

PIXE L3 8T 4S R  
Industrial Layer 3  
10 Gbps Ethernet Switch  
Web User Manual

This page left blank intentionally

## About This Manual

### Introduction

This document chapter includes an introduction to the Case Communications L3 WebGUI Network Management, which also contains Case Communications 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©2025 Case Communications 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 Case Communications.

Information provided by Case Communications is believed to be accurate and reliable. However, no responsibility is assumed by Case Communications 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 Case Communications.

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

### Trademarks

Case Communications' 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

Revision History Version	Date	Author	Reasons of Change	Section(s) Affected
1.0	11.2. 25	Tech Pubs	Initial Release	All

This page left blank intentionally



## INDEX

<b>1.</b>	<b>Introduction</b>	<b>1-1</b>
1.1	About Web- Gui Management	1-1
1.2	Preparing for Web Management	1-1
<b>2</b>	<b>Status</b>	<b>2-1</b>
2.1	System Information	2-1
2.2.	Logging Message	2-2
2.3	Port	2-3
2.3.1	Statistics	2-3
2.3.2	Error Disabled	2-5
2.3.3	Bandwidth Utilisation	2-6
2.4	Link Aggregation Display	2-7
2.5	MAC Address Table	2-8
<b>3.</b>	<b>Network</b>	<b>3-1</b>
3.1	IP Address	3-1
3.2	System Time	3-2
<b>4</b>	<b>Port</b>	<b>4-1</b>
4.1	Port Setting	4-1
4.2	Error Disabled	4-3
4.3	Link Aggregation	4-4
4.3.1	Group	4-4
4.3.2	Port Setting	4-5
4.3.3	LACP	4-7
4.4	EEE	4-8
4.5	Jumbo Frame	4-9
<b>5</b>	<b>VLAN</b>	<b>5-1</b>
5.1	VLAN	5-1
5.2.1	Create VLAN	5-1
5.2.2	VLAN Configuration	5-2
5.2.3	Membership	5-2
5.2.4	Port Setting	5-4
5.2	Voice VLAN	5-6
5.2.1	Displaying The Voice VLAN	5-6
5.2.2	Voice OUI	5-7
5.3	Protocol VLAN	5-9
5.3.1	Protocol Group	5-9
5.3.2	Group Binding	5-10
5.4	MAC VLAN	5-11
5.6.1	MAC Group	5-11
5.6.2	Group Binding	5-12
5.5	Surveillance VLAN	5-13
5.5.1	Property	5-13
5.5.2	Surveillance OUI (Organisation Unique Identifier)	5-15

5.6	GVRP	5-16
5.6.1	Displaying GVRP	5-16
5.6.2	GVRP VLAN Membership	5-17
5.6.3	GVRP Port Statistics	5-18
<b>6</b>	<b>MAC Address Table</b>	<b>6-1</b>
6.1	Dynamic Address	6-1
6.2	Static Address	6-1
6.3	Filtering Address	6-2
<b>7</b>	<b>STP</b>	<b>7-1</b>
7.1	Property	7-1
7.2	Port Setting	7-2
7.3	MST Instance	7-4
7.4	MST Port Setting	7-6
7.5	Statistics	7-7
<b>8</b>	<b>Discovery</b>	<b>8-1</b>
8.1	LLDP	8-1
8.1.1	LLDP Property Settings	8-1
8.1.2	MED Network Policy	8-3
8.1.3	LLDP MED Port <b>Setting</b>	8-4
8.1.4	Packet View	8-5
8.1.5	LLDP Local Device Information	8-7
8.1.6	Display LLDP Remote Device Neighbour	8-10
<b>9</b>	<b>Multicast</b>	<b>9-1</b>
9.1	General Multicast IGMP and MLD	9-1
9.1.1	Displaying the Multicast Pages	9-1
9.1.2	Displaying Multicast Group Address	9-2
9.1.3	Router Port	9-4
9.1.4	Forward All	9-5
9.1.5	Throttling	9-7
9.1.6	Filtering Profile	9-8
9.1.7	Filtering Binding	9-10
9.2	IGMP Snooping	9-12
9.2.1	How to Display IGMP Snooping	9-12
9.2.2	IGMP Snooping Querier	9-14
9.2.3	IGMP Snooping Statistics	9-15
9.3	MLD Snooping	9-15
9.3.1	Display MLD Snooping and VLAN Setting	9-16
9.3.2	MLD Snooping Statistics	9-18
9.4	MVR	9-19
9.4.1	Displaying Multicast MVR Property Settings	9-19
9.4.2	MVR Port Settings	9-20
9.4.3	Multicast MVR Group Address	9-21

<b>10</b>	<b>Security</b>	<b>10-1</b>
10.1	RADIUS	10-1
10.2	TACACS+	10-3
10.3	AAA	10-4
10.3.1	Method List	10-4
10.3.2	Login Authentication	10-6
10.4	Management Access	10-7
10.4.1	Management VLAN	10-7
10.4.2	Management Services	10-7
10.3.3	Management ACL	10-8
10.4.4	Management Services	10-9
10.4.5	Management ACL	10-10
10.4.6	Management ACE	10-10
10.5	Authentication Manager	10-12
10.5.1	Property	10-12
10.5.2	Port Setting	10-15
10.5.3	MAC-Based Local Account	10-17
10.5.4	Sessions	10-20
10.6	Port Security	10-22
10.7	The Protected Port	10-23
10.8	Storm Control	10-24
10.9	DoS	10-26
10.10	Dynamic ARP Inspection	10-28
10.11.1	Display Security Property Page	10-28
10.11.2	Statistics	10-30
10.11	DHCP Snooping	10-31
10.11.1	Displaying DHCP Security Page	10-31
10.11.2	Displaying DHCP Statistics	10-32
10.11.3	Option 82 Property	10-32
10.11.4	Option 82 Client ID	10-34
10.12	IP Source Guard	10-35
10.12.1	Port Setting	10-35
10.12.2	IMPV Binding	10-36
<b>11</b>	<b>ACL</b>	<b>11-1</b>
11.1	MAC ACL	11-1
11.2	MAC ACE	11-1
11.3	IPv4 ACL	11-3
11.4	IPv4 ACE	11-4
11.5	IPv6 ACL	11-7
11.6	IPv6 ACE	11-8
11.7	ACL Binding	11-11

<b>12</b>	<b>QoS</b>	<b>12-1</b>
12.1	General	12-1
12.1.1	Displaying the property for QoS	12-1
12.1.2	Queue Scheduling	12-3
12.2.3	CoS Mapping	12-4
12.2.4	DSCP Mapping	12-5
12.1.2	IP Precedence Mapping	12-6
12.2	Rate Limiting	12-7
12.2.1	Ingress/Egress Port	12-7
12.2.2	Egress Queue	12-8
<b>13</b>	<b>Diagnostics</b>	<b>13-1</b>
13.1	Logging	13-1
13.1.1	Enabling / Disabling Logging	13-1
13.1.2	Remote Server	13-2
13.1.3	Displaying UDLD Property	13-6
13.1.4	Display UDLD Neighbour	13-8
<b>14</b>	<b>Management</b>	<b>14-1</b>
14.1	User Accounts	14-1
14.2	Firmware	14-2
14.2.1	Upgrade / Backup	14-2
14.2.2	Active Image	14-4
14.3	Configuration	14-6
14.3.1	Upgrade / Backup	14-6
14.3.2	Display The Saved Configuration	14-8
14.4	SNMP	14-9
14.4.1	Display the SNMP View Table	14-9
14.4.2	SNMP Group	14-9
14.4.3	SNMP Community	14-11
14.4.4	Configuring and Displaying SNMP Users	14-13
14.4.5	Engine ID	14-16
14.4.6	Trap Event	14-18
14.4.7	Configure Hosts to Receive Notifications	14-18
14.5	RMON	14-21
14.5.1	Statistics	14-21
14.5.2	History	14-22
14.5.3	RMON Events	14-24
14.5.4	RMON Alarms	14-26
<b>15</b>	<b>PoE Settings</b>	<b>15-1</b>
15.1	PoE Port Setting	15-1
15.2	PoE Port Timer Setting	15-1

<b>16</b>	<b>Routing</b>	<b>16-1</b>
16.1	IPV4 Management and Interface	16-1
16.1.1	IPv4 Interface Table	16-1
16.1.2	IPv4 Routes	16-1
16.1.3	ARP Interface	16-2
16.2	IPv6 management and interface	16-3
16.2.1	IPv6 Interfaces	16-3
16.2.2	IPv6 Address	16-3
16.2.3	IPv6 Routes	16-4
16.2.4	IPv6 Neighbours	16-5
16.3	RIP Route Management	16-5
16.4	OSPF Routing Management	16-6
16.5	VRRP Management	16-7
<b>17</b>	<b>ERPS</b>	<b>17-1</b>
17.1	Feature Configuration	17-2
17.2	ERPS Instances	17-2

This page left blank intentionally

## **1. Introduction**

### **1.1. About Web-GUI Management**

There is an embedded HTML web site residing in flash memory on the 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 Case Communications Network Switch default management IP Addresses, subnet mask, username and password are listed as below:

❖ IP Address: 192.168.16.1

❖ HTTP service: Enable

❖ User Name: root

❖ Password: case



Username:

Password:

Language:

Login

This page left blank intentionally



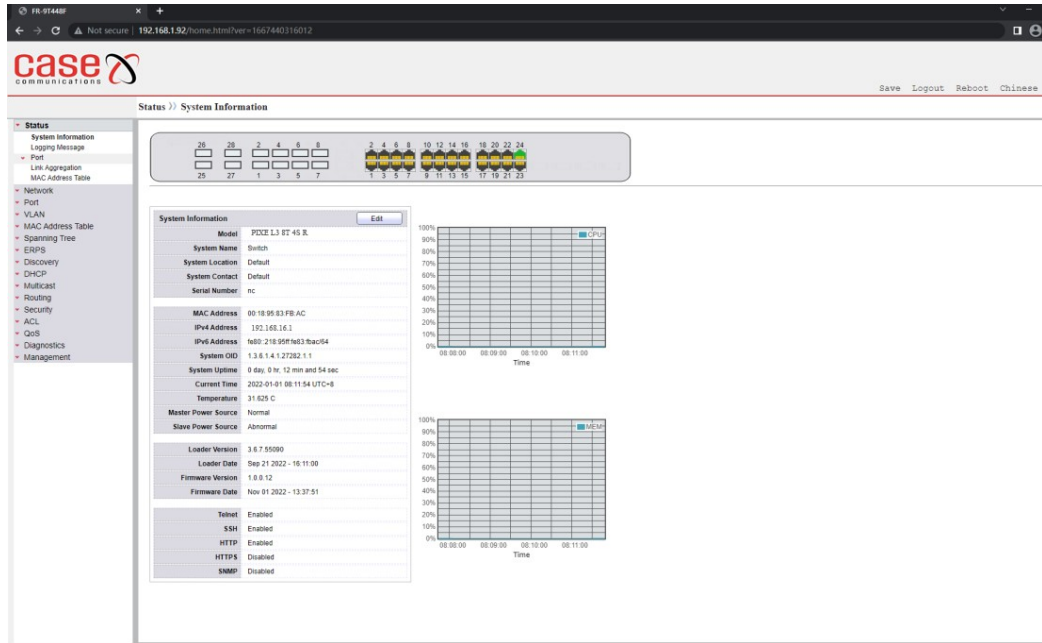
## 2. Status

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 the switch panel, CPU Utilisation , Memory Utilisation and other system current information. It also allows users to edit some system information.



<b>MAC Address</b>	Base MAC address of the switch
<b>IPv4 Address</b>	Current system IPv4 address
<b>IPv6 Address</b>	Current system IPv6 address
<b>System OID</b>	SNMP system object ID
<b>System Uptime</b>	Total elapsed time from booting
<b>Current Time</b>	Current system time
<b>Loader Version</b>	Boot loader image version
<b>Loader Date</b>	Boot loader image build date
<b>Firmware Version</b>	Current running firmware image version
<b>Firmware Date</b>	Current running firmware image build date
<b>Telnet</b>	Current Telnet service enable/disable state
<b>SSH</b>	Current SSH service enable/disable state
<b>HTTP</b>	Current HTTP service enable/disable state
<b>HTTPS</b>	Current HTTPS service enable/disable state
<b>SNMP</b>	Current SNMP service enable/disable state

**Table 2-1 Current System Information**

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

**Figure 2.2: System> Edit the System Information**

**Edit System Information**

System Name	Switch
System Location	Default
System Contact	Default

Apply Close

**Table 2.2 System Information Field**

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

## 2.2. Logging Message

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

**Logging Message Table**

Viewing **RAM**

Showing **All** entries Showing 1 to 3 of 3 entries

Log ID	Time	Severity	Description
1	Jan 01 2020 08:01:12	notice	AAA-0-CONNECT: New http connection for user admin, source 192.168.1.100 ACCEPTED
2	Jan 01 2020 08:00:07	notice	PORT-5-LINK_UP: Interface GigabitEthernet8 link up
3	Jan 01 2020 00:00:05	notice	SYSTEM-5-COLDSTART: Cold startup

Clear Refresh

First Previous 1 Next Last

**Figure 2-3/ Status 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: <b>RAM:</b> Show the logging messages stored on the RAM. <b>Flash:</b> Show the logging messages stored on the Flash.
Clear	Clear the logging messages.
Refresh	Refresh the logging messages.

**Table 2-4: Logging Message buttons.**

## 2.3 Port

The Port configuration page displays port summary and status information.

### 2.3.1 Statistics

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

This page displays standard counters on network traffic from the Interfaces, Ethernet-like and RMON MIB. Interfaces and Ethernet-like counters display errors on the traffic passing through each port.

RMON counters provide a total count of different frame types and sizes passing **through each port**.

The “Clear” button will clear MIB counter of current selected port.

Port	GE1 ▼
MIB Counter	<input checked="" type="radio"/> All <input type="radio"/> Interface <input type="radio"/> Etherlike <input type="radio"/> RMON
Refresh Rate	<input type="radio"/> None <input type="radio"/> 5 sec <input checked="" type="radio"/> 10 sec <input type="radio"/> 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 <ul style="list-style-type: none"> <li><b>All:</b> All counters.</li> <li><b>Interface:</b> Interface related MIB counters</li> <li><b>Etherlike:</b> Ethernet-like related MIB counters</li> <li><b>RMON:</b> RMON related MIB counters</li> </ul>
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 the port error disabled, click Status > Port > Error Disabled.

Error Disabled Table

	Port	Reason	Time Left (sec)
<input type="checkbox"/>	GE1	---	---
<input type="checkbox"/>	GE2	---	---
<input type="checkbox"/>	GE3	---	---
<input type="checkbox"/>	GE4	---	---
<input type="checkbox"/>	GE5	---	---
<input type="checkbox"/>	GE6	---	---
<input type="checkbox"/>	GE7	---	---
<input type="checkbox"/>	GE8	---	---
<input type="checkbox"/>	GE9	---	---
<input type="checkbox"/>	GE10	---	---
<input type="checkbox"/>	LAG1	---	---
<input type="checkbox"/>	LAG2	---	---
<input type="checkbox"/>	LAG3	---	---
<input type="checkbox"/>	LAG4	---	---
<input type="checkbox"/>	LAG5	---	---
<input type="checkbox"/>	LAG6	---	---
<input type="checkbox"/>	LAG7	---	---
<input type="checkbox"/>	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 <ul style="list-style-type: none"><li>UDLD</li><li>Self Loop</li><li>Broadcast Flood</li><li>Unknown Multicast Flood</li><li>Unicast Flood</li><li>ACL</li><li>Port Security Violation</li><li>DHCP rate limit</li><li>ARP rate limit</li></ul>
Time Left (sec)	The time left in second for the error recovery.

Table 2-6: Error Disabled Status fields.

### 2.3.3 Bandwidth Utilisation

To display the Bandwidth Utilisation web page, click Status > Port > Bandwidth Utilisation  
 This page allow user to browse ports' bandwidth Utilisation in real time. This page will refresh automatically in every refresh period

Status> Port> Bandwidth Utilisation

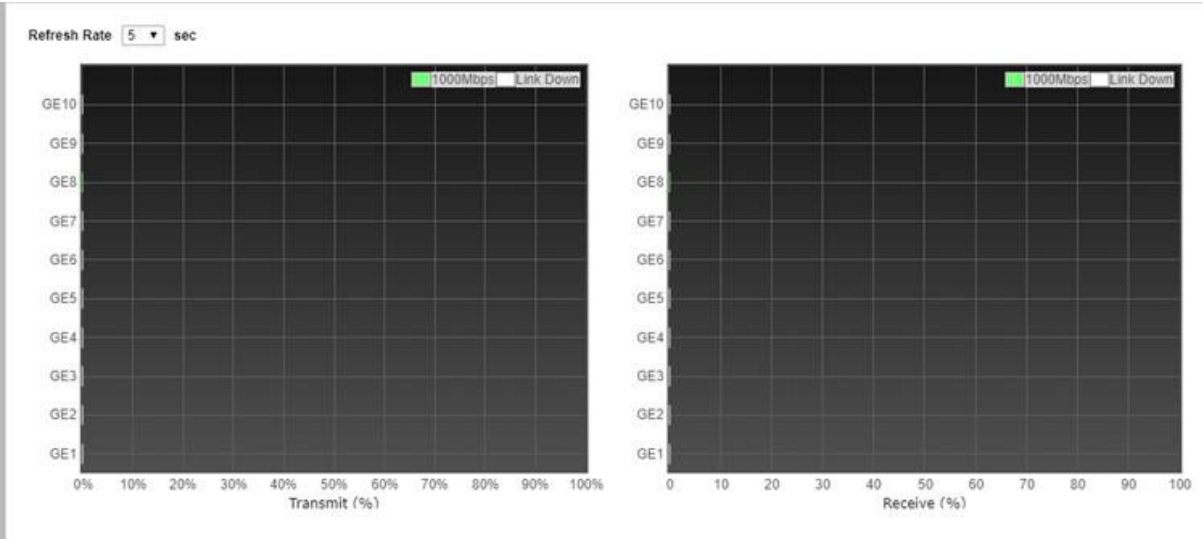


Figure 2-6 Port Bandwidth Utilisation Page

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

Table 2-7 Bandwidth Utilisation Field



## 2.4. Link Aggregation Display

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

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 2-7 Link Aggregation Status Page

Field	Description
<b>LAG</b>	LAG Name
<b>Name</b>	LAG port description
<b>Type</b>	<p>The type of the LAG</p> <ul style="list-style-type: none"> <li><b>Static:</b> The group of ports assigned to a static LAG are always active members.</li> <li><b>LACP:</b> The group of ports assigned to dynamic LAG are candidate ports. LACP determines which candidate ports are active member ports.</li> </ul>
<b>Link Status</b>	LAG port link status
<b>Active Member</b>	Active member ports of the LAG
<b>Inactive Member</b>	Inactive member ports of the LAG

Table 2-8 LAG Status Fields

## 2.5. MAC Address Table

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

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

Status>> MAC Address Status.

**MAC Address Table**

Showing All entries Showing 1 to 2 of 2 entries

VLAN	MAC Address	Type	Port
1	00:E0:4C:00:00:00	Management	CPU
1	00:0E:C6:D8:58:EC	Dynamic	GE8

First Previous 1 Next Last

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

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

Figure 3-1: IP Address page.

Field	Description
Address Type	The address type of switch IP configuration including <b>Static:</b> Static IP configured by users will be used. <b>Dynamic:</b> 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

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 DHCPv4 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.

Source

☐ SNTP
☐ From Computer
☒ Manual Time

Time Zone

UTC +8:00

Sntp

Address Type

☒ Hostname
☐ IPv4

Server Address

Server Port

123

(1 - 65535, default 123)

Manual Time

Date

2020-01-01

YYYY-MM-DD

Time

08:14:20

HH:MM:SS

Daylight Saving Time

Type

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

Offset

60

Min (1 - 1440, default 60)

Recurring

From: Day 

Sun

 Week 

First

 Month 

Jan

 Time

To: Day 

Sun

 Week 

First

 Month 

Jan

 Time

Non-recurring

From:  YYYY-MM-DD  HH:MM

To:  YYYY-MM-DD  HH:MM

Operational Status

Current Time

2020-01-01 08:14:20 UTC+8

Apply

Figure 3-2 System Time Page

Field	Description
<b>Source</b>	Select the time source. <ul style="list-style-type: none"> <li>• <b>SNTP:</b> Time sync from NTP server.</li> <li>• <b>From Computer:</b> Time set from browser host.</li> <li>• <b>Manual Time:</b> Time set by manually configure.</li> </ul>
<b>Time Zone</b>	Select a time zone difference from listing district.
<b>SNTP</b>	<b>Description</b>
<b>Address Type</b>	Select the address type of NTP server. This is enabled when time source is SNTP.
<b>Server Address</b>	Input IPv4 address or hostname for NTP server. This is enabled when time source is SNTP.
<b>Server Port</b>	Input NTP port for NTP server. Default is 123. This is enabled when time source is SNTP.
<b>Manual Time</b>	<b>Description</b>
<b>Date</b>	Input manual date. This is enabled when time source is manual.
<b>Time</b>	Input manual time. This is enabled when time source is manual.
<b>Daylight Saving Time</b>	Description
<b>Type</b>	<p><b>Select the mode of daylight saving time.</b></p> <p><b>Disable:</b> Disable daylight saving time.</p> <p><b>Recurring:</b> Using recurring mode of daylight saving time.</p> <p><b>Non-Recurring:</b> Using non-recurring mode of daylight saving time.</p> <p><b>USA:</b> Using daylight saving time in the United States that starts on the second Sunday of March and ends on the first Sunday of November</p> <p><b>European:</b> Using daylight saving time in the Europe that starts on the last Sunday in March and ending on the last Sunday in October</p>
<b>Offset</b>	Specify the adjust offset of daylight saving time.
<b>Recurring From</b>	Specify the starting time of recurring daylight saving time. This field available when selecting “Recurring” mode.
<b>Recurring To</b>	Specify the ending time of recurring daylight saving time. This field available when selecting “Recurring” mode.
<b>Non-recurring From</b>	Specify the starting time of non-recurring daylight saving time. This field available when selecting “Non-Recurring” mode.
<b>Non recurring To</b>	Specify the ending time of recurring daylight saving time. This field available when selecting “Non-Recurring” mode.

Table 3-4 System Time Fields

<b>PIXE L3 8T 4S-R</b> <b>Chapter 4 Port Settings</b>	<b>Rev 1.1</b> <b>Date. February 2025</b>
--	--

This page left blank Intentionally

## 4. Port

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

### 4.1. Port Setting

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

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

#### Port >> Settings

**Port Setting Table**

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

Figure 4-1 Port Setting Table

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

Table 4-1 Port Setting Table Fields

Port>> Port Settings

Edit Port Setting

Port

GE7-GE10

Description

State

☒ Enable

Speed

☒ Auto

☐ Auto - 10M

☐ Auto - 100M

☐ Auto - 1000M

☐ Auto - 10M/100M

☐ 10M

☐ 100M

☐ 1000M

☐ 10G

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.
Table 4-2 Edit Port Setting Fields	

## 4.2. Error Disabled

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

Recovery Interval	300	Sec (30 - 86400)
BPDU Guard	<input checked="" type="checkbox"/>	Enable
UDLD	<input checked="" type="checkbox"/>	Enable
Self Loop	<input checked="" type="checkbox"/>	Enable
Broadcast Flood	<input checked="" type="checkbox"/>	Enable
Unknown Multicast Flood	<input checked="" type="checkbox"/>	Enable
Unicast Flood	<input checked="" type="checkbox"/>	Enable
ACL	<input checked="" type="checkbox"/>	Enable
Port Security	<input checked="" type="checkbox"/>	Enable
DHCP Rate Limit	<input checked="" type="checkbox"/>	Enable
ARP Rate Limit	<input checked="" type="checkbox"/>	Enable

Apply

Figure 4-3 Error Disabled Page

Field	Description
<b>Recover Interval</b>	Auto recovery after this interval for error disabled port.
<b>BPDU Guard</b>	Enabled to auto shutdown port when BPDU Guard reason occur. This reason caused by STP BPDU Guard mechanism.
<b>UDLD</b>	Enabled to auto shutdown port when UDLD violation occur.
<b>Self Loop</b>	Enabled to auto shutdown port when Self Loop reason occur.
<b>Broadcast Flood</b>	Enabled to auto shutdown port when Broadcast Flood reason occur. This reason caused by broadcast rate exceed broadcast storm control rate.
<b>Unknown Multicast Flood</b>	Enabled to auto shutdown port when Unknown Multicast Flood reason occur. This reason caused by unknown multicast rate exceed unknown multicast storm control rate.
<b>Unicast Flood</b>	Enabled to auto shutdown port when Unicast Flood reason occur. This reason caused by unicast rate exceed unicast storm control rate.
<b>ACL</b>	Enabled to auto shutdown port when ACL shutdown port reason occur. This reason caused packet match the ACL shutdown port action.
<b>Port Security</b>	Enabled to auto shutdown port when Port Security Violation reason occur. This reason caused by violation port security rules
<b>DHCP Rate Limit</b>	Enabled to auto shutdown port when DHCP rate limit reason occur. This reason caused by DHCP packet rate exceed DHCP rate limit.
<b>ARP Rate Limit</b>	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 <b>src-dst-mac:</b> Based on MAC address <b>src-dst-mac-ip:</b> 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
<input checked="" type="radio"/> LAG 1		---	---		
<input type="radio"/> LAG 2		---	---		
<input type="radio"/> LAG 3		---	---		
<input type="radio"/> LAG 4		---	---		
<input type="radio"/> LAG 5		---	---		
<input type="radio"/> LAG 6		---	---		
<input type="radio"/> LAG 7		---	---		
<input type="radio"/> LAG 8		---	---		

Edit

Figure 4-5 LAG Group Setting Table

Field	Description
LAG	LAG Name
Name	LAG port description
Type	The type of the LAG <b>Static:.</b> <b>LACP:</b> 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

The dialog box for editing a Link Aggregation Group (LAG) is shown. It has a title bar 'Edit Link Aggregation Group'. Inside, there are several sections: 'LAG' with a value of '1', 'Name' with an empty text box, 'Type' with radio buttons for 'Static' (selected) and 'LACP', and a 'Member' section. The 'Member' section contains two lists: 'Available Port' (GE3, GE4, GE5, GE6, GE7, GE8, GE9, GE10) and 'Selected Port' (GE1, GE2). There are arrow buttons between the lists. At the bottom, there are 'Apply' and 'Close' buttons.

Figure 4-6 Edit LAG Group Setting Dialog

Field	Description
LAG	Selected LAG group ID
Name	LAG port description
Type	<b>The type of the LAG</b> <ul style="list-style-type: none"> <li><b>Static:</b> The group of ports assigned to a static LAG are always active members.</li> <li><b>LACP:</b> The group of ports assigned to dynamic LAG are candidate ports. LACP determines which candidate ports are active member ports.</li> </ul>
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

The LAG Port Setting Table is shown. It has a search bar at the top right. The table has columns: LAG, Type, Description, State, Link Status, Speed, Duplex, and Flow Control. There are 8 rows of LAG entries (LAG 1 to LAG 8). All LAGs are 'Enabled' and 'Down'. The 'Speed' and 'Duplex' are 'Auto', and 'Flow Control' is 'Disabled'. Below the table is an 'Edit' button.

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	<b>LAG Port admin state.</b> <b>Enabled:</b> Enable the port. <b>Disabled:</b> Disable the port.
Link Status	<b>Current LAG port link status</b> <b>Up:</b> Port is link up <b>Down:</b> 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. <b>Enable:</b> Enable the port. <b>Disable:</b> Disable the port.
Speed	Port speed capabilities. <b>Auto:</b> Auto speed with all capabilities <b>Auto-10M:</b> Auto speed with 10M ability only <b>Auto-100M:</b> Auto speed with 100M ability only

	<b>Auto-1000M:</b> Auto speed with 1000M ability only <b>Auto-10M/100M:</b> Auto speed with 10M/100M abilities <b>10M:</b> Force speed with 10M ability <b>100M:</b> Force speed with 100M ability <b>1000M:</b> Force speed with 1000M ability
<b>Flow Control</b>	Port flow control. <b>Auto:</b> Auto flow control by negotiation. <b>Enabled:</b> Enable flow control ability. <b>Disabled:</b> Disable flow control ability.
<b>Table 4-8 Port Setting Status Fields</b>	

### 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**

**Figure 4-9 LACP Global Setting**

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

**Table 4-9 LACP Priority**

**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

**Figure 4-10 LACP Port Setting Table**



Field	Description
Port	Port Name
State	Port EEE admin state. <b>Enabled:</b> EEE is enabled <b>Disabled:</b> EEE is disabled
Operational Status	Port EEE operational status. <b>Enabled:</b> EEE is operating <b>Disabled:</b> EEE is no operating
Table 4-12 EEE Setting Table Fields	

#### Port >> EEE

Field	Description
Port	Selected port list
State	<b>Port EEE admin state.</b> <b>Enable:</b> Enable EEE <b>Disable:</b> Disable EEE
Table 4-13 Edit EEE Setting Fields	

## 4.5. Jumbo Frame

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

This page allow user to configure switch jumbo frame size

#### Port>> Jumbo Frame

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	

This page left blank intentionally

## 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.

#### 5.2.1. Create VLAN

To display the 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

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

VLAN>> VLAN>> Create VLAN

Figure 5-2 Edit VLAN Name Dialog

Field	Description
Name	Input VLAN name.

