

AN-SM28P24

24-Gigabit PoE Port + 4-Gigabit Combo Port

Web Manual

Ver. 1.0

Content

AN-SM28P24	1
24-Gigabit PoE Port + 4-Gigabit Combo Port.....	1
Web Manual.....	1
Ver. 1.0.....	1
0 Foreword.....	6
0.1 Target Audience.....	6
0.2 Manual Convention.....	6
1 Management Software Specification.....	7
2 Web Page Login.....	9
2.1 Log in the Network Management Client.....	9
2.2 Constitution of Client Interface.....	10
2.3 Navigation Tree on Web Interface.....	11
3 System Configuration.....	18
3.1 System Info.....	18
3.2 Network Configuration.....	18
3.3 User Configuration.....	19
3.4 Log Configuration.....	20
3.5 Telnet Configuration.....	22
3.6 HTTPS Configuration.....	22
3.7 Diagnostics Test.....	23
4 Port Configuration.....	25
4.1 Physical Port.....	25
4.2 Storm Policing.....	26
4.3 Port Rate limiting.....	28
4.4 Port Mirroring.....	29
4.5 Link Aggregation.....	31
4.5.1 About Link Aggregation.....	31
4.5.2 Add Static Link Aggregation.....	32
4.5.3 Add Dynamic Link Aggregation.....	35

4.6 Port Isolation.....	38
4.7 Port Statistics.....	39
5 PoE.....	41
5.1 PoE Port Setting.....	41
5.2 POE Port Timer Setting.....	42
6 L2 Configuration.....	43
6.1 VLAN Configuration.....	43
6.2 MAC VLAN.....	49
6.3 Protocol VLAN.....	52
6.4 Voice VLAN.....	57
6.5 MAC Configuration.....	62
6.5.1 MAC Configuration.....	62
6.6 MSTP Configuration.....	65
6.6.1 Global Configuration.....	66
6.6.2 Instance Configuration.....	68
6.6.3 Instance Port Configuration.....	70
6.6.4 Port Configuration.....	71
6.7 IGMP Snooping Configuration.....	76
6.7.1 IGMP Snooping Configuration.....	76
6.7.2 Static Multicast.....	78
6.8 DHCP Snooping Configuration.....	79
6.8.1 DHCP Snooping Global Configuration.....	80
6.8.2 Static Binding.....	82
6.8.3 DHCP Snooping Port Configuration.....	83
7 Network Security.....	88
7.1 DoS Attack Resistance.....	88
7.1.1 Function Configuration.....	88
7.1.2 Port Configuration.....	89
7.2 ACL Configuration.....	90
7.2.1 MAC ACL Configuration.....	91

7.2.2 IPv4 ACL Configuration.....	93
7.2.3 IPv6 ACL Configuration.....	95
7.2.4 ACL Binding Configuration.....	98
8 Advanced Configuration.....	99
8.1 QoS Configuration.....	101
8.1.1 Basic Configuration.....	101
8.1.2 Queue Scheduling.....	102
8.1.3 CoS Mapping.....	103
8.1.4 DSCP Mapping.....	104
8.1.5 IP Priority Mapping.....	105
8.2 LLDP Configuration.....	106
8.2.1 LLDP Function Configuration.....	107
8.2.2 Port Configuration.....	108
8.2.3 Neighbor Info.....	110
8.3 SNMP Configuration.....	110
8.3.1 View Configuration.....	111
8.3.2 Group Configuration.....	112
8.3.3 Group Configuration.....	113
8.3.4 User Configuration.....	114
8.3.5 Engine ID Configuration.....	116
8.3.6 Trap Configuration.....	116
8.3.7 Notification Configuration.....	117
8.4 RMON Configuration.....	118
8.4.1 Port Statistics.....	119
8.4.2 History Configuration.....	119
8.4.3 Event Configuration.....	121
8.4.4 Alarm Configuration.....	122
8.5 DNS Configuration.....	124
8.6 System Time.....	126
9 DHCP.....	127

9.1 DHCP Server brief introduction.....	127
9.2 IP address assignment of DHCP.....	128
9.2.1 IP address allocation strategy.....	128
9.2.2 Dynamic IP address acquisition process.....	128
9.3 DHCP global configuration.....	129
9.4 IP Pool Setting.....	130
9.5 VLAN IF Address Group Setting.....	131
9.6 Client List.....	132
9.7 Client Static Binding Table.....	133
10 System Maintenance.....	133
10.1 Configuration Management.....	133
10.2 Configuration Saving.....	135
10.4 Firmware Management.....	136

Revision history

Date	Version	Description
Oct. 10, 2020	V 1.0	The first edition

0 Foreword

0.1 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.

0.2 Manual Convention

The following approaches should prevail.

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

1 Management Software Specification

1. Layer 2 Functions			
1.1	Port Management	Enable/disable ports	Available
		Configure the speed, duplex and MTU	Available
		Flow control	Available
		Check the port information	Available
1.2	Port Mirroring	Ingress/egress directions of port and aggregation group	Available
1.3	Rate Limit	Determine the bit rate by chips	Available Bit rate of 32 Kbps
1.4	Port Isolation	Configure port isolation	Available
1.5	Storm Policing	Suppress the storms generated from unknown unicast, unknown multicast, and broadcast	Available
1.6	Link Aggregation	Static link aggregation in manual mode	Available
		Dynamic aggregation in LACP mode	Available
1.7	VLAN	Access	Available
		Trunk	Available
		Hybrid	Available
		QinQ and VLAN division based on port, protocol and MAC	Available
		Dynamic VLAN registration of GVRP	(128) Available
		Voice VLAN (to be available)	(16 OUI) Available
1.8	MAC	Add or delete statically	Available
		Restrict the number of MAC address entries learned by an interface	Available
		Set the dynamic aging time	Available
1.9	Spanning Tree	802.1d (STP)	Available

		802.1w (RSTP)	Available
		802.1s (MSTP)	Available
1.10	Multicast	Add or delete statically; IGMP Snooping	Available
		MLD Snooping	Available
		V1/2/3 dynamic multicast snooping	Available
1.11	DDM	SFP/SFP+DDM	Available
2. Extended Functions			
2.1	ACL	Port numbers based on Source/Destination MAC, protocol type, Source/Destination IP, and L4 port.	Available
2.2	QoS	Classified by 802.1p (CoS)	Available
		Classified by DSCP	Available
		Classified by Source/Destination IP and port	Available
		SP and WRR scheduling algorithms	Available
		Committed Access Rate (CAR)	Available
2.3	LLDP	Link Layer Discovery Protocol (LLDP)	Available
2.4	User Configuration	Add/delete a user	Available
2.5	Log	Login, operation, state, and event logs	Available
2.6	Attack Resistance	DoS defense	Available
		Protect CPU and restrict message uploading rate	Available
		ARP binding (IP, MAC, Port)	Available
2.7	Authentication	802.1x port authentication	Available
		AAA	Available
2.8	Network Diagnostics	Ping, Telnet and traceroute	Available
2.9	System Management	Unit resetting, configuration saving/restoring, upgrade, time setting, etc.	Available

4. Management Functions			
4.1	CLI	Manage serial port command lines	Available
4.2	Telnet	Remotely control Telnet	Available
4.3	SSH	Remotely control SSHv1/SSHv2	Available
4.4	SNMP	SNMP v1/2/3	Available
		Trap: ColdStart, WarmStart, LinkDown, and LinkUp	Available
4.5	Web	L2 setting, L2&3 discovery	Available
4.6	RMON	RMON v1	Available
5. Other Functions			
5.1 DHCP Snooping and Option 82			
5.2 PoE configuration, scheduling management, etc.			
5.3 Dynamic ARP inspection			
5.4 TACACS and authentication			
5.5 DNS configuration			
5.6 Port security configuration			
5.7 MVR protocol			
5.8 VCT			
5.9 UDLD protocol			

2 Web Page Login

2.1 Log in the Network Management Client

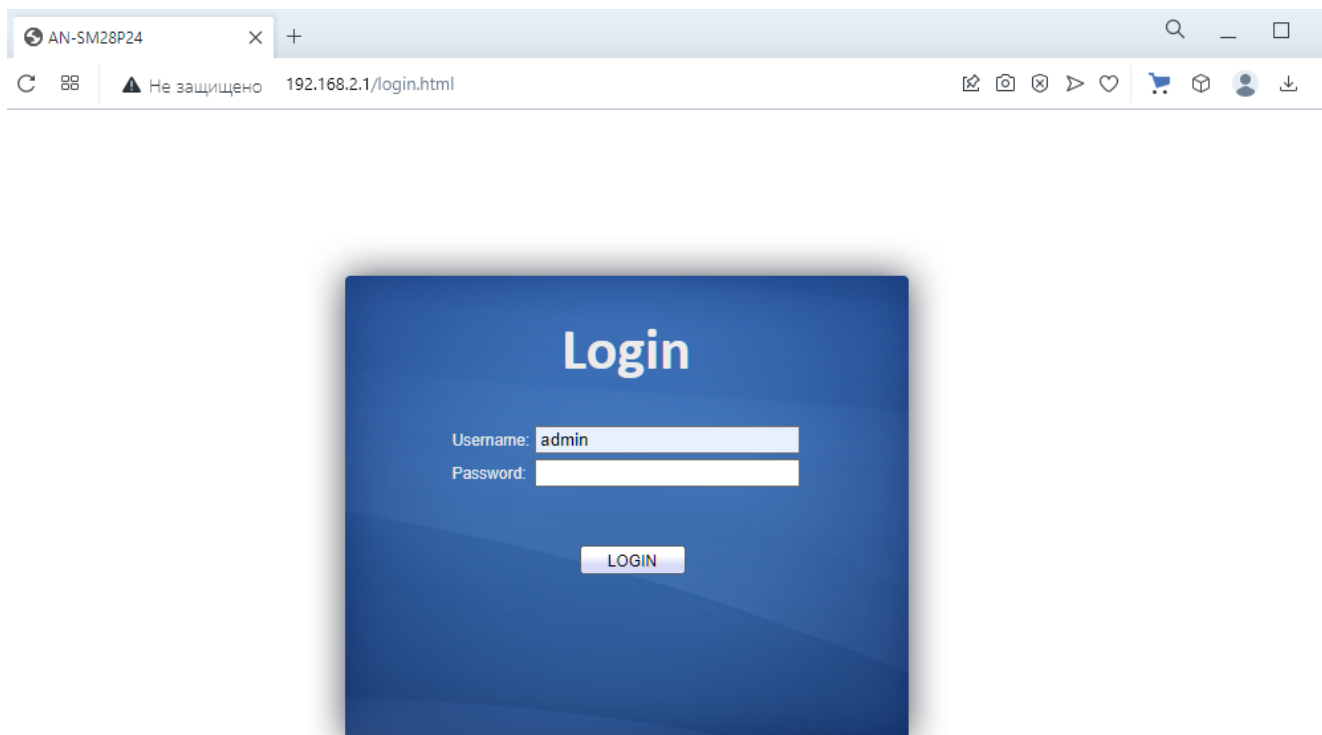
Type in the default switch address: `http://192.168.2.1` and press “Enter”.

Description:

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

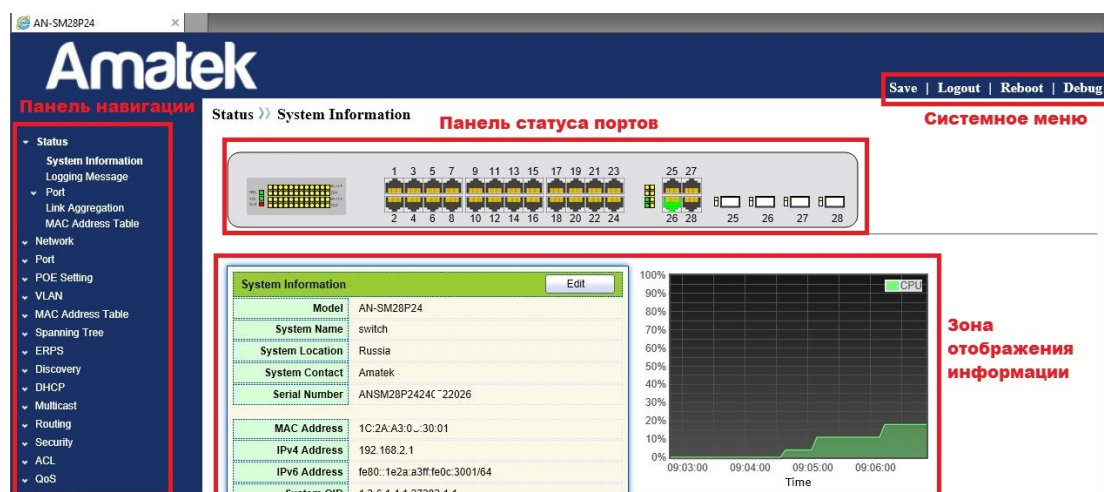
Keep the IP network segment of PC consistent with that of switch but differentiate the IP address as you log in. Set PC’s IP address of `192.168.2.x` and the subnet mask of `255.255.255.0` for the first login ($1 < x \leq 254$).

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.



2.3 Navigation Tree on Web Interface

Menu items such as system state, network configuration, port, PoE setting, VLAN function, MAC address table, STP, topology discovery, multicast, security, ACL, QoS, device diagnostics and management are available on the web network management client. Each item contains submenus. Navigation tree is detailed as follows:

Menu Items	Submenus	Secondary Submenus	Description
System State	System		Display the port state and product info
	Log		Display the device running and operation logs
	Port	Port Statistics	Display the detailed port statistics
		Port Fault Protection	Display the faults occurring to ports
		Bandwidth Utilization Rate	Display the bandwidth utilization per unit time of all ports
	Link Aggregation		Display the aggregation group state and members
	MAC Address Table		Display the MAC address table of the current device
Network Configuration	IP Address		Configure and view the management IP of the current device
	DNS		Configure and view the DNS and server setting
	DNS Host		Configure and view the DNS Server and dynamic host mapping table
	System Time		Configure and view the current system time
Port	Port Configuration		Configure and view all ports
	Port Fault Protection		Configure and view the fault protection
	Link Aggregation	LAG Configuration	Configure and view the port & strategy balancing algorithms contained in LAG
		Port Configuration	Configure and view the LAG
		LACP Configuration	Check LACP system priority and port configuration
	EEE Configuration		Configure and view the EEE state and info

	Jumbo Frame Configuration		Configure and view the length of the max message forwarded by system
	Port Security		Configure and view the rate limiting of port security, as well as port state
	Port Isolation		Configure and view the port isolation
	Storm Policing		Configure and view the port storm policing
	Mirroring		Configure and view the port mirroring
PoE Configuration	PoE Port		Configure and view the PoE port
	PoE Port Timing		Configure and view the timing switch of PoE port
VLAN Function	VLAN Configuration	VLAN Creating	Configure and view the VLAN info of the device
		VLAN Setting	Configure and view the VLAN configuration of all ports
		Member Configuration	Configure and view the port info of VLANs
		Port Configuration	Configure and view the PVID and VLAN attributes of ports
	Voice VLAN	Function Configuration	Configure and view the function switch and port state
		Voice OUI Configuration	Configure and view the OUI performance
	Protocol VLAN Configuration	Protocol Group Configuration	Configure and view the protocol VLAN group
		Protocol Group Binding	Configure and view the protocol VLAN port and group binding.
	MAC VLAN Configuration	MAC Group Configuration	Configure and view the MAC VLAN group
		MAC Group Binding	Configure and view the MAC VLAN port and group binding
	GVRP	Function Configuration	Configure and view the functional system and port state
		Member List	Configure and view the VLANs learned and the port members
		Message Statistics	Configure and view the message statistics related to ports
MAC Address Table	Dynamic MAC Address Table		Configure and view the dynamic MAC addresses and aging time of the device
	Static MAC		Configure and view the static MAC

