

Руководство по настройке линейки промышленных коммутаторов

Управление через WEB-интерфейс

История изменений

Revision	Release Date	Summary
1.0	2024-07	First release

Содержание

1. Вход в систему Web Manager	Ошибка! Закладка не определена.
2. Введение	6
3. Состояние	7
3.1. Информация о системе	7
3.2. Сообщения	10
3.3. Порт	11
3.3.1. Статистика	11
3.3.2. Error Disabled	13
3.3.3. Bandwidth Utilization	15
3.4. Link Aggregation	15
3.5. MAC Address Table	17
4. Сеть	18
4.1. DNS 18	
4.2. HOSTS	19
4.3. System Time	19
4.4. Configuration Case	22
5. Порты	22
5.1. Port Setting	23
5.2. Error Disabled	25
5.3. Link Aggregation	26
5.3.1. Group	26
5.3.2. Port Setting	29
5.3.3. LACP	31
5.4. EEE 33	
5.5. Jumbo Frame	35
5.6. Port Security	35
5.7. Protected Port	36
5.8. Storm Control	37
5.9. Пример конфигурации	40
6. PoE	43
6.1. PoE настройки	44
6.2. Настройка таймера порта POE	44
6.3. Пример конфигурации	44
7. VLAN	45
7.1. VLAN	45
7.1.1. Создание VLAN	45
7.1.2. Конфигурация VLAN	46
7.1.3. Membership	47
7.1.4. Port Setting	50
7.2. Voice VLAN	52
7.2.1. Property	52
7.2.2. Voice OUI	54
7.3. Protocol VLAN	55
7.3.1. Protocol Group	55
7.3.2. Group Binding	57
7.4. MAC VLAN	59
7.4.1. MAC Group	59
7.4.2. Group Binding	61
7.5. Surveillance VLAN	62
7.5.1. Property	62
7.5.2. Surveillance OUI	66
7.6. GVRP	66
7.6.1. Property	67
7.6.2. Membership	69
7.6.3. Statistics	69
7.7. Пример конфигурации	72

8. MAC Address Table.....	78
8.1. Dynamic Address.....	78
8.2. Static Address.....	78
8.3. Filtering Address	79
8.4. Пример конфигурации.....	79
9. STP	81
9.1. Property	81
9.2. Port Setting	83
9.3. MST Instance.....	86
9.4. MST Port Setting	89
9.5. Statistics	91
9.6. Пример конфигурации	93
10. ERPS	95
10.1. Function configuration.....	96
10.2. Examples of ERPS	97
10.3. Example of configuration	97
11. Discovery	101
11.1. LLDP.....	101
11.1.1. Property	101
11.1.2. Port Setting	103
11.1.3. MED Network Policy.....	105
11.1.4. MED Port Setting.....	107
11.1.5. Packet View	109
11.1.6. Local Information	111
11.1.7. Neighbor.....	114
11.1.8. Statistics	114
11.2. Пример конфигурации.....	116
12. DHCP	122
12.1. Function configuration.....	122
12.2. Address pool configuration.....	123
12.3. VLAN interface address group configuration	123
12.4. Client list	124
12.5. Client Static Binding Table	124
12.6. Пример конфигурации	124
13. Multicast	126
13.1. General.....	127
13.1.1. Property	127
13.1.2. Group Address.....	128
13.1.3. Router Port.....	130
13.1.4. Forward All	133
13.1.5. Throttling.....	136
13.1.6. Filtering Profile	138
13.1.7. Filtering Binding	140
13.2. Igmp Snooping	142
13.2.1. Property	142
13.2.2. Querier	145
13.2.3. Statistics	147
13.3. MLD Snooping	148
13.3.1. Property	148
13.3.2. Statistics	152
13.4. MVR.....	153
13.4.1. Property	153
13.4.2. Port Setting	154
13.4.3. Group Address.....	156
13.5. Пример конфигурации.....	158
14. Routing.....	160
14.1. IPv4 Management and Interfaces	160
14.1.1. IPv4 Interface	160
14.1.2. IPv4 Routes.....	161
14.1.3. ARP.....	162
14.2. IPv6 Management and Interfaces	163
14.2.1. IPv6 Interface	163
14.2.2. IPv6 Addresses	164
14.2.3. IPv6 Routes.....	165
14.2.4. IPv6 Neighbors	166

14.3. Пример конфигурации	167
15. Security	169
15.1. RADIUS	170
15.2. TACACS+	172
15.3. AAA.....	175
15.3.1. Method List	175
15.3.2. Login Authentication	178
15.4. Management Access	179
15.4.1. Management Service.....	179
15.4.2. Management ACL.....	180
15.4.3. Management ACE.....	181
15.5. Authentication Manager	183
15.5.1. Property	183
15.5.2. Port Setting	189
15.5.3. MAC-Based Local Account.....	193
15.5.4. WEB-Based Local Account.....	195
15.5.5. Sessions	197
15.6. DoS	198
15.6.1. Property	199
15.6.2. Port Setting	200
15.7. Dynamic ARP Inspection	201
15.7.1. Property	201
15.7.2. Statistics	204
15.8. DHCP Snooping	205
15.8.1. Property	205
15.8.2. Statistics	207
15.8.3. Option82 Property.....	208
15.8.4. Option82 Circuit ID.....	209
15.9. IP Source Guard.....	210
15.9.1. Port Setting	210
15.9.2. IMPV Binding.....	212
15.9.3. Save Database	213
15.10. Пример конфигурации	214
16. ACL	217
16.1. MAC ACL.....	217
16.2. MAC ACE	218
16.3. IPv4 ACL.....	222
16.4. IPv4 ACE	223
16.5. IPv6 ACL.....	228
16.6. IPv6 ACE	229
16.7. ACL Binding	220
16.8. Пример конфигурации	221
17. QoS.....	223
17.1. General.....	223
17.1.1. Property	223
17.1.2. Queue Scheduling	226
17.1.3. CoS Mapping	227
17.1.4. DSCP Mapping.....	229
17.1.5. IP Precedence Mapping.....	230
17.2. Rate Limit	231
17.2.1. Ingress / Egress Port.....	231
17.2.2. Egress Queue.....	233
17.3. Configuration Case	237
18. Diagnostics	237
18.1. Logging	238
18.1.1. Property	238
18.1.2. Remove Server	239
18.2. Mirroring	240
18.3. Ping	241
18.4. Traceroute.....	241
18.5. Copper Test.....	242
18.6. Fiber Module.....	243
18.7. UDLD	246
18.7.1. Property	246
18.7.2. Neighbor.....	248
18.8. Configuration Case	249

19. Management	250
19.1. User Account	250
19.2. Firmware	252
19.2.1. Upgrade / Backup	252
19.2.2. Active Image	255
19.3. Configuration	256
19.3.1. Upgrade / Backup	256
19.3.2. Save Configuration	261
19.4. SNMP	262
19.4.1. View	262
19.4.2. Group	262
19.4.3. Community	266
19.4.4. User	268
19.4.5. Engine ID	272
19.4.6. Trap Event	274
19.4.7. Notification	275
19.4.8. Configuration Case	279
19.5. RMON	280
19.5.1. Statistics	280
19.5.2. History	282
19.5.3. Event	286
19.5.4. Alarm	289
19.5.5. Configuration Case	295

1. Вход в систему Web Manager.

Enter the IP address of the device in the browser (installed on your computer) to manage the switch. The URL format in the address bar is:

http://xxx.xxx.xxx. The xxx, where xxx represents the IP address of the switch.



Note: The default factory IP address is 192.168.0.1.

The user authentication window of the management module is popup, as shown below.

The image shows a dark blue background with a white login form. The form contains two input fields: 'Username:' and 'Password:'. Below these fields is a blue button labeled 'Login'.

Web Login

User name is admin, Password is admin, and click Login to open the Web-based user interface.

2. Introduction

managed switch software provides rich functionality for switches in your networks. This guide describes how to use Web-based management interface (Web UI) to configure managed switch software features.

The Web UI supports all frequently used web browsers listed below:

- Internet Explorer 8 and above
- Firefox 20.0 and above
- Chrome 23.0 and above

- Safari 5.1.7 and above

In the Web UI, the left column shows the configuration menu. The top row shows the switch's current link status. Green squares indicate the port link is up, while black squares indicate the port link is down. Below the switch panel, you can find a common toolbar to provide useful functions for users. The rest of the screen area displays the configuration settings.

The screenshot displays the 'Status >> System Information' page in the Web UI. On the left is a sidebar menu with categories like Status, Network, Port, and Management. The top right of the page has buttons for 'Save', 'Logout', 'Reboot', and 'Debug'. The main area shows a port status panel with 48 ports (1-48) and 3 additional ports (49-51). Below this is a 'System Information' table with fields like Model, System Name, System Location, System Contact, Serial Number, MAC Address, IPv4 Address, IPv6 Address, and System OID. To the right of the table is a CPU utilization graph showing usage over time from 08:23:00 to 08:26:00.

System Information	
Model	RTL9311
System Name	Switch
System Location	Default
System Contact	Default
Serial Number	
MAC Address	82:24:02:19:00:01
IPv4 Address	192.168.0.1
IPv6 Address	fe80::8224:2ff:fe19:1/64 fe80::8024:2ff:fe19:1/64
System OID	1.3.6.1.4.1.27282.1.3

Web User Interface

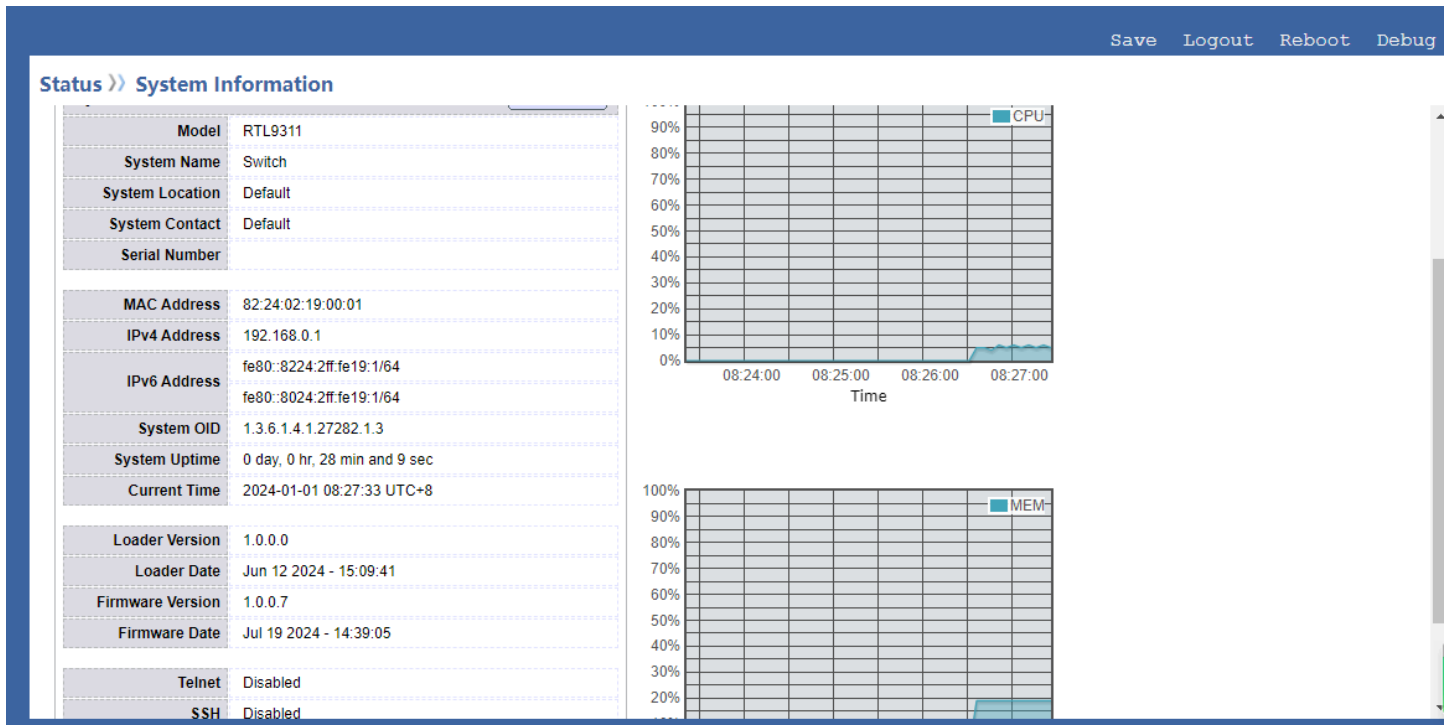
3. Status

Use the Status pages to view system information and status.

1.1. System Information

To display System Information web page, click **Status > System Information**

This page shows switch panel, CPU utilization, Memory utilization and other system current information. It also allows user to edit some system information.



System Information Page

Field	Description
Model	Model name of the switch
System Name	System name of the switch. This name will also use as CLI prefix of each line. ("Switch>" or "Switch#")
System Location	Location information of the switch
System Contact	Contact information of the switch
MAC Address	Base MAC address of the switch
IPv4 Address	Current system IPv4 address
IPv6 Address	Current system IPv6 address
System OID	SNMP system object ID
System Uptime	Total elapsed time from booting
Current Time	Current system time
Loader Version	Boot loader image version
Loader Date	Boot loader image build date

Firmware Version	Current running firmware image version
Firmware Date	Current running firmware image build date
Telnet	Current Telnet service enable/disable state
SSH	Current SSH service enable/disable state
HTTP	Current HTTP service enable/disable state
HTTPS	Current HTTPS service enable/disable state
SNMP	Current SNMP service enable/disable state

Current System Information

Click “Edit” button on the table title to edit following system information.

Status >> System Information

Edit System Information

System Name	Switch
System Location	Default
System Contact	Default

Edit System Information dialog

Field	Description
System Name	System name of the switch. This name will also use as CLI prefix of each line. ("Switch>" or "Switch#")
System Location	Location information of the switch
System Contact	Contact information of the switch

System Information Fields

1.2. Logging Message

To view the logging messages stored on the RAM and Flash, click **Status > Logging Message**.

Status >> Logging Message

Logging Message Table

Viewing RAM

Showing All entries

Showing 1 to 11 of 11 entries

Log ID	Time	Severity	Description
1	Jan 01 2024 08:26:34	notice	AAA-0-CONNECT: New http connection for user admin, source 192.168.0.111 ACCEPTED
2	Jan 01 2024 08:25:41	notice	AAA-5-DISCONNECT: http connection for user (null), source 192.168.0.111 TERMINATED
3	Jan 01 2024 08:09:59	notice	PORT-5-LINK_UP: Interface VLAN1 link up
4	Jan 01 2024 08:09:59	notice	PORT-5-LINK_UP: Interface GigabitEthernet47 link up
5	Jan 01 2024 08:02:38	notice	PORT-5-LINK_DOWN: Interface VLAN1 link down
6	Jan 01 2024 08:02:38	notice	PORT-5-LINK_DOWN: Interface GigabitEthernet47 link down
7	Jan 01 2024 08:01:44	notice	AAA-5-CONNECT: New http connection for user admin, source 192.168.0.111 ACCEPTED
8	Jan 01 2024 08:00:53	notice	AAA-5-CONNECT: New http connection for user admin, source 192.168.0.111 ACCEPTED
9	Jan 01 2024 08:00:12	notice	PORT-5-LINK_UP: Interface VLAN1 link up
10	Jan 01 2024 08:00:12	notice	PORT-5-LINK_UP: Interface GigabitEthernet47 link up
11	Jan 01 2024 00:00:09	notice	SYSTEM-5-WARMSTART: Warm startup

Clear

Refresh

First

Previous

1

Next

Last

Logging Message page

Field	Description
Log ID	The log identifier.
Time	The time stamp for the logging message.
Severity	The severity for the logging message.
Description	The description of logging message.

Logging Message fields.

Field	Description
Viewing	The logging view including: - RAM: Show the logging messages stored on the RAM. - Flash: Show the logging messages stored on the Flash.
Clear	Clear the logging messages.
Refresh	Refresh the logging messages.

Logging Message buttons.

1.3.Port

The Port configuration page displays port summary and status information.

1.3.1. Statistics

To display Port Counters web page, click **Status > Port > Statistics**

This page displays standard counters on network traffic from the Interfaces, Ethernet-like and RMON MIB. Interfaces and Ethernet-like counters display errors on the traffic passing through each port. RMON counters provide a total count of different frame types and sizes passing through each port. The “Clear” button will clear MIB counter of current selected port.

Status >> Port >> Statistics

Port	GE1 ▼
MIB Counter	☒ All ☐ Interface ☐ Etherlike ☐ RMON
Refresh Rate	☐ None ☐ 5 sec ☒ 10 sec ☐ 30 sec

Interface	
ifInOctets	0
ifInUcastPkts	0
ifInNUcastPkts	0
ifInDiscards	0

Interface	
ifInOctets	0
ifInUcastPkts	0
ifInNUcastPkts	0
ifInDiscards	0
ifOutOctets	0
ifOutUcastPkts	0
ifOutNUcastPkts	0
ifOutDiscards	0
ifInMulticastPkts	0
ifInBroadcastPkts	0
ifOutMulticastPkts	0
ifOutBroadcastPkts	0

Etherlike	
dot3StatsAlignmentErrors	0
dot3StatsFCSErrors	0
dot3StatsSingleCollisionFrames	0
dot3StatsMultipleCollisionFrames	0
dot3StatsDeferredTransmissions	0
dot3StatsLateCollisions	0
dot3StatsExcessiveCollisions	0
dot3StatsFrameTooLongs	0
dot3StatsSymbolErrors	0
dot3ControlInUnknownOpCodes	0
dot3InPauseFrames	0
dot3OutPauseFrames	0

RMON	
etherStatsDropEvents	0
etherStatsOctets	0
etherStatsPkts	0
etherStatsBroadcastPkts	0
etherStatsMulticastPkts	0
etherStatsCRCAlignErrors	0
etherStatsUnderSizePkts	0
etherStatsOverSizePkts	0
etherStatsFragments	0
etherStatsJabbers	0
etherStatsCollisions	0
etherStatsPkts64Octets	0
etherStatsPkts65to127Octets	0
etherStatsPkts128to255Octets	0
etherStatsPkts256to511Octets	0
etherStatsPkts512to1023Octets	0
etherStatsPkts1024to1518Octets	0

Port Counters Page

Field	Description
Port	Select one port to show counter statistics.
MIB Counter	Select the MIB counter to show different counter type • All: All counters. • Interface: Interface related MIB counters • Etherlike: Ethernet-like related MIB counters • RMON: RMON related MIB counters
Refresh Rate	Refresh the web page every period of seconds to get new counter of specified port

Port Counters Fields

1.3.2. Error Disabled

To display the status of port error disabled, click **Status > Port > Error Disabled**.

Status >> Port >> Error Disabled

Error Disabled Table

☐	Port	Reason	Time Left (sec)
☐	GE1	---	---
☐	GE2	---	---
☐	GE3	---	---
☐	GE4	---	---
☐	GE5	---	---
☐	GE6	---	---
☐	GE7	---	---
☐	GE8	---	---
☐	GE9	---	---
☐	GE10	---	---
☐	GE11	---	---
☐	GE12	---	---
☐	GE13	---	---
☐	GE14	---	---
☐	GE15	---	---
☐	GE16	---	---
☐	GE17	---	---

Error Disabled Status page.

Field	Description
Port	Interface or port number.
Reason	Port will be disabled by one of the following error reason: BPDU Guard UDLD Self Loop Broadcast Flood Unknown Multicast Flood Unicast Flood ACL Port Security Violation DHCP rate limit

	ARP rate limit
Time Left (sec)	The time left in second for the error recovery.

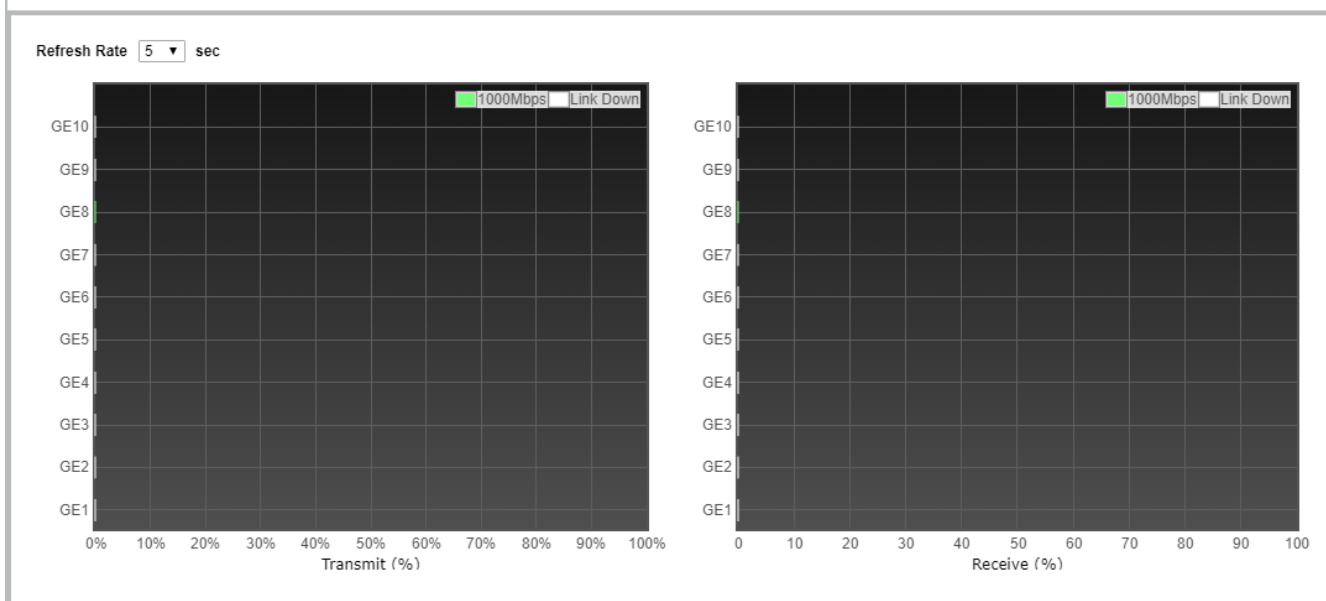
Error Disabled Status fields.

1.3.3. Bandwidth Utilization

To display Bandwidth Utilization web page, click **Status > Port > Bandwidth Utilization**

This page allow user to browse ports' bandwidth utilization in real time. This page will refresh automatically in every refresh period.

Status >> Port >> Bandwidth Utilization



Port Bandwidth Utilization Page

Field	Description
Refresh Rate	Refresh the web page every period of seconds to get new bandwidth utilization data

Bandwidth Utilization Fields

1.4. Link Aggregation

To display Link Aggregation status web page, click **Status > Link Aggregation**.

Status >> Link Aggregation

Link Aggregation Table

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		---	---			

Link Aggregation Status Page

Field	Description
LAG	LAG Name
Name	LAG port description
Type	The type of the LAG Static: The group of ports assigned to a static LAG are always active members. LACP: The group of ports assigned to dynamic LAG are candidate ports. LACP determines which candidate ports are active member ports.
Link Status	LAG port link status
Active Member	Active member ports of the LAG
Inactive Member	Inactive member ports of the LAG

LAG Status Fields

1.5.MAC Address Table

To display MAC Address Table status web page, click **Status > MAC Address Table**.

The MAC address table page displays all MAC address entries on the switch including static MAC address created by administrator or auto learned from hardware. The “Clear” button will clear all dynamic entries and “Refresh” button will retrieve latest MAC address entries and show them on page.

Status >> MAC Address Table

MAC Address Table

Showing

All

 entries

Showing 1 to 2 of 2 entries

VLAN	MAC Address	Type	Port
1	82:24:02:19:00:01	Management	CPU
1	68:F7:28:A1:B8:A0	Dynamic	GE47

Clear

Refresh

First

Previous

1

Next

Last

MAC Address Status Page

Field	Description
VLAN	VLAN ID of the mac address
MAC Address	MAC address

Type	The type of MAC address Management: DUT's base mac address for management purpose Static: Manually configured by administrator Dynamic: Auto learned by hardware
Port	The type of Port CPU: DUT's CPU port for management purpose Other: Normal switch port

MAC Address Status Fields

2. Network

Use the Network pages to configure settings for the switch network interface and how the switch connects to a remote server to get services.

2.1.DNS

To configure the Switch IP/IPv6 address and DNS configuration, click **Network** > DNS.

Network >> DNS

DNS Configuration

DNS Status

☐ Disable
☒ Enable

DNS Default Name

(1 to 255 alphanumeric characters)

Apply

DNS Server Configuration

☐ Preference ☒ DNS Server

0 results found.

Add Delete

DNS page.

Field	Description
DNS Status	Disable enable
DNS Default	(1 to 255 alphanumeric characters)
DNS Server Configuration	IPv4/IPv6 Address

DNS Fields.

2.2.HOSTS

To configure the Switch IP/IPv6 address and DNS configuration, click **Network > Hosts**.

Network >> Hosts

DNS Host Configuration

Q

☐	Host	IPv4/IPv6 Address
0 results found.		

Add Delete

Dynamic Host Mapping

Q

Host	Total	Elapsed	Type	IPv4/IPv6 Address
0 results found.				

Clear

DNS Host Configuration page.

Field	Description
DNS Host Configuration	Host--(1 to 255 alphanumeric characters) IPv4/IPv6 Address
DNS Default	(1 to 255 alphanumeric characters)
Dynamic Host Mapping	Show dynamic host

Hosts Fields.

2.3.System Time

To display System Time page, click **Network > System Time**

This page allow user to set time source, static time, time zone and daylight saving settings. Time zone and daylight saving takes effect both static time or time from SNTP server.

Network >> System Time

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	2024-01-01 YYYY-MM-DD
Time	09:01:12 HH:MM:SS

Daylight Saving Time	
Type	☒ None ☐ Recurring ☐ Non-recurring ☐ USA ☐ European

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	2024-01-01 09:01:12 UTC+8

System Time Page

Field	Description
-------	-------------

Source	Select the time source. SNTP: Time sync from NTP server. From Computer: Time set from browser host. Manual Time: Time set by manually configure.
Time Zone	Select a time zone difference from listing district.
SNTP	Description
Address Type	Select the address type of NTP server. This is enabled when time source is SNTP.
Server Address	Input IPv4 address or hostname for NTP server. This is enabled when time source is SNTP.
Server Port	Input NTP port for NTP server. Default is 123. This is enabled when time source is SNTP.
Manual Time	Description
Date	Input manual date. This is enabled when time source is manual.
Time	Input manual time. This is enabled when time source is manual.
Daylight Saving Time	Description
Type	Select the mode of daylight saving time. Disable: Disable daylight saving time. Recurring: Using recurring mode of daylight saving time. Non-Recurring: Using non-recurring mode of daylight saving time. USA: Using daylight saving time in the United States that starts on the second Sunday of March and ends on the first Sunday of November. European: Using daylight saving time in the Europe that starts on the last Sunday in March and ending on the last Sunday in October.
Offset	Specify the adjust offset of daylight saving time.
Recurring From	Specify the starting time of recurring daylight saving time. This field available when selecting "Recurring" mode.
Recurring To	Specify the ending time of recurring daylight saving time. This field available when selecting "Recurring" mode.
Non-recurring From	Specify the starting time of non-recurring daylight saving time. This field available when selecting "Non-Recurring" mode.

Non-recurring To	Specify the ending time of recurring daylight saving time. This field available when selecting “Non-Recurring” mode.
------------------	--

System Time Fields

2.4.Configuration Case

Case requirement: Configure the local NTP server time of the switch

- Web

Network >> System Time

Source	☒ SNTP ☐ From Computer ☐ Manual Time
Time Zone	UTC +8:00

SNTP

Address Type	☐ Hostname ☒ IPv4
Server Address	192.168.0.111
Server Port	123 (1 - 65535, default 123)

Manual Time

Date	2024-01-01	YYYY-MM-DD
Time	08:32:03	HH:MM:SS

- CLI

Configure SNTP service functionality

```
switch #config
switch(config)# clock source sntp
switch(config)# sntp host 192.168.0.111 port 123
switch(config)# clock timezone "1" 8 minutes 0
```

Check the switch clock time

```
switch(config)# show clock
2024-02-01 13:24:49 1(UTC+8)
Time source is sntp
```

3. Port

Use the Port pages to configure settings for switch port related features

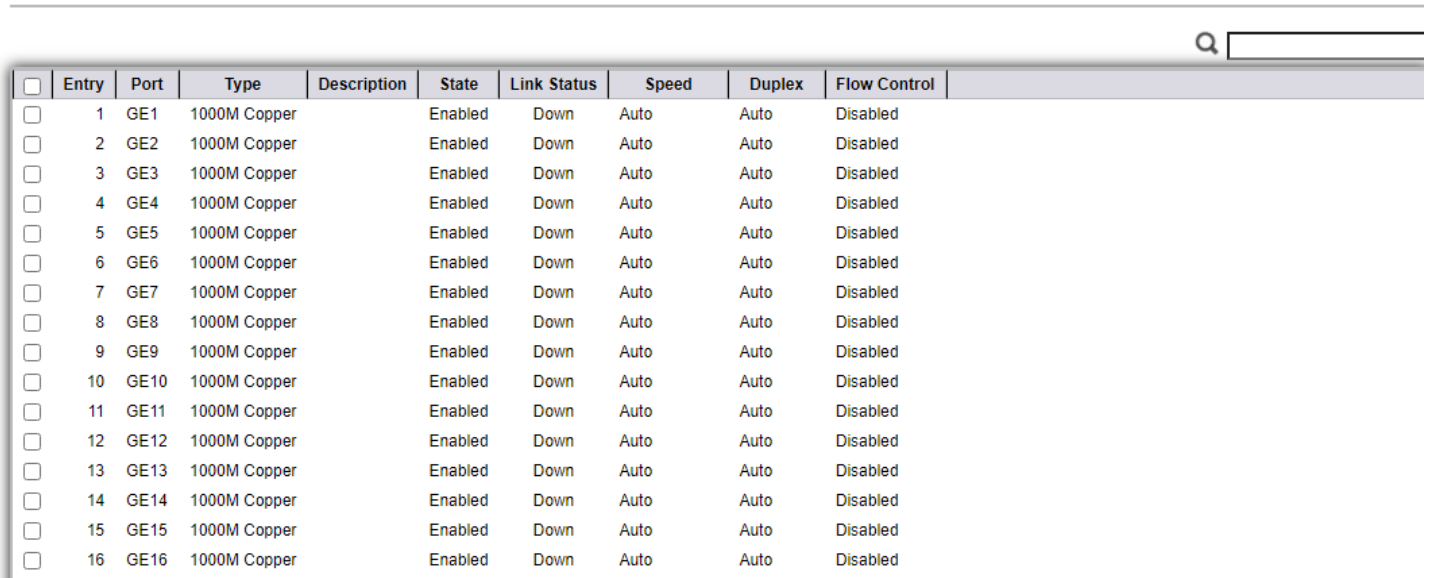
3.1.Port Setting

To display Port Setting web page, click **Port > Port Setting**

This page shows port current status and allow user to edit port configurations. Select port entry and click “Edit” button to edit port configurations.

[Port >> Port Setting](#)

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	Down	Auto	Auto	Disabled
☐	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	Down	Auto	Auto	Disabled
☐	11	GE11	1000M Copper	Enabled	Down	Auto	Auto	Disabled
☐	12	GE12	1000M Copper	Enabled	Down	Auto	Auto	Disabled
☐	13	GE13	1000M Copper	Enabled	Down	Auto	Auto	Disabled
☐	14	GE14	1000M Copper	Enabled	Down	Auto	Auto	Disabled
☐	15	GE15	1000M Copper	Enabled	Down	Auto	Auto	Disabled
☐	16	GE16	1000M Copper	Enabled	Down	Auto	Auto	Disabled

Port Setting Table

Field	Description
Port	Port Name
Type	Port media type
Description	Port description
State	Port admin state. Enabled: Enable the port. Disabled: Disable the port.
Link Status	Current port link status Up: Port is link up Down: Port is link down
Speed	Current port speed configuration and link speed status
Duplex	Current port duplex configuration and link duplex status
Flow Control	Current port flow control configuration and link flow control status

Port Setting Table Fields

Port >> Port Setting

Edit Port Setting

Port	GE7-GE10
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

Apply Close

Edit Port Setting Dialog

Field	Description
Port	Selected port list
Description	Port description
State	Port admin state. Enabled: Enable the port. Disabled: Disable the port.
Speed	Port speed capabilities. Auto: Auto speed with all capabilities Auto-10M: Auto speed with 10M ability only Auto-100M: Auto speed with 100M ability only Auto-1000M: Auto speed with 1000M ability only Auto-10M/100M: Auto speed with 10M/100M abilities 10M: Force speed with 10M ability 100M: Force speed with 100M ability

	1000M: Force speed with 1000M ability
Duplex	Port duplex capabilities. Auto: Auto duplex with all capabilities Half: Auto speed with 10M and 100M ability only Full: Auto speed with 10M/100M/1000M ability only
Flow Control	Port flow control. Auto: Auto flow control by negotiation. Enabled: Enable flow control ability. Disabled: Disable flow control ability.

Edit Port Setting Fields

3.2. Error Disabled

To display Error Disabled web page, click **Port > Error Disabled**.

Port >> Error Disabled

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

Error Disabled Page

Field	Description
-------	-------------

Recover Interval	Auto recovery after this interval for error disabled port.
BPDU Guard	Enabled to auto shutdown port when BPDU Guard reason occur. This reason caused by STP BPDU Guard mechanism.
UDLD	Enabled to auto shutdown port when UDLD violation occur.
Self Loop	Enabled to auto shutdown port when Self Loop reason occur.
Broadcast Flood	Enabled to auto shutdown port when Broadcast Flood reason occur. This reason caused by broadcast rate exceed broadcast storm control rate.
Unknown Multicast Flood	Enabled to auto shutdown port when Unknown Multicast Flood reason occur. This reason caused by unknown multicast rate exceed unknown multicast storm control rate.
Unicast Flood	Enabled to auto shutdown port when Unicast Flood reason occur. This reason caused by unicast rate exceed unicast storm control rate.
ACL	Enabled to auto shutdown port when ACL shutdown port reason occur. This reason caused packet match the ACL shutdown port action.
Port Security	Enabled to auto shutdown port when Port Security Violation reason occur. This reason caused by violation port security rules.
DHCP rate limit	Enabled to auto shutdown port when DHCP rate limit reason occur. This reason caused by DHCP packet rate exceed DHCP rate limit.
ARP rate limit	Enabled to auto shutdown port when ARP rate limit reason occur. This reason caused by DHCP packet rate exceed ARP rate limit.

Error Disabled Fields

3.3. Link Aggregation

3.3.1. Group

To display LAG Setting web page, click **Port > Link Aggregation > Group**.

This page allow user to configure link aggregation group load balance algorithm and group member.

Port >> Link Aggregation >> Group

Load Balance Algorithm

☒ MAC Address
☐ IP-MAC Address
☐ Dst-MAC Address
☐ Src-MAC Address
☐ Dst-IP Address
☐ Src-IP Address

Apply

LAG Global Setting

Field	Description
Load Balance Algorithm	LAG load balance distribution algorithm MAC Address :Based on MAC address IP-MAC Address:Based on MAC address and IP address Dst-MAC Address:Based on Dst-MAC address Src-MAC Address:Based on Src-MAC address Dst-IP Address:Based on Dst-IP address Src-IP Address:Based on Src-IP address

LAG Global Setting Fields

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

LAG Group Setting Table

Field	Description
-------	-------------

LAG	LAG Name
Name	LAG port description
Type	The type of the LAG Static: The group of ports assigned to a static LAG are always active members. LACP: The group of ports assigned to dynamic LAG are candidate ports. LACP determines which candidate ports are active member ports.
Link Status	LAG port link status
Active Member	Active member ports of the LAG
Inactive Member	Inactive member ports of the LAG

LAG Group Setting Fields

Port >> Link Aggregation >> Group

Edit Link Aggregation Group

Edit LAG Group Setting Dialog

Field	Description
LAG	Selected LAG group ID
Name	LAG port description

Type	The type of the LAG Static: The group of ports assigned to a static LAG are always active members. LACP: The group of ports assigned to dynamic LAG are candidate ports. LACP determines which candidate ports are active member ports.
Member	Select available port to be LAG group member port

Edit LAG Group Setting Field

3.3.2. Port Setting

To display LAG Port Setting web page, click **Port > Link Aggregation > Port Setting**.

This page shows LAG port current status and allow user to edit LAG port configurations. Select LAG entry and click “Edit” button to edit LAG port configurations.

Port >> Link Aggregation >> Port Setting

Port Setting Table

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

Edit

LAG Port Setting Table

Field	Description
LAG	LAG Port Name
Type	LAG Port media type
Description	LAG Port description
State	LAG Port admin state. Enabled: Enable the port. Disabled: Disable the port.
Link Status	Current LAG port link status Up: Port is link up Down: Port is link down
Speed	Current LAG port speed configuration and link speed status
Duplex	Current LAG port duplex configuration and link duplex status
Flow Control	Current LAG port flow control configuration and link flow control status

Port Setting Status Fields

Port >> Link Aggregation >> Port Setting

Port Setting Table

Q

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

Edit

Edit LAG Port Setting Dialog

Field	Description
Port	Selected port list
Description	Port description
State	Port admin state. Enable: Enable the port. Disable: Disable the port.
Speed	Port speed capabilities. Auto: Auto speed with all capabilities Auto-10M: Auto speed with 10M ability only Auto-100M: Auto speed with 100M ability only Auto-1000M: Auto speed with 1000M ability only Auto-10M/100M: Auto speed with 10M/100M abilities 10M: Force speed with 10M ability 100M: Force speed with 100M ability 1000M: Force speed with 1000M ability
Flow Control	Port flow control. Auto: Auto flow control by negotiation. Enabled: Enable flow control ability. Disabled: Disable flow control ability.

Port Setting Status Fields

3.3.3. LACP

To display LACP Setting web page, click **Port > Link Aggregation > LACP**.

This page allow user to configure LACP global and port configurations. Select ports and click “Edit” button to edit port configuration.

Port >> Link Aggregation >> LACP

System Priority

32768

(1 - 65535, default 32768)

Apply



LACP Global Setting

Field	Description
System Priority	Configure the system priority of LACP. This decides the system priority field in LACP PDU.

LACP Global Setting Fields

LACP Port Setting Table

	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
☐	6	GE6	1	Long
☐	7	GE7	1	Long
☐	8	GE8	1	Long
☐	9	GE9	1	Long
☐	10	GE10	1	Long

Edit

LACP Port Setting Table

Field	Description
Port	Port Name
Port Priority	LACP priority value of the port
Timeout	The periodic transmissions type of LACP PDUs. Long: Transmit LACP PDU with slow periodic (30s). Short: Transmit LACPP DU with fast periodic (1s).

LACP Port Setting Table Fields

Port >> Link Aggregation >> LACP

Edit LACP Port Setting

Port	GE1	
Port Priority	1	(1 - 65535, default 1)
Timeout	☒ Long ☐ Short	

Edit LACP Port Setting

Field	Description
Port	Selected port list
Port Priority	Enter the LACP priority value of the port
Timeout	The periodic transmissions type of LACP PDUs. Long: Transmit LACP PDU with slow periodic (30s). Short: Transmit LACPP DU with fast periodic (1s).

Edit LACP Port Setting Fields

3.4.EEE

To display EEE web page, click **Port > EEE**

This page allow user to configure Energy Efficient Ethernet settings.

