

Ethernet Switch Web Manual

USING THIS DOCUMENT

This document is intended for the software engineer's general information on the usage of switch source files for the chip development of the switch team.

Though every effort has been made to ensure that this document is current and accurate, more information may have become available subsequent to the production of this guide.

Table of Contents

Contents

Ethernet Switch Web Manual	Error! Bookmark not defined.
USING THIS DOCUMENT	1
1. Introduction	5
2. Status	6
2.1. System Information	6
2.2. Logging Message	8
2.3. Port	10
2.4. Link Aggregation	17
2.5. MAC Address Table	18
3. Network	21
3.1. System Time	22
4. Port	26
4.1. Port Setting	26
4.2. Error Disabled	25
4.3. Link Aggregation	28
4.4. EEE	37
4.5. Jumbo Frame	40
4.6. Port Security	41
4.7. Protected Port	42
4.8. Storm Control	43
5. VLAN	44
5.1. VLAN	36
5.2. Voice VLAN	45
5.3. Protocol VLAN	48
5.4. MAC VLAN	52
5.5. Surveillance VLAN	57
5.6. GVRP	64
6. MAC Address Table	70
6.1. Dynamic Address	70
6.2. Static Address	72
6.3. Filtering Address	72
7. STP	74
7.1. Property	74
7.2. Port Setting	67
7.3. MST Instance	70
7.4. MST Port Setting	72
7.5. Statistics	75
8. Discovery	77
8.1. LLDP	77
9. Multicast	96
9.1. General	97

9.2.	IGMP Snooping	113
9.3.	MLD Snooping	120
9.4.	MVR	126
17	Routing	132
17.1	IPv4 Management and Interfaces	132
17.1.1	IPv4 Interface	132
17.1.2	IPv4 Routing	133
17.1.3	ARP	134
17.2	Ipv6 Management and Interfaces	135
17.2.1	Ipv6 Interfaces	135
17.2.2	Ipv6 address	136
17.2.3	Ipv6 routes	137
17.2.4	IPv6 Neighbor	138
17.3	Rip Routes Management	139
17.4	Ospf Routes Management	140
17.5	VRRP management	141
10	Security	142
10.1.	RADIUS	142
10.2.	TACACS+	146
10.3.	AAA	150
10.4.	Management Access	143
10.4.1.	Management VLAN	143
10.4.2.	Management Service	143
10.4.3.	Management ACL	145
10.4.4.	Management ACE	147
10.5.	Authentication Manager	150
10.6.	DoS	165
10.10.	Dynamic ARP Inspection	173
10.11.	DHCP Snooping	178
10.12.	IP Source Guard	183
11	ACL	189
11.1.	MAC ACL	191
11.2.	MAC ACE	191
11.3.	IPv4 ACL	190
11.4.	IPv4 ACE	192
11.5.	IPv6 ACL	198
11.6.	IPv6 ACE	200
11.7.	ACL Binding	206
12	QoS	210
12.1.	General	210
12.2.	Rate Limit	213
13	Diagnostics	218
13.1.	Logging	218
13.2.	Mirroring	222
13.3.	Ping	222
13.4.	Traceroute	223
13.5.	Copper Test	224
13.6.	Fiber Module	225
13.7.	UDLD	226
14	Management	22
14.1.	User Account	22

14.2.	Firmware	231
14.3.	Configuration	235
14.4.	SNMP	241
14.5.	RMON	259
15	ERPS	276
15.1	Property	277
15.2	ERPS instance	277
16	DHCP	278
16.1	Property	278
16.2	IP pool setting	279
16.3	VLAN IF Address Group Setting	280
16.4	Client List	281
16.5	Client Static Binding Table	281
18	Network	282
18.1	DNS	282
18.2	Hosts	284
19	POE	285
19.1	POE port setting	285
19.2	POE Port Timing Settings	286

1. 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.

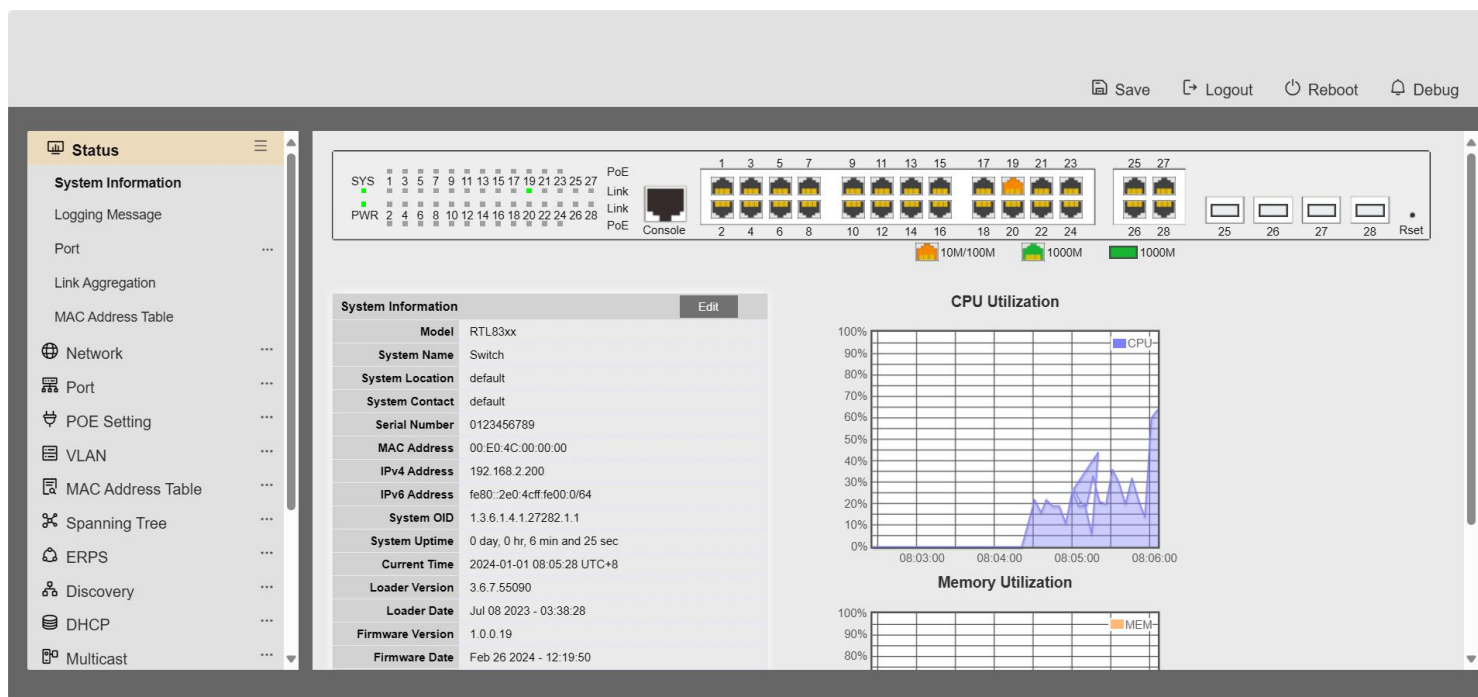


Figure 1-1 Web User Interface

2. Status

Use the Status pages to view system information and status.

2.1. 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.

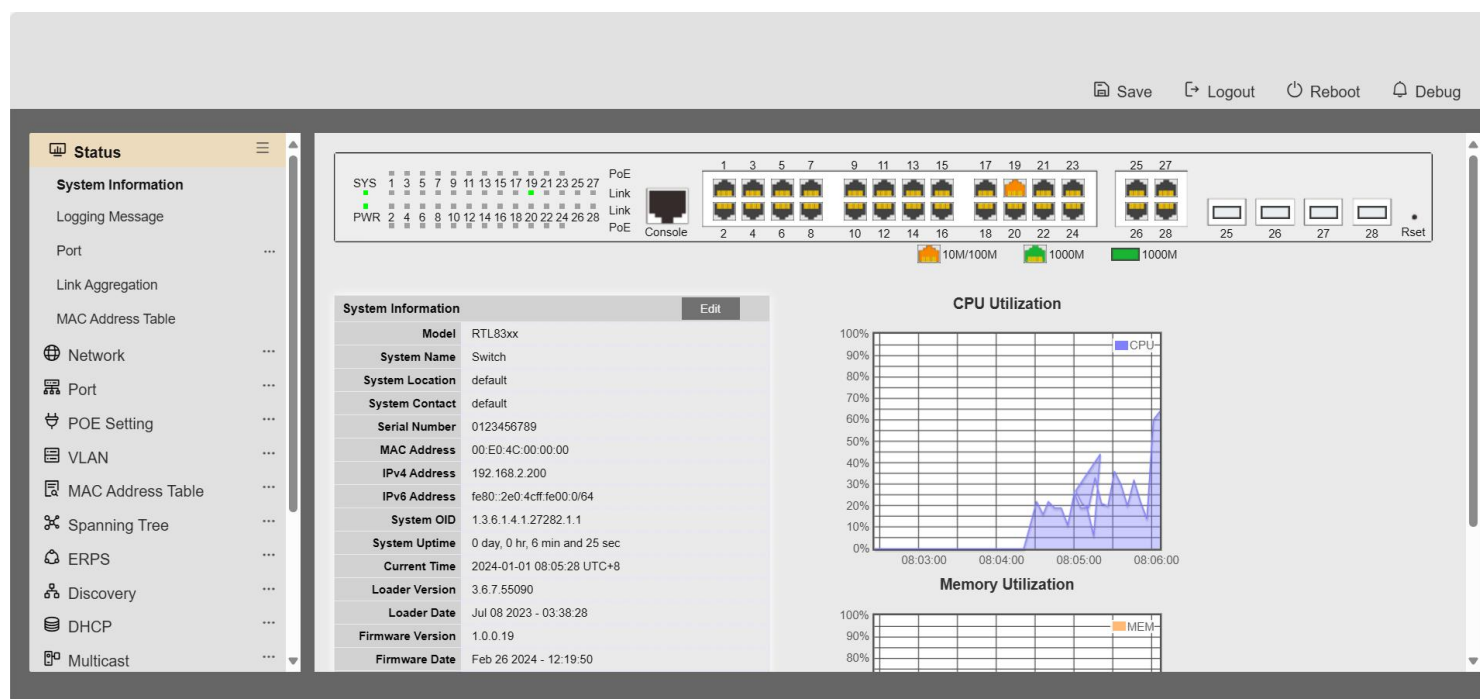


Figure 2-1 System Information Page

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

Table 2-1 Current System Information

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

Edit System Information

System Name

Switch

System Location

Default

System Contact

Default

Apply

Close

Figure 2-2 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

Table 2-2 System Information Fields

2.2. Logging Message

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

Web User Interface

Status

System Information

Logging Message

Port

Link Aggregation

MAC Address Table

Network

Port

VLAN

MAC Address Table

Spanning Tree

ERPS

Discovery

DHCP

Multicast

Routing

Security

ACL

Save Logout Reboot Debug

Logging Message Table

Viewing RAM

Showing All entries

Showing 1 to 8 of 8 entries

Log ID	Time	Severity	Description
1	Jan 01 2022 10:04:43	notice	AAA-0-CONNECT: New http connection for user admin, source 192.168.2.50 ACCEPTED
2	Jan 01 2022 10:04:21	notice	AAA-5-CONNECT: New http connection for user admin, source 192.168.2.50 ACCEPTED
3	Jan 01 2022 08:11:49	notice	AAA-5-DISCONNECT: console connection for user admin, source async TERMINATED
4	Jan 01 2022 08:01:01	notice	AAA-5-CONNECT: New http connection for user admin, source 192.168.2.50 ACCEPTED
5	Jan 01 2022 08:00:27	notice	AAA-5-CONNECT: New console connection for user admin, source async ACCEPTED
6	Jan 01 2022 08:00:08	notice	PORT-5-LINK_UP: Interface VLAN1 link up
7	Jan 01 2022 08:00:08	notice	PORT-5-LINK_UP: Interface GigabitEthernet1 link up
8	Jan 01 2022 00:00:08	notice	SYSTEM-5-COLDSTART: Cold startup

Clear Refresh

First Previous 1 Next Last

Figure 2-3: 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.

Table 2-3: Logging Message fields.

Field	Description
Viewing	The logging view including: <ul style="list-style-type: none">• 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.

Table 2-4: Logging Message buttons.

2.3. Port

The Port configuration page displays port summary and status information.

2.3.1. 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.

Port

GE1

MIB Counter

All

Interface

Etherlike

RMON

Refresh Rate

None

5 sec

10 sec

30 sec

Clear

Save Logout Reboot

Status

System Information

Logging Message

Port

Statistics

Error Disabled

Bandwidth Utilization

Link Aggregation

MAC Address Table

Network

Port

VLAN

MAC Address Table

Spanning Tree

ERPS

Discovery

DHCP

Multicast

Interface

ifInOctets	629
ifInUcastPkts	5
ifInNUcastPkts	0
ifInDiscards	0
ifOutOctets	497
ifOutUcastPkts	5
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

Web User Interface

Save

Logout

Reboot

Debug

Status

System Information

Logging Message

Port

Statistics

Error Disabled

Bandwidth Utilization

Link Aggregation

MAC Address Table

Network

Port

VLAN

MAC Address Table

Spanning Tree

ERPS

Discovery

DHCP

Multicast

dot3StatsExcessiveCollisions

0

dot3StatsFrameTooLongs

0

dot3StatsSymbolErrors

0

dot3ControlInUnknownOpCodes

0

dot3InPauseFrames

0

dot3OutPauseFrames

0

RMON

etherStatsDropEvents

0

etherStatsOctets

6154

etherStatsPkts

39

etherStatsBroadcastPkts

0

etherStatsMulticastPkts

5

etherStatsCRCAlignErrors

0

etherStatsUnderSizePkts

0

etherStatsOverSizePkts

0

etherStatsFragments

0

etherStatsJabbers

0

etherStatsCollisions

0

etherStatsPkts64Octets

22

etherStatsPkts65to127Octets

7

etherStatsPkts128to255Octets

4

etherStatsPkts256to511Octets

0

etherStatsPkts512to1023Octets

6

etherStatsPkts1024to1518Octets

0

Figure 2-4 Port Counters Page

Field	Description
Port	Select one port to show counter statistics.
MIB Counter	Select the MIB counter to show different counter type <ul style="list-style-type: none"> • 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

Table 2-5 Port Counters Fields

2.3.2. Error Disabled

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

<input type="checkbox"/>	Port	Reason	Time Left (sec)
<input type="checkbox"/>	GE1	---	---
<input type="checkbox"/>	GE2	---	---
<input type="checkbox"/>	GE3	---	---
<input type="checkbox"/>	GE4	---	---
<input type="checkbox"/>	GE5	---	---
<input type="checkbox"/>	GE6	---	---
<input type="checkbox"/>	GE7	---	---
<input type="checkbox"/>	GE8	---	---
<input type="checkbox"/>	GE9	---	---
<input type="checkbox"/>	GE10	---	---
<input type="checkbox"/>	GE11	---	---
<input type="checkbox"/>	GE12	---	---
<input type="checkbox"/>	GE13	---	---
<input type="checkbox"/>	GE14	---	---
<input type="checkbox"/>	GE15	---	---
<input type="checkbox"/>	GE16	---	---
<input type="checkbox"/>	GE17	---	---
<input type="checkbox"/>	GE18	---	---
<input type="checkbox"/>	GE19	---	---
<input type="checkbox"/>	GE20	---	---
<input type="checkbox"/>	GE21	---	---
<input type="checkbox"/>	GE22	---	---
<input type="checkbox"/>	GE23	---	---
<input type="checkbox"/>	GE24	---	---
<input type="checkbox"/>	TE1	---	---
<input type="checkbox"/>	TE2	---	---
<input type="checkbox"/>	TE3	---	---
<input type="checkbox"/>	TE4	---	---

Figure 2-5: Error Disabled Status page.

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

Port	Interface or port number.
Reason	Port will be disabled by one of the following error reason: <ul style="list-style-type: none">• 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.

Table 2-6: Error Disabled Status fields.

2.3.3. 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.

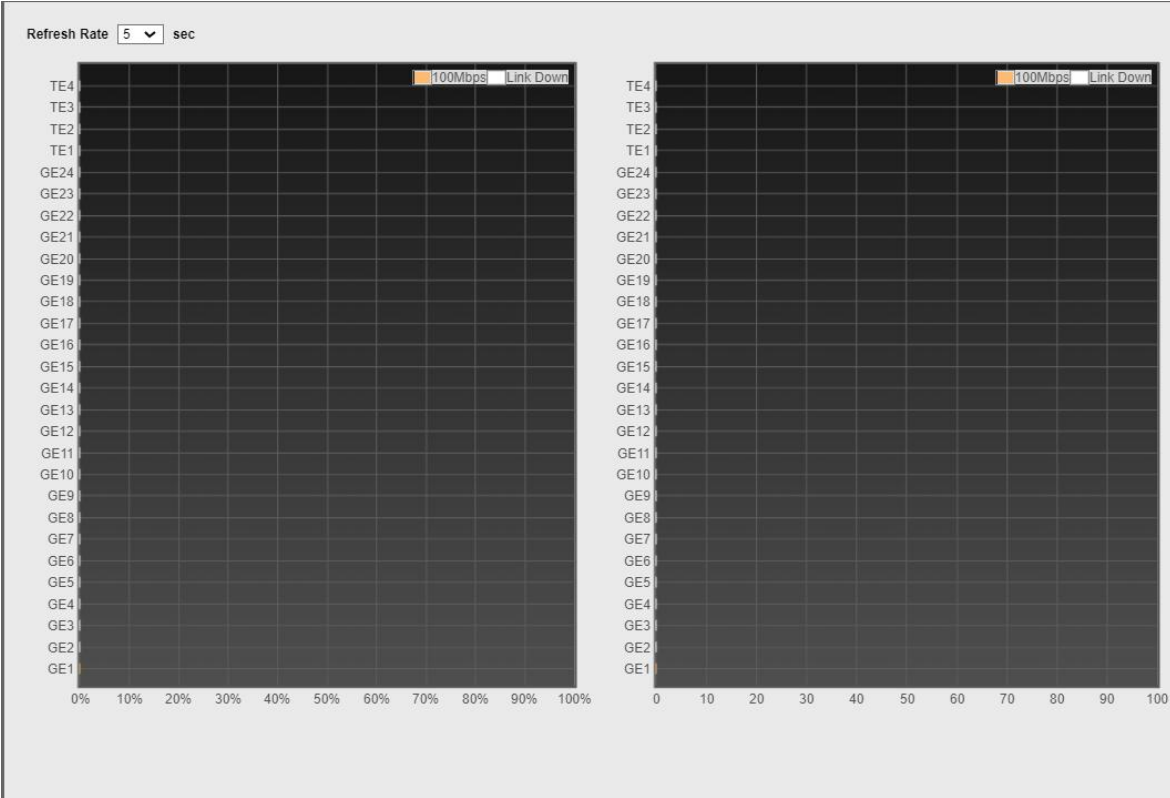


Figure 2-6 Port Bandwidth Utilization Page

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

Table 2-7 Bandwidth Utilization Fields

2.4. Link Aggregation

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

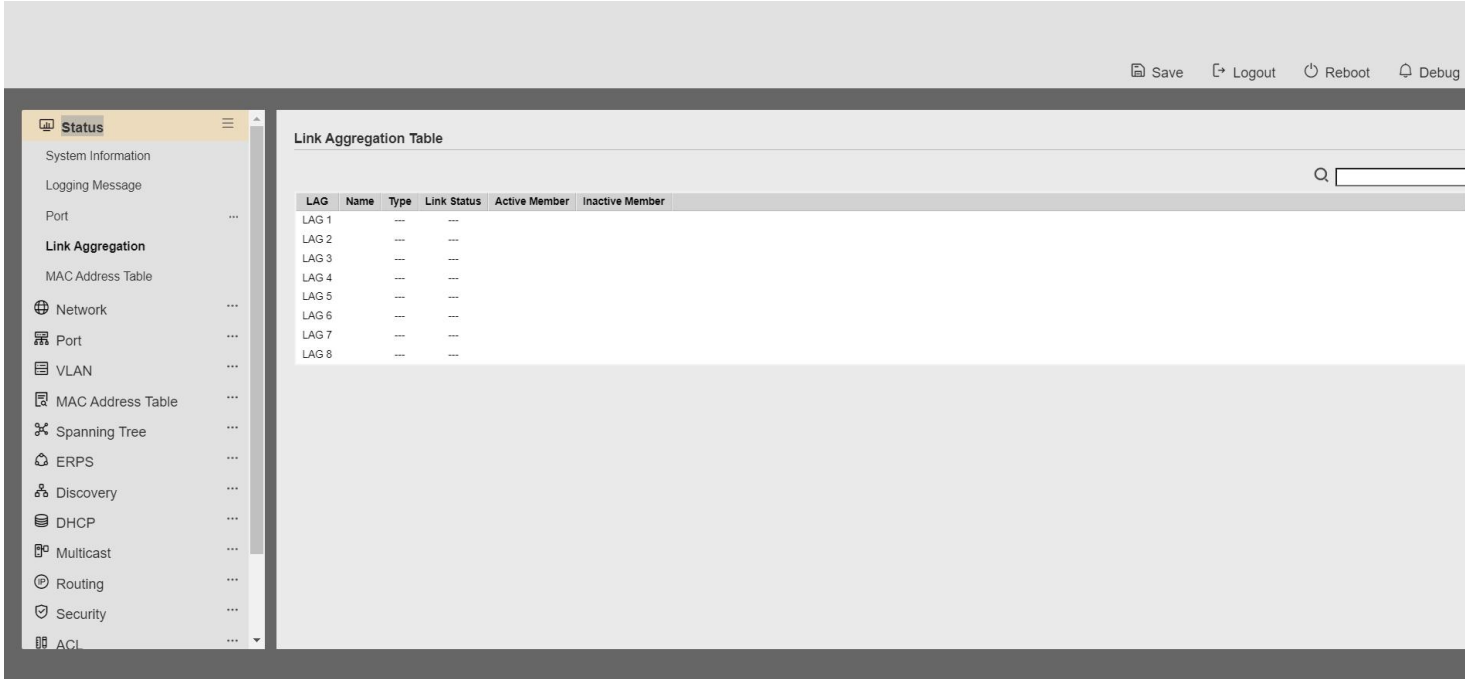


Figure 2-7 Link Aggregation Status Page

Field	Description
LAG	LAG Name
Name	LAG port description
Type	The type of the LAG <ul style="list-style-type: none">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

Table 2-8 LAG Status Fields

2.5. 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.

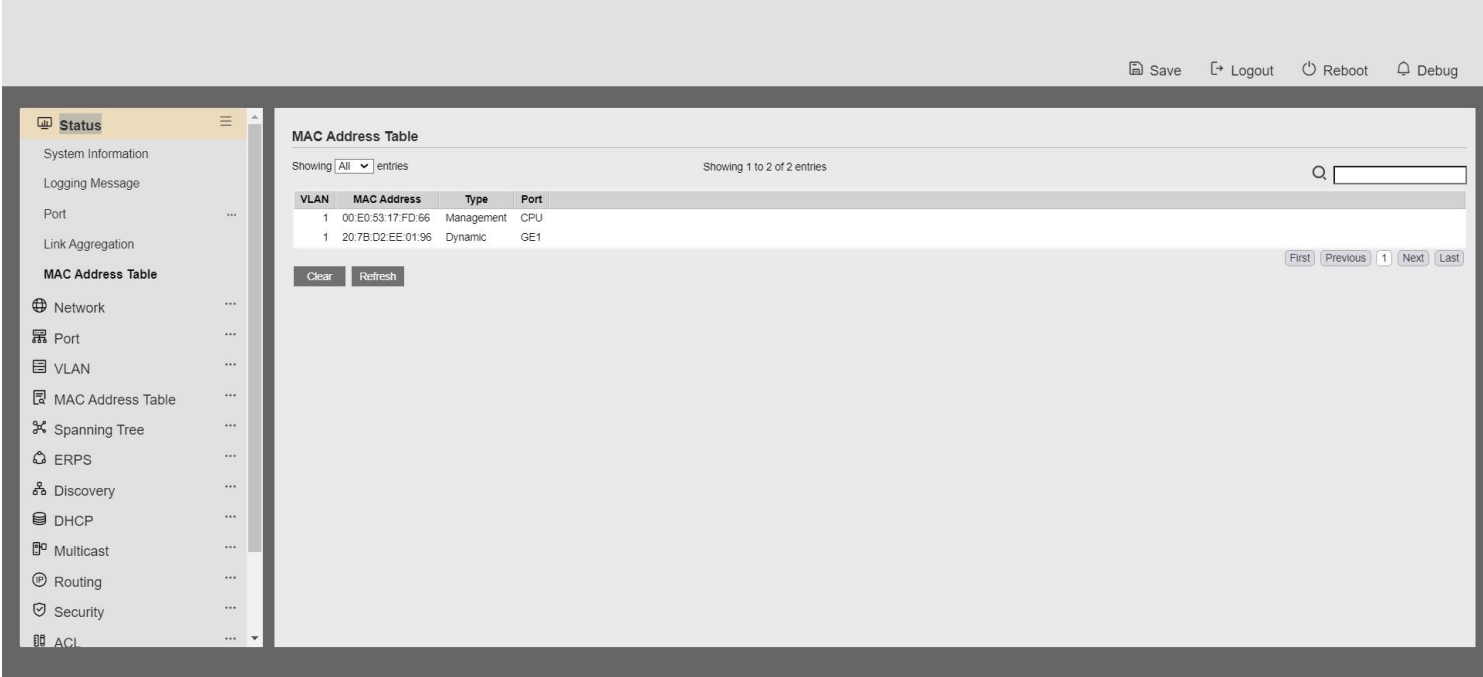


Figure 2-8 MAC Address Status Page

Field	Description
VLAN	VLAN ID of the mac address
MAC Address	MAC address
Type	<p>The type of MAC address</p> <ul style="list-style-type: none"> • Management: DUT’s base mac address for management purpose • Static: Manually configured by administrator • Dynamic: Auto learned by hardware
Port	<p>The type of Port</p> <ul style="list-style-type: none"> • CPU: DUT’s CPU port for management purpose • Other: Normal switch port

Table 2-9 MAC Address Status Fields

3. 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.

3.1. 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.

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

2024-04-07 YYYY-MM-DD

Time

10:32:36 HH:MM:SS

Daylight Saving Time

Type

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

Offset

60 Min (1 - 1440, default 60)

Recurring

From:

Day Sun ▾ Week First ▾ Month Jan ▾ Time

To:

Day Sun ▾ Week First ▾ Month Jan ▾ Time

Non-recurring

From:

YYYY-MM-DD HH:MM

To:

YYYY-MM-DD HH:MM

Operational Status

Current Time

2024-04-07 10:32:36 UTC+8

Figure 3-2 System Time Page

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

Source	Select the time source. <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • 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.

4. Port

Table 3-4 System Time Fields

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

4.1. 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.

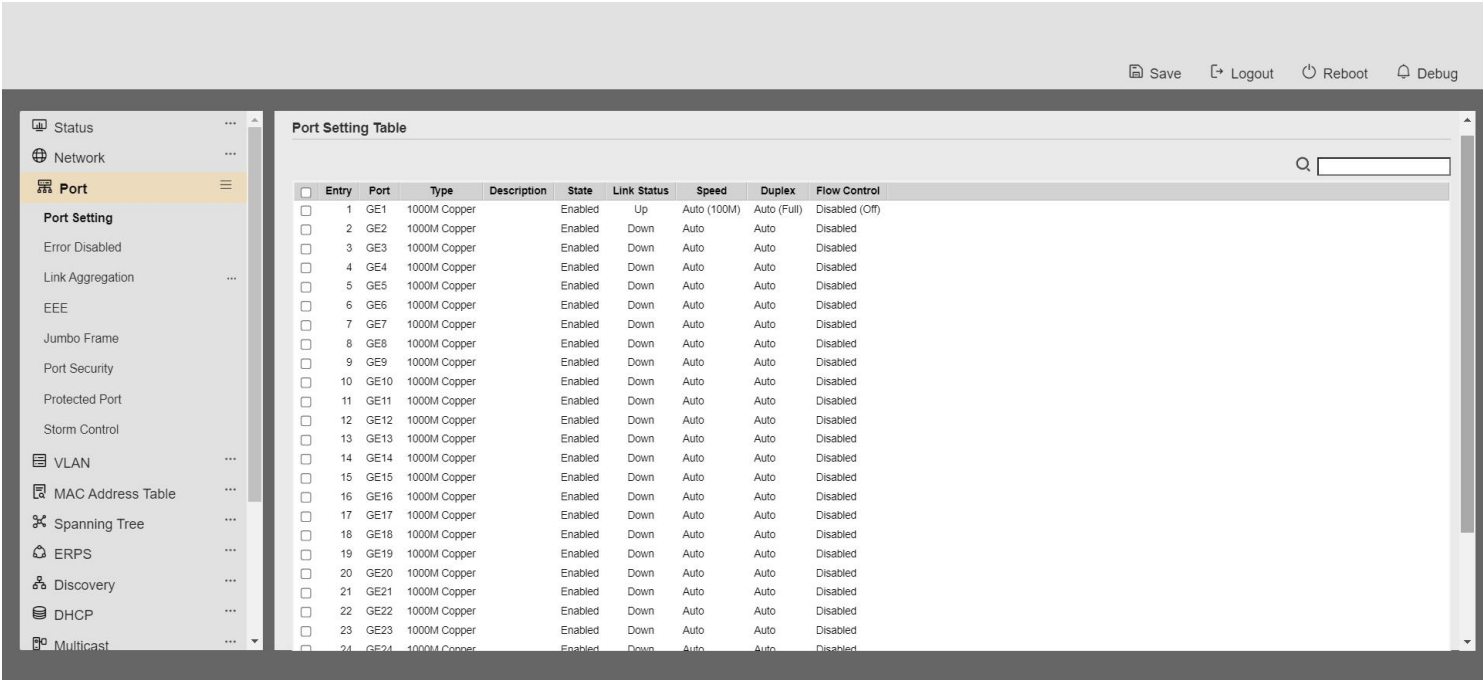


Figure 4-1 Port Setting Table

Field	Description
Port	Port Name
Type	Port media type
Description	Port description
State	Port admin state. <ul style="list-style-type: none">Enabled: Enable the port.Disabled: Disable the port.

Link Status	Current port link status <ul style="list-style-type: none"> • 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

Table 4-1 Port Setting Table Fields

Port Setting Table

<input type="checkbox"/>	Entry	Port	Type	Description	State	Link Status	Speed	Duplex	Flow Control
<input type="checkbox"/>	1	GE1	1000M Copper		Enabled	Up	Auto (100M)	Auto (Full)	Disabled (Off)
<input type="checkbox"/>	2	GE2	1000M Copper		Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	3	GE3	1000M Copper		Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	4	GE4	1000M Copper		Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	5	GE5	1000M Copper		Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	6	GE6	1000M Copper		Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	7	GE7	1000M Copper		Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	8	GE8	1000M Copper		Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	9	GE9	1000M Copper		Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	10	GE10	1000M Copper		Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	11	GE11	1000M Copper		Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	12	GE12	1000M Copper		Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	13	GE13	1000M Copper		Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	14	GE14	1000M Copper		Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	15	GE15	1000M Copper		Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	16	GE16	1000M Copper		Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	17	GE17	1000M Copper		Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	18	GE18	1000M Copper		Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	19	GE19	1000M Copper		Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	20	GE20	1000M Copper		Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	21	GE21	1000M Copper		Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	22	GE22	1000M Copper		Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	23	GE23	1000M Copper		Enabled	Down	Auto	Auto	Disabled

Figure 4-2 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.
	<ul style="list-style-type: none"> • 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.
	<ul style="list-style-type: none"> • 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.
	<ul style="list-style-type: none"> • Auto: Auto flow control by negotiation. • Enabled: Enable flow control ability. • Disabled: Disable flow control ability.

Table 4-2 Edit Port Setting Fields

4.2. Error Disabled

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

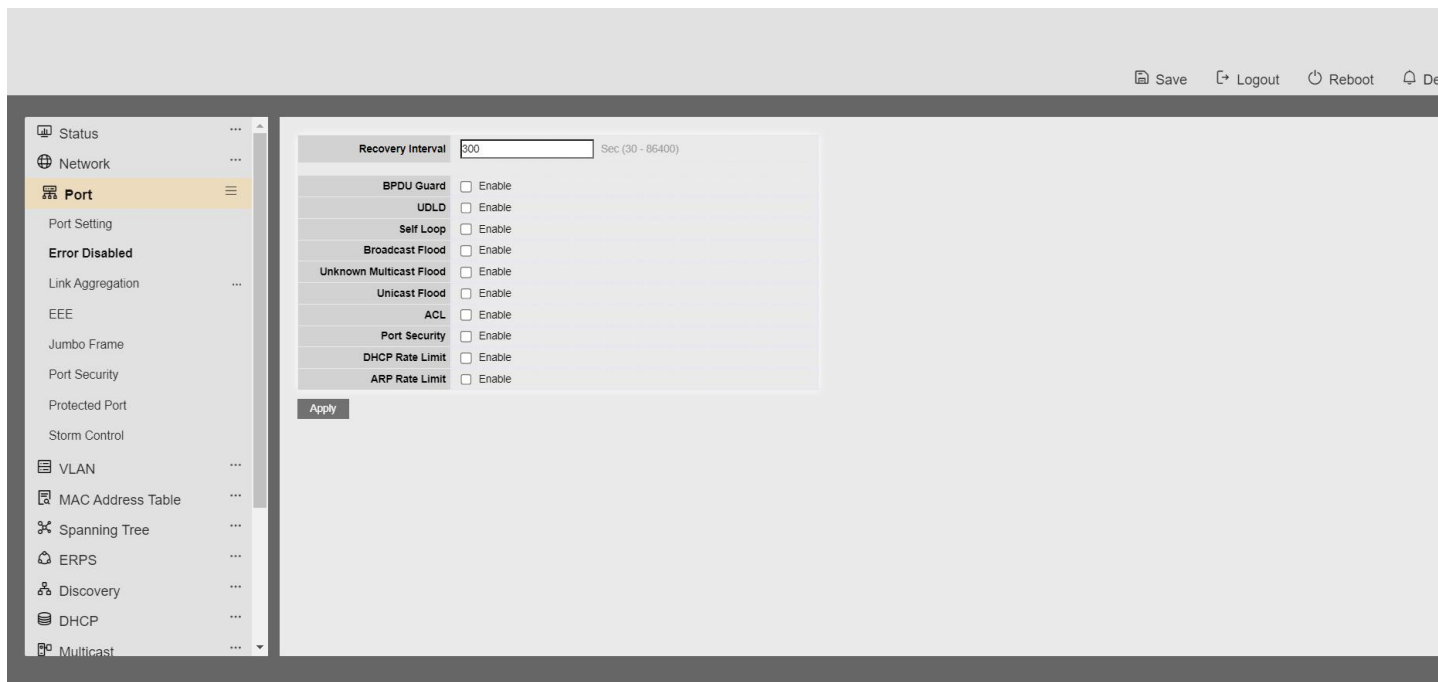


Figure 4-3 Error Disabled Page

Field	Description
Recover Interval	Auto recovery after this interval for error disabled port.
BPD Guard	Enabled to auto shutdown port when BPD Guard reason occur. This reason caused by STP BPD 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
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.

Table 4-3 Error Disabled Fields

4.3. Link Aggregation

4.3.1. 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.

Link Aggregation Table

Q

LAG	Name	Type	Link Status	Active Member	Inactive Member
<input type="radio"/>	LAG 1	---	---		
<input type="radio"/>	LAG 2	---	---		
<input type="radio"/>	LAG 3	---	---		
<input type="radio"/>	LAG 4	---	---		
<input type="radio"/>	LAG 5	---	---		
<input type="radio"/>	LAG 6	---	---		
<input type="radio"/>	LAG 7	---	---		
<input type="radio"/>	LAG 8	---	---		

Edit

Figure 4-4 LAG Global Setting

Field	Description
Load Balance Algorithm	LAG load balance distribution algorithm <ul style="list-style-type: none"> • src-dst-mac: Based on MAC address • src-dst-mac-ip: Based on MAC address and IP

Table 4-4 LAG Global Setting Fields

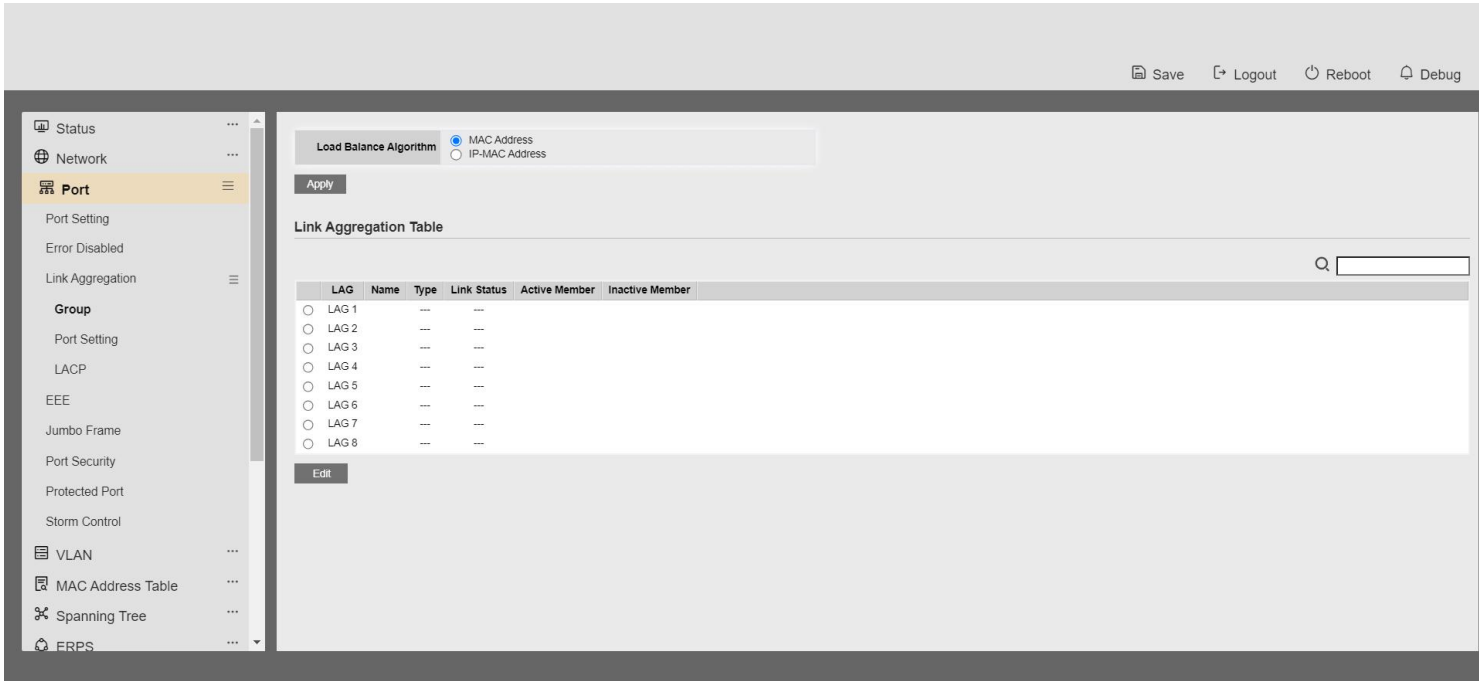


Figure 4-5 LAG Group Setting Table

Field	Description
LAG	LAG Name
Name	LAG port description
Type	The type of the LAG <ul style="list-style-type: none">• 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

Table 4-5 LAG Group Setting Fields



Figure 4-6 Edit LAG Group Setting Dialog

Field	Description
LAG	Selected LAG group ID
Name	LAG port description
Type	The type of the LAG <ul style="list-style-type: none">• 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

Table 4-6 Edit LAG Group Setting Field

4.3.2. 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.

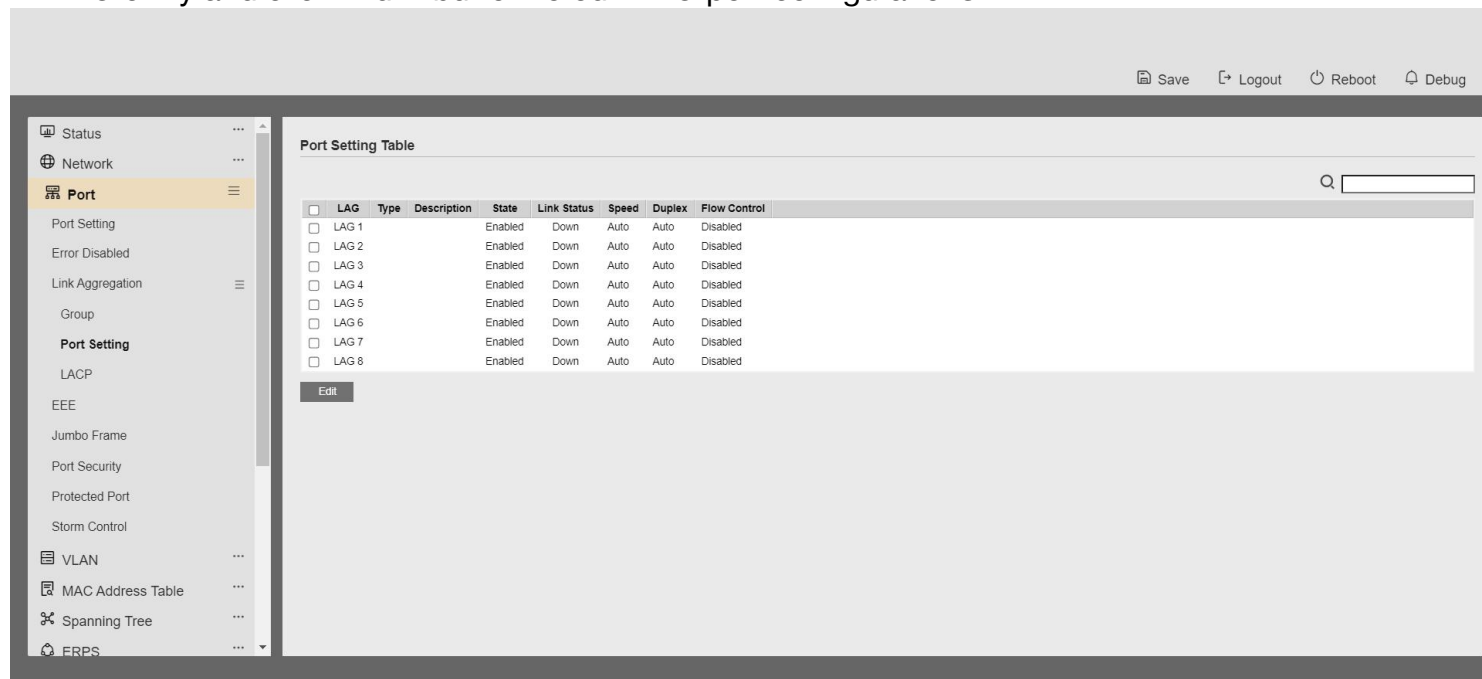


Figure 4-7 LAG Port Setting Table

Field	Description
LAG	LAG Port Name
Type	LAG Port media type
Description	LAG Port description
State	LAG Port admin state. <ul style="list-style-type: none"> • Enabled: Enable the port. • Disabled: Disable the port.
Link Status	Current LAG port link status <ul style="list-style-type: none"> • 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

Table 4-7 Port Setting Status Fields

Edit Port Setting

Port

LAG1

Description

State

☒ Enable

Speed

☒ Auto
 ☐ Auto - 10M
 ☐ Auto - 100M
 ☐ Auto - 1000M
 ☐ Auto - 10M/100M
 ☐ 10M
 ☐ 100M
 ☐ 1000M
 ☐ 10G

Flow Control

☐ Auto
 ☐ Enable
 ☒ Disable

Apply

Close

Figure 4-8 Edit LAG Port Setting Dialog

Field	Description
Port	Selected port list
Description	Port description
State	Port admin state. <ul style="list-style-type: none"> Enable: Enable the port. Disable: Disable the port.
Speed	Port speed capabilities. <ul style="list-style-type: none"> 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. <ul style="list-style-type: none"> Auto: Auto flow control by negotiation. Enabled: Enable flow control ability. Disabled: Disable flow control ability.

Table 4-8 Port Setting Status Fields

4.3.3. 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.



Figure 4-9 LACP Global Setting

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

Table 4-9 LACP Global Setting Fields

					Q <input type="text"/>	
<input type="checkbox"/>	Entry	Port	Port Priority	Timeout		
<input type="checkbox"/>	1	GE1	1	Long		
<input type="checkbox"/>	2	GE2	1	Long		
<input type="checkbox"/>	3	GE3	1	Long		
<input type="checkbox"/>	4	GE4	1	Long		
<input type="checkbox"/>	5	GE5	1	Long		
<input type="checkbox"/>	6	GE6	1	Long		
<input type="checkbox"/>	7	GE7	1	Long		
<input type="checkbox"/>	8	GE8	1	Long		
<input type="checkbox"/>	9	GE9	1	Long		
<input type="checkbox"/>	10	GE10	1	Long		
<input type="checkbox"/>	11	GE11	1	Long		
<input type="checkbox"/>	12	GE12	1	Long		
<input type="checkbox"/>	13	GE13	1	Long		
<input type="checkbox"/>	14	GE14	1	Long		
<input type="checkbox"/>	15	GE15	1	Long		
<input type="checkbox"/>	16	GE16	1	Long		
<input type="checkbox"/>	17	GE17	1	Long		
<input type="checkbox"/>	18	GE18	1	Long		
<input type="checkbox"/>	19	GE19	1	Long		
<input type="checkbox"/>	20	GE20	1	Long		
<input type="checkbox"/>	21	GE21	1	Long		
<input type="checkbox"/>	22	GE22	1	Long		
<input type="checkbox"/>	23	GE23	1	Long		
<input type="checkbox"/>	24	GE24	1	Long		
<input type="checkbox"/>	25	TF1	1	Long		

Web User Interface

Status

Network

Port

Port Setting

Error Disabled

Link Aggregation

Group

Port Setting

LACP

EEE

Jumbo Frame

Port Security

Protected Port

Storm Control

VLAN

MAC Address Table

Spanning Tree

ERPS

System Priority

32768

(1 - 65535, default 32768)

Apply

LACP Port Setting Table

Q

<input type="checkbox"/>	Entry	Port	Port Priority	Timeout
<input type="checkbox"/>	1	GE1	1	Long
<input type="checkbox"/>	2	GE2	1	Long
<input type="checkbox"/>	3	GE3	1	Long
<input type="checkbox"/>	4	GE4	1	Long
<input type="checkbox"/>	5	GE5	1	Long
<input type="checkbox"/>	6	GE6	1	Long
<input type="checkbox"/>	7	GE7	1	Long
<input type="checkbox"/>	8	GE8	1	Long
<input type="checkbox"/>	9	GE9	1	Long
<input type="checkbox"/>	10	GE10	1	Long
<input type="checkbox"/>	11	GE11	1	Long
<input type="checkbox"/>	12	GE12	1	Long
<input type="checkbox"/>	13	GE13	1	Long
<input type="checkbox"/>	14	GE14	1	Long
<input type="checkbox"/>	15	GE15	1	Long
<input type="checkbox"/>	16	GE16	1	Long
<input type="checkbox"/>	17	GE17	1	Long
<input type="checkbox"/>	18	GE18	1	Long
<input type="checkbox"/>	19	GE19	1	Long

Edit LACP Port Setting

Port	GE1	
Port Priority	<input type="text" value="1"/>	(1 - 65535, default 1)
Timeout	<input checked="" type="radio"/> Long <input type="radio"/> Short	
<div>ApplyClose</div>		

Field	Description
Port	Port Name
Port Priority	LACP priority value of the port
Timeout	The periodic transmissions type of LACP PDUs. <ul style="list-style-type: none">• Long: Transmit LACP PDU with slow periodic (30s).• Short: Transmit LACPP DU with fast periodic (1s).

Table 4-10 LACP Port Setting Table Fields

Edit LACP Port Setting

Port

GE2

Port Priority

(1 - 65535, default 1)

Timeout

☒ Long
☐ Short

Apply

Close

Figure 4-11 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. <ul style="list-style-type: none">• Long: Transmit LACP PDU with slow periodic (30s).• Short: Transmit LACPP DU with fast periodic (1s).

Table 4-11 Edit LACP Port Setting Fields

4.4. *EEE*

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

This page allow user to configure Energy Efficient Ethernet settings.

EEE Setting Table			
<input type="checkbox"/>	Entry	Port	State
<input type="checkbox"/>	1	GE1	Disabled
<input type="checkbox"/>	2	GE2	Disabled
<input type="checkbox"/>	3	GE3	Disabled
<input type="checkbox"/>	4	GE4	Disabled
<input type="checkbox"/>	5	GE5	Disabled
<input type="checkbox"/>	6	GE6	Disabled
<input type="checkbox"/>	7	GE7	Disabled
<input type="checkbox"/>	8	GE8	Disabled
<input type="checkbox"/>	9	GE9	Disabled
<input type="checkbox"/>	10	GE10	Disabled
<input type="checkbox"/>	11	GE11	Disabled
<input type="checkbox"/>	12	GE12	Disabled
<input type="checkbox"/>	13	GE13	Disabled
<input type="checkbox"/>	14	GE14	Disabled
<input type="checkbox"/>	15	GE15	Disabled
<input type="checkbox"/>	16	GE16	Disabled
<input type="checkbox"/>	17	GE17	Disabled
<input type="checkbox"/>	18	GE18	Disabled

Figure 4-12 EEE Setting Table

Field	Description
Port	Port Name
State	Port EEE admin state. <ul style="list-style-type: none">• Enabled: EEE is enabled• Disabled: EEE is disabled
Operational Status	Port EEE operational status. <ul style="list-style-type: none">• Enabled: EEE is operating• Disabled: EEE is no operating

Table 4-12 EEE Setting Table Fields

Edit EEE Setting

Port	GE10
State	<input type="checkbox"/> Enable

Apply

Close

Figure 4-13 Edit EEE Setting Dialog

Field	Description
Port	Selected port list
State	Port EEE admin state. <ul style="list-style-type: none">• Enable: Enable EEE• Disable: Disable EEE

Table 4-13 Edit EEE Setting Fields

4.5. Jumbo Frame

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

Frame. This page allow user to configure switch jumbo

frame size.

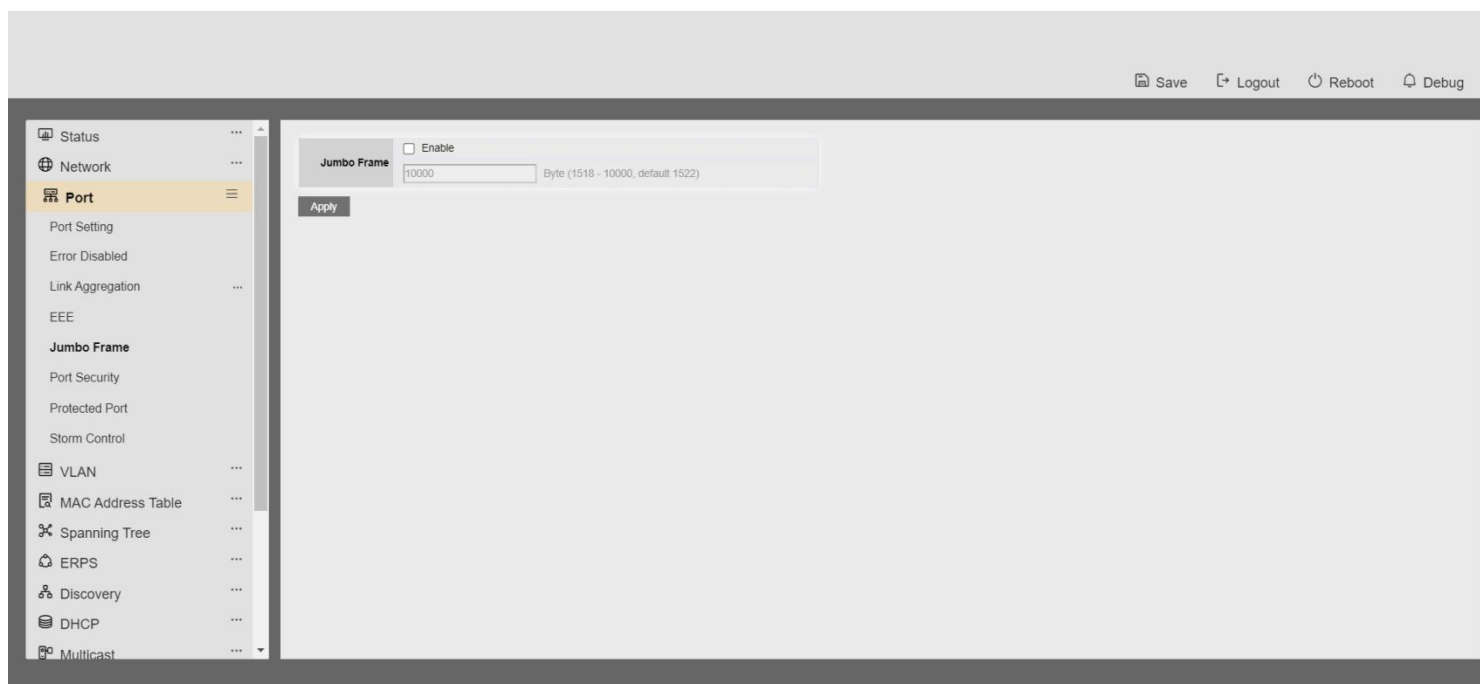


Figure 4-14 Jumbo Frame Page

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.

Table 4-14 Jumbo Frame Fields

4.6. Port Security

1. Click the "Port > Port Security" menu in the navigation bar to enter the Port Security Configuration page, where you can enable the port security status and view the port security configuration information, as shown in the following figure

State ☐ Enable

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

Apply

Port Security Table

<input type="checkbox"/>	Entry	Port	State	Address Limit	Total	Configured	Violate Number	Violate Action	Sticky
<input type="checkbox"/>	1	GE1	Disabled	1	0	0	0	Protect	Disabled
<input type="checkbox"/>	2	GE2	Disabled	1	0	0	0	Protect	Disabled
<input type="checkbox"/>	3	GE3	Disabled	1	0	0	0	Protect	Disabled
<input type="checkbox"/>	4	GE4	Disabled	1	0	0	0	Protect	Disabled
<input type="checkbox"/>	5	GE5	Disabled	1	0	0	0	Protect	Disabled
<input type="checkbox"/>	6	GE6	Disabled	1	0	0	0	Protect	Disabled
<input type="checkbox"/>	7	GE7	Disabled	1	0	0	0	Protect	Disabled
<input type="checkbox"/>	8	GE8	Disabled	1	0	0	0	Protect	Disabled
<input type="checkbox"/>	9	GE9	Disabled	1	0	0	0	Protect	Disabled
<input type="checkbox"/>	10	GE10	Disabled	1	0	0	0	Protect	Disabled
<input type="checkbox"/>	11	GE11	Disabled	1	0	0	0	Protect	Disabled
<input type="checkbox"/>	12	GE12	Disabled	1	0	0	0	Protect	Disabled
<input type="checkbox"/>	13	GE13	Disabled	1	0	0	0	Protect	Disabled
<input type="checkbox"/>	14	GE14	Disabled	1	0	0	0	Protect	Disabled
<input type="checkbox"/>	15	GE15	Disabled	1	0	0	0	Protect	Disabled
<input type="checkbox"/>	16	GE16	Disabled	1	0	0	0	Protect	Disabled
<input type="checkbox"/>	17	GE17	Disabled	1	0	0	0	Protect	Disabled
<input type="checkbox"/>	18	GE18	Disabled	1	0	0	0	Protect	Disabled

2. Select (multiple selectable) ports and click the Modify button to enable or disable port override action, maximum MAC learning number, and port security status, as shown in the following figure:

Edit Port Security

Port

GE1

State

☐ Enable

Address Limit

(1 - 256, default 1)

Violate Action

☒ Protect
☐ Restrict
☐ Shutdown

Sticky

☐ Enable

Apply

Close

4.7.Protected Port

Port traffic sometimes do not need to communicate with each other, but broadcast, multicast and other messages will flood to each port, at this time you can use the port isolation function to achieve port-to-port message isolation.

Operation steps:

1. Click the "Port > Port Isolation" menu in the navigation bar to enter the port isolation configuration interface, check the ports that need to be isolated, you can select more than one, click Modify to configure the isolation function of the switch, as shown in the following figure:

Protected Port Table			
<input type="checkbox"/>	Entry	Port	State
<input type="checkbox"/>	1	GE1	Unprotected
<input type="checkbox"/>	2	GE2	Unprotected
<input type="checkbox"/>	3	GE3	Unprotected
<input checked="" type="checkbox"/>	4	GE4	Unprotected
<input type="checkbox"/>	5	GE5	Unprotected
<input type="checkbox"/>	6	GE6	Unprotected
<input type="checkbox"/>	7	GE7	Unprotected
<input type="checkbox"/>	8	GE8	Unprotected
<input type="checkbox"/>	9	GE9	Unprotected
<input type="checkbox"/>	10	GE10	Unprotected
<input type="checkbox"/>	11	GE11	Unprotected
<input type="checkbox"/>	12	GE12	Unprotected
<input type="checkbox"/>	13	GE13	Unprotected
<input type="checkbox"/>	14	GE14	Unprotected

Edit Protected Port

Port
GE4

State
☐ Protected

Apply
Close

4.8.storm control

Introducing the storm suppression feature allows you to control these three types of message traffic and prevent broadcast storms.

Procedure:

Click the "Port > Storm Control" menu in the navigation bar to enter the Storm Control page. The page allows you to configure storm control related properties, such as mode, etc. The interface is as follows:

Mode

☐ Packet / Sec
☒ Kbits / Sec

IFG

☒ Exclude
☐ Include

Apply

The page allows you to configure the broadcast, multicast, and unknown unicast storm control rate for each port separately, select the port you need to configure, and then click the Modify button:

Edit Port Setting

Port
GE15

State
☐ Enable

Broadcast

☐ Enable

Kbps (16 - 1000000, default 10000)

Unknown Multicast

☐ Enable

Kbps (16 - 1000000, default 10000)

Unknown Unicast

☐ Enable

Kbps (16 - 1000000, default 10000)

Action

☒ Drop
☐ Shutdown

Apply
Close

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.




Figure 5-1 Create VLAN Page

Fiel	Description
d	
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 VLANs from right box then move to left box to delete.

Table 5-1 Create VLAN Fields



The dialog box is titled "Edit VLAN Name". It contains a text input field labeled "Name" with the value "VLAN0002". Below the input field are two buttons: "Apply" and "Close".

