

FIBERROAD

Layer 3 Ethernet Switch
Web-based
Network Management
User Manual



About This Manual

Introduction

This document chapter includes an introduction to the Fiberroad L3 WebGUI Network Management, which also contains Fiberroad Industrial Grade Ethernet Switch and Commercial Grade Ethernet Switch Series.

Conventions

This document contains notices, figures, screen captures, and certain text conventions.

Figures and Screen Captures

This document provides figures and screen captures as examples. These examples contain sample data. This data may vary from the actual data on an installed system.

Copyright©2022 Fiberroad Technology Co., Ltd. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form, be it electronically, mechanically, or by any other means such as photocopying, recording or otherwise, without the prior written permission of Fiberroad Technology Co., Ltd. (Fiberroad)

Information provided by Fiberroad is believed to be accurate and reliable. However, no responsibility is assumed by Fiberroad for its use nor for any infringements of patents or other rights of third parties that may result from its use. No license is granted by implication or otherwise under any patent rights of Fiberroad.

The information contained in this publication is subject to change without notice.

Trademarks

Fiberroad's trademarks have been identified as such. However, the presence or absence of such identification does not affect the legal status of any brand.

Units of Measurement

Units of measurement in this publication conform to SI standards and practices.

Jan 01, 2022

Version number: 1.0

CONTENTS

Revision History	8
1. Introduction	9
1.1 About Web-GUI Management.....	9
1.2 Preparing for Web Management.....	9
2. Status.....	10
2.1 System Information	10
2.2.Logging Message	12
2.3Port	13
2.3.1 Statistics.....	13
2.3.2 Error Disabled	15
2.3.3 Bandwidth Utilization	17
2.3 Link Aggregation	17
2.4 MAC Address Table.....	18
3. Network.....	19
3.1 IP Address.....	19
3.2 System Time	21
4.Port	23
4.1 Port Setting.....	23
4.2 Error Disabled	25
4.3 Link Aggregation	26
4.3.1 Group	26
4.3.2 Port Setting.....	28
4.3.3 LACP	30
4.4 EEE.....	31
4.5 Jumbo Frame.....	32
5. VLAN	33
5.1 VLAN.....	33
5.1.1 Creat VLAN.....	33
5.1.2 VLAN Configuration	34
5.1.3 Membership	35
5.1.4 Port Setting.....	37
5.2 Voice VLAN	39
5.2.1 Property.....	39
5.2.2 Voice OUI	41
5.3 Protocol VLAN	42

5.3.1 Protocol Group.....	42
5.3.2 Group Binding	43
5.4 MAC VLAN.....	45
5.4.1 MAC Group	45
5.4.2 Group Binding	46
5.5 Surveillance VLAN	47
5.5.1 Property	47
5.5.2 Surveillance OUI	49
5.6 GVRP	50
5.6.1 Property	50
5.6.2 Membership	52
5.6.3 Statistics	53
6. MAC Address Table	55
6.1 Dynamic Address	55
6.2 Static Address.....	55
6.3 Filtering Address	56
7. STP	57
7.1 Property.....	57
7.2 Port Setting.....	59
7.3 MST Instance	61
7.4 MST Port Setting	63
7.5 Statistics.....	65
8.Discovery	67
8.1 LLDP	67
8.1.1 Property	67
8.1.2 Port Setting.....	68
8.1.3 MED Network Policy.....	69
8.1.4 MED Port Setting	70
8.1.5 Packet View.....	72
8.1.6 Local Information.....	74
8.1.7 Neighbor	77
8.1.8 Statistics.....	78
9. Multicast.....	80
9.1 General	80
9.1.1 Property	80

9.1.2 Group Address	81
9.1.3 Router Port	83
9.1.4 Forward All.....	86
9.1.5 Throttling	88
9.1.6 Filtering Profile	89
9.1.7 Filtering Binding	92
9.2 IGMP Snooping	93
9.2.1 Property	93
9.2.2 Querier	96
9.2.3 Statistics	97
9.3 MLD Snooping.....	99
9.3.1 Property	99
9.3.2 Statistics	102
9.4 MVR.....	103
9.4.1 Property	103
9.4.2 Port Setting.....	104
9.4.3 Group Address	106
10.Security.....	108
10.1 RADIUS.....	108
10.2 TACACS+	110
10.3 AAA.....	112
10.3.1 Method List.....	112
10.3.2 Login Authentication.....	115
10.4 Management Access.....	115
10.4.1 Management VLAN	115
10.4.2 Management Services	116
10.4.3 Management ACL.....	117
10.4.4 Management ACE.....	118
10.5 Authentication Manager	120
10.5.1 Property	120
10.5.2 Port Setting.....	122
10.5.3 MAC-Based Local Account.....	126
10.5.4 WEB-Based Local Account.....	128
10.5.5 Sessions	130
10.6 Port Security.....	131

10.7 Protected Port.....	132
10.8 Storm Control.....	133
10.9 DoS.....	135
10.9.1 Property.....	135
10.9.2 Port Setting.....	137
10.10 Dynamic ARP Inspection	138
10.10.1 Property.....	138
10.10.2 Statistics.....	140
10.11 DHCP Snooping.....	141
10.11.1 Property.....	141
10.11.2 Statistics.....	142
10.11.3 Option 82 Property	143
10.12 IP Source Guard	146
10.12.1 Port Setting.....	146
10.12.2 IMPV Binding	147
10.12.3 Save Database.....	149
11.ACL.....	150
11.1 MAC ACL	150
11.2 MAC ACE.....	150
11.3 IPv4 ACL.....	152
11.4 IPv4 ACE.....	153
11.5 IPv6 ACL.....	156
11.6 IPv6 ACE.....	157
11.7 ACL Binding	162
12.QoS	164
12.1 General	164
12.1.1 Property.....	164
12.1.2 Queue Scheduling.....	166
12.1.3 CoS Mapping	167
12.1.4 DSCP Mapping.....	169
12.1.5 IP Precedence Mapping.....	170
12.2 Rate Limit.....	171
12.2.1 Ingress/Egress Port.....	171
12.2.2 Egress Queue	172
13.Diagnostics.....	175

13.1 Logging	175
13.1.1 Property	175
13.1.2 Remove Server	176
13.2 Mirroring	177
13.3 Ping	177
13.4 Traceroute	178
13.5 Copper Test	179
13.6 Fiber Module	179
13.7 UDLD	181
13.7.1 Property	181
13.7.2 Neighbor	182
14. Management	183
14.1 User Account	184
14.2 Firmware	185
14.2.1 Upgrade / Backup	185
14.2.2 Active Image	188
14.3 Configuration	189
14.3.1 Upgrade / Backup	189
14.3.2 Save Configuration	192
14.4 SNMP	193
14.4.1 View	193
14.4.2 Group	193
14.4.3 Community	196
14.4.4 User	198
14.4.5 Engine ID	202
14.4.6 Trap Event	204
14.4.7 Notification	204
14.5 RMON	208
14.5.1 Statistics	208
14.5.2 History	210
14.5.3 Event	213
14.5.4 Alarm	215
15. PoE Setting	220
15.1 PoE Port Setting	220
15.2 PoE Port Timer Setting	220

Revision History

Version	Date	Author	Reasons of Change	Section(s) Affected
1.0	2020/12/04		Initial Release	All

1. Introduction

1.1 About Web-GUI Management

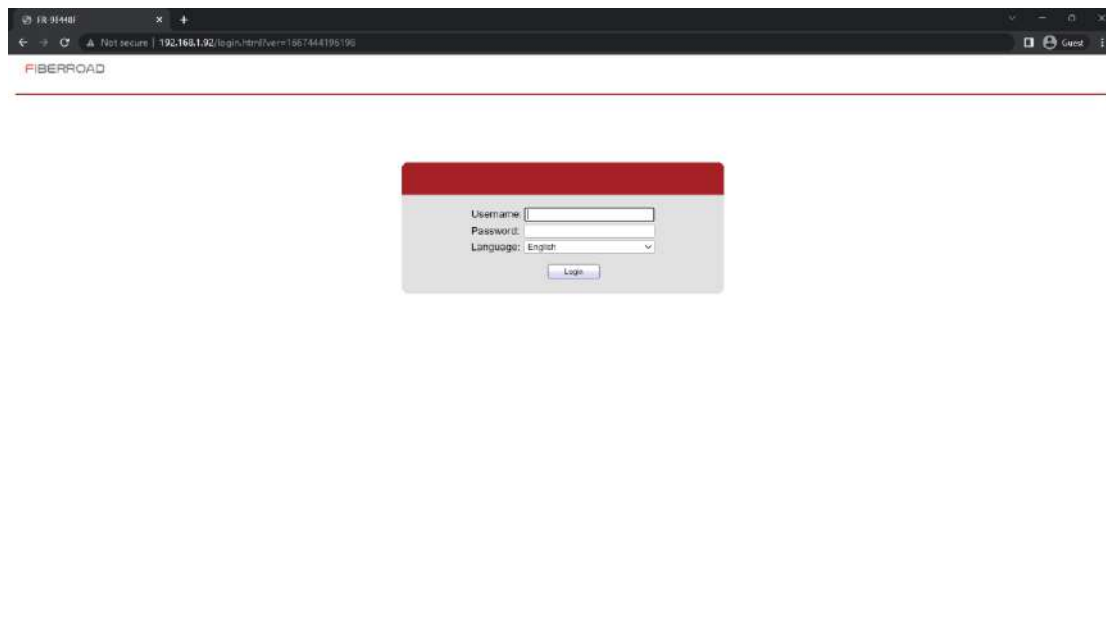
There is an embedded HTML web site residing in flash memory on CPU board of the switch, which offers advanced management features and allows users to manage the switch from anywhere on the network through a standard browser such as Mozilla Firefox or Chrome. (Note: Window IE is not supported) The Web-Based Management supports Mozilla Firefox 54.X or later, or Chrome 59.X or later. The Web browser is a program that can read hypertext.

1.2 Preparing for Web Management

Before using the web management, install the Ethernet Switch on the network and make sure that any one of the PCs on the network can connect with the Ethernet through the web browser.

All of the Fiberroad Network Switch default value of IP, subnet mask, username and password are listed as below:

- ❖ IP Address: 192.168.1.6
- ❖ HTTP service: Enable
- ❖ User Name: admin
- ❖ Password: admin



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.

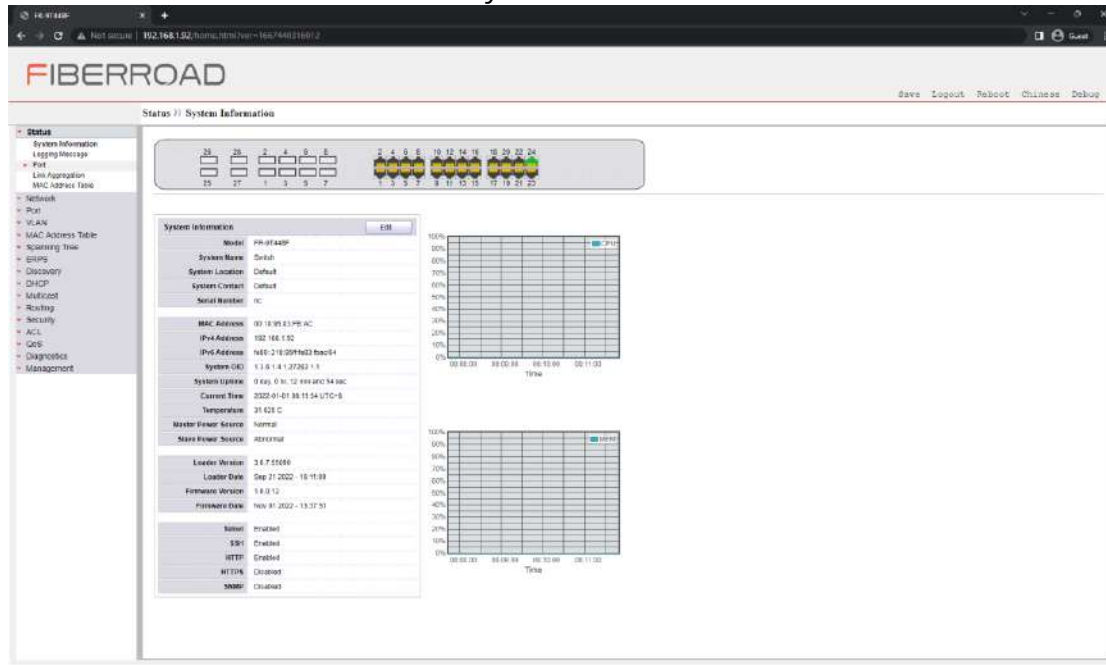


Figure 2-1 System Information Page

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.

The screenshot shows a web interface with a breadcrumb trail 'Status >> System Information'. Below this is a dialog box titled 'Edit System Information'. Inside the dialog, there are three rows of input fields: 'System Name' (containing 'Switch'), 'System Location' (containing 'Default'), and 'System Contact' (containing 'Default'). At the bottom of the dialog are two buttons: 'Apply' and '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.



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: 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.

2.3Port

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.

Status >> Port >> Statistics

Port: GE1 ▼

MIB Counter: ☒ All ☐ Interface ☐ Etherlike ☐ RMON

Refresh Rate: ☐ None ☐ 5 sec ☒ 10 sec ☐ 30 sec

Clear

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

Etherlike	
dot3StatsAlignmentErrors	0
dot3StatsFCSErrors	0
dot3StatsSingleCollisionFrames	0
dot3StatsMultipleCollisionFrames	0
dot3StatsDeferredTransmissions	0
dot3StatsLateCollisions	0
dot3StatsExcessiveCollisions	0
dot3StatsFrameTooLongs	0
dot3StatsSymbolErrors	0
dot3ControlInUnknownOpCodes	0
dot3InPauseFrames	0
dot3OutPauseFrames	0
RMON	
etherStatsDropEvents	0
etherStatsOctets	0
etherStatsPkts	0
etherStatsBroadcastPkts	0
etherStatsMulticastPkts	0
etherStatsCRCAlignErrors	0
etherStatsUnderSizePkts	0
etherStatsOverSizePkts	0
etherStatsFragments	0
etherStatsJabbers	0
etherStatsCollisions	0
etherStatsPkts64Octets	0
etherStatsPkts65to127Octets	0
etherStatsPkts128to255Octets	0
etherStatsPkts256to511Octets	0
etherStatsPkts512to1023Octets	0
etherStatsPkts1024to1518Octets	0

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
	• 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.

Status >> Port >> Error Disabled

Error Disabled Table

	Port	Reason	Time Left (sec)
☐	GE1	---	---
☐	GE2	---	---
☐	GE3	---	---
☐	GE4	---	---
☐	GE5	---	---
☐	GE6	---	---
☐	GE7	---	---
☐	GE8	---	---
☐	GE9	---	---
☐	GE10	---	---
☐	LAG1	---	---
☐	LAG2	---	---
☐	LAG3	---	---
☐	LAG4	---	---
☐	LAG5	---	---
☐	LAG6	---	---
☐	LAG7	---	---
☐	LAG8	---	---

Refresh Recover

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: BPDU Guard

-
- **UDLD** Table 2-6: Error Disabled Status fields.
 - **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.

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

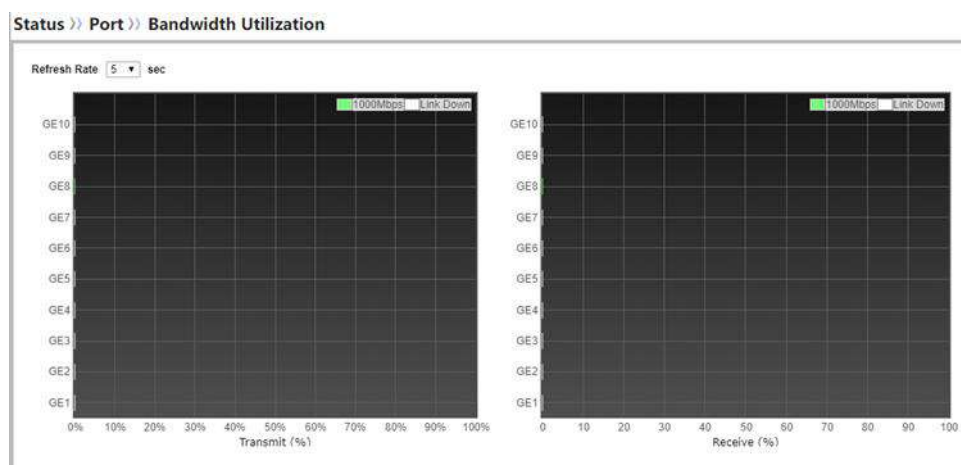


Figure 2-6 Port Bandwidth Utilization Page

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

Table 2-7 Bandwidth Utilization Field

2.3 Link Aggregation

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

LAG	Name	Type	Link Status	Active Member	Inactive Member
LAG 1	---	---	---		
LAG 2	---	---	---		
LAG 3	---	---	---		
LAG 4	---	---	---		
LAG 5	---	---	---		
LAG 6	---	---	---		
LAG 7	---	---	---		
LAG 8	---	---	---		

Figure 2-7 Link Aggregation Status Page

Field	Description
LAG	LAG Name
Name	LAG port description

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

Table 2-8 LAG Status Fields

2.4 MAC Address Table

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

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

Status >> MAC Address Table

Figure 2-8 MAC Address Status Page

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

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 IP Address

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

Network >> IP Address

IPv4 Address	
Address Type	☐ Static ☒ Dynamic
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.254

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

Operational Status	
IPv4 Address	192.168.1.1
IPv4 Default Gateway	192.168.1.254
IPv6 Address	::
IPv6 Gateway	::
Link Local Address	fe80::2e0:4cff:fe00:0/64

Apply

Figure 3-1: IP Address page.

Field	Description
Address Type	The address type of switch IP configuration including Static: Static IP configured by users will be used. Dynamic: Enable the DHCP to obtain the IP address from a DHCP server.
IP Address	Specify the switch static IP address on the static configuration.
Subnet Mask	Specify the switch subnet mask on the static configuration
Default Gateway	Specify the default gateway on the static configuration. The default gateway must be in the same subnet with switch IP address configuration.

Default Gateway	Specify the default gateway on the static configuration. The default gateway must be in the same subnet with switch IP address configuration.
DNS Server 1	Specify the primary user-defined IPv4 DNS server configuration
DNS Server 2	Specify the secondary user-defined IPv4 DNS server configuration

Table 3-1: IPv4 Address fields.

Field	Description
Auto Configuration	Enable/Disable the IPv6 auto configuration.
DHCPv6 Client	Enable/Disable the DHCPv6 client.
IPv6 Address	Specify the IPv6 address, when the IPv6 auto configuration and DHCPv6 client are disabled.
IPv6 Prefix	Specify the prefix for the IPv6 address, when the IPv6 auto configuration and DHCPv6 client are disabled.
Gateway	Specify the IPv6 default gateway, when the IPv6 auto configuration and DHCPv6 client are disabled.
DNS Server 1	Specify the primary user-defined IPv6 DNS server configuration.
DNS Server 2	Specify the secondary user-defined IPv6 DNS server configuration.

Table 3-2: IPv6 Address fields.

Field	Description
IPv4 Address	The operational IPv4 address of the switch.
IPv4 Gateway	The operational IPv4 gateway of the switch.
IPv6 Address	The operational IPv6 address of the switch.
IPv6 Gateway	The operational IPv6 gateway of the switch.
Link Local Address	The IPv6 link local address for the switch.

Table 3-3: Operational Status fields.

3.2 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.

Figure 3-2 System Time Page

Field	Description
Source	Select the time source. • SNTP: Time sync from NTP server. • From Computer: Time set from browser host. • Manual Time: Time set by manually configure.
Time Zone	Select a time zone difference from listing district.
SNTP	Description
Address Type	Select the address type of NTP server. This is enabled when time source is SNTP.
Server Address	Input IPv4 address or hostname for NTP server. This is enabled when time source is SNTP.
Server Port	Input NTP port for NTP server. Default is 123. This is enabled when time source is SNTP.
Manual Time	Description

Date	Input manual date. This is enabled when time source is manual.
Time	Input manual time. This is enabled when time source is manual.
Daylight Saving Time	Description
Type	Select the mode of daylight saving time. • Disable: Disable daylight saving time. • Recurring: Using recurring mode of daylight saving time. • Non-Recurring: Using non-recurring mode of daylight saving time. • USA: Using daylight saving time in the United States that starts on the second Sunday of March and ends on the first Sunday of November • European: Using daylight saving time in the Europe that starts on the last Sunday in March and ending on the last Sunday in October
Offset	Specify the adjust offset of daylight saving time.
Recurring From	Specify the starting time of recurring daylight saving time. This field available when selecting "Recurring" mode.
Recurring To	Specify the ending time of recurring daylight saving time. This field available when selecting "Recurring" mode.
Non-recurring From	Specify the starting time of non-recurring daylight saving time. This field available when selecting "Non-Recurring" mode.
Non recurring To	Specify the ending time of recurring daylight saving time. This field available when selecting "Non-Recurring" mode.

Table 3-4 System Time Fields

4.Port

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.

Port >> Port Setting

Port Setting Table

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

Edit

Figure 4-1 Port Setting Table

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

Table 4-1 Port Setting Table Fields

Port >> Port Setting

Edit Port Setting

Port	GE7-GE10	
Description		
State	☒ Enable	
Speed	☒ Auto ☐ 10M ☐ Auto - 10M ☐ 100M ☐ Auto - 100M ☐ 1000M ☐ Auto - 1000M ☐ 10G ☐ Auto - 10M/100M	
Duplex	☒ Auto ☐ Full ☐ Half	
Flow Control	☐ Auto ☐ Enable ☒ Disable	
Apply Close		

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.

Port speed capabilities.**Speed**

- **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

Port duplex capabilities.**Duplex**

- **Auto:** Auto duplex with all capabilities
- **Half:** Auto speed with 10M and 100M ability only
- **Full:** Auto speed with 10M/100M/1000M ability only

Port flow control.**Flow Control**

- **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**

Port >> Error Disabled

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

Figure 4-3 Error Disabled Page

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

DHCP Rate Limit	Enabled to auto shutdown port when DHCP rate limit reason occur. This reason caused by DHCP packet rate exceed DHCP rate limit.
ARP Rate Limit	Enabled to auto shutdown port when ARP rate limit reason occur. This reason caused by DHCP packet rate exceed ARP rate limit.

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.

Figure 4-4 LAG Global Setting

Field	Description
Load Balance Algorithm	LAG load balance distribution algorithm • src-dst-mac: Based on MAC address • src-dst-mac-ip: Based on MAC address and IP address

Table 4-4 LAG Global Setting Fields

Link Aggregation Table

LAG	Name	Type	Link Status	Active Member	Inactive Member
☒ LAG 1		---	---		
☐ LAG 2		---	---		
☐ LAG 3		---	---		
☐ LAG 4		---	---		
☐ LAG 5		---	---		
☐ LAG 6		---	---		
☐ LAG 7		---	---		
☐ LAG 8		---	---		

Figure 4-5 LAG Group Setting Table

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

Table 4-5 LAG Group Setting Fields

Port >> Link Aggregation >> Group

Edit Link Aggregation Group

LAG

1

Name

Type

☒ Static
☐ LACP

Member

Available Port

GE3
GE4
GE5
GE6
GE7
GE8
GE9
GE10

>
<

Selected Port

GE1
GE2

Apply

Close

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
	• 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.

Port >> Link Aggregation >> Port Setting

Port Setting Table

Q

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

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. • Enabled: Enable the port. • Disabled: Disable the port.
Link Status	Current LAG port link status • Up: Port is link up • Down: Port is link down
Speed	Current LAG port speed configuration and link speed status
Duplex	Current LAG port duplex configuration and link duplex status

Flow Control

Current LAG port flow control configuration and link flow control status

Table 4-7 Port Setting Status Fields

Port >> Link Aggregation >> Port Setting

Edit Port Setting

Port

LAG1

Description

State

☒ Enable

Speed

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

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. • Enable: Enable the port. • Disable: Disable the port.
Speed	Port speed capabilities. • Auto: Auto speed with all capabilities • Auto-10M: Auto speed with 10M ability only • Auto-100M: Auto speed with 100M ability only • Auto-1000M: Auto speed with 1000M ability only • Auto-10M/100M: Auto speed with 10M/100M abilities • 10M: Force speed with 10M ability • 100M: Force speed with 100M ability • 1000M: Force speed with 1000M ability
Flow Control	Port flow control. • Auto: Auto flow control by negotiation. • Enabled: Enable flow control ability. • Disabled: Disable flow control ability.

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.

Port >> Link Aggregation >> LACP

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

Apply

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.

LACP Port Setting Table

Entry	Port	Port Priority	Timeout
1	GE1	1	Long
2	GE2	1	Long
3	GE3	1	Long
4	GE4	1	Long
5	GE5	1	Long
6	GE6	1	Long
7	GE7	1	Long
8	GE8	1	Long
9	GE9	1	Long
10	GE10	1	Long

Edit

Figure 4-10 LACP Port Setting Table

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

Table 4-10 LACP Port Setting Table Fields

Port >> Link Aggregation >> LACP

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. • 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 > EEE

This page allow user to configure Energy Efficient Ethernet settings.

Port >> EEE

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

Figure 4-12 EEE Setting Table

Field	Description
Port	Port Name
State	Port EEE admin state. • Enabled: EEE is enabled • Disabled: EEE is disabled

Operational Status

Port EEE operational status.

- **Enabled:** EEE is operating
- **Disabled:** EEE is no operating

Table 4-12 EEE Setting Table Fields

Field	Description
Port	Selected port list
State	Port EEE admin state. • 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.

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

5. VLAN

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

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

5.1 VLAN

Use the VLAN pages to configure settings of VLAN.

5.1.1 Create VLAN

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

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

VLAN >> VLAN >> Create VLAN

Available VLAN

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

Created VLAN

- VLAN 1

Apply

VLAN Table

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

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

Edit **Delete** **First** **Previous** **1** **Next** **Last**

Figure 5-1 Create VLAN Page

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

Table 5-1 Create VLAN Fields

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.

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	Select the membership for this port of the specified VLAN ID.
	• Forbidden: Specify the port is forbidden in the VLAN. • Excluded: Specify the port is excluded in the VLAN. • Tagged: Specify the port is tagged member in the VLAN. • Untagged: Specify the port is untagged member in the VLAN.
PVID	Display if it is PVID of interface.

