and set by the Agent). MIB defines the attributes of the management object, including the name, state, access right and data type. The following functions can be realized through MIB: Agent will master the instant device info by inquiring MIB and set the state configuration items by changing MIB.

17.4.1 View

1. Click the "Management > SNMP > View" in the navigation bar as follows.



View Table

Show	ing All	✓ entries	Showi	ing 1 to 1 of 1 entries		Q,			
	View	OID Subtree	Туре						
	all	.1	Included						
A	dd	Delete		Fir	rst	Previous	1	Next	Last

Interface data are as follows.

Configuration	Description
ltems	
View	View name
OID Subtree	View OID
Туре	View type: "Included" or "Excluded"

2. "Add" the corresponding configuration, "Apply" and finish.

Add View

View			
OID Subtree			
Туре	 Included Excluded 		
	Close		

.....

17.4.2 Group

1. Click the "Management > SNMP > Group" in the navigation bar as follows.

Group Table

Crown	Manajara	Manajara	Coourity Lough		View					
Group	Version	Security Level	Read	Write	Notify					
		0	results f	ound.						
					First	Previous	1	Next	Last	



Interface data are as follows.

Configuration	Description
Items	
Group	Group name
Version	V1, V2, V3
Security Level	Security level
View	Views are divided into view reading, writing and notification.

2. Click the "Add" to fill in corresponding configuration. "Apply" and finish.

Add Group Group SNMPv1 SNMPv2 Version SNMPv3 No Security Security Level Authentication O Authentication and Privacy Read all 👻 Write View all 👻 Notify all 🚽 Close Apply

17.4.3 Community

1. Click the "Management > SNMP > Community" in the navigation bar as follows.

Community Table Showing All v entries Showing 1 to 1 of 1 entries Q Community Group View Access public all Read-Only First Previous Next Last 1 The access right of a community is defined by a group under advanced mode. Configure SNMP Group to associate a group with a community. Add Edit Delete

Interface data are as follows.

Configuration	Description
ltems	



Community	Community configuration
Group	Group name
View	View name
Access:	Authority: read only or read-write

2. "Add" the corresponding configuration. "Apply" and finish.

Add Community

Туре	 Basic Advanced
View	all 💌
Access	
Group	

17.4.4 User

1. Click the "Management > SNMP > User" in the navigation bar as follows.

User Table

Show	ing All	✓ entrie	es	Showing 0 to 0 of 0 entrie	s		Q T			
	User	Group	Security Level	Authentication Method	Privacy Meth	od				
				0 results found						
					(First	Previous	1	Next	Last
Confi	gure SN	MP Group	to associate an S	NMPv3 group with an SNM	Pv3 user.					
	Add) <u> </u>	Edit Del	lete						

Interface data are as follows.

Configuration Items	Description		
User	Username		
Group	Group name		
Security Level	Security level		
Authentication Method	Authentication mode		
Privacy Method	Encryption mode		

2. "Add" the corresponding configuration. "Apply" and finish.



Add User

Group	d 🗸
Security Level	 No Security Authentication Authentication and Privacy
thentication	
Method	 None MD5 SHA
Password	
vacy	
Method	 None DES
Password	

17.4.5 Engine ID

1. Click the "Management > SNMP > Engine ID" in the navigation bar as follows.

Local Engine	ID								
	User Defined								
Engine ID	80006a92031c2aa3003424 (10 - 64 Hexadecimal Characters)								
Apply									
	gine ID Table								
Showing All •	entries Showing 0 to 0 of 0 entries Q								
Server A	ddress Engine ID								
	0 results found.								
	First Previous 1 Next Last								
Add	Edit Delete								

2. Click the "User Automation" to fill in corresponding ID value. "Apply" and finish.



17.4.6 Trap Event

1. Click the "Management > SNMP > Trap Event" in the navigation bar as follows.

Authentication Failure	Enable
Link Up / Down	
10 10 10 10 10 10 10 10 10 10 10 10 10 1	🖂 Enable
Warm Start	Enable

Apply

Interface data are as follows.

Configuration	Description
Items	
Authentication	Authentication error
Failure	
Link Up / Down	Port link up/down
Cold start	Cold start
Warm start	Warm start

2. "Apply" and finish.

17.4.7 Notification

1. Click the "Management > SNMP > Notification" in the navigation bar as follows.

Notification Table

Showing All ~ entries		Showing	9 0 to 0 of	0 entries		Q	
Server Address	Server Port	Timeout	Retry	Version	Туре	Community / User	Security Level
			0 resu	Its found.			
For SNMPv1,2 Notification For SNMPv3 Notification, Add Edi	SNMP User mu			fined.		First Previous	i Next Last



Add Notification

Address Type	 Hostname IPv4 IPv6 						
Server Address							
Version	 SNMPv1 SNMPv2 SNMPv3 						
Туре	 Trap Inform 						
Community / User	No Security						
Security Level							
Server Port	Use Default	(1 - 65535, default 162)					
Timeout	Use Default	Sec (1 - 300, default 15)					
Retry	Use Default	(1 - 255, default 3)					

Interface data are as follows.