Figure 5-2 Edit VLAN Name Dialog

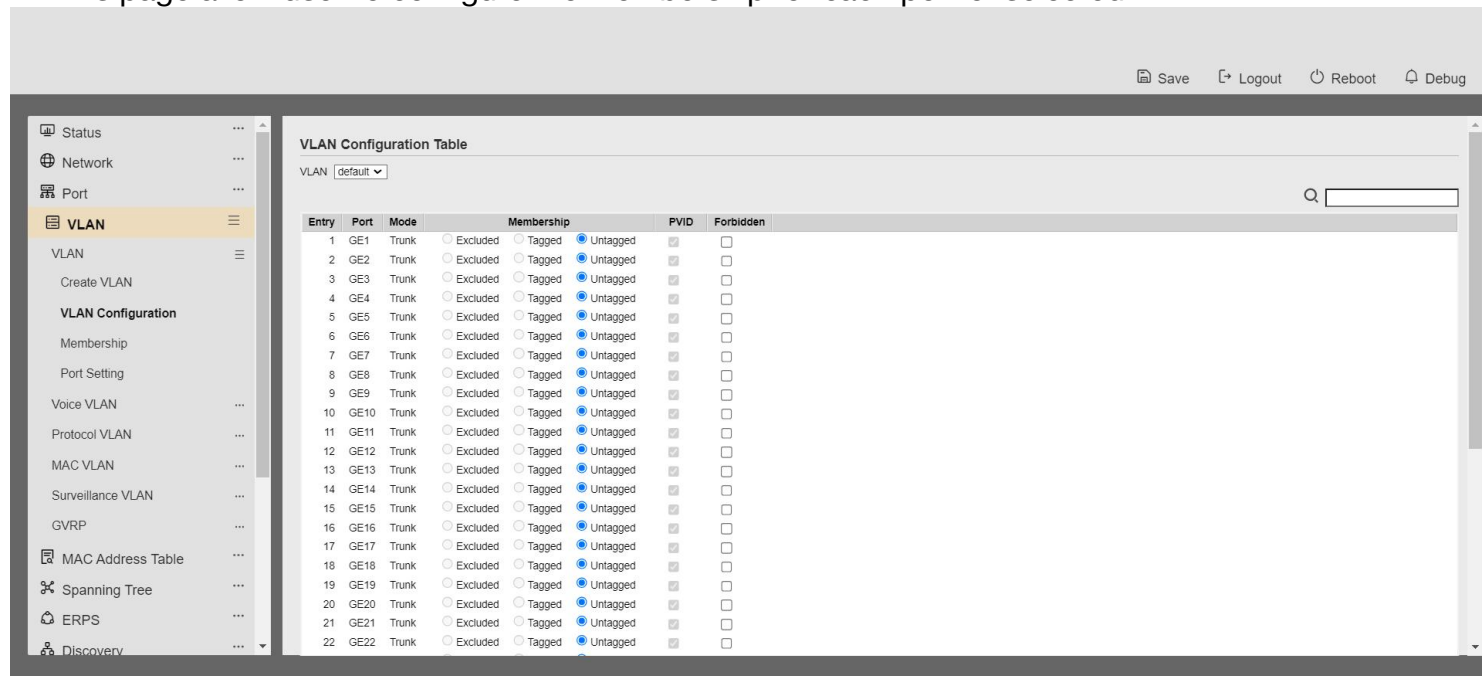
Field	Description
Name	Input VLAN name.

Table 5-2 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.



The screenshot shows the "VLAN Configuration Table" page. On the left is a sidebar menu with options like Status, Network, Port, VLAN, VLAN Configuration, Membership, Port Setting, Voice VLAN, Protocol VLAN, MAC VLAN, Surveillance VLAN, GVRP, MAC Address Table, Spanning Tree, ERPS, and Discovery. The main area displays a table with columns: Entry, Port, Mode, Membership, PVID, and Forbidden. The table lists 22 entries (GE1 to GE22) with their respective configurations. At the top right of the main area are buttons for Save, Logout, Reboot, and Debug. A search bar is also present.

Entry	Port	Mode	Membership	PVID	Forbidden
1	GE1	Trunk	Excluded Tagged Untagged	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2	GE2	Trunk	Excluded Tagged Untagged	<input checked="" type="checkbox"/>	<input type="checkbox"/>
3	GE3	Trunk	Excluded Tagged Untagged	<input checked="" type="checkbox"/>	<input type="checkbox"/>
4	GE4	Trunk	Excluded Tagged Untagged	<input checked="" type="checkbox"/>	<input type="checkbox"/>
5	GE5	Trunk	Excluded Tagged Untagged	<input checked="" type="checkbox"/>	<input type="checkbox"/>
6	GE6	Trunk	Excluded Tagged Untagged	<input checked="" type="checkbox"/>	<input type="checkbox"/>
7	GE7	Trunk	Excluded Tagged Untagged	<input checked="" type="checkbox"/>	<input type="checkbox"/>
8	GE8	Trunk	Excluded Tagged Untagged	<input checked="" type="checkbox"/>	<input type="checkbox"/>
9	GE9	Trunk	Excluded Tagged Untagged	<input checked="" type="checkbox"/>	<input type="checkbox"/>
10	GE10	Trunk	Excluded Tagged Untagged	<input checked="" type="checkbox"/>	<input type="checkbox"/>
11	GE11	Trunk	Excluded Tagged Untagged	<input checked="" type="checkbox"/>	<input type="checkbox"/>
12	GE12	Trunk	Excluded Tagged Untagged	<input checked="" type="checkbox"/>	<input type="checkbox"/>
13	GE13	Trunk	Excluded Tagged Untagged	<input checked="" type="checkbox"/>	<input type="checkbox"/>
14	GE14	Trunk	Excluded Tagged Untagged	<input checked="" type="checkbox"/>	<input type="checkbox"/>
15	GE15	Trunk	Excluded Tagged Untagged	<input checked="" type="checkbox"/>	<input type="checkbox"/>
16	GE16	Trunk	Excluded Tagged Untagged	<input checked="" type="checkbox"/>	<input type="checkbox"/>
17	GE17	Trunk	Excluded Tagged Untagged	<input checked="" type="checkbox"/>	<input type="checkbox"/>
18	GE18	Trunk	Excluded Tagged Untagged	<input checked="" type="checkbox"/>	<input type="checkbox"/>
19	GE19	Trunk	Excluded Tagged Untagged	<input checked="" type="checkbox"/>	<input type="checkbox"/>
20	GE20	Trunk	Excluded Tagged Untagged	<input checked="" type="checkbox"/>	<input type="checkbox"/>
21	GE21	Trunk	Excluded Tagged Untagged	<input checked="" type="checkbox"/>	<input type="checkbox"/>
22	GE22	Trunk	Excluded Tagged Untagged	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Figure 5-3 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	<p>Select the membership for this port of the specified VLAN ID.</p> <ul style="list-style-type: none"> • 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.

Table 5-3 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

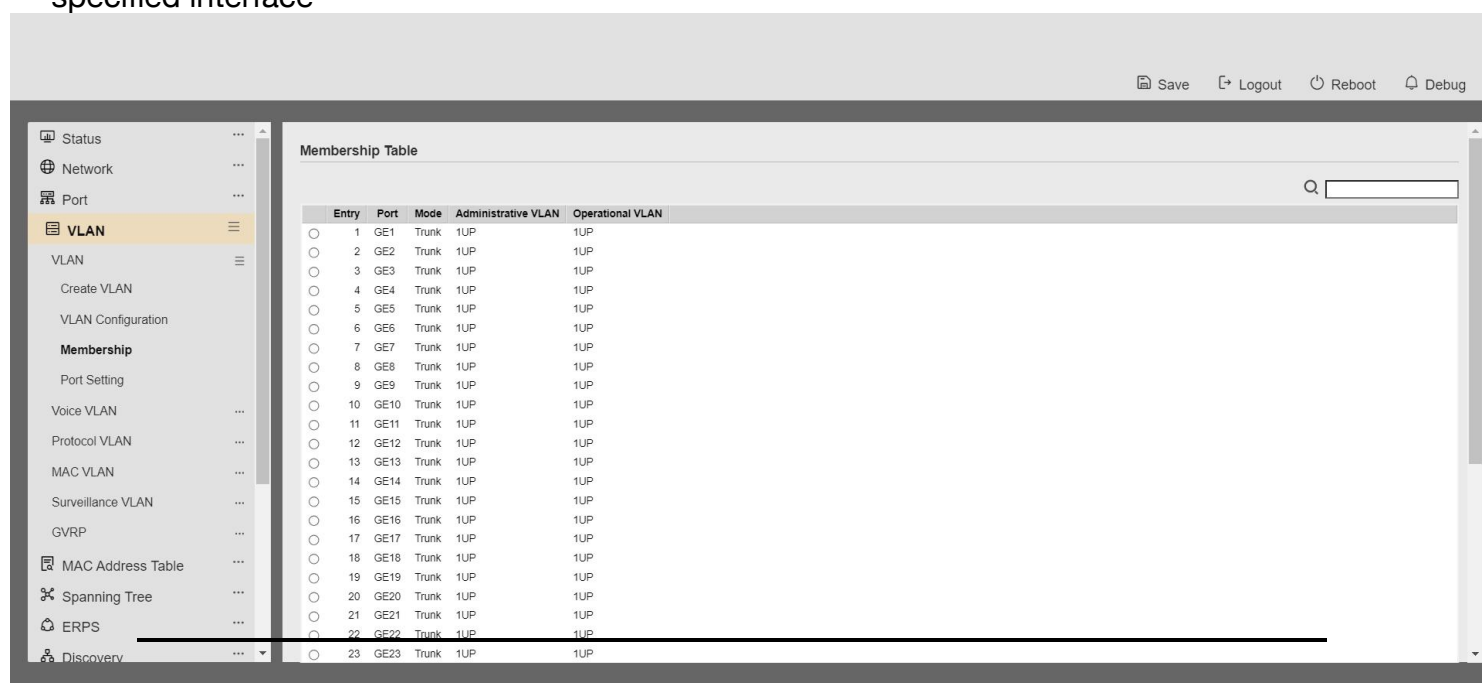


Figure 5-4 Membership Page

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.

Table 5-4 Membership Fields

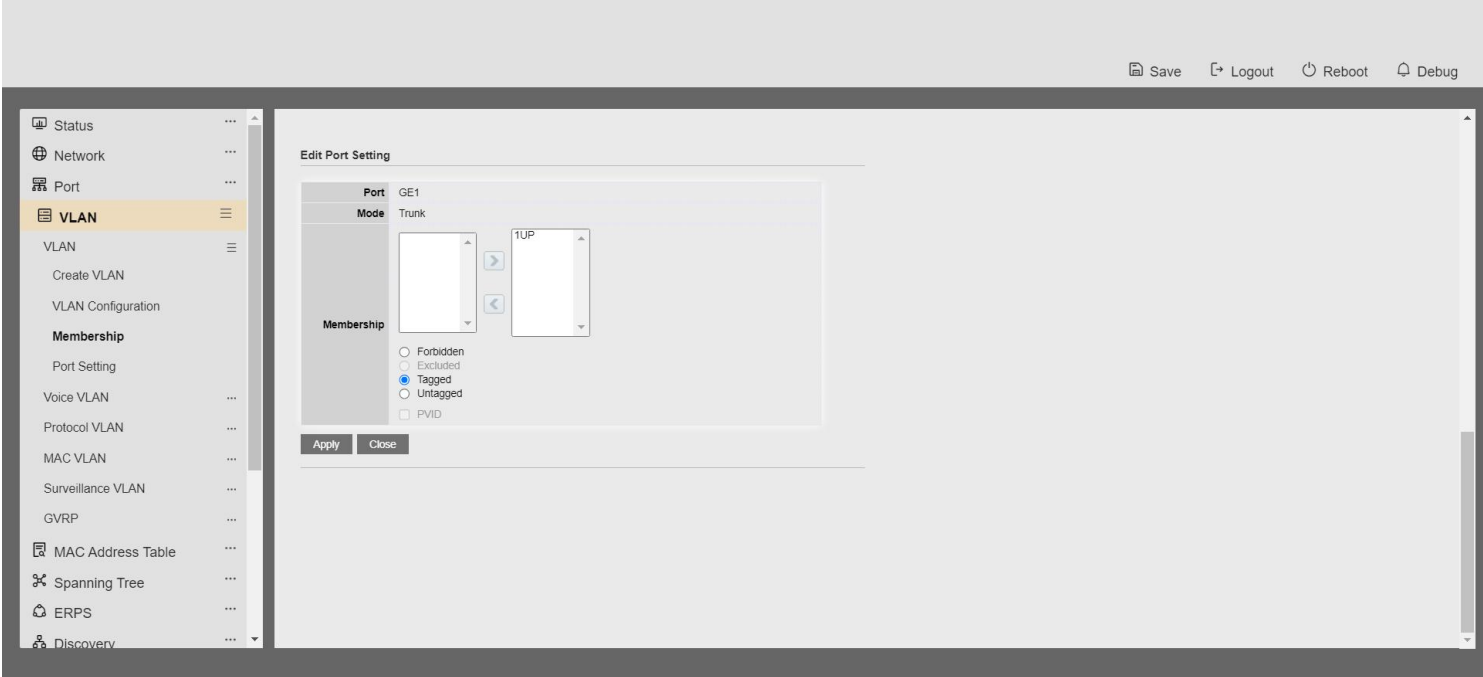


Figure 5-5 Edit Membership Dialog

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.

Table 5-5 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.

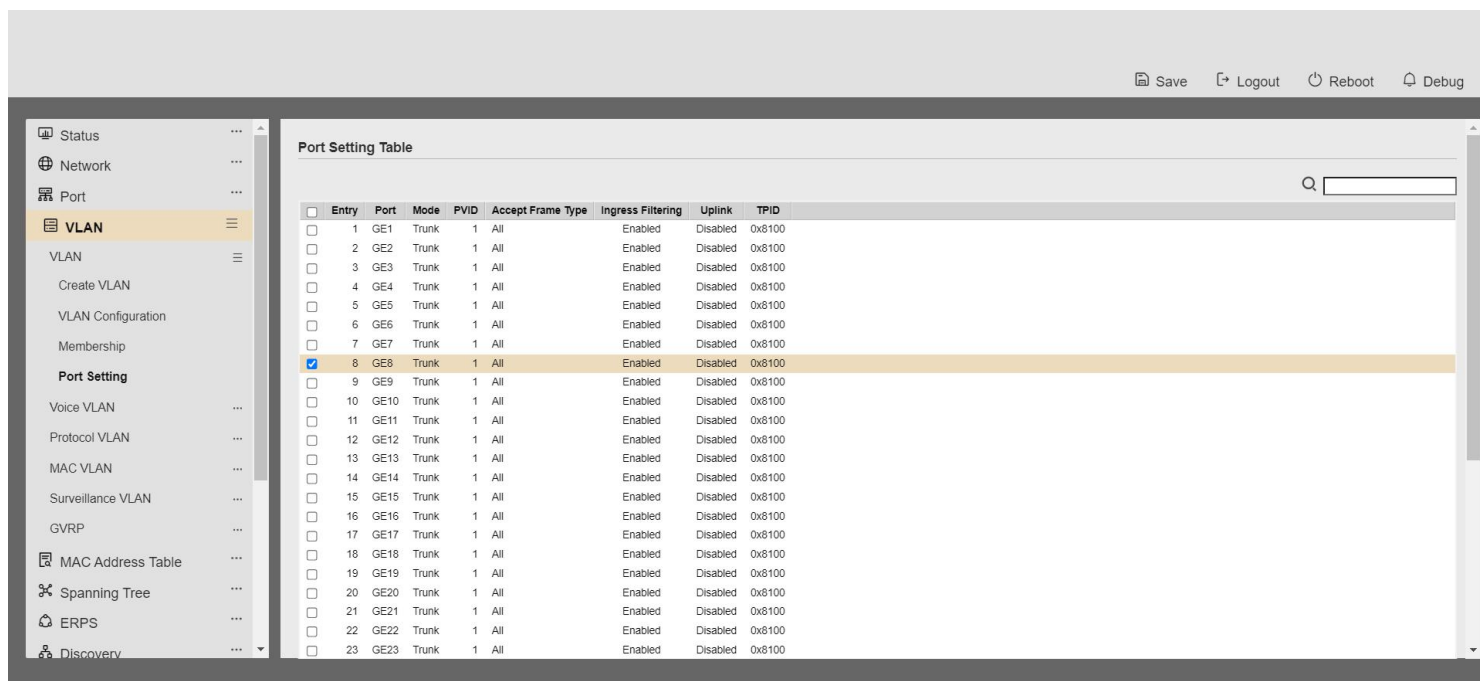


Figure 5-6 Port Setting Page

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.

Table 5-6 Port setting Fields

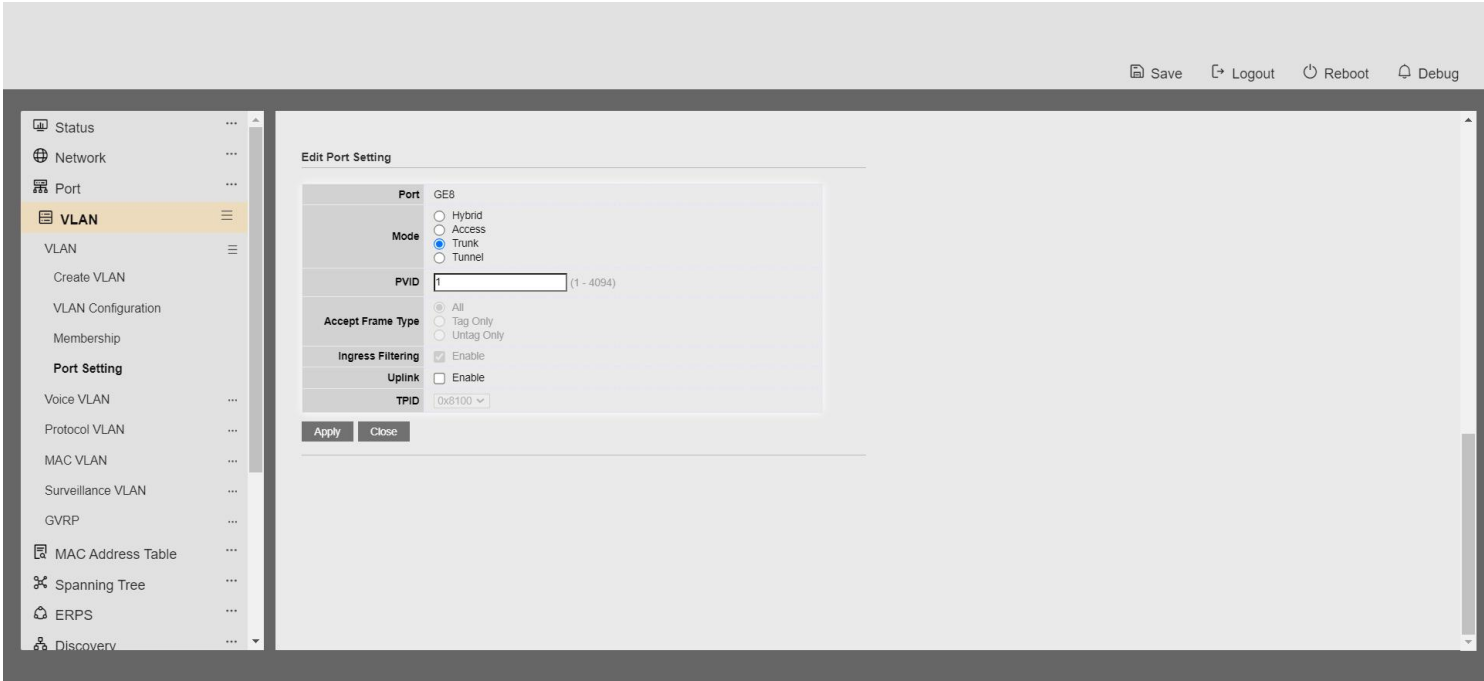


Figure 5-7 Edit Port Setting Dialog

Field	Description
Port	Display selected port to be edited.
Mode	Select the VLAN mode of the interface. <ul style="list-style-type: none">• 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.

Table 5-7 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.

State

☐ Enable

VLAN

None

CoS / 802.1p
Remarking

☐ Enable

6

Aging Time

1440

Min (30 - 65536, default 1440)

Apply

Figure 5-8 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 Remarking	Select a value of VPT. Qualified packets will use this VPT value as inner priority. 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.

Table 5-8 Property Fields

Status

Network

Port

VLAN

VLAN

Voice VLAN

Property

Voice OUI

Protocol VLAN

MAC VLAN

Surveillance VLAN

GVRP

MAC Address Table

Spanning Tree

ERPS

Discovery

DHCP

Multicast

State

VLAN

CoS / 802.1p

Remark

Aging Time

Apply

Port Setting Table

Q

	Entry	Port	State	Mode	QoS Policy
<input type="checkbox"/>	1	GE1	Disabled	Auto	Voice Packet
<input type="checkbox"/>	2	GE2	Disabled	Auto	Voice Packet
<input type="checkbox"/>	3	GE3	Disabled	Auto	Voice Packet
<input type="checkbox"/>	4	GE4	Disabled	Auto	Voice Packet
<input type="checkbox"/>	5	GE5	Disabled	Auto	Voice Packet
<input type="checkbox"/>	6	GE6	Disabled	Auto	Voice Packet
<input type="checkbox"/>	7	GE7	Disabled	Auto	Voice Packet
<input type="checkbox"/>	8	GE8	Disabled	Auto	Voice Packet
<input type="checkbox"/>	9	GE9	Disabled	Auto	Voice Packet
<input type="checkbox"/>	10	GE10	Disabled	Auto	Voice Packet
<input type="checkbox"/>	11	GE11	Disabled	Auto	Voice Packet
<input type="checkbox"/>	12	GE12	Disabled	Auto	Voice Packet
<input type="checkbox"/>	13	GE13	Disabled	Auto	Voice Packet
<input type="checkbox"/>	14	GE14	Disabled	Auto	Voice Packet

Figure 5-9 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

Table 5-9 Property Port Fields

Edit Port Setting

Port

State

Mode

QoS Policy

GE1

☐ Enable

☒ Auto
☐ Manual

☒ Voice Packet
☐ All

Apply

Close

Figure 5-10 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 <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • 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.

Table 5-10 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.

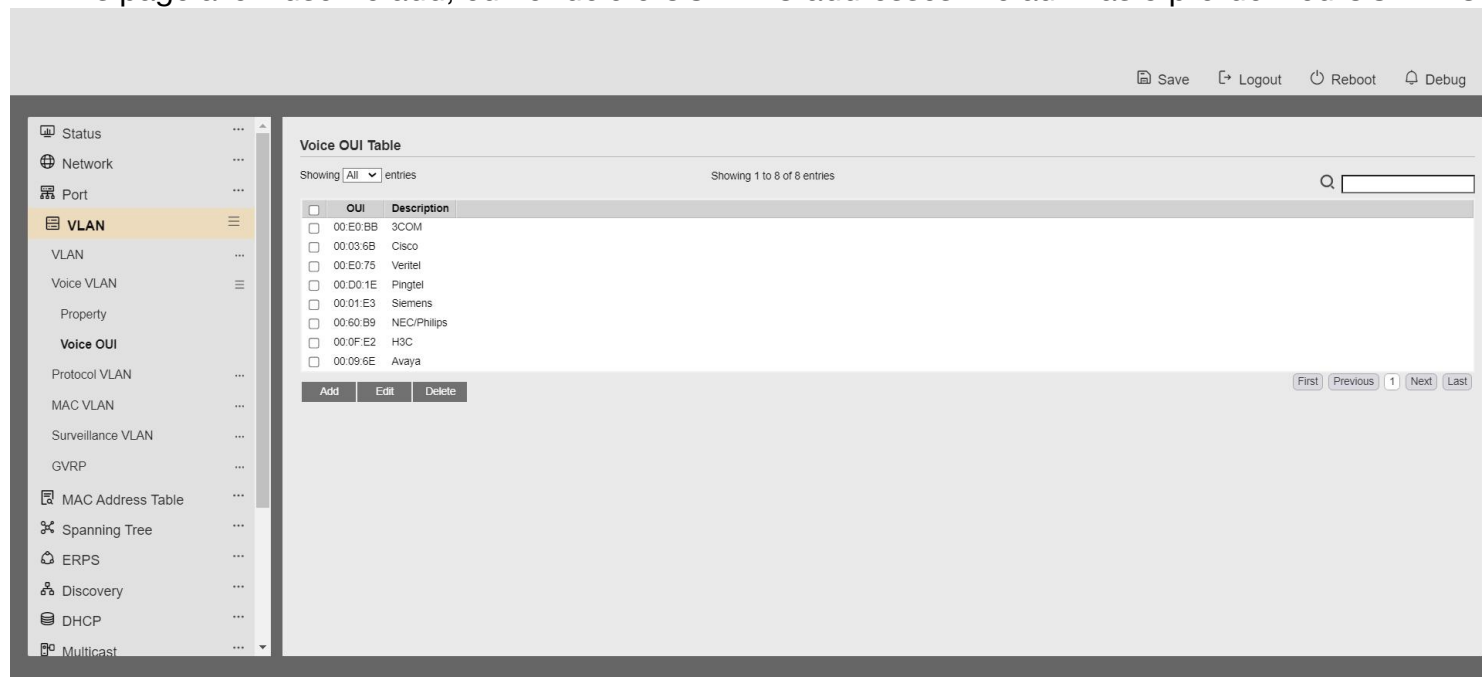


Figure 5-11 Voice OUI Page

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

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

Table 5-11 Voice OUI Mac Setting Fields

Add Voice OUI

OUI

Description

Apply

Close

Edit Voice OUI

OUI

00:E0:BB

Description

3COM

Apply

Close

Figure 5-12 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

Table 5-12 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.

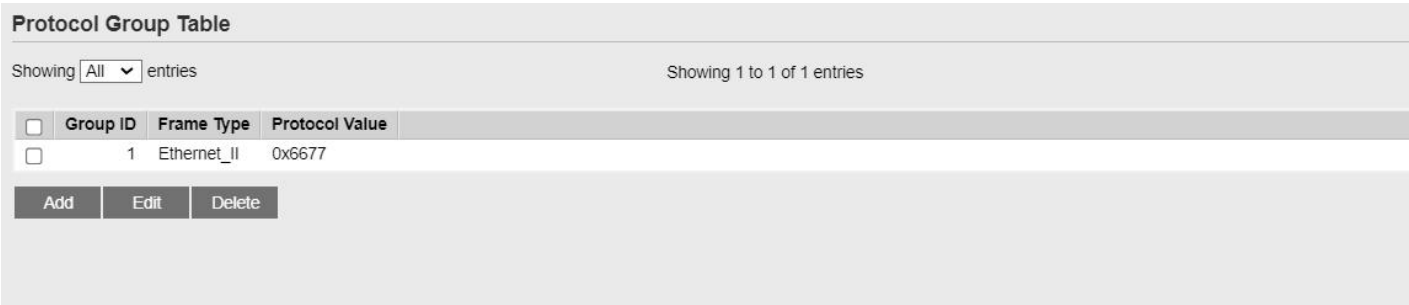
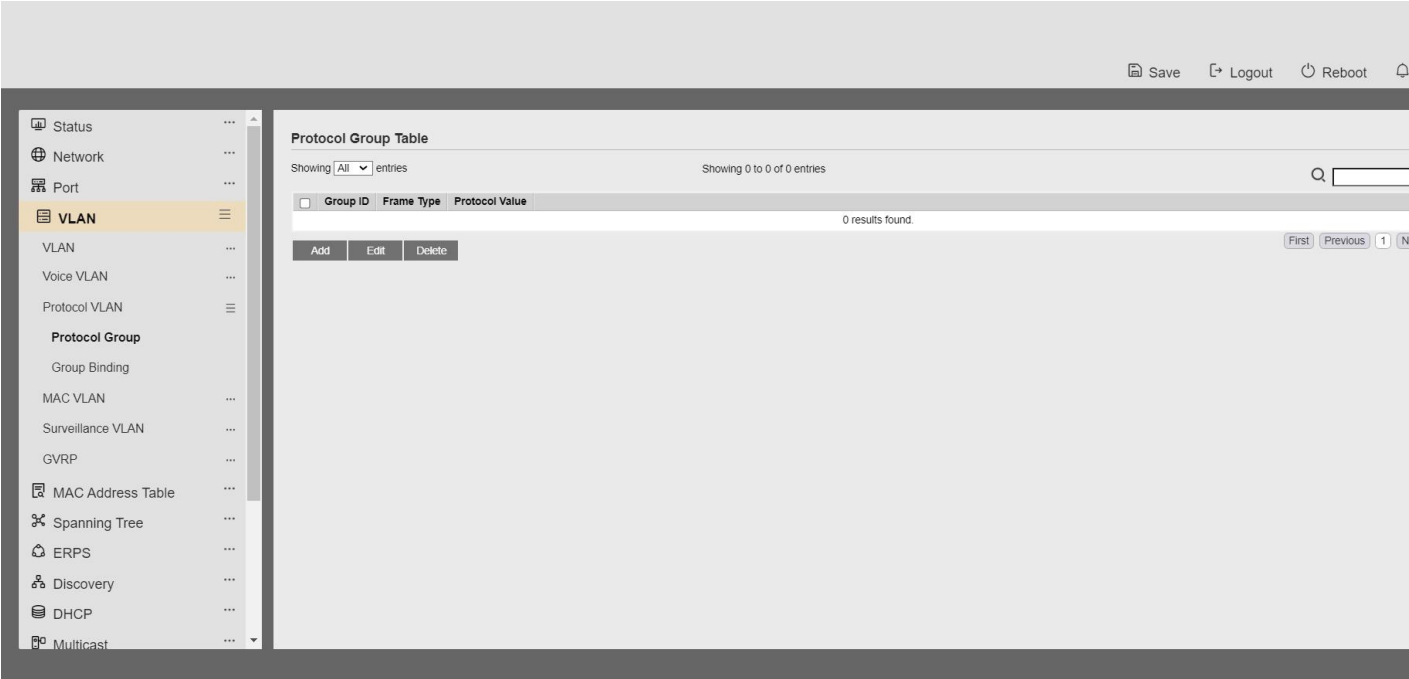


Figure 5-13 Protocol Group Page

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

Table 5-13 Protocol Group Fields

Figure 5-14 Add and Edit Protocol Group Dialog

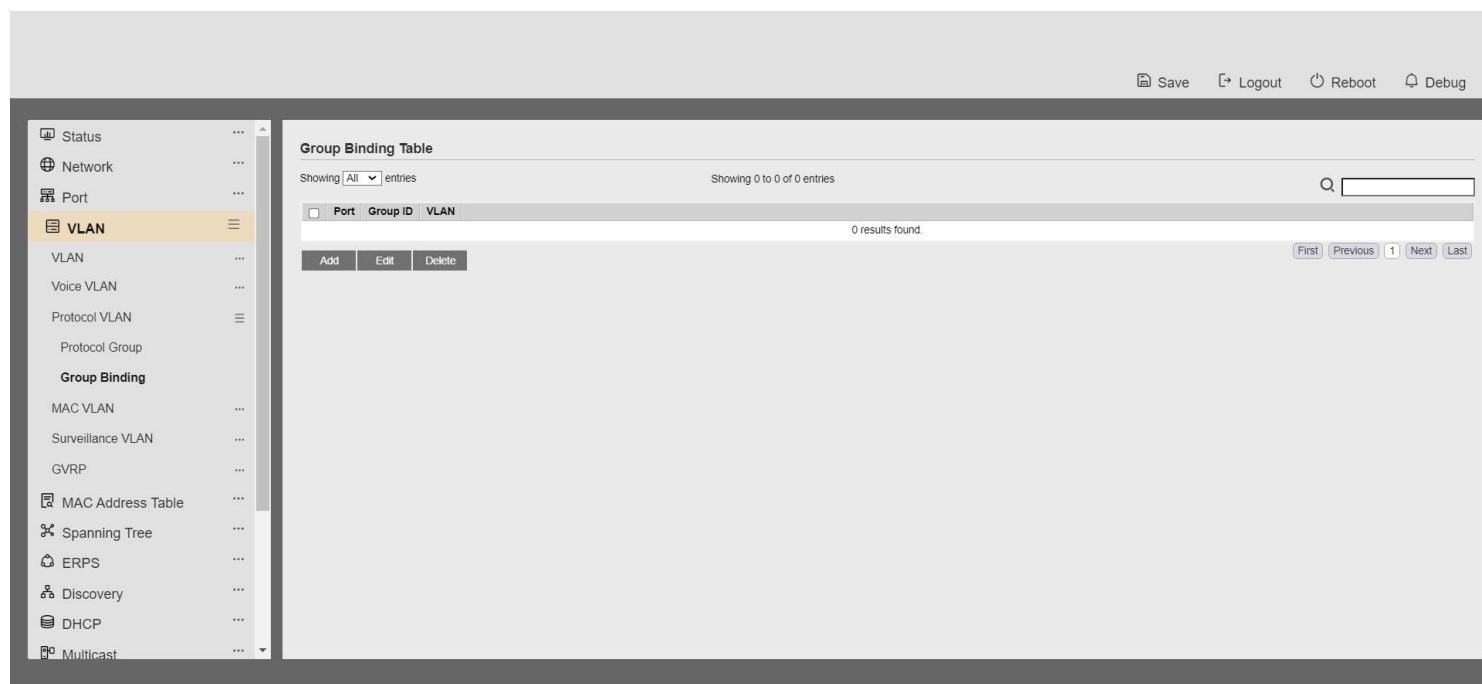
Field	Description
-------	-------------

Group ID	Select group ID of list. The range from 1 to 8.
Frame Type	<p>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.</p> <ul style="list-style-type: none"> • Ethernet_II: packet type is Ethernet version 2. • IEEE802.3_LL_C_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.

Table 5-14 Add and Edit Protocol Group Fields

5.3.2. Group Binding

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



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

Figure 5-15 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

Table 5-15 Group Binding Fields

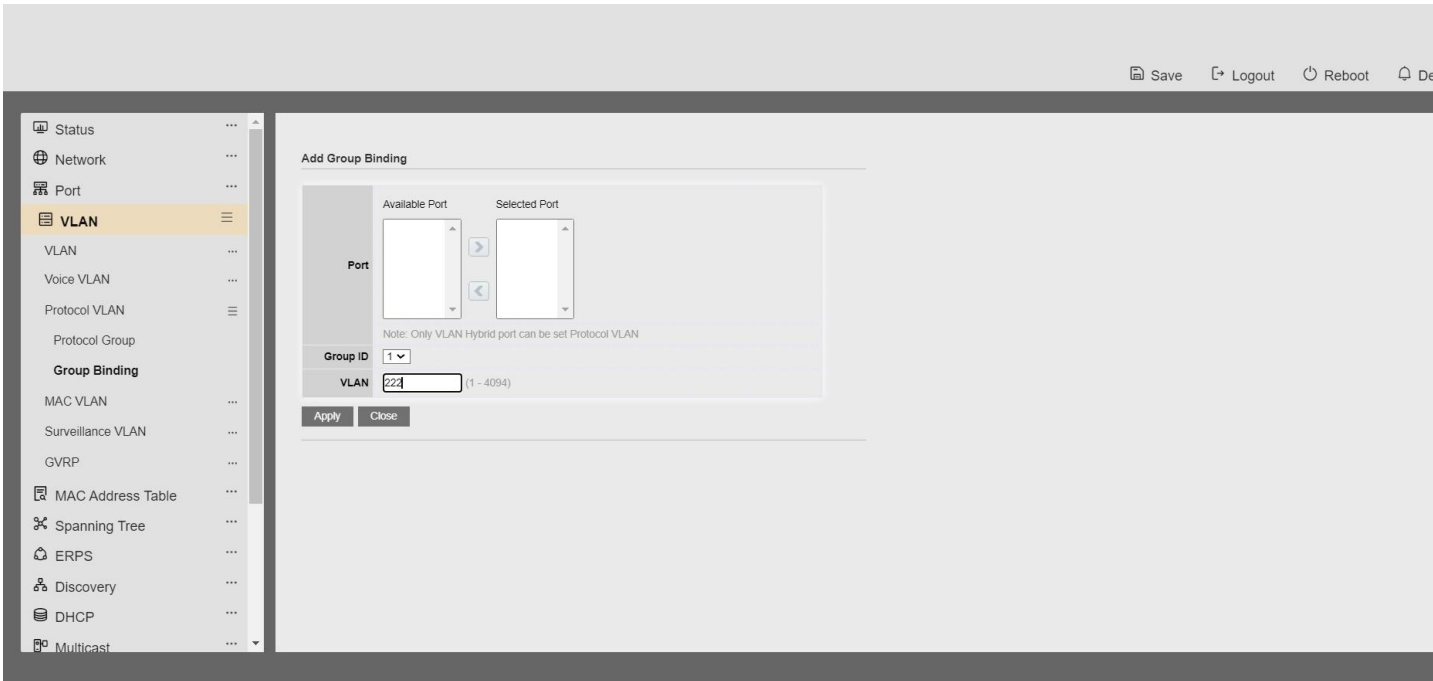


Figure 5-16 Add and Edit Group Binding Dialog

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.

Table 5-16 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.

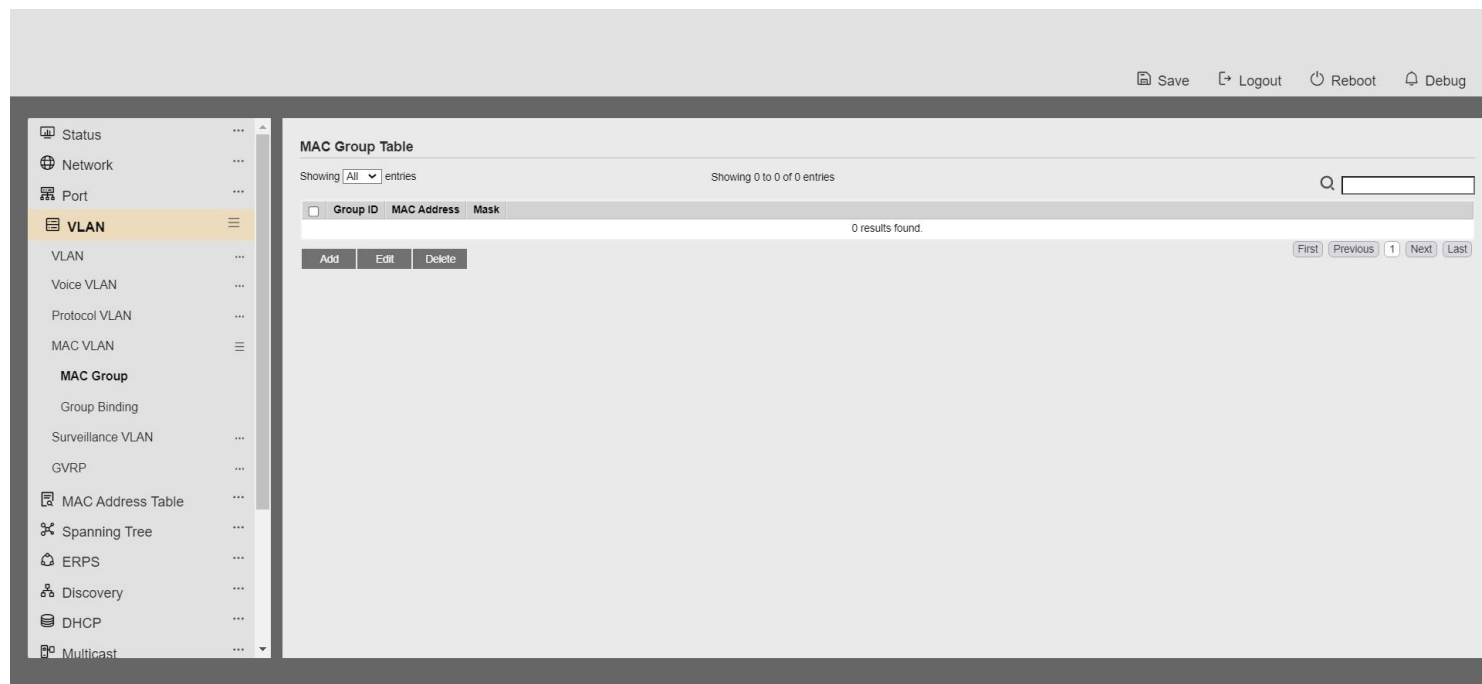


Figure 5-17 MAC Group Page

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.

Table 5-17 MAC Group Fields

Add MAC Group

Group ID	<input type="text"/>	(1 - 2147483647)
MAC Address	<input type="text"/>	(A:B:C:D:E:F)
Mask	<input type="text"/>	(9 - 48)

Apply

Close

Figure 5-18 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.

Table 5-18 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.

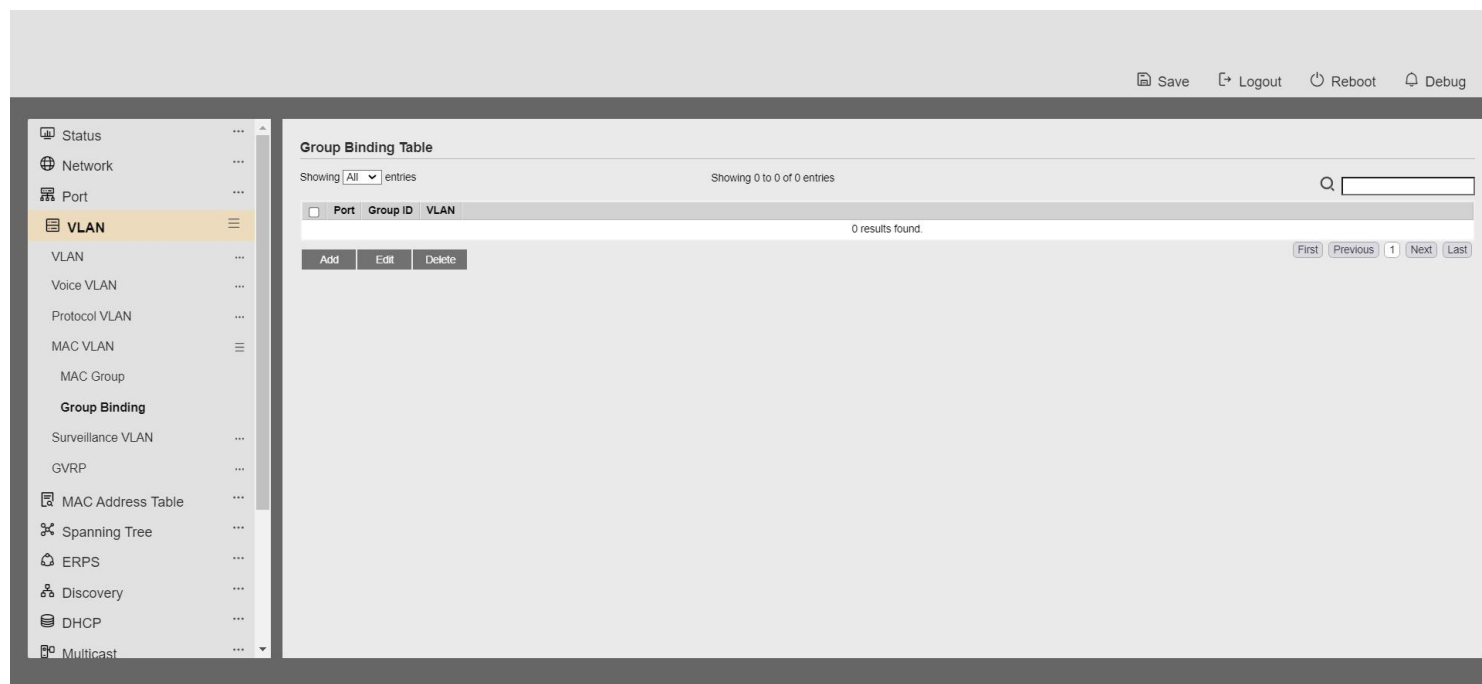


Figure 5-19 Group binding Page

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

Table 5-19 Group Binding Fields

Add Group Binding

Port

Available Port

Selected Port

>

<

Note: Only VLAN Hybrid port can be set MAC VLAN

Group ID

None

VLAN

(1 - 4094)

Apply

Close

Edit Group Binding

Port

GE1

Group ID

1

VLAN

3333

(1 - 4094)

Apply

Close

Figure 5-20 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.

VLAN

5.5. Surveillance

Managed Switch

57

Rev. 1.0

Table 5-20 Group Binding Fields

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.

State

☐ Enable

VLAN

None ▾

CoS / 802.1p
Remarking

☐ Enable

6 ▾

Aging Time

1440

Min (30 - 65536, default 1440)

Apply

Figure 5-21 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.

Table 5-21 Property Fields

Status

...

Network

...

Port

...

VLAN

...

VLAN

...

Voice VLAN

...

Protocol VLAN

...

MAC VLAN

...

MAC Group

...

Group Binding

...

Surveillance VLAN

...

Property

...

Surveillance OUI

...

GVRP

...

MAC Address Table

...

Spanning Tree

...

ERPS

...

Discovery

...

Save

Logout

Reboot

Debug

Entry	Port	State	Mode	QoS Policy	
<input type="checkbox"/>	1	GE1	Disabled	Auto	Video Packet
<input type="checkbox"/>	2	GE2	Disabled	Auto	Video Packet
<input type="checkbox"/>	3	GE3	Disabled	Auto	Video Packet
<input type="checkbox"/>	4	GE4	Disabled	Auto	Video Packet
<input type="checkbox"/>	5	GE5	Disabled	Auto	Video Packet
<input type="checkbox"/>	6	GE6	Disabled	Auto	Video Packet
<input type="checkbox"/>	7	GE7	Disabled	Auto	Video Packet
<input type="checkbox"/>	8	GE8	Disabled	Auto	Video Packet
<input type="checkbox"/>	9	GE9	Disabled	Auto	Video Packet
<input type="checkbox"/>	10	GE10	Disabled	Auto	Video Packet
<input type="checkbox"/>	11	GE11	Disabled	Auto	Video Packet
<input type="checkbox"/>	12	GE12	Disabled	Auto	Video Packet
<input type="checkbox"/>	13	GE13	Disabled	Auto	Video Packet
<input type="checkbox"/>	14	GE14	Disabled	Auto	Video Packet
<input type="checkbox"/>	15	GE15	Disabled	Auto	Video Packet
<input type="checkbox"/>	16	GE16	Disabled	Auto	Video Packet
<input type="checkbox"/>	17	GE17	Disabled	Auto	Video Packet
<input type="checkbox"/>	18	GE18	Disabled	Auto	Video Packet
<input type="checkbox"/>	19	GE19	Disabled	Auto	Video Packet
<input type="checkbox"/>	20	GE20	Disabled	Auto	Video Packet
<input type="checkbox"/>	21	GE21	Disabled	Auto	Video Packet
<input type="checkbox"/>	22	GE22	Disabled	Auto	Video Packet
<input type="checkbox"/>	23	GE23	Disabled	Auto	Video Packet
<input type="checkbox"/>	24	GE24	Disabled	Auto	Video Packet
<input type="checkbox"/>	25	TE1	Disabled	Auto	Video Packet
<input type="checkbox"/>	26	TE2	Disabled	Auto	Video Packet
<input type="checkbox"/>	27	TE3	Disabled	Auto	Video Packet

Figure 5-22 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

Table 5-22 Property Port Fields

VLAN >> Surveillance VLAN >> Property

Edit Port Setting

Port	GE6
State	<input checked="" type="checkbox"/> Enable
Mode	<input checked="" type="radio"/> Auto <input type="radio"/> Manual
QoS Policy	<input checked="" type="radio"/> Video Packet <input type="radio"/> All

Apply Close

Figure 5-23 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 <ul style="list-style-type: none"> • 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.

Table 5-23 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.

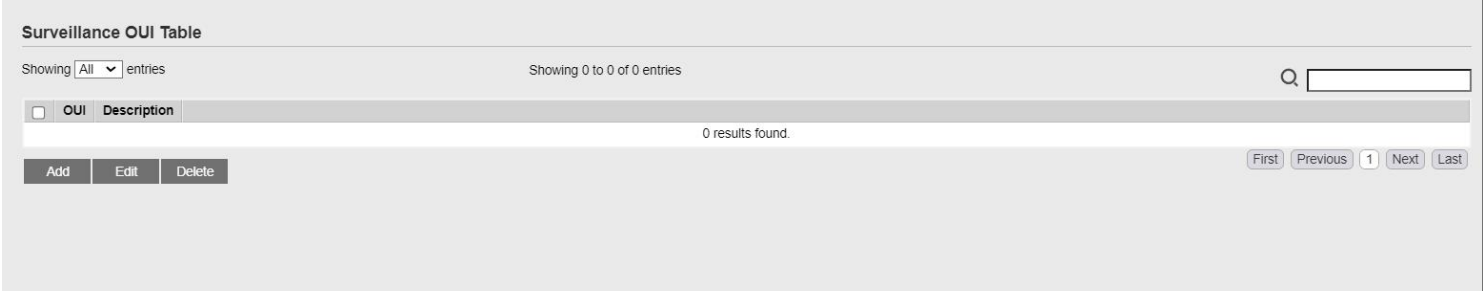


Figure 5-24 Surveillance OUI Page

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

Table 5-24 Surveillance OUI Fields



Figure 5-25 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

Table 5-25 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

Figure 5-26 GVRP Setting Page

Field	Description
State	Set the enabling status of GVRP functionality <ul style="list-style-type: none">• 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.

Table 5-26 GVRP Setting Fields

Port Setting Table					
<div>Q</div>					
<input type="checkbox"/>	Entry	Port	State	VLAN Creation	Registration
<input type="checkbox"/>	1	GE1	Disabled	Enabled	Normal
<input type="checkbox"/>	2	GE2	Disabled	Enabled	Normal
<input type="checkbox"/>	3	GE3	Disabled	Enabled	Normal
<input type="checkbox"/>	4	GE4	Disabled	Enabled	Normal
<input type="checkbox"/>	5	GE5	Disabled	Enabled	Normal
<input type="checkbox"/>	6	GE6	Disabled	Enabled	Normal
<input type="checkbox"/>	7	GE7	Disabled	Enabled	Normal
<input type="checkbox"/>	8	GE8	Disabled	Enabled	Normal
<input type="checkbox"/>	9	GE9	Disabled	Enabled	Normal
<input type="checkbox"/>	10	GE10	Disabled	Enabled	Normal
<input type="checkbox"/>	11	GE11	Disabled	Enabled	Normal
<input type="checkbox"/>	12	GE12	Disabled	Enabled	Normal
<input type="checkbox"/>	13	GE13	Disabled	Enabled	Normal
<input type="checkbox"/>	14	GE14	Disabled	Enabled	Normal
<input type="checkbox"/>	15	GE15	Disabled	Enabled	Normal
<input type="checkbox"/>	16	GE16	Disabled	Enabled	Normal
<input type="checkbox"/>	17	GE17	Disabled	Enabled	Normal
<input type="checkbox"/>	18	GE18	Disabled	Enabled	Normal
<input type="checkbox"/>	19	GE19	Disabled	Enabled	Normal
<input type="checkbox"/>	20	GE20	Disabled	Enabled	Normal
<input type="checkbox"/>	21	GE21	Disabled	Enabled	Normal
<input type="checkbox"/>	22	GE22	Disabled	Enabled	Normal
<input type="checkbox"/>	23	GE23	Disabled	Enabled	Normal
<input type="checkbox"/>	24	GE24	Disabled	Enabled	Normal

Figure 5-27 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

Table 5-27 GVRP port setting Fields

State

☐ Enable

Operational Timeout

Join

cs (2 - 16375, default 20)

Leave

cs (45 - 32760, default 60)

LeaveAll

cs (65 - 32765, default 1000)

Apply

Figure 5-28 GVRP port Setting Edit Page

Field	Description
Port	Display the selected port list
State	Set the enabling status of GVRP port <ul style="list-style-type: none"> Enable: Enable/Disable port of GVRP state.
Vlan Creation	Set the enabling status of GVRP port create VLAN <ul style="list-style-type: none"> Enable: Enable/Disable port create dynamic VLAN.
Register Mode	Set the register mode of GVRP port <ul style="list-style-type: none"> 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

Table 5-28 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.

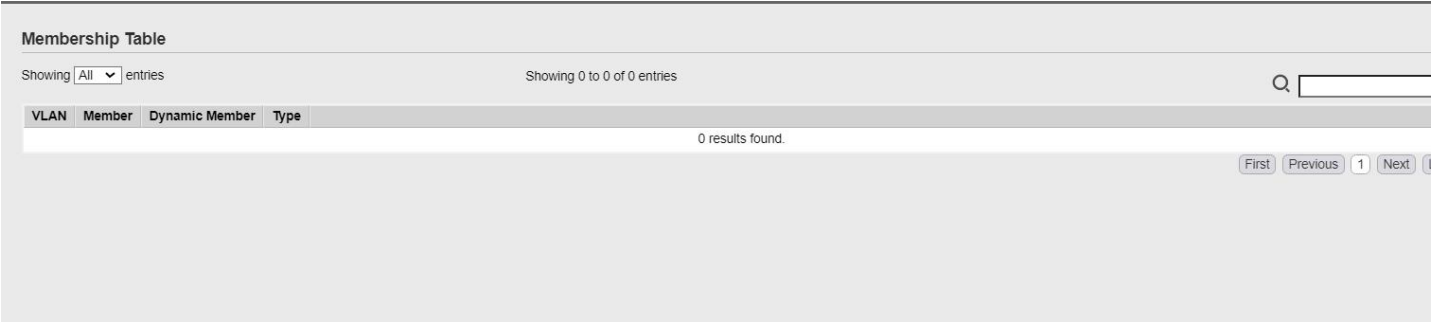


Figure 5-29 GVRP VLAN Information Page

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.

Table 5-29 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.

Port

GE1

Statistics

☒ All

☐ Receive

☐ Transmit

☐ Error

Refresh Rate

☐ None

☐ 5 sec

☒ 10 sec

☐ 30 sec

Clear

Figure 5-30 GVRP Port Statistics Display Setting

Field	Description
Port	Port ID
Statistics	Type of statistics <ul style="list-style-type: none">• 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 <ul style="list-style-type: none">• 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

Table 5-30 GVRP Port Statistics Display Setting Fields

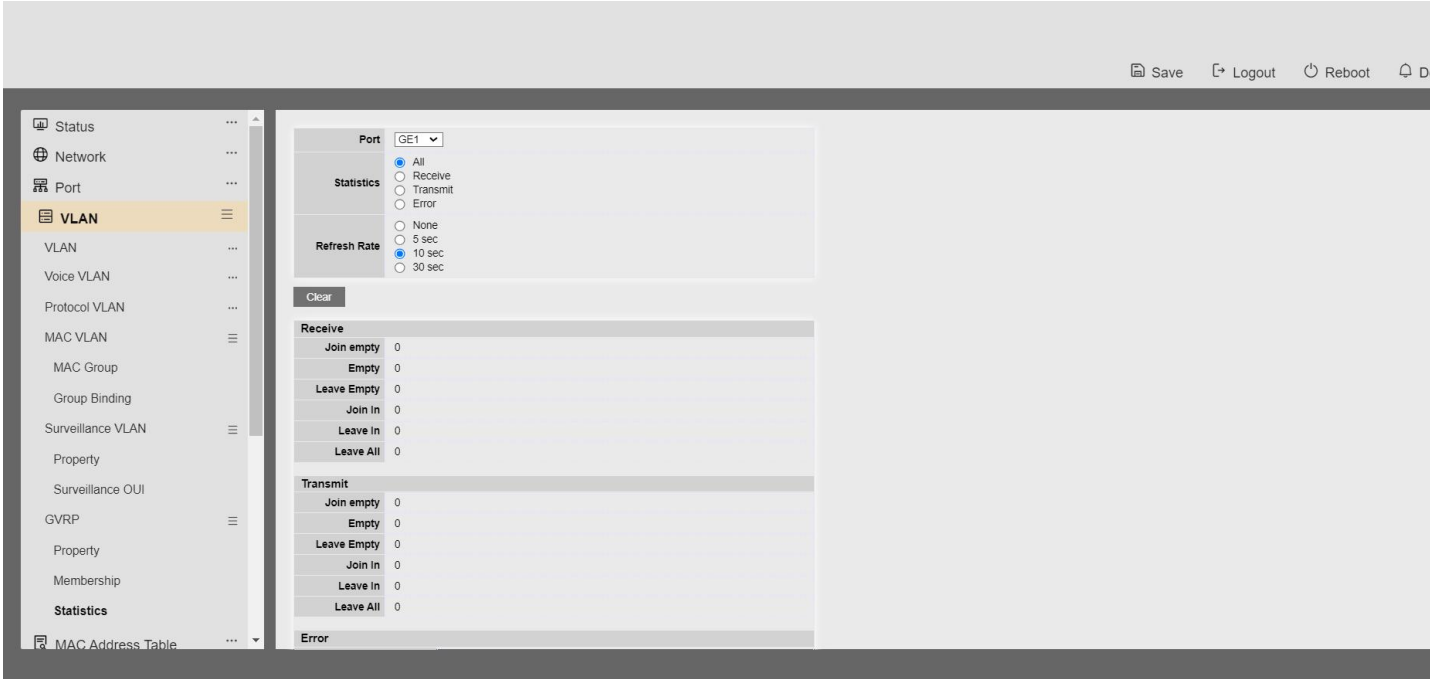


Figure 5-31 GVRP Port Statistics

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.

Table 5-31 GVRP Port Statistics Fields

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**.

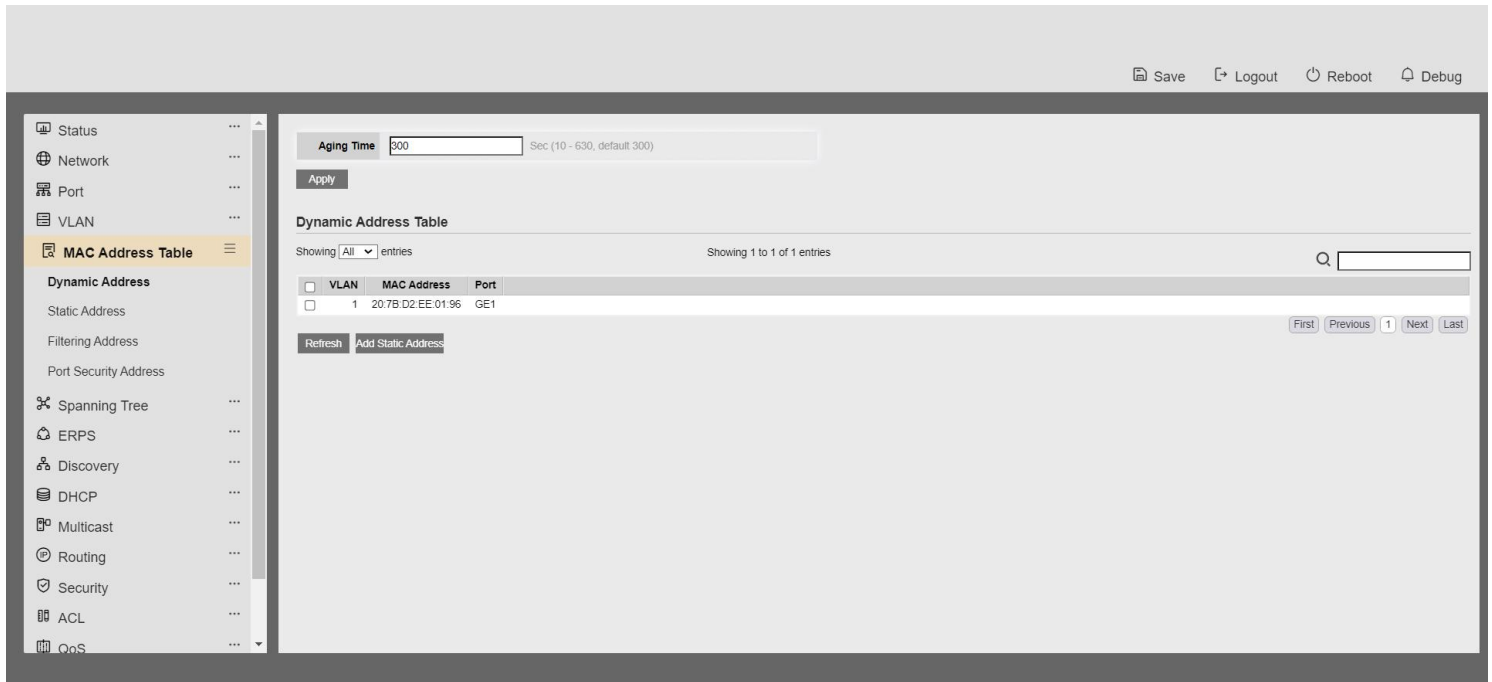


Figure 6-1: Dynamic Address Setting page.

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..

Table 6-1: Dynamic Address Setting fields.