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

VLAN >> VLAN >> Membership

Membership Table					
	Entry	Port	Mode	Administrative VLAN	Operational VLAN
	1	GE1	Trunk	1UP	1UP
	2	GE2	Trunk	1UP	1UP
	3	GE3	Trunk	1UP	1UP
	4	GE4	Trunk	1UP	1UP
	5	GE5	Trunk	1UP	1UP
	6	GE6	Trunk	1UP	1UP
	7	GE7	Trunk	1UP	1UP
	8	GE8	Trunk	1UP	1UP
	9	GE9	Trunk	1UP	1UP
	10	GE10	Trunk	1UP	1UP
	11	LAG1	Trunk	1UP	1UP
	12	LAG2	Trunk	1UP	1UP
	13	LAG3	Trunk	1UP	1UP
	14	LAG4	Trunk	1UP	1UP
	15	LAG5	Trunk	1UP	1UP
	16	LAG6	Trunk	1UP	1UP
	17	LAG7	Trunk	1UP	1UP
	18	LAG8	Trunk	1UP	1UP

Edit

Figure 5-4 Membership Page

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

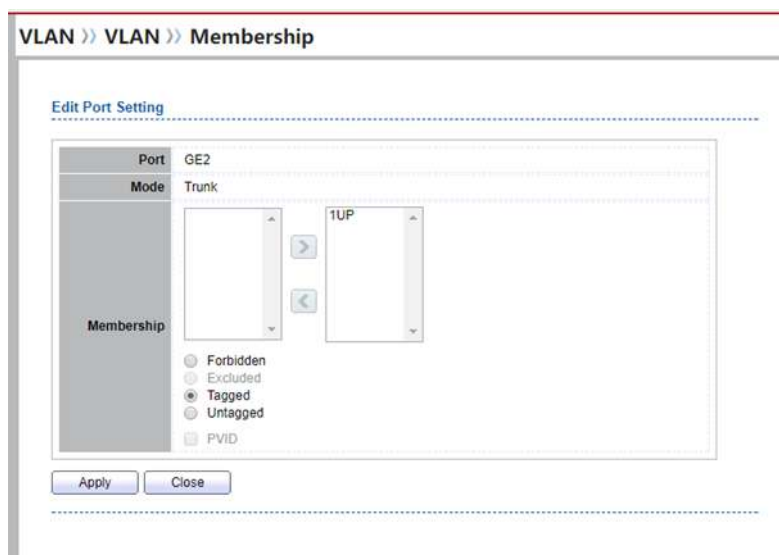


Figure 5-5 Edit Membership Dialog

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.

VLAN >> VLAN >> Port Setting

Port Setting Table

	Entry	Port	Mode	PVID	Accept Frame Type	Ingress Filtering	Uplink	TPID
☐	1	GE1	Trunk	1	All	Enabled	Disabled	0x8100
☐	2	GE2	Trunk	1	All	Enabled	Disabled	0x8100
☐	3	GE3	Trunk	1	All	Enabled	Disabled	0x8100
☐	4	GE4	Trunk	1	All	Enabled	Disabled	0x8100
☐	5	GE5	Trunk	1	All	Enabled	Disabled	0x8100
☐	6	GE6	Trunk	1	All	Enabled	Disabled	0x8100
☒	7	GE7	Trunk	1	All	Enabled	Disabled	0x8100
☐	8	GE8	Trunk	1	All	Enabled	Disabled	0x8100
☐	9	GE9	Trunk	1	All	Enabled	Disabled	0x8100
☐	10	GE10	Trunk	1	All	Enabled	Disabled	0x8100
☐	11	LAG1	Trunk	1	All	Enabled	Disabled	0x8100
☐	12	LAG2	Trunk	1	All	Enabled	Disabled	0x8100
☐	13	LAG3	Trunk	1	All	Enabled	Disabled	0x8100
☐	14	LAG4	Trunk	1	All	Enabled	Disabled	0x8100
☐	15	LAG5	Trunk	1	All	Enabled	Disabled	0x8100
☐	16	LAG6	Trunk	1	All	Enabled	Disabled	0x8100
☐	17	LAG7	Trunk	1	All	Enabled	Disabled	0x8100
☐	18	LAG8	Trunk	1	All	Enabled	Disabled	0x8100

Edit

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

VLAN >> VLAN >> Port Setting

Edit Port Setting

Port	GE7
Mode	☐ Hybrid ☐ Access ☒ Trunk ☐ Tunnel
PVID	1 (1 - 4094)
Accept Frame Type	☒ All ☐ Tag Only ☐ Untag Only
Ingress Filtering	☒ Enable
Uplink	☒ Enable
TPID	0x9100 ▼

Apply Close

Figure 5-7 Edit Port Setting Dialog

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

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.

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	Select a value of VPT. Qualified packets will use this VPT value as inner priority.
Remarking	Set checkbox to enable or disable 1p remarking. If enabled, qualified packets will be remark by this value.
Aging Time	Input value of aging time. Default is 1440 minutes. A voice VLAN entry will be age out after this time if without any packet pass through.

Table 5-8 Property Fields

Port Setting Table

	Entry	Port	State	Mode	QoS Policy
☐	1	GE1	Disabled	Auto	Voice Packet
☐	2	GE2	Disabled	Auto	Voice Packet
☐	3	GE3	Disabled	Auto	Voice Packet
☐	4	GE4	Disabled	Auto	Voice Packet
☐	5	GE5	Disabled	Auto	Voice Packet
☐	6	GE6	Disabled	Auto	Voice Packet
☐	7	GE7	Disabled	Auto	Voice Packet
☐	8	GE8	Disabled	Auto	Voice Packet
☐	9	GE9	Disabled	Auto	Voice Packet
☐	10	GE10	Disabled	Auto	Voice Packet
☐	11	LAG1	Disabled	Auto	Voice Packet
☐	12	LAG2	Disabled	Auto	Voice Packet
☐	13	LAG3	Disabled	Auto	Voice Packet
☐	14	LAG4	Disabled	Auto	Voice Packet
☐	15	LAG5	Disabled	Auto	Voice Packet

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

VLAN >> Voice VLAN >> Property

Edit Port Setting

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

Apply Close

Table 5-9 Property Port Fields

VLAN >> Voice VLAN >> Property

Edit Port Setting

Port	GE1
State	☐ Enable
Mode	☒ Auto ☐ Manual
QoS Policy	☒ 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
	• Auto: Voice VLAN auto detect packets that match OUI table and add received port into voice VLAN ID tagged member. • Manual: User need add interface to VLAN ID tagged member manually.
QoS Policy	Select port QoS Policy mode
	• Voice Packet: QoS attributes are applied to packets with OUIs in the source MAC address. • All: QoS attributes are applied to packets that are classified to the Voice VLAN.

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



The 'Edit Voice OUI' dialog box contains two input fields: 'OUI' with the value '00:E0:BB' and 'Description' with the value '3COM'. Below the fields are 'Apply' and 'Close' buttons.

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

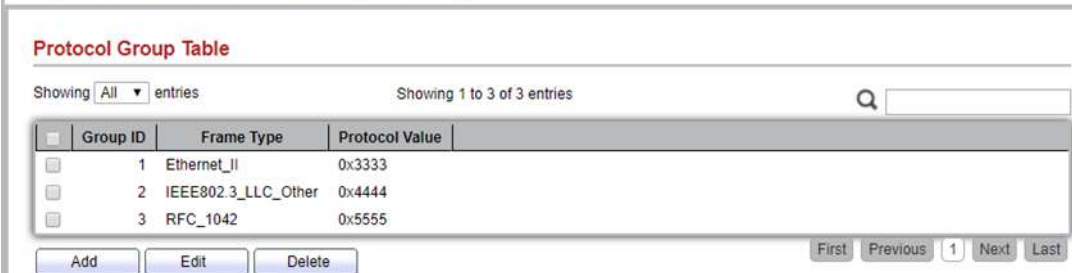
5.3 Protocol VLAN

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.



The 'Protocol Group Table' interface shows a table with 3 entries. The table has columns for Group ID, Frame Type, and Protocol Value. Below the table are 'Add', 'Edit', and 'Delete' buttons. Navigation buttons 'First', 'Previous', '1', 'Next', and 'Last' are also present.

Group ID	Frame Type	Protocol Value
1	Ethernet_II	0x3333
2	IEEE802.3_LL_C_Other	0x4444
3	RFC_1042	0x5555

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

VLAN >> Protocol VLAN >> Protocol Group

Add Protocol Group

Group ID

4 ▼

Frame Type

Ethernet_II ▼

Protocol Value

0x (0x600 ~ 0xFFFFE)

Apply

Close

Edit Protocol Group

Group ID

1

Frame Type

Ethernet_II ▼

Protocol Value

0x 3333 (0x600 ~ 0xFFFFE)

Apply

Close

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	Select frame type of list that maps packets to protocol-defined VLANs by examining the type octet within the packet header to discover the type of protocol associated with it. Ethernet_II: packet type is Ethernet version 2. IEEE802.3_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.

VLAN >> Protocol VLAN >> Group Binding

Group Binding Table

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

☐	Port	Group ID	VLAN
☐	GE1	1	22

Add

Edit

Delete

First

Previous

1

Next

Last

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

VLAN >> Protocol VLAN >> Group Binding

Add Group Binding

Port

Available Port

Selected Port

GE1

Note: Only VLAN Hybrid port can be set Protocol VLAN

Group ID

VLAN (1 - 4094)

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.

VLAN >> MAC VLAN >> MAC Group

MAC Group Table

Showing All entries Showing 1 to 3 of 3 entries

	Group ID	MAC Address	Mask
☐	1	02:03:04:05:06:07	48
☐	2	04:05:06:07:08:09	9
☐	3	AA:BB:CC:DD:EE:FF	32

Add Edit Delete

First Previous 1 Next Last

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

VLAN >> MAC VLAN >> MAC Group

Add MAC Group

Group ID (1 - 2147483647)

MAC Address

Mask (9 - 48)

Apply Close

Edit MAC Group

Group ID 1

MAC Address 02:03:04:05:06:07

Mask 48 (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

Edit Group Binding

Port	GE1
Group ID	1
VLAN	3333 (1 - 4094)

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.

Table 5-20 Group Binding Fields

5.5 Surveillance VLAN

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

5.5.1 Property

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

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

VLAN >> Surveillance VLAN >> Property

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

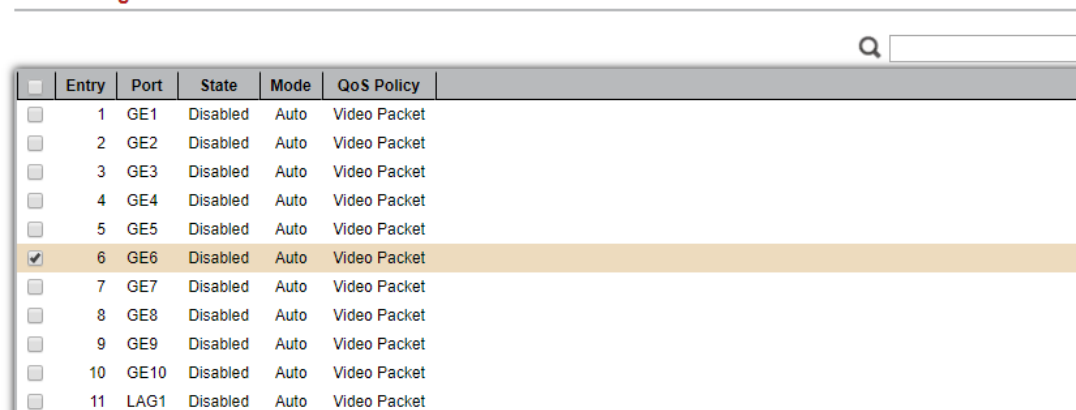
Figure 5-21 Property Page

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

Port Setting Table



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

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	☒ Enable
Mode	☐ Auto ☐ Manual
QoS Policy	☒ Video Packet ☐ 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 • 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.

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.

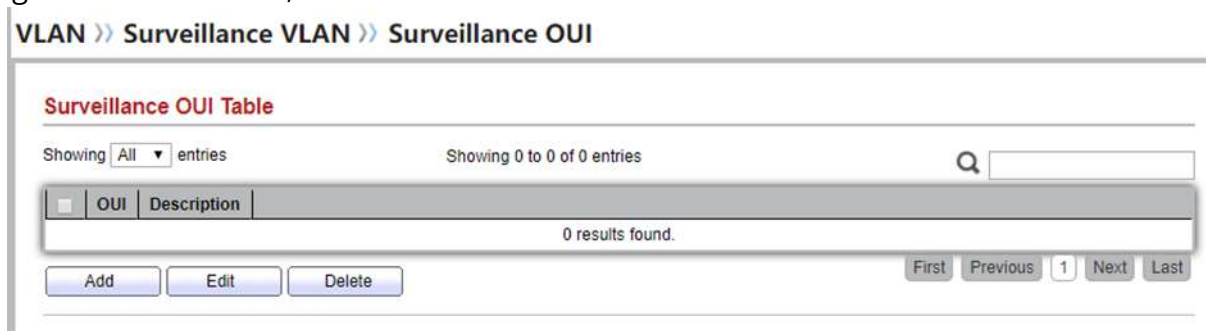


Figure 5-24 Surveillance OUI Page

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

Table 5-24 Surveillance OUI Fields

VLAN >> Surveillance VLAN >> Surveillance OUI

Add Surveillance OUI

OUI	: :
Description	

Apply Close

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

VLAN >> GVRP >> Property

State	☐ Enable
Operational Timeout	
Join	20 ms
Leave	60 ms
LeaveAll	1000 ms

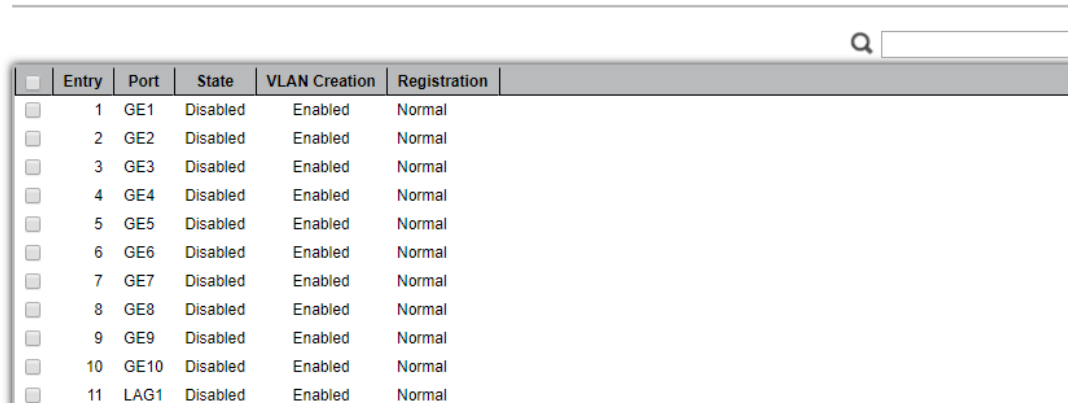
Apply

Figure 5-26 GVRP Setting Page

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

Table 5-26 GVRP Setting Fields

Port Setting Table

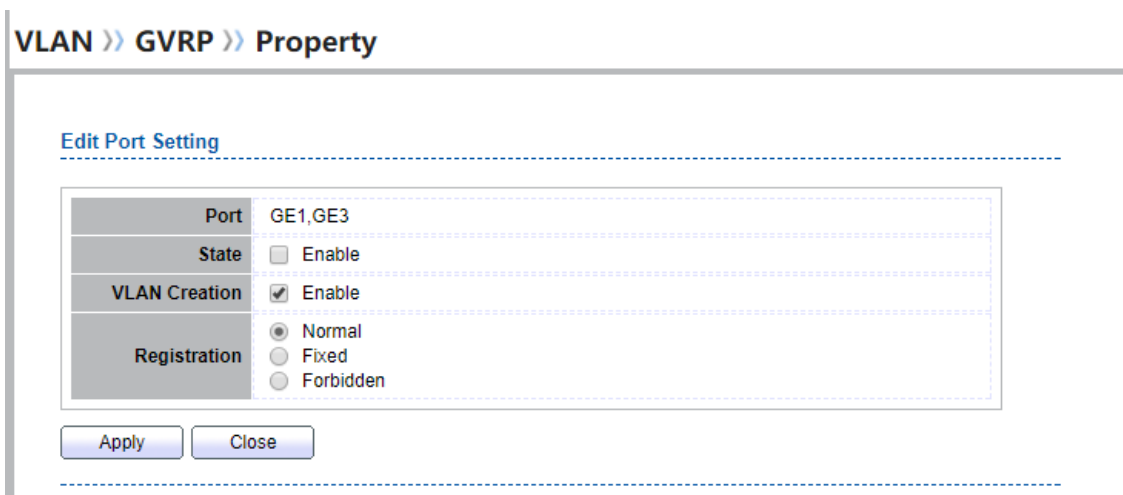


☐	Entry	Port	State	VLAN Creation	Registration
☐	1	GE1	Disabled	Enabled	Normal
☐	2	GE2	Disabled	Enabled	Normal
☐	3	GE3	Disabled	Enabled	Normal
☐	4	GE4	Disabled	Enabled	Normal
☐	5	GE5	Disabled	Enabled	Normal
☐	6	GE6	Disabled	Enabled	Normal
☐	7	GE7	Disabled	Enabled	Normal
☐	8	GE8	Disabled	Enabled	Normal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

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



VLAN >> GVRP >> Property

Edit Port Setting

Port	GE1,GE3
State	☐ Enable
VLAN Creation	☒ Enable
Registration	☒ Normal ☐ Fixed ☐ Forbidden

Apply Close

Figure 5-28 GVRP port Setting Edit Page

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

Vlan Creation	Set the enabling status of GVRP port create VLAN Enable: Enable/Disable port create dynamic VLAN.
Register Mode	Set the register mode of GVRP port • Normal: Normal mode. • Fixed: The port will not learn any dynamic VLAN. Only send static VLAN information to neighbor and allow static VLAN packet pass. • Forbidden: The port will not learn any dynamic VLAN and only allow default VLAN packet pass

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.

VLAN >> GVRP >> Membership

Membership Table

Showing

All

 entries

Showing 1 to 1 of 1 entries

VLAN	Member	Dynamic Member	Type
1	GE1-GE10,LAG1-LAG8		Static

First

Previous

1

Next

Last

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.

Figure 5-30 GVRP Port Statistics Display Setting

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

Table 5-30 GVRP Port Statistics Display Setting Fields

Receive	
Join empty	0
Empty	0
Leave Empty	0
Join In	0
Leave In	0
Leave All	0
Transmit	
Join empty	0
Empty	0
Leave Empty	0
Join In	0
Leave In	0
Leave All	0
Error	
Invalid Protocol ID	0
Invalid Attribute Type	0
Invalid Attribute Value	0
Invalid Attribute Length	0
Invalid Event	0

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 Attribut 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**.

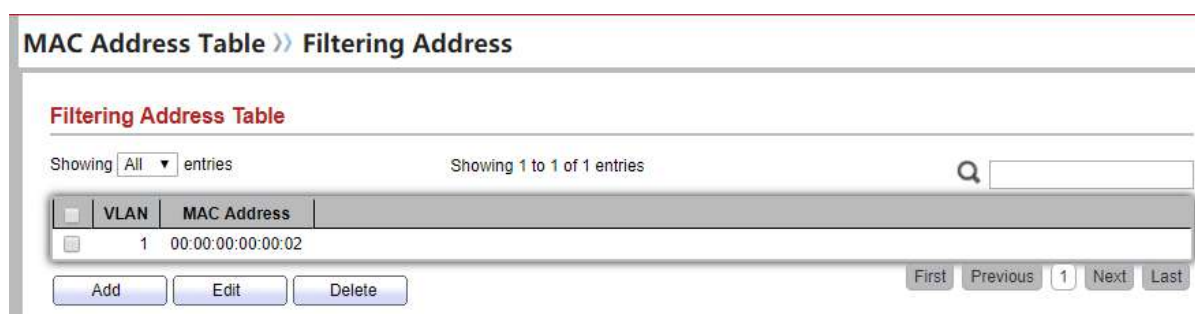


Figure 6-3: Filtering Address page.

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

Table 6-3: Filtering Address Setting fields.

7. STP

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

7.1 Property

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

Spanning Tree >> Property

State	☒ Enable
Operation Mode	☐ STP ☒ RSTP ☐ MSTP
Path Cost	☒ Long ☐ Short
BPDU Handling	☐ Filtering ☒ Flooding
Priority	32768 (0 - 61440, default 32768)
Hello Time	2 Sec (1 - 10, default 2)
Max Age	20 Sec (6 - 40, default 20)
Forward Delay	15 Sec (4 - 30, default 15)
Tx Hold Count	6 (1 - 10, default 6)
Region Name	00:E0:4C:00:00:00
Revision	0 (0 - 65535, default 0)
Max Hop	20 (1 - 40, default 20)
Operational Status	
Bridge Identifier	32768-00:E0:4C:00:00:00
Designated Root Bridge	0-00:00:00:00:00:00
Root Port	N/A
Root Path Cost	0
Topology Change Count	0
Last Topology Change	0D/0H/0M/0S

Figure 7-1: STP Property

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

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

Table 7-1: STP Property field.

Field	Description
Bridge Identifier	Bridge identifier of the switch.
Designated Identifier Root	Bridge identifier of the designated root bridge.
Root Port	Operational root port of the switch.
Root Path Cost	Operational root path cost.
Topology Change Count	Numbers of the topology changes.
Last Topology	The last time for the topology change

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**.

Spanning Tree >> Port Setting

Port Setting Table

☐	Entry	Port	State	Path Cost	Priority	BPDU Filter	BPDU Guard	Operational Edge	Operational Point-to-Point	Port Role
☐	1	GE1	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled
☐	2	GE2	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled
☐	3	GE3	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled
☐	4	GE4	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled
☐	5	GE5	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled
☐	6	GE6	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled
☐	7	GE7	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled
☐	8	GE8	Disabled	20000	128	Disabled	Disabled	Disabled	Enabled	Disabled
☐	9	GE9	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled
☐	10	GE10	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled
☐	11	LAG1	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled
☐	12	LAG2	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled
☐	13	LAG3	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled
☐	14	LAG4	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled
☐	15	LAG5	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled
☐	16	LAG6	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled
☐	17	LAG7	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled
☐	18	LAG8	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled

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 "Backup".
Port State	The current port state on the specified port. The possible values are: "Disabled", "Discarding", "Learning", and "Forwarding".
Designated Bridge	The bridge ID of the designated bridge.
Designated Port ID	The designated port ID on the switch.
Designated Cost	The path cost of the designated port on the switch

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

☒ Enable

Path Cost

(0 - 200000000) (0 = Auto)

Priority

128 ▾

Edge Port

☐ Enable

BPDU Filter

☐ Enable

BPDU Guard

☐ Enable

Point-to-Point

☒ Auto
☐ Enable
☐ Disable

Port State

Disabled

Designated Bridge

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

Designated Port ID

128-1

Designated Cost

20000

Operational Edge

False

Operational Point-to-Point

False

Apply

Close

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. • Enable: Force to true state (as link to a host). • Disable: Force to false state (as link to a bridge). In the edge mode, the interface would be put into the Forwarding state immediately upon link up. If the edge mode is enabled for the interface and there are BPDUs received on the interface, the loop might be occurred in the short time before the STP state change.
BPDU Filter	The BPDU Filter configuration avoids receiving/transmitting BPDU from the specified ports. • Enable: Enable BPDU filter function. • Disable: Disable BPDU filter function.
BPDU Guard	The BPDU Guard configuration to drop the received BPDU directly. • Enable: Enable BPDU guard function. • Disable: Disable BPDU guard function.
Point-to-Point	Specify the Point-to-Point port configuration: • Auto: The state is depended on the duplex setting of the port • Enable: Force to true state. • Disable: Force to false state.

Table 7-5: Edit STP Port Setting fields.

7.3 MST Instance

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

Spanning Tree >> MST Instance

MST Instance Table									
	MSTI	Priority	Bridge Identifier	Designated Root Bridge	Root Port	Root Path Cost	Remaining Hop	VLAN	
☐	0	32768	32768-00:E0:4C:00:00:00	0-00:00:00:00:00:00	N/A	0	0	1-4094	
☐	1	32768	32768-00:E0:4C:00:00:00	0-00:00:00:00:00:00	N/A	0	0		
☐	2	32768	32768-00:E0:4C:00:00:00	0-00:00:00:00:00:00	N/A	0	0		
☐	3	32768	32768-00:E0:4C:00:00:00	0-00:00:00:00:00:00	N/A	0	0		
☐	4	32768	32768-00:E0:4C:00:00:00	0-00:00:00:00:00:00	N/A	0	0		
☐	5	32768	32768-00:E0:4C:00:00:00	0-00:00:00:00:00:00	N/A	0	0		
☐	6	32768	32768-00:E0:4C:00:00:00	0-00:00:00:00:00:00	N/A	0	0		
☐	7	32768	32768-00:E0:4C:00:00:00	0-00:00:00:00:00:00	N/A	0	0		
☐	8	32768	32768-00:E0:4C:00:00:00	0-00:00:00:00:00:00	N/A	0	0		
☐	9	32768	32768-00:E0:4C:00:00:00	0-00:00:00:00:00:00	N/A	0	0		
☐	10	32768	32768-00:E0:4C:00:00:00	0-00:00:00:00:00:00	N/A	0	0		
☐	11	32768	32768-00:E0:4C:00:00:00	0-00:00:00:00:00:00	N/A	0	0		
☐	12	32768	32768-00:E0:4C:00:00:00	0-00:00:00:00:00:00	N/A	0	0		
☐	13	32768	32768-00:E0:4C:00:00:00	0-00:00:00:00:00:00	N/A	0	0		
☐	14	32768	32768-00:E0:4C:00:00:00	0-00:00:00:00:00:00	N/A	0	0		
☐	15	32768	32768-00:E0:4C:00:00:00	0-00:00:00:00:00:00	N/A	0	0		

Edit

Figure 7-4: MST Instance page

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

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

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**.