**Table 5-2 Edit VLAN Name Fields**

### 5.2.2. VLAN Configuration

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

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

**VLAN>VLAN>VLAN Configuration**

**VLAN Configuration Table**

VLAN: VLAN0002

Entry	Port	Mode	Membership			PVID	Forbidden
1	GE1	Trunk	<input checked="" type="radio"/> Excluded	<input type="radio"/> Tagged	<input type="radio"/> Untagged	<input type="checkbox"/>	<input type="checkbox"/>
2	GE2	Trunk	<input checked="" type="radio"/> Excluded	<input type="radio"/> Tagged	<input type="radio"/> Untagged	<input type="checkbox"/>	<input type="checkbox"/>
3	GE3	Trunk	<input checked="" type="radio"/> Excluded	<input type="radio"/> Tagged	<input type="radio"/> Untagged	<input type="checkbox"/>	<input type="checkbox"/>
4	GE4	Trunk	<input checked="" type="radio"/> Excluded	<input type="radio"/> Tagged	<input type="radio"/> Untagged	<input type="checkbox"/>	<input type="checkbox"/>
5	GE5	Trunk	<input checked="" type="radio"/> Excluded	<input type="radio"/> Tagged	<input type="radio"/> Untagged	<input type="checkbox"/>	<input type="checkbox"/>
6	GE6	Trunk	<input checked="" type="radio"/> Excluded	<input type="radio"/> Tagged	<input type="radio"/> Untagged	<input type="checkbox"/>	<input type="checkbox"/>
7	GE7	Trunk	<input checked="" type="radio"/> Excluded	<input type="radio"/> Tagged	<input type="radio"/> Untagged	<input type="checkbox"/>	<input type="checkbox"/>
8	GE8	Trunk	<input checked="" type="radio"/> Excluded	<input type="radio"/> Tagged	<input type="radio"/> Untagged	<input type="checkbox"/>	<input type="checkbox"/>
9	GE9	Trunk	<input checked="" type="radio"/> Excluded	<input type="radio"/> Tagged	<input type="radio"/> Untagged	<input type="checkbox"/>	<input type="checkbox"/>
10	GE10	Trunk	<input checked="" type="radio"/> Excluded	<input type="radio"/> Tagged	<input type="radio"/> Untagged	<input type="checkbox"/>	<input type="checkbox"/>
11	LAG1	Trunk	<input checked="" type="radio"/> Excluded	<input type="radio"/> Tagged	<input type="radio"/> Untagged	<input type="checkbox"/>	<input type="checkbox"/>
12	LAG2	Trunk	<input checked="" type="radio"/> Excluded	<input type="radio"/> Tagged	<input type="radio"/> Untagged	<input type="checkbox"/>	<input type="checkbox"/>
13	LAG3	Trunk	<input checked="" type="radio"/> Excluded	<input type="radio"/> Tagged	<input type="radio"/> Untagged	<input type="checkbox"/>	<input type="checkbox"/>
14	LAG4	Trunk	<input checked="" type="radio"/> Excluded	<input type="radio"/> Tagged	<input type="radio"/> Untagged	<input type="checkbox"/>	<input type="checkbox"/>
15	LAG5	Trunk	<input checked="" type="radio"/> Excluded	<input type="radio"/> Tagged	<input type="radio"/> Untagged	<input type="checkbox"/>	<input type="checkbox"/>
16	LAG6	Trunk	<input checked="" type="radio"/> Excluded	<input type="radio"/> Tagged	<input type="radio"/> Untagged	<input type="checkbox"/>	<input type="checkbox"/>
17	LAG7	Trunk	<input checked="" type="radio"/> Excluded	<input type="radio"/> Tagged	<input type="radio"/> Untagged	<input type="checkbox"/>	<input type="checkbox"/>
18	LAG8	Trunk	<input checked="" type="radio"/> Excluded	<input type="radio"/> Tagged	<input type="radio"/> Untagged	<input type="checkbox"/>	<input type="checkbox"/>

**Figure 5-3 VLAN configuration Page**

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

**Table 5-3 VLAN Configuration Settings Fields**

### 5.2.3. Membership

To display the 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> VLAN Membership

**Membership Table**

Q

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

Edit

Figure 5-4 Membership Page

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

**Table 5-4 Membership Fields**

## VLAN>VLAN> VLAN Membership

**Edit Port Setting**

Port

GE2

Mode

Trunk

Membership

1UP

>

<

☐ Forbidden  
☐ Excluded  
☒ Tagged  
☐ Untagged  
☐ PVID

Apply

Close

Figure 5-5 Edit Membership Dialog

Field	Description
Port	Display the interface.
Mode	Display the VLAN mode of interface.
Membership	<p>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.</p> <p>Select the time source.</p> <p><b>Forbidden:</b> Set VLAN as forbidden VLAN.</p> <p><b>Excluded:</b> This option is always disabled.</p> <p><b>Tagged:</b> Set VLAN as tagged VLAN.</p> <p><b>Untagged:</b> Set VLAN as untagged VLAN.</p> <p><b>PVID:</b> 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.</p>

Table 5-5 Edit Membership Fields

#### 5.2.4. 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
<input type="checkbox"/>	1	GE1	Trunk	1	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	2	GE2	Trunk	1	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	3	GE3	Trunk	1	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	4	GE4	Trunk	1	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	5	GE5	Trunk	1	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	6	GE6	Trunk	1	All	Enabled	Disabled	0x8100
<input checked="" type="checkbox"/>	7	GE7	Trunk	1	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	8	GE8	Trunk	1	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	9	GE9	Trunk	1	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	10	GE10	Trunk	1	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	11	LAG1	Trunk	1	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	12	LAG2	Trunk	1	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	13	LAG3	Trunk	1	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	14	LAG4	Trunk	1	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	15	LAG5	Trunk	1	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	16	LAG6	Trunk	1	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	17	LAG7	Trunk	1	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	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 accepts 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	<input type="radio"/> Hybrid <input type="radio"/> Access <input checked="" type="radio"/> Trunk <input type="radio"/> Tunnel
PVID	1 (1 - 4094)
Accept Frame Type	<input checked="" type="radio"/> All <input type="radio"/> Tag Only <input type="radio"/> Untag Only
Ingress Filtering	<input checked="" type="checkbox"/> Enable
Uplink	<input checked="" type="checkbox"/> 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. <b>Hybrid:</b> Support all functions as defined in IEEE 802.1Q specification. <b>Access:</b> Accepts only untagged frames and join an untagged VLAN. <b>Trunk:</b> 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. Displaying The Voice VLAN

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

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

VLAN>>Voice VLAN>> Property

Figure 5-8 VLAN Voice> 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

## VLAN>>Voice VLAN>> Property

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

(NB: An OUI is the first 24 bits of a 48-bit MAC address assigned to each vendor by the Institute of Electrical and Electronics Engineers (IEEE). Voice packets sent by IP phones can be identified by the MAC address ranges requested by IP phone vendors.

In voice VLAN, the OUI is user-defined and not necessarily 24 bits long. The OUI is the result of the AND operation between the MAC address and mask in the **voice-vlan mac-address** command)

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

VLAN>Voice VLAN> Voice OUI

**Voice OUI Table**

Showing **All** entries Showing 1 to 8 of 8 entries

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

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

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

VLAN>Voice VLAN> Voice OUI

**Add Voice OUI**

**OUI**  :  :

**Description**

**Apply Close**

**Edit Voice OUI**

**OUI** 00:E0:BB

**Description** 3COM

**Apply Close**

Figure 5-12 Add and Edit Voice OUI Dialog



### 5.3. Protocol VLAN

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

(NB: A Virtual Local Area Network (VLAN) is mainly used to form groups among the hosts regardless of where the hosts are physically located. Thus, a VLAN improves security with the help of group formation among the hosts. One of the most common reasons to set up a VLAN is to set up a VLAN for voice, and a separate VLAN for data. This directs the packets for both types of data despite using the same network)

#### 5.3.1. Protocol Group

With these settings, protocol-based groups can be defined and bound to a port; therefore, every packet originating from the protocol groups is assigned to the configured VLAN on the page

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

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

VLAN>>Protocol VLAN>> Protocol Group

**Protocol Group Table**

Showing All entries Showing 1 to 3 of 3 entries

	Group ID	Frame Type	Protocol Value
<input type="checkbox"/>	1	Ethernet_II	0x3333
<input type="checkbox"/>	2	IEEE802.3_LLC_Other	0x4444
<input type="checkbox"/>	3	RFC_1042	0x5555

First Previous 1 Next Last

Add Edit Delete

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. <b>Ethernet_II:</b> packet type is Ethernet version 2. <b>IEEE802.3_LLC_Other:</b> packet type is 802.3 packet with LLC other header. <b>RFC_1042:</b> 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

<input type="checkbox"/>	Port	Group ID	VLAN
<input type="checkbox"/>	GE1	1	22

**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

1

VLAN

2222 (1 - 4094)

**Figure 5-16 Add and Edit Group Binding Dialog**



Field	Description
<b>Port</b>	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.
<b>Group ID</b>	Select a Group ID to associate with port. Only available on Add dialog.
<b>VLAN</b>	Input VLAN ID that will assign to packets which match protocol group.
<b>Table 5-16 Group Binding Fields</b>	

## 5.4. MAC VLAN

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

NB MAC VLAN is a way of classifying packets based on the source MAC address<sup>123</sup>. It allows incoming untagged packets to be assigned to a VLAN and thus classify traffic based on the source MAC address of the packet. You can define a MAC to VLAN mapping by configuring an entry in the MAC to VLAN table<sup>2</sup>. The MAC-based VLAN classification enables packets to be classified according to their source MAC address<sup>3</sup>. It is mainly used to connect container interfaces directly with host interfaces.

### 5.6.1. 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>> MACVLAN>> MAC Group**

The screenshot shows the 'MAC Group Table' interface. At the top, it says 'Showing All entries' and 'Showing 1 to 3 of 3 entries'. Below this is a table with 4 columns: a checkbox, 'Group ID', 'MAC Address', and 'Mask'. There are three rows of data. Below the table are 'Add', 'Edit', and 'Delete' buttons. At the bottom right, there are navigation buttons: 'First', 'Previous', '1' (selected), 'Next', and 'Last'.

	Group ID	MAC Address	Mask
<input type="checkbox"/>	1	02:03:04:05:06:07	48
<input type="checkbox"/>	2	04:05:06:07:08:09	9
<input type="checkbox"/>	3	AA:BB:CC:DD:EE:FF	32

**Figure 5-17 MAC Group Page**

Field	Description
<b>Group ID</b>	Display group ID of entry.
<b>MAC Address</b>	Display mac address of entry.
<b>Mask</b>	Display mask of mac address for classified packet.
<b>Table 5-17 MAC Group Fields</b>	

## VLAN>> MACVLAN>> MAC Group

### Add MAC Group

Group ID

 (1 - 2147483647)

MAC Address

Mask

 (9 - 48)

---

### Edit MAC Group

Group ID

1

MAC Address

Mask

 (9 - 48)

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**

### 5.6.2. Group Binding

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

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

## VLAN>> MACVLAN>> MAC Group Binding

### Group Binding Table

Showing All entries
 Showing 1 to 1 of 1 entries

<input type="checkbox"/>	Port	Group ID	VLAN
<input type="checkbox"/>	GE1	1	3333

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**

## VLAN>>MAC VLAN>>Group Binding

### Add Group Binding

Port	Available Port	Selected Port
	<div></div>	GE1
Note: Only VLAN Hybrid port can be set MAC VLAN		
Group ID	1	
VLAN		
(1 - 4094)		
<div>Apply</div> <div>Close</div>		

### Edit Group Binding

Port	GE1
Group ID	1
VLAN	3333
(1 - 4094)	
<div>Apply</div> <div>Close</div>	

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

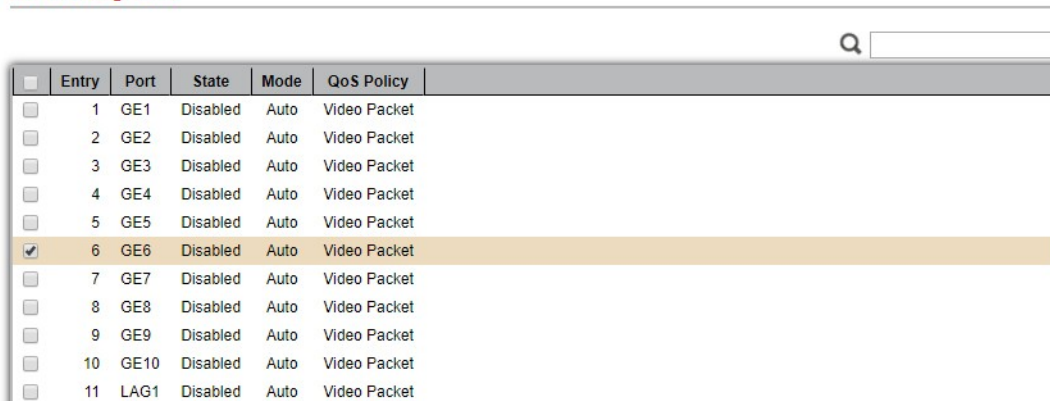
State	<input checked="" type="checkbox"/> Enable
VLAN	VLAN0002
CoS / 802.1p Remarking	<input checked="" type="checkbox"/> Enable
	6
Aging Time	1440
	Min (30 - 65536, default 1440)
<div>Apply</div>	

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



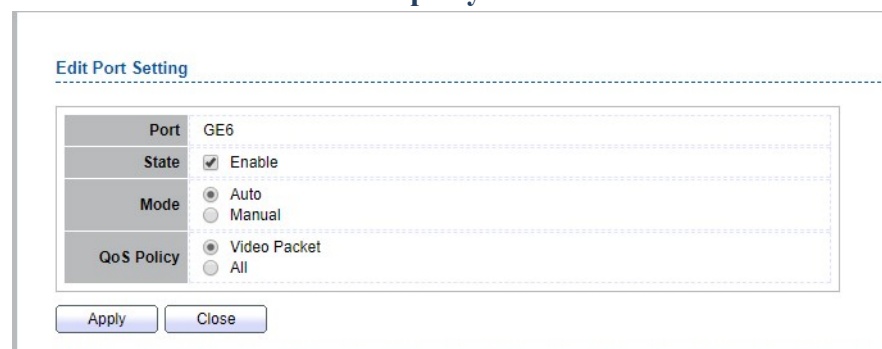
Entry	Port	State	Mode	QoS Policy
<input type="checkbox"/>	1 GE1	Disabled	Auto	Video Packet
<input type="checkbox"/>	2 GE2	Disabled	Auto	Video Packet
<input type="checkbox"/>	3 GE3	Disabled	Auto	Video Packet
<input type="checkbox"/>	4 GE4	Disabled	Auto	Video Packet
<input type="checkbox"/>	5 GE5	Disabled	Auto	Video Packet
<input checked="" type="checkbox"/>	6 GE6	Disabled	Auto	Video Packet
<input type="checkbox"/>	7 GE7	Disabled	Auto	Video Packet
<input type="checkbox"/>	8 GE8	Disabled	Auto	Video Packet
<input type="checkbox"/>	9 GE9	Disabled	Auto	Video Packet
<input type="checkbox"/>	10 GE10	Disabled	Auto	Video Packet
<input type="checkbox"/>	11 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>> Property



Edit Port Setting

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

Apply Close

Figure 5-23 Edit Property Port Dialog

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

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

**Table 5-24 Edit Property Port Dialog**

### 5.5.2. Surveillance OUI (Organisation Unique Identifier)

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

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

**VLAN>> Surveillance VLAN>> Surveillance OUI**

**Figure 5-24 Surveillance OUI Page**

Field	Description
<b>OUI</b>	Display OUI MAC address.
<b>Description</b>	Display description of OUI entry.

**Table 5-24 Surveillance OUI Fields**

### 5-25 Add and Edit Surveillance OUI Dialog

Field	Description
<b>OUI</b>	Input OUI MAC address. Can't be edited in edit dialog.
<b>Description</b>	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. Displaying GVRP

GVRP, short for **GARP VLAN Registration Protocol** or Generic VLAN Registration Protocol, is a protocol designed to manage virtual local area networks (VLANs) within a larger network infrastructure 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**

Figure 5-26 GVRP Setting Page

Field	Description
<b>State</b>	Set the enabling status of GVRP functionality <b>Enable:</b> if Checked Enable GVRP, else is Disable GVRP
<b>Operational Timeout</b>	
<b>Join</b>	GVRP Join time out.
<b>Leave</b>	GVRP leave time out.
<b>Leave All</b>	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
<b>Entry</b>	Entry of number
<b>Port</b>	Port Name
<b>State</b>	Display port GVRP state
<b>Vlan Creation</b>	Display port GVRP creation vlan state
<b>Registration</b>	Display port GVRP registration mode

Table 5-27 GVRP port setting Fields



## VLAN>> GVRP>> Property

### Edit Port Setting

Port	GE1,GE3
State	<input type="checkbox"/> Enable
VLAN Creation	<input checked="" type="checkbox"/> Enable
Registration	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden

Figure 5-28 GVRP port Setting Edit Page

Field	Description
<b>Port</b>	Display the selected port list
<b>State</b>	Set the enabling status of GVRP port <b>Enable:</b> Enable/Disable port of GVRP state.
<b>Vlan Creation</b>	Set the enabling status of GVRP port create VLAN Enable: Enable/Disable port create dynamic VLAN.
<b>Register Mode</b>	Set the register mode of GVRP port <b>Normal:</b> Normal mode. <b>Fixed:</b> The port will not learn any dynamic VLAN. Only send static VLAN information to neighbour and allow static VLAN packet pass. <b>Forbidden:</b> 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. GVRP VLAN 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  entries      Showing 1 to 1 of 1 entries     

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

Figure 5-29 GVRP VLAN Information Page

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

Table 5-29 GVRP Port Status Fields

### 5.6.3. GVRP Port Statistics

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

This page allow user to display GVRP port statics by type and clear GVRP port statistics by port.  
**VLAN>> GVRP>> Statistics**

Figure 5-30 GVRP Port Statistics Display Setting

Field	Description
<b>Port</b>	Port ID
<b>Statistics</b>	Type of statistics <ul style="list-style-type: none"> <li><b>All:</b> Display Receiver, Transmit and Error port statistics</li> <li><b>Receive:</b> Display Receive port statistics</li> <li><b>Transmit:</b> Display Transmit port statistics</li> <li><b>Error:</b> Display Error port statistics</li> </ul>
<b>Refresh Rate</b>	Web refresh rate <ul style="list-style-type: none"> <li><b>None:</b> Not auto refresh display port statistics</li> <li><b>5 sec:</b> Refresh display port statistics per 5 seconds</li> <li><b>10 sec:</b> Refresh display port statistics per 10 seconds</li> <li><b>30 sec:</b> Refresh display port statistics per 30 seconds</li> </ul>

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
<b>Join empty</b>	The number of Receive or Transmit Join empty attribute value.
<b>Empty</b>	The number of Receive or Transmit Empty attribute value.
<b>Leave Empty</b>	The number of Receive or Transmit Leave Empty attribute value.
<b>Join In</b>	The number of Receive or Transmit Join In attribute value.
<b>Leave In</b>	The number of Receive or Transmit Leave In empty attribute value.
<b>Leave All</b>	The number of Receive or Transmit Leave All attribute value.
<b>Invalid Protocol ID</b>	The number of Receive Invalid Protocol ID
<b>Invalid Attribute Type</b>	The number of Receive Invalid Attribute Type
<b>Invalid Attribute Value</b>	The number of Receive Invalid Attribute value.
<b>Invalid Attribute Length</b>	The number of Receive Invalid Attribute Length.
<b>Invalid Event</b>	The number of Receive Invalid Event.

**Table 5-31 GVRP Port Statistics Fields**

This page left blank intentionally

## 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**.

The screenshot displays the 'Dynamic Address Setting' page. At the top, there is a configuration box for 'Aging Time' with a value of 300 and a note 'Sec (10 - 630, default 300)'. An 'Apply' button is located below this box. The main section is titled 'Dynamic Address Table'. It shows 'Showing 1 to 1 of 1 entries'. Below this is a table with columns: 'VLAN', 'MAC Address', and 'Port'. The table contains one entry: VLAN 1, MAC Address 00:0E:C6:D8:58:EC, and Port GE8. At the bottom of the table, there are navigation buttons: 'First', 'Previous', '1', 'Next', and 'Last'. There are also 'Refresh' and 'Add Static Address' buttons at the bottom left.

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**.

#### MAC Address Table >> Static Address

The screenshot displays the 'Static Address Page'. It shows a table titled 'Static Address Table'. Above the table, it says 'Showing 0 to 0 of 0 entries'. The table itself is empty, with a message '0 results found.' below it. At the bottom of the table, there are navigation buttons: 'First', 'Previous', '1', 'Next', and 'Last'. There are also 'Add', 'Edit', and 'Delete' buttons at the bottom left.

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**.

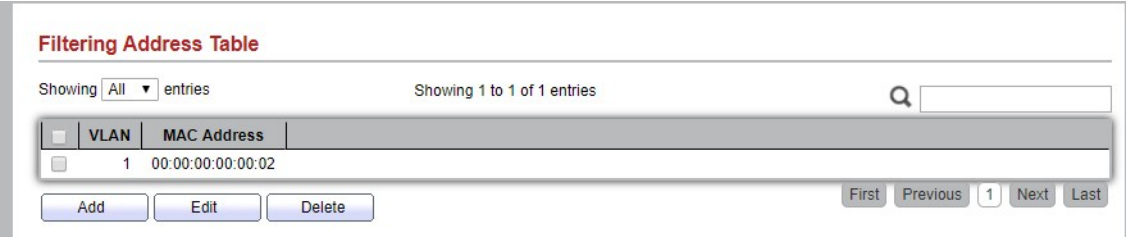


Figure 6-3: Filtering Address page.

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**.

State	<input checked="" type="checkbox"/> Enable
Operation Mode	<input type="radio"/> STP <input checked="" type="radio"/> RSTP <input type="radio"/> MSTP
Path Cost	<input checked="" type="radio"/> Long <input type="radio"/> Short
BPDU Handling	<input type="radio"/> Filtering <input checked="" type="radio"/> 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)
<b>Operational Status</b>	
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

Apply

Figure 7-1: STP Property

Field	Description
State	Enable/Disable the Spanning Tree on the switch.
Operation Mode	Specify the Spanning Tree operation mode. <b>STP:</b> Enable the Spanning Tree (STP) operation.
<b>RSTP: Enable the Rapid Spanning Tree (RSTP) operation.</b> <b>MSTP: Enable the Multiple Spanning Tree (MSTP) operation.</b>	
Path Cost	Specify the path cost method. <ul style="list-style-type: none"> <li><b>Long:</b> Specifies that the default port path costs are within the range: 1-200,000,000..</li> <li><b>Short:</b> Specifies that the default port path costs are within the range:1-65,535.</li> </ul>
BPDU Handling	Specify the BPDU forward method when the STP is disabled. <ul style="list-style-type: none"> <li><b>Filtering:</b> Filter the BPDU when STP is disabled.</li> <li><b>Flooding:</b> Flood the BPDU when STP is disabled.</li> </ul>
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.

<b>Forward Delay</b>	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.
<b>TX Hold Count</b>	Specify the tx-hold-count used to limit the maximum numbers of packets transmission per second. The valid range is from 1 to 10.
<b>Region Name</b>	The MSTP instance name. Its maximum length is 32 characters. The default value is the MAC address of the switch.
<b>Revision</b>	The MSTP revision number. Its valid range is from 0 to 65535.
<b>Max Hops</b>	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.**

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

**Table 7-2: STP Operational Status field.**

## 7.2. Port Setting

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

**Port Setting Table**

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

**Figure 7-2: STP Port Setting page.**

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

**Table 7-3: STP Port Setting fields.**

### Spanning Tree>> Port Settings

**Edit Port Setting**

---

<b>Port</b>	GE1-GE4
<b>State</b>	<input checked="" type="checkbox"/> Enable
<b>Path Cost</b>	<input type="text" value="0"/> (0 - 200000000) (0 = Auto)
<b>Priority</b>	<input type="text" value="128"/> ▼
<b>Edge Port</b>	<input type="checkbox"/> Enable
<b>BPDU Filter</b>	<input type="checkbox"/> Enable
<b>BPDU Guard</b>	<input type="checkbox"/> Enable
<b>Point-to-Point</b>	<input checked="" type="radio"/> Auto <input type="radio"/> Enable <input type="radio"/> Disable
<b>Port State</b>	Disabled
<b>Designated Bridge</b>	0-00:00:00:00:00:00
<b>Designated Port ID</b>	128-1
<b>Designated Cost</b>	20000
<b>Operational Edge</b>	False
<b>Operational Point-to-Point</b>	False

**Figure 7-3: Edit STP Port Setting page.**



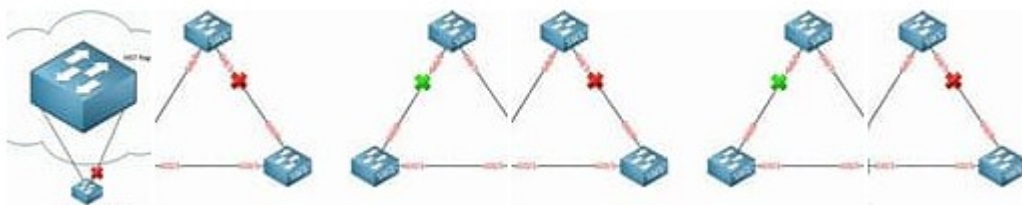
Field	Description
<b>State</b>	Enable/Disable the STP on the specified port.
<b>Path Cost</b>	Specify the STP path cost on the specified port.
<b>Priority</b>	Specify the STP path cost on the specified port.
<b>Edge Port</b>	Specify the edge mode. <b>Enable:</b> Force to true state (as link to a host). <b>Disable:</b> 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.
<b>BPDU Filter</b>	The BPDU Filter configuration avoids receiving/transmitting BPDU from the specified ports. <b>Enable:</b> Enable BPDU filter function. <b>Disable:</b> Disable BPDU filter function.
<b>BPDU Guard</b>	The BPDU Guard configuration to drop the received BPDU directly. <b>Enable:</b> Enable BPDU guard function. <b>Disable:</b> Disable BPDU guard function.
<b>Point-to-Point</b>	Specify the Point-to-Point port configuration: <b>Auto:</b> The state is depended on the duplex setting of the port <b>Enable:</b> Force to true state. <b>Disable:</b> Force to false state.

**Table 7-5: Edit STP Port Setting fields.**

### 7.3. MST Instance

The **Multiple Spanning Tree Protocol (MSTP)** and algorithm, provides both simple and full connectivity assigned to any given virtual LAN (VLAN) throughout a bridged local area network. MSTP uses bridge protocol data unit (BPDUs) to exchange information between spanning-tree compatible devices, to prevent loops in each Multiple Spanning Tree instance (MSTI) and in the common and internal spanning tree (CIST), by selecting active and blocked paths. This is done as well as in Spanning Tree Protocol (STP) without the need of manually enabling backup links and getting rid of switching loop danger.

Moreover, MSTP allows frames/packets assigned to different VLANs to follow separate paths, each based on an independent MSTI, within MST regions composed of local area networks (LANs) and MST bridges. These regions and the other bridges and LANs are connected into a single common spanning tree (CST)



To configure MST instance setting, click **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	<div>Available VLAN</div> <div>Selected VLAN</div>
Priority	32768 (0 - 61440, default 32768)
Bridge Identifier	32768-00:E0:4C:00:00:00
Designated Root Bridge	0-00:00:00:00:00:00
Root Port	
Root Path Cost	0
Remaining Hop	0

Apply Close

Figure 7-5: Edit MST Instance page.

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

Table 7-7: Edit MST Instance fields.

## 7.4. MST Port Setting

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

**MST Port Setting Table**

MSTI 0

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

Edit

Figure 7-6: MST Port Setting page.

Field	Description
<b>MSTI</b>	Specify the port setting on the specified MSTI
<b>Port</b>	Specify the interface ID or the list of interface IDs.
<b>Path Cost</b>	The port path cost on the specified MSTI.
<b>Priority</b>	The port priority on the specified MSTI.
<b>Port Role</b>	The current port role on the specified port. The possible values are: <b>“Disabled”, “Master”, “Root”, “Designated”, “Alternative”, and “Backup”.</b>
<b>Port State</b>	The current port state on the specified port. The possible values are: “Disabled”, “Discarding”, “Learning”, and “Forwarding”.
<b>Mode</b>	The operational STP mode on the specified port.
<b>Type</b>	The possible values for the port type are: <ul style="list-style-type: none"> <li><b>Boundary:</b> The port attaching an MST Bridge to a LAN that is not in the same region.</li> <li><b>Internal:</b> The port attaching an MST Bridge to a LAN that is not in the same region.</li> </ul>
<b>Designated Bridge</b>	The bridge ID of the designated bridge.
<b>Designated Port ID</b>	The designated port ID on the switch.
<b>Designated Cost</b>	The path cost of the designated port on the switch
<b>Remaining Hop</b>	The remaining hops count on the specified port.

Table 7-8: MST Port Setting fields.