	Address Table		address tables of the device
	MAC Address Filtering Table		Configure and view the MAC address tables to be filtered
	MAC Address Table for Port Security		Configure and view the MAC address table learned by port security
STP	Function Configuration		Configure and view the STP state and attributes
	Port Configuration		Configure and view the port attributions of STP
	Instance Configuration		Configure and view the instance attributes of STPs
	Instance Port Configuration		Configure and view the instances (incl. port info) of STPs
	Message Statistics		Configure and view the STP message statistics of each port
Topology Discovery	LLDP	Function Configuration	Configure and view the attributes related to LLDP
		Port Configuration	Configure and view the transmitting & receiving state of LLDP at each port
		MED Network Strategy Configuration	Configure and view the MED network strategy table entry
		MED Port Configuration	Configure and view the MED state at each port
		Message Preview	Configure and view the detailed LLDP messages at each port
		Device Info	Configure and view the LLDP and LLDP-MED state
		Neighbor Info	Configure and view the LLDP neighbor info
		Message Statistics	Configure and view the transmitting & receiving state of LLDP message at each port
Multicast	Basic Functions	Function Configuration	Configure and view the function configuration
		Static Multicast Configuration	Configure and view the relevant static multicast info
		Routed Port Configuration	Configure and view the multicast routed port info
		Forwarding Port	Configure and view the multicast

		Configuration	forwarding port info
		Port Limit	Configure and view the multicast limit at each port
		Filtering Rule Configuration	Configure and view the multicast addresses filtered
		Filtering Rule Binding	Configure and view the binding info related to filtering rule and ports
	IGMP Snooping	Function Configuration	Configure and view the switch, version, etc.
		Querier Configuration	Configure and view the querier state
		Message Statistics	Configure and view the protocol messages
	MLD Snooping	Function Configuration	Configure and view the protocol, switch, etc.
		Message Statistics	Configure and view the protocol messages
	MVR	Function Configuration	Configure and view the attribute info such as switch
		Port Configuration	Configure and view the state at each port
		Group Address Configuration	Configure and view the function, VLAN and group address
Security	RADIUS		Configure and view the info related to the servers
	TACACS+		Configure and view the info related to the servers
	AAA	Authentication Method Configuration	Configure and view the login authentication method
		Login Authentication	Configure and view the authentication methods of terminals
	Management Channel Configuration	VLAN Management	Configure and view the current VLAN management info
		Service Management	Configure and view the service management mode and relevant attributes
		ACL Management	Configure and view the ACL aiming at management channels
		ACE Management	Configure and view the ACE configuration of management channels

	Authentication Function	Function Configuration	Configure and view the authentication attributes
		Port Configuration	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
		Session Info	Configure and view the info related to session authentication
	DoS Attack Resistance	Function Configuration	Configure and view the switch option
		Port Configuration	Configure and view the switch option at ports
	Dynamic ARP Inspection	Function Configuration	Configure and view the dynamic ARP inspection
		Message Statistics	Configure and view the messages statistics in APR inspection state at each port
	DHCP Snooping	Function Configuration	Configure and view the switch and state
		Message Statistics	Configure and view the DHCP message statistics received by each port
		Option 82 Function Configuration	Configure and view the attributes related to Option 82
		Option 82 Circuit ID Configuration	Configure and view the Circuit ID of Option 82
	IP Source Guard	Port Configuration	Configure and view the state at ports
		IMPV Binding	Configure and view the binding tables of IP, MAC, Port and VLAN
		Database Storage	Configure and view the storage and info of the binding table entry
ACL	MAC ACL Configuration		Configure and view the MAC ACL rules
	MAC ACE Configuration		Configure and view the MAC ACE table entries
	IPv4 ACL Configuration		Configure and view the IPv4 ACL rules
	IPv4 ACE Configuration		Configure and view the IPv4 ACE table entries

	IPv6 ACL Configuration		Configure and view the IPv6 ACL rules
	IPv6 ACE Configuration		Configure and view the IPv6 ACE table entries
	ACL Binding		Configure and view the ACL rules and the port binding application
QoS	Basic Function	Function Configuration	Configure and view the QoS switch and state
		Queue Scheduling	Configure and view the algorithm of queue scheduling
		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 Priority Mapping	Configure and view the priority and local queue mapping table
	Bandwidth Rate Limiting	Rate Limiting	Configure and view the configuration of port rate limiting
		Egress Queue Rate Limiting	Configure and view the rate limiting configuration based on egress queue
Device Diagnostics	Log Function	Function Configuration	Configure and view the switch and state
		Remote Server Configuration	Configure and view the address of remote servers
	Ping		Network diagnostics by Ping
	Traceroute		Network diagnostics by traceroute
	Electrical Interface Test		Electrical interface link diagnostics by VCT
	Optical Module		Check the SFP module at optical interfaces
	UDLD Protocol	Function Configuration	Configure and view the switch and state
		Neighbor Info	Configure and view the neighbor state
Device Management	User Configuration		Configure and view the user info
	Firmware Management	Upgrade/Backups	Update software
	Configuration Management	Upgrade/Backups	Update configuration files
		Configuration Saving	Save the configuration files supporting device running

	SNMP Configuration	View Configuration	Configure and view the SNMP function view table entry
		Group Configuration	Configure and view the SNMP group
		Community Configuration	Configure and view the SNMP Community
		User Configuration	Configure and view the SNMP user attributes
		Engine ID Configuration	Configure and view the SNMP and remote Engine IDs
		Trap Configuration	Configure and view the SNMP Trap switch and state
		Notification Configuration	Configure and view the SNMP Notification server state
	RMON Configuration	Message Statistics	Configure and view the message statistics history of all ports
		History Configuration	Configure and view the history record state
		Event Configuration	Configure and view the event state
		Alarm Configuration	Configure and view the alarm state

3 System Configuration

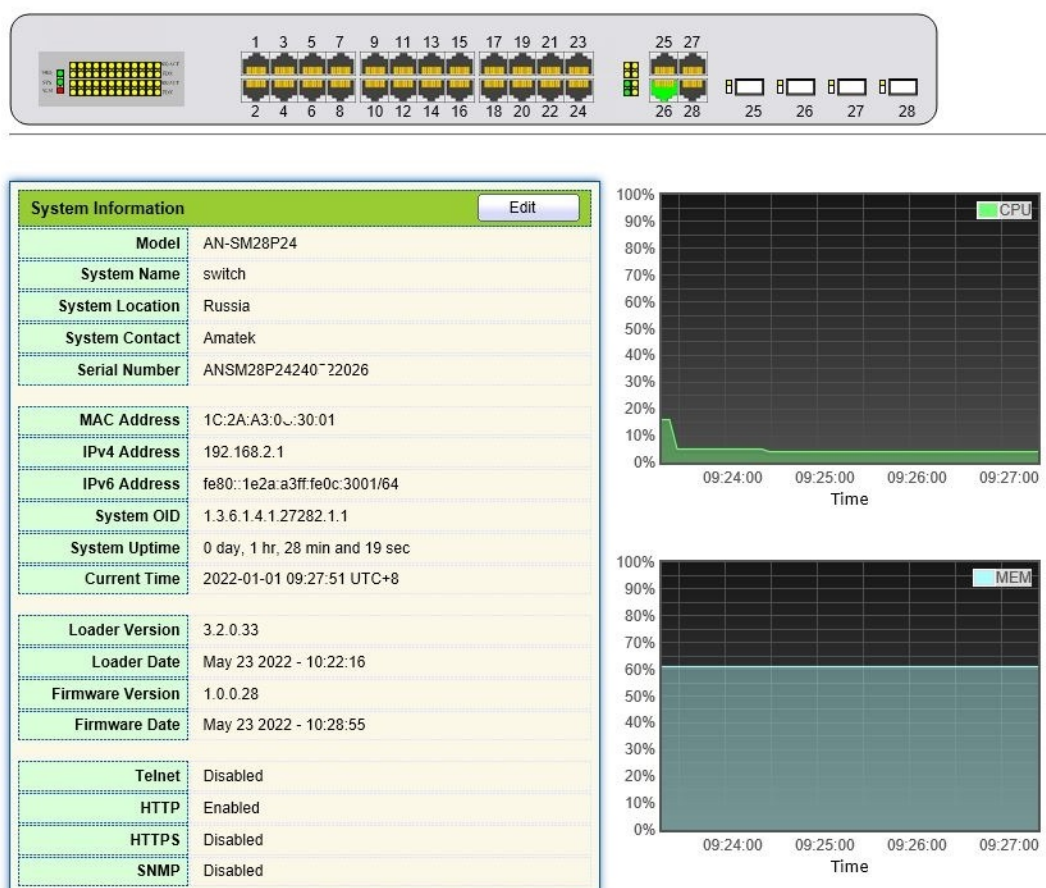
3.1 System Info

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 “System Configuration > System Info” in the navigation tree as follows:

Status >> System Information



Description:

Mouseover a port to check the port No., type, rate and state.

“Modify” the “System Name”, “Location” and “Contact” in the product info. “Apply” and finish.

3.2 Network Configuration

Change the management IP address on web interface.

Instructions:

1. Click the “Network Configuration > IP Address Setting” in the navigation bar to discover IPv4 address of 192.168.2.1/24 by default as follows:
2. Repeat this step, select the “Static” address type, enter the IPv4 address of 192.168.2.1, the subnet mask of 255.255.255.0, and the network management of 192.168.2.254. “Apply” and finish.

IPv4 Address	
Address Type	☒ Static ☐ Dynamic
IP Address	192.168.2.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.2.254

Sub IPv4 Address	
Enabled	☐ Enable
IP Address	0.0.0.0
Subnet Mask	0.0.0.0

IPv6 Address	
Auto Configuration	☒ Enable
DHCPv6 Client	☐ Enable
IPv6 Address	
Prefix Length	0 (0 - 128)
IPv6 Gateway	

Operational Status	
IPv4 Address	192.168.2.1
IPv4 Default Gateway	192.168.2.254
Sub IPv4 Address	0.0.0.0
IPv6 Address	::
IPv6 Gateway	::
Link Local Address	fe80::1e2a:a3ff:fe00:24/64

Apply

3.3 User Configuration

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

Instructions:

1. Click the “Device Management > User Configuration” in the navigation bar to discover the username of “admin” and the authority of “administrator” by default as follows:

User Account

Showing entries Showing 1 to 1 of 1 entries

☐	Username	Privilege
☐	admin	Admin

First Previous **1** Next Last

2. “Add” a new user account and “Modify” the selected user attribute as follows:

Add User Account

Username	
Password	
Confirm Password	
Privilege	☒ Admin ☐ User

Edit User Account

Username	admin
Password	
Confirm Password	
Privilege	☒ Admin ☐ User

3.4 Log Configuration

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 “Device Diagnostics > Log Function > Function Configuration” in the navigation bar to switch logs on/off, select the egress terminal, configure the severity level, etc. as follows:

State ☒ Enable

Aggregation ☒ Enable

Aging Time Sec (15 - 3600, default 300)

Console Logging

State ☒ Enable

Minimum Severity

 Note: Emergency, Alert, Critical, Error, Warning, Notice

RAM Logging

State ☒ Enable

Minimum Severity

 Note: Emergency, Alert, Critical, Error, Warning, Notice

Flash Logging

State ☐ Enable

Minimum Severity

 Note: Emergency, Alert, Critical, Error, Warning, Notice

- Click the “Device Diagnostics > Log Function > Remote Server Configuration” in the navigation bar to add and view the server configuration as follows:

Remote Server Table

☐	Entry	Server Address	Server Port	Facility	Minimum Severity
0 results found.					

- “Add” a new remote log server and “Modify” 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 Severity	Notice Note: Emergency, Alert, Critical, Error, Warning, Notice

3.5 Telnet Configuration

Users can enable or disable the Telnet login option on web interface.

Instructions:

1. Click the “Security > Management Channel Configuration > Service Management” in the navigation bar to enable or disable the service by checking the “Telnet” tag. “Apply” and finish as follows:

Management Service		
Telnet	☒	Enable
SSH	☐	Enable
HTTP	☒	Enable
HTTPS	☐	Enable
SNMP	☐	Enable

Session Timeout		
Console	10	Min (0 - 65535, default 10)
Telnet	10	Min (0 - 65535, default 10)
SSH	10	Min (0 - 65535, default 10)
HTTP	10	Min (0 - 65535, default 10)
HTTPS	10	Min (0 - 65535, default 10)

3.6 HTTPS Configuration

Users can enable or disable the HTTP & HTTPS

login options on web interface.

Instructions:

1. Click the “Security > Management Channel Configuration > Service Management” in the navigation bar to enable or disable the services by checking the “HTTP” and “HTTPS” tags. “Apply” and finish as follows:

Management Service	
Telnet	☐ Enable
SSH	☐ Enable
HTTP	☒ Enable
HTTPS	☒ Enable
SNMP	☐ Enable

Session Timeout	
Console	10 Min (0 - 65535, default 10)
Telnet	10 Min (0 - 65535, default 10)
SSH	10 Min (0 - 65535, default 10)
HTTP	10 Min (0 - 65535, default 10)
HTTPS	10 Min (0 - 65535, default 10)

3.7 Diagnostics Test

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

Instructions:

1. Click the “Device 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)

Ping Stop

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

Ping Result

Packet Status	
Status	Success.
Transmit Packet	4
Receive Packet	4
Packet Lost	0 %
Round Trip Time	
Min	0 ms
Max	0 ms
Average	0 ms

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

Instructions:

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

Address Type	☐ Hostname ☒ IPv4
Server Address	192.168.1.122
Time to Live	☐ User Defined 30 (2 - 255, default 30)

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

Traceroute Result

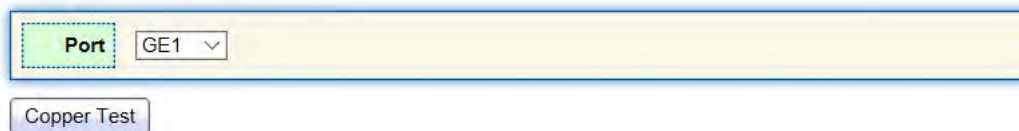
```
traceroute to 192.168.1.122 (192.168.1.122), 30 hops max, 38 byte packets
1 192.168.1.122 (192.168.1.122) 0.000 ms 0.000 ms 0.000 ms
```

Electrical interface 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 “Device Diagnostics > Electrical Interface Test” in the navigation bar to select a port for test as follows:



Port GE1

Copper Test

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

Copper Test Result

Cable Status	
Port	GE1
Result	Open Cable
Length	2.92 M

4 Port Configuration

4.1 Physical Port

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

Instructions:

1. Click the “Port > Port Configuration” in the navigation bar:

Port Setting Table

	Entry	Port	Type	Description	State	Link Status	Speed	Duplex	Flow Control
☐	1	GE1	1000M Copper		Enabled	Down	Auto	Auto	Disabled
☐	2	GE2	1000M Copper		Enabled	Down	Auto	Auto	Disabled
☐	3	GE3	1000M Copper		Enabled	Down	Auto	Auto	Disabled
☐	4	GE4	1000M Copper		Enabled	Up	Auto (1000M)	Auto (Full)	Disabled (Off)
☐	5	GE5	1000M Copper		Enabled	Down	Auto	Auto	Disabled
☐	6	GE6	1000M Copper		Enabled	Down	Auto	Auto	Disabled
☐	7	GE7	1000M Copper		Enabled	Down	Auto	Auto	Disabled
☐	8	GE8	1000M Copper		Enabled	Down	Auto	Auto	Disabled
☐	9	GE9	1000M Copper		Enabled	Down	Auto	Auto	Disabled
☐	10	GE10	1000M Copper		Enabled	Up	Auto (100M)	Auto (Full)	Disabled (Off)

2. Select the port(s) to be configured, and “Modify” as follows:

Edit Port Setting

Port	GE3-GE5	
Description		
State	☒ Enable	
Speed	☒ Auto ☐ 10M ☐ Auto - 10M ☐ 100M ☐ Auto - 100M ☐ 1000M ☐ Auto - 1000M ☐ 10G ☐ Auto - 10M/100M	
Duplex	☒ Auto ☐ Full ☐ Half	
Flow Control	☐ Auto ☐ Enable ☒ Disable	

Configuration items are as follows.