Spanning Tree >> MST Port Setting

MST Port Setting Table

MSTI 0 ▼

	Entry	Port	Path Cost	Priority	Port Role	Port State	Mode	Type	Designated Bridge	Designated Port ID	Designate
☐	1	GE1	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-1	
☐	2	GE2	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-2	
☐	3	GE3	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-3	
☐	4	GE4	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-4	
☐	5	GE5	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-5	
☐	6	GE6	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-6	
☐	7	GE7	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-7	
☐	8	GE8	20000	128	Disabled	Forwarding	RSTP	Boundary	0-00:00:00:00:00:00	128-8	
☐	9	GE9	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-9	
☐	10	GE10	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-10	
☐	11	LAG1	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-11	
☐	12	LAG2	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-12	
☐	13	LAG3	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-13	
☐	14	LAG4	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-14	
☐	15	LAG5	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-15	
☐	16	LAG6	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-16	
☐	17	LAG7	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-17	
☐	18	LAG8	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-18	

Figure 7-6: MST Port Setting page.

Field	Description
MSTI	Specify the port setting on the specified MSTI
Port	Specify the interface ID or the list of interface IDs.
Path Cost	The port path cost on the specified MSTI.
Priority	The port priority on the specified MSTI.
Port Role	The current port role on the specified port. The possible values are:

	“Disabled”, “Master”, “Root”, “Designated”, “Alternative”, and “Backup”.
Port State	The current port state on the specified port. The possible values are: “Disabled”, “Discarding”, “Learning”, and “Forwarding”.
Mode	The operational STP mode on the specified port.
Type	The possible value for the port type are: • Boundary: The port attaching an MST Bridge to a LAN that is not in the same region. • Internal: The port attaching an MST Bridge to a LAN that is not in the same region.
Designated Bridge	The bridge ID of the designated bridge.
Designated Port ID	The designated port ID on the switch.
Designated Cost	The path cost of the designated port on the switch
Remaining Hop	The remaining hops count on the specified port.

Table 7-8: MST Port Setting fields.

Spanning Tree >> MST Port Setting

Edit MST Port Setting

MSTI	0
Port	GE1-GE4
Path Cost	0 (0 - 200000000) (0 = Auto)
Priority	128 ▼
Port Role	Disabled
Port State	Disabled
Mode	RSTP
Type	Boundary
Designated Bridge	0-00:00:00:00:00:00
Designated Port ID	128-1
Designated Cost	20000
Remaining Hop	20

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.

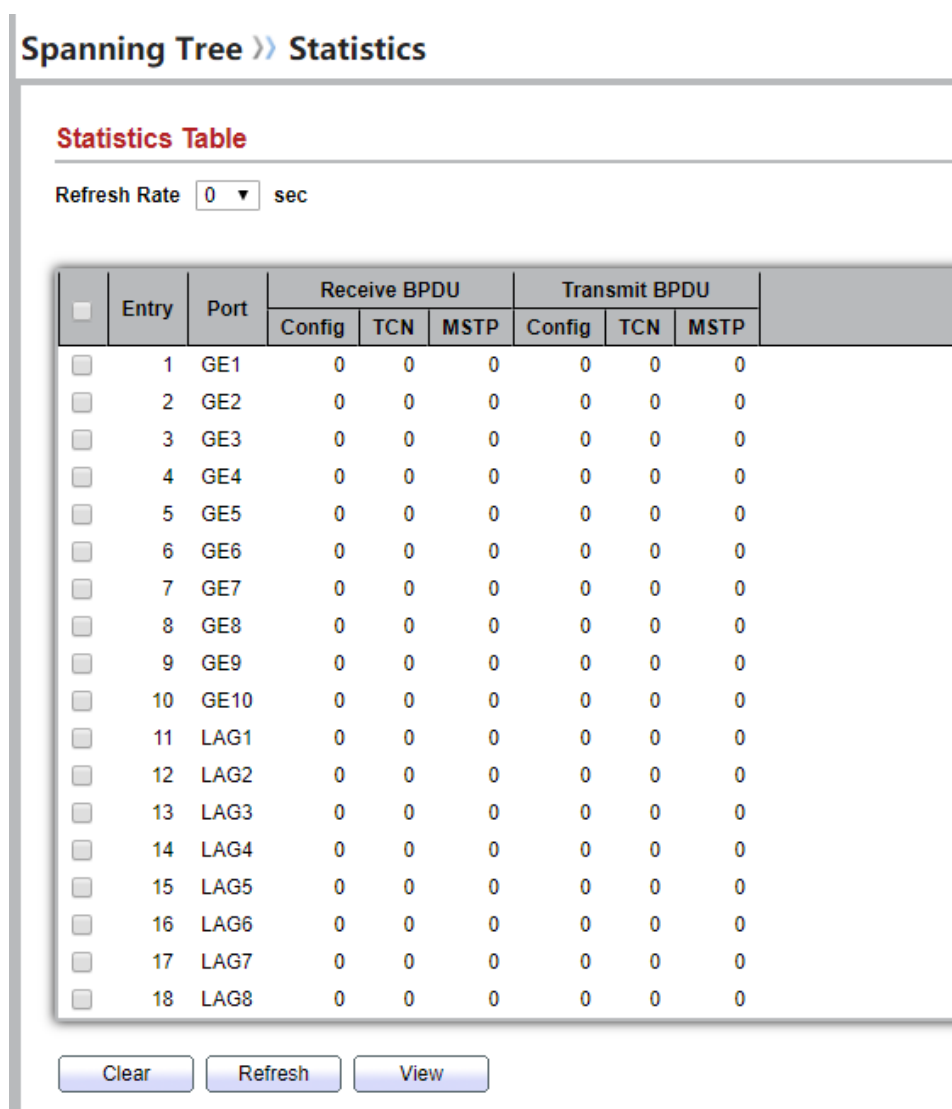


Figure 7-8: STP Statistics page

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 (MSTP)	The counts of the received MSTP BPDU.
Transmit BPDUs (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.

Spanning Tree >> Statistics

STP Port Statistic

Port

GE1

Refresh Rate

☒ None
☐ 5 sec
☐ 10 sec
☐ 30 sec

Receive BPDU

Config

0

TCN

0

MSTP

0

Transmit BPDU

Config

0

TCN

0

MSTP

0

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.Discovery

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**.

Discovery >> LLDP >> Property

LLDP

State ☒ Enable

LLDP Handling ☐ Filtering ☐ Bridging ☒ Flooding

TLV Advertise Interval Sec (5 - 32767, default 30)

Hold Multiplier (2 - 10, default 4)

Reinitializing Delay Sec (1 - 10, default 2)

Transmit Delay Sec (1 - 8191, default 2)

LLDP-MED

Fast Start Repeat Count (1 - 10, default 3)

Apply

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**.

Discovery >> LLDP >> Port Setting

Port Setting Table

Q

☐	Entry	Port	Mode	Selected TLV
☐	1	GE1	Normal	802.1 PVID
☐	2	GE2	Normal	802.1 PVID
☐	3	GE3	Normal	802.1 PVID
☐	4	GE4	Normal	802.1 PVID
☐	5	GE5	Normal	802.1 PVID
☐	6	GE6	Normal	802.1 PVID
☐	7	GE7	Normal	802.1 PVID
☐	8	GE8	Normal	802.1 PVID
☐	9	GE9	Normal	802.1 PVID
☐	10	GE10	Normal	802.1 PVID

Figure 8-2 LLDP Port Setting Page

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

Discovery >> LLDP >> Port Setting

Edit Port Setting

Port
GE1

Mode
☐ Transmit
☐ Receive
☒ Normal
☐ Disable

Optional TLV

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

Selected TLV
 802.1 PVID

802.1 VLAN Name

Available VLAN
 VLAN 1
 VLAN 2
 VLAN 3

Selected VLAN

Figure 8-3 LLDP Port Edit Page

Field	Description
Port	Select specified port or all ports to configure LLDP state.
Mode	Select the transmission state of LLDP port interface. • Disable: Disable the transmission of LLDP PDUs. • RX Only: Receive LLDP PDUs only. • TX Only: Transmit LLDP PDUs only. • TX And RX: Transmit and receive LLDP PDUs both.
Optional TLV	Select the LLDP optional TLVs to be carried (multiple selection is allowed). • System Name • Port Description • System Description • System Capability • 802.3 MAC-PHY • 802.3 Link Aggregation • 802.3 Maximum Frame Size • Management Address • 802.1 PVID
802.1 Name	VLAN Select the VLAN Name ID to be carried (multiple selection is allowed).

8.1.3 MED Network Policy

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

Discovery >> LLDP >> MED Network Policy

MED Network Policy Table

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

	Policy ID	Application	VLAN	VLAN Tag	Priority	DSCP
☐	1	Voice Signaling	2	Tagged	0	0

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**

Add MED Network Policy

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

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. • Voice • Voice Signaling • Guest Voice • Guest Voice Signaling • Softphone Voice • Video Conferencing • App Streaming Video • Video Signaling
VLAN	Set the VLAN ID, range from 1 to 4094.
VLAN Tag	Set the VLAN tag status. • Tagged: Traffic is tagged. • Untagged: Traffic is untagged.
Priority	Set the L2 priority, range from 0 to 7.
DSCP	Set the DSCP value, range from 0 to 63

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**.

Discovery >> LLDP >> MED Port Setting

MED Port Setting Table

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

Edit

Figure 8-6 LLDP MED Setting Page

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

Discovery >> LLDP >> MED Port Setting

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) • 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 8-3 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**.

Discovery >> LLDP >> Packet View

Packet View Table

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

Detail

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 (Bytes)	Total number of available bytes left for additional LLDP 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**

Discovery >> LLDP >> Packet View

Packet View Detail

Port	GE1
Mandatory TLVs	
Size (Bytes)	21
Operational Status	Transmitted
MED Capabilities	
Size (Bytes)	9
Operational Status	Transmitted
MED Location	
Size (Bytes)	0
Operational Status	Transmitted
MED Network Policy	
Size (Bytes)	0
Operational Status	Transmitted
MED Inventory	
Size (Bytes)	0
Operational Status	Transmitted
MED Extended Power via MDI	
Size (Bytes)	0
Operational Status	Transmitted
802.3 TLVs	
Size (Bytes)	0
Operational Status	Transmitted
Optional TLVs	
Size (Bytes)	0
Operational Status	Transmitted
802.1 TLVs	
Size (Bytes)	8
Operational Status	Transmitted
Total	
In-Use (Bytes)	38
Available (Bytes)	1450

Close

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 Detail 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.

Discovery >> LLDP >> Local Information

Device Summary

Chassis ID Subtype	MAC address
Chassis ID	00:E0:4C:00:00:00
System Name	Switch
System Description	IG80
Supported Capabilities	Bridge
Enabled Capabilities	Bridge
Port ID Subtype	Local

Port Status Table

	Entry	Port	LLDP State	LLDP-MED State
☐	1	GE1	Normal	Enabled
☐	2	GE2	Normal	Enabled
☐	3	GE3	Normal	Enabled
☐	4	GE4	Normal	Enabled
☐	5	GE5	Normal	Enabled
☐	6	GE6	Normal	Enabled
☐	7	GE7	Normal	Enabled
☐	8	GE8	Normal	Enabled
☐	9	GE9	Normal	Enabled
☐	10	GE10	Normal	Enabled

Detail

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.

Discovery >> LLDP >> Local Information

Local Information Detail

Chassis ID Subtype	MAC address
Chassis ID	00:E0:4C:00:00:00
System Name	Switch
System Description	IG80
Supported Capabilities	Bridge
Enabled Capabilities	Bridge
Port ID	GE1
Port ID Subtype	Local
Port Description	WWW

Management Address Table

Address Subtype	Address	Interface Subtype	Interface Number
0 results found.			

MAC/PHY Detail

Auto-Negotiation Supported	N/A
Auto-Negotiation Enabled	N/A
Auto-Negotiation Advertised Capabilities	N/A
Operational MAU Type	N/A

802.3 Detail

802.3 Maximum Frame Size	N/A
--------------------------	-----

802.3 Link Aggregation

Aggregation Capability	N/A
Aggregation Status	N/A
Aggregation Port ID	N/A

MED Detail

Capabilities Supported	Capabilities , Network policy
Current Capabilities	Capabilities , Network policy

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.

Discovery >> LLDP >> Neighbor

Neighbor Table

Showing All ▾ entries Showing 0 to 0 of 0 entries 🔍

☐	Local Port	Chassis ID Subtype	Chassis ID	Port ID Subtype	Port ID	System Name	Time to Live
0 results found.							

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.

Discovery >> LLDP >> Statistics

Global Statistics

Insertions	0
Deletions	0
Drops	0
AgeOuts	0

Statistics Table

	Entry	Port	Transmit Frame	Receive Frame			Receive TLV		Neighbor Timeout
			Total	Total	Discard	Error	Discard	Unrecognized	
☐	1	GE1	0	0	0	0	0	0	0
☐	2	GE2	0	0	0	0	0	0	0
☐	3	GE3	0	0	0	0	0	0	0
☐	4	GE4	0	0	0	0	0	0	0
☐	5	GE5	0	0	0	0	0	0	0
☐	6	GE6	0	0	0	0	0	0	0
☐	7	GE7	0	0	0	0	0	0	0
☐	8	GE8	344	0	0	0	0	0	0
☐	9	GE9	0	0	0	0	0	0	0
☐	10	GE10	0	0	0	0	0	0	0

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 expired.
Port	Interface or port number.
Transmit Frame Total	Number of LLDP frames transmitted on the corresponding port.
Receive Frame Total	Number of LLDP frames received by this LLDP agent on the corresponding port, while the LLDP agent is enabled.
Receive Frame Discard	Number of LLDP frames discarded for any reason by the LLDP agent on the corresponding port.
Receive Frame Error	Number of invalid LLDP frames received by the LLDP agent on the corresponding port, while the LLDP agent is enabled.
Receive TLV Discard	Number of TLVs of LLDP frames discarded for any reason by the LLDP agent on the corresponding port.
Receive TLV Unrecognized	Number of TLVs of LLDP frames that are unrecognized while the LLDP agent is enabled
Neighbor Timeout	Number of age out LLDP frames.

Table 8-9 LLDP Statistics Fields

9. Multicast

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.

Multicast >> General >> Property

Unknown Multicast Action

- ☒ Flood
- ☐ Drop
- ☐ Forward to Router Port

Multicast Forward Method

IPv4

- ☒ DMAC-VID
- ☐ DIP-VID

IPv6

- ☒ DMAC-VID
- ☐ DIP-VID

Apply

Figure 9-1 Multicast General Properties Page

Field	Description
Unknown Multicast Action	Set the unknown multicast action • Drop: drop the unknown multicast data. • Flood: flood the unknown multicast data. • Router port: forward the unknown multicast data to router port.
IPv4	Set the ipv4 multicast forward method. • MAC-VID: forward method dmac+vid. • DIP-VID: forward method dip+vid.
Pv6	Set the ipv6 multicast forward method. • 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.

Multicast >> General >> Group Address

Figure 9-2 Multicast Group Address Table Page

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

Table 9-2 Multicast Group Address Table Fields

Figure 9-3 Multicast Group Address Add Page

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

Table 9-3 Multicast Group Address Add Fields

Multicast >> General >> Group Address

[Edit Group Address](#)

VLAN

1

Group Address

224.1.1.1

Member

Available Port

GE2
GE3
GE4
GE5
GE6
GE7
GE8
GE9

>
<

Selected Port

GE1

Apply

Close

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. • 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.

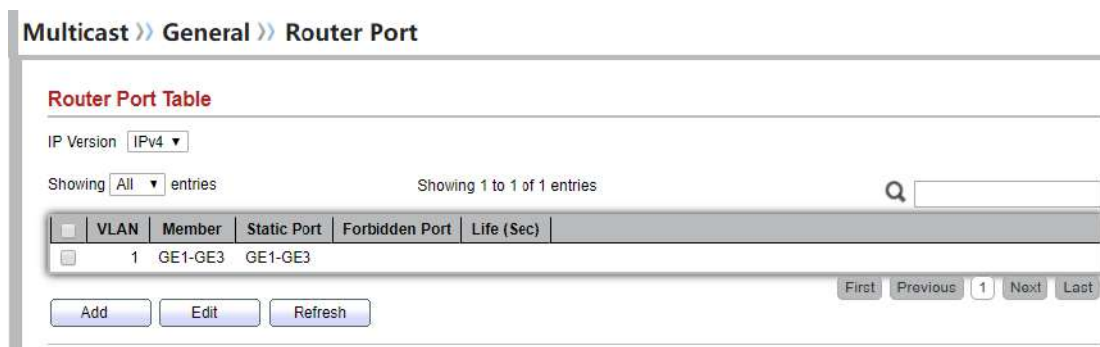


Figure 9-5 Multicast Router Table Page

Field	Description
IP Version	IP Version
	• 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

Multicast >> General >> Router Port

Add Router Port

VLAN	Available VLAN	Selected VLAN
	2 3	
IP Version	IPv4 ▼	
Type	☒ Static ☐ Forbidden	
Port	Available Port	Selected Port
	GE1 GE2 GE3 GE4 GE5 GE6 GE7 GE8	

Apply Close

Figure 9-6 Multicast Router Add Page

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

Table 9-6 Multicast Router Add Fields

Multicast » General » Router Port

[Edit Router Port](#)

VLAN

1

IP Version

IPv4

Type

☒ Static
☐ Forbidden

Port

Available Port

GE4
GE5
GE6
GE7
GE8
GE9
GE10
LAG1

Selected Port

GE1
GE2
GE3

Apply

Close

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 • Static: static router port • Forbidden: forbidden router port, can't learn dynamic router port member
Port	The member ports of router entry for selected port type. • Available Port: Optional router port member • Selected Port: Selected router port member

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.

Multicast >> General >> Forward All

Forward All Table

IP Version

Showing entries Showing 1 to 2 of 2 entries

	VLAN	Static Port	Forbidden Port
☐	2	GE2-GE3	
☐	3	GE1-GE2	

Figure 9-8 Multicast Forward All Table Page

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

Table 9-8 Multicast Forward All Table Fields

Multicast >> General >> Forward All

Add Forward All

VLAN

Available VLAN

1

Selected VLAN

IP Version

IPv4

Type

☒ Static
☐ Forbidden

Port

Available Port

GE1
GE2
GE3
GE4
GE5
GE6
GE7
GE8

Selected Port

Figure 9-9 Multicast Forward All Add Page

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

Table 9-9 Multicast Forward All Add Fields

Multicast >> General >> Forward All

[Edit Forward All](#)

VLAN

3

IP Version

IPv4

Type

☒ Static
☐ Forbidden

Port

Available Port

GE3
GE4
GE5
GE6
GE7
GE8
GE9
GE10

>
<

Selected Port

GE1
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 • Static: static forward all port • Forbidden: forbidden forward all port
Port	The member ports of forward all entry for selected port type. • Available Port: Optional router port member • Selected Port: Selected router port member

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

Multicast >> General >> Throttling

Throttling Table

IP Version IPv4 ▼

☐	Entry	Port	Max Group	Exceed Action
☐	1	GE1	256	Deny
☐	2	GE2	256	Deny
☐	3	GE3	256	Deny
☐	4	GE4	256	Deny
☐	5	GE5	256	Deny
☐	6	GE6	256	Deny
☐	7	GE7	256	Deny
☐	8	GE8	256	Deny
☐	9	GE9	256	Deny
☐	10	GE10	256	Deny
☐	11	LAG1	256	Deny
☐	12	LAG2	256	Deny
☐	13	LAG3	256	Deny
☐	14	LAG4	256	Deny
☐	15	LAG5	256	Deny
☐	16	LAG6	256	Deny
☐	17	LAG7	256	Deny
☐	18	LAG8	256	Deny

Edit

Figure 9-11 Multicast Throttling Table Page

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

Table 9-11 Multicast Throttling Table Fields

Multicast >> General >> Throttling

Edit Throttling

Port	GE2,GE4	
IP Version	IPv4	
Max Group	256	(0 - 256)
Exceed Action	☒ Deny ☐ Replace	

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 • 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.

Multicast >> General >> Filtering Profile

Filtering Profile Table

IP Version: IPv4 ▼

Showing All ▼ entries Showing 1 to 1 of 1 entries

Q

	Profile ID	Start Address	End Address	Action
☐	1	224.1.1.1	224.1.2.3	Allow

Figure 9-13 Multicast Profile Table Page

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

Table 9-13 Multicast Profile Table Fields

Multicast >> General >> Filtering Profile

Add Profile

Profile ID	(1 - 128)
IP Version	IPv4 ▼
Start Address	
End Address	
Action	☒ Allow ☐ Deny

Apply Close

Figure 9-14 Multicast Profile Add Page

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

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	☒ Allow ☐ 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: • Allow: permit the group can learned that match the profile. • Deny: deny the group to learn the group that 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

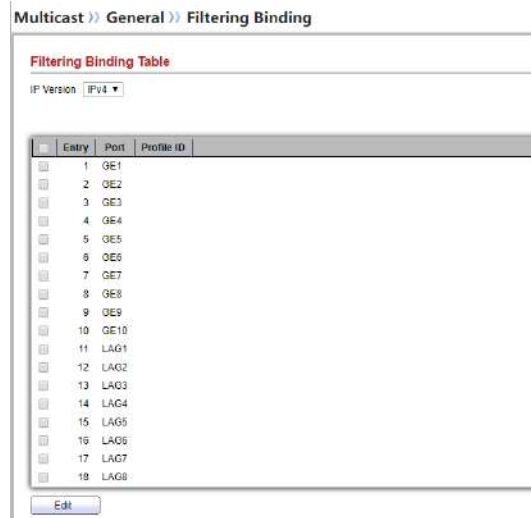


Figure 9-16 Multicast Filtering Table Page

Field	Description
IP Version	IP Version • 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

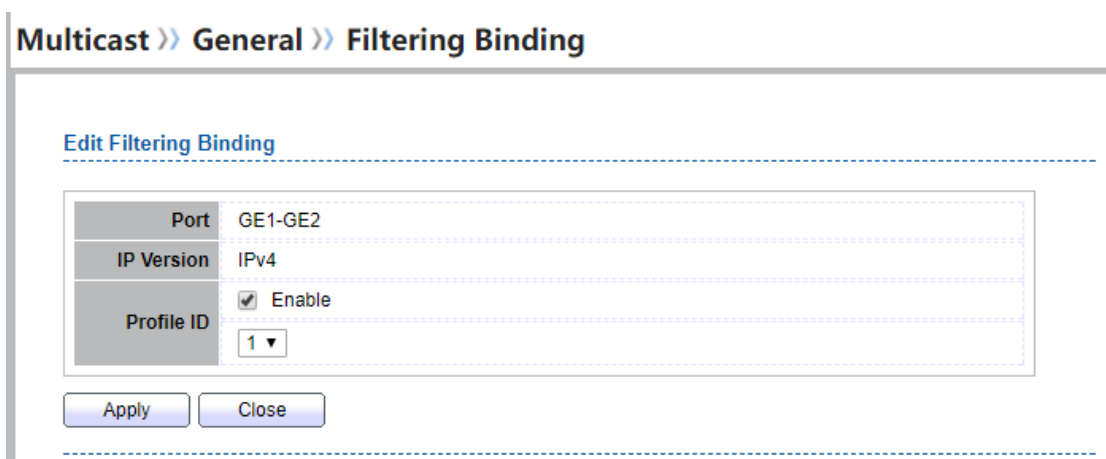


Figure 9-17 Multicast Filtering Edit Page

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.

Multicast >> IGMP Snooping >> Property

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

Apply

VLAN Setting Table

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

Edit

Figure 9-18 IGMP Snooping Property Page

Field	Description
State	Set the enabling status of IGMP Snooping functionality Enable: If Checked Enable IGMP Snooping, else is Disabled IGMP Snooping.
Version	Set the igmp snooping version IGMPv2: Only support process igmp v2 packet. IGMPv3: Support v3 basic and v2.
Report Suppression	Set the enabling status of IGMP v2 report suppression Enable: If Checked Enable IGMP Snooping v2 report suppression, else Disable the report suppression function
VLAN	The IGMP entry VLAN ID

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

Table 9-18 IGMP Snooping Property Fields

Multicast >> IGMP Snooping >> Property

[Edit VLAN Setting](#)

VLAN	3,5
State	☐ Enable
Router Port Auto Learn	☒ Enable
Immediate leave	☐ Enable
Query Robustness	2 (1 - 7, default 2)
Query Interval	125 Sec (30 - 18000, default 125)
Query Max Response Interval	10 Sec (5 - 20, default 10)
Last Member Query Counter	2 (1 - 7, default 2)
Last Member Query Interval	1 Sec (1 - 25, default 1)
Operational Status	
Status	Disabled
Query Robustness	2
Query Interval	125 (Sec)
Query Max Response Interval	10 (Sec)
Last Member Query Counter	2
Last Member Query Interval	1 (Sec)

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

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.