.....

Configuration	Description
ltems	
Address Type	Address type: "Host Name", "IPv4" or "IPv6"
Server Address	Server address info
Version	SNMP versions: v1, v2 and v3
Туре	Notification type: "Trap" or "Inform"
Community / User	Community or username
Security Level	Security level
Server port	162 by default ranging from 1 to 65,535
Timeout	Timeout period: 15s by default ranging from 1 to 300s.
Retry	The retry interval ranges from 1 to 255s with 3s by default.

2. "Add" the corresponding configuration. "Apply" and finish.

17.5 RMON

RMON (Remote Monitoring) is a MIB defined by the IETF (Internet Engineering Task Force) and significantly emphasizes the MIB II standard. It mainly monitors data flow in a network segment or even the whole network, which is one of the widely used network management standards. RMON includes NMS (Network Management Station) and Agent running on various Network devices. RMON Agent running on network monitors or



detectors will track and count flow info (e.g. the total number of messages on a network segment during a certain period of time, or that of correct messages sent to a host) on the network segment connected to the port. Based on SNMP architecture, RMON is compatible with the existing SNMP framework. SNMP monitors remote network devices in a more efficient and active manner to supervise subnet operation. RMON can reduce communication flow between NMS and SNMP Agent to manage the large-scale interconnection network conveniently and effectively. Multiple monitors can collect data by 2 means: The exclusive RMON probe is used to collect data, and the NMS directly manages info and controls network resources. All RMON MIB info can be obtained. RMON Agent with direct access to network devices (router, switch, HUB, etc.) will become the network facility with RMON probe function. RMON NMS exchanges data with SNMP Agent with SNMP basic command to collect network management info. However, limited by device resources, it generally fails to obtain all data of RMON MIB. Most devices collect data from only four groups: alarm, event, history and statistics groups. Area-type switch realizes RMON in the second way. RMON Agent directly accessing switches will become the network facility with RMON probe function. By running the SNMP Agent supported by switches, NMS can obtain overall flow, error statistics, performance statistics and other info on the network segments connected to ports, in order to manage the network.

17.5.1 Statistics

The statistics group info reflects the statistics of each monitoring interface on the switch, namely the info accumulated from the beginning of group creation. Statistics include the number of network conflicts, CRC error messages, too-small (too-large) data messages, broadcast/multicast messages, bytes and messages received, etc. With the RMON statistics and management functions, port usage and errors occurred can be monitored and counted respectively.

Instructions

1. Click the "Management > RMON > Statistics" in the navigation bar as follows, which reveals the port-related message statistics.

Stati	istics	Table																	
Refre	sh Rate	0 💌	sec															c	
	Entry	Port	Bytes Received	Drop Events	Packets Received	Broadcast Packets	Multicast Packets	CRC & Align Errors	Undersize Packets	Oversize Packets		Jabbers	Collisions	Frames of 64 Bytes	Frames of 65 to 127 Bytes	Frames of 128 to 255 Bytes	Frames of 256 to 511 Bytes	Frames of 512 to 1023 Bytes	Frames Greater than 1024 Bytes
1	1	GE1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	2	GE2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	3	GE3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	4	GE4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
٥	5	GE5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
177	6	GE6	0	0	0	0	0	0	0	0	0	0	0	0		0	0	0	0

2. "Clear" and "Refresh" the statistics of the selected port. "View" such statistics as follows.



View Port Statistics

Port	GE8
Refresh Rate	 None 5 sec 10 sec 30 sec
Received Bytes (Octets)	0
Drop Events	0
Received Packets	0
Broadcast Packets Received	0
Multicast Packets Received	0
CRC & Align Errors	0
Undersize Packets	0
Oversize Packets	0
Fragments	0
Jabbers	0
Collisions	0
Frames of 64 Bytes	0
Frames of 65 to 127 Bytes	0
Frames of 128 to 255 Bytes	0
Frames of 256 to 511 Bytes	0
Frames Greater than 1024 Bytes	0
Clear Refresh Close	
Clear Reifesh Close	

3. Select the specified refresh frequency to operate automatically.

17.5.2 History

Once configuring the RMON history group, the switches will periodically collect and temporarily store the network statistics for processing ease, providing historical data on network segment flow, error packets, broadcast packets, bandwidth utilization, and other statistics. Historical data management can be used to set up devices in terms of historical data collection including periodical collection and maintenance of the data of specified ports.