Port >> EEE

EEE Setting Table

☐	Entry	Port	State
☐	1	GE1	Disabled
☐	2	GE2	Disabled
☐	3	GE3	Disabled
☐	4	GE4	Disabled
☐	5	GE5	Disabled
☐	6	GE6	Disabled
☐	7	GE7	Disabled
☐	8	GE8	Disabled
☐	9	GE9	Disabled
☐	10	GE10	Disabled
☐	11	GE11	Disabled

EEE Setting Table

Field	Description
Port	Port Name
State	Port EEE admin state. Enabled: EEE is enabled. Disabled: EEE is disabled
Operational Status	Port EEE operational status. Enabled: EEE is operating. Disabled: EEE is no operating

EEE Setting Table Fields

Port >> EEE

Edit EEE Setting

Port	GE1-GE3
State	☐ Enable

Apply

Close

Edit EEE Setting Dialog

Field	Description
Port	Selected port list
State	Port EEE admin state. Enable: Enable EEE. Disable: Disable EEE

Edit EEE Setting Fields

3.5.Jumbo Frame

To display Jumbo Frame web page, click **Port > Jumbo>Frame**.

This page allow user to configure switch jumbo frame size.

Port >> Jumbo Frame

Jumbo Frame ☐ Enable

10000 Byte (1518 - 10000, default 1522)

Apply

Jumbo Frame Page

Field	Description
Jumbo Frame	Enable or disable jumbo frame. When jumbo frame is enabled, switch max frame size is allowed to configure. When jumbo frame is disabled, default frame size 1522 will be used.

Jumbo Frame Fields

3.6.Port Security

To display Port Security web page, click **port > Port Security**

This page allow user to configure port security settings for each interface. When port security is enabled on interface, action will be perform once learned MAC address over limitation.

Port >> Protected Port

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
☐	8	GE8	Unprotected
☐	9	GE9	Unprotected

Port Security Page

Field	Description
Port	Select one or multiple ports to configure.
State	Select the status of port security Disable: Disable port security function. Enable: Enable port security function.
MAC Address	Specify the number of how many mac addresses can be learned.
Action	Select the action if learned mac addresses Forward: Forward this packet whose SMAC is new to system and exceed the learning-limit number. Discard: Discard this packet whose SMAC is new to system and exceed the learning-limit number. Shutdown: Shutdown this port when receives a packet whose SMAC is new to system and exceed the learning limit number.

Port Security Fields

3.7.Protected Port

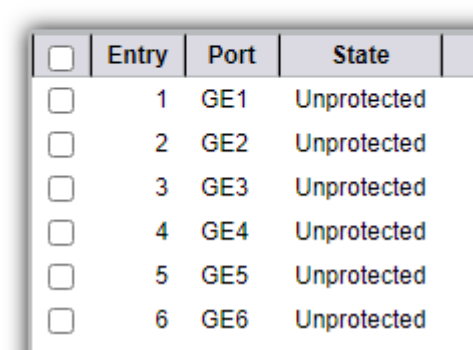
To display Protected Port web page, click **port > Protected Port**

This page allow user to configure protected port setting to prevent the selected ports from communication with

each other. Protected port is only allowed to communicate with unprotected port. In other words, protected port is not allowed to communicate with another protected port.

Port >> Protected Port

Protected Port Table



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

Protected Port Table

Field	Description
Port	Port Name
State	Port protected admin state. Protected: Port is protected. Unprotected: Port is unprotected

Protected Port Table Fields

Edit Protected Port



Port
GE1-GE2

State
☐ Protected

Apply
Close

Edit Protected Port dialog

Field	Description
Port	Selected port list
State	Port protected admin state. Protected: Enable protecting function. Unprotected: Disable protecting function.

Edit Protected Port Fields

3.8. Storm Control

To display Storm Control global setting web page, click **port > Storm Control**

Port >> Storm Control

Mode	☐ Packet / Sec ☒ Kbits / Sec
IFG	☒ Exclude ☐ Include

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

Storm Control Setting Page

Field	Description
Unit	Select the unit of storm control Packet / Sec: storm control rate calculates by packet-based Kbits / Sec: storm control rate calculates by octet-based
IFG	Select the rate calculates w/o preamble & IFG (20 bytes) Excluded: exclude preamble & IFG (20 bytes) when count ingress storm control rate. Included: include preamble & IFG (20 bytes) when count ingress storm control rate.

Storm Control Global Setting Fields

To Edit Storm Control port setting web page, select the port which to set, click button **Edit**

Edit Port Setting

Port	GE1	
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	

Apply

Close

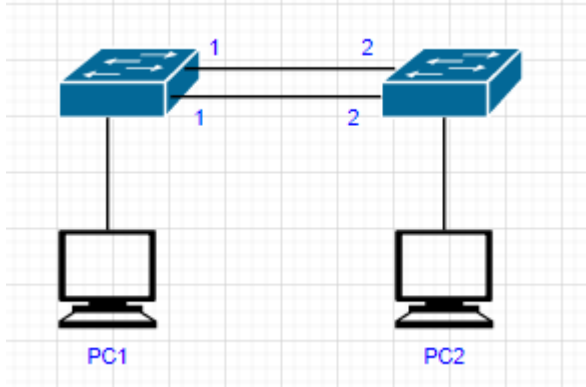
Storm Control Edit Port Setting Page

Field	Description
Port	Select the setting ports
State	Select the state of setting Enable: Enable the storm control function.
Broadcast	Enable: Enable the storm control function of Broadcast packet. Value of storm control rate, Unit: pps (packet per-second, range 1- 262143) or Kbps (Kbits per-second, range16 - 1000000) depends on global mode setting.
Unknown Multicast	Enable: Enable the storm control function of Unknown multicast packet. Value of storm control rate, Unit: pps (packet per-second, range 1- 262143) or Kbps (Kbits per-second, range16 - 1000000) depends on global mode setting.
Unknown Unicast	Enable: Enable the storm control function of Unknown unicast packet. Value of storm control rate, Unit: pps (packet per-second, range 1- 262143) or Kbps (Kbits per-second, range16 - 1000000) depends on global mode setting.
Action	Select the state of setting Drop: Packets exceed storm control rate will be dropped. Shutdown: Port will be shutdown when packets exceed storm control rate.

Storm Control Port Setting Fields

3.9. Configuration Case

Case 1: Two switches increase bandwidth by configuring static aggregation



- SW1/SW2 webconfig

- Status
- Network
- Port
 - Port Setting
 - Error Disabled
 - Link Aggregation
 - Group**
 - Port Setting
 - LACP
 - EEE
 - Jumbo Frame
 - Port Security
 - Protected Port
 - Storm Control
- POE Setting
- VLAN
- MAC Address Table
- Spanning Tree
- ERPS

Port >> Link Aggregation >> Group

Load Balance Algorithm

☒ MAC Address
☐ IP-MAC Address
☐ Dst-MAC Address
☐ Src-MAC Address
☐ Dst-IP Address
☐ Src-IP Address

Apply

Link Aggregation Table

	LAG	Name	Type	Link Status	Active Member	Inactive Member
☐	LAG 1		Static	Down		GE1-GE2
☐	LAG 2		---	---		
☐	LAG 3		---	---		
☐	LAG 4		---	---		

SW1/SW2CLIconfig

```

interface gi1
  lag 1 mode static
!
interface gi2
  lag 1 mode static
  
```

Case 2: Two switches increase bandwidth by configuring dynamic aggregation

- SW1/SW2 webconfig

Port >> Link Aggregation >> Group

Load Balance Algorithm

☒ MAC Address
☐ IP-MAC Address
☐ Dst-MAC Address
☐ Src-MAC Address
☐ Dst-IP Address
☐ Src-IP Address

Apply

Link Aggregation Table

	LAG	Name	Type	Link Status	Active Member	Inactive Member
☐	LAG 1		LACP	Down		GE1-GE2
☐	LAG 2		---	---		
☐	LAG 3		---	---		
☐	LAG 4		---	---		
☐	LAG 5		---	---		

- SW1/SW2CLI config

```

interface gi1
  lag 1 mode active
!
interface gi2
  lag 1 mode active
  
```

Case 3: Configure port 0/1 unknown multicast speed limit to 1000Kb/s total bandwidth.

- Web config

Port >> Storm Control

Mode

☐ Packet / Sec
☒ Kbits / Sec

IFG

☒ Exclude
☐ Include

Apply

Port Setting Table

	Entry	Port	State	Broadcast		Unknown Multicast		Unknown Unicast		Action
				State	Rate (Kbps)	State	Rate (Kbps)	State	Rate (Kbps)	
☐	1	GE1	Enabled	Disabled	10000	Enabled	1008	Disabled	10000	Drop

- CLI Config

1. Enter the 0/1 port interface configuration mode

```
switch >enable

switch #configure

switch (Config)#interface GigabitEthernet 1
```

2. Configure unknown multicast speed limit strategy for the interface

```
switch (config-if-GigabitEthernet1)#storm-control unknown-multicast level 1008
```

Case 4: Configuring Port 1 and Port 2 Port Isolation

● Web Config

Port >> Protected Port

Protected Port Table

☐	Entry	Port	State
☐	1	GE1	Protected
☐	2	GE2	Protected

● CLI Config

端口1和端口2配置隔离:

```
switch >enable

switch #configure

switch (Config)#interface rang GigabitEthernet 1-2
Switch(config-if-range-GigabitEthernet1-2)# protected
```

Case 5: Configuring a secure MAC address for Port 2

● WEB

MAC Address Table >> Port Security Address

Port Security Address Table

Showing All entries

Showing 1 to 1 of 1 entries

☐	VLAN	MAC Address	Type	Port
☐	2	68:F7:28:A1:B8:A0	SecureConfigured	GE2

Add

Edit

Delete

Port >> Port Security

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

Port Security Table

☐	Entry	Port	State	Address Limit	Total	Configured	Violate Number	Violate Action	Sticky
☐	1	GE1	Disabled	1	0	0	0	Protect	Disabled
☐	2	GE2	Enabled	1	1	1	0	Protect	Enabled

- CLI Config

```
vlan 2
interface gi2
port-security
    port-security
    port-security mac-address sticky
    port-security mac-address 68:F7:28:A1:B8:A0 vlan 2
```

4. **PoE**

Use the PoE pages to configure settings for switch port related features

4.1. PoE Setting

To display PoE Setting web page, click **Port Setting> PoE Port Setting**

This page shows port current status and allow user to edit port configurations. Select port entry and click “Edit” button to edit port configurations.

[POE Setting](#) >> [POE Port Setting](#)

System info

System Power(W)	0
Refresh Rate	☐ None ☐ 5 sec ☒ 10 sec ☐ 30 sec

Port Setting Table

☐	Entry	Port	PortEnable	Status	Type	Level	Actual Power(W)	Voltage(V)	Current(mA)
☐	1	GE1	Enabled	Off	N/A	0	0	0	0
☐	2	GE2	Enabled	Off	N/A	0	0	0	0
☐	3	GE3	Enabled	Off	N/A	0	0	0	0
☐	4	GE4	Enabled	Off	N/A	0	0	0	0
☐	5	GE5	Enabled	Off	N/A	0	0	0	0

4.2. POE Port Timer Setting

To display PoE Setting web page, click **Port Setting> POE Port Timer Setting**

[POE Setting](#) >> [POE Port Timer Setting](#)

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	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒

4.3. Configuration Case

Case 1: Configuring Port 0/1 Power Supply Enable

- Web Config

POE Setting >> POE Port Setting

System info

System Power(W)	0
Refresh Rate	☐ None ☐ 5 sec ☒ 10 sec ☐ 30 sec

Port Setting Table

☐	Entry	Port	PortEnable	Status	Type	Level	Actual Power(W)	Voltage(V)	Current(mA)
☐	1	GE1	Enabled	Off	N/A	0	0	0	0

● CLI Config

```
switch(config)# interface GigabitEthernet 1
switch(config-if-GigabitEthernet1)# poe
```

5. VLAN

A virtual local area network, virtual LAN or VLAN, is a group of hosts with a common set of requirements that communicate as if they were attached to the same broadcast domain, regardless of their physical location. A VLAN has the same attributes as a physical local area network (LAN), but it allows for end stations to be grouped together even if they are not located on the same network switch.

VLAN membership can be configured through software instead of physically relocating devices or connections.

5.1. VLAN

Use the VLAN pages to configure settings of VLAN.

5.1.1. Create VLAN

To display Create VLAN page, click **VLAN > VLAN > Create VLAN**

This page allows user to add or delete VLAN ID entries and browser all VLAN entries that add statically or dynamic learned by GVRP. Each VLAN entry has a unique name, user can edit VLAN name in edit page.

VLAN >> VLAN >> Create VLAN

VLAN

Available VLAN

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

>

<

Created VLAN

VLAN 1

Apply

VLAN Table

Showing All entriesShowing 1 to 1 of 1 entries

Q

☐	VLAN	Name	Type	VLAN Interface State
☐	1	default	Default	Enabled

FirstPrevious1NextLast

EditDelete

Create VLAN Page

Field	Description
Available VLAN	VLAN has not created yet. Select available VLANs from left box then move to right box to add.
Created VLAN	VLAN had been created. Select created VLAN from right box then move to left box to delete.

Create VLAN Fields

VLAN >> VLAN >> Create VLAN

Edit VLAN Name

Name

VLAN0002

ApplyClose

Edit VLAN Name Dialog

Field	Description
Name	Input VLAN name.

Edit VLAN Name Fields

5.1.2. VLAN Configuration

To display VLAN Configuration page, click **VLAN > VLAN > VLAN Configuration**

This page allow user to configure the membership for each port of selected VLAN.

VLAN >> VLAN >> VLAN Configuration

VLAN Configuration Table

VLAN

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	☒	☐
9	GE9	Trunk	☐ Excluded	☐ Tagged	☒ Untagged	☒	☐
10	GE10	Trunk	☐ Excluded	☐ Tagged	☒ Untagged	☒	☐
11	GE11	Trunk	☐ Excluded	☐ Tagged	☒ Untagged	☒	☐

VLAN configuration Page

Field	Description
VLAN	Select specified VLAN ID to configure VLAN configuration.
Port	Display the interface of port entry.
Mode	Display the interface VLAN mode of port.
Membership	Select the membership for this port of the specified VLAN ID. Forbidden: Specify the port is forbidden in the VLAN. Excluded: Specify the port is excluded in the VLAN. Tagged: Specify the port is tagged member in the VLAN. Untagged: Specify the port is untagged member in the VLAN.
PVID	Display if it is PVID of interface.

VLAN Configuration Settings Fields

5.1.3. Membership

To display Membership page, click **VLAN > VLAN > Membership**

This page allow user to view membership information for each port and edit membership for specified

interface

VLAN >> VLAN >> Membership

Membership Table

	Entry	Port	Mode	Administrative VLAN	Operational VLAN
☐	1	GE1	Trunk	1UP	1UP
☐	2	GE2	Trunk	1UP	1UP
☐	3	GE3	Trunk	1UP	1UP
☐	4	GE4	Trunk	1UP	1UP
☐	5	GE5	Trunk	1UP	1UP
☐	6	GE6	Trunk	1UP	1UP
☐	7	GE7	Trunk	1UP	1UP
☐	8	GE8	Trunk	1UP	1UP
☐	9	GE9	Trunk	1UP	1UP
☐	10	GE10	Trunk	1UP	1UP
☐	11	GE11	Trunk	1UP	1UP
☐	12	GE12	Trunk	1UP	1UP

Membership Page

Field	Description
Port	Display the interface of port entry.
Mode	Display the interface VLAN mode of port.
Administrative VLAN	Display the administrative VLAN list of this port.
Operational VLAN	Display the operational VLAN list of this port. Operational VLAN means the VLAN status that really runs in device. It may different to administrative VLAN.

Membership Fields

VLAN >> VLAN >> Membership

Edit Port Setting

Port: GE2

Mode: Trunk

Membership

Left list: 2

Right list: 1UP

Options:

- ☐ Forbidden
- ☐ Excluded
- ☒ Tagged
- ☐ Untagged
- ☐ PVID

Buttons: Apply, Close

Edit Membership Dialog

Field	Description
Port	Display the interface.
Mode	Display the VLAN mode of interface.
Membership	Select VLANs of left box and select one of following membership then move to right box to add membership. Select VLANs of right box then move to left box to remove membership. Tagging membership may not choose in differ VLAN port mode. Select the time source. Forbidden: Set VLAN as forbidden VLAN. Excluded: This option is always disabled. Tagged: Set VLAN as tagged VLAN. Untagged: Set VLAN as untagged VLAN. PVID: Check this checkbox to select the VLAN ID to be the port-based VLAN ID for this port. PVID may auto select or can't select in differ settings.

Edit Membership Fields

5.1.4. Port Setting

To display Port Setting page, click **VLAN > VLAN > Port Setting**

This page allow user to configure ports VLAN settings such as VLAN port mode, PVID etc...The attributes depend on different VLAN port mode.

VLAN >> VLAN >> Port Setting

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
☐	9	GE9	Trunk	1	All	Enabled	Disabled	0x8100
☐	10	GE10	Trunk	1	All	Enabled	Disabled	0x8100
☐	11	GE11	Trunk	1	All	Enabled	Disabled	0x8100
☐	12	GE12	Trunk	1	All	Enabled	Disabled	0x8100
☐	13	GE13	Trunk	1	All	Enabled	Disabled	0x8100

Port Setting Page

Field	Description
Port	Display the interface.
Mode	Display the VLAN mode of port.
PVID	Display the Port-based VLAN ID of port.
Accept Frame Type	Display accept frame type of port
Ingress Filtering	Display ingress filter status of port
Uplink	Display uplink status.
TPID	Display TPID used of interface.

Port setting Fields

VLAN >> VLAN >> Port Setting

Edit Port Setting

Port	GE1
Mode	☐ Hybrid ☐ Access ☒ Trunk ☐ Tunnel
PVID	1 (1 - 4094)
Accept Frame Type	☒ All ☐ Tag Only ☐ Untag Only
Ingress Filtering	☒ Enable
Uplink	☐ Enable
TPID	0x8100 ▾

Edit Port Setting Dialog

Field	Description
Port	Display selected port to be edited.
Mode	Select the VLAN mode of the interface. Hybrid: Support all functions as defined in IEEE 802.1Q specification. Access: Accepts only untagged frames and join an untagged VLAN. Trunk: An untagged member of one VLAN at most, and is a tagged member of zero or more VLANs.
PVID	Specify the port-based VLAN ID (1-4094). It's only available with Hybrid and Trunk mode.
Accepted Type	Specify the acceptable-frame-type of the specified interfaces. It's only available with Hybrid mode.
Ingress Filtering	Set checkbox to enable/disable ingress filtering. It's only available with Hybrid mode.

Uplink	Set checkbox to enable/disable uplink mode. It's only available with trunk mode.
TPID	Select TPID used of interface. It's only available with trunk mode.

Edit Port Setting Fields

5.2. Voice VLAN

Use the Voice VLAN pages to configure settings of Voice VLAN.

5.2.1. Property

To display Property page, click **VLAN> Voice VLAN> Property**

This page allow user to configure global and per interface settings of voice VLAN.

VLAN >> Voice VLAN >> Property

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

Apply

Property Page

Field	Description
State	Set checkbox to enable or disable voice VLAN function.
VLAN	Select Voice VLAN ID. Voice VLAN ID cannot be default VLAN.
Cos/802.1p	Select a value of VPT. Qualified packets will use this VPT value as inner priority.
Remarking	Set checkbox to enable or disable 1p remarking. If enabled, qualified packets will be remark by this value.
Aging Time	Input value of aging time. Default is 1440 minutes. A voice VLAN entry will be age out after this time if without any packet pass through.

Property Fields

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
☐	9	GE9	Disabled	Auto	Voice Packet
☐	10	GE10	Disabled	Auto	Voice Packet
☐	11	LAG1	Disabled	Auto	Voice Packet
☐	12	LAG2	Disabled	Auto	Voice Packet
☐	13	LAG3	Disabled	Auto	Voice Packet
☐	14	LAG4	Disabled	Auto	Voice Packet
☐	15	LAG5	Disabled	Auto	Voice Packet

Property Port Page

Field	Description
Port	Display port entry.
State	Display enable/disabled status of interface.
Mode	Display voice VLAN mode.
QoS Policy	Display voice VLAN remark will effect which kind of packet

Property Port Fields

VLAN >> Voice VLAN >> Property

Edit Port Setting

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

Apply Close

Edit Property Port Dialog

Field	Description
Port	Display selected port to be edited.
State	Set checkbox to enable/disabled voice VLAN function of interface.

Mode	Select port voice VLAN mode Auto: Voice VLAN auto detect packets that match OUI table and add received port into voice VLAN ID tagged member. Manual: User need add interface to VLAN ID tagged member manually.
QoS Policy	Select port QoS Policy mode Voice Packet: QoS attributes are applied to packets with OUIs in the source MAC address. All: QoS attributes are applied to packets that are classified to the Voice VLAN.

Edit Property Port Fields

5.2.2. Voice OUI

To display Voice OUI page, click **VLAN> Voice VLAN> Voice OUI**

This page allow user to add, edit or delete OUI MAC addresses. Default has 8 pre-defined OUI MAC.

VLAN >> Voice VLAN >> Voice OUI

Voice OUI Table

Showing All entries Showing 1 to 8 of 8 entries Q

☐	OUI	Description
☐	00:E0:BB	3COM
☐	00:03:6B	Cisco
☐	00:E0:75	Veritel
☐	00:D0:1E	Pingtel
☐	00:01:E3	Siemens
☐	00:60:B9	NEC/Philips
☐	00:0F:E2	H3C
☐	00:09:6E	Avaya

First Previous 1 Next Last

Figure 7-2-2-1 Voice OUI Page

Field	Description
OUI	Display OUI MAC address.
Description	Display description of OUI entry.

Voice OUI Mac Setting Fields

VLAN >> Voice VLAN >> Voice OUI

Add Voice OUI

OUI

:

:

Description

Apply

Close

VLAN >> Voice VLAN >> Voice OUI

Edit Voice OUI

OUI

00:E0:BB

Description

3COM

Apply

Close

Add and Edit Voice OUI Dialog

Field	Description
OUI	Input OUI MAC address. Can't be edited in edit dialog.
Description	Input description of the specified MAC address to the voice VLAN OUI table

Add and Edit Voice OUI Fields

5.3.Protocol VLAN

Use the Protocol VLAN pages to configure settings of Protocol VLAN.

5.3.1. Protocol Group

To display Protocol Group page, click **VLAN > Protocol VLAN > Protocol Group**

This page allow user to add or edit groups settings of protocol VLAN.

VLAN >> Protocol VLAN >> Protocol Group

Protocol Group Table

Showing All entriesShowing 0 to 0 of 0 entries

☐	Group ID	Frame Type	Protocol Value
0 results found.			

Add

Edit

Delete

First

Previous

1

Next

La

Protocol Group Page

Field	Description
Group ID	Display group ID of entry.
Frame Type	Display frame type of entry.
Protocol Value	Display protocol value of entry.

Protocol Group Fields

VLAN >> Protocol VLAN >> Protocol Group

Add Protocol Group

Group ID

1

Frame Type

Ethernet_II

Protocol Value

0x

(0x600 ~ 0xFFFE)

Apply

Close

Managed Switch software

5

www.ewindnet.com

VLAN >> Protocol VLAN >> Protocol Group

Edit Protocol Group

Group ID	1
Frame Type	Ethernet_II
Protocol Value	0x 0600 (0x600 ~ 0xFFFE)

Apply

Close

Add and Edit Protocol Group Dialog

Field	Description
Group ID	Select group ID of list. The range from 1 to 8.
Frame Type	Select frame type of list that maps packets to protocol-defined VLANs by examining the type octet within the packet header to discover the type of protocol associated with it. Ethernet_II: packet type is Ethernet version 2. IEEE802.3_LLC_Other: packet type is 802.3 packet with LLC other header. RFC_1042: packet type is rfc 1042 packet.
Protocol Value	Input protocol value of the target protocol. Packets match this protocol value classified to specified VLAN ID.

Add and Edit Protocol Group Fields

5.3.2. Group Binding

To display Group Binding page, click **VLAN> Protocol VLAN > Group Binding**

VLAN >> Protocol VLAN >> Group Binding

Group Binding Table

Showing entries

Showing 0 to 0 of 0 entries

☐	Port	Group ID	VLAN	
0 results found.				
Add Edit Delete				

This page allow user to bind protocol VLAN group to each port with VLAN ID.

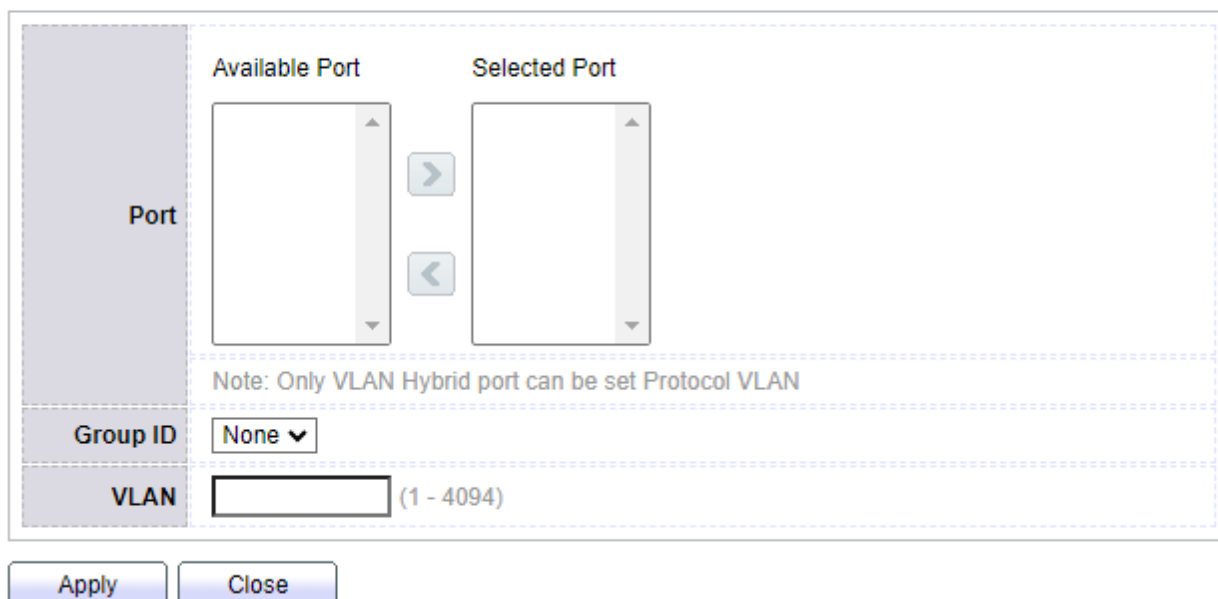
Group binding Page

Field	Description
Port	Display port ID that binding with protocol group entry
Group ID	Display group ID that port binding with
VLAN	Display VLAN ID that assign to packets which match protocol group

Group Binding Fields

VLAN >> Protocol VLAN >> Group Binding

Add Group Binding



The dialog box is titled "Add Group Binding". It contains a "Port" section with two lists: "Available Port" and "Selected Port". Between these lists are two arrows, one pointing right and one pointing left. Below the lists is a note: "Note: Only VLAN Hybrid port can be set Protocol VLAN". At the bottom, there are two fields: "Group ID" with a dropdown menu showing "None" and "VLAN" with a text input field and a range "(1 - 4094)". At the very bottom are two buttons: "Apply" and "Close".

Add and Edit Group Binding Dialog

Field	Description
Port	Select ports in left box then move to right to binding with protocol group. Or select ports in right box then move to left to unbind with protocol group. Only interface has hybrid VLAN mode can be selected and bound with protocol group. Only available on Add dialog.
Group ID	Select a Group ID to associate with port. Only available on Add dialog.
VLAN	Input VLAN ID that will assign to packets which match protocol group.

Group Binding Fields

5.4. MAC VLAN

Use the MAC VLAN pages to configure settings of MAC VLAN.

5.4.1. MAC Group

To display MAC Group page, click **VLAN > MAC VLAN > MAC Group**

This page allow user to add or edit groups settings of MAC VLAN.

VLAN >> MAC VLAN >> MAC Group

MAC Group Table

Showing entries

Showing 0 to 0 of 0 entries

☐	Group ID	MAC Address	Mask	
0 results found.				
Add Edit Delete				

MAC Group Page

Field	Description
Group ID	Display group ID of entry.
MAC Address	Display mac address of entry.
Mask	Display mask of mac address for classified packet.

MAC Group Fields

VLAN >> MAC VLAN >> MAC Group

Add MAC Group

Group ID		(1 - 2147483647)
MAC Address		(A:B:C:D:E:F)
Mask		(9 - 48)

Apply

Close

Edit MAC Group

Group ID	1
MAC Address	02:03:04:05:06:07
Mask	48 (9 - 48)

Add and Edit MAC Group Dialog

Field	Description
Group ID	Input group ID that is a unique ID of mac group entry. The range from 1 to 2147483647. Only available on Add Dialog
MAC Address	Input mac address for classifying packets.
Mask	Input mask of mac address.

Add and Edit MAC Group Fields

5.4.2. Group Binding

To display Group Binding page, click **VLAN> MAC VLAN > Group Binding**

This page allow user to bind MAC VLAN group to each port with VLAN ID.

VLAN >> MAC VLAN >> Group Binding

MAC Group Table

Showing All entries Showing 0 to 0 of 0 entries

☐ Group ID MAC Address Mask

0 results found.

Group binding Page

Field	Description
Port	Display port ID that binding with MAC group entry
Group ID	Display group ID that port binding with
VLAN	Display VLAN ID that assign to packets which match MAC group

Group Binding Fields

VLAN >> MAC VLAN >> Group Binding

Add MAC Group

Group ID		(1 - 2147483647)
MAC Address		(A:B:C:D:E:F)
Mask		(9 - 48)

Edit Group Binding

Port	GE1
Group ID	1
VLAN	(1 - 4094)

Add and Edit Group Binding Dialog

Field	Description
Port	Select ports in left box then move to right to binding with MAC group. Or select ports in right box then move to left to unbind with MAC group. Only interface has hybrid VLAN mode can be selected and bound with protocol group. Only available on Add dialog.
Group ID	Select a Group ID to associate with port. Only available on Add dialog
VLAN	Input VLAN ID that will assign to packets which match MAC group.

Group Binding Fields

5.5. Surveillance VLAN

Use the Surveillance VLAN pages to configure settings of Surveillance VLAN.

5.5.1. Property

To display Property page, click **VLAN> Surveillance VLAN> Property**

This page allow user to configure global and per interface settings of Surveillance VLAN.

VLAN >> Surveillance VLAN >> Property

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

Apply

Property Page

Field	Description
State	Set checkbox to enable or disable Surveillance VLAN function.
VLAN	Select Surveillance VLAN ID. Surveillance VLAN ID cannot be default VLAN.
Cos/802.1p	Select a value of VPT. Qualified packets will use this VPT value as inner priority.
Remarking	Set checkbox to enable or disable 1p remarking. If enabled, qualified packets will be remark by this value.
Aging Time	Input value of aging time. Default is 1440 minutes. A video VLAN entry will be age out after this time if without any packet pass through.

Property Fields

Port Setting Table

	Entry	Port	State	Mode	QoS Policy
☐	1	GE1	Disabled	Auto	Video Packet
☐	2	GE2	Disabled	Auto	Video Packet
☐	3	GE3	Disabled	Auto	Video Packet
☐	4	GE4	Disabled	Auto	Video Packet
☐	5	GE5	Disabled	Auto	Video Packet
☒	6	GE6	Disabled	Auto	Video Packet
☐	7	GE7	Disabled	Auto	Video Packet
☐	8	GE8	Disabled	Auto	Video Packet
☐	9	GE9	Disabled	Auto	Video Packet
☐	10	GE10	Disabled	Auto	Video Packet
☐	11	LAG1	Disabled	Auto	Video Packet

Property Port Page

Field	Description
Port	Display port entry.
State	Display enable/disabled status of interface.
Mode	Display voice VLAN mode.
QoS Policy	Display Surveillance VLAN remark will effect which kind of packet

Property Port Fields

VLAN >> Surveillance VLAN >> Property

Edit Port Setting

Port	GE6
State	☒ Enable
Mode	☒ Auto ☐ Manual
QoS Policy	☒ Video Packet ☐ All

Apply

Close

Edit Property Port Dialog

Field	Description
Port	Display selected port to be edited.
State	Set checkbox to enable/disabled Surveillance VLAN function of interface.
Mode	Select port Surveillance VLAN mode Auto: Video VLAN auto detect packets that match OUI table and add received port into surveillance VLAN ID tagged member. Manual: User need add interface to VLAN ID tagged member manually.

QoS Policy	Select port QoS Policy mode Video Packet: QoS attributes are applied to packets with OUIs in the source MAC address. All: QoS attributes are applied to packets that are classified to the Surveillance VLAN.
------------	--

Edit Property Port Fields

5.5.2. Surveillance OUI

To display Surveillance OUI page, click **VLAN> Surveillance VLAN> Surveillance OUI**

This page allow user to add, edit or delete OUI MAC addresses.

VLAN >> Surveillance VLAN >> Surveillance OUI

Surveillance OUI Table

Showing All entries

Showing 0 to 0 of 0 entries

Q

☐

OUI

Description

0 results found.

Add

Edit

Delete

First

Previous

1

Next

Last

Surveillance OUI Page

Field	Description
OUI	Display OUI MAC address.
Description	Display description of OUI entry.

Surveillance OUI Fields

VLAN >> Surveillance VLAN >> Surveillance OUI

Add Surveillance OUI

OUI

Description

Apply

Close

Add and Edit Surveillance OUI Dialog

Field	Description
OUI	Input OUI MAC address. Can't be edited in edit dialog.
Description	Input description of the specified MAC address to the Surveillance VLAN OUI table

Add and Edit Surveillance OUI Fields

5.6. GVRP

5.6.1. Property

To display GVRP Global and Port Setting web page, click **VLAN> GVRP> Property**

This page allow user to enable or disable GVRP function and GVRP port setting

VLAN >> GVRP >> Property

State
☐ Enable

Operational Timeout

Join
cs (2 - 16375, default 20)

Leave
cs (45 - 32760, default 60)

LeaveAll
cs (65 - 32765, default 1000)

Apply

GVRP Setting Page

Field	Description
State	Set the enabling status of GVRP functionality Enable: if Checked Enable GVRP, else is Disable GVRP
Operational Timeout	
Join	GVRP Join time out.
Leave	GVRP leave time out.
Leave All	GVRP leave all time out.

GVRP Setting Fields

Port Setting Table

	Entry	Port	State	VLAN Creation	Registration
☐	1	GE1	Disabled	Enabled	Normal
☐	2	GE2	Disabled	Enabled	Normal
☐	3	GE3	Disabled	Enabled	Normal
☐	4	GE4	Disabled	Enabled	Normal
☐	5	GE5	Disabled	Enabled	Normal
☐	6	GE6	Disabled	Enabled	Normal
☐	7	GE7	Disabled	Enabled	Normal
☐	8	GE8	Disabled	Enabled	Normal
☐	9	GE9	Disabled	Enabled	Normal
☐	10	GE10	Disabled	Enabled	Normal
☐	11	LAG1	Disabled	Enabled	Normal

GVRP port Setting Page

Field	Description
Entry	Entry of number
Port	Port Name
State	Display port GVRP state
Vlan Creation	Display port GVRP creation vlan state
Registration	Display port GVRP registration mode

GVRP port setting Fields

VLAN >> GVRP >> Property

Edit Port Setting

Port

GE2

State

☐ Enable

VLAN Creation

☒ Enable

Registration

☒ Normal
☐ Fixed
☐ Forbidden

Apply

Close

GVRP port Setting Edit Page

Field	Description
Port	Display the selected port list
State	Set the enabling status of GVRP port Enable: Enable/Disable port of GVRP state.
Vlan Creation	Set the enabling status of GVRP port create VLAN Enable: Enable/Disable port create dynamic VLAN.

Register Mode	Set the register mode of GVRP port Normal: Normal mode. Fixed: The port will not learn any dynamic VLAN. Only send static VLAN information to neighbor and allow static VLAN packet pass. Forbidden: The port will not learn any dynamic VLAN and only allow default VLAN packet pass
---------------	--

GVRP port setting Edit Fields

5.6.2. Membership

To display GVRP VLAN database web page, click **VLAN> GVRP> Membership**.

This page allow user to browser all VLAN member settings that learned by GVRP protocol or configure by user.

[VLAN](#) >> [GVRP](#) >> [Membership](#)

Membership Table

Showing All entries

Showing 0 to 0 of 0 entries



VLAN	Member	Dynamic Member	Type
0 results found.			

First Previous 1 Next Last

GVRP VLAN Information Page

Field	Description
VLAN	VLAN ID
Member	VLAN port members include static and dynamic member
Dynamic Ports	GVRP learned dynamic ports
Vlan Type	The type of VLAN is static or dynamic.

GVRP Port Status Fields

5.6.3. Statistics

To display GVRP port statistics web page, click **VLAN> GVRP> Statistics**

This page allow user to display GVRP port statics by type and clear GVRP port statistics by port.

VLAN >> GVRP >> Statistics

Port	GE1 ▼
Statistics	☒ All ☐ Receive ☐ Transmit ☐ Error
Refresh Rate	☐ None ☐ 5 sec ☒ 10 sec ☐ 30 sec

Clear

GVRP Port Statistics Display Setting

Field	Description
Port	Port ID
Statistics	Type of statistics All: Display Receiver, Transmit and Error port statistics Receive: Display Receive port statistics Transmit: Display Transmit port statistics Error: Display Error port statistics
Refresh Rate	Web refresh rate None: Not auto refresh display port statistics 5 sec: Refresh display port statistics per 5 seconds 10 sec: Refresh display port statistics per 10 seconds 30 sec: Refresh display port statistics per 30 seconds

GVRP Port Statistics Display Setting Fields

Receive	
Join empty	0
Empty	0
Leave Empty	0
Join In	0
Leave In	0
Leave All	0
Transmit	
Join empty	0
Empty	0
Leave Empty	0
Join In	0
Leave In	0
Leave All	0

Error	
Invalid Protocol ID	0
Invalid Attribute Type	0
Invalid Attribute Value	0
Invalid Attribute Length	0
Invalid Event	0

GVRP Port Statistics

Field	Description
Join empty	The number of Receive or Transmit Join empty attribute value.
Empty	The number of Receive or Transmit Empty attribute value.
Leave Empty	The number of Receive or Transmit Leave Empty attribute value.
Join In	The number of Receive or Transmit Join In attribute value.
Leave In	The number of Receive or Transmit Leave In empty attribute value.
Leave All	The number of Receive or Transmit Leave All attribute value.
Invalid Protocol ID	The number of Receive Invalid Protocol ID
Invalid Attribute Type	The number of Receive Invalid Attribute Type
Invalid Attribute Value	The number of Receive Invalid Attribute value.
Invalid Attribute Length	The number of Receive Invalid Attribute Length.

Invalid Event

The number of Receive Invalid Event.