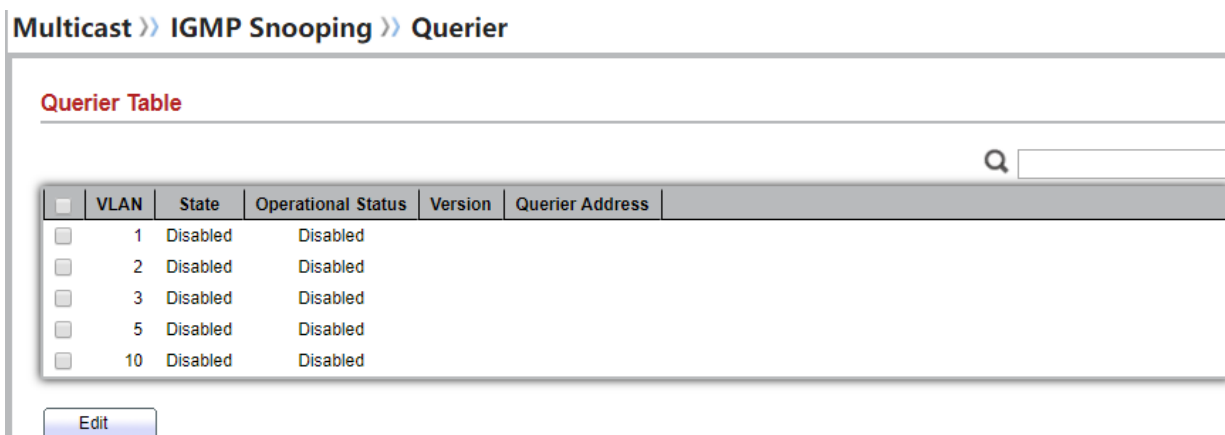


Figure 9-20 IGMP Snooping Querier Table Page

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

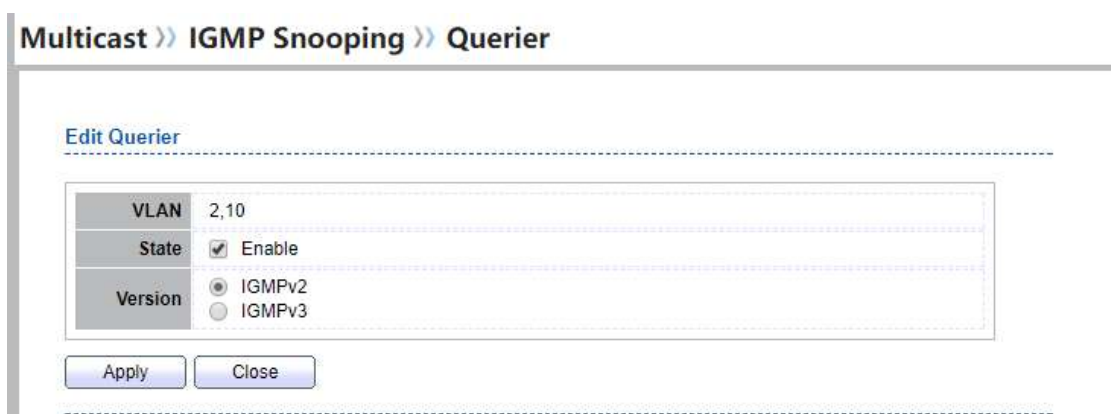


Figure 9-21 IGMP Snooping Querier Edit Page

Field	Description
VLAN	The Selected Edit IGMP Snooping querier VLAN List

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

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.

Multicast >> IGMP Snooping >> Statistics

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

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

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.

Multicast >> MLD Snooping >> Property

The screenshot shows the 'Multicast >> MLD Snooping >> Property' configuration page. It contains a form for global settings and a table for VLAN settings.

Global Settings:

- State:** ☐ Enable
- Version:** ☒ MLDv1, ☐ MLDv2
- Report Suppression:** ☒ Enable

Buttons: Apply, Edit

VLAN Setting Table:

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

Figure 9-23 MLD Snooping Property Page

Field	Description
State	Set the enabling status of IGMP Snooping functionality Enable: If Checked Enable IGMP Snooping, else is Disabled IGMP Snooping.
Version	Set the MLD snooping version MLDv1: Only support process MLD v1 packet. MLDv2: Support v2 basic and v1.
Report Suppression	Set the enabling status of MLD v1 report suppression Enable: If Checked Enable MLD Snooping v1 report suppression, else Disable the report suppression function
VLAN	The MLD entry VLAN ID
Operation Status	The enable status of MLD snooping VLAN functionality
Router Port Auto Learn	The enabling status of MLD snooping router port auto learning

Query Robustness	The Query Robustness allows tuning for the expected packet loss on a subnet.
Query Interval	The interval of querier to send general query
Query Max Response Interval	In Membership Query Messages, it specifies the maximum allowed time before sending a responding report in units of 1/10 second.
Last Member Query count	The count that Querier-switch sends Group-Specific Queries when it receives a Leave Group message for a group.
Last Member Query Interval	The interval that Querier-switch sends Group-Specific Queries when it receives a Leave Group message for a group.
Immediate leave	The immediate leave status of the group will immediate leave when receive MLD Leave message.

Table 9-23 MLD Snooping Property Fields

Multicast >> MLD Snooping >> Property

[Edit VLAN Setting](#)

VLAN	5,10
State	☐ Enable
Router Port Auto Learn	☒ Enable
Immediate leave	☐ Enable

Query Robustness	2 (1 - 7, default 2)
Query Interval	125 Sec (30 - 18000, default 125)
Query Max Response Interval	10 Sec (5 - 20, default 10)

Last Member Query Counter	2 (1 - 7, default 2)
Last Member Query Interval	1 Sec (1 - 25, default 1)

Operational Status	
Status	Disabled
Query Robustness	2
Query Interval	125 (Sec)
Query Max Response Interval	10 (Sec)
Last Member Query Counter	2
Last Member Query Interval	1 (Sec)

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 • Enable: If Checked Enable MLD Snooping VLAN, else is Disabled MLD Snooping VLAN.
Router Learn Port Auto	Set the enabling status of MLD Snooping router port learning • Enable: If checked Enable learning router port by query and PIM, DVRMP, else Disable the learning router port
Immediate leave	Immediate Leave the group when receive MLD Leave message. • Enable: If checked Enable immediate leave, else disable immediate leave
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.

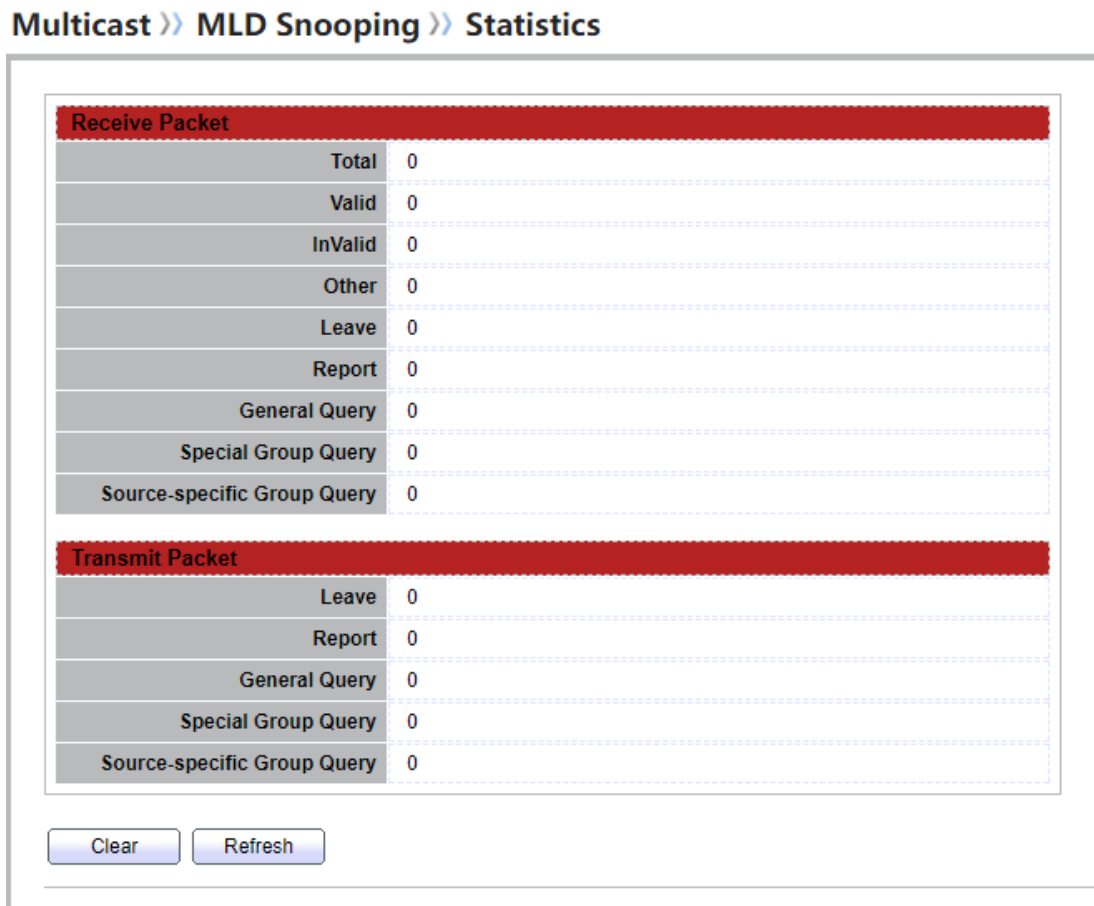


Figure 9-25 MLD Snooping Statistics Page

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 Query	Group	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 Query	Group	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.

Multicast >> MVR >> Property

State	☒ Enable
VLAN	2 ▼
Mode	☒ Compatible ☐ Dynamic
Group Start	224.1.1.1
Group Count	8 (1 - 128)
Query Time	1 Sec (1 - 10)
Operational Group	
Maximum	128
Current	0

Apply

Figure 9-26 Multicast MVR Properties Page

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

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

Multicast >> MVR >> Port Setting

Port Setting Table

☐	Entry	Port	Role	Immediate Leave
☐	1	GE1	None	Disabled
☐	2	GE2	None	Disabled
☐	3	GE3	None	Disabled
☐	4	GE4	None	Disabled
☐	5	GE5	None	Disabled
☐	6	GE6	None	Disabled
☐	7	GE7	None	Disabled
☐	8	GE8	None	Disabled
☐	9	GE9	None	Disabled
☐	10	GE10	None	Disabled
☐	11	LAG1	None	Disabled
☐	12	LAG2	None	Disabled
☐	13	LAG3	None	Disabled
☐	14	LAG4	None	Disabled
☐	15	LAG5	None	Disabled
☐	16	LAG6	None	Disabled
☐	17	LAG7	None	Disabled
☐	18	LAG8	None	Disabled

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 • None: port role is none • Receiver: port role is receiver • Source: port role is source
Immediate Leave	MVR Port immediate leave • Enable: if checked is enable immediate leave, else disable immediate leave.

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.

Multicast >> MVR >> Group Address

Group Address Table

Showing All entries Showing 0 to 0 of 0 entries

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

First Previous 1 Next Last

Add Edit Delete Refresh

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 (224.1.1.1 - 224.1.1.1)

Member

Available Port Selected Port

Apply Close

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. • 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. • 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 9-37 MVR Group Address Edit Fields

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.

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

RADIUS Table

Showing All entries Showing 1 to 1 of 1 entries

☐	Server Address	Server Port	Priority	Retry	Timeout	Usage
☐	192.168.1.98	1812	1	3	3	All

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 • Login: For login authentication • 802.1x: For 802.1x authentication • All: For all types

Table 10-2 RADIUS Table Fields

Security >> RADIUS

Add RADIUS Server

Address Type	☒ Hostname ☐ IPv4 ☐ IPv6
Server Address	192.168.1.98
Server Port	1812 (0 - 65535, default 1812)
Priority	1 (0 - 65535)
Key String	☒ Use Default
Retry	☒ Use Default 3 (1 - 10, default 3)
Timeout	☒ Use Default 3 Sec (1 - 30, default 3)
Usage	☐ Login ☐ 802.1X ☒ All

Security >> RADIUS

Edit RADIUS Server

Server Address	192.168.1.98
Server Port	1812 (0 - 65535, default 1812)
Priority	1 (0 - 65535)
Key String	☒ Use Default
Retry	☒ Use Default 3 (1 - 10, default 3)
Timeout	☒ Use Default 3 Sec (1 - 30, default 3)
Usage	☐ Login ☐ 802.1X ☒ All

Figure 10-3 Add/Edit RADIUS Server Dialog

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

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

TACACS+ Table

Showing All entries Showing 1 to 1 of 1 entries

☐	Server Address	Server Port	Priority	Timeout
☐	192.168.1.97	49	1	5

First
Previous
1
Next
Last

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	192.168.1.97
Server Port	49 (0 - 65535, default 49)
Priority	1 (0 - 65535)
Key String	☒ Use Default
Timeout	☒ Use Default 5 Sec (1 - 30, default 5)

Security >> TACACS+

Edit TACACS+ Server

Server Address	192.168.1.97
Server Port	49 (0 - 65535, default 49)
Priority	1 (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 • 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.

Security >> AAA >> Method List

Method List Table

Showing entries Showing 1 to 2 of 2 entries

☐	Name	Sequence
☐	default	(1) Local
☐	TEST	(1) TACACS+

Figure 10-7 Method List Table

Field	Description
Name	Login authentication list name. This name should be different from other existing lists.
Sequence	Priority of login authentication method. • None: Authenticated with any condition. • Local: Use local accounts database to authenticate • TACACS+: Use remote TACACS+ server to authenticate. • RADIUS: Use remote Radius server to authenticate. • Enable: Use local enable password to authenticate

Table 10-7 Method List Table Fields

Security >> AAA >> Method List

[Add Method List](#)

Name

Method 1

☒ Empty
☐ None
☐ Local
☐ Enable
☐ RADIUS
☐ TACACS+

Method 2

☒ Empty
☐ None
☐ Local
☐ Enable
☐ RADIUS
☐ TACACS+

Method 3

☒ Empty
☐ None
☐ Local
☐ Enable
☐ RADIUS
☐ TACACS+

Method 4

☒ Empty
☐ None
☐ Local
☐ Enable
☐ RADIUS
☐ TACACS+

Security >> AAA >> Method List

Edit Method List

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

Apply Close

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	Select first priority of login authentication method. • None: Authenticated with any condition. • Local: Use local accounts database to authenticate • TACACS+: Use remote TACACS+ server to authenticate. • RADIUS: Use remote Radius server to authenticate. Enable: Use local enable password to authenticate
Method 2	Select second priority of login authentication method. • None: Authenticated with any condition. • Local: Use local accounts database to authenticate TACACS+: Use remote TACACS+ server to authenticate. • RADIUS: Use remote Radius server to authenticate. - Enable: Use local enable password to authenticate
Method 3	Select thrid priority of login authentication method. • None: Authenticated with any condition. • Local: Use local accounts database to authenticate • TACACS+: Use remote TACACS+ server to authenticate. • RADIUS: Use remote Radius server to authenticate. Enable: Use local enable password to authenticate
Method 4	Select fourth priority of login authentication method. • None: Authenticated with any condition. • Local: Use local accounts database to authenticate • TACACS+: Use remote TACACS+ server to authenticate. • RADIUS: Use remote Radius server to authenticate. Enable: Use local enable password to authenticate

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.

Interface	Authentication List	Count
Console	default	(1) Local
Telnet	default	(1) Local
SSH	TEST	(1) TACACS+
HTTP	default	(1) Local
HTTPS	TEST	(1) TACACS+

Apply

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.

Management VLAN: 1 - default

Note: Change Management VLAN may cause connection interrupted

Apply

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 Services

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

This page allow user to change management services related configurations.

Security >> Management Access >> Management Service

Management Service

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

Session Timeout

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

Password Retry Count

Console	3	(0 - 120, default 3)
Telnet	3	(0 - 120, default 3)
SSH	3	(0 - 120, default 3)

Silent Time

Console	0	Sec (0 - 65535, default 0)
Telnet	0	Sec (0 - 65535, default 0)
SSH	0	Sec (0 - 65535, default 0)

Apply

Figure 10-11 Management Service Page

Field	Description
Management Service	Management service admin state. Telnet: Connect CLI through telnet SSH: Connect CLI through SSH HTTP: Connect WEBUI through HTTP HTTPS: Connect WEBUI through HTTPS SNMP: Manage switch trough SNMP

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

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

Management ACL Table

Showing All entries Showing 1 to 3 of 3 entries

	ACL Name	State	Rule
☐	aaa	Deactive	0
☐	bbb	Deactive	0
☐	ccc	Deactive	0

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

Edit Managemet ACE

ACL Name	aaa	
Priority	1	
Service	☐ All ☐ Http ☐ Https ☒ Snmp ☐ SSH ☐ Telnet	
Action	☐ Permit ☒ Deny	
Port	Available Port GE2 GE4 GE5 GE7 GE8 GE9 GE10 LAG1	Selected Port GE1 GE3 GE6
IP Version	☒ All ☐ IPv4 ☐ IPv6	
IPv4	/ 255.255.255.255	
IPv6	/ 128 (1 - 128)	

Apply Close

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. • All: All services • HTTP: Only HTTP service. • HTTPs: Only HTTPs service. • SNMP: Only SNMP service. • SSH: Only SSH service. • Telnet: Only Telnet service.
Action	Select the action after ACE match packet. • Permit: Forward packets that meet the ACE criteria. • Deny: Drop packets that meet the ACE criteria.
Port	Select ports which will be matched.
IP Version	Select the type of source IP address. • All: All IP addresses can access. • IPv4: Specify IPv4 address ca access • IPv6: Specify IPv6 address ca access
IPv4	Enter the source IPv4 address value and mask to which will be matched.
IPv6	Enter the source IPv6 address value and mask to which will be matched.

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	Set checkbox to enable/disable following authentication types • 802.1x: Use IEEE 802.1x to do authentication • MAC-Based: Use MAC address to do authentication • WEB-Based: Prompt authentication web page for user to do authentication
Guest VLAN	Set checkbox to enable/disable guest VLAN, if guest VLAN is enabled, you need to select one available VLAN ID to be guest VID.
MAC-Based User ID Format	Select mac-based authentication RADIUS username/password ID format. • 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-XXXXXXXXXX-XXXXXX • XXXXXX.XXXXXXXXXXX.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					
☐	1	GE1	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
☐	2	GE2	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
☐	3	GE3	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
☐	4	GE4	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
☐	5	GE5	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
☐	6	GE6	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
☐	7	GE7	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
☐	8	GE8	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
☐	9	GE9	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
☐	10	GE10	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static

Figure 10-17 Port Mode Table

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

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

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

Security >> Authentication Manager >> Port Setting

Port Setting Table

	Entry	Port	Port Control	Reauthentication	Max Hosts	Common Timer			802.1x Param		
						Reauthentication	Inactive	Quiet	TX Period	Supplicant Timeout	Se
☐	1	GE1	Disabled	Disabled	256	3600	60	60	30	30	
☐	2	GE2	Disabled	Disabled	256	3600	60	60	30	30	
☐	3	GE3	Disabled	Disabled	256	3600	60	60	30	30	
☐	4	GE4	Disabled	Disabled	256	3600	60	60	30	30	
☐	5	GE5	Disabled	Disabled	256	3600	60	60	30	30	
☐	6	GE6	Disabled	Disabled	256	3600	60	60	30	30	
☐	7	GE7	Disabled	Disabled	256	3600	60	60	30	30	
☐	8	GE8	Disabled	Disabled	256	3600	60	60	30	30	
☐	9	GE9	Disabled	Disabled	256	3600	60	60	30	30	
☐	10	GE10	Disabled	Disabled	256	3600	60	60	30	30	

Figure 10-19: Authentication Manager Port Setting Table

Field	Description
Port	Port name
Port Control	Support following authentication port control types. • Disable: Disable authentication function and all clients have network accessibility. • Force Authorized: Port is force authorized and all clients have network accessibility. • Force Unauthorized: Port is force unauthorized and all clients have no network accessibility. • Auto: Need passing authentication procedure to get network accessibility.
Reauthentication	Reauthenticate state • Enabled: Host will be reauthenticated after reauthentication period • Disabled: Host will not be reauthenticated after reauthentication period
Max Hosts	In Multiple Authentication mode, total host number cannot not exceed max hosts number
Common Timer (Reauthentication)	After re-authenticate period, host will return to initial state and need to pass authentication procedure again.
Common Timer (Inactive)	If no packet from the authenticated host, the inactive timer will increase. After inactive timeout, the host will be unauthorized and corresponding session will be deleted. In multi-host mode, the packet is counting on the authorized host only and not all packets on the port.
Common Timer (Quiet)	When port is in Locked state after authenticating fail several times, the host will be locked in quiet period. After this quiet period, the host is allowed to authenticate again.

802.1X Params (TX Period)	Number of seconds that the device waits for a response to an Extensible Authentication Protocol (EAP) request/identity frame from the supplicant (client) before resending the request.
802.1X Params (Supplicant Timeout)	The maximum number of EAP requests that can be sent. If a response is not received after the defined period (supplicant timeout), the authentication process is restarted.
802.1X Params (Server Timeout)	Number of seconds that lapses before EAP requests are resent to the supplicant.
802.1X Params (Max Request)	Number of seconds that lapses before the device resends a request to the authentication server.
Web-Based Param (Max Login)	Allow user login fail number. After login fail number exceed, the host will enter Lock state and is not able to authenticate until quiet period exceed.

Table 10-19: Authentication Manager Port Setting Table Fields

Security >> Authentication Manager >> Port Setting

Edit Port Setting

Port	GE1-GE3	
Port Control	☒ Disabled ☐ Force Authorized ☐ Force Unauthorized ☐ Auto	
Reauthentication	☐ Enable	
Max Hosts	256	(1 - 256, default 256)
Common Timer		
Reauthentication	3600	Sec (300 - 2147483647, default 3600)
Inactive	60	Sec (60 - 65535, default 60)
Quiet	60	Sec (0 - 65535, default 60)
802.1x Parameters		
TX Period	30	Sec (1 - 65535, default 30)
Supplicant Timeout	30	Sec (1 - 65535, default 30)
Server Timeout	30	Sec (1 - 65535, default 30)
Max Request	2	(1 - 10, default 2)
Web-Based Parameters		
Max Login	☐ Infinite 3	(3 - 10, default 3)
Apply Close		

Figure 10-20: Authentication Manager Port Setting Dialog

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

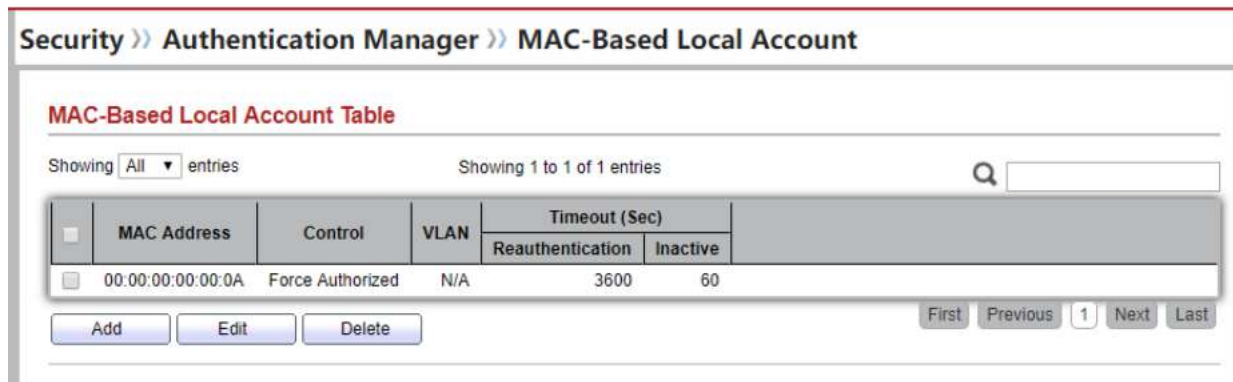


Figure 10-21 MAC-Based Local Account Table

Field	Description
MAC Address	Authenticated host MAC address, and each MAC allow only one entry in local database.
Control	Control Type • 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 10-21 MAC-Based Local Account Table Fields

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

Add MAC-Based Local Account

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

Apply Close

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

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

Field	Description
MAC Address	Authenticated host MAC address, and each MAC allow only one entry in local database.
Control	Control Type • Force Authorized: Host will be force authorized • Force Unauthorized: Host will be force unauthorized
VLAN	Assigned VLAN ID for the authenticated host.

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

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 Manager > WEB-Based Local Account**

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

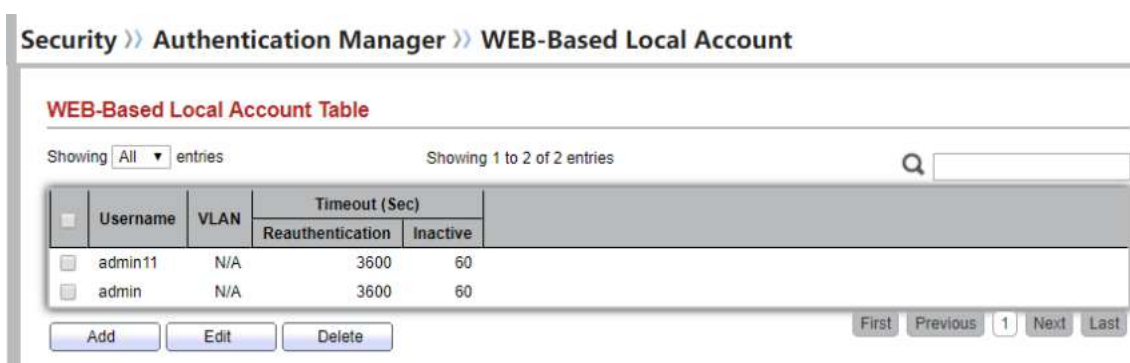


Figure 10-23 WEB-Based Local Account Table

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

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

Add WEB-Based Local Account

Username	admin11	
Password		
Confirm Password		
VLAN	☐ User Defined 1 (1 - 4094)	
Assigned Timer		
Reauthentication	☒ User Defined 3600 Sec (300 - 2147483647)	
Inactive	☒ User Defined 60 Sec (60 - 65535)	

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

Edit WEB-Based Local Account

Username	admin11	
Password		
Confirm Password		
VLAN	☐ User Defined (1 - 4094)	
Assigned Timer		
Reauthentication	☒ User Defined 3600 Sec (300 - 2147483647)	
Inactive	☒ User Defined 60 Sec (60 - 65535)	

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

	Session ID	Port	MAC Address	Current Type	Status	Operational Information				Authorized Information		
						VLAN	Session Time	Inactived 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 • 802.1x: Use IEEE 802.1X to do authenticating • MAC-Based:Use MAC-Based authentication to do authenticating • WEB-Based:Use WEB-Based authentication to do authenticating
Status	Show host authentication session status • Disable: This session is ready to be deleted • Running: Authentication process is running • Authorized:Authentication is passed and getting network accessibility. • UnAuthorized: Authentication is not passed and not getting network accessibility. • Locked:Host is locked and do not allow to do authenticating until quiet period. • Guest: Host is in the guest VLAN

Operational (VLAN)	Shows host operational VLAN ID.
Operational (Session Time)	In “Authorized” state, it shows total time after authorized.
Operational (Inactived)	In “Authorized” state, it shows how long the host do not send any packet.
Operational (Quiet Time)	In “Locked” state, it shows total time after locked.
Authorized (VLAN)	Shows VLAN ID given from authorized procedure.
Authorized (Reauthentication Period)	Shows reauthentication period given from authorized procedure.
Authorized (Inactive Timeouts)	Shows inactive timeout given from authorized procedure.