Configuration Items	Description
Interpretation	Users can identify the specified ports by interpreting them as required.
State	Users can enable or disable the ports as required.
Rate	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.

4.2 Storm Policing

Storm policing principles

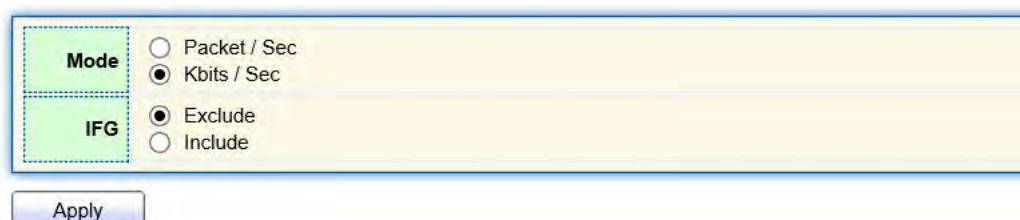
Storms generated via broadcast, unknown multicast and unicast messages are prevented as follows. These messages will be suppressed subject to packet rates respectively. The average rate of the messages received by monitoring interfaces will be compared with the max threshold configured during an inspection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

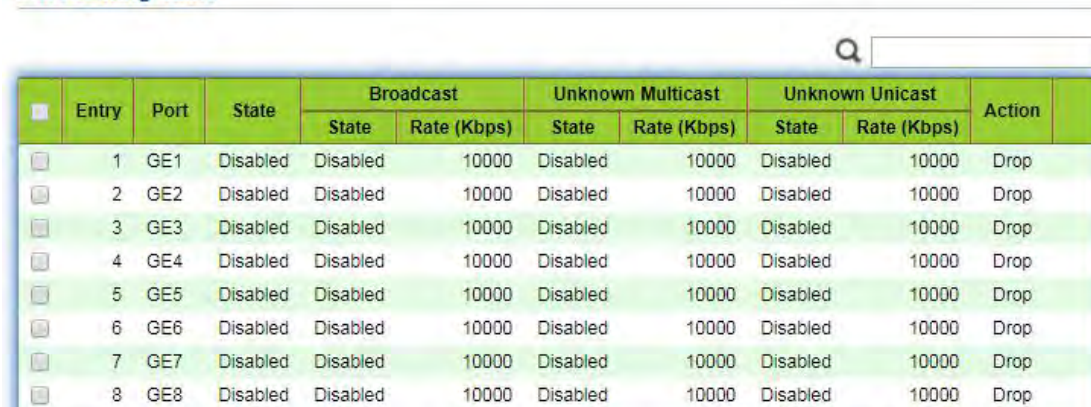
Instructions:

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



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

Port Setting Table



	Entry	Port	State	Broadcast		Unknown Multicast		Unknown Unicast		Action
				State	Rate (Kbps)	State	Rate (Kbps)	State	Rate (Kbps)	
	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
	8	GE8	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop

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

Edit Port Setting

Port	GE3-GE5
State	☒ Enable
Broadcast	☒ Enable
	10000 Kbps (16 - 1000000, default 10000)
Unknown Multicast	☒ Enable
	10000 Kbps (16 - 1000000, default 10000)
Unknown Unicast	☒ Enable
	10000 Kbps (16 - 1000000, default 10000)
Action	☐ Drop ☐ Shutdown

4.3 Port Rate limiting

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

Background

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 > Bandwidth Rate Limiting > Port Rate Limiting” in the navigation bar to choose a rate-limiting port and check the current configuration as follows:

Ingress / Egress Port Table

	Entry	Port	Ingress		Egress	
			State	Rate (Kbps)	State	Rate (Kbps)
☐	1	GE1	Disabled		Disabled	
☐	2	GE2	Disabled		Disabled	
☐	3	GE3	Disabled		Disabled	
☐	4	GE4	Disabled		Disabled	
☐	5	GE5	Disabled		Disabled	
☐	6	GE6	Disabled		Disabled	
☐	7	GE7	Disabled		Disabled	
☐	8	GE8	Disabled		Disabled	

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

Edit Ingress / Egress Port

Port	GE3-GE5	
Ingress	☒ Enable	
	1000000	Kbps (16 - 1000000)
Egress	☒ Enable	
	1000000	Kbps (16 - 1000000)

Configuration parameters

Configuration Items		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

4.4 Port 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:



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:

Mirroring Table

	Session ID	State	Monitor Port	Ingress Port	Egress Port
☐	1	Enabled	GE1 (Normal*)	GE2-GE4	GE2-GE4
☐	2	Disabled	---	---	---
☐	3	Disabled	---	---	---
☐	4	Disabled	---	---	---

Edit

*** Allow the monitor port to send or receive normal packets

2. Select one session and “Modify” it in the mirroring group configuration interface:

Edit Mirroring

Session ID 1

State ☒ Enable

Monitor Port GE1

☒ Send or Receive Normal Packet

Ingress Port

Available Port: GE1, GE5, GE6, GE7, GE8, GE9, GE10, GE11

Selected Port: GE2, GE3, GE4

Egress Port

Available Port: GE1, GE5, GE6, GE7, GE8, GE9, GE10, GE11

Selected Port: GE2, GE3, GE4

Apply Close

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.
Destination Port	Only one ordinary physical port can be selected, excluding link aggregation port and source port.
Source Ingress Port	Any message received will be mirrored to the destination port.
Source Egress Port	Any message transmitted will be mirrored to the destination port.

4.5 Link Aggregation

4.5.1 About Link Aggregation

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

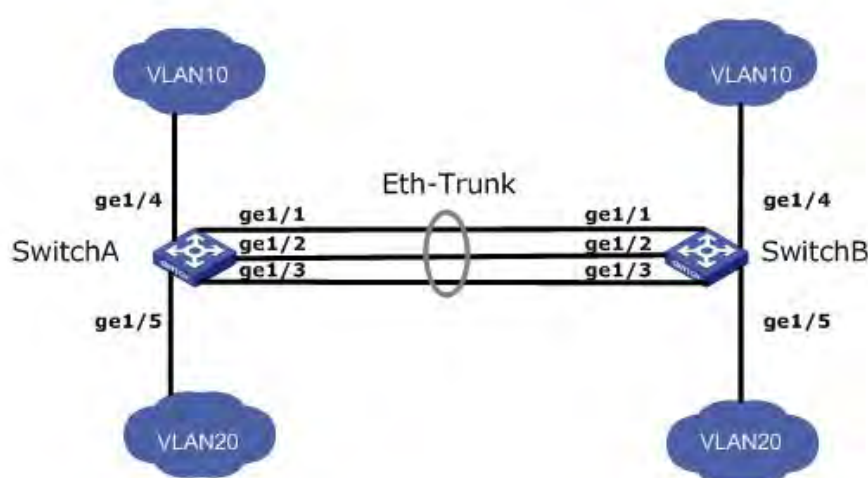
logical interface.

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.

4.5.2 Add Static Link Aggregation

Instructions for adding a Static Link Aggregation:

1. Click the “Port > Aggregation > LAG Configuration”, 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	Type	Link Status	Active Member	Inactive Member	
☐	LAG 1		---	---			
☐	LAG 2		---	---			
☐	LAG 3		---	---			
☐	LAG 4		---	---			
☐	LAG 5		---	---			
☐	LAG 6		---	---			
☐	LAG 7		---	---			
☐	LAG 8		---	---			

Edit

- Select one of 8 LAGs available, “Modify” the configuration page as follows:

Edit Link Aggregation Group

LAG

1

Name

Type

☒ Static
☐ LACP

Member

Available Port

GE1

GE2

GE3

GE4

GE5

GE6

GE7

GE8

>

<

Selected Port

Apply

Close

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.

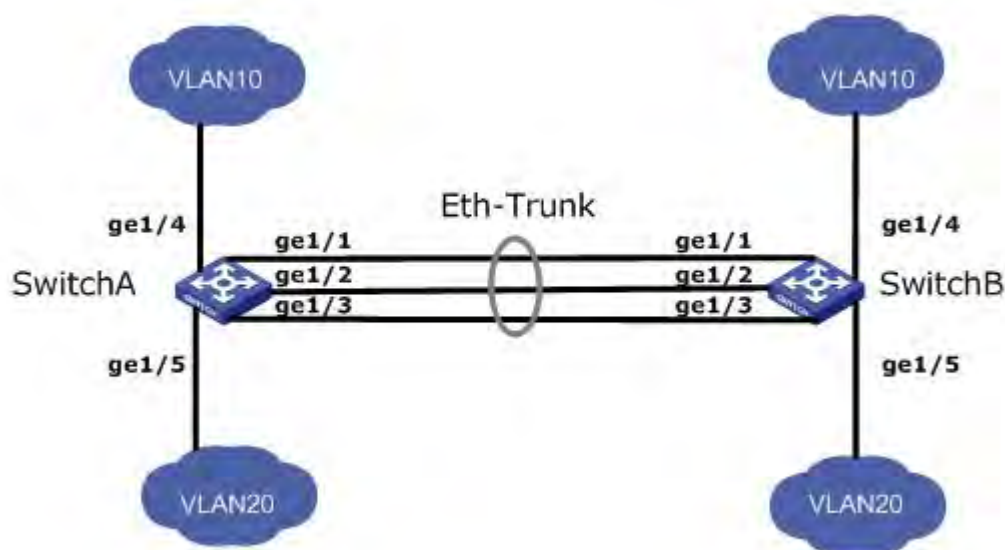
Mode	Select from the manual mode and the LACP mode.
Member	Up to 8 member ports are available in LAG.

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. Similar to the steps of Switch B configuration, Switch A creates an Eth-Trunk interface and accesses member interfaces to broaden link bandwidth. Click the “Port > Aggregation > LAG Configuration”, choose “LAG 1” and port GE1, 2 and 3 and move them to the selected ports on the right. “Apply” and finish as follows.

Edit Link Aggregation Group

LAG	1
Name	
Type	☒ Static ☐ LACP
Member	Available Port GE4 GE5 GE6 GE7 GE8 GE9 GE10 GE11 Selected Port GE1 GE2 GE3

Apply Close

4.5.3 Add Dynamic Link Aggregation

Dynamic Link Aggregation

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 > Aggregation > LAG Configuration” in the navigation bar, select the LAG ID and LACP mode, “Modify” them as follows:

Edit Link Aggregation Group

LAG	2	
Name		
Type	☐ Static ☒ LACP	
Member	Available Port GE1 GE2 GE3 GE7 GE8 GE9 GE10 GE11	Selected Port GE4 GE5 GE6

- Click the “Port > Aggregation > LACP Configuration” in the navigation bar to configure the LACP attributes such as system priority, port priority and timeout method as follows:

System Priority	32768	(1 - 65535, default 32768)
------------------------	------------------------------------	----------------------------

LACP Port Setting Table

Q

	Entry	Port	Port Priority	Timeout
☐	1	GE1	1	Long
☐	2	GE2	1	Long
☐	3	GE3	1	Long
☐	4	GE4	1	Long
☐	5	GE5	1	Long

Interface data are as follows

Configuration Items	Description
Mode	Static mode and LACP mode Static mode A static link aggregation should be created and the member interfaces should be added for better bandwidth and reliability between two

	devices in case LACP is unavailable to one of them. LACP mode Links between two devices are able to backup redundantly in the dynamic LACP mode. Backup links ensure the uninterrupted data transmission by replacing the partially failed links.
System Priority	LACP determines the active and passive modes between two devices subject to priority standard.
Port Priority	LACP determines the dynamic LAG member mode subject to the port priority with a superior system.
Timeout Period	It decides the transmission frequency of LACP messages.

Description:

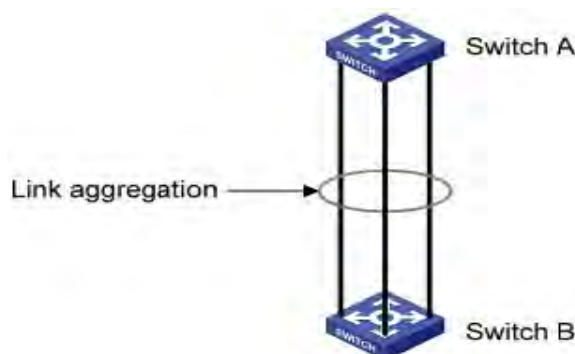
Please make sure there is no member interface accessing the Eth-Trunk before changing its work pattern, otherwise it fails.

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, so as to share the load by each member port.

The following configurations are exemplified by means of dynamic aggregation.



Instructions:

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 > Aggregation > LAG Configuration” in the navigation bar, “Modify” with LAG 2, select GE1-GE3 in LACP mode. “Apply” and finish as follows:

Edit Link Aggregation Group

LAG	1
Name	
Type	☐ Static ☒ LACP
Member	Available Port GE4 GE5 GE6 GE7 GE8 GE9 GE10 GE11 Selected Port GE1 GE2 GE3

4.6 Port Isolation

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 > Port Isolation” in the navigation bar, check the port(s) to be isolated, “Modify” to switch this function as follows:

Protected Port Table

☐	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

Port	GE1-GE4
State	☒ Protected

The following figure illustrates that PC1, 2 and 3 access GE1, 2 and 3 severally, but they are expected to be isolated.

Instructions:

1. Click the “Port > Port Isolation” in the navigation bar, check and “Modify” the GE1, 2 and 3 to be isolated. “Apply” and finish as follows:

Protected Port Table

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

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

4.7 Port Statistics

- a. Introduce the detailed flow statistics of all ports and that to be refreshed or cleared manually by users.



Note: Cleared flow statistics cannot be restored. Please think twice before operation.

Instructions:

1. Click the “Device Management > RMON Configuration> Message Statistics” in the navigation bar as follows:

Statistics Table

Refresh Rate 0 sec

Entry	Port	Bytes Received	Drop Events	Packets Received	Broadcast Packets	Multicast Packets	CRC & Align Errors	Undersize Packets	Oversize Packets	Fragments	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	GE1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
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
4	GE4	4160	0	57	28	29	0	0	0	0	0	0	57	0	0	0	0	0
5	GE5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	GE6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	GE7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	GE8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Description:

“Refresh” to get the updated flow statistics.

“Clear” to remove the flow statistics at all ports and refresh the page.

“View” the specified port for detailed flow statistics.