GVRP Port Statistics Fields

5.7. Configuration Case

Case 1: Configure port 1 as an access port, belonging to vlan10

- web

VLAN >> VLAN >> Port Setting

Port Setting Table

☐	Entry	Port	Mode	PVID	Accept Frame Type	Ingress Filtering	Uplink	TPID
☐	1	GE1	Access	10	Untag Only	Enabled	Disabled	0x8100

- CLI

```
switch(config)# interface GigabitEthernet 1
switch(config-if-GigabitEthernet1)# switchport mode access
switch(config-if-GigabitEthernet1)# switchport access vlan 10
```

Case 2: Configure port 1 as a trunk port, allowing vlan10 to pass through

- WEB

VLAN >> VLAN >> Membership

Membership Table

☐	Entry	Port	Mode	Administrative VLAN	Operational VLAN
☐	1	GE1	Trunk	1UP, 10T	1UP, 10T

- CLI

```
switch (config)#interface gil
switch(config-if-GigabitEthernet1)# switchport mode trunk
switch(config-if-GigabitEthernet1)# switchport trunk allowed vlan add 10
```

Case 3: Configure port 0/1 as a hybrid port, label vlan10 as tagged, and label vlan20 as untagged

- WEB

VLAN >> VLAN >> Membership

Membership Table

☐	Entry	Port	Mode	Administrative VLAN	Operational VLAN
☐	1	GE1	Hybrid	1UP, 10T, 20U	1UP, 10T, 20U

- CLI


```
switch (config)#interface gi 1
switch(config-if-GigabitEthernet1)#switchport mode hybrid
switch(config-if-GigabitEthernet1)#switchport hybrid allowed vlan add 20 untagged
switch(config-if-GigabitEthernet1)#switchport hybrid allowed vlan add 10 tagged
```

Case 4: Configure Port 2 voice VLAN to be 2

- Web

VLAN >> Voice VLAN >> Property

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	Manual	Voice Packet
☐	2	GE2	Disabled	Auto	Voice Packet

- CLI

```
configure
vlan 2
voice-vlan cos 6 remarkvoice-vlan vlan 2
voice-vlan
voice-vlan cos 6 remark
interface gi1
voice-vlan mode manual
switchport trunk allowed vlan add 2
voice-vlan mode manual
voice-vlan
```

Case 5: Configure the MAC VLAN for Port 1 and Port 2 to be 2

- WEB

1、 mac group Config

VLAN >> MAC VLAN >> MAC Group

MAC Group Table

Showing All entries

☐	Group ID	MAC Address	Mask
☐	1	00:24:E8:B7:0C:70	48
☐	2	68:F7:28:A1:B8:A0	48

Add

Edit

Delete

2、grouping binding Config

VLAN >> MAC VLAN >> Group Binding

Group Binding Table

Showing All entries

Showing 1 to 4 of 4 entries

☐	Port	Group ID	VLAN
☐	GE1	1	2
☐	GE1	2	2
☐	GE2	1	2
☐	GE2	2	2

Add

Edit

Delete

● CLI

```

configure
vlan 2
vlan mac-vlan group 1 00:24:E8:B7:0C:70 mask 48
vlan mac-vlan group 2 68:F7:28:A1:B8:A0 mask 48
interface gi1
switchport mode hybrid
switchport hybrid allowed vlan add 2 untagged
vlan mac-vlan group 1 vlan 2
vlan mac-vlan group 2 vlan 2
interface gi2
switchport mode hybrid
switchport hybrid allowed vlan add 2 untagged
vlan mac-vlan group 1 vlan 2
vlan mac-vlan group 2 vlan 2

```

Case 6: Configure the protocol VLAN for port 1 and port 2 to be 2

● Web

1、Protocol Group Table

VLAN >> Protocol VLAN >> Protocol Group

Protocol Group Table

Showing All entries

Showing 1 to 2 of 2 entries

☐	Group ID	Frame Type	Protocol Value	
☐	1	Ethernet_II	0x0806	
☐	2	Ethernet_II	0x0800	

Add
Edit
Delete

2、grouping binding

VLAN >> Protocol VLAN >> Group Binding

Group Binding Table

Showing All entries

Showing 1 to 4 of 4 entries

☐	Port	Group ID	VLAN	
☐	GE1	1	2	
☐	GE1	2	2	
☐	GE2	1	2	
☐	GE2	2	2	

Add
Edit
Delete

● CLI

```

configure
vlan 2
!
vlan protocol-vlan group 1 frame-type ethernet_ii protocol-value 0x806
vlan protocol-vlan group 2 frame-type ethernet_ii protocol-value 0x800
interface gi1
switchport mode hybrid
switchport hybrid allowed vlan add 2 untagged
vlan protocol-vlan group 1 vlan 2
vlan protocol-vlan group 2 vlan 2
!
interface gi2
switchport mode hybrid
switchport hybrid allowed vlan add 2 untagged
vlan protocol-vlan group 1 vlan 2
vlan protocol-vlan group 2 vlan 2

```

Case 7: Configure the Surveillance VLAN for Port 1 to be 2

- Web

VLAN >> Surveillance VLAN >> Property

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	Manual	All

VLAN >> Surveillance VLAN >> Surveillance OUI

Surveillance OUI Table

Showing All ▼ entries

Showing 1 to 1 of 1 entries

☐	OUI	Description
☐	00:00:01	

Add Edit Delete

- CLI

```

configure
vlan 2
surveillance-vlan vlan 2
surveillance-vlan
surveillance-vlan cos 6 remark
surveillance-vlan oui-table 00:00:01 ""
interface vlan1
ip address 192.168.0.1/24
ipv6 enable
interface gil
switchport trunk allowed vlan add 2
voice-vlan mode manual
voice-vlan

```

```
!
interface gi2
switchport trunk allowed vlan add 2
```

Case 8: Configure GVRP-VLAN for Port 3 to be 2

- web

VLAN >> GVRP >> Property

State	☒ Enable
Operational Timeout	
Join	20 cs (2 - 16375, default 20)
Leave	60 cs (45 - 32760, default 60)
LeaveAll	1000 cs (65 - 32765, default 1000)
Apply	

Port Setting Table

☐	Entry	Port	State	VLAN Creation	Registration
☐	1	GE1	Disabled	Enabled	Normal
☐	2	GE2	Disabled	Enabled	Normal
☐	3	GE3	Enabled	Enabled	Normal
☐	4	GE4	Disabled	Enabled	Normal

VLAN >> GVRP >> Membership

Membership Table

Showing entries

Showing 1 to 2 of 2 entries

VLAN	Member	Dynamic Member	Type
1	GE1-GE48,TE1-TE6,LAG1-LAG8		Static
2	GE1-GE3		Static

- CLI

```
configure
vlan 2
gvrp
interface gi3
switchport trunk allowed vlan add 2
gvrp
```

6. MAC Address Table

Use the MAC Address Table pages to show dynamic MAC table and configure settings for static MAC entries.

6.1. Dynamic Address

To configure the aging time of the dynamic address, click **MAC Address Table > Dynamic Address**.

MAC Address Table >> Dynamic Address

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	68:F7:28:A1:B8:A0	GE47

Refresh Add Static Address

First Previous 1 Next Last

Dynamic Address Setting page.

Field	Description
Aging Time	The time in seconds that an entry remains in the MAC address table. Its valid range is from 10 to 630 seconds, and the default value is 300 seconds..

Dynamic Address Setting fields.

6.2. Static Address

To display the static MAC address, click **MAC Address Table > Static Address**.

MAC Address Table >> Static Address

Static Address Table

Showing All entries Showing 0 to 0 of 0 entries

☐	VLAN	MAC Address	Port
0 results found.			

Add Edit Delete

First Previous 1 Next Last

Static Address Page.

Field	Description
MAC Address	The MAC address to which packets will be statically forwarded.
VLAN	Specify the VLAN to show or clear MAC entries.

Port	Interface or port number.
------	---------------------------

Static Address Setting fields.

6.3. Filtering Address

To configure and display the MAC filtering settings, click **MAC Address Table > Filtering Address**.

[MAC Address Table](#) >> [Filtering Address](#)

Filtering Address Table

Showing All entries Showing 1 to 1 of 1 entries Q

☐	VLAN	MAC Address
☐	1	00:D0:F8:00:00:01

First Previous 1 Next Last

Filtering Address page.

Field	Description
MAC Address	Specify unicast MAC address in the packets to be dropped.
VLAN	Specify the VLAN ID for the specific MAC address.

Filtering Address Setting fields

6.4. Configuration Case

Case 1: Configuring Port 1 to Bind Static MAC

● web

Static Address Table

Showing All entries

☐	VLAN	MAC Address	Port
☐	2	00:D0:F8:00:00:01	GE1

● CLI (config)

```
mac address-table static 00:D0:F8:00:00:01 vlan 2 interfaces gil
```

Case 2: Configuring Aging Time

● web

MAC Address Table >> Dynamic Address

Aging Time	10	Sec (10 - 630, d
Apply		

Dynamic Address Table

Showing entries

☐	VLAN	MAC Address	Port
--------------------------	------	-------------	------

● CLI (Config)

```
mac address-table aging-time 10
```

Case 2: Configuring Aging Time

● web

Filtering Address Table

Showing entries

☐	VLAN	MAC Address
☐	2	00:D0:F8:00:00:01
Add Edit Delete		

● CLI

```
mac address-table static 00:D0:F8:00:00:01 vlan 2 drop
```


7. STP

The Spanning Tree Protocol (STP) is a network protocol that ensures a loop-free topology for any bridged Ethernet local area network.

7.1. Property

To configure and display STP property configuration, click **Spanning Tree > Property**.

Spanning Tree >> Property

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	82:24:02:19:00:01	
Revision	0	(0 - 65535, default 0)
Max Hop	20	(1 - 40, default 20)
Operational Status		
Bridge Identifier	32768-82:24:02:19:00:01	
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	0D/0H/0M/0S	

STP Property.

Field	Description
State	Enable/Disable the Spanning Tree on the switch.
Operation Mode	Specify the Spanning Tree operation mode. STP: Enable the Spanning Tree (STP) operation. RSTP: Enable the Rapid Spanning Tree (RSTP) operation. MSTP: Enable the Multiple Spanning Tree (MSTP) operation.

Path Cost	Specify the path cost method. Long: Specifies that the default port path costs are within the range: 1-200,000,000.. Short: Specifies that the default port path costs are within the range: 1-65,535.
BPDU Handling	Specify the BPDU forward method when the STP is disabled. Filtering: Filter the BPDU when STP is disabled. Flooding: Flood the BPDU when STP is disabled.
Priority	Specify the bridge priority. The valid range is from 0 to 61440, and the value should be the multiple of 4096. It ensures the probability that the switch is selected as the root bridge, and the lower value has the higher priority for the switch to be selected as the root bridge of the topology.
Hello Time	Specify the STP hello time in second to broadcast its hello message to other bridges by Designated Ports. Its valid range is from 1 to 10 seconds.
Max Age	Specify the time interval in seconds for a switch to wait the configuration messages, without attempting to redefine its own configuration.
Forward Delay	Specify the STP forward delay time, which is the amount of time that a port remains in the Listening and Learning states before it enters the Forwarding state. Its valid range is from 4 to 10 seconds.
TX Hold Count	Specify the tx-hold-count used to limit the maximum numbers of packets transmission per second. The valid range is from 1 to 10.
Region Name	The MSTP instance name. Its maximum length is 32 characters. The default value is the MAC address of the switch.
Revision	The MSTP revision number. Its valid range is from 0 to 65535.
Max Hops	Specify the number of hops in an MSTP region before the BPDU is discarded. The valid range is 1 to 40.

Field	Description
Bridge Identifier	Bridge identifier of the switch.
Designated Root Identifier	Bridge identifier of the designated root bridge.
Root Port	Operational root port of the switch.
Root Path Cost	Operational root path cost.

Topology Change	Numbers of the topology changes.
Count	
Last Topology Change	The last time for the topology change.

STP Operational Status field.

7.2. Port Setting

To configure and display the STP port settings, click **Spanning Tree > Port Setting**.

Spanning Tree >> Port Setting

Port Setting Table

☐	Entry	Port	State	Path Cost	Priority	BPDU Filter	BPDU Guard	Operational Edge	Operational Point-to-Point	Port Role	Port State	Designated Bridge	Design
☐	1	GE1	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-1
☐	2	GE2	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-2
☐	3	GE3	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-3
☐	4	GE4	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-4
☐	5	GE5	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-5
☐	6	GE6	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-6
☐	7	GE7	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-7
☐	8	GE8	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-8
☐	9	GE9	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-9
☐	10	GE10	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-10
☐	11	GE11	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-11
☐	12	GE12	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-12

STP Port Setting page.

Field	Description
Port	Specify the interface ID or the list of interface IDs.
State	The operational state on the specified port.
Path Cost	STP path cost on the specified port.
Priority	STP priority on the specified port.
BPDU Filter	The states of BPDU filter on the specified port.
BPDU Guard	The states of BPDU guard on the specified port.
Operational Edge	The operational edge port status on the specified port.
Operational Point-to-Point	The operational point-to-point status on the specified port.
Port Role	The current port role on the specified port. The possible values are: "Disabled", "Master", "Root", "Designated", "Alternative", and "Backup".
Port State	The current port state on the specified port. The possible values are: "Disabled", "Discarding", "Learning", and "Forwarding".
Designated Bridge	The bridge ID of the designated bridge.
Designated Port ID	The designated port ID on the switch.
Designated Cost	The path cost of the designated port on the switch

STP Port Setting fields.

Field	Description
Protocol Migration Check	Restart the Spanning Tree Protocol (STP) migration process (re-negotiate with its neighborhood) on the specific interface.

STP Port Setting buttons.

Spanning Tree >> Port Setting

Edit Port Setting

Port	GE1
State	☐ Enable
Path Cost	0 (0 - 200000000) (0 = Auto)
Priority	128 ▼
Edge Port	☒ Auto ☐ Enable ☐ Disable
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

Edit STP Port Setting page.

Field	Description
State	Enable/Disable the STP on the specified port.
Path Cost	Specify the STP path cost on the specified port.
Priority	Specify the STP path cost on the specified port.
Edge Port	Specify the edge mode. Enable: Force to true state (as link to a host). Disable: Force to false state (as link to a bridge). In the edge mode, the interface would be put into the Forwarding state immediately upon link up. If the edge mode is enabled for the interface and there are BPDUs received on the interface, the loop might be occurred in the short time before the STP state change.

BPDU Filter	The BPDU Filter configuration avoids receiving/transmitting BPDU from the specified ports. Enable: Enable BPDU filter function. Disable: Disable BPDU filter function.
BPDU Guard	The BPDU Guard configuration to drop the received BPDU directly. Enable: Enable BPDU guard function. Disable: Disable BPDU guard function.
Point-to-Point	Specify the Point-to-Point port configuration: Auto: The state is depended on the duplex setting of the port Enable: Force to true state. Disable: Force to false state.

Edit STP Port Setting fields.

7.3. MST Instance

To configure MST instance setting, click **Spanning Tree > MST Instance**.

Spanning Tree >> MST Instance

MST Instance Table

	MSTI	Priority	Bridge Identifier	Designated Root Bridge	Root Port	Root Path Cost	Remaining Hop	VLAN
☐	0	32768	32768-82:24:02:19:00:01	0-00:00:00:00:00:00	N/A	0	0	1-4094
☐	1	32768	32768-82:24:02:19:00:01	0-00:00:00:00:00:00	N/A	0	0	
☐	2	32768	32768-82:24:02:19:00:01	0-00:00:00:00:00:00	N/A	0	0	
☐	3	32768	32768-82:24:02:19:00:01	0-00:00:00:00:00:00	N/A	0	0	
☐	4	32768	32768-82:24:02:19:00:01	0-00:00:00:00:00:00	N/A	0	0	
☐	5	32768	32768-82:24:02:19:00:01	0-00:00:00:00:00:00	N/A	0	0	
☐	6	32768	32768-82:24:02:19:00:01	0-00:00:00:00:00:00	N/A	0	0	
☐	7	32768	32768-82:24:02:19:00:01	0-00:00:00:00:00:00	N/A	0	0	
☐	8	32768	32768-82:24:02:19:00:01	0-00:00:00:00:00:00	N/A	0	0	
☐	9	32768	32768-82:24:02:19:00:01	0-00:00:00:00:00:00	N/A	0	0	
☐	10	32768	32768-82:24:02:19:00:01	0-00:00:00:00:00:00	N/A	0	0	
☐	11	32768	32768-82:24:02:19:00:01	0-00:00:00:00:00:00	N/A	0	0	
☐	12	32768	32768-82:24:02:19:00:01	0-00:00:00:00:00:00	N/A	0	0	
☐	13	32768	32768-82:24:02:19:00:01	0-00:00:00:00:00:00	N/A	0	0	
☐	14	32768	32768-82:24:02:19:00:01	0-00:00:00:00:00:00	N/A	0	0	
☐	15	32768	32768-82:24:02:19:00:01	0-00:00:00:00:00:00	N/A	0	0	

Edit

MST Instance page.

Field	Description
MSTI	MST instance ID.
Priority	The bridge priority on the specified MSTI.
Bridge Identifier	The bridge identifier on the specified MSTI.
Designated Root Bridge	The designated root bridge identifier on the specified MSTI.
Root Port	The designated root port on the specified MSTI.
Root Path Cost	The designated root path cost on the specified MSTI.
Remaining Hop	The configuration of remaining hop on the specified MSTI.
VLAN	The VLAN configuration on the specified MSTI.

MST Instance fields.

Spanning Tree >> MST Instance

Edit MST Instance Setting

MSTI

0

Priority

(0 - 61440, default 32768)

Bridge Identifier

32768-82:24:02:19:00:01

Designated Root Bridge

0-00:00:00:00:00:00

Root Port

Root Path Cost

0

Remaining Hop

0

Apply

Close

Edit MST Instance page.

Field	Description
VLAN	Select the VLAN list for the specified MSTI.

Priority	Specify the bridge priority on the specified MSTI. The valid range is from 0 to 61440, and the value must be the multiple of 4096. It ensures the probability that the switch is selected as the root bridge, and the lower values has the higher priority for the switch to be selected as the root bridge of the STP topology.
----------	--

Edit MST Instance fields.

7.4. MST Port Setting

To configure and display MST port setting, click **Spanning Tree > MST Port Setting**.

Spanning Tree >> MST Port Setting

MST Port Setting Table

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	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-4	0	20
☐	5	GE5	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-5	0	20
☐	6	GE6	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-6	0	20
☐	7	GE7	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-7	0	20
☐	8	GE8	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-8	0	20
☐	9	GE9	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-9	0	20
☐	10	GE10	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-10	0	20
☐	11	GE11	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-11	0	20

MST Port Setting page.

Field	Description
MSTI	Specify the port setting on the specified MSTI
Port	Specify the interface ID or the list of interface IDs.
Path Cost	The port path cost on the specified MSTI.
Priority	The port priority on the specified MSTI.
Port Role	The current port role on the specified port. The possible values are: "Disabled", "Master", "Root", "Designated", "Alternative", and "Backup".
Port State	The current port state on the specified port. The possible values are: "Disabled", "Discarding", "Learning", and "Forwarding".
Mode	The operational STP mode on the specified port.

Type	The possible value for the port type are: Boundary: The port attaching an MST Bridge to a LAN that is not in the same region. Internal: The port attaching an MST Bridge to a LAN that is not in the same region.
Designated Bridge	The bridge ID of the designated bridge.
Designated Port ID	The designated port ID on the switch.
Designated Cost	The path cost of the designated port on the switch
Remaining Hop	The remaining hops count on the specified port.

MST Port Setting fields.

Spanning Tree >> MST Port Setting

Edit MST Port Setting

MSTI	0
Port	GE1
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

Edit MST Port Setting page.

Field	Description
-------	-------------

Path Cost	Specify the STP port path cost on the specified MSTI.
Priority	Specify the STP port priority on the specified MSTI.

Edit MST Port Setting fields.

7.5. Statistics

To display the STP statistics, click **Spanning Tree > Statistics**.

Spanning Tree >> Statistics

Statistics Table

Refresh Rate sec

☐	Entry	Port	Receive BPDU			Transmit BPDU			
			Config	TCN	MSTP	Config	TCN	MSTP	
☐	1	GE1	0	0	0	0	0	0	
☐	2	GE2	0	0	0	0	0	0	
☐	3	GE3	0	0	0	0	0	0	
☐	4	GE4	0	0	0	0	0	0	
☐	5	GE5	0	0	0	0	0	0	
☐	6	GE6	0	0	0	0	0	0	
☐	7	GE7	0	0	0	0	0	0	
☐	8	GE8	0	0	0	0	0	0	

STP Statistics page.

Spanning Tree >> Statistics

STP Port Statistic

Port	GE1
Refresh Rate	☒ None ☐ 5 sec ☐ 10 sec ☐ 30 sec
Receive BPDU	
Config	0
TCN	0
MSTP	0
Transmit BPDU	
Config	0
TCN	0
MSTP	0

View STP Port Statistics page.

Field	Description
Refresh Rate	The option to refresh the statistics automatically.
Receive BPDU (Config)	The counts of the received CONFIG BPDU.
Receive BPDU (TCN)	The counts of the received TCN BPDU.
Receive BPDU (MSTP)	The counts of the received MSTP BPDU.
Transmit BPDU (Config)	The counts of the transmitted CONFIG BPDU.
Transmit BPDU (TCN)	The counts of the transmitted TCN BPDU.
Transmit BPDU (MSTP)	The counts of the transmitted MSTP BPDU.
Clear	Clear the statistics for the selected interfaces
View	View the statistics for the interface.

View STP Statistic fields.

Field	Description
-------	-------------

Clear	Clear the statistics for the selected interfaces
View	View the statistics for the interface.

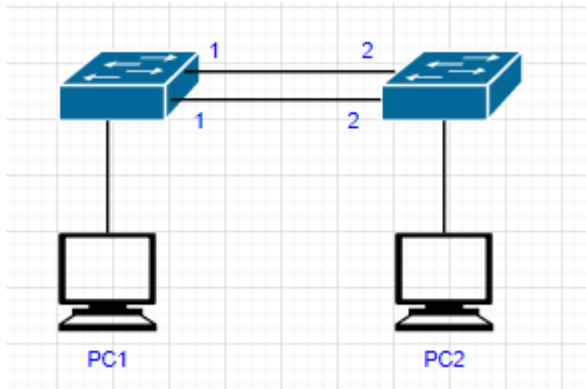
View STP Statistic buttons.

Field	Description
Refresh Rate	The option to refresh the statistics automatically.
Clear	Clear the statistics for the selected interfaces

View STP Port Statistic buttons.

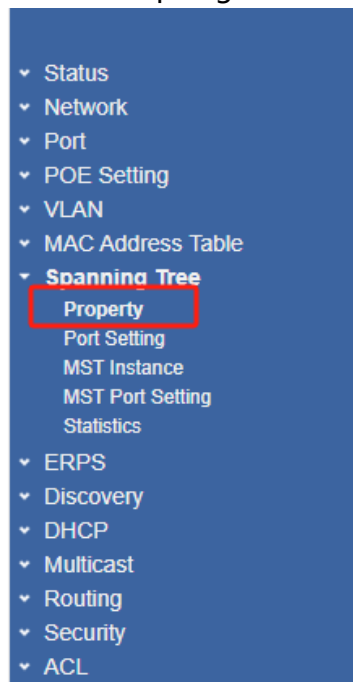
7.6.Example of configuration

Case 1: Two switches form a ring through RSTP to eliminate the loop, with SW1 serving as the root bridge.



WEB SW1

1. Enable rstp in global mode and configure rstp priority to 4096



Spanning Tree >> Property

State	☒ Enable
Operation Mode	☐ STP ☒ RSTP ☐ MSTP
Path Cost	☒ Long ☐ Short
BPDU Handling	☐ Filtering ☒ Flooding
Priority	4096 (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)

2. Enable rstp under the port

Spanning Tree >> Port Setting

Port Setting Table

Entry	Port	State	Path Cost	Priority	BPDU Filter	BPDU Guard	Operational Edge	Operational Point-to-Point	Port Role	Port State	Designated Bridge
1	GE1	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00 1
2	GE2	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00 1
3	GE3	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00 1
4	GE4	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00 1
5	GE5	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00 1
6	GE6	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00 1

- SW2 webconfig

1. Enable RSTP globally

Spanning Tree >> Property

State ☒ Enable

Operation Mode ☐ STP ☒ RSTP ☐ MSTP

Path Cost ☒ Long ☐ Short

BPDU Handling ☐ Filtering ☒ Flooding

Priority (0 - 61440, default 32768)

Hello Time Sec (1 - 10, default 2)

Max Age Sec (6 - 40, default 20)

Forward Delay Sec (4 - 30, default 15)

Tx Hold Count (1 - 10, default 6)

Region Name

2. Enable rstp under the port

Spanning Tree >> Port Setting

Port Setting Table

Entry	Port	State	Path Cost	Priority	BPDU Filter	BPDU Guard	Operational Edge	Operational Point-to-Point	Port Role	Port State	Designated Bridge
1	GE1	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00 1
2	GE2	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00 1
3	GE3	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00 1
4	GE4	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00 1
5	GE5	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00 1
6	GE6	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00 1

- SW1/SW2 CLI config

SW1:

spanning-tree

spanning-tree priority 4096

spanning-tree mst configuration

name "00:E0:4C:00:00:00"

spanning-tree mst 0 priority 4096

interface gi1

spanning-tree

!

```
interface gi2
 spanning-tree
SW2:
 spanning-tree
 spanning-tree mst configuration
  name "00:E0:4C:00:00:00"
interface gi1
 spanning-tree
!
interface gi2
 spanning-tree
```

8. ERPS

ERPS (Ethernet Ring Protection Switching) is a G.8032 ring network protection protocol issued by ITU-T. The convergence speed can meet the requirements of carrier-class reliability. If all the devices in the ring network support this protocol, they can realize intercommunication.

The concept of ERPS protocol mainly includes ERPS ring, node, port role and port status.

1. ERPS example

Unlike spanning tree instances, it is a concept of domains similar to ERRP. A group of switches configured with the same instance ID and control VLAN and interconnected constitutes an ERPS instance.

2. Control VLAN

The control VLAN is the transmission VLAN of ERPS protocol packets, which has the same function as the control VLAN in ERRP, and the protocol packets will carry the TAG corresponding to the control VLAN.

3. RPL

Ring Protection Link, Link designated by mechanism that is blocked during Idle state to prevent loop on Bridged ring

4. ERPS ring

It consists of a group of interconnected Layer 2 switching devices configured with the same control VLAN, and is the basic unit of the ERPS protocol.

5. Node

Layer 2 switching devices joining the ERPS ring are called nodes. Each node cannot join more than two ports in the same ERPS ring. Nodes are divided into four categories: RPL Owner, Neighbor, Next Neighbor and Common.

6. Port role

According to the ERPS protocol, the port roles mainly include RPL Owner, Neighbor, Next Neighbor and Common port four categories:

- RPL Owner: An ERPS ring has only one RPL Owner port, which is determined by user configuration. Blocking the RPL Owner port prevents loops in the ERPS ring. A node with an RPL Owner port becomes an RPL Owner

node.

- RPL Neighbor: An ERPS ring has only one RPL Neighbor (neighbor) port, which is configured by the user and must be the port connected to the RPL Owner port. When the network is normal, it will be blocked together with the RPL Owner port to prevent loops in the ERPS ring. Nodes with RPL Neighbor ports become RPL Neighbor nodes.
- RPL Next Neighbor: An ERPS ring can have up to 2 RPL Next Neighbor ports, which are configured by the user. They must be ports connected to the RPL Owner node or the RPL Neighbor node. The node with the RPL Next Neighbor port on the port becomes the RPL Next Neighbor node.
- Note: RPL Next Neighbor nodes are not much different from common nodes, and can be replaced by Common nodes during configuration.
- Common: common port, all ports other than RPL Owner, Neighbor, and Next Neighbor ports are common ports. If a node has only common ports, the node becomes a common node.

7. Port Status

In the ERPS ring, there are three types of port states for starting the ERPS protocol.

- Forwarding: In the Forwarding state, the port not only forwards user traffic but also receives/sends R-APS packets, and can also forward R-APS packets of other nodes.
- Discarding: In the Discarding state, the port can only receive/send R-APS packets, and cannot forward R-APS packets of other nodes.
- Disable: The state when the port is Linkdown.

8. Wrok Mode: ERPS working mode

There are revertive (reversible) and non revertive (irreversible) two.

- Revertive mode, when the link fails, the RPL link releases protection, and when the faulty link returns to normal, the RPL link is re-protected to prevent loops;
- Non revertive mode, after the fault is restored, the faulty node remains faulty (does not enter Forwarding), and the RPL link is always in the release protection state.

8.1. Function configuration

Click the "ERPS>Function Configuration" menu in the navigation tree to enter the "Function Configuration" interface, and configure the ERPS protocol to be enabled or disabled.

ERPS >> Property

Erps Status

☐ Disable
☒ Enable

Apply

8.2. Examples of ERPS

1. Click the "ERPS>ERPS Instance" menu in the navigation tree to enter the "ERPS Instance" interface, create an ERPS instance, view the configuration information of each instance, and delete the instance.

ERPS >> ERPS Instance

Erps Instance

1 (0 - 15)

Apply

ERPS Instance Setting

Instance	Ring Status	Mel	Control Vlan	WTR Time	Guard Time	Work Mode	Ring ID	Ring Type	Protected Instance	Port0	Port Role	Port Status	Port1	Port Role	Port Status	N
Ins0	Disabled	0	0	5	500	revertive	1	0	---	N/A	N/A	N/A	N/A	N/A	N/A	ini
Ins1	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

2.Select the instance, note that the instance needs to be created first, and click the Modify button to enter the instance configuration page.

ERPS >> ERPS Instance

Ring Instane Config

Ins

0

Ring Status

☒ Disable
 ☐ Enable

Mel

0 (Valid range is 0-7)

Protected Instance

0 (Valid range is 0-15)

Control Vlan

0 (Valid range is 1-4094)

WTR Time

5 (Valid range is 1-12 Min Default is 5 Min)

Guard Time

500 (Valid range is 100-2000 ms. Default is 500 ms)

Work Mode

☒ Revertive
 ☐ Non_revertive

Ring ID

1 (Valid range is 1-239)

Ring Type

0 (0-master ring, 1-sub ring)

Port0

N/A

Port0 Role

☒ Normal
 ☐ owner
 ☐ neighbour
 ☐ next-neighbour

Port1

N/A

Port1 Role

☒ Normal
 ☐ owner
 ☐ neighbour
 ☐ next-neighbour

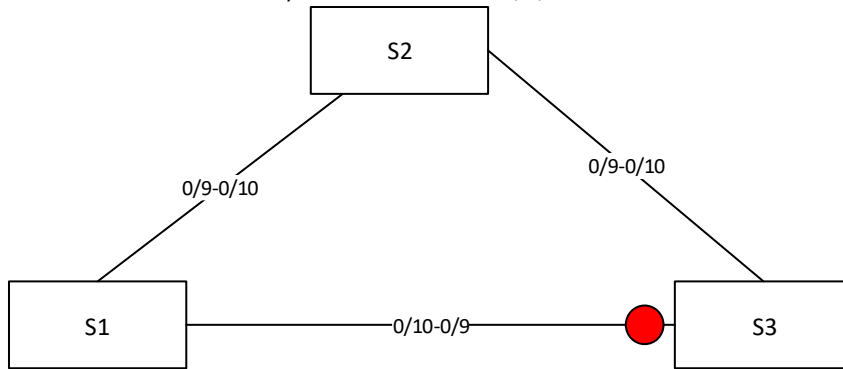
Apply

Close

8.3. Example of configuration

As shown in the figure, the configuration defaults to blocking the direct link between S1 and S2, and promptly restoring the link in case of a failure

to ensure network availability. The data VLANs are 1, 2, and 3.



- WEB config
1.S1/S2:
1.1.Create data VLAN 2,3,1000; VLAN 1 exists by default

VLAN >> VLAN >> Create VLAN

- 1.2.Change the interface mode to trunk, which by default will add all data VLANs and management VLANs to the interface forwarding

VLAN >> VLAN >> Membership

Membership Table

	Entry	Port	Mode	Administrative VLAN	Operational VLAN
☐	1	GE1	Trunk	1UP	1UP
☐	2	GE2	Trunk	1UP	1UP
☐	3	GE3	Trunk	1UP	1UP
☐	4	GE4	Trunk	1UP	1UP
☐	5	GE5	Trunk	1UP	1UP
☐	6	GE6	Trunk	1UP	1UP
☐	7	GE7	Trunk	1UP	1UP
☐	8	GE8	Trunk	1UP	1UP
☐	9	GE9	Trunk	1UP, 2T, 3T, 1000T	1UP, 2T, 3T, 1000T
☐	10	GE10	Trunk	1UP, 2T, 3T, 1000T	1UP, 2T, 3T, 1000T
☐	11	GE11	Trunk	1UP	1UP

- 1.3.Create ERPs ring 1 and associate instance0

ERPS >> Propety

Erps Status ☐ Disable ☒ Enable

Apply

ERPS >> ERPS Instance

Erps Instance (0 - 15)

Apply

RPS Instance Setting

☐	Instance	Ring Status	MeI	Control Vlan	WTR Time	Guard Time	Work Mode	Ring ID	Ring Type	Protected Instance	Port0	Port Role	Port Status	Port1	Port Rol
☐	Ins0	Enabled	0	1000	1	500	revertive	1	0	0	gi9	rpl	disabled	gi10	rpl
☐	Ins1	---					---								

2.S3:

2.1.Create data VLAN 2,31000; VLAN 1 exists by default

VLAN >> VLAN >> Create VLAN

VLAN

Available VLAN

VLAN 4
VLAN 5
VLAN 6
VLAN 7
VLAN 8
VLAN 9
VLAN 10
VLAN 11

Created VLAN

VLAN 1
VLAN 2
VLAN 3
VLAN 1000

Apply

2.2.the interface mode to trunk, which by default will add all data VLANs and management VLANs to the interface forwarding

VLAN >> VLAN >> Membership

Membership Table

	Entry	Port	Mode	Administrative VLAN	Operational VLAN
☐	1	GE1	Trunk	1UP	1UP
☐	2	GE2	Trunk	1UP	1UP
☐	3	GE3	Trunk	1UP	1UP
☐	4	GE4	Trunk	1UP	1UP
☐	5	GE5	Trunk	1UP	1UP
☐	6	GE6	Trunk	1UP	1UP
☐	7	GE7	Trunk	1UP	1UP
☐	8	GE8	Trunk	1UP	1UP
☐	9	GE9	Trunk	1UP, 2T, 3T, 1000T	1UP, 2T, 3T, 1000T
☐	10	GE10	Trunk	1UP, 2T, 3T, 1000T	1UP, 2T, 3T, 1000T
☐	11	GE11	Trunk	1UP	1UP

2.3.Create ERPs ring 1 and associate instance0

ERPS >> Property

Erps Status

☐ Disable
☒ Enable

Apply

ERPS >> ERPS Instance

Erps Instance (0 - 15)

Apply

ERPS Instance Setting

☐	Instance	Ring Status	Mei	Control Vlan	WTR Time	Guard Time	Work Mode	Ring ID	Ring Type	Protected Instance	Port0	Port Role	Port Status	Port1	Port R
☐	Ins0	Enabled	0	1000	1	500	revertive	1	0	0	gi9	owner	disabled	gi10	rpl
☐	Ins1	---													

- CLI

1.S1/S2:

Enter global configuration mode, create ERPS and set relevant parameters. The command reference list is as follows:
Create data VLAN 2,3,1000; VLAN 1 exists by default

```
s1 #config
s1(config)# vlan 2-3,1000
s1(config-vlan)#
```

Change the interface mode to trunk, which by default will add all data VLANs and management VLANs to the interface forwarding

```
s1(config)# interface range GigabitEthernet 9-10
s1(config-if-range-GigabitEthernet9-10)# switchport mode trunk
s1(config-if-range-GigabitEthernet9-10)# switchport trunk allowed vlan add 2,3,1000
```

Create ERPs ring 1 and associate instance0

```
s1 (Config)#erps
s1(config)# erps instance 0
s1(config-erps-inst)#
s1(config-erps-inst)# wtr-timer 1
s1(config-erps-inst)# port0 gi9
s1(config-erps-inst)# port1 gi10
s1(config-erps-inst)# protected-instance 0
s1(config-erps-inst)# control-vlan 1000
s1(config-erps-inst)# ring enable
s1(config-erps-inst)#
```

2.S3:

Enter global configuration mode, create ERPS and set relevant parameters. The command reference list is as follows:
Create data VLAN 2,3,1000; VLAN 1 exists by default

```
s3 #config
s3(config)# vlan 2-3,1000
s3(config-vlan)#
```

Change the interface mode to trunk, which by default will add all data VLANs and management VLANs to the interface forwarding

```
s3(config)# interface range GigabitEthernet 9-10
s3(config-if-range-GigabitEthernet9-10)# switchport mode trunk
s3(config-if-range-GigabitEthernet9-10)# switchport trunk allowed vlan add 2,3,1000
```

Create ERPs ring 1 and associate instance0

```
s3 (Config)#erps
s3 (config)# erps instance 0
s3 (config-erps-inst)#
s3 (config-erps-inst)# wtr-timer 1
s3 (config-erps-inst)# port0 gi9 owner
s3 (config-erps-inst)# port1 gi10
s3 (config-erps-inst)# protected-instance 0
s3 (config-erps-inst)# control-vlan 1000
s3 (config-erps-inst)# ring enable
s3 (config-erps-inst)#
```

9. Discovery

9.1. LLDP

LLDP is a one-way protocol; there are no request/response sequences. Information is advertised by stations implementing the transmit function, and is received and processed by stations implementing the receive function. The LLDP category contains LLDP and LLDP-MED pages.

9.1.1. Property

To display LLDP Property Setting web page, click **Discovery > LLDP > Property**.

Discovery >> LLDP >> Property

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)

LLDP Property Setting

Field	Description
State	Enable/ Disable LLDP protocol on this switch.
LLDP Handling	Select LLDP PDU handling action to be filtered, bridging or flooded when LLDP is globally disabled. Filtering: Deletes the packet. Bridging: (VLAN-aware flooding) Forwards the packet to all VLAN members. Flooding: Forwards the packet to all ports
TLV Advertise Interval	Select the interval at which frames are transmitted. The default is 30 seconds, and the valid range is 5–32767 seconds.
Holdtime Multiplier	Select the multiplier on the transmit interval to assign to TTL (range 2–10, default = 4).
Reinitialization Delay	Select the delay before a re-initialization (range 1–10 seconds, default = 2).
Transmit Delay	Select the delay after an LLDP frame is sent (range 1–8191 seconds, default = 3).
Fast Start Repeat Count	Select fast start repeat count when port link up (range 1–10, default = 3).

LLDP Property Setting Fields

9.1.2. Port Setting

To display LLDP Port Setting, click **Discovery > LLDP > Port Setting**.

Discovery >> LLDP >> Port Setting

Port Setting Table

☐	Entry	Port	Mode	Selected TLV	
☐	1	GE1	Normal	802.1 PVID	
☐	2	GE2	Normal	802.1 PVID	
☐	3	GE3	Normal	802.1 PVID	
☐	4	GE4	Normal	802.1 PVID	
☐	5	GE5	Normal	802.1 PVID	
☐	6	GE6	Normal	802.1 PVID	
☐	7	GE7	Normal	802.1 PVID	
☐	8	GE8	Normal	802.1 PVID	

LLDP Port Setting Page

To Edit LLDP port setting web page, select the port which to set, click button **Edit**.

Discovery >> LLDP >> Port Setting

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

LLDP Port Edit Page

Field	Description
Port	Select specified port or all ports to configure LLDP state.
Mode	Select the transmission state of LLDP port interface. Disable: Disable the transmission of LLDP PDUs. RX Only: Receive LLDP PDUs only. TX Only: Transmit LLDP PDUs only. TX And RX: Transmit and receive LLDP PDUs both.
Optional TLV	Select the LLDP optional TLVs to be carried (multiple selection is allowed). System Name Port Description System Description System Capability

	802.3 MAC-PHY 802.3 Link Aggregation 802.3 Maximum Frame Size Management Address 802.1 PVID
802.1 VLAN Name	Select the VLAN Name ID to be carried (multiple selection is allowed).