Table 10-25 Sessions Table Fields

10.6 Port Security

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

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

Security >> Port Security

State ☐ Enable

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

Port Security Table

☐	Entry	Port	State	Address Limit	Total	Configured	Violate Number	Violate Action	Sticky
☐	1	GE1	Disabled	1	0	0	0	Protect	Disabled
☐	2	GE2	Disabled	1	0	0	0	Protect	Disabled
☐	3	GE3	Disabled	1	0	0	0	Protect	Disabled
☐	4	GE4	Disabled	1	0	0	0	Protect	Disabled
☐	5	GE5	Disabled	1	0	0	0	Protect	Disabled
☐	6	GE6	Disabled	1	0	0	0	Protect	Disabled
☐	7	GE7	Disabled	1	0	0	0	Protect	Disabled
☐	8	GE8	Disabled	1	0	0	0	Protect	Disabled
☐	9	GE9	Disabled	1	0	0	0	Protect	Disabled
☐	10	GE10	Disabled	1	0	0	0	Protect	Disabled

Figure 10-26 Port Security Page

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

Table 10-26 Port Security Fields

10.7 Protected Port

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

This page allow user to configure protected port setting to prevent the selected ports from communication with each other. Protected port is only allowed to communicate with unprotected port. In other words, protected port is not allowed to communicate with another protected port.

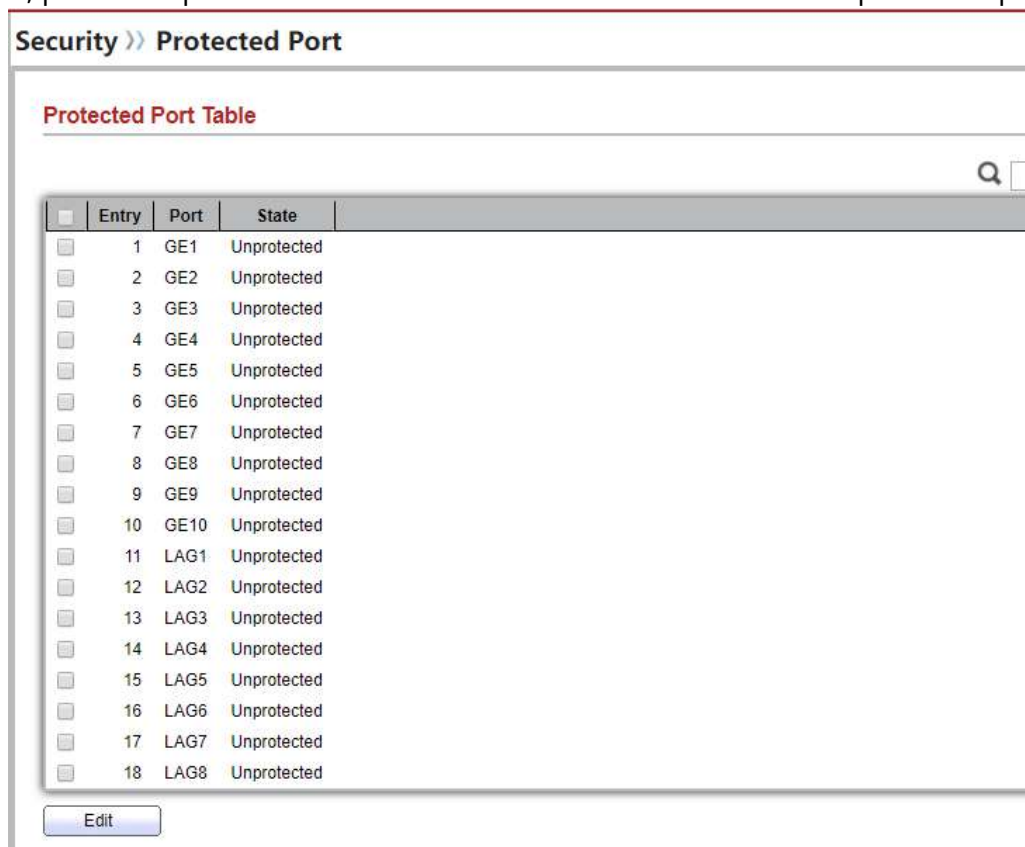


Figure 10-27 Protected Port Table

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

Figure 10-28 Edit Protected Port dialog

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

Table 10-28 Edit Protected Port Fields

10.8 Storm Control

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

Security >> Storm Control

Mode
☐ Packet / Sec
☒ Kbits / Sec

IFG
☒ Exclude
☐ Include

Port Setting Table

	Entry	Port	State	Broadcast		Unknown Multicast		Unknown Unicast		Action
				State	Rate (Kbps)	State	Rate (Kbps)	State	Rate (Kbps)	
☐	1	GE1	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
☐	2	GE2	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
☐	3	GE3	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
☐	4	GE4	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
☐	5	GE5	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
☐	6	GE6	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
☐	7	GE7	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
☐	8	GE8	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
☐	9	GE9	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
☐	10	GE10	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop

Figure 10-29 Storm Control Setting Page

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

ingress storm control rate.

- **Included:** include preamble & IFG (20 bytes) when count ingress storm control rate.

Table 10-29 Storm Control Global Setting Fields

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

The screenshot shows the 'Security >> Storm Control' web page. A dialog box titled 'Edit Port Setting' is displayed. It contains the following fields and options:

- Port:** GE1
- State:** ☐ Enable
- Broadcast:** ☐ Enable, 10000 Kbps (16 - 1000000, default 10000)
- Unknown Multicast:** ☐ Enable, 10000 Kbps (16 - 1000000, default 10000)
- Unknown Unicast:** ☐ Enable, 10000 Kbps (16 - 1000000, default 10000)
- Action:** ☒ Drop, ☐ Shutdown

At the bottom of the dialog are 'Apply' and 'Close' buttons.

Figure 10-30 Storm Control Edit Port Setting Page

Field	Description
Port	Select the setting ports
State	Select the state of setting Enable: Enable the storm control function.
Broadcast	Enable: Enable the storm control function of Broadcast packet. Value of storm control rate, Unit: pps (packet per-second, range 1 - 262143) or Kbps (Kbits per-second, range 16 - 1000000) depends on global mode setting.
Unknown Multicast	Enable: Enable the storm control function of Unknown multicast packet. Value of storm control rate, Unit: pps (packet per-second, range 1 - 262143) or Kbps (Kbits per-second, range 16 - 1000000) depends on global mode setting.
Unknown Unicast	Enable: Enable the storm control function of Unknown unicast packet. Value of storm control rate, Unit: pps (packet per-second, range 1- 262143) or Kbps (Kbits per-second, range 16 - 1000000) depends on global mode setting.
Action	Select the state of setting Drop: Packets exceed storm control rate will be dropped. Shutdown: Port will be shutdown when packets exceed storm control rate.

Table 10-30 Storm Control Port Setting Fields

10.9 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.

10.9.1 Property

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

Security >> DoS >> Property

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

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 Attack	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 Attack SYN-FIN	Drops the packets with SYN and FIN bits set.
TCP Attack SYN-RST	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.

10.9.2 Port Setting

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

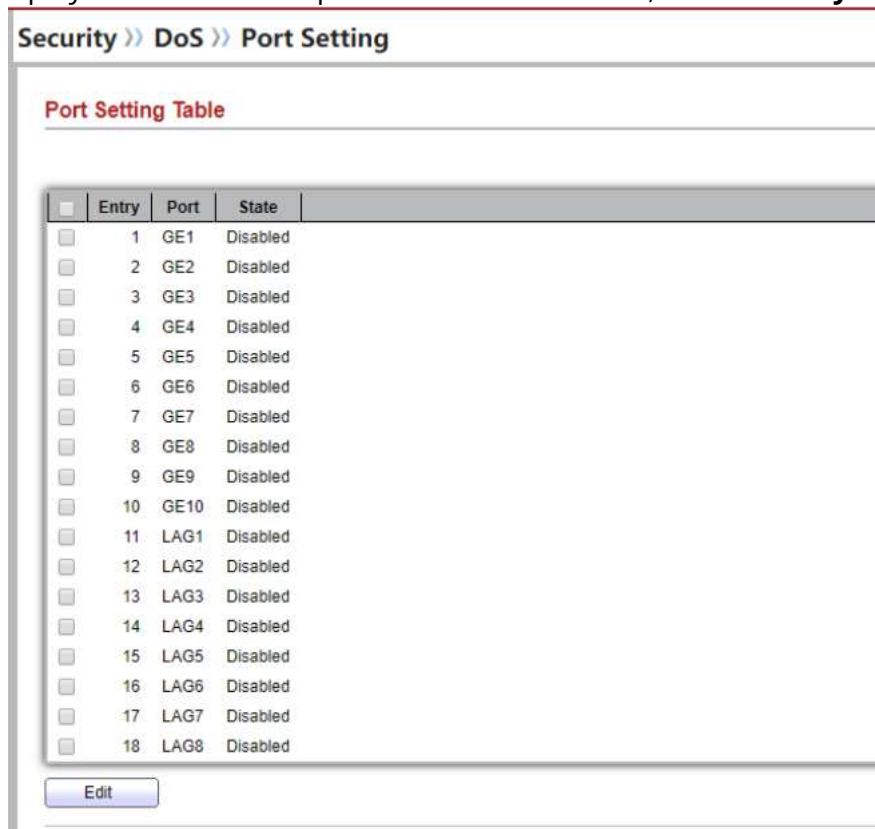


Figure 10-32: Port Setting page.

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.

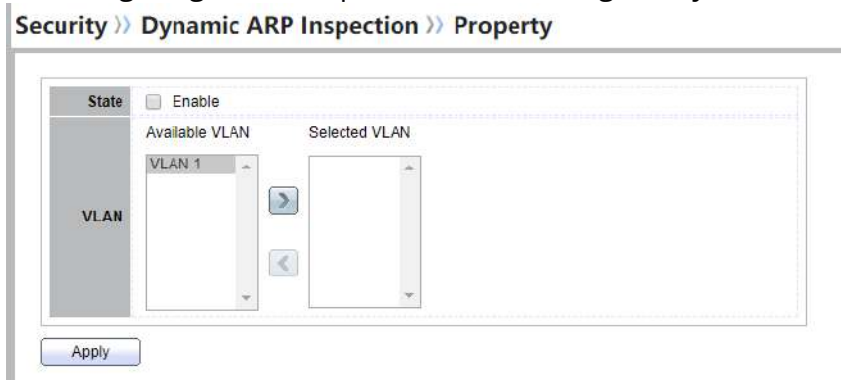


Figure 10-33 Property Page

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	
☐	1	GE1	Disabled	Disabled	Disabled	Disabled	Unlimited	
☐	2	GE2	Disabled	Disabled	Disabled	Disabled	Unlimited	
☐	3	GE3	Disabled	Disabled	Disabled	Disabled	Unlimited	
☐	4	GE4	Disabled	Disabled	Disabled	Disabled	Unlimited	
☐	5	GE5	Disabled	Disabled	Disabled	Disabled	Unlimited	
☐	6	GE6	Disabled	Disabled	Disabled	Disabled	Unlimited	
☐	7	GE7	Disabled	Disabled	Disabled	Disabled	Unlimited	
☐	8	GE8	Disabled	Disabled	Disabled	Disabled	Unlimited	
☐	9	GE9	Disabled	Disabled	Disabled	Disabled	Unlimited	
☐	10	GE10	Disabled	Disabled	Disabled	Disabled	Unlimited	
☐	11	LAG1	Disabled	Disabled	Disabled	Disabled	Unlimited	
☐	12	LAG2	Disabled	Disabled	Disabled	Disabled	Unlimited	
☐	13	LAG3	Disabled	Disabled	Disabled	Disabled	Unlimited	
☐	14	LAG4	Disabled	Disabled	Disabled	Disabled	Unlimited	
☐	15	LAG5	Disabled	Disabled	Disabled	Disabled	Unlimited	
☐	16	LAG6	Disabled	Disabled	Disabled	Disabled	Unlimited	
☐	17	LAG7	Disabled	Disabled	Disabled	Disabled	Unlimited	
☐	18	LAG8	Disabled	Disabled	Disabled	Disabled	Unlimited	

Edit

Figure 10-34 Property Port Page

Field	Description
Port	Display port ID.
Trust	Display enable/disabled trust attribute of interface
Source Address	MAC 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

Security >> Dynamic ARP Inspection >> Property

Edit Port Setting

Port	GE1
Trust	☒ Enable
Source MAC Address	☒ Enable
Destination MAC Address	☒ Enable
IP Address	☒ Enable
	☒ Allow Zero (0.0.0.0)
Rate Limit	20 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 destination mac address validation. Default is disabled.

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

Table 10-35 Edit Property Port Fields

10.10.2 Statistics

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

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

Entry	Port	Forward	Source MAC Failure	Destination MAC Failure	Source IP Validation Failure	Destination IP Validation Failure	IP-MAC Mismatch Failure
1	GE1	0	0	0	0	0	0
2	GE2	0	0	0	0	0	0
3	GE3	0	0	0	0	0	0
4	GE4	0	0	0	0	0	0
5	GE5	0	0	0	0	0	0
6	GE6	0	0	0	0	0	0
7	GE7	0	0	0	0	0	0
8	GE8	0	0	0	0	0	0
9	GE9	0	0	0	0	0	0
10	GE10	0	0	0	0	0	0
11	LAG1	0	0	0	0	0	0
12	LAG2	0	0	0	0	0	0
13	LAG3	0	0	0	0	0	0
14	LAG4	0	0	0	0	0	0
15	LAG5	0	0	0	0	0	0
16	LAG6	0	0	0	0	0	0
17	LAG7	0	0	0	0	0	0
18	LAG8	0	0	0	0	0	0

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.
---------------------------------	---

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

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

Table 10-38 Property Port Fields

Security >> DHCP Snooping >> Property

Edit Port Setting

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

Apply Close

Figure 10-39 Edit Property Port Dialog

Field	Description
Port	Display selected port to be edited.
Trust	Set checkbox to enable/disable 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.

Table 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.

Security >> DHCP Snooping >> Statistics

Statistics Table

Q

	Entry	Port	Forward	Chaddr Check Drop	Untrust Port Drop	Untrust Port with Option82 Drop	Invalid Drop	
☐	1	GE1	0	0	0	0	0	
☐	2	GE2	0	0	0	0	0	
☐	3	GE3	0	0	0	0	0	
☐	4	GE4	0	0	0	0	0	
☐	5	GE5	0	0	0	0	0	
☐	6	GE6	0	0	0	0	0	
☐	7	GE7	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 Drop	Display how many packets dropped by chaddr validation.
Untrusted Port Drop	Display how many DHCP server packets that are received by untrusted port dropped.
Untrusted Port with Option82 Drop	Display how many packets dropped by untrusted port with option82 checking.
Invalid Drop	Display how many packets dropped by invalid checking.

10.11.3 Option 82 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.

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

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

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

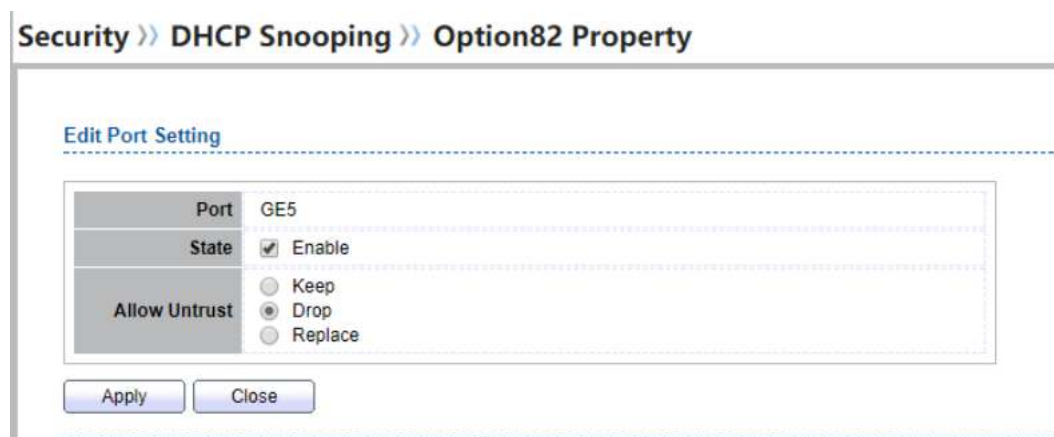


Figure 10-43 Edit Option82 Port Dialog

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. • 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 Option 82 Client 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

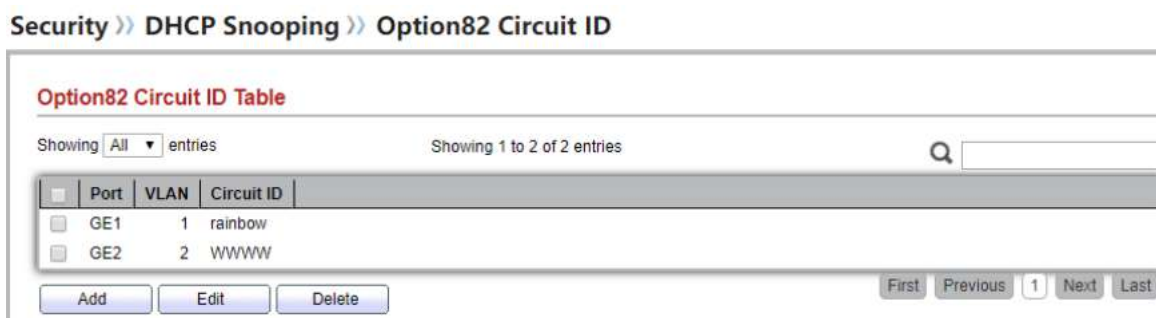


Figure 10-44 Option82 Circuit ID Page

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

The screenshot displays two web-based dialog boxes for configuring Option82 Circuit ID fields. The top dialog, titled 'Add Option82 Circuit ID', contains three input fields: 'Port' with a dropdown menu showing 'GE5', 'VLAN' with a text box containing '2' and a note '(1 - 4094) (Keep empty to set without VLAN)', and 'Circuit ID' with a text box containing 'dddd'. Below these fields are 'Apply' and 'Close' buttons. The bottom dialog, titled 'Edit Option82 Circuit ID', contains three input fields: 'Port' with a dropdown menu showing 'GE1', 'VLAN' with a text box containing '1', and 'Circuit ID' with a text box containing 'rainbow'. Below these fields are 'Apply' and 'Close' buttons.

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

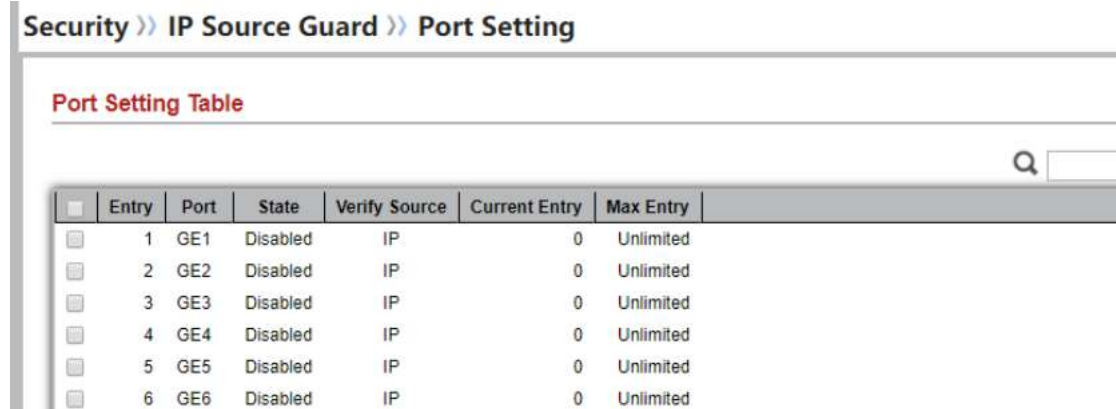
10.12 IP Source Guard

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.

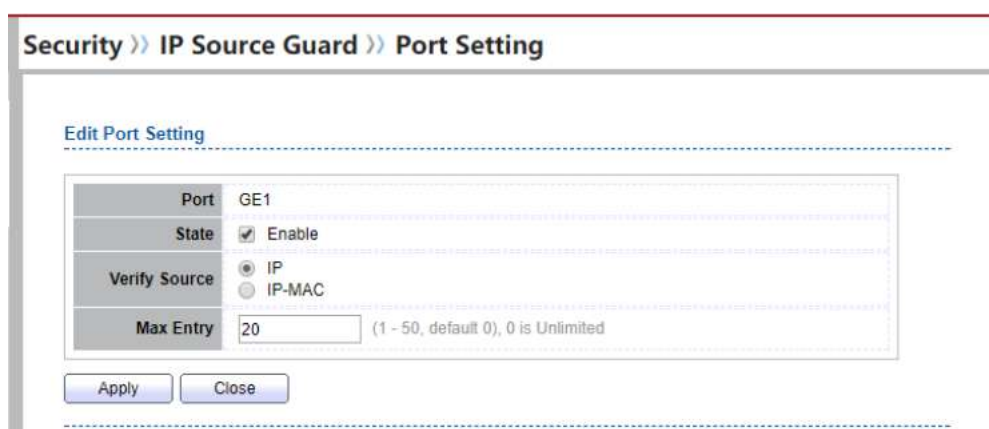


Entry	Port	State	Verify Source	Current Entry	Max Entry
1	GE1	Disabled	IP	0	Unlimited
2	GE2	Disabled	IP	0	Unlimited
3	GE3	Disabled	IP	0	Unlimited
4	GE4	Disabled	IP	0	Unlimited
5	GE5	Disabled	IP	0	Unlimited
6	GE6	Disabled	IP	0	Unlimited

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



Security >> IP Source Guard >> Port Setting

Edit Port Setting

Port	GE1
State	☒ Enable
Verify Source	☒ IP ☐ IP-MAC
Max Entry	20 (1 - 50, default 0), 0 is Unlimited

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 • 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.

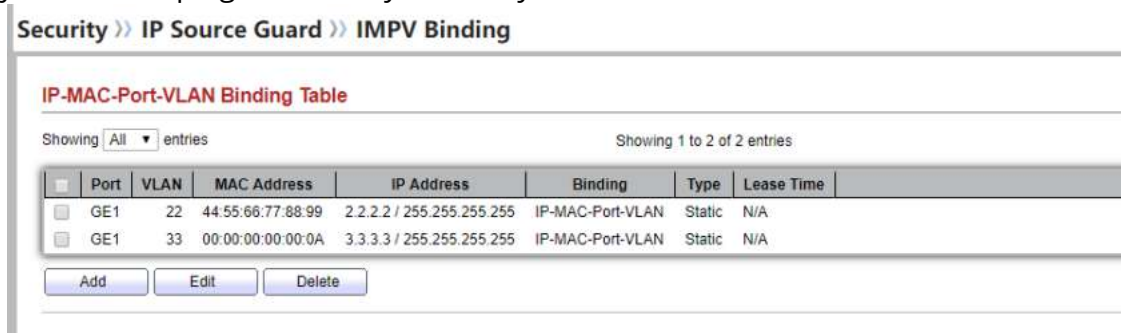


Figure 10-48 IPMV Binding Page

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 • 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

Security >> IP Source Guard >> IMPV Binding

Add IP-MAC-Port-VLAN Binding

Port	GE1 ▼	
VLAN	33 (1 - 4094)	
Binding	☒ IP-MAC-Port-VLAN ☐ IP-Port-VLAN	
MAC Address	00:00:00:00:00:0A	
IP Address	3.3.3.3 / 255.255.255.255	

Apply Close

Edit IP-MAC-Port-VLAN Binding

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

Apply Close

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 • 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.

Figure 10-50 Save Database Page

Field	Description
Type	Select the type of database agent. • 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. • 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.

Table 10-50 Save Database Fields

11.ACL

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

ACL Table

Showing All entries Showing 1 to 3 of 3 entries

☐	ACL Name	Rule	Port
☐	AAAA	0	
☐	SSSS	0	
☐	DDDD	0	

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.

☐	Sequence	Action	Source MAC		Destination MAC		Ethertype	VLAN	802.1p	
			Address	Mask	Address	Mask			Value	Mask
☐	1	Permit	Any	Any	Any	Any	Any	Any	Any	Any
☐	22	Shutdown	Any	Any	Any	Any	Any	Any	Any	Any

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

Figure 11-4 Add and Edit MAC ACE Dialog

Field	Description
ACL Name	Display the ACL name to which an ACE is being added.
Sequence	Specify the sequence of the ACE. ACEs with higher sequence are processed first (1 is the highest priority). Only available on Add Dialog.
Action	Select the action after ACE match packet. Permit: Forward packets that meet the ACE criteria. Deny: Drop packets that meet the ACE criteria. Shutdown: Drop packets that meet the ACE criteria, and disable the port from where the packets were received. Such ports can be reactivated from the Port Settings page.

Source MAC	Select the type for source MAC address. • Any: All source addresses are acceptable. • User Defined: Only a source address or a range of source addresses which users define are acceptable. Enter the source MAC address and mask to which will be matched.
Destination MAC	Select the type for Destination MAC address. • Any: All destination addresses are acceptable. • User Defined: Only a destination address or a range of destination addresses which users define are acceptable. Enter the destination MAC address and mask to which will be matched.
Ethertype	Select the type for Ethernet frame type. • Any: All Ethernet frame type is acceptable. • User Defined: Only an Ethernet frame type which users define is acceptable. Enter the Ethernet frame type value to which will be matched.
VLAN ID	Select the type for VLAN ID. • Any: All VLAN ID is acceptable. • User Defined: Only a VLAN ID which users define is acceptable. Enter the VLAN ID to which will be matched.
802.1p	Select the type for 802.1p value. • Any: All 802.1p value is acceptable. • User Defined: Only an 802.1p value or a range of 802.1p value which users define is acceptable. Enter the 802.1p value and mask to which will be matched.

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

ACL >> IPv4 ACL

ACL Name

Apply

ACL Table

Showing All entries Showing 1 to 3 of 3 entries

	ACL Name	Rule	Port
☐	IP11	0	
☐	IP23	0	
☐	IP8	0	

Delete

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.