6.2. Static Address

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

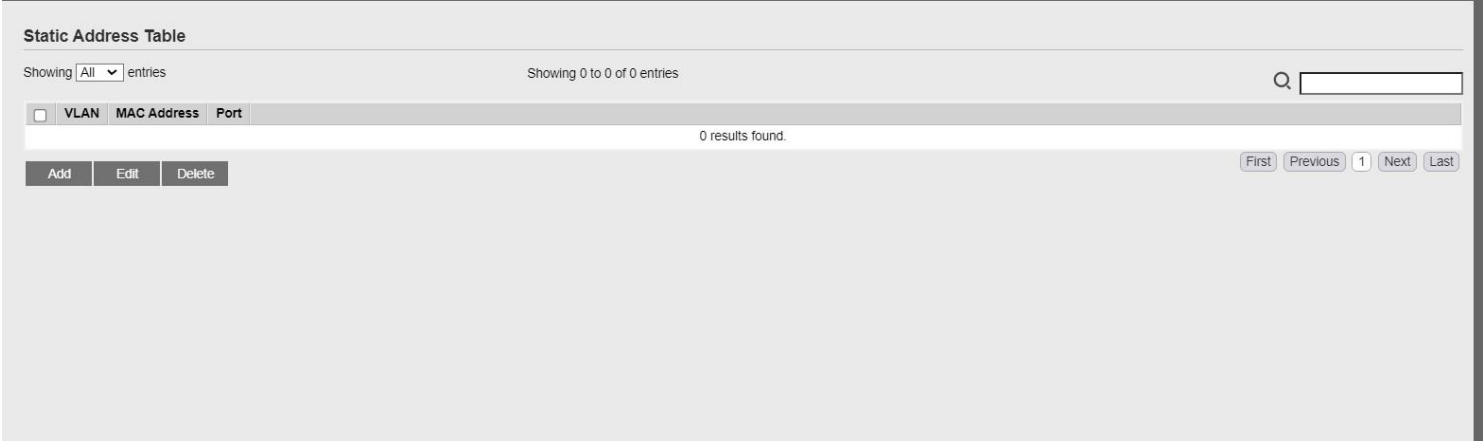


Figure 6-2: Static Address Page.

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.

Table 6-2: Static Address Setting fields.

6.3. Filtering Address

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



Figure 6-3: 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.

7 **ST**
P **Table 6-3: Filtering Address Setting fields.**

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**.

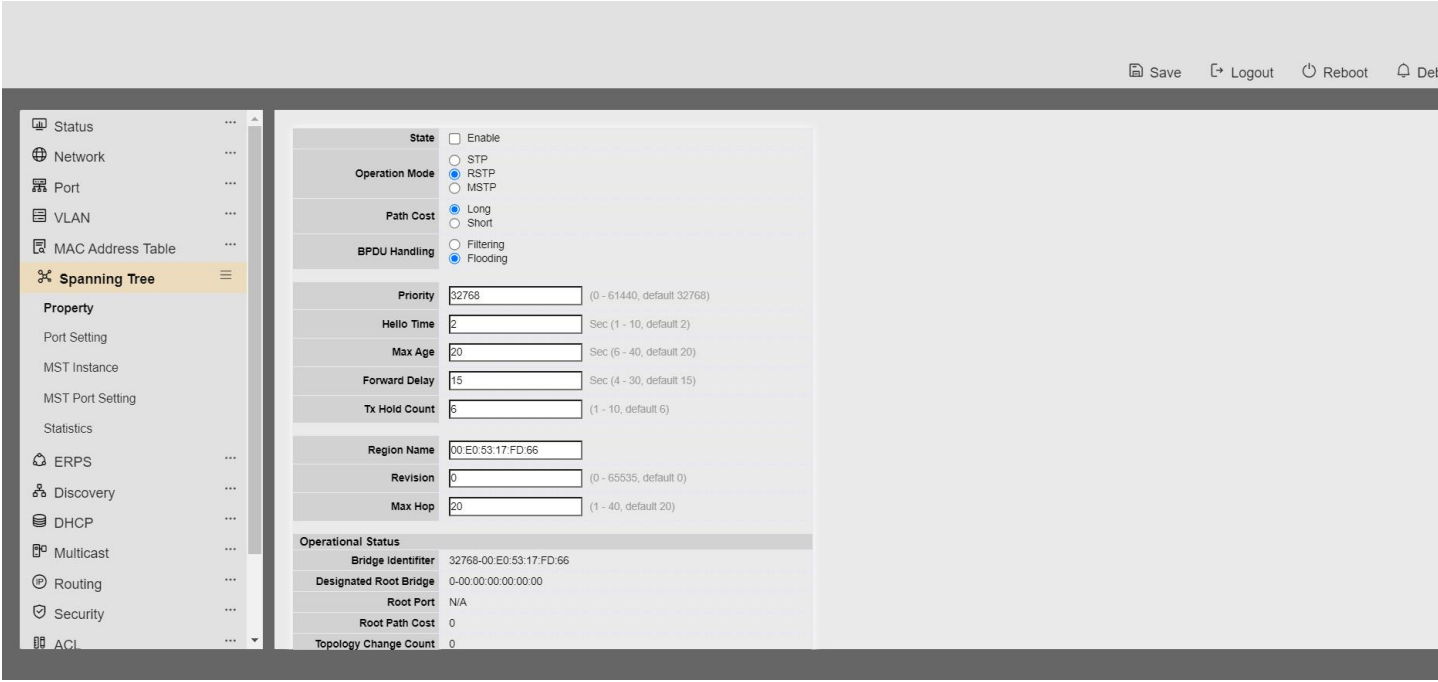


Figure 7-1: STP Property.

Field	Description
State	Enable/Disable the Spanning Tree on the switch.
Operation Mode	Specify the Spanning Tree operation mode. <ul style="list-style-type: none">• STP: Enable the Spanning Tree (STP) operation.

	<ul style="list-style-type: none">• RSTP: Enable the Rapid Spanning Tree (RSTP) operation.• MSTP: Enable the Multiple Spanning Tree (MSTP) operation.
Path Cost	<p>Specify the path cost method.</p> <ul style="list-style-type: none">• 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	<p>Specify the BPDU forward method when the STP is disabled.</p> <ul style="list-style-type: none">• Filtering: Filter the BPDU when STP is disabled.• Flooding: Flood the BPDU when STP is disabled.
Priority	<p>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</p>
Hello Time	<p>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</p>
Max Age	<p>Specify the time interval in seconds for a switch to wait the configuration messages, without attempting to redefine its own configuration.</p>
Forward Delay	<p>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.</p>
TX Hold Count	<p>Specify the tx-hold-count used to limit the maximum numbers of packets transmission per second. The valid range is from 1 to 10.</p>
Region Name	<p>The MSTP instance name. Its maximum length is 32 characters. The default value is the MAC address of the switch.</p>
Revision	<p>The MSTP revision number. Its valid rage is from 0 to 65535.</p>
Max Hops	<p>Specify the number of hops in an MSTP region before the BPDU is discarded. The valid range is 1 to 40.</p>

Table 7-1: STP Property field.

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.

Table 7-2: STP Operational Status field.

7.2. Port Setting

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

Port Setting Table

Q

<input type="checkbox"/>	Entry	Port	State	Path Cost	Priority	BPDU Filter	BPDU Guard	Operational Edge	Operational Point-to-Point	Port Role	Port State	Designated Bridge	Designated Port ID	Designated Cost
<input type="checkbox"/>	1	GE1	Disabled	20000	128	Disabled	Disabled	Disabled	Enabled	Disabled	Forwarding	0-00:00:00:00:00:00	128-1	20000
<input type="checkbox"/>	2	GE2	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-2	20000
<input type="checkbox"/>	3	GE3	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-3	20000
<input type="checkbox"/>	4	GE4	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-4	20000
<input type="checkbox"/>	5	GE5	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-5	20000
<input type="checkbox"/>	6	GE6	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-6	20000
<input type="checkbox"/>	7	GE7	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-7	20000
<input type="checkbox"/>	8	GE8	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-8	20000
<input type="checkbox"/>	9	GE9	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-9	20000
<input type="checkbox"/>	10	GE10	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-10	20000
<input type="checkbox"/>	11	GE11	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-11	20000
<input type="checkbox"/>	12	GE12	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-12	20000
<input type="checkbox"/>	13	GE13	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-13	20000
<input type="checkbox"/>	14	GE14	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-14	20000
<input type="checkbox"/>	15	GE15	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-15	20000
<input type="checkbox"/>	16	GE16	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-16	20000
<input type="checkbox"/>	17	GE17	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-17	20000
<input type="checkbox"/>	18	GE18	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-18	20000
<input type="checkbox"/>	19	GE19	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-19	20000
<input type="checkbox"/>	20	GE20	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-20	20000
<input type="checkbox"/>	21	GE21	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-21	20000
<input type="checkbox"/>	22	GE22	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-22	20000
<input type="checkbox"/>	23	GE23	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-23	20000

Figure 7-2: 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
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

Table 7-3: 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.

Table 7-4: STP Port Setting buttons.

Spanning Tree >> Port Setting

Edit Port Setting

Port	GE1-GE4
State	<input checked="" type="checkbox"/> Enable
Path Cost	<input type="text" value="0"/> (0 - 200000000) (0 = Auto)
Priority	128 ▼
Edge Port	<input type="checkbox"/> Enable
BPDU Filter	<input type="checkbox"/> Enable
BPDU Guard	<input type="checkbox"/> Enable
Point-to-Point	<input checked="" type="radio"/> Auto <input type="radio"/> Enable <input type="radio"/> 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

Figure 7-3: 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. <ul style="list-style-type: none"> • 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.

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



Field	Description
<hr/>	

MST I	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.

Table 7-6: MST Instance fields.

Spanning Tree >> MST Instance

Edit MST Instance Setting

MSTI

1

VLAN

Available VLAN

1
2
3
4
5
6
7
8

Selected VLAN

Priority

(0 - 61440, default 32768)

Bridge Identifier

32768-00:E0:4C:00:00:00

Designated Root Bridge

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

Root Port

Root Path Cost

0

Remaining Hop

0

Apply

Close

Figure 7-5: 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.

Table 7-7: Edit MST Instance fields.

7.4. MST Port Setting

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

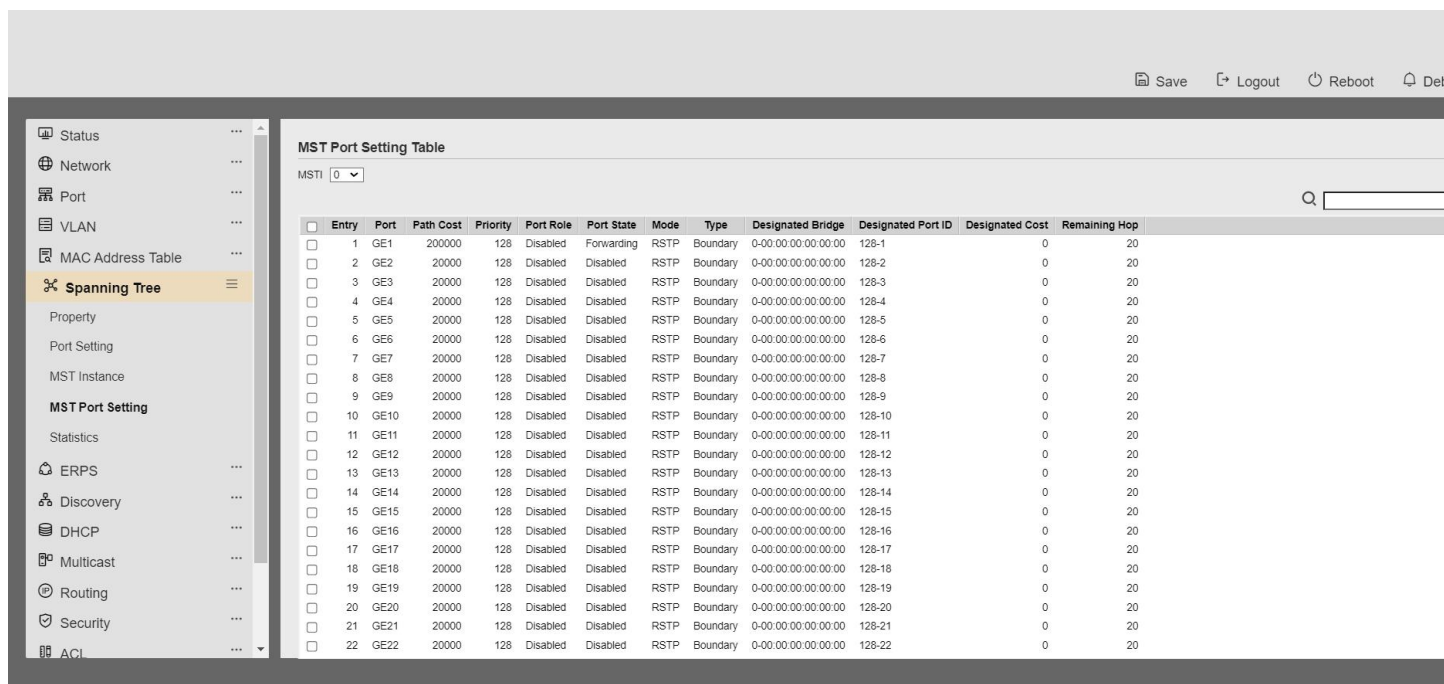


Figure 7-6: MST Port Setting page.

Fiel	Descripti
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: <ul style="list-style-type: none"> • 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.

Table 7-8: MST Port Setting fields.

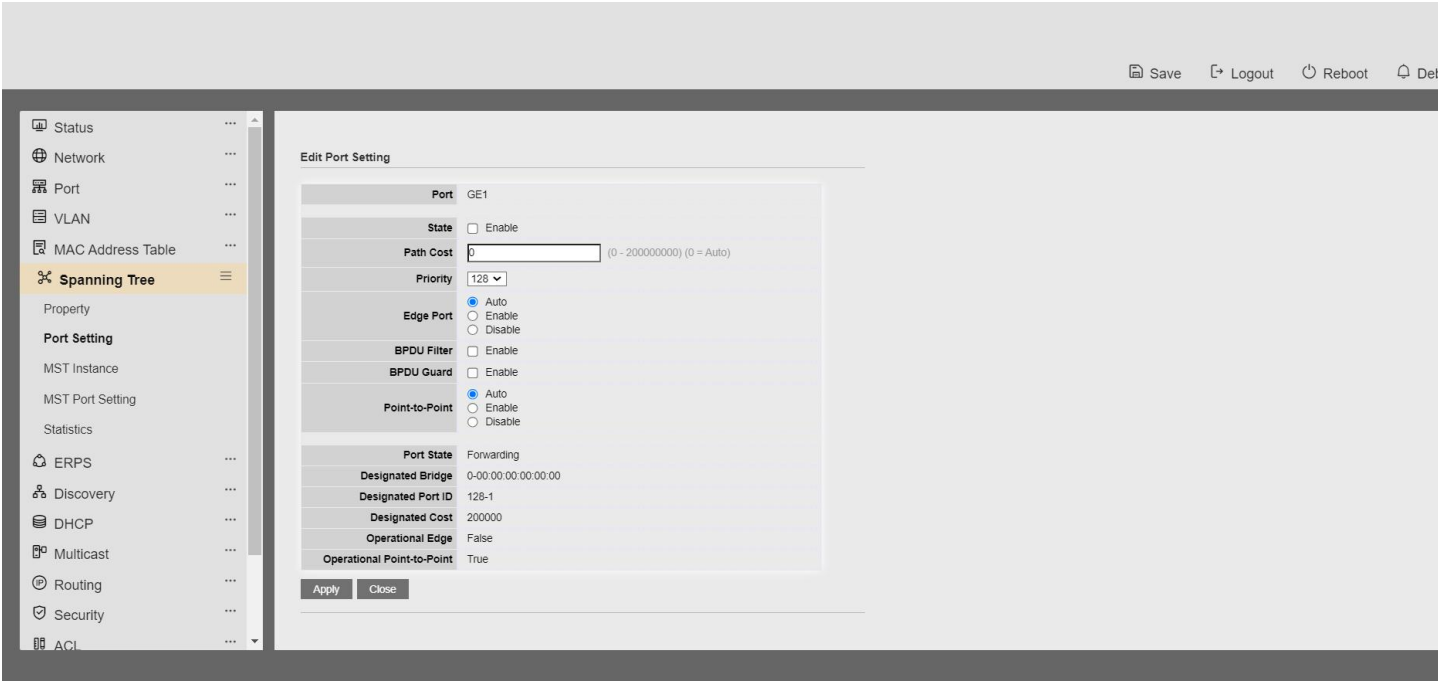


Figure 7-7: Edit MST Port Setting page.

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

Table 7-9: Edit MST Port Setting fields.

7.5. Statistics

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

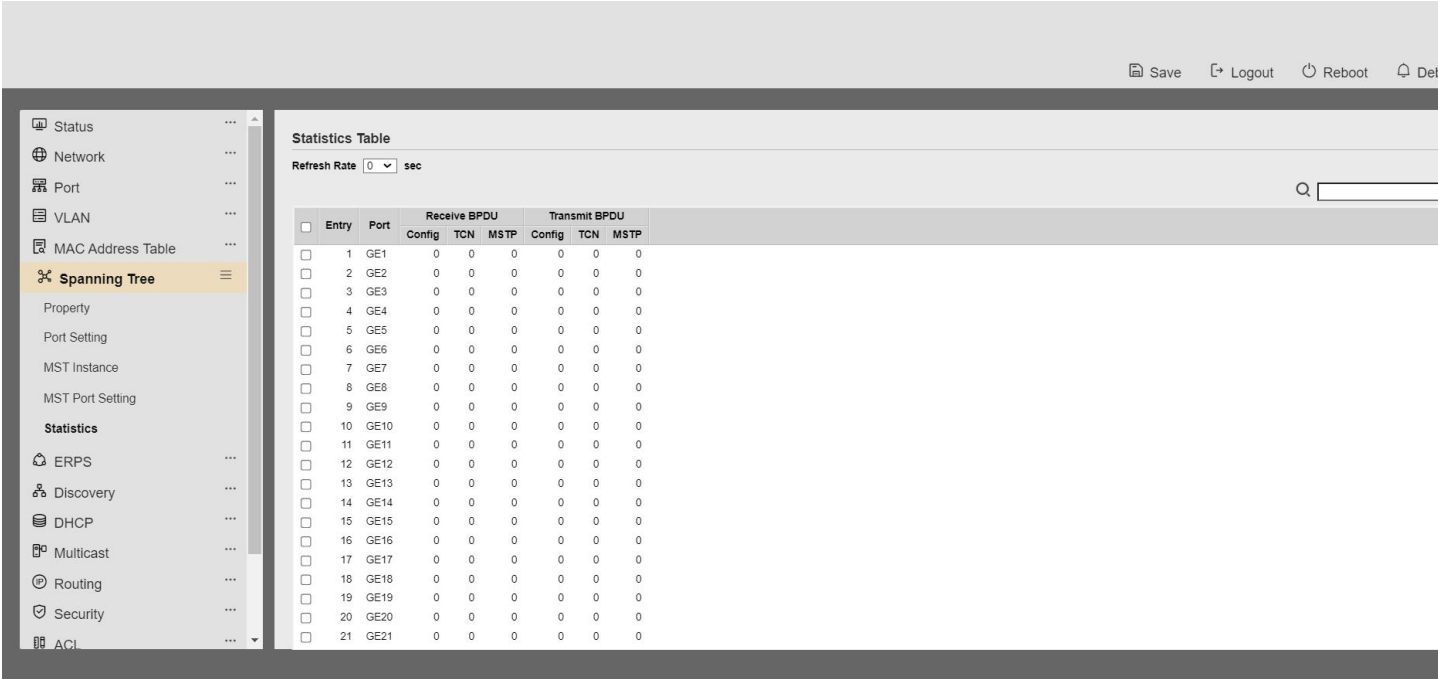


Figure 7-8: STP Statistics page.

Field	Description
Refresh Rate	The option to refresh the statistics automatically.
Receive BPDUs (Config)	The counts of the received CONFIG BPDU.
Receive BPDUs (TCN)	The counts of the received TCN BPDU.
Receive BPDUs	The counts of the received MSTP BPDU.

(MSTP)	
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.

Table 7-10: View STP Statistic fields.

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

Table 7-11: View STP Statistic buttons.

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

Refresh

Clear

Close

Figure 7-9: View STP Port Statistics page.

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

Table 7-12: View STP Port Statistic buttons.

8 Discover

8.1. 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.

8.1.1. Property

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

The screenshot shows the 'LLDP Property Setting' web page. The left sidebar lists various network configuration options, with 'Discovery' and 'LLDP' expanded, and 'Property' selected. The main panel displays the following settings:

- 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)

An 'Apply' button is located at the bottom of the settings panel.

Figure 8-1 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).

Table 8-1 LLDP Property Setting Fields

8.1.2. Port Setting

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

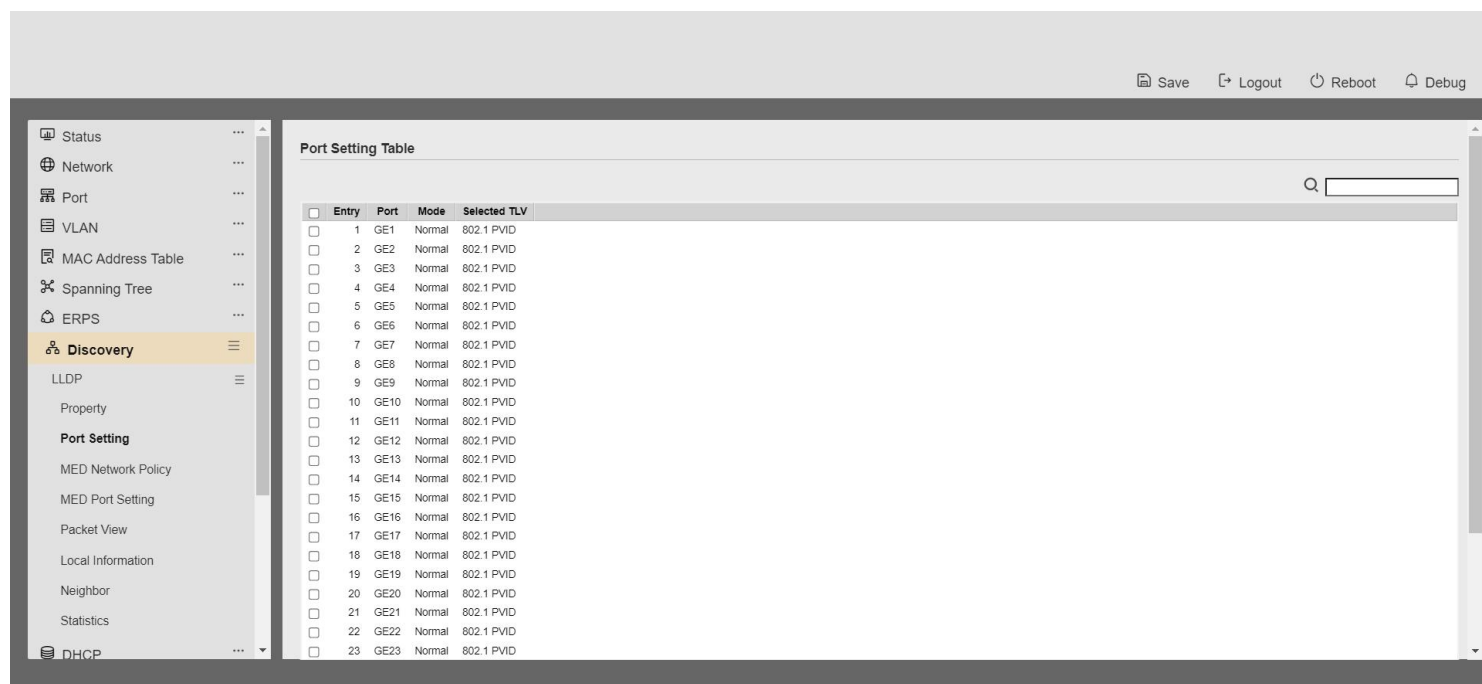


Figure 8-2 LLDP Port Setting Page

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

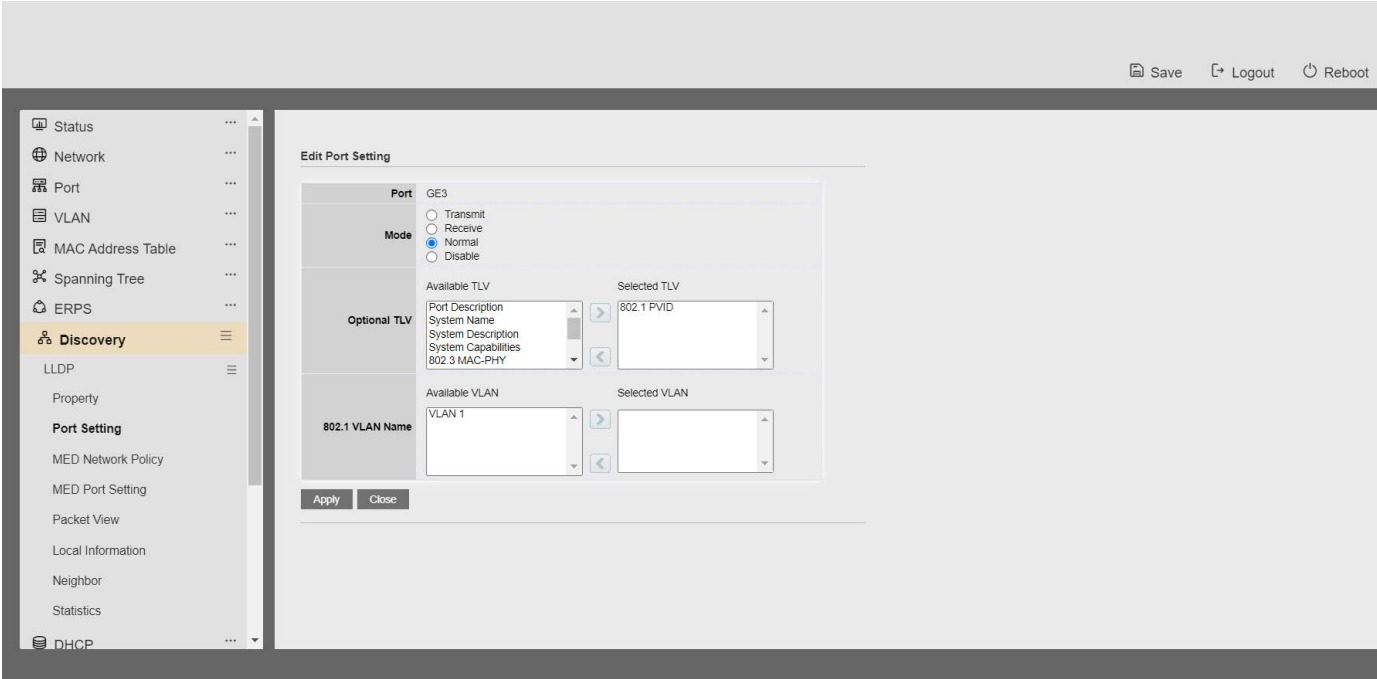


Figure 8-3 LLDP Port Edit Page

Field	Description
Port	Select specified port or all ports to configure LLDP state.
Mode	<p>Select the transmission state of LLDP port interface.</p> <ul style="list-style-type: none"> • 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	<p>Select the LLDP optional TLVs to be carried (multiple selection is allowed).</p> <ul style="list-style-type: none"> • 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).
--------------------	--

Table 8-2 LLDP Port Configuration Fields

8.1.3. MED Network Policy

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



Figure 8-4 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**



Figure 8-5 LLDP MED Network Policy Setting Page

Field	Description
Policy ID	Select specified network policy ID to configure.
Application	Select the network policy application type. <ul style="list-style-type: none">• 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. <ul style="list-style-type: none">• 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

Table 8-3 LLDP MED Network Policy Configuration Fields

8.1.4. MED Port Setting

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

Status

Network

Port

VLAN

MAC Address Table

Spanning Tree

ERPS

Discovery

LLDP

Property

Port Setting

MED Network Policy

MED Port Setting

Packet View

Local Information

Neighbor

Statistics

DHCP

MED Port Setting Table

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

11

GE11

Enabled

Yes

No

No

12

GE12

Enabled

Yes

No

No

13

GE13

Enabled

Yes

No

No

14

GE14

Enabled

Yes

No

No

15

GE15

Enabled

Yes

No

No

16

GE16

Enabled

Yes

No

No

17

GE17

Enabled

Yes

No

No

18

GE18

Enabled

Yes

No

No

19

GE19

Enabled

Yes

No

No

20

GE20

Enabled

Yes

No

No

21

GE21

Enabled

Yes

No

No

22

GE22

Enabled

Yes

No

No

Figure 8-6 LLDP MED Setting Page

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

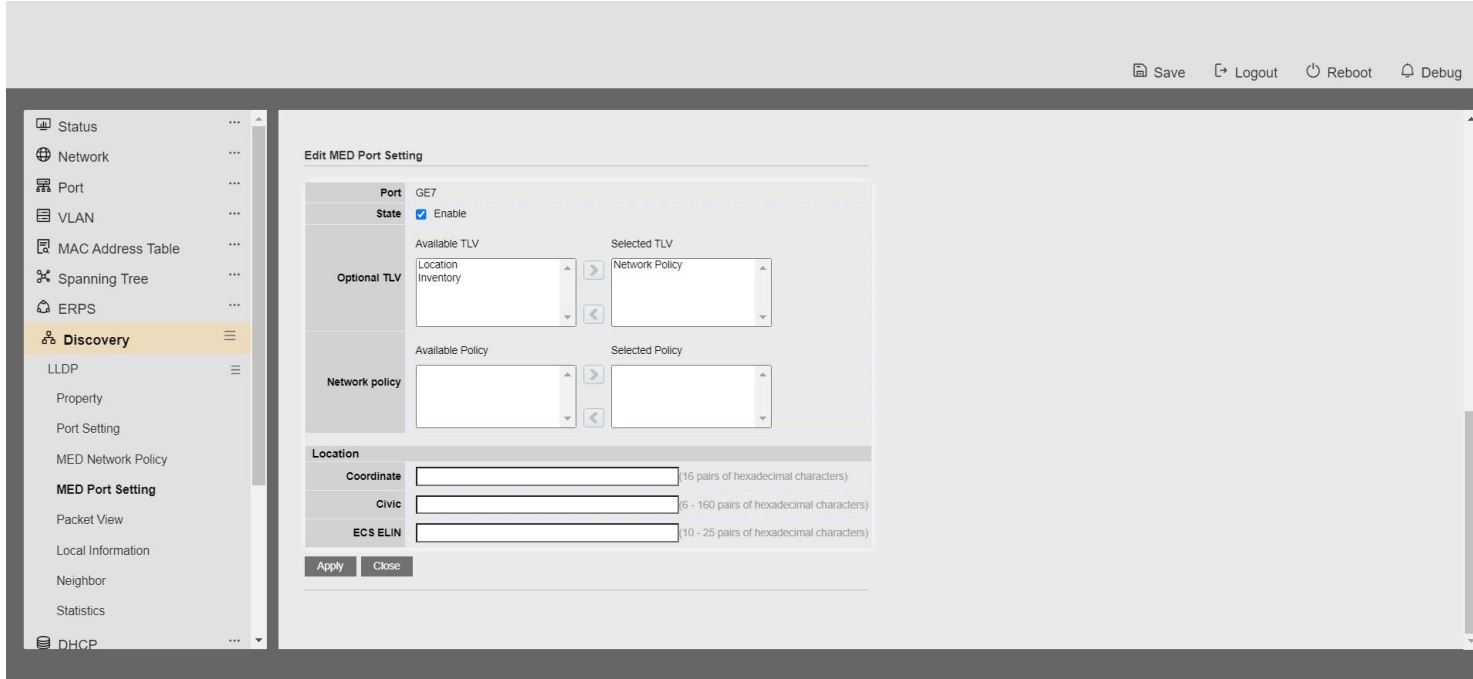


Figure 8-7 LLDP MED Add/Edit Page

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) <ul style="list-style-type: none"> 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.

Table 1-4 LLDP MED Port Configuration Fields

Field	Description
Coordinate	Set Coordinate
Civic	Set Civic
ECS ELIN	Set ECS ELIN

Table 8-4 LLDP MED Port Location Configuration Fields

8.1.5. Packet View

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

The screenshot displays the 'Packet View Table' in the Web User Interface. The table has five columns: Entry, Port, In-Use (Bytes), Available (Bytes), and Operational Status. It lists 23 entries for ports GE1 through GE23. All entries show 'Not Overloading' status. The left sidebar shows the navigation menu with 'Discovery' and 'LLDP' selected. The top right of the interface shows 'Save', 'Logout', 'Reboot', and 'Debug' buttons.

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
11	GE11	39	1449	Not Overloading
12	GE12	39	1449	Not Overloading
13	GE13	39	1449	Not Overloading
14	GE14	39	1449	Not Overloading
15	GE15	39	1449	Not Overloading
16	GE16	39	1449	Not Overloading
17	GE17	39	1449	Not Overloading
18	GE18	39	1449	Not Overloading
19	GE19	39	1449	Not Overloading
20	GE20	39	1449	Not Overloading
21	GE21	39	1449	Not Overloading
22	GE22	39	1449	Not Overloading
23	GE23	39	1449	Not Overloading

Figure 8-8 LLDP Overloading Page

Field	Description
Port	Port Name
In-Use (Bytes)	Total number of bytes of LLDP information in each packet.
Available	Total number of available bytes left for additional LLDP

(Bytes)

information in each packet.

Operational Status

Overloading or not

Table 8-5 LLDP Overloading Fields

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

Packet View Detail

PortGE1

Mandatory TLVs

Size (Bytes)21

Operational StatusTransmitted

MED Capabilities

Size (Bytes)9

Operational StatusTransmitted

MED Location

Size (Bytes)0

Operational StatusTransmitted

MED Network Policy

Size (Bytes)0

Operational StatusTransmitted

MED Inventory

Size (Bytes)0

Operational StatusTransmitted

MED Extended Power via MDI

Size (Bytes)0

Operational StatusTransmitted

Size (Bytes)0

Operational StatusTransmitted

MED Inventory

Size (Bytes)0

Operational StatusTransmitted

MED Extended Power via MDI

Size (Bytes)0

Operational StatusTransmitted

802.3 TLVs

Size (Bytes)0

Operational StatusTransmitted

Optional TLVs

Size (Bytes)0

Operational StatusTransmitted

802.1 TLVs

Size (Bytes)8

Operational StatusTransmitted

Total

In-Use (Bytes)38

Available (Bytes)1450

Close

Managed Switch

87

Rev. 1.0

Figure 8-9 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.

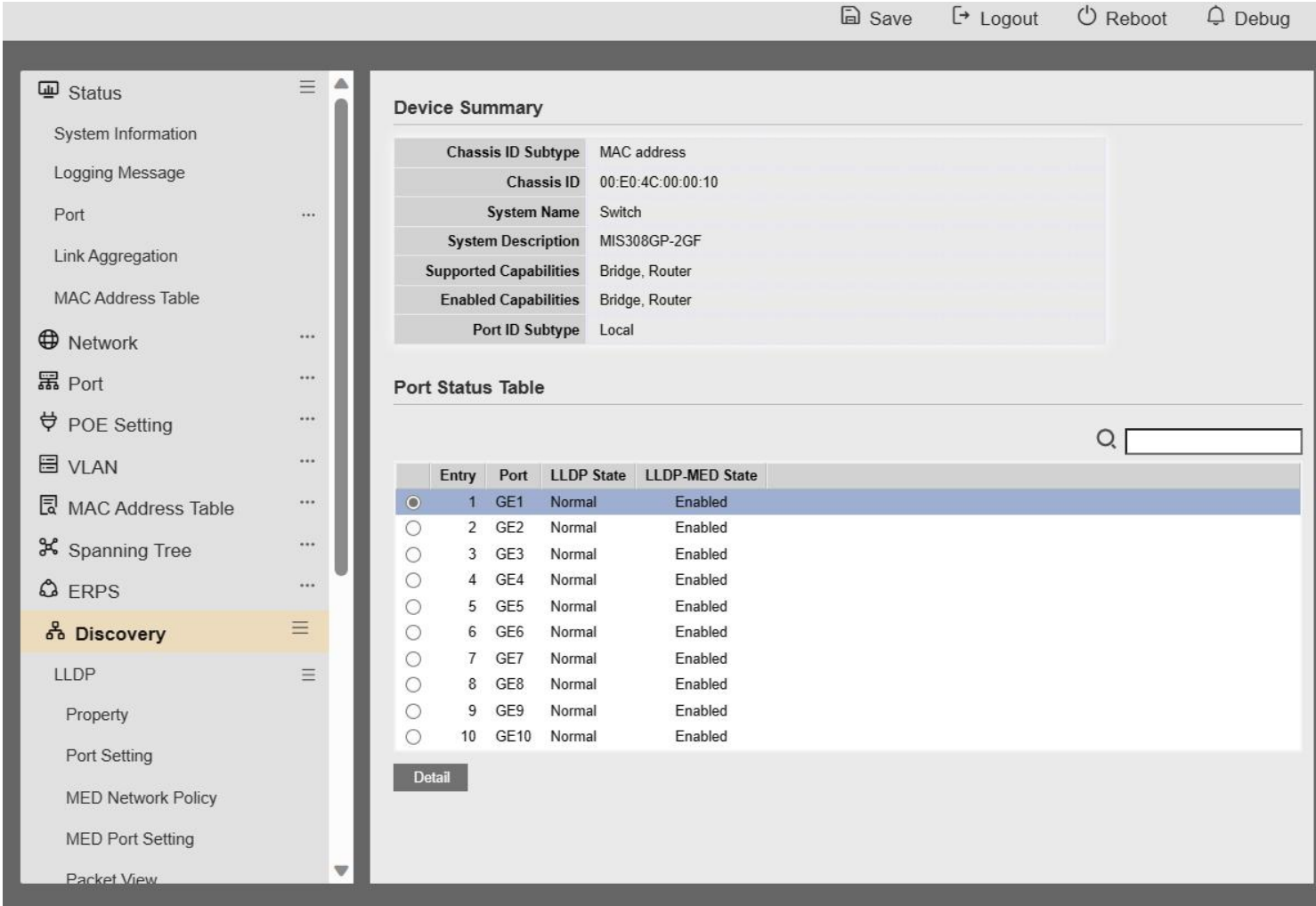
802.1 TLVs	Total 802.1 TLVs byte size. Status is sent or overloading.
Total	Total number of bytes of LLDP information in each packet.

Table 8-6 LLDP Overloading Detial Fields

8.1.6. Local Information

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

Information.



Use the LLDP Local Information to view LLDP local device

information.

Local Information Detail	
Chassis ID Subtype	MAC address
Chassis ID	00:E0:53:17:FD:66
System Name	Switch
System Description	XW9000-GW24GE4TF
Supported Capabilities	Bridge, Router
Enabled Capabilities	Bridge, Router
Port ID	GE1
Port ID Subtype	Local
Port Description	

Figure 8-10 LLDP Local Information Page

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.

Table 8-7 LLDP Local Information Fields

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

Device Summary

Chassis ID Subtype	MAC address
Chassis ID	00:E0:4C:00:00:10
System Name	Switch
System Description	MIS308GP-2GF
Supported Capabilities	Bridge, Router
Enabled Capabilities	Bridge, Router
Port ID Subtype	Local

Port Status Table

Q

	Entry	Port	LLDP State	LLDP-MED State
<input type="radio"/>	1	GE1	Normal	Enabled
<input type="radio"/>	2	GE2	Normal	Enabled
<input type="radio"/>	3	GE3	Normal	Enabled
<input type="radio"/>	4	GE4	Normal	Enabled
<input type="radio"/>	5	GE5	Normal	Enabled
<input type="radio"/>	6	GE6	Normal	Enabled
<input type="radio"/>	7	GE7	Normal	Enabled
<input type="radio"/>	8	GE8	Normal	Enabled
<input type="radio"/>	9	GE9	Normal	Enabled
<input type="radio"/>	10	GE10	Normal	Enabled

Detail

MED Detail				
Capabilities Supported	Capabilities , Network policy			
Current Capabilities	Capabilities , Network policy			
Device Class	Network Connectivity			
PoE Device Type	N/A			
PoE Power Source	N/A			
PoE Power Priority	N/A			
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				

Figure 8-11 LLDP Local Information Detail Page

8.1.7. Neighbor

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

Neighbor. Use the LLDP Neighbor page to view LLDP

neighbors information.

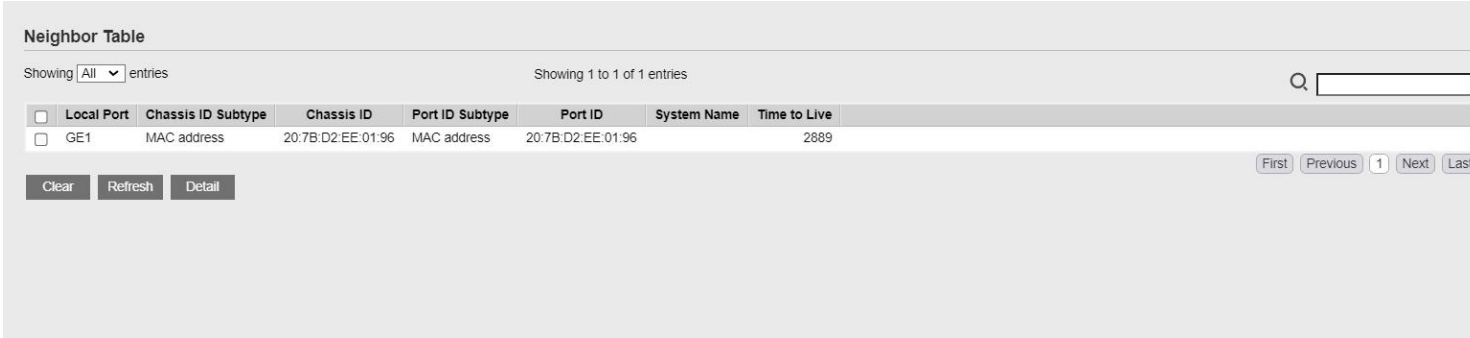


Figure 8-12 LLDP Neighbor Page

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.

Table 8-8 LLDP Neighbor Fields

Click “detail” to view selected neighbor detail information.

8.1.8. 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.

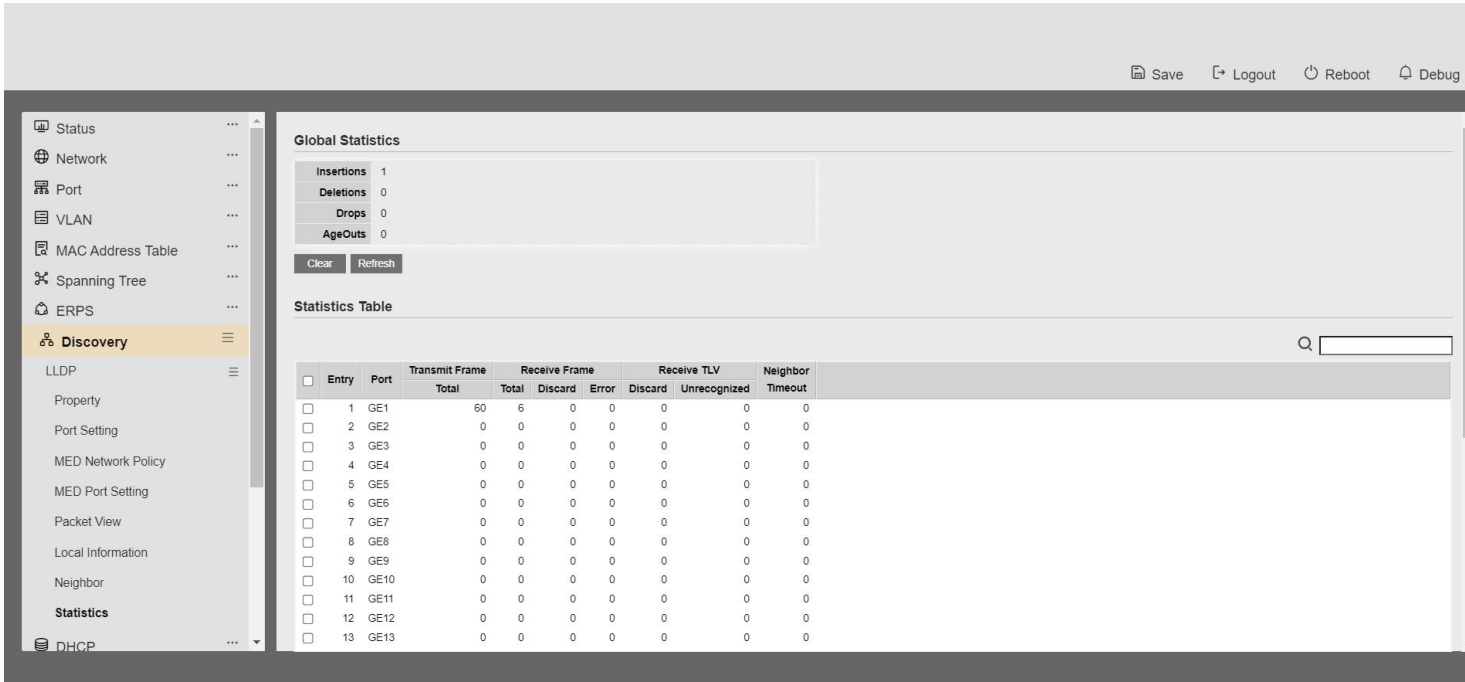


Figure 8-14 LLDP Statistics Page

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
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.

st

9 Multica

Table 8-9 LLDP Statistics Fields

9.1. General

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

9.1.1. 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.

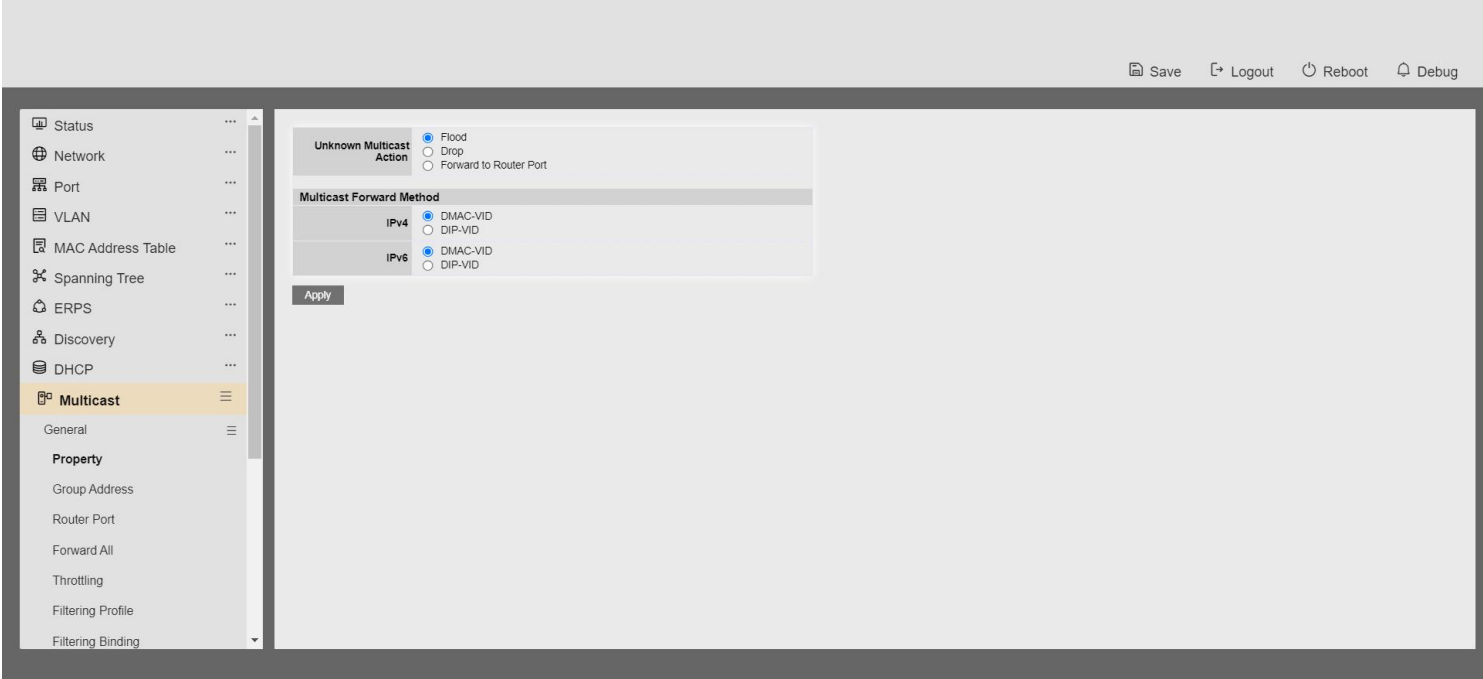


Figure 9-1 Multicast General Properties Page

Field	Description
Unknown Multicast Action	Set the unknown multicast action <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • MAC-VID: forward method dmac+vid. • DIP-VID: forward method dip+vid.
IPv6	Set the ipv6 multicast forward method. <ul style="list-style-type: none"> • MAC-VID: forward method dmac+vid. • DIP-VID: forward method dip+vid(dip is ipv6 low 32 bit).

Table 9-1 Multicast General Property Setting Fields

9.1.2. 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.

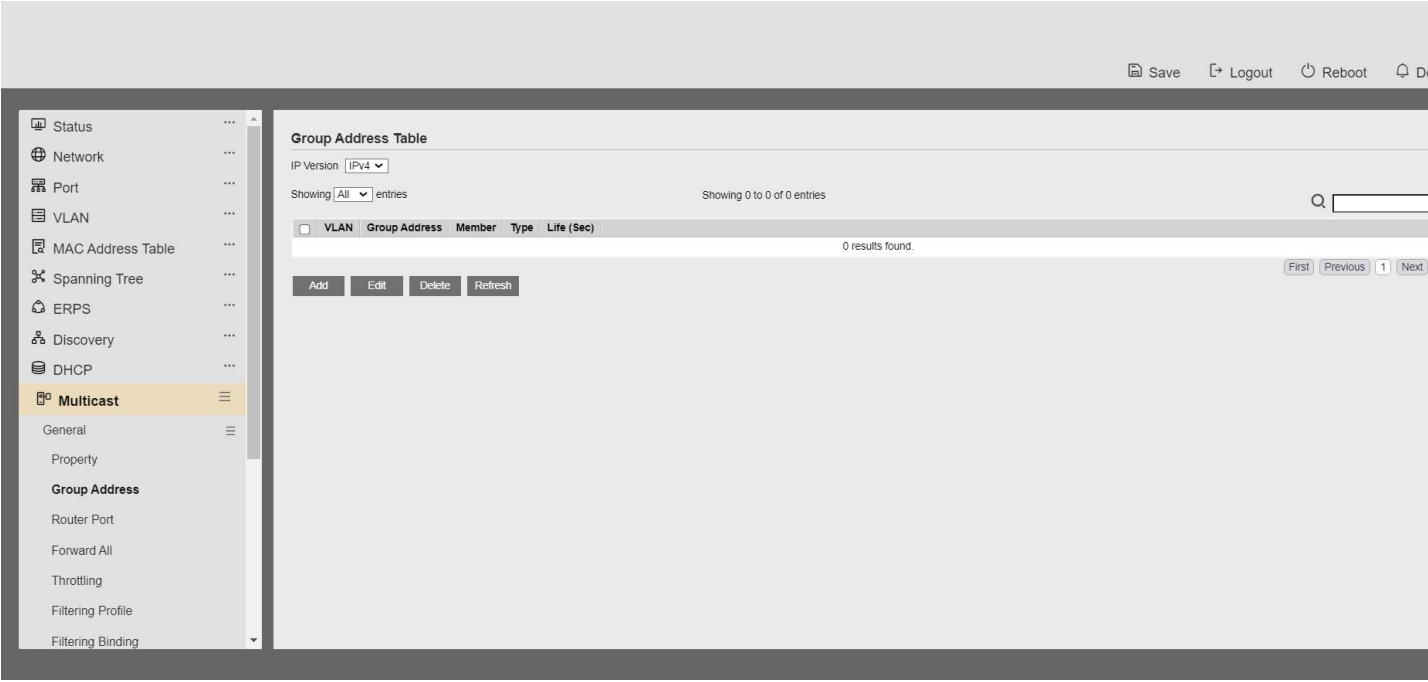


Figure 9-2 Multicast Group Address Table Page

Field	Description
IP Version	IP Version <ul style="list-style-type: none">• 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.

Table 9-2 Multicast Group Address Table Fields

Add Group Address

VLAN

1

IP Version

IPv4

Group Address

Member

Available Port

GE1

GE2

GE3

GE4

GE5

GE6

GE7

GE8

Selected Port

Apply

Close

Figure 9-3 Multicast Group Address Add Page

Field	Description
VLAN	The VLAN ID of group.
IP Version	IP Version <ul style="list-style-type: none"> IPv4: ipv4 multicast group IPv6: ipv6 multicast group
Group Address	The group IP address.
Member	The member ports of group. <ul style="list-style-type: none"> Available Port: Optional port member Selected Port: Selected port member

Table 9-3 Multicast Group Address Add Fields

Figure 9-4 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. <ul style="list-style-type: none">• Available Port: Optional port member• Selected Port: Selected port member

Table 9-4 Multicast Group Address Edit Fields

9.1.3. 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.

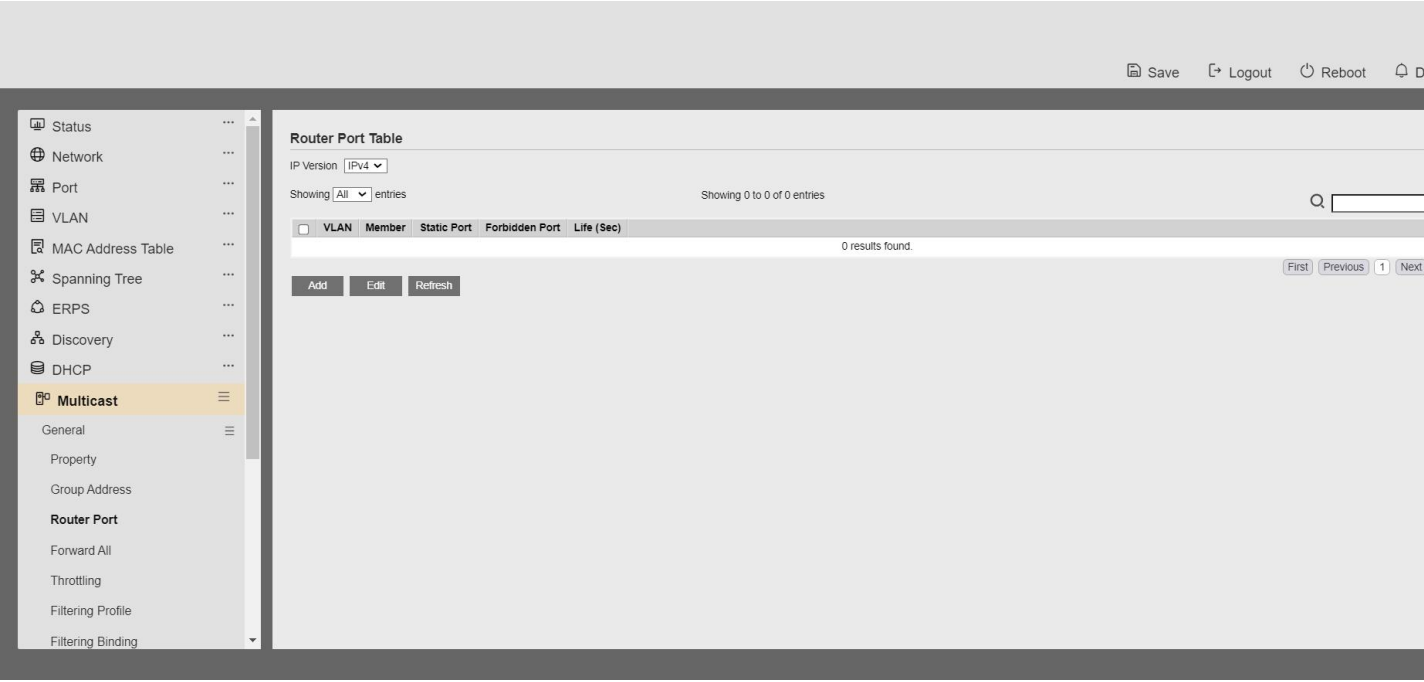


Figure 9-5 Multicast Router Table Page

Field	Description
IP Version	IP Version <ul style="list-style-type: none"> 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.

Table 9-5 Multicast Router Table Fields

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

Figure 9-6 Multicast Router Add Page

Field	Description
VLAN	<div>The VLAN ID for router entry</div> <ul style="list-style-type: none">• Available VLAN: Optional VLAN member• Selected VLAN: Selected VLAN member
IP Version	<div>IP Version</div> <ul style="list-style-type: none">• IPv4: ipv4 multicast router• IPv6: ipv6 multicast router
Type	<div>The router port type</div> <ul style="list-style-type: none">• 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

Table 9-6 Multicast Router Add Fields

Edit Router Port

VLAN	1
IP Version	IPv4
Type	<input checked="" type="radio"/> Static <input type="radio"/> Forbidden
Port	<div>Available Port</div> <div>GE4 GE5 GE6 GE7 GE8 GE9 GE10 LAG1</div> <div>Selected Port</div> <div>GE1 GE2 GE3</div>

Figure 9-7 Multicast Router Edit Page

Field	Description
VLAN	VLAN ID of Selected router entry
IP Version	Selected IP version
Type	The router port type <ul style="list-style-type: none">• 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. <ul style="list-style-type: none">• Available Port: Optional router port member• Selected Port: Selected router port member

Table 9-7 Multicast Router Edit Fields

9.1.4. 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.