## Spanning Tree>> MSTP 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**.

Statistics Table										
Refresh Rate		0 ▼	sec							
	Entry	Port	Receive BPDU			Transmit BPDU				
			Config	TCN	MSTP	Config	TCN	MSTP		
<input type="checkbox"/>	1	GE1	0	0	0	0	0	0		
<input type="checkbox"/>	2	GE2	0	0	0	0	0	0		
<input type="checkbox"/>	3	GE3	0	0	0	0	0	0		
<input type="checkbox"/>	4	GE4	0	0	0	0	0	0		
<input type="checkbox"/>	5	GE5	0	0	0	0	0	0		
<input type="checkbox"/>	6	GE6	0	0	0	0	0	0		
<input type="checkbox"/>	7	GE7	0	0	0	0	0	0		
<input type="checkbox"/>	8	GE8	0	0	0	0	0	0		
<input type="checkbox"/>	9	GE9	0	0	0	0	0	0		
<input type="checkbox"/>	10	GE10	0	0	0	0	0	0		
<input type="checkbox"/>	11	LAG1	0	0	0	0	0	0		
<input type="checkbox"/>	12	LAG2	0	0	0	0	0	0		
<input type="checkbox"/>	13	LAG3	0	0	0	0	0	0		
<input type="checkbox"/>	14	LAG4	0	0	0	0	0	0		
<input type="checkbox"/>	15	LAG5	0	0	0	0	0	0		
<input type="checkbox"/>	16	LAG6	0	0	0	0	0	0		
<input type="checkbox"/>	17	LAG7	0	0	0	0	0	0		
<input type="checkbox"/>	18	LAG8	0	0	0	0	0	0		

Figure 7-8: STP Statistics page

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

Table 7-11: View STP Statistic buttons.

STP Port Statistic

---

Port	GE1
Refresh Rate	<input checked="" type="radio"/> None <input type="radio"/> 5 sec <input type="radio"/> 10 sec <input type="radio"/> 30 sec
<b>Receive BPDU</b>	
Config	0
TCN	0
MSTP	0
<b>Transmit BPDU</b>	
Config	0
TCN	0
MSTP	0

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. LLDP Property Settings

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

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. <ul style="list-style-type: none"> <li>• <b>Filtering:</b> Deletes the packet.</li> <li>• <b>Bridging:</b> (VLAN-aware flooding) Forwards the packet to all VLAN members.</li> <li>• <b>Flooding:</b> Forwards the packet to all ports</li> </ul>
TLV Advertise Interval	Select the interval at which frames are transmitted. The default is 30 seconds, and the valid range is 5–32767 seconds.
Hold time 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 =
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



## Discovery>> LLDP>> Port Setting

Port Setting Table

Entry	Port	Mode	Selected TLV
<input type="checkbox"/> 1	GE1	Normal	802.1 PVID
<input type="checkbox"/> 2	GE2	Normal	802.1 PVID
<input type="checkbox"/> 3	GE3	Normal	802.1 PVID
<input type="checkbox"/> 4	GE4	Normal	802.1 PVID
<input type="checkbox"/> 5	GE5	Normal	802.1 PVID
<input type="checkbox"/> 6	GE6	Normal	802.1 PVID
<input type="checkbox"/> 7	GE7	Normal	802.1 PVID
<input type="checkbox"/> 8	GE8	Normal	802.1 PVID
<input type="checkbox"/> 9	GE9	Normal	802.1 PVID
<input type="checkbox"/> 10	GE10	Normal	802.1 PVID

Edit

Figure 8-2 LLDP Port Setting Page

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

## Discovery>> LLDP>> Port Setting

Edit Port Setting

Port	GE1		
Mode	<input type="radio"/> Transmit <input type="radio"/> Receive <input checked="" type="radio"/> Normal <input type="radio"/> Disable		
Optional TLV	Available TLV Port Description System Name System Description System Capabilities 802.3 MAC-PHY	<input type="button" value="→"/> <input type="button" value="←"/>	Selected TLV 802.1 PVID
802.1 VLAN Name	Available VLAN VLAN 1 VLAN 2 VLAN 3	<input type="button" value="→"/> <input type="button" value="←"/>	Selected VLAN 

Apply Close

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. <ul style="list-style-type: none"> <li>• <b>Disable:</b> Disable the transmission of LLDP PDUs.</li> <li>• <b>RX Only:</b> Receive LLDP PDUs only.</li> <li>• <b>TX Only:</b> Transmit LLDP PDUs only.</li> <li>• <b>TX And RX:</b> Transmit and receive LLDP PDUs both.</li> </ul>
Optional TLV	Select the LLDP optional TLVs to be carried (multiple selection is allowed). <ul style="list-style-type: none"> <li>• System Name</li> <li>• Port Description</li> <li>• System Description</li> <li>• System Capability</li> <li>• 802.3 MAC-PHY</li> <li>• 802.3 Link Aggregation</li> <li>• 802.3 Maximum Frame Size</li> <li>• Management Address</li> <li>• 802.1 PVID</li> </ul>
802.1 VLAN Name	Select the VLAN Name ID to be carried (multiple selection is allowed).

Table 8-3 LLDP Port Edit Page

### 8.1.2. MED Network Policy

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

#### MED Network Policy Table

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

<input type="checkbox"/>	Policy ID	Application	VLAN	VLAN Tag	Priority	DSCP
<input type="checkbox"/>	1	Voice Signalling	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	<input type="text" value="1"/>
Application	<input type="text" value="Voice"/>
VLAN	<input type="text"/> Range (0 - 4095)
VLAN Tag	<input checked="" type="radio"/> Tagged <input type="radio"/> Untagged
Priority	<input type="text" value="0"/>
DSCP	<input type="text" value="0"/>

**Figure 8-5 LLDP MED Network Policy Setting Page**

Field	Description
<b>Policy ID</b>	Select specified network policy ID to configure.
<b>Application</b>	Select the network policy application type. <ul style="list-style-type: none"> <li><b>Voice</b></li> <li><b>Voice Signalling</b></li> <li><b>Guest Voice</b></li> <li><b>Guest Voice Signalling</b></li> <li><b>Softphone Voice</b></li> <li><b>Video Conferencing</b></li> <li><b>App Streaming Video</b></li> <li><b>Video Signalling</b></li> </ul>
<b>VLAN</b>	Set the VLAN ID, range from 1 to 4094.
<b>VLAN Tag</b>	Set the VLAN tag status. <ul style="list-style-type: none"> <li><b>Tagged:</b> Traffic is tagged.</li> <li><b>Untagged:</b> Traffic is untagged.</li> </ul>
<b>Priority</b>	Set the L2 priority, range from 0 to 7.
<b>DSCP</b>	Set the DSCP value, range from 0 to 63

**Table 8-3 LLDP MED Network Policy Configuration Fields**

### 8.1.3. LLDP MED Port Setting

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

**MED Port Setting Table**

	Entry	Port	State	Network Policy		Location	Inventory	
				Active	Application			
<input type="checkbox"/>	1	GE1	Enabled	Yes		No	No	
<input type="checkbox"/>	2	GE2	Enabled	Yes		No	No	
<input type="checkbox"/>	3	GE3	Enabled	Yes		No	No	
<input type="checkbox"/>	4	GE4	Enabled	Yes		No	No	
<input type="checkbox"/>	5	GE5	Enabled	Yes		No	No	
<input type="checkbox"/>	6	GE6	Enabled	Yes		No	No	
<input type="checkbox"/>	7	GE7	Enabled	Yes		No	No	
<input type="checkbox"/>	8	GE8	Enabled	Yes		No	No	
<input type="checkbox"/>	9	GE9	Enabled	Yes		No	No	
<input type="checkbox"/>	10	GE10	Enabled	Yes		No	No	

**Figure 8-6 LLDP MED Setting Page**

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

#### Discovery>> LLDP>> MED Port Settings

**Edit MED Port Setting**

<b>Port</b>	GE1		
<b>State</b>	<input checked="" type="checkbox"/> Enable		
<b>Optional TLV</b>	Available TLV	Selected TLV	
	Location Inventory	Network Policy	
<b>Network policy</b>	Available Policy	Selected Policy	
	1 (Voice Signaling)		
<b>Location</b>			
<b>Coordinate</b>	<input type="text"/> (16 pairs of hexadecimal characters)		
<b>Civic</b>	<input type="text"/> (6 - 160 pairs of hexadecimal characters)		
<b>ECS ELIN</b>	<input type="text"/> (10 - 25 pairs of hexadecimal characters)		

**Figure 8-7 LLDP MED Add/Edit Page**



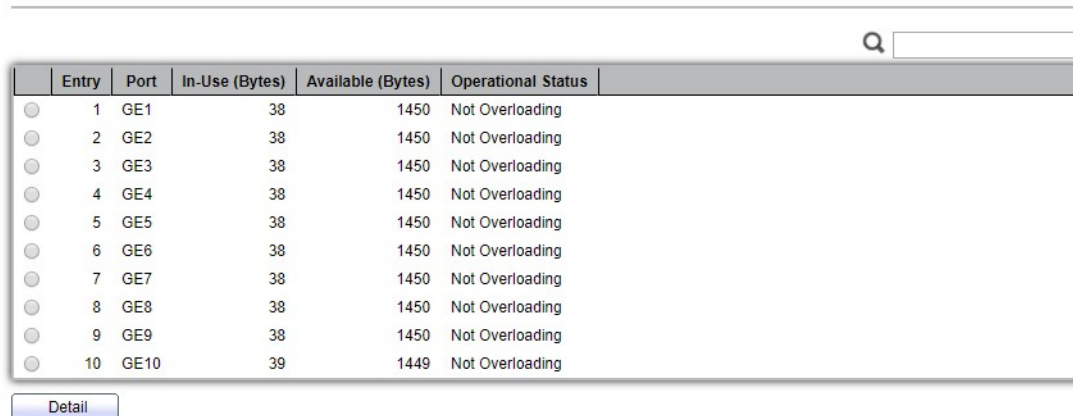
Field	Description
<b>Port</b>	Select specified port or all ports to configure LLDP MED.
<b>State</b>	Select LLDP MED enable status
<b>Optional TLV</b>	Select LLDP MED optional TLVs (multiple selection is allowed) <ul style="list-style-type: none"> <li>• <b>Network Policy</b></li> <li>• <b>Location</b></li> <li>• <b>Inventory</b></li> </ul>
<b>Network Policy</b>	Select the network policy IDs to be bound to ports. The network policy should be created in MED Network Policy page at first.

**Table 8-4 LLDP MED Port Location Configuration Fields**

#### 8.1.4. Packet View

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

**Packet View Table**



The screenshot shows a web interface for the 'Packet View Table'. At the top right, there is a search icon and a search input field. Below this is a table with the following columns: Entry, Port, In-Use (Bytes), Available (Bytes), and Operational Status. The table contains 10 rows of data, each with a radio button in the 'Entry' column. Below the table, there is a 'Detail' button.

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

Detail

**Figure 8-8 LLDP Overloading Page**

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

**Table 8-5 LLDP Overloading Fields**

If more detailed information is required, select the port, then click **detail**

## Discovery>> LLDP>> PacketView

### Packet View Detail

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

Close

<b>Optional TLVs</b>	
Size (Bytes)	0
Operational Status	Transmitted
<b>802.1 TLVs</b>	
Size (Bytes)	8
Operational Status	Transmitted
<b>Total</b>	
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

### 8.1.5. LLDP Local Device Information

To display LLDP Local Device, click **Discovery > LLDP > Local Information**.  
Use the LLDP Local Information to view LLDP local device 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
<input type="radio"/>	1 GE1	Normal	Enabled
<input type="radio"/>	2 GE2	Normal	Enabled
<input type="radio"/>	3 GE3	Normal	Enabled
<input type="radio"/>	4 GE4	Normal	Enabled
<input type="radio"/>	5 GE5	Normal	Enabled
<input type="radio"/>	6 GE6	Normal	Enabled
<input type="radio"/>	7 GE7	Normal	Enabled
<input type="radio"/>	8 GE8	Normal	Enabled
<input type="radio"/>	9 GE9	Normal	Enabled
<input type="radio"/>	10 GE10	Normal	Enabled

Detail

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 the “detail” button on the page to view detailed 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

### 8.1.6. Display LLDP Remote Device Neighbour

To display LLDP Remote Device, click **Discovery > LLDP > Neighbour**. Use the LLDP Neighbour page to view LLDP neighbours' information.

### Neighbour Page

Showing  entries      Showing 0 to 0 of 0 entries     

<input type="checkbox"/>	Local Port	Chassis ID Subtype	Chassis ID	Port ID Subtype	Port ID	System Name	Time to Live
0 results found.							

Field	Description
Local Port	Number of the local port to which the neighbour is connected.
Chassis ID Subtype	Type of chassis ID (for example, MAC address).
Chassis ID	Identifier of the 802 LAN neighbouring 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 neighbour is deleted.

Table 8-8 LLDP Neighbour Fields

Click “detail” to view selected neighbour detail information

### 8.1.7. 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

Clear

Refresh

#### Statistics Table

	Entry	Port	Transmit Frame	Receive Frame			Receive TLV		Neighbor Timeout	
			Total	Total	Discard	Error	Discard	Unrecognized		
<input type="checkbox"/>	1	GE1	0	0	0	0	0	0	0	
<input type="checkbox"/>	2	GE2	0	0	0	0	0	0	0	
<input type="checkbox"/>	3	GE3	0	0	0	0	0	0	0	
<input type="checkbox"/>	4	GE4	0	0	0	0	0	0	0	
<input type="checkbox"/>	5	GE5	0	0	0	0	0	0	0	
<input type="checkbox"/>	6	GE6	0	0	0	0	0	0	0	
<input type="checkbox"/>	7	GE7	0	0	0	0	0	0	0	
<input type="checkbox"/>	8	GE8	344	0	0	0	0	0	0	
<input type="checkbox"/>	9	GE9	0	0	0	0	0	0	0	
<input type="checkbox"/>	10	GE10	0	0	0	0	0	0	0	

Clear

Refresh

**Figure 8-14 LLDP Statistics Page**

Field	Description
<b>Insertions</b>	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.
<b>Deletions</b>	The number of times the complete set of information advertised by MSAP has been deleted from tables associated with the remote systems.
<b>Drops</b>	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.
<b>Age Outs</b>	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.
<b>Port</b>	Interface or port number.
<b>Transmit Frame Total</b>	Number of LLDP frames transmitted on the corresponding port.
<b>Receive Frame Total</b>	Number of LLDP frames received by this LLDP agent on the corresponding port, while the LLDP agent is enabled.
<b>Receive Frame Discard</b>	Number of LLDP frames discarded for any reason by the LLDP agent on the corresponding port.
<b>Receive Frame Error</b>	Number of invalid LLDP frames received by the LLDP agent on the corresponding port, while the LLDP agent is enabled.
<b>Receive TLV Discard</b>	Number of TLVs of LLDP frames discarded for any reason by the LLDP agent on the corresponding port.
<b>Receive TLV Unrecognized</b>	Number of TLVs of LLDP frames that are unrecognized while the LLDP agent is enabled
<b>Neighbour Timeout</b>	Number of age out LLDP frames.

Table 8-9 LLDP Statistics Fields

This page left blank Intentionally



## 9. Multicast

### 9.1. General Multicast IGMP and MLD

**Multicast** is a method of group communication in computer networking where data is transmitted to a group of destination computers simultaneously. It allows for **one-to-many or many-to-many distribution**, enabling efficient data delivery to multiple receivers at once. In multicast routing, packets are forwarded to multiple receivers using a multicast group address, which helps optimize network resource usage. Additionally, **IP multicast** is a specific implementation that efficiently delivers data to interested groups of receivers rather than to a single destination or all device. The **Internet Group Management Protocol (IGMP)** is a communications protocol used by hosts and adjacent routers on IPv4 networks to establish multicast group memberships. IGMP is an integral part of IP multicast and allows the network to direct multicast transmissions only to hosts that have requested them.

**Multicast Listener Discovery (MLD)** is a component of the Internet Protocol Version 6 (IPv6) suite. MLD is used by IPv6 routers for discovering multicast listeners on a directly attached link, much like Internet Group Management Protocol (IGMP) is used in IPv4. The protocol is embedded in ICMPv6 instead of using a separate protocol. MLDv1 is similar to IGMPv2 and MLDv2 similar to IGMPv3.

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

#### 9.1.1. Displaying the Multicast Pages

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**

The screenshot displays the 'Multicast General Properties' configuration page. It features two main sections: 'Unknown Multicast Action' and 'Multicast Forward Method'. The 'Unknown Multicast Action' section has three radio button options: 'Flood' (selected), 'Drop', and 'Forward to Router Port'. The 'Multicast Forward Method' section is divided into two parts, one for IPv4 and one for IPv6. Each part has two radio button options: 'DMAC-VID' (selected) and 'DIP-VID'. An 'Apply' button is located at the bottom left of the configuration area.

Figure 9-1 Multicast General Properties Page

Field	Description
Unknown Multicast Action	Set the unknown multicast action <ul style="list-style-type: none"> <li>• <b>Drop:</b> drop the unknown multicast data.</li> <li>• <b>Flood:</b> flood the unknown multicast data.</li> <li>• <b>Router port:</b> forward the unknown multicast data to router port.</li> </ul>
IPv4	Set the ipv4 multicast forward method. <ul style="list-style-type: none"> <li>• <b>MAC-VID:</b> forward method dmac+vid.</li> <li>• <b>DIP-VID:</b> forward method dip+vid.</li> </ul>
IPv6	Set the ipv6 multicast forward method. <ul style="list-style-type: none"> <li>• <b>MAC-VID:</b> forward method dmac+vid.</li> <li>• <b>DIP-VID:</b> forward method dip+vid(dip is ipv6 low 32 bit).</li> </ul>

Table 9-1 Multicast General Property Setting Fields

### 9.1.2. Displaying Multicast 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 <ul style="list-style-type: none"> <li>• <b>IPv4:</b> ipv4 multicast group</li> <li>• <b>IPv6:</b> ipv6 multicast group</li> </ul>
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

## Multicast>> General>>Group address

### Add Group Address

The screenshot shows the 'Add Group Address' configuration window. It has a title bar 'Add Group Address'. Inside, there are three main sections: 'VLAN' with a dropdown set to '1', 'IP Version' with a dropdown set to 'IPv4', and 'Group Address' with an empty text box. Below these is a 'Member' section containing two lists: 'Available Port' (GE1, GE2, GE3, GE4, GE5, GE6, GE7, GE8) and 'Selected Port' (empty). There are right and left arrow buttons between the two lists. At the bottom are 'Apply' and 'Close' buttons.

Figure 9-3 Multicast Group Address Add Page

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

Table 9-3 Multicast Group Address Add Fields

## Multicast>> General>> group Address.

### Edit Group Address

The screenshot shows the 'Edit Group Address' configuration window. It has a title bar 'Edit Group Address'. Inside, there are three main sections: 'VLAN' with a dropdown set to '1', 'Group Address' with a text box containing '224.1.1.1', and a 'Member' section containing two lists: 'Available Port' (GE2, GE3, GE4, GE5, GE6, GE7, GE8, GE9) and 'Selected Port' (GE1). There are right and left arrow buttons between the two lists. At the bottom are 'Apply' and 'Close' buttons.

Figure 9-4 Multicast Group Address Edit Page

Field	Description
VLAN	The VLAN ID of edited group.
Group Address	The group IP address.
Member	The member ports of group. <ul style="list-style-type: none"> <li>Available Port: Optional port member</li> <li>Selected Port: Selected port member</li> </ul>

Table 9-4 Multicast Group Address Edit Fields

### 9.1.3. Router Port

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

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

Figure 9-5 Multicast Router Table Page

Field	Description
IP Version	IP Version <ul style="list-style-type: none"> <li>IPv4: ipv4 multicast router</li> <li>IPv6: ipv6 multicast router</li> </ul>
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.**

Figure 9-6 Multicast Router Add Page

Field	Description
VLAN	The VLAN ID for router entry <ul style="list-style-type: none"> <li><b>Available VLAN:</b> Optional VLAN member</li> <li><b>Selected VLAN:</b> Selected VLAN member</li> </ul>
IP Version	IP Version <ul style="list-style-type: none"> <li><b>IPv4:</b> ipv4 multicast router</li> <li><b>IPv6:</b> ipv6 multicast router</li> </ul>
Type	The router port type <ul style="list-style-type: none"> <li><b>Static:</b> static router port</li> <li><b>Forbidden:</b> forbidden router port, can't learn dynamic router port member</li> </ul>
Port	The member ports of router entry. <ul style="list-style-type: none"> <li><b>Available Port:</b> Optional router port member</li> <li><b>Selected Port:</b> Selected router port member</li> </ul>

Table 9-6 Multicast Router Add Fields

Multicast>> General>> Router Port.

Field	Description
VLAN	VLAN ID of Selected router entry
IP Version	Selected IP version
Type	The router port type <ul style="list-style-type: none"> <li><b>Static:</b> static router port</li> <li><b>Forbidden:</b> forbidden router port, can't learn dynamic router port member</li> </ul>
Port	The member ports of router entry for selected port type. <ul style="list-style-type: none"> <li><b>Available Port:</b> Optional router port member</li> <li><b>Selected Port:</b> Selected router port member</li> </ul>

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 allows the user to add and edit forward all entry.

Multicast>> General>> Forward All

**Forward All Table**

IP Version IPv4 ▾

Showing All ▾ entries Showing 1 to 2 of 2 entries Q

<input type="checkbox"/>	VLAN	Static Port	Forbidden Port
<input type="checkbox"/>	2	GE2-GE3	
<input type="checkbox"/>	3	GE1-GE2	

Add Edit Delete First Previous 1 Next Last

Figure 9-8 Multicast Forward All Table Page

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

Table 9-8 Multicast Forward All Table Fields

**Add Forward All**

VLAN

Available VLAN

1

Selected VLAN

IP Version

IPv4 ▾

Type

☒ Static  
☐ Forbidden

Port

Available Port

GE1  
GE2  
GE3  
GE4  
GE5  
GE6  
GE7  
GE8

Selected Port

Apply Close

Figure 9-9 Multicast Forward All Add Page

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

**Table 9-9 Multicast Forward All Add Fields**

**Figure 9-10 Multicast Forward All Edit Page**

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

**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



**Throttling Table**

IP Version IPv4 ▼

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

[Edit](#)

Figure 9-11 Multicast Throttling Table Page

Field	Description
IP Version	IP Version <ul style="list-style-type: none"> <li><b>IPv4:</b> ipv4 for igmp snooping throttling</li> <li><b>IPv6:</b> ipv6 for mld snooping throttling</li> </ul>
Entry	Entry of number
Port	Port Name
Max Group	Max number of group for port
Exceed Action	Display the port exceed max number group learning group action

Table 9-11 Multicast Throttling Table Fields

[Edit Throttling](#)

Port

GE2,GE4

IP Version

IPv4

Max Group

(0 - 256)

Exceed Action

☒ Deny  
☐ Replace

[Apply](#)
[Close](#)

Figure 9-12 Multicast Throttling Edit Page

Field	Description
Port	Display the selected port list
IP Version	Display the selected IP version
Max Group	Max number of group for port
Exceed Action	Excess Max number of port learning group action <ul style="list-style-type: none"> <li><b>Deny:</b> do not allow in learning group.</li> <li><b>Replace:</b> random replace one exist group</li> </ul>

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

Showing  entries Showing 1 to 1 of 1 entries

<input type="checkbox"/>	Profile ID	Start Address	End Address	Action
<input type="checkbox"/>	1	224.1.1.1	224.1.2.3	Allow

Figure 9-13 Multicast Profile Table Page

Field	Description
IP Version	IP version: <ul style="list-style-type: none"> <li><b>IPv4:</b> IGMP snooping profile</li> <li><b>IPv6:</b> MLD snooping profile</li> </ul>
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

(1 - 128)

IP Version

Start Address

End Address

Action ☒ Allow ☐ Deny

Figure 9-14 Multicast Profile Add Page

Field	Description
Profile ID	Profile ID
IP Version	IP version: <ul style="list-style-type: none"> <li><b>IPv4:</b> IGMP snooping profile</li> <li><b>IPv6:</b> MLD snooping profile</li> </ul>
Start Address	The start group address of profile
End Address	The end group address of profile
Action	The action of profile: <ul style="list-style-type: none"> <li><b>Allow:</b> permit all packets that match the profile.</li> <li><b>Deny:</b> deny all packets that match the profile.</li> </ul>

Table 9-14 Multicast Profile Add Fields

**Multicast>> General>> Filtering Profile.**

[Edit Profile](#)

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

**Figure 9-15 Multicast Profile Edit Page**

Field	Description
<b>Profile ID</b>	Edit Profile ID
<b>IP Version</b>	Display the edit profile ip version
<b>Start Address</b>	The start group address of profile
<b>End Address</b>	The end group address of profile
<b>Action</b>	The action of profile: <ul style="list-style-type: none"> <li><b>Allow:</b> permit the group can learned that match the profile.</li> <li><b>Deny:</b> deny the group to learn the group that match the profile.</li> </ul>

**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

### Filtering Binding Table

IP Version IPv4 ▼

<input type="checkbox"/>	Entry	Port	Profile ID
<input type="checkbox"/>	1	GE1	
<input type="checkbox"/>	2	GE2	
<input type="checkbox"/>	3	GE3	
<input type="checkbox"/>	4	GE4	
<input type="checkbox"/>	5	GE5	
<input type="checkbox"/>	6	GE6	
<input type="checkbox"/>	7	GE7	
<input type="checkbox"/>	8	GE8	
<input type="checkbox"/>	9	GE9	
<input type="checkbox"/>	10	GE10	
<input type="checkbox"/>	11	LAG1	
<input type="checkbox"/>	12	LAG2	
<input type="checkbox"/>	13	LAG3	
<input type="checkbox"/>	14	LAG4	
<input type="checkbox"/>	15	LAG5	
<input type="checkbox"/>	16	LAG6	
<input type="checkbox"/>	17	LAG7	
<input type="checkbox"/>	18	LAG8	

Edit

Figure 9-16 Multicast Filtering Table Page

Field	Description
IP Version	IP Version <ul style="list-style-type: none"> <li><b>IPv4:</b> ipv4 for igmp snooping throttling</li> <li><b>IPv6:</b> ipv6 for mld snooping throttling</li> </ul>
Entry	Entry of number
Port	Port Name
Profile ID	Port Binding Profile ID

Table 9-16 Multicast Filtering Table Fields

### Edit Filtering Binding

Port	GE1-GE2
IP Version	IPv4
Profile ID	<input checked="" type="checkbox"/> Enable 1 ▼

Apply Close

Figure 9-17 Multicast Filtering Edit Page

Field	Description
Port	Selected Port List
IP Version	Display Selected Port filtering IP version
Profile ID	If check Enable, or select or change profile ID. Otherwise 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. How to Display IGMP Snooping

To display IGMP Snooping global setting and VLAN Setting web page, select,

**Multicast> IGMP Snooping> Property**

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

**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
<input type="checkbox"/>	1	Disabled	Enabled	2	125	10	2	1	Disabled
<input type="checkbox"/>	2	Disabled	Enabled	2	125	10	2	1	Disabled
<input type="checkbox"/>	3	Disabled	Enabled	2	125	10	2	1	Disabled
<input type="checkbox"/>	5	Disabled	Enabled	2	125	10	2	1	Disabled
<input type="checkbox"/>	10	Disabled	Enabled	2	125	10	2	1	Disabled

Edit

Figure 9-18 IGMP Snooping Property Page

Field	Description
<b>State</b>	Set the enabling status of IGMP Snooping functionality <ul style="list-style-type: none"> <li><b>Enable:</b> If Checked Enable IGMP Snooping, else is Disabled IGMP Snooping.</li> </ul>
<b>Version</b>	Set the igmp snooping version <ul style="list-style-type: none"> <li><b>IGMPv2:</b> Only support process igmp v2 packet.</li> <li><b>IGMPv3:</b> Support v3 basic and v2.</li> </ul>
<b>Report Suppression</b>	Set the enabling status of IGMP v2 report suppression <ul style="list-style-type: none"> <li><b>Enable:</b> If Checked Enable IGMP Snooping v2 report suppression, else Disable the report suppression function</li> </ul>
<b>VLAN</b>	The IGMP entry VLAN ID
<b>Operation Status</b>	The enable status of IGMP snooping VLAN functionality
<b>Router Port Auto Learn</b>	The enabling status of IGMP snooping router port auto learning
<b>Query Robustness</b>	The Query Robustness allows tuning for the expected packet loss on a subnet.
<b>Query Interval</b>	The interval of querier to send general query
<b>Query Max Response Interval</b>	In Membership Query Messages, it specifies the maximum allowed time before sending a responding report in units of 1/10 second.
<b>Last Member Query count</b>	The count that Querier-switch sends Group-Specific Queries when it receives a Leave Group message for a group.
<b>Last Member Query Interval</b>	The interval that Querier-switch sends Group-Specific Queries when it receives a Leave Group message for a group.
<b>Immediate leave</b>	The immediate leave status of the group will immediately leave when it receives an IGMP Leave message.