LLDP Port Configuration Fields

9.1.3. MED Network Policy

To display LLDP MED Network Policy Setting, click **Discovery > LLDP > MED Network Policy**.

Discovery >> LLDP >> MED Network Policy

MED Network Policy Table

Showing All ▼ entries

Showing 0 to 0 of 0 entries

☐	Policy ID	Application	VLAN	VLAN Tag	Priority	DSCP	
0 results found.							
Add Edit Delete							

LLDP MED Network Policy Page

To Add LLDP MED Network Policy entry, Click button **Add**

To Edit LLDP MED Network Policy entry, select the entry which to edit, Click button **Edit**

Discovery >> LLDP >> MED Network Policy

Add MED Network Policy

Policy ID	1 ▼
Application	Voice ▼
VLAN	Range (0 - 4095)
VLAN Tag	☒ Tagged ☐ Untagged
Priority	0 ▼
DSCP	0 ▼

LLDP MED Network Policy Setting Page

Field	Description
Policy ID	Select specified network policy ID to configure.
Application	Select the network policy application type. Voice Voice Signaling Guest Voice Guest Voice Signaling Softphone Voice Video Conferencing App Streaming Video Video Signaling
VLAN	Set the VLAN ID, range from 1 to 4094.
VLAN Tag	Set the VLAN tag status. Tagged: Traffic is tagged. Untagged: Traffic is untagged.
Priority	Set the L2 priority, range from 0 to 7.
DSCP	Set the DSCP value, range from 0 to 63

LLDP MED Network Policy Configuration Fields

9.1.4. MED Port Setting

To display LLDP MED Port Setting, click **Discovery > LLDP > MED Port Setting**.

Discovery >> LLDP >> MED Port Setting

MED Port Setting Table

☐	Entry	Port	State	Network Policy		Location	Inventory	
				Active	Application			
☐	1	GE1	Enabled	Yes		No	No	
☐	2	GE2	Enabled	Yes		No	No	
☐	3	GE3	Enabled	Yes		No	No	
☐	4	GE4	Enabled	Yes		No	No	
☐	5	GE5	Enabled	Yes		No	No	
☐	6	GE6	Enabled	Yes		No	No	
☐	7	GE7	Enabled	Yes		No	No	
☐	8	GE8	Enabled	Yes		No	No	
☐	9	GE9	Enabled	Yes		No	No	
☐	10	GE10	Enabled	Yes		No	No	

LLDP MED Setting Page

To Edit LLDP MED port setting web page, select the port which to set, click button **Edit**.

Discovery >> LLDP >> MED Port Setting

Edit MED Port Setting

Port
GE1

State
☒ Enable

Optional TLV

Available TLV

Location
Inventory

Selected TLV

Network Policy

Network policy

Available Policy

Selected Policy

Location

Coordinate

(16 pairs of hexadecimal characters)

Civic

(6 - 160 pairs of hexadecimal characters)

ECS ELIN

(10 - 25 pairs of hexadecimal characters)

Apply

Close

LLDP MED Add/Edit Page

Field	Description
Port	Select specified port or all ports to configure LLDP MED.
State	Select LLDP MED enable status
Optional TLV	Select LLDP MED optional TLVs (multiple selection is allowed) Network Policy Location Inventory
Network Policy	Select the network policy IDs to be bound to ports. The network policy should be created in MED Network Policy page at first.

LLDP MED Port Configuration Fields

Field	Description
Coordinate	Set Coordinate
Civic	Set Civic

ECS ELIN

Set ECS ELIN

LLDP MED Port Location Configuration Fields

9.1.5. Packet View

To display LLDP Overloading, click **Discovery > LLDP > Packet View**.

Discovery >> LLDP >> Packet View

Packet View Table

	Entry	Port	In-Use (Bytes)	Available (Bytes)	Operational Status
☐	1	GE1	38	1450	Not Overloading
☐	2	GE2	38	1450	Not Overloading
☐	3	GE3	38	1450	Not Overloading
☐	4	GE4	38	1450	Not Overloading
☐	5	GE5	38	1450	Not Overloading
☐	6	GE6	38	1450	Not Overloading
☐	7	GE7	38	1450	Not Overloading
☐	8	GE8	38	1450	Not Overloading
☐	9	GE9	38	1450	Not Overloading
☐	10	GE10	39	1449	Not Overloading

LLDP Overloading Page

Field	Description
Port	Port Name
In-Use (Bytes)	Total number of bytes of LLDP information in each packet.
Available(Bytes)	Total number of available bytes left for additional LLDP information in each packet.
Operational Status	Overloading or not

LLDP Overloading Fields

If need detail information, select the port, then click **detail**

Discovery >> LLDP >> Packet View

Packet View Detail

Port	GE1
Mandatory TLVs	
Size (Bytes)	21
Operational Status	Transmitted
MED Capabilities	
Size (Bytes)	9
Operational Status	Transmitted
MED Location	
Size (Bytes)	0
Operational Status	Transmitted
MED Network Policy	
Size (Bytes)	0
Operational Status	Transmitted

Size (Bytes)	0
Operational Status	Transmitted
802.3 TLVs	
Size (Bytes)	0
Operational Status	Transmitted
Optional TLVs	
Size (Bytes)	0
Operational Status	Transmitted
802.1 TLVs	
Size (Bytes)	8
Operational Status	Transmitted
Total	
In-Use (Bytes)	38
Available (Bytes)	1450

Close

LLDP Overloading Detail Page

Field	Description
Port	Port Name
Mandatory TLVs	Total mandatory TLV byte size. Status is sent or overloading.
MED Capabilities	Total MED Capabilities TLV byte size. Status is sent or overloading.
MED Location	Total MED Location byte size. Status is sent or overloading.
MED Network Policy	Total MED Network Policy byte size. Status is sent or overloading.
MED Inventory	Total MED Inventory byte size. Status is sent or overloading.
MED Extended Power via MDI	Total MED Extended Power via MDI byte size. Status is sent or overloading.
802.3 TLVs	Total 802.3 TLVs byte size. Status is sent or overloading.
Optional TLVs	Total Optional TLV byte size. Status is sent or overloading.
802.1 TLVs	Total 802.1 TLVs byte size. Status is sent or overloading.
Total	Total number of bytes of LLDP information in each packet.

LLDP Overloading Detail Fields

9.1.6. Local Information

To display LLDP Local Device, click **Discovery > LLDP > Local Information**.

Use the LLDP Local Information to view LLDP local device information.

Discovery >> LLDP >> Local Information

Device Summary

Chassis ID Subtype	MAC address
Chassis ID	82:24:02:19:00:01
System Name	Switch
System Description	RTL9311
Supported Capabilities	Bridge, Router
Enabled Capabilities	Bridge, Router
Port ID Subtype	Local

Port Status Table

Field	Description
Chassis ID Subtype	Type of chassis ID, such as the MAC address.
Chassis ID	Identifier of chassis. Where the chassis ID subtype is a MAC address, the MAC address of the switch is displayed.
System Name	Name of switch.
System Description	Description of the switch.
Capabilities Supported	Primary functions of the device, such as Bridge, WLAN AP, or Router.
Capabilities Enabled	Primary enabled functions of the device.
Port ID Subtype	Type of the port identifier that is shown.
LLDP Status	LLDP Tx and Rx abilities.
LLDP Med Status	LLDP MED enable state.

LLDP Local Information Fields

Click “detail” button on the page to view detail information of the selected port.

Discovery >> LLDP >> Local Information

Detail

Local Information Detail

Chassis ID Subtype	MAC address
Chassis ID	82:24:02:19:00:01
System Name	Switch
System Description	RTL9311
Supported Capabilities	Bridge, Router
Enabled Capabilities	Bridge, Router
Port ID	GE37
Port ID Subtype	Local
Port Description	

Management Address Table				
Address Subtype	Address	Interface Subtype	Interface Number	
0 results found.				

MAC/PHY Detail	
Auto-Negotiation Supported	N/A
Auto-Negotiation Enabled	N/A
Auto-Negotiation Advertised Capabilities	N/A
Operational MAU Type	N/A
802.3 Detail	
802.3 Maximum Frame Size	N/A
802.3 Link Aggregation	
Aggregation Capability	N/A
Aggregation Status	N/A
Aggregation Port ID	N/A
MED Detail	
Capabilities Supported	Capabilities , Network policy
Current Capabilities	Capabilities , Network policy
Device Class	Network Connectivity
PoE Device Type	N/A

[Detail](#)

PoE Power Value	N/A
Hardware Revision	N/A
Firmware Revision	N/A
Software Revision	N/A
Serial Number	N/A
Manufacturer Name	N/A
Model Name	N/A
Asset ID	N/A

Location Information	
Civic	N/A
Coordinate	N/A
ECS ELIN	N/A

Network Policy Table					
Application Type	VLAN	VLAN Type	Priority	DSCP	
0 results found.					

[Close](#)

LLDP Local Information Detail Page

9.1.7. Neighbor

To display LLDP Remote Device, click **Discovery > LLDP > Neighbor**.

Use the LLDP Neighbor page to view LLDP neighbors information.

Click “detail” to view selected neighbor detail information.

Discovery >> LLDP >> Neighbor

Neighbor Table

Showing 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
☐	GE47	MAC address	68:F7:28:A1:B8:A0	MAC address	68:F7:28:A1:B8:A0		2887

Clear

Refresh

Detail

LLDP Neighbor Page

Field	Description
Local Port	Number of the local port to which the neighbor is connected.
Chassis ID Subtype	Type of chassis ID (for example, MAC address).
Chassis ID	Identifier of the 802 LAN neighboring device's chassis.
Port ID Subtype	Type of the port identifier that is shown.
Port ID	Identifier of port.
System Name	Published name of the switch.
Time to Live	Time interval in seconds after which the information for this neighbor is deleted.

LLDP Neighbor Fields

9.1.8. Statistics

To display LLDP Statistics status, click **Discovery > LLDP > Statistics**.

The Link Layer Discovery Protocol (LLDP) Statistics page displays summary and per-port information for LLDP frames transmitted and received on the switch.

Discovery >> LLDP >> Statistics

Global Statistics

Insertions	1
Deletions	0
Drops	0
AgeOuts	0

Clear

Refresh

Statistics Table

☐	Entry	Port	Transmit Frame	Receive Frame			Receive TLV		Neighbor Timeout	
			Total	Total	Discard	Error	Discard	Unrecognized		
☐	1	GE1	0	0	0	0	0	0	0	
☐	2	GE2	0	0	0	0	0	0	0	
☐	3	GE3	0	0	0	0	0	0	0	
☐	4	GE4	0	0	0	0	0	0	0	

LLDP Statistics Page

Field	Description
Insertions	The number of times the complete set of information advertised by a particular MAC Service Access Point (MSAP) has been inserted into tables associated with the remote systems.
Deletions	The number of times the complete set of information advertised by MSAP has been deleted from tables associated with the remote systems.
Drops	The number of times the complete set of information advertised by MSAP could not be entered into tables associated with the remote systems because of insufficient resources.
Age Outs	The number of times the complete set of information advertised by MSAP has been deleted from tables associated with the remote systems because the information timeliness interval has expired.
Port	Interface or port number.
Transmit Frame Total	Number of LLDP frames transmitted on the corresponding port.
Receive Frame Total	Number of LLDP frames received by this LLDP agent on the corresponding port, while the LLDP agent is enabled.
Receive Frame Discard	Number of LLDP frames discarded for any reason by the LLDP agent on the corresponding port.
Receive Frame Error	Number of invalid LLDP frames received by the LLDP agent on the corresponding port, while the LLDP agent is enabled.
Receive TLV Discard	Number of TLVs of LLDP frames discarded for any reason by the LLDP agent on the corresponding port.
Receive TLV Unrecognized	Number of TLVs of LLDP frames that are unrecognized while the LLDP agent is enabled
Neighbor Timeout	Number of age out LLDP frames.

LLDP Statistics Fields

9.2. Example of Basic LDP Function Configuration

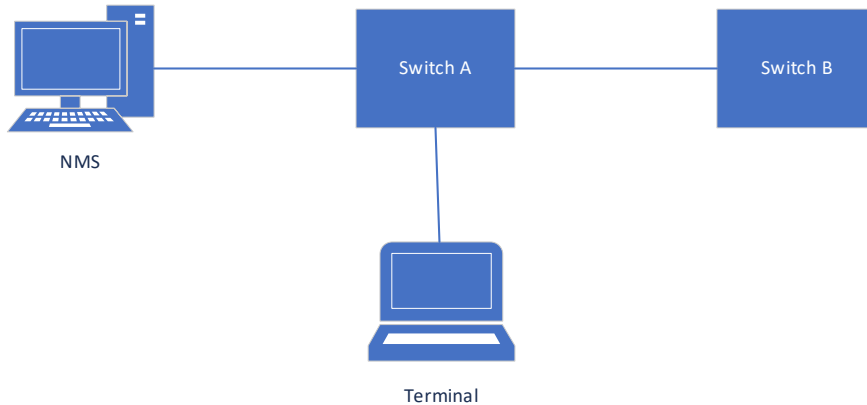
Networking requirements

NMS (Network Management System) is connected to switch A, which is respectively connected to terminal devices and switch B.

By configuring LLDP functionality on switch A and switch B, NMS can assess the communication status between switch A and terminal devices, as well as between switch A and switch B.

Networking diagram

LLDP Basic Function Configuration Network Diagram



- Web
 - 1.Enable LLDP globally

Discovery >> LLDP >> Property

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

- 2.Enable LLDP on Port 1 and Port 2

Discovery >> LLDP >> Port Setting

Port Setting Table

☐	Entry	Port	Mode	Selected TLV
☐	1	GE1	Normal	Port Description , System Name , System Description , System Capabilities , 802.3 MAC-PHY , 802.3 Link Aggregation , 802.3 Maximum Frame Size , Management
☐	2	GE2	Normal	Port Description , System Name , System Description , System Capabilities , 802.3 MAC-PHY , 802.3 Link Aggregation , 802.3 Maximum Frame Size , Management
☐	3	GE3	Normal	802.1 PVID

- CLI
 - switch A/B:

```

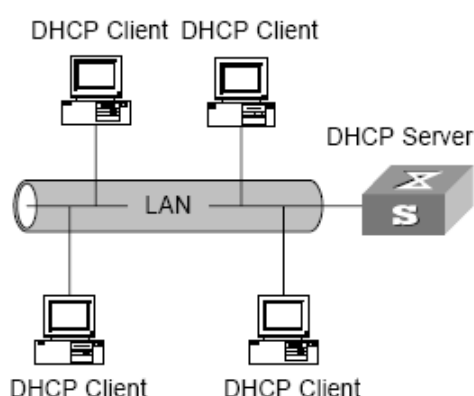
interface gi1
lldp tlv-select port-desc sys-name sys-desc sys-cap mac-phy lag max-frame-size management-addr
lldp tlv-select vlan-name add 1

interface gi2
lldp tlv-select port-desc sys-name sys-desc sys-cap mac-phy lag max-frame-size management-addr
lldp tlv-select vlan-name add 1
  
```

10. DHCP

With the expansion of the network scale and the improvement of the network complexity, the network configuration becomes more and more complex, and the computer location changes (such as a laptop or wireless network) and the number of computers exceeds the assignable IP addresses often occur. The Dynamic Host Configuration Protocol (DHCP) was developed to meet these requirements. The DHCP protocol works in the client/server mode. The DHCP Client dynamically requests configuration information from the DHCP Server, and the DHCP Server returns corresponding configuration information according to policies.

In a typical application of DHCP, it generally includes a DHCP server and multiple clients (such as PCs and laptops)



10.1. Function configuration

1. Click the "DHCP>Property" menu in the navigation tree to enter the "DHCP Function Configuration" interface, enable the configuration of the dhcpserver, and view the DHCP Port configuration information.

DHCP >> Property

State	☐ Enable
Static Binding First	☐ Enable

Apply

DHCP Port Setting Table

☐	Entry	Port	State
☐	1	GE1	Disabled
☐	2	GE2	Disabled
☐	3	GE3	Disabled
☐	4	GE4	Disabled
☐	5	GE5	Disabled
☐	6	GE6	Disabled
☐	7	GE7	Disabled
☐	8	GE8	Disabled

2. Click Modify to enter the port configuration page, where you can enable or disable the dhcp server function under the port.

DHCP >> Property

Edit Port Setting

Port	GE1
State	☐ Enable

10.2. Address pool configuration

1. Click Modify to enter the port configuration page, where you can enable or disable the dhcp server function under the port.

1CP >> IP Pool Setting

Pool Table

Showing 0 to 0 of 0 entries

Pool	Section	Start Address	End Address	Gateway	Mask	DNS Primary Server	DNS Second Server	option 43		Lease time
								Address	Format	
0 results found.										

2. Click the Add or Modify button to increase the address pool.

DHCP >> IP Pool Setting

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
option 43	☐ ascii ☐ hex
Lease time	1 Day 00 Hour 00 Minute

10.3. VLAN interface address group configuration

1. Click the "DHCP> VLAN IF Address Group Setting" menu in the navigation tree to enter the "VLAN interface address group configuration" interface, configure and view the VLAN interface address group configuration and the dhcp server group table.

DHCP >> VLAN IF Address Group Setting

Vlan Interface Address Pool Table

Interface	VLAN 1
DHCP Server Group	

Apply

DHCP Server Group Table

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

Add Edit Delete

2. Click the Add or Modify button to add a DHCP server group.

DHCP >> VLAN IF Address Group Setting

DHCP Server Group Table

DHCP Server Group	1
Group IP Address	

Apply Close

10.4. Client list

1. Click the "DHCP> Client List" menu in the navigation tree to enter the "Client List" interface to view the DHCP client list information.

DHCP >> Client List

DHCP Client List

Showing All entries Showing 0 to 0 of 0 entries

MAC Address Table	IPv4 Address	VLAN	Hostname	
0 results found.				

Refresh

First Previous 1 Next Last

10.5. Client Static Binding Table

1. Click the "DHCP>Client Static Binding Table" menu in the navigation tree to enter the "Client Static Binding Table" interface.

DHCP >> Client Static Binding Table

Static Binding Table

Showing All entries Showing 0 to 0 of 0 entries

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

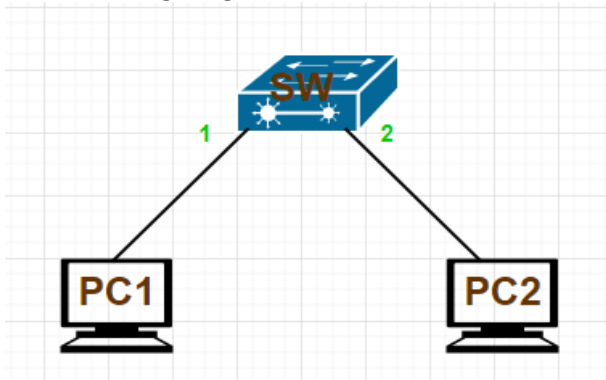
Add Delete

First Previous 1 Next Last

3. Click the Add button to configure the static binding table for the client.

10.6. Example of configuration

Case 1: Configuring Port Authentication



PC2 according to radius server

- WEB

1. Configure the address of vianif1, enable DHCP globally, and enable DHCP on ports

[Routing](#) >> [IPv4 Management and Interfaces](#) >> [IPv4 Interface](#)

IPv4 Interface Table

☐	Interface	IP Address Type	IP Address	Mask	Status	Roles
☐	VLAN 1	Static	192.168.0.1	255.255.255.0	Valid	primary

DHCP >> Property

State ☒ Enable

Static Binding First ☐ Enable

DHCP Port Setting Table

☐	Entry	Port	State
☐	1	GE1	Disabled
☐	2	GE2	Enabled
☐	3	GE3	Disabled

2. Configure pool

DHCP >> IP Pool Setting

IP Pool Table

Showing All entries

Showing 1 to 1 of 1 entries

Q

☐	Pool	Section			Gateway	Mask	DNS Primary Server	DNS Second Server	option 43		Lease time	
		Section	Start Address	End Address					Address	Format		
☐	1	1	192.168.0.2	192.168.0.100	192.168.0.1	255.255.255.0	114.114.114.114	0.0.0.0	ascii		1:0:0	

First Previous 1 Next Last

3. Configure VLAN address

DHCP >> VLAN IF Address Group Setting

Vlan Interface Address Pool Table

Interface

VLAN 1

DHCP Server Group

1

Apply

DHCP Server Group Table

	Group ID	Group IP Address	Bind VLAN Interface
☐	1	192.168.0.1	vlan 1

Add

Edit

Delete

● CLI

```

interface vlan1
ip address 192.168.0.1/24
dhcp-server group 1
interface gi2
dhcp-relay
exit
config
dhcp-server
dhcp-server group 1 ip 192.168.0.1
ip pool 1
gateway 192.168.0.1/24
dns primary-ip 114.114.114.114
dns second-ip'8.8.8.8
section 1 192.168.0.2 192.168.0.100

```

11. Multicast

11.1. General

Use the General pages to configure settings of IGMP and MLD common function.

11.1.1. Property

To display multicast general property Setting web page, click **Multicast> General> Property**

This page allow user to set multicast forwarding method and unknown multicast action.

Multicast >> General >> Property

Multicast General Properties Page

Field	Description
Unknown Multicast Action	Set the unknown multicast action Drop: drop the unknown multicast data. Flood: flood the unknown multicast data. Router port: forward the unknown multicast data to router port.
IPv4	Set the ipv4 multicast forward method. MAC-VID: forward method dmac+vid. DIP-VID: forward method dip+vid.
IPv6	Set the ipv6 multicast forward method. MAC-VID: forward method dmac+vid. DIP-VID: forward method dip+vid(dip is ipv6 low 32 bit).

Multicast General Property Setting Fields

11.1.2. Group Address

To display Multicast General Group web page, click **Multicast> General> Group Address**

This page allow user to browse all multicast groups that dynamic learned or statically added.

Multicast >> General >> Group Address

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 Edit Delete Refresh						

Multicast Group Address Table Page

Field	Description
IP Version	IP Version IPv4: ipv4 multicast group. IPv6: ipv6 multicast group
VLAN	The VLAN ID of group.
Group Address	The group IP address.
Member	The member ports of group.
Type	The type of group. Static or Dynamic.
Life(Sec)	The life time of this dynamic group.

Multicast Group Address Table Fields

Multicast >> General >> Group Address

Add Group Address

The screenshot shows the 'Add Group Address' configuration window. It includes the following elements:

- VLAN:** A dropdown menu currently showing '1'.
- IP Version:** A dropdown menu currently showing 'IPv4'.
- Group Address:** An empty text input field.
- Member:** A large container box with two sub-sections:
 - Available Port:** A list box containing the following items: GE1, GE2, GE3, GE4, GE5, GE6, GE7, and GE8.
 - Selected Port:** An empty list box.
 - Between the two list boxes are two arrow buttons: a right-pointing arrow and a left-pointing arrow.
- Buttons:** At the bottom of the window are two buttons: 'Apply' and 'Close'.

Multicast Group Address Add Page

Field	Description
VLAN	The VLAN ID of group.
IP Version	IP Version IPv4: ipv4 multicast group IPv6: ipv6 multicast group
Group Address	The group IP address.
Member	The member ports of group. Available Port: Optional port member. Selected Port: Selected port member

Multicast Group Address Add Fields

Multicast >> General >> Group Address

Add Group Address

VLAN

1

IP Version

IPv4

Group Address

Member

Available Port

Selected Port

GE1

GE2

GE3

GE4

GE5

GE6

GE7

GE8

Apply

Close

Multicast Group Address Edit Page

Field	Description
VLAN	The VLAN ID of edited group.
Group Address	The group IP address.
Member	The member ports of group. Available Port: Optional port member. Selected Port: Selected port member.

Table 9-4 Multicast Group Address Edit Fields

11.1.3. Router Port

To display multicast router port table web page, click **Multicast> General> Router Port**

This page allow user to browse all router port information. The static and forbidden router port can set by user.

Router Port Table

IP Version

IPv4

Showing

All

 entries

Showing 0 to 0 of 0 entries

Q

☐	VLAN	Member	Static Port	Forbidden Port	Life (Sec)
--------------------------	------	--------	-------------	----------------	------------

0 results found.

Add

Edit

Refresh

First

Previous

1

Next

Last

Multicast Router Table Page

Field	Description
IP Version	IP Version IPv4: ipv4 multicast router IPv6: ipv6 multicast router
VLAN	The VLAN ID router entry
Member	Router Port member (include static and learned port member).
Static Port	Static router port member
Forbidden Port	Forbidden router port member
Life (Sec)	The expiry time of the router entry.

Multicast Router Table Fields

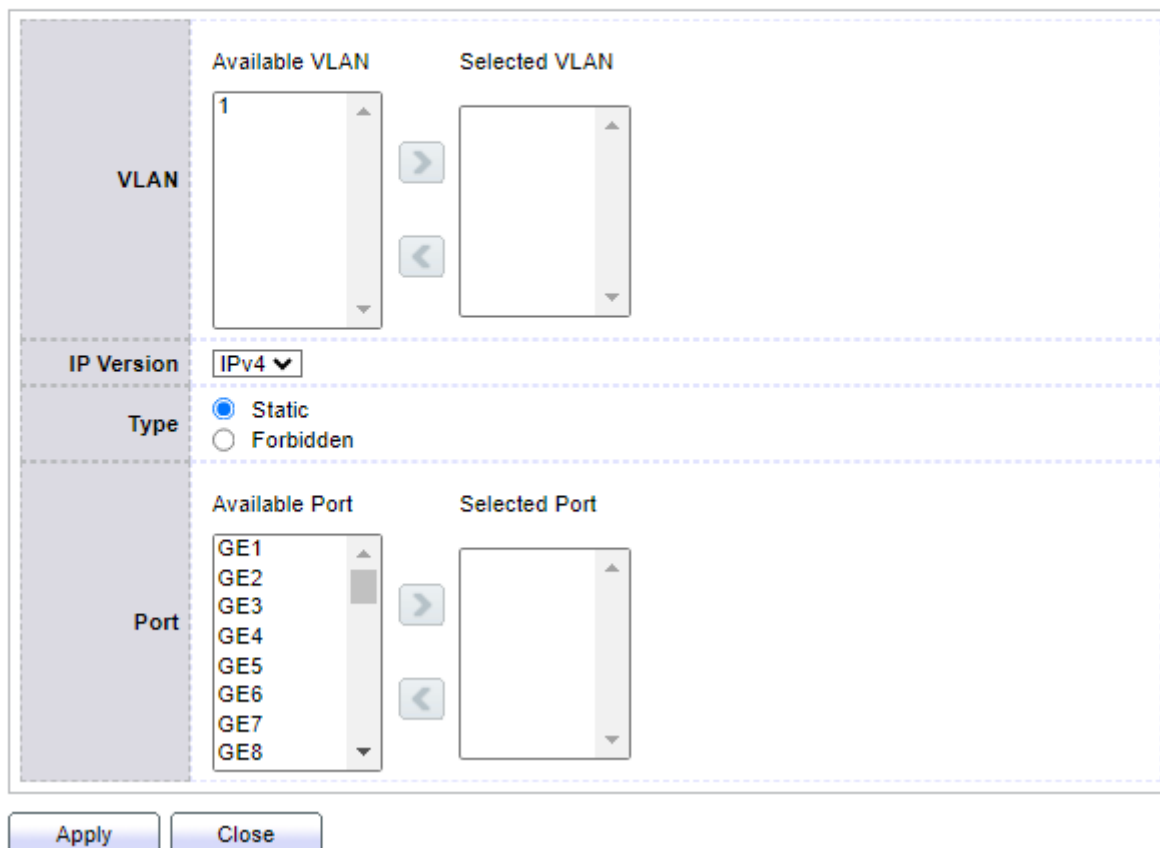
Managed Switch software

1

www.ewindnet.com

Multicast >> General >> Router Port

Add Router Port



The 'Add Router Port' window is divided into four main sections: VLAN, IP Version, Type, and Port. The VLAN section contains two lists: 'Available VLAN' with '1' selected and 'Selected VLAN' which is empty. The IP Version section has a dropdown menu set to 'IPv4'. The Type section has two radio buttons: 'Static' (selected) and 'Forbidden'. The Port section contains two lists: 'Available Port' with 'GE1' through 'GE8' listed, and 'Selected Port' which is empty. Navigation buttons 'Apply' and 'Close' are at the bottom.

Multicast Router Add Page

Field	Description
VLAN	The VLAN ID for router entry Available VLAN: Optional VLAN member Selected VLAN: Selected VLAN member
IP Version	IP Version IPv4: ipv4 multicast router IPv6: ipv6 multicast router
Type	The router port type Static: static router port Forbidden: forbidden router port, can't learn dynamic router port member
Port	The member ports of router entry. Available Port: Optional router port member Selected Port: Selected router port member

Multicast Router Add Fields

Multicast >> General >> Router Port

Add Router Port

VLAN

Available VLAN

1

Selected VLAN

>

<

IP Version

IPv4

Type

☒ Static
 ☐ Forbidden

Port

Available Port

GE1
GE2
GE3
GE4
GE5
GE6
GE7
GE8

Selected Port

>

<

Apply

Close

Multicast Router Edit Page

Field	Description
VLAN	VLAN ID of Selected router entry
IP Version	Selected IP version
Type	The router port type Static: static router port Forbidden: forbidden router port, can't learn dynamic router port member
Port	The member ports of router entry for selected port type. Available Port: Optional router port member Selected Port: Selected router port member

Multicast Router Edit Field

11.1.4. Forward All

To display multicast Forward All web page, click **Multicast> General> Forward All**

This page allow user to add and edit forward all entry.

[Multicast](#) >> [General](#) >> [Forward All](#)

Forward All Table

IP Version IPv4 ▼

Showing All ▼ entries Showing 0 to 0 of 0 entries

☐ **VLAN** ☐ Static Port ☐ Forbidden Port

0 results found.

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

Multicast Forward All Table Page

Field	Description
IP Version	IP Version IPv4: ipv4 multicast forward all IPv6: ipv6 multicast forward all
VLAN	VLAN ID of forward all entry
Static Port	Known multicast group always forward port member
Forbidden Port	Known multicast group always not forward port member

Multicast Forward All Table Fields

Multicast >> General >> Forward All

Add Forward All

The screenshot shows the 'Add Forward All' configuration interface. It features four main sections: **VLAN**, **IP Version**, **Type**, and **Port**. The **VLAN** section includes an 'Available VLAN' list with '1' and an empty 'Selected VLAN' list, connected by left and right arrows. The **IP Version** section has a dropdown menu currently set to 'IPv4'. The **Type** section contains two radio buttons: 'Static' (which is selected) and 'Forbidden'. The **Port** section includes an 'Available Port' list with options GE1 through GE8 and an empty 'Selected Port' list, also connected by left and right arrows. At the bottom of the form are 'Apply' and 'Close' buttons.

Multicast Forward All Add Page

Field	Description
VLAN	The VLAN ID for forward all entry Available VLAN: Optional VLAN member Selected VLAN: Selected VLAN member
IP Version	IP Version IPv4: ipv4 multicast forward all IPv6: ipv6 multicast forward all
Type	The forward all port type Static: static forward all port Forbidden: forbidden forward all port
Port	The member ports of router entry. Available Port: Optional router port member Selected Port: Selected router port member

Multicast Forward All Add Fields

Multicast >> General >> Forward All

Add Forward All

VLAN

Available VLAN: 1

Selected VLAN:

IP Version: IPv4

Type: ☒ Static ☐ Forbidden

Port

Available Port: GE1, GE2, GE3, GE4, GE5, GE6, GE7, GE8

Selected Port:

Apply Close

Multicast Forward All Edit Page

Field	Description
VLAN	VLAN ID of Selected forward all entry
IP Version	Selected IP version
Type	The forward all port type Static: static forward all port Forbidden: forbidden forward all port
Port	The member ports of forward all entry for selected port type. Available Port: Optional router port member Selected Port: Selected router port member

Multicast Forward All Edit Fields

11.1.5. Throttling

To display multicast max-group number and action setting web page, click **Multicast> General>**

Throttling.

This page allow user to configure port can learned max group number and if port group number arrived max group number action

Multicast >> General >> Throttling

Throttling Table

IP Version IPv4 ▼

☐	Entry	Port	Max Group	Exceed Action
☐	1	GE1	256	Deny
☐	2	GE2	256	Deny
☐	3	GE3	256	Deny
☐	4	GE4	256	Deny
☐	5	GE5	256	Deny
☐	6	GE6	256	Deny
☐	7	GE7	256	Deny
☐	8	GE8	256	Deny

Multicast Throttling Table Page

Field	Description
IP Version	IP Version IPv4: ipv4 for igmp snooping throttling IPv6: ipv6 for mld snooping throttling
Entry	Entry of number
Port	Port Name
Max Group	Max number of group for port
Exceed Action	Display the port exceed max number group learning group action

Multicast Throttling Table Fields

Edit Throttling

Port

GE1

IP Version

IPv4

Max Group

256

(0 - 256)

Exceed Action

☒ Deny

☐ Replace

Apply

Close

Multicast Throttling Edit Page

Field	Description
Port	Display the selected port list
IP Version	Display the selected IP version
Max Group	Max number of group for port
Exceed Action	Excess Max number of port learning group action Deny: do not learning group. Replace: random replace one exist group

Multicast Throttling Table Edit Fields

11.1.6. Filtering Profile

To display Multicast Profile Setting web page, click **Multicast> General> Filtering Profile**

This page allow user to add, edit or delete profile for IGMP or MLD snooping.

Filtering Profile Table

IP Version

IPv4

Showing

All

entries

Showing 0 to 0 of 0 entries

Q

☐	Profile ID	Start Address	End Address	Action
0 results found.				

Add

Edit

Delete

First

Previous

1

Next

Last

Multicast Profile Table Page

Field	Description
IP Version	IP version: IPv4 : IGMP snooping profile IPv6 : MLD snooping profile
Profile ID	Display profile ID
Start Address	The start group address of profile
End Address	The end group address of profile
Action	Display profile action

Multicast Profile Table Fields

Multicast >> General >> Filtering Profile

Add Profile

Profile ID

 (1 - 128)

IP Version

IPv4 ▼

Start Address

End Address

Action

☒ Allow
☐ Deny

Multicast Profile Add Page

Field	Description
Profile ID	Profile ID
IP Version	IP version: IPv4 : IGMP snooping profile IPv6 : MLD snooping profile
Start Address	The start group address of profile
End Address	The end group address of profile
Action	The action of profile: Allow : permit all packets that match the profile. Deny : deny all packets that match the profile.

Multicast Profile Add Fields

Multicast >> General >> Filtering Profile

Add Profile

Profile ID

 (1 - 128)

IP Version

IPv4 ▼

Start Address

End Address

Action

☒ Allow
 ☐ Deny

Multicast Profile Edit Page

Field	Description
Profile ID	Edit Profile ID
IP Version	Display the edit profile ip version
Start Address	The start group address of profile
End Address	The end group address of profile
Action	The action of profile: Allow: permit the group can learned that match the profile. Deny: deny the group to learn the groupthat match the profile.

Multicast Profile Edit Fields

11.1.7. Filtering Binding

To display Multicast port filter binding profile web page, click Multicast> General> Filtering Binding

This page allow user to bind/remove profile for each port

Multicast >> General >> Filtering Binding

Filtering Binding Table

IP Version IPv4 ▼

☐	Entry	Port	Profile ID
☐	1	GE1	
☐	2	GE2	
☐	3	GE3	
☐	4	GE4	
☐	5	GE5	
☐	6	GE6	
☐	7	GE7	
☐	8	GE8	
☐	9	GE9	

Multicast Filtering Table Page

Field	Description
IP Version	IP Version IPv4 : ipv4 for igmp snooping throttling IPv6 : ipv6 for mld snooping throttling
Entry	Entry of number
Port	Port Name
Profile ID	Port binding Profile ID

Multicast Filtering Table Fields

Multicast >> General >> Filtering Binding

Edit Filtering Binding

Port	GE1
IP Version	IPv4
Profile ID	☐ Enable ▼

Apply

Close

Multicast Filtering Edit Page

Field	Description
Port	Selected Port List
IP Version	Display Selected Port filtering IP version
Profile ID	If check Enable, can select or change profile ID, Else it will delete port filter profile binding

Multicast Filtering Edit Fields

11.2. Igmp Snooping

Use the IGMP Snooping pages to configure settings of IGMP snooping function.

11.2.1. Property

To display IGMP Snooping global setting and VLAN Setting web page, click **Multicast> IGMP Snooping> Property**

This page allow user to configure global settings of IGMP snooping and configure specific VLAN settings of IGMP Snooping.

Multicast >> IGMP Snooping >> Property

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	

Edit

IGMP Snooping Property Page

Field	Description
State	Set the enabling status of IGMP Snooping functionality Enable: If Checked Enable IGMP Snooping, else is Disabled IGMP Snooping.
Version	Set the igmp snooping version IGMPv2: Only support process igmp v2 packet.

	IGMPv3: Support v3 basic and v2.
Report Suppression	Set the enabling status of IGMP v2 report suppression Enable: If Checked Enable IGMP Snooping v2 report suppression, else Disable the report suppression function
VLAN	The IGMP entry VLAN ID
Operation Status	The enable status of IGMP snooping VLAN functionality
Router Port Auto Learn	The enabling status of IGMP snooping router port auto learning
Query Robustness	The Query Robustness allows tuning for the expected packet loss on a subnet.
Query Interval	The interval of querier to send general query
Query Max Response Interval	In Membership Query Messages, it specifies the maximum allowed time before sending a responding report in units of 1/10 second.
Last Member Query count	The count that Querier-switch sends Group-Specific Queries when it receives a Leave Group message for a group.
Last Member Query Interval	The interval that Querier-switch sends Group-Specific Queries when it receives a Leave Group message for a group.
Immediate leave	The immediate leave status of the group will immediate leave when receive IGMP Leave message.

IGMP Snooping Property Fields

Multicast >> IGMP Snooping >> Property

Edit VLAN Setting

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

IGMP Snooping VLAN Edit Page

Field	Description
VLAN	The selected VLAN List
State	Set the enabling status of IGMP Snooping VLAN functionality Enable: If Checked Enable IGMP Snooping VLAN, else is Disabled IGMP Snooping VLAN.
Router Port Auto Learn	Set the enabling status of IGMP Snooping router port learning Enable: If checked Enable learning router port by query and PIM, DVRMP, else Disable the learning router port
Immediate leave	Immediate Leave the group when receive IGMP Leave message. Enable: If checked Enable immediate leave, else disable immediate leave
Query Robustness	The Admin Query Robustness allows tuning for the expected packet loss on a subnet.

Query Interval	The Admin interval of querier to send general query
Query Max Response Interval	The Admin query max response interval, In Membership Query Messages, it specifies the maximum allowed time before sending a responding report in units of 1/10 second.
Last Member Query Counter	The Admin last member query count that Querier-switch sends Group-Specific Queries when it receives a Leave Group message for a group.
Last Member Query Interval	The Admin last member query interval that Querier-switch sends Group-Specific Queries when it receives a Leave Group message for a group.
Operational Status	
Status	Operational IGMP snooping status, must both IGMP snooping global and IGMP snooping enable the status will be enable.
Query Robustness	Operational Query Robustness
Query Interval	Operational Query Interval
Query Max Response Interval	Operational Query Max Response Interval
Last Member Query Counter	Operational Last Member Query Count
Last Member Query Interval	Operational Last Member Query Interval

IGMP Snooping VLAN Edit Fields

11.2.2. Querier

To display IGMP Snooping Querier Setting web page, click **Multicast> IGMP Snooping> Querier**

This page allow user to configure querier settings on specific VLAN of IGMP Snooping.