Instructions

1. Click the "Management > RMON > History" in the navigation bar as follows.

History Table

Showing All	 ✓ ent 	ries				Showing 0 to 0 of 0 en
_				Sam	ple	
Entry	Port	Interval	Owner	Maximum	Current	
Add		Edit	Delet		ce must be enabled.	
Configura	tion	De	escriptio	on		
ltems						



Entry	Serial No. of event groups
Port	Ports to be counted
Interval	Sampling interval ranging from 1 to 3,600 (unit: s), with 1,800s by default.
Owner	Owner
Maximum	The max number of samples ranges from 0 to 50, with 50 by default.
Current	Current number of samples

2. "Add" corresponding configuration items to configure history group.

Entry	1	
Port	GE1 💌	
Max Sample	50	(1 - 50, default 50)
Interval	1800	(1 - 3600, default 1800)
Owner		

3. "Apply" and finish as follows.

History Table

Entry	Bert	Interval	Owner	Sam	ple
Entry	Port	interval	Owner	Maximum	Current
1	GE1	1800		50	50

17.5.3 Event

Defining event No. and process way, event group is mainly for the events triggered by alarm group configuration items and extended alarm group configuration items. There are several solutions to them: recording in a log table; transmitting a Trap messages to NMS; recording a log and transmitting a Trap message; Don't care.

Instructions

1. Click the "Management > RMON > Event" in the navigation bar as follows.



Event Table

Entry	O and a second second second	10								
	Community	Description	Notification	Time	Owner					
			0 results	s found.						
						First	Previous	1	Next	Las
	ice is currently		NMP service m							

Interface data are as follows.

Configuration	Description
Items	
Entry	Serial No. of event groups
Community	Community name
Description	Description
Notification	Notification
Timer	Time
Owner	Owner

2. "Add" corresponding configuration items to configure the event group.

Add Event

Entry	1	
Notification	 None Event Log Trap Event Log and Trap 	
Community	Default Community	
Description	Default Description	
Owner		

3. "Add" and finish as follows.



Event Table

ing All	 ✓ entries 	Showing 1 to 1 o	of 1 entries		Q	
Entry	Community	Description	Notification	Time	Owner	
1	Default Description	Default Description	Event Log and Trap			
	rvice is currently disab nfiguration to be effect	led. ive, the SNMP service	must be enabled.	First	Previous	1 Next L
Add	Edit	Delete View	N			

17.5.4 Alarm

RMON alarm management monitors specific alarm variables, such as port statistics. An alarm event occurs when the value of monitored data exceeds the defined threshold in the corresponding direction, which will be treated according to the prescribed treatment mode. Event definition is realized in event group. After the user defines the alarm entry, the system will process as follows: The alarm-variable defined by sampling-time should be sampled and the value should be compared with the threshold. For higher threshold, the corresponding event will be triggered.

1. Click the "Management > RMON > Alarm" in the navigation bar as follows.

wc	ing All	 ✓ entr 	ries		Show	ing 0 to 0 o	f 0 entries			Q			
1	Enter	Dent	Cou	inter	Conselling	Convellant Internet	Internet			Rising		Falling	
	Entry	Port	Name	Value	Sampling	Interval	Owner	Trigger	Threshold	Event	Threshold Event		
						0 res	sults found		Fir	et Brox	vious 1 N	lext La	
				disabled.									
R	MON cor	nfigurati	on to be	effective,	the SNMP se	ervice must	be enable	d.					

Interface data are as follows.

Configuration Items	Description
Entry	Serial No. of alarm groups
Port	Enter the ports to be counted
Counter	Sample parameters of alarms
Interval	Sampling interval ranges from 1 to 2,147,483,647 with the unit of second. 100s by default.
Sampling	Sample types: Absolute and Delete
Owner	Owner
Threshold (Rising)	The threshold of rising edge ranges from 0 to 2,147,483,647.
Event (Rising)	Event group index. Corresponding event will be activated when



	alarm is triggered.
Threshold (Falling)	The threshold of falling edge ranges from 0 to 21,474,836,475.
Event (Falling)	Event group index. Corresponding event will be activated when alarm is triggered.

2. "Add" corresponding configuration items to configure the alarm group.

Add Alarm

	1	
Port	GE1 🗸	
Counter	Drop Events	~
Sampling	AbsoluteDelta	
Interval	100	Sec (1 - 2147483647, default 100)
Owner		
Trigger	 Rising Falling Rising and Falling 	
eina		
sing Threshold	100	(0 - 2147483647, default 100)
	100 1 - Default Description	Terra and a second second from the second from the second s
Threshold		Terra and a second second from the second from the second s
Threshold Event		Terra and a second second from the second from the second s

3. "Apply" and finish as follows.

how	ing All	∨ enti	ries		- 3	Showing 1	to 1 of 1 e	ntries		Q			
	Enter		Count	er	Compliant	Interval	0	ner Trigger		Rising		Falling	
	Entry	Port	Name	Value	Sampling		Owner		Threshold	Event	Threshold	Event	
	1	GE1	DropEvents	0	Absolute	100		Rising	100	Default Description	20	Default Description	
r R		nfigurati	currently disab on to be effect		NMP service	must be er	abled.				First Previ	ous 1 Next La	