Table 9-18 IGMP Snooping Property Fields

## Multicast> IGMP Snooping> Property

Edit VLAN Setting

VLAN	3,5
State	<input type="checkbox"/> Enable
Router Port Auto Learn	<input checked="" type="checkbox"/> Enable
Immediate leave	<input type="checkbox"/> 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)
<b>Operational Status</b>	
Status	Disabled
Query Robustness	2
Query Interval	125 (Sec)
Query Max Response Interval	10 (Sec)
Last Member Query Counter	2
Last Member Query Interval	1 (Sec)

Apply Close

Figure 9-19 IGMP Snooping VLAN Edit Page

Field	Description
VLAN	The selected VLAN List
State	Set the enabling status of IGMP Snooping VLAN functionality <ul style="list-style-type: none"> <li><b>Enable:</b> If Checked Enable IGMP Snooping VLAN, else is Disabled IGMP Snooping VLAN.</li> </ul>
Router Port Auto Learn	Set the enabling status of IGMP Snooping router port learning <ul style="list-style-type: none"> <li><b>Enable:</b> If checked Enable learning router port by query and PIM, DVRMP, else Disable the learning router port</li> </ul>
Immediate leave	Immediate Leave the group when receive IGMP Leave message. <ul style="list-style-type: none"> <li><b>Enable:</b> If checked Enable immediate leave, else disable immediate leave</li> </ul>
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.
<b>Operational Status</b>	
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

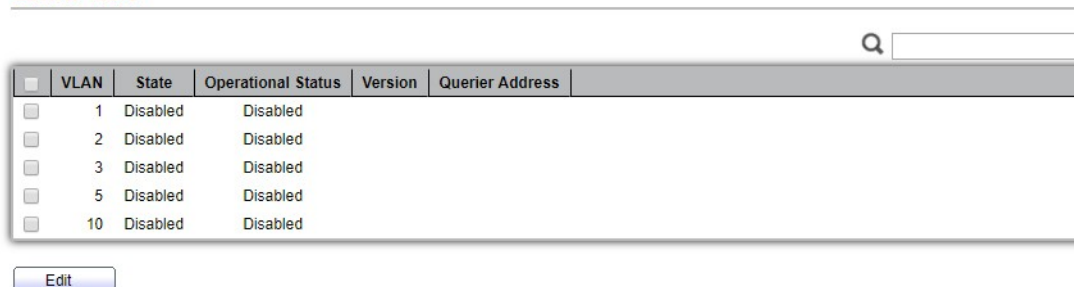
### 9.2.2. IGMP Snooping Querier

An IGMP Snooping Querier is a network function involved in the management of Multicast traffic when using IGMP in conjunction with IGMP snooping] on a switch.

IGMP Snooping Querier is a function that can be enabled Case Communications network switches to maintain efficient multicast traffic distribution in environments lacking a dedicated multicast router. It helps in managing multicast memberships by soliciting reports from hosts, thereby allowing the switch to make informed decisions about where to forward multicast traffic.

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.

Querier Table



	VLAN	State	Operational Status	Version	Querier Address
<input type="checkbox"/>	1	Disabled	Disabled		
<input type="checkbox"/>	2	Disabled	Disabled		
<input type="checkbox"/>	3	Disabled	Disabled		
<input type="checkbox"/>	5	Disabled	Disabled		
<input type="checkbox"/>	10	Disabled	Disabled		

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

### Multicast>> IGMP Snooping>>Querier



Figure 9-21 IGMP Snooping Querier Edit Page

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

Table 9-21 IGMP Snooping Querier Edit Fields



### 9.2.3. IGMP Snooping 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

Clear Refresh

**Figure 9-22 IGMP Snooping Statistics Page**

Field	Description
<b>Receive Packet</b>	
Total	Total RX igmp packet, include ipv4 multicast data to CPU.
Valid	A valid igmp snooping process packet.
In Valid	An 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
<b>Transmit Packet</b>	
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

Multicast Listener Discovery (MLD) snooping constrains the flooding of IPv6 multicast traffic on VLANs. When MLD snooping is enabled on a VLAN, a networks devices examine the MLD messages between hosts and multicast routers and learns which hosts are interested in receiving traffic for a multicast group. On the basis of what it learns, the device then forwards multicast traffic only to those interfaces in the VLAN that are connected to interested receivers instead of flooding the traffic to all interfaces.

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



### 9.3.1. Display MLD Snooping and VLAN Setting

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.

State

☐ Enable

Version

☒ MLDv1  
☐ MLDv2

Report Suppression

☒ Enable

Apply

VLAN Setting Table

Q

<input type="checkbox"/>	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
<input type="checkbox"/>	1	Disabled	Enabled	2	125	10	2	1	Disabled
<input type="checkbox"/>	2	Disabled	Enabled	2	125	10	2	1	Disabled
<input type="checkbox"/>	3	Disabled	Enabled	2	125	10	2	1	Disabled
<input type="checkbox"/>	5	Disabled	Enabled	2	125	10	2	1	Disabled
<input type="checkbox"/>	10	Disabled	Enabled	2	125	10	2	1	Disabled

Edit

Figure 9-23 MLD Snooping Property Page

Field	Description
State	Set the enabling status of IGMP Snooping functionality <ul style="list-style-type: none"> <li><b>Enable:</b> If Checked Enable IGMP Snooping, else is Disabled IGMP Snooping.</li> </ul>
Version	Set the MLD snooping version <ul style="list-style-type: none"> <li><b>MLDv1:</b> Only support process MLD v1 packet.</li> <li><b>MLDv2:</b> Support v2 basic and v1.</li> </ul>
Report Suppression	Set the enabling status of MLD v1 report suppression <ul style="list-style-type: none"> <li><b>Enable:</b> If Checked Enable MLD Snooping v1 report suppression, else Disable the report suppression function</li> </ul>
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	<input type="checkbox"/> Enable	
Router Port Auto Learn	<input checked="" type="checkbox"/> Enable	
Immediate leave	<input type="checkbox"/> 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)
<b>Operational Status</b>		
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
<b>VLAN</b>	The selected VLAN List
<b>State</b>	Set the enabling status of MLD Snooping VLAN functionality <ul style="list-style-type: none"> <li><b>Enable:</b> If Checked Enable MLD Snooping VLAN, else is Disabled MLD Snooping VLAN.</li> </ul>
<b>Router Port Auto Learn</b>	Set the enabling status of MLD Snooping router port learning <ul style="list-style-type: none"> <li><b>Enable:</b> If checked Enable learning router port by query and PIM, DVRMP, else Disable the learning router port</li> </ul>
<b>Immediate leave</b>	Immediate Leave the group when receive MLD Leave message. <ul style="list-style-type: none"> <li><b>Enable:</b> If checked Enable immediate leave, else disable immediate leave</li> </ul>
<b>Query Robustness</b>	The Admin Query Robustness allows tuning for the expected packet loss on a subnet.
<b>Query Interval</b>	The Admin interval of querier to send general query
<b>Query Max Response Interval</b>	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.
<b>Last Member Query Counter</b>	The Admin last member query count that Querier-switch sends Group-Specific Queries when it receives a Leave Group message for a group.
<b>Last Member Query Interval</b>	The Admin last member query interval that Querier-switch sends Group-Specific Queries when it receives a Leave Group message for a group.
<b>Operational Status</b>	

<b>Status</b>	Operational MLD snooping status, must both MLD snooping global and MLD snooping enable the status will be enable.
<b>Query Robustness</b>	Operational Query Robustness
<b>Query Interval</b>	Operational Query Interval
<b>Query Max Response Interval</b>	Operational Query Max Response Interval
<b>Last Member Query Counter</b>	Operational Last Member Query Count
<b>Last Member Query Interval</b>	Operational Last Member Query Interval

**Table 9-24 MLD Snooping VLAN Edit Fields**

### 9.3.2. MLD Snooping Statistics

To display MLD Snooping Statistics, click Multicast> MLD Snooping> Statistics  
This page allow user to clear MLD snooping statics.

**Multicast>> MLD Snooping>> Statistic**

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 9-25 MLD Snooping Statistics Page**

Field	Description
<b>Rx Packet Total</b>	Total RX MLD packet, include ipv4 multicast data to CPU.
<b>Valid MLD Snooping</b>	The valid MLD snooping process packet.
<b>In Valid MLD Snooping</b>	The invalid MLD snooping process packet.
<b>Other</b>	The ICMPV6 type is not MLD, and is not ipv6 multicast data packet, and is not IPV6 router protocol.
<b>Leave</b>	MLD leave packet.
<b>Report</b>	MLD join and report packet
<b>General Query</b>	MLD General Query packet
<b>Special Group Query</b>	MLD Special Group General Query packet
<b>Source-specific Group Query</b>	MLD Special Source and Group General Query packet
Transmit Packet	
<b>Leave</b>	MLD leave packet
<b>Report</b>	MLD join and report packet
<b>General Query</b>	MLD general query packet
<b>Special Group Query</b>	MLD special group query packet
<b>Source-specific Group Query</b>	MLD Special Source and Group General Query packet

**Table 9-25 MLD Snooping Statistics Fields**

## 9.4. MVR

Multicast VLAN registration (MVR) enables more efficient distribution of IPTV multicast streams across an Ethernet ring-based Layer 2 network.

In a standard Layer 2 network, a multicast stream received on one VLAN is never distributed to interfaces outside that VLAN. If hosts in multiple VLANs request the same multicast stream, a separate copy of that multicast stream is distributed to each requesting VLAN.

When you configure MVR, you create a *multicast VLAN* (MVLAN) that becomes the only VLAN over which IPTV multicast traffic flows throughout the Layer 2 network. Devices with MVR enabled selectively forward IPTV multicast traffic from interfaces on the MVLAN (source interfaces) to hosts that are connected to interfaces that are not part of the MVLAN that you designate as *MVR receiver ports*. MVR receiver ports can receive traffic from a port on the MVLAN but cannot send traffic onto the MVLAN, and those ports remain in their own VLANs for bandwidth and security reasons.

Use the MVR pages to configure settings of MVR function.

### 9.4.1. Displaying Multicast MVR Property Settings

To display multicast MVR property Setting web page, click **Multicast> MVR> Property**  
This page allow user to set MVR property.

Figure 9-26 Multicast MVR Properties Page

Field	Description
State	<ul style="list-style-type: none"> <li><b>Enable:</b> if checked enable the MVR state, else disable the MVR state</li> </ul>
VLAN	The MVR VLAN ID
Mode	Set the MVR mode. <ul style="list-style-type: none"> <li><b>Compatible:</b> compatible mode</li> <li><b>Dynamic:</b> dynamic mode, will learn group member on source port</li> </ul>
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. MVR Port Settings

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**

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

Edit

**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	<input checked="" type="radio"/> None <input type="radio"/> Receiver <input type="radio"/> Source
Immediate Leave	<input checked="" type="checkbox"/> Enable

Apply Close

**Figure 9-30 Multicast MVR Port Setting Edit Page**



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

Table 9-31 MVR Port Setting Edit Fields

### 9.4.3. Multicast MVR 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.

#### Group Address Table

Showing  entries Showing 0 to 0 of 0 entries

<input type="checkbox"/>	VLAN	Group Address	Member	Type	Life (Sec)
0 results found.					

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 lifetime of this dynamic MVR group.

Table 9-33 MVR Group Address Table Fields

**Multicast >>MVR >>Group Address**

#### Add Group Address

VLAN 2

Group Address

Member

Available Port

Selected Port

Figure 9-34 Multicast MVR Group Address Add Page

Field	Description
VLAN	The VLAN ID of MVR group.
Group Address	MVR group IP address.
Member	The member ports of MVR group. <ul style="list-style-type: none"> <li><b>Available Port:</b> Optional port member, it is only receiver port when MVR mode is compatible, it include source port when mode is dynamic</li> <li><b>Selected Port:</b> Selected port member</li> </ul>

Table 9-35 MVR Group Address Add Fields

## Multicast> MVR> Group Address

### Edit Group Address

Figure 9-36 Multicast MVR Group Address Edit Page

Field	Description
<b>VLAN</b>	The VLAN ID of edited MVR group.
<b>Group Address</b>	The edited MVR group IP address.
<b>Member</b>	<p>The member ports of MVR group.</p> <ul style="list-style-type: none"> <li><b>Available Port:</b> Optional port member, it is only receiver port when MVR mode is compatible, it include source port when mode is dynamic</li> <li><b>Selected Port:</b> Selected port member</li> </ul>

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.

Security >> RADIUS

Use Default Parameter

Retry	<input type="text" value="3"/>	(1 - 10, default 3)
Timeout	<input type="text" value="3"/>	Sec (1 - 30, default 3)
Key String	<input type="text"/>	

Apply

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
<input type="checkbox"/>	192.168.1.98	1812	1	3	3	All

Add Edit Delete First Previous 1 Next Last

Figure 10-2 RADIUS Table

Field	Description
Server Address	RADIUS server address
Server Port	RADIUS server port
Priority	RADIUS server priority (smaller value has higher priority). RADIUS session will try to establish with the server setting which has highest priority. If failed, it will try to connect to the server with next higher priority.
Retry	RADIUS server retry value. If it is fail to connect to server, it will keep trying until timeout with retry times.
Timeout	RADIUS server timeout value. If it is fail to connect to server, it will keep trying until timeout.
Usage	RADIUS server usage type <ul style="list-style-type: none"> <li>Login: For login authentication</li> <li>802.1x: For 802.1x authentication</li> </ul> All: For all types

Table 10-2 RADIUS Table Fields

### Add RADIUS Server

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

### Edit RADIUS Server

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

**Figure 10-3 Add/Edit RADIUS Server Dialog**

Field	Description
<b>Address Type</b>	In add dialog, user need to specify server Address Type <ul style="list-style-type: none"> <li><b>Hostname:</b> Use domain name as server address</li> <li><b>IPv4:</b> Use IPv4 as server address</li> <li><b>IPv6:</b> Use IPv6 as server address</li> </ul>
<b>Server Address</b>	In add dialog, user need to input server address based on address type. In edit dialog, it shows current edit server address.
<b>Server Port</b>	Set RADIUS server port
<b>Priority</b>	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.
<b>Retry</b>	Set RADIUS server retry value. If it is fail to connect to server, it will keep trying until timeout with retry times.
<b>Timeout</b>	Set RADIUS server timeout value. If it is fail to connect to server, it will keep trying until timeout.
<b>Usage</b>	Set RADIUS server usage type <ul style="list-style-type: none"> <li><b>Login:</b> For login authentication</li> <li><b>802.1x:</b> For 802.1x authentication</li> <li><b>All:</b> For all types</li> </ul>

**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

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

#### Edit TACACS+ Server

Server Address	192.168.1.97	
Server Port	49	(0 - 65535, default 49)
Priority	1	(0 - 65535)
Key String	<input checked="" type="checkbox"/> Use Default <input type="text"/>	
Timeout	<input checked="" type="checkbox"/> Use Default <input type="text" value="5"/> Sec (1 - 30, default 5)	

Field	Description
Address Type	In add dialog, user need to specify server Address Type <ul style="list-style-type: none"> <li><b>Hostname:</b> Use domain name as server address</li> <li><b>IPv4:</b> Use IPv4 as server address</li> <li><b>IPv6:</b> Use IPv6 as server address</li> </ul>
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 a connection with the server setting which has highest priority. If it fails, it will try to connect to the server with next higher priority.
Timeout	Set TACACS+ server timeout value. If it fails to connect to the 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.

#### Method List Table

Showing  entries      Showing 1 to 2 of 2 entries     

<input type="checkbox"/>	Name	Sequence
<input type="checkbox"/>	default	(1) Local
<input type="checkbox"/>	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. <ul style="list-style-type: none"> <li>• <b>None:</b> Authenticated with any condition.</li> <li>• <b>Local: Use local accounts database to authenticate</b></li> <li>• <b>TACACS+:</b> Use remote TACACS+ server to authenticate.</li> <li>• <b>RADIUS:</b> Use remote Radius server to authenticate.</li> <li>• <b>Enable:</b> Use local enable password to authenticate</li> </ul>

Table 10-7 Method List Table Fields

Add Method List

Name	<input type="text"/>
Method 1	<input checked="" type="radio"/> Empty <input type="radio"/> None <input type="radio"/> Local <input type="radio"/> Enable <input type="radio"/> RADIUS <input type="radio"/> TACACS+
Method 2	<input checked="" type="radio"/> Empty <input type="radio"/> None <input type="radio"/> Local <input type="radio"/> Enable <input type="radio"/> RADIUS <input type="radio"/> TACACS+
Method 3	<input checked="" type="radio"/> Empty <input type="radio"/> None <input type="radio"/> Local <input type="radio"/> Enable <input type="radio"/> RADIUS <input type="radio"/> TACACS+
Method 4	<input checked="" type="radio"/> Empty <input type="radio"/> None <input type="radio"/> Local <input type="radio"/> Enable <input type="radio"/> RADIUS <input type="radio"/> TACACS+

Edit Method List

Name	TEST
Method 1	<input type="radio"/> Empty <input type="radio"/> None <input type="radio"/> Local <input type="radio"/> Enable <input type="radio"/> RADIUS <input checked="" type="radio"/> TACACS+
Method 2	<input checked="" type="radio"/> Empty <input type="radio"/> None <input type="radio"/> Local <input type="radio"/> Enable <input type="radio"/> RADIUS <input type="radio"/> TACACS+
Method 3	<input type="radio"/> Empty <input type="radio"/> None <input checked="" type="radio"/> Local <input type="radio"/> Enable <input type="radio"/> RADIUS <input type="radio"/> TACACS+
Method 4	<input checked="" type="radio"/> Empty <input type="radio"/> None <input type="radio"/> Local <input type="radio"/> Enable <input type="radio"/> RADIUS <input type="radio"/> TACACS+

Figure 10-8 Add/Edit Method List Dialog

Field	Description
<b>Name</b>	Login authentication list name. This name should be different from other existing lists.
<b>Method 1</b>	Select first priority of login authentication method. <ul style="list-style-type: none"> <li>• <b>None:</b> Authenticated with any condition. <b>Local: Use local accounts database to authenticate</b></li> <li>• <b>TACACS+:</b> Use remote TACACS+ server to authenticate.</li> <li>• <b>RADIUS:</b> Use remote Radius server to authenticate.</li> <li>• <b>Enable:</b> Use local enable password to authenticate</li> </ul>
<b>Method 2</b>	Select second priority of login authentication method. <ul style="list-style-type: none"> <li>• <b>None:</b> Authenticated with any condition.</li> <li>• <b>Local: Use local accounts database to authenticate</b></li> <li>• <b>TACACS+:</b> Use remote TACACS+ server to authenticate.</li> </ul>
	<ul style="list-style-type: none"> <li>• <b>RADIUS:</b> Use remote Radius server to authenticate.</li> <li>• <b>Enable:</b> Use local enable password to authenticate</li> </ul>
<b>Method 3</b>	Select third priority of login authentication method. <ul style="list-style-type: none"> <li>• <b>None:</b> Authenticated with any condition.</li> <li>• <b>Local:</b> Use local accounts database to authenticate</li> <li>• <b>TACACS+:</b> Use remote TACACS+ server to authenticate.</li> <li>• <b>RADIUS:</b> Use remote Radius server to authenticate.</li> <li>• <b>Enable:</b> Use local enable password to authenticate</li> </ul>
<b>Method 4</b>	Select fourth priority of login authentication method. <ul style="list-style-type: none"> <li>• <b>None:</b> Authenticated with any condition.</li> <li>• <b>Local: Use local accounts database to authenticate</b></li> <li>• <b>TACACS+:</b> Use remote TACACS+ server to authenticate.</li> <li>• <b>RADIUS:</b> Use remote Radius server to authenticate.</li> <li>• <b>Enable:</b> Use local enable password to authenticate</li> </ul>

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.

The screenshot shows a web interface for configuring login authentication. It features a table with five rows, each representing a different management interface. Each row has a label (Console, Telnet, SSH, HTTP, HTTPS) and a configuration area. The configuration area includes a dropdown menu for the authentication method and a text field for the authentication list name. Below the table is an 'Apply' button.

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.

**Security>> management Access>> Management VLAN**

Management VLAN

1 - default

Note: Change Management VLAN may cause connection interrupted

Apply

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.

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. <ul style="list-style-type: none"> <li>• Telnet: Connect CLI through telnet</li> <li>• SSH: Connect CLI through SSH</li> <li>• HTTP: Connect WEBUI through HTTP</li> <li>• HTTPS: Connect WEBUI through HTTPS</li> <li>• SNMP: Manage switch through SNMP</li> </ul>
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.

### 10.3.3. 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.

#### Security>>Management Access>>Management ACL

**Figure 10-12 Management ACL Page**

Field	Description
ACL Name	Input MAC ACL name

**Table 10-12 Management ACL Fields**

#### Management ACL Table

**Figure 10-13 Management ACL Table Page**

#### 10.4.4. Management Services

To display the Management Service click **Security > Management Access > Management Service**  
This page allow user to change management services related configurations.

**Management Service**

Telnet	<input type="checkbox"/> Enable
SSH	<input type="checkbox"/> Enable
HTTP	<input checked="" type="checkbox"/> Enable
HTTPS	<input type="checkbox"/> Enable
SNMP	<input type="checkbox"/> Enable

**Session Timeout**

Console	<input type="text" value="10"/>	Min (0 - 65535, default 10)
Telnet	<input type="text" value="10"/>	Min (0 - 65535, default 10)
SSH	<input type="text" value="10"/>	Min (0 - 65535, default 10)
HTTP	<input type="text" value="10"/>	Min (0 - 65535, default 10)
HTTPS	<input type="text" value="10"/>	Min (0 - 65535, default 10)

**Password Retry Count**

Console	<input type="text" value="3"/>	(0 - 120, default 3)
Telnet	<input type="text" value="3"/>	(0 - 120, default 3)
SSH	<input type="text" value="3"/>	(0 - 120, default 3)

**Silent Time**

Console	<input type="text" value="0"/>	Sec (0 - 65535, default 0)
Telnet	<input type="text" value="0"/>	Sec (0 - 65535, default 0)
SSH	<input type="text" value="0"/>	Sec (0 - 65535, default 0)

Figure 10-11 Management Service Page

Field	Description
Management Service	Management service admin state. <ul style="list-style-type: none"> <li>• <b>Telnet:</b> Connect CLI through telnet</li> <li>• <b>SSH:</b> Connect CLI through SSH</li> <li>• <b>HTTP:</b> Connect WEBUI through HTTP</li> <li>• <b>HTTPS:</b> Connect WEBUI through HTTPS</li> <li>• <b>SNMP:</b> Manage switch trough SNMP</li> </ul>
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

### 10.4.5. Management ACL

To display Management ACL page, click **Security > Management Access > Management ACL**. This page allow user to add or delete management ACL rule. A rule cannot be deleted if under active.

**Security>> Management Access>> Management ACL**

**Figure 10-12 Management ACL Page**

Field	Description
ACL Name	Input MAC ACL name

**Table 10-12 Management ACL Fields**

**Figure 10-13 Management ACL Table Page**

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

**Table 10-13 Management ACL Table Fields**

### 10.4.6. 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**

### Add Managemet ACE

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

### Edit Managemet ACE

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

**Figure 10-15 Add and Edit Management ACE Dialog**

Field	Description
<b>ACL Name</b>	Display the ACL name to which an ACE is being added.
<b>Priority</b>	Specify the priority of the ACE. ACEs with higher sequence are processed first (1 is the highest priority). Only available on Add Dialogue
<b>Service</b>	Select the type service of rule. <ul style="list-style-type: none"> <li>• All: All services</li> <li>• HTTP: Only HTTP service.</li> <li>• HTTPs: Only HTTPs service.</li> <li>• SNMP: Only SNMP service.</li> <li>• SSH: Only SSH service.</li> <li>• Telnet: Only Telnet service.</li> </ul>
<b>Action</b>	Select the action after ACE match packet. <ul style="list-style-type: none"> <li>• Permit: Forward packets that meet the ACE criteria.</li> <li>• Deny: Drop packets that meet the ACE criteria.</li> </ul>
<b>Port</b>	Select ports which will be matched.
<b>IP Version</b>	<ul style="list-style-type: none"> <li>• Select the type of source IP address.</li> <li>• All: All IP addresses can access.</li> <li>• IPv4: Specify IPv4 address ca access</li> <li>• IPv6: Specify IPv6 address ca access</li> </ul>
<b>IPv4</b>	Enter the source IPv4 address value and mask to which will be matched.
<b>IPv6</b>	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.

**Security>> Authentication Manager>> Property**

The screenshot displays the 'Authentication Manager' configuration page. It features a sidebar on the left with the title 'Authentication Manager' and a main content area on the right. The main area is divided into three sections: 'Authentication Type' with four unchecked checkboxes (802.1x, MAC-Based, WEB-Based, Enable), 'Guest VLAN' with a dropdown menu set to '1', and 'MAC-Based User ID Format' with a dropdown menu set to 'XXXXXXXXXXXX'. An 'Apply' button is located at the bottom left of the main content area.

**Figure 10-16 Authentication Manager Global Setting**

Field	Description
<b>Authentication Type</b>	Set checkbox to enable/disable following authentication types <ul style="list-style-type: none"> <li><b>802.1x:</b> Use IEEE 802.1x to do authentication</li> <li><b>AC-Based:</b> Use MAC address to do authentication</li> <li><b>WEB-Based:</b> Prompt authentication web page for user to do authentication</li> </ul>
<b>Guest VLAN</b>	Set checkbox to enable/disable guest VLAN, if guest VLAN is enabled, you need to select one available VLAN ID to be guest VID.
<b>MAC-Based User ID Format</b>	Select mac-based authentication RADIUS username/password ID format. XXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXX 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 XXXXXXXX:XXXXXXXX xxxxxxx:xxxxxxx XXXXXXXX-XXXXX xxxxxx-xxxxxxx XXXXXXXX.XXXXX xxxxxx.xxxxxx XXXXXXXX.XXXXX xxxxxx.xxxxxx

Table 10-16 Authentication Manager Global Setting Fields

Port Mode Table

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

Edit

Figure 10-17 Port Mode Table



Field	Description
<b>Authentication Type (802.1X)</b>	802.1 X authentication type state <b>Enabled:</b> 802.1X is enabled <b>Disabled:</b> 802.1X is disabled
<b>Authentication Type (MAC-Based)</b>	MAC-Based authentication type state <b>Enabled:</b> MAC-Based authentication is enabled <b>Disabled:</b> MAC-Based authentication is disabled
<b>Authentication Type (WEB-Based)</b>	WEB-Based authentication type state <b>Enabled:</b> WEB-Based authentication is enabled <b>Disabled:</b> WEB-Based authentication is disabled
<b>Host Mode</b>	Authenticating host mode <b>Multiple Authentication:</b> In this mode, every client need to pass authenticate procedure individually. <b>Multiple Hosts:</b> 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. <b>Single Host:</b> 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.
<b>Order</b>	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. <b>802.1x</b> <b>MAC-Based</b> <b>WEB-Based</b> <b>802.1x MAC-Based</b> <ul style="list-style-type: none"> <li>802.1x WEB-Based</li> <li>MAC-Based 802.1x</li> <li>WEB-Based 802.1x</li> <li>802.1x MAC-Based WEB-Based</li> <li>802.1x WEB-Based MAC-Based</li> </ul>
<b>Method</b>	Support following authentication method order combinations. These orders only available on MAC-Based authentication and WEB-Based authentication. 802.1x only support Radius method. <ul style="list-style-type: none"> <li><b>Local:</b> Use DUT's local database to do authentication</li> <li><b>Radius:</b> Use remote RADIUS server to do authentication</li> <li>Local Radius</li> <li>Radius Local</li> </ul>
<b>Guest VLAN</b>	Port guest VLAN enable state <ul style="list-style-type: none"> <li><b>Enabled:</b> Guest VLAN is enabled on port</li> <li><b>Disabled:</b> Guest VLAN is disabled on port</li> </ul>
<b>VLAN Assign Mode</b>	Support following VLAN assign mode and only apply when source is RADIUS <ul style="list-style-type: none"> <li><b>Disable:</b> Ignore the VLAN authorization result and keep original VLAN of host.</li> <li><b>Reject:</b> If get VLAN Authorised information, just use it. However, if there is no VLAN Authorised information, reject the host and make it unAuthorised.</li> <li><b>Static:</b> If get VLAN Authorised information, just use it. If there is no VLAN Authorised information, keep original VLAN of host.</li> </ul>

Table 10-17 Port Mode



### 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
<input type="checkbox"/>	1	GE1	Disabled	Disabled	256	3600	60	60	30	30	
<input type="checkbox"/>	2	GE2	Disabled	Disabled	256	3600	60	60	30	30	
<input type="checkbox"/>	3	GE3	Disabled	Disabled	256	3600	60	60	30	30	
<input type="checkbox"/>	4	GE4	Disabled	Disabled	256	3600	60	60	30	30	
<input type="checkbox"/>	5	GE5	Disabled	Disabled	256	3600	60	60	30	30	
<input type="checkbox"/>	6	GE6	Disabled	Disabled	256	3600	60	60	30	30	
<input type="checkbox"/>	7	GE7	Disabled	Disabled	256	3600	60	60	30	30	
<input type="checkbox"/>	8	GE8	Disabled	Disabled	256	3600	60	60	30	30	
<input type="checkbox"/>	9	GE9	Disabled	Disabled	256	3600	60	60	30	30	
<input type="checkbox"/>	10	GE10	Disabled	Disabled	256	3600	60	60	30	30	

Edit

**Figure 10-19: Authentication Manager Port Setting Table**

Field	Description
<b>Port</b>	Port name
<b>Port Control</b>	Support following authentication port control types. <b>Disable:</b> Disable authentication function and all clients have network accessibility. <b>Force Authorised:</b> Port is force Authorised and all clients have network accessibility. <b>Force Unauthorised:</b> Port is force unAuthorised and all clients have no network accessibility. <b>Auto:</b> Need passing authentication procedure to get network accessibility.
<b>Reauthentication</b>	<b>Reauthenticate state</b> <b>Enabled:</b> Host will be reauthenticated after reauthentication period <b>Disabled:</b> Host will not be reauthenticated after reauthentication period
<b>Max Hosts</b>	In Multiple Authentication mode, total host number cannot not exceed max hosts number
<b>Common Timer (Reauthentication)</b>	After re-authenticate period, host will return to initial state and need to pass authentication procedure again.
<b>Common Timer (Inactive)</b>	If no packet from the authenticated host, the inactive timer will increase. After inactive timeout, the host will be unauthorised and corresponding session will be deleted. In multi-host mode, the packet is counting on the Authorised host only and not all packets on the port.
<b>Common Timer (Quiet)</b>	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.