Multicast >> IGMP Snooping >> Querier

Querier Table

☐	VLAN	State	Operational Status	Version	Querier Address
☐	1	Disabled	Disabled		

Edit

IGMP Snooping Querier Table Page

Field	Description
VLAN	IGMP Snooping querier entry VLAN ID
State	The IGMP Snooping querier Admin State.
Operational Status	The IGMP Snooping querier operational status
Querier Version	The IGMP Snooping querier operational version.
Querier IP	The operational Querier IP address on the VLAN

IGMP Snooping Querier Table Fields

Multicast >> IGMP Snooping >> Querier

Edit Querier

VLAN

1

State

☐ Enable

Version

☒ IGMPv2
☐ IGMPv3

Apply

Close

IGMP Snooping Querier Edit Page

Field	Description
VLAN	The Selected Edit IGMP Snooping querier VLAN List

State	Set the enabling status of IGMP Querier Election on the chose VLANs Enabled: if checked Enable IGMP Querier else Disable IGMP Querier
Version	Set the query version of IGMP Querier Election on the chose VLANs IGMPv2: Querier version 2. IGMPv3: Querier version 3. (IGMP Snooping version should be IGMPv3)

IGMP Snooping Querier Edit Fields

11.2.3. Statistics

To display IGMP Snooping Statistics, click **Multicast> IGMP Snooping> Statistics**

This page allow user to clear igmp snooping statics.

Multicast >> IGMP Snooping >> Statistics

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

IGMP Snooping Statistics Page

Field	Description
Receive Packet	
Total	Total RX igmp packet, include ipv4 multicast data to CPU.

Valid	The valid igmp snooping process packet.
InValid	The invalid igmp snooping process packet.
Other	The ICMP protocol is not 2, and is not ipv4 multicast data packet.
Leave	IGMP leave packet.
Report	IGMP join and report packet
General Query	IGMP General Query packet
Special Group Query	IGMP Special Group General Query packet
Source-specific Group Query	IGMP Special Source and Group General Query packet
Transmit Packet	
Leave	IGMP leave packet
Report	IGMP join and report packet
General Query	IGMP general query packet include querier transmit general query packet
Special Group Query	IGMP special group query packet include querier transmit special group query packet
Source-specific Group Query	IGMP Special Source and Group General Query packet

IGMP Snooping Statistics Fields

11.3. MLD Snooping

Use the MLD Snooping pages to configure settings of MLD snooping function.

11.3.1. Property

To display MLD Snooping global setting and VLAN Setting web page, click **Multicast> MLD Snooping> Property**

This page allow user to configure global settings of MLD snooping and configure specific VLAN settings of MLD Snooping.

Multicast >> MLD Snooping >> Property

State	☐ Enable
Version	☒ MLDv1 ☐ MLDv2
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	

Edit

MLD Snooping Property Page

Field	Description
State	Set the enabling status of IGMP Snooping functionality Enable: If Checked Enable IGMP Snooping, else is Disabled IGMP Snooping.
Version	Set the MLD snooping version MLDv1: Only support process MLD v1 packet. MLDv2: Support v2 basic and v1.
Report Suppression	Set the enabling status of MLD v1 report suppression Enable: If Checked Enable MLD Snooping v1 report suppression, else Disable the report suppression function
VLAN	The MLD entry VLAN ID
Operation Status	The enable status of MLD snooping VLAN functionality
Router Port Auto Learn	The enabling status of MLD snooping router port auto learning
Query Robustness	The Query Robustness allows tuning for the expected packet loss on a subnet.
Query Interval	The interval of querier to send general query
Query Max Response Interval	In Membership Query Messages, it specifies the maximum allowed time before sending a responding report in units of 1/10 second.

Last Member Query count	The count that Querier-switch sends Group-Specific Queries when it receives a Leave Group message for a group.
Last Member Query Interval	The interval that Querier-switch sends Group-Specific Queries when it receives a Leave Group message for a group.
Immediate leave	The immediate leave status of the group will immediate leave when receive MLD Leave message.

MLD Snooping Property Fields

Multicast >> MLD Snooping >> Property

Edit VLAN Setting

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

MLD Snooping VLAN Edit Page

Field	Description
VLAN	The selected VLAN List

State	Set the enabling status of MLD Snooping VLAN functionality Enable: If Checked Enable MLD Snooping VLAN, else is Disabled MLD Snooping VLAN.
Router Port Auto Learn	Set the enabling status of MLD Snooping router port learning Enable: If checked Enable learning router port by query and PIM, DVRMP, else Disable the learning router port
Immediate leave	Immediate Leave the group when receive MLD Leave message. Enable: If checked Enable immediate leave, else disable immediate leave immediate leave
Query Robustness	The Admin Query Robustness allows tuning for the expected packet loss on a subnet.
Query Interval	The Admin interval of querier to send general query
Query Max Response Interval	The Admin query max response interval, In Membership Query Messages, it specifies the maximum allowed time before sending a responding report in units of 1/10 second.
Last Member Query Counter	The Admin last member query count that Querier-switch sends Group-Specific Queries when it receives a Leave Group message for a group.
Last Member Query Interval	The Admin last member query interval that Querier-switch sends Group-Specific Queries when it receives a Leave Group message for a group.
Operational Status	
Status	Operational MLD snooping status, must both MLD snooping global and MLD snooping enable the status will be enable.
Query Robustness	Operational Query Robustness
Query Interval	Operational Query Interval
Query Max Response Interval	Operational Query Max Response Interval
Last Member	Operational Last Member Query Count

Query Counter	
Last Member Query Interval	Operational Last Member Query Interval

MLD Snooping VLAN Edit Fields

11.3.2. Statistics

To display MLD Snooping Statistics, click **Multicast> MLD Snooping> Statistics**

This page allow user to clear MLD snooping statics.

Multicast >> MLD Snooping >> Statistics

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

Transmit Packet	
Leave	0
Report	0
General Query	0
Special Group Query	0
Source-specific Group Query	0

MLD Snooping Statistics Page

Field	Description
Receive Packet	
Total	Total RX MLD packet, include ipv4 multicast data to CPU.
Valid	The valid MLD snooping process packet.

InValid	The invalid MLD snooping process packet.
Other	The ICMPV6 type is not MLD, and is not ipv6 multicast data packet, and is not IPV6 router protocol.
Leave	MLD leave packet.
Report	MLD join and report packet
General Query	MLD General Query packet
Special Group Query	MLD Special Group General Query packet
Source-specific Group Query	MLD Special Source and Group General Query packet
Transmit Packet	
Leave	MLD leave packet
Report	MLD join and report packet
General Query	MLD general query packet
Special Group Query	MLD special group query packet
Source-specific Group Query	MLD Special Source and Group General Query packet

MLD Snooping Statistics Fields

11.4. MVR

Use the MVR pages to configure settings of MVR function.

11.4.1. Property

To display multicast MVR property Setting web page, click **Multicast> MVR> Property**

This page allow user to set MVR property.

Multicast >> MVR >> Property

State	☐ Enable
VLAN	1 ▾
Mode	☒ Compatible ☐ Dynamic
Group Start	0.0.0.0
Group Count	1 (1 - 128)
Query Time	1 Sec (1 - 10)
Operational Group	
Maximum	128
Current	0

Apply

Multicast MVR Properties Page

Field	Description
State	Enable: if checked enable the MVR state, else disable the MVR state
VLAN	The MVR VLAN ID
Mode	Set the MVR mode. Compatible: compatible mode Dynamic: dynamic mode, will learn group member on source port
Group Start	MVR group range start
Group Count	MVR group continue count
Query Time	MVR query time when receive MVR leave MVR group packet
Maximum	The max number of MVR group database
Current	The learned MVR group current time

MVR Property Fields

11.4.2. Port Setting

To display MVR port role and immediate leave state setting web page, click **Multicast> MVR> Port Setting**

This page allow user to configure port role and port immediate leave

Multicast >> MVR >> Port Setting

Port Setting Table

☐	Entry	Port	Role	Immediate Leave	
☐	1	GE1	None	Disabled	
☐	2	GE2	None	Disabled	
☐	3	GE3	None	Disabled	
☐	4	GE4	None	Disabled	
☐	5	GE5	None	Disabled	
☐	6	GE6	None	Disabled	
☐	7	GE7	None	Disabled	
☐	8	GE8	None	Disabled	

Multicast MVR Port Setting Table Page

Field	Description
Entry	Entry of number
Port	Port Name
Role	Port Role for MVR, the type is None/Receiver/Source
Immediate Leave	Status of immediate leave

MVR Port Setting Fields

Multicast >> MVR >> Port Setting

Edit Port Setting

Port	GE1
Role	☒ None ☐ Receiver ☐ Source
Immediate Leave	☐ Enable

Multicast MVR Port Setting Edit Page

Field	Description
Port	Display the selected port list
Role	MVR port role None: port role is none Receiver: port role is receiver Source: port role is source
Immediate Leave	MVR Port immediate leave Enable: if checked is enable immediate leave, else disable immediate leave.

MVR Port Setting Edit Fields

11.4.3. Group Address

To display Multicast MVR Group web page, click **Multicast> MVR> Group Address**

This page allow user to browse all multicast MVR groups that dynamic learned or statically added.

Multicast >> MVR >> Group Address

Group Address Table

Showing All entries

Showing 0 to 0 of 0 entries


☐ VLAN | Group Address | Member | Type | Life (Sec)

0 results found.

Multicast MVR Group Address Table Page

Field	Description
VLAN	The VLAN ID of MVR group.
Group Address	The MVR group IP address.
Member	The member ports of MVR group.
Type	The type of MVR group. Static or Dynamic.
Life(Sec)	The life time of this dynamic MVR group.

MVR Group Address Table Fields

Multicast >> MVR >> Group Address

Add Group Address

VLAN

1

Group Address

(0.0.0.0 - 0.0.0.0)

Member

Available Port

Selected Port

Apply

Close

Multicast MVR Group Address Add Page

Field	Description
VLAN	The VLAN ID of MVR group.
Group Address	MVR group IP address.
Member	The member ports of MVR group. Available Port: Optional port member, it is only receiver port when MVR mode is compatible, it include source port when mode is dynamic

	Selected Port: Selected port member
--	--

MVR Group Address Add Fields

Multicast >> MVR >> Group Address

Add Group Address

VLAN

1

Group Address

(0.0.0.0 - 0.0.0.0)

Member

Available Port

Selected Port

Apply

Close

Multicast MVR Group Address Edit Page

Field	Description
VLAN	The VLAN ID of edited MVR group.
Group Address	The edited MVR group IP address.
Member	The member ports of MVR group. Available Port: Optional port member, it is only receiver port when MVR mode is compatible, it include source when mode is dynamic Selected Port: Selected port member port

MVR Group Address Edit Fields

11.5. Example of configuration

Case 1: Enable IGMP snooping on the switch

- WEB
- 1. Enable IGMP globally

Multicast >> IGMP Snooping >> Property

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

Apply

- 2. Enable multicast VLAN

Multicast >> IGMP Snooping >> Property

Edit VLAN Setting

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

- 3. Enable multicast query tool

Multicast >> IGMP Snooping >> Querier

Edit Querier

VLAN	1
State	☒ Enable
Version	☒ IGMPv2 ☐ IGMPv3

Apply Close

● CLI

Enable multicast in global mode, enable multicast query, enable multicast VLAN, and enable multicast under the interface

```
ip igmp snooping
ip igmp snooping vlan 1
ip igmp snooping vlan 1 immediate-leave
ip igmp snooping vlan 1 querier version 2
```

12. Routing

12.1. IPv4 Management and Interfaces

12.1.1. IPv4 Interface

1.To display multicast IPv4 Interface Setting web page, click **Routing >> IPv4 Management and Interfaces >> IPv4 Interface**

Routing >> IPv4 Management and Interfaces >> IPv4 Interface

IPv4 Interface Table

☐	Interface	IP Address Type	IP Address	Mask	Status	Roles	
☐	VLAN 1	Static	192.168.0.1	255.255.255.0	Valid	primary	

Add Edit Delete

2、click add

Routing >> IPv4 Management and Interfaces >> IPv4 Interface

Edit IPv4 Interface

Interface	VLAN 1		
Address Type	☐ Dynamic ☒ Static		
IP Address	192.168.0.1		
Mask	☒ Network Mask	255.255.255.0	
	☐ Prefix Length		(8 - 30)
Roles	☒ primary ☐ sub		

Apply

Close

12.1.2. IPv4 Routes

1.To display multicast IPv4 Routes Setting web page, click **Routing >> IPv4 Management and Interfaces >> IPv4 Routes**

Routing >> IPv4 Management and Interfaces >> IPv4 Routes

IPv4 Routing Table

☐	Destination IP Prefix	Prefix Length	Route Type	Next Hop Router IP Address	Metric	Administrative Distance	Outgoing Interface	
☐	192.168.0.0	24	Directly Connected				VLAN 1*	

AddEditDelete

2.click add

Routing >> IPv4 Management and Interfaces >> IPv4 Routes

Add IPv4 Static Route

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

12.1.3. ARP

1.To displayARP web page, click **Routing >> IPv4 Management and Interfaces >> ARP**

Routing >> IPv4 Management and Interfaces >> ARP

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

ARP Table

☐	Interface	IP Address	MAC Address	Status
☐	VLAN 1	192.168.0.111	68:f7:28:a1:b8:a0	Dynamic

2.click add

1. To display multicast IPv6 Interface Setting web page, click **Routing** » **IPv6 Management and Interfaces** » **IPv6 Interface**

Routing >> IPv6 Management and Interfaces >> IPv6 Interface

Routing >> IPv6 Management and Interfaces >> IPv6 Interface

Add IPv6 Interface

Interface	☒ VLAN 1
	☐ Loopback
Auto Configuration	☒ Enable
DAD Attempts	1 (0 - 600, default 1)
DHCPv6 Client	
Stateless	☐ Enable
Information Refresh Time	86400 (86400 - 4294967294, default 86400)
Minimum Information Refresh Time	600 (600 - 4294967294, default 600)

Apply

Close

12.2.2. IPv6 Addresses

1. To display multicast IPv6 Interface Setting web page, click **Routing >> IPv6 Management and Interfaces >> IPv6 Addresses**

Routing >> IPv6 Management and Interfaces >> IPv6 Addresses

IPv6 Address Table

Interface

☐	IPv6 Address Type	IPv6 Address	IPv6 Prefix Length	DAD Status
☐	Link Local	fe80::8224:2ff:fe19:1	64	Active
☐	Multicast	ff02::1:ff19:1		
☐	Multicast	ff02::1		
☐	Multicast	ff01::1		

Add

Delete

2.click add

Routing >> IPv6 Management and Interfaces >> IPv6 Addresses

Add IPv6 Interface

Interface	VLAN 1
IPv6 Address Type	☒ Global ☐ Link Local
IPv6 Address	
Prefix Length	(3 - 128)
EUI-64	☐ Enable

12.2.3. IPv6 Routes

1. To display multicast IPv6 Interface Setting web page, click **Routing >> IPv6 Management and Interfaces >> IPv6 Routes**

Routing >> IPv6 Management and Interfaces >> IPv6 Routes

IPv6 Routing Table

Q

Destination IP Prefix

Prefix Length

Route Type

Next Hop Router IP Address

Metric

Administrative Distance

Outgoing Interface

0 results found.

Add

Edit

Delete

Routing >> IPv6 Management and Interfaces >> IPv6 Routes**Add IPv6 Static Route**

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

Apply

Close

12.2.4. IPv6 Neighbors

1. To display multicast IPv6 Interface Setting web page, click **Routing >> IPv6 Management and Interfaces >> IPv6 Neighbors**

Routing >> IPv6 Management and Interfaces >> IPv6 Neighbors

Clear Neighbor Table	☐ All ☐ Dynamic ☐ Static ☒ N/A
----------------------	--

Apply

Cancel

IPv6 Neighbor Table

☐	Interface	IPv6 Address	MAC Address	Status	Router
0 results found.					

Add Edit Delete

2.click add

Routing >> IPv6 Management and Interfaces >> IPv6 Neighbors

Add Neighbor

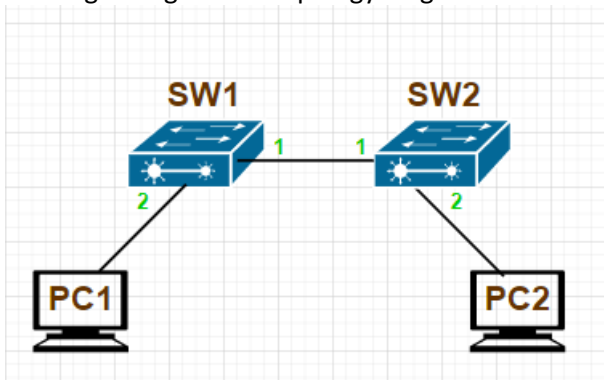
Interface	VLAN 1 ▼
IP Address	
MAC Address	

Apply

Close

12.3. Example of configuration

Routing configuration topology diagram



Case 1: Static Routing/Default

- WEB
- 1、sw1
- 1.1IPv4 address

Routing >> IPv4 Management and Interfaces >> IPv4 Interface

IPv4 Interface Table

☐	Interface	IP Address Type	IP Address	Mask	Status	Roles
☐	VLAN 1	Static	192.168.0.1	255.255.255.0	Valid	primary
☐	VLAN 2	Static	192.168.2.1	255.255.255.0	Valid	primary
☐	VLAN 12	Static	192.168.12.1	255.255.255.0	Valid	primary

Add

Edit

Delete

1.2Default routing configuration

Routing >> IPv4 Management and Interfaces >> IPv4 Routes

IPv4 Routing Table

☐	Destination IP Prefix	Prefix Length	Route Type	Next Hop Router IP Address	Metric	Administrative Distance	Outgoing Interface
☐	0.0.0.0	0	Default	192.168.12.2	1	1	inactive
☐	192.168.0.0	24	Directly Connected				VLAN 1*

- 2、sw2 config
2.1IPv4 address

Routing >> IPv4 Management and Interfaces >> IPv4 Interface

IPv4 Interface Table

☐	Interface	IP Address Type	IP Address	Mask	Status	Roles
☐	VLAN 1	Static	192.168.0.1	255.255.255.0	Valid	primary
☐	VLAN 3	Static	192.168.3.1	255.255.255.0	Valid	primary
☐	VLAN 12	Static	192.168.12.2	255.255.255.0	Valid	primary

2.2 Static routing configuration

Routing >> IPv4 Management and Interfaces >> IPv4 Routes

IPv4 Routing Table

☐	Destination IP Prefix	Prefix Length	Route Type	Next Hop Router IP Address	Metric	Administrative Distance	Outgoing Interface
☐	192.168.0.0	24	Directly Connected				VLAN 1*
☐	192.168.2.0	24	Static	192.168.12.1	1	1	VLAN 1

- CLI

Enable multicast in global mode, enable multicast query, enable multicast VLAN, and enable multicast under the interface

SW1:

system name "sw1"

vlan 2,12

interface vlan2

ip address 192.168.2.1/24

interface vlan12

```
ip address 192.168.12.1/24

interface gi1

    switchport mode access

    switchport access vlan 12

!

interface gi2

    switchport mode access

    switchport access vlan 2

ip route 0.0.0.0/0 192.168.12.2


SW2:

system name "sw2"

vlan 3,12

interface vlan3

    ip address 192.168.3.1/24

interface vlan12

    ip address 192.168.12.2/24

interface gi1

    switchport mode access

    switchport access vlan 12

!

interface gi2

    switchport mode access

    switchport access vlan 3

ip route 192.168.2.0/24 192.168.12.1
```

13. Security

Use the Security pages to configure settings for the switch security features.

13.1. RADIUS

To display RADIUS web page, click **Security > RADIUS**

This page allow user to add, edit or delete RADIUS server settings and modify default parameter of RADIUS server.

Security >> RADIUS

Use Default Parameter

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

Apply

RADIUS Default Setting

Field	Description
Retry	Set default retry number
Timeout	Set default timeout value
Key String	Set default RADIUS key string

RADIUS Default Setting Fields

RADIUS Table

Showing All entries
Showing 0 to 0 of 0 entries

Q

☐	Server Address	Server Port	Priority	Retry	Timeout	Usage	
--------------------------	----------------	-------------	----------	-------	---------	-------	--

0 results found.

Add
Edit
Delete

First
Previous
1
Next
Last

RADIUS Table

Field	Description
Server Address	RADIUS server address
Server Port	RADIUS server port

Priority	RADIUS server priority (smaller value has higher priority). RADIUS session will try to establish with the server setting which has highest priority. If failed, it will try to connect to the server with next higher priority.
Retry	RADIUS server retry value. If it is fail to connect to server, it will keep trying until timeout with retry times.
Timeout	RADIUS server timeout value. If it is fail to connect to server, it will keep trying until timeout.
Usage	RADIUS server usage type Login: For login authentication 802.1x: For 802.1x authentication All: For all types

RADIUS Table Fields

Security >> RADIUS

Add RADIUS Server

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

Add/Edit RADIUS Server Dialog

Field	Description
Address Type	In add dialog, user need to specify server Address Type Hostname: Use domain name as server address IPv4: Use IPv4 as server address IPv6: Use IPv6 as server address
Server Address	In add dialog, user need to input server address based on address type. In edit dialog, it shows current edit server address.
Server Port	Set RADIUS server port
Priority	Set RADIUS server priority (smaller value has higher priority). RADIUS session will try to establish with the server setting which has highest priority. If failed, it will try to connect to the server with next higher priority.
Retry	Set RADIUS server retry value. If it is fail to connect to server, it will keep trying until timeout with retry times.
Timeout	Set RADIUS server timeout value. If it is fail to connect to server, it will keep trying until timeout.
Usage	Set RADIUS server usage type Login: For login authentication 802.1x: For 802.1x authentication All: For all types

Add/Edit RADIUS Server Fields

13.2. TACACS+

To display TACACS+ web page, click **Security > TACACS+**

This page allow user to add, edit or delete TACACS+ server settings and modify default parameter of TACACS+ server.

Security >> TACACS+

Use Default Parameter

Timeout

5

Sec (1 - 30, default 5)

Key String

Apply

TACACS+ Table

Showing

All

 entries

Showing 0 to 0 of 0 entries

Q

☐	Server Address	Server Port	Priority	Timeout
0 results found.				

Add

Edit

Delete

First

Previous

1

Next

Last

TACACS+ Default Setting

Field	Description
Timeout	Set default timeout value
Key String	Set default TACACS+ key string

TACACS+ Default Setting Fields

Security >> TACACS+

Add TACACS+ Server

Address Type

☒ Hostname

☐ IPv4

☐ IPv6

Server Address

Server Port

49

(0 - 65535, default 49)

Priority

(0 - 65535)

Key String

☒ Use Default

Timeout

☒ Use Default

5

Sec (1 - 30, default 5)

Apply

Close

TACACS+ Table

Field	Description
Server Address	TACACS+ server address
Server Port	TACACS+ server port
Priority	TACACS+ server priority (smaller value has higher priority). TACACS+ session will try to establish with the server setting which has highest priority. If failed, it will try to connect to the server with next higher priority.
Timeout	TACACS+ server timeout value. If it is fail to connect to server, it will keep trying until timeout.

RADIUS Table Fields

Security >> TACACS+

Add TACACS+ Server

Address Type

☒ Hostname
☐ IPv4
☐ IPv6

Server Address

Server Port

49

(0 - 65535, default 49)

Priority

(0 - 65535)

Key String

☒ Use Default

Timeout

☒ Use Default

5

Sec (1 - 30, default 5)

Apply

Close

Add/Edit TACACS+ Server Dialog

Field	Description
Address Type	In add dialog, user need to specify server Address Type Hostname: Use domain name as server address

	IPv4: Use IPv4 as server address IPv6: Use IPv6 as server address
Server Address	In add dialog, user need to input server address based on address type. In edit dialog, it shows current edit server address.
Server Port	Set TACACS+ server port
Priority	Set TACACS+ server priority (smaller value has higher priority). TACACS+ session will try to establish with the server setting which has highest priority. If failed, it will try to connect to the server with next higher priority.
Timeout	Set TACACS+ server timeout value. If it is fail to connect to server, it will keep trying until timeout.

Add/Edit TACACS+ Server Fields

13.3. AAA

13.3.1. Method List

To display Method List web page, click **Security > AAA > Method List**

This page allow user to add, edit or delete login authentication list settings (The “default” list cannot be deleted.). The line combined to this list will authenticate login user by methods in this list. If the first method is failed, it will try to use the next priority method to authenticate if it exists. With RADIUS and TACACS+ methods, the failed means connecting to server fail. With Local method, the failed means cannot find the user in local database.

Method List Table

Field	Description
Name	Login authentication list name. This name should be different from other existing lists.

Sequence	Priority of login authentication method. None: Authenticated with any condition. Local: Use local accounts database to authenticate TACACS+: Use remote TACACS+ server to authenticate. RADIUS: Use remote Radius server to authenticate. Enable: Use local enable password to authenticate
----------	--

Method List Table Fields

Security >> AAA >> Method List

Add Method List

Name	
Method 1	☒ Empty ☐ None ☐ Local ☐ Enable ☐ RADIUS ☐ TACACS+
Method 2	☒ Empty ☐ None ☐ Local ☐ Enable ☐ RADIUS ☐ TACACS+
Method 3	☒ Empty ☐ None ☐ Local ☐ Enable ☐ RADIUS ☐ TACACS+
Method 4	☒ Empty ☐ None ☐ Local ☐ Enable ☐ RADIUS ☐ TACACS+

Add/Edit Method List Dialog

Field	Description
Name	Login authentication list name. This name should be different from other existing lists.
Method 1	Select first priority of login authentication method. None: Authenticated with any condition. Local: Use local accounts database to authenticate TACACS+: Use remote TACACS+ server to authenticate. RADIUS: Use remote Radius server to authenticate. Enable: Use local enable password to authenticate
Method 2	Select second priority of login authentication method. None: Authenticated with any condition. Local: Use local accounts database to authenticate TACACS+: Use remote TACACS+ server to authenticate. RADIUS: Use remote Radius server to authenticate. Enable: Use local enable password to authenticate
Method 3	Select thrid priority of login authentication method. None: Authenticated with any condition. Local: Use local accounts database to authenticate TACACS+: Use remote TACACS+ server to authenticate. RADIUS: Use remote Radius server to authenticate. Enable: Use local enable password to authenticate

Method 4	Select fourth priority of login authentication method. None: Authenticated with any condition. Local: Use local accounts database to authenticate TACACS+: Use remote TACACS+ server to authenticate. RADIUS: Use remote Radius server to authenticate. Enable: Use local enable password to authenticate
----------	--

Add/Edit Method List Fields

13.3.2. Login Authentication

To display the login authentication combined web page, click **Security > AAA > Login Authentication**.

This page allow user to combine AAA login authentication list to all management interfaces.

Security >> AAA >> Login Authentication

Console	default ▼	(1) Local
Telnet	default ▼	(1) Local
SSH	default ▼	(1) Local
HTTP	default ▼	(1) Local
HTTPS	default ▼	(1) Local

Apply

Login Authentication Page

Field	Description
Console	Specify login authentication list combined on console
Telnet	Specify login authentication list combined on Telnet
SSH	Specify login authentication list combined on SSH
HTTP	Specify login authentication list combined on HTTP
HTTPS	Specify login authentication list combined on HTTPS

Login Authentication Page Fields

13.4. Management Access

Use the Management Access pages to configure settings of management access.

13.4.1. Management Service

To display Management Service click **Security > Management Access > Management Service**

This page allow user to change management services related configurations.

Security >> Management Access >> Management Service

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)
Password Retry Count		
Console	3	(0 - 120, default 3)
Telnet	3	(0 - 120, default 3)
SSH	3	(0 - 120, default 3)
Silent Time		
Console	0	Sec (0 - 65535, default 0)
Telnet	0	Sec (0 - 65535, default 0)
SSH	0	Sec (0 - 65535, default 0)

Apply

Management Service Page

Field	Description
Management Service	Management service admin state. Telnet: Connect CLI through telnet SSH: Connect CLI through SSH HTTP: Connect WEBUI through HTTP

	HTTPS: Connect WEBUI through HTTPS SNMP: Manage switch through SNMP
Session Timeout	Set session timeout minutes for user access to user interface. 0 minutes means never timeout.
Password Retry Count	Retry count is the number which CLI password input error tolerance count. After input error password exceeds this count, the CLI will freeze after silent time.
Silent Time	After input error password exceeds password retry count, the CLI will freeze after silent time.

Management Service Fields

13.4.2. Management ACL

To display Management ACL page, click **Security > Management Access > Management ACL**

This page allow user to add or delete management ACL rule. A rule cannot be deleted if under active.

Security >> Management Access >> Management ACL

ACL Name

Apply

Management ACL Table

Showing entries

Showing 0 to 0 of 0 entries

☐	ACL Name	State	Rule
0 results found.			

Active Deactive Delete

First Previous 1 Next Last

Management ACL Page

Management ACL Table

Showing entries

☐	ACL Name	State	Rule
☒	111	Active	0

Active Deactive Delete

Field	Description
ACL Name	Input MAC ACL name

Management ACL Fields

Management ACL Table Page

Field	Description
ACL Name	Display Management ACL name
State	Display Management ACL whether active.
Rule	Display the number Management ACE rule of ACL

Management ACL Table Fields

13.4.3. Management ACE

To display Management ACE page, click **Security > Management Access > Management ACE**

This page allow user to add, edit or delete ACE rule. An ACE rule cannot be edited or deleted if ACL under active. New ACE cannot be added if ACL under active.

Security >> Management Access >> Management ACE

Management ACE Table

ACL Name (Active)

Showing entries

Showing 0 to 0 of 0 entries



☐	Priority	Action	Service	Port	Address / Mask
0 results found.					
Add	Edit	Delete			
			First	Previous	1 Next Last

Management ACE Page

Field	Description
ACL Name	Select the ACL name to which an ACE is being added.
Priority	Display the priority of ACE.
Action	Display the action of ACE
Service	Display the service ACE.
Port	Display the port list of ACE.
Address/ Mask	Display the source IP address and mask of ACE.

Management ACE Fields

Security >> Management Access >> Management ACE

Add Managemet ACE

ACL Name	111																						
Priority	1 (1 - 65535)																						
Service	☐ All ☐ Http ☐ Https ☒ Snmp ☐ SSH ☐ Telnet																						
Action	☐ Permit ☒ Deny																						
Port	<table border="1"><thead><tr><th>Available Port</th><th></th><th>Selected Port</th></tr></thead><tbody><tr><td>GE1</td><td rowspan="8"> > < </td><td></td></tr><tr><td>GE2</td><td></td></tr><tr><td>GE3</td><td></td></tr><tr><td>GE4</td><td></td></tr><tr><td>GE5</td><td></td></tr><tr><td>GE6</td><td></td></tr><tr><td>GE7</td><td></td></tr><tr><td>GE8</td><td></td></tr></tbody></table>			Available Port		Selected Port	GE1	> <		GE2		GE3		GE4		GE5		GE6		GE7		GE8	
Available Port		Selected Port																					
GE1	> <																						
GE2																							
GE3																							
GE4																							
GE5																							
GE6																							
GE7																							
GE8																							
IP Version	☒ All ☐ IPv4 ☐ IPv6																						
IPv4	/ 255.255.255.255																						
IPv6	/ 128 (1 - 128)																						

Apply Close

Add and Edit Management ACE Dialog

Field	Description
ACL Name	Display the ACL name to which an ACE is being added.
Priority	Specify the priority of the ACE. ACEs with higher sequence are processed first (1 is the highest priority). Only available on Add Dialog.
Service	Select the type service of rule. All: All services HTTP: Only HTTP service. HTTPs: Only HTTPs service. SNMP: Only SNMP service. SSH: Only SSH service. Telnet: Only Telnet service.
Action	Select the action after ACE match packet. Permit: Forward packets that meet the ACE criteria. Deny: Drop packets that meet the ACE criteria.
Port	Select ports which will be matched.
IP Version	Select the type of source IP address. All: All IP addresses can access. IPv4: Specify IPv4 address ca access IPv6: Specify IPv6 address ca access
IPv4	Enter the source IPv4 address value and mask to which will be matched.
IPv6	Enter the source IPv6 address value and mask to which will be matched.

Add and Edit Management ACE Fields

13.5. Authentication Manager

13.5.1. Property

To display authentication manager property web page, click **Security > Authentication Manger > Property**

This page allow user to edit authentication global settings and some port mods' configurations.

Security >> Authentication Manager >> Property

Authentication Type	☐ 802.1x ☐ MAC-Based ☐ WEB-Based
Guest VLAN	☐ Enable 1
MAC-Based User ID Format	XXXXXXXXXXXXX

Apply

Port Mode Table

	Entry	Port	Authentication Type			Host Mode	Order	Method	Guest VLAN	VLAN Assign Mode
			802.1x	MAC-Based	WEB-Based					
☐	1	GE1	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
☐	2	GE2	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
☐	3	GE3	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static

Authentication Manager Global Setting

Field	Description
Authentication Type	Set checkbox to enable/disable following authentication types 802.1x: Use IEEE 802.1x to do authentication MAC-Based: Use MAC address to do authentication WEB-Based: Prompt authentication web page for user to do authentication
Guest VLAN	Set checkbox to enable/disable guest VLAN, if guest VLAN is enabled, you need to select one available VLAN ID to be guest VID.
MAC-Based User ID Format	Select mac-based authentication RADIUS username/password ID format. XXXXXXXXXXXXX xxxxxxxxxxxxxx XX:XX:XX:XX:XX:XX xx:xx:xx:xx:xx:xx XX-XX-XX-XX-XX-XX xx-xx-xx-xx-xx-xx XX.XX.XX.XX.XX.XX

XX.XX.XX.XX.XX.XX
XXXX:XXXX:XXXX
XXXX:XXXX:XXXX
XXXX-XXXX-XXXX
XXXX-XXXX-XXXX
XXXX.XXXX.XXXX
XXXX.XXXX.XXXX
XXXXXX:XXXXXX
XXXXXX:XXXXXX
XXXXXX-XXXXXX
XXXXXX-XXXXXX
XXXXXX.XXXXXX
XXXXXX.XXXXXX

Authentication Manager Global Setting Fields

Port Mode Table

	Entry	Port	Authentication Type			Host Mode	Order	Method	Guest VLAN	VLAN Assign Mode
			802.1x	MAC-Based	WEB-Based					
☐	1	GE1	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
☐	2	GE2	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
☐	3	GE3	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
☐	4	GE4	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
☐	5	GE5	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
☐	6	GE6	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
☐	7	GE7	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
☐	8	GE8	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
☐	9	GE9	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
☐	10	GE10	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static

Edit

Port Mode Table

Field	Description
Port	Port name

Authentication Type (802.1X)	X authentication type state Enabled: 802.1X is enabled Disabled: 802.1X is disabled
Authentication Type (MAC-Based)	MAC-Based authentication type state Enabled: MAC-Based authentication is enabled Disabled: MAC-Based authentication is disabled
Authentication Type (WEB-Based)	WEB-Based authentication type state Enabled: WEB-Based authentication is enabled Disabled: WEB-Based authentication is disabled
Host Mode	Authenticating host mode Multiple Authentication: In this mode, every client need to pass authenticate procedure individually. Multiple Hosts: In this mode, only one client need to be authenticated and other clients will get the same access accessibility. Web-auth cannot be enabled in this mode. Single Host: In this mode, only one host is allowed to be authenticated. It is the same as Multi-auth mode with max hosts number configure to be 1.
Order	Support following authentication type order combinations. Web Authentication should always be the last type. The authentication manager will go to next type if current type is not enabled or authenticated fail. 802.1x MAC-Based WEB-Based 802.1x MAC-Based 802.1x WEB-Based MAC-Based 802.1x WEB-Based 802.1x 802.1x MAC-Based WEB-Based 802.1x WEB-Based MAC-Based

Method	Support following authentication method order combinations. These orders only available on MAC-Based authentication and WEB-Based authentication. 802.1x only support Radius method. Local: Use DUT's local database to do authentication Radius: Use remote RADIUS server to do authentication Local Radius Radius Local
Guest VLAN	Port guest VLAN enable state Enabled: Guest VLAN is enabled on port Disabled: Guest VLAN is disabled on port
VLAN Assign Mode	Support following VLAN assign mode and only apply when source is RADIUS Disable: Ignore the VLAN authorization result and keep original VLAN of host. Reject: If get VLAN authorized information, just use it. However, if there is no VLAN authorized information, reject the host and make it unauthorized. Static: If get VLAN authorized information, just use it. If there is no VLAN authorized information, keep original VLAN of host.

Port Mode Table Fields

Security >> Authentication Manager >> Property

Edit Port Mode

The screenshot shows the 'Edit Port Mode' dialog box with the following configuration:

- Port:** GE1
- Authentication Type:** ☐ 802.1x, ☐ MAC-Based, ☐ WEB-Based
- Host Mode:** ☒ Multiple Authentication, ☐ Multiple Hosts, ☐ Single Host
- Order:** Available Type: MAC-Based, WEB-Based; Select Type: 802.1x
- Method:** Available Method: Local; Select Method: RADIUS
- Guest VLAN:** ☐ Enable, ☐ Disable, ☐ Reject
- VLAN Assign Mode:** ☒ Static

Buttons: Apply, Close

Edit Port Mode Dialog

Field	Description
Port	Selected port list
Authentication Type	Set checkbox to enable/disable authentication types.
Host Mode	Select authenticating host mode Multiple Authentication: In this mode, every client need to pass authenticate procedure individually. Multiple Hosts: In this mode, only one client need to be authenticated and other clients will get the same access accessibility. Web-auth cannot be enabled in this mode. Single Host: In this mode, only one host is allowed to be authenticated. It is the same as Multi-auth mode with max hosts number configure to be 1.

Order	Support following authentication type order combinations. Web Authentication should always be the last type. The authentication manager will go to next type if current type is not enabled or authenticated fail. 802.1x MAC-Based WEB-Based 802.1x MAC-Based 802.1x WEB-Based MAC-Based 802.1x WEB-Based 802.1x 802.1x MAC-Based WEB-Based 802.1x WEB-Based MAC-Based
Method	Support following authentication method order combinations. These orders only available on MAC-Based authentication and WEB-Based authentication. 802.1x only support Radius method. Local: Use DUT's local database to do authentication Radius: Use remote RADIUS server to do authentication Local Radius Radius Local
Guest VLAN	Set checkbox to enable/disable guest VLAN
VLAN Assign Mode	Support following VLAN assign mode and only apply when source is RADIUS Disable: Ignore the VLAN authorization result and keep original VLAN of host. Reject: If get VLAN authorized information, just use it. However, if there is no VLAN authorized information, reject the host and make it unauthorized. Static: If get VLAN authorized information, just use it. If there is no VLAN authorized information, keep original VLAN of host.

Edit Port Mode Fields

13.5.2. Port Setting

To display the authentication manager Port Setting web page, click **Security > Authentication**

Manager> Port Setting.