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

1. Click the “System State > Port Info> Port Statistics” in the navigation bar as follows:

Port

GE4

MIB Counter

☒ All
☐ Interface
☐ Etherlike
☐ RMON

Refresh Rate

☐ None
☐ 5 sec
☒ 10 sec
☐ 30 sec

Clear

Interface

ifInOctets	4224
ifInUcastPkts	0
ifInNUcastPkts	58
ifInDiscards	0
ifOutOctets	1655143
ifOutUcastPkts	0
ifOutNUcastPkts	16252
ifOutDiscards	0
ifInMulticastPkts	30
ifInBroadcastPkts	28
ifOutMulticastPkts	10220
ifOutBroadcastPkts	6032

Description:

“Clear” the flow statistics at the current port and refresh the page.

5 PoE

PoE (Power over Ethernet) transmits data signal for the terminals based on IP (e.g. IP phone, WAP, and IP camera) and supplies the devices with direct current, without changing the existing Cat-5 network cabling status. It ensures safe structured cabling and normal network operation to minimize the cost.

5.1 PoE Port Setting

Instructions:

1. Click the “POE Setting > POE Port Setting” in the navigation bar as follows:

System info

System Power(mW)	8164
System Temperature(C)	60
Refresh Rate	☐ None ☐ 5 sec ☒ 10 sec ☐ 30 sec

Port Setting Table

	Entry	Port	PortEnable	Status	Type	Level	Actual Power(mW)	Voltage(V)	Current(mA)	WatchDog
☐	1	GE1	Enabled	Off	AF(U)	0	N/A	N/A	N/A	Disabled
☐	2	GE2	Enabled	Off	AF(U)	0	N/A	N/A	N/A	Disabled
☐	3	GE3	Enabled	Off	AF(U)	0	N/A	N/A	N/A	Disabled
☐	4	GE4	Enabled	Off	AF(U)	0	N/A	N/A	N/A	Disabled
☐	5	GE5	Enabled	Off	AF(U)	0	N/A	N/A	N/A	Disabled
☐	6	GE6	Enabled	Off	AF(U)	0	N/A	N/A	N/A	Disabled
☐	7	GE7	Enabled	Off	AF(U)	0	N/A	N/A	N/A	Disabled

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

Edit Port Setting

Port	GE1
PortEnable	☐ Enable ☐ Disable
WatchDog	☐ Enable ☐ Disable

Configuration items are as follows.

Configuration Items	Description
PortEnable	Enable/Disable Poe port power
WatchDog	Enable/Disable Poe port watchdog function; After enabling the watchdog function, when the POE port is continuously powered but there is no traffic, the POE watchdog will be triggered. After 2 minutes of detection, the power supply will be stopped and then powered on. The total detection cycle is 5 times

5.2 POE Port Timer Setting

Instructions:

1. Click the “POE Setting > POE Port Setting” , Select the power supply time of Poe schedule. “Apply” and finish as follows:

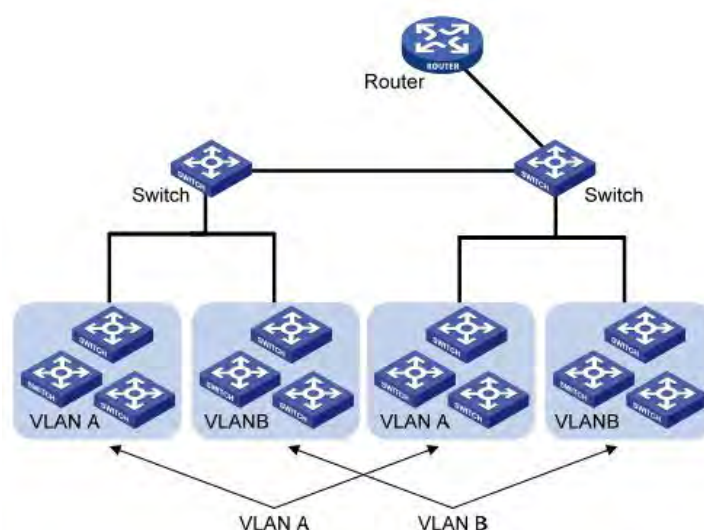
Port

	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Mon	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
Tue	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
Wed	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
Thu	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
Fri	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
Sat	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
Sun	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒

6 L2 Configuration

6.1 VLAN Configuration

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.



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.

a. Instructions for creating a new VLAN:

1. Click the “VLAN Function > VLAN Configuration > VLAN Creating” 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:

VLAN

Available VLAN

Created VLAN

Apply

VLAN Table

Showing All entries Showing 1 to 2 of 2 entries

VLAN	Name	Type	VLAN Interface State
1	default	Default	Disabled
2	VLAN0002	Static	Disabled

Edit Delete

First Previous 1 Next Last

2. The VLAN created will be displayed in the VLAN Table. Users can “Modify” the VLAN as follows:

Edit VLAN Name

Name

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.

b. Instructions for adding the current port to a specified VLAN

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.

The first method:

1. Click the “VLAN Function > VLAN Configuration > VLAN Setting” in the navigation tree, 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	☐ Tagged	☒ Untagged	☒	☐
2	GE2	Trunk	☐ Excluded	☐ Tagged	☒ Untagged	☒	☐
3	GE3	Trunk	☐ Excluded	☐ Tagged	☒ Untagged	☒	☐
4	GE4	Trunk	☐ Excluded	☐ Tagged	☒ Untagged	☒	☐
5	GE5	Trunk	☐ Excluded	☐ Tagged	☒ Untagged	☒	☐
6	GE6	Trunk	☐ Excluded	☐ Tagged	☒ Untagged	☒	☐
7	GE7	Trunk	☐ Excluded	☐ Tagged	☒ Untagged	☒	☐
8	GE8	Trunk	☐ Excluded	☐ Tagged	☒ Untagged	☒	☐

Interface data are as follows.

Configuration Items	Description
VLAN	VLAN ID to be configured
Member	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

The second method:

1. Click the “VLAN Function > VLAN Configuration > Member Configuration” in the navigation tree, select the port to be configured and “Modify” to configure its attributes:

Edit Port Setting

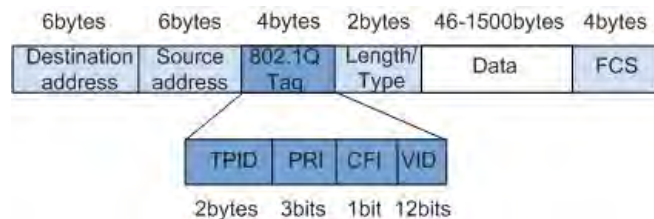
Interface data are as follows.

Configuration Items	Description
Port	Port No. to be configured
Mode	Modify the current VLAN mode in port configuration: Hybrid: port in this mode can serve as the Tagged & Untagged members of VLANs. Access: port in this mode serves as the only one member of VLAN Trunk: port in this mode serves as the Untagged member of PVID only and the Tagged member of VLANs
Member	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

c. Introduction to 802.1q

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



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.

d. Instructions for trunk interface configuration:

- Click the “VLAN Function > VLAN Configuration > Port Configuration” in the navigation tree, select the port and “Modify” it to configure the attributes:

Port Setting Table

☐	Entry	Port	Mode	PVID	Accept Frame Type	Ingress Filtering	Uplink	TPID
☐	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	Modify the current VLAN mode in the port configuration: 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 member of PVID and the Tagged member of VLANs
PVID	Port PVLAN

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 decided to filter VLAN messages excluded at the port
Uplink	Whether in uplink mode or not
TPID	Identification No. of VLAN Tag

Illustration

Connection interfaces and 2 VLANs should be added to support the user communication in VLAN 2 and 3 of the links between Switch A and B. That is, VLAN 2 and 3 should be added to the GE1-3 Ethernet Interfaces of Switch A and B.

Instructions:

Create VLAN 2 and 3 in Switch A and B. Add GE1 port connected to user interfaces to VLAN2, with GE2 to VLAN3. Set GE3 in the trunk work pattern and add it to VLAN2 and 3.

6.2 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 Function > MAC VLAN Configuration > MAC Group Configuration” in the navigation tree, and “Add” a new MAC group as follows:

MAC Group Table

Showing entries Showing 1 to 1 of 1 entries

☐	Group ID	MAC Address	Mask
☐	1	00:0A:5A:00:00:00	24

Add MAC Group

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

Apply Close

Interface data are as follows.

Configuration Items	Description
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.

2. Create a relevant VLAN.
3. Add Ethernet interfaces to the VLAN in a correct way.
4. 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 Function > VLAN Configuration > VLAN Creating” in the navigation tree, add VLAN10 to the VLAN Creating List on the right, “Apply” and finish as follows:

The interface shows a 'VLAN' configuration window. On the left, under 'Available VLAN', are VLANs 11 through 18. On the right, under 'Created VLAN', are VLANs 3 through 10. Arrows between the lists allow moving VLANs from available to created. An 'Apply' button is at the bottom.

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.

Port Setting Table

☐	Entry	Port	Mode	PVID	Accept Frame Type	Ingress Filtering	Uplink	TPID
☐	1	GE1	Hybrid	100	All	Enabled	Disabled	0x8100
☐	2	GE2	Trunk	1	All	Enabled	Disabled	0x8100

Membership Table

☐	Entry	Port	Mode	Administrative VLAN	Operational VLAN
☐	1	GE1	Hybrid	1U, 10U, 100P	1U, 10U, 100P
☐	2	GE2	Trunk	1UP, 10T	1UP, 10T
☐	3	GE3	Trunk	1UP	1UP

3. 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 Function > MAC VLAN Configuration > MAC Group Configuration" in the navigation tree, 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:

MAC Group Table

Showing All entries Showing 1 to 3 of 3 entries

☐	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

First Previous 1 Next Last

- Click the “VLAN Function > MAC VLAN Configuration > MAC Group Binding” in the navigation tree, “Add” to select the Hybrid port only, MAC group ID to be bound, and specified VLAN ID. “Apply” and finish:

MAC Group Table

Showing entries Showing 1 to 3 of 3 entries

☐	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

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

6.3 Protocol VLAN

Protocol-based 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 a large number of resources consumed.

Instructions:

- Click the “VLAN Function > Protocol VLAN Configuration > Protocol Group Configuration” in the navigation tree as follows:

Protocol Group Table

Showing entries Showing 1 to 1 of 1 entries

☐	Group ID	Frame Type	Protocol Value
☐	1	Ethernet_II	0x8888

Add Protocol Group

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

Interface data are as follows.

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

- Fill in corresponding configuration items.
- “Apply” and finish.

Protocol Group Table

Showing All entries Showing 1 to 2 of 2 entries

	Group ID	Frame Type	Protocol Value
☐	1	Ethernet_II	0x8888
☐	2	RFC_1042	0x8889

- Click the “VLAN Function > Protocol VLAN Configuration > Protocol Group Binding” in the navigation tree to bind the protocol No., port No. and VLAN ID, to bring the configuration into effect as follows:

Group Binding Table

Showing All entries Showing 1 to 1 of 1 entries

	Port	Group ID	VLAN
☐	GE1	1	10

Add Group Binding

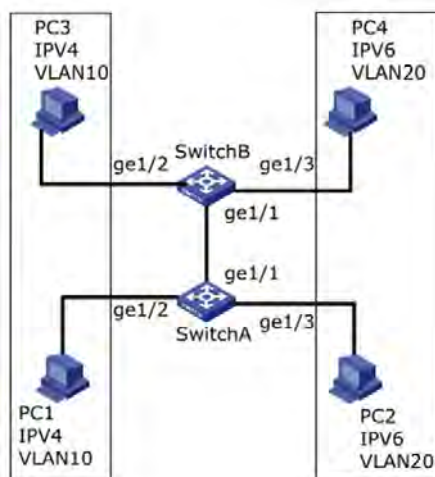
Port	Available Port	Selected Port
	GE1	
Group ID	1	
VLAN		
Note: Only VLAN Hybrid port can be set Protocol VLAN		
Apply Close		

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



Instructions:

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

VLAN

Available VLAN

VLAN 2
VLAN 3
VLAN 4
VLAN 5
VLAN 6
VLAN 7
VLAN 8
VLAN 9

Created VLAN

VLAN 1
VLAN 10
VLAN 20

Apply

VLAN Table

Showing All entries Showing 1 to 3 of 3 entries

VLAN	Name	Type	VLAN Interface State
☐ 1	default	Default	Disabled
☐ 10	VLAN0010	Static	Disabled
☐ 20	VLAN0020	Static	Disabled

First Previous 1 Next Last

2. Configure GE2 and GE3 interfaces of Switch A in Hybrid mode. Click the “VLAN Function > VLAN Configuration > Port Configuration”, “Modify” the interfaces in Hybrid mode:

Port Setting Table

Q

	Entry	Port	Mode	PVID	Accept Frame Type	Ingress Filtering	Uplink	TPID
☐	1	GE1	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 Function > VLAN Configuration > VLAN Setting”, 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

VLAN VLAN0010 Q

Entry	Port	Mode	Membership			PVID	Forbidden
1	GE1	Trunk	☒ Excluded	☐ Tagged	☐ Untagged	☐	☐
2	GE2	Hybrid	☐ Excluded	☐ Tagged	☒ Untagged	☐	☐
3	GE3	Hybrid	☒ Excluded	☐ Tagged	☐ Untagged	☐	☐

VLAN Configuration Table

VLAN VLAN0020

Entry	Port	Mode	Membership			PVID	Forbidden
1	GE1	Trunk	☒ Excluded	☐ Tagged	☐ Untagged	☐	☐
2	GE2	Hybrid	☒ Excluded	☐ Tagged	☐ Untagged	☐	☐
3	GE3	Hybrid	☐ 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 similar to 2 and 3.

5. Add the Tagged GE1 interface of Switch A to VLAN10 and 20. Click the “VLAN Function > VLAN Configuration > VLAN Setting”, drop down the list to select VLAN10 and the Tagged member of GE1. Configure VLAN20 similarly.

VLAN Configuration Table

VLAN VLAN0010

Entry	Port	Mode	Membership			PVID	Forbidden
1	GE1	Trunk	☐ Excluded	☒ Tagged	☐ Untagged	☐	☐

VLAN Configuration Table

VLAN VLAN0020

Entry	Port	Mode	Membership			PVID	Forbidden
1	GE1	Trunk	☐ Excluded	☒ Tagged	☐ 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 Function > Protocol VLAN Configuration > Protocol Group Configuration” in the navigation tree to add 2 rules for protocol groups:

Protocol Group Table

Showing All entries

Showing 1 to 2 of 2 entries

☐	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 Function > Protocol VLAN Group >

Protocol Group Binding”, “Add” to bind GE2 and binding group ID1 with VLAN10, and to bind GE3 and binding group ID2 with VLAN20:

Group Binding Table

Showing entries Showing 1 to 2 of 2 entries

☐	Port	Group ID	VLAN
☐	GE2	1	10
☐	GE3	2	20

6.4 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.

As long as 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 Function > Voice VLAN > Function Configuration” in the navigation tree as follows.

State	☐ Enable
VLAN	None v
CoS / 802.1p Remarking	☐ Enable 6 v
Aging Time	1440 v Min (30 – 65536, default 1440)

Port Setting Table

☐	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
☐	7	GE7	Disabled	Auto	Voice Packet
☐	8	GE8	Disabled	Auto	Voice Packet

Edit Port Setting

Port	GE1
State	☐ Enable
Mode	☒ Auto ☐ Manual
QoS Policy	☒ Voice Packet ☐ All

Configuration Items	Description
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 Remark	Whether to redefine the Voice VLAN message priority or not
Aging Time	Table aging time
Port	Enabled Voice VLAN port
Mode	Voice VLAN port can be operated in auto mode and manual mode.
QoS Strategy	Select the message to be affected by QoS

- Click the “VLAN Function > Voice VLAN > Voice OUI Configuration” in the navigation tree to configure the address segment of OUI of Voice VLAN as follows:

Voice OUI Table

Showing All entries Showing 1 to 8 of 8 entries

☐	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 Voice OUI

OUI	: :
Description	

- Fill in corresponding configuration items.
- “Apply” and finish as follows.