ACL >> IPv4 ACE

ACE Table

ACL Name IP11

Showing All entries Showing 1 to 1 of 1 entries

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

Add Edit Delete

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

ACL >> IPv4 ACE

Add ACE

ACL Name	IP11
Sequence	(1 - 2147483647)
Action	☒ Permit ☐ Deny ☐ Shutdown
Protocol	☒ Any ☐ Select ICMP v ☐ Define (0 - 255)
Source IP	☒ Any / (Address / Mask)
Destination IP	☒ Any / (Address / Mask)
Type of Service	☒ Any ☐ DSCP (0 - 63) ☐ IP Precedence (0 - 7)
Source Port	☒ Any ☐ Single (0 - 65535) ☐ Range - (0 - 65535)
Destination Port	☒ Any ☐ Single (0 - 65535) ☐ Range - (0 - 65535)
TCP Flags	Urg: ☐ Set ☐ Unset ☒ Don't care Ack: ☐ Set ☐ Unset ☒ Don't care Psh: ☐ Set ☐ Unset ☒ Don't care Rst: ☐ Set ☐ Unset ☒ Don't care

ACL » IPv4 ACE

Edit ACE

ACL Name	IP11
Sequence	23
Action	☒ Permit ☐ Deny ☐ Shutdown
Protocol	☒ Any ☐ Select ICMP (0 - 255) ☐ Define (0 - 255)
Source IP	☒ Any / (Address / Mask)
Destination IP	☒ Any / (Address / Mask)
Type of Service	☒ Any ☐ DSCP (0 - 63) ☐ IP Precedence (0 - 7)
Source Port	☒ Any ☐ Single (0 - 65535) ☐ Range - (0 - 65535)
Destination Port	☒ Any ☐ Single (0 - 65535) ☐ Range - (0 - 65535)
TCP Flags	Urg: ☐ Set ☐ Unset ☒ Don't care Ack: ☐ Set ☐ Unset ☒ Don't care Psh: ☐ Set ☐ Unset ☒ Don't care Rst: ☐ Set ☐ Unset ☒ Don't care Syn: ☐ Set ☐ Unset ☒ Don't care Fin: ☐ Set ☐ Unset ☒ Don't care
ICMP Type	☒ Any ☐ Select Echo Reply (0 - 255) ☐ Define (0 - 255)
ICMP Code	☒ Any ☐ Define (0 - 255)

Apply Close

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	Select the action for a match. • Permit: Forward packets that meet the ACE criteria. • Deny: Drop packets that meet the ACE criteria. • Shutdown: Drop packets that meet the ACE criteria, and disable the port from where the packets were received. Such ports can be reactivated from the Port Settings page.

Protocol	Select the type of protocol for a match. • Any (IP): All IP protocols are acceptable. • Select from list: Select one of the following protocols from the drop-down list. (ICMP/IPinIP/TCP/EGP/IGP/UDP/HMP/RDP/IPV6/IPV6:ROUT/IPV6:FRAG/RSVP/IPV6:ICMP/OSPF/PIM/L2TP) • Protocol ID to match: Enter the protocol ID.
Source IP	Select the type for source IP address. • Any: All source addresses are acceptable. • User Defined: Only a source address or a range of source addresses which users define are acceptable. Enter the source IP address value and mask to which will be matched.
Destination IP	Select the type for destination IP address. • Any: All destination addresses are acceptable. • User Defined: Only a destination address or a range of destination addresses which users define are acceptable. Enter the destination IP address value and mask to which will be matched.
Source Port	Select the type of protocol for a match. Only available when protocol is TCP or UDP. • Any: All source ports are acceptable. • Single: Enter a single TCP/UDP source port to which packets are matched. • Range: Select a range of TCP/UDP source ports to which the packet is matched. There are eight different port ranges that can be configured (shared between source and destination ports). TCP and UDP protocols each have eight port ranges.
TCP Flags	Select one or more TCP flags with which to filter packets. Filtered packets are either forwarded or dropped. Filtering packets by TCP flags increases packet control, which increases network security. Only available when protocol is TCP.
Type of Service	Select the type of service for a match. • Any: All types of service are acceptable. • DSCP to match: Enter a Differentiated Services Code Point (DSCP) to match. • IP Precedence to match: Enter a IP Precedence to match.
ICMP Type	Either select the message type by name or enter the message type number. Only available when protocol is ICMP. • Any: All message types are acceptable. • Select from list: Select message type by name. • Protocol ID to match: Enter the number of message type.
ICMP Code	Select the type for ICMP code. Only available when protocol is ICMP. • Any: All codes are acceptable. • User Defined: Enter an ICMP code to match.

Table 11-8 Add and Edit IPv4 ACL Fields

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.

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

ACL >> IPv6 ACE

Add ACE

ACL Name	IP61	
Sequence	(1 - 2147483647)	
Action	☒ Permit ☐ Deny ☐ Shutdown ☐ Any	
Protocol	☐ Select TCP ☐ Define (0 - 255)	
Source IP	☒ Any / (Address / Prefix (0 - 128))	
Destination IP	☒ Any / (Address / Prefix (0 - 128))	
Type of Service	☐ Any ☐ DSCP (0 - 63) ☐ IP Precedence (0 - 7)	
Source Port	☐ Any ☐ Single (0 - 65535) ☐ Range - (0 - 65535)	
Destination Port	☐ Any ☐ Single (0 - 65535) ☐ Range - (0 - 65535)	
TCP Flags	Urg: ☐ Set ☐ Unset ☒ Don't care Ack: ☐ Set ☐ Unset ☒ Don't care Psh: ☐ Set ☐ Unset ☒ Don't care Rst: ☐ Set ☐ Unset ☒ Don't care Syn: ☐ Set ☐ Unset ☒ Don't care Fin: ☐ Set ☐ Unset ☒ Don't care ☐ Any	
ICMP Type	☐ Select Destination Unreachable ☐ Define (0 - 255)	
ICMP Code	☐ Any ☐ Define (0 - 255)	

ACL » IPv6 ACE

Edit ACE

ACL Name	IP61
Sequence	22334
Action	☒ Permit ☐ Deny ☐ Shutdown
Protocol	☒ Any ☐ Select TCP ▾ ☐ Define (0 - 255)
Source IP	☒ Any ☐ / (Address / Prefix (0 - 128))
Destination IP	☒ Any ☐ / (Address / Prefix (0 - 128))
Type of Service	☒ Any ☐ DSCP (0 - 63) ☐ IP Precedence (0 - 7)
Source Port	☒ Any ☐ Single (0 - 65535) ☐ Range - (0 - 65535)
Destination Port	☒ Any ☐ Single (0 - 65535) ☐ Range - (0 - 65535)
TCP Flags	Urg: ☐ Set ☐ Unset ☒ Don't care Ack: ☐ Set ☐ Unset ☒ Don't care Psh: ☐ Set ☐ Unset ☒ Don't care Rst: ☐ Set ☐ Unset ☒ Don't care Syn: ☐ Set ☐ Unset ☒ Don't care Fin: ☐ Set ☐ Unset ☒ Don't care
ICMP Type	☒ Any ☐ Select Destination Unreachable ▾ ☐ Define (0 - 255)
ICMP Code	☒ Any ☐ Define (0 - 255)

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. • Permit: Forward packets that meet the ACE criteria. • Deny: Drop packets that meet the ACE criteria. • Shutdown: Drop packets that meet the ACE criteria, and disable the port from where the packets were received. Such ports can be reactivated from the Port Settings page.
Protocol	Select the type of protocol for a match. • Any (IP): All IP protocols are acceptable. • Select from list: Select one of the following protocols from the drop-down list.(TCP / UDP / ICMP) • Protocol ID to match: Enter the protocol ID.
Source IP	Select the type for source IP address. • Any: All source addresses are acceptable. • User Defined: Only a source address or a range of source addresses which users define are acceptable. Enter the source IP address value and prefix length to which will be matched.
Destination IP	Select the type for destination IP address. • Any: All destination addresses are acceptable. • User Defined: Only a destination address or a range of destination addresses which users define are acceptable. Enter the destination IP address value and prefix to which will be matched.
Source Port	Select the type of protocol for a match. Only available when protocol is TCP or UDP. • Any: All source ports are acceptable. • Single: Enter a single TCP/UDP source port to which packets are matched. • Range: Select a range of TCP/UDP source ports to which the packet is matched. There are eight different port ranges that can be configured (shared between source and destination ports). TCP and UDP protocols each have eight port ranges.
Destination Port	Select the type of protocol for a match. Only available when protocol is TCP or UDP. • Any: All source ports are acceptable. • Single: Enter a single TCP/UDP source port to which packets are matched. • Range: Select a range of TCP/UDP source ports to which packet is matched. There are eight different port ranges that can be configured(share between source and destination ports). TCP and UDP potocols each have eight port ranges.

TCP Flags	Select one or more TCP flags with which to filter packets. Filtered packets are either forwarded or dropped. Filtering packets by TCP flags increases packet control, which increases network security. Only available when protocol is TCP.
Type of Service	Select the type of service for a match. • Any: All types of service are acceptable. • DSCP to match: Enter a Differentiated Services Code Point (DSCP) to match. • IP Precedence to match: Enter a IP Precedence to match.
ICMP Type	Either select the message type by name or enter the message type number. Only available when protocol is ICMP. • Any: All message types are acceptable. • Select from list: Select message type by name. • Protocol ID to match: Enter the number of message type.
ICMP Code	Select the type for ICMP code. Only available when protocol is ICMP. • Any: All codes are acceptable. • User Defined: Enter an ICMP code to match.

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.

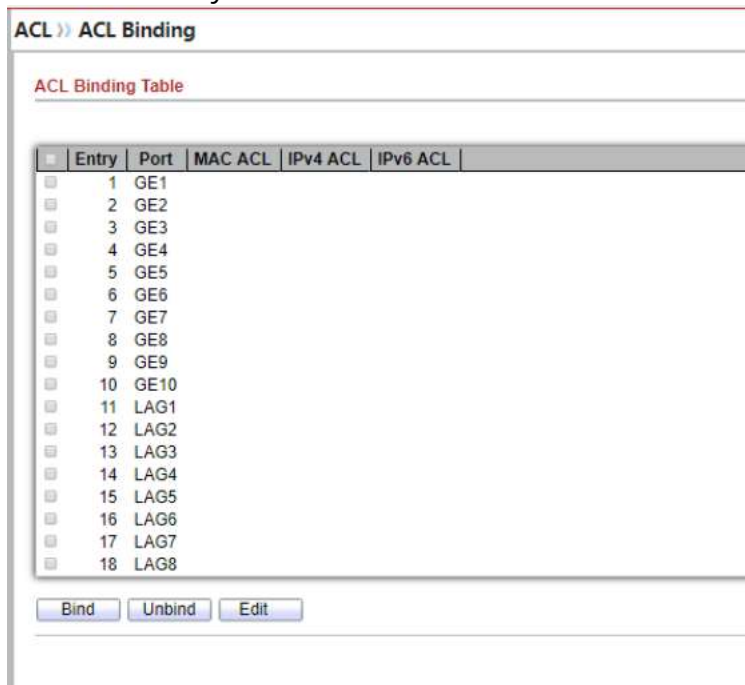


Figure 11-13 ACL Binding Page

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

ACL >> ACL Binding

Add ACL Binding

Port

GE1

Note: ACL without any rules cannot be bound

MAC ACL

AAAA ▾

IPv4 ACL

IP11 ▾

IPv6 ACL

None ▾

Apply

Close

Edit ACL Binding

Port

GE1

Note: ACL without any rules cannot be bound

MAC ACL

AAAA ▾

IPv4 ACL

IP11 ▾

IPv6 ACL

None ▾

Apply

Close

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

	Entry	Port	CoS	Trust	Remarking		
					CoS	DSCP	IP Precedence
☐	1	GE1	0	Enabled	Disabled	Disabled	Disabled
☐	2	GE2	0	Enabled	Disabled	Disabled	Disabled
☐	3	GE3	0	Enabled	Disabled	Disabled	Disabled
☐	4	GE4	0	Enabled	Disabled	Disabled	Disabled
☐	5	GE5	0	Enabled	Disabled	Disabled	Disabled
☐	6	GE6	0	Enabled	Disabled	Disabled	Disabled
☐	7	GE7	0	Enabled	Disabled	Disabled	Disabled
☐	8	GE8	0	Enabled	Disabled	Disabled	Disabled
☐	9	GE9	0	Enabled	Disabled	Disabled	Disabled
☐	10	GE10	0	Enabled	Disabled	Disabled	Disabled
☐	11	LAG1	0	Enabled	Disabled	Disabled	Disabled
☐	12	LAG2	0	Enabled	Disabled	Disabled	Disabled
☐	13	LAG3	0	Enabled	Disabled	Disabled	Disabled
☐	14	LAG4	0	Enabled	Disabled	Disabled	Disabled
☐	15	LAG5	0	Enabled	Disabled	Disabled	Disabled
☐	16	LAG6	0	Enabled	Disabled	Disabled	Disabled
☐	17	LAG7	0	Enabled	Disabled	Disabled	Disabled
☐	18	LAG8	0	Enabled	Disabled	Disabled	Disabled

Edit

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 • Enabled: Traffic will follow trust mode in global setting • Disabled: Traffic will always use best efforts
Remarking (CoS)	Port CoS remarking admin state • Enabled: CoS remarking is enabled • Disabled: CoS remarking is disabled
Remarking (DSCP)	Port DSCP remarking admin state • Enabled: DSCP remarking is enabled • Disabled: DSCP remarking is disabled
Remarking (IP Precedence)	Port IP Precedence remarking admin state • Enable: IP Precedence remarking is enabled • Disable: IP Precedence remarking is disabled

Table 12-2 QoS Port Setting Table Fields

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

o 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	Method			
	Strict Priority	WRR	Weight	WRR Bandwidth (%)
1	☒	☐	1	33.33%
2	☐	☒	2	66.67%
3	☐	☒	3	
4	☐	☒	4	
5	☐	☒	5	
6	☐	☒	9	
7	☐	☒	13	
8	☐	☒	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.

QoS >> General >> CoS Mapping

CoS to Queue Mapping

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

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

Queue to CoS Mapping

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

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.

QoS >> General >> DSCP Mapping

DSCP to Queue Mapping

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

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.

QoS >> General >> IP Precedence Mapping

IP Precedence to Queue Mapping

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

Apply

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

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 12-10 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.

QoS >> Rate Limit >> Ingress / Egress Port						
Ingress / Egress Port Table						
	Entry	Port	Ingress		Egress	
			State	Rate (Kbps)	State	Rate (Kbps)
☐	1	GE1	Disabled		Disabled	
☐	2	GE2	Disabled		Disabled	
☐	3	GE3	Disabled		Disabled	
☐	4	GE4	Disabled		Disabled	
☐	5	GE5	Disabled		Disabled	
☐	6	GE6	Disabled		Disabled	
☐	7	GE7	Disabled		Disabled	
☐	8	GE8	Disabled		Disabled	
☐	9	GE9	Disabled		Disabled	
☐	10	GE10	Disabled		Disabled	

Edit

Figure 12-11 Ingress/Egress Port Table

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

Egress (State)	Port egress rate limit state
	• Enabled: Egress rate limit is enabled • Disabled: Egress rate limit is disabled
Egress (Rate)	Port egress rate limit value if egress rate state is enabled

Table 12-11 Ingress/Egress Port Table Fields

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.

Entry	Port	Queue 1		Queue 2		Queue 3		Queue 4		Queue 5		Queue 6		Queue 7	
		State	CIR (Kbps)	State	CIR (Kbps)	State	CIR (Kbps)	State	CIR (Kbps)	State	CIR (Kbps)	State	CIR (Kbps)	State	CIR (Kbps)
1	GE1	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
2	GE2	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
3	GE3	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
4	GE4	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
5	GE5	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
6	GE6	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
7	GE7	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
8	GE8	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
9	GE9	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
10	GE10	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	

Figure 12-13: Egress Queue Table

Field	Description
Port	Port name
Queue 1 (State)	Port egress queue 1 rate limit state • Enabled: Egress queue rate limit is enabled • Disabled: Egress queue rate limit is disabled
Queue 1 (CIR)	Queue 1 egress committed information rate
Queue 2 (State)	Port egress queue 2 rate limit state • Enabled: Egress queue rate limit is enabled • Disabled: Egress queue rate limit is disabled
Queue 2 (CIR)	Queue 2 egress committed information rate
Queue 3 (State)	Port egress queue 3 rate limit state • Enabled: Egress queue rate limit is enabled • Disabled: Egress queue rate limit is disabled
Queue 3 (CIR)	Queue 3 egress committed information rate
Queue 4 (State)	Port egress queue 4 rate limit state • Enabled: Egress queue rate limit is enabled • Disabled: Egress queue rate limit is disabled
Queue 4 (CIR)	Queue 4 egress committed information rate
Queue 5 (State)	Port egress queue 5 rate limit state • Enabled: Egress queue rate limit is enabled • Disabled: Egress queue rate limit is disabled
Queue 5 (CIR)	Queue 5 egress committed information rate
Queue 6 (State)	Port egress queue 6 rate limit state • Enabled: Egress queue rate limit is enabled • Disabled: Egress queue rate limit is disabled
Queue 6 (CIR)	Queue 6 egress committed information rate
Queue 7 (State)	Port egress queue 7 rate limit state • Enabled: Egress queue rate limit is enabled • Disabled: Egress queue rate limit is disabled
Queue 7 (CIR)	Queue 7 egress committed information rate
Queue 8 (State)	Port egress queue 8 rate limit state • Enabled: Egress queue rate limit is enabled • Disabled: Egress queue rate limit is disabled
Queue 8 (CIR)	Queue 8 egress committed information rate

Table 12-13: Egress Queue Table Fields.

QoS >> Rate Limit >> Egress Queue

Edit Egress Queue

Port	GE1-GE3	
Queue 1	☒ Enable	1000000 Kbps (16 - 1000000)
Queue 2	☒ Enable	1000000 Kbps (16 - 1000000)
Queue 3	☒ Enable	1000000 Kbps (16 - 1000000)
Queue 4	☒ Enable	1000000 Kbps (16 - 1000000)
Queue 5	☐ Enable	1000000 Kbps (16 - 1000000)
Queue 6	☐ Enable	1000000 Kbps (16 - 1000000)
Queue 7	☐ Enable	1000000 Kbps (16 - 1000000)
Queue 8	☐ Enable	1000000 Kbps (16 - 1000000)

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.Diagnostics

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**.

Diagnostics >> Logging >> Property

State	☒ Enable
Aggregation	☒ Enable
Aging Time	300 Sec (15 - 3600, default 300)
Console Logging	
State	☒ Enable
Minimum Severity	Notice Note: Emergency, Alert, Critical, Error, Warning, Notice
RAM Logging	
State	☒ Enable
Minimum Severity	Notice Note: Emergency, Alert, Critical, Error, Warning, Notice
Flash Logging	
State	☐ Enable
Minimum Severity	Notice Note: Emergency, Alert, Critical, Error, Warning, Notice

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**.

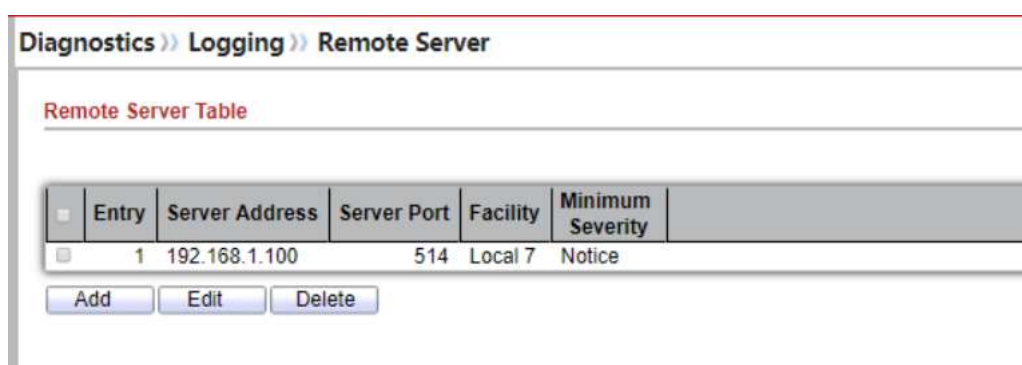


Figure 13-2: Remote Server page.

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**

Session ID	State	Monitor Port	Ingress Port	Egress Port
1	Disabled	---	---	---
2	Disabled	---	---	---
3	Disabled	---	---	---
4	Disabled	---	---	---

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 • Enabled: Enable port based mirror • Disabled: Disable mirror.
Monitor Port	Select mirror session monitor port, and select whether normal packet could be sent or received by monitor port.
Ingress port	Select mirror session source rx ports
Egress ports	Select mirror session source tx ports

Table 13-6 Mirroring Fields

13.3 Ping

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

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**.

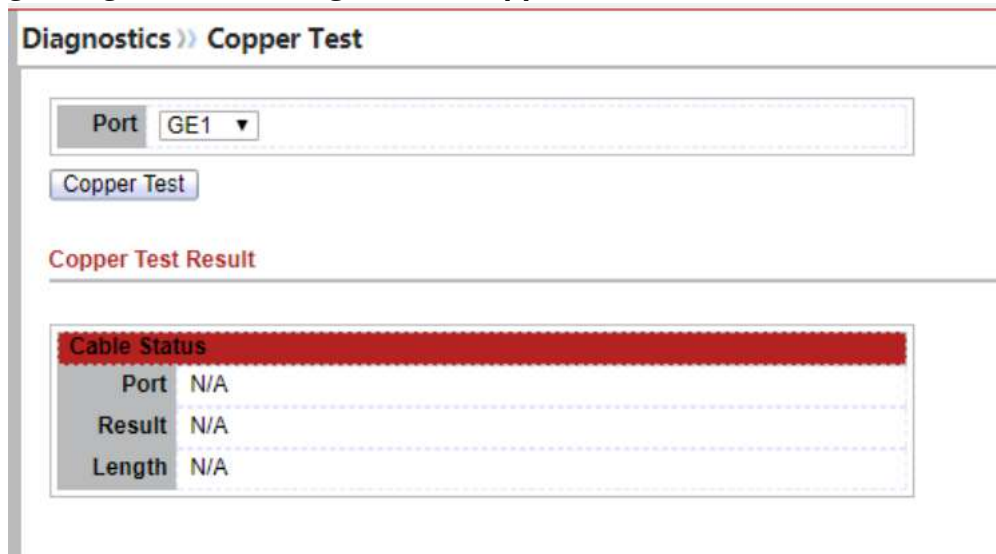
Figure 13-5: Traceroute page.

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**.



Diagnostics >> Copper Test

Port: GE1 ▼

Copper Test

Copper Test Result

Cable Status	
Port	N/A
Result	N/A
Length	N/A

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	The status of copper test. It include: • OK: Correctly terminated pair. • Short Cable: Shorted pair. • Open Cable: Open pair, no link partner. • Impedance Mismatch: Terminating impedance is not in the reference range. • Line Drive:
Length	Distance in meter from the port to the location on the cable where the fault was discovered.

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**.

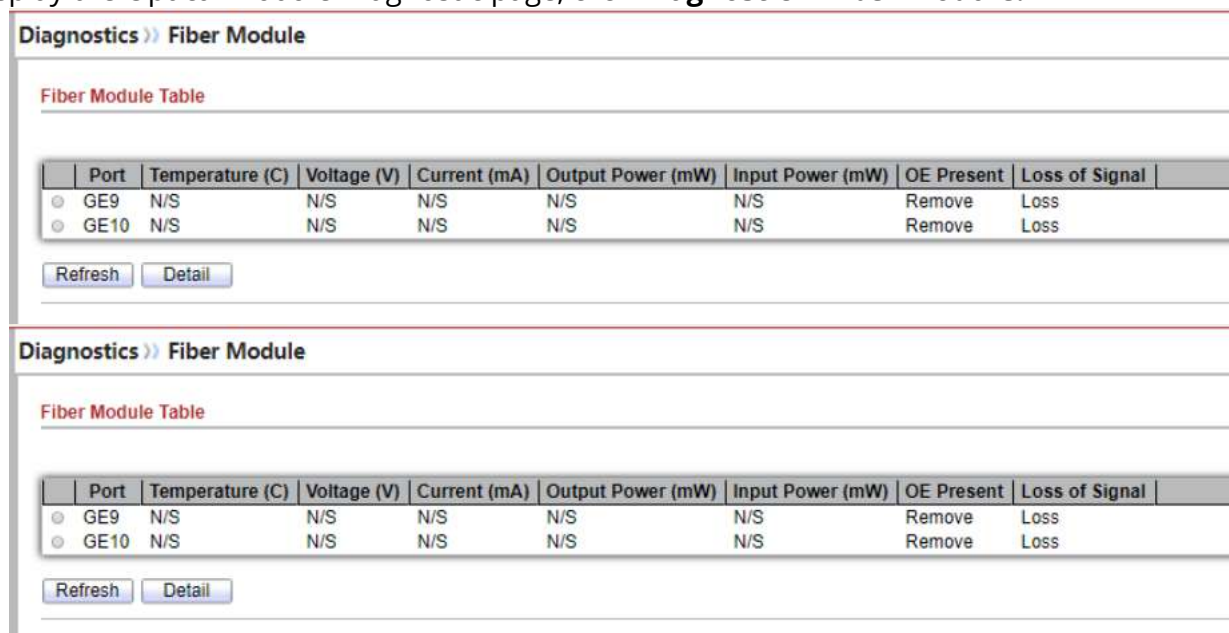


Figure 13-7: Fiber Module page.

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.