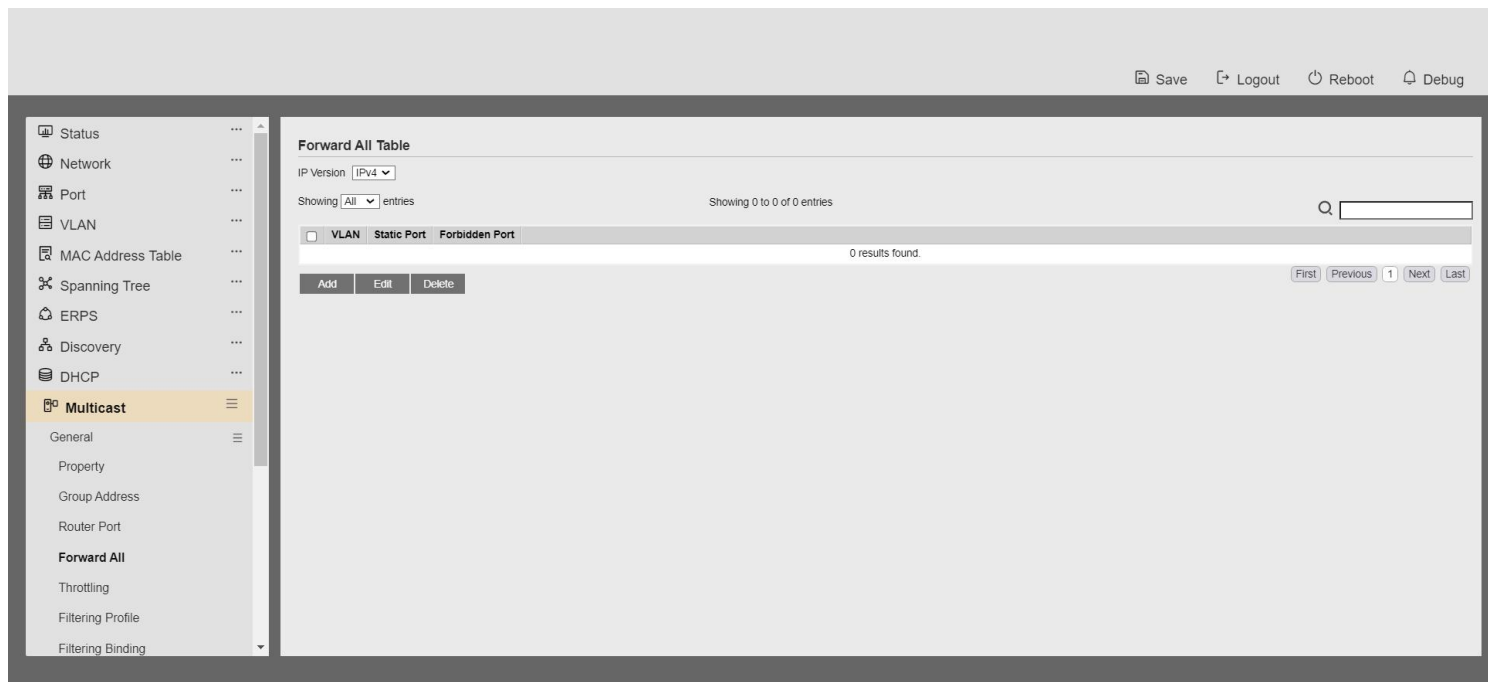


Figure 9-8 Multicast Forward All Table Page

Field	Description
IP Version	IP Version <ul style="list-style-type: none">• 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

Table 9-8 Multicast Forward All Table Fields

Add Forward All

VLAN

Available VLAN

1

2

>

<

Selected VLAN

IP Version

IPv4 ▾

Type

☒ Static

☐ Forbidden

Port

Available Port

GE1

GE2

GE3

GE4

GE5

GE6

GE7

GE8

>

<

Selected Port

Apply

Close

Figure 9-9 Multicast Forward All Add Page

Field	Description
VLAN	The VLAN ID for forward all entry <ul style="list-style-type: none">• Available VLAN: Optional VLAN member• Selected VLAN: Selected VLAN member
IP Version	IP Version <ul style="list-style-type: none">• IPv4: ipv4 multicast forward all• IPv6: ipv6 multicast forward all
Type	The forward all port type <ul style="list-style-type: none">• Static: static forward all port• Forbidden: forbidden forward all port
Port	The member ports of router entry. <ul style="list-style-type: none">• Available Port: Optional router port member• Selected Port: Selected router port member

Table 9-9 Multicast Forward All Add Fields

Edit Forward All

VLAN

2

IP Version

IPv4

Type

Static

Forbidden

Port

Available Port

GE1

GE3

GE4

GE5

GE6

GE7

GE8

GE9

>

<

Selected Port

GE2

Apply

Close

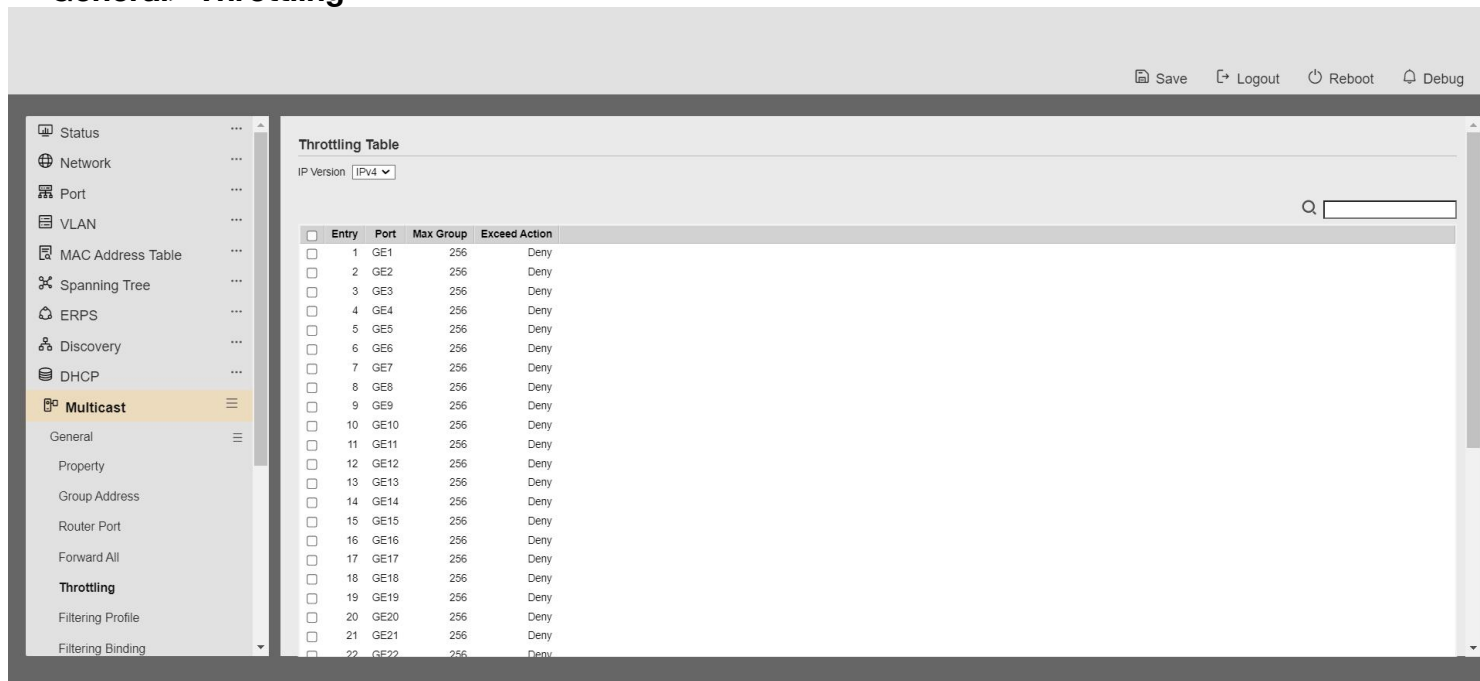
Figure 9-10 Multicast Forward All Edit Page

Field	Description
VLAN	VLAN ID of Selected forward all entry
IP Version	Selected IP version
Type	The forward all port type <ul style="list-style-type: none">• Static: static forward all port• Forbidden: forbidden forward all port
Port	The member ports of forward all entry for selected port type. <ul style="list-style-type: none">• Available Port: Optional router port member• Selected Port: Selected router port member

Table 9-10 Multicast Forward All Edit Fields

9.1.5. 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

Figure 9-11 Multicast Throttling Table Page

Field	Description
IP Version	IP Version <ul style="list-style-type: none"> • 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
---------------	--

Table 9-11 Multicast Throttling Table Fields

Edit Throttling

Port

GE1

IP Version

IPv4

Max Group

256

(0 - 256)

Exceed Action

☒ Deny

☐ Replace

Apply

Close

Figure 9-12 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 <ul style="list-style-type: none">Deny: do not learning group.Replace: random replace one exist group

Table 9-12 Multicast Throttling Table Edit Fields

9.1.6. 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.

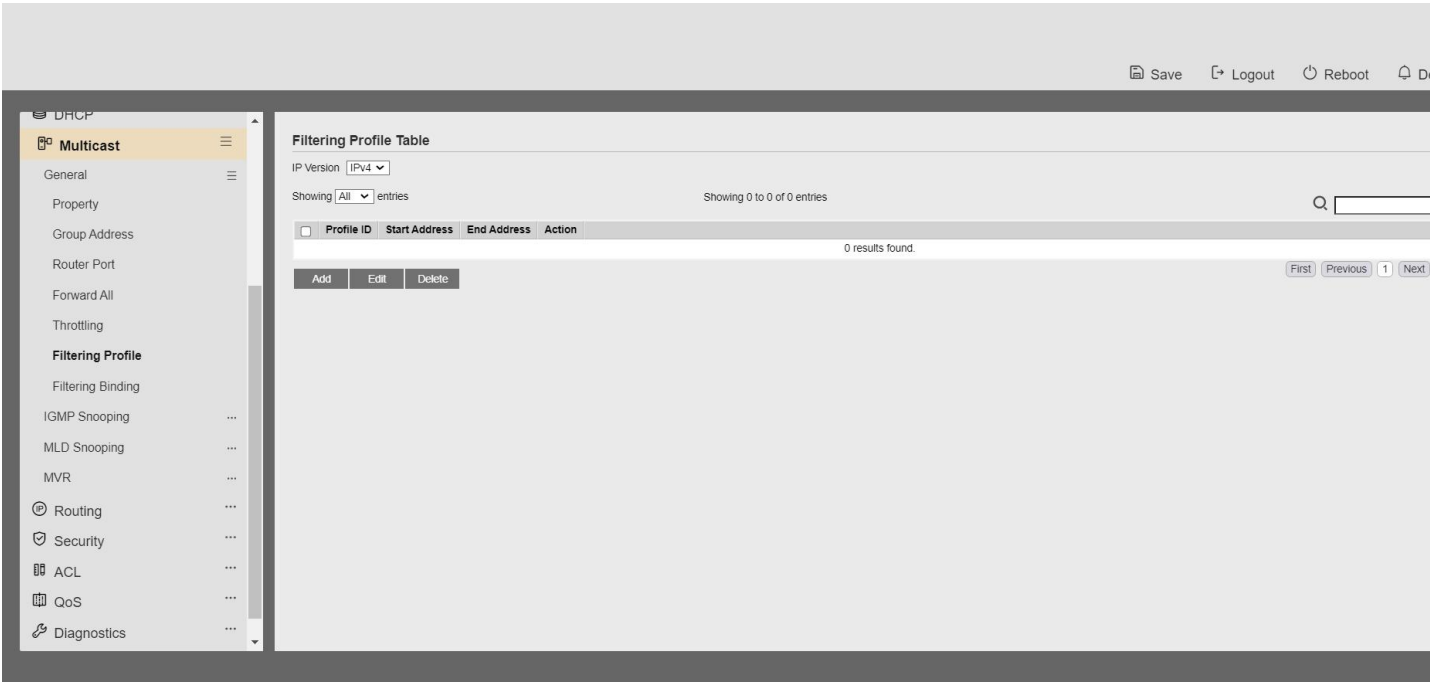


Figure 9-13 Multicast Profile Table Page

Field	Description
IP Version	IP version: <ul style="list-style-type: none">IPv4: IGMP snooping profileIPv6: 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

Table 9-13 Multicast Profile Table Fields

Add Profile

Profile ID	<input type="text"/>	(1 - 128)
IP Version	IPv4 ▾	
Start Address	<input type="text"/>	
End Address	<input type="text"/>	
Action	<input checked="" type="radio"/> Allow <input type="radio"/> Deny	

Apply

Close

Figure 9-14 Multicast Profile Add Page

Field	Description
Profile ID	Profile ID
IP Version	IP version: <ul style="list-style-type: none">• 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: <ul style="list-style-type: none">• Allow: permit all packets that match the profile.• Deny: deny all packets that match the profile.

Table 9-14 Multicast Profile Add Fields

Multicast >> General >> Filtering Profile

Edit Profile

Profile ID	1
IP Version	IPv4
Start Address	224.1.1.1
End Address	224.1.2.3
Action	<input checked="" type="radio"/> Allow <input type="radio"/> Deny

Apply Close

Figure 9-15 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: <ul style="list-style-type: none"> Allow: permit the group can learned that match the profile. Deny: deny the group to learn the groupthat match the profile.

Table 9-15 Multicast Profile Edit Fields

9.1.7. 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

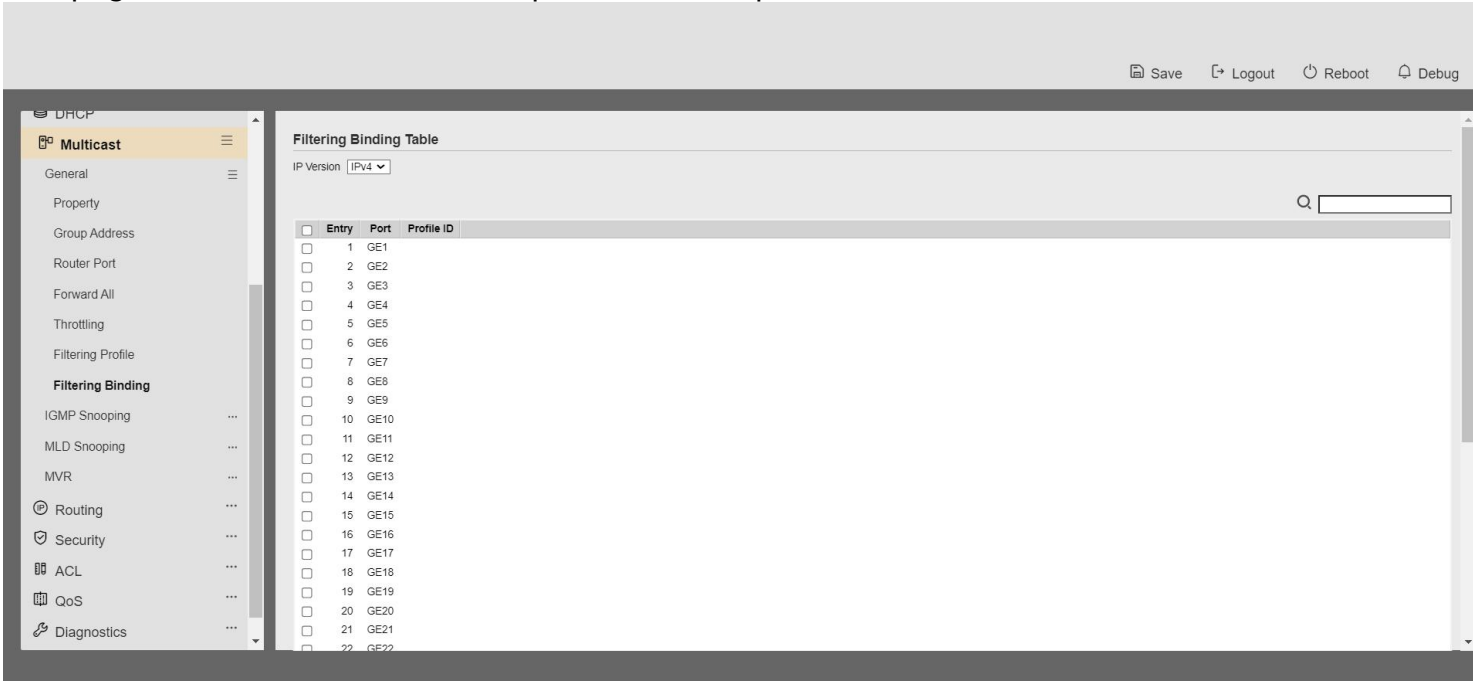


Figure 9-16 Multicast Filtering Table Page

Field	Description
IP Version	IP Version <ul style="list-style-type: none"> 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

Table 9-16 Multicast Filtering Table Fields

Edit Filtering Binding

Port

GE2

IP Version

IPv4

Profile ID

☐ Enable

Apply

Close

Figure 9-17 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

Table 9-17 Multicast Filtering Edit Fields

9.2. IGMP Snooping

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

9.2.1. 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.

Figure 9-18 IGMP Snooping Property Page

Field	Description
State	Set the enabling status of IGMP Snooping functionality <ul style="list-style-type: none"> Enable: If Checked Enable IGMP Snooping, else is Disabled IGMP Snooping.
Version	Set the igmp snooping version <ul style="list-style-type: none"> IGMPv2: Only support process igmp v2 packet. IGMPv3: Support v3 basic and v2.
Report Suppression	Set the enabling status of IGMP v2 report suppression <ul style="list-style-type: none"> Enable: If Checked Enable IGMP Snooping v2 report suppression, else Disable the report suppression
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.

Table 9-18 IGMP Snooping Property Fields

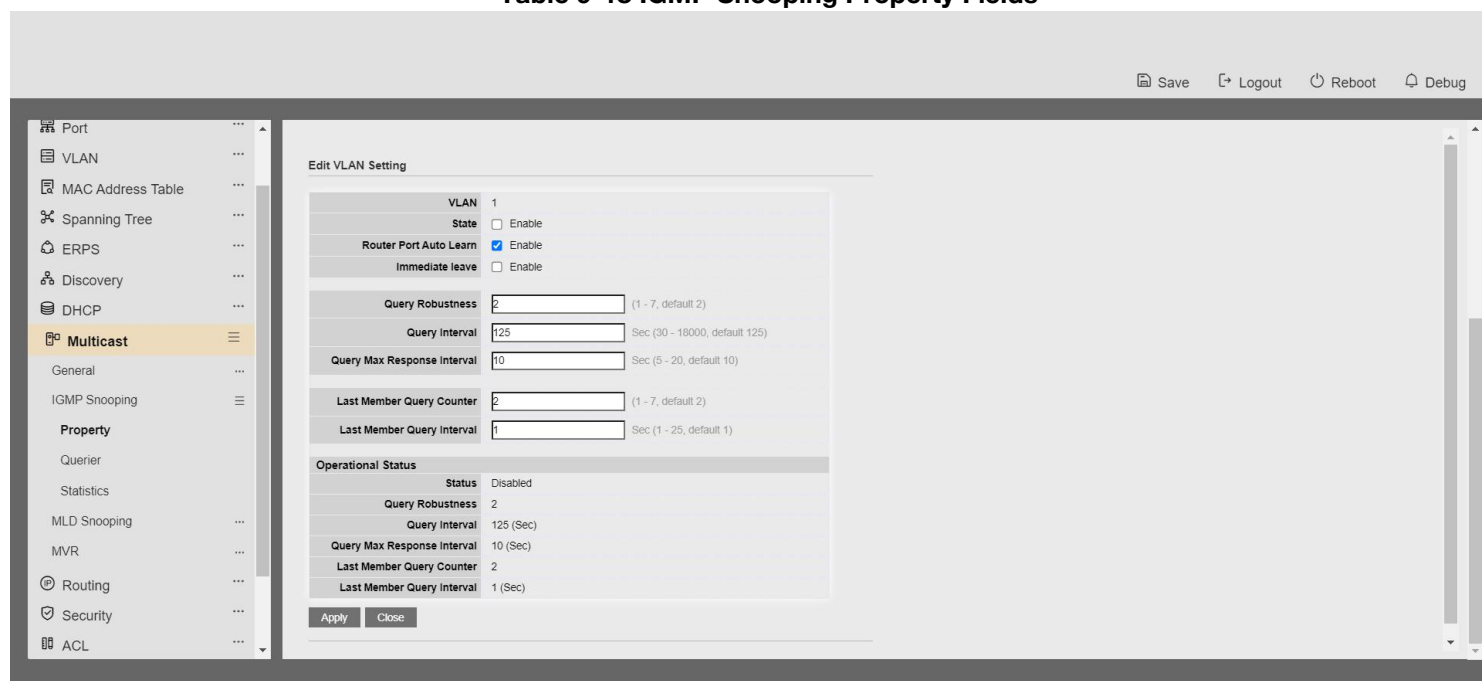


Figure 9-19 IGMP Snooping VLAN Edit Page

Field	Description
VLAN	The selected VLAN List
State	Set the enabling status of IGMP Snooping VLAN functionality <ul style="list-style-type: none">• 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 <ul style="list-style-type: none">• Enable: If checked Enable learning router port by query and PIM, DVRMP, else Disable the learning router
Immediate leave	Immediate Leave the group when receive IGMP Leave message. <ul style="list-style-type: none">• 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

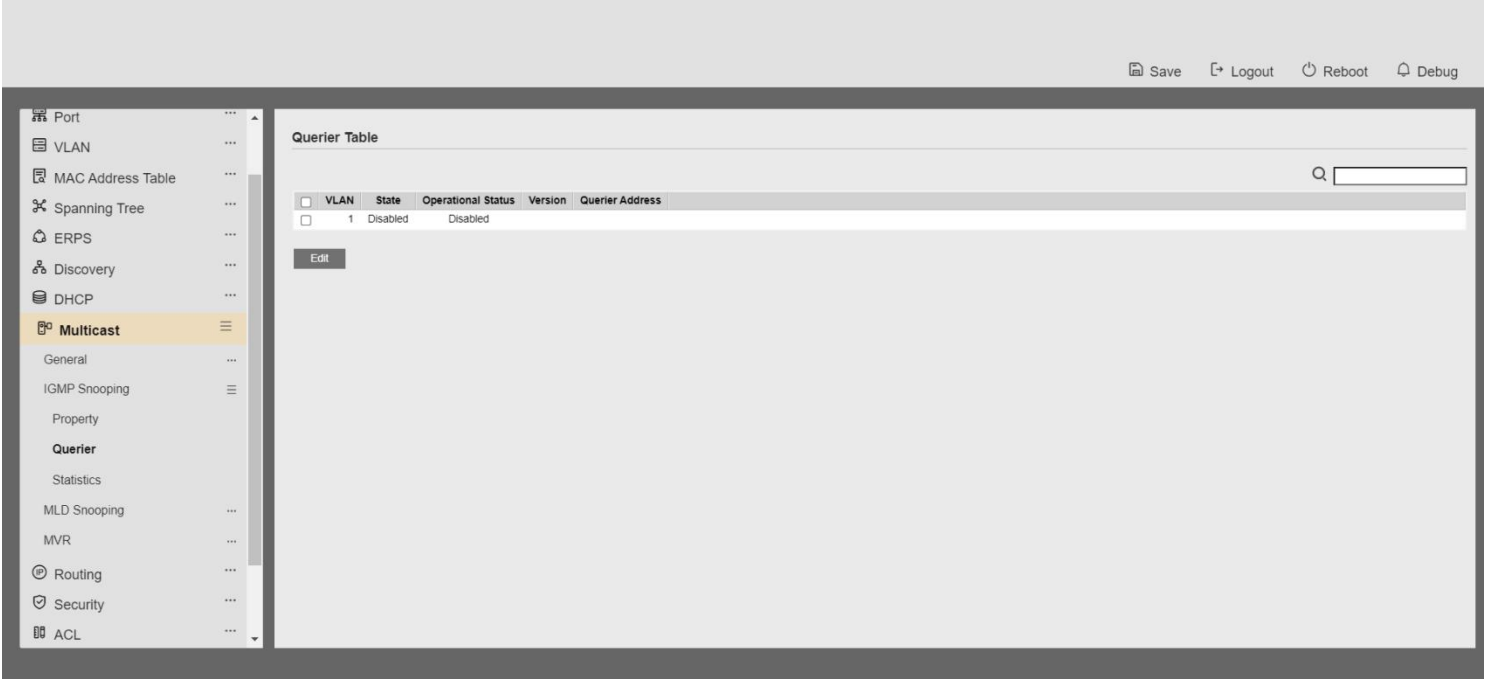
Last Member Query Interval

Operational Last Member Query Interval

Table 9-19 IGMP Snooping VLAN Edit Fields

9.2.2. 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.

Figure 9-20 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

Table 9-20 IGMP Snooping Querier Table Fields

Edit Querier

VLAN

1

State

☐ Enable

Version

☒ IGMPv2

☐ IGMPv3

Apply

Close

Figure 9-21 IGMP Snooping Querier Edit Page

Field	Description
VLAN	The Selected Edit IGMP Snooping querier VLAN List
State	<div>Set the enabling status of IGMP Querier Election on the chose VLANs</div> <div><ul style="list-style-type: none">Enabled: if checked Enable IGMP Querier else Disable IGMP Querier</div>
Version	<div>Set the query version of IGMP Querier Election on the chose VLANs</div> <div><ul style="list-style-type: none">IGMPv2: Querier version 2.IGMPv3: Querier version 3. (IGMP Snooping version should be IGMPv3)</div>

Table 9-21 IGMP Snooping Querier Edit Fields

9.2.3. Statistics

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

This page allow user to clear igmp snooping statics.

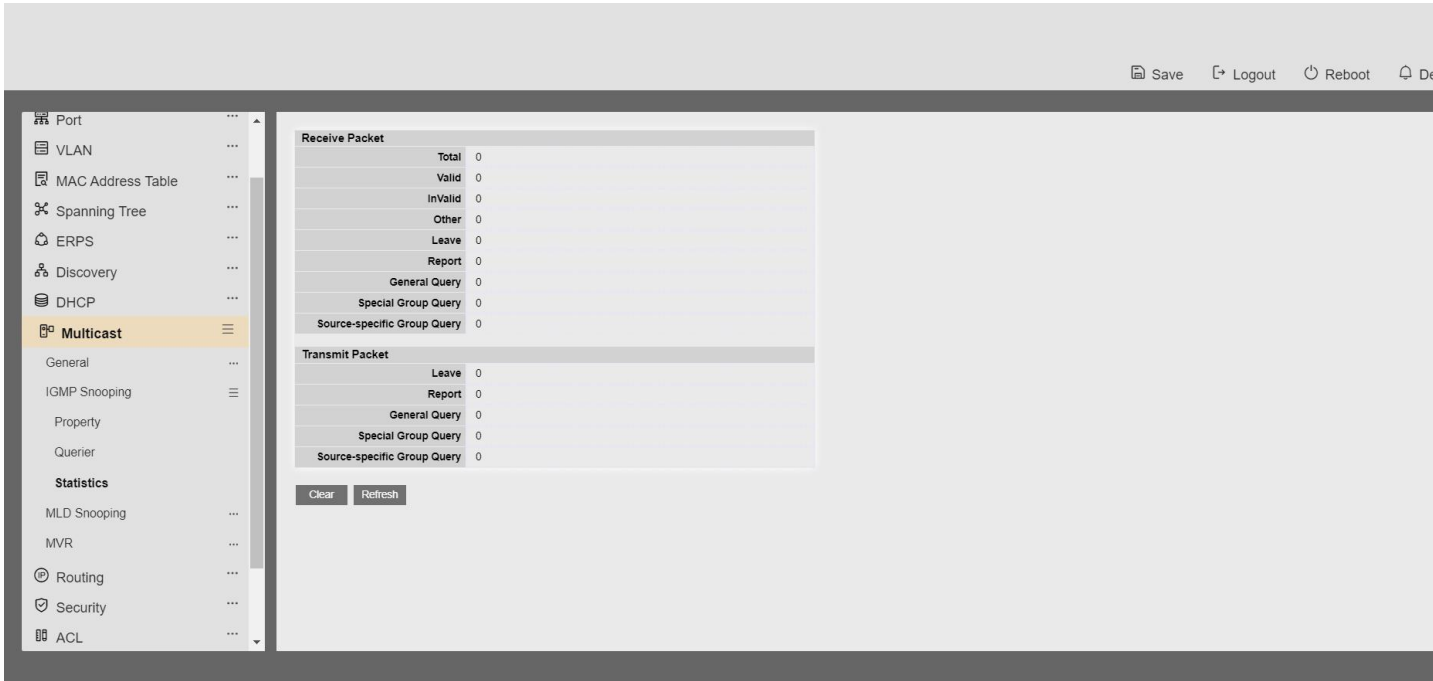


Figure 9-22 IGMP Snooping Statistics Page

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

Table 9-22 IGMP Snooping Statistics Fields

9.3. MLD Snooping

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

9.3.1. 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.

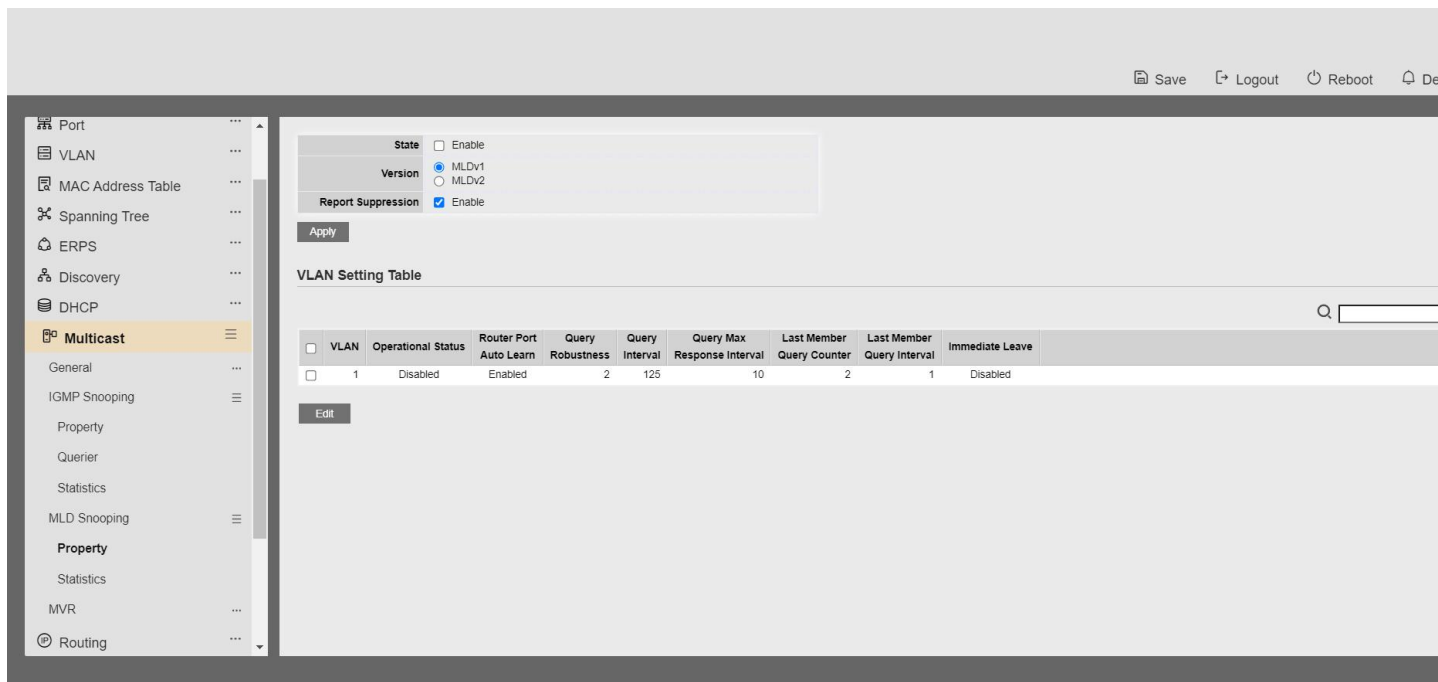


Figure 9-23 MLD Snooping Property Page

Field	Description
State	Set the enabling status of IGMP Snooping functionality <ul style="list-style-type: none">Enable: If Checked Enable IGMP Snooping, else is Disabled IGMP Snooping.
Version	Set the MLD snooping version <ul style="list-style-type: none">MLDv1: Only support process MLD v1 packet.MLDv2: Support v2 basic and v1.
Report Suppression	Set the enabling status of MLD v1 report suppression <ul style="list-style-type: none">Enable: If Checked Enable MLD Snooping v1 report suppression, else Disable the report suppression
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.

Table 9-23 MLD Snooping Property Fields

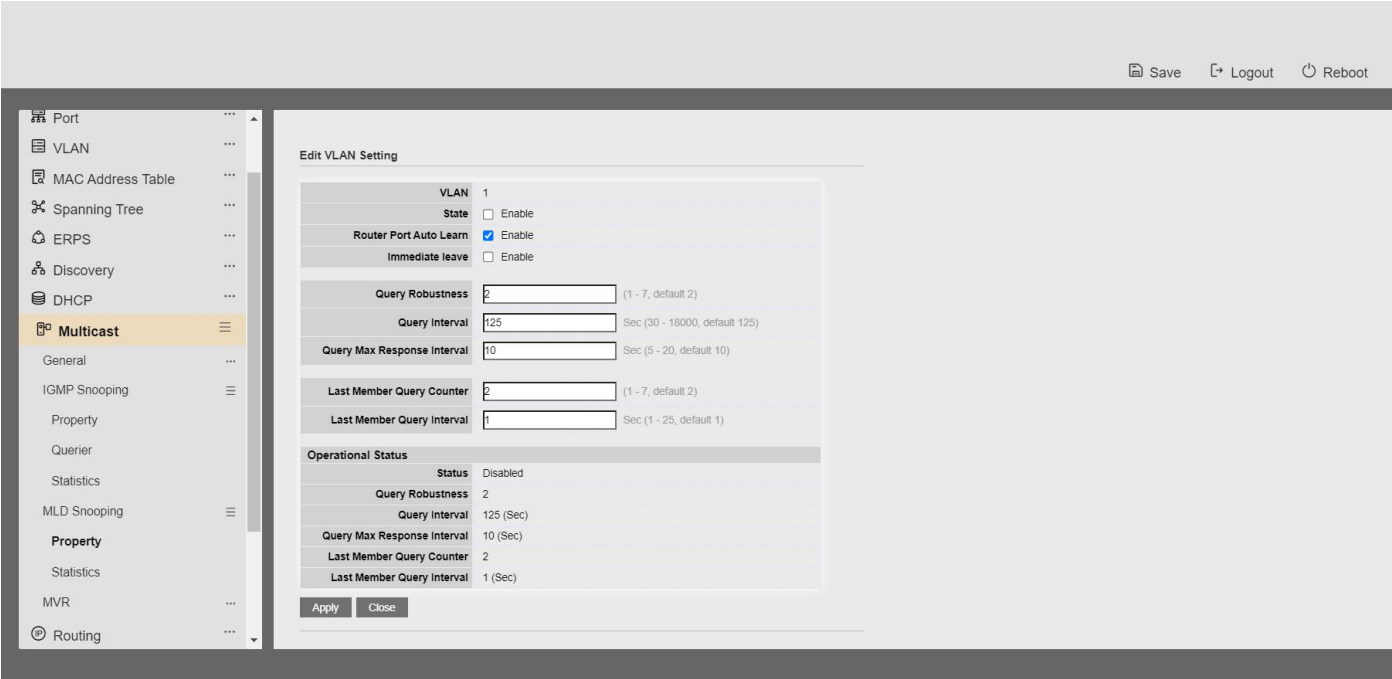


Figure 9-24 MLD Snooping VLAN Edit Page

Field	Description
VLAN	The selected VLAN List
State	Set the enabling status of MLD Snooping VLAN functionality <ul style="list-style-type: none">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 <ul style="list-style-type: none">Enable: If checked Enable learning router port by query and PIM, DVRMP, else Disable the learning router
Immediate leave	Immediate Leave the group when receive MLD Leave message. <ul style="list-style-type: none">Enable: If checked Enable immediate leave, else

	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 Query Counter	Operational Last Member Query Count
Last Member Query Interval	Operational Last Member Query Interval

Table 9-24 MLD Snooping VLAN Edit Fields

9.3.2. Statistics

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

This page allow user to clear MLD snooping statics.

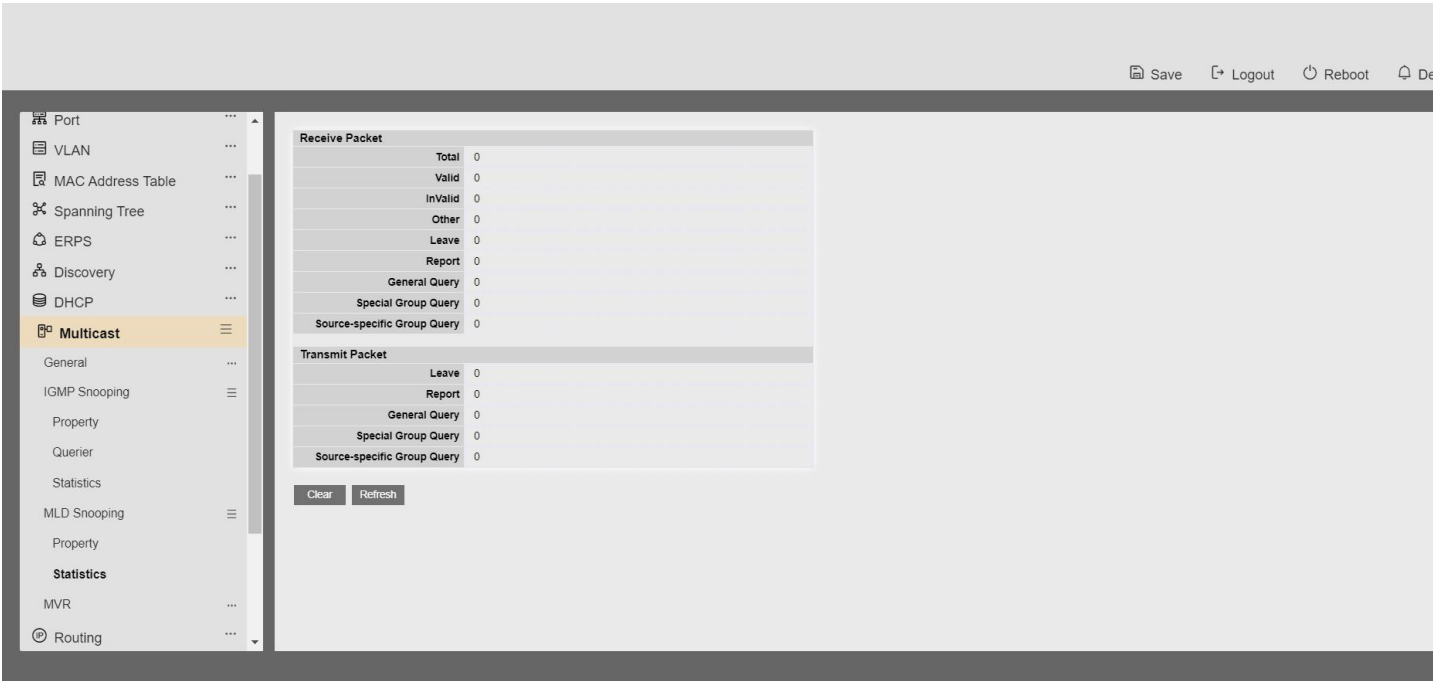


Figure 9-25 MLD Snooping Statistics Page

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

Table 9-25 MLD Snooping Statistics Fields

9.4. MVR

Use the MVR pages to configure settings of MVR function.

9.4.1. Property

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

This page allow user to set MVR property.

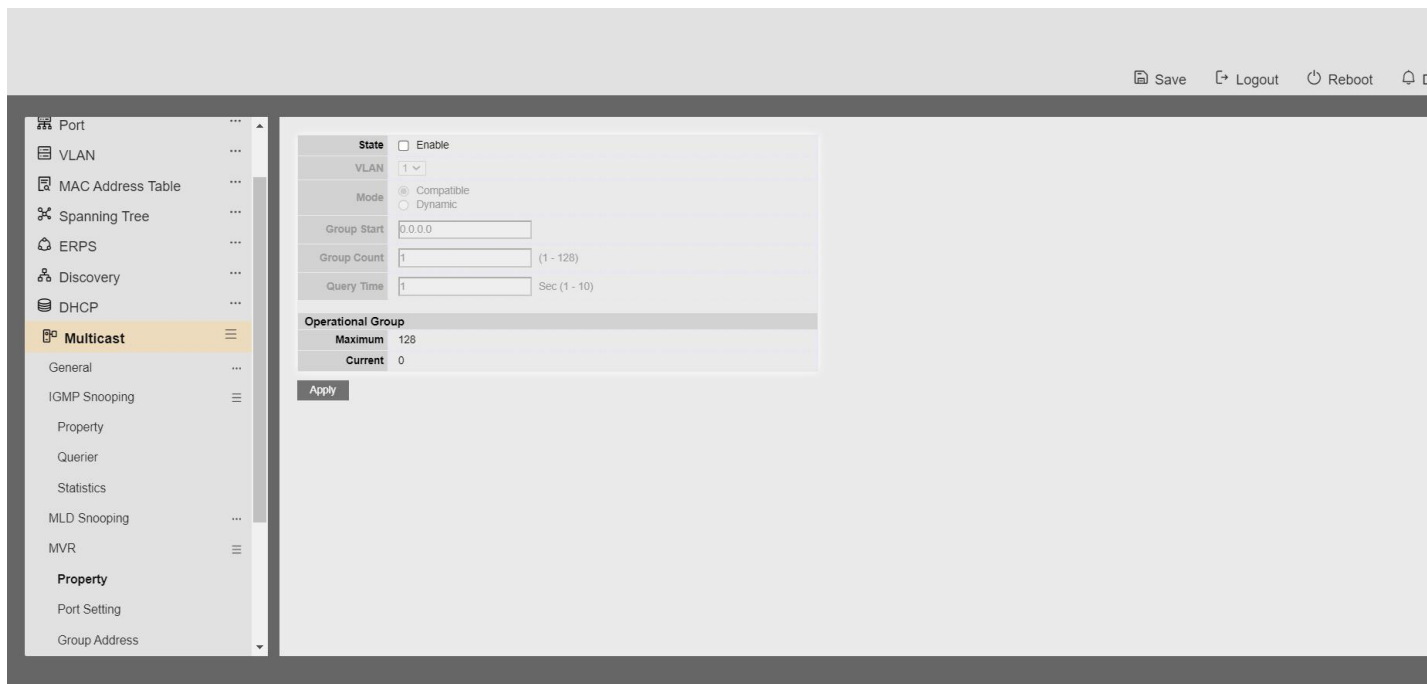


Figure 9-26 Multicast MVR Properties Page

Field	Description
State	<ul style="list-style-type: none"> Enable: if checked enable the MVR state, else disable the MVR state
VLAN	The MVR VLAN ID
Mode	Set the MVR mode. <ul style="list-style-type: none"> 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

Table 9-27 MVR Property Fields

9.4.2. 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

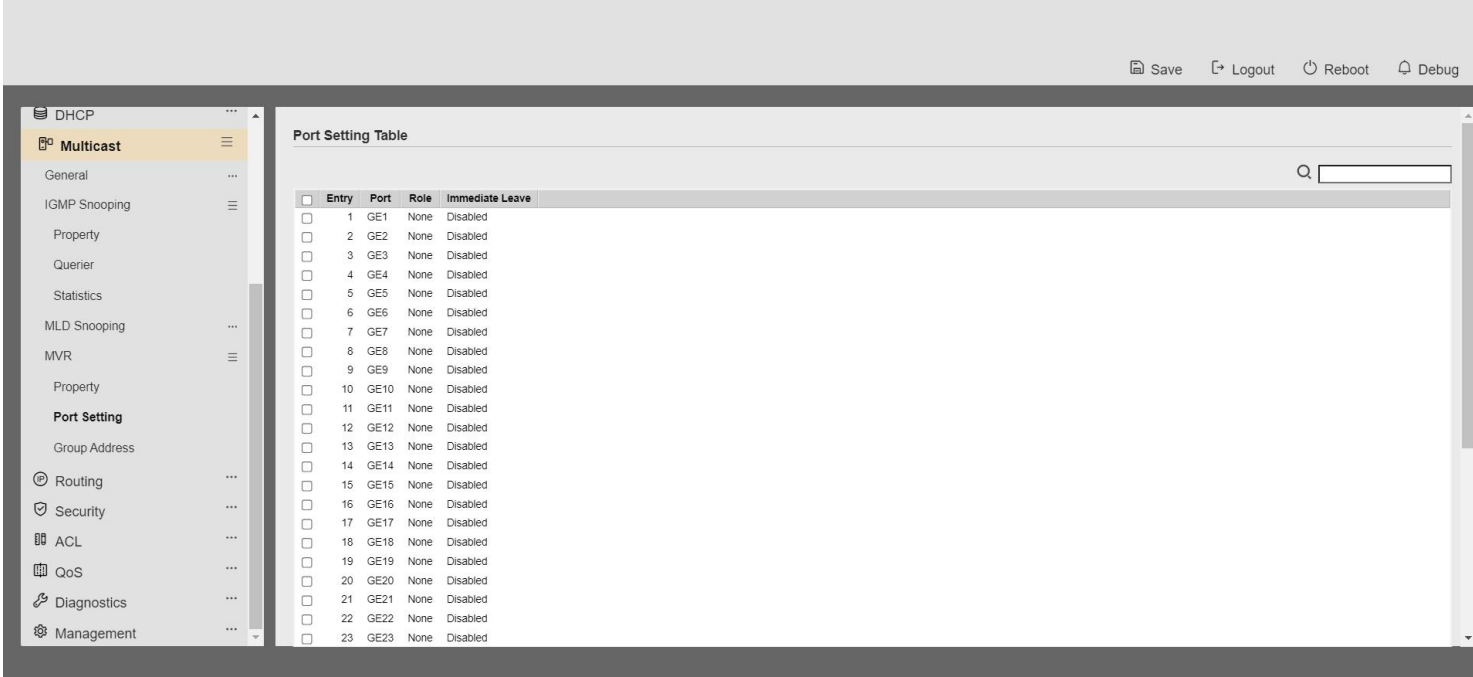


Figure 9-28 Multicast MVR Port Setting Table Page

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

Table 9-29 MVR Port Setting Fields

Multicast >> MVR >> Port Setting

Edit Port Setting

Port

GE1-GE2,GE4-GE5

Role

☒ None

☐ Receiver

☐ Source

Immediate Leave

☒ Enable

Apply

Close

Figure 9-30 Multicast MVR Port Setting Edit Page

Field	Description
Port	Display the selected port list
Role	MVR port role <ul style="list-style-type: none">None: port role is noneReceiver: port role is receiverSource: port role is source
Immediate Leave	MVR Port immediate leave <ul style="list-style-type: none">Enable: if checked is enable immediate leave, else disable immediate leave.

Table 9-31 MVR Port Setting Edit Fields

9.4.3. 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.

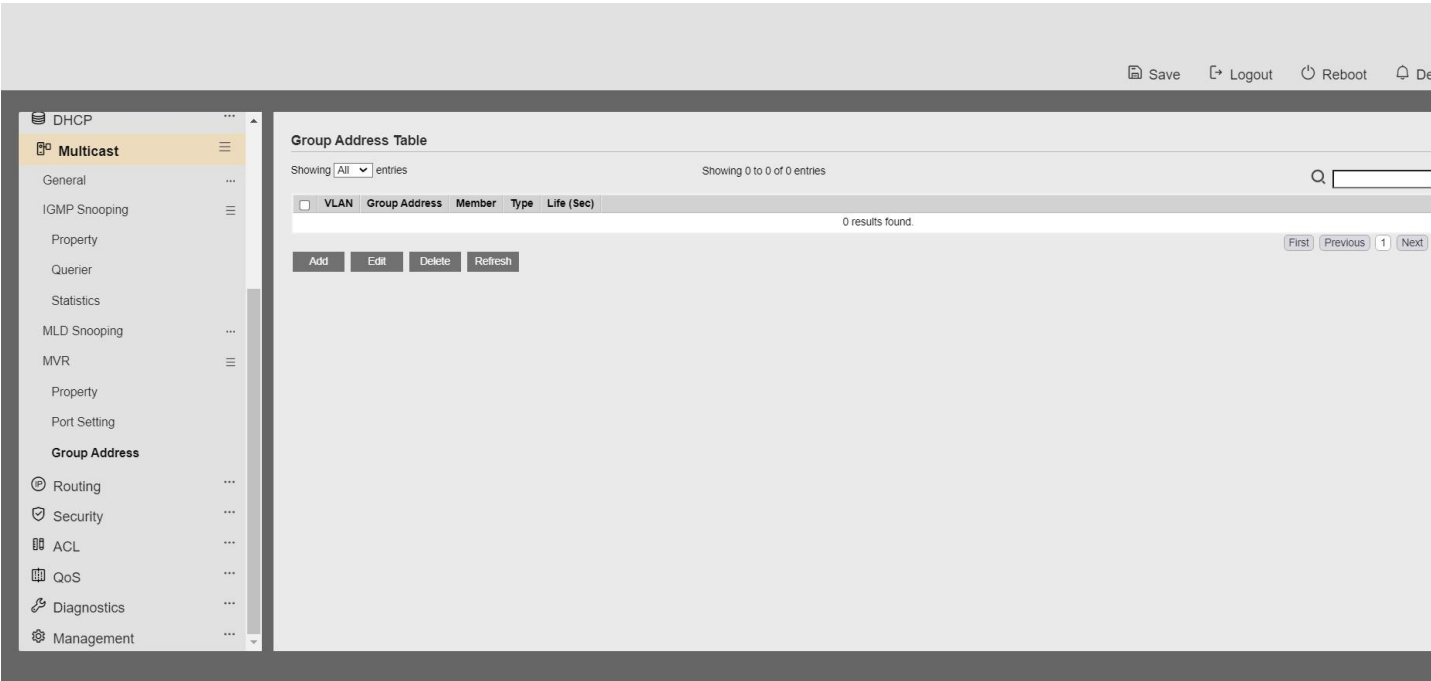


Figure 9-32 Multicast MVR Group Address Table Page

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.

Table 9-33 MVR Group Address Table Fields

Multicast >> MVR >> Group Address

Add Group Address

VLAN	2	
Group Address	<input type="text"/> (224.1.1.1 - 224.1.1.1)	
Member	Available Port	Selected Port
	<div><div></div><div></div></div>	<div><div></div><div></div></div>
<div><div>Apply</div><div>Close</div></div>		

Figure 9-34 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. <ul style="list-style-type: none">• 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

Table 9-35 MVR Group Address Add Fields

Figure 9-36 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. <ul style="list-style-type: none">• 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

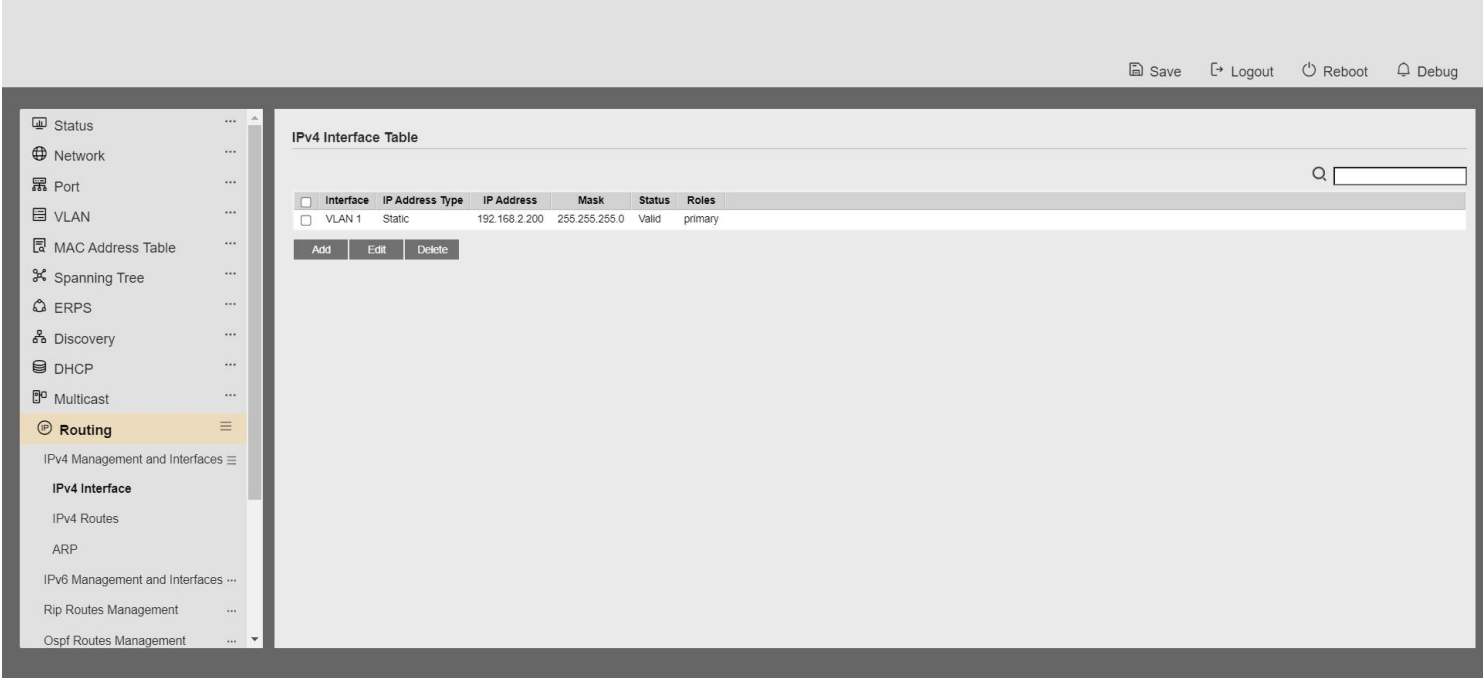
Table 9-37 MVR Group Address Edit Fields

17 Routing

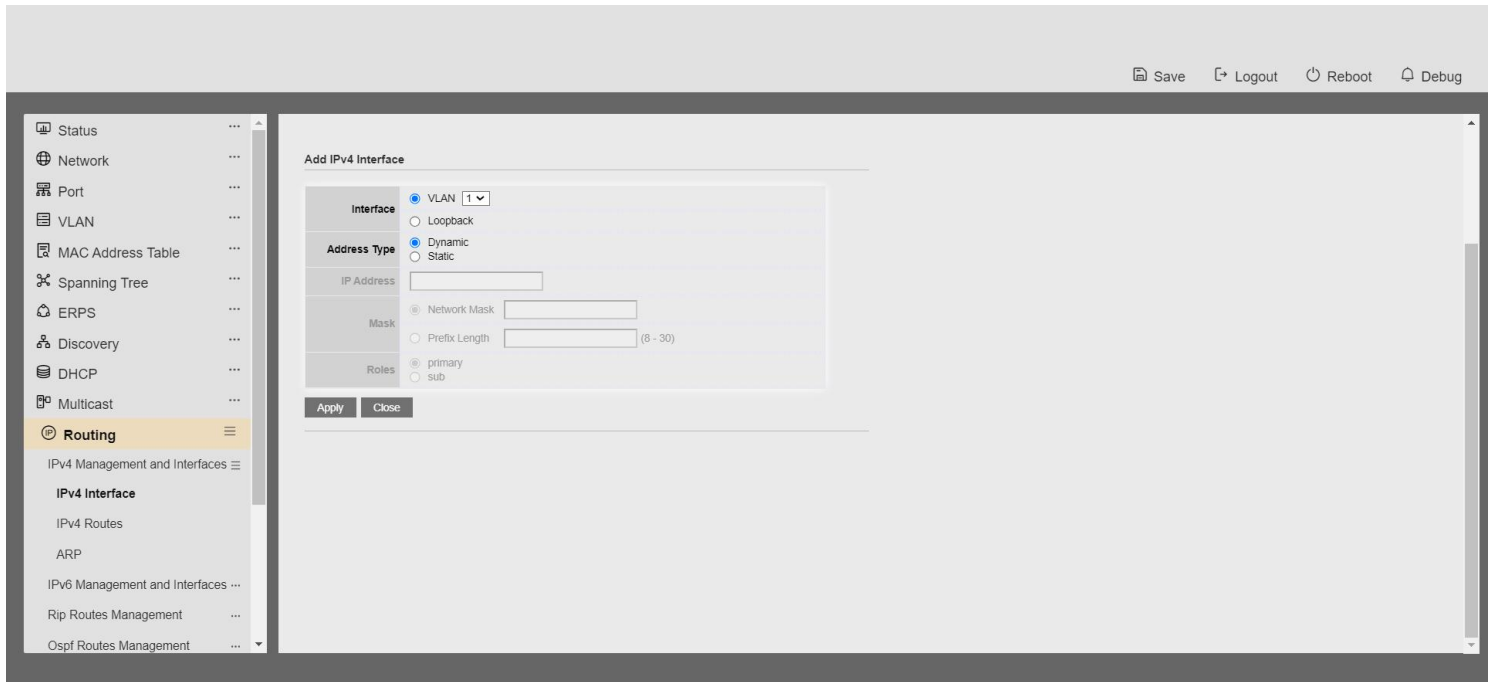
17.1 IPv4 Management and Interfaces

17.1.1 IPv4 Interface

1. Click the "Routing > ipv4 Management Interface > ipv4 Interface" menu in the navigation tree to enter the "ipv4 Interface" interface, as shown in the following figure.

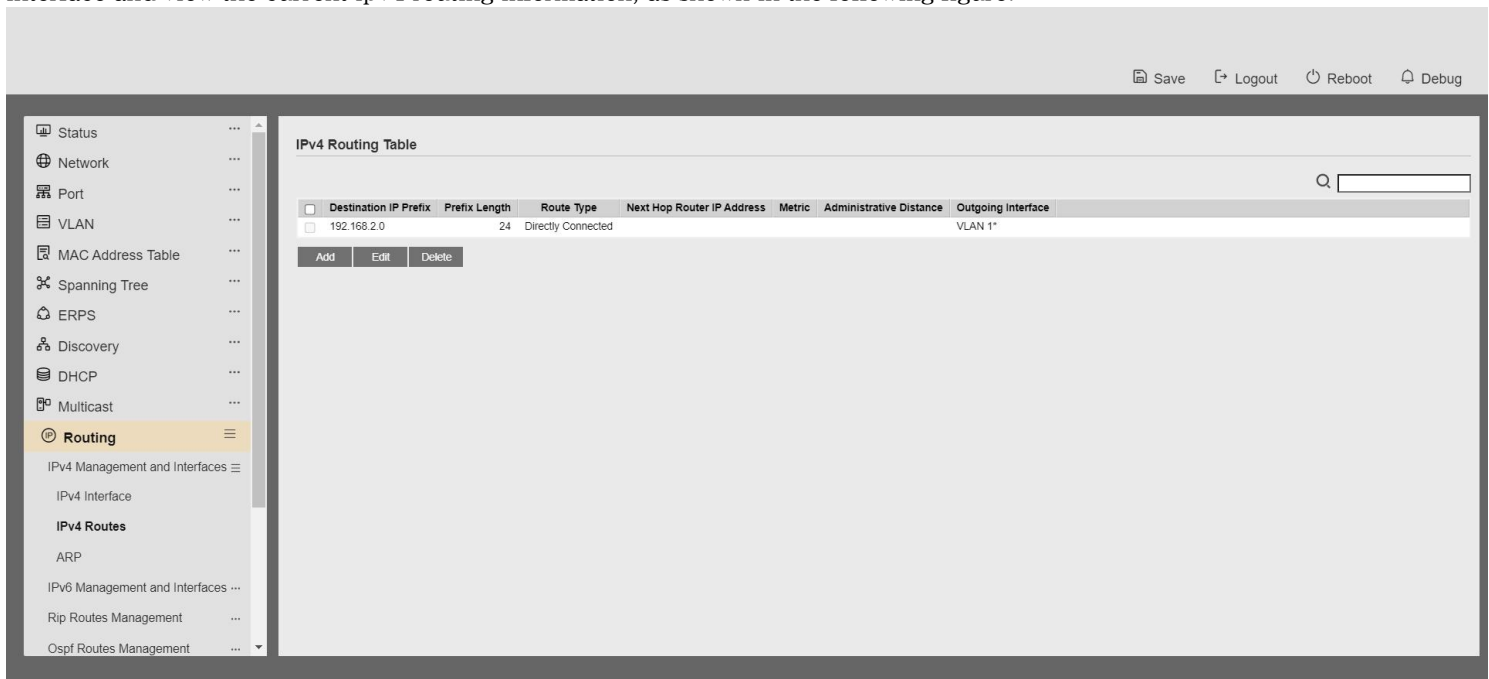


2. Click Add to enter the Configure ipv4 Interface Address interface to add a device ipv4 address as shown in the following figure:

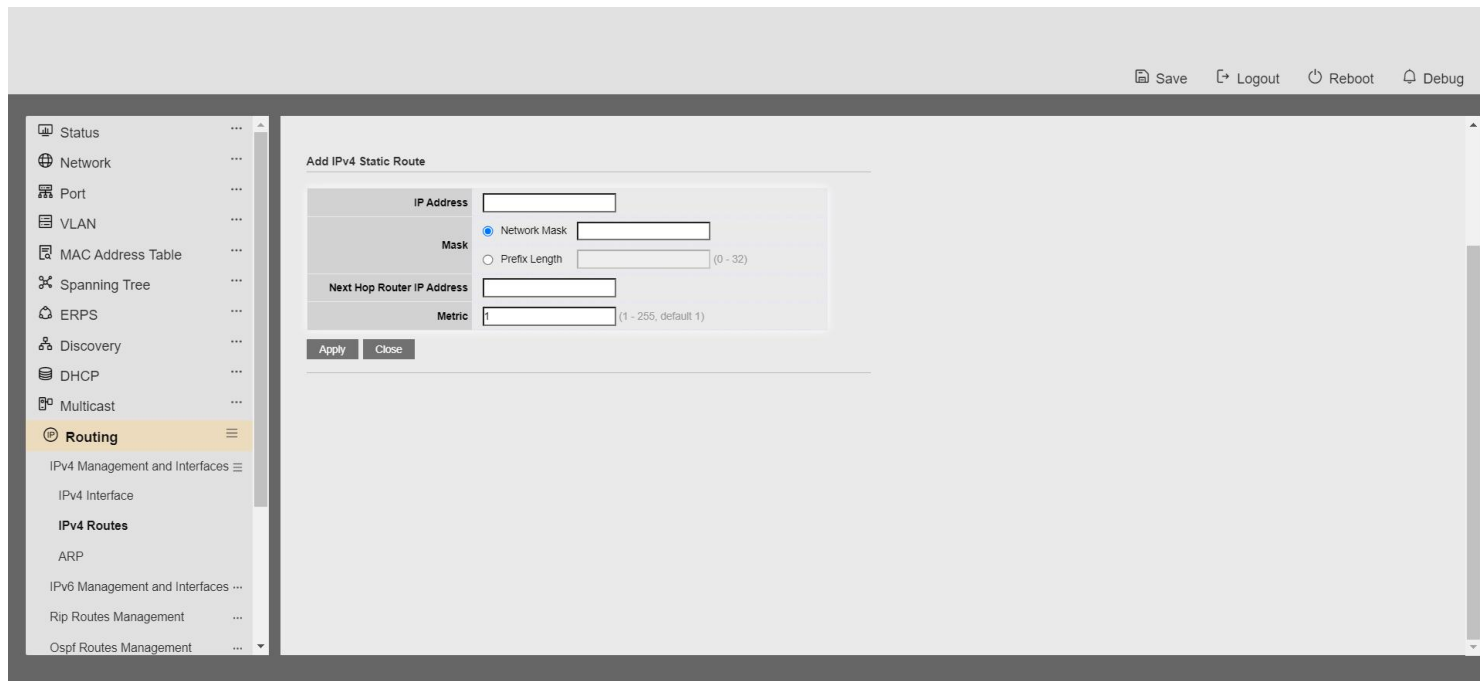


17.1.2 IPv4 Routing

1. Click the "Routing > ipv4 Management Interface > ipv4 Routing" menu in the navigation tree to enter the "ipv4 Routing" interface and view the current ipv4 routing information, as shown in the following figure.