<b>802.1X Params (TX Period)</b>	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.
<b>802.1X Params (Supplicant Timeout)</b>	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.
<b>802.1X Params (Server Timeout)</b>	Number of seconds that lapses before EAP requests are resent to the supplicant.
<b>802.1X Params (Max Request)</b>	Number of seconds that lapses before the device resends a request to the authentication server.
<b>Web-Based Param (Max Login)</b>	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	<input checked="" type="radio"/> Disabled <input type="radio"/> Force Authorized <input type="radio"/> Force Unauthorized <input type="radio"/> Auto	
Reauthentication	<input type="checkbox"/> Enable	
Max Hosts	256	(1 - 256, default 256)
<b>Common Timer</b>		
Reauthentication	3600	Sec (300 - 2147483647, default 3600)
Inactive	60	Sec (60 - 65535, default 60)
Quiet	60	Sec (0 - 65535, default 60)
<b>802.1x Parameters</b>		
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)
<b>Web-Based Parameters</b>		
Max Login	<input type="checkbox"/> Infinite 3	(3 - 10, default 3)

**Figure 10-20: Authentication Manager Port Setting Dialog**

Field	Description
<b>Port</b>	Port name
<b>Port Control</b>	Support following authentication port control types. <b>Disable:</b> Disable authentication function and all clients have network accessibility. <b>Force Authorised:</b> Port is force Authorised and all clients have network accessibility. <b>Force Unauthorised:</b> Port is force unAuthorised and all clients have no network accessibility. <b>Auto:</b> Need passing authentication procedure to get network accessibility.
<b>Reauthentication</b>	Set checkbox to enable/disable reauthentication
<b>Max Hosts</b>	In Multiple Authentication mode, total host number cannot not exceed max number hosts number
<b>Common Timer (Reauthentication)</b>	After re-authenticate period, host will return to initial state and need to pass authentication procedure again.
<b>Common Timer (Inactive)</b>	If no packet from the authenticated host, the inactive timer will increase. After inactive timeout, the host will be unauthorised, and corresponding session will be deleted. In multi-host mode, the packet is counting on the Authorised host only and not all packets on the port.
<b>Common Timer (Quiet)</b>	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
<b>802.1X Params (TX Period)</b>	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.
<b>802.1X Params (Supplicant Timeout)</b>	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.
<b>802.1X Params (Server Timeout)</b>	Number of seconds that lapses before EAP requests are resent to the supplicant.
<b>802.1X Params (Max Request)</b>	Number of seconds that lapses before the device resends a request to the authentication server.
<b>Web-Based Param (Max Login)</b>	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.

**Security>> Authentication Manager>> MAC Based Local Account.**

**MAC-Based Local Account Table**

Showing  entries      Showing 1 to 1 of 1 entries     

	MAC Address	Control	VLAN	Timeout (Sec)	
				Reauthentication	Inactive
<input type="checkbox"/>	00:00:00:00:00:0A	Force Authorized	N/A	3600	60

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	<b>Control Type</b> <b>Force Authorised:</b> Host will be force Authorised <b>Force UnAuthorised:</b> Host will be force unAuthorised
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	<input type="text"/>
Port Control	<input type="radio"/> Force Authorized <input checked="" type="radio"/> Force Unauthorized
VLAN	<input type="checkbox"/> User Defined <input type="text" value="1"/> (1 - 4094)
<b>Assigned Timer</b>	
Reauthentication	<input type="checkbox"/> User Defined <input type="text" value="3600"/> Sec (300 - 2147483647)
Inactive	<input type="checkbox"/> User Defined <input type="text" value="60"/> Sec (60 - 65535)

**Edit MAC-Based Local Account**

<b>MAC Address</b>	00:00:00:00:00:0A		
<b>Port Control</b>	<input checked="" type="radio"/> Force Authorized <input type="radio"/> Force Unauthorized		
<b>VLAN</b>	<input type="checkbox"/> User Defined <input type="text" value="1"/> (1 - 4094)		
<b>Assigned Timer</b>			
<b>Reauthentication</b>	<input checked="" type="checkbox"/> User Defined	<input type="text" value="3600"/>	Sec (300 - 2147483647)
<b>Inactive</b>	<input checked="" type="checkbox"/> User Defined	<input type="text" value="60"/>	Sec (60 - 65535)

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

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

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

#### 10.5.4 WEB-Based Local Account

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

This page allow user to add/edit/delete WEB-Based authentication local accounts.  
**Security>> Authentication Manager>> WEB Based Local Account.**

**WEB-Based Local Account Table**

Showing All entries Showing 1 to 2 of 2 entries

	Username	VLAN	Timeout (Sec)	
			Reauthentication	Inactive
<input type="checkbox"/>	admin11	N/A	3600	60
<input type="checkbox"/>	admin	N/A	3600	60

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.
<b>Table 10-23 WEB-Based Local Account Table Fields</b>	

### Security>> Authentication Manager>> WEB Based Local Account.

#### Add WEB-Based Local Account

Username	admin11	
Password	*****	
Confirm Password	*****	
VLAN	<input type="checkbox"/> User Defined <input type="text" value="1"/> (1 - 4094)	
<b>Assigned Timer</b>		
Reauthentication	<input checked="" type="checkbox"/> User Defined <input type="text" value="3600"/> Sec (300 - 2147483647)	
Inactive	<input checked="" type="checkbox"/> User Defined <input type="text" value="60"/> Sec (60 - 65535)	
<input type="button" value="Apply"/> <input type="button" value="Close"/>		

#### Edit WEB-Based Local Account

Username	admin11	
Password		
Confirm Password	*****	
VLAN	<input type="checkbox"/> User Defined <input type="text" value=""/> (1 - 4094)	
<b>Assigned Timer</b>		
Reauthentication	<input checked="" type="checkbox"/> User Defined <input type="text" value="3600"/> Sec (300 - 2147483647)	
Inactive	<input checked="" type="checkbox"/> User Defined <input type="text" value="60"/> Sec (60 - 65535)	
<input type="button" value="Apply"/> <input type="button" value="Close"/>		

**Figure 10-24 Add/Edit WEB-Based Local Account Dialog**

Field	Description
Username	Authenticating account user name
Password	Authenticating account password
Confirm Password	Confirm authenticating account password
VLAN	Assigned VLAN ID for the authenticated host.
Timeout (Reauthentication)	Assigned reauthentication period for the authenticated host.
Timeout (Inactive)	Assigned inactive timeout for the authenticated host.
<b>Table 10-24 Add/Edit WEB-Based Local Account Fields</b>	

### 10.5.4. Sessions

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

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

Security>> Authentication Manager>> Sessions

**Sessions Table**

Showing  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.												

Figure 10-25 Sessions Table

Field	Description
<b>Session ID</b>	Session ID is unique of each session
<b>Port</b>	Port name which the host located
<b>MAC Address</b>	Host MAC address
<b>Current Type</b>	Show current authenticating type <b>802.1x:</b> Use IEEE 802.1X to do authenticating <b>MAC-Based:</b> Use MAC-Based authentication to do authenticating <b>WEB-Based:</b> Use WEB-Based authentication to do authenticating
<b>Status</b>	Show host authentication session status <b>Disable:</b> This session is ready to be deleted <b>Running:</b> Authentication process is running <b>Authorised:</b> Authentication is passed and getting network accessibility. <b>UnAuthorised:</b> Authentication is not passed and not getting network accessibility. <b>Locked:</b> Host is locked and do not allow to do authenticating until quiet period. <b>Guest :</b> Host is in the guest VLAN
<b>Operational (VLAN)</b>	Shows host operational VLAN ID.
<b>Operational (Session Time)</b>	In "Authorised" state, it shows total time after Authorised.
<b>Operational (Inactive)</b>	In "Authorised" state, it shows how long the host do not send any packet.
<b>Operational (Quiet Time)</b>	In "Locked" state, it shows total time after locked.
<b>Authorised (VLAN)</b>	Shows VLAN ID given from Authorised procedure.
<b>Authorised (Reauthentication Period)</b>	Shows reauthentication period given from Authorised procedure.
<b>Authorised (Inactive Timeouts)</b>	Shows inactive timeout given from Authorised 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 a learned MAC address has gone over its limit.

State

☐ Enable

Rate Limit

 Packet / Sec (1 - 600, default 100)

Apply

Edit

Figure 10-26 Port Security Page

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

To display the 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.

#### Security > Protected Port

##### Protected Port Table

<input type="checkbox"/>	Entry	Port	State
<input type="checkbox"/>	1	GE1	Unprotected
<input type="checkbox"/>	2	GE2	Unprotected
<input type="checkbox"/>	3	GE3	Unprotected
<input type="checkbox"/>	4	GE4	Unprotected
<input type="checkbox"/>	5	GE5	Unprotected
<input type="checkbox"/>	6	GE6	Unprotected
<input type="checkbox"/>	7	GE7	Unprotected
<input type="checkbox"/>	8	GE8	Unprotected
<input type="checkbox"/>	9	GE9	Unprotected
<input type="checkbox"/>	10	GE10	Unprotected
<input type="checkbox"/>	11	LAG1	Unprotected
<input type="checkbox"/>	12	LAG2	Unprotected
<input type="checkbox"/>	13	LAG3	Unprotected
<input type="checkbox"/>	14	LAG4	Unprotected
<input type="checkbox"/>	15	LAG5	Unprotected
<input type="checkbox"/>	16	LAG6	Unprotected
<input type="checkbox"/>	17	LAG7	Unprotected
<input type="checkbox"/>	18	LAG8	Unprotected

Figure 10-27 The Protected Port Table

Field	Description
Port	Port Name
State	Port protected admin state. <b>Protected:</b> Port is protected. <b>Unprotected:</b> Port is unprotected

Table 10-28 Edit Protected Port Fields

## 10.8. Storm Control

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

Mode

☐ Packet / Sec  
☒ Kbits / Sec

IFG

☒ Exclude  
☐ Include

Apply

**Port Setting Table**

Q

	Entry	Port	State	Broadcast		Unknown Multicast		Unknown Unicast		Action
				State	Rate (Kbps)	State	Rate (Kbps)	State	Rate (Kbps)	
<input type="checkbox"/>	1	GE1	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
<input type="checkbox"/>	2	GE2	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
<input type="checkbox"/>	3	GE3	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
<input type="checkbox"/>	4	GE4	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
<input type="checkbox"/>	5	GE5	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
<input type="checkbox"/>	6	GE6	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
<input type="checkbox"/>	7	GE7	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
<input type="checkbox"/>	8	GE8	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
<input type="checkbox"/>	9	GE9	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
<input type="checkbox"/>	10	GE10	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop

Edit

Figure 10-29 Storm Control Setting Page

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

Table 10-29 Storm Control Global Setting Fields

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

**Edit Port Setting**

---

<b>Port</b>	GE1
<b>State</b>	<input type="checkbox"/> Enable
<b>Broadcast</b>	<input type="checkbox"/> Enable 10000 Kbps (16 - 1000000, default 10000)
<b>Unknown Multicast</b>	<input type="checkbox"/> Enable 10000 Kbps (16 - 1000000, default 10000)
<b>Unknown Unicast</b>	<input type="checkbox"/> Enable 10000 Kbps (16 - 1000000, default 10000)
<b>Action</b>	<input checked="" type="radio"/> Drop <input type="radio"/> Shutdown

Apply Close

**Figure 10-30 Storm Control Edit Port Setting Page**

Field	Description
<b>Port</b>	Select the setting ports
<b>State</b>	Select the state of setting <b>Enable:</b> Enable the storm control function.
<b>Broadcast</b>	<b>Enable:</b> 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.
<b>Unknown Multicast</b>	<b>Enable:</b> 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.
<b>Unknown Unicast</b>	<b>Enable:</b> 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.
<b>Action</b>	Select the state of setting <b>Drop: Packets exceed storm control rate will be dropped.</b> 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 when a hacker attempts 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.

### 10.10.1. DOS Global Setting

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

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

Apply

**Figure 10-31 DoS Property Page**

Field	Description
<b>POD</b>	Avoids ping of death attack.
<b>Land</b>	Drops the packets if the source IP address is equal to the destination IP address.
<b>UDP Blat</b>	Drops the packets if the UDP source port equals to the UDP destination port.
<b>TCP Blat</b>	Drops the packages if the TCP source port is equal to the TCP destination port.
<b>DMAC = SMAC</b>	Drops the packets if the destination MAC address is equal to the source MAC address.
<b>Null Scan Attack</b>	Drops the packets with NULL scan.
<b>X-Mas Scan Attack</b>	Drops the packets if the sequence number is zero, and the FIN, URG and PSH bits are set.
<b>TCP SYN-FIN Attack</b>	Drops the packets with SYN and FIN bits set.
<b>TCP SYN-RST Attack</b>	Drops the packets with SYN and RST bits set.

<b>ICMP Fragment</b>	Drops the fragmented ICMP packets.
<b>TCP-SYN(SPORT&lt;1024)</b>	Drops SYN packets with sport less than 1024.
<b>TCP Fragment (Offset = 1)</b>	Drops the TCP fragment packets with offset equals to one.
<b>Ping Max Size</b>	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.
<b>IPv4 Ping Max Size</b>	Checks the maximum size of ICMP ping packets, and drops the packets larger than the maximum packet size.
<b>IPv6 Ping Max Size</b>	Checks the maximum size of ICMPv6 ping packets, and drops the packets larger than the maximum packet size.
<b>TCP Min Hdr Size</b>	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.
<b>IPv6 Min Fragment</b>	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.
<b>Smurf Attack</b>	Avoids smurf attack. The length range of the netmask is from 0 to 323 bytes, and default length is 0 bytes.
<b>Table 10-31: DoS Property fields.</b>	

### 10.9.2 Port Setting

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

Port Setting Table

<input type="checkbox"/>	Entry	Port	State
<input type="checkbox"/>	1	GE1	Disabled
<input type="checkbox"/>	2	GE2	Disabled
<input type="checkbox"/>	3	GE3	Disabled
<input type="checkbox"/>	4	GE4	Disabled
<input type="checkbox"/>	5	GE5	Disabled
<input type="checkbox"/>	6	GE6	Disabled
<input type="checkbox"/>	7	GE7	Disabled
<input type="checkbox"/>	8	GE8	Disabled
<input type="checkbox"/>	9	GE9	Disabled
<input type="checkbox"/>	10	GE10	Disabled
<input type="checkbox"/>	11	LAG1	Disabled
<input type="checkbox"/>	12	LAG2	Disabled
<input type="checkbox"/>	13	LAG3	Disabled
<input type="checkbox"/>	14	LAG4	Disabled
<input type="checkbox"/>	15	LAG5	Disabled
<input type="checkbox"/>	16	LAG6	Disabled
<input type="checkbox"/>	17	LAG7	Disabled
<input type="checkbox"/>	18	LAG8	Disabled

Edit

Figure 10-32: Port Setting page.

Field	Description
<b>Port</b>	Interface or port number.
<b>State</b>	Enable/Disable the DoS protection on the interface.
<b>Table 10-32: Port Setting fields.</b>	



## 10.10. Dynamic ARP Inspection

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

### 10.11.1. Display Security Property Page

To display the 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	
<input type="checkbox"/>	1	GE1	Disabled	Disabled	Disabled	Disabled	Unlimited	
<input type="checkbox"/>	2	GE2	Disabled	Disabled	Disabled	Disabled	Unlimited	
<input type="checkbox"/>	3	GE3	Disabled	Disabled	Disabled	Disabled	Unlimited	
<input type="checkbox"/>	4	GE4	Disabled	Disabled	Disabled	Disabled	Unlimited	
<input type="checkbox"/>	5	GE5	Disabled	Disabled	Disabled	Disabled	Unlimited	
<input type="checkbox"/>	6	GE6	Disabled	Disabled	Disabled	Disabled	Unlimited	
<input type="checkbox"/>	7	GE7	Disabled	Disabled	Disabled	Disabled	Unlimited	
<input type="checkbox"/>	8	GE8	Disabled	Disabled	Disabled	Disabled	Unlimited	
<input type="checkbox"/>	9	GE9	Disabled	Disabled	Disabled	Disabled	Unlimited	
<input type="checkbox"/>	10	GE10	Disabled	Disabled	Disabled	Disabled	Unlimited	
<input type="checkbox"/>	11	LAG1	Disabled	Disabled	Disabled	Disabled	Unlimited	
<input type="checkbox"/>	12	LAG2	Disabled	Disabled	Disabled	Disabled	Unlimited	
<input type="checkbox"/>	13	LAG3	Disabled	Disabled	Disabled	Disabled	Unlimited	
<input type="checkbox"/>	14	LAG4	Disabled	Disabled	Disabled	Disabled	Unlimited	
<input type="checkbox"/>	15	LAG5	Disabled	Disabled	Disabled	Disabled	Unlimited	
<input type="checkbox"/>	16	LAG6	Disabled	Disabled	Disabled	Disabled	Unlimited	
<input type="checkbox"/>	17	LAG7	Disabled	Disabled	Disabled	Disabled	Unlimited	
<input type="checkbox"/>	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 MAC Address	Display enable/disabled source mac address validation attribute of interface
Destination MAC Address	Display enable/disabled destination mac address validation attribute of interface
IP Address	Display enable/disabled IP address validation attribute of interface. Allow zero which means allow 0.0.0.0 IP address
Rate Limit	Display rate limitation value of interface.

**Table 10-34 Property Port Fields**

Security>> Dynamic ARP Inspection>> Property.

Edit Port Setting

Port	GE1
Trust	<input checked="" type="checkbox"/> Enable
Source MAC Address	<input checked="" type="checkbox"/> Enable
Destination MAC Address	<input checked="" type="checkbox"/> Enable
IP Address	<input checked="" type="checkbox"/> Enable
	<input checked="" type="checkbox"/> 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**

### 10.11.2. 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.

**Statistics Table**

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

Table 10-36 Statistics Page

## 10.11. DHCP Snooping

Use the DHCP Snooping pages to configure settings for DHCP Snooping

### 10.11.1. Displaying DHCP Security Page

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
<input type="checkbox"/>	1	GE1	Disabled	Disabled	Unlimited
<input type="checkbox"/>	2	GE2	Disabled	Disabled	Unlimited
<input type="checkbox"/>	3	GE3	Disabled	Disabled	Unlimited
<input type="checkbox"/>	4	GE4	Disabled	Disabled	Unlimited
<input type="checkbox"/>	5	GE5	Disabled	Disabled	Unlimited
<input type="checkbox"/>	6	GE6	Disabled	Disabled	Unlimited
<input type="checkbox"/>	7	GE7	Disabled	Disabled	Unlimited
<input type="checkbox"/>	8	GE8	Disabled	Disabled	Unlimited

**Figure 10-38 Property Port Fields**

**Edit Port Setting**

**Figure 10-39 Edit Property Port Dialog**

Field	Description
<b>Port</b>	Display selected port to be edited.
<b>Trust</b>	Set checkbox to enable/disabled trust of interface. All DHCP packet will be forward directly if enable trust. Default is disabled.
<b>Verify Chaddr</b>	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.
<b>Rate Limit</b>	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. Displaying DHCP Statistics

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

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

**Statistics Table**

	Entry	Port	Forward	Chaddr Check Drop	Untrust Port Drop	Untrust Port with Option82 Drop	Invalid Drop	
<input type="checkbox"/>	1	GE1	0	0	0	0	0	
<input type="checkbox"/>	2	GE2	0	0	0	0	0	
<input type="checkbox"/>	3	GE3	0	0	0	0	0	
<input type="checkbox"/>	4	GE4	0	0	0	0	0	
<input type="checkbox"/>	5	GE5	0	0	0	0	0	
<input type="checkbox"/>	6	GE6	0	0	0	0	0	
<input type="checkbox"/>	7	GE7	0	0	0	0	0	

**Figure 10-40 DHCP Snooping Statistics Page**

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

**Table 10-40 DHCP Snooping Statistics**

### 10.11.3. Option 82 Property

You can use DHCP option 82, also known as the DHCP relay agent information option, to help protect supported network devices against attacks including spoofing (forging) of IP addresses and MAC addresses, and DHCP IP address starvation.

In a common scenario, various hosts are connected to the network via untrusted access interfaces on the switch, and these hosts request and are assigned IP addresses from the DHCP server. Bad actors can spoof DHCP requests using forged network addresses, however, to gain an improper connection to the network.

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
<input type="checkbox"/>	1	GE1	Disabled	Drop
<input type="checkbox"/>	2	GE2	Disabled	Drop
<input type="checkbox"/>	3	GE3	Disabled	Drop
<input type="checkbox"/>	4	GE4	Disabled	Drop
<input checked="" type="checkbox"/>	5	GE5	Disabled	Drop
<input type="checkbox"/>	6	GE6	Disabled	Drop
<input type="checkbox"/>	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

## Security > DHCP Snooping > Option82 Property

Edit Port Setting

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. <b>Keep:</b> Keep original option82 content. <b>Replace:</b> Replace option82 content by switch setting <b>Drop:</b> 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

**Option82 Circuit ID Table**

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

	Port	VLAN	Circuit ID
<input type="checkbox"/>	GE1	1	rainbow
<input type="checkbox"/>	GE2	2	WWW

Add Edit Delete

First Previous 1 Next Last

Figure 10-44 Option82 Circuit ID Page

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

Table 10-44 Option82 Circuit ID Fields

**Add Option82 Circuit ID**

Port: GE5

VLAN: 2 (1 - 4094) (Keep empty to set without VLAN)

Circuit ID: dddd

Apply Close

**Edit Option82 Circuit ID**

Port: GE1

VLAN: 1

Circuit ID: rainbow

Apply Close

Figure 10-45 Add and Edit Option82 Circuit ID Dialog



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

**Table 10-45 Option82 Circuit ID Fields**

## 10.12. IP Source Guard

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

### 10.12.1. Port Setting

To display Port Setting page, click **Security > IP Source Guard > Port Setting**  
This page allow user to configure per port settings of IP Source Guard.

Port Setting Table

	Entry	Port	State	Verify Source	Current Entry	Max Entry
<input type="checkbox"/>	1	GE1	Disabled	IP	0	Unlimited
<input type="checkbox"/>	2	GE2	Disabled	IP	0	Unlimited
<input type="checkbox"/>	3	GE3	Disabled	IP	0	Unlimited
<input type="checkbox"/>	4	GE4	Disabled	IP	0	Unlimited
<input type="checkbox"/>	5	GE5	Disabled	IP	0	Unlimited
<input type="checkbox"/>	6	GE6	Disabled	IP	0	Unlimited

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	<input checked="" type="checkbox"/> Enable
Verify Source	<input checked="" type="radio"/> IP <input type="radio"/> IP-MAC
Max Entry	20 (1 - 50, default 0), 0 is Unlimited

Apply Close

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.

#### IP-MAC-Port-VLAN Binding Table

Showing All entries Showing 1 to 2 of 2 entries

	Port	VLAN	MAC Address	IP Address	Binding	Type	Lease Time
<input type="checkbox"/>	GE1	22	44:55:66:77:88:99	2.2.2.2 / 255.255.255.255	IP-MAC-Port-VLAN	Static	N/A
<input type="checkbox"/>	GE1	33	00:00:00:00:00:0A	3.3.3.3 / 255.255.255.255	IP-MAC-Port-VLAN	Static	N/A

Add Edit Delete

**Figure 10-48 IPMV Binding Page**

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

**Table 10-48 IPMV Binding Fields**

Add IP-MAC-Port-VLAN Binding

Port	GE1
VLAN	33 (1 - 4094)
Binding	<input checked="" type="radio"/> IP-MAC-Port-VLAN <input type="radio"/> IP-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**

#### 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 <b>IP-MAC-Port-VLAN:</b> packet must match IP address MAC address, Port and VLAN ID. <b>IP-Port-VLAN:</b> packet must match IP address or subnet,Port and VLAN ID.
MAC Address	Input MAC address. Only available on IP-MAC-Port-VLAN mode.
IP Address	Input IP address and mask. Mask only available on IP-MAC-Port mode.

Table 10-49 Add and Edit IPMV Binding Fields

### 10.12.3 Save Database

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

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

Type	<input type="radio"/> None <input type="radio"/> Flash <input checked="" type="radio"/> TFTP
Filename	33333
Address Type	<input checked="" type="radio"/> Hostname <input type="radio"/> IPv4
Server Address	192.168.1.100
Write Delay	300 Sec (15 - 86400, default 300)
Timeout	300 Sec (0 - 86400, default 300)

Apply

Figure 10-50 Save Database Page

Field	Description
Type	Select the type of database agent. <b>None:</b> Disable database agent service. <b>Flash:</b> Save DHCP dynamic binding entries to flash. <b>TFTP:</b> 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. <b>Hostname:</b> TFTP server address is hostname. <b>IPv4:</b> 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

This page left blank intentionally

## 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

<input type="checkbox"/>	ACL Name	Rule	Port
<input type="checkbox"/>	AAAA	0	
<input type="checkbox"/>	SSSS	0	
<input type="checkbox"/>	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.

**ACE Table**

ACL Name AAAA

Showing All entries Showing 1 to 2 of 2 entries

<input type="checkbox"/>	Sequence	Action	Source MAC		Destination MAC		Ethertype	VLAN	802.1p	
			Address	Mask	Address	Mask			Value	Mask
<input type="checkbox"/>	1	Permit	Any	Any	Any	Any	Any	Any	Any	Any
<input type="checkbox"/>	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**

ACL >> MAC ACE

**Add ACE**

ACL Name: AAAA

Sequence:  (1 - 2147483647)

Action: ☐ Permit ☐ Deny ☐ Shutdown

Source MAC: ☒ Any  /  (Address / Mask)

Destination MAC: ☒ Any  /  (Address / Mask)

Ethertype: ☒ Any  0x  (0x600 ~ 0xFFFF)

VLAN: ☒ Any  (1 - 4094)

802.1p: ☒ Any  /  (Value / Mask) (0 - 7)

**Edit ACE**

ACL Name: AAAA

Sequence: 22

Action: ☐ Permit ☐ Deny ☒ Shutdown

Source MAC: ☒ Any  /  (Address / Mask)

Destination MAC: ☒ Any  /  (Address / Mask)

Ethertype: ☒ Any  0x  (0x600 ~ 0xFFFF)

VLAN: ☒ Any  (1 - 4094)

802.1p: ☒ Any  /  (Value / Mask) (0 - 7)

**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. <b>Permit:</b> Forward packets that meet the ACE criteria. <b>Deny:</b> Drop packets that meet the ACE criteria. <b>Shutdown:</b> 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. <b>Any:</b> All source addresses are acceptable. <b>User Defined:</b> 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. <b>Any:</b> All destination addresses are acceptable.