Voice OUI Table

Showing All entries

Showing 1 to 9 of 9 entries



☐	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
☐	98:00:36	H7650

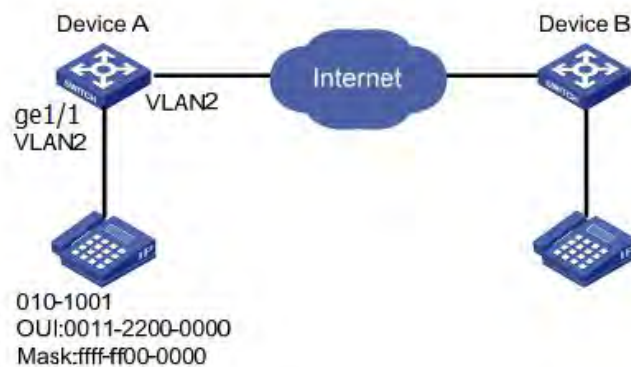
First Previous **1** Next Last

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 have to customize an OUI (0011-22 31-05e1) 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 Function > VLAN Configuration > VLAN Creating” in the navigation tree to add VLAN2 to the VLAN list on the right. “Apply” and finish:

VLAN

Available VLAN

VLAN 3
VLAN 4
VLAN 5
VLAN 6
VLAN 7
VLAN 8
VLAN 9
VLAN 10

Created VLAN

VLAN 1
VLAN 2

Apply

VLAN Table

Showing All entries Showing 1 to 2 of 2 entries

	VLAN	Name	Type	VLAN Interface State
☐	1	default	Default	Disabled
☐	2	VLAN0002	Static	Disabled

- Configure the Ethernet interface GE1 of Switch A in Trunk mode. Click the “VLAN Function > VLAN Configuration > Port Configuration” in the navigation tree, “Modify” GE1 in Trunk mode:

Port Setting Table

Showing 1 to 1 of 1 entries

	Entry	Port	Mode	PVID	Accept Frame Type	Ingress Filtering	Uplink	TPID
☐	1	GE1	Trunk	1	All	Enabled	Disabled	0x8100

- Click the “VLAN Function > Voice VLAN > Voice OUI Configuration” in the navigation tree 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:

Voice OUI Table

Showing All entries Showing 1 to 1 of 1 entries

	OUI	Description
☐	00:11:22	aaa

- Enable the Voice VLAN of port GE1. Click the “VLAN Function > Voice VLAN > Function Configuration” in the navigation tree to enable the global configuration, select VLAN2. Select port GE1 in the configuration list, “Modify” and enable the auto mode. “Apply” and finish as follows:

State	☒ Enable
VLAN	VLAN0002 ▾
CoS / 802.1p Remarking	☐ Enable 6 ▾
Aging Time	1440 Min (30 - 65536, default 1440)

Apply

Port Setting Table

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

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

6.5 MAC Configuration

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 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.

6.5.1 MAC Configuration

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 a large number of 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.

Generally speaking, the aging time recommended is 300 seconds by default.

Instructions for aging time setting:

1. Click the “MAC Address Table > Dynamic MAC Address Table” in the navigation tree to the configuration and display interface:

Aging Time 300 Sec (10 - 630, default 300)

Apply

Dynamic Address Table

Showing All entries Showing 1 to 1 of 1 entries

	VLAN	MAC Address	Port
☐	1	50:3E:AA:B3:B7:BA	GE25

First Previous 1 Next Last

Refresh Add Static Address

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.

Check the instructions for MAC address table:

4. Click the “System State > MAC Address Table” to check all MAC address info as follows:

MAC Address Table

Showing entries Showing 1 to 2 of 2 entries

VLAN	MAC Address	Type	Port
1	00:E0:4C:00:11:21	Management	CPU
1	50:3E:AA:B3:B7:BA	Dynamic	GE25

Interface data are as follows.

Query Items	Description
MAC	Destination MAC Address
VLAN	VLAN ID belonging to MAC address
Port	Message egress corresponding to MAC address
Type	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.

6.5.2 Static MAC

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

Steps of establishing a static MAC address

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

Static Address Table

Showing entries Showing 1 to 1 of 1 entries

☐	VLAN	MAC Address	Port
☐	1	00:00:11:11:22:22	GE3

Add Static Address

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

Interface data are as follows.

Configuration Items	Description
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.

- Fill in corresponding configuration items.
- “Apply” and finish.

6.6 MSTP Configuration

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 broadcast storms and redundant backups. It converges slowly.	All VLANs can be shared without discrimination in user 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 broadcast storms and redundant backups. It converges rapidly. Spanning trees balance the load among VLANs. Flow of different VLANs will be forwarded subject to paths.	Distinguish the user and business flow for load sharing. Different VLANs forward the flow through separate spanning trees.

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.

6.6.1 Global Configuration

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

Instructions:

1. Click the “STP > Function Configuration” in the navigation tree as follows:

State	☐ Enable	
Operation Mode	☐ STP ☒ RSTP ☐ MSTP	
Path Cost	☒ Long ☐ Short	
BPDU Handling	☐ Filtering ☒ Flooding	
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:A3:00:00:24	
Revision	0	(0 - 65535, default 0)
Max Hop	20	(1 - 40, default 20)
Operational Status		
Bridge Identifier	32768-1C:2A:A3:00:00:24	
Designated Root Bridge	0-00:00:00:00:00:00	
Root Port	N/A	
Root Path Cost	0	
Topology Change Count	0	
Last Topology Change	00/00/00/00	

Interface data are as follows.

Configuration Items	Description
Enabled	It is checked by default to enable the spanning tree on behalf of switches.
Running Mode	3 modes are available, namely STP, RSTP and MSTP.
Path Cost Mode	In Long mode and Short mode
BPDU Forwarding Method	The method to handle the BPDU messages received by the device
Priority	Port priority
Hello Time	Intervals between Hello messages
Max Age	Max aging time
Forward Delay	Forward delay time
Domain 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.
--	--

2. Fill in corresponding configuration items.
3. “Apply” and finish.

6.6.2 Instance Configuration

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 “STP > Instance Configuration” in the navigation tree, “Modify” the selected spanning tree instances to be configured as follows:

MST Instance Table

	MSTI	Priority	Bridge Identifier	Designated Root Bridge	Root Port	Root Path Cost	Remaining Hop	VLAN
	0	32768	32768-1C:2A:A3:00:00:24	0-00:00:00:00:00:00	N/A	0	0	1-4094
	1	32768	32768-1C:2A:A3:00:00:24	0-00:00:00:00:00:00	N/A	0	0	
	2	32768	32768-1C:2A:A3:00:00:24	0-00:00:00:00:00:00	N/A	0	0	
	3	32768	32768-1C:2A:A3:00:00:24	0-00:00:00:00:00:00	N/A	0	0	
	4	32768	32768-1C:2A:A3:00:00:24	0-00:00:00:00:00:00	N/A	0	0	
	5	32768	32768-1C:2A:A3:00:00:24	0-00:00:00:00:00:00	N/A	0	0	
	6	32768	32768-1C:2A:A3:00:00:24	0-00:00:00:00:00:00	N/A	0	0	
	7	32768	32768-1C:2A:A3:00:00:24	0-00:00:00:00:00:00	N/A	0	0	

Edit MST Instance Setting

MSTI 1

VLAN

Available VLAN: 1, 2, 3, 4, 5, 6, 7, 8

Selected VLAN:

Priority 32768 (0 - 61440, default 32768)

Bridge Identifier 32768-1C:2A:A3:00:00:24

Designated Root Bridge 0-00:00:00:00:00:00

Root Port

Root Path Cost 0

Remaining Hop 0

Apply Close

Interface data are as follows.

Configuration Items	Description
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.
Bridge ID	The bridge ID of the spanning tree instance corresponding to this device consists of the priority and MAC address.
Root Bridge ID	The elected instance root bridge ID consists of the priority and MAC address.
Root Port	The elected instance root port ID
Root Cost	Path cost to the root bridge

- Fill in corresponding configuration items.
- “Apply” and finish as follows.

MST Instance Table

Q

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

6.6.3 Instance Port Configuration

1. Click the “STP > Instance Port Configuration” in the navigation tree, check the port to be modified from the list of all ports of the device, “Modify” to enter the detailed configuration interface as follows:

MSTI 0

	Entry	Port	Path Cost	Priority	Port Role	Port State	Mode	Type	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	Forwarding	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

Edit MST Port Setting

MSTI

0

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

Apply

Close

Interface data are as follows.

Configuration Items	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
Type	The port types in the instance contain boundary and internal ports

2. Fill in corresponding configuration items.
3. “Apply” and finish.

6.6.4 Port Configuration

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

1. Click the “STP Function > Port Configuration” in the navigation tree, select the port and “Modify” to configure its attributes:

Port Setting Table

Entry	Port	State	Path Cost	Priority	RPDU Filter	RPDU 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	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-3	20000
4	GE4	Enabled	20000	128	Disabled	Disabled	Disabled	Enabled	Disabled	Forwarding	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	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-7	20000
8	GE8	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-8	20000

Edit Port Setting

Port	GE1
State	☒ Enable
Path Cost	0 (0 - 200000000) (0 = Auto)
Priority	128
Edge Port	☐ Enable
BPDU Filter	☐ Enable
BPDU Guard	☐ Enable
Point-to-Point	☒ Auto ☐ Enable ☐ Disable
Port State	Disabled
Designated Bridge	0-00:00:00:00:00:00
Designated Port ID	128-1
Designated Cost	20000
Operational Edge	False
Operational Point-to-Point	False

Apply Close

Interface data are as follows.

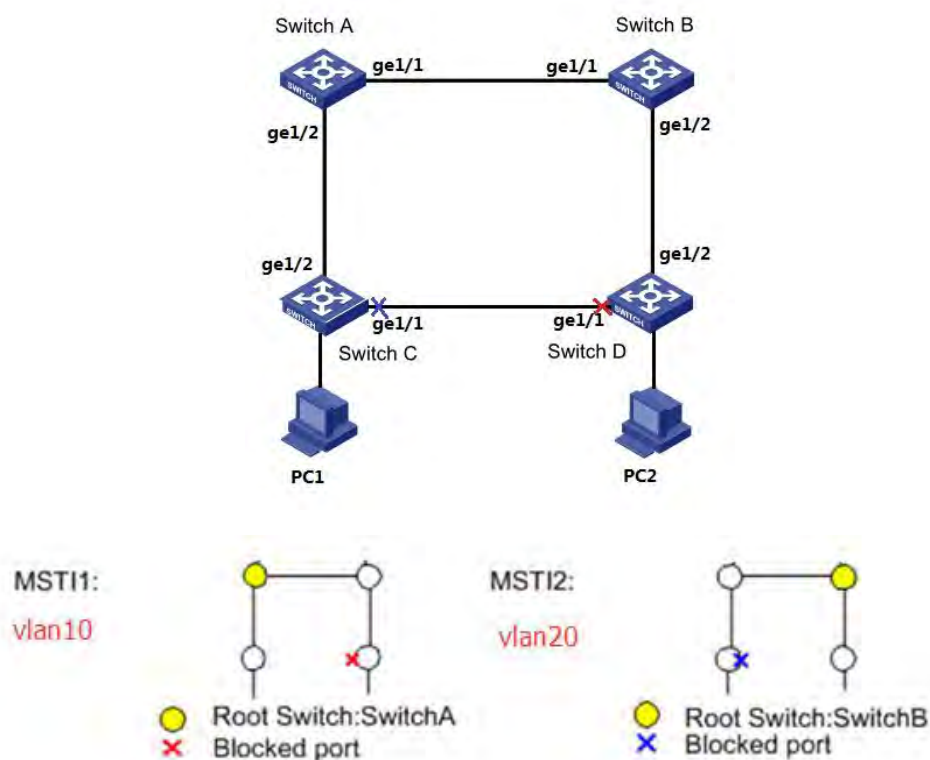
Configuration Items	Description
Port	The port No. to configure attributes
State	Enable STP or not
Edge Port	Rather than another switch or network segment, the edge port should be connected directly to user terminals. It can quickly transit to the forward state since topology changes create no loops. 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.

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:

1. 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 Function > VLAN Configuration > VLAN Creating” in the navigation tree, fill in the corresponding configurations. “Apply” and finish as follows.

VLAN

Available VLAN

VLAN 2
VLAN 3
VLAN 4
VLAN 5
VLAN 6
VLAN 7
VLAN 8
VLAN 9

Created VLAN

VLAN 1
VLAN 10
VLAN 20

Apply

VLAN Table

Showing All entries Showing 1 to 3 of 3 entries

VLAN	Name	Type	VLAN Interface State
☐ 1	default	Default	Disabled
☐ 10	VLAN0010	Static	Disabled
☐ 20	VLAN0020	Static	Disabled

- VLANs are added to the switch ports ingress loops. Click the “VLAN Function > VLAN Configuration > Member Configuration” in the navigation tree, 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

Port

GE1

Mode

Trunk

Membership

10
20

1UP

☐ Forbidden
☐ Excluded
☒ Tagged
☐ Untagged
☐ PVID

Apply

Close

- Click the “STP > Function Configuration” in the navigation tree, and choose MSTP mode as follows:

State	☒ Enable	
Operation Mode	☐ STP ☐ RSTP ☒ MSTP	
Path Cost	☒ Long ☐ Short	
BPDU Handling	☐ Filtering ☒ Flooding	
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:A3:00:00:24	
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 “STP > Instance Configuration” to fill in corresponding parameters, and “Add” them as follows:

MST Instance Table

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



Note:

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.

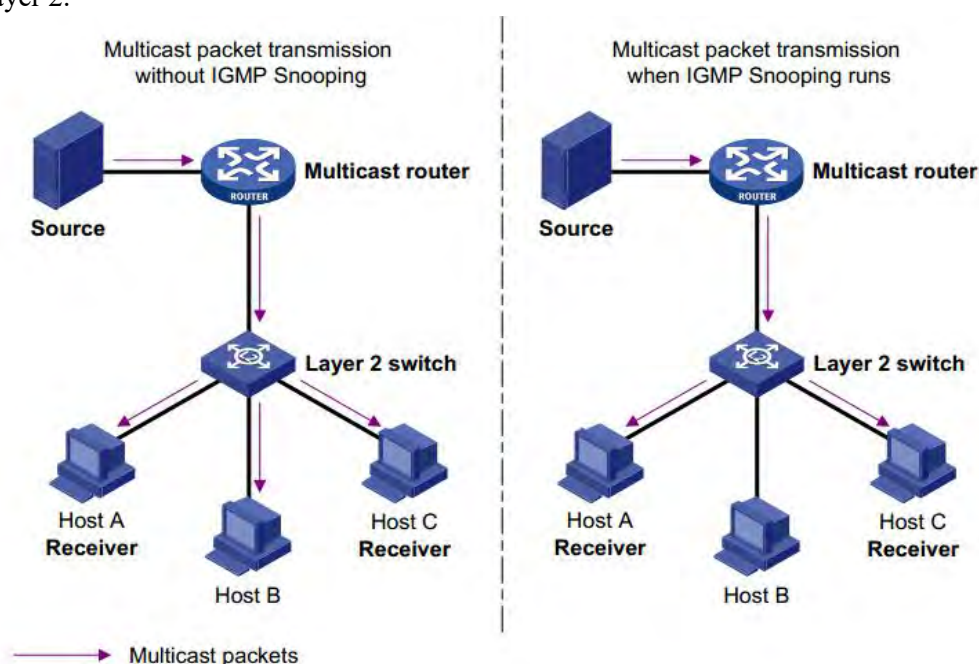
6. The tree-shaped network will eliminate loops.