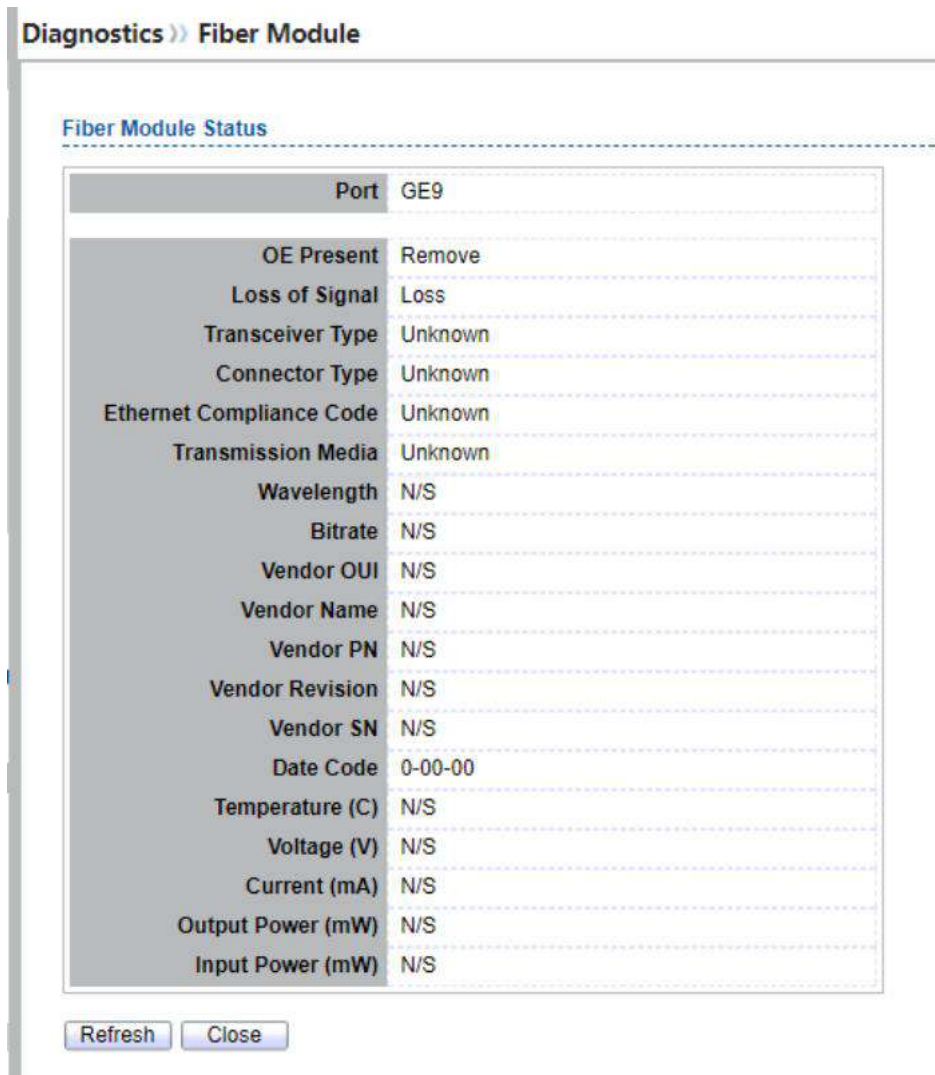


Figure 13-8: Fiber Module Status page.

13.7 UDLD

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.

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

Table 13-12 Property Fields

Port Setting Table

	Entry	Port	Mode	Bidirectional State	Operational Status	Neighbor	
☐	1	GE1	Disabled	Unknown		0	
☐	2	GE2	Disabled	Unknown		0	
☐	3	GE3	Disabled	Unknown		0	
☐	4	GE4	Disabled	Unknown		0	
☐	5	GE5	Disabled	Unknown		0	
☐	6	GE6	Disabled	Unknown		0	
☐	7	GE7	Disabled	Unknown		0	
☐	8	GE8	Disabled	Unknown		0	
☐	9	GE9	Disabled	Unknown		0	
☐	10	GE10	Disabled	Unknown		0	

Edit

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 Status	Display operational status of interface
Neighbor	Display the number of neighbor of interface

Table 13-13 Property Port Fields

Diagnostics >> UDLD >> Property

Edit Port Setting

Port

GE1

Mode

☒ Disabled
☐ Normal
☐ Aggressive

Apply Close

Figure 13-11: Edit Property Port page.

Field	Description
Port	Display selected port to be edited.
Mode	Select UDLD running mode of interface. • Disabled: Disable UDLD function. • Normal: Running on normal mode that port goes to Link Up One phase after last neighbor ages out. • Aggressive: Running on aggressive mode that port goes to Re-Establish phase after last neighbor ages out.

Table 13-14 Edit Property Port Fields

13.7.2 Neighbor

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

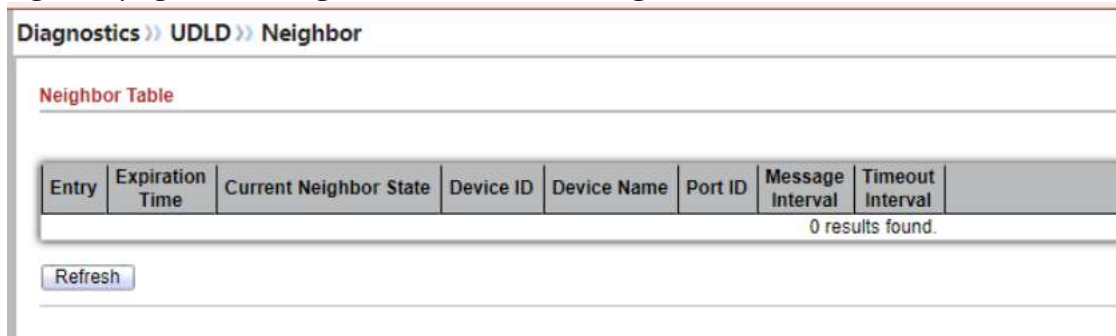


Figure 13-12: Neighbor page.

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.

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.

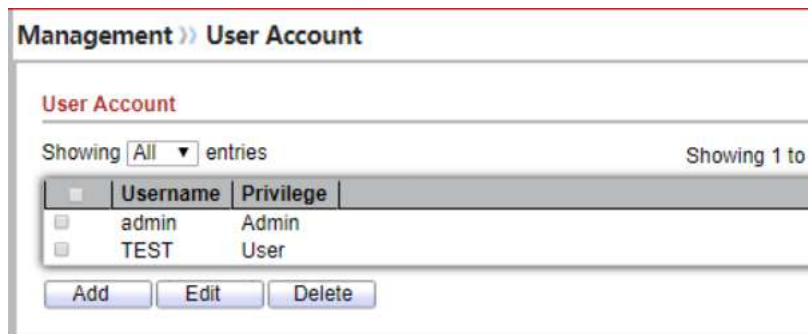


Figure 14-1 User Account Table

Field	Description
Username	User name of the account
Privilege	Select privilege level for new account. Admin: Allow to change switch settings. Privilege value equals to 15. User: See switch settings only. Not allow to change it. Privilege level equals to 1.

Table 14-1 User Account Table Fields

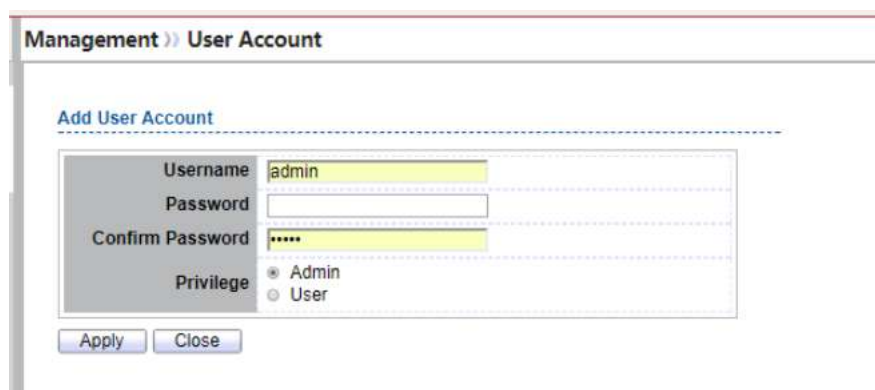


Figure 14-2 Add/Edit User Account Dialog

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	Select privilege level for new account. • Admin: Allow to change switch settings. Privilege value equals to 15. • User: See switch settings only. Not allow to change it. Privilege level equals to 1.

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

Field	Description
	Firmware operations
Action	• Upgrade: Upgrade firmware from remote host to DUT • Backup: Backup firmware image from DUT to remote host
	Firmware upgrade / backup method
Method	• TFTP: Using TFTP to upgrade/backup firmware • HTTP: Using WEB browser to upgrade/backup firmware
Filename	Use browser to upgrade firmware, you should select firmware image file on your host PC.

Table 14-3 Upgrade Firmware through HTTP Fields

Figure 14-4 Upgrade Firmware through TFTP

Field	Description
	Firmware operations
Action	• Upgrade: Upgrade firmware from remote host to DUT • Backup: Backup firmware image from DUT to remote host
	Firmware upgrade / backup method
Method	• TFTP: Using TFTP to upgrade/backup firmware • HTTP: Using WEB browser to upgrade/backup firmwar
	Specify TFTP server address type
Address Type	• Hostname: Use domain name as server address • IPv4: Use IPv4 as server address • IPv6: Use IPv6 as server address
Server Address	Specify TFTP server address.
Filename	Firmware image file name on remote TFTP server

Table 14-4 Upgrade Firmware through TFTP Fields

The screenshot shows the 'Management >> Firmware >> Upgrade / Backup' page. It features a configuration panel with three sections: 'Action' with radio buttons for 'Upgrade' and 'Backup' (where 'Backup' is selected); 'Method' with radio buttons for 'TFTP' and 'HTTP' (where 'HTTP' is selected); and 'Firmware' with radio buttons for 'Image0' and 'Image1' (where 'Image0' is selected). An 'Apply' button is located at the bottom left of the configuration area.

Figure 14-5 Backup Firmware through HTTP

Field	Description
Action	Firmware operations
	• Upgrade: Upgrade firmware from remote host to DUT • Backup: Backup firmware image from DUT to remote host
Method	Firmware upgrade / backup method
	• TFTP: Using TFTP to upgrade/backup firmware • HTTP: Using WEB browser to upgrade/backup firmware
Firmware	Firmware partition need to backup
	• Image0: Firmware image in flash partition 0 • Image1: Firmware image in flash partition 1

Table 14-5 Backup Firmware through HTTP Fields

The screenshot shows the 'Management >> Firmware >> Upgrade / Backup' page. It features a configuration panel with six sections: 'Action' with radio buttons for 'Upgrade' and 'Backup' (where 'Backup' is selected); 'Method' with radio buttons for 'TFTP' and 'HTTP' (where 'TFTP' is selected); 'Firmware' with radio buttons for 'Image0' and 'Image1' (where 'Image0' is selected); 'Address Type' with radio buttons for 'Hostname', 'IPv4', and 'IPv6' (where 'Hostname' is selected); 'Server Address' with a text input field; and 'Filename' with a text input field. An 'Apply' button is located at the bottom left of the configuration area.

Figure 14-6 Backup Firmware through TFTP

Field	Description
Action	Firmware operations • Upgrade: Upgrade firmware from remote host to DUT • Backup: Backup firmware image from DUT to remote host
Method	Firmware upgrade / backup method • TFTP: Using TFTP to upgrade/backup firmware • HTTP: Using WEB browser to upgrade/backup firmware
Firmware	Firmware partition need to backup • Image0: Firmware image in flash partition • Image1: Firmware image in flash partition 1
Address Type	Specify TFTP server address type • Hostname: Use domain name as server address • IPv4: Use IPv4 as server address • IPv6: Use IPv6 as server address
Server Address	Specify TFTP server address.
Filename	File name saved on remote TFTP server

Table 14-6 Backup Firmware through TFTP Fields

14.2.2 Active Image

To display the Active Image web page, click **Management > Firmware > Active Image**.

This page allow user to select firmware image on next booting and show firmware information on both flash partitions

The screenshot shows a web interface for managing firmware images. At the top, under 'Active Image', there are two radio buttons: 'Image0' (selected) and 'Image1'. A note below states: 'Note: the image was selected for the next boot'. Below this, there are two sections: 'Active Image' and 'Backup Image', each containing a table of details.

Active Image	
Firmware	Image0
Version	3.1.0.b10
Name	
Size	5882191 Bytes
Created	2014-09-22 16:53:53

Backup Image	
Firmware	Image1
Version	3.1.0.50153
Name	vmlinux.bix
Size	6284117 Bytes
Created	2014-10-09 18:32:26

An 'Apply' button is located at the bottom left of the form.

Figure 14-7 Active Image Page

Field	Description
Active Image	Select firmware image to use on next booting
Firmware	Firmware flash partition name
Version	Firmware version
Name	Firmware name
Size	Firmware image size
Created	Firmware image created date

Table 14-7 Active Image 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.



Figure 14-8 Upgrade Configuration through HTTP

Field	Description
Action	Configuration operations
	• Upgrade: Upgrade firmware from remote host to DUT • Backup: Backup firmware image from DUT to remote host
Method	Configuration upgrade / backup method
	• TFTP: Using TFTP to upgrade/backup firmware • HTTP: Using WEB browser to upgrade/backup firmware

Configuration	Configuration types
	• Running Configuration: Merge to current running configuration file
	• Startup Configuration: Replace startup configuration file
	• Backup Configuration: Replace backup configuration file
Filename	Use browser to upgrade configuration, you should select configuration file on your host PC

Table 14-8 Upgrade Configuration through HTTP Fields

Figure 14-9 Upgrade Configuration through TFTP

Field	Description
Action	Configuration operations
	• Upgrade: Upgrade firmware from remote host to DUT • Backup: Backup firmware image from DUT to remote host
Method	Configuration upgrade / backup method
	• TFTP: Using TFTP to upgrade/backup firmware • HTTP: Using WEB browser to upgrade/backup firmware
Configuration	Configuration types
	• Running Configuration: Merge to current running configuration file • Startup Configuration: Replace startup configuration file • Backup Configuration: Replace backup configuration file
Address Type	Specify TFTP server address type
	• Hostname: Use domain name as server address • IPv4: Use IPv4 as server address • IPv6: Use IPv6 as server address
Server Address	Specify TFTP server address
Filename	Configuration file name on remote TFTP server

Table 14-9 Upgrade Firmware through TFTP Fields

Management >> Configuration >> Upgrade / Backup

Action

- ☐ Upgrade
- ☒ Backup

Method

- ☐ TFTP
- ☒ HTTP

Configuration

- ☒ Running Configuration
- ☐ Startup Configuration
- ☐ Backup Configuration
- ☐ RAM Log
- ☐ Flash Log

Apply

Figure 14-10 Backup Configuration through HTTP

Field	Description
Action	Configuration operations • Upgrade: Upgrade configuration from remote host to DUT • Backup: Backup configuration from DUT to remote host
Method	Configuration upgrade / backup method • TFTP: Using TFTP to upgrade/backup configuration • HTTP: Using WEB browser to upgrade/backup configuration
Configuration	Configuration types • Running Configuration: Backup running configuration file • Startup Configuration: Backup start configuration file • Backup Configuration: Backup backup configuration file • RAM Log: Backup log file stored in RAM • Flash Log: Backup log files store in Flash

Table 14-10 Backup Configuration through HTTP Fields

Management >> Configuration >> Upgrade / Backup

Action

- ☐ Upgrade
- ☒ Backup

Method

- ☒ TFTP
- ☐ HTTP

Configuration

- ☒ Running Configuration
- ☐ Startup Configuration
- ☐ Backup Configuration
- ☐ RAM Log
- ☐ Flash Log

Address Type

- ☒ Hostname
- ☐ IPv4
- ☐ IPv6

Server Address

Filename

Apply

Figure 14-11 Backup Configuration through TFTP

Field	Description
Action	Firmware operations • Upgrade: Upgrade firmware from remote host to DUT • Backup: Backup firmware image from DUT to remote host
Method	Firmware upgrade / backup method • TFTP: Using TFTP to upgrade/backup firmware • HTTP: Using WEB browser to upgrade/backup firmware
Configuration	Configuration types • Running Configuration: Backup running configuration file • Startup Configuration: Backup start configuration file • Backup Configuration: Backup backup configuration file • RAM Log: Backup log file stored in RAM • Flash Log: Backup log files store in Flash
Address Type	Specify TFTP server address type • Hostname: Use domain name as server address • IPv4: Use IPv4 as server address • IPv6: Use IPv6 as server address
Server Address	Specify TFTP server address.
Filename	File name saved on remote TFTP server

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.

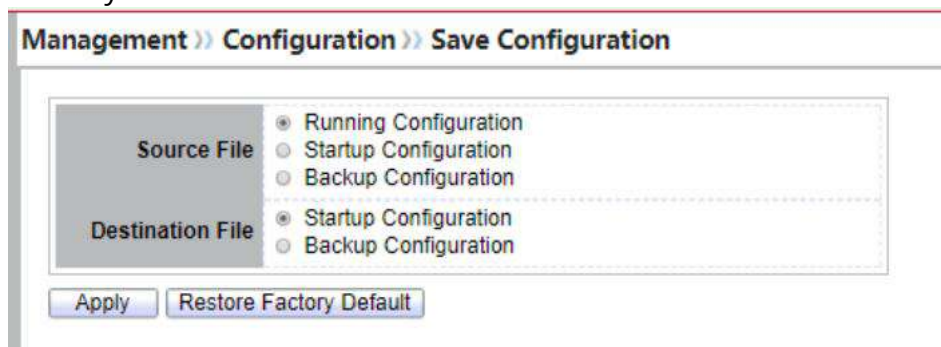


Figure 14-12 Save Configuration Page

Field	Description
Source File	Source file types • Running Configuration: Copy running configuration file to destination • Startup Configuration: Copy startup configuration file to destination • Backup Configuration: Copy backup configuration file to destination

Destination file

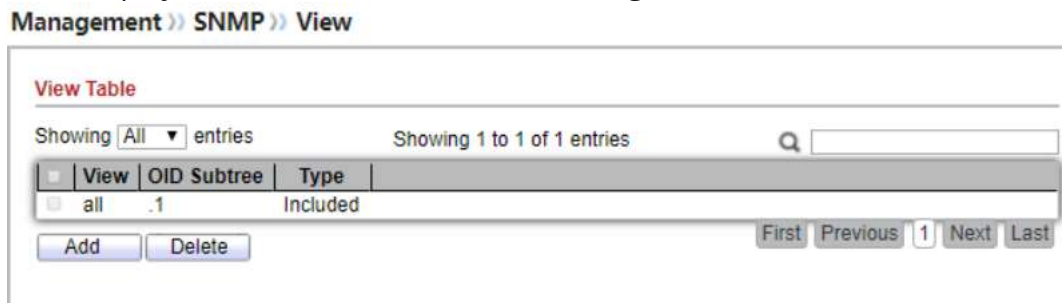
- Destination File**
- **Startup Configuration:** Save file as startup configuration
 - **Backup Configuration:** Save file as backup configuration

Table 14-11 Backup Firmware through TFTP Fields

14.4 SNMP

14.4.1 View

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



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**.

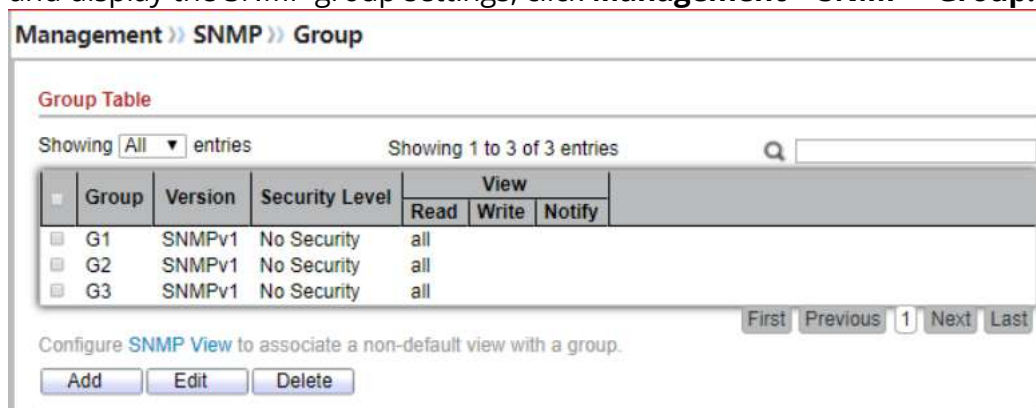


Figure 14-14 SNMP Group Table Page

Field	Description
Group	Specify SNMP group name, and the maximum length is 30 characters.

Version	Specify SNMP version • SNMPv1: SNMP Version 1. • SNMPv2: Community-based SNMP Version 2c. • SNMPv3: User security model SNMP version 3.
Security Level	Specify SNMP security level • No Security : Specify that no packet authentication is performed. • Authentication: Specify that no packet authentication without encryption is performed. • Authentication and Privacy: Specify that no packet authentication with encryption is performed.
View	
Read	Group read view name
Write	Group write view name.
Notify	The view name that sends only traps with contents that is included in SNMP view selected for notification.

Table 14-14 SNMP Group Table Fields

Figure 14-15 SNMP Group Add Page

Field	Description
Group	Specify SNMP group name, and the maximum length is 30 characters.
Version	Specify SNMP version • SNMPv1: SNMP Version 1. • SNMPv2: Community-based SNMP Version 2c. • SNMPv3: User security model SNMP version 3.

Security Level	Specify SNMP security level
	• No Security : Specify that no packet authentication is performed. • Authentication: Specify that no packet authentication without encryption is performed. • Authentication and Privacy: Specify that no packet authentication with encryption is performed.
View	
Read	Select read view name if Read is checked
Write	Select write view name, if Write is checked
Notify	Select notify view name, if Notify is checked

Table 14-15 SNMP Group Add Fields

Management >> SNMP >> Group

Edit Group

Group: G2

Version:

- ☒ SNMPv1
- ☐ SNMPv2
- ☐ SNMPv3

Security Level:

- ☒ No Security
- ☐ Authentication
- ☐ Authentication and Privacy

Read: ☒ Read

Read View: all ▼

Write: ☒ Write

Write View: all ▼

Notify: ☒ Notify

Notify View: all ▼

Apply Close

Figure 14-16 SNMP Group Edit Page

Field	Description
Group	Display the edit group name
Version	Specify SNMP version • SNMPv1: SNMP Version 1. • SNMPv2: Community-based SNMP Version 2c. • SNMPv3: User security model SNMP version 3.
Security Level	Specify SNMP security level • No Security : Specify that no packet authentication is performed. • Authentication: Specify that no packet authentication without encryption is performed. • Authentication and Privacy: Specify that no packet authentication with encryption is performed.

View	
Read	Select read view name if Read is checked
Write	Select write view name, if Write is checked
Notify	Select notify view name, if Notify is checked

Table 14-16 SNMP Group Add Fields

14.4.3 Community

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

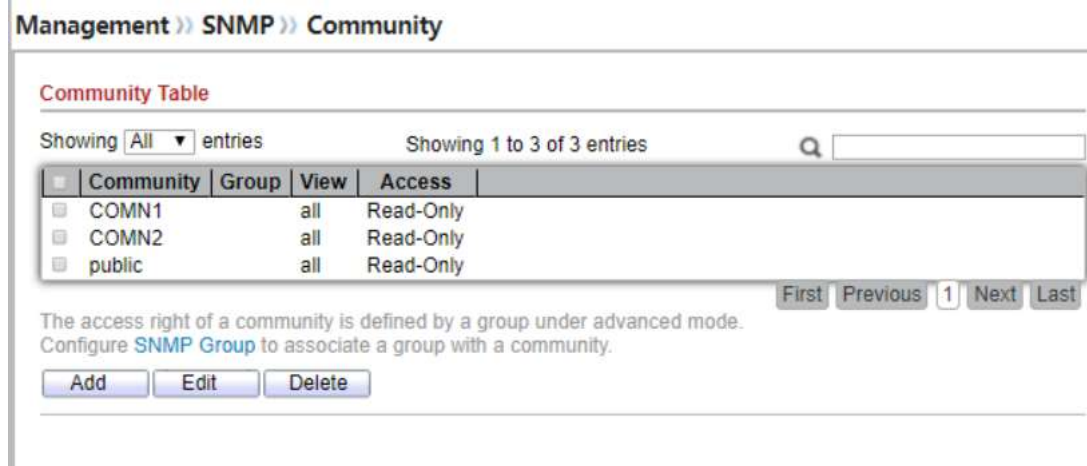
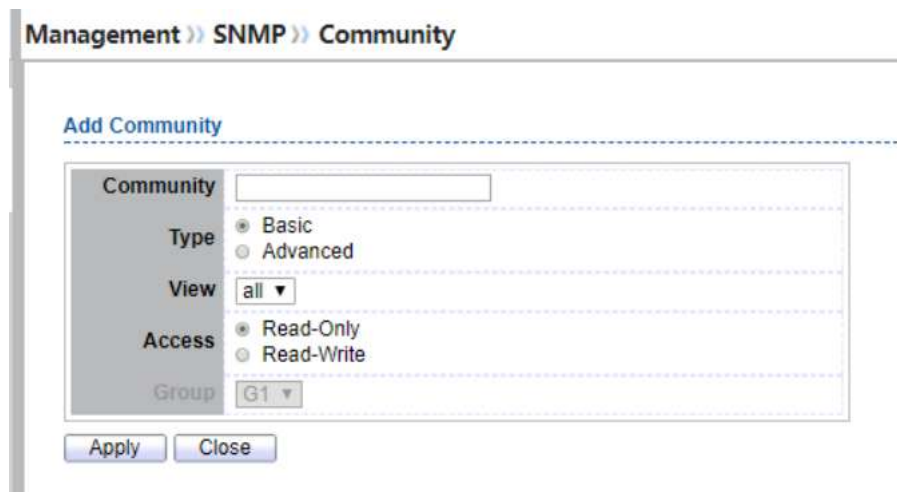


Figure 14-17 SNMP Community Table Page

Field	Description
Community	The SNMP community name. Its maximum length is 20 characters.
Community Mode	SNMP Community mode • Basic: snmp community specifies view and access right. • Advanced: snmp community specifies group.
Group Name	Specify the SNMP group configured by the command snmp group to define the object available to the community.
View Name	Specify the SNMP view to define the object available to the community.
Access Right	SNMP access mode • Read-Only: Read only. • Read-Wrtie: Read and write.

Table 14-17 SNMP Community Table Fields



Management » SNMP » Community

Add Community

Community

Type ☒ Basic ☐ Advanced

View

Access ☒ Read-Only ☐ Read-Write

Group

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 • Basic: SNMP community specifies view and access right. • Advanced: SNMP community specifies group.
View	Specify the SNMP view to define the object available to the community.
Access	SNMP access mode • Read-Only: Read only. • Read-Write: Read and write.
Group	Specify the SNMP group configured by user to define the object available to the community.