	<b>User Defined:</b> 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.
<b>Ethertype</b>	Select the type for Ethernet frame type. <b>Any:</b> All Ethernet frame type is acceptable. <b>User Defined:</b> Only an Ethernet frame type which users define is acceptable. Enter the Ethernet frame type value to which will be matched.
<b>VLAN ID</b>	Select the type for VLAN ID. <b>Any:</b> All VLAN ID is acceptable. <b>User Defined:</b> Only a VLAN ID which users define is acceptable. Enter the VLAN ID to which will be matched.
<b>802.1p</b>	Select the type for 802.1p value. <b>Any:</b> All 802.1p value is acceptable. <b>User Defined:</b> Only an 802.1p value or a range of 802.1p value which users define
<b>Table 11-4 Add and Edit MAC ACE Fields</b>	

### 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
<b>Table 11-5 IPv4 ACL Fields</b>	

**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
<b>Table 11-6 IPv4 ACL Table Fields</b>	

## 11.4. IPv4 ACE

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

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

**ACE Table**

ACL Name: 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
<input type="checkbox"/>	23	Permit	Any (IP)	Any	Any	Any	Any				Any	Any		

Add Edit Delete

**Figure 11-7 IPv4 ACE Page**

Field	Description
<b>ACL Name</b>	Select the ACL name to which an ACE is being added.
<b>Sequence</b>	Display the sequence of ACE.
<b>Action</b>	Display the action of ACE
<b>Protocol</b>	Display the protocol value of ACE
<b>Source IP</b>	Display the source IP address and mask of ACE
<b>Destination IP</b>	Display the destination IP address and mask of ACE
<b>Source Port</b>	Display single source port or a range of source ports of ACE. Only available when protocol is TCP or UDP.
<b>Destination Port</b>	Display single destination port or a range of destination ports of ACE. Only available when protocol is TCP or UDP.
<b>TCP Flags</b>	Display the TCP flag value if ACE. Only available when protocol is TCP.
<b>Type of Service</b>	Display the ToS value of ACE which could be DSCP or IP Precedence.
<b>ICMP</b>	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	<input checked="" type="radio"/> Permit <input type="radio"/> Deny <input type="radio"/> Shutdown
Protocol	<input checked="" type="radio"/> Any <input type="radio"/> Select ICMP <input type="radio"/> Define (0 - 255)
Source IP	<input checked="" type="checkbox"/> Any <input type="text"/> / <input type="text"/> (Address / Mask)
Destination IP	<input checked="" type="checkbox"/> Any <input type="text"/> / <input type="text"/> (Address / Mask)
Type of Service	<input checked="" type="radio"/> Any <input type="radio"/> DSCP (0 - 63) <input type="radio"/> IP Precedence (0 - 7)
Source Port	<input checked="" type="radio"/> Any <input type="radio"/> Single (0 - 65535) <input type="radio"/> Range - (0 - 65535)
Destination Port	<input checked="" type="radio"/> Any <input type="radio"/> Single (0 - 65535) <input type="radio"/> Range - (0 - 65535)
TCP Flags	Urg: <input type="radio"/> Set <input type="radio"/> Unset <input checked="" type="radio"/> Don't care Ack: <input type="radio"/> Set <input type="radio"/> Unset <input checked="" type="radio"/> Don't care Psh: <input type="radio"/> Set <input type="radio"/> Unset <input checked="" type="radio"/> Don't care Rst: <input type="radio"/> Set <input type="radio"/> Unset <input checked="" type="radio"/> Don't care

### Add ACE

ACL Name	IP11
Sequence	(1 - 2147483647)
Action	<input checked="" type="radio"/> Permit <input type="radio"/> Deny <input type="radio"/> Shutdown
Protocol	<input checked="" type="radio"/> Any <input type="radio"/> Select ICMP <input type="radio"/> Define (0 - 255)
Source IP	<input checked="" type="checkbox"/> Any <input type="text"/> / <input type="text"/> (Address / Mask)
Destination IP	<input checked="" type="checkbox"/> Any <input type="text"/> / <input type="text"/> (Address / Mask)
Type of Service	<input checked="" type="radio"/> Any <input type="radio"/> DSCP (0 - 63) <input type="radio"/> IP Precedence (0 - 7)
Source Port	<input checked="" type="radio"/> Any <input type="radio"/> Single (0 - 65535) <input type="radio"/> Range - (0 - 65535)
Destination Port	<input checked="" type="radio"/> Any <input type="radio"/> Single (0 - 65535) <input type="radio"/> Range - (0 - 65535)
TCP Flags	Urg: <input type="radio"/> Set <input type="radio"/> Unset <input checked="" type="radio"/> Don't care Ack: <input type="radio"/> Set <input type="radio"/> Unset <input checked="" type="radio"/> Don't care Psh: <input type="radio"/> Set <input type="radio"/> Unset <input checked="" type="radio"/> Don't care Rst: <input type="radio"/> Set <input type="radio"/> Unset <input checked="" type="radio"/> Don't care

Figure 11-8 Add and Edit IPv4 ACE Dialog

Field	Description
ACL Name	Display the ACL name to which an ACE is being added.
Sequence	Specify the sequence of the ACE. ACEs with higher sequence are processed first (1 is the highest sequence). Only available on Add dialog.
Action	<p>Select the action for a match.</p> <p><b>Permit:</b> Forward packets that meet the ACE criteria.</p> <p><b>Deny:</b> Drop packets that meet the ACE criteria.</p> <p><b>Shutdown:</b> 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.</p>
<p><b>Select the type of protocol for a match.</b></p> <ul style="list-style-type: none"> <li><b>Any (IP):</b> All IP protocols are acceptable.</li> <li><b>Select from list:</b> 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)</li> <li><b>Protocol ID to match:</b> Enter the protocol ID.</li> </ul>	
Source IP	<p>Select the type for source IP address.</p> <ul style="list-style-type: none"> <li><b>Any:</b> All source addresses are acceptable.</li> <li><b>User Defined:</b> 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.</li> </ul>
Destination IP	<p>Select the type for destination IP address.</p> <ul style="list-style-type: none"> <li><b>Any:</b> All destination addresses are acceptable.</li> <li><b>User Defined:</b> 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.</li> </ul>
Source Port	<p>Select the type of protocol for a match. Only available when protocol is TCP or UDP.</p> <ul style="list-style-type: none"> <li><b>Any:</b> All source ports are acceptable.</li> <li><b>Single:</b> Enter a single TCP/UDP source port to which packets are matched.</li> <li><b>Range:</b> 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.</li> </ul>
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	<p>Select the type of service for a match.</p> <ul style="list-style-type: none"> <li><b>Any:</b> All types of service are acceptable.</li> <li><b>DSCP to match:</b> Enter a Differentiated Services Code Point (DSCP) to match.</li> <li><b>IP Precedence to match:</b> Enter a IP Precedence to match.</li> </ul>
ICMP Type	<p>Either select the message type by name or enter the message type number. Only available when protocol is ICMP.</p> <ul style="list-style-type: none"> <li><b>Any:</b> All message types are acceptable.</li> <li><b>Select from list:</b> Select message type by name.</li> <li><b>Protocol ID to match:</b> Enter the number of message type.</li> </ul>
ICMP Code	<p>Select the type for ICMP code. Only available when protocol is ICMP.</p> <ul style="list-style-type: none"> <li><b>Any:</b> All codes are acceptable.</li> <li><b>User Defined:</b> Enter an ICMP code to match.</li> </ul>

Table 11-8 Add and Edit IPv4 ACL Fields

### 11.5. IPv6 ACL

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

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

ACL Name

Apply

Figure 11-9 IPv6 ACL Page

Field	Description
ACL Name	Input IPv6 ACL name

Table 11-9 IPv6 ACL Fields

ACL Table

Showing All entries

Showing 1 to 3 of 3 entries

	ACL Name	Rule	Port
<input type="checkbox"/>	IP61	0	
<input type="checkbox"/>	IP62	0	
<input type="checkbox"/>	IP89	0	

Delete

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.

**ACE Table**

ACL Name **IP61** ▼

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	Prefix	Address	Prefix				DSCP	IP Precedence	Type	Code
<input type="checkbox"/>	22334	Permit	Any (IP)	Any	Any	Any	Any				Any		Any	

**Add** **Edit** **Delete**

**Figure 11-11 IPv6 ACE Page**

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

**Table 11-11 IPv6 ACE Fields**

#### Add ACE

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

#### Edit ACE

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

Figure 11-12 Add and Edit IPv6 ACE Dialog



Field	Description
<b>ACL Name</b>	Display the ACL name to which an ACE is being added.
<b>Sequence</b>	Specify the sequence of the ACE. ACEs with higher sequence are processed first (1 is the highest sequence). Only available on Add dialog.
<b>Action</b>	Select the action for a match. <b>Permit:</b> Forward packets that meet the ACE criteria. <b>Deny:</b> Drop packets that meet the ACE criteria. <b>Shutdown:</b> 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.
<b>Protocol</b>	Select the type of protocol for a match. <b>Any (IP):</b> All IP protocols are acceptable. <b>Select from list:</b> Select one of the following protocols from the drop- down list.(TCP / UDP / ICMP) <b>Protocol ID to match:</b> Enter the protocol ID.
<b>Source IP</b>	Select the type for source IP address. <b>Any:</b> All source addresses are acceptable. <b>User Defined:</b> 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.
<b>Destination IP</b>	Select the type for destination IP address. <b>Any:</b> All destination addresses are acceptable. <b>User Defined:</b> 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.
<b>Source Port</b>	Select the type of protocol for a match. Only available when protocol is TCP or UDP. <b>Any:</b> All source ports are acceptable. <b>Single:</b> Enter a single TCP/UDP source port to which packets are matched. <b>Range:</b> 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.
<b>Destination Port</b>	Select the type of protocol for a match. Only available when protocol is TCP or UDP. <b>Any:</b> All source ports are acceptable. <b>Single:</b> Enter a single TCP/UDP source port to which packets are matched. <b>Range:</b> 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.
<b>TCP Flags</b>	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.
<b>Type of Service</b>	Select the type of service for a match. <b>Any:</b> All types of service are acceptable. <b>DSCP to match:</b> Enter a Differentiated Serves Code Point (DSCP) to match. <b>IP Precedence to match:</b> Enter a IP Precedence to match.
<b>ICMP Type</b>	Either select the message type by name or enter the message type number. Only available when protocol is ICMP. <b>Any:</b> All message types are acceptable. <b>Select from list:</b> Select message type by name. <b>Protocol ID to match:</b> Enter the number of message type.
<b>ICMP Code</b>	Select the type for ICMP code. Only available when protocol is ICMP. <b>Any:</b> All codes are acceptable. <b>User Defined:</b> Enter an ICMP code to match.
<b>Table 11-12 Add and Edit IPv6 ACE Fields</b>	

## 11.7. ACL Binding

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

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

### ACL Binding Table

	Entry	Port	MAC ACL	IPv4 ACL	IPv6 ACL
<input type="checkbox"/>	1	GE1			
<input type="checkbox"/>	2	GE2			
<input type="checkbox"/>	3	GE3			
<input type="checkbox"/>	4	GE4			
<input type="checkbox"/>	5	GE5			
<input type="checkbox"/>	6	GE6			
<input type="checkbox"/>	7	GE7			
<input type="checkbox"/>	8	GE8			
<input type="checkbox"/>	9	GE9			
<input type="checkbox"/>	10	GE10			
<input type="checkbox"/>	11	LAG1			
<input type="checkbox"/>	12	LAG2			
<input type="checkbox"/>	13	LAG3			
<input type="checkbox"/>	14	LAG4			
<input type="checkbox"/>	15	LAG5			
<input type="checkbox"/>	16	LAG6			
<input type="checkbox"/>	17	LAG7			
<input type="checkbox"/>	18	LAG8			

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

### Add ACL Binding

Port

GE1

Note: ACL without any rules cannot be bound

MAC ACL

AAAA ▼

IPv4 ACL

IP11 ▼

IPv6 ACL

None ▼



### 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. Displaying the property for QoS

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	<p>Select QoS trust mode</p> <p><b>CoS:</b> 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.</p> <p><b>DSCP:</b> 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.</p> <p><b>CoS-DSCP:</b> Uses the trust CoS mode for non-IP traffic and trust DSCP mode for IP traffic</p> <p><b>IP Precedence:</b> 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.</p>

**Table 12-1 QoS Global Setting Fields**

Port Setting Table

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

Edit

Figure 12-2 QoS Port Setting Table

Field	Description
<b>Port</b>	Port name
<b>CoS</b>	Port default CoS priority value for the selected ports
<b>Trust</b>	<b>Port trust state</b> <b>Enabled:</b> Traffic will follow trust mode in global setting <b>Disabled:</b> Traffic will always use best efforts
<b>Remarking (CoS)</b>	Port CoS remarking admin state <b>Enabled:</b> CoS remarking is enabled <b>Disabled:</b> CoS remarking is disabled
<b>Remarking (DSCP)</b>	Port DSCP remarking admin state <b>Enabled:</b> DSCP remarking is enabled <b>Disabled:</b> DSCP remarking is disabled
<b>Remarking (IP Precedence)</b>	Port IP Precedence remarking admin state <b>Enable:</b> IP Precedence remarking is enabled <b>Disable:</b> IP Precedence remarking is disabled
<b>Table 12-2 QoS Port Setting Table Fields</b>	

Figure 12-3 Edit QoS Port Setting

Field	Description
Port	Select port list
CoS	Set default CoS/802.1p priority value for the selected ports
Trust	Set checkbox to enable/disable port trust state
Remarking (CoS)	Set checkbox to enable/disable port CoS remarking
Remarking (DSCP)	Set checkbox to enable/disable port DSCP remarking
Remarking (IP Precedence)	Set checkbox to enable/disable port IP Precedence remarking

Table 12-3 Edit QoS Port Setting Fields

### 12.1.2. Queue Scheduling

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

The switch supports eight queues for each interface. Queue number 8 is the highest priority queue. Queue number 1 is the lowest priority queue. There are two ways of determining how traffic in queues is handled.

1. Strict Priority (SP)
2. 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 provides the highest level of priority of traffic to the highest numbered queue.

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

The queuing modes can be selected on the Queue page. When the queuing mode is by Strict Priority, the priority sets the order in which queues are serviced, starting with queue\_8 (the highest priority queue) and going to the next lower queue when each queue is completed.

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

QoS > General > Queue Scheduling.

Queue Scheduling Table

Queue	Method			
	Strict Priority	WRR	Weight	WRR Bandwidth (%)
1	<input type="radio"/>	<input checked="" type="radio"/>	1	33.33%
2	<input type="radio"/>	<input checked="" type="radio"/>	2	66.67%
3	<input checked="" type="radio"/>	<input type="radio"/>	3	
4	<input checked="" type="radio"/>	<input type="radio"/>	4	
5	<input checked="" type="radio"/>	<input type="radio"/>	5	
6	<input checked="" type="radio"/>	<input type="radio"/>	9	
7	<input checked="" type="radio"/>	<input type="radio"/>	13	
8	<input checked="" type="radio"/>	<input type="radio"/>	15	

Apply

Figure 12-4: Queue Scheduling Table

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

**Table 12-4: Queue Scheduling Table fields.**

### 12.2.3. CoS Mapping

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

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

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

CoS to Queue Mapping

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

Apply

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 ▼

Apply

Figure 12-6 Queue to CoS Mapping Table

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

**Table 12-6 Queue to CoS Mapping Table Fields**

### 12.2.4. DSCP Mapping

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

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

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

DSCP to Queue Mapping

DSCP	Queue	DSCP	Queue	DSCP	Queue	DSCP	Queue
0 [CS0]	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	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**

### 12.1.2. IP Precedence Mapping

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

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

#### IP Precedence to Queue Mapping

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

Apply

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 Limiting

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

### 12.2.1. Ingress/Egress Port

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

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

### Ingress / Egress Port Table

	Entry	Port	Ingress		Egress	
			State	Rate (Kbps)	State	Rate (Kbps)
<input type="checkbox"/>	1	GE1	Disabled		Disabled	
<input type="checkbox"/>	2	GE2	Disabled		Disabled	
<input type="checkbox"/>	3	GE3	Disabled		Disabled	
<input type="checkbox"/>	4	GE4	Disabled		Disabled	
<input type="checkbox"/>	5	GE5	Disabled		Disabled	
<input type="checkbox"/>	6	GE6	Disabled		Disabled	
<input type="checkbox"/>	7	GE7	Disabled		Disabled	
<input type="checkbox"/>	8	GE8	Disabled		Disabled	
<input type="checkbox"/>	9	GE9	Disabled		Disabled	
<input type="checkbox"/>	10	GE10	Disabled		Disabled	

Edit

Figure 12-11 Ingress/Egress Port Table

Field	Description
Port	Port name
Ingress (State)	Port ingress rate limit state <b>Enabled:</b> Ingress rate limit is enabled <b>Disabled:</b> 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 <b>Enabled:</b> Egress rate limit is enabled <b>Disabled:</b> 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**

#### Edit Ingress / Egress Port

Port

GE1-GE3

Ingress

☒ Enable

Kbps (16 - 1000000)

Egress

☒ Enable

Kbps (16 - 1000000)

Apply

Close

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 needs 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.

#### Egress Queue Table

	Entry	Port	Queue 1		Queue 2		Queue 3		Queue 4		Queue 5		Queue 6		Queue	
			State	CIR (Kbps)	State	CIR (Kbps)	State	CIR (Kbps)	State	CIR (Kbps)	State	CIR (Kbps)	State	CIR (Kbps)	State	CIR
<input type="checkbox"/>	1	GE1	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
<input type="checkbox"/>	2	GE2	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
<input type="checkbox"/>	3	GE3	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
<input type="checkbox"/>	4	GE4	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
<input type="checkbox"/>	5	GE5	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
<input type="checkbox"/>	6	GE6	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
<input type="checkbox"/>	7	GE7	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
<input type="checkbox"/>	8	GE8	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
<input type="checkbox"/>	9	GE9	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
<input type="checkbox"/>	10	GE10	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	

Edit

Figure 12-13: Egress Queue Table

Field	Description
<b>Port</b>	Port name
<b>Queue 1 (State)</b>	Port egress queue 1 rate limit state <b>Enabled:</b> Egress queue rate limit is enabled <b>Disabled:</b> Egress queue rate limit is disabled
<b>Queue 1 (CIR)</b>	Queue 1 egress committed information rate
<b>Queue 2 (State)</b>	Port egress queue 2 rate limit state <b>Enabled:</b> Egress queue rate limit is enabled <b>Disabled:</b> Egress queue rate limit is disabled
<b>Queue 2 (CIR)</b>	Queue 2 egress committed information rate
<b>Queue 3 (State)</b>	Port egress queue 3 rate limit state <b>Enabled:</b> Egress queue rate limit is enabled <b>Disabled:</b> Egress queue rate limit is disabled
<b>Queue 3 (CIR)</b>	Queue 3 egress committed information rate
<b>Queue 4 (State)</b>	Port egress queue 4 rate limit state <b>Enabled:</b> Egress queue rate limit is enabled <b>Disabled:</b> Egress queue rate limit is disabled
<b>Queue 4 (CIR)</b>	Queue 4 egress committed information rate
<b>Queue 5 (State)</b>	Port egress queue 5 rate limit state <b>Enabled:</b> Egress queue rate limit is enabled <b>Disabled:</b> Egress queue rate limit is disabled
<b>Queue 5 (CIR)</b>	Queue 5 egress committed information rate
<b>Queue 6 (State)</b>	Port egress queue 6 rate limit state <b>Enabled:</b> Egress queue rate limit is enabled <b>Disabled:</b> Egress queue rate limit is disabled
<b>Queue 6 (CIR)</b>	Queue 6 egress committed information rate
<b>Queue 7 (State)</b>	Port egress queue 7 rate limit state <b>Enabled:</b> Egress queue rate limit is enabled <b>Disabled:</b> Egress queue rate limit is disabled
<b>Queue 7 (CIR)</b>	Queue 7 egress committed information rate
<b>Queue 8 (State)</b>	Port egress queue 8 rate limit state <b>Enabled:</b> Egress queue rate limit is enabled <b>Disabled:</b> Egress queue rate limit is disabled
<b>Queue 8 (CIR)</b>	Queue 8 egress committed information rate
<b>Table 12-13: Egress Queue Table Fields.</b>	

Edit Egress Queue

Port	GE1-GE3	
Queue 1	<input checked="" type="checkbox"/> Enable	<input type="text" value="1000000"/> Kbps (16 - 1000000)
Queue 2	<input checked="" type="checkbox"/> Enable	<input type="text" value="1000000"/> Kbps (16 - 1000000)
Queue 3	<input checked="" type="checkbox"/> Enable	<input type="text" value="1000000"/> Kbps (16 - 1000000)
Queue 4	<input checked="" type="checkbox"/> Enable	<input type="text" value="1000000"/> Kbps (16 - 1000000)
Queue 5	<input type="checkbox"/> Enable	<input type="text" value="1000000"/> Kbps (16 - 1000000)
Queue 6	<input type="checkbox"/> Enable	<input type="text" value="1000000"/> Kbps (16 - 1000000)
Queue 7	<input type="checkbox"/> Enable	<input type="text" value="1000000"/> Kbps (16 - 1000000)
Queue 8	<input type="checkbox"/> Enable	<input type="text" value="1000000"/> Kbps (16 - 1000000)
<input type="button" value="Apply"/> <input type="button" value="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. Enabling / Disabling Logging

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

The screenshot shows the 'Logging Property' configuration page. It has several sections:

- Global Logging:** 'State' is checked 'Enable'. 'Aggregation' is checked 'Enable'. 'Aging Time' is set to '300' with a note 'Sec (15 - 3600, default 300)'.
- Console Logging:** 'State' is checked 'Enable'. 'Minimum Severity' is set to 'Notice' with a dropdown arrow. A note below says 'Note: Emergency, Alert, Critical, Error, Warning, Notice'.
- RAM Logging:** 'State' is checked 'Enable'. 'Minimum Severity' is set to 'Notice' with a dropdown arrow. A note below says 'Note: Emergency, Alert, Critical, Error, Warning, Notice'.
- Flash Logging:** 'State' is unchecked. 'Minimum Severity' is set to 'Notice' with a dropdown arrow. A note below says 'Note: Emergency, Alert, Critical, Error, Warning, Notice'.

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

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 13-4: Flash Logging fields

### 13.1.2. Remote Server

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

Remote Server Table

<input type="checkbox"/>	Entry	Server Address	Server Port	Facility	Minimum Severity
<input type="checkbox"/>	1	192.168.1.100	514	Local 7	Notice

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	<p>The minimum severity.</p> <p><b>Emergency:</b> System is not usable.</p> <p><b>Alert:</b> Immediate action is needed.</p> <p><b>Critical:</b> System is in the critical condition.</p> <p><b>Error:</b> System is in error condition</p> <p><b>Warning:</b> System warning has occurred</p> <p><b>Notice:</b> System is functioning properly, but a system notice has occurred.</p> <p><b>Informational:</b> Device information.</p> <p><b>Debug:</b> Provides detailed information about an event.</p>

Table 13-5: Remote Server fields.

## 13.2. Port Mirroring

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

Mirroring Table

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

☐ Allow the monitor port to send or receive normal packets

Figure 13-3 Mirroring Page



Field	Description
<b>Session ID</b>	Select mirror session ID
<b>State</b>	Select mirror session state : port-base mirror or disable <b>Enabled:</b> Enable port-based mirror <b>Disabled:</b> Disable mirror.
<b>Monitor Port</b>	Select mirror session monitor port,and select whether normal packet could be sent or received by monitor port.
<b>Ingress port</b>	Select mirror session source rx ports
<b>Egress ports</b>	Select mirror session source tx ports

**Table 13-6 Mirroring Fields**

### 13.3. Ping

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

Address Type

☒ Hostname  
☐ IPv4  
☐ IPv6

Server Address

Count

4 (1 - 65535)

Ping

Stop

**Ping Result**

Packet Status	
Status	N/A
Transmit Packet	0
Receive Packet	0
Packet Lost	0%
Round Trip Time	
Min	0.0 ms
Max	0.0 ms
Average	0.0 ms

**Figure 13-4: Ping page.**

Field	Description
<b>Address Type</b>	Specify the address type to “Hostname”, “IPv6”, or “IPv4”.
<b>Server Address</b>	Specify the Hostname/IPv4/IPv6 address for the remote logging server.
<b>Count</b>	Specify the numbers of each ICMP ping request.

**Table 13-7: Ping fields.**



## 13.4. Traceroute

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

Address Type: ☒ Hostname ☐ IPv4

Server Address:

Time to Live:  (2 - 255, default 30)

☐ User Defined

**Traceroute Result**

Figure 13-5: Traceroute page.

Field	Description
Address Type	Specify the address type to “Hostname”, or “IPv4”.
Server Address	Specify the Hostname/IPv4 address for the remote logging server.
Time to Live	Specify the max hops of hosts for traceroute.

**Table 13-8: Traceroute fields.**

## 13.5. Copper Test

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

Port:

**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
<b>Port</b>	The interface for the copper test.
<b>Result</b>	The status of copper test. It include: <b>OK:</b> Correctly terminated pair. <b>Short Cable:</b> Shorted pair. <b>Open Cable:</b> Open pair, no link partner. <b>Impedance Mismatch:</b> Terminating impedance is not in the reference range. <b>Line Drive:</b>
<b>Length</b>	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. Fibre Module

The Optical Module Status page displays the operational information reported by the Small Form-factor Pluggable (SFP) transceiver. Some information may not be available for SFPs without the supports of digital diagnostic monitoring standard SFF-8472.

To display the Optical Module Diagnostic page, click **Diagnostic > Fiber Module**.

**Fiber Module Table**

	Port	Temperature (C)	Voltage (V)	Current (mA)	Output Power (mW)	Input Power (mW)	OE Present	Loss of Signal
<input type="radio"/>	GE9	N/S	N/S	N/S	N/S	N/S	Remove	Loss
<input type="radio"/>	GE10	N/S	N/S	N/S	N/S	N/S	Remove	Loss

Refresh Detail

**Fiber Module Table**

	Port	Temperature (C)	Voltage (V)	Current (mA)	Output Power (mW)	Input Power (mW)	OE Present	Loss of Signal
<input type="radio"/>	GE9	N/S	N/S	N/S	N/S	N/S	Remove	Loss
<input type="radio"/>	GE10	N/S	N/S	N/S	N/S	N/S	Remove	Loss

Refresh Detail

**Figure 13-7: Fibre Module page.**

Field	Description
<b>Port</b>	Interface or port number.
<b>Temperature</b>	Internally measured transceiver temperature.
<b>Voltage</b>	Internally measured supply voltage.
<b>Current</b>	Measured TX bias current.
<b>Output Power</b>	Measured TX output power in milliwatts.
<b>Input Power</b>	Measured RX received power in milliwatts.
<b>Transmitter Fault</b>	State of TX fault.
<b>OE Present</b>	Indicate transceiver has achieved power up and data is ready.
<b>Loss of Signal</b>	Loss of signal.
<b>Refresh</b>	Refresh the page.
<b>Detail</b>	The detail information on the specified port

**Table 13-11: Fibre Module fields.**

Fiber Module Status

Port	GE9
OE Present	Remove
Loss of Signal	Loss
Transceiver Type	Unknown
Connector Type	Unknown
Ethernet Compliance Code	Unknown
Transmission Media	Unknown
Wavelength	N/S
Bitrate	N/S
Vendor OUI	N/S
Vendor Name	N/S
Vendor PN	N/S
Vendor Revision	N/S
Vendor SN	N/S
Date Code	0-00-00
Temperature (C)	N/S
Voltage (V)	N/S
Current (mA)	N/S
Output Power (mW)	N/S
Input Power (mW)	N/S

Refresh Close

Figure 13-8: Fiber Module Status page.

## 13.7. UDLD

### Uni- Directional Link Detection

Imagine that you have a dual-core fibre run between two buildings. Somewhere along the run, one of the cores gets damaged. This may leave you in a position where you have a uni-directional link. You have enough of a link to send in one direction, but not the other.

Devices at each end may have trouble noticing the link impairment. Traffic still flows, in one direction at least, so they may think the link is still up.

Spanning-tree may allow some layer-2 loops through the network. Why? It is unable to send BPDU's to a connected switch. One way to protect against this specific problem is Loop Guard. If a port expects BPDU's, but does not receive them, Loop Guard disables the port.

How do we protect against other problems? This is when you use **Unidirectional Link Detection**, or *UDLD*. This has been adapted to an industry standard in RFC 5171. Two devices with UDLD will send each other hello packets every 15 seconds. If the responses are missing, the switch disabled the port.

Enable UDLD globally or per interface. It can also be set to **enable** or **aggressive mode**. Enable mode will take no action other than to generate syslog messages. Aggressive mode will try to reestablish the link. If it is unable to, it will disable the port. The recommendation is to enable UDLD globally, in aggressive mode. Syslog messages are too easy to miss.

**Recommendation:** Use aggressive mode

Use the UDLD pages to configure settings of UDLD function.

### 13.1.3. Displaying UDLD 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	
<input type="checkbox"/>	1	GE1	Disabled	Unknown		0	
<input type="checkbox"/>	2	GE2	Disabled	Unknown		0	
<input type="checkbox"/>	3	GE3	Disabled	Unknown		0	
<input type="checkbox"/>	4	GE4	Disabled	Unknown		0	
<input type="checkbox"/>	5	GE5	Disabled	Unknown		0	
<input type="checkbox"/>	6	GE6	Disabled	Unknown		0	
<input type="checkbox"/>	7	GE7	Disabled	Unknown		0	
<input type="checkbox"/>	8	GE8	Disabled	Unknown		0	
<input type="checkbox"/>	9	GE9	Disabled	Unknown		0	
<input type="checkbox"/>	10	GE10	Disabled	Unknown		0	

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
Neighbour	Display the number of neighbours on the interface

Table 13-13 Property Port Fields

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. <b>Disabled:</b> Disable UDLD function. <b>Normal:</b> Running on normal mode that port goes to Link Up One phase after last neighbour ages out. <b>Aggressive:</b> Running on aggressive mode that port goes to Re-Establish phase after last neighbour ages out.

Table 13-14 Edit Property Port Fields

### 13.1.4. Display UDLD Neighbour

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

Neighbor Table

Entry	Expiration Time	Current Neighbor State	Device ID	Device Name	Port ID	Message Interval	Timeout Interval	
0 results found.								
Refresh								

Figure 13-12: Neighbour page.

Field	Description
Entry	Display entry index
Expiration Time	Display expiration time before age out.
Current Neighbor State	Display neighbour current state
Device ID	Display neighbour device ID.
Device Name	Display neighbour device name.
Port ID	Display neighbour port ID that connected.
Message Interval	Display neighbour message interval.
Timeout Interval	Display neighbour timeout interval

Table 13-15: Neighbour fields.

## 14. Management

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

### 14.1. User Accounts

To display User Account web page, click Management > User Account

The default username/password is admin/admin. And default account is not able to be deleted.

Use this page to add additional users that are permitted to manage the switch or to change the passwords of existing users.

#### Management>> User Account

**User Account**

Showing  entries Showing 1 to :

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

Figure 14-1 User Account Table

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

**Table 14-1 User Account Table Fields**

#### Add User Account

Username

Password

Confirm Password

Privilege ☒ Admin ☐ User

#### Edit User Account

Username

Password

Confirm Password

Privilege ☐ Admin ☒ User

Figure 14-2 Add/Edit User Account Dialog

Field	Description
<b>Username</b>	User name of the account
<b>Password</b>	Set password of the account
<b>Confirm Password</b>	Set the same password of the account as in “Password” field
<b>Privilege</b>	Select privilege level for new account. <b>Admin:</b> Allow to change switch settings. Privilege value equals to 15. <b>User:</b> 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.

The screenshot shows a web form for upgrading or backing up firmware. It has three sections: 'Action' with radio buttons for 'Upgrade' and 'Backup', 'Method' with radio buttons for 'TFTP' and 'HTTP' (which is selected), and 'Filename' with a text input field containing 'Case'. An 'Apply' button is at the bottom.

**Figure 14-3 Upgrade Firmware through HTTP**

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

**Table 14-3 Upgrade Firmware through HTTP Fields**

The screenshot shows a web form for upgrading or backing up firmware. It has four sections: 'Action' with radio buttons for 'Upgrade' and 'Backup', 'Method' with radio buttons for 'TFTP' (which is selected) and 'HTTP', 'Address Type' with radio buttons for 'Hostname', 'IPv4', and 'IPv6', and 'Server Address' and 'Filename' with text input fields. An 'Apply' button is at the bottom.