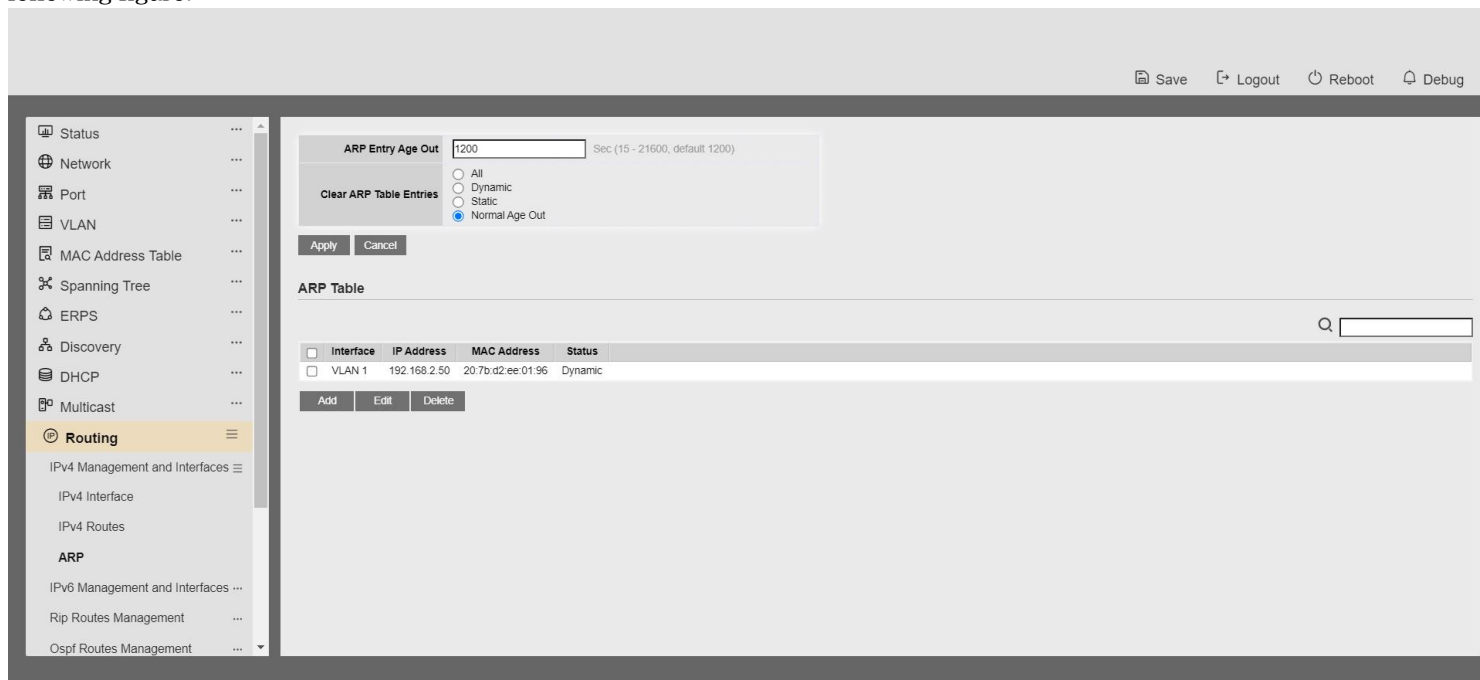


2. The ipv4 routing interface clicks Add to add ipv4 routing information as shown in the following figure:

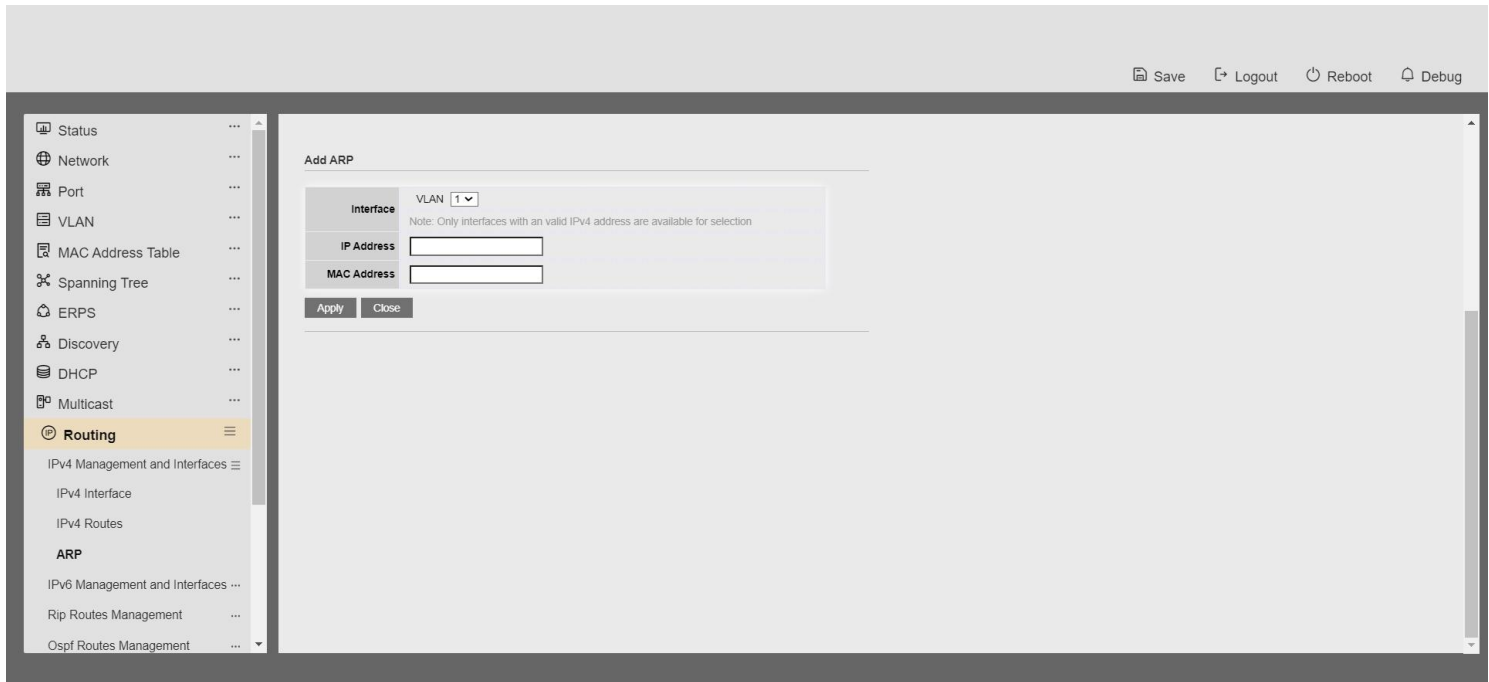


17.1.3 ARP

1. Click the "Routing > ipv4 Management Interface > ARP" menu in the navigation tree to enter the "ARP" interface, where you can view the current ARP table information, configure the ARP aging time, and clear the ARP table entries, as shown in the following figure.



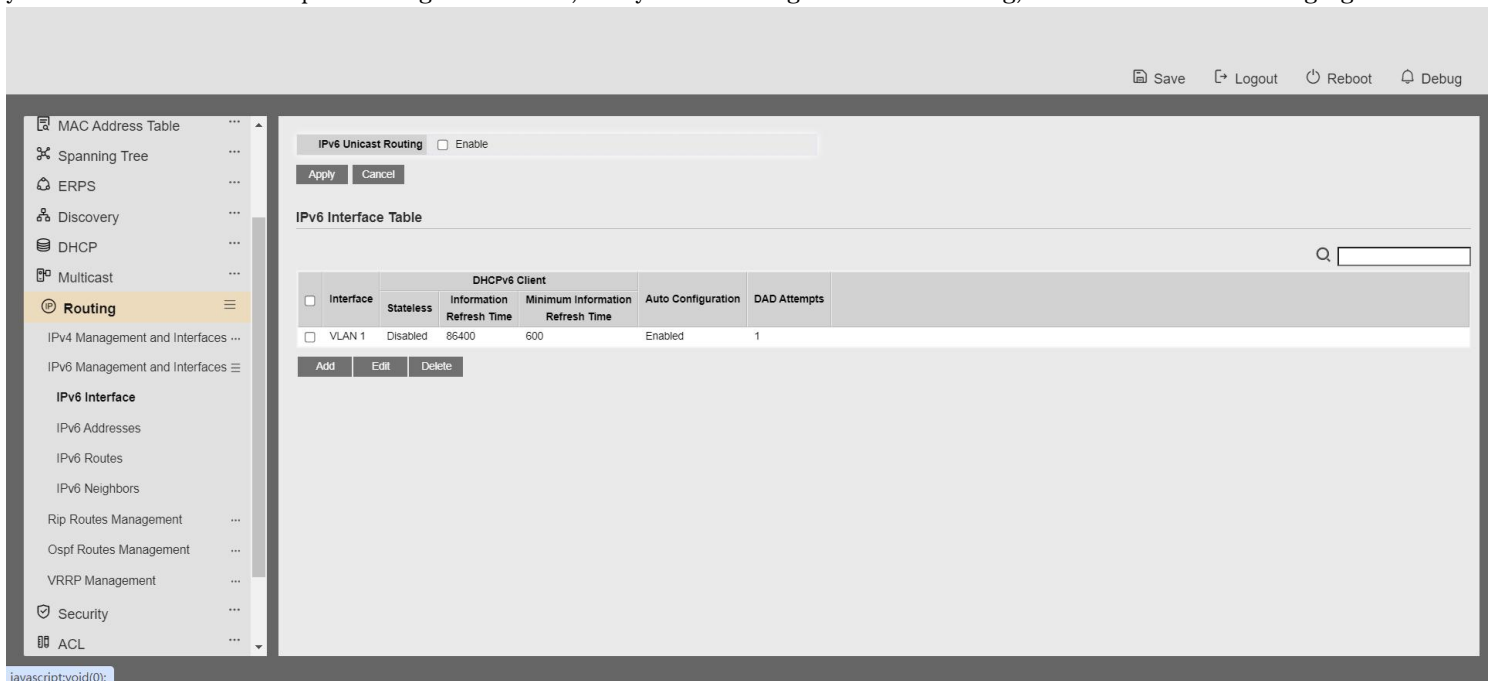
2. ARP screen click Add to add static ARP table entries as shown below:



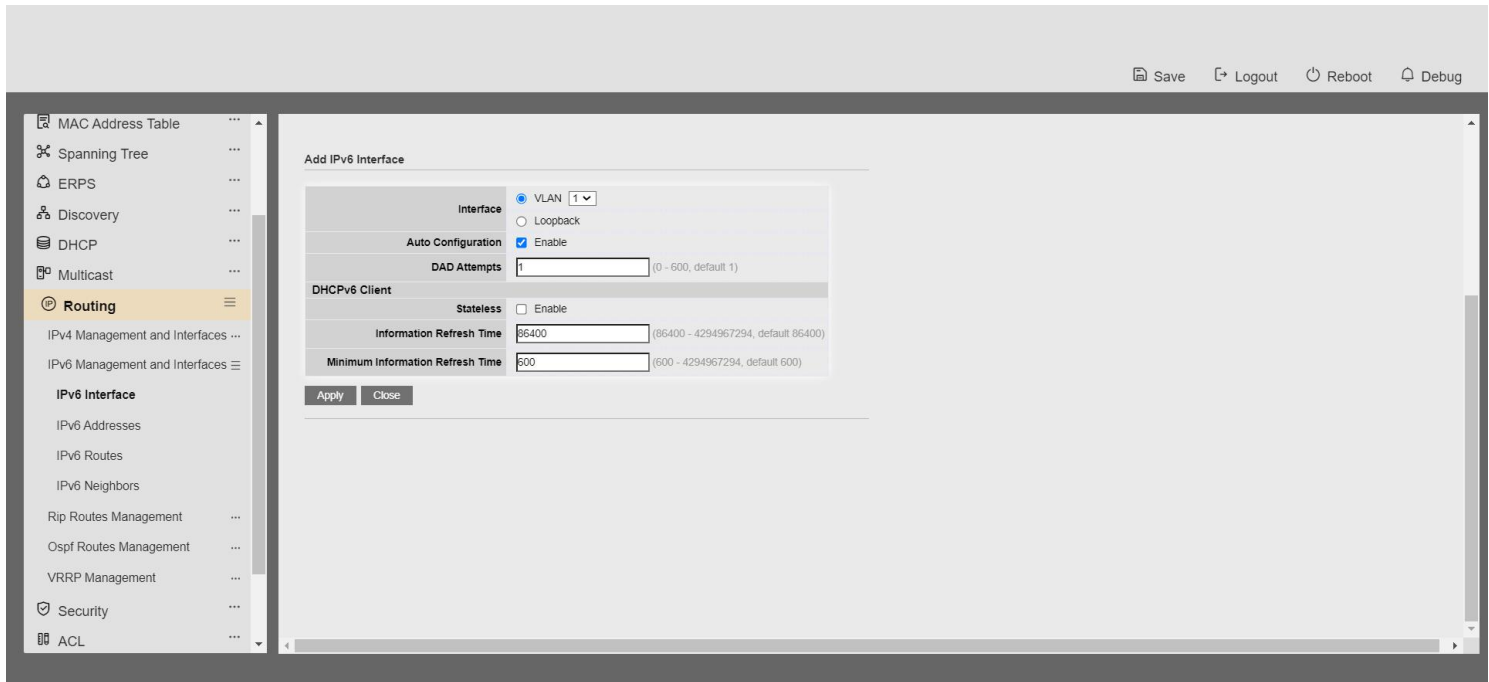
17.2 Ipv6 Management and Interfaces

17.2.1 Ipv6 Interfaces

1. Click "Routing > ipv6 Management Interface > ipv6 Interface" in the navigation tree to enter the "ipv6 Interface" interface, you can view the current ipv6 routing information, and you can configure unicast routing, as shown in the following figure.

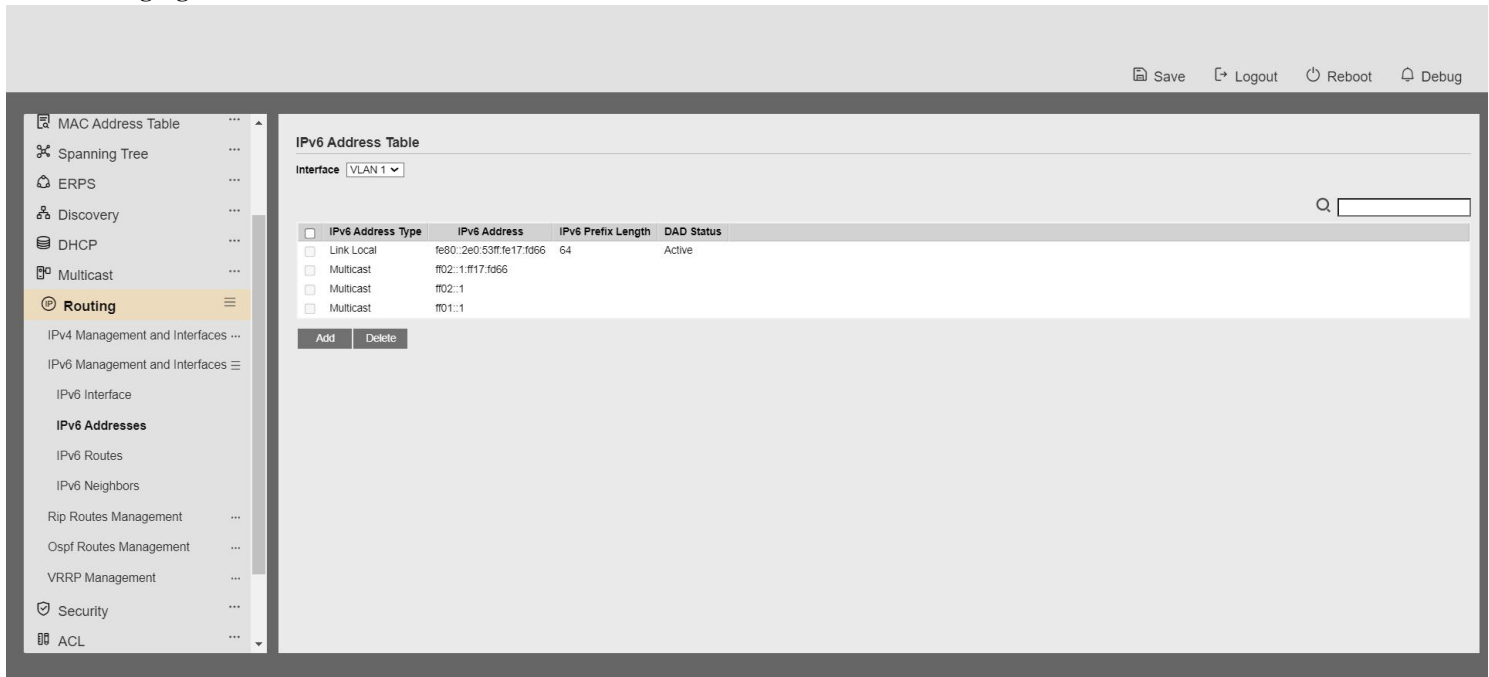


2 Click the Add button to configure the address for ipv6 autoconfiguration. you can configure the dhcpV6 client state as shown in the following figure:

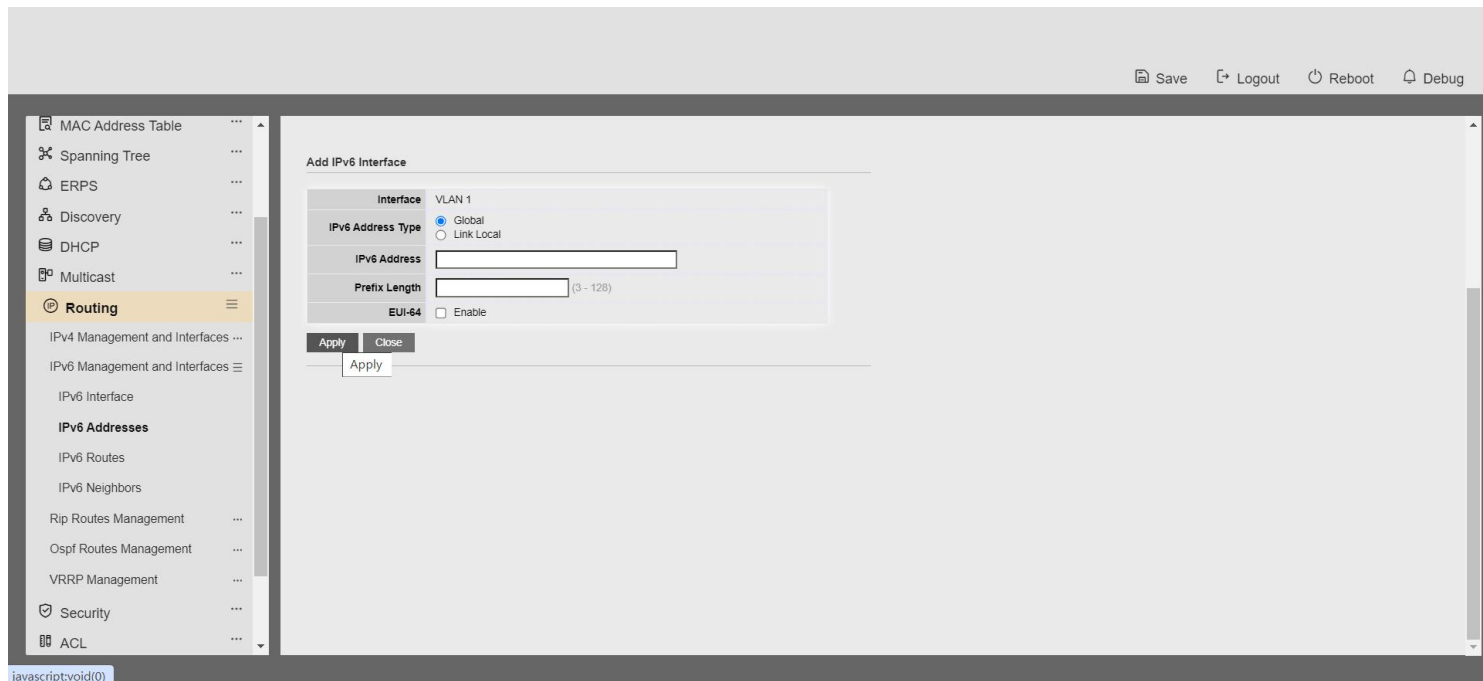


17.2.2 ipv6 address

1. Click the "Routing > ipv6 Management Interface > ipv6 Address" menu in the navigation tree to enter the "ipv6 Address" interface, you can view the current interface ipv6 address information, and you can delete the interface ipv6 address, as shown in the following figure.

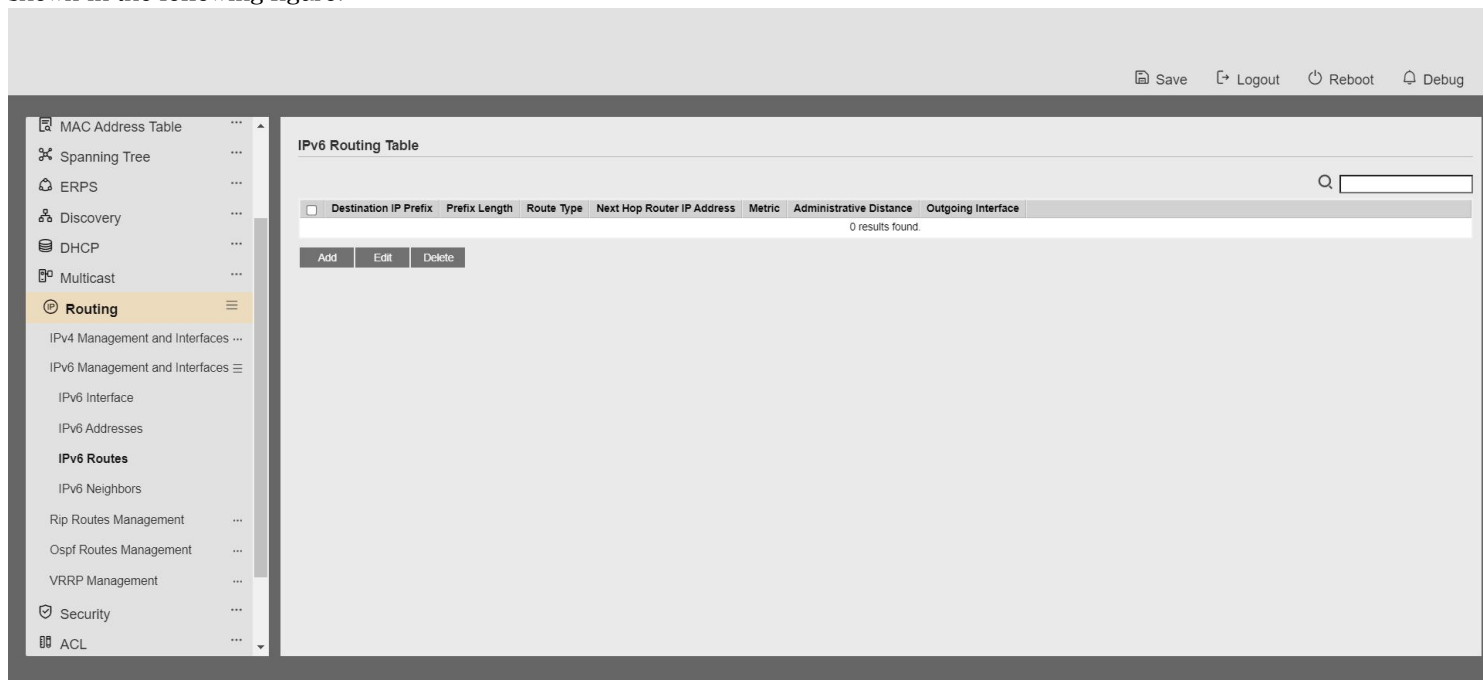


2. Click the Add button to add the interface ipv6 address, as shown below

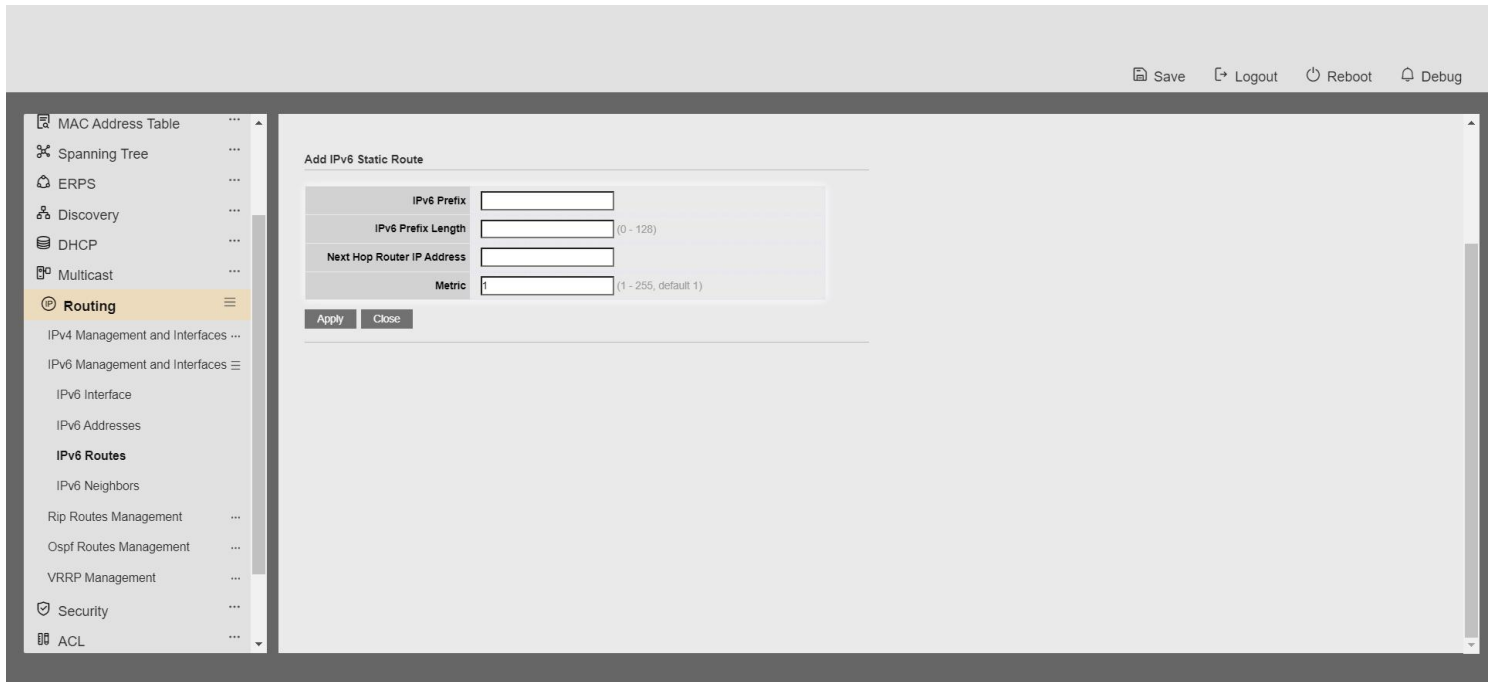


17.2.3 ipv6 routes

1. Click the "Routing > ipv6 Management Interface > ipv6 Routing" menu in the navigation tree to enter the "ipv6 Routing" interface, you can view the current ipv6 routing information, and you can delete, add, and modify the routing information, as shown in the following figure.

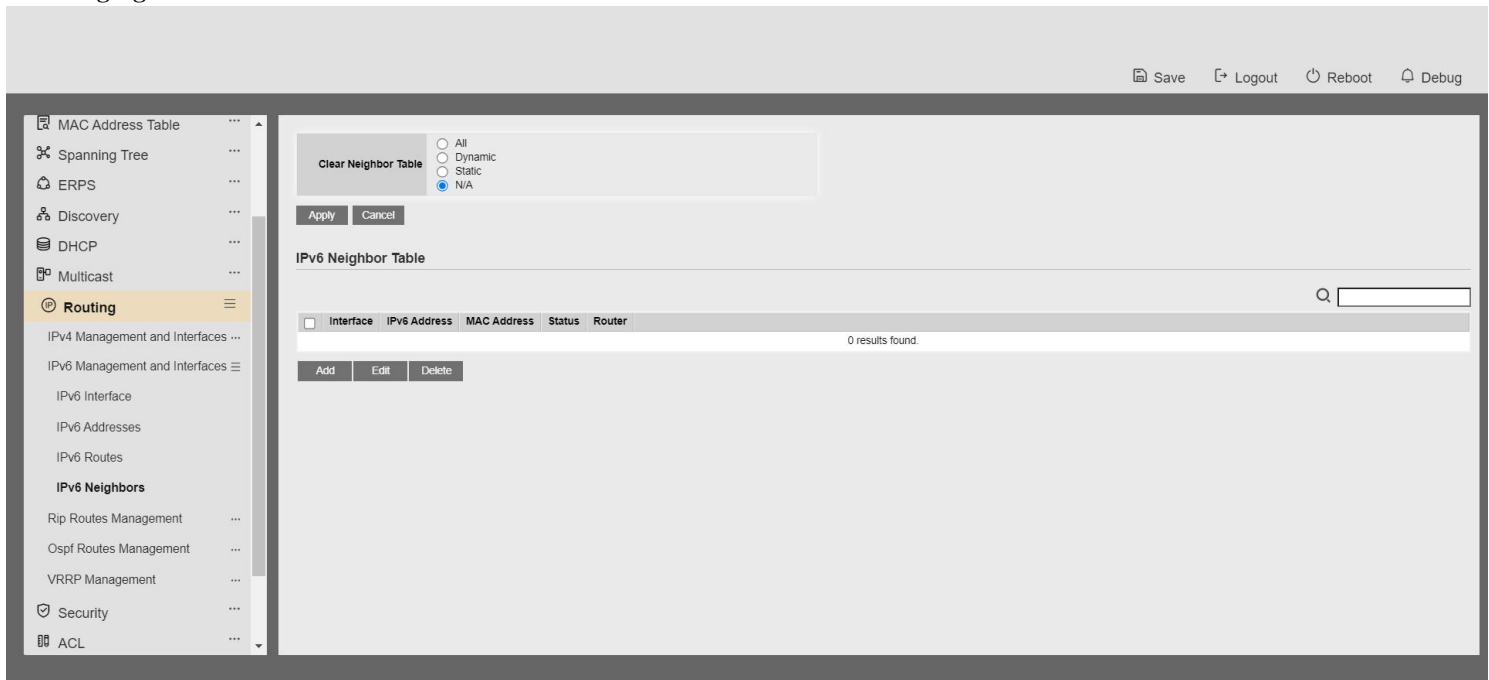


2. Click the Add button to configure the routing information as shown below:

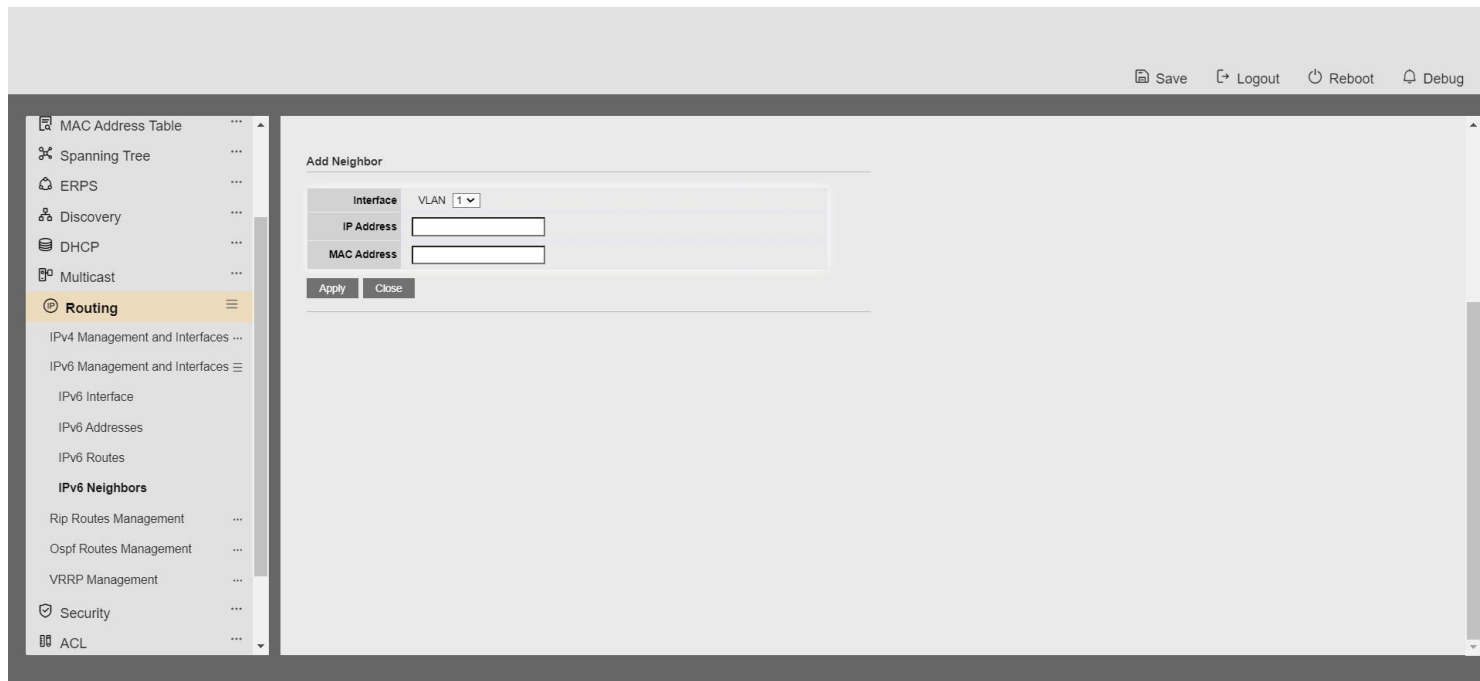


17.2.4 IPv6 Neighbor

1. Click "Routing > ipv6 Management Interface > ipv6 Neighbours" in the navigation tree to enter the "ipv6 Neighbours" interface, which allows you to view the current ipv6 Neighbours table and delete the neighbour table entries, as shown in the following figure.

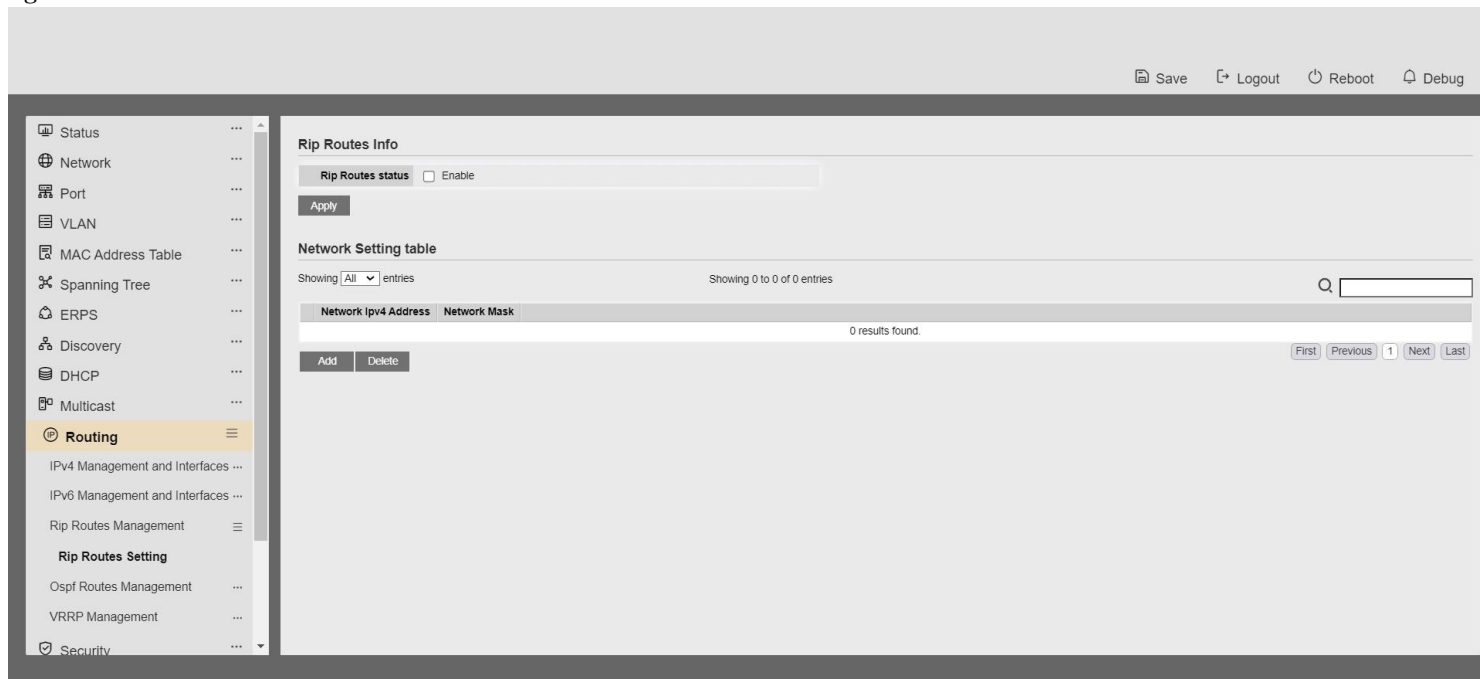


2. Click the Add button to add ipv6 neighbour information as shown below:

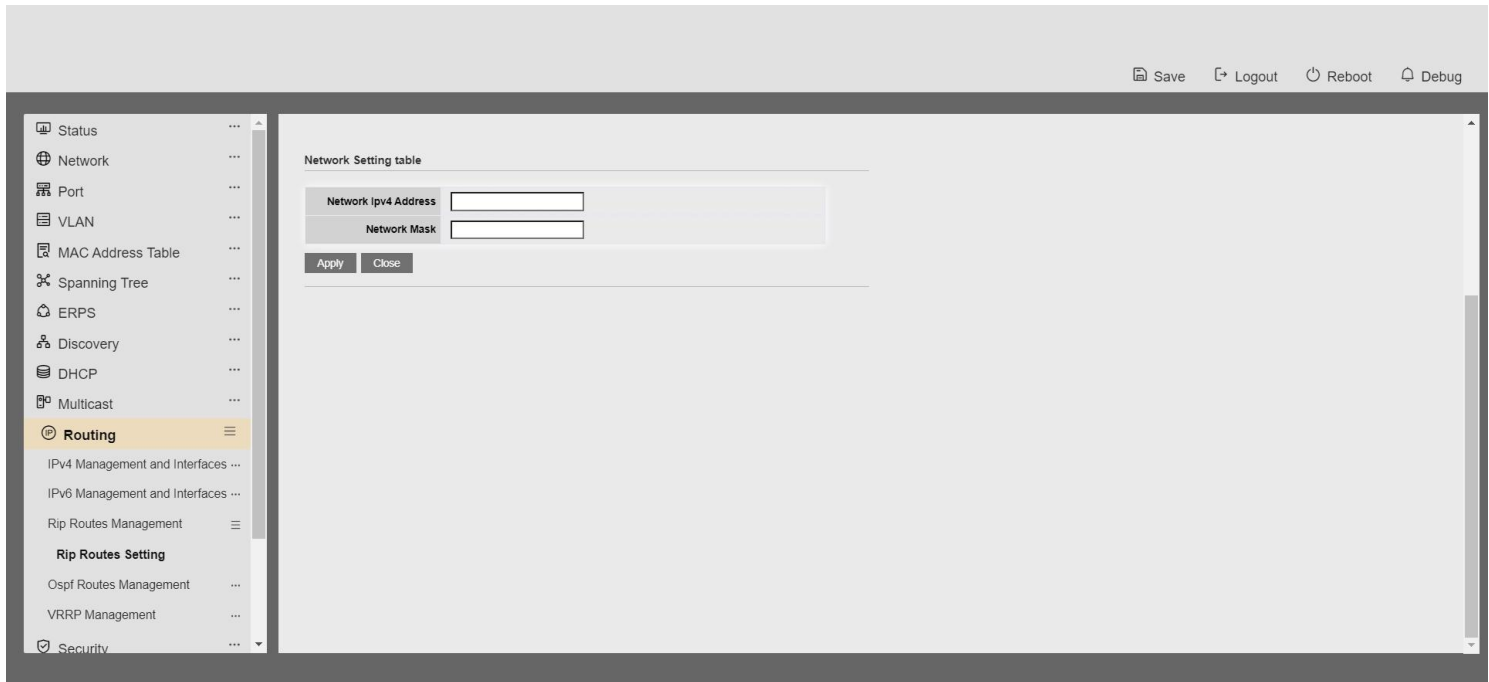


17.3 Rip Routes Management

1. Click "Routing > Rip Route Management > Rip Route Configuration" in the navigation tree to enter the "Rip Route Configuration" interface, where you can enable the rip and view the setup of the advertisement route, as shown in the following figure.

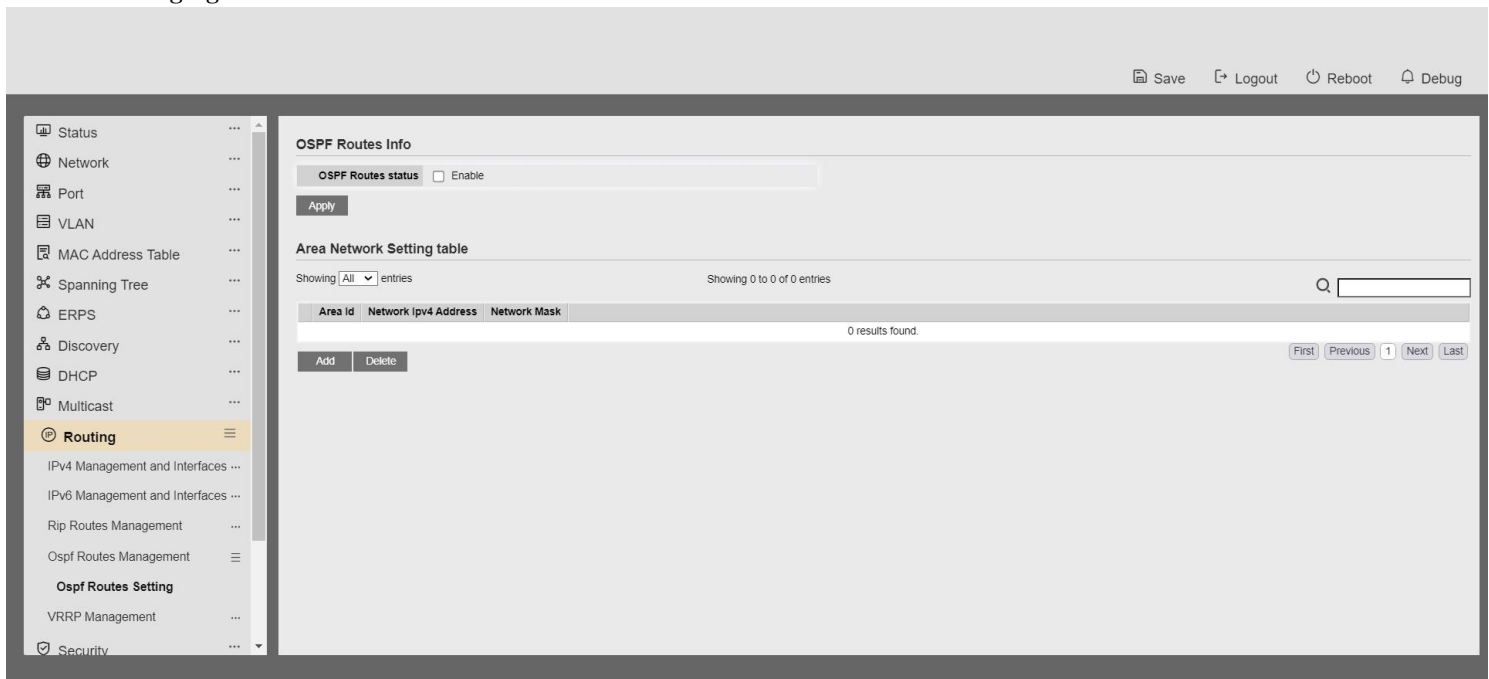


2. Click the Add button to add a working network configuration as shown below:

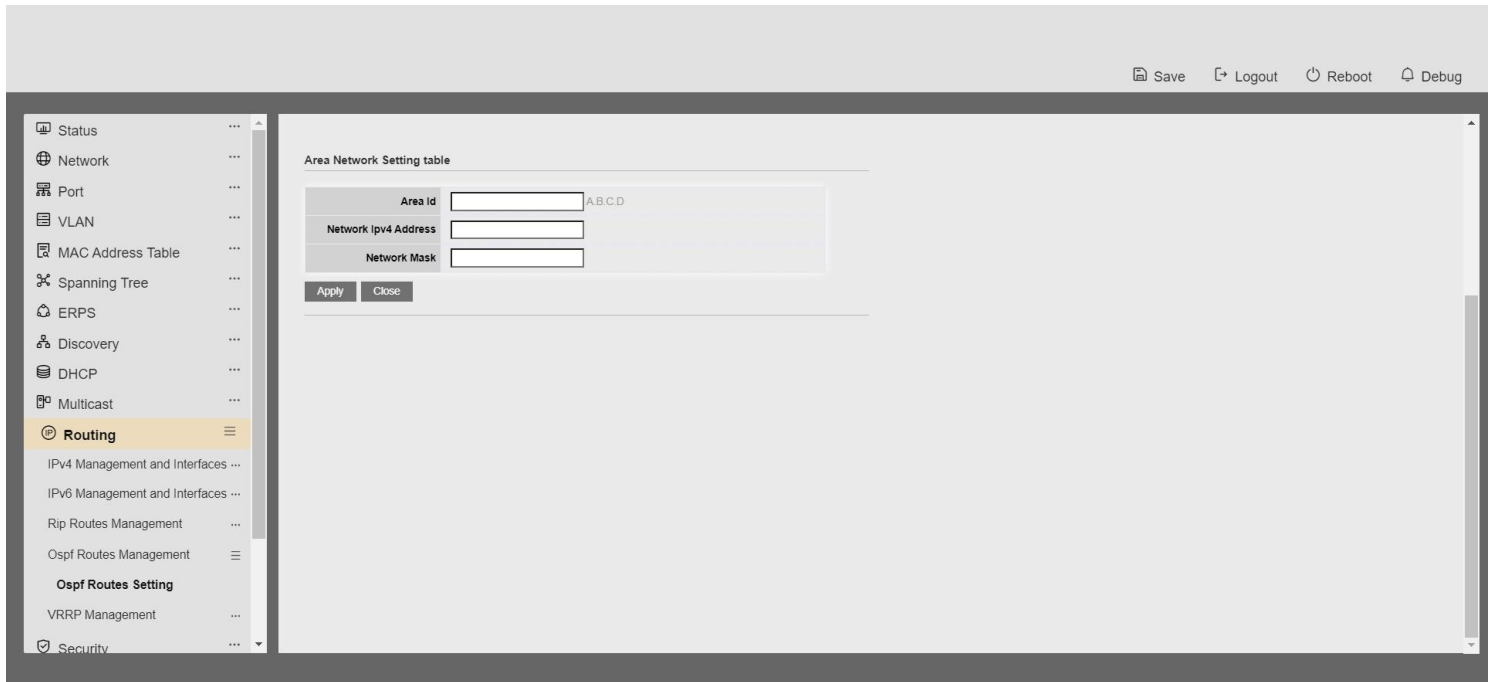


17.4 Ospf Routes Management

1. Click the "Routing > Ospf Route Management > Ospf Route Configuration" menu in the navigation tree to enter the "Ospf Route Configuration" interface, configure the ospf enable configuration, and view the area network configuration table, as shown in the following figure.

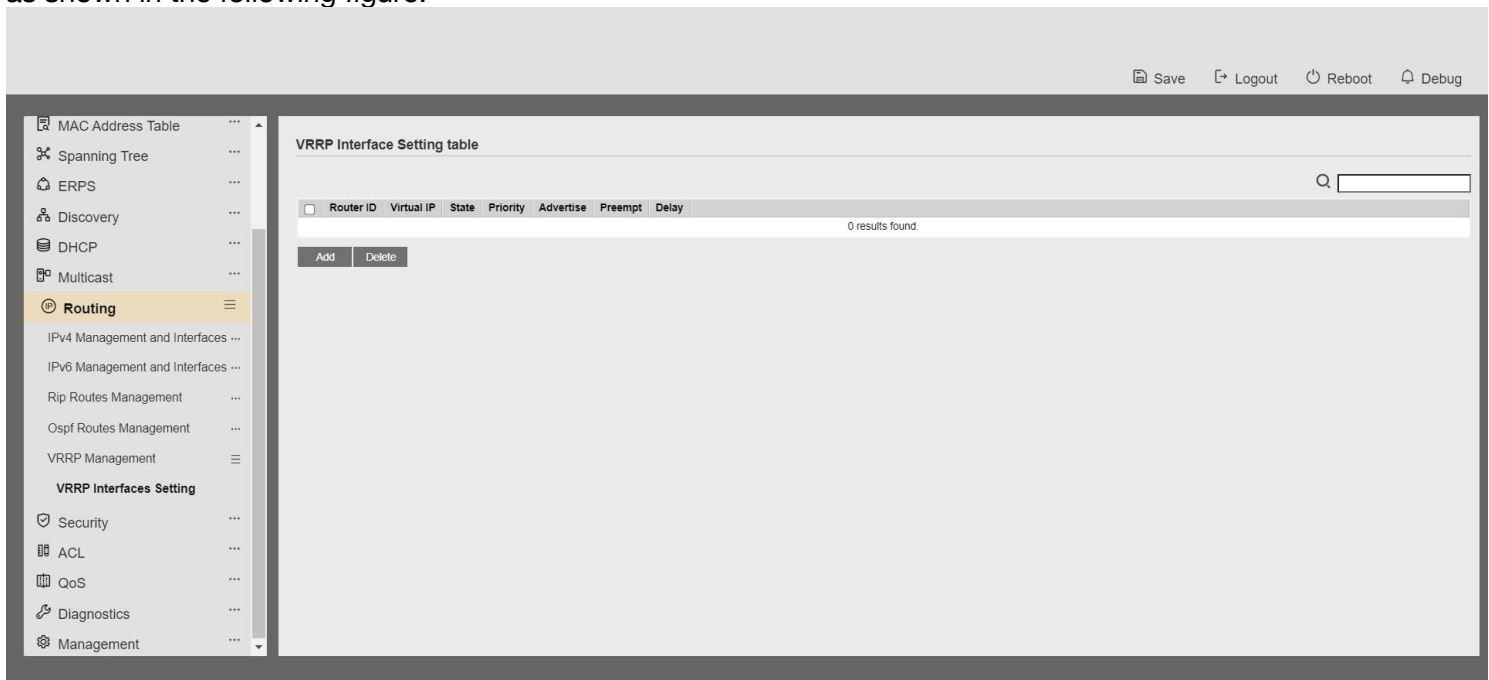


2. Click the Add button to add the Regional Network Configuration Table as shown below:

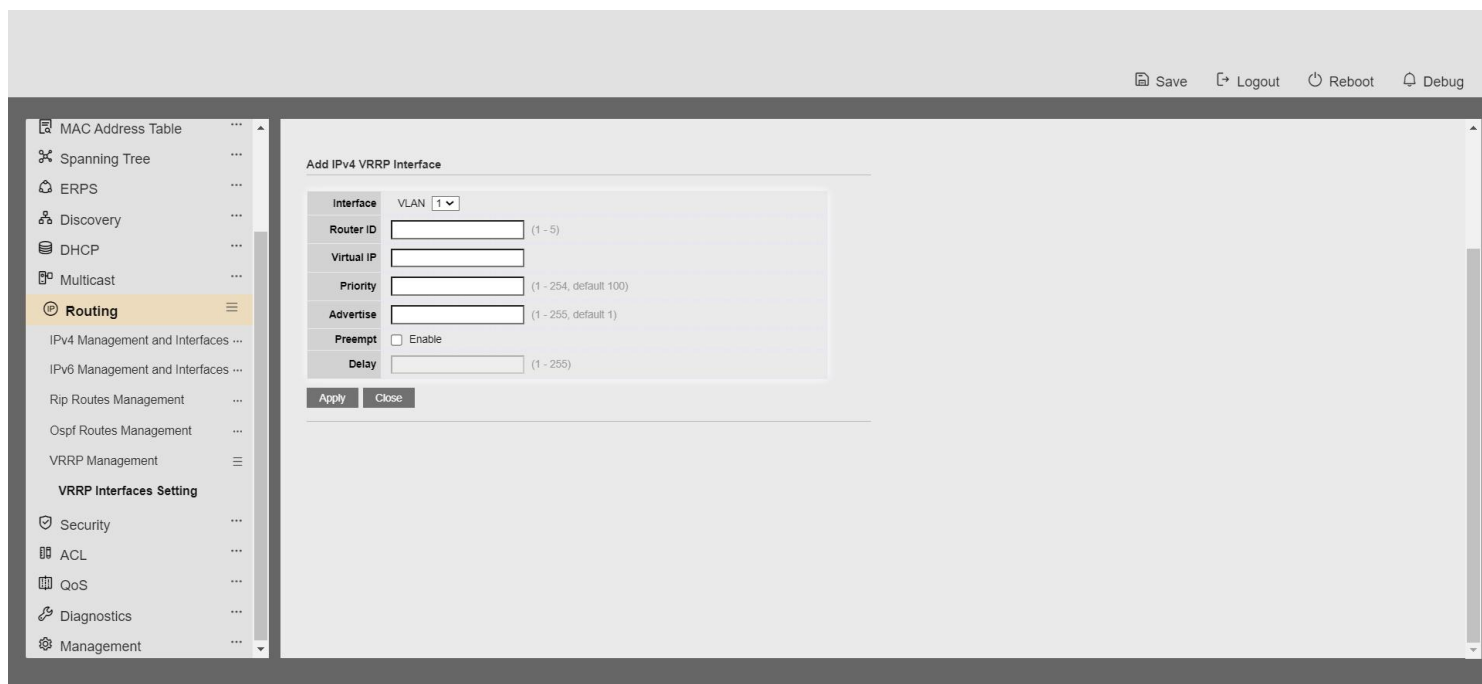


17.5 vrrp management

1. Click the "Routing > vrrp Management" menu in the navigation tree to enter the "vrrp Management" interface, as shown in the following figure.



2. Click Add to enter the configuration screen as shown below:



10 Security

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

10.1. 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.

Status

Network

Port

VLAN

MAC Address Table

Spanning Tree

ERPS

Discovery

DHCP

Multicast

Routing

Security

RADIUS

TACACS+

AAA

Management Access

Authentication Manager

DoS

Use Default Parameter

Retry

3

(1 - 10, default 3)

Timeout

3

Sec (1 - 30, default 3)

Key String

Apply

RADIUS Table

Showing All entries

Showing 0 to 0 of 0 entries

Server Address

Server Port

Priority

Retry

Timeout

Usage

0 results found.

Add

Edit

Delete

First

Previous

1

Next

Last

Figure 10-1 RADIUS Default Setting

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

Table 10-1 RADIUS Default Setting Fields

Managed Switch

143

Rev. 1.0

RADIUS Table

Showing All entries

Showing 1 to 1 of 1 entries

Q

<input type="checkbox"/>	Server Address	Server Port	Priority	Retry	Timeout	Usage
<input type="checkbox"/>	192.168.1.2	1812	32768	3	3	All

Add

Edit

Delete

First

Previous

1

Next

Last

Figure 10-2 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 <ul style="list-style-type: none"> • Login: For login authentifation • 802.1x: For 802.1x authentication • All: For all types

Table 10-2 RADIUS Table Fields

Security >> RADIUS

Add RADIUS Server

Address Type	<input checked="" type="radio"/> Hostname <input type="radio"/> IPv4 <input type="radio"/> IPv6	
Server Address	<input type="text" value="192.168.1.98"/>	
Server Port	<input type="text" value="1812"/>	(0 - 65535, default 1812)
Priority	<input type="text" value="1"/>	(0 - 65535)
Key String	<input checked="" type="checkbox"/> Use Default <input type="text"/>	
Retry	<input checked="" type="checkbox"/> Use Default <input type="text" value="3"/> (1 - 10, default 3)	
Timeout	<input checked="" type="checkbox"/> Use Default <input type="text" value="3"/> Sec (1 - 30, default 3)	
Usage	<input type="radio"/> Login <input type="radio"/> 802.1X <input checked="" type="radio"/> All	

Security >> RADIUS

Edit RADIUS Server

Server Address	<input type="text" value="192.168.1.98"/>	
Server Port	<input type="text" value="1812"/>	(0 - 65535, default 1812)
Priority	<input type="text" value="1"/>	(0 - 65535)
Key String	<input checked="" type="checkbox"/> Use Default <input type="text"/>	
Retry	<input checked="" type="checkbox"/> Use Default <input type="text" value="3"/> (1 - 10, default 3)	
Timeout	<input checked="" type="checkbox"/> Use Default <input type="text" value="3"/> Sec (1 - 30, default 3)	
Usage	<input type="radio"/> Login <input type="radio"/> 802.1X <input checked="" type="radio"/> All	

Figure 10-3 Add/Edit RADIUS Server Dialog

Field	Description
Address Type	In add dialog, user need to specify server Address Type <ul style="list-style-type: none">• 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 <ul style="list-style-type: none">• Login: For login authentication• 802.1x: For 802.1x authentication• All: For all types

Table 10-3 Add/Edit RADIUS Server Fields

10.2. 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.