6.7 IGMP Snooping Configuration

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.



6.7.1 IGMP Snooping Configuration

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, so as 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 > Function Configuration”, select the VLAN to be configured from the created VLAN info, and “Modify” the details as follows:

State	☐ Enable
Version	☒ IGMPv2 ☐ IGMPv3
Report Suppression	☒ Enable

Apply

VLAN Setting Table

	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

Routed Port Learning	
Fast Leave	
Number of Query	Max number of multicast queries
Query Interval	The interval between message queries
Max Response Time of Queries	Timeout (over the max response time) of a query message
Number of Queries for a Specified Group	Max number of queries for a specified group
Query Intervals for a Specified Group	The interval between message queries for a specified group

2. Fill in corresponding configuration items.
3. “Apply” and finish.

6.7.2 Static Multicast

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 > Basic Function > Static Multicast Configuration”, “Add” a new static multicast item, and “Modify” the existing ones as follows:

Group Address Table

IP Version

Showing entries Showing 0 to 0 of 0 entries

☐	VLAN	Group Address	Member	Type	Life (Sec)
0 results found.					

Add Group Address

Interface data are as follows.

Configuration Items	Description
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

	VLAN	Group Address	Member	Type	Life (Sec)
☐	1	224.1.1.111	GE1-GE8	Static	

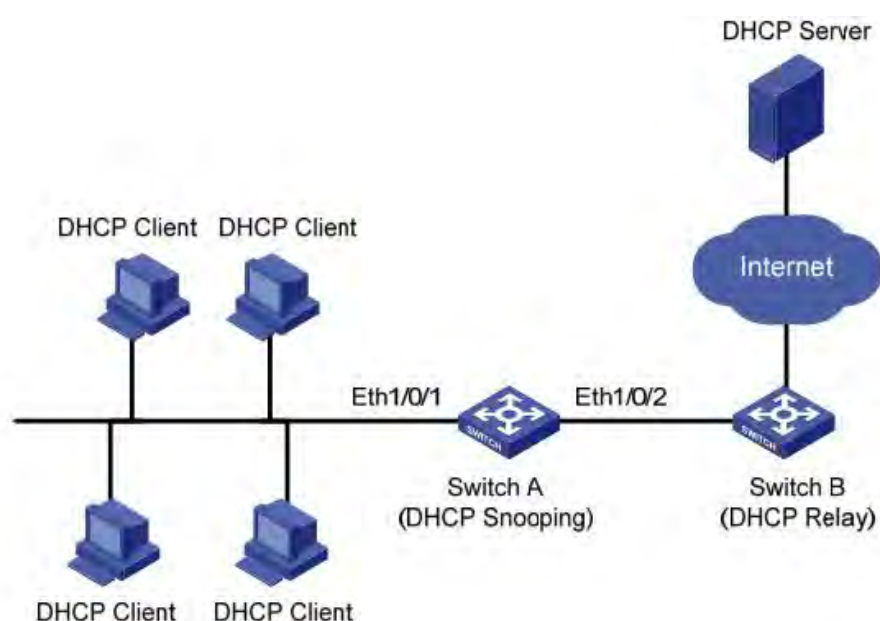
6.8 DHCP Snooping Configuration

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.



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

6.8.1 DHCP Snooping Global Configuration

Enable DHCP Snooping

Instructions:

1. Click the “Security > DHCP Snooping > Function Configuration”. DHCP Snooping interface is divided into global configuration and port configuration. Select the port to be modified in the port configuration and “Modify” the details as follows:

State

☐ Enable

VLAN

Available VLAN

VLAN 1
VLAN 10
VLAN 20

Selected VLAN

Apply

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

Edit Port Setting

Port

GE1-GE2

Trust

☐ Enable

Verify Chaddr

☐ Enable

Rate Limit

pps (1 - 300, default 0), 0 is Unlimited

Apply

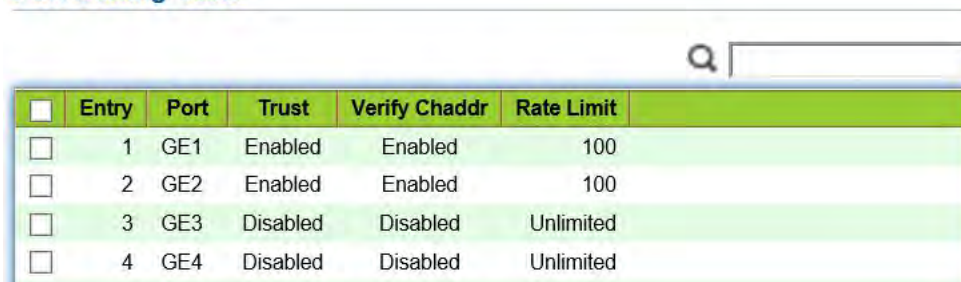
Close

Interface data are as follows.

Configuration 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 Inspection	Whether the consistency inspection for Client addresses is 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.

Port Setting Table



☐	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

6.8.2 Static Binding

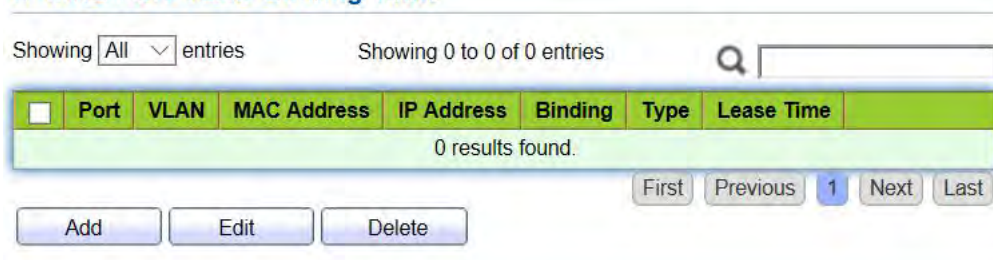
In DHCP network, users (non-DHCP users) obtaining IP addresses statically may attack the network by imitating DHCP Server, constructing DHCP Request message, etc. Legal DHCP users may suffer from security risks when using the network normally.

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 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-MAC-Port-VLAN Binding Table



Showing entries Showing 0 to 0 of 0 entries

☐	Port	VLAN	MAC Address	IP Address	Binding	Type	Lease Time
0 results found.							

Add IP-MAC-Port-VLAN Binding

Port	GE1
VLAN	(1 - 4094)
Binding	☒ IP-MAC-Port-VLAN ☐ IP-Port-VLAN
MAC Address	
IP Address	/ 255.255.255.255

Interface data are as follows.

Configuration Items	Description
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 entries Showing 1 to 1 of 1 entries

	Port	VLAN	MAC Address	IP Address	Binding	Type	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

6.8.3 DHCP Snooping Port Configuration

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.

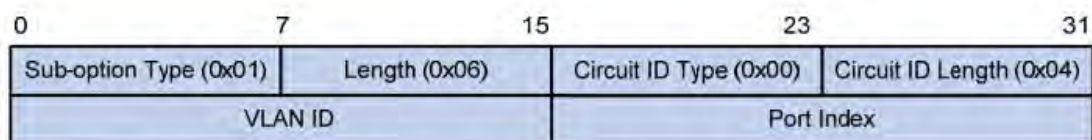
Option 82 is the Relay Agent Information Option in DHCP messages, which records the location of DHCP Client. When the DHCP relay (or DHCP Snooping device) receives the Request message sent from DHCP Client to DHCP Server, administrators can add the Option 82 to locate the DHCP Client and control the 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.

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:

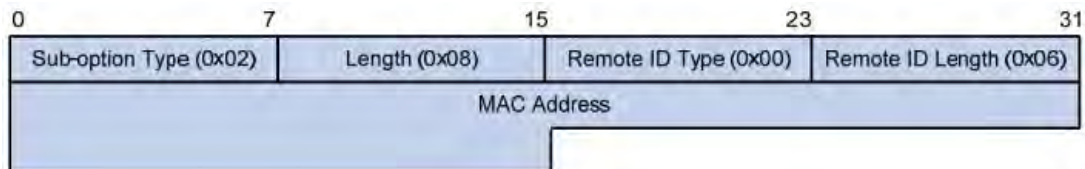
Sub-option 1: VLAN No. and port index (port physical number minuses 1) of the port receiving the Request message sent by DHCP Client.

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.



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



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:

1. Click the “Security > DHCP Snooping > Option 82 Function Configuration”. Global and port configurations are contained. Select the port to be configured and “Modify” the details as follows:

Remote ID

☐ User Defined

Operational Status

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

Apply

Port Setting Table

	Entry	Port	State	Allow Untrust
☐	1	GE1	Disabled	Drop
☐	2	GE2	Disabled	Drop
☐	3	GE3	Disabled	Drop
☐	4	GE4	Disabled	Drop
☐	5	GE5	Disabled	Drop
☐	6	GE6	Disabled	Drop
☐	7	GE7	Disabled	Drop

Edit Port Setting

Port

GE1-GE2

State

☐ Enable

Allow Untrust

☐ Keep
☒ Drop
☐ Replace

Apply

Close

Interface data are as follows.

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

Remote ID	Fill in the Remote ID fields in Option 82 (such as user-defined abcd)
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 particular 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.

Port Setting Table

	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

1. DHCP Snooping supports Option 82

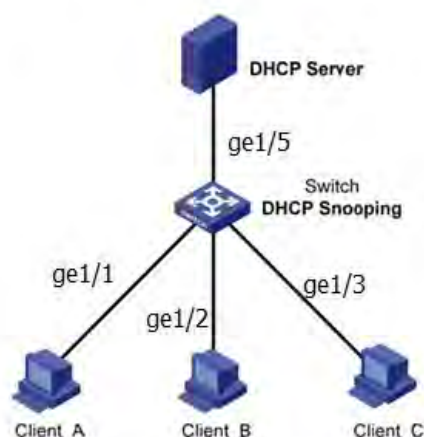
As shown below, Switch port GE1-5 is connected to DHCP Server, and ports GE1-1, 2 and 3 are connected to DHCP Client A, B and C respectively.

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



Configure DHCP snooping to support Option 82

Instructions:

2. Enable the DHCP Snooping of switch. Click the “DHCP Snooping Configuration > Function Configuration” in the navigation tree to enable the function as follows:

State ☒ Enable

Available VLAN

Selected VLAN

VLAN 1
VLAN 10
VLAN 20

Apply

3. Set the GE1-5 as the trust port of DHCP Snooping, fill in corresponding configurations and “Modify” as follows:

Port Setting Table

	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	Enabled	Disabled	Unlimited
☐	6	GE6	Disabled	Disabled	Unlimited

4. Configure on the port GE1-3 so that user defined remote ID can be set by Option 82. Click the “DHCP Snooping Configuration > Option 82 Function Configuration”, check and configure the port. “Apply” and finish as follows:

Remote ID ☒ User Defined
aaaaa

Operational Status

Remote ID aaaaa

Apply

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

5. Configure on the port GE1-3 so that the circuit ID can be set by Option 82. Click the “DHCP Snooping Configuration > Option 82 Circuit ID Function Configuration” to configure the port. “Apply” and finish as follows:

Option82 Circuit ID Table

Showing All entries Showing 1 to 1 of 1 entries

	Port	VLAN	Circuit ID
☐	GE3	1	ge1/3

Add Edit Delete First Previous 1 Next Last

7 Network Security

7.1 DoS Attack Resistance

7.1.1 Function Configuration

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

Instructions

1. Click the “Security > DoS Attack Resistance > Function Configuration” to the “DoS Global Configuration” to enable the “PoD Attack Resistance”, “Land Attack Resistance”, “Source/Destination MAC Same Packet Discarding”, “ICMP Fragment Packet Discarding”. “Apply” and finish as follows.

POD	☒ Enable
Land	☒ Enable
UDP Blat	☒ Enable
TCP Blat	☒ Enable
DMAC = SMAC	☒ Enable
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 Note: Source Port < 1024
TCP Fragment	☒ Enable Note: Offset = 1
Ping Max Size	☒ Enable IPv4 ☒ Enable IPv6 512 Byte (0 - 65535, default 512)
TCP Min Hdr size	☒ Enable 20 Byte (0 - 31, default 20)
IPv6 Min Fragment	☒ Enable 1240 Byte (0 - 65535, default 1240)
Smurf Attack	☒ Enable 0 Netmask Length (0 - 32, default 0)

Apply

7.1.2 Port Configuration

DoS attack resistance is enabled based on ports.

Instructions

1. Click the “Security > DoS Attack Resistance > Port Configuration” as follows:

Port Setting Table

	Entry	Port	State
☐	1	GE1	Disabled
☐	2	GE2	Disabled
☐	3	GE3	Disabled
☐	4	GE4	Disabled

2. Select and “Modify” the port to enable or disable the DoS attack resistance function as follows.

Edit Port Setting

Port	GE1
State	☒ Enable

7.2 ACL Configuration

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 particular 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 the source/destination address, port No., etc. ACL can be divided into the 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.

7.2.1 MAC ACL Configuration

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 Configuration” in the navigation tree as follows.

The screenshot shows a web interface for MAC ACL Configuration. It features a text input field labeled 'ACL Name' and a button labeled 'Apply' below it.

Interface data are as follows.

Configuration Items	Description
ACL Name	Name the MAC ACL Rules

2. Click on the “ACL > MAC ACL Configuration” in the navigation tree, “Add” the ACL name as follows:

The screenshot shows the 'ACE Table' interface. It includes a search bar, a dropdown for 'Showing All entries', and a table with the following columns: Sequence, Action, Source MAC (Address, Mask), Destination MAC (Address, Mask), Ethertype, VLAN, and 802.1p (Value, Mask). The table is currently empty, displaying '0 results found.' Below the table are buttons for 'Add', 'Edit', 'Delete', and pagination controls (First, Previous, 1, Next, Last).

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

Interface data are as follows.

Configuration Items	Description
Serial No.	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 Address	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 Address	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
Ethernet Type	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.

ACE Table

ACL Name

Showing entries Showing 1 to 1 of 1 entries

	Sequence	Action	Source MAC		Destination MAC		Ethertype	VLAN	802.1p	
			Address	Mask	Address	Mask			Value	Mask
☐	1	Permit	00:00:00:00:20:00	FF:FF:FF:FF:FF:00	00:00:00:00:10:00	FF:FF:FF:FF:FF:00	Any	Any	Any	Any

7.2.2 IPv4 ACL Configuration

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 Configuration" in the navigation tree as follows.

ACL Name

Interface data are as follows.

Configuration Items	Description
ACL Name	Name the IPv4 ACL rules

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

ACE Table

ACL Name

Showing entries Showing 0 to 0 of 0 entries

	Sequence	Action	Protocol	Source IP		Destination IP		Source Port	Destination Port	TCP Flags	Type of Service		ICMP	
				Address	Mask	Address	Mask				DSCP	IP Precedence	Type	Code
0 results found.														