This page allow user to configure authentication manger port settings

[Security](#) >> [Authentication Manager](#) >> [Port Setting](#)

Port Setting Table

	Entry	Port	Port Control	Reauthentication	Max Hosts	Common Timer			802.1x Parameters				Web-Based Parameters	
						Reauthentication	Inactive	Quiet	TX Period	Supplicant Timeout	Server Timeout	Max Request	Max Login	
☐	1	GE1	Disabled	Disabled	256	3600	60	60	30	30	30	2	3	
☐	2	GE2	Disabled	Disabled	256	3600	60	60	30	30	30	2	3	
☐	3	GE3	Disabled	Disabled	256	3600	60	60	30	30	30	2	3	
☐	4	GE4	Disabled	Disabled	256	3600	60	60	30	30	30	2	3	
☐	5	GE5	Disabled	Disabled	256	3600	60	60	30	30	30	2	3	
☐	6	GE6	Disabled	Disabled	256	3600	60	60	30	30	30	2	3	
☐	7	GE7	Disabled	Disabled	256	3600	60	60	30	30	30	2	3	
☐	8	GE8	Disabled	Disabled	256	3600	60	60	30	30	30	2	3	
☐	9	GE9	Disabled	Disabled	256	3600	60	60	30	30	30	2	3	
☐	10	GE10	Disabled	Disabled	256	3600	60	60	30	30	30	2	3	
☐	11	GE11	Disabled	Disabled	256	3600	60	60	30	30	30	2	3	
☐	12	GE12	Disabled	Disabled	256	3600	60	60	30	30	30	2	3	
☐	13	GE13	Disabled	Disabled	256	3600	60	60	30	30	30	2	3	
☐	14	GE14	Disabled	Disabled	256	3600	60	60	30	30	30	2	3	
☐	15	GE15	Disabled	Disabled	256	3600	60	60	30	30	30	2	3	

Authentication Manager Port Setting Table

Field	Description
Port	Port name
Port Control	Support following authentication port control types. Disable: Disable authentication function and all clients have network accessibility. Force Authorized: Port is force authorized and all clients have network accessibility. Force Unauthorized: Port is force unauthorized and all clients have no network accessibility. Auto: Need passing authentication procedure to get network accessibility.
Reauthentication	Reautheticate state Enabled: Host will be reauthenticated after reauthentication period Disabled: Host will not be reauthenticated after reauthentication period
Max Hosts	In Multiple Authentication mode, total host number cannot not exceed max hosts number
Common Timer (Reauthentication)	After re-authenticate period, host will return to initial state and need to pass authentication procedure again.

Common Timer (Inactive)	If no packet from the authenticated host, the inactive timer will increase. After inactive timeout, the host will be unauthorized and corresponding session will be deleted. In multi-host mode, the packet is counting on the authorized host only and not all packets on the port.
Common Timer (Quiet)	When port is in Locked state after authenticating fail several times, the host will be locked in quiet period. After this quiet period, the host is allowed to authenticate again.
802.1X Params (TX Period)	Number of seconds that the device waits for a response to an Extensible Authentication Protocol (EAP) request/identity frame from the supplicant (client) before resending the request.
802.1X Params (Supplicant Timeout)	The maximum number of EAP requests that can be sent. If a response is not received after the defined period (supplicant timeout), the authentication process is restarted.
802.1X Params (Server Timeout)	Number of seconds that lapses before EAP requests are resent to the supplicant.
802.1X Params (Max Request)	Number of seconds that lapses before the device resends a request to the authentication server.
Web-Based Param (Max Login)	Allow user login fail number. After login fail number exceed, the host will enter Lock state and is not able to authenticate until quiet period exceed.

Authentication Manager Port Setting Table Fields

Security >> Authentication Manager >> Port Setting

Edit Port Setting

Port	GE1	
Port Control	☒ Disabled ☐ Force Authorized ☐ Force Unauthorized ☐ Auto	
Reauthentication	☐ Enable	
Max Hosts	256	(1 - 256, default 256)
Common Timer		
Reauthentication	3600	Sec (300 - 2147483647, default 3600)
Inactive	60	Sec (60 - 65535, default 60)
Quiet	60	Sec (0 - 65535, default 60)
802.1x Parameters		
TX Period	30	Sec (1 - 65535, default 30)
Supplicant Timeout	30	Sec (1 - 65535, default 30)
Server Timeout	30	Sec (1 - 65535, default 30)
Max Request	2	(1 - 10, default 2)
Web-Based Parameters		
Max Login	☐ Infinite 3	(3 - 10, default 3)

Authentication Manager Port Setting Dialog

Field	Description
Port	Port name
Port Control	Support following authentication port control types. Disable: Disable authentication function and all clients have network accessibility. Force Authorized: Port is force authorized and all clients have network accessibility. Force Unauthorized: Port is force unauthorized and all clients have no network accessibility. Auto: Need passing authentication procedure to get network accessibility.
Reauthentication	Set checkbox to enable/disable reauthentication
Max Hosts	In Multiple Authentication mode, total host number cannot not exceed max hosts

	number
Common Timer (Reauthentication)	After re-authenticate period, host will return to initial state and need to pass authentication procedure again.
Common Timer (Inactive)	If no packet from the authenticated host, the inactive timer will increase. After inactive timeout, the host will be unauthorized and corresponding session will be deleted. In multi-host mode, the packet is counting on the authorized host only and not all packets on the port.
Common Timer (Quiet)	When port is in Locked state after authenticating fail several times, the host will be locked in quiet period. After this quiet period, the host is allowed to authenticate again.
802.1X Params (TX Period)	Number of seconds that the device waits for a response to an Extensible Authentication Protocol (EAP) request/identity frame from the supplicant (client) before resending the request.
802.1X Params (Supplicant Timeout)	The maximum number of EAP requests that can be sent. If a response is not received after the defined period (supplicant timeout), the authentication process is restarted.
802.1X Params (Server Timeout)	Number of seconds that lapses before EAP requests are resent to the supplicant.
802.1X Params (Max Request)	Number of seconds that lapses before the device resends a request to the authentication server.
Web-Based Param (Max Login)	Set checkbox to set max login number to be infinite or specify max login number.

Authentication Manager Port Setting Table Fields

13.5.3. MAC-Based Local Account

To display MAC-Based Local Account web page, click **Security > Authentication Manger > MAC-Based Local Account**

This page allow user to add/edit/delete MAC-Based authentication local accounts.

Security >> Authentication Manager >> MAC-Based Local Account

MAC-Based Local Account Table

Showing All entries

Showing 0 to 0 of 0 entries



☐	MAC Address	Control	VLAN	Timeout (Sec)	
				Reauthentication	Inactive
0 results found.					
Add Edit Delete					
First Previous 1 Next					

MAC-Based Local Account Table

Field	Description
MAC Address	Authenticated host MAC address, and each MAC allow only one entry in local database.
Control	Control Type Force Authorized: Host will be force authorized Force Unauthorized: Host will be force unauthorized
VLAN	Assigned VLAN ID for the authenticated host.
Timeout (Reauthentication)	Assigned reauthentication period for the authenticated host.
Timeout (Inactive)	Assigned inactive timeout for the authenticated host.

MAC-Based Local Account Table Fields

Security >> Authentication Manager >> MAC-Based Local Account

Add MAC-Based Local Account

MAC Address	
Port Control	☒ Force Authorized ☐ Force Unauthorized ☐ User Defined
VLAN	1 (1 - 4094)
Assigned Timer	
Reauthentication	☐ User Defined 3600 Sec (300 - 2147483647)
Inactive	☐ User Defined 60 Sec (60 - 65535)
Apply Close	

Add/Edit MAC-Based Local Account Dialog

Field	Description
MAC Address	Authenticated host MAC address, and each MAC allow only one entry in local database.
Control	Control Type Force Authorized: Host will be force authorized Force Unauthorized: Host will be force unauthorized
VLAN	Assigned VLAN ID for the authenticated host.
Timeout (Reauthentication)	Assigned reauthentication period for the authenticated host.
Timeout (Inactive)	Assigned inactive timeout for the authenticated host.

Add/Edit MAC-Based Local Account Fields

13.5.4. WEB-Based Local Account

To display WEB-Based Local Account web page, click **Security > Authentication Manger > WEB-Based Local Account**

This page allow user to add/edit/delete WEB-Based authentication local accounts.

Security >> Authentication Manager >> WEB-Based Local Account

WEB-Based Local Account Table

Showing entries Showing 0 to 0 of 0 entries

	Username	VLAN	Timeout (Sec)	Reauthentication	Inactive
0 results found.					

WEB-Based Local Account Table

Field	Description
Username	Authenticating account user name
VLAN	Assigned VLAN ID for the authenticated host.

Timeout (Reauthentication)	Assigned reauthentication period for the authenticated host.
Timeout (Inactive)	Assigned inactive timeout for the authenticated host.

WEB-Based Local Account Table Fields

Security >> Authentication Manager >> WEB-Based Local Account

Add WEB-Based Local Account

Username

Password

Confirm Password

VLAN

☐ User Defined
 (1 - 4094)

Assigned Timer

Reauthentication

☐ User Defined
 Sec (300 - 2147483647)

Inactive

☐ User Defined
 Sec (60 - 65535)

Add/Edit WEB-Based Local Account Dialog

Field	Description
Username	Authenticating account user name
Password	Authenticating account password
Confirm Password	Confirm authenticating account password
VLAN	Assigned VLAN ID for the authenticated host.
Timeout (Reauthentication)	Assigned reauthentication period for the authenticated host.
Timeout (Inactive)	Assigned inactive timeout for the authenticated host.

Add/Edit WEB-Based Local Account Fields

13.5.5. Sessions

To display Sessions web page, click **Security > Authentication Manger > Sessions**

This page show all detail information of authentication sessions and allow user to select specific session to delete by clicking “Clear ” button.

Security >> Authentication Manager >> Sessions

Sessions Table

Showing All entries Showing 0 to 0 of 0 entries Q

	Session ID	Port	MAC Address	Current Type	Status	Operational Information				Authorized Information			
						VLAN	Session Time	Inactivated Time	Quiet Time	VLAN	Reauthentication Period	Inactive Timeout	

0 results found.

Clear Refresh First Previous 1 Next Last

Sessions Table

Field	Description
Session ID	Session ID is unique of each session
Port	Port name which the host located
MAC Address	Host MAC address
Current Type	Show current authenticating type 802.1x: Use IEEE 802.1X to do authenticating MAC-Based: Use MAC-Based authentication to do authenticating WEB-Based: Use WEB-Based authentication to do authenticating

Status	Show host authentication session status Disable: This session is ready to be deleted Running: Authentication process is running Authorized: Authentication is passed and getting network accessibility. UnAuthorized: Authentication is not passed and not getting network accessibility. Locked: Host is locked and do not allow to do authenticating until quiet period. Guest: Host is in the guest VLAN.
Operational (VLAN)	Shows host operational VLAN ID.
Operational (Session Time)	In “Authorized” state, it shows total time after authorized.
Operational (Inactived)	In “Authorized” state, it shows how long the host do not send any packet.
Operational (Quiet Time)	In “Locked” state, it shows total time after locked.
Authorized (VLAN)	Shows VLAN ID given from authorized procedure.
Authorized (Reauthentication Period)	Shows reauthentication period given from authorized procedure.
Authorized (Inactive Timeouts)	Shows inactive timeout given from authorized procedure.

Sessions Table Fields

13.6. DoS

A Denial of Service (DoS) attack is a hacker attempt to make a device unavailable to its users. DoS attacks saturate the device with external communication requests, so that it cannot respond to legitimate traffic. These attacks usually lead to a device CPU overload.

The DoS protection feature is a set of predefined rules that protect the network from malicious attacks. The DoS Security Suite Settings enables activating the security suite.

13.6.1. Property

To display Dos Global Setting web page, click **Security > Dos > Property**

Security >> DoS >> Property

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)

DoS Property Page

Field	Description
POD	Avoids ping of death attack.
Land	Drops the packets if the source IP address is equal to the destination IP address.
UDP Blat	Drops the packets if the UDP source port equals to the UDP destination port.
TCP Blat	Drops the packages if the TCP source port is equal to the TCP destination port.
DMAC = SMAC	Drops the packets if the destination MAC address is equal to the source MAC address.
Null Scan Attach	Drops the packets with NULL scan.

X-Mas Scan Attack	Drops the packets if the sequence number is zero, and the FIN, URG and PSH bits are set.
TCP SYN-FIN Attack	Drops the packets with SYN and FIN bits set.
TCP SYN-RST Attack	Drops the packets with SYN and RST bits set.
ICMP Fragment	Drops the fragmented ICMP packets.
TCP- SYN (SPORT<1024)	Drops SYN packets with sport less than 1024.
TCP Fragment (Offset = 1)	Drops the TCP fragment packets with offset equals to one.
Ping Max Size	Specify the maximum size of the ICMPv4/ICMPv6 ping packets. The valid range is from 0 to 65535 bytes, and the default value is 512 bytes.
IPv4 Ping Max Size	Checks the maximum size of ICMP ping packets, and drops the packets larger than the maximum packet size.
IPv6 Ping Max Size	Checks the maximum size of ICMPv6 ping packets, and drops the packets larger than the maximum packet size.
TCP Min Hdr Size	Checks the minimum TCP header and drops the TCP packets with the header smaller than the minimum size. The length range is from 0 to 31 bytes, and default length is 20 bytes.
IPv6 Min Fragment	Checks the minimum size of IPv6 fragments, and drops the packets smaller than the minimum size. The valid range is from 0 to 65535 bytes, and default value is 1240 bytes.
Smurf Attack	Avoids smurf attack. The length range of the netmask is from 0 to 323 bytes, and default length is 0 bytes.

DoS Property fields.

13.6.2. Port Setting

To configure and display the state of DoS protection for interfaces, click **Security > DoS > Port Setting**.

Security >> DoS >> Port Setting

Port Setting Table

☐	Entry	Port	State
☐	1	GE1	Disabled
☐	2	GE2	Disabled
☐	3	GE3	Disabled
☐	4	GE4	Disabled
☐	5	GE5	Disabled
☐	6	GE6	Disabled
☐	7	GE7	Disabled
☐	8	GE8	Disabled
☐	9	GE9	Disabled
☐	10	GE10	Disabled
☐	11	GE11	Disabled
☐	12	GE12	Disabled
☐	13	GE13	Disabled
☐	14	GE14	Disabled
☐	15	GE15	Disabled
☐	16	GE16	Disabled
☐	17	GE17	Disabled
☐	18	GE18	Disabled

Port Setting page.

Field	Description
Port	Interface or port number.
State	Enable/Disable the DoS protection on the interface.

Port Setting fields.

13.7. Dynamic ARP Inspection

Use the Dynamic ARP Inspection pages to configure settings of Dynamic ARP Inspection

13.7.1. Property

To display property page, click **Security > Dynamic ARP Inspection > Property**

This page allow user to configure global and per interface settings of Dynamic ARP Inspection.

Property Page

Field	Description
State	Set checkbox to enable/disable Dynamic ARP Inspection function.

VLAN

Select VLANs in left box then move to right to enable Dynamic ARP Inspection. Or select VLANs in right box then move to left to disable Dynamic ARP Inspection.

Security >> Dynamic ARP Inspection >> Property

State ☐ Enable

Available VLAN Selected VLAN

VLAN 1

Apply

Property Fields

Port Setting Table

	Entry	Port	Trust	Source MAC Address	Destination MAC Address	IP Address	Rate Limit	
☐	1	GE1	Disabled	Disabled	Disabled	Disabled	Unlimited	
☐	2	GE2	Disabled	Disabled	Disabled	Disabled	Unlimited	
☐	3	GE3	Disabled	Disabled	Disabled	Disabled	Unlimited	
☐	4	GE4	Disabled	Disabled	Disabled	Disabled	Unlimited	
☐	5	GE5	Disabled	Disabled	Disabled	Disabled	Unlimited	
☐	6	GE6	Disabled	Disabled	Disabled	Disabled	Unlimited	
☐	7	GE7	Disabled	Disabled	Disabled	Disabled	Unlimited	
☐	8	GE8	Disabled	Disabled	Disabled	Disabled	Unlimited	
☐	9	GE9	Disabled	Disabled	Disabled	Disabled	Unlimited	
☐	10	GE10	Disabled	Disabled	Disabled	Disabled	Unlimited	
☐	11	LAG1	Disabled	Disabled	Disabled	Disabled	Unlimited	
☐	12	LAG2	Disabled	Disabled	Disabled	Disabled	Unlimited	
☐	13	LAG3	Disabled	Disabled	Disabled	Disabled	Unlimited	
☐	14	LAG4	Disabled	Disabled	Disabled	Disabled	Unlimited	
☐	15	LAG5	Disabled	Disabled	Disabled	Disabled	Unlimited	
☐	16	LAG6	Disabled	Disabled	Disabled	Disabled	Unlimited	
☐	17	LAG7	Disabled	Disabled	Disabled	Disabled	Unlimited	
☐	18	LAG8	Disabled	Disabled	Disabled	Disabled	Unlimited	

Edit

Property Port Page

Field	Description
Port	Display port ID.
Trust	Display enable/disabled trust attribute of interface
Source MAC	Display enable/disabled source mac address validation attribute of interface

Address	
Destination MAC Address	Display enable/disabled destination mac address validation attribute of interface
IP Address	Display enable/disabled IP address validation attribute of interface. Allow zero which means allow 0.0.0.0 IP address
Rate Limit	Display rate limitation value of interface.

Property Port Fields

Security >> Dynamic ARP Inspection >> Property

Edit Port Setting

Port
GE1

Trust
☐ Enable

Source MAC Address
☐ Enable

Destination MAC Address
☐ Enable

IP Address
☐ Enable

☐ Allow Zero (0.0.0.0)

Rate Limit
 pps (1 - 50, default 0), 0 is Unlimited

Edit Property Port Dialog

Field	Description
Port	Display selected port to be edited.
Trust	Set checkbox to enable/disabled trust of interface. All ARP packet will be forward directly if enable trust. Default is disabled.
Source MAC Address	Set checkbox to enable or disable source mac address validation of interface. All ARP packets will be checked whether sender mac is same as source mac in Ethernet header if enable source mac address validation. Default is disabled.
Destination MAC Address	Set checkbox to enable or disable destination mac address validation of interface. All ARP packets will be checked whether target mac is same as destination mac in Ethernet header if enable destination mac address validation. Default is disabled.

IP Address	Set checkbox to enable or disable IP address validation of interface. All ARP packets will be checked whether IP address is 0.0.0.0, 255.255.255.255 or multicast address. Default is disabled.
IP Address – Allow Zero	Set checkbox to enable or disable allow zero of IP address validation. 0.0.0.0 IP address is valid if allow zero enable. Default is disabled.
Rate Limit	Input rate limitation of ARP packets. The unit is pps. 0 means unlimited. Default is unlimited.

Edit Property Port Fields

13.7.2. Statistics

To display Statistics page, click **Security > Dynamic ARP Inspection > Statistics**

This page allow user to browse all statistics that recorded by Dynamic ARP Inspection function.

Security >> Dynamic ARP Inspection >> Statistics

Statistics Table

☐	Entry	Port	Forward	Source MAC Failure	Destination MAC Failure	Source IP Validation Failure	Destination IP Validation Failure	IP-MAC Mismatch Failure	
☐	1	GE1	0	0	0	0	0	0	
☐	2	GE2	0	0	0	0	0	0	
☐	3	GE3	0	0	0	0	0	0	
☐	4	GE4	0	0	0	0	0	0	
☐	5	GE5	0	0	0	0	0	0	
☐	6	GE6	0	0	0	0	0	0	
☐	7	GE7	0	0	0	0	0	0	
☐	8	GE8	0	0	0	0	0	0	
☐	9	GE9	0	0	0	0	0	0	
☐	10	GE10	0	0	0	0	0	0	
☐	11	GE11	0	0	0	0	0	0	
☐	12	GE12	0	0	0	0	0	0	
☐	13	GE13	0	0	0	0	0	0	
☐	14	GE14	0	0	0	0	0	0	

Statistics Page

Field	Description
Port	Display port ID
Forwarded	Display how many packets forwarded normally.
Source MAC Failures	Display how many packets dropped by source MAC validation.
Destination MAC Failures	Display how many packets dropped by destination MAC validation.

Source IP Validation Failures	Display how many packets dropped by source IP validation.
Destination IP Validation Failures	Display how many packets dropped by destination IP validation
IP-MAC Mismatch Failures	Display how many packets dropped by IP-MAC doesn't match in IP Source Guard binding table.

Statistics Fields

13.8. DHCP Snooping

Use the DHCP Snooping pages to configure settings of DHCP Snooping

13.8.1. Property

To display property page, click **Security > DHCP Snooping > Property**

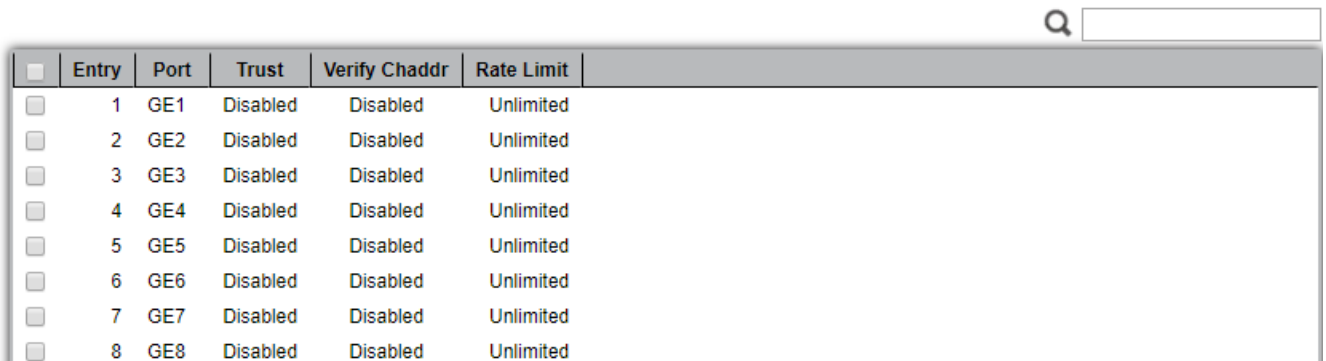
This page allow user to configure global and per interface settings of DHCP Snooping.

Property Page

Field	Description
State	Set checkbox to enable/disable DHCP Snooping function.
VLAN	Select VLANs in left box then move to right to enable DHCP Snooping. Or select VLANs in right box then move to left to disable DHCP Snooping.

Property Fields

Port Setting Table

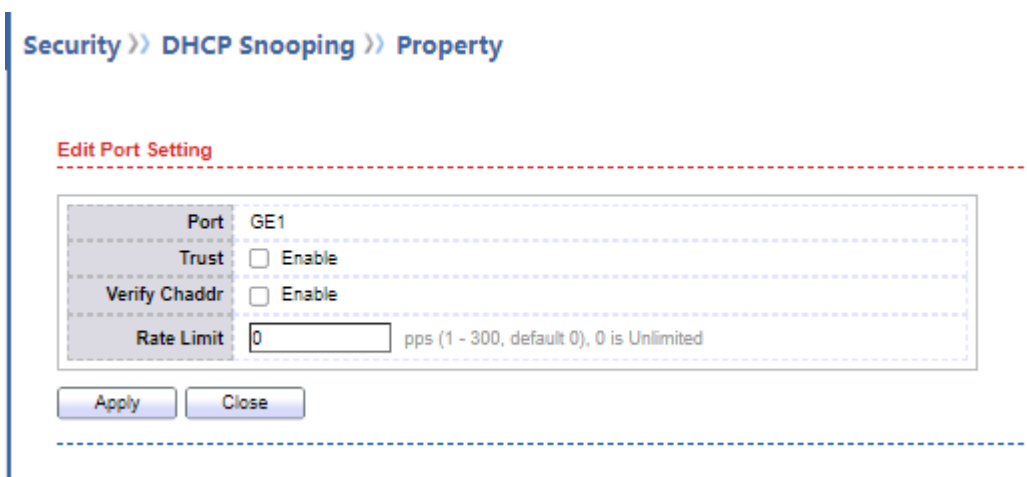


☐	Entry	Port	Trust	Verify Chaddr	Rate Limit
☐	1	GE1	Disabled	Disabled	Unlimited
☐	2	GE2	Disabled	Disabled	Unlimited
☐	3	GE3	Disabled	Disabled	Unlimited
☐	4	GE4	Disabled	Disabled	Unlimited
☐	5	GE5	Disabled	Disabled	Unlimited
☐	6	GE6	Disabled	Disabled	Unlimited
☐	7	GE7	Disabled	Disabled	Unlimited
☐	8	GE8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

Property Port Page

Field	Description
Port	Display port ID.
Trust	Display enable/disabled trust attribute of interface
Verify Chaddr	Display enable/disabled chaddr validation attribute of interface
Rate Limit	Display rate limitation value of interface.

Property Port Fields



Security >> DHCP Snooping >> Property

Edit Port Setting

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

Apply Close

Edit Property Port Dialog

Field	Description
Port	Display selected port to be edited.
Trust	Set checkbox to enable/disabled trust of interface. All DHCP packet will be forward directly if enable trust. Default is disabled.

Verify Chaddr	Set checkbox to enable or disable chaddr validation of interface. All DHCP packets will be checked whether client hardware mac address is same as source mac in Ethernet header if enable chaddr validation. Default is disabled.
Rate Limit	Input rate limitation of DHCP packets. The unit is pps. 0 means unlimited. Default is unlimited.

Edit Property Port Fields

13.8.2. Statistics

To display Statistics page, click **Security > DHCP Snooping > Statistic**

This page allow user to browse all statistics that recorded by DHCP snooping function.

Security >> DHCP Snooping >> Statistics

Statistics Table

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

DHCP Snooping Statistics Page

Field	Description
Port	Display port ID
Forwarded	Display how packets forwarded normally.
Chaddr Check Drop	Display how many packets dropped by chaddr validation.
Untrusted Port Drop	Display how many DHCP server packets that are received by untrusted port dropped.
Untrusted Port with Option82 Drop	Display how many packets dropped by untrusted port with option82 checking.
Invalid Drop	Display how many packets dropped by invalid checking.

Statistics Fields

13.8.3. Option82 Property

To display Option82 Property page, click **Security > DHCP Snooping > Option82 Property**

This page allow user to set string of DHCP option82 remote ID filed. The string will attach in option82 if option inserted.

Security >> DHCP Snooping >> Option82 Property

Option82 Property Page

Field	Description
User Defined	Set checkbox to enable user-defined remote-ID. By default, remote ID is switch mac in byte order.
Remote ID	Input user-defined remote ID. Only available when enable user-define remote ID

Table 10-41 DHCP Snooping Option82 Fields

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

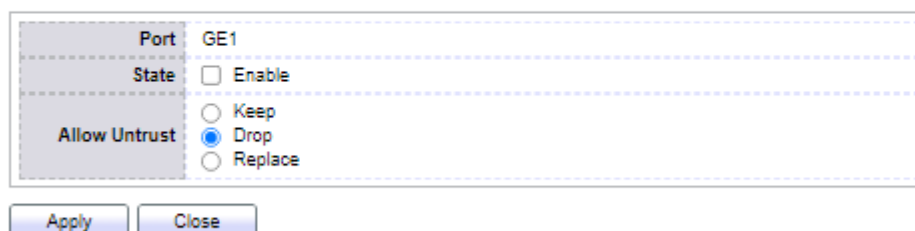
Option82 Port Page

Field	Description
Port	Display port ID
Enable	Display option82 enable/disable status of interface
Allow untrusted	Display allow untrusted action of interface

Option82 Port Fields

Security >> DHCP Snooping >> Option82 Property

Edit Port Setting



The dialog box shows the configuration for port GE1. The 'State' checkbox is unchecked. Under 'Allow Untrust', the 'Drop' radio button is selected, while 'Keep' and 'Replace' are unselected. 'Apply' and 'Close' buttons are at the bottom.

Edit Option82 Port Dialog

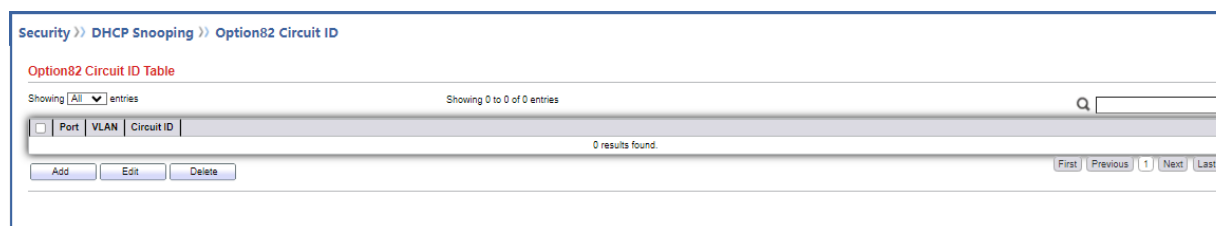
Field	Description
Port	Display selected port to be edited
State	Set checkbox to enable/disable option82 function of interface
Allow untrusted	Select the action perform when untrusted port receive DHCP packet has option82 filed. Default is drop. Keep: Keep original option82 content. Replace: Replace option82 content by switch setting Drop: Drop packets with option82.

Edit Option82 Port Fields

13.8.4. Option82 Circuit ID

To display Option82 Circuit ID page, click **Security > DHCP Snooping > Option82 Circuit ID**

This page allow user to set string of DHCP option82 circuit ID filed. The string will attach in option82 if option inserted.



The page shows the 'Option82 Circuit ID Table' with a search bar and a table. The table has columns for Port, VLAN, and Circuit ID. It shows 0 results found. There are 'Add', 'Edit', and 'Delete' buttons at the bottom left, and 'First', 'Previous', '1', 'Next', and 'Last' buttons at the bottom right.

Option82 Circuit ID Page

Field	Description
-------	-------------

Port	Display port ID of entry
VLAN	Display associate VLAN of entry
Circuit ID	Display circuit ID string of entry

Option82 Circuit ID Fields

Add Option82 Circuit ID

Port

GE1 ▼

VLAN

(1 - 4094) (Keep empty to set without VLAN)

Circuit ID

Apply

Close

Add and Edit Option82 Circuit ID Dialog

Field	Description
Port	Select port from list to associate to CID entry. Only available on Add dialog.
VLAN	Input VLAN ID to associate to circuit ID entry. VLAN ID is not mandatory. Only available on Add dialog.
Circuit ID	Input String as circuit ID. Packets match port and VLAN will be inserted circuit ID.

Option82 Circuit ID Fields

13.9. IP Source Guard

Use the IP Source Guard pages to configure settings of IP Source Guard.

13.9.1. Port Setting

To display Port Setting page, click **Security > IP Source Guard > Port Setting**

This page allow user to configure per port settings of IP Source Guard.

Security >> IP Source Guard >> Port Setting

Port Setting Table

☐	Entry	Port	State	Verify Source	Current Entry	Max Entry
☐	1	GE1	Disabled	IP	0	Unlimited
☐	2	GE2	Disabled	IP	0	Unlimited
☐	3	GE3	Disabled	IP	0	Unlimited
☐	4	GE4	Disabled	IP	0	Unlimited
☐	5	GE5	Disabled	IP	0	Unlimited
☐	6	GE6	Disabled	IP	0	Unlimited
☐	7	GE7	Disabled	IP	0	Unlimited
☐	8	GE8	Disabled	IP	0	Unlimited

Port Setting Page

Field	Description
Port	Display port ID
State	Display IP Source Guard enable/disable status of interface
Verify Source	Display mode of IP Source Guard verification
Current Binding Entry	Display current binding entries of a interface.
Max Binding Entry	Display the number of maximum binding entry of interface

Port Setting Fields

Security >> IP Source Guard >> Port Setting

Edit Port Setting

Port

GE1

State

☐ Enable

Verify Source

☒ IP
☐ IP-MAC

Max Entry

(1 - 50, default 0), 0 is Unlimited

Apply

Close

Edit Port Setting Dialog

Field	Description
Port	Display selected port to be edited.
Status	Set checkbox to enable or disable IP Source Guard function. Default is disabled

Verify Source	Select the mode of IP Source Guard verification IP: Only verify source IP address of packet IP-MAC: Verify source IP and source MAC address of packet
Max Binding Entry	Input the maximum number of entries that a port can be bounded. Default is unlimited on all ports. No entry will be bound if limitation reached.

Edit Port Setting Fields

13.9.2. IMPV Binding

To display IMPV Binding page, click **Security > IP Source Guard > IMPV Binding**

This page allow user to add static IP source guard entry and browse all IP source guard entries that learned by DHCP snooping or statically create by user.

Security >> IP Source Guard >> IMPV Binding

IP-MAC-Port-VLAN Binding Table

Showing All entries

Showing 0 to 0 of 0 entries

☐	Port	VLAN	MAC Address	IP Address	Binding	Type	Lease Time	
0 results found.								
Add Edit Delete								First Previous 1 Next Last

IPMV Binding Page

Field	Description
Port	Display port ID of entry.
VLAN	Display VLAN ID of entry
MAC Address	Display MAC address of entry. Only available of IP-MAC binding entry
IP Address	Display IP address of entry. Mask always to be 255.255.255.255 for IP-MAC binding. IP binding entry display user input.
Binding	Display binding type of entry
Type	Type of existing binding entry Static: Entry added by user. Dynamic: Entry learned by DHCP snooping.
Lease Time	Lease time of DHCP Snooping learned entry. After lease time entry will be deleted. Only available of dynamic entry.

IPMV Binding Fields

Security >> IP Source Guard >> IMPV Binding

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

Apply Close

Edit IP-MAC-Port-VLAN Binding

Port	GE1 ▼
VLAN	33
Binding	IP-MAC-Port-VLAN
MAC Address	00:00:00:00:00:0A
IP Address	3.3.3.3 / 255.255.255.255

Apply Close

Add and Edit IPMV Binding Dialog

Field	Description
Port	Select port from list of a binding entry.
VLAN	Specify a VLAN ID of a binding entry
Binding	Select matching mode of binding entry IP-MAC-Port-VLAN: packet must match IP address, MAC Address, Port and VLAN ID. IP-Port-VLAN: packet must match IP address or subnet, Port and VLAN ID.
MAC Address	Input MAC address. Only available on IP-MAC-Port-VLAN mode.
IP Address	Input IP address and mask. Mask only available on IP-MAC-Port mode.

Add and Edit IPMV Binding Fields

13.9.3. Save Database

To display Save Database page, click **Security > DHCP Snooping > Save Database**

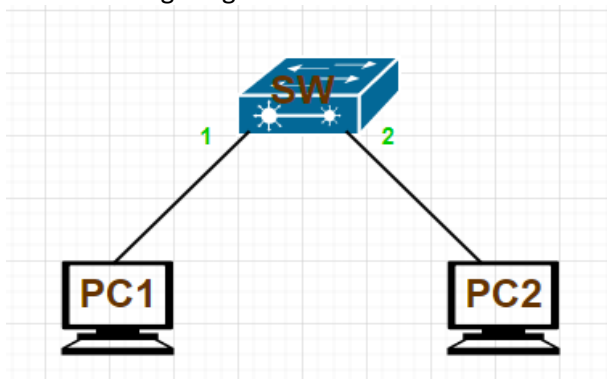
This page allow user to configure DHCP snooping database which can backup and restore dynamic DHCP snooping entries.

Security >> IP Source Guard >> Save Database

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

13.10. Configuration Case

Case 1: Configuring Port Authentication



PC2 according to radius server

- WEB

1、Radius config

Security >> RADIUS

Use Default Parameter	
Retry	3 (1 - 10, default 3)
Timeout	3 Sec (1 - 30, default 3)
Key String	testing123

RADIUS Table

Showing entries

Showing 1 to 1 of 1 entries

☐	Server Address	Server Port	Priority	Retry	Timeout	Usage
☐	192.168.0.111	1812	100	3	3	All

2、802.1x config

Security >> Authentication Manager >> Property

Authentication Type	☒ 802.1x ☐ MAC-Based ☐ WEB-Based
Guest VLAN	☐ Enable 1
MAC-Based User ID Format	XXXXXXXXXX

Port Mode Table

☐	Entry	Port	Authentication Type			Host Mode	Order	Method	Guest VLAN	VLAN Assign Mode
			802.1x	MAC-Based	WEB-Based					
☐	1	GE1	Enabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
☐	2	GE2	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static

Security >> Authentication Manager >> Port Setting

Port Setting Table

☐	Entry	Port	Port Control	Reauthentication	Max Hosts	Common Time	
						Reauthentication	Inactivity
☐	1	GE1	Auto	Disabled	256	3600	

- CLI

```
radius default-config key PrwP3pa64xXsG7yxb0K8yA== retransmit 3 timeout 3
radius host 192.168.0.111 auth-port 1812 priority 100 type all
authentication dot1x
interface vlan1
 ip address 192.168.0.1/24
 ipv6 enable
interface gil
 authentication dot1x
 authentication port-control auto
```

Case 2: Configuring MAC Authentication

- WEB

1、Radius config

Security >> RADIUS

Use Default Parameter	
Retry	3 (1 - 10, default 3)
Timeout	3 Sec (1 - 30, default 3)
Key String	testing123

RADIUS Table

Showing entries

Showing 1 to 1 of 1 entries

☐	Server Address	Server Port	Priority	Retry	Timeout	Usage
☐	192.168.0.111	1812	100	3	3	All

2、802.1x config

Security >> Authentication Manager >> Property

Authentication Type	☐ 802.1x ☒ MAC-Based ☐ WEB-Based
Guest VLAN	☐ Enable 1
MAC-Based User ID Format	XXXXXXXXXXXXX

Apply

Port Mode Table

	Entry	Port	Authentication Type			Host Mode	Order	Method	Guest VLAN	VLAN Assign Mode
			802.1x	MAC-Based	WEB-Based					
☐	1	GE1	Disabled	Enabled	Disabled	Multiple Authentication	MAC-Based	RADIUS	Disabled	Static

Security >> Authentication Manager >> Port Setting

Port Setting Table

	Entry	Port	Port Control	Reauthentication	Max Hosts	Common Time	
						Reauthentication	Inactivity
☐	1	GE1	Auto	Disabled	256	3600	

- CLI

```
radius default-config key PrwP3pa64xXsG7yxb0K8yA== retransmit 3 timeout 3
radius host 192.168.0.111 auth-port 1812 priority 100 type all
authentication dot1x
interface vlan1
 ip address 192.168.0.1/24
 ipv6 enable
interface gil
authentication mac
authentication port-control auto
authentication order mac
```

14. ACL

Use the ACL pages to configure settings for the switch ACL features.

14.1. MAC ACL

To display MAC ACL page, click **ACL > MAC ACL**

This page allow user to add or delete ACL rule. A rule cannot be deleted if under binding.

ACL >> MAC ACL

ACL Name

Apply

MAC ACL Page

Field	Description
ACL Name	Input MAC ACL name

MAC ACL Fields

ACL Table

Showing All entries
Showing 1 to 1 of 1 entries

☐	ACL Name	Rule	Port
☐	111	0	

Delete
First Previous 1 Next Last

MAC ACL Table Page

Field	Description
ACL Name	Display MAC ACL name
Rule	Display the number ACE rule of ACL
Port	Display the port list that bind this ACL

MAC ACL Table Fields

14.2. MAC ACE

To display MAC ACE page, click **ACL > MAC ACE**

This page allow user to add, edit or delete ACE rule. An ACE rule cannot be edited or deleted if ACL under binding.
New ACE cannot be added if ACL under binding.

ACL >> MAC ACE

ACE Table

ACL Name 111

Showing All entries Showing 0 to 0 of 0 entries Q

☐	Sequence	Action	Source MAC		Destination MAC		Ethertype	VLAN	802.1p		
			Address	Mask	Address	Mask			Value	Mask	

0 results found.

AddEditDelete

FirstPrevious1NextLast

MAC ACE Page

Field	Description
ACL Name	Select the ACL name to which an ACE is being added.
Sequence	Display the sequence of ACE.
Action	Display the action of ACE
Source MAC	Display the source MAC address and mask of ACE.
Destination MAC	Display the destination MAC address and mask of ACE.
Ethertype	Display the Ethernet frame type of ACE.
VLAN ID	Display the VLAN ID of ACE
802.1p Value	Display the 802.1p value of ACE.
802.1p Mask	Display the 802.1p mask of ACE.