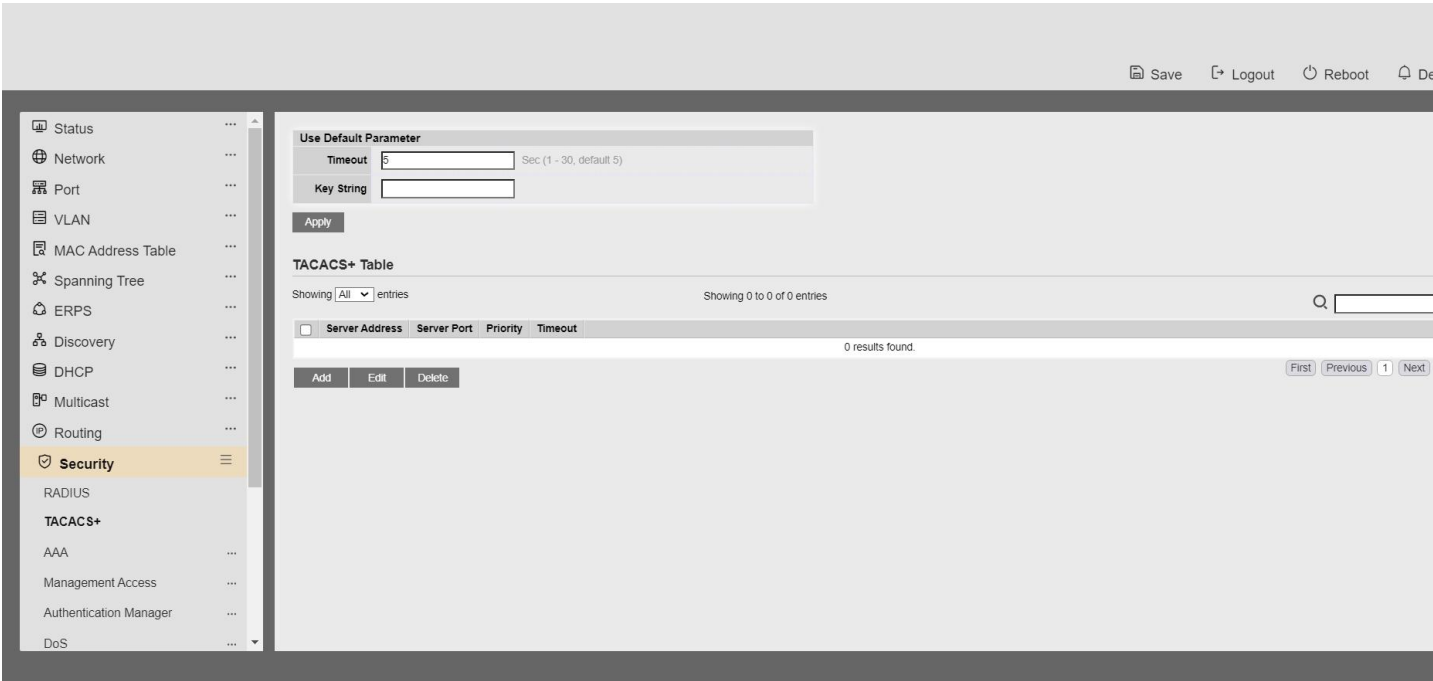


Figure 10-4 TACACS+ Default Setting

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

Table 10-4 TACACS+ Default Setting Fields



Edit TACACS+ Server

Server Address

192.168.1.3

Server Port

49

(0 - 65535, default 49)

Priority

32768

(0 - 65535)

Key String

☒ Use Default

Timeout

☒ Use Default

5

Sec (1 - 30, default 5)

Apply

Close

Figure 10-5 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.

Table 10-5 RADIUS Table Fields

Security >> TACACS+

Add TACACS+ Server

Address Type

☒ Hostname

☐ IPv4

☐ IPv6

Server Address

Server Port

(0 - 65535, default 49)

Priority

(0 - 65535)

Key String

☒ Use Default

Timeout

☒ Use Default

Sec (1 - 30, default 5)

Apply

Close

Security >> TACACS+

Edit TACACS+ Server

Server Address

Server Port

(0 - 65535, default 49)

Priority

(0 - 65535)

Key String

☒ Use Default

Timeout

☒ Use Default

Sec (1 - 30, default 5)

Apply

Close

Figure 10-6 Add/Edit TACACS+ Server Dialog

Field	Description
Address Type	In add dialog, user need to specify server Address Type <ul style="list-style-type: none"> 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.

Table 10-6 Add/Edit TACACS+ Server Fields

10.3. AAA

10.3.1. 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.

Web User Interface

MAC Address Table

Spanning Tree

ERPS

Discovery

DHCP

Multicast

Routing

Security

RADIUS

TACACS+

AAA

Method List

Login Authentication

Management Access

Authentication Manager

DoS

Dynamic ARP Inspection

DHCP Snooping

Method List Table

Showing All entriesShowing 1 to 1 of 1 entries

Name

Sequence

default

(1) Local

Add

Edit

Delete

First

Previous

1

Next

Last

Figure 10-7 Method List Table

Field	Description
Name	Login authentication list name. This name should be different from other existing lists.
Sequence	<p>Priority of login authentication method.</p> <ul style="list-style-type: none"> • 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

Table 10-7 Method List Table Fields

The screenshot shows the 'Add Method List' configuration window in the Web User Interface. The window has a 'Name' field and four 'Method' sections (Method 1 to Method 4). Each method section has radio buttons for 'Empty', 'None', 'Local', 'Enable', 'RADIUS', and 'TACACS+'. The 'Security' menu is open on the left, showing 'Method List' and 'Login Authentication'.

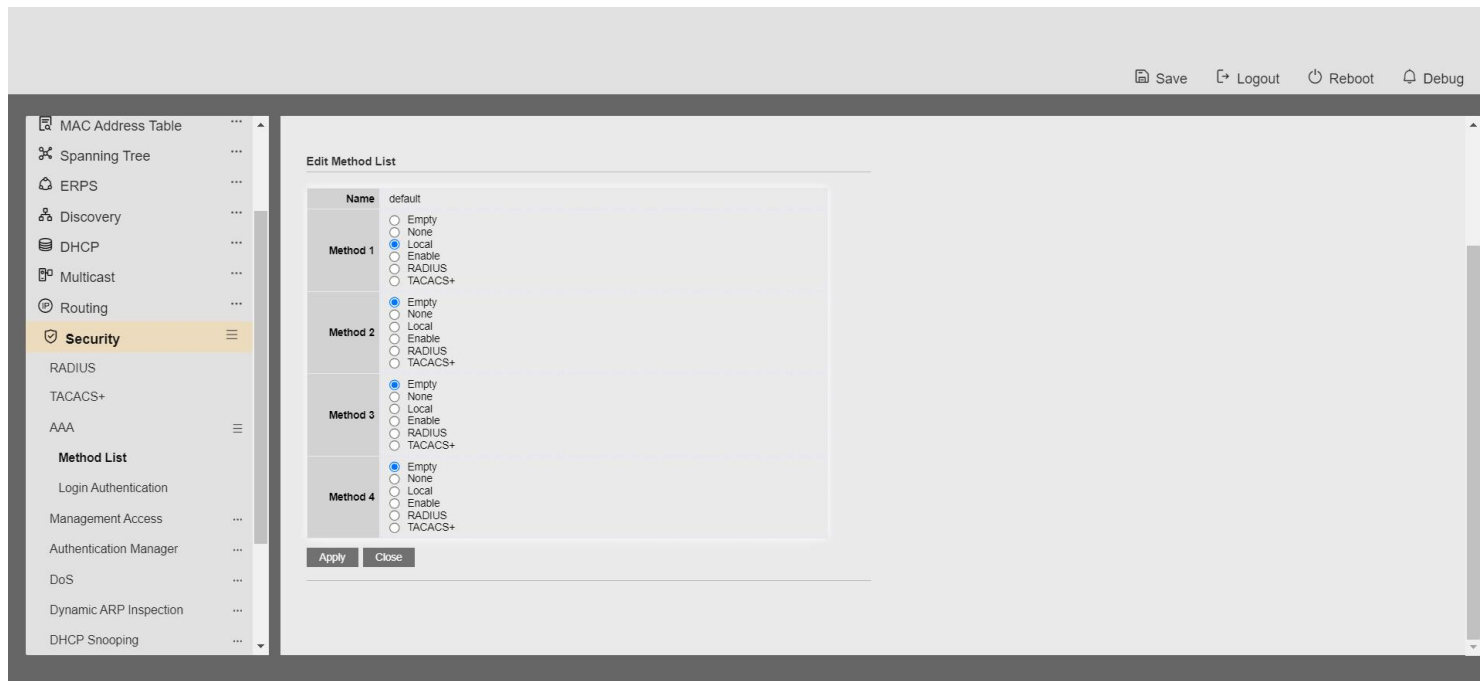


Figure 10-8 Add/Edit Method List Dialog

Field	Description
Name	Login authentication list name. This name should be different from other existing lists.
Method 1	<p>Select first priority of login authentication method.</p> <ul style="list-style-type: none"> • 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	<p>Select second priority of login authentication method.</p> <ul style="list-style-type: none"> • None: Authenticated with any condition. • Local: Use local accounts database to authenticate • TACACS+: Use remote TACACS+ server to

	<ul style="list-style-type: none"> • RADIUS: Use remote Radius server to authenticate. • Enable: Use local enable password to authenticate
	Select third priority of login authentication method.
Method 3	<ul style="list-style-type: none"> • 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
	Select fourth priority of login authentication method.
Method 4	<ul style="list-style-type: none"> • 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

Table 10-8 Add/Edit Method List Fields

10.3.2. 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.

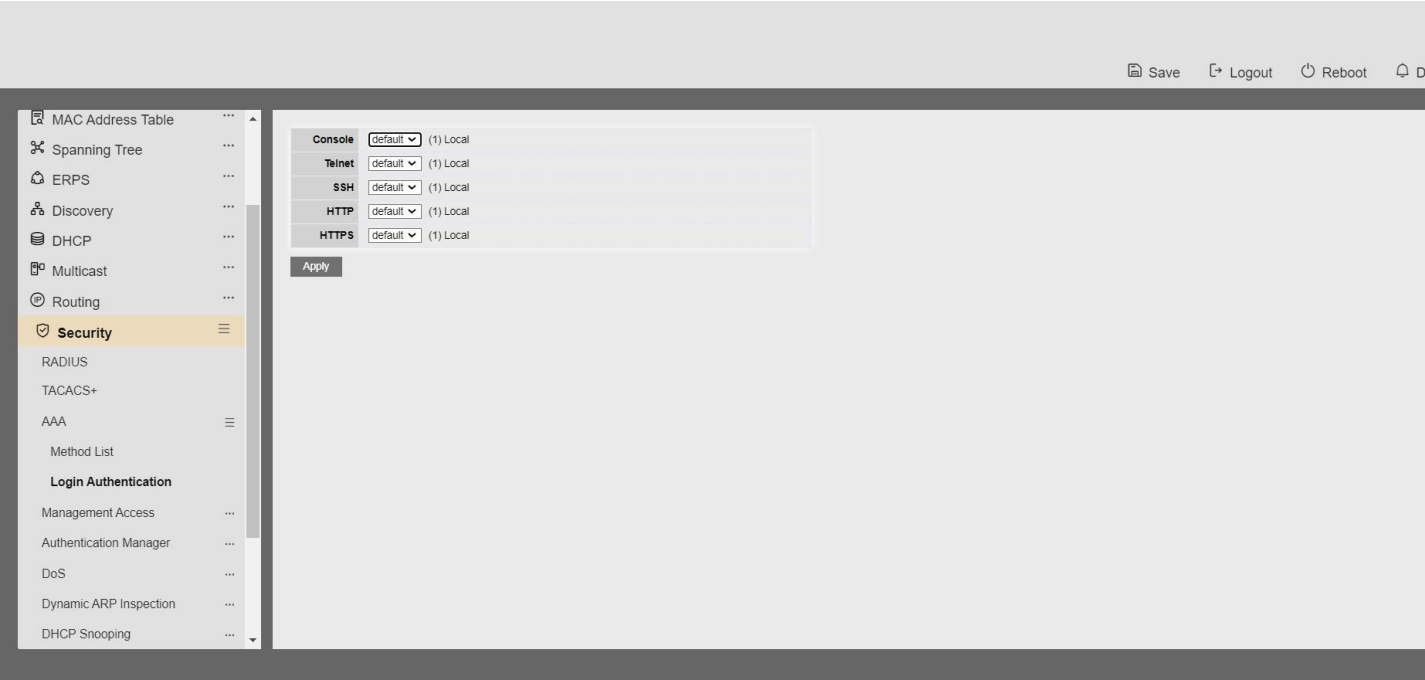


Figure 10-9: Login Authentication Page

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

Table 10-9: Login Authentication Page Fields

10.4. Management Access

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

10.4.1. Management VLAN

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

This page allow user to change management VLAN.

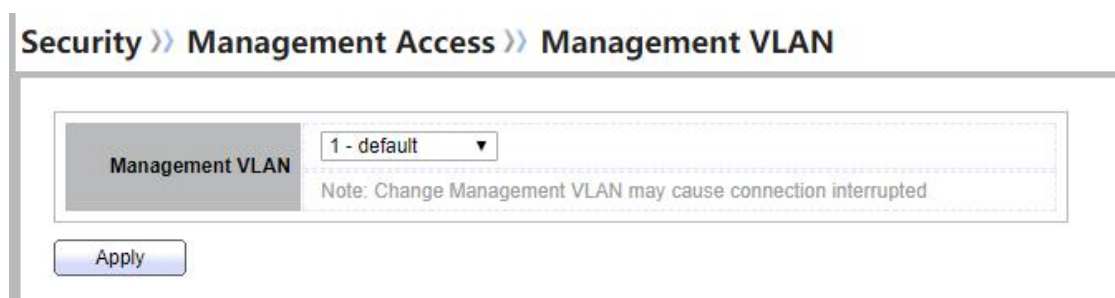


Figure 10-10 Management VLAN Page

Field	Description
Management VLAN	Select management VLAN in option list. Management connection, such as http, https, snmp etc., has the same VLAN of management VLAN are allow connecting to device. Others will be dropped.

Table 10-10 Management VLAN Fields

10.4.2. Management Service

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

This page allow user to change management services related configurations.

MAC Address Table

Spanning Tree

ERPS

Discovery

DHCP

Multicast

Routing

Security

RADIUS

TACACS+

AAA

Management Access

Management Service

Management ACL

Management ACE

Authentication Manager

Property

Port Setting

Management Service

Telnet

SSH

HTTP

HTTPS

SNMP

Enable

Enable

Enable

Enable

Enable

Session Timeout

Console

Telnet

SSH

HTTP

HTTPS

10

10

10

10

10

Min (0 - 65535, default 10)

Min (0 - 65535, default 10)

Min (0 - 65535, default 10)

Min (0 - 65535, default 10)

Min (0 - 65535, default 10)

Password Retry Count

Console

Telnet

SSH

3

3

3

(0 - 120, default 3)

(0 - 120, default 3)

(0 - 120, default 3)

Silent Time

Console

Telnet

SSH

0

0

0

Sec (0 - 65535, default 0)

Sec (0 - 65535, default 0)

Sec (0 - 65535, default 0)

Save

Logout

Reboot

Debug

Figure 10-11 Management Service Page

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

Management Service	<p>Management service admin state.</p> <ul style="list-style-type: none"> • 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	<p>Set session timeout minutes for user access to user interface.</p> <p>0 minutes means never timeout.</p>
Password Retry Count	<p>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.</p>
Silent Time	<p>After input error password exceeds password retry count, the CLI will freeze after silent time.</p>

Table 10-11 Management Service Fields

10.4.3. 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.

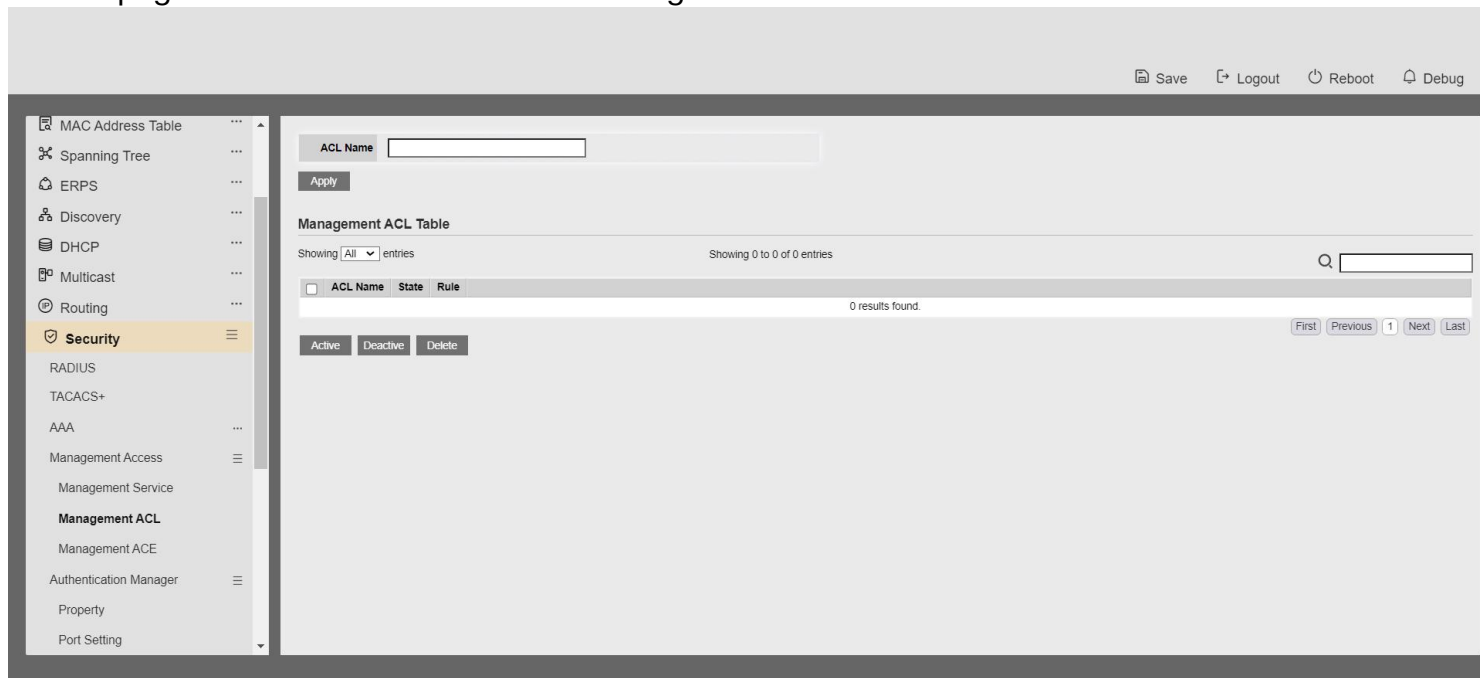


Figure 10-12 Management ACL Page

Field	Description
ACL Name	Input MAC ACL name

Table 10-12 Management ACL Fields

Figure 10-13 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

Table 10-13 Management ACL Table Fields

10.4.4. 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.

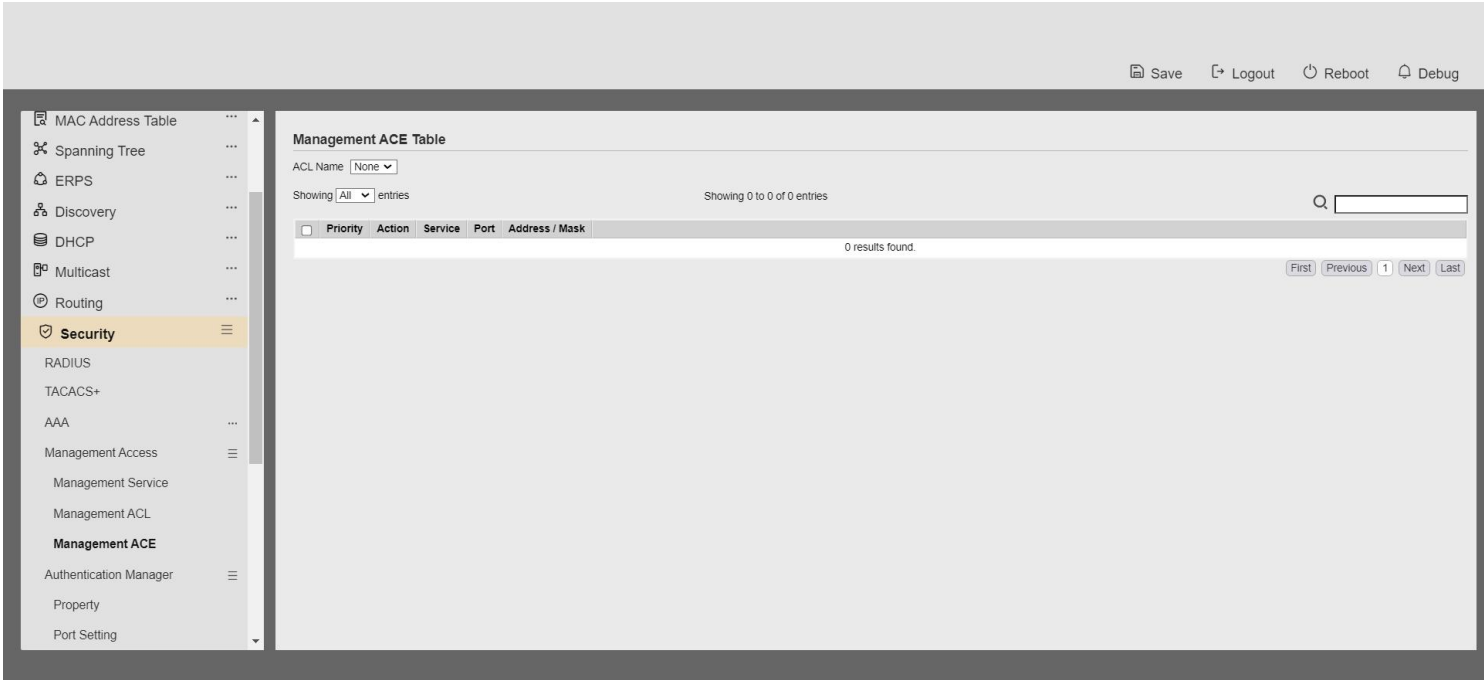


Figure 10-14 Management ACE Page

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.

Table 10-14 Management ACE Fields

Security >> Management Access >> Management ACE

Add Managemet ACE

ACL Name	aaa		
Priority	1 (1 - 65535)		
Service	<input type="radio"/> All <input type="radio"/> Http <input type="radio"/> Https <input checked="" type="radio"/> Snmp <input type="radio"/> SSH <input type="radio"/> Telnet		
Action	<input type="radio"/> Permit <input checked="" type="radio"/> Deny		
Port	Available Port GE1 GE2 GE3 GE4 GE5 GE6 GE7 GE8	<input type="button" value="→"/> <input type="button" value="←"/>	Selected Port
IP Version	<input checked="" type="radio"/> All <input type="radio"/> IPv4 <input type="radio"/> IPv6		
IPv4	/ 255.255.255.255		
IPv6	/ 128 (1 - 128)		

Security >> Management Access >> Management ACE

Edit Managemet ACE

ACL Name	aaa		
Priority	1		
Service	<input type="radio"/> All <input type="radio"/> Http <input type="radio"/> Https <input checked="" type="radio"/> Snmp <input type="radio"/> SSH <input type="radio"/> Telnet		
Action	<input type="radio"/> Permit <input checked="" type="radio"/> Deny		
Port	Available Port GE2 GE4 GE5 GE7 GE8 GE9 GE10 LAG1	<input type="button" value="→"/> <input type="button" value="←"/>	Selected Port GE1 GE3 GE6
IP Version	<input checked="" type="radio"/> All <input type="radio"/> IPv4 <input type="radio"/> IPv6		
IPv4	/ 255.255.255.255		
IPv6	/ 128 (1 - 128)		

Figure 10-15 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. <ul style="list-style-type: none">• 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. <ul style="list-style-type: none">• 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. <ul style="list-style-type: none">• 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.

Table 10-15 Add and Edit Management ACE Fields

10.5. Authentication Manager

10.5.1. 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.



Figure 10-16 Authentication Manager Global Setting

Field	Description
Authentication Type	<p>Set checkbox to enable/disable following authentication types</p> <ul style="list-style-type: none"> 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	<p>Set checkbox to enable/disable guest VLAN, if guest VLAN is enabled, you need to select one available VLAN ID to be</p>
MAC-Based User ID Format	<p>Select mac-based authentication RADIUS username/password ID format.</p> <ul style="list-style-type: none"> XXXXXXXXXXXX XXXXXXXXXXXX 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

Table 10-16 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					
<input type="checkbox"/>	1	GE1	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
<input type="checkbox"/>	2	GE2	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
<input type="checkbox"/>	3	GE3	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
<input type="checkbox"/>	4	GE4	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
<input type="checkbox"/>	5	GE5	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
<input type="checkbox"/>	6	GE6	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
<input type="checkbox"/>	7	GE7	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
<input type="checkbox"/>	8	GE8	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
<input type="checkbox"/>	9	GE9	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
<input type="checkbox"/>	10	GE10	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
<input type="checkbox"/>	11	GE11	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
<input type="checkbox"/>	12	GE12	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
<input type="checkbox"/>	13	GE13	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
<input type="checkbox"/>	14	GE14	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
<input type="checkbox"/>	15	GE15	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
<input type="checkbox"/>	16	GE16	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
<input type="checkbox"/>	17	GE17	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
<input type="checkbox"/>	18	GE18	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
<input type="checkbox"/>	19	GE19	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static

Figure 10-17 Port Mode Table

Field	Description
Port	Port name
Authentication Type (802.1X)	802.1X authentication type state <ul style="list-style-type: none"> • Enabled: 802.1X is enabled • Disabled: 802.1X is disabled
Authentication Type (MAC-Based)	MAC-Based authentication type state <ul style="list-style-type: none"> • Enabled: MAC-Based authentication is enabled • Disabled: MAC-Based authentication is disabled
Authentication Type (WEB-Based)	WEB-Based authentication type state <ul style="list-style-type: none"> • Enabled: WEB-Based authentication is enabled • Disabled: WEB-Based authentication is disabled
Host Mode	Authenticating host mode <ul style="list-style-type: none"> • 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.

	<ul style="list-style-type: none"> • 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	<p>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.</p> <ul style="list-style-type: none"> • 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	<p>Support following authentication method order combinations. These orders only available on MAC-Based authentication and WEB-Based authentication. 802.1x only support Radius method.</p> <ul style="list-style-type: none"> • Local: Use DUT's local database to do authentication • Radius: Use remote RADIUS server to do authentication • Local Radius • Radius Local
Guest VLAN	<p>Port guest VLAN enable state</p> <ul style="list-style-type: none"> • Enabled: Guest VLAN is enabled on port • Disabled: Guest VLAN is disabled on port
VLAN Assign Mode	<p>Support following VLAN assign mode and only apply when source is RADIUS</p> <ul style="list-style-type: none"> • 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.

Table 10-17 Port Mode Table Fields

Edit Port Mode

Port

GE7

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

VLAN Assign Mode

☐ Disable

☐ Reject

☒ Static

Apply

Close

Figure 10-18 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 <ul style="list-style-type: none">Multiple Authentication: In this mode, every client need to pass authenticate procedure individually.

	<ul style="list-style-type: none"> • 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	<p>Support following authentication type order combinations.</p> <p>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.</p> <ul style="list-style-type: none"> • 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	<p>Support following authentication method order combinations. These orders only available on MAC-Based authentication and WEB-Based authentication. 802.1x only support Radius method.</p> <ul style="list-style-type: none"> • Local: Use DUT's local database to do authentication • Radius: Use remote RADIUS server to do authentication • Local Radius • Radius Local
Guest VLAN	<p>Set checkbox to enable/disable guest VLAN</p>
VLAN Assign Mode	<p>Support following VLAN assign mode and only apply when source is RADIUS</p> <ul style="list-style-type: none"> • 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.

Table 10-18 Edit Port Mode Fields

10.5.2. 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

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
<input type="checkbox"/>	1 GE1	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
<input type="checkbox"/>	2 GE2	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
<input type="checkbox"/>	3 GE3	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
<input type="checkbox"/>	4 GE4	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
<input type="checkbox"/>	5 GE5	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
<input type="checkbox"/>	6 GE6	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
<input type="checkbox"/>	7 GE7	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
<input type="checkbox"/>	8 GE8	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
<input type="checkbox"/>	9 GE9	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
<input type="checkbox"/>	10 GE10	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
<input type="checkbox"/>	11 GE11	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
<input type="checkbox"/>	12 GE12	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
<input type="checkbox"/>	13 GE13	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
<input type="checkbox"/>	14 GE14	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
<input type="checkbox"/>	15 GE15	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
<input type="checkbox"/>	16 GE16	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
<input type="checkbox"/>	17 GE17	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
<input type="checkbox"/>	18 GE18	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
<input type="checkbox"/>	19 GE19	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
<input type="checkbox"/>	20 GE20	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
<input type="checkbox"/>	21 GE21	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
<input type="checkbox"/>	22 GE22	Disabled	Disabled	256	3600	60	60	30	30	30	2	3

Figure 10-19: Authentication Manager Port Setting Table

Field	Description
Port	Port name
Port Control	<p>Support following authentication port control types.</p> <ul style="list-style-type: none"> • 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	<p>Reauthenticate state</p> <ul style="list-style-type: none"> • Enabled: Host will be reauthenticated after reauthentication period • Disabled: Host will not be reauthenticated after 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)	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.

Table 10-19: Authentication Manager Port Setting Table Fields

The screenshot shows the 'Edit Port Setting' dialog in the Web User Interface. The dialog is titled 'Edit Port Setting' and contains the following sections:

- 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:**
 - ☐ Infinite
 - Max Login:** 3 (3 - 10, default 3)

At the bottom of the dialog are 'Apply' and 'Close' buttons. The left sidebar shows a navigation menu with 'Security' selected. The top right of the interface has buttons for 'Save', 'Logout', 'Reboot', and 'Debug'.

Figure 10-20: Authentication Manager Port Setting Dialog

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

Port

Port name

Support following authentication port control types.

Port Control

- **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.

	<ul style="list-style-type: none"> • 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.

Table 10-20: Authentication Manager Port Setting Table Fields

10.5.3. 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.

MAC-Based Local Account Table

Showing

All

 entries

Showing 0 to 0 of 0 entries

<input type="checkbox"/>	MAC Address	Control	VLAN	Timeout (Sec)	
				Reauthentication	Inactive

0 results found.

Add

Edit

Delete

Figure 10-21 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 <ul style="list-style-type: none">Force Authorized: Host will be force authorizedForce 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.

Table 10-21 MAC-Based Local Account Table Fields

Add MAC-Based Local Account

MAC Address

Port Control

☒ Force Authorized

☐ Force Unauthorized

VLAN

☐ User Defined

1

(1 - 4094)

Assigned Timer

Reauthentication

☐ User Defined

3600

Sec (300 - 2147483647)

Inactive

☐ User Defined

60

Sec (60 - 65535)

Apply

Close

Edit MAC-Based Local Account

MAC Address

00:00:00:00:00:0A

Port Control

☒ Force Authorized

☐ Force Unauthorized

VLAN

☒ User Defined

1

(1 - 4094)

Assigned Timer

Reauthentication

☒ User Defined

3600

Sec (300 - 2147483647)

Inactive

☒ User Defined

60

Sec (60 - 65535)

Apply

Close

Figure 10-22 Add/Edit MAC-Based Local Account Dialog

Manaa	Field	Description	ev. 1.0
-------	-------	-------------	---------

MAC Address	Authenticated host MAC address, and each MAC allow only one entry in local database.
Control	Control Type <ul style="list-style-type: none"> • 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.

Table 10-22 Add/Edit MAC-Based Local Account Fields

10.5.4. 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.

WEB-Based Local Account Table

Showing All entries

Showing 0 to 0 of 0 entries

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

Add

Edit

Delete

Figure 10-23 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.

Table 10-23 WEB-Based Local Account Table Fields

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)

Apply

Close

Figure 10-24 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.

Table 10-24 Add/Edit WEB-Based Local Account Fields

10.5.5. 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.

Sessions Table

Showing

All

 entries

Showing 0 to 0 of 0 entries

<div></div>	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

Figure 10-25 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 <ul style="list-style-type: none"> • 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 (Inactivated)	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.

Table 10-25 Sessions Table Fields

10.6. 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.

10.6.1. Property

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

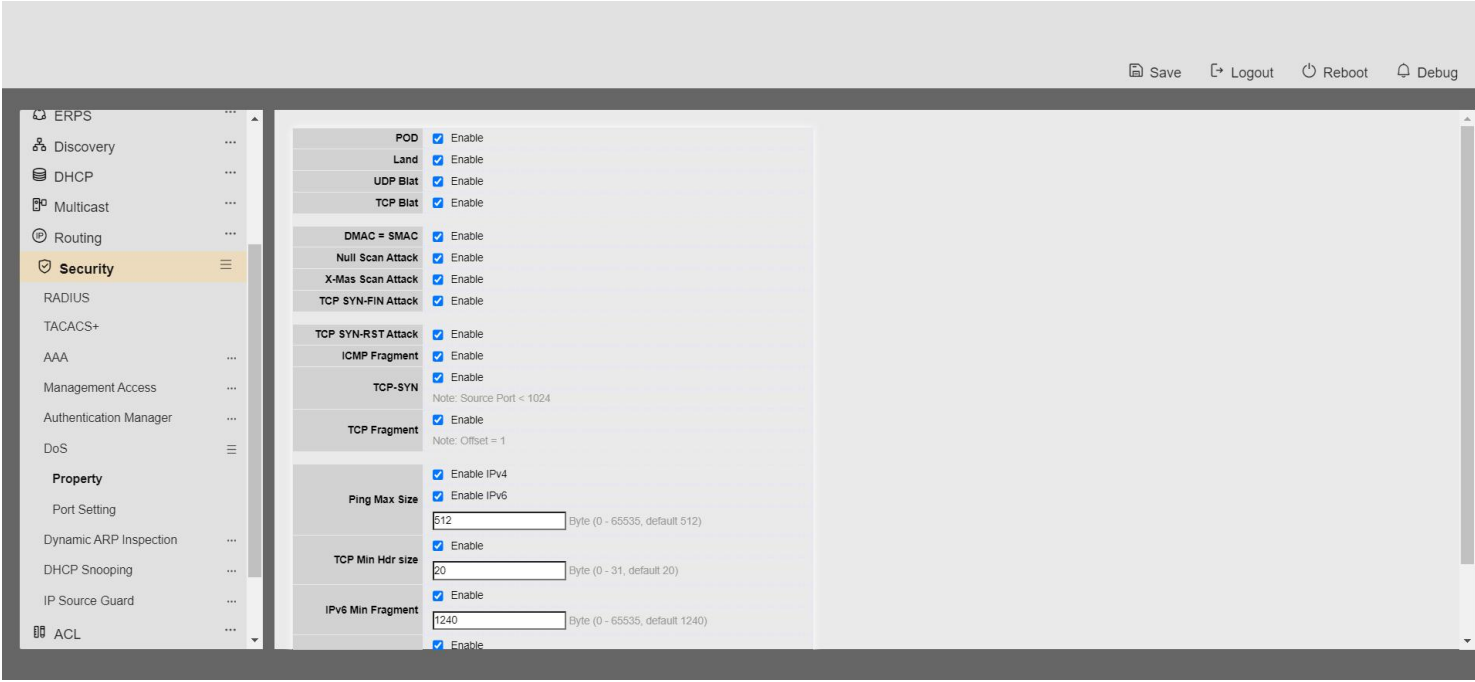


Figure 10-31 DoS Property Page

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.

Table 10-31: DoS Property fields.

10.6.2. Port Setting

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

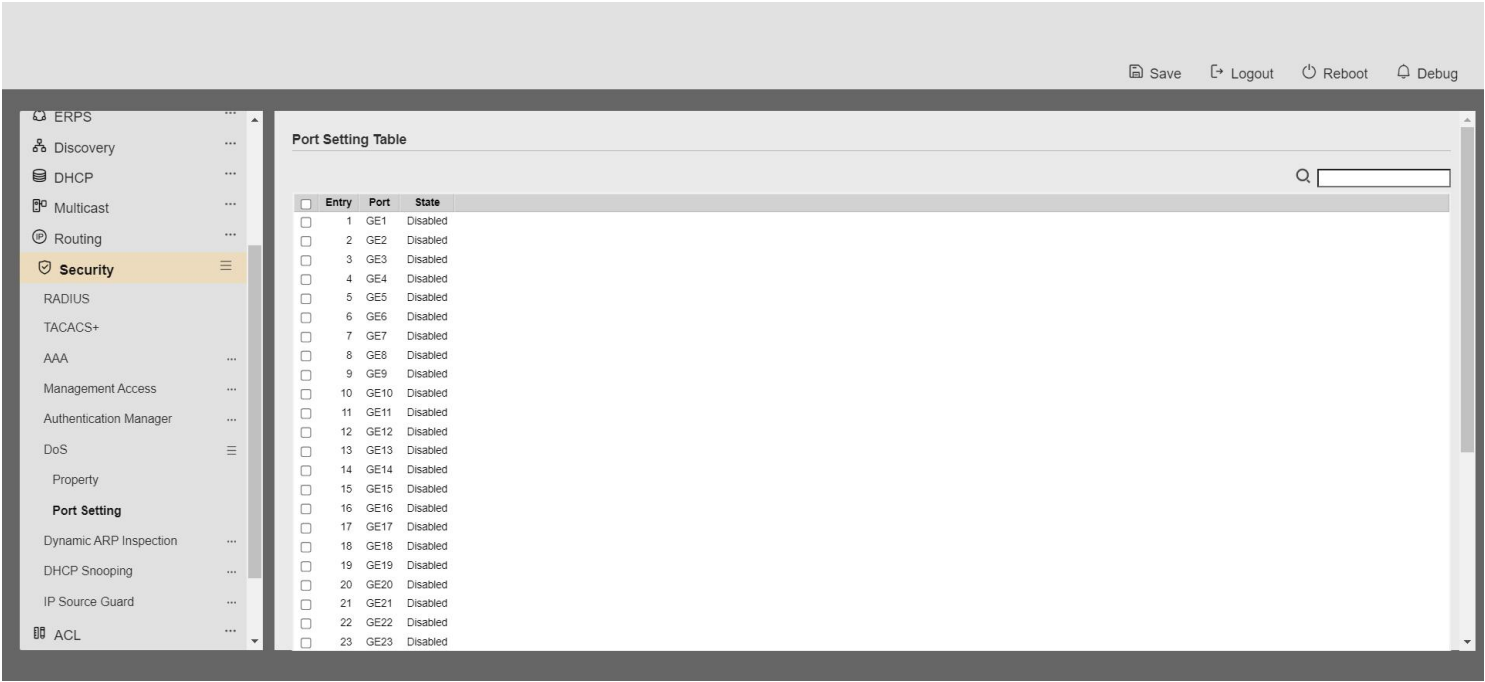


Figure 10-32: Port Setting page.

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

Table 10-32: Port Setting fields.

10.10. Dynamic ARP Inspection

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

10.10.1.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.

State

☐ Enable

VLAN

Available VLAN

Selected VLAN

VLAN 1

Apply

Figure 10-33 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.

Table 10-33 Property Fields

Port Setting Table

	Entry	Port	Trust	Source MAC Address	Destination MAC Address	IP Address	Rate Limit
<input type="checkbox"/>	1	GE1	Disabled	Disabled	Disabled	Disabled	Unlimited
<input type="checkbox"/>	2	GE2	Disabled	Disabled	Disabled	Disabled	Unlimited
<input checked="" type="checkbox"/>	3	GE3	Disabled	Disabled	Disabled	Disabled	Unlimited
<input type="checkbox"/>	4	GE4	Disabled	Disabled	Disabled	Disabled	Unlimited
<input type="checkbox"/>	5	GE5	Disabled	Disabled	Disabled	Disabled	Unlimited
<input type="checkbox"/>	6	GE6	Disabled	Disabled	Disabled	Disabled	Unlimited
<input type="checkbox"/>	7	GE7	Disabled	Disabled	Disabled	Disabled	Unlimited
<input type="checkbox"/>	8	GE8	Disabled	Disabled	Disabled	Disabled	Unlimited
<input type="checkbox"/>	9	GE9	Disabled	Disabled	Disabled	Disabled	Unlimited
<input type="checkbox"/>	10	GE10	Disabled	Disabled	Disabled	Disabled	Unlimited
<input type="checkbox"/>	11	GE11	Disabled	Disabled	Disabled	Disabled	Unlimited
<input type="checkbox"/>	12	GE12	Disabled	Disabled	Disabled	Disabled	Unlimited
<input type="checkbox"/>	13	GE13	Disabled	Disabled	Disabled	Disabled	Unlimited
<input type="checkbox"/>	14	GE14	Disabled	Disabled	Disabled	Disabled	Unlimited
<input type="checkbox"/>	15	GE15	Disabled	Disabled	Disabled	Disabled	Unlimited
<input type="checkbox"/>	16	GE16	Disabled	Disabled	Disabled	Disabled	Unlimited
<input type="checkbox"/>	17	GE17	Disabled	Disabled	Disabled	Disabled	Unlimited
<input type="checkbox"/>	18	GE18	Disabled	Disabled	Disabled	Disabled	Unlimited
<input type="checkbox"/>	19	GE19	Disabled	Disabled	Disabled	Disabled	Unlimited
<input type="checkbox"/>	20	GE20	Disabled	Disabled	Disabled	Disabled	Unlimited
<input type="checkbox"/>	21	GE21	Disabled	Disabled	Disabled	Disabled	Unlimited
<input type="checkbox"/>	22	GE22	Disabled	Disabled	Disabled	Disabled	Unlimited

Figure 10-34 Property Port Page

Field	Description
Port	Display port ID.
Trust	Display enable/disable trust attribute of interface

Source MAC Address	Display enable/disabled source mac address validation attribute of interface
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.

Table 10-34 Property Port Fields

Edit Port Setting

Port	GE3
Trust	<input type="checkbox"/> Enable
Source MAC Address	<input type="checkbox"/> Enable
Destination MAC Address	<input type="checkbox"/> Enable
IP Address	<input type="checkbox"/> Enable <input type="checkbox"/> Allow Zero (0.0.0.0)
Rate Limit	<input type="text" value="0"/> pps (1 - 50, default 0), 0 is Unlimited

Apply

Close

Figure 10-35 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 <hr/> 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. <hr/>

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.

le 10-35 Edit Property Port Fields

10.10.2. Statistics

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

Statistics Table									
									Q. <input type="text"/>
<input type="checkbox"/>	Entry	Port	Forward	Source MAC Failure	Destination MAC Failure	Source IP Validation Failure	Destination IP Validation Failure	IP-MAC Mismatch Failure	
<input type="checkbox"/>	1	GE1	0	0	0	0	0	0	
<input type="checkbox"/>	2	GE2	0	0	0	0	0	0	
<input type="checkbox"/>	3	GE3	0	0	0	0	0	0	
<input type="checkbox"/>	4	GE4	0	0	0	0	0	0	
<input type="checkbox"/>	5	GE5	0	0	0	0	0	0	
<input type="checkbox"/>	6	GE6	0	0	0	0	0	0	
<input type="checkbox"/>	7	GE7	0	0	0	0	0	0	
<input type="checkbox"/>	8	GE8	0	0	0	0	0	0	
<input type="checkbox"/>	9	GE9	0	0	0	0	0	0	
<input type="checkbox"/>	10	GE10	0	0	0	0	0	0	
<input type="checkbox"/>	11	GE11	0	0	0	0	0	0	
<input type="checkbox"/>	12	GE12	0	0	0	0	0	0	
<input type="checkbox"/>	13	GE13	0	0	0	0	0	0	
<input type="checkbox"/>	14	GE14	0	0	0	0	0	0	
<input type="checkbox"/>	15	GE15	0	0	0	0	0	0	
<input type="checkbox"/>	16	GE16	0	0	0	0	0	0	
<input type="checkbox"/>	17	GE17	0	0	0	0	0	0	
<input type="checkbox"/>	18	GE18	0	0	0	0	0	0	
<input type="checkbox"/>	19	GE19	0	0	0	0	0	0	
<input type="checkbox"/>	20	GE20	0	0	0	0	0	0	
<input type="checkbox"/>	21	GE21	0	0	0	0	0	0	
<input type="checkbox"/>	22	GE22	0	0	0	0	0	0	

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

Figure 10-36 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.
---	--

Table 10-36 Statistics Fields

10.11. DHCP Snooping

Use the DHCP Snooping pages to configure settings of DHCP Snooping

10.11.1.Property

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

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

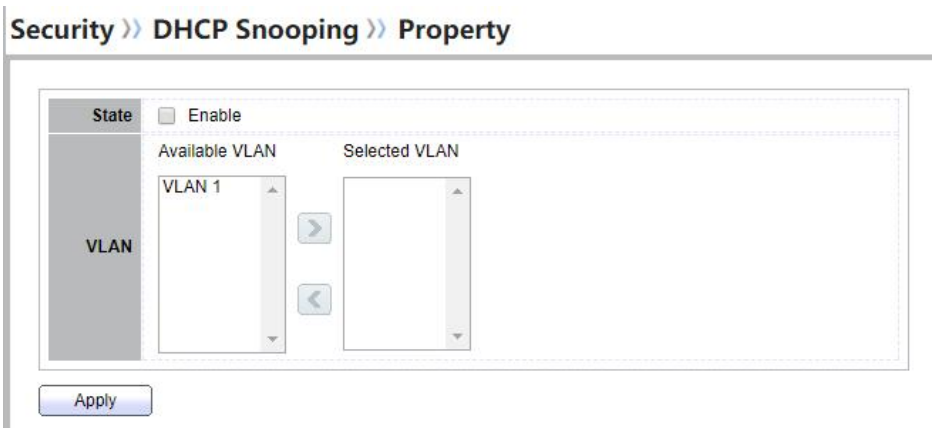


Figure 10-37 Property Page

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.

Table 10-37 Property Fields

Port Setting Table					
<input type="checkbox"/>	Entry	Port	Trust	Verify Chaddr	Rate Limit
<input type="checkbox"/>	1	GE1	Disabled	Disabled	Unlimited
<input type="checkbox"/>	2	GE2	Disabled	Disabled	Unlimited
<input type="checkbox"/>	3	GE3	Disabled	Disabled	Unlimited
<input type="checkbox"/>	4	GE4	Disabled	Disabled	Unlimited
<input type="checkbox"/>	5	GE5	Disabled	Disabled	Unlimited
<input type="checkbox"/>	6	GE6	Disabled	Disabled	Unlimited
<input type="checkbox"/>	7	GE7	Disabled	Disabled	Unlimited
<input type="checkbox"/>	8	GE8	Disabled	Disabled	Unlimited
<input type="checkbox"/>	9	GE9	Disabled	Disabled	Unlimited
<input type="checkbox"/>	10	GE10	Disabled	Disabled	Unlimited
<input type="checkbox"/>	11	GE11	Disabled	Disabled	Unlimited
<input type="checkbox"/>	12	GE12	Disabled	Disabled	Unlimited
<input type="checkbox"/>	13	GE13	Disabled	Disabled	Unlimited
<input type="checkbox"/>	14	GE14	Disabled	Disabled	Unlimited
<input type="checkbox"/>	15	GE15	Disabled	Disabled	Unlimited
<input type="checkbox"/>	16	GE16	Disabled	Disabled	Unlimited
<input type="checkbox"/>	17	GE17	Disabled	Disabled	Unlimited
<input type="checkbox"/>	18	GE18	Disabled	Disabled	Unlimited
<input type="checkbox"/>	19	GE19	Disabled	Disabled	Unlimited
<input type="checkbox"/>	20	GE20	Disabled	Disabled	Unlimited
<input type="checkbox"/>	21	GE21	Disabled	Disabled	Unlimited
<input type="checkbox"/>	22	GE22	Disabled	Disabled	Unlimited

Figure 10-38 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.

Table 10-38 Property Port Fields

Edit Port Setting

Port

GE14

Trust

☐ Enable

Verify Chaddr

☐ Enable

Rate Limit

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

Apply

Close

Figure 10-39 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.

le 10-39 Edit Property Port Fields

10.11.2.Statistics

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

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

Statistics Table								
<input type="checkbox"/>	Entry	Port	Forward	Chaddr Check Drop	Untrust Port Drop	Untrust Port with Option82 Drop	Invalid Drop	
<input type="checkbox"/>	1	GE1	0	0	0	0	0	0
<input type="checkbox"/>	2	GE2	0	0	0	0	0	0
<input type="checkbox"/>	3	GE3	0	0	0	0	0	0
<input type="checkbox"/>	4	GE4	0	0	0	0	0	0
<input type="checkbox"/>	5	GE5	0	0	0	0	0	0
<input type="checkbox"/>	6	GE6	0	0	0	0	0	0
<input type="checkbox"/>	7	GE7	0	0	0	0	0	0
<input type="checkbox"/>	8	GE8	0	0	0	0	0	0
<input type="checkbox"/>	9	GE9	0	0	0	0	0	0
<input type="checkbox"/>	10	GE10	0	0	0	0	0	0
<input type="checkbox"/>	11	GE11	0	0	0	0	0	0
<input type="checkbox"/>	12	GE12	0	0	0	0	0	0
<input type="checkbox"/>	13	GE13	0	0	0	0	0	0
<input type="checkbox"/>	14	GE14	0	0	0	0	0	0
<input type="checkbox"/>	15	GE15	0	0	0	0	0	0
<input type="checkbox"/>	16	GE16	0	0	0	0	0	0
<input type="checkbox"/>	17	GE17	0	0	0	0	0	0
<input type="checkbox"/>	18	GE18	0	0	0	0	0	0
<input type="checkbox"/>	19	GE19	0	0	0	0	0	0
<input type="checkbox"/>	20	GE20	0	0	0	0	0	0
<input type="checkbox"/>	21	GE21	0	0	0	0	0	0

Figure 10-40 DHCP Snooping Statistics Page

Field	Description
Port	Display port ID
Forwarded	Display how packets forwarded normally.
Chaddr Check	Display how many packets dropped by chaddr validation.

Drop

**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.
--------------	---

Table 10-40 Statistics Fields

10.11.3.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.

Remote ID

☐ User Defined

Operational Status

Remote ID

00:e0:53:17:fd:66 (Switch Mac in Byte Order)

Apply

Figure 10-41 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					<input type="text"/>	
<input type="checkbox"/>	Entry	Port	State	Allow Untrust		
<input type="checkbox"/>	1	GE1	Disabled	Drop		
<input type="checkbox"/>	2	GE2	Disabled	Drop		
<input type="checkbox"/>	3	GE3	Disabled	Drop		
<input type="checkbox"/>	4	GE4	Disabled	Drop		
<input type="checkbox"/>	5	GE5	Disabled	Drop		
<input type="checkbox"/>	6	GE6	Disabled	Drop		
<input type="checkbox"/>	7	GE7	Disabled	Drop		
<input type="checkbox"/>	8	GE8	Disabled	Drop		
<input type="checkbox"/>	9	GE9	Disabled	Drop		
<input type="checkbox"/>	10	GE10	Disabled	Drop		
<input type="checkbox"/>	11	GE11	Disabled	Drop		
<input type="checkbox"/>	12	GE12	Disabled	Drop		
<input type="checkbox"/>	13	GE13	Disabled	Drop		
<input type="checkbox"/>	14	GE14	Disabled	Drop		
<input type="checkbox"/>	15	GE15	Disabled	Drop		
<input type="checkbox"/>	16	GE16	Disabled	Drop		
<input type="checkbox"/>	17	GE17	Disabled	Drop		
<input type="checkbox"/>	18	GE18	Disabled	Drop		
<input type="checkbox"/>	19	GE19	Disabled	Drop		
<input type="checkbox"/>	20	GE20	Disabled	Drop		
<input type="checkbox"/>	21	GE21	Disabled	Drop		
<input type="checkbox"/>	22	GE22	Disabled	Drop		
<input type="checkbox"/>	23	GE23	Disabled	Drop		
<input type="checkbox"/>	24	GE24	Disabled	Drop		

Figure 10-42 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

Table 10-42 Option82 Port Fields

Security >> DHCP Snooping >> Option82 Property

Edit Port Setting

Port	GE5
State	<input checked="" type="checkbox"/> Enable
Allow Untrust	<input type="radio"/> Keep <input checked="" type="radio"/> Drop <input type="radio"/> Replace

Apply Close

Figure 10-43 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. <ul style="list-style-type: none">• Keep: Keep original option82 content.• Replace: Replace option82 content by switch setting• Drop: Drop packets with option82.

Table 10-43 Edit Option82 Port Fields

10.11.4. 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.

Option82 Circuit ID Table

Showing

All

 entries

Showing 0 to 0 of 0 entries

☐

Port

VLAN

Circuit ID

0 results found.

Add

Edit

Delete

Figure 10-44 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

Table 10-44 Option82 Circuit ID Fields

Add Option82 Circuit ID

Port

GE1

VLAN

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

Circuit ID

Apply

Close

Edit Option82 Circuit ID

Port	GE1
VLAN	1
Circuit ID	<input type="text" value="rainbow"/>

Apply

Close

Figure 10-45 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.

Table 10-45 Option82 Circuit ID Fields

10.12. IP Source Guard

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

10.12.1.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.

Port Setting Table							
<input type="checkbox"/>	Entry	Port	State	Verify Source	Current Entry	Max Entry	
<input type="checkbox"/>	1	GE1	Disabled	IP	0	Unlimited	
<input type="checkbox"/>	2	GE2	Disabled	IP	0	Unlimited	
<input type="checkbox"/>	3	GE3	Disabled	IP	0	Unlimited	
<input type="checkbox"/>	4	GE4	Disabled	IP	0	Unlimited	
<input type="checkbox"/>	5	GE5	Disabled	IP	0	Unlimited	
<input type="checkbox"/>	6	GE6	Disabled	IP	0	Unlimited	
<input type="checkbox"/>	7	GE7	Disabled	IP	0	Unlimited	
<input type="checkbox"/>	8	GE8	Disabled	IP	0	Unlimited	
<input type="checkbox"/>	9	GE9	Disabled	IP	0	Unlimited	
<input type="checkbox"/>	10	GE10	Disabled	IP	0	Unlimited	
<input type="checkbox"/>	11	GE11	Disabled	IP	0	Unlimited	
<input type="checkbox"/>	12	GE12	Disabled	IP	0	Unlimited	
<input type="checkbox"/>	13	GE13	Disabled	IP	0	Unlimited	
<input type="checkbox"/>	14	GE14	Disabled	IP	0	Unlimited	
<input type="checkbox"/>	15	GE15	Disabled	IP	0	Unlimited	
<input type="checkbox"/>	16	GE16	Disabled	IP	0	Unlimited	
<input type="checkbox"/>	17	GE17	Disabled	IP	0	Unlimited	
<input type="checkbox"/>	18	GE18	Disabled	IP	0	Unlimited	
<input type="checkbox"/>	19	GE19	Disabled	IP	0	Unlimited	
<input type="checkbox"/>	20	GE20	Disabled	IP	0	Unlimited	
<input type="checkbox"/>	21	GE21	Disabled	IP	0	Unlimited	
<input type="checkbox"/>	22	GE22	Disabled	IP	0	Unlimited	
<input type="checkbox"/>	23	GE23	Disabled	IP	0	Unlimited	

Figure 10-46 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

Table 10-46 Port Setting Fields

Figure 10-47 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 <ul style="list-style-type: none"> 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 un-limited on all ports. No entry will be bound if limitation reached.

Table 10-47 Edit Port Setting Fields

10.12.2.IMPV Binding

To display IPMV 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.

IP-MAC-Port-VLAN Binding Table

Showing All entries

Showing 0 to 0 of 0 entries

<input type="checkbox"/>	Port	VLAN	MAC Address	IP Address	Binding	Type	Lease Time
0 results found.							

Add

Edit

Delete

Figure 10-48 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 <ul style="list-style-type: none"> 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.

Table 10-48 IPMV Binding Fields

Add IP-MAC-Port-VLAN Binding

Port

GE1

VLAN

Empty value is invalid.

Binding

☒ IP-MAC-Port-VLAN

☐ IP-Port-VLAN

MAC Address

Empty value is invalid.

IP Address

Empty value is invalid.

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

Figure 10-49 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 <ul style="list-style-type: none">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.
-------------------	---

Table 10-49 Add and Edit IPMV Binding Fields

10.12.3. 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.

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)

Apply

Figure 10-50 Save Database Page

Field	Description
Type	Select the type of database agent. <ul style="list-style-type: none">None: Disable database agent service.Flash: Save DHCP dynamic binding entries to flash.TFTP: Save DHCP dynamic binding entries to remote TFTP server.
Filename	Input filename for backup file. Only available when selecting type “flash” and “TFTP”.
Address Type	Select the type of TFTP server. <ul style="list-style-type: none">Hostname: TFTP server address is hostname.IPv4: TFTP server address is IPv4 address.
Server Address	Input remote TFTP server hostname or IP address. Only available when selecting type “TFTP”
Write Delay	Input delay timer for doing backup after change happened. Default is 300 seconds.
Timeout	Input aborts timeout for doing backup failure. Default is 300 seconds.

11

AC

L

Save Database Fields

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

11.1. 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.

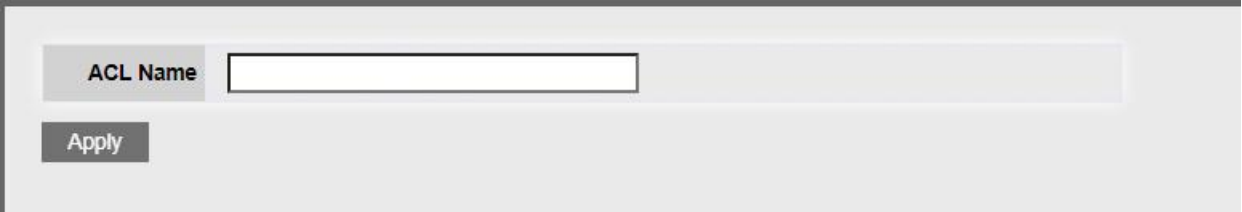


Figure 11-1 MAC ACL Page

Field	Description
ACL Name	Input MAC ACL name

Table 11-1 MAC ACL Fields



Figure 11-2 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

Table 11-2 MAC ACL Table Fields

11.2. 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.

ACE Table

ACL Name None

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.										

First
Previous
1
Next
Last

Figure 11-3 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.

Table 11-3 MAC ACE Fields

Add ACE

ACL Name	aaaaaa		
Sequence	<input type="text" value="32768"/>	(1 - 2147483647)	
Action	<input checked="" type="radio"/> Permit <input type="radio"/> Deny <input type="radio"/> Shutdown		
Source MAC	<input checked="" type="checkbox"/> Any <div><input type="text"/></div> / <div><input type="text"/></div> (Address / Mask)		
Destination MAC	<input checked="" type="checkbox"/> Any <div><input type="text"/></div> / <div><input type="text"/></div> (Address / Mask)		
Ethertype	<input checked="" type="checkbox"/> Any 0x <div><input type="text"/></div> (0x600 ~ 0xFFFF)		
VLAN	<input checked="" type="checkbox"/> Any <div><input type="text"/></div> (1 - 4094)		
802.1p	<input checked="" type="checkbox"/> Any <div><input type="text"/></div> / <div><input type="text"/></div> (Value / Mask) (0 - 7)		

Apply

Close

Edit ACE

ACL Name	aaaaaa		
Sequence	32768		
Action	<input checked="" type="radio"/> Permit <input type="radio"/> Deny <input type="radio"/> Shutdown		
Source MAC	<input checked="" type="checkbox"/> Any		
	<input type="text"/>	/	<input type="text"/> (Address / Mask)
Destination MAC	<input checked="" type="checkbox"/> Any		
	<input type="text"/>	/	<input type="text"/> (Address / Mask)
Ethertype	<input checked="" type="checkbox"/> Any		
	0x	<input type="text"/>	(0x600 ~ 0xFFFF)
VLAN	<input checked="" type="checkbox"/> Any		
	<input type="text"/>	(1 - 4094)	
802.1p	<input checked="" type="checkbox"/> Any		
	<input type="text"/>	/	<input type="text"/> (Value / Mask) (0 - 7)

Apply

Close

Figure 11-4 Add and Edit MAC ACE Dialog

Fiel	Description
d	
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	<p>Select the action after ACE match packet.</p> <ul style="list-style-type: none"> • 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. <p><u>Such ports can be reactivated from the Port Settings</u></p>
Source MAC	<p>Select the type for source MAC address.</p> <ul style="list-style-type: none"> • 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 <p><u>source MAC address and mask to which will be</u></p>
Destination MAC	<p>Select the type for Destination MAC address.</p> <ul style="list-style-type: none"> • 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 <p><u>be matched.</u></p>
Ethertype	<p>Select the type for Ethernet frame type.</p> <ul style="list-style-type: none"> • 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 <p><u>which will be matched.</u></p>
VLAN ID	<p>Select the type for VLAN ID.</p> <ul style="list-style-type: none"> • 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 <p><u>matched.</u></p>
802.1p	<p>Select the type for 802.1p value.</p> <ul style="list-style-type: none"> • 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.