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	B
Sequence	100 (1 - 2147483647)
Action	☒ Permit ☐ Deny ☐ Shutdown
Protocol	☒ Any ☐ Select ICMP ☐ Define (0 - 255)
Source IP	☒ Any / (Address / Mask)
Destination IP	☒ Any / (Address / Mask)
Type of Service	☒ Any ☐ DSCP (0 - 63) ☐ IP Precedence (0 - 7)
Source Port	☒ Any ☐ Single (0 - 65535) ☐ Range - (0 - 65535)
Destination Port	☒ Any ☐ Single (0 - 65535) ☐ Range - (0 - 65535)
TCP Flags	Urg: ☐ Set ☐ Unset ☒ Don't care Ack: ☐ Set ☐ Unset ☒ Don't care Psh: ☐ Set ☐ Unset ☒ Don't care Rst: ☐ Set ☐ Unset ☒ Don't care Syn: ☐ Set ☐ Unset ☒ Don't care Fin: ☐ Set ☐ Unset ☒ Don't care
ICMP Type	☒ Any ☐ Select Echo Reply ☐ Define (0 - 255)
ICMP Code	☒ Any ☐ Define (0 - 255)

Interface data are as follows.

Configuration Items	Description
No.	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.
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.
Service Type	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 Field	Enter the ICMP field value of ACL rules. Select “Any” to represent any field value.

3. “Apply” and finish as follows.

ACE Table

ACL Name:

Showing entries Showing 1 to 1 of 1 entries

	Sequence	Action	Protocol	Source IP		Destination IP		Source Port	Destination Port	TCP Flags	Type of Service		ICMP	
				Address	Mask	Address	Mask				DSCP	IP Precedence	Type	Code
☐	100	Permit	Any (IP)	Any	Any	Any	Any				Any	Any		

7.2.3 IPv6 ACL Configuration

Instructions

1. Click the “ACL > IPv6 ACL Configuration” in the navigation tree as follows.

ACL Name

Interface data are as follows.

Configuration Items	Description
ACL Name	Name the IPv6 ACL rules

2. Click the “ACL > IPv6 ACE Configuration” in the navigation tree, “Add” the ACL Name as follows:

ACE Table

ACL Name

Showing entries Showing 0 to 0 of 0 entries

	Sequence	Action	Protocol	Source IP		Destination IP		Source Port	Destination Port	TCP Flags	Type of Service		ICMP	
				Address	Prefix	Address	Prefix				DSCP	IP Precedence	Type	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 ☐ Define (0 - 255)
Source IP	☒ Any ☐ / (Address / Prefix (0 - 128))
Destination IP	☒ Any ☐ / (Address / Prefix (0 - 128))
Type of Service	☒ Any ☐ DSCP (0 - 63) ☐ IP Precedence (0 - 7)
Source Port	☒ Any ☐ Single (0 - 65535) ☐ Range - (0 - 65535)
Destination Port	☒ Any ☐ Single (0 - 65535) ☐ Range - (0 - 65535)
TCP Flags	Urg: ☐ Set ☐ Unset ☒ Don't care Ack: ☐ Set ☐ Unset ☒ Don't care Psh: ☐ Set ☐ Unset ☒ Don't care Rst: ☐ Set ☐ Unset ☒ Don't care Syn: ☐ Set ☐ Unset ☒ Don't care Fin: ☐ Set ☐ Unset ☒ Don't care
ICMP Type	☒ Any ☐ Select Destination Unreachable ☐ Define (0 - 255)
ICMP Code	☒ Any ☐ Define (0 - 255)

Interface data are as follows.

Configuration Items	Description
No.	IPv6 ACL ranges from 1 to 2,147,483,647.
Action	ACL actions are divided into “Permit” or “Deny”, as well as “Shutdown”.
No.	MAC ACL ranges from 1 to 2,147,483,647.

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.
Service Type	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 Field	Enter the ICMP field value of ACL rules. Select “Any” to represent any field value.

3. “Apply” and finish as follows.

ACE Table

ACL Name

Showing entries Showing 1 to 1 of 1 entries

	Sequence	Action	Protocol	Source IP		Destination IP		Source Port	Destination Port	TCP Flags	Type of Service		ICMP	
				Address	Prefix	Address	Prefix				DSCP	IP Precedence	Type	Code
☐	100	Permit	Any (IP)	Any	Any	Any	Any				Any	Any		

7.2.4 ACL Binding Configuration

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

Instructions:

1. Click the “ACL > ACL Binding” in the navigation tree as follows.

ACL Binding Table

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

Interface data are as follows.

Configuration Items	Description
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)

- Fill in corresponding configuration items, taking the created MAC ACL a, IPv4 ACL b, IPv6 ACL c as examples.
- “Apply” and finish as follows.

Add ACL Binding

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

Apply Close

8 Advanced Configuration

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 rate of business flow in a given 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. Packet loss rate refers to the percentage of lost business flow during transmission. 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.

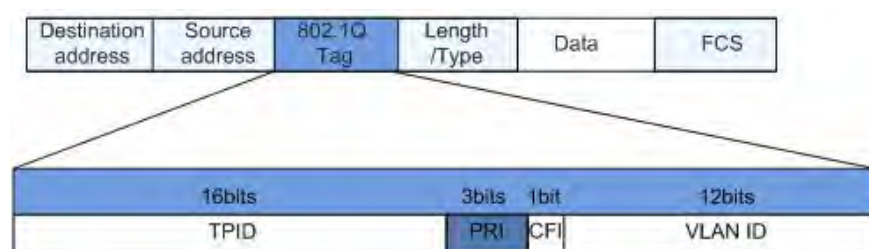
The ability to distinguish business types is the prerequisite to provide corresponding services, so the traditional best-effort service no longer meets the application needs. Therefore, QoS comes into being. It regulates the network flow to avoid and handle network congestion and reduce packet loss rate. 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

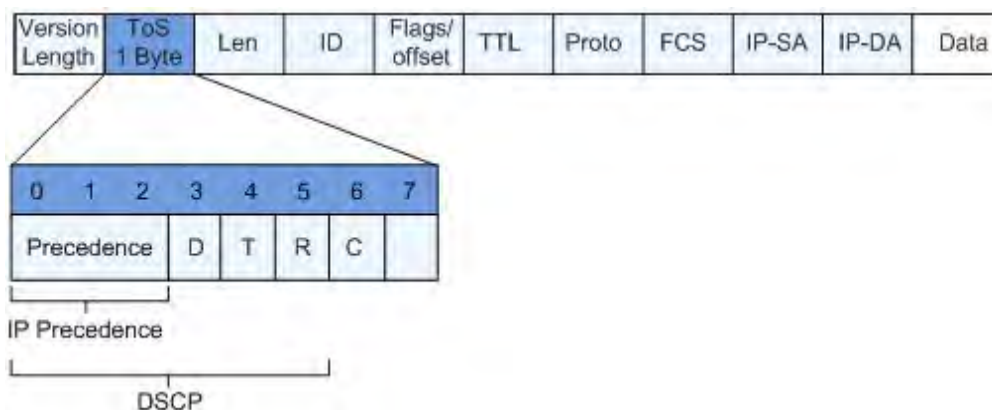


The 802.1Q header contains 3-bit PRI fields. PRI field defines 8 CoS of business priority ranging from 7 to 0 from high to low.

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.

8.1 QoS Configuration

8.1.1 Basic Configuration

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 > Basic Function > Function Configuration” in the navigation tree as follows.

State

☐ Enable

Trust Mode

☒ CoS
☐ DSCP
☐ CoS-DSCP
☐ IP Precedence

Apply

Port Setting Table

Q

	Entry	Port	CoS	Trust	Remarking		
					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

Interface data of global configuration are as follows.

Configuration Items	Description
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 Items	Description
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

8.1.2 Queue Scheduling

1. Click the “QoS > Queue Scheduling”. “Apply” and finish as follows.

Queue Scheduling Table

Queue	Method			
	Strict Priority	WRR	Weight	WRR Bandwidth (%)
1	☒	☐	1	
2	☒	☐	2	
3	☒	☐	3	
4	☒	☐	4	
5	☒	☐	5	
6	☒	☐	9	
7	☒	☐	13	
8	☒	☐	15	

Apply

Interface data are as follows.

Configuration Items	Description
SP	SP mode
WRR	WRR mode
Weight	Bandwidth percentage of WRR accounted for by Queue

8.1.3 CoS Mapping

1. Click the “QoS > CoS Mapping” in the navigation tree. “Apply” and finish as follows.

CoS to Queue Mapping

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

Apply

Queue to CoS Mapping

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

Apply

Interface data are as follows.

Configuration Items	Description
SP	SP mode
WRR	WRR mode
Weight	Bandwidth percentage of WRR accounted for by Queue

8.1.4 DSCP Mapping

1. Click the “QoS > Queue Scheduling”. “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] ▾

Apply

Interface data are as follows.

Configuration Items	Description
SP	SP mode
WRR	WRR mode
Weight	Bandwidth percentage of WRR accounted for by Queue

8.1.5 IP Priority Mapping

1. Click the “QoS > Basic Functions > 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	

Apply

Queue to IP Precedence Mapping

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

Apply

Interface data are as follows.

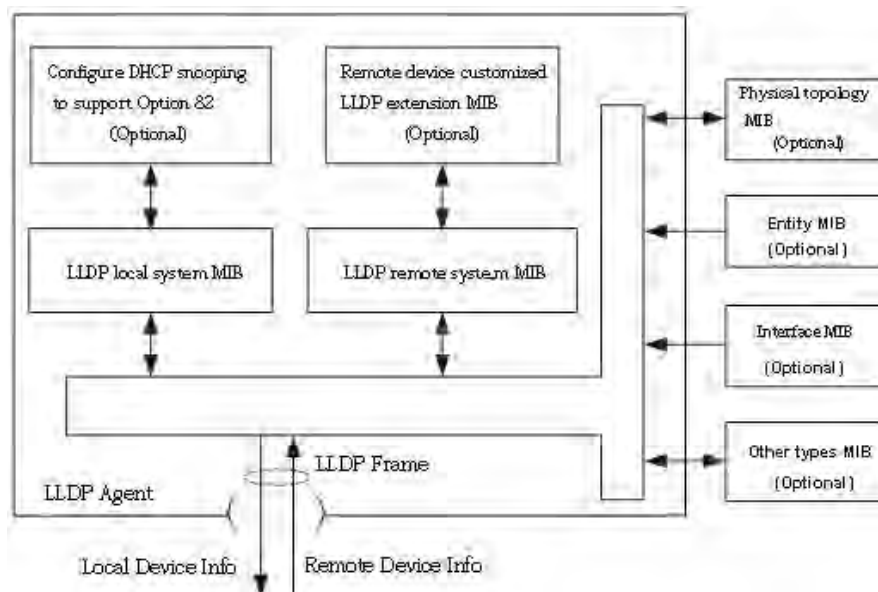
Configuration Items	Description
SP	SP mode
WRR	WRR mode
Weight	Bandwidth percentage of WRR accounted for by Queue

8.2 LLDP Configuration

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.

8.2.1 LLDP Function Configuration

Instructions:

1. Click the “Topology Discovery > LLDP > Function Configuration” in the navigation tree as follows.

LLDP	
State	☒ Enable
LLDP Handling	☐ Filtering ☐ Bridging ☒ Flooding
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)
LLDP-MED	
Fast Start Repeat Count	3 (1 - 10, default 3)

Apply

Interface data are as follows.

Configuration Items	Description
State	Enable or disable the LLDP
LLDP Message Processing	LLDP messages will be processed by means of “Filtering”, “Bridging” and “Flooding” when disabling the LLDP.
Transmission Period	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.
Delay Re-initialization	2s by default ranging from:1 to 10s.
Transfer Delay	2s by default ranging from:1 to 8,191s.
Repeat Count Quick Start	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.

8.2.2 Port Configuration

Instructions

1. Click the “Topology Discovery > LLDP > Port Configuration” in the navigation tree as follows.

Port Setting Table

Q

☐	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	Multiple ports are available.
Transmitting & Receiving Mode	LLDP transmitting & receiving mode
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 “Modify” the port configuration. “Apply” and finish as follows.

Edit Port Setting

Port

GE1

Mode

☐ Transmit
☐ Receive
☒ Normal
☐ Disable

Optional TLV

Available TLV

Port Description
System Name
System Description
System Capabilities
802.3 MAC-PHY

Selected TLV

802.1 PVID

802.1 VLAN Name

Available VLAN

VLAN 1

Selected VLAN

Apply

Close

Interface data are as follows.

Configuration Items	Description
Port	Multiple ports are available
Transmitting & Receiving Mode	LLDP transmitting & receiving mode. 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
VLAN Name	Select the VLAN name

8.2.3 Neighbor Info

Instructions for LLDP neighbor displaying

Click the “Topology Discovery > LLDP > Neighbor Info” in the navigation tree as follows.

Neighbor Table

Showing All entries Showing 1 to 1 of 1 entries

☐	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

First Previous 1 Next Last

Clear Refresh Detail

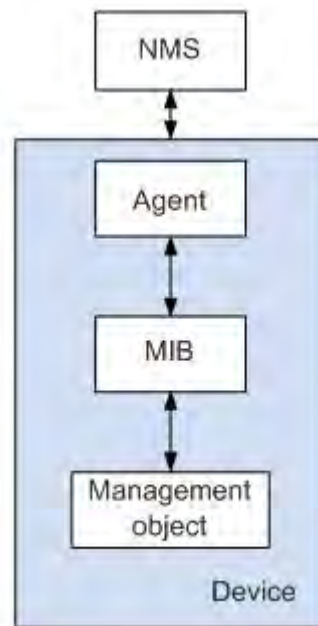
8.3 SNMP Configuration

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 statuses 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.

8.3.1 View Configuration

1. Click the “Device Management > SNMP Configuration > View Configuration” in the navigation tree as follows.

View Table

Showing entries Showing 1 to 1 of 1 entries

☐	View	OID Subtree	Type
☐	all	.1	Included

Interface data are as follows.

Configuration Items	Description
View	View name
OID	View OID
Type	View type: “Included” or “Excluded”

2. “Add” the corresponding configuration, “Apply” and finish.

Add View

View		Empty value is invalid.
OID Subtree		Empty value is invalid.
Type	☐ Included ☒ Excluded	

8.3.2 Group Configuration

1. Click the “Device Management > SNMP Configuration > Group Configuration” in the navigation tree as follows.

Group Table

Showing entries Showing 0 to 0 of 0 entries

☐	Group	Version	Security Level	View		
				Read	Write	Notify
0 results found.						

First Previous **1** Next Last

Configure [SNMP View](#) to associate a non-default view with a group.

Interface data are as follows.

Configuration Items	Description
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

Version

☒ SNMPv1
☐ SNMPv2
☐ SNMPv3

Security Level

☒ No Security
☐ Authentication
☐ Authentication and Privacy

View

☒ Read
☐ Write
☐ Notify

8.3.3 Group Configuration

1. Click the “Device Management > SNMP Configuration > Group Configuration” in the navigation tree as

follows.

Community Table

Showing entries

Showing 1 to 1 of 1 entries

☐	Community	Group	View	Access
☐	public		all	Read-Only

First Previous **1** Next Last

The access right of a community is defined by a group under advanced mode.
Configure [SNMP Group](#) to associate a group with a community.

Interface data are as follows.

Configuration Items	Description
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

Community

Type

☒ Basic
☐ Advanced

View

Access

☒ Read-Only
☐ Read-Write

Group

8.3.4 User Configuration

1. Click the “Device Management > SNMP Configuration > User Configuration” in the navigation tree as follows.

User Table

Showing All entries

Showing 0 to 0 of 0 entries



☐	User	Group	Security Level	Authentication Method	Privacy Method
0 results found.					