**Figure 14-4 Upgrade Firmware through TFTP**



Field	Description
<b>Action</b>	Firmware operations <b>Upgrade:</b> Upgrade firmware from remote host to DUT <b>Backup:</b> Backup firmware image from DUT to remote host
<b>Method</b>	Firmware upgrade / backup method <b>TFTP:</b> Using TFTP to upgrade/backup firmware <b>HTTP:</b> Using WEB browser to upgrade/backup firmwar
<b>Address Type</b>	Specify TFTP server address type <b>Hostname:</b> Use domain name as server address <b>IPv4:</b> Use IPv4 as server address <b>IPv6:</b> Use IPv6 as server address
<b>Server Address</b>	Specify TFTP server address.
<b>Filename</b>	Firmware image file name on remote TFTP server
<b>Table 14-4 Upgrade Firmware through TFTP Fields</b>	

The screenshot shows a configuration window with three sections: Action, Method, and Firmware. Each section has two radio button options. In the Action section, 'Backup' is selected. In the Method section, 'HTTP' is selected. In the Firmware section, 'Image0' is selected. An 'Apply' button is located at the bottom left of the window.

<b>Action</b>	<input type="radio"/> Upgrade <input checked="" type="radio"/> Backup
<b>Method</b>	<input type="radio"/> TFTP <input checked="" type="radio"/> HTTP
<b>Firmware</b>	<input checked="" type="radio"/> Image0 <input type="radio"/> Image1

Apply

**Figure 14-5 Backup Firmware through HTTP**

Field	Description
<b>Action</b>	Firmware operations <b>Upgrade:</b> Upgrade firmware from remote host to DUT <b>Backup:</b> Backup firmware image from DUT to remote host
<b>Method</b>	Firmware upgrade / backup method <b>TFTP:</b> Using TFTP to upgrade/backup firmware <b>HTTP:</b> Using WEB browser to upgrade/backup firmware
<b>Firmware</b>	Firmware partition need to backup <b>Image0:</b> Firmware image in flash partition 0 <b>Image1:</b> Firmware image in flash partition 1
<b>Table 14-5 Backup Firmware through HTTP Fields</b>	

Action	<input type="radio"/> Upgrade <input checked="" type="radio"/> Backup
Method	<input checked="" type="radio"/> TFTP <input type="radio"/> HTTP
Firmware	<input checked="" type="radio"/> Image0 <input type="radio"/> Image1
Address Type	<input checked="" type="radio"/> Hostname <input type="radio"/> IPv4 <input type="radio"/> IPv6
Server Address	<input type="text"/>
Filename	<input type="text"/>

**Figure 14-6 Backup Firmware through TFTP**

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

Active Image

☒ Image0  
☐ Image1

Note: the image was selected for the next boot

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

Apply

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.

The screenshot shows a web form for configuration upgrade/backup. It has four main sections: Action, Method, Configuration, and Filename. Each section has a list of radio buttons. The 'Action' section has 'Upgrade' and 'Backup'. The 'Method' section has 'TFTP' and 'HTTP'. The 'Configuration' section has 'Running Configuration', 'Startup Configuration', 'Backup Configuration', 'RAM Log', and 'Flash Log'. The 'Filename' section has a text input field with the value 'Case'. Below the form is an 'Apply' button.

Figure 14-8 Upgrade Configuration through HTTP

Field	Description
Action	Configuration operations <b>Upgrade:</b> Upgrade firmware from remote host to DUT <b>Backup:</b> Backup firmware image from DUT to remote host
Method	Configuration upgrade / backup method <b>TFTP:</b> Using TFTP to upgrade/backup firmware <b>HTTP:</b> Using WEB browser to upgrade/backup firmware
Configuration	Configuration types <b>Running Configuration:</b> Merge to current running configuration file <b>Startup Configuration:</b> Replace startup configuration file <b>Backup Configuration:</b> 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

This screenshot shows the same form as Figure 14-8 but with additional fields. It includes 'Address Type' with radio buttons for 'Hostname', 'IPv4', and 'IPv6'. Below that are two text input fields for 'Server Address' and 'Filename'. An 'Apply' button is at the bottom.

**Figure 14-9 Upgrade Configuration through TFTP**

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

**Table 14-9 Upgrade Firmware through TFTP Fields**

The screenshot shows a configuration window with three main sections: **Action**, **Method**, and **Configuration**. Each section contains a list of options with radio buttons. In the **Action** section, 'Backup' is selected. In the **Method** section, 'HTTP' is selected. In the **Configuration** section, 'Running Configuration' is selected. An 'Apply' button is located at the bottom left of the window.

**Figure 14-10 Backup Configuration through HTTP**

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

**Table 14-10 Backup Configuration through HTTP Fields**

Figure 14-11 Backup Configuration through TFTP

Field	Description
Action	Firmware operations <b>Upgrade:</b> Upgrade firmware from remote host to DUT <b>Backup:</b> Backup firmware image from DUT to remote host
Method	Firmware upgrade / backup method <b>TFTP:</b> Using TFTP to upgrade/backup firmware <b>HTTP:</b> Using WEB browser to upgrade/backup firmware
Configuration	Configuration types <b>Running Configuration:</b> Backup running configuration file <b>Startup Configuration:</b> Backup start configuration file <b>Backup Configuration:</b> Backup backup configuration file <b>RAM Log:</b> Backup log file stored in RAM <b>Flash Log:</b> Backup log files store in Flash
Address Type	Specify TFTP server address type <b>Hostname:</b> Use domain name as server address <b>IPv4:</b> Use IPv4 as server address <b>IPv6:</b> Use IPv6 as server address
Server Address	Specify TFTP server address.
Filename	File name saved on remote TFTP server
<b>14-11 Backup Firmware through TFTP Fields</b>	

### 14.3.2. Display The Saved 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



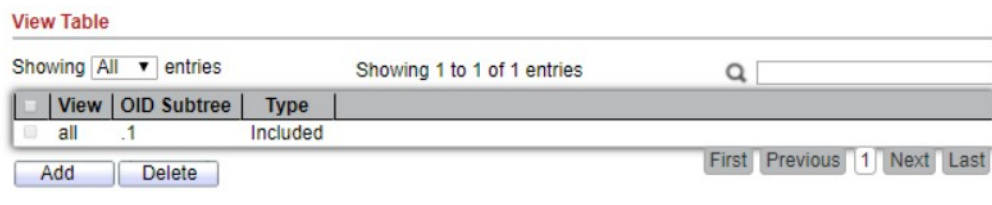
Field	Description
Source File	Source file types <b>Running Configuration:</b> Copy running configuration file to destination <b>Startup Configuration:</b> Copy startup configuration file to destination <b>Backup Configuration:</b> Copy backup configuration file to destination
Destination File	Destination file <b>Startup Configuration:</b> Save file as startup configuration <b>Backup Configuration:</b> Save file as backup configuration

**Table 14-11 Backup Firmware through TFTP Fields**

## 14.4. SNMP

### 14.4.1. Display the SNMP View Table

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



**Figure 14-13 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. SNMP Group

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

Field	Description
Group	Specify SNMP group name, and the maximum length is 30 characters.
Version	Specify SNMP version <b>SNMPv1:</b> SNMP Version 1. <b>SNMPv2:</b> Community-based SNMP Version 2c. <b>SNMPv3:</b> User security model SNMP version 3.
Security Level	Specify SNMP security level <b>No Security :</b> Specify that no packet authentication is performed. <b>Authentication:</b> Specify that no packet authentication without encryption is performed. <b>Authentication and Privacy:</b> 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**



## Management>>SNMP>> Group

**Add Group**

<b>Group</b>	G3
<b>Version</b>	<input checked="" type="radio"/> SNMPv1 <input type="radio"/> SNMPv2 <input type="radio"/> SNMPv3
<b>Security Level</b>	<input checked="" type="radio"/> No Security <input type="radio"/> Authentication <input type="radio"/> Authentication and Privacy
<b>View</b>	<input checked="" type="checkbox"/> Read <input type="checkbox"/> Write <input type="checkbox"/> Notify
	<input type="text" value="all"/> <input type="button" value="v"/> <input type="text" value="all"/> <input type="button" value="v"/> <input type="text" value="all"/> <input type="button" value="v"/>

Figure 14-15 SNMP Group Add Page

Field	Description
<b>Group</b>	Specify SNMP group name, and the maximum length is 30 characters.
<b>Version</b>	Specify SNMP version <b>SNMPv1:</b> SNMP Version 1. <b>SNMPv2:</b> Community-based SNMP Version 2c. <b>SNMPv3:</b> User security model SNMP version 3.
Specify SNMP security level <ul style="list-style-type: none"> <li><b>No Security</b> : Specify that no packet authentication is performed.</li> <li><b>Authentication:</b> Specify that no packet authentication without entryption is performed.</li> <li><b>Authentication and Privacy:</b> Specify that no packet authentication with entryption is performed.</li> </ul>	
<b>View</b>	
<b>Read</b>	Select read view name if Read is checked
<b>Write</b>	Select write view name, if Write is checked
<b>Notify</b>	Select notify view name, if Notify is checked

Table 14-15 SNMP Group Add Fields

**Edit Group**

<b>Group</b>	G2
<b>Version</b>	<input checked="" type="radio"/> SNMPv1 <input type="radio"/> SNMPv2 <input type="radio"/> SNMPv3
<b>Security Level</b>	<input checked="" type="radio"/> No Security <input type="radio"/> Authentication <input type="radio"/> Authentication and Privacy
<b>View</b>	<input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write <input checked="" type="checkbox"/> Notify
	<input type="text" value="all"/> <input type="button" value="v"/> <input type="text" value="all"/> <input type="button" value="v"/> <input type="text" value="all"/> <input type="button" value="v"/>

Figure 14-16 SNMP Group Edit Page

Field	Description
<b>Group</b>	Display the edit group name
<b>Version</b>	Specify SNMP version <b>SNMPv1:</b> SNMP Version 1. <b>SNMPv2:</b> Community-based SNMP Version 2c. <b>SNMPv3:</b> User security model SNMP version 3.
<b>Security Level</b>	Specify SNMP security level <b>No Security:</b> Specify that no packet authentication is performed. <b>Authentication:</b> Specify that no packet authentication without encryption is performed. <b>Authentication and Privacy:</b> Specify that no packet authentication with encryption is performed.
<b>View</b>	
<b>Read</b>	Select read view name if Read is checked
<b>Write</b>	Select write view name, if Write is checked
<b>Notify</b>	Select notify view name, if Notify is checked

**Table 14-16 SNMP Group Add Fields**

### 14.4.3. SNMP Community

In SNMP (Simple Network Management Protocol), community strings act as a form of authentication between the SNMP client and the SNMP agent.

When it comes to ensuring SNMP security, SNMP community strings are of vital importance. If you don't have the appropriate community string, you'll be unable to access key device information across your network.

The "SNMP community string" is like a user ID or password that allows access to the SNMP agent, for example, a router's, firewall's, or other network device's statistics.

SNMP strings are used only by devices which support the SNMPv1 and SNMPv2c version of SNMP. SNMPv3 uses username/password authentication, along with an encryption key

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

**Community Table**

Showing  entries      Showing 1 to 3 of 3 entries     

<input type="checkbox"/>	Community	Group	View	Access
<input type="checkbox"/>	COMN1		all	Read-Only
<input type="checkbox"/>	COMN2		all	Read-Only
<input type="checkbox"/>	public		all	Read-Only

First Previous 1 Next Last

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

**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 <b>Basic:</b> SNMP community specifies view and access right. <b>Advanced:</b> SNMP community specifies group.
Group Name	Specify the SNMP group configured by the command <b>snmp group</b> 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 <b>Read-Only:</b> Read only. <b>Read-Write:</b> Read and write.

**Table 14-17 SNMP Community Table Fields**

#### Add Community

Figure 14-18 SNMP Community Add Page

Field	Description
Community	The SNMP community name. Its maximum length is 20 characters.
Type	SNMP Community mode <b>Basic:</b> SNMP community specifies view and access right. <b>Advanced:</b> SNMP community specifies group.
View	Specify the SNMP view to define the object available to the community.
Access	SNMP access mode <b>Read-Only:</b> Read only. <b>Read-Write:</b> 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

Figure 14-19 SNMP Community Edit Page

Field	Description
<b>Community</b>	The Edit SNMP community name
<b>Type</b>	SNMP Community mode <b>Basic:</b> SNMP community specifies view and access right. <b>Advanced:</b> SNMP community specifies group.
<b>View</b>	Specify the SNMP view to define the object available to the community.
<b>Access</b>	SNMP access mode <b>Read-Only:</b> Read only. <b>Read-Write:</b> Read and write.
<b>Group</b>	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. Configuring and Displaying SNMP Users

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

**User Table**

Showing All entries Showing 1 to 3 of 3 entries

<input type="checkbox"/>	User	Group	Security Level	Authentication Method	Privacy Method
<input type="checkbox"/>	user1	g1	Authentication and Privacy	SHA	DES
<input type="checkbox"/>	user2	g2	Authentication	MD5	None
<input type="checkbox"/>	user3	g3	No Security	None	None

First Previous 1 Next Last

Add Edit Delete

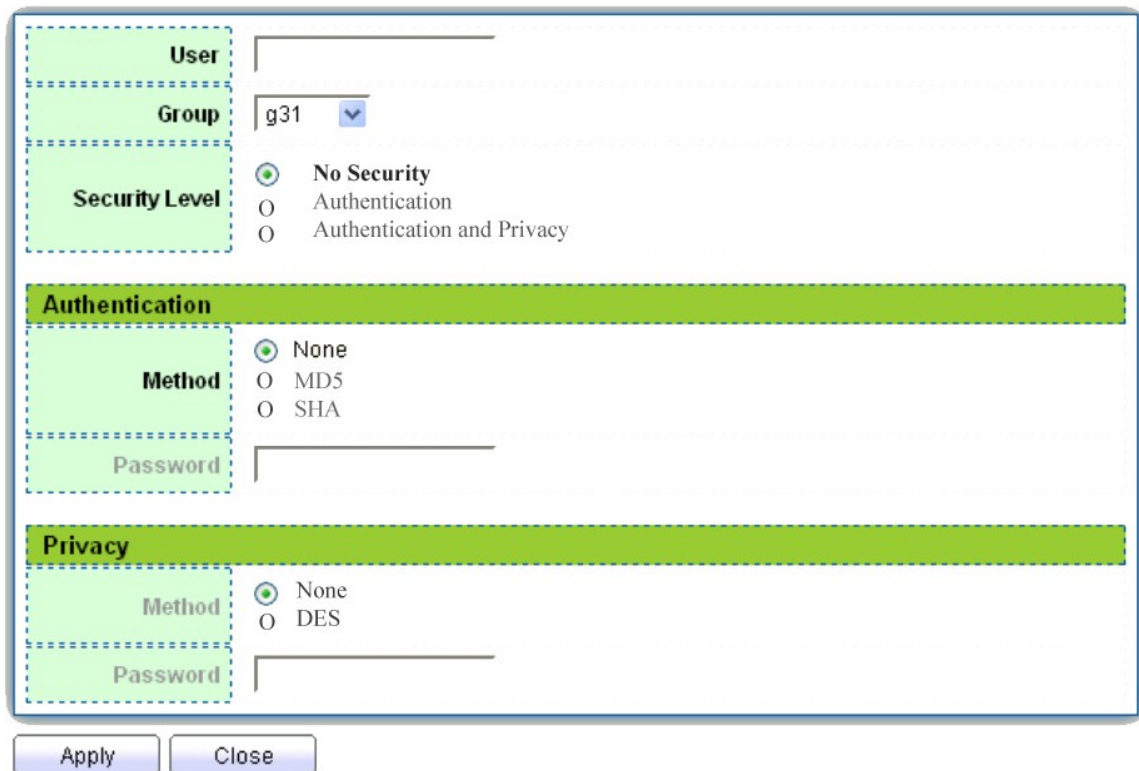
Configure SNMP Group to associate an SNMPv3 group with an SNMPv3 User

Figure 14-20 SNMP User Table Page

Field	Description
<b>User</b>	Specify the SNMP username 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
<b>Group</b>	Specify the SNMP group to which the SNMP user belongs.
<b>Security Level</b>	SNMP privilege mode <b>No Security :</b> Specify that no packet authentication is performed. <b>Authentication:</b> Specify that no packet authentication without encryption is performed. <b>Authentication and Privacy:</b> Specify that no packet authentication with encryption is performed.
<b>Authentication Method</b>	Authentication Protocol which is available when Privilege Mode is <b>Authentication</b> or <b>Authentication and Privacy</b> . <b>None:</b> No authentication required. <b>MD5:</b> Specify the HMAC-MD5-96 authentication protocol. <b>SHA:</b> Specify the HMAC-SHA-96 authentication protocol.
<b>Privacy Method</b>	Encryption Protocol <b>None:</b> No privacy required. <b>DES:</b> DES algorithm

Table 14-20 SNMP User Table Fields

#### Add User



The form is titled "Add User" and is enclosed in a blue border. It contains several sections with dashed green borders:

- User:** A text input field.
- Group:** A dropdown menu showing "g31".
- Security Level:** Three radio buttons: "No Security" (selected), "Authentication", and "Authentication and Privacy".
- Authentication:** A green header bar.
- Method:** Three radio buttons: "None" (selected), "MD5", and "SHA".
- Password:** A text input field.
- Privacy:** A green header bar.
- Method:** Two radio buttons: "None" (selected) and "DES".
- Password:** A text input field.

At the bottom, there are two buttons: "Apply" and "Close".

Figure 14-21 SNMP User Add Page

Field	Description
User	Specify the SNMP user name on the host that connects to the SNMP agent. The max character is 30 characters.
Group	Specify the SNMP group to which the SNMP user belongs.
Security Level	SNMP privilege mode <b>No Security</b> : Specify that no packet authentication is performed. <b>Authentication</b> : Specify that no packet authentication without encryption is performed. <b>Authentication and Privacy</b> : Specify that no packet authentication with encryption is performed.
<b>Authentication</b>	
Method	Authentication Protocol which is available when Privilege Mode is <b>Authentication</b> or <b>Authentication and Privacy</b> . <b>None</b> : No authentication required. <b>MD5</b> : Specify the HMAC-MD5-96 authentication protocol. <b>SHA</b> : Specify the HMAC-SHA-96 authentication protocol
Password	The authentication password, The number of character range is 8 to 32 characters.
<b>Privacy</b>	
Method	Encryption Protocol <b>None</b> : No privacy required. <b>DES</b> : DES algorithm
Password	The privacy password, The number of character range is 8 to 64 characters.

Table 14-21 SNMP User Add Fields



Edit User

The screenshot shows the 'Edit User' configuration page. It includes fields for 'User' (text input with 'user1'), 'Group' (dropdown menu with 'g1'), and 'Security Level' (radio buttons for 'No Security', 'Authentication', and 'Authentication and Privacy', with the last one selected). Below these are two main sections: 'Authentication' and 'Privacy'. Each section has a 'Method' dropdown (with 'None', 'MD5', and 'SHA' for Authentication; 'None' and 'DES' for Privacy) and a 'Password' text input field. The 'SHA' and 'DES' options are selected. At the bottom, there are 'Apply' and 'Close' buttons.

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 <b>No Security</b> : Specify that no packet authentication is performed. <b>Authentication</b> : Specify that no packet authentication without encryption is performed. <b>Authentication and Privacy</b> : Specify that no packet authentication with encryption is performed.
<b>Authentication</b>	
Method	Authentication Protocol which is available when Privilege Mode is Authentication or Authentication and Privacy. <b>None</b> : No authentication required. <b>MD5</b> : Specify the HMAC-MD5-96 authentication protocol. <b>SHA</b> : Specify the HMAC-SHA-96 authentication protocol.
Password	The authentication password, The number of character range is 8 to 32 characters.
<b>Privacy</b>	
Method	Encryption Protocol <b>None</b> : No privacy required. <b>DES</b> : DES algorithm
Password	The privacy password, The number of character range is 8 to 64 characters

Field	Description
User	Edit User name
Group	Specify the SNMP group to which the SNMP user belongs.
Security Level	SNMP privilege mode <b>No Security</b> : Specify that no packet authentication is performed. <b>Authentication</b> : Specify that no packet authentication without encryption is performed. <b>Authentication and Privacy</b> : Specify that no packet authentication with encryption is performed.
Authentication	
30 days credit	Authentication Protocol which is available when Privilege Mode is <b>Authentication</b> or <b>Authentication and Privacy</b> . <b>None</b> : No authentication required. <b>MD5</b> : Specify the HMAC-MD5-96 authentication protocol. <b>SHA</b> : Specify the HMAC-SHA-96 authentication protocol.
Password	The authentication password, the number of character range is 8 to 32 characters.
Privacy	
Method	Encryption Protocol <ul style="list-style-type: none"> <li><b>None</b>: No privacy required.</li> <li><b>DES</b>: DES algorithm</li> </ul>
Password	The privacy password, the number of character range is 8 to 64 characters.

**Table 14-22 SNMP User Edit Fields**

#### 14.4.5. Engine ID

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

**Local Engine ID**

☐ User Defined

Engine ID: 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	112223FDEDFE
192.168.1.99	00004DADDDDDDD

Add Edit Delete First Previous 1 Next Last

Figure 14-23 SNMP Engine ID Page



Field	Description
<b>Local Engine ID</b>	
<b>Engine ID</b>	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.
<b>Remote Engine ID Table</b>	
<b>Server Address</b>	Remote host
<b>Engine ID</b>	Specify Remote SNMP engine ID. The engine ID is range10 to 64 hexadecimal characters, and the hexadecimal number must be divided by 2.

**Table 14-23 SNMP Engine ID Fields**

Management>> SNMP>> Engine ID

Add Remote Engine ID

Figure 14-24 SNMP Remote Engine ID Add Page

Field	Description
<b>Address Type</b>	Remote host address type for Hostname/IPv4/IPv6
<b>Server Address</b>	Remote host
<b>Engine ID</b>	Specify Remote SNMP engine ID. The engine ID is range10 to 64 hexadecimal characters, and the hexadecimal number must be divided by 2.

**Table 14-24 SNMP Remote Engine ID Add Page**

Management>> SNMP>> Engine ID

Edit Remote Engine ID

Figure 14-25 SNMP Remote Engine ID Edit Page

Field	Description
<b>Server Address</b>	Edit Remote host address
<b>Engine ID</b>	Specify Remote SNMP engine ID. The engine ID is range10 to 64 hexadecimal characters, and the hexadecimal number must be divided by 2.

**Table 14-25 SNMP Remote Engine ID Edit Fields**

#### 14.4.6. Trap Event

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

Authentication Failure	<input checked="" type="checkbox"/> Enable
Link Up / Down	<input checked="" type="checkbox"/> Enable
Cold Start	<input type="checkbox"/> Enable
Warm Start	<input type="checkbox"/> Enable

Apply

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. Configure Hosts to Receive Notifications

To configure the hosts to receive SNMPv1/v2/v3 notification, click **Management > SNMP > Notification**.

**Notification Table**

Showing All entries Showing 1 to 2 of 2 entries

	Server Address	Server Port	Timeout	Retry	Version	Type	Community / User	Security Level
<input type="checkbox"/>	192.168.1.110	162			SNMPv1	Trap	COMN1	No Security
<input type="checkbox"/>	192.168.1.88	162			SNMPv1	Trap	COMN1	No Security

First Previous 1 Next Last

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

Add Edit Delete

Figure 14-27 SNMP Notification Table Page

Field	Description
Server Address	IP address or the hostname of the SNMP trap recipients.
Server Port	Recipients server UDP port number
Timeout	Specify the SNMP informs timeout
Retry	Specify the retry counter of the SNMP informs.
Version	Specify SNMP notification version <b>SNMPv1:</b> SNMP Version 1 notification. <b>SNMPv2:</b> SNMP Version 2 notification. <b>SNMPv3:</b> SNMP Version 3 notification.
Type	Notification Type <b>Trap:</b> Send SNMP traps to the host. <b>Inform:</b> 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

<b>Security Level</b>	<p>SNMP trap packet security level</p> <p><b>No Security:</b> Specify that no packet authentication is performed.</p> <p><b>Authentication:</b> Specify that no packet authentication without encryption is performed.</p> <p><b>Authentication and Privacy:</b> Specify that no packet authentication with encryption is performed.</p>
<b>Table 14-27 SNMP Notification Table Fields</b>	

**Add Notification**

<b>Address Type</b>	<input checked="" type="radio"/> Hostname <input type="radio"/> IPv4 <input type="radio"/> IPv6
<b>Server Address</b>	<input type="text"/>
<b>Version</b>	<input checked="" type="radio"/> SNMPv1 <input type="radio"/> SNMPv2 <input type="radio"/> SNMPv3
<b>Type</b>	<input checked="" type="radio"/> Trap <input type="radio"/> Inform
<b>Community / User</b>	COMN1 ▼
<b>Security Level</b>	<input checked="" type="radio"/> No Security <input type="radio"/> Authentication <input type="radio"/> Authentication and Privacy
<b>Server Port</b>	<input checked="" type="checkbox"/> Use Default <input type="text" value="162"/> (1 - 65535, default 162)
<b>Timeout</b>	<input checked="" type="checkbox"/> Use Default <input type="text" value="15"/> Sec (1 - 300, default 15)
<b>Retry</b>	<input checked="" type="checkbox"/> Use Default <input type="text" value="3"/> (1 - 255, default 3)

**Figure 14-28 SNMP Notification Add Page**

<b>Field</b>	<b>Description</b>
<b>Address Type</b>	Notify recipients host address type
<b>Server Address</b>	IP address or the hostname of the SNMP trap recipients.
<b>Version</b>	<p>Specify SNMP notification version</p> <p><b>SNMPv1:</b> SNMP Version 1 notification.</p> <p><b>SNMPv2:</b> SNMP Version 2 notification.</p> <p><b>SNMPv3:</b> SNMP Version 3 notification.</p>
<b>Type</b>	<p>Notification Type</p> <p><b>Trap:</b> Send SNMP traps to the host.</p> <p><b>Inform:</b> Send SNMP informs to the host.(version 1 have no inform)</p>
<b>Table 14-28 SNMP Notification Add Fields</b>	

Edit Notification

Server Address	192.168.1.110
Version	<input checked="" type="radio"/> SNMPv1 <input type="radio"/> SNMPv2 <input type="radio"/> SNMPv3
Type	<input checked="" type="radio"/> Trap <input type="radio"/> Inform
Community / User	COMN1 ▼
Security Level	<input checked="" type="radio"/> No Security <input type="radio"/> Authentication <input type="radio"/> Authentication and Privacy
Server Port	<input checked="" type="checkbox"/> Use Default <input type="text" value="162"/> (1 - 65535, default 162)
Timeout	<input checked="" type="checkbox"/> Use Default <input type="text" value="15"/> Sec (1 - 300, default 15)
Retry	<input checked="" type="checkbox"/> Use Default <input type="text" value="3"/> (1 - 255, default 3)

Figure 14-29 SNMP Notification Edit Page

Field	Description
Server Address	Edit SNMP notify recipients address.
Version	Specify SNMP notification version <b>SNMPv1:</b> SNMP Version 1 notification. <b>SNMPv2:</b> SNMP Version 2 notification. <b>SNMPv3:</b> SNMP Version 3 notification.
Type	Notification Type <b>Trap:</b> Send SNMP traps to the host. <b>Inform:</b> 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 <b>No Security:</b> Specify that no packet authentication is performed. <b>Authentication:</b> Specify that no packet authentication without encryption is performed. <b>Authentication and Privacy:</b> Specify that no packet authentication with encryption is performed.
Server Port	Recipients server UDP port number, if “use default” checked the value is 162, else user configure
Timeout	Specify the SNMP informs timeout, if “use default” checked the value is 15, else user configure
Retry	Specify the SNMP informs retry count, if “use default” checked the value is 3, else user configure

Table 14-29 SNMP Notification Edit Fields

## 14.5. RMON

### 14.5.1. Statistics

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

#### Statistics Table

Refresh Rate  sec

	Entry	Port	Bytes Received	Drop Events	Packets Received	Broadcast Packets	Multicast Packets	CRC & Align Errors	Undersize Packets	Oversize Packets
<input type="checkbox"/>	1	GE1	0	0	0	0	0	0	0	0
<input type="checkbox"/>	2	GE2	0	0	0	0	0	0	0	0
<input type="checkbox"/>	3	GE3	0	0	0	0	0	0	0	0
<input type="checkbox"/>	4	GE4	0	0	0	0	0	0	0	0
<input type="checkbox"/>	5	GE5	0	0	0	0	0	0	0	0
<input type="checkbox"/>	6	GE6	0	0	0	0	0	0	0	0
<input type="checkbox"/>	7	GE7	396656	0	2488	113	454	0	0	0
<input type="checkbox"/>	8	GE8	0	0	0	0	0	0	0	0
<input type="checkbox"/>	9	GE9	0	0	0	0	0	0	0	0
<input type="checkbox"/>	10	GE10	0	0	0	0	0	0	0	0
<input type="checkbox"/>	11	LAG1	0	0	0	0	0	0	0	0
<input type="checkbox"/>	12	LAG2	0	0	0	0	0	0	0	0
<input type="checkbox"/>	13	LAG3	0	0	0	0	0	0	0	0
<input type="checkbox"/>	14	LAG4	0	0	0	0	0	0	0	0
<input type="checkbox"/>	15	LAG5	0	0	0	0	0	0	0	0
<input type="checkbox"/>	16	LAG6	0	0	0	0	0	0	0	0
<input type="checkbox"/>	17	LAG7	0	0	0	0	0	0	0	0
<input type="checkbox"/>	18	LAG8	0	0	0	0	0	0	0	0

Clear

Refresh

View

Figure 14-30: RMON Statistics page.