Table 11-4 Add and Edit MAC ACE Fields

11.3. 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.



Figure 11-5 IPv4 ACL Page

Field	Description
ACL Name	Input IPv4 ACL name

Table 11-5 IPv4 ACL Fields

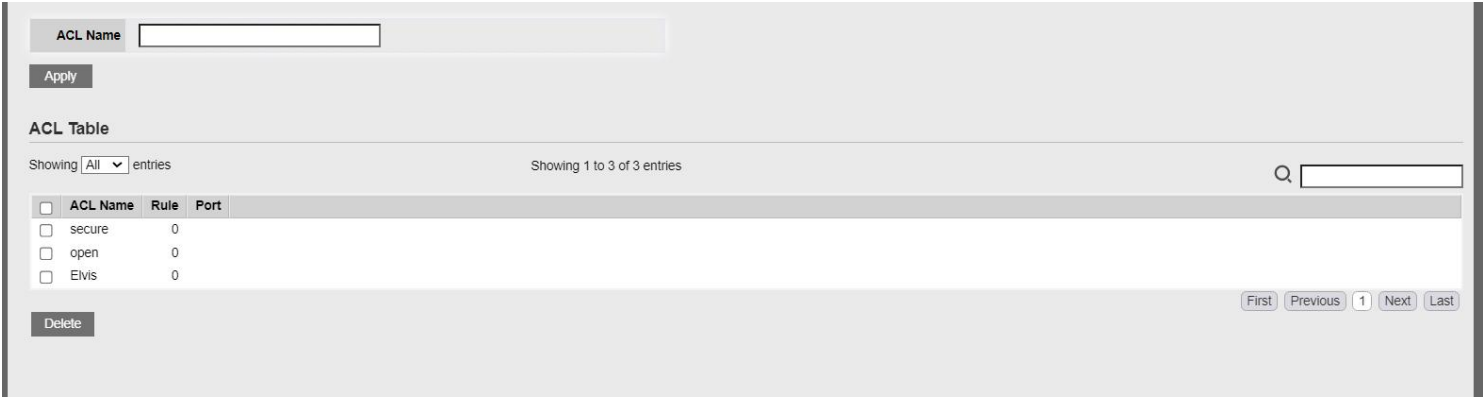


Figure 11-6 IPv4 ACL Table Page

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

Table 11-6 IPv4 ACL Table Fields

11.4. 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.

ACE Table

ACL Name secure

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.

Add

Edit

Delete

First

Previous

1

Next

Last

Figure 11-7 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

Table 11-7 IPv4 ACL Fields

Add ACE

ACL Name	secure	
Sequence	<input type="text" value="32768"/> (1 - 2147483647)	
Action	<input checked="" type="radio"/> Permit <input type="radio"/> Deny <input type="radio"/> Shutdown	
Protocol	<input checked="" type="radio"/> Any <input type="radio"/> Select <input type="text" value="ICMP"/> <input type="button" value="v"/> <input type="radio"/> Define <input type="text" value=""/> (0 - 255)	
Source IP	<input checked="" type="checkbox"/> Any <input type="text" value=""/> / <input type="text" value=""/> (Address / Mask)	
Destination IP	<input checked="" type="checkbox"/> Any <input type="text" value=""/> / <input type="text" value=""/> (Address / Mask)	
Type of Service	<input checked="" type="radio"/> Any <input type="radio"/> DSCP <input type="text" value=""/> (0 - 63) <input type="radio"/> IP Precedence <input type="text" value=""/> (0 - 7)	
Source Port	<input checked="" type="radio"/> Any <input type="radio"/> Single <input type="text" value=""/> (0 - 65535) <input type="radio"/> Range <input type="text" value=""/> - <input type="text" value=""/> (0 - 65535) <input checked="" type="radio"/> Any	

Spanning Tree

ERPS

Discovery

DHCP

Multicast

Routing

Security

ACL

MAC ACL

MAC ACE

IPv4 ACL

IPv4 ACE

IPv6 ACL

IPv6 ACE

ACL Binding

QoS

Diagnostics

Management

Save

Logout

Reboot

Success.

ACL Name

secure

Sequence

32768

Action

Permit

Deny

Shutdown

Protocol

Any

Select

ICMP

Define

(0 - 255)

Source IP

Any

/

(Address / Mask)

Destination IP

Any

/

(Address / Mask)

Type of Service

Any

DSCP

(0 - 63)

IP Precedence

(0 - 7)

Source Port

Any

Single

(0 - 65535)

Range

-

(0 - 65535)

Figure 11-8 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	<p>Select the action for a match.</p> <ul style="list-style-type: none"> • 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	<p>Select the type of protocol for a match.</p> <ul style="list-style-type: none"> • 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	<p>Select the type for source IP address.</p> <ul style="list-style-type: none"> • 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	<p>Select the type for destination IP address.</p> <ul style="list-style-type: none"> • 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	<p>Select the type of protocol for a match. Only available when protocol is TCP or UDP.</p> <ul style="list-style-type: none"> • 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

- **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

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.

Table 11-8 Add and Edit IPv4 ACL Fields

11.5. 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 Name

Apply

ACL Table

Showing All entries Showing 0 to 0 of 0 entries

Q

ACL Name	Rule	Port
0 results found.		

First Previous 1 Next Last

Delete

Figure 11-9 IPv6 ACL Page

Field	Description
ACL Name	Input IPv6 ACL name

Table 11-9 IPv6 ACL Fields

Figure 11-10 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

Table 11-10 IPv6 ACL Table Fields

11.6. 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.

Figure 11-11 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

Table 11-11 IPv6 ACE Fields

Add ACE

ACL Name	test1	
Sequence	<input type="text" value="32768"/> (1 - 2147483647)	
Action	<input checked="" type="radio"/> Permit <input type="radio"/> Deny <input type="radio"/> Shutdown	
Protocol	<input checked="" type="radio"/> Any <input type="radio"/> Select <input type="text" value="TCP"/> <input type="button" value="v"/> <input type="radio"/> Define <input type="text"/> (0 - 255)	
Source IP	<input checked="" type="checkbox"/> Any <input type="text"/> / <input type="text"/> (Address / Prefix (0 - 128))	
Destination IP	<input checked="" type="checkbox"/> Any <input type="text"/> / <input type="text"/> (Address / Prefix (0 - 128))	
Type of Service	<input checked="" type="radio"/> Any <input type="radio"/> DSCP <input type="text"/> (0 - 63) <input type="radio"/> IP Precedence <input type="text"/> (0 - 7)	
Source Port	<input checked="" type="radio"/> Any <input type="radio"/> Single <input type="text"/> (0 - 65535) <input type="radio"/> Range <input type="text"/> - <input type="text"/> (0 - 65535) <input type="radio"/> Any	

Edit ACE

ACL Name	test1		
Sequence	32768		
Action	<input checked="" type="radio"/> Permit <input type="radio"/> Deny <input type="radio"/> Shutdown		
Protocol	<input checked="" type="radio"/> Any <input type="radio"/> Select <input type="text" value="TCP"/> <input type="button" value="v"/> <input type="radio"/> Define <input type="text"/> (0 - 255)		
Source IP	<input checked="" type="checkbox"/> Any <input type="text"/> / <input type="text"/> (Address / Prefix (0 - 128))		
Destination IP	<input checked="" type="checkbox"/> Any <input type="text"/> / <input type="text"/> (Address / Prefix (0 - 128))		
Type of Service	<input checked="" type="radio"/> Any <input type="radio"/> DSCP <input type="text"/> (0 - 63) <input type="radio"/> IP Precedence <input type="text"/> (0 - 7)		
Source Port	<input checked="" type="radio"/> Any <input type="radio"/> Single <input type="text"/> (0 - 65535) <input type="radio"/> Range <input type="text"/> - <input type="text"/> (0 - 65535)		
	<input checked="" type="radio"/> Any		

Figure 11-12 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. <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • 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
-

	<p>matched.</p> <ul style="list-style-type: none"> • 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	<p>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</p>
Type of Service	<p>Select the type of service for a match.</p> <ul style="list-style-type: none"> • 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 <code>IP_Precedence</code> to match.
ICMP Type	<p>Either select the message type by name or enter the message type number. Only available when protocol is ICMP.</p> <ul style="list-style-type: none"> • 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	<p>Select the type for ICMP code. Only available when protocol is ICMP.</p> <ul style="list-style-type: none"> • Any: All codes are acceptable. • User Defined: Enter an ICMP code to match.

Table 11-12 Add and Edit IPv6 ACE Fields

11.7. 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 Binding Table

<input type="checkbox"/>	Entry	Port	MAC ACL	IPv4 ACL	IPv6 ACL
<input type="checkbox"/>	1	GE1			
<input type="checkbox"/>	2	GE2			
<input type="checkbox"/>	3	GE3			
<input type="checkbox"/>	4	GE4			
<input type="checkbox"/>	5	GE5			
<input type="checkbox"/>	6	GE6			
<input type="checkbox"/>	7	GE7			
<input type="checkbox"/>	8	GE8			
<input type="checkbox"/>	9	GE9			
<input type="checkbox"/>	10	GE10			
<input type="checkbox"/>	11	GE11			
<input type="checkbox"/>	12	GE12			
<input type="checkbox"/>	13	GE13			
<input type="checkbox"/>	14	GE14			
<input type="checkbox"/>	15	GE15			
<input type="checkbox"/>	16	GE16			
<input type="checkbox"/>	17	GE17			
<input type="checkbox"/>	18	GE18			
<input type="checkbox"/>	19	GE19			
<input type="checkbox"/>	20	GE20			
<input type="checkbox"/>	21	GE21			
<input type="checkbox"/>	22	GE22			
<input type="checkbox"/>	23	GE23			

Figure 11-13 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.

Table 11-13 ACL Binding Fields

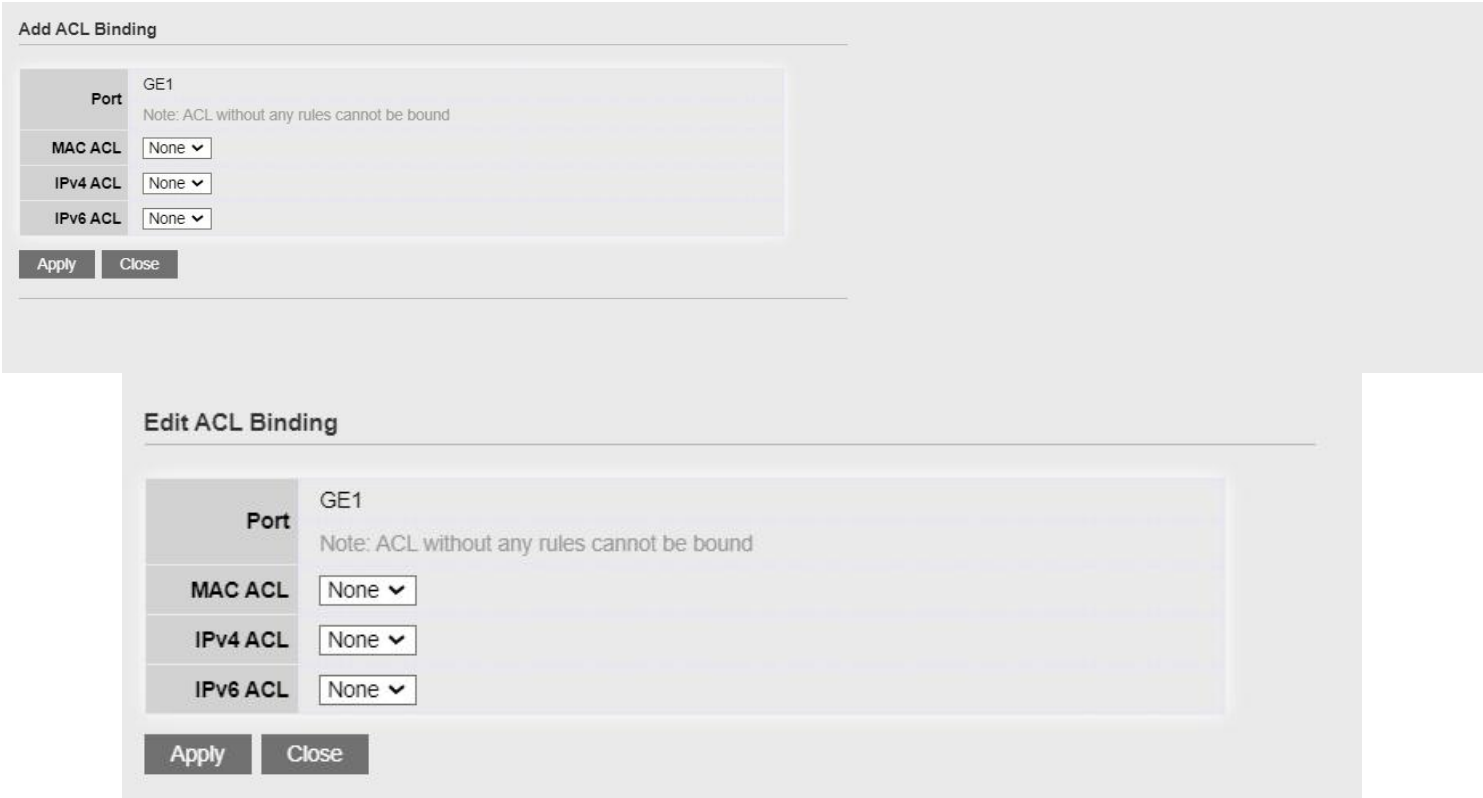


Figure 11-14 Add and Edit ACL Binding Dialog

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	Select IPv6 ACL name from list to bind.

Table 11-14 Add and Edit ACL Binding Fields

12 QoS

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

12.1. General

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

12.1.1. Property

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



Figure 12-1 QoS Global Setting

Field	Description
State	Set checkbox to enable/disable QoS.
Trust Mode	<div>Select QoS trust mode<ul style="list-style-type: none">• 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</div>

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.

Table 12-1 QoS Global Setting Fields

Port Setting Table							
<input type="checkbox"/>	Entry	Port	CoS	Trust	Remarking		
					CoS	DSCP	IP Precedence
<input type="checkbox"/>	1	GE1	0	Enabled	Disabled	Disabled	Disabled
<input type="checkbox"/>	2	GE2	0	Enabled	Disabled	Disabled	Disabled
<input type="checkbox"/>	3	GE3	0	Enabled	Disabled	Disabled	Disabled
<input type="checkbox"/>	4	GE4	0	Enabled	Disabled	Disabled	Disabled
<input type="checkbox"/>	5	GE5	0	Enabled	Disabled	Disabled	Disabled
<input type="checkbox"/>	6	GE6	0	Enabled	Disabled	Disabled	Disabled
<input type="checkbox"/>	7	GE7	0	Enabled	Disabled	Disabled	Disabled
<input type="checkbox"/>	8	GE8	0	Enabled	Disabled	Disabled	Disabled
<input type="checkbox"/>	9	GE9	0	Enabled	Disabled	Disabled	Disabled
<input type="checkbox"/>	10	GE10	0	Enabled	Disabled	Disabled	Disabled
<input type="checkbox"/>	11	GE11	0	Enabled	Disabled	Disabled	Disabled
<input type="checkbox"/>	12	GE12	0	Enabled	Disabled	Disabled	Disabled
<input type="checkbox"/>	13	GE13	0	Enabled	Disabled	Disabled	Disabled
<input type="checkbox"/>	14	GE14	0	Enabled	Disabled	Disabled	Disabled
<input type="checkbox"/>	15	GE15	0	Enabled	Disabled	Disabled	Disabled
<input type="checkbox"/>	16	GE16	0	Enabled	Disabled	Disabled	Disabled
<input type="checkbox"/>	17	GE17	0	Enabled	Disabled	Disabled	Disabled
<input type="checkbox"/>	18	GE18	0	Enabled	Disabled	Disabled	Disabled
<input type="checkbox"/>	19	GE19	0	Enabled	Disabled	Disabled	Disabled
<input type="checkbox"/>	20	GE20	0	Enabled	Disabled	Disabled	Disabled
<input type="checkbox"/>	21	GE21	0	Enabled	Disabled	Disabled	Disabled

Figure 12-2 QoS Port Setting Table

Field	Description
Port	Port name
CoS	Port default CoS priority value for the selected ports
Trust	Port trust state <ul style="list-style-type: none"> • Enabled: Traffic will follow trust mode in global setting • Disabled: Traffic will always use best efforts
Remarking (CoS)	Port CoS remarking admin state <ul style="list-style-type: none"> • Enabled: CoS remarking is enabled • Disabled: CoS remarking is disabled
Remarking (DSCP)	Port DSCP remarking admin state <ul style="list-style-type: none"> • 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

Table 12-2 QoS Port Setting Table Fields

Edit Port Setting

PortGE1

CoS

0

(0 - 7)

Trust☒ Enable

Remarking

CoS☐ Enable

DSCP☐ Enable

IP Precedence☐ Enable

Apply

Close

Figure 12-3 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

Table 12-3 Edit QoS Port Setting Fields

12.1.2. 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).

Queue Scheduling Table

Queue	Method			
	Strict Priority	WRR	Weight	WRR Bandwidth (%)
1	<input checked="" type="radio"/>	<input type="radio"/>	1	
2	<input checked="" type="radio"/>	<input type="radio"/>	2	
3	<input checked="" type="radio"/>	<input type="radio"/>	3	
4	<input checked="" type="radio"/>	<input type="radio"/>	4	
5	<input checked="" type="radio"/>	<input type="radio"/>	5	
6	<input checked="" type="radio"/>	<input type="radio"/>	9	
7	<input checked="" type="radio"/>	<input type="radio"/>	13	
8	<input checked="" type="radio"/>	<input type="radio"/>	15	

Apply

Figure 12-4: 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

Table 12-4: Queue Scheduling Table fields.

12.1.3. 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.

CoS to Queue Mapping

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

Apply

Queue to CoS Mapping

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

Apply

Figure 12-5 CoS to Queue Mapping Table

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

Table 12-5 CoS to Queue Mapping Table Fields

CoS to Queue Mapping

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

Apply

Figure 12-6 Queue to CoS Mapping Table

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

Table 12-6 Queue to CoS Mapping Table Fields

12.1.4. 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.

DSCP to Queue Mapping

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

Apply

Figure 12-7 DSCP to Queue Mapping Table

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

Table 12-7 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

Figure 12-8 Queue to DSCP Mapping Table

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

Table 12-8 Queue to DSCP Mapping Table Fields

12.1.5. 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.

IP Precedence to Queue Mapping

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

Apply

Queue to IP Precedence Mapping

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

Apply

Figure 12-9 IP Precedence to Queue Mapping Table

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

Table 12-9 IP Precedence to Queue Mapping Table Fields

Figure 12-10 Queue to IP Precedence Mapping Table

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

Table 12-10 Queue to IP Precedence Mapping Table Fields

12.2. 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.

12.2.1. 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.

Ingress / Egress Port Table

<input type="checkbox"/>	Entry	Port	Ingress		Egress	
			State	Rate (Kbps)	State	Rate (Kbps)
<input type="checkbox"/>	1	GE1	Disabled		Disabled	
<input type="checkbox"/>	2	GE2	Disabled		Disabled	
<input type="checkbox"/>	3	GE3	Disabled		Disabled	
<input type="checkbox"/>	4	GE4	Disabled		Disabled	
<input type="checkbox"/>	5	GE5	Disabled		Disabled	
<input type="checkbox"/>	6	GE6	Disabled		Disabled	
<input type="checkbox"/>	7	GE7	Disabled		Disabled	
<input type="checkbox"/>	8	GE8	Disabled		Disabled	
<input type="checkbox"/>	9	GE9	Disabled		Disabled	
<input type="checkbox"/>	10	GE10	Disabled		Disabled	
<input type="checkbox"/>	11	GE11	Disabled		Disabled	
<input type="checkbox"/>	12	GE12	Disabled		Disabled	
<input type="checkbox"/>	13	GE13	Disabled		Disabled	
<input type="checkbox"/>	14	GE14	Disabled		Disabled	
<input type="checkbox"/>	15	GE15	Disabled		Disabled	
<input type="checkbox"/>	16	GE16	Disabled		Disabled	
<input type="checkbox"/>	17	GE17	Disabled		Disabled	
<input type="checkbox"/>	18	GE18	Disabled		Disabled	
<input type="checkbox"/>	19	GE19	Disabled		Disabled	
<input type="checkbox"/>	20	GE20	Disabled		Disabled	
<input type="checkbox"/>	21	GE21	Disabled		Disabled	
<input type="checkbox"/>	22	GE22	Disabled		Disabled	

Figure 12-11 Ingress/Egress Port Table

Field	Description
Port	Port name
Ingress (State)	Port ingress rate limit state <ul style="list-style-type: none">• 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 <ul style="list-style-type: none">• 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

Table 12-11 Ingress/Egress Port Table Fields

Egress Queue Table

	Entry	Port	Queue 1		Queue 2		Queue 3		Queue 4		Queue 5		Queue 6		Queue 7		Queue 8		
			State	CIR (Kbps)	State	CIR (Kbps)	State	CIR (Kbps)	State	CIR (Kbps)	State	CIR (Kbps)	State	CIR (Kbps)	State	CIR (Kbps)	State	CIR (Kbps)	
<input type="checkbox"/>	1	GE1	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		
<input type="checkbox"/>	2	GE2	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		
<input type="checkbox"/>	3	GE3	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		
<input type="checkbox"/>	4	GE4	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		
<input type="checkbox"/>	5	GE5	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		
<input type="checkbox"/>	6	GE6	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		
<input type="checkbox"/>	7	GE7	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		
<input type="checkbox"/>	8	GE8	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		
<input type="checkbox"/>	9	GE9	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		
<input type="checkbox"/>	10	GE10	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		
<input type="checkbox"/>	11	GE11	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		
<input type="checkbox"/>	12	GE12	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		
<input type="checkbox"/>	13	GE13	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		
<input type="checkbox"/>	14	GE14	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		
<input type="checkbox"/>	15	GE15	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		
<input type="checkbox"/>	16	GE16	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		
<input type="checkbox"/>	17	GE17	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		
<input type="checkbox"/>	18	GE18	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		
<input type="checkbox"/>	19	GE19	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		
<input type="checkbox"/>	20	GE20	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		
<input type="checkbox"/>	21	GE21	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		
<input type="checkbox"/>	22	GE22	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		

Figure 12-12 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.

Table 12-12 Edit Ingress/Egress Port Fields

12.2.2. Egress Queue

To display Egress Queue web page, click **QoS > Rate Limit >**

Egress Queue. Egress rate limiting is performed by shaping the output load.

Figure 12-13: Egress Queue Table

Field	Description
Port	Port name
Queue 1 (State)	Port egress queue 1 rate limit state <ul style="list-style-type: none">• 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 <ul style="list-style-type: none">• 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 <ul style="list-style-type: none">• 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 <ul style="list-style-type: none">• 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 <ul style="list-style-type: none">• 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 <ul style="list-style-type: none">• Enabled: Egress queue rate limit is enabled• Disabled: Egress queue rate limit is disabled
Queue 6	Queue 6 egress committed information rate

(CIR)

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 <ul style="list-style-type: none">• Enabled: Egress queue rate limit is enabled• Disabled: Egress queue rate limit is disabled
Queue 8 (CIR)	Queue 8 egress committed information rate

Table 12-13: Egress Queue Table Fields.

Edit Egress Queue

Port	GE24	
Queue 1	<div><input type="checkbox"/> Enable</div> <div><input type="text" value="1000000"/> Kbps (16 - 1000000)</div>	
Queue 2	<div><input type="checkbox"/> Enable</div> <div><input type="text" value="1000000"/> Kbps (16 - 1000000)</div>	
Queue 3	<div><input type="checkbox"/> Enable</div> <div><input type="text" value="1000000"/> Kbps (16 - 1000000)</div>	
Queue 4	<div><input type="checkbox"/> Enable</div> <div><input type="text" value="1000000"/> Kbps (16 - 1000000)</div>	
Queue 5	<div><input type="checkbox"/> Enable</div> <div><input type="text" value="1000000"/> Kbps (16 - 1000000)</div>	
Queue 6	<div><input type="checkbox"/> Enable</div> <div><input type="text" value="1000000"/> Kbps (16 - 1000000)</div>	
Queue 7	<div><input type="checkbox"/> Enable</div> <div><input type="text" value="1000000"/> Kbps (16 - 1000000)</div>	
Queue 8	<div><input type="checkbox"/> Enable</div> <div><input type="text" value="1000000"/> Kbps (16 - 1000000)</div>	

Apply

Close

Figure 12-14: 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.

Table 12-14: Edit Egress Queue Fields.

13 Diagnosti CS

Use the Diagnostics pages to configure settings for the switch diagnostics feature or operating diagnostic utilities.

13.1. Logging

13.1.1. Property

To enable/disable the logging service, click **Diagnostic > Logging > Property**.

State ☒ Enable

Aggregation ☐ Enable

Aging Time Sec (15 - 3600, default 300)

Console Logging

State ☒ Enable

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

RAM Logging

State ☒ Enable

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

Flash Logging

State ☐ Enable

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

Apply

Figure 13-1: 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.

Table 13-1: Logging Property fields.

Field	Description
State	Enable/Disable the console logging service.
Minimum Severity	The minimum severity for the console logging.

Table 13-2: Console Logging fields.

Field	Description
State	Enable/Disable the RAM logging service.
Minimum Severity	The minimum severity for the RAM logging.

Table 13-3: RAM Logging fields.

Field	Description
State	Enable/Disable the flash logging service.
Minimum Severity	The minimum severity for the flash logging.

Table 13-4: Flash Logging fields.

13.1.2. Remove Server

To configure the remote logging server, click **Diagnostic > Logging > Remote Server**.

Remote Server Table

<input type="checkbox"/>	Entry	Server Address	Server Port	Facility	Minimum Severity	
--------------------------	-------	----------------	-------------	----------	------------------	--

0 results found.

Add Edit Delete

Figure 13-2: 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.

Table 13-5: Remote Server fields.

13.2. Mirroring

To display Port Mirroring web page, click **Diagnostics > Mirroring**

Mirroring Table

	Session ID	State	Monitor Port	Ingress Port	Egress Port
<input type="radio"/>	1	Disabled	---	---	---
<input type="radio"/>	2	Disabled	---	---	---
<input type="radio"/>	3	Disabled	---	---	---
<input type="radio"/>	4	Disabled	---	---	---

Edit

NOTE Allow the monitor port to send or receive normal packets

Figure 13-3 Mirroring Page

Field	Description
Session ID	Select mirror session ID
State	Select mirror session state : port-base mirror or disable <ul style="list-style-type: none"> • Enabled: Enable port based mirror • Disabled: Disable mirror.
Monitor Port	Select mirror session monitor port, and select <small>whether normal packet could be sent or received by monitor port.</small>
Ingress port	Select mirror session source rx ports
Egress ports	Select mirror session source tx ports

Table 13-6 Mirroring Fields

13.3. Ping

For the ping functionality, click **Diagnostic > Ping**.

Address Type

☒ Hostname
☐ IPv4
☐ IPv6

Server Address

Count

(1 - 32)

Ping

Stop

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

Figure 13-4: 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.

Table 13-7: Ping fields.

13.4. Traceroute

For trace route functionality, click **Diagnostic > Traceroute**.

Address Type

☒ Hostname
☐ IPv4

Server Address

Time to Live

☐ User Defined
 (2 - 255, default 30)

Apply

Stop

Traceroute Result

Figure 13-5: 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.

Table 13-8: Traceroute fields.

13.5. Copper Test

For copper length diagnostic, click **Diagnostic > Copper Test**.

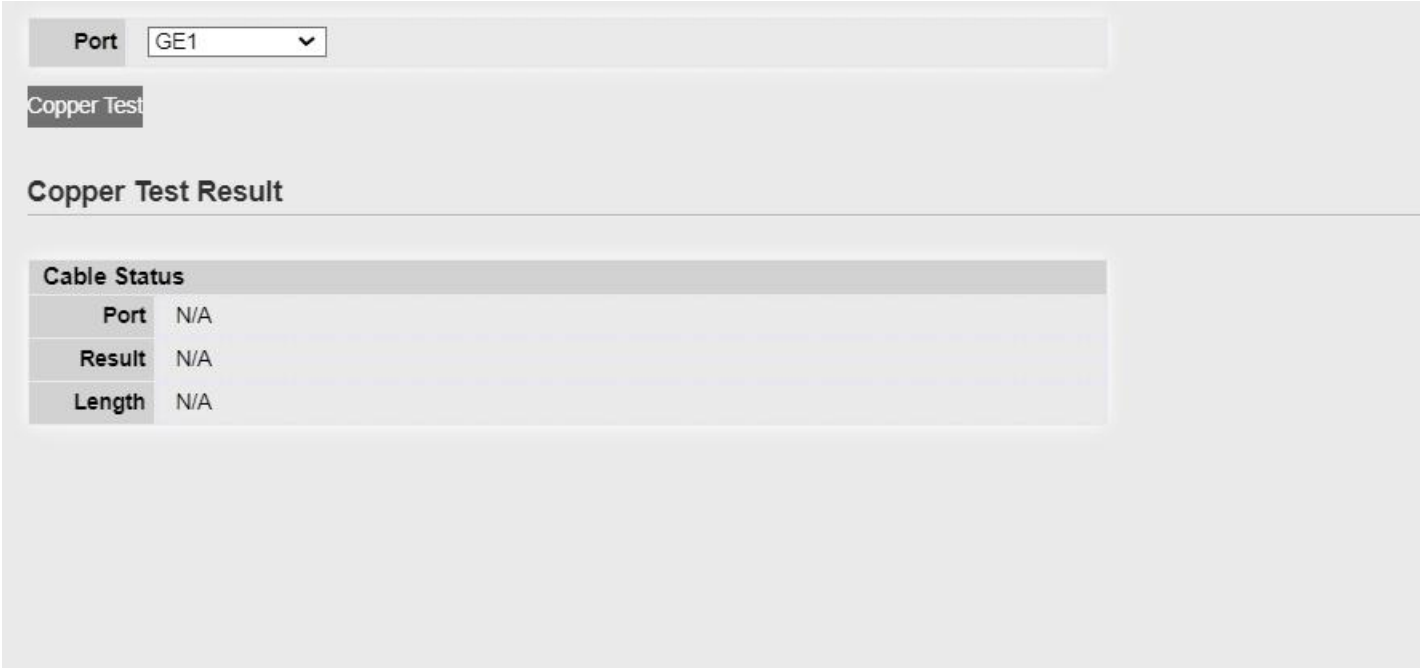


Figure 13-6: Copper Test page.

Field	Description
Port	Specify the interface for the copper test.

Table 13-9: Copper Test fields.

Field	Description
Port	The interface for the copper test.
Result	<p>The status of copper test. It include:</p> <ul style="list-style-type: none"> • 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.

Table 13-10: Copper Result fields.

13.6. 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**.

Fiber Module Table

	Port	Temperature (C)	Voltage (V)	Current (mA)	Output Power (mW)	Input Power (mW)	OE Present	Loss of Signal	
<input type="radio"/>	TE1	N/A	N/A	N/A	N/A	N/A	Remove	Loss	
<input type="radio"/>	TE2	N/A	N/A	N/A	N/A	N/A	Remove	Loss	
<input type="radio"/>	TE3	N/A	N/A	N/A	N/A	N/A	Remove	Loss	
<input type="radio"/>	TE4	N/A	N/A	N/A	N/A	N/A	Remove	Loss	

Refresh

Detail

Figure 13-7: 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.

Table 13-11: Fiber Module fields.

Fiber Module Status	
Port	TE1
OE Present	Remove
Loss of Signal	Loss
Transceiver Type	N/A
Connector Type	N/A
Ethernet Compliance Code	N/A
Transmission Media	N/A
Wavelength	N/A
Bitrate	N/A
Vendor OUI	N/A
Vendor Name	N/A
Vendor PN	N/A
Vendor Revision	N/A
Vendor SN	N/A
Date Code	N/A
Temperature (C)	N/A
Voltage (V)	N/A
Current (mA)	N/A
Output Power (mW)	N/A
Input Power (mW)	N/A

Figure 13-8: Fiber Module Status page.

13.7. UDL
D

Use the UDLD pages to configure settings of UDLD function.

13.7.1. Property

To display Property page, click **Diagnostics > UDLD > Property**

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

Message Time

15

Sec (1 - 90, default 15)

Apply

Port Setting Table

<input type="checkbox"/>	Entry	Port	Mode	Bidirectional State	Operational Status	Neighbor
<input type="checkbox"/>	1	GE1	Disabled	Unknown		0
<input type="checkbox"/>	2	GE2	Disabled	Unknown		0
<input type="checkbox"/>	3	GE3	Disabled	Unknown		0
<input type="checkbox"/>	4	GE4	Disabled	Unknown		0
<input type="checkbox"/>	5	GE5	Disabled	Unknown		0
<input type="checkbox"/>	6	GE6	Disabled	Unknown		0
<input type="checkbox"/>	7	GE7	Disabled	Unknown		0
<input type="checkbox"/>	8	GE8	Disabled	Unknown		0
<input type="checkbox"/>	9	GE9	Disabled	Unknown		0
<input type="checkbox"/>	10	GE10	Disabled	Unknown		0
<input type="checkbox"/>	11	GE11	Disabled	Unknown		0
<input type="checkbox"/>	12	GE12	Disabled	Unknown		0
<input type="checkbox"/>	13	GE13	Disabled	Unknown		0
<input type="checkbox"/>	14	GE14	Disabled	Unknown		0
<input type="checkbox"/>	15	GE15	Disabled	Unknown		0
<input type="checkbox"/>	16	GE16	Disabled	Unknown		0
<input type="checkbox"/>	17	GE17	Disabled	Unknown		0
<input type="checkbox"/>	18	GE18	Disabled	Unknown		0
<input type="checkbox"/>	19	GE19	Disabled	Unknown		0

Figure 13-9: Property page.

Field	Description
Message Time	Input the interval for sending message. Range is 1 -90 seconds.

Table 13-12 Property Fields

Figure 13-10: Property Port page.

Field	Description
Port	Display port ID of entry.
Mode	Display UDLD running mode of interface.
Bidirectional State	Display bidirectional state of interface.
Operational	Display operational status of interface

Status

Neighbor

Display the number of neighbor of interface

Table 13-13 Property Port Fields

Edit Port Setting

Port

GE11

Mode

☒ Disabled

☐ Normal

☐ Aggressive

Apply

Close

Figure 13-11: Edit Property Port page.

Field	Description
Port	Display selected port to be edited.
Mode	<div>Select UDLD running mode of interface.</div> <ul style="list-style-type: none">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.

Table 13-14 Edit Property Port Fields

13.7.2. Neighbor

To display Neighbor page, click **Diagnostics > UDLD > Neighbor**

Neighbor Table

Q

Entry	Expiration Time	Current Neighbor State	Device ID	Device Name	Port ID	Message Interval	Timeout Interval	
-------	-----------------	------------------------	-----------	-------------	---------	------------------	------------------	--

0 results found.

Refresh

Figure 13-12: 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

Table 13-15: Neighbor fields.

14 Management

Use the Management pages to configure settings for the switch management features.

14.1. 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.

User Account

Showing

All

 entries

Showing 1 to 1 of 1 entries

Q

<input type="checkbox"/>	Username	Privilege
<input type="checkbox"/>	admin	Admin

Add

Edit

Delete

First

Previous

1

Next

Last

Figure 14-1 User Account Table

Field	Description
Username	User name of the account
Privilege	Select privilege level for new account. <ul style="list-style-type: none">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.

Table 14-1 User Account Table Fields

Add User Account

Username

aaa

Password

...

Confirm Password

...

Privilege

☒ Admin

☐ User

Apply

Close

Edit User Account

Username

admin

Password

Confirm Password

Privilege

☒ Admin

☐ User

Apply

Close

Figure 14-2 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	<div>Select privilege level for new account.<ul style="list-style-type: none">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.</div>

Table 14-2 Add/Edit User Account Fields

14.2. Firmware

14.2.1. 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.

Figure 14-3 Upgrade Firmware through HTTP

Table 14-3 Upgrade Firmware through HTTP Fields

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

Action	Firmware operations <ul style="list-style-type: none">• Upgrade: Upgrade firmware from remote host to DUT• Backup: Backup firmware image from DUT to remote
Method	Firmware upgrade / backup method <ul style="list-style-type: none">• TFTP: Using TFTP to upgrade/backup firmware• HTTP: Using WEB browser to upgrade/backup
Address Type	Specify TFTP server address type <ul style="list-style-type: none">• 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

Table 14-4 Upgrade Firmware through TFTP Fields

Action

☒ Upgrade

Backup

Method

☐ TFTP

☒ HTTP

Filename

选择文件 未选择任何文件

Apply

Figure 14-5 Backup Firmware through HTTP

Field	Description
Action	Firmware operations <ul style="list-style-type: none">• Upgrade: Upgrade firmware from remote host to DUT• Backup: Backup firmware image from DUT to remote
Method	Firmware upgrade / backup method <ul style="list-style-type: none">• TFTP: Using TFTP to upgrade/backup firmware• HTTP: Using WEB browser to upgrade/backup firmware
Firmware	Firmware partition need to backup <ul style="list-style-type: none">• Image0: Firmware image in flash partition 0• Image1: Firmware image in flash partition 1

Table 14-5 Backup Firmware through HTTP Fields

Management >> Firmware >> Upgrade / Backup

Action

Method

Firmware

Address Type

Server Address

Filename

☐ Upgrade
☒ Backup

☒ TFTP
☐ HTTP

☒ Image0
☐ Image1

☒ Hostname
☐ IPv4
☐ IPv6

Figure 14-6 Backup Firmware through TFTP

Field	Description
Action	Firmware operations <ul style="list-style-type: none"> Upgrade: Upgrade firmware from remote host to DUT Backup: Backup firmware image from DUT to remote
Method	Firmware upgrade / backup method <ul style="list-style-type: none"> TFTP: Using TFTP to upgrade/backup firmware HTTP: Using WEB browser to upgrade/backup
Firmware	Firmware partition need to backup <ul style="list-style-type: none"> Image0: Firmware image in flash partition 0 Image1: Firmware image in flash partition 1
Address Type	Specify TFTP server address type <ul style="list-style-type: none"> 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

Table 14-6 Backup Firmware through TFTP Fields

14.3. Configuration

14.3.1. 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.

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

Apply

Figure 14-8 Upgrade Configuration through HTTP

Field	Description
Action	Configuration operations <ul style="list-style-type: none">Upgrade: Upgrade firmware from remote host to DUTBackup: Backup firmware image from DUT to remote
Method	Configuration upgrade / backup method <ul style="list-style-type: none">TFTP: Using TFTP to upgrade/backup firmwareHTTP: Using WEB browser to upgrade/backup firmware
Configuration	Configuration types <ul style="list-style-type: none">Running Configuration: Merge to current running configuration fileStartup Configuration: Replace startup configuration

- **Backup Configuration:** Replace backup configuration file

Filename

Use browser to upgrade configuration, you should select configuration file on your host PC.

Table 14-8 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

Address Type

☒ Hostname
 ☐ IPv4
 ☐ IPv6

Server Address

Filename

Apply

Figure 14-9 Upgrade Configuration through TFTP

Field	Description
Action	Configuration operations <ul style="list-style-type: none"> • Upgrade: Upgrade firmware from remote host to DUT • Backup: Backup firmware image from DUT to remote
Method	Configuration upgrade / backup method <ul style="list-style-type: none"> • TFTP: Using TFTP to upgrade/backup firmware • HTTP: Using WEB browser to upgrade/backup firmware
Configuration	Configuration types <ul style="list-style-type: none"> • Running Configuration: Merge to current running configuration file • Startup Configuration: Replace startup configuration file • Backup Configuration: Replace backup configuration
Address Type	Specify TFTP server address type <ul style="list-style-type: none"> • Hostname: Use domain name as server address • IPv4: Use IPv4 as server address

	<ul style="list-style-type: none"> • IPv6: Use IPv6 as server address
Server Address	Specify TFTP server address.
Filename	Configuration file name on remote TFTP server

Table 14-9 Upgrade Firmware through TFTP Fields

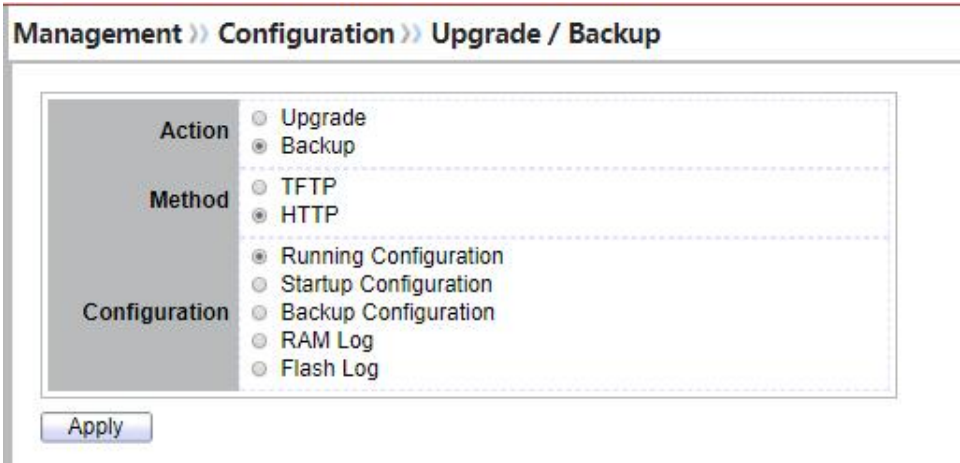


Figure 14-10 Backup Configuration through HTTP

Field	Description
Action	Configuration operations <ul style="list-style-type: none"> • Upgrade: Upgrade configuration from remote host to DUT • Backup: Backup configuration from DUT to remote host
Method	Configuration upgrade / backup method <ul style="list-style-type: none"> • TFTP: Using TFTP to upgrade/backup configuration • HTTP: Using WEB browser to upgrade/backup
Configuration	Configuration types <ul style="list-style-type: none"> • 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

Table 14-10 Backup Configuration through HTTP Fields

Management >> Configuration >> Upgrade / Backup

Action

Method

Configuration

Address Type

Server Address

Filename

☐ Upgrade

☒ Backup

☒ TFTP

☐ HTTP

☒ Running Configuration

☐ Startup Configuration

☐ Backup Configuration

☐ RAM Log

☐ Flash Log

☒ Hostname

☐ IPv4

☐ IPv6

Apply

Figure 14-11 Backup Configuration through TFTP

Field	Description
Action	<div>Firmware operations</div> <div><ul style="list-style-type: none">Upgrade: Upgrade firmware from remote host to DUTBackup: Backup firmware image from DUT to remote</div>
Method	<div>Firmware upgrade / backup method</div> <div><ul style="list-style-type: none">TFTP: Using TFTP to upgrade/backup firmwareHTTP: Using WEB browser to upgrade/backup</div>
Configuration	<div>Configuration types</div> <div><ul style="list-style-type: none">Running Configuration: Backup running configuration fileStartup Configuration: Backup start configuration fileBackup Configuration: Backup backup configuration fileRAM Log: Backup log file stored in RAMFlash Log: Backup log files store in Flash</div>
Address Type	<div>Specify TFTP server address type</div> <div><ul style="list-style-type: none">Hostname: Use domain name as server addressIPv4: Use IPv4 as server addressIPv6: Use IPv6 as server address</div>
Server Address	<div>Specify TFTP server address.</div>

Filename

File name saved on remote TFTP server

Table 14-11 Backup Firmware through TFTP Fields

14.3.2. 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.

Source File

☒ Running Configuration
☐ Startup Configuration
☐ Backup Configuration

Destination File

☒ Startup Configuration
☐ Backup Configuration

Apply

Restore Factory Default

Figure 14-12 Save Configuration Page

Field	Description
Source File	<div>Source file types</div> <ul style="list-style-type: none">Running Configuration: Copy running configuration file to destinationStartup Configuration: Copy startup configuration file to destinationBackup Configuration: Copy backup configuration file to destination
Destination File	<div>Destination file</div> <ul style="list-style-type: none">Startup Configuration: Save file as startup configurationBackup Configuration: Save file as backup configuration

Table 14-12 Save Configuration Fields

14.4. SNMP

14.4.1. View

To configure and display the SNMP view table, click **Management > SNMP > View**.

View Table

Showing

All

 entries

Showing 1 to 1 of 1 entries

<input type="checkbox"/>	View	OID Subtree	Type
<input type="checkbox"/>	all	.1	Included

Add

Delete

Figure 14-13 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.

Table 14-13 SNMP View Fields

14.4.2. Group

To configure and display the SNMP group settings, click **Management > SNMP > Group**.

Group Table

Showing All entries

Showing 0 to 0 of 0 entries

<input type="checkbox"/>	Group	Version	Security Level	View			
				Read	Write	Notify	
0 results found.							

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

AddEditDelete

Figure 14-14 SNMP Group Table Page

Field	Description
Group	Specify SNMP group name, and the maximum length is 30 characters.
Version	Specify SNMP version <ul style="list-style-type: none">• SNMPv1: SNMP Version 1.• SNMPv2: Community-based SNMP Version 2c.• SNMPv3: User security model SNMP version 3.
Security Level	Specify SNMP security level <ul style="list-style-type: none">• 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.

Table 14-14 SNMP Group Table Fields

Add Group

Group

Version

☒ SNMPv1

☐ SNMPv2

☐ SNMPv3

Security Level

☒ No Security

☐ Authentication

☐ Authentication and Privacy

View

☒ Read

all

☐ Write

all

☐ Notify

all

Apply

Close

Figure 14-15 SNMP Group Add Page

Field	Description
Group	Specify SNMP group name, and the maximum length is 30 characters.
Version	Spedify SNMP version <ul style="list-style-type: none">SNMPv1: SNMP Version 1.SNMPv2: Community-based SNMP Version 2c.SNMPv3: User security model SNMP version 3.
Security Level	Specify SNMP security level <ul style="list-style-type: none">No Security : Specify that no packet authentication is performed.Authentication: Specify that no packet authentication without entryption is performed.Authentication and Privacy: Specify that no packet authentication with entryption 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

Table 14-15 SNMP Group Add Fields

Edit Group

Group

111

Version

☒ SNMPv1

☐ SNMPv2

☐ SNMPv3

Security Level

☒ No Security

☐ Authentication

☐ Authentication and Privacy

View

☒ Read

all

☐ Write

all

☐ Notify

all

Apply

Close

Figure 14-16 SNMP Group Edit Page

Field	Description
Group	Display the edit group name
Version	<div>Specify SNMP version</div> <ul style="list-style-type: none">SNMPv1: SNMP Version 1.SNMPv2: Community-based SNMP Version 2c.SNMPv3: User security model SNMP version 3.
Security Level	<div>Specify SNMP security level</div> <ul style="list-style-type: none">No Security : Specify that no packet authentication is performed.Authentication: Specify that no packet authentication without entryption is performed.Authentication and Privacy: Specify that no packet authentication with entryption 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

Table 14-16 SNMP Group Edit Fields

14.4.3. Community

To configure and display the SNMP community settings, click **Management > SNMP > Community**.



Figure 14-17 SNMP Community Table Page

Field	Description
Community	The SNMP community name. Its maximum length is 20 characters.
Community Mode	SNMP Community mode <ul style="list-style-type: none">• 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 <ul style="list-style-type: none">• Read-Only: Read only.• Read-Wrtie: Read and write.

Table 14-17 SNMP Community Table Fields

Add Community

Community

Type

View

Access

Group

☒ Basic
☐ Advanced

all

▼

☒ Read-Only
☐ Read-Write

111

▼

Apply

Close

Figure 14-18 SNMP Community Add Page

Field	Description
Community	The SNMP community name. Its maximum length is 20 characters.
Type	SNMP Community mode <ul style="list-style-type: none">• 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 <ul style="list-style-type: none">• 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.

Table 14-18 SNMP Community Add Fields

Edit Community

Community

public

Type

☒ Basic

☐ Advanced

View

all ▾

Access

☒ Read-Only

☐ Read-Write

Group

111 ▾

Apply

Close

Figure 14-19 SNMP Community Edit Page

Field	Description
Community	The Edit SNMP community name
Type	SNMP Community mode <ul style="list-style-type: none">• 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 <ul style="list-style-type: none">• 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.

Table 14-19 SNMP Community Edit Fields

14.4.4. User

To configure and display the SNMP users, click **Management > SNMP > User**.

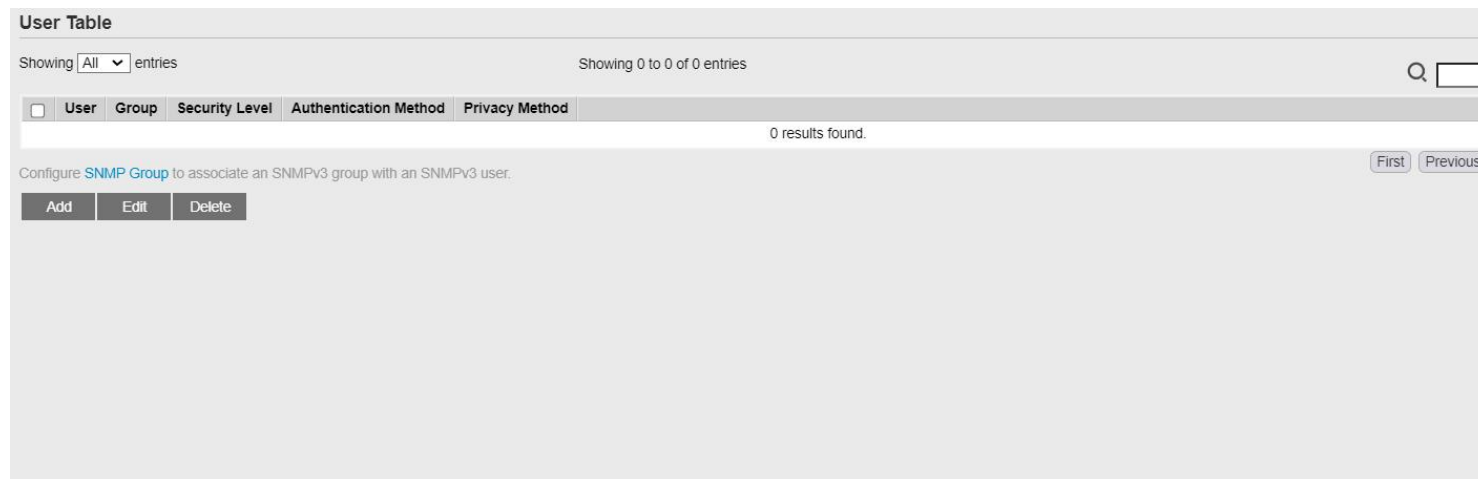


Figure 14-20 SNMP User Table Page

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 <ul style="list-style-type: none"> • 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 . <ul style="list-style-type: none"> • None: No authentication required. • MD5: Specify the HMAC-MD5-96 authentication protocol. • SHA: Specify the HMAC-SHA-96 authentication protocol.
Privacy Method	Encryption Protocol <ul style="list-style-type: none"> • None: No privacy required. • DES: DES algorithm

Table 14-20 SNMP User Table Fields

Add User

User

admin

Group

111

Security Level

☒ No Security

☐ Authentication

☐ Authentication and Privacy

Authentication

Method

☒ None

☐ MD5

☐ SHA

Password

Privacy

Method

☒ None

☐ DES

Password

Apply

Close

Figure 14-21 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 <ul style="list-style-type: none"> 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 . <ul style="list-style-type: none"> None: No authentication required.

	<ul style="list-style-type: none">• 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 <ul style="list-style-type: none">• None: No privacy required.• DES: DES algorithm
Password	The privacy password, The number of character range is 8 to 64 characters.

Table 14-21 SNMP User Add Fields

Edit User

Useradmin

Group111

Security Level

No Security

Authentication

Authentication and Privacy

Authentication

Method

None

MD5

SHA

Password

Privacy

Method

None

DES

Password

Apply

Close

Figure 14-22 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.
-

	<ul style="list-style-type: none"> • 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 . <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • None: No privacy required. • DES: DES algorithm
Password	The privacy password, The number of character range is 8 to 64 characters.

Table 14-22 SNMP User Edit Fields

14.4.5. Engine ID

To configure and display SNMP local and remote engine ID, click **Management > SNMP > Engine ID**.

Local Engine ID

☐ User Defined

Engine ID

80006a920300e05317fd66 (10 - 64 Hexadecimal Characters)

Apply

Remote Engine ID Table

Showing All entriesShowing 0 to 0 of 0 entries

☐

Server Address

Engine ID

0 results found.

Add

Edit

Delete

First

Previous

1

Next

Last

Figure 14-23 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.

Table 14-23 SNMP Engine ID Fields

Add Remote Engine ID

Address Type

☒ Hostname
☐ IPv4
☐ IPv6

Server Address

Engine ID

(10 - 64 Hexadecimal Characters)

Apply

Close

Figure 14-24 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.

Table 14-24 SNMP Remote Engine ID Add Fields

Edit Remote Engine ID

Server Address

192.168.1.2

Engine ID

1122334422

(10 - 64 Hexadecimal Characters)

Apply

Close

Figure 14-25 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.

Table 14-25 SNMP Remote Engine ID Edit Fields

14.4.6. Trap Event

To configure and display SNMP trap event, click **Management > SNMP > Trap Event**.



Figure 14-26 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

Table 14-26 SNMP Trap Event Fields

14.4.7. Notification

To configure the hosts to receive SNMPv1/v2/v3 notification, click **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.

Add

Edit

Delete

Figure 14-27 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 <ul style="list-style-type: none">SNMPv1: SNMP Version 1 notification.SNMPv2: SNMP Version 2 notification.SNMPv3: SNMP Version 3 notification.
Type	Notification Type <ul style="list-style-type: none">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.

Table 14-27 SNMP Notification Table Fields

Add Notification

Address Type

☒ Hostname
☐ IPv4
☐ IPv6

Server Address

Version

☒ SNMPv1
☐ SNMPv2
☐ SNMPv3

Type

☒ Trap
☐ Inform

Community / User

Security Level

☒ No Security
☐ Authentication
☐ Authentication and Privacy

Server Port

☒ Use Default

(1 - 65535, default 162)

Timeout

☒ Use Default

Sec (1 - 300, default 15)

Retry

☒ Use Default

(1 - 255, default 3)

Apply

Close

Figure 14-28 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 <ul style="list-style-type: none">SNMPv1: SNMP Version 1 notification.SNMPv2: SNMP Version 2 notification.SNMPv3: SNMP Version 3 notification.
Type	Notification Type <ul style="list-style-type: none">Trap: Send SNMP traps to the host.Inform: Send SNMP informs to the host.(version 1 have no inform)

Community/Us er	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 <ul style="list-style-type: none"> • 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

Table 14-28 SNMP Notification Add Fields

Server Address

192.168.1.110

Version

☒ SNMPv1
☐ SNMPv2
☐ SNMPv3

Type

☒ Trap
☐ Inform

Community / User

COMN1 ▾

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)

Figure 14-29 SNMP Notification Edit Page

Field	Description

Server Address	Edit SNMP notify recipients address.
Version	Specify SNMP notification version <ul style="list-style-type: none"> • SNMPv1: SNMP Version 1 notification. • SNMPv2: SNMP Version 2 notification. • SNMPv3: SNMP Version 3 notification.
Type	Notification Type <ul style="list-style-type: none"> • Trap: Send SNMP traps to the host. • Inform: Send SNMP informs to the host.(version 1 have no inform)
Community/Us er	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 <ul style="list-style-type: none"> • 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

Table 14-29 SNMP Notification Edit Fields

14.5. RMON

14.5.1. Statistics

To display RMON Statistics, click **Management > RMON > Statistics**.

Statistics Table																		
Refresh Rate 0 sec																		
<input type="checkbox"/>	Entry	Port	Bytes Received	Drop Events	Packets Received	Broadcast Packets	Multicast Packets	CRC & Align Errors	Undersize Packets	Oversize Packets	Fragments	Jabbers	Collisions	Frames of 64 Bytes	Frames of 65 to 127 Bytes	Frames of 128 to 255 Bytes	Frames of 256 to 511 Bytes	Frames of 512 to 1023 Bytes
<input type="checkbox"/>	1	GE1	708185	0	4078	12	315	0	0	0	0	0	0	2330	729	215	12	0
<input type="checkbox"/>	2	GE2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	3	GE3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	4	GE4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	5	GE5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	6	GE6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	7	GE7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	8	GE8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	9	GE9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	10	GE10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	11	GE11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	12	GE12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	13	GE13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	14	GE14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	15	GE15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	16	GE16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	17	GE17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	18	GE18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	19	GE19	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	20	GE20	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Figure 14-30: 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.

Packet s Receive d	Number of packets received, including bad packets, Multicast packets, and Broadcast packets.
Broadca st Packet s	Number of good Broadcast packets received. This number does not include Multicast packets.
Multica st Packet s	Number of good Multicast packets received.
CRC & Align Errors	Number of CRC and Align errors that have occurred.
Undersi ze Packag es	Number of undersized packets (less than 64 octets) received.
Oversiz e Packag es	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: <ul style="list-style-type: none"> • 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	Number of frames, containing 512 to 1023 bytes that were received.

1024 Bytes	
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.

Table 14-30: RMON Statistics fields.

View Port Statistics

Port	GE9
Refresh Rate	<input checked="" type="radio"/> None <input type="radio"/> 5 sec <input type="radio"/> 10 sec <input type="radio"/> 30 sec
Received Bytes (Octets)	710747
Drop Events	0
Received Packets	4093
Broadcast Packets Received	12
Multicast Packets Received	315
CRC & Align Errors	0
Undersize Packets	0
Oversize Packets	0
Fragments	0
Jabbers	0
Collisions	0
Frames of 64 Bytes	2340
Frames of 65 to 127 Bytes	731
Frames of 128 to 255 Bytes	215
Frames of 256 to 511 Bytes	12
Frames Greater than 1024 Bytes	0

Clear Refresh Close

Figure 14-31: View RMON Statistics page.

14.5.2. History

For the RMON history, click **Management > RMON > History**.

History Table

Showing

All

 entries

<input type="checkbox"/>	Entry	Port	Interval	Owner	Sample		
					Maximum	Current	

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

Add

Edit

Delete

View

Figure 14-32: 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.

Table 14-31: 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.

Table 14-32: RMON History buttons.

Add History

Entry

1

Port

GE1 ▾

Max Sample

50

(1 - 50, default 50)

Interval

1800

(1 - 3600, default 1800)

Owner

Apply

Close

Figure 14-33: 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).

Table 14-33: RMON History Add fields.

Edit History

Entry	1
Port	GE1 ▾
Max Sample	<input type="text" value="50"/> (1 - 50, default 50)
Interval	<input type="text" value="1800"/> (1 - 3600, default 1800)
Owner	<input type="text"/>

Apply

Close

Figure 14-34: 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).

Table 14-34: RMON History Edit fields.

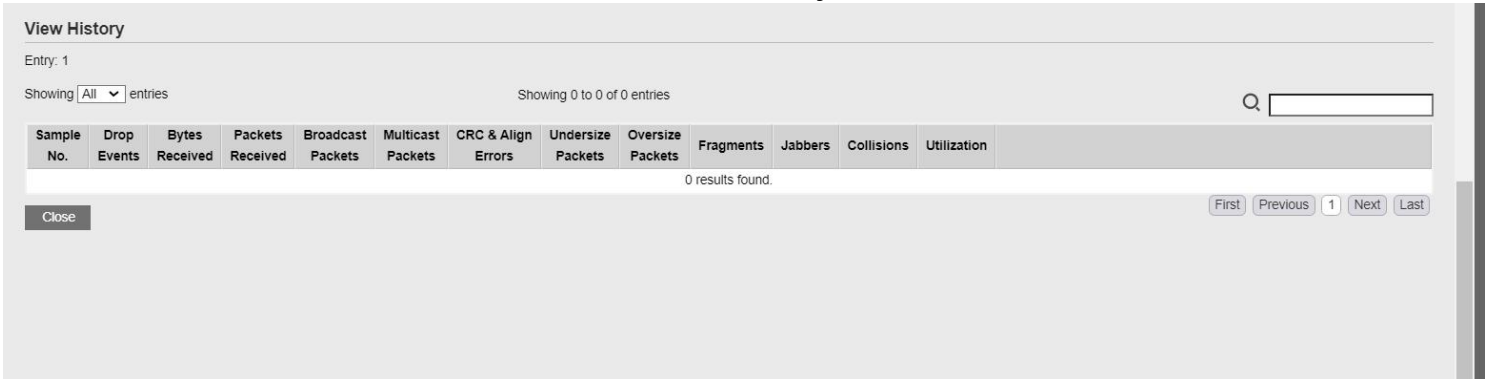


Figure 14-35: RMON History Log page.