[First](#) [Previous](#) [1](#) [Next](#) [Last](#)

Configure [SNMP Group](#) to associate an SNMPv3 group with an SNMPv3 user.

[Add](#)

[Edit](#)

[Delete](#)

Interface data are as follows.

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

2. “Add” the corresponding configuration. “Apply” and finish.

Add User

User

Group

d

Security Level

☒ No Security
☐ Authentication
☐ Authentication and Privacy

Authentication

Method

☒ None
☐ MD5
☐ SHA

Password

Privacy

Method

☒ None
☐ DES

Password

Apply

Close

8.3.5 Engine ID Configuration

1. Click the “Device Management > SNMP Configuration > Engine ID Configuration” in the navigation tree as follows.

Local Engine ID

Engine ID

☐ User Defined

80006a92031c2aa3000024 (10 - 64 Hexadecimal Characters)

Apply

Remote Engine ID Table

Showing All entries Showing 0 to 0 of 0 entries

Server AddressEngine ID

0 results found.

AddEditDelete

FirstPrevious1NextLast

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

8.3.6 Trap Configuration

1. Click the “Device Management > SNMP Configuration > Trap Configuration” in the navigation tree as follows.

Authentication Failure

Link Up / Down

Cold Start

Warm Start

☒ Enable

☒ Enable

☒ Enable

☒ Enable

Apply

Interface data are as follows.

Configuration Items	Description
Authen Failure	Authentication error

Link Up/Down	Port link up/down
Cold start	Cold start
Warm start	Warm start

2. “Apply” and finish.

8.3.7 Notification Configuration

1. Click the “Device Management > SNMP Configuration > Notification Configuration” in the navigation tree as follows.

Notification Table

Showing entries Showing 0 to 0 of 0 entries

☐	Server Address	Server Port	Timeout	Retry	Version	Type	Community / User	Security Level
0 results found.								

For SNMPv1,2 Notification, [SNMP Community](#) needs to be defined.
For SNMPv3 Notification, [SNMP User](#) must be created.

First Previous 1 Next Last

Interface data are as follows.

Configuration Items	Description
Address Type	Address type: “Host Name”, “IPv4” or “IPv6”
Server Address	Server address info
Version	SNMP versions: v1, v2 and v3
Type	Notification type: “Trap” or “Inform”
Community/User	Community or username
Security Level	Security level
Server port No.	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.

Add Notification

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

8.4 RMON Configuration

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 are allowed to 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, so as to manage the network.

8.4.1 Port 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 “Device Management > RMON Configuration > Message Statistics” in the navigation tree as follows, which reveals the port-related message statistics.

Statistics Table

Refresh Rate 0 sec

Entry	Port	Bytes Received	Drop Events	Packets Received	Broadcast Packets	Multicast Packets	CRC & Align Errors	Undersize Packets	Oversize Packets	Fragments	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	GE1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
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
4	GE4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	GE5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	GE6	0	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

3. Select the specified refresh frequency to operate automatically.

8.4.2 History Configuration

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 “Device Management > RMON Configuration > History Configuration” in the navigation tree as follows.

History Table

Showing entries

Showing 0 to 0 of 0 entries

☐	Entry	Port	Interval	Owner	Sample	
					Maximum	Current

The SNMP service is currently disabled.
For RMON configuration to be effective, the [SNMP service](#) must be enabled.

Add

Edit

Delete

View

Interface data are as follows.

Configuration Items	Description
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

3. “Add” corresponding configuration items to configure history group.

Add History

Entry	1
Port	GE1
Max Sample	50 (1 - 50, default 50)
Interval	1800 (1 - 3600, default 1800)
Owner	

Apply Close

4. “Apply” and finish as follows.

History Table

Showing entries

Showing 1 to 1 of 1 er

☐	Entry	Port	Interval	Owner	Sample	
					Maximum	Current
☐	1	GE1	1800		50	50

The SNMP service is currently disabled.
For RMON configuration to be effective, the [SNMP service](#) must be enabled.

8.4.3 Event Configuration

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 “Device Management > RMON Configuration > Event Configuration” in the navigation tree as follows.

Event Table

Showing entries

Showing 0 to 0 of 0 entries

☐	Entry	Community	Description	Notification	Time	Owner
0 results found.						

The SNMP service is currently disabled.
For RMON configuration to be effective, the [SNMP service](#) must be enabled.

Interface data are as follows.

Configuration Items	Description
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

Showing All entries Showing 1 to 1 of 1 entries

☐	Entry	Community	Description	Notification	Time	Owner
☐	1	Default Community	Default Description	Event Log and Trap		

The SNMP service is currently disabled.
For RMON configuration to be effective, the [SNMP service](#) must be enabled.

8.4.4 Alarm Configuration

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. System will process as follows after a user defines the alarm entry: 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.

Click the “Device Management > RMON Configuration > Alarm Configuration” in the navigation tree as follows.

Alarm Table

Showing All entries Showing 0 to 0 of 0 entries

	Entry	Port	Counter		Sampling	Interval	Owner	Trigger	Rising		Falling	
			Name	Value					Threshold	Event	Threshold	Event
0 results found.												

[First](#)
[Previous](#)
[1](#)
[Next](#)
[Last](#)

The SNMP service is currently disabled.
For RMON configuration to be effective, the [SNMP service](#) must be enabled.

[Add](#)
[Edit](#)
[Delete](#)

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

Entry	1		
Port	GE1		
Counter	Drop Events		
Sampling	☒ Absolute ☐ Delta		
Interval	100	Sec (1 - 2147483647, default 100)	
Owner			
Trigger	☒ Rising ☐ Falling ☐ Rising and Falling		
Rising			
Threshold	100	(0 - 2147483647, default 100)	
Event	1 - Default Description		
Falling			
Threshold	20	(0 - 2147483647, default 20)	
Event	1 - Default Description		

3. “Apply” and finish as follows.

Alarm Table

Showing All entries Showing 1 to 1 of 1 entries

	Entry	Port	Counter		Sampling	Interval	Owner	Trigger	Rising		Falling	
			Name	Value					Threshold	Event	Threshold	Event
☐	1	GE1	DropEvents	0	Absolute	100		Rising	100	Default Description	20	Default Description

The SNMP service is currently disabled.
For RMON configuration to be effective, the **SNMP service** must be enabled.

8.5 DNS Configuration

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 Configuration > DNS Configuration” in the navigation tree as follows.

DNS Configuration

DNS Status	☐ Disable ☒ Enable
DNS Default Name	(1 to 255 alphanumeric characters)

Apply

DNS Server Configuration

Q

☐ Preference	DNS Server
0 results found.	

Add Delete

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.

Add DNS Server

IPv4/IPv6 Address	114.114.114.114
--------------------------	--

Apply Close

3. “Apply” and finish as follows.

Add DNS Server

IPv4/IPv6 Address	114.114.114.114
--------------------------	--

Apply Close

8.6 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 Configuration > System Time” in the navigation tree as follows.

Source

☐ SNTP
☐ From Computer
☒ Manual Time

Time Zone UTC +8:00 ▼

SNTP

Address Type ☒ Hostname ☐ IPv4

Server Address

Server Port 123 (1 - 65535, default 123)

Manual Time

Date 2020-01-01 YYYY-MM-DD

Time 08:50:59 HH:MM:SS

Daylight Saving Time

Type ☒ None ☐ Recurring ☐ Non-recurring ☐ USA ☐ European

Offset 60 Min (1 - 1440, default 60)

Recurring

From: Day Sun Week First Month Jan Time

To: Day Sun Week First Month Jan Time

Non-recurring

From: YYYY-MM-DD HH:MM

To: YYYY-MM-DD HH:MM

Operational Status

Current Time 2020-01-01 08:50:59 UTC+8

Apply

Interface data are as follows.

Configuration Items	Description
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: s/min/hr (with time source set in manual mode)
Type	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

9 DHCP

9.1 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.

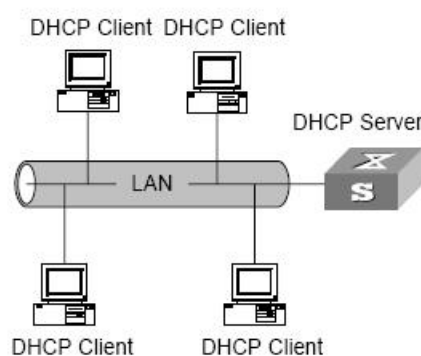


Figure 1-1. In a typical application of DHCP

9.2 IP address assignment of DHCP

9.2.1 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. The vast majority of clients get this dynamic address assignment.

9.2.2 Dynamic IP address acquisition process

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

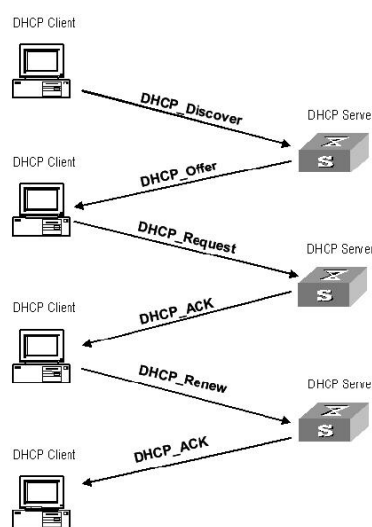


Figure 2-1. Interaction process

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.

9.3 DHCP global configuration

DHCP global and static binding configuration

1. Click the “DHCP > Property” in the navigation tree as follows.

The screenshot shows a configuration window with two sections. The first section, labeled "State", has a checkbox "Enable" which is unchecked. The second section, labeled "Static Binding First", also has a checkbox "Enable" which is unchecked. Below these sections is an "Apply" button.

DHCP Port Setting Table

The screenshot shows a table with 4 columns: Entry, Port, State, and an empty column. There are 6 rows of data. A search icon and a search input field are located above the table.

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

Port DHCP configuration

1. Click the “DHCP > Property”, and select the port and click “Edit” as follows.

Edit Port Setting

The screenshot shows a configuration window with two sections. The first section, labeled "Port", has a text field containing "GE1-GE2". The second section, labeled "State", has a checkbox "Enable" which is checked. Below these sections are "Apply" and "Close" buttons.

Notice:

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

9.4 IP Pool Setting

DHCP IP pool configuration

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

IP Pool Table

Showing All entries

Showing 0 to 0 of 0 entries



☐	Pool	Section			Gateway	Mask	DNS Primary Server	DNS Second Server	Lease time										
		Section	Start Address	End Address															
0 results found.																			
Add			Edit				Delete												
First			Previous				1				Next			Last					

IP Pool Table

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

Notice:

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

9.5 VLAN IF Address Group Setting

Server group configuration

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.

DHCP Server Group Table

Q

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

DHCP Server Group Table

DHCP Server Group

Group IP Address

VLAN interface and server group binding configuration

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.

Vlan Interface Address Pool Table

Interface

DHCP Server Group

9.6 Client List

Client list information

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

DHCP Client List

Showing entries

Showing 0 to 0 of 0 entries



☐	MAC Address Table	IPv4 Address	VLAN	Hostname
0 results found.				

First Previous **1** Next Last

Refresh

9.7 Client Static Binding Table

Static IP address assignment configuration

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

Static Binding Table

Showing entries

Showing 0 to 0 of 0 entries



☐	MAC Address Table	IPv4 Address	VLAN	User Name
0 results found.				

Add

Delete

First Previous **1** Next Last

Notice:

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

10 System Maintenance

10.1 Configuration Management

1. Click the “Device Management > Configuration Management > Upgrade/Backups” in the navigation tree as follows.

Action	☒ Upgrade ☐ Backup
Method	☐ TFTP ☒ HTTP
Configuration	☒ Running Configuration ☐ Startup Configuration ☐ Backup Configuration ☐ RAM Log ☐ Flash Log
Filename	浏览...

2. Instructions for configuration file 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	浏览...

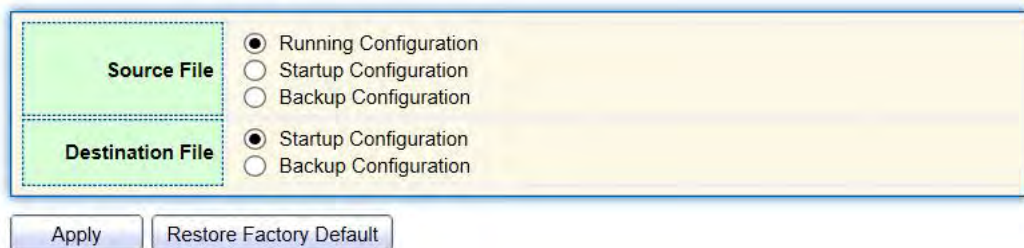
3. Instructions for file backup configuration: click the “Backup” in mode of “TFTP” or “HTTP”, select the files or logs to be upgraded (servers should be illustrated in TFTP mode). “Apply” and finish as follows.

Action	☐ Upgrade ☒ Backup
Method	☐ TFTP ☒ HTTP
Configuration	☐ Running Configuration ☐ Startup Configuration ☒ Backup Configuration ☐ RAM Log ☐ Flash Log

10.2 Configuration Saving

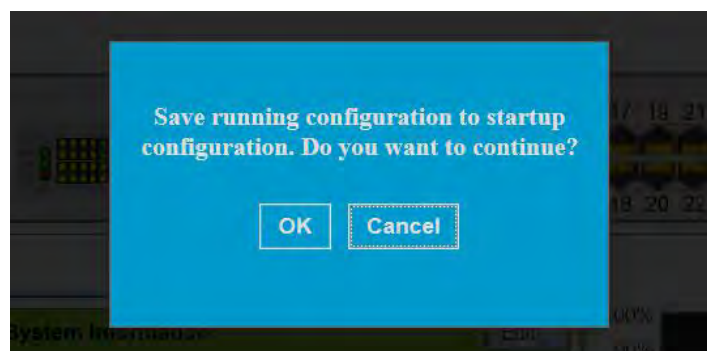
Instructions:

1. Click the “Device Management > Configuration Management > Configuration Saving” in the navigation tree, select the source and target files to be saved, “Apply” and finish. Click the “Factory Reset” as needed as follows:



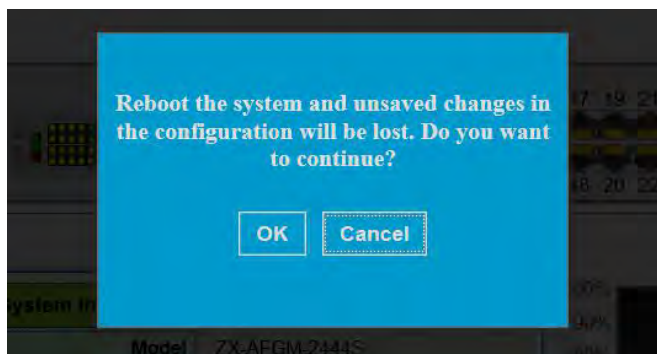
Note:

1. Click the “Factory Reset” and “Device Restart” to restore factory settings.
2. 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”).
3. Click the “Save” on the upper right to save the running configuration as the start configuration as follows.



10.3 Device Restart

Click the “Restart” on the upper right as guided as follows.



10.4 Firmware Management

Instructions:

1. Click the “Device Management > Firmware Management > Upgrade/Backups” in the navigation tree as follows.

Check the “Upgrade” in mode of “TFTP” or “HTTP” and select the system files (xx.bix) to be upgrade. “Apply” and finish as follows.

File Type	☒ Image ☐ FactoryFile
Action	☒ Upgrade
Method	☐ TFTP ☒ HTTP
Filename	选择文件 未选择任何文件