MAC ACE Fields

ACL >> MAC ACE

Add ACE

ACL Name	111
Sequence	(1 - 2147483647)
Action	☒ Permit ☐ Deny ☐ Shutdown
Source MAC	☒ Any / (Address / Mask)
Destination MAC	☒ Any / (Address / Mask)
Ethertype	☒ Any 0x (0x600 ~ 0xFFFF)
VLAN	☒ Any (1 - 4094)
802.1p	☒ Any / (Value / Mask) (0 - 7)

Add and Edit MAC ACE Dialog

Field	Description
ACL Name	Display the ACL name to which an ACE is being added.
Sequence	Specify the sequence of the ACE. ACEs with higher sequence are processed first (1 is the highest priority). Only available on Add Dialog.
Action	Select the action after ACE match packet. Permit: Forward packets that meet the ACE criteria. Deny: Drop packets that meet the ACE criteria. Shutdown: Drop packets that meet the ACE criteria, and disable the port from where the packets were received. Such ports can be reactivated from the Port Settings page.
Source MAC	Select the type for source MAC address. Any: All source addresses are acceptable. User Defined: Only a source address or a range of source addresses which users define are acceptable. Enter the source MAC address and mask to which will be matched.
Destination MAC	Select the type for Destination MAC address. Any: All destination addresses are acceptable. User Defined: Only a destination address or a range of destination addresses which users define are acceptable. Enter the destination MAC address and mask to which will be matched.
Ethertype	Select the type for Ethernet frame type. Any: All Ethernet frame type is acceptable. User Defined: Only an Ethernet frame type which users define is acceptable. Enter the Ethernet frame type value to which will be matched.
VLAN ID	Select the type for VLAN ID. Any: All VLAN ID is acceptable. User Defined: Only a VLAN ID which users define is acceptable. Enter the VLAN ID to which will be matched.

802.1p

Select the type for 802.1p value.

Any: All 802.1p value is acceptable.

User Defined: Only an 802.1p value or a range of 802.1p value which users define is acceptable. Enter the 802.1p value and mask to which will be matched.

Add and Edit MAC ACE Fields**14.3. IPv4 ACL**

To display IPv4 ACL page, click **ACL > IPv4 ACL**

This page allow user to add or delete Ipv4 ACL rule. A rule cannot be deleted if under binding.

ACL >> IPv4 ACL

ACL Name

111

Apply

IPv4 ACL Page

Field	Description
ACL Name	Input IPv4 ACL name

IPv4 ACL Fields**ACL >> IPv4 ACL**

ACL Name

Apply

ACL Table

Showing All entries

Showing 1 to 1 of 1 entries



☐	ACL Name	Rule	Port
☐	222	0	

First Previous 1 Next Last

Delete

IPv4 ACL Table Page

Field	Description
ACL Name	Display IPv4 ACL name

Rule	Display the number ACE rule of ACL
Port	Display the port list that bind this ACL

IPv4 ACL Table Fields

14.4. IPv4 ACE

To display IPv4 ACE page, click **ACL > IPv4 ACE**

This page allow user to add, edit or delete ACE rule. An ACE rule cannot be edited or deleted if ACL under binding. New ACE cannot be added if ACL under binding.

ACL >> IPv4 ACE

ACE Table

ACL Name 222 ▼

Showing All ▼ 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.

First Previous 1 Next Last

IPv4 ACE Page

Field	Description
ACL Name	Select the ACL name to which an ACE is being added.
Sequence	Display the sequence of ACE.
Action	Display the action of ACE
Protocol	Display the protocol value of ACE
Source IP	Display the source IP address and mask of ACE
Destination IP	Display the destination IP address and mask of ACE
Source Port	Display single source port or a range of source ports of ACE. Only available when protocol is TCP or UDP.
Destination Port	Display single destination port or a range of destination ports of ACE. Only available when protocol is TCP or UDP.
TCP Flags	Display the TCP flag value if ACE. Only available when protocol is TCP.
Type of Service	Display the ToS value of ACE which could be DSCP or IP Precedence.
ICMP	Display the ICMP type and code of ACE. Only available when protocol is ICMP

ACL >> IPv4 ACE

Add ACE

ACL Name	222
Sequence	(1 - 2147483647)
Action	☒ Permit ☐ Deny ☐ Shutdown
Protocol	☒ Any ☐ Select ICMP v ☐ Define (0 - 255)
Source IP	☒ Any / (Address / Mask)
Destination IP	☒ Any / (Address / Mask)
Type of Service	☒ Any ☐ DSCP (0 - 63) ☐ IP Precedence (0 - 7) ☐ Any

Add and Edit IPv4 ACE Dialog

Field	Description
ACL Name	Display the ACL name to which an ACE is being added.
Sequence	Specify the sequence of the ACE. ACEs with higher sequence are processed first (1 is the highest sequence). Only available on Add dialog.
Action	Select the action for a match. Permit: Forward packets that meet the ACE criteria. Deny: Drop packets that meet the ACE criteria. Shutdown: Drop packets that meet the ACE criteria, and disable the port from where the packets were received. Such ports can be reactivated from the Port Settings page.
Protocol	Select the type of protocol for a match. Any (IP): All IP protocols are acceptable. Select from list: Select one of the following protocols from the drop-down list. (ICMP/IPinIP/TCP/EGP/IGP/UDP/HMP/RDP/IPV6/IPV6:ROUT/IPV6:FRAG/RSVP/IPV6:ICMP/OSPF/PIM/L2TP) Protocol ID to match: Enter the protocol ID.
Source IP	Select the type for source IP address. Any: All source addresses are acceptable. User Defined: Only a source address or a range of source addresses which users define are acceptable. Enter the source IP address value and mask to which will be matched.
Destination IP	Select the type for destination IP address. Any: All destination addresses are acceptable. User Defined: Only a destination address or a range of destination addresses which users define are acceptable. Enter the destination IP address value and mask to which will be matched.

Source Port	Select the type of protocol for a match. Only available when protocol is TCP or UDP. Any: All source ports are acceptable. Single: Enter a single TCP/UDP source port to which packets are matched. Range: Select a range of TCP/UDP source ports to which the packet is matched. There are eight different port ranges that can be configured (shared between source and destination ports). TCP and UDP protocols each have eight port ranges.
Destination Port	Select the type of protocol for a match. Only available when protocol is TCP or UDP. Any: All source ports are acceptable. Single: Enter a single TCP/UDP source port to which packets are matched. Range: Select a range of TCP/UDP source ports to which the packet is matched. There are eight different port ranges that can be configured (shared between source and destination ports). TCP and UDP protocols each have eight port ranges.
TCP Flags	Select one or more TCP flags with which to filter packets. Filtered packets are either forwarded or dropped. Filtering packets by TCP flags increases packet control, which increases network security. Only available when protocol is TCP.
Type of Service	Select the type of service for a match. Any: All types of service are acceptable. DSCP to match: Enter a Differentiated Services Code Point (DSCP) to match. IP Precedence to match: Enter a IP Precedence to match.
ICMP Type	Either select the message type by name or enter the message type number. Only available when protocol is ICMP. Any: All message types are acceptable. Select from list: Select message type by name. Protocol ID to match: Enter the number of message type.
ICMP Code	Select the type for ICMP code. Only available when protocol is ICMP. Any: All codes are acceptable. User Defined: Enter an ICMP code to match.

Add and Edit IPv4 ACL Fields

14.5. IPv6 ACL

To display IPv6 ACL page, click **ACL > IPv6 ACL**

This page allow user to add or delete Ipv6 ACL rule. A rule cannot be deleted if under binding.

ACL >> IPv6 ACL

ACL Name

Apply

IPv6 ACL Page

Field	Description
ACL Name	Input IPv6 ACL name

IPv6 ACL Fields

ACL Table

Showing **All** entries Showing 1 to 1 of 1 entries

☐	ACL Name	Rule	Port
☐	333	0	

First Previous 1 Next Last

Delete

IPv6 ACL Table Page

Field	Description
ACL Name	Display IPv6 ACL name
Rule	Display the number ACE rule of ACL
Port	Display the port list that bind this ACL

IPv6 ACL Table Fields

14.6. IPv6 ACE

To display IPv6 ACE page, click **ACL > IPv6 ACE**

This page allow user to add, edit or delete ACE rule. An ACE rule cannot be edited or deleted if ACL under binding. New ACE cannot be added if ACL under binding.

ACL >> IPv6 ACE

ACE Table

ACL Name **333**

Showing **All** 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.														

Add Edit Delete

First Previous 1 Next Last

IPv6 ACE Page

Field	Description
ACL Name	Select the ACL name to which an ACE is being added.
Sequence	Display the sequence of ACE.
Action	Display the action of ACE
Protocol	Display the protocol value of ACE
Source IP	Display the source IP address and prefix of ACE

Destination IP	Display the destination IP address and prefix of ACE
Source Port	Display single source port or a range of source ports of ACE. Only available when protocol is TCP or UDP.
Destination Port	Display single destination port or a range of destination ports of ACE. Only available when protocol is TCP or UDP.
TCP Flags	Display the TCP flag value if ACE. Only available when protocol is TCP.
Type of Service	Display the ToS value of ACE which could be DSCP or IP Precedence.
ICMP	Display the ICMP type and code of ACE. Only available when protocol is ICMP

IPv6 ACE Fields

ACL >> IPv6 ACE

Add ACE

ACL Name	333
Sequence	(1 - 2147483647)
Action	☒ Permit ☐ Deny ☐ Shutdown
Protocol	☒ Any ☐ Select TCP v ☐ 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) ☐ Any

Add and Edit IPv6 ACE Dialog

Field	Description
ACL Name	Display the ACL name to which an ACE is being added.
Sequence	Specify the sequence of the ACE. ACEs with higher sequence are processed first (1 is the highest sequence). Only available on Add dialog.
Action	Select the action for a match. Permit: Forward packets that meet the ACE criteria. Deny: Drop packets that meet the ACE criteria. Shutdown: Drop packets that meet the ACE criteria, and disable the port from where the packets were received. Such ports can be reactivated from the Port Settings page.
Protocol	Select the type of protocol for a match. Any (IP): All IP protocols are acceptable. Select from list: Select one of the following protocols from the drop- down list. (TCP / UDP / ICMP) Protocol ID to match: Enter the protocol ID.
Source IP	Select the type for source IP address. Any: All source addresses are acceptable. User Defined: Only a source address or a range of source addresses which users define are acceptable. Enter the source IP address value and prefix length to which will be matched.
Destination IP	Select the type for destination IP address. Any: All destination addresses are acceptable. User Defined: Only a destination address or a range of destination addresses which users define are acceptable. Enter the destination IP address value and prefix to which will be matched.

Source Port	Select the type of protocol for a match. Only available when protocol is TCP or UDP. Any: All source ports are acceptable. Single: Enter a single TCP/UDP source port to which packets are matched. Range: Select a range of TCP/UDP source ports to which the packet is matched. There are eight different port ranges that can be configured (shared between source and destination ports). TCP and UDP protocols each have eight port ranges.
Destination Port	Select the type of protocol for a match. Only available when protocol is TCP or UDP. Any: All source ports are acceptable. Single: Enter a single TCP/UDP source port to which packets are matched. Range: Select a range of TCP/UDP source ports to which the packet is matched. There are eight different port ranges that can be configured (shared between source and destination ports). TCP and UDP protocols each have eight port ranges.
TCP Flags	Select one or more TCP flags with which to filter packets. Filtered packets are either forwarded or dropped. Filtering packets by TCP flags increases packet control, which increases network security. Only available when protocol is TCP.
Type of Service	Select the type of service for a match. Any: All types of service are acceptable. DSCP to match: Enter a Differentiated Services Code Point (DSCP) to match. IP Precedence to match: Enter a IP Precedence to match.
ICMP Type	Either select the message type by name or enter the message type number. Only available when protocol is ICMP. Any: All message types are acceptable. Select from list: Select message type by name. Protocol ID to match: Enter the number of message type.

ICMP Code	Select the type for ICMP code. Only available when protocol is ICMP. Any: All codes are acceptable. User Defined: Enter an ICMP code to match.
-----------	---

Add and Edit IPv6 ACE Fields

14.7. ACL Binding

To display ACL Binding page, click **ACL > ACL Binding**

This page allow user to bind or unbind ACL rule to or from interface. IPv4 and Ipv6 ACL cannot be bound to the same port simultaneously.

ACL >> ACL Binding

ACL Binding Table

☐	Entry	Port	MAC ACL	IPv4 ACL	IPv6 ACL
☐	1	GE1			
☐	2	GE2			
☐	3	GE3			
☐	4	GE4			
☐	5	GE5			
☐	6	GE6			
☐	7	GE7			

ACL Binding Page

Field	Description
Port	Display port entry ID.
MAC ACL	Display mac ACL name that bound of interface. Empty means no rule bound.
IPv4 ACL	Display ipv4 ACL name that bound of interface. Empty means no rule bound.
IPv6 ACL	Display ipv6 ACL name that bound of interface. Empty means no rule bound.

ACL Binding Fields

ACL >> ACL Binding

Add ACL Binding

Port

GE1

Note: ACL without any rules cannot be bound

MAC ACL

None ▼

IPv4 ACL

None ▼

IPv6 ACL

None ▼

Apply

Close

Add and Edit ACL Binding Dialog

Field	Description
Port	Display port entry ID.
MAC ACL	Select mac ACL name from list to bind.
IPv4 ACL	Select IPv4 ACL name from list to bind.
IPv6 ACL	Select IPv6 ACL name from list to bind.

Add and Edit ACL Binding Fields

14.8. Configuration Case

Case 1: Create Port 1 to reject all IP traffic

- Web
 1. Configure ACL name

ACL >> IPv4 ACL

ACL Name

Apply

ACL Table

Showing All ▾ entries

Showing 1 to 1 of 1 entries

☐	ACL Name	Rule	Port
☐	222	1	gi1

Delete

2.Configure ACL rules

ACL >> IPv4 ACL

ACL Name

Apply

ACL Table

Showing All ▾ entries

Showing 1 to 1 of 1 entries

☐	ACL Name	Rule	Port
☐	222	1	gi1

Delete

3.Bind Port 1 to Port 1

ACL >> IPv4 ACL

ACL Name	
----------	----------------------

ACL Table

Showing All entries

Showing 1 to 1 of 1 entries

☐	ACL Name	Rule	Port
☐	222	1	gi1

- CLI

```
ip acl 222
sequence 1 deny ip any any
exit

interface gi1
ip acl 222
```

15. QoS

Use the QoS pages to configure settings for the switch QoS interface.

15.1. General

Use the QoS general pages to configure settings for general purpose.

15.1.1. Property

To display Property web page, click **QoS > General > Property**

QoS >> General >> Property

State	☐ Enable
Trust Mode	☒ CoS ☐ DSCP ☐ CoS-DSCP ☐ IP Precedence

QoS Global Setting

Field	Description
-------	-------------

State	Set checkbox to enable/disable QoS.
Trust Mode	Select QoS trust mode CoS: Traffic is mapped to queues based on the CoS field in the VLAN tag, or based on the per-port default CoS value (if there is no VLAN tag on the incoming packet), the actual mapping of the CoS to queue can be configured on port setting dialog. DSCP: All IP traffic is mapped to queues based on the DSCP field in the IP header. The actual mapping of the DSCP to queue can be configured on the DSCP mapping page. If traffic is not IP traffic, it is mapped to the best effort queue. CoS-DSCP: Uses the trust CoS mode for non-IP traffic trust DSCP mode for IP traffic. IP Precedence: Traffic is mapped to queues based on the IP precedence. The actual mapping of the IP precedence to queue can be configured on the IP Precedence mapping page.

QoS Global Setting Fields

Port Setting Table

☐	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
☐	4	GE4	0	Enabled	Disabled	Disabled	Disabled
☐	5	GE5	0	Enabled	Disabled	Disabled	Disabled

QoS Port Setting Table

Field	Description
Port	Port name
CoS	Port default CoS priority value for the selected ports
Trust	Port trust state Enabled: Traffic will follow trust mode in global setting Disabled: Traffic will always use best efforts

Remarking (CoS)	Port CoS remarking admin state Enabled: CoS remarking is enabled Disabled: CoS remarking is disabled
Remarking (DSCP)	Port DSCP remarking admin state Enabled: DSCP remarking is enabled Disabled: DSCP remarking is disabled
Remarking (IP Precedence)	Port IP Precedence remarking admin state Enabled: IP Precedence remarking is enabled Disabled: IP Precedence remarking is disabled

QoS Port Setting Table Fields

QoS >> General >> Property

Edit Port Setting

Port
GE1

CoS
 (0 - 7)

Trust
☒ Enable

Remarking

CoS
☐ Enable

DSCP
☐ Enable

IP Precedence
☐ Enable

Apply

Close

Edit QoS Port Setting

Field	Description
Port	Select port list
CoS	Set default CoS/802.1p priority value for the selected ports
Trust	Set checkbox to enable/disable port trust state

Remarking (CoS)	Set checkbox to enable/disable port CoS remarking
Remarking (DSCP)	Set checkbox to enable/disable port DSCP remarking
Remarking (IP Precedence)	Set checkbox to enable/disable port IP Precedence remarking

Edit QoS Port Setting Fields

15.1.2. Queue Scheduling

To display Queue Scheduling web page, click **QoS > General > Queue Scheduling**.

The switch supports eight queues for each interface. Queue number 8 is the highest priority queue. Queue number 1 is the lowest priority queue. There are two ways of determining how traffic in queues is handled, Strict Priority (SP) and Weighted Round Robin (WRR).

Strict Priority (SP)—Egress traffic from the highest priority queue is transmitted first. Traffic from the lower queues is processed only after the highest queue has been transmitted, which provide the highest level of priority of traffic to the highest numbered queue.

Weighted Round Robin (WRR)—In WRR mode the number of packets sent from the queue is proportional to the weight of the queue (the higher the weight, the more frames are sent).

The queuing modes can be selected on the Queue page. When the queuing mode is by Strict Priority, the priority sets the order in which queues are serviced, starting with queue_8 (the highest priority queue) and going to the next lower queue when each queue is completed.

When the queuing mode is Weighted Round Robin, queues are serviced until their quota has been used up and then another queue is serviced. It is also possible to assign some of the lower queues to WRR, while keeping some of the higher queues in Strict Priority. In this case traffic for the SP queues is always sent before traffic from the WRR queues. After the SP queues have been emptied, traffic from the WRR queues is forwarded. (The relative portion from each WRR queue depends on its weight).

QoS >> General >> Queue Scheduling

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

Queue Scheduling Table

Field	Description
Queue	Queue ID to configure
Strict Priority	Set queue to strict priority type
WRR	Set queue to Weight round robin type
Weight	If the queue type is WRR, set the queue weight for the queue.
WRR Bandwidth	Percentage of WRR queue bandwidth

Queue Scheduling Table fields.

15.1.3. CoS Mapping

To display CoS Mapping web page, click **QoS > General > CoS Mapping**

The CoS to Queue table determines the egress queues of the incoming packets based on the 802.1p priority in their VLAN tags. For incoming untagged packets, the 802.1p priority will be the default CoS/802.1p priority assigned to the ingress ports.

Use the Queues to CoS table to remark the CoS/802.1p priority for egress traffic from each queue.

QoS >> General >> CoS Mapping

CoS to Queue Mapping

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

Apply

CoS to Queue Mapping Table

Field	Description
CoS	CoS value
Queue	Select queue id for the CoS value

CoS to Queue Mapping Table Fields

Queue to CoS Mapping

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

Apply

Queue to CoS Mapping Table

Field	Description
Queue	Queue ID

Cos

Select CoS value for the queue id

Queue to CoS Mapping Table Fields

15.1.4. DSCP Mapping

To display DSCP Mapping web page, click **QoS > General > DSCP Mapping**

The DSCP to Queue table determines the egress queues of the incoming IP packets based on their DSCP values. The original VLAN Priority Tag (VPT) of the packet is unchanged.

Use the Queues to DSCP page to remark DSCP value for egress traffic from each queue.

QoS >> General >> DSCP Mapping

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

DSCP to Queue Mapping Table

Field	Description
DSCP	DSCP value
Queue	Select queue id for DSCP value

DSCP to Queue Mapping Table Fields

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

Queue to DSCP Mapping Table

Field	Description
Queue	Queue ID
DSCP	Select DSCP value for queue id

Queue to DSCP Mapping Table Fields

15.1.5. IP Precedence Mapping

To display IP Precedence Mapping web page, click **QoS > General > IP Precedence Mapping**

This page allow user to configure IP Precedence to Queue mapping and Queue to IP Precedence mapping.

QoS >> General >> IP Precedence Mapping

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

IP Precedence to Queue Mapping Table

Field	Description
IP Precedence	IP Precedence value
Queue	Queue value which IP Precedence is mapped

IP Precedence to Queue Mapping Table Fields

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

Queue to IP Precedence Mapping Table

Field	Description
Queue	Queue ID
IP Precedence	IP Precedence value which queue is mapped

Queue to IP Precedence Mapping Table Fields

15.2. Rate Limit

Use the Rate Limit pages to define values that determine how much traffic the switch can receive and send on specific port or queue.

15.2.1. Ingress / Egress Port

To display Ingress / Egress Port web page, click **QoS > Rate Limit > Ingress / Egress Port**

This page allow user to configure ingress port rate limit and egress port rate limit. The ingress rate limit is the number of bits per second that can be received from the ingress interface. Excess bandwidth above this limit is discarded.

QoS >> Rate Limit >> Ingress / Egress Port

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	

Ingress/Egress Port Table

Field	Description
Port	Port name
Ingress (State)	Port ingress rate limit state Enabled: Ingress rate limit is enabled Disabled: Ingress rate limit is disabled
Ingress (Rate)	Port ingress rate limit value if ingress rate state is enabled
Egress (State)	Port egress rate limit state Enabled: Egress rate limit is enabled Disabled: Egress rate limit is disabled
Egress (Rate)	Port egress rate limit value if egress rate state is enabled

Ingress/Egress Port Table Fields

QoS >> Rate Limit >> Ingress / Egress Port

Edit Ingress / Egress Port

Port

GE1

Ingress

☐ Enable

Kbps (16 - 1000000)

Egress

☐ Enable

Kbps (16 - 1000000)

Apply

Close

Edit Ingress/Egress Port

Field	Description
Port	Select port list
Ingress	Set checkbox to enable/disable ingress rate limit. If ingress rate limit is enabled, rate limit value need to be assigned.
Egress	Set checkbox to enable/disable egress rate limit. If egress rate limit is enabled, rate limit value need to be assigned.

Edit Ingress/Egress Port Fields

15.2.2. Egress Queue

To display Egress Queue web page, click **QoS > Rate Limit > Egress Queue**. Egress rate limiting is performed by shaping the output load.

QoS >> Rate Limit >> Egress Queue

Egress Queue Table

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

Egress Queue Table

Field	Description
Port	Port name
Queue 1 (State)	Port egress queue 1 rate limit state Enabled: Egress queue rate limit is enabled Disabled: Egress queue rate limit is disabled
Queue 1 (CIR)	Queue 1 egress committed information rate
Queue 2 (State)	Port egress queue 2 rate limit state Enabled: Egress queue rate limit is enabled Disabled: Egress queue rate limit is disabled
Queue 2 (CIR)	Queue 2 egress committed information rate
Queue 3 (State)	Port egress queue 3 rate limit state Enabled: Egress queue rate limit is enabled Disabled: Egress queue rate limit is disabled
Queue 3 (CIR)	Queue 3 egress committed information rate
Queue 4 (State)	Port egress queue 4 rate limit state Enabled: Egress queue rate limit is enabled Disabled: Egress queue rate limit is disabled
Queue 4 (CIR)	Queue 4 egress committed information rate

Queue 5 (State)	Port egress queue 5 rate limit state Enabled: Egress queue rate limit is enabled Disabled: Egress queue rate limit is disabled
Queue 5 (CIR)	Queue 5 egress committed information rate
Queue 6 (State)	Port egress queue 6 rate limit state Enabled: Egress queue rate limit is enabled Disabled: Egress queue rate limit is disabled
Queue 6 (CIR)	Queue 6 egress committed information rate
Queue 7 (State)	Port egress queue 7 rate limit state Enabled: Egress queue rate limit is enabled Disabled: Egress queue rate limit is disabled
Queue 7 (CIR)	Queue 7 egress committed information rate
Queue 8 (State)	Port egress queue 8 rate limit state Enabled: Egress queue rate limit is enabled Disabled: Egress queue rate limit is disabled
Queue 8 (CIR)	Queue 8 egress committed information rate

Egress Queue Table Fields.

QoS >> Rate Limit >> Egress Queue

Edit Egress Queue

Port	GE1	
Queue 1	☐ Enable	
	1000000	Kbps (16 - 1000000)
Queue 2	☐ Enable	
	1000000	Kbps (16 - 1000000)
Queue 3	☐ Enable	
	1000000	Kbps (16 - 1000000)
Queue 4	☐ Enable	
	1000000	Kbps (16 - 1000000)
Queue 5	☐ Enable	
	1000000	Kbps (16 - 1000000)
Queue 6	☐ Enable	
	1000000	Kbps (16 - 1000000)
Queue 7	☐ Enable	
	1000000	Kbps (16 - 1000000)

Edit Egress Queue

Field	Description
Port	Select port list
Queue 1	Set checkbox to enable/disable egress queue 1 rate limit. If egress rate limit is enabled, rate limit value need to be assigned.
Queue 2	Set checkbox to enable/disable egress queue 2 rate limit. If egress rate limit is enabled, rate limit value need to be assigned.
Queue 3	Set checkbox to enable/disable egress queue 3 rate limit. If egress rate limit is enabled, rate limit value need to be assigned.
Queue 4	Set checkbox to enable/disable egress queue 4 rate limit. If egress rate limit is enabled, rate limit value need to be assigned.
Queue 5	Set checkbox to enable/disable egress queue 5 rate limit. If egress rate limit is enabled, rate limit value need to be assigned.
Queue 6	Set checkbox to enable/disable egress queue 6 rate limit. If egress rate limit is

	enabled, rate limit value need to be assigned.
Queue 7	Set checkbox to enable/disable egress queue 7 rate limit. If egress rate limit is enabled, rate limit value need to be assigned.
Queue 8	Set checkbox to enable/disable egress queue 8 rate limit. If egress rate limit is enabled, rate limit value need to be assigned.

Edit Egress Queue Fields.

15.3. Configuration Case

Case 1: The speed limit for port 1 entrance and exit is 1000kbps

- Web

QoS >> Rate Limit >> Ingress / Egress Port

Ingress / Egress Port Table

☐	Entry	Port	Ingress		Egress	
			State	Rate (Kbps)	State	Rate (Kbps)
☐	1	GE1	Enabled	1008	Enabled	1008

- CLI

```
interface gil
rate-limit ingress 1008
rate-limit egress 1008
```

16. Diagnostics

Use the Diagnostics pages to configure settings for the switch diagnostics feature or operating diagnostic utilities.

16.1. Logging

16.1.1. Property

To enable/disable the logging service, click **Diagnostic > Logging > Property**.

Diagnostics >> Logging >> Property

State	☒ Enable
Aggregation	☐ Enable
Aging Time	300 Sec (15 - 3600, default 300)
Console Logging	
State	☒ Enable
Minimum Severity	Notice Note: Emergency, Alert, Critical, Error, Warning, Notice
RAM Logging	
State	☒ Enable
Minimum Severity	Notice Note: Emergency, Alert, Critical, Error, Warning, Notice
Flash Logging	
State	☐ Enable
Minimum Severity	Notice Note: Emergency, Alert, Critical, Error, Warning, Notice

Logging Property page.

Field	Description
State	Enable/Disable the global logging services. When the logging service is enabled, logging configuration of each destination rule can be individually configured. If the logging service is disabled, no messages will be sent to these destinations.

Logging Property fields.

Field	Description
State	Enable/Disable the console logging service.

Minimum Severity	The minimum severity for the console logging.
------------------	---

Console Logging fields.

Field	Description
State	Enable/Disable the RAM logging service.
Minimum Severity	The minimum severity for the RAM logging.

RAM Logging fields.

Field	Description
State	Enable/Disable the flash logging service.
Minimum Severity	The minimum severity for the flash logging.

Flash Logging fields.**16.1.2. Remove Server**

To configure the remote logging server, click **Diagnostic > Logging > Remote Server**.

[Diagnostics](#) >> [Logging](#) >> [Remote Server](#)

Remote Server Table

						Q
☐	Entry	Server Address	Server Port	Facility	Minimum Severity	
0 results found.						
Add Edit Delete						

Remote Server page.

Field	Description
Server Address	The IP address of the remote logging server.
Server Ports	The port number of the remote logging server.
Facility	The facility of the logging messages. It can be one of the following values: local0, local1, local2, local3, local4, local5, local6, and local7.

Severity	The minimum severity. Emergency: System is not usable. Alert: Immediate action is needed. Critical: System is in the critical condition. Error: System is in error condition Warning: System warning has occurred Notice: System is functioning properly, but a system notice has occurred. Informational: Device information. Debug: Provides detailed information about an event.
----------	--

Remote Server fields.

16.2. Mirroring

To display Port Mirroring web page, click **Diagnostics > Mirroring**

Diagnostics >> Mirroring

Mirroring Table

Session ID	State	Monitor Port	Ingress Port	Egress Port	
☐ 1	Disabled	---	---	---	
☐ 2	Disabled	---	---	---	
☐ 3	Disabled	---	---	---	
☐ 4	Disabled	---	---	---	

Edit

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

Mirroring Page

Field	Description
Session ID	Select mirror session ID
State	Select mirror session state : port-base mirror or disable Enabled: Enable port based mirror Disabled: Disable mirror.
Monitor Port	Select mirror session monitor port, and select whether normal packet could be sent or received by monitor port.

Ingress port	Select mirror session source rx ports
Egress ports	Select mirror session source tx ports

Mirroring Fields

16.3. Ping

For the ping functionality, click **Diagnostic > Ping**.

Diagnostics >> Ping

Address Type	☒ Hostname ☐ IPv4 ☐ IPv6
Server Address	
Count	4 (1 - 32)

Ping Result

Packet Status	
Status	N/A
Transmit Packet	0
Receive Packet	0
Packet Lost	0%

Round Trip Time	
Min	0.0 ms
Max	0.0 ms
Average	0.0 ms

Ping page.

Field	Description
Address Type	Specify the address type to "Hostname", "IPv6", or "IPv4".
Server Address	Specify the Hostname/IPv4/IPv6 address for the remote logging server.
Count	Specify the numbers of each ICMP ping request.

Ping fields.

16.4. Traceroute

For trace route functionality, click **Diagnostic > Traceroute**.

Diagnostics >> Traceroute

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

Traceroute Result

Traceroute page.

Field	Description
Address Type	Specify the address type to “Hostname”, or “IPv4”.
Server Address	Specify the Hostname/IPv4 address for the remote logging server.
Time to Live	Specify the max hops of hosts for traceroute.

Traceroute fields.

16.5. Copper Test

For copper length diagnostic, click **Diagnostic > Copper Test**.

Diagnostics >> Copper Test

Port	GE1 ▼
------	-------

Copper Test

Copper Test Result

Cable Status	
Port	N/A
Result	N/A
Length	N/A

Copper Test page.

Field	Description
Port	Specify the interface for the copper test.

Copper Test fields.

Field	Description
Port	The interface for the copper test.
Result	The status of copper test. It include: OK: Correctly terminated pair. Short Cable: Shorted pair. Open Cable: Open pair, no link partner. Impedance Mismatch: Terminating impedance is not in the reference range. Line Drive:
Length	Distance in meter from the port to the location on the cable where the fault was discovered.

Copper Result fields.

16.6. Fiber Module

The Optical Module Status page displays the operational information reported by the Small Form-factor Pluggable (SFP) transceiver. Some information may not be available for SFPs without the

supports of digital diagnostic monitoring standard SFF-8472.

To display the Optical Module Diagnostic page, click **Diagnostic > Fiber Module**.

[Diagnostics](#) >> [Fiber Module](#)

Fiber Module Table

	Port	Temperature (C)	Voltage (V)	Current (mA)	Output Power (mW)	Input Power (mW)	OE Present	Loss of Signal	
☐	TE1	N/A	N/A	N/A	N/A	N/A	Remove	Loss	
☐	TE2	N/A	N/A	N/A	N/A	N/A	Remove	Loss	
☐	TE3	N/A	N/A	N/A	N/A	N/A	Remove	Loss	
☐	TE4	N/A	N/A	N/A	N/A	N/A	Remove	Loss	
☐	TE5	N/A	N/A	N/A	N/A	N/A	Remove	Loss	
☐	TE6	N/A	N/A	N/A	N/A	N/A	Remove	Loss	

Refresh
Detail

Fiber Module page.

Field	Description
Port	Interface or port number.
Temperature	Internally measured transceiver temperature.
Voltage	Internally measured supply voltage.
Current	Measured TX bias current.
Output Power	Measured TX output power in milliwatts.
Input Power	Measured RX received power in milliwatts.
Transmitter Fault	State of TX fault.
OE Present	Indicate transceiver has achieved power up and data is ready.
Loss of Signal	Loss of signal.
Refresh	Refresh the page.
Detail	The detail information on the specified port.

Fiber Module fields.

Fiber Module Table

Q

	Port	Temperature (C)	Voltage (V)	Current (mA)	Output Power (mW)	Input Power (mW)	OE Present	Loss of Signal	
☐	TE1	N/A	N/A	N/A	N/A	N/A	Remove	Loss	
☐	TE2	N/A	N/A	N/A	N/A	N/A	Remove	Loss	
☐	TE3	N/A	N/A	N/A	N/A	N/A	Remove	Loss	
☐	TE4	N/A	N/A	N/A	N/A	N/A	Remove	Loss	
☐	TE5	N/A	N/A	N/A	N/A	N/A	Remove	Loss	
☐	TE6	N/A	N/A	N/A	N/A	N/A	Remove	Loss	

Refresh

Detail

Fiber Module Status page.

16.7. UDLD

Use the UDLD pages to configure settings of UDLD function.

16.7.1. Property

To display Property page, click **Diagnostics > UDLD > Property**

This page allow user to configure global and per interface settings of UDLD.

Diagnostics >> UDLD >> Property

Message Time	15	Sec (1 - 90, default 15)
---------------------	---------------------------------	--------------------------

Port Setting Table

☐	Entry	Port	Mode	Bidirectional State	Operational Status	Neighbor	
☐	1	GE1	Disabled	Unknown		0	
☐	2	GE2	Disabled	Unknown		0	
☐	3	GE3	Disabled	Unknown		0	
☐	4	GE4	Disabled	Unknown		0	
☐	5	GE5	Disabled	Unknown		0	
☐	6	GE6	Disabled	Unknown		0	
☐	7	GE7	Disabled	Unknown		0	

Figure 14-9: Property page.

Port Setting Table

☐	Entry	Port	Mode	Bidirectional State	Operational Status	Neighbor	
☐	1	GE1	Disabled	Unknown		0	
☐	2	GE2	Disabled	Unknown		0	
☐	3	GE3	Disabled	Unknown		0	
☐	4	GE4	Disabled	Unknown		0	
☐	5	GE5	Disabled	Unknown		0	
☐	6	GE6	Disabled	Unknown		0	
☐	7	GE7	Disabled	Unknown		0	

Property Port page.

Diagnostics >> UDLD >> Property

Edit Port Setting

Port

GE1

Mode

☒ Disabled
☐ Normal
☐ Aggressive

Apply

Close

Edit Property Port page.

Field	Description
Message Time	Input the interval for sending message. Range is 1 -90 seconds.

Property Fields

Field	Description
Port	Display port ID of entry.
Mode	Display UDLD running mode of interface.
Bidirectional State	Display bidirectional state of interface.
Operational Status	Display operational status of interface
Neighbor	Display the number of neighbor of interface

Property Port Fields

Field	Description
Port	Display selected port to be edited.
Mode	Select UDLD running mode of interface. Disabled: Disable UDLD function. Normal: Running on normal mode that port goes to Link Up One phase after last neighbor ages out. Aggressive: Running on aggressive mode that port goes to Re-Establish phase after last

neighbor ages out.

Edit Property Port Fields

16.7.2. Neighbor

To display Neighbor page, click **Diagnostics > UDLD > Neighbor**

Diagnostics >> UDLD >> Neighbor

Neighbor Table

Entry	Expiration Time	Current Neighbor State	Device ID	Device Name	Port ID	Message Interval	Timeout Interval	
0 results found.								
Refresh								

Neighbor page.

Field	Description
Entry	Display entry index.
Expiration Time	Display expiration time before age out.
Current Neighbor State	Display neighbor current state
Device ID	Display neighbor device ID.
Device Name	Display neighbor device name.
Port ID	Display neighbor port ID that connected.
Message Interval	Display neighbor message interval.
Timeout Interval	Display neighbor timeout interval

Neighbor fields.

16.8. Configuration Case

Case 1: Monitor the incoming/outgoing messages of Gigabit Ethernet 2 using port Gigabit Ethernet 1.

- Web

Diagnostics >> Mirroring

4 Disabled --- ---

Edit

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

Session ID	1	
State	☒ Enable	
Monitor Port	GE1 ▾ ☒ Send or Receive Normal Packet	
Ingress Port	Available Port GE1 GE3 GE4 GE5 GE6 GE7 GE8 GE9	Selected Port GE2
Egress Port	Available Port GE1 GE3 GE4	Selected Port GE2

● CLI

```
switch#configure
switch(config)# mirror session 1 source interfaces gi2 rx
switch(config)# mirror session 1 source interfaces gi2 tx
switch(config)# mirror session 1 destination interface gi1 allow-ingress
```

17. Management

Use the Management pages to configure settings for the switch management features.

17.1. User Account

To display User Account web page, click **Management > User Account**

The default username/password is **admin/admin**. And default account is not able to be deleted.

Use this page to add additional users that are permitted to manage the switch or to change the passwords of existing users.

Management >> User Account

User Account

Showing All ▾ entries

☐	Username	Privilege
☐	admin	Admin

User Account Table

Field	Description
Username	User name of the account
Privilege	Select privilege level for new account. Admin: Allow to change switch settings. Privilege value equals to 15. User: See switch settings only. Not allow to change it. Privilege level equals to 1.

User Account Table Fields

Management >> User Account

Edit User Account

Username	admin
Password	
Confirm Password	
Privilege	☒ Admin ☐ User

Add/Edit User Account Dialog

Field	Description
Username	User name of the account
Password	Set password of the account
Confirm Password	Set the same password of the account as in “Password” field
Privilege	Select privilege level for new account. Admin: Allow to change switch settings. Privilege value equals to 15. User: See switch settings only. Not allow to change it. Privilege level equals to 1.

Add/Edit User Account Fields

17.2. Firmware

17.2.1. Upgrade / Backup

To display firmware upgrade or backup web page, click **Management > Firmware > Upgrade/Backup**

This page allow user to upgrade or backup firmware image through HTTP or TFTP server.

Management >> Firmware >> Upgrade / Backup

The screenshot shows a web interface for firmware upgrade/backup. It has three main sections: 'Action' with radio buttons for 'Upgrade' (selected) and 'Backup'; 'Method' with radio buttons for 'TFTP' and 'HTTP' (selected); and 'Filename' with a file selection button '选择文件' and the text '未选择任何文件'. An 'Apply' button is at the bottom.