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: <ul style="list-style-type: none">• 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.

Table 14-35: RMON History Log fields.

14.5.3. Event

For the RMON event, click **Management > RMON > Event**.



Figure 14-36: 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: <ul style="list-style-type: none">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.

Table 14-36: RMON Event fields.

Add Event

Entry

2

Notification

☒ None

☐ Event Log

☐ Trap

☐ Event Log and Trap

Community

Default Community

Description

Default Description

Owner

Apply

Close

Figure 14-37: 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: <ul style="list-style-type: none">• 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.

Table 14-37: RMON Event Add fields.

Edit Event

Entry

1

Notification

☒ None

☐ Event Log

☐ Trap

☐ Event Log and Trap

Community

Description

Default

Owner

Apply

Close

Figure 14-38: 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: <ul style="list-style-type: none">• 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.

Table 14-38: RMON Event Edit fields.

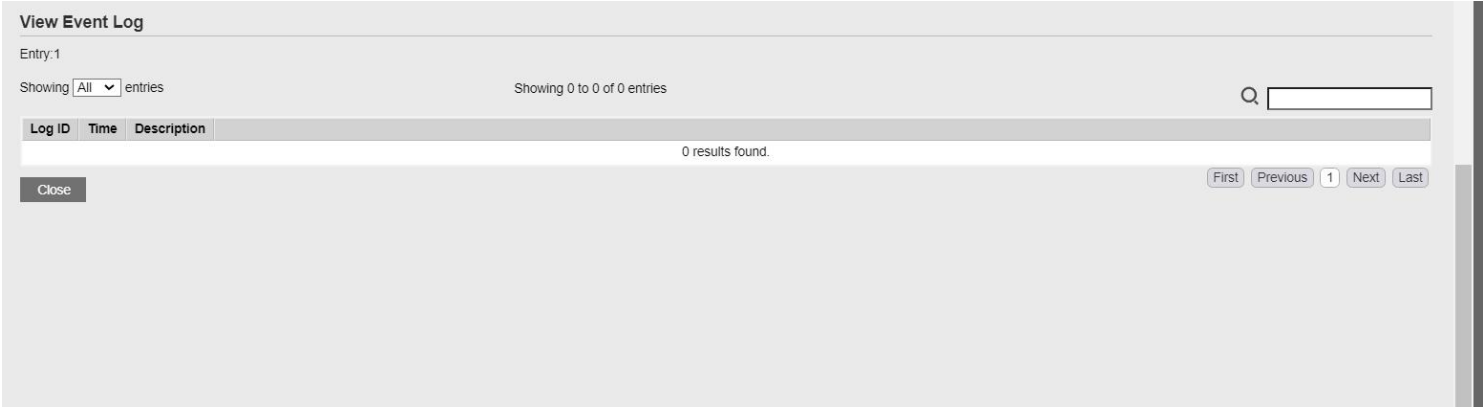


Figure 14-39: RMON Event Log page.

Field	Description
Log ID	The log identifier.
Time	The time that the event was triggered.
Description	The description for the event.

Table 14-39: RMON Event Log fields.

14.5.4. Alarm

For the RMON Alarm, click **Management > RMON > Alarm**.



Figure 14-40: RMON Alarm page.

Field	Description
Port	The port configuration for the RMON alarm.
Counter	<div>The counter for sampling<ul style="list-style-type: none">• 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.• CRCAlignError (CRC and Align Error): CRC alignment error.• UndersizePkts (Undersize Packets): Number of undersized packets.</div>

	<ul style="list-style-type: none">• 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.• Pkts1024to1518Octets (Frames Greater than 1024 Bytes): Number of packets size 1024 to 1518 octets.
Sampling	The sampling type including: <ul style="list-style-type: none">• 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.

Table 14-40: RMON Alarm fields.

Add Alarm

Entry1

PortGE1

CounterDrop Events

Sampling☒ Absolute
☐ Delta

Interval100Sec (1 - 2147483647, default 100)

Owner

Trigger☒ Rising
☐ Falling
☐ Rising and Falling

Rising

Threshold100(0 - 2147483647, default 100)

Event1 - Default

Falling

Threshold20(0 - 2147483647, default 20)

Event1 - Default

Apply

Close

Figure 14-41: RMON Alarm Add page.

Field	Description
Port	Specify the port for sampling
Counter	<div>Specify the counter for sampling</div> <ul style="list-style-type: none">• 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.

	<ul style="list-style-type: none"> • 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	<p>Specify the sampling type.</p> <ul style="list-style-type: none"> • 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.

Table 14-41: RMON Alarm Add fields.

Edit Alarm

Entry

1

Port

GE1

Counter

Drop Events

Sampling

☒ Absolute

☐ Delta

Interval

100

Sec (1 - 2147483647, default 100)

Owner

Trigger

☒ Rising

☐ Falling

☐ Rising and Falling

Rising

Threshold

100

(0 - 2147483647, default 100)

Event

1 - Default

Falling

Threshold

20

(0 - 2147483647, default 20)

Event

1 - Default

Apply

Close

Figure 14-42: RMON Alarm Edit page.

Field	Description
Port	Specify the port for sampling
Counter	<div>Specify the counter for sampling</div> <div><ul style="list-style-type: none">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.</div>

	<ul style="list-style-type: none">• 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	<p>Specify the sampling type.</p> <ul style="list-style-type: none">• 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.

Table 14-42: RMON Alarm Edit fields.

15 ERPS

ERPS (Ethernet Ring Protection Switching) is a G.8032 ring protection protocol released by ITU-T. The convergence speed can meet the requirements for carrier-grade reliability, and interoperability can be achieved if all devices within the ring network support the protocol.

The concepts of the ERPS protocol mainly include the ERPS ring, nodes, port roles, and port states.

1. ERPS Instance

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

2. Control VLAN

The control VLAN is the transmission VLAN for ERPS protocol messages. It serves the same purpose as the control VLAN in ERRP, and the protocol messages carry a TAG corresponding to the control VLAN.

3. RPL

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

4. ERPS ring

An ERPS ring is 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

A Layer 2 switching device that joins an ERPS ring is called a node. Each node cannot have more than two ports joining the same ERPS ring. Nodes are classified into four categories: RPL Owner, Neighbour, Next Neighbour and Common.

6. Port Role

According to the ERPS protocol, port roles are mainly RPL Owner , Neighbour , Next Neighbour and Common ports. There are four categories of port roles in the ERPS protocol: RPL Owner, Neighbour, Next Neighbour and Common:

① RPL Owner: There is only one RPL Owner port in an ERPS ring, which is determined by the user's configuration, and prevents loops from being generated in the ERPS ring by blocking the RPL Owner port. A node with an RPL Owner port becomes an RPL Owner node.

② RPL Neighbour: An ERPS ring has only one RPL Neighbour (neighbour) port, which is configured by the user and must be the port connecting to the RPL Owner port. When the network is normal, it will be blocked together with the RPL Owner port to prevent loops from being generated in the ERPS ring. A node with an RPL Neighbour port becomes an RPL Neighbour node.

RPL Next Neighbour: An ERPS ring can have up to two RPL Next Neighbour ports, which are configured by the user and must be the ports connecting to the RPL Owner node or the RPL Neighbour node, and the node that owns the RPL Next Neighbour port becomes the RPL Next Neighbour node. Neighbour node.

Note: The RPL Next Neighbour node is not much different from the common node, so you can replace it with the Common node in the configuration.

⑤ Common: Common ports, ports other than RPL Owner , Neighbour ,Next Neighbour ports are Common ports, if a node has only Common ports, then the node becomes a Common node.

7. Port Status

In ERPS ring, there are three types of port states to start ERPS protocol.

Forwarding: In Forwarding state, the port forwards user traffic as well as receives/sends R-APS messages and forwards R-APS messages from other nodes.

Discarding: In Discarding state, the port can only receive/send R-APS messages and cannot forward R-APS messages from other nodes.

③Disable: the state of the port when it is Linkdown.

8. Wrok Mode: ERPS operation mode

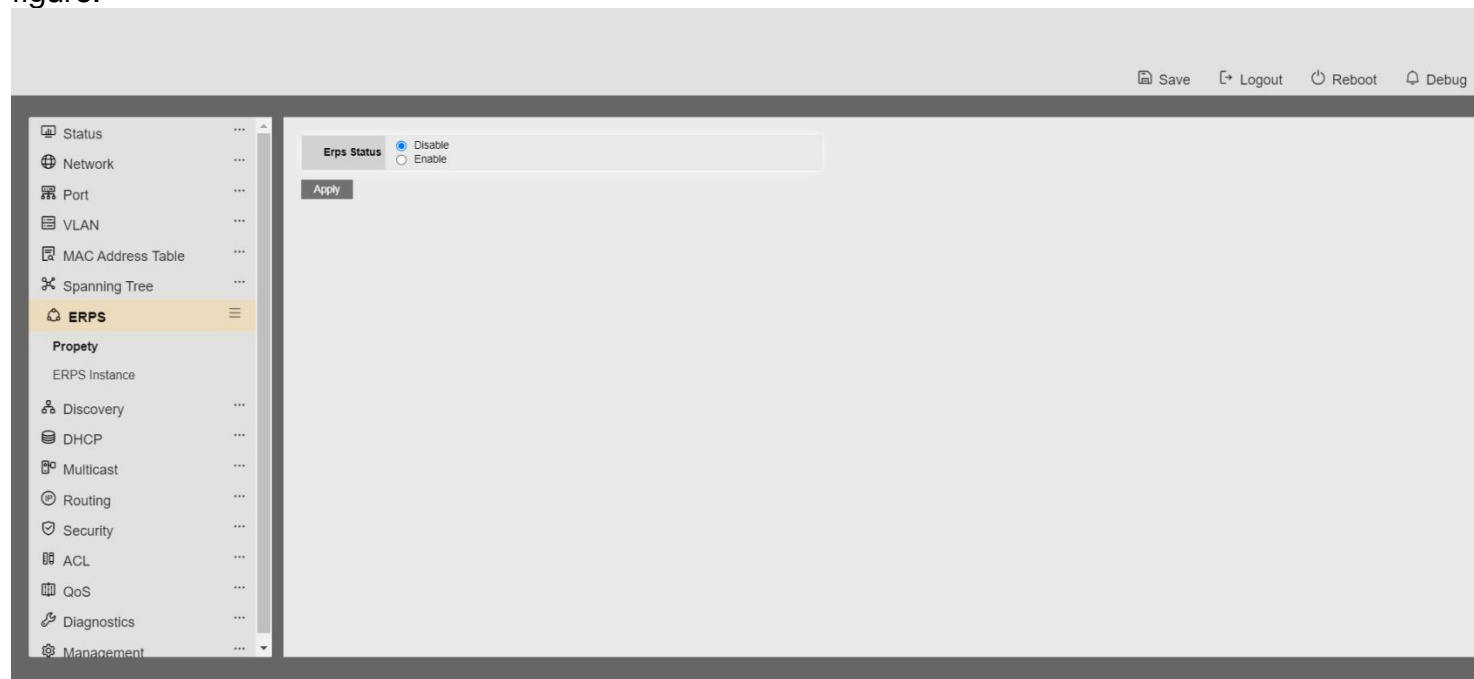
There are two types of ERPS operating modes: revertive and non revertive.

In revertive mode, when the link fails, the RPL link is released from protection, and then when the failed link returns to normal, the RPL link is re-protected to prevent loops;

② non revertive mode, after the fault recovery, the faulty node has been kept fault (not into the Forwarding), the RPL link has been in the state of release protection.

15.1 property

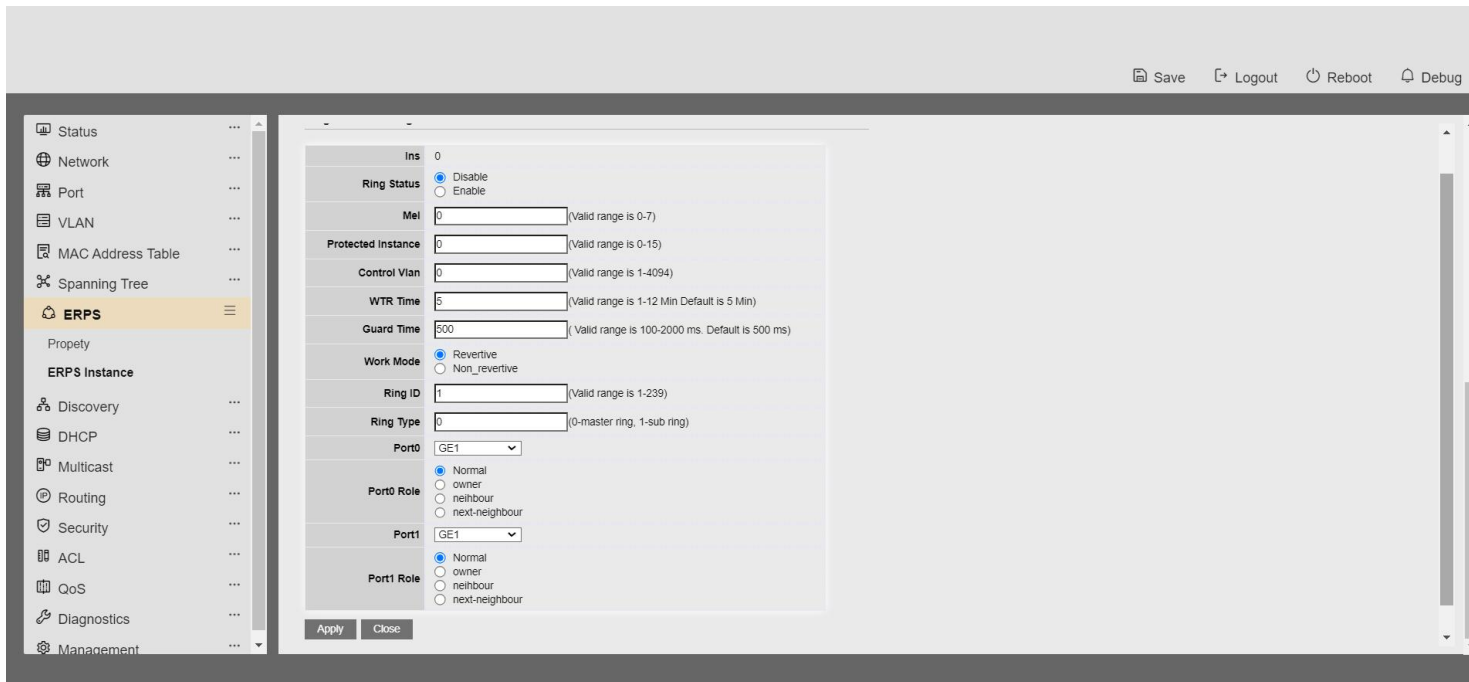
Click the "ERPS>Function Configuration" menu in the navigation tree to enter the "Function Configuration" interface and configure ERPS protocol enable or disable, as shown in the following figure.



15.2 ERPS instance

1.Click the ERP > ERP Instance menu in the navigation tree to enter the ERP Instance page, create an ERP instance, view the configuration information of each instance, and delete the instance, as shown in the following figure.

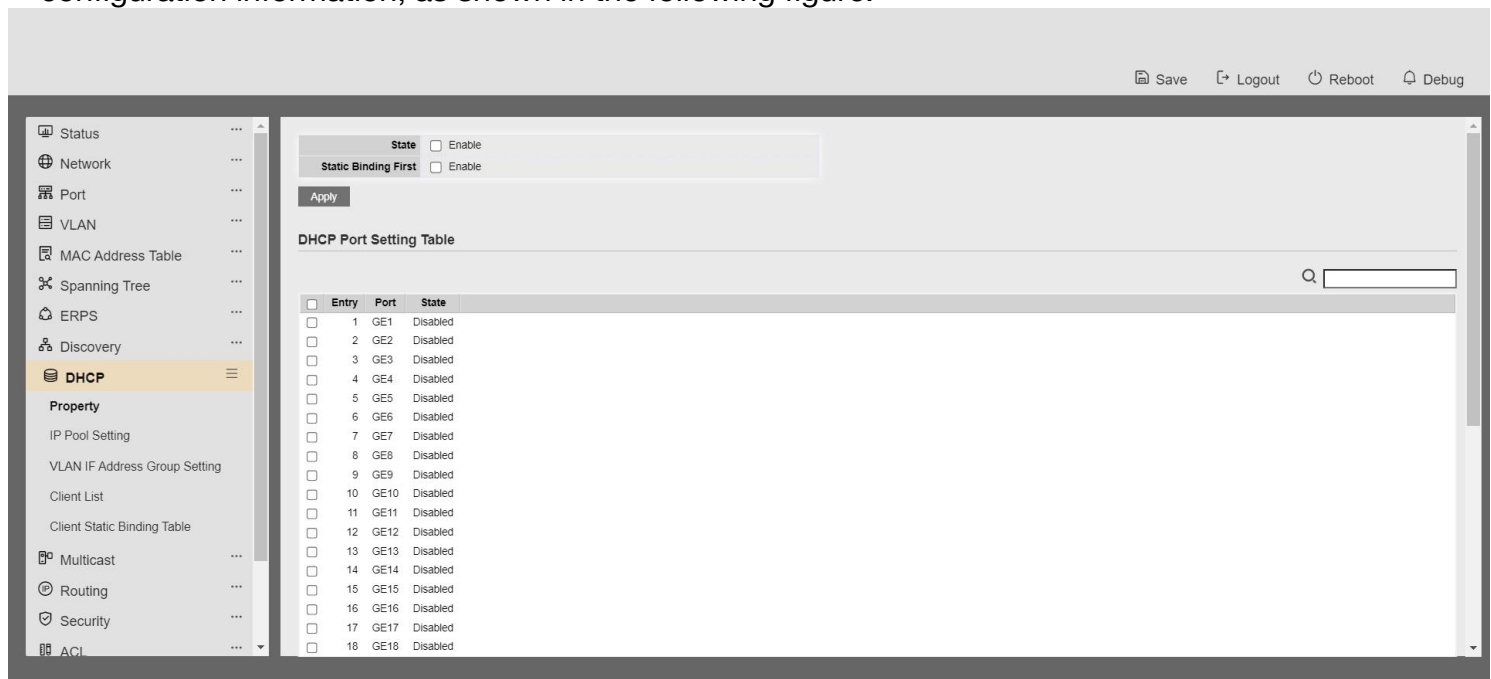
2.Select the instance, note that the instance needs to be created first, click the Modify button to enter the instance configuration page, as shown in the following figure:



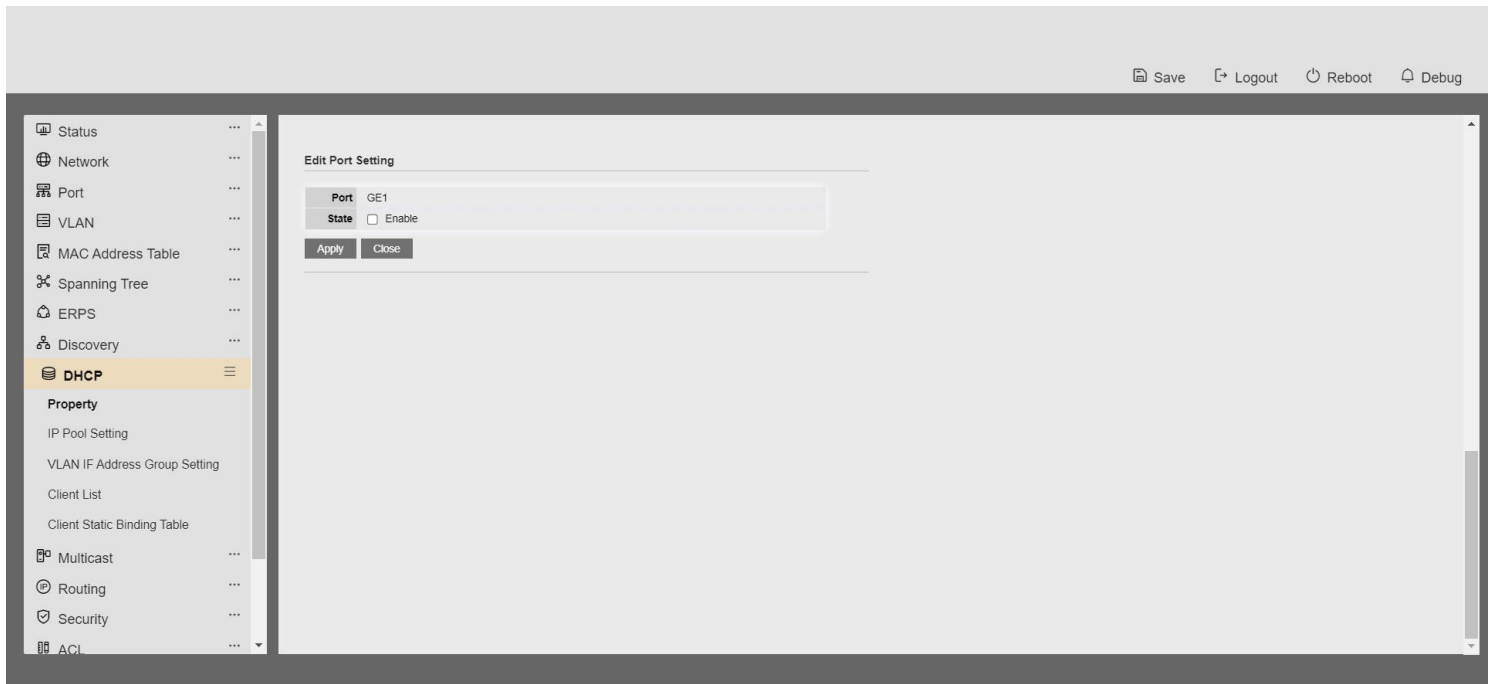
16 DHCP

16.1 property

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

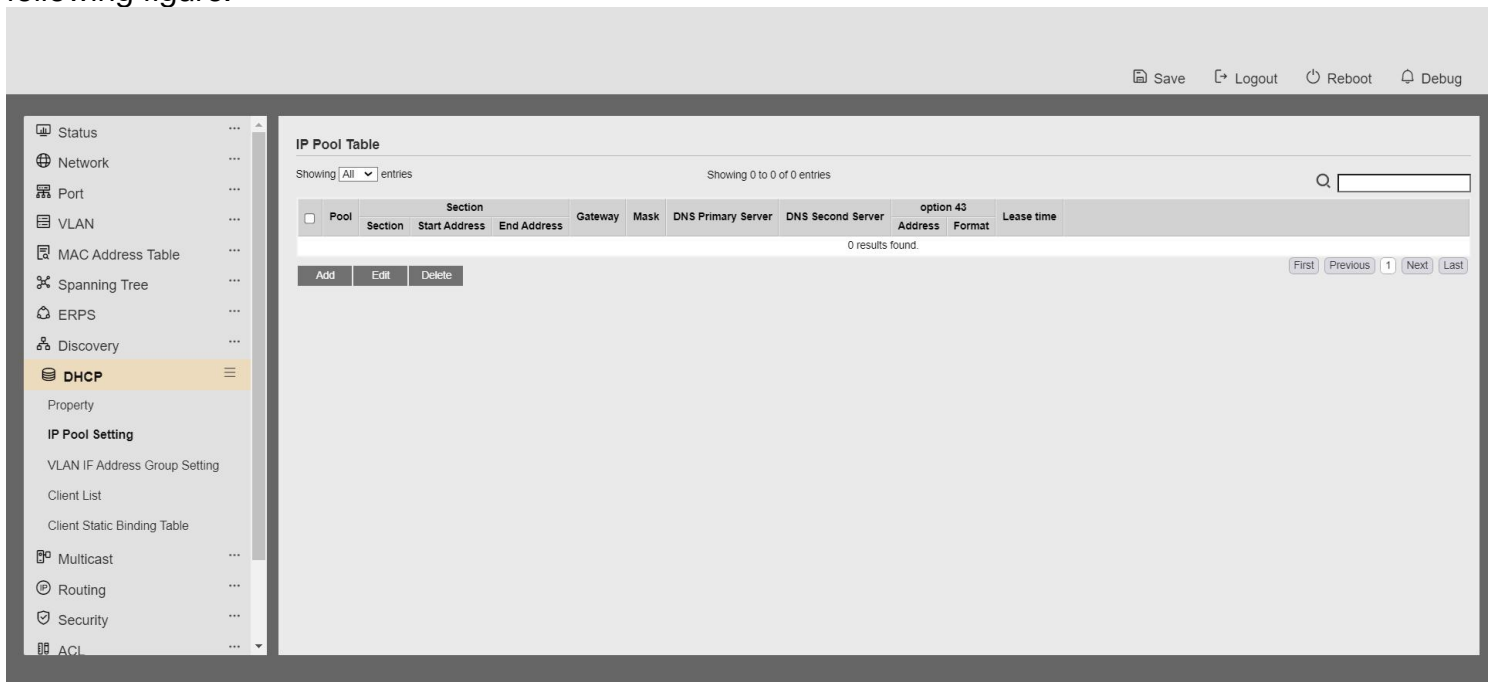


2. Click Modify to enter the Port Configuration page to enable or disable the dhcp server function under the port, as shown in the following figure:

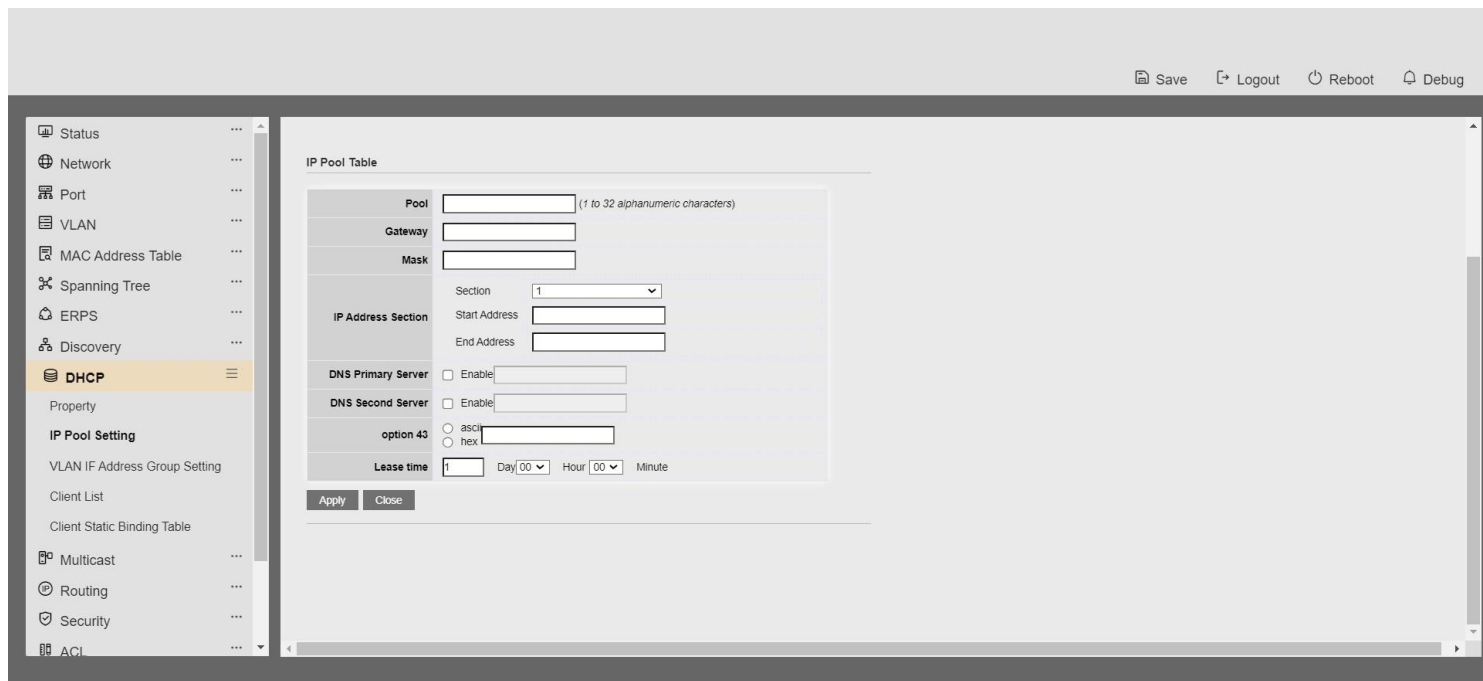


16.2 ip pool setting

1. Click the "DHCP> Address Pool Configuration" menu in the navigation tree to enter the "Address Pool Configuration" interface to view and configure the address pool for dhcpserver, as shown in the following figure.

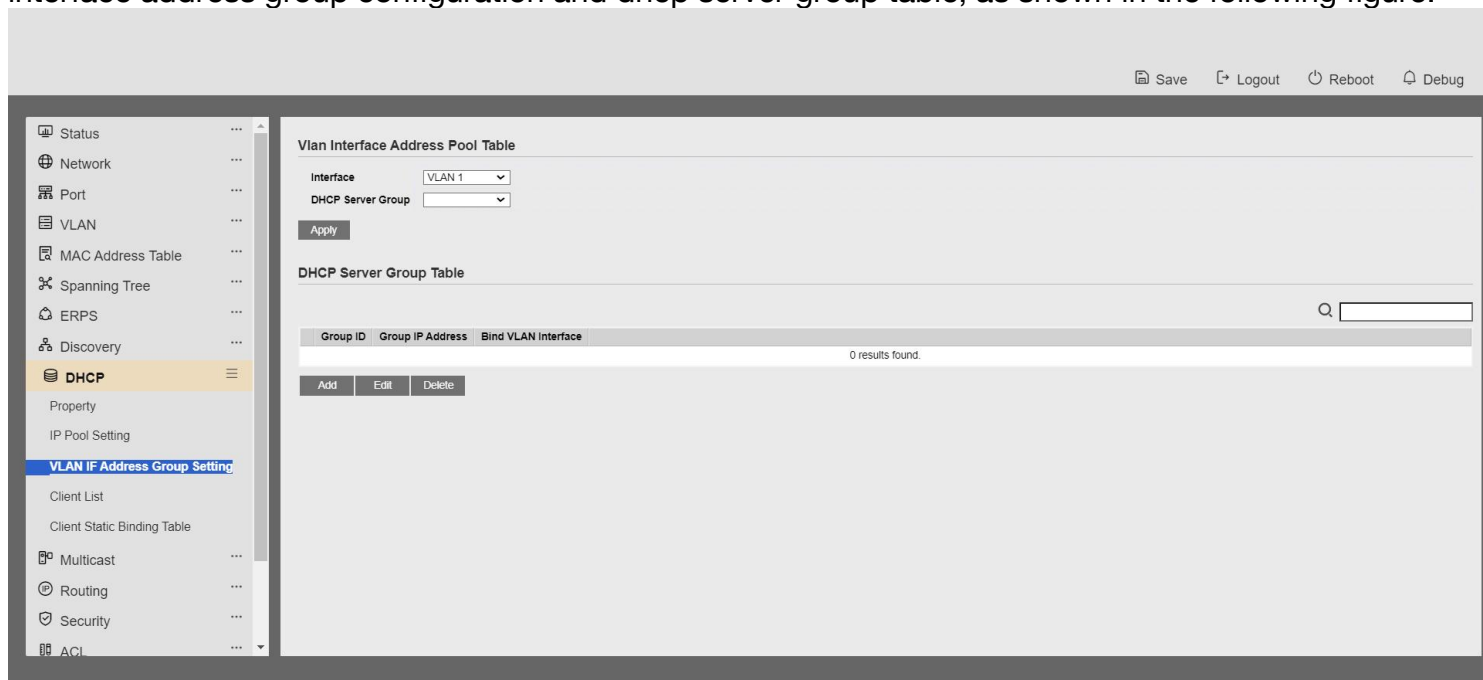


2. Click the Add or Modify button to add an address pool, as shown below



16.3 VLAN IF Address Group Setting

1. Click the "DHCP > VLAN Interface Address Group Configuration" menu in the navigation tree to enter the "VLAN Interface Address Group Configuration" interface to configure and view the vlan interface address group configuration and dhcp server group table, as shown in the following figure.

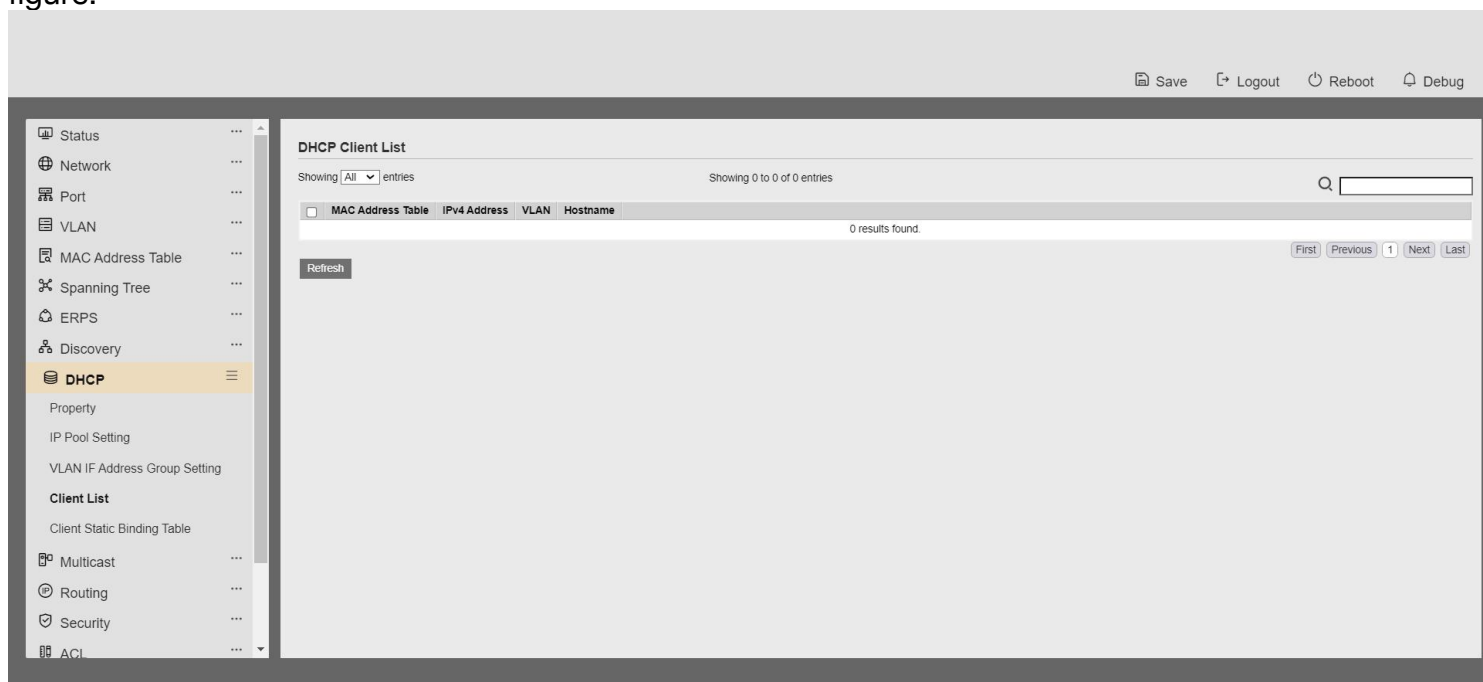


2. Click the Add or Modify button to add a DHCP server group, as shown below



16.4 Client List

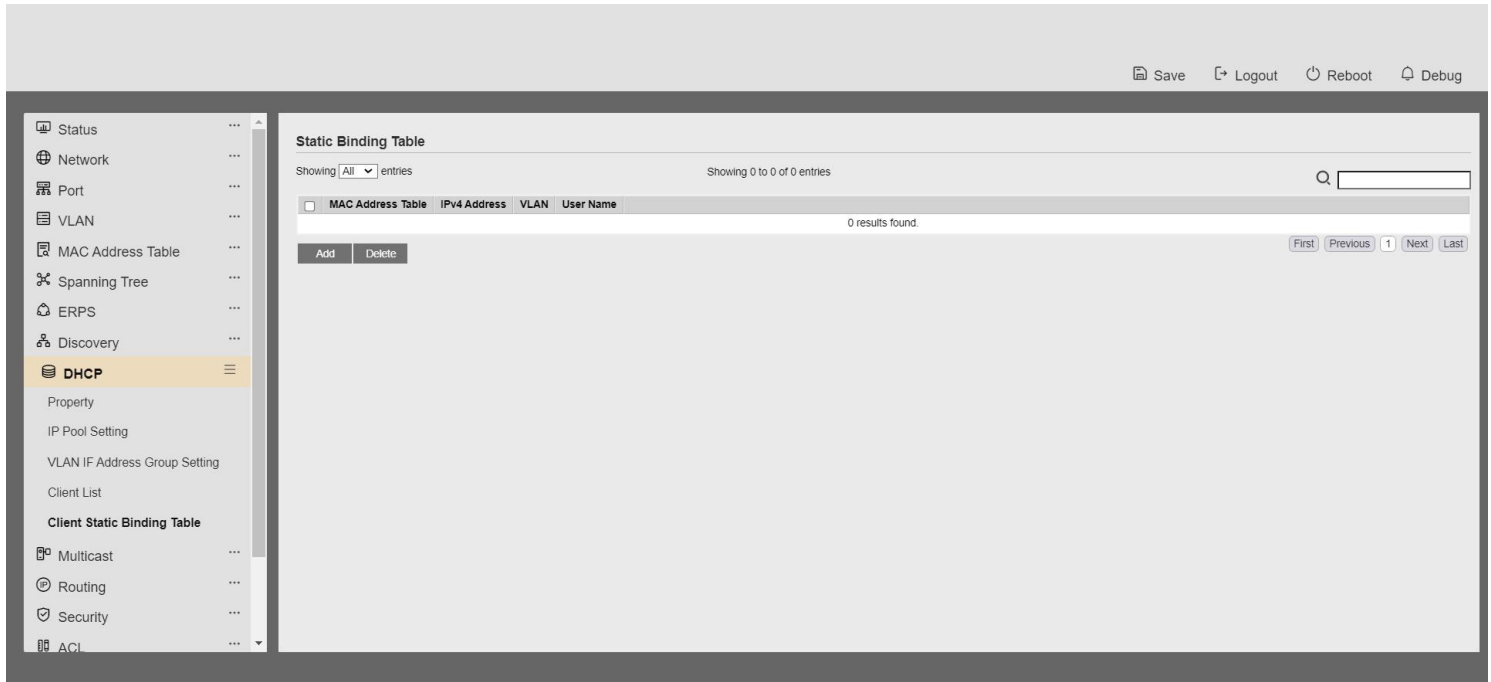
1. Click the "DHCP > Client List" menu in the navigation tree to enter the "Client List" interface and view the dhcp client list information, as shown in the following figure.



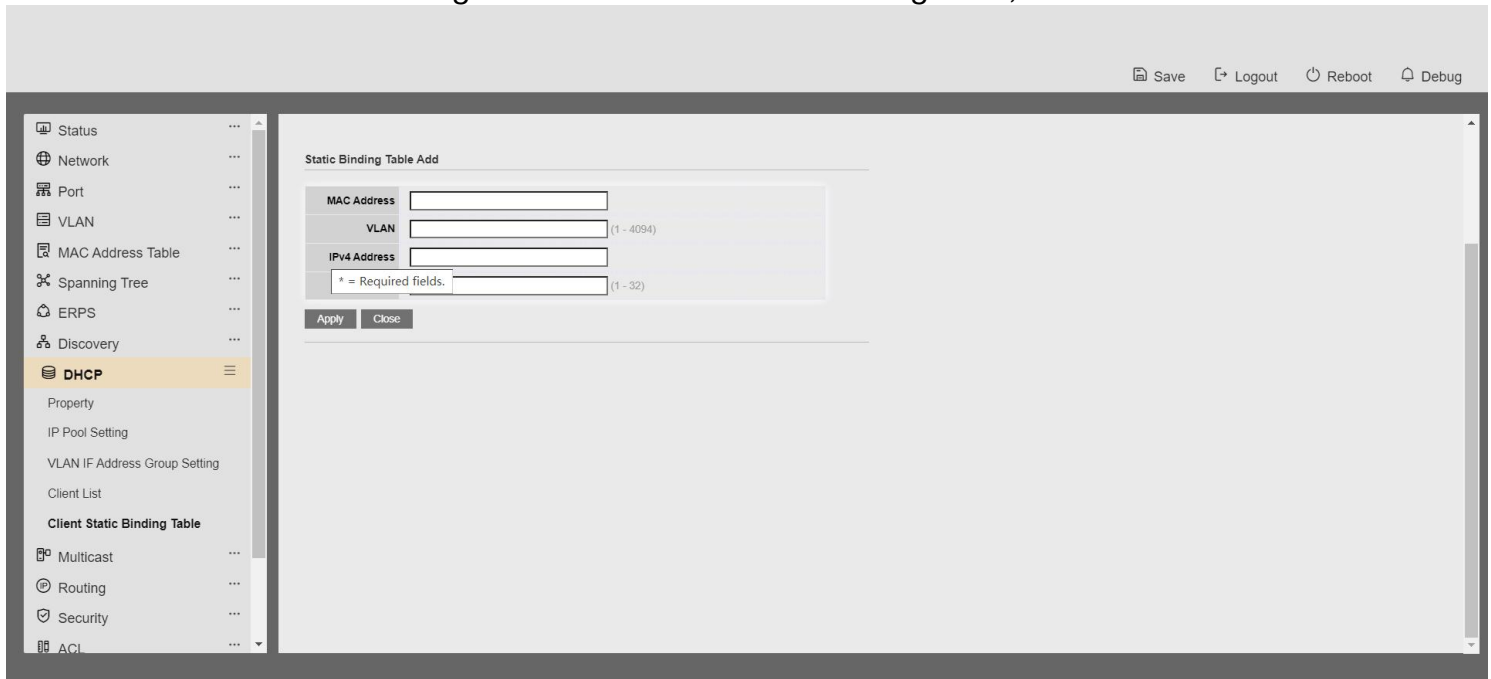
16.5 Client Static Binding Table

1. Click the "DHCP > Client Static Binding Table" menu in the navigation tree to enter the "Client Static Binding Table" interface to view and configure client static bindings, as shown in the following figure.

Web User Interface



2. Click the Add button to configure the client-side static binding table, as shown below



18 Network

18.1 DNS

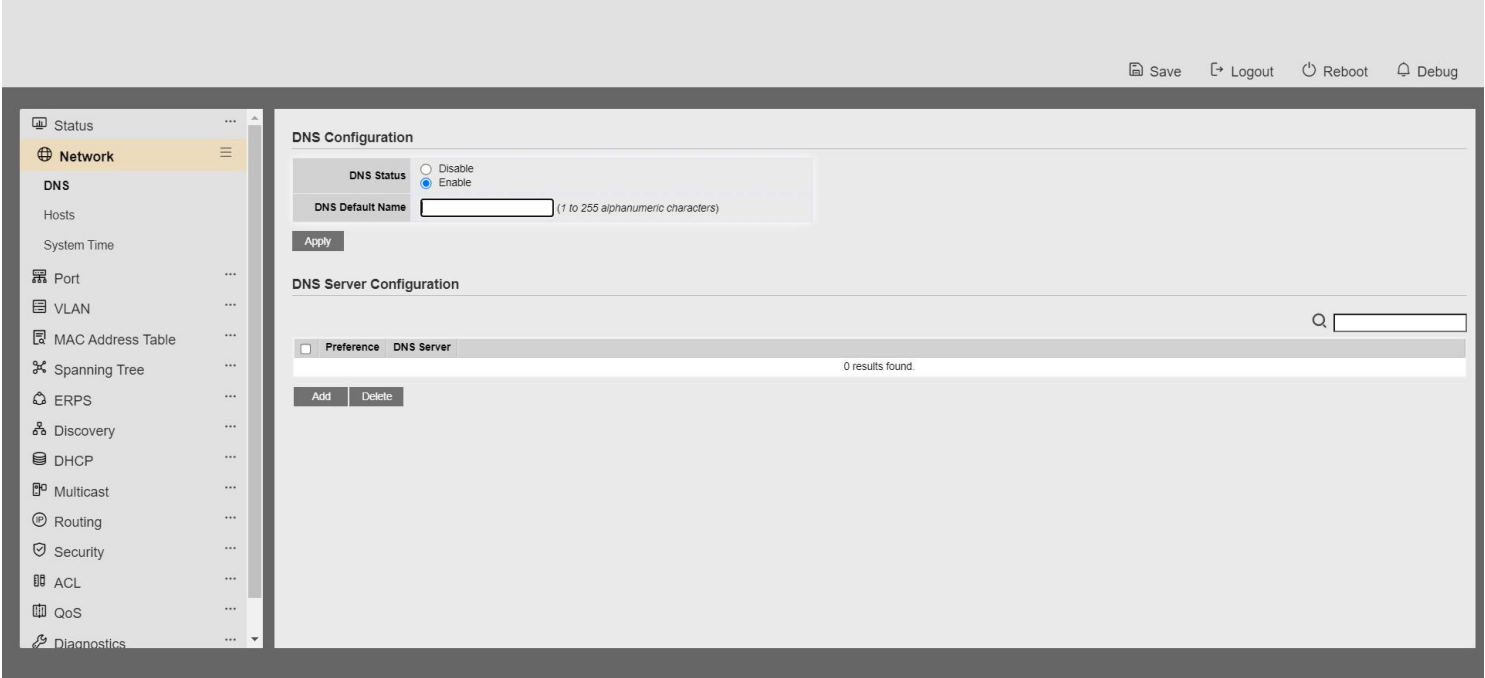
DNS stands for Domain Name System, which is used to name computers and network services organised into a domain hierarchy. Domain names are composed of a string of words or abbreviations separated by dots, and each domain name corresponds to a unique IP address, and there is a one-to-one correspondence between domain names and IP addresses on the Internet, and DNS is the server

Web User Interface

that carries out domain name resolution.DNS naming is used to find computers and services in TCP/IP networks such as the Internet, through user-friendly names.DNS is a core service of the Internet, and it serves as a means to organise computers and network services into a domain name hierarchy. DNS is a core service of the Internet, which serves as a distributed database that can map domain names and IP addresses to each other.

Steps:

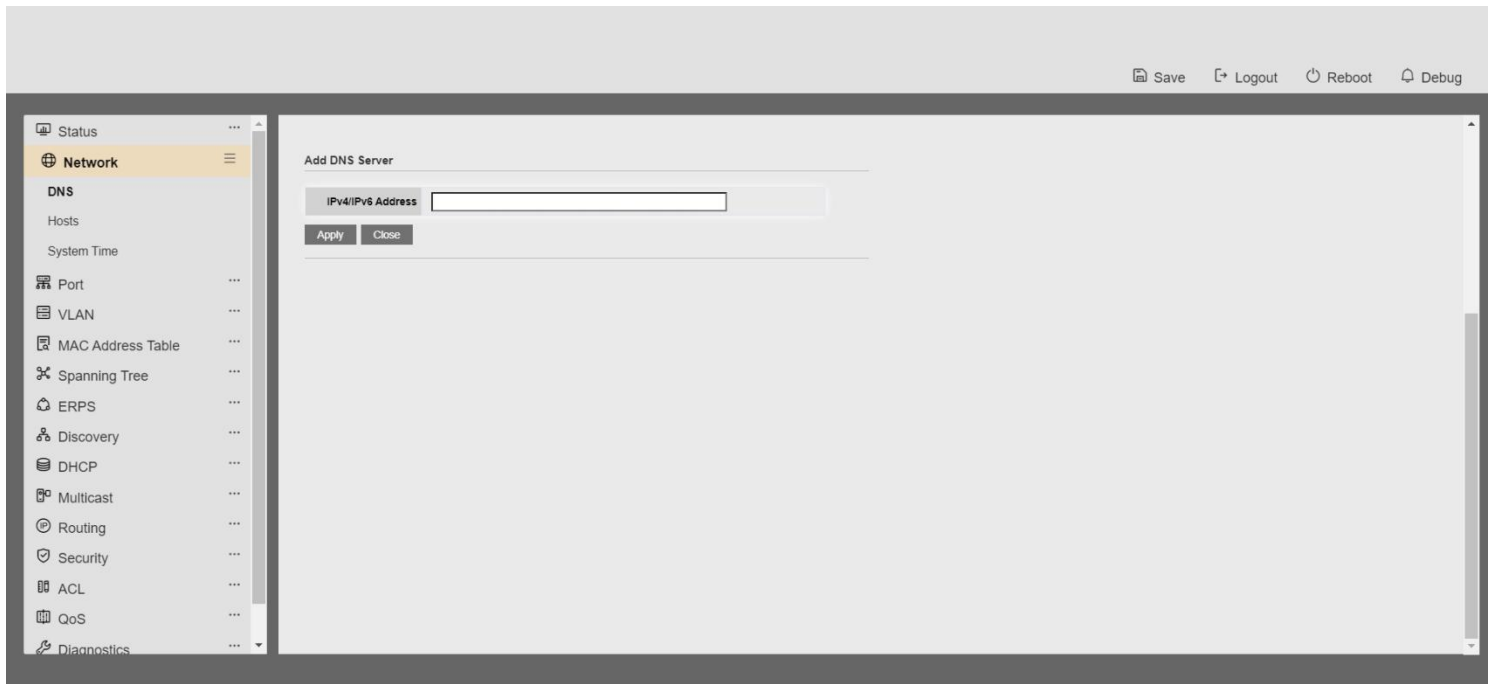
1. Click "Network Configuration > DNS Settings" in the navigation tree to enter the "DNS Settings" interface, as shown in the following figure.



The meaning of the interface is shown in the table below

Configuration Item Description	Configuration Item Description	Configuration Item Description
DNS Status DNS Switch	DNS Status DNS Switch	DNS Status DNS Switch
DNS Default Name Enter the DNS default name.	DNS Default Name Enter the DNS default name.	DNS Default Name Enter the DNS default name.

2. Click "Add" to set the DNS server.



3. Click Set to complete the configuration, as shown in the following

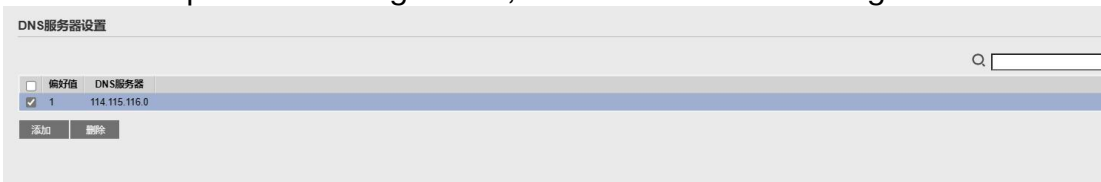
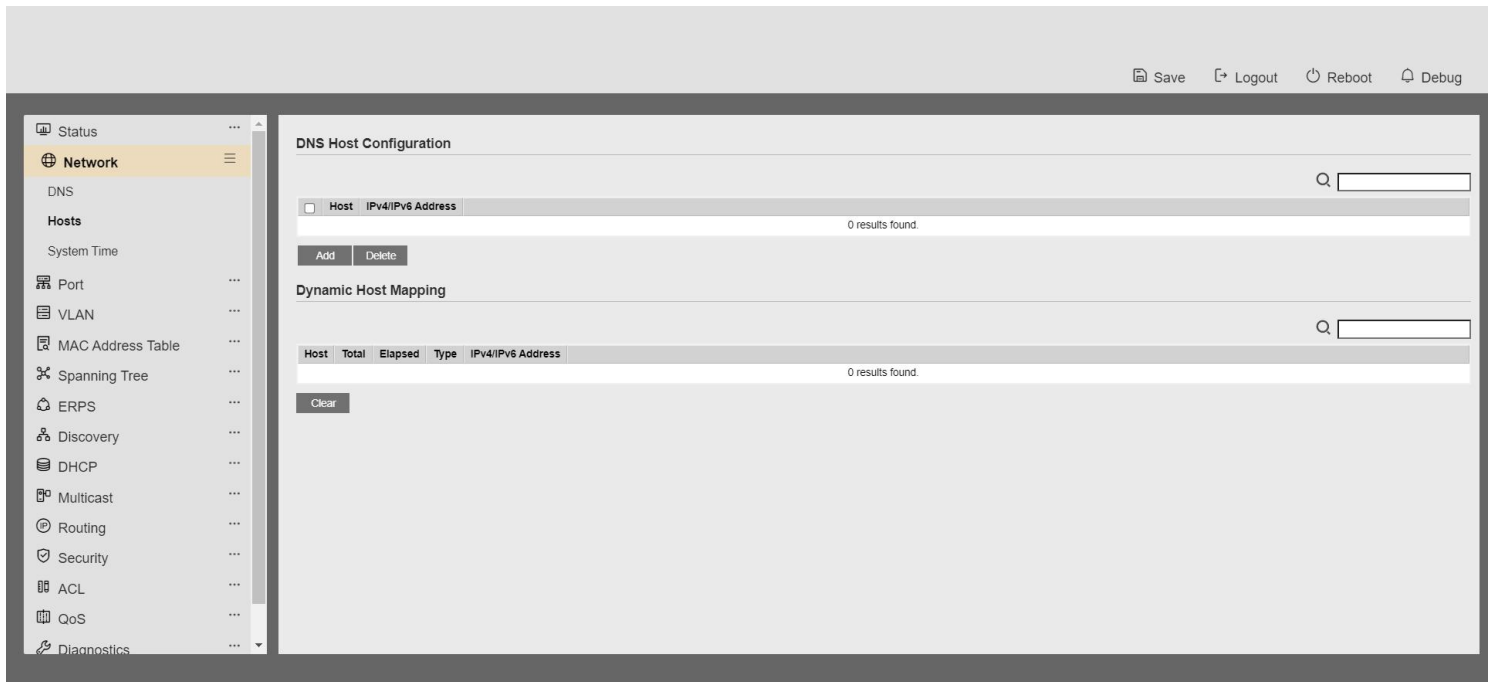


figure.

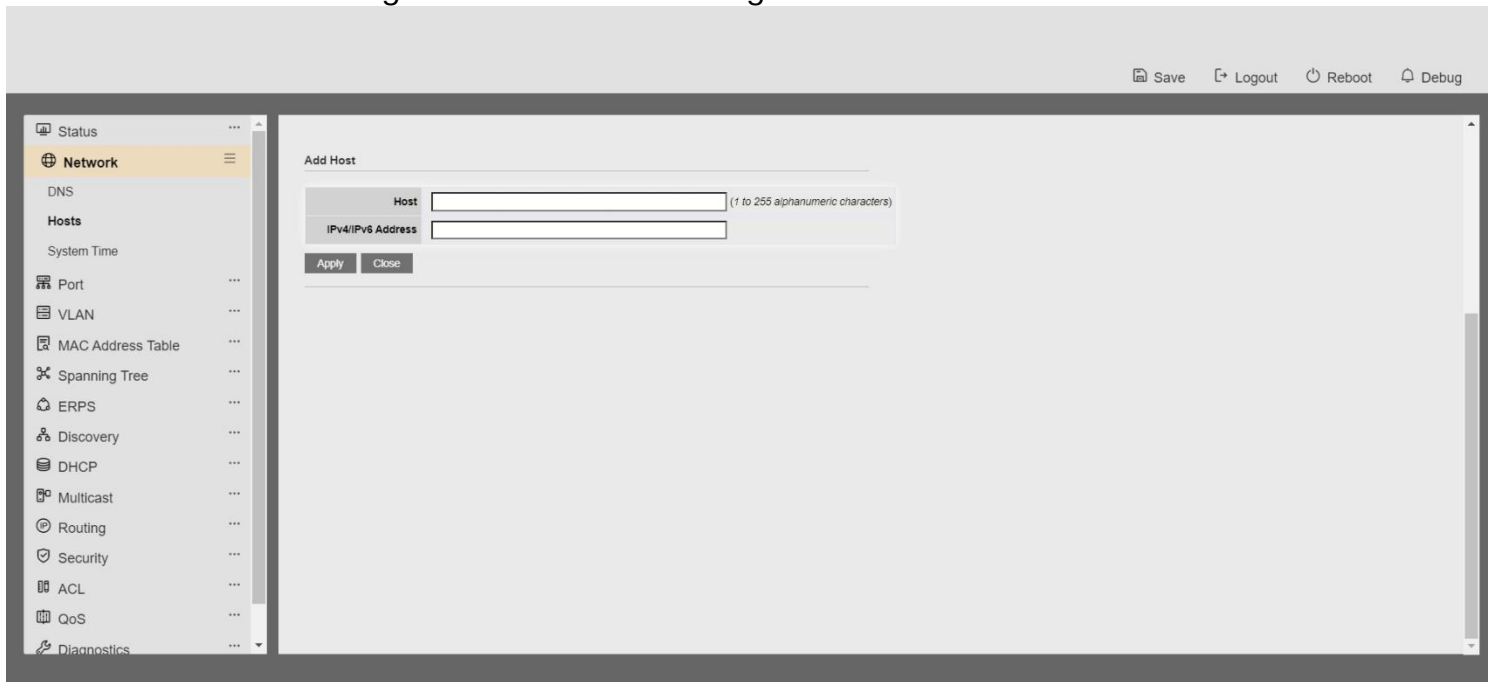
18.2 Hosts

1. Click Network Configuration > DNS Host Configuration in the navigation tree to enter the DNS Host Configuration interface, as shown in the following figure.

Web User Interface



2. Click the Add button to go to the DNS Host Configuration screen.



19 POE

19.1 POE port setting

1. Click the "POE Settings > POE Port Settings" menu in the navigation bar to enter the POE Port Settings interface, as shown in the following figure:

System info

System Power(W)	0
System Temperature(C)	45
Refresh Rate	<input type="radio"/> None <input type="radio"/> 5 sec <input checked="" type="radio"/> 10 sec <input type="radio"/> 30 sec

Port Setting Table

<input type="checkbox"/>	Entry	Port	PortEnable	Status	Type	Level	Actual Power(W)	Voltage(V)	Current(mA)
<input type="checkbox"/>	1	GE1	Enabled	Off	N/A	N/A	N/A	N/A	N/A
<input type="checkbox"/>	2	GE2	Enabled	Off	N/A	N/A	N/A	N/A	N/A
<input type="checkbox"/>	3	GE3	Enabled	Off	N/A	N/A	N/A	N/A	N/A
<input type="checkbox"/>	4	GE4	Enabled	Off	N/A	N/A	N/A	N/A	N/A
<input type="checkbox"/>	5	GE5	Enabled	Off	N/A	N/A	N/A	N/A	N/A
<input type="checkbox"/>	6	GE6	Enabled	Off	N/A	N/A	N/A	N/A	N/A
<input type="checkbox"/>	7	GE7	Enabled	Off	N/A	N/A	N/A	N/A	N/A
<input type="checkbox"/>	8	GE8	Enabled	Off	N/A	N/A	N/A	N/A	N/A

2. Select a port and click Modify to modify the management status and watchdog status of the current port.

Edit Port Setting

Port	GE1
PortEnable	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
WatchDog	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
<input type="button" value="Apply"/> <input type="button" value="Close"/>	

19.2 POE Port Timing Settings

1. Click "POE Settings > POE Port Timer Settings" menu in the navigation bar to enter the POE Port Timer Settings interface, as shown in the following figure:

Status

Network

Port

POE Setting

POE Port Setting

POE Port Timer Setting

VLAN

MAC Address Table

Spanning Tree

ERPS

Discovery

DHCP

Multicast

Routing

Security

ACL

Port GE1

<input type="checkbox"/>	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	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Tue	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Wed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Thu	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Fri	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sat	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sun	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Apply