Table 14-18 SNMP Community Add Fields



Management » SNMP » Community

Edit Community

Community

Type ☒ Basic ☐ Advanced

View

Access ☒ Read-Only ☐ Read-Write

Group

Apply Close

Figure 14-19 SNMP Community Edit Page

Field	Description
Community	The Edit SNMP community name
Type	SNMP Community mode • Basic: SNMP community specifies view and access right. • Advanced: SNMP community specifies group.
View	Specify the SNMP view to define the object available to the community.
Access	SNMP access mode • Read-Only: Read only. • Read-Write: Read and write.
Group	Specify the SNMP group configured by user to define the object available to the community.

Table 14-19 SNMP Community Edit Fields

14.4.4 User

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

User Table

Showing All entries Showing 1 to 3 of 3 entries

☐	User	Group	Security Level	Authentication Method	Privacy Method
☐	user1	g1	Authentication and Privacy	SHA	DES
☐	user2	g2	Authentication	MD5	None
☐	user3	g3	No Security	None	None

Configure **SNMP Group** to associate an SNMPv3 group with an SNMPv3 user.

First Previous 1 Next Last

Add Edit Delete

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 • No Security : Specify that no packet authentication is performed. • Authentication: Specify that no packet authentication without encryption is performed. • Authentication and Privacy: Specify that no packet authentication with encryption is performed.
Authentication Method	Authentication Protocol which is available when Privilege Mode is Authentication or Authentication and Privacy . • None: No authentication required. • MD5: Specify the HMAC-MD5-96 authentication protocol. • SHA: Specify the HMAC-SHA-96 authentication protocol.

Encryption Protocol

- Privacy Method**
- **None:** No privacy required.
 - **DES:** DES algorithm

Table 14-20 SNMP User Table Fields

Add User

User

Group

Security Level

☒ No Security

☐ Authentication

☐ Authentication and Privacy

Authentication

Method

☒ None

☐ MD5

☐ SHA

Password

Privacy

Method

☒ None

☐ DES

Password

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 • No Security : Specify that no packet authentication is performed. • Authentication: Specify that no packet authentication without encryption is performed. • Authentication and Privacy: Specify that no packet authentication with encryption is performed.
Authentication	
Method	Authentication Protocol which is available when Privilege Mode is Authentication or Authentication and Privacy . • None: No authentication required. • MD5: Specify the HMAC-MD5-96 authentication protocol.

	• SHA: Specify the HMAC-SHA-96 authentication protocol
Password	The authentication password, The number of character range is 8 to 32 characters.
Privacy	
	Encryption Protocol
Method	• 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

Field	Description
User	Edit User name
Group	Specify the SNMP group to which the SNMP user belongs.
Security Level	SNMP privilege mode No Security : Specify that no packet authentication is performed. Authentication: Specify that no packet authentication without encryption is performed. Authentication and Privacy: Specify that no packet authentication with encryption is performed.
Authentication	
	Authentication Protocol which is available when Privilege Mode is Authentication or Authentication and Privacy.
Method	• None: No authentication required. • MD5: Specify the HMAC-MD5-96 authentication protocol. • SHA: Specify the HMAC-SHA-96 authentication protocol.
Password	The authentication password, The number of character range is 8 to 32 characters.
Privacy	

Method	Encryption Protocol
	None: No privacy required. DES: DES algorithm
Password	The privacy password, The number of character range is 8 to 64 characters.

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. • Authentication: Specify that no packet authentication without encryption is performed. • Authentication and Privacy: Specify that no packet authentication with encryption is performed.
Authentication	
Method	Authentication Protocol which is available when Privilege Mode is Authentication or Authentication and Privacy . • None: No authentication required. • MD5: Specify the HMAC-MD5-96 authentication protocol. • SHA: Specify the HMAC-SHA-96 authentication protocol.

Password	The authentication password, The number of character range is 8 to 32 characters.
Privacy	
Method	Encryption Protocol • None: No privacy required. • DES: DES algorithm
Password	The privacy password, The number of character range is 8 to 64 characters.

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**.

Management >> SNMP >> Engine ID

Local Engine ID

Engine ID ☐ User Defined

80006a920300e04c000000 (10 - 64 Hexadecimal Characters)

Apply

Remote Engine ID Table

Showing All entries Showing 1 to 2 of 2 entries

Server Address	Engine ID
192.168.1.100	112223FDED FE
192.168.1.99	00004DADDDDDDD

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 range 10 to 64 hexadecimal characters, and the hexadecimal number must be divided by 2.

Table 14-23 SNMP Engine ID Fields

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 range 10 to 64 hexadecimal characters, and the hexadecimal number must be divided by 2.

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**.

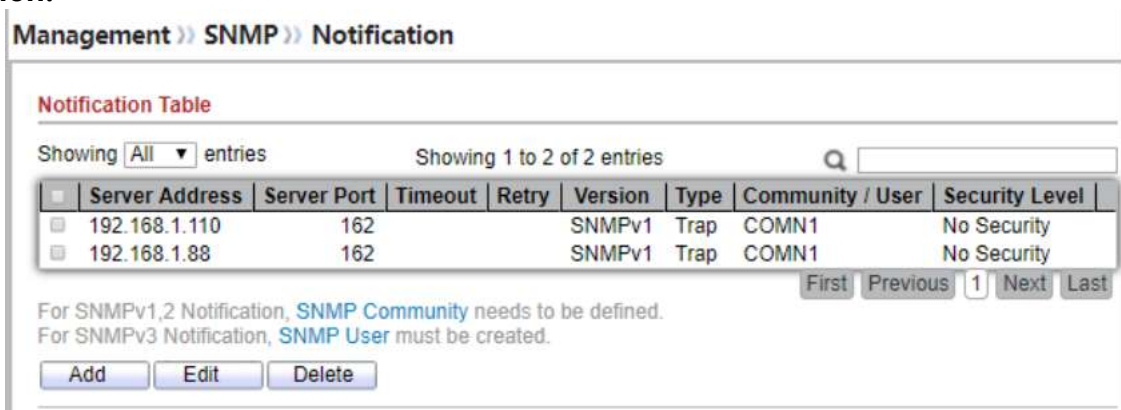


Figure 14-27 SNMP Notification Table Page

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 • SNMPv1: SNMP Version 1 notification. • SNMPv2: SNMP Version 2 notification. • SNMPv3: SNMP Version 3 notification.
Type	Notification Type • Trap: Send SNMP traps to the host. • Inform: Send SNMP informs to the host.
Community/User	SNMP community/user name for notification. If version is SNMPv3 the name is user name, else is community name
UDP Port	Specify the UDP port number.
Timeout	Specify the SNMP informs timeout
Security Level	SNMP trap packet security level • No Security: Specify that no packet authentication is performed. • Authentication: Specify that no packet authentication without encryption is performed. • Authentication and Privacy: Specify that no packet authentication with encryption is performed.

Table 14-27 SNMP Notification Table Fields

Management >> SNMP >> Notification

Add Notification

Address Type	☒ Hostname ☐ IPv4 ☐ IPv6
Server Address	
Version	☒ SNMPv1 ☐ SNMPv2 ☐ SNMPv3
Type	☒ Trap ☐ Inform
Community / User	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)

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 • SNMPv1: SNMP Version 1 notification. • SNMPv2: SNMP Version 2 notification. • SNMPv3: SNMP Version 3 notification.
Type	Notification Type • Trap: Send SNMP traps to the host. • Inform: Send SNMP informs to the host.(version 1 have no inform)
Community/User	SNMP community/user name for notification. If version is SNMPv3 the name is user name, else is community name
Security Level	SNMP notification packet security level, the security level must less than or equal to the community/user name • No Security: Specify that no packet authentication is performed. • Authentication: Specify that no packet authentication without encryption is performed. • Authentication and Privacy: Specify that no packet authentication with encryption is performed.
Server Port	Recipients server UDP port number, if “use default” checked the value is 162, else user configure
Timeout	Specify the SNMP informs timeout, if “use default” checked the value is 15, else user configure
Retry	Specify the SNMP informs retry count, if “use default” checked the value is 3, else user configure

Table 14-28 SNMP Notification Add Fields

Management » SNMP » Notification

Edit Notification

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)

Apply Close

Figure 14-29 SNMP Notification Edit Page

Field	Description
Server Address	Edit SNMP notify recipients address.
Version	Specify SNMP notification version • SNMPv1: SNMP Version 1 notification. • SNMPv2: SNMP Version 2 notification. • SNMPv3: SNMP Version 3 notification.
Type	Notification Type • Trap: Send SNMP traps to the host. • Inform: Send SNMP informs to the host.(version 1 have no inform)
Community/User	SNMP community/user name for notification. If version is SNMPv3 the name is user name, else is community name
Security Level	SNMP notification packet security level, the security level must less than or equal to the community/user name • No Security: Specify that no packet authentication is performed. • Authentication: Specify that no packet authentication without encryption is performed. • Authentication and Privacy: Specify that no packet authentication with encryption is performed.
Server Port	Recipients server UDP port number, if “use default” checked the value is 162, else user configure
Timeout	Specify the SNMP informs timeout, if “use default” checked the value is 15, else user configure
Retry	Specify the SNMP informs retry count, if “use default” checked the value is 3, else user configure

Table 14-29 SNMP Notification Edit Fields

14.5 RMON

14.5.1 Statistics

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

Entry	Port	Bytes Received	Drop Events	Packets Received	Broadcast Packets	Multicast Packets	CRC & Align Errors	Undersize Packages	Oversize Packages
1	GE1	0	0	0	0	0	0	0	0
2	GE2	0	0	0	0	0	0	0	0
3	GE3	0	0	0	0	0	0	0	0
4	GE4	0	0	0	0	0	0	0	0
5	GE5	0	0	0	0	0	0	0	0
6	GE6	0	0	0	0	0	0	0	0
7	GE7	396656	0	2488	113	454	0	0	0
8	GE8	0	0	0	0	0	0	0	0
9	GE9	0	0	0	0	0	0	0	0
10	GE10	0	0	0	0	0	0	0	0
11	LAG1	0	0	0	0	0	0	0	0
12	LAG2	0	0	0	0	0	0	0	0
13	LAG3	0	0	0	0	0	0	0	0
14	LAG4	0	0	0	0	0	0	0	0
15	LAG5	0	0	0	0	0	0	0	0
16	LAG6	0	0	0	0	0	0	0	0
17	LAG7	0	0	0	0	0	0	0	0
18	LAG8	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.
Packets Received	Number of packets received, including bad packets, Multicast packets, and Broadcast packets.
Broadcast Packets	Number of good Broadcast packets received. This number does not include Multicast packets.
Multicast Packets	Number of good Multicast packets received.
CRC & Align Errors	Number of CRC and Align errors that have occurred.
Undersize Packages	Number of undersized packets (less than 64 octets) received.
Oversize Packages	Number of oversized packets (over 1518 octets) received.
Fragments	Number of fragments (packets with less than 64 octets, excluding framing bits, but including FCS octets) received.
Jabbers	Number of received packets that were longer than 1632 octets. This number excludes frame bits, but includes FCS octets that had either a bad FCS (Frame Check Sequence) with an integral number of octets (FCS Error) or a bad FCS with a non-integral octet (Alignment Error) number. A Jabber packet is defined as an Ethernet frame that satisfies the following criteria:

- Packet data length is greater than MRU.
- Packet has an invalid CRC.
- RX error event has not been detected.

Collision	Number of collisions received. If Jumbo Frames are enabled, the threshold of Jabber Frames is raised to the maximum size of Jumbo Frames.
Frames of 64 Bytes	Number of frames, containing 64 bytes that were received.
Frames of 65 to 127 Bytes	Number of frames, containing 65 to 127 bytes that were received.
Frames of 128 to 255 Bytes	Number of frames, containing 128 to 255 bytes that were received.
Frames of 256 to 511 Bytes	Number of frames, containing 256 to 511 bytes that were received.
Frames of 512 to 1024 Bytes	Number of frames, containing 512 to 1023 bytes that were received.
Frames Greater than 1024 Bytes	Number of frames, containing 1024 to 1518 bytes that were received.
Clear	Clear the statistics for the selected ports
View	View the statistics on the specified port.

Table 14-30: RMON Statistics fields.

Management >> RMON >> Statistics

View Port Statistics

Port	GE1
Refresh Rate	☒ None ☐ 5 sec ☐ 10 sec ☐ 30 sec
Received Bytes (Octets)	0
Drop Events	0
Received Packets	0
Broadcast Packets Received	0
Multicast Packets Received	0
CRC & Align Errors	0
Undersize Packets	0
Oversize Packets	0
Fragments	0
Jabbers	0
Collisions	0
Frames of 64 Bytes	0
Frames of 65 to 127 Bytes	0
Frames of 128 to 255 Bytes	0
Frames of 256 to 511 Bytes	0
Frames Greater than 1024 Bytes	0

Figure 14-31: View RMON Statistics page.

14.5.2 History

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

Management >> RMON >> History

History Table

Showing **All** entries Showing 1 to 2 of 2 entries

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

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

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.

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 buttons.

Management >> RMON >> History

Edit History

Entry	2
Port	GE1 ▼
Max Sample	50 (1 - 50, default 50)
Interval	1800 (1 - 3600, default 1800)
Owner	CERR

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.

Management >> RMON >> History

View History

Entry: 1

Showing All ▼ entries Showing 0 to 0 of 0 entries

Sample No.	Drop Events	Bytes Received	Packets Received	Broadcast Packets	Multicast Packets	CRC & Align Errors	Undersize Packets	Oversize Packets
0 results found.								

Close

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: • 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**.

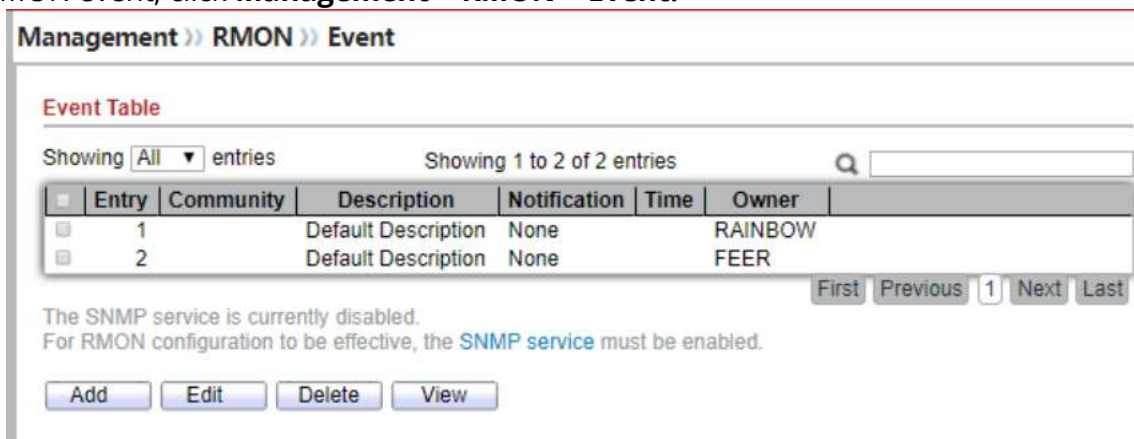


Figure 14-36: RMON Event page.

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:
	• 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.

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: • 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.

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: • 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.

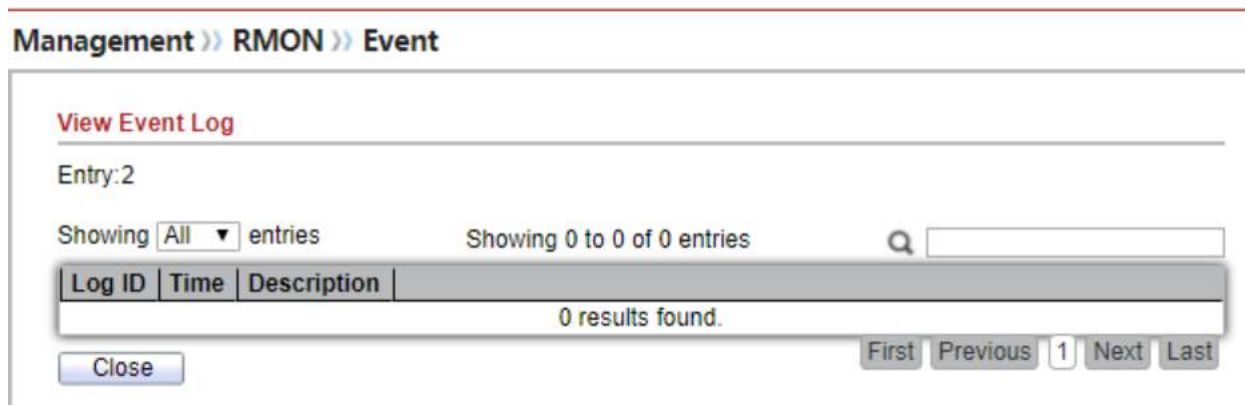


Figure 14-39: RMON Event Log page.

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**.

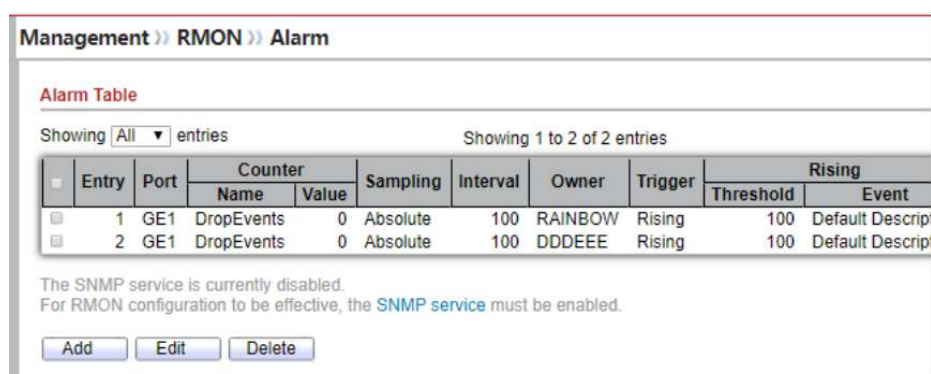


Figure 14-40: RMON Alarm page.

Field	Description
Port	The port configuration for the RMON alarm.
Counter	The counter for sampling • DropEvents (Drop Event): Total number of events received in which the packets were dropped. • Octes (Received Bytes): Octets. • Pkts (Received Packets): Number of packets. • BroadcastPkts (Broadcast Packets Received): Broadcast packets. • MulticastPkts (Multicast Packets Received): Multicast packets. • CRCAlignError (CRC and Align Error): CRC alignment error. • UndersizePkts (Undersize Packets): Number of undersized packets. • OversizePkts (Oversize Packets): Number of oversized packets. • Fragments (Fragments): Total number of packet fragment. • Jabbers (Jabbers): Total number of packet jabber. • Collisions (Collisions): Collision. • Pkts64Octetes (Frames of 64 Bytes): Number of packets size 64 octets. • Pkts65to127Octetes (Frames of 65 to 127 Bytes): Number of packets size 65 to 127 octets. • Pkts128to255Octetes (Frames of 128 to 255 Bytes): Number of packets size 128 to 255 octets. • Pkts256to511Octetes (Frames of 256 to 511 Bytes): Number of packets size 256 to 511 octets. • Pkts512to1023Octetes (Frames of 512 to 1023 Bytes): Number of packets size 512 to 1023 octets. • Pkts1024to1518Octetes (Frames Greater than 1024 Bytes): Number of packets size 1024 to 1518 octets.
Sampling	The sampling type including: • Absolute: The selected variable value is compared directly with the thresholds at the end of the sampling interval. • Delta: The selected variable value of the last sample is subtracted from the current value and the difference is compared with the thresholds.
Interval	The number of seconds for each sample.
Owner	The owner for the alarm entry.
Trigger	The type of event triggering.
Rising Threshold	The threshold for firing rising event.
Rising Event	The rising event when alarm was fired.
Falling Threshold	The threshold for firing falling event.
Falling Event	The falling event when alarm was fired.

Table 14-40: RMON Alarm fields.

Add Alarm

Entry	3
Port	GE1 ▼
Counter	Drop Events ▼
Sampling	☒ Absolute ☐ Delta
Interval	100 Sec (1 - 2147483647, default 100)
Owner	
Trigger	☒ Rising ☐ Falling ☐ Rising and Falling
Rising	
Threshold	100 (0 - 2147483647, default 100)
Event	1 - Default Description ▼
Falling	
Threshold	20 (0 - 2147483647, default 20)
Event	1 - Default Description ▼

Apply Close

Figure 14-41: RMON Alarm Add page.

Field	Description
Port	Specify the port for sampling
Counter	Specify the counter for sampling • Drop Event: Total number of events received in which the packets were dropped. • Received Bytes (Octets): Octets. • Received Packets: Number of packets. • Broadcast Packets Received: Broadcast packets. • Multicast Packets Received: Multicast packets. • CRC and Align Error: CRC alignment error. • Undersize Packets: Number of undersized packets. • Oversize Packets: Number of oversized packets.
	• Fragments: Total number of packet fragment. • Jabbers: Total number of packet jabber. • Collisions: Collision. • Frames of 64 Bytes: Number of packets size 64 octets. • Frames of 65 to 127 Bytes: Number of packets size 65 to 127 octets. • Frames of 128 to 255 Bytes: Number of packets size 128 to 255 octets. • Frames of 256 to 511 Bytes: Number of packets size 256 to 511 octets. • Frames of 512 to 1023 Bytes: Number of packets size 512 to 1023 octets. • Frames Greater than 1024 Bytes: Number of packets size 1024 to 1518 octets.
Sampling	Specify the sampling type. • Absolute: The selected variable value is compared directly with the thresholds at the end of the sampling interval. • Delta: The selected variable value of the last sample is subtracted from the current value and the difference is compared with the thresholds.

Interval	Specify the sampling interval.
Owner	Specify the owner for the sampling.
Trigger	Specify the type for the alarm trigger.
Rising Threshold	Specify the threshold for firing rising event.
Rising Event	Specify the index of rising event when alarm was fired.
Falling Threshold	Specify the threshold for firing falling event.
Falling Event	Specify the index of falling event when alarm was fired.

Table 14-41: RMON Alarm Add fields.

Management » RMON » Alarm

Edit Alarm

Entry	2
Port	GE1 ▼
Counter	Drop Events ▼
Sampling	☒ Absolute ☐ Delta
Interval	100 Sec (1 - 2147483647, default 100)
Owner	DDDEEE
Trigger	☒ Rising ☐ Falling ☐ Rising and Falling
Rising	
Threshold	100 (0 - 2147483647, default 100)
Event	1 - Default Description ▼
Falling	
Threshold	20 (0 - 2147483647, default 20)
Event	1 - Default Description ▼

Apply Close

Figure 14-42: RMON Alarm Edit page.

Field	Description
Port	Specify the port for sampling
Counter	Specify the counter for sampling • Drop Event: Total number of events received in which the packets were dropped. • Received Bytes (Octets): Octets. • Received Packets: Number of packets. • Broadcast Packets Received: Broadcast packets. • Multicast Packets Received: Multicast packets. • CRC and Align Error: CRC alignment error. • Undersize Packets: Number of undersized packets. • Oversize Packets: Number of oversized packets.
	• Fragments: Total number of packet fragment. • Jabbers: Total number of packet jabber. • Collisions: Collision. • Frames of 64 Bytes: Number of packets size 64 octets. • Frames of 65 to 127 Bytes: Number of packets size 65 to 127 octets. • Frames of 128 to 255 Bytes: Number of packets size 128 to 255 octets. • Frames of 256 to 511 Bytes: Number of packets size 256 to 511 octets. • Frames of 512 to 1023 Bytes: Number of packets size 512 to 1023 octets. • Frames Greater than 1024 Bytes: Number of packets size 1024 to 1518 octets.
Sampling	Specify the sampling type. • Absolute: The selected variable value is compared directly with the thresholds at the end of the sampling interval. • Delta: The selected variable value of the last sample is subtracted from the current value and the difference is compared with the thresholds.
Interval	Specify the sampling interval.
Owner	Specify the owner for the sampling.
Trigger	Specify the type for the alarm trigger.
Rising Threshold	Specify the threshold for firing rising event.
Rising Event	Specify the index of rising event when alarm was fired.
Falling Threshold	Specify the threshold for firing falling event.
Falling Event	Specify the index of falling event when alarm was fired.

Table 14-42: RMON Alarm Edit fields.

15. PoE Setting

15.1 PoE Port Setting

To configure and display the PoE Setting, click PoE Setting> PoE Port Setting.

POE Setting >> POE Port Setting

System info

System Power(W)	0
System Temperature(C)	25
Refresh Rate	☐ None ☐ 5 sec ☒ 10 sec ☐ 30 sec

Port Setting Table

Entry	Port	PortEnable	Status	Type	Level	Actual Power(mW)	Voltage(V)	Current(mA)
☐	1	GE1	Enabled	Off	N/A	N/A	N/A	N/A
☐	2	GE2	Enabled	Off	N/A	N/A	N/A	N/A
☐	3	GE3	Enabled	Off	N/A	N/A	N/A	N/A
☐	4	GE4	Enabled	Off	N/A	N/A	N/A	N/A
☐	5	GE5	Enabled	Off	N/A	N/A	N/A	N/A
☐	6	GE6	Enabled	Off	N/A	N/A	N/A	N/A
☐	7	GE7	Enabled	Off	N/A	N/A	N/A	N/A
☐	8	GE8	Enabled	Off	N/A	N/A	N/A	N/A

Edit

Figure 15-43: System Info and Port Setting Table

To select the one port you want to configure, and then Click “Edit” button on the table title to edit

POE Setting >> POE Port Setting

Edit Port Setting

Port: GE1

PortEnable: ☒ Enable ☐ Disable

Apply Close

15.2 PoE Port Timer Setting

To configure and display the PoE Timer Setting, click PoE Setting> PoE Timer Setting

POE Setting >> POE Port Timer Setting

Port: GE1

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

Apply

The information in this document is subject to change without notice. Fiberroad has made all effects to ensure the accuracy of the information, but all information in this document does not constitute any kind of warranty. If you have any questions please feel free to contact to us.

Fiberroad Technology Co., Limited

www.fiberroad.com

Sales Support: sales@fiberroad.com

Technical Support: support@fiberroad.com

Service Support: service@fiberroad.com