Upgrade Firmware through HTTP

Field	Description
Action	Firmware operations Upgrade: Upgrade firmware from remote host to DUT Backup: Backup firmware image from DUT to remote host
Method	Firmware upgrade / backup method TFTP: Using TFTP to upgrade/backup firmware HTTP: Using WEB browser to upgrade/backup firmware

Filename	Use browser to upgrade firmware, you should select firmware image file on your host PC.
----------	---

Upgrade Firmware through HTTP Fields

Management >> Firmware >> Upgrade / Backup

The screenshot shows a configuration window for firmware upgrade/backup. It is divided into three sections: Action, Method, and Filename. In the Action section, 'Upgrade' is selected with a radio button. In the Method section, 'HTTP' is selected with a radio button. In the Filename section, there is a button labeled '选择文件' (Select File) and the text '未选择任何文件' (No file selected). Below these sections is an 'Apply' button.

Upgrade Firmware through TFTP

Field	Description
Action	Firmware operations Upgrade: Upgrade firmware from remote host to DUT Backup: Backup firmware image from DUT to remote host
Method	Firmware upgrade / backup method TFTP: Using TFTP to upgrade/backup firmware HTTP: Using WEB browser to upgrade/backup firmware
Address Type	Specify TFTP server address type Hostname: Use domain name as server address IPv4: Use IPv4 as server address IPv6: Use IPv6 as server address
Server Address	Specify TFTP server address.
Filename	Firmware image file name on remote TFTP server

Upgrade Firmware through TFTP Fields

Management >> Firmware >> Upgrade / Backup

Action	☒ Upgrade ☐ Backup
Method	☐ TFTP ☒ HTTP
Filename	选择文件 未选择任何文件

Backup Firmware through HTTP

Field	Description
Action	Firmware operations Upgrade: Upgrade firmware from remote host to DUT Backup: Backup firmware image from DUT to remote host
Method	Firmware upgrade / backup method TFTP: Using TFTP to upgrade/backup firmware HTTP: Using WEB browser to upgrade/backup firmware
Firmware	Firmware partition need to backup Image0: Firmware image in flash partition 0 Image1: Firmware image in flash partition 1

Backup Firmware through HTTP Fields

Management >> Firmware >> Upgrade / Backup

Action	☒ Upgrade ☐ Backup
Method	☒ TFTP ☐ HTTP
Address Type	☒ Hostname ☐ IPv4 ☐ IPv6
Server Address	
Filename	

Backup Firmware through TFTP

Field	Description
Action	Firmware operations Upgrade: Upgrade firmware from remote host to DUT Backup: Backup firmware image from DUT to remote host
Method	Firmware upgrade / backup method TFTP: Using TFTP to upgrade/backup firmware HTTP: Using WEB browser to upgrade/backup firmware
Firmware	Firmware partition need to backup Image0: Firmware image in flash partition 0 Image1: Firmware image in flash partition 1
Address Type	Specify TFTP server address type Hostname: Use domain name as server address IPv4: Use IPv4 as server address IPv6: Use IPv6 as server address
Server Address	Specify TFTP server address.
Filename	File name saved on remote TFTP server

Backup Firmware through TFTP Fields

17.2.2. Active Image

To display the Active Image web page, click **Management > Firmware > Active Image**

This page allow user to select firmware image on next booting and show firmware information on both flash partitions

Management >> Firmware >> Active Image

Active Image

☐ Image0
☒ Image1

Note: the image was selected for the next boot

Active Image	
Firmware	Image1*
Version	1.0.0.7
Name	
Size	8478928 Bytes
Created	2024-07-19 14:39:05

Backup Image	
Firmware	Image0
Version	1.0.0.7
Name	
Size	8311581 Bytes
Created	2024-06-12 15:09:34

Apply

Active Image Page

Field	Description
Active Image	Select firmware image to use on next booting
Firmware	Firmware flash partition name
Version	Firmware version
Name	Firmware name
Size	Firmware image size
Created	Firmware image created date

Active Image Fields

17.3. Configuration

17.3.1. Upgrade / Backup

To display firmware upgrade or backup web page, click **Management > Configuration >**

Upgrade/Backup

This page allow user to upgrade or backup configuration file through HTTP or TFTP server.

Management >> Configuration >> Upgrade / Backup

Action	☒ Upgrade ☐ Backup
Method	☐ TFTP ☒ HTTP
Configuration	☒ Running Configuration ☐ Startup Configuration ☐ Backup Configuration ☐ RAM Log ☐ Flash Log
Filename	选择文件 未选择任何文件

Upgrade Configuration through HTTP

Field	Description
Action	Configuration operations Upgrade: Upgrade firmware from remote host to DUT Backup: Backup firmware image from DUT to remote host
Method	Configuration upgrade / backup method TFTP: Using TFTP to upgrade/backup firmware HTTP: Using WEB browser to upgrade/backup firmware
Configuration	Configuration types Running Configuration: Merge to current running configuration file Startup Configuration: Replace startup configuration file Backup Configuration: Replace backup configuration file
Filename	Use browser to upgrade configuration, should you select configuration file on your host PC.

Upgrade Configuration through HTTP Fields

Management >> Configuration >> Upgrade / Backup

Action	☒ Upgrade ☐ Backup
Method	☐ TFTP ☒ HTTP
Configuration	☒ Running Configuration ☐ Startup Configuration ☐ Backup Configuration ☐ RAM Log ☐ Flash Log
Filename	选择文件 未选择任何文件

Upgrade Configuration through TFTP

Field	Description
Action	Configuration operations Upgrade: Upgrade firmware from remote host to DUT Backup: Backup firmware image from DUT to remote host
Method	Configuration upgrade / backup method TFTP: Using TFTP to upgrade/backup firmware HTTP: Using WEB browser to upgrade/backup firmware
Configuration	Configuration types Running Configuration: Merge to current running configuration file Startup Configuration: Replace startup configuration file Backup Configuration: Replace backup configuration file
Address Type	Specify TFTP server address type Hostname: Use domain name as server address IPv4: Use IPv4 as server address IPv6: Use IPv6 as server address
Server Address	Specify TFTP server address.
Filename	Configuration file name on remote TFTP server

Upgrade Firmware through TFTP Fields

Management >> Configuration >> Upgrade / Backup

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

Apply

Backup Configuration through HTTP

Field	Description
Action	Configuration operations Upgrade: Upgrade configuration from remote host to DUT Backup: Backup configuration from DUT to remote host
Method	Configuration upgrade / backup method TFTP: Using TFTP to upgrade/backup configuration HTTP: Using WEB browser to upgrade/backup configuration
Configuration	Configuration types Running Configuration: Backup running configuration file Startup Configuration: Backup start configuration file Backup Configuration: Backup backup configuration file RAM Log: Backup log file stored in RAM Flash Log: Backup log files store in Flash

Backup Configuration through HTTP Fields

Management >> Configuration >> Upgrade / Backup

Action	☐ Upgrade ☒ Backup
Method	☒ TFTP ☐ HTTP
Configuration	☒ Running Configuration ☐ Startup Configuration ☐ Backup Configuration ☐ RAM Log ☐ Flash Log
Address Type	☒ Hostname ☐ IPv4 ☐ IPv6
Server Address	
Filename	

Backup Configuration through TFTP

Field	Description
Action	Firmware operations Upgrade: Upgrade firmware from remote host to DUT Backup: Backup firmware image from DUT to remote host
Method	Firmware upgrade / backup method TFTP: Using TFTP to upgrade/backup firmware HTTP: Using WEB browser to upgrade/backup firmware
Configuration	Configuration types Running Configuration: Backup running configuration file Startup Configuration: Backup start configuration file Backup Configuration: Backup backup configuration file RAM Log: Backup log file stored in RAM Flash Log: Backup log files store in Flash
Address Type	Specify TFTP server address type

	Hostname: Use domain name as server address IPv4: Use IPv4 as server address IPv6: Use IPv6 as server address
Server Address	Specify TFTP server address.
Filename	File name saved on remote TFTP server

Backup Firmware through TFTP Fields

17.3.2. Save Configuration

To display the Save Configuration web page, click **Management > Configuration > Save Configuration**. This page allow user to manage configuration file saved on DUT and click “Restore Factory Default” button to restore factory defaults.

Management >> Configuration >> Save Configuration

Source File	☒ Running Configuration ☐ Startup Configuration ☐ Backup Configuration
Destination File	☒ Startup Configuration ☐ Backup Configuration

Save Configuration Page

Field	Description
Source File	Source file types Running Configuration: Copy running configuration file to destination Startup Configuration: Copy startup configuration file to destination Backup Configuration: Copy backup configuration file to destination
Destination File	Destination file Startup Configuration: Save file as startup configuration Backup Configuration: Save file as backup configuration

Save Configuration Fields

17.4. SNMP

17.4.1. View

To configure and display the SNMP view table, click **Management > SNMP > View**.

Management >> SNMP >> View

View Table

Showing All entries Showing 1 to 1 of 1 entries

☐	View	OID Subtree	Type
☐	all	.1	Included

First Previous 1 Next Last

SNMP View Table Page

Field	Description
View	The SNMP view name. Its maximum length is 30 characters.
Subtree OID	Specify the ASN.1 subtree object identifier (OID) to be included or excluded from the SNMP view.
View Type	Include or exclude the selected MIBs in the view.

SNMP View Fields

17.4.2. Group

To configure and display the SNMP group settings, click **Management > SNMP > Group**.

Management >> SNMP >> Group

Group Table

Showing All entries Showing 0 to 0 of 0 entries

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

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

First Previous 1 Next Last

SNMP Group Table Page

Field	Description
Group	Specify SNMP group name, and the maximum length is 30 characters.

Version	Specify SNMP version SNMPv1: SNMP Version 1. SNMPv2: Community-based SNMP Version 2c. SNMPv3: User security model SNMP version 3.
Security Level	Specify SNMP security level No Security : Specify that no packet authentication is performed. Authentication: Specify that no packet authentication without encryption is performed. Authentication and Privacy: Specify that no packet authentication with encryption is performed.
View	
Read	Group read view name
Write	Group write view name.
Notify	The view name that sends only traps with contents that is included in SNMP View selected for notification.

SNMP Group Table Fields

Management >> SNMP >> Group

Add Group

Group

Version

☒ SNMPv1
☐ SNMPv2
☐ SNMPv3

Security Level

☒ No Security
☐ Authentication
☐ Authentication and Privacy

View

☒ Read

all ▼

☐ Write

all ▼

☐ Notify

all ▼

Apply

Close

SNMP Group Add Page

Field	Description
Group	Specify SNMP group name, and the maximum length is 30 characters.
Version	Specify SNMP version SNMPv1: SNMP Version 1. SNMPv2: Community-based SNMP Version 2c. SNMPv3: User security model SNMP version 3.
Security Level	Specify SNMP security level No Security : Specify that no packet authentication is performed. Authentication: Specify that no packet authentication without encryption is performed. Authentication and Privacy: Specify that no packet authentication with encryption is performed.
View	
Read	Select read view name if Read is checked
Write	Select write view name, if Write is checked
Notify	Select notify view name, if Notify is checked

SNMP Group Add Fields

Management >> SNMP >> Group

Add Group

Group

Version

☒ SNMPv1
☐ SNMPv2
☐ SNMPv3

Security Level

☒ No Security
☐ Authentication
☐ Authentication and Privacy

View

☒ Read

all ▼

☐ Write

all ▼

☐ Notify

all ▼

Apply

Close

SNMP Group Edit Page

Field	Description
Group	Display the edit group name
Version	Specify SNMP version SNMPv1: SNMP Version 1. SNMPv2: Community-based SNMP Version 2c. SNMPv3: User security model SNMP version 3.
Security Level	Specify SNMP security level No Security : Specify that no packet authentication is performed. Authentication: Specify that no packet authentication without encryption is performed. Authentication and Privacy: Specify that no packet authentication with encryption is performed.
View	
Read	Select read view name if Read is checked

Write	Select write view name, if Write is checked
Notify	Select notify view name, if Notify is checked

SNMP Group Edit Fields

17.4.3. Community

To configure and display the SNMP community settings, click **Management > SNMP > Community**.

Management >> SNMP >> Community

Community Table

Showing All entries Showing 1 to 1 of 1 entries

☐	Community	Group	View	Access
☐	public		all	Read-Only

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

SNMP Community Table Page

Field	Description
Community	The SNMP community name. Its maximum length is 20 characters.
Community Mode	SNMP Community mode Basic: snmp community specifies view and access right. Advanced: snmp community specifies group.
Group Name	Specify the SNMP group configured by the command snmp group to define the object available to the community.
View Name	Specify the SNMP view to define the object available to the community.
Access Right	SNMP access mode Read-Only: Read only. Read-Wrtie: Read and write.

SNMP Community Table Fields

Management >> SNMP >> Community

Add Community

The screenshot shows a 'Add Community' dialog box with the following fields and options:

- Community:** A text input field.
- Type:** Radio buttons for **Basic** (selected) and **Advanced**.
- View:** A dropdown menu currently showing 'all'.
- Access:** Radio buttons for **Read-Only** (selected) and **Read-Write**.
- Group:** A dropdown menu.
- Buttons:** 'Apply' and 'Close' buttons at the bottom.

SNMP Community Add Page

Field	Description
Community	The SNMP community name. Its maximum length is 20 characters.
Type	SNMP Community mode Basic: SNMP community specifies view and access right. Advanced: SNMP community specifies group.
View	Specify the SNMP view to define the object available to the community.
Access	SNMP access mode Read-Only: Read only. Read-Write: Read and write.
Group	Specify the SNMP group configured by user to define the object available to the community.

SNMP Community Add Fields

Management >> SNMP >> Community

Edit Community

Community	public
Type	☒ Basic ☐ Advanced
View	all ▼
Access	☒ Read-Only ☐ Read-Write
Group	▼

Apply Close

SNMP Community Edit Page

Field	Description
Community	The Edit SNMP community name
Type	SNMP Community mode Basic: SNMP community specifies view and access right. Advanced: SNMP community specifies group.
View	Specify the SNMP view to define the object available to the community.
Access	SNMP access mode Read-Only: Read only. Read-Write: Read and write.
Group	Specify the SNMP group configured by user to define the object available to the community.

SNMP Community Edit Fields

17.4.4. User

To configure and display the SNMP users, click **Management > SNMP > User**.

User Table

Showing **All** entries

Showing 0 to 0 of 0 entries



☐	User	Group	Security Level	Authentication Method	Privacy Method
--------------------------	------	-------	----------------	-----------------------	----------------

0 results found.

Configure **SNMP Group** to associate an SNMPv3 group with an SNMPv3 user.

First Previous 1 Next Last

Add

Edit

Delete

SNMP User Table Page

Field	Description
User	Specify the SNMP user name on the host that connects to the SNMP agent. The max character is 30 characters. For the SNMP v1 or v2c, the user name must match the community name
Group	Specify the SNMP group to which the SNMP user belongs.
Security Level	SNMP privilege mode No Security : Specify that no packet authentication is performed. Authentication: Specify that no packet authentication without encryption is performed. Authentication and Privacy: Specify that no packet authentication with encryption is performed.
Authentication Method	Authentication Protocol which is available when Privilege Mode is Authentication or Authentication and Privacy. None: No authentication required. MD5: Specify the HMAC-MD5-96 authentication protocol. SHA: Specify the HMAC-SHA-96 authentication protocol.
Privacy Method	Encryption Protocol None: No privacy required. DES: DES algorithm

SNMP User Table Fields

Management >> SNMP >> User

Add User

User

Group

111 ▼

Security Level

☒ No Security
☐ Authentication
☐ Authentication and Privacy

Authentication

Method

☒ None
☐ MD5
☐ SHA

Password

Privacy

Method

☐ None
☐ DES

Password

Apply

Close

SNMP User Add Page

Field	Description
User	Specify the SNMP user name on the host that connects to the SNMP agent. The max character is 30 characters.
Group	Specify the SNMP group to which the SNMP user belongs.
Security Level	SNMP privilege mode No Security : Specify that no packet authentication is performed. Authentication : Specify that no packet authentication without encryption is performed. Authentication and Privacy : Specify that no packet authentication with encryption is performed.
Authentication Method	Authentication Protocol which is available when Privilege Mode is Authentication or Authentication and Privacy.

	None: No authentication required. MD5: Specify the HMAC-MD5-96 authentication protocol. SHA: Specify the HMAC-SHA-96 authentication protocol.
Password	The authentication password, The number of character range is 8 to 32 characters.
Privacy Method	Encryption Protocol None: No privacy required. DES: DES algorithm
Password	The privacy password, The number of character range is 8 to 64 characters.

SNMP User Add Fields

Management >> SNMP >> User

Edit User

User

1111

Group

111 ▼

Security Level

☒ No Security
☐ Authentication
☐ Authentication and Privacy

Authentication

Method

☒ None
☐ MD5
☐ SHA

Password

Privacy

Method

☒ None
☐ DES

Password

Apply

Close

SNMP User Edit Page

Field	Description
User	Edit User name
Group	Specify the SNMP group to which the SNMP user belongs.

Security Level	SNMP privilege mode No Security : Specify that no packet authentication is performed.
Authentication Method	Authentication : Specify that no packet authentication without encryption is performed. Authentication and Privacy : Specify that no packet authentication with encryption is performed. Authentication Protocol which is available when Privilege Mode is Authentication or Authentication and Privacy. None : No authentication required. MD5 : Specify the HMAC-MD5-96 authentication protocol. SHA : Specify the HMAC-SHA-96 authentication protocol.
Password	The authentication password, The number of character range is 8 to 32 characters.
Privacy Method	Encryption Protocol None : No privacy required. DES : DES algorithm
Password	The privacy password, The number of character range is 8 to 64 characters.

SNMP User Edit Fields

17.4.5. Engine ID

To configure and display SNMP local and remote engine ID, click **Management > SNMP > Engine ID**.

Management >> SNMP >> Engine ID

Local Engine ID

☐ User Defined

Engine ID

80006a9203822402190001 (10 - 64 Hexadecimal Characters)

Apply

Remote Engine ID Table

Showing [All] entries

Showing 0 to 0 of 0 entries



☐	Server Address	Engine ID
0 results found.		
Add	Edit	Delete

First Previous 1 Next Last

SNMP Engine ID Page

Field	Description
Local Engine ID	
Engine ID	If checked "User Defined", the local engine ID is configure by user, else use the default Engine ID which is made up of MAC and Enterprise ID. The user defined engine ID is range 10 to 64 hexadecimal characters, and the hexadecimal number must be divided by 2.
Remote Engine ID Table	
Server Address	Remote host
Engine ID	Specify Remote SNMP engine ID. The engine ID is range10 to 64 hexadecimal characters, and the hexadecimal number must be divided by 2.

SNMP Engine ID Fields

Management >> SNMP >> Engine ID

Add Remote Engine ID

Address Type

☒ Hostname
☐ IPv4
☐ IPv6

Server Address

Engine ID

 (10 - 64 Hexadecimal Characters)

SNMP Remote Engine ID Add Page

Field	Description
Address Type	Remote host address type for Hostname/IPv4/IPv6
Server Address	Remote host
Engine ID	Specify Remote SNMP engine ID. The engine ID is range10 to 64 hexadecimal characters, and the hexadecimal number must be divided by 2.

SNMP Remote Engine ID Add Fields

[Management](#) >> [SNMP](#) >> [Engine ID](#)

Edit Remote Engine ID

Server Address	192.168.0.111
Engine ID	80006a9203822402190001 (10 - 64 Hexadecimal Characters)

Apply

Close

SNMP Remote Engine ID Edit Page

Field	Description
Server Address	Edit Remote host address
Engine ID	Specify Remote SNMP engine ID. The engine ID is range 10 to 64 hexadecimal characters, and the hexadecimal number must be divided by 2.

SNMP Remote Engine ID Edit Fields

17.4.6. Trap Event

To configure and display SNMP trap event, click **Management > SNMP > Trap Event**.

[Management](#) >> [SNMP](#) >> [Trap Event](#)

Authentication Failure	☒ Enable
Link Up / Down	☒ Enable
Cold Start	☒ Enable
Warm Start	☒ Enable

Apply

SNMP Trap Event Page

Field	Description
-------	-------------

Authentication Failure	SNMP authentication failure trap, when community not match or user authentication password not match.
Link Up/Down	Port link up or down trap
Cold Start	Device reboot configure by user trap
Warm Start	Device reboot by power down trap

SNMP Trap Event Fields

17.4.7. Notification

To configure the hosts to receive SNMPv1/v2/v3 notification, click **Management > SNMP > Notification**.

Management >> SNMP >> Notification

Notification Table

Showing All 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

SNMP Notification Table Page

Field	Description
Server Address	IP address or the hostname of the SNMP trap recipients.
Server Port	Recipients server UDP port number
Timeout	Specify the SNMP informs timeout
Retry	Specify the retry counter of the SNMP informs.
Version	Specify SNMP notification version SNMPv1: SNMP Version 1 notification. SNMPv2: SNMP Version 2 notification. SNMPv3: SNMP Version 3 notification.
Type	Notification Type Trap: Send SNMP traps to the host. Inform: Send SNMP informs to the host.
Community/User	SNMP community/user name for notification. If version is SNMPv3 the name is user name, else is community name

UDP Port	Specify the UDP port number.
Timeout	Specify the SNMP informs timeout
Security Level	SNMP trap packet security level No Security: Specify that no packet authentication is performed. Authentication: Specify that no packet authentication without encryption is performed. Authentication and Privacy: Specify that no packet authentication with encryption is performed.

SNMP Notification Table Fields

Management >> SNMP >> Notification

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)

SNMP Notification Add Page

Field	Description
Address Type	Notify recipients host address type

Server Address	IP address or the hostname of the SNMP trap recipients.
Version	Specify SNMP notification version SNMPv1: SNMP Version 1 notification. SNMPv2: SNMP Version 2 notification. SNMPv3: SNMP Version 3 notification.
Type	Notification Type Trap: Send SNMP traps to the host. Inform: Send SNMP informs to the host.(version 1 have no inform)
Community/User	SNMP community/user name for notification. If version is SNMPv3 the name is user name, else is community name
Security Level	SNMP notification packet security level, the security level must less than or equal to the community/user name No Security: Specify that no packet authentication is performed. Authentication: Specify that no packet authentication without encryption is performed. Authentication and Privacy: Specify that no packet authentication with encryption is performed.
Server Port	Recipients server UDP port number, if “use default” checked the value is 162, else user configure
Timeout	Specify the SNMP informs timeout, if “use default” checked the value is 15, else user configure
Retry	Specify the SNMP informs retry count, if “use default” checked the value is 3, else user configure

SNMP Notification Add Fields

Management >> SNMP >> Notification

Edit Notification

Server Address	192.168.0.111	
Version	☐ SNMPv1 ☐ SNMPv2 ☒ SNMPv3	
Type	☒ Trap ☐ Inform	
Community / User	1111 ▼	
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)

SNMP Notification Edit Page

Field	Description
Server Address	Edit SNMP notify recipients address.
Version	Specify SNMP notification version SNMPv1: SNMP Version 1 notification. SNMPv2: SNMP Version 2 notification. SNMPv3: SNMP Version 3 notification.
Type	Notification Type Trap: Send SNMP traps to the host. Inform: Send SNMP informs to the host.(version 1 have no inform)
Community/User	SNMP community/user name for notification. If version is SNMPv3 the name is user name, else is community name

Security Level	SNMP notification packet security level, the security level must less than or equal to the community/user name No Security: Specify that no packet authentication is performed. Authentication: Specify that no packet authentication without encryption is performed. Authentication and Privacy: Specify that no packet authentication with encryption is performed.
Server Port	Recipients server UDP port number, if “use default” checked the value is 162, else user configure
Timeout	Specify the SNMP informs timeout, if “use default” checked the value is 15, else user configure
Retry	Specify the SNMP informs retry count, if “use default” checked the value is 3, else user configure

SNMP Notification Edit Fields

17.4.8. Configuration Case

Case requirement: The SNMP network management server IP address is 2.2.2.2, and the read and write communication group characters are unified as public.

- WEB
 1. Enable SNMP globally

Security >> Management Access >> Management Service

The screenshot shows a web interface for configuring management services. It has a title bar 'Management Service' and a list of services with checkboxes: Telnet (unchecked), SSH (unchecked), HTTP (checked), HTTPS (unchecked), and SNMP (checked). The SNMP row is highlighted with a red rectangular box.

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

2. Configure read-write groups

Management >> SNMP >> Community

Community Table

Showing **All** entries

Showing 1 to 1 of 1 entries

☐	Community	Group	View	Access
☐	public		all	Read-Write

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

Add

Edit

Delete

● CLI

Enter global configuration mode to configure

```
no snmp community "public"
snmp community "public" rw
snmp
```

17.5. RMON

17.5.1. Statistics

To display RMON Statistics, click **Management > RMON > Statistics**.

Management >> RMON >> 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
☐	1	GE1	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
☐	3	GE3	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
☐	5	GE5	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

RMON Statistics page.

Field	Description
Port	The port for the RMON statistics.
Bytes Received	Number of octets received, including bad packets and FCS octets, but excluding framing bits.
Drop Events	Number of packets that were dropped.

Packets Received	Number of packets received, including bad packets, Multicast packets, and Broadcast packets.
Broadcast Packets	Number of good Broadcast packets received. This number does not include Multicast packets.
Multicast Packets	Number of good Multicast packets received.
CRC & Align Errors	Number of CRC and Align errors that have occurred.
Undersized Packages	Number of undersized packets (less than 64 octets) received.
Oversize Packages	Number of oversized packets (over 1518 octets) received.
Fragments	Number of fragments (packets with less than 64 octets, excluding framing bits, but including FCS octets) received.
Jabbers	Number of received packets that were longer than 1632 octets. This number excludes frame bits, but includes FCS octets that had either a bad FCS (Frame Check Sequence) with an integral number of octets (FCS Error) or a bad FCS with a non-integral octet (Alignment Error) number. A Jabber packet is defined as an Ethernet frame that satisfies the following criteria: Packet data length is greater than MRU. Packet has an invalid CRC. RX error event has not been detected.
Collision	Number of collisions received. If Jumbo Frames are enabled, the threshold of Jabber Frames is raised to the maximum size of Jumbo Frames.
Frames of 64 Bytes	Number of frames, containing 64 bytes that were received.
Frames of 65 to 127 Bytes	Number of frames, containing 65 to 127 bytes that were received.
Frames of 128 to 255 Bytes	Number of frames, containing 128 to 255 bytes that were received.
Frames of 256 to 511 Bytes	Number of frames, containing 256 to 511 bytes that were received.
Frames of 512 to 1024 Bytes	Number of frames, containing 512 to 1023 bytes that were received.

Frames Greater than 1024 Bytes	Number of frames, containing 1024 to 1518 bytes that were received.
Clear	Clear the statistics for the selected ports
View	View the statistics on the specified port.

RMON Statistics fields.

Management >> RMON >> Statistics

View Port Statistics

Port	GE1
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

View RMON Statistics page.

17.5.2. History

For the RMON history, click **Management > RMON > History**.

Management >> RMON >> History

History Table

Showing All entries

Showing 0 to 0 of 0 entries

☐	Entry	Port	Interval	Owner	Sample		
					Maximum	Current	
0 results found.							

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

Add

Edit

Delete

View

RMON History page.

Field	Description
Port	The port for the RMON history.
Interval	The number of seconds for each sample.
Owner	The owner name of event (0~31 characters).
Sample Maximum	The maximum number of buckets.
Sample Current	The current number of buckets.

RMON History fields.

Field	Description
Add	Add the new RMON history entries
Edit	Edit the RMON history
Delete	Delete the RMON histories.
View	View the history log.

RMON History buttons.

Management >> RMON >> History

Add History

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

RMON History Add page.

Field	Description
Port	Specify port for the RMON history.
Max Sample	Specify the maximum number of buckets.
Interval	Specify the number of seconds for each sample.
Owner	Specify the owner name of event (0~31 characters).

RMON History Add fields.

Management >> RMON >> History

Edit History

Entry	1	
Port	GE1 ▼	
Max Sample	50	(1 - 50, default 50)
Interval	1800	(1 - 3600, default 1800)
Owner	111	

RMON History Edit page

Field	Description
-------	-------------

Port	Specify port for the RMON history.
Max Sample	Specify the maximum number of buckets.
Interval	Specify the number of seconds for each sample.
Owner	Specify the owner name of event (0~31 characters).

RMON History Edit fields.

Management >> RMON >> History

View History

Entry: 1

Showing All entries

Showing 0 to 0 of 0 entries

Q

Sample No.	Drop Events	Bytes Received	Packets Received	Broadcast Packets	Multicast Packets	CRC & Align Errors	Undersize Packets	Oversize Packets	Fragments	Jabbers	Collisions	Utilization	
0 results found.													
Close First Previous 1 Next Last													

RMON History Log page.

Field	Description
Port	The port for the RMON statistics.
Bytes Received	Number of octets received, including bad packets and FCS octets, but excluding framing bits.
Drop Events	Number of packets that were dropped.
Packets Received	Number of packets received, including bad packets, Multicast packets, and Broadcast packets.
Broadcast Packets	Number of good Broadcast packets received. This number does not include Multicast packets.
Multicast Packets	Number of good Multicast packets received.
CRC & Align Errors	Number of CRC and Align errors that have occurred.
Undersize Packages	Number of undersized packets (less than 64 octets) received.
Oversize Packages	Number of oversized packets (over 1518 octets) received.

Fragments	Number of fragments (packets with less than 64 octets, excluding framing bits, but including FCS octets) received.
Jabbers	Number of received packets that were longer than 1632 octets. This number excludes frame bits, but includes FCS octets that had either a bad FCS (Frame Check Sequence) with an integral number of octets (FCS Error) or a bad FCS with a non-integral octet (Alignment Error) number. A Jabber packet is defined as an Ethernet frame that satisfies the following criteria: Packet data length is greater than MRU. Packet has an invalid CRC. RX error event has not been detected.
Collision	Number of collisions received. If Jumbo Frames are enabled, the threshold of Jabber Frames is raised to the maximum size of Jumbo Frames.
Utilization	Percentage of current interface traffic compared to the maximum traffic that the interface can handle.

RMON History Log fields.

17.5.3. Event

For the RMON event, click **Management > RMON > Event**.

Management >> RMON >> Event

Event Table

Showing **All** 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.

First Previous 1 Next Last

Add

Edit

Delete

View

RMON Event page.

Field	Description
Community	The SNMP community when the notification type is specified as trap.
Description	The description for the event.

Notification	The notification type for the event, and the possible value are: None: Nothing for notification. Event Log: Logging the event in the RMON Event Log table. Trap: Send a SNMP trap. Event Log and Trap: Logging the event and send the SNMP trap.
Time	The time that the event was triggered.
Owner	The owner for the event.

RMON Event fields.

Management >> RMON >> Event

Add Event

Entry

1

Notification

☒ None
☐ Event Log
☐ Trap
☐ Event Log and Trap

Community

Default Community

Description

Default Description

Owner

Apply

Close

RMON Event Add page.

Field	Description
Community	Specify the SNMP community when the notification type is specified as "Trap" or "Event Log and Trap".
Description	Specify the description for the event.

Notification	Specify the notification type for the event, and the possible value are: None: Nothing for notification. Event Log: Logging the event in the RMON Event Log table. Trap: Send a SNMP trap. Event Log and Trap: Logging the event and send the SNMP trap.
Owner	Specify owner for the event.

RMON Event Add fields.

Management >> RMON >> Event

Edit Event

Entry

1

Notification

☒ None
☐ Event Log
☐ Trap
☐ Event Log and Trap

Community

Description

Default Description

Owner

111

Apply

Close

RMON Event Edit page.

Field	Description
Community	Specify the SNMP community when the notification type is specified as “Trap” or “Event Log and Trap”.
Description	Specify the description for the event.
Notification	Specify the notification type for the event, and the possible value are: None: Nothing for notification. Event Log: Logging the event in the RMON Event Log table.

	Trap: Send a SNMP trap. Event Log and Trap: Logging the event and send the SNMP trap.
Owner	Specify owner for the event.

RMON Event Edit fields.

Management >> RMON >> Event

View Event Log

Entry:1

Showing

All

 entries

Showing 0 to 0 of 0 entries

Q

Log ID	Time	Description
0 results found.		

Close

FirstPrevious1NextLast

RMON Event Log page.

Field	Description
Log ID	The log identifier.
Time	The time that the event was triggered.
Description	The description for the event.

RMON Event Log fields.

17.5.4. Alarm

For the RMON Alarm, click **Management > RMON > Alarm**.

Management >> RMON >> Alarm

Alarm Table

Showing

All

 entries

Showing 0 to 0 of 0 entries

Q

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

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

AddEditDelete

FirstPrevious1NextLast

RMON Alarm page.

Managed Switch software

2

www.ewindnet.com

Field	Description
Port	The port configuration for the RMON alarm.
Counter	The counter for sampling DropEvents (Drop Event): Total number of events received in which the packets were dropped. Octes (Received Bytes): Octets. Pkts (Received Packets): Number of packets. BroadcastPkts (Broadcast Packets Received): Broadcast packets. MulticastPkts (Multicast Packets Received): Multicast packets. CRCAAlignError (CRC and Align Error): CRC alignment error. UndersizePkts (Undersize Packets): Number of undersized packets. OversizePkts (Oversize Packets): Number of oversized packets. Fragments (Fragments): Total number of packet fragment. Jabbers (Jabbers): Total number of packet jabber. Collisions (Collisions): Collision. Pkts64Octetes (Frames of 64 Bytes): Number of packets size 64 octets. Pkts65to127Octetes (Frames of 65 to 127 Bytes): Number of packets size 65 to 127 octets. Pkts128to255Octetes (Frames of 128 to 255 Bytes): Number of packets size 128 to 255 octets. Pkts256to511Octetes (Frames of 256 to 511 Bytes): Number of packets size 256 to 511 octets. Pkts512to1023Octetes (Frames of 512 to 1023 Bytes): Number of packets size 512 to 1023 octets. Pkts1024to1518Octetes (Frames Greater than 1024 Bytes): Number of packets size 1024 to 1518 octets.
Sampling	The sampling type including: Absolute: The selected variable value is compared directly with the

	thresholds at the end of the sampling interval. Delta: The selected variable value of the last sample is subtracted from the current value and the difference is compared with the thresholds.
Interval	The number of seconds for each sample.
Owner	The owner for the alarm entry.
Trigger	The type of event triggering.
Rising Threshold	The threshold for firing rising event.
Rising Event	The rising event when alarm was fired.
Falling Threshold	The threshold for firing falling event.
Falling Event	The falling event when alarm was fired.

RMON Alarm fields.**Management >> RMON >> Alarm****Add Alarm**

Entry	2
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 ▼

RMON Alarm Add page.

Field	Description
Port	Specify the port for sampling
Counter	Specify the counter for sampling Drop Event: Total number of events received in which the packets were dropped. Received Bytes (Octets): Octets. Received Packets: Number of packets. Broadcast Packets Received: Broadcast packets. Multicast Packets Received: Multicast packets. CRC and Align Error: CRC alignment error. Undersize Packets: Number of undersized packets. Oversize Packets: Number of oversized packets. Fragments: Total number of packet fragment. Jabbers: Total number of packet jabber. Collisions: Collision. Frames of 64 Bytes: Number of packets size 64 octets. Frames of 65 to 127 Bytes: Number of packets size 65 to 127 octets. Frames of 128 to 255 Bytes: Number of packets size 128 to 255 octets. Frames of 256 to 511 Bytes: Number of packets size 256 to 511 octets. Frames of 512 to 1023 Bytes: Number of packets size 512 to 1023 octets. Frames Greater than 1024 Bytes: Number of packets size 1024 to 1518 octets.
Sampling	Specify the sampling type. Absolute: The selected variable value is compared directly with the thresholds at the end of the sampling interval. Delta: The selected variable value of the last sample is subtracted from the current value and the difference is compared with the thresholds.
Interval	Specify the sampling interval.
Owner	Specify the owner for the sampling.
Trigger	Specify the type for the alarm trigger.

Rising Threshold	Specify the threshold for firing rising event.
Rising Event	Specify the index of rising event when alarm was fired.
Falling Threshold	Specify the threshold for firing falling event.
Falling Event	Specify the index of falling event when alarm was fired.

RMON Alarm Add fields.

Management >> RMON >> Alarm

Edit Alarm

Entry

1

Port

GE1 ▾

Counter

Drop Events ▾

Sampling

☒ Absolute
☐ Delta

Interval

Sec (1 - 2147483647, default 100)

Owner

Trigger

☒ Rising
☐ Falling
☐ Rising and Falling

Rising

Threshold

(0 - 2147483647, default 100)

Event

1 - Default Description ▾

Falling

Threshold

(0 - 2147483647, default 20)

Event

1 - Default Description ▾

Apply

Close

RMON Alarm Edit page.

Field	Description
Port	Specify the port for sampling
Counter	Specify the counter for sampling Drop Event: Total number of events received in which the packets were dropped. Received Bytes (Octets): Octets.

	Received Packets: Number of packets. Broadcast Packets Received: Broadcast packets. Multicast Packets Received: Multicast packets. CRC and Align Error: CRC alignment error. Undersize Packets: Number of undersized packets. Oversize Packets: Number of oversized packets. Fragments: Total number of packet fragment. Jabbers: Total number of packet jabber. Collisions: Collision. Frames of 64 Bytes: Number of packets size 64 octets. Frames of 65 to 127 Bytes: Number of packets size 65 to 127 octets. Frames of 128 to 255 Bytes: Number of packets size 128 to 255 octets. Frames of 256 to 511 Bytes: Number of packets size 256 to 511 octets. Frames of 512 to 1023 Bytes: Number of packets size 512 to 1023 octets. Frames Greater than 1024 Bytes: Number of packets size 1024 to 1518 octets.
Sampling	Specify the sampling type. Absolute: The selected variable value is compared directly with the thresholds at the end of the sampling interval. Delta: The selected variable value of the last sample is subtracted from the current value and the difference is compared with the thresholds.
Interval	Specify the sampling interval.
Owner	Specify the owner for the sampling.
Trigger	Specify the type for the alarm trigger.
Rising Threshold	Specify the threshold for firing rising event.
Rising Event	Specify the index of rising event when alarm was fired.
Falling Threshold	Specify the threshold for firing falling event.

Falling Event

Specify the index of falling event when alarm was fired.

RMON Alarm Edit fields.**17.5.5. Configuration Case****Case requirements**

The IP address of the SNMP network management server is 2.2.2.2, and the read and write communication group characters are unified as public. The network management server needs to query the traffic of device port 1 through RMON. The network management server needs to monitor the input traffic of device port 1 through RMON, with a cycle of 10 seconds. Once the number of input bytes changes by more than 1MB (1000000B), an alarm will be triggered and a log will be recorded

Configuration steps

- WEB

1. Enable SNMP globally

Security >> Management Access >> Management Service

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

2. Configure read-write groups

Management >> SNMP >> Community**Community Table**

Showing All entries

Showing 1 to 1 of 1 entries

☐	Community	Group	View	Access
☐	public		all	Read-Write

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

Add

Edit

Delete

3. Configure RMON event

Management >> RMON >> Event

Event Table

Showing All entries

Showing 1 to 1 of 1 entries

☐	Entry	Community	Description	Notification	Time	Owner
☐	1	public	abc	Event Log and Trap	(0) 0:00:00.00	abc

Add

Edit

Delete

View

4. Configure RMON alarm

Management >> RMON >> Alarm

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	abc	Rising and Falling	10000	abc	1000	abc

First

Previous

1

Next

Last

Add

Edit

Delete

● CLI

Enter global configuration mode to configure

```

no snmp community "public"
snmp community "public" rw
snmp
rmon event 1 log trap "public" description "abc" owner "abc"
rmon alarm 1 interface gil drop-events 100 absolute rising 10000 1 falling 1000 1 startup rising-
falling owner "abc"

```