Field	Description
<b>Port</b>	The port for the RMON statistics.
<b>Bytes Received</b>	Number of octets received, including bad packets and FCS octets, but excluding framing bits.
<b>Drop Events</b>	Number of packets that were dropped.
<b>Packets Received</b>	Number of packets received, including bad packets, Multicast packets, and Broadcast packets.
<b>Broadcast Packets</b>	Number of good Broadcast packets received. This number does not include Multicast packets.
<b>Multicast Packets</b>	Number of good Multicast packets received.
<b>CRC &amp; Align Errors</b>	Number of CRC and Align errors that have occurred.
<b>Undersize Packages</b>	Number of undersized packets (less than 64 octets) received.
<b>Oversize Packages</b>	Number of oversized packets (over 1518 octets) received.
<b>Fragments</b>	Number of fragments (packets with less than 64 octets, excluding framing bits, but including FCS octets) received.
<b>Jabbers</b>	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:
<b>Packet data length is greater than MRU.</b> <b>Packet has an invalid CRC.</b> <b>RX error event has not been detected.</b>	



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

Clear

Refresh

Close

**Figure 14-31: View RMON Statistics page.**

## 14.5.2. History

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

History Table

Showing All entries

Showing 1 to 2 of 2 entries

Q

	Entry	Port	Interval	Owner	Sample	
					Maximum	Current
<input type="checkbox"/>	1	GE1	1800	RAINBOW	50	50
<input type="checkbox"/>	2	GE1	1800	CERR	50	50

First

Previous

1

Next

Last

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

Add

Edit

Delete

View

**Figure 14-32: RMON History page.**



Field	Description
Port	The port for the RMON history.
Interval	The number of seconds for each sample.
Owner	The owner name of event (0~31 characters).
Sample Maximum	The maximum number of buckets.
Sample Current	The current number of buckets.

**Table 14-31: RMON History fields.**

Field	Description
Add	Add the new RMON history entries
Edit	Edit the RMON history
Delete	Delete the RMON histories.
View	View the history log.

**Table 14-32: RMON History buttons.**

Add History

Entry 3

Port GE1 ▼

Max Sample 50 (1 - 50, default 50)

Interval 1800 (1 - 3600, default 1800)

Owner

Apply Close

Figure 14-33: RMON History Add page.

Field	Description
Port	Specify port for the RMON history.
Max Sample	Specify the maximum number of buckets.
Interval	Specify the number of seconds for each sample.
Owner	Specify the owner name of event (0~31 characters).

**Table 14-33: RMON History buttons.**

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.**

[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
<b>Port</b>	The port for the RMON statistics.
<b>Bytes Received</b>	Number of octets received, including bad packets and FCS octets, but excluding framing bits.
<b>Drop Events</b>	Number of packets that were dropped.
<b>Packets Received</b>	Number of packets received, including bad packets, Multicast packets, and Broadcast packets.
<b>Broadcast Packets</b>	Number of good Broadcast packets received. This number does not include Multicast packets.
<b>Multicast Packets</b>	Number of good Multicast packets received.
<b>CRC &amp; Align Errors</b>	Number of CRC and Align errors that have occurred.
<b>Undersize Packages</b>	Number of undersized packets (less than 64 octets) received.
<b>Oversize Packages</b>	Number of oversized packets (over 1518 octets) received.
<b>Fragments</b>	Number of fragments (packets with less than 64 octets, excluding framing bits, but including FCS octets) received.
<b>Jabbers</b>	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.
<b>Collision</b>	Number of collisions received. If Jumbo Frames are enabled, the threshold of Jabber Frames is raised to the maximum size of Jumbo Frames.
<b>Utilisation</b>	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. RMON Events

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

[Event Table](#)

Showing **All** entries

Showing 1 to 2 of 2 entries

<input type="checkbox"/>	Entry	Community	Description	Notification	Time	Owner
<input type="checkbox"/>	1		Default Description	None		RAINBOW
<input type="checkbox"/>	2		Default Description	None		FEER

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

The SNMP service is currently disabled.

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

[Add](#)

[Edit](#)

[Delete](#)

[View](#)

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: <b>None:</b> Nothing for notification. <b>Event Log:</b> Logging the event in the RMON Event Log table. <b>Trap:</b> Send a SNMP trap. <b>Event Log and Trap:</b> Logging the event and send the SNMP trap.
Time	The time that the event was triggered.
Owner	The owner for the event.

**Table 14-36 RMON Event fields.**

**Add Event**

---

Entry	3
Notification	<input checked="" type="radio"/> None <input type="radio"/> Event Log <input type="radio"/> Trap <input type="radio"/> Event Log and Trap
Community	Default Community
Description	Default Description
Owner	

Apply Close

**Figure 14-37: RMON Event Add page.**

Field	Description
Community	Specify the SNMP community when the notification type is specified as “Trap” or “Event Log and Trap”.
Description	Specify the description for the event.
Notification	Specify the notification type for the event, and the possible value are: <b>None:</b> Nothing for notification. <b>Event Log:</b> Logging the event in the RMON Event Log table. <b>Trap:</b> Send a SNMP trap. <b>Event Log and Trap:</b> Logging the event and send the SNMP trap.
Owner	Specify owner for the event.

**Table 14-37: RMON Event Add fields.**

**Edit Event**

---

Entry	2
Notification	<input checked="" type="radio"/> None <input type="radio"/> Event Log <input type="radio"/> Trap <input type="radio"/> Event Log and Trap
Community	
Description	Default Description
Owner	FEER

Apply Close

**Figure 14-38: RMON Event Edit page.**

Field	Description
Community	Specify the SNMP community when the notification type is specified as “Trap” pr “Event Log and Trap”.
Description	Specify the description for the event.
Notification	Specify the notification type for the event, and the possible value are: <b>None:</b> Nothing for notification. <b>Event Log:</b> Logging the event in the RMON Event Log table. <b>Trap:</b> Send a SNMP trap. <b>Event Log and Trap:</b> Logging the event and send the SNMP trap.
Owner	Specify owner for the event.

**Table 14-38: RMON Event Edit fields.**

#### View Event Log

Entry: 2

Showing All entries

Showing 0 to 0 of 0 entries



Log ID	Time	Description
0 results found.		
<div> <span>Close</span> <span>First</span> <span>Previous</span> <span>1</span> <span>Next</span> <span>Last</span> </div>		

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. RMON Alarms

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

#### Alarm Table

Showing All entries

Showing 1 to 2 of 2 entries

	Entry	Port	Counter		Sampling	Interval	Owner	Trigger	Rising	
			Name	Value					Threshold	Event
<input type="checkbox"/>	1	GE1	DropEvents	0	Absolute	100	RAINBOW	Rising	100	Default Descript
<input type="checkbox"/>	2	GE1	DropEvents	0	Absolute	100	DDDEEE	Rising	100	Default Descript

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

Add
Edit
Delete

**Figure 14-40: RMON Alarm page.**

Field	Description
Port	The port configuration for the RMON alarm.
Counter	<p>The counter for sampling</p> <p><b>DropEvents (Drop Event):</b> Total number of events received in which the packets were dropped.</p> <p><b>Octets (Received Bytes):</b> Octets.</p> <p><b>Pkts (Received Packets):</b> Number of packets.</p> <p><b>BroadcastPkts (Broadcast Packets Received):</b> Broadcast packets.</p> <p><b>MulticastPkts (Multicast Packets Received):</b> Multicast packets.</p> <p><b>CRCAlignError (CRC and Align Error):</b> CRC alignment error.</p> <p><b>UndersizePkts (Undersize Packets):</b> Number of undersized packets.</p>

**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.

<b>Sampling</b>	The sampling type including: <b>Absolute:</b> The selected variable value is compared directly with the thresholds at the end of the sampling interval. <b>Delta:</b> The selected variable value of the last sample is subtracted from the current value and the difference is compared with the thresholds.
<b>Interval</b>	The number of seconds for each sample.
<b>Owner</b>	The owner for the alarm entry.
<b>Trigger</b>	The type of event triggering.
<b>Rising Threshold</b>	The threshold for firing rising event.
<b>Rising Event</b>	The rising event when alarm was fired.
<b>Falling Threshold</b>	The threshold for firing falling event.
<b>Falling Event</b>	The falling event when alarm was fired.
<b>14-40: RMON Alarm fields.</b>	

**Add Alarm**

<b>Entry</b>	3
<b>Port</b>	GE1
<b>Counter</b>	Drop Events
<b>Sampling</b>	<input checked="" type="radio"/> Absolute <input type="radio"/> Delta
<b>Interval</b>	100 Sec (1 - 2147483647, default 100)
<b>Owner</b>	
<b>Trigger</b>	<input checked="" type="radio"/> Rising <input type="radio"/> Falling <input type="radio"/> Rising and Falling
<b>Rising</b>	
<b>Threshold</b>	100 (0 - 2147483647, default 100)
<b>Event</b>	1 - Default Description
<b>Falling</b>	
<b>Threshold</b>	20 (0 - 2147483647, default 20)
<b>Event</b>	1 - Default Description

Apply Close

**Figure 14-41: RMON Alarm Add page.**

Field	Description
<b>Port</b>	Specify the port for sampling
<b>Counter</b>	Specify the counter for sampling <b>Drop Event:</b> Total number of events received in which the packets were dropped. <b>Received Bytes (Octets):</b> Octets. <b>Received Packets:</b> Number of packets. <b>Broadcast Packets Received:</b> Broadcast packets. <b>Multicast Packets Received:</b> Multicast packets. <b>CRC and Align Error:</b> CRC alignment error.



	<b>Undersize Packets:</b> Number of undersized packets. <b>Oversize Packets:</b> Number of oversized packets.
	<b>Fragments:</b> Total number of packet fragment. <b>Jabbers:</b> Total number of packet jabber. <b>Collisions:</b> Collision. <b>Frames of 64 Bytes:</b> Number of packets size 64 octets. <b>Frames of 65 to 127 Bytes:</b> Number of packets size 65 to 127 octets. <b>Frames of 128 to 255 Bytes:</b> Number of packets size 128 to 255 octets. <b>Frames of 256 to 511 Bytes:</b> Number of packets size 256 to 511 octets. <b>Frames of 512 to 1023 Bytes:</b> Number of packets size 512 to 1023 octets. <b>Frames Greater than 1024 Bytes:</b> Number of packets size 1024 to 1518 octets.
<b>Sampling</b>	Specify the sampling type. <b>Absolute:</b> The selected variable value is compared directly with the thresholds at the end of the sampling interval. <b>Delta:</b> The selected variable value of the last sample is subtracted from the current value and the difference is compared with the thresholds.
<b>Interval</b>	Specify the sampling interval.
<b>Owner</b>	Specify the owner for the sampling.
<b>Trigger</b>	Specify the type for the alarm trigger.
<b>Rising Threshold</b>	Specify the threshold for firing rising event.
<b>Rising Event</b>	Specify the index of rising event when alarm was fired.
<b>Falling Threshold</b>	Specify the threshold for firing falling event.
<b>Falling Event</b>	Specify the index of falling event when alarm was fired.

**Table 14-41: RMON Alarm Add fields.**

[Edit Alarm](#)

<b>Entry</b>	2
<b>Port</b>	GE1 ▼
<b>Counter</b>	Drop Events ▼
<b>Sampling</b>	<input checked="" type="radio"/> Absolute <input type="radio"/> Delta
<b>Interval</b>	100 Sec (1 - 2147483647, default 100)
<b>Owner</b>	DDDEEE
<b>Trigger</b>	<input checked="" type="radio"/> Rising <input type="radio"/> Falling <input type="radio"/> Rising and Falling
<b>Rising</b>	
<b>Threshold</b>	100 (0 - 2147483647, default 100)
<b>Event</b>	1 - Default Description ▼
<b>Falling</b>	
<b>Threshold</b>	20 (0 - 2147483647, default 20)
<b>Event</b>	1 - Default Description ▼
<input type="button" value="Apply"/> <input type="button" value="Close"/>	

**Figure 14-42: RMON Alarm Edit page.**



Field	Description
Port	Specify the port for sampling
Counter	Specify the counter for sampling <b>Drop Event:</b> Total number of events received in which the packets were dropped. <b>Received Bytes (Octets):</b> Octets. <b>Received Packets:</b> Number of packets. <b>Broadcast Packets Received:</b> Broadcast packets. <b>Multicast Packets Received:</b> Multicast packets. <b>CRC and Align Error:</b> CRC alignment error. <b>Undersize Packets:</b> Number of undersized packets. <b>Oversize Packets:</b> Number of oversized packets.
<b>Fragments:</b> Total number of packet fragment. <b>Jabbers:</b> Total number of packet jabber. <b>Collisions:</b> Collision. <b>Frames of 64 Bytes:</b> Number of packets size 64 octets. <b>Frames of 65 to 127 Bytes:</b> Number of packets size 65 to 127 octets. <b>Frames of 128 to 255 Bytes:</b> Number of packets size 128 to 255 octets. <b>Frames of 256 to 511 Bytes:</b> Number of packets size 256 to 511 octets. <b>Frames of 512 to 1023 Bytes:</b> Number of packets size 512 to 1023 octets. <b>Frames Greater than 1024 Bytes:</b> Number of packets size 1024 to 1518 octets.	
Sampling	Specify the sampling type. <b>Absolute:</b> The selected variable value is compared directly with the thresholds at the end of the sampling interval. <b>Delta:</b> 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.
<b>Table 14-42: RMON Alarm Edit fields.</b>	

This page left blank intentionally

## 15. PoE Settings

### 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	<input type="radio"/> None <input type="radio"/> 5 sec <input checked="" type="radio"/> 10 sec <input type="radio"/> 30 sec

**Port Setting Table**

Entry	Port	PortEnable	Status	Type	Level	Actual Power(mW)	Voltage(V)	Current(mA)
<input type="checkbox"/>	1	GE1	Enabled	Off	N/A	N/A	N/A	N/A
<input type="checkbox"/>	2	GE2	Enabled	Off	N/A	N/A	N/A	N/A
<input type="checkbox"/>	3	GE3	Enabled	Off	N/A	N/A	N/A	N/A
<input type="checkbox"/>	4	GE4	Enabled	Off	N/A	N/A	N/A	N/A
<input type="checkbox"/>	5	GE5	Enabled	Off	N/A	N/A	N/A	N/A
<input type="checkbox"/>	6	GE6	Enabled	Off	N/A	N/A	N/A	N/A
<input type="checkbox"/>	7	GE7	Enabled	Off	N/A	N/A	N/A	N/A
<input type="checkbox"/>	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 port you want to configure, Click the “Edit” button on the table title to edit

#### Edit Port Setting

**Port** GE1

**PortEnable** ☒ Enable ☐ Disable

[Apply](#) [Close](#)

**Figure 15-44: Edit PoE Port Setting**

### 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	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Tue	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Thu	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Sun	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Sat	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Mon	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Fri	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

[Apply](#)

This page left blank intentionally

## 16. Routing

### 16.1. IPV4 Management and Interface

#### 16.1.1. IPv4 Interface Table

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

**Routing >> IPv4 Management and interfaces>> IPv4 Interface**

**Figure 16:1 IP V4 Interface Table**

<input type="checkbox"/>	Interface	IP Address Type	IP Address	Mask	Status	Roles
<input type="checkbox"/>	VLAN 1	Static	192.168.1.16	255.255.255.0	Valid	primary

Buttons: Add, Edit, Delete

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

**Figure 16:2 Routing >> IPv4 Management and interfaces>> IPv4 Interface**

**Add IPv4 Interface**

<b>Interface</b>	<input checked="" type="radio"/> VLAN <span>1</span>
	<input type="radio"/> Loopback
<b>Address Type</b>	<input checked="" type="radio"/> Dynamic
	<input type="radio"/> Static
<b>IP Address</b>	<input type="text"/>
<b>Mask</b>	<input checked="" type="radio"/> Network Mask <input type="text"/> <input type="radio"/> Prefix Length <input type="text"/> (8 - 30)
<b>Roles</b>	<input checked="" type="radio"/> primary
	<input type="radio"/> sub

Buttons: Apply, Close

#### 16.1.2. IPv4 Routes

1. Click 'Routing > ipv4 Management Interface > ipv4 Routes' to display the menu in the navigation tree which will allow you to enter the 'ipv4 Routes' interface to view the current ipv4 routes information, as shown in the following figure.

2. Ipv4 routing interface click Add to add ipv4 routing information as shown below:

## Add IPv4 Static Route

Figure 16:3 Adding an IPv4 Static Route

### Add IPv4 Static Route

IP Address	<input type="text"/>
Mask	<input checked="" type="radio"/> Network Mask <input type="text"/> <input type="radio"/> Prefix Length <input type="text"/> (0 - 32)
Next Hop Router IP Address	<input type="text"/>
Metric	<input type="text"/> 1 (1 - 255, default 1)

## 16.1.3. ARP Interface

1. Click the 'Routing > IPV4 Management and Interface > ARP' menu in the navigation tree to enter the 'ARP' interface. This will allow you to view the current ARP table information, configure the ARP aging time, and clear the ARP table entries, as shown in the following figure

Figure 16:4 IPv4 Management Interface

- Status
  - System Information
  - Logging Message
- Port
  - Link Aggregation
  - MAC Address Table
- Network
  - Port
  - VLAN
  - MAC Address Table
  - Spanning Tree
  - ERPS
  - Discovery
  - DHCP
  - Multicast
- Routing**
  - IPv4 Management and Interfaces
    - IPv4 Interface
    - IPv4 Routes
    - ARP**
  - IPv6 Management and Interfaces
    - Rip Routes Management
    - Osfp Routes Management
    - VRRP Management
  - Security
    - ACL
    - QoS
  - Diagnostics
  - Management

ARP Entry Age Out

1200 Sec (15 - 21600, default 1200)

Clear ARP Table Entries

☐ All  
☐ Dynamic  
☐ Static  
☒ Normal Age Out

ARP Table

	Interface	IP Address	MAC Address	Status
<input type="checkbox"/>	VLAN 1	192.168.1.1	24:4c:07:33:17:64	Dynamic
<input type="checkbox"/>	VLAN 1	192.168.1.18	d4:5d:df:13:42:86	Dynamic
<input type="checkbox"/>	VLAN 1	192.168.1.66	f8:0d:60:74:d0:9f	Dynamic
<input type="checkbox"/>	VLAN 1	192.168.1.74	00:18:93:15:3f:a5	Dynamic
<input type="checkbox"/>	VLAN 1	192.168.1.75	08:97:98:f3:77:26	Dynamic
<input type="checkbox"/>	VLAN 1	192.168.1.82	b8:f8:83:b9:4e:52	Dynamic
<input type="checkbox"/>	VLAN 1	192.168.1.93	3c:97:0e:cc:41:53	Dynamic
<input type="checkbox"/>	VLAN 1	192.168.1.108	c4:34:6b:15:07:db	Dynamic
<input type="checkbox"/>	VLAN 1	192.168.1.109	24:69:68:a0:be:f5	Dynamic
<input type="checkbox"/>	VLAN 1	192.168.1.111	d0:5f:64:3e:37:ad	Dynamic
<input type="checkbox"/>	VLAN 1	192.168.1.117	5c:b9:01:ae:52:2e	Dynamic
<input type="checkbox"/>	VLAN 1	192.168.1.119	d0:bf:9c:21:2e:fd	Dynamic
<input type="checkbox"/>	VLAN 1	192.168.1.135	fc:aa:14:4e:21:7a	Dynamic

3. Click Add in the ARP interface to add static ARP table entries, as shown in the following figure:

Figure 16:5 Adding an IP v4 Management interface and ARP

- Status
  - System Information
  - Logging Message
- Port
  - Link Aggregation
  - MAC Address Table
- Network
  - Port
  - VLAN
  - MAC Address Table
  - Spanning Tree
  - ERPS
  - Discovery
  - DHCP
  - Multicast
- Routing**
  - IPv4 Management and Interfaces
    - IPv4 Interface
    - IPv4 Routes
    - ARP**

Add ARP

Interface

VLAN 1

Note: Only interfaces with an valid IPv4 address are available for selection

IP Address

MAC Address



## 16.2. IPv6 management and interface

### 16.2.1. IPv6 Interfaces

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

**Figure 16:6 IPv6 Management Interface**

IPv6 Unicast Routing ☐ Enable

Apply Cancel

**IPv6 Interface Table**

Interface	DHCPv6 Client		Auto Configuration	DAD Attempts
	Stateless	Information Refresh Time		
<input type="checkbox"/> VLAN 1	Disabled	86400	Enabled	1

Add Edit Delete

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

**Figure 16:7 Add IPv6 Interface**

**Add IPv6 Interface**

Interface: ☒ VLAN 1 ☐ Loopback

Auto Configuration: ☒ Enable

DAD Attempts:  (0 - 600, default 1)

**DHCPv6 Client**

Stateless: ☐ Enable

Information Refresh Time:  (86400 - 4294967294, default 86400)

Minimum Information Refresh Time:  (600 - 4294967294, default 600)

Apply Close

### 16.2.2. IPv6 Address

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

**Figure 16: 8 IPv6 Address table**

**IPv6 Address Table**

Interface:

IPv6 Address Type	IPv6 Address	IPv6 Prefix Length	DAD Status
<input type="checkbox"/> Link Local	fe80::2e0:4cffe02:4e	64	Active
<input type="checkbox"/> Multicast	ff02::1:ff02:4e		
<input type="checkbox"/> Multicast	ff02::1		
<input type="checkbox"/> Multicast	ff01::1		

Add Delete

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

**Figure 16: 9 Add IPv6 Interface**

**Add IPv6 Interface**

Interface	VLAN 1
IPv6 Address Type	<input checked="" type="radio"/> Global <input type="radio"/> Link Local
IPv6 Address	<input type="text"/>
Prefix Length	<input type="text"/> (3 - 128)
EUI-64	<input type="checkbox"/> Enable

### 16.2.3. IPv6 Routes

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

**Figure 16:10 IPv6 Routing Table**

**IPv6 Routing Table**

<input type="checkbox"/>	Destination IP Prefix	Prefix Length	Route Type	Next Hop Router IP Address	Metric	Administrative Distance	Outgoing Interface
0 results found.							

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

**Figure 16:11 Add IPv6 Static Route**

**Add IPv6 Static Route**

IPv6 Prefix	<input type="text"/>
IPv6 Prefix Length	<input type="text"/> (0 - 128)
Next Hop Router IP Address	<input type="text"/>
Metric	<input type="text"/> (1 - 255, default 1)

### 16.2.4. IPv6 Neighbours

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

**Figure 16:12 View Current IPv6 Neighbours**

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

**Figure 16:13 Add IPv6 neighbours.**

## 16.3. RIP Route Management

1. Click 'Routing > Rip Route Management > Rip Route setting' menu in the navigation tree to enter the 'Rip Route setting' interface, you can enable the rip, and you can check the setup of notification routes, as shown in the following figure.

**Figure 16:14 RIP Route Information**

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

Figure 16:15 Network Setting table

**Network Setting table**

---

Network Ipv4 Address	<input type="text"/>
Network Mask	<input type="text"/>

## 16.4. OSPF Routing Management

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

Figure 16:16 OSPF Route Information

**OSPF Routes Info**

OSPF Routes status ☐ Enable

**Area Network Setting table**

Showing All entries Showing 0 to 0 of 0 entries

Area Id	Network Ipv4 Address	Network Mask
0 results found.		

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

Figure 16: 17 Area Network Setting Table

**Area Network Setting table**

---

Area Id	<input type="text" value="A.B.C.D"/>
Network Ipv4 Address	<input type="text"/>
Network Mask	<input type="text"/>

### 16.5. VRRP Management

1. Click ‘Routing > VRRP Management>VRRP Setting, configuration table as shown in the following figure.

Figure 16:18 VRRP Interface Setting table

VRRP Interface Setting table

<input type="checkbox"/>	Router ID	Virtual IP	State	Priority	Advertise	Preempt	Delay	
--------------------------	-----------	------------	-------	----------	-----------	---------	-------	--

0 results found.

Add

Delete

2.Click the Add button to add VRRP as shown below:

Figure 16:19 Add IPv4 VRRP Interface

Add IPv4 VRRP Interface

Interface

VLAN 

1

Router ID

(1 - 5)

Virtual IP

Priority

(1 - 254, default 100)

Advertise

(1 - 255, default 1)

Preempt

☐ Enable

Delay

(1 - 255)

Apply

Close

This page left blank intentionally



## **17. ERPS**

ERPS (Ethernet Ring Protection Switching) is the G.8032 ring protection protocol standardized by ITU-T. It achieves carrier-grade reliability with sub-50ms convergence speed. If all devices in the ring support this protocol, interoperability can be ensured.

**The key concepts of ERPS include ERPS ring, node, port roles, and port states.**

- **ERPS Instance**

Unlike STP instances, an ERPS instance functions similarly to an ERSP domain. It consists of switches configured with the same instance ID and control VLAN, interconnected to form a logical group.

- **Control VLAN**

The control VLAN carries ERPS protocol packets (e.g., R-APS messages). Similar to ERSP, protocol packets are tagged with the control VLAN ID.

- **RPL (Ring Protection Link)**

A designated link blocked during normal operation to prevent loops in the bridged ring.

- **ERPS Ring**

A basic ERPS unit composed of Layer 2 switches interconnected with the same control VLAN.

### **ERPS Nodes**

A Layer 2 switch participating in an ERPS ring is called a node. Each node can have no more than two ports in the same ERPS ring. Nodes are categorized into four types:

1. RPL Owner Node
2. RPL Neighbour Node
3. RPL Next Neighbour Node
4. Common Node

### **Port Roles**

ERPS defines four port roles:

#### **1. RPL Owner Port**

Only one RPL Owner Port exists per ERPS ring (manually configured).

Blocks traffic during normal operation to prevent loops.

The node hosting this port becomes the RPL Owner Node.

#### **2. RPL Neighbour Port**

Only one RPL Neighbour Port exists per ERPS ring.

Must connect to the RPL Owner Port.

Blocked alongside the RPL Owner Port during normal operation.

The node hosting this port becomes the RPL Neighbour Node.

#### **3. RPL Next Neighbour Port**

Up to two RPL Next Neighbour Ports can exist per ERPS ring.

Must connect to the RPL Owner Node or RPL Neighbour Node.

Nodes hosting these ports are RPL Next Neighbour Nodes.

Note: Functionally similar to Common Nodes and can be replaced by them in configurations.

#### **4. Common Port**

All ports not classified as RPL Owner/Neighbour/Next Neighbour.

Nodes with only Common Ports are Common Nodes

## Port States

ERPS port states:

- **Forwarding**  
Forwards user traffic and processes/sends R-APS messages.  
Relays R-APS packets from other nodes.
- **Discarding**  
Processes/sends R-APS messages only.  
Blocks user traffic and R-APS packet relaying.
- **Disabled**  
Port is inoperable (e.g., due to link down).

## 8. ERPS Working Modes

- **Revertive Mode**  
Upon link failure: RPL unblocks for protection.  
After failure recovery: RPL re-blocks to prevent loops.
- **Non-Revertive Mode**  
After failure recovery: Faulty port remains blocked indefinitely.  
RPL stays unblocked permanently.

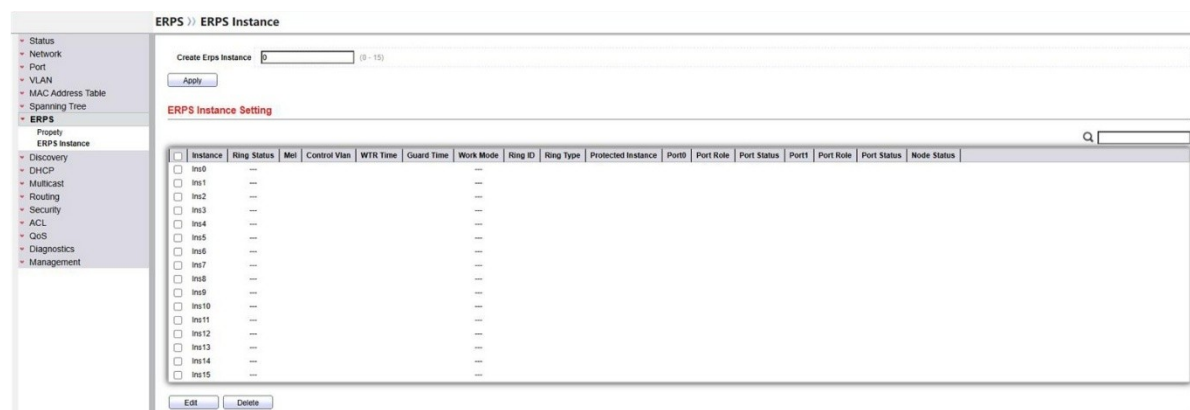
## 17.1. Feature Configuration

Click the “ERPS” menu in the navigation tree to access the Feature Configuration interface, where you can enable or disable the ERPS protocol, as shown in the figure below.



## 17.2. ERPS Instances

1. Click ‘ERPS > ERPS Instance’ menu in the navigation tree to enter the ‘ERPS Instance’ interface to create ERPS instances, view the configuration information of each instance, and delete instances, as shown in the following figure.



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

ERPS >> ERPS Instance

Ring Instance Config

Ins: 0

Ring Status: ☒ Disable ☐ Enable

Met: 0 (Valid range is 0-7)

Protected Instance: 0 (Valid range is 0-15)

Control Vlan: 0 (Valid range is 1-4094)

WTR Time: 5 (Valid range is 1-12 Min Default is 5 Min)

Guard Time: 500 (Valid range is 100-2000 ms (Default is 500 ms))

Work Mode: ☒ Revertive ☐ Non\_revertive

Ring ID: 1 (Valid range is 1-239)

Ring Type: 0 (0-master ring, 1-sub ring)

Port0: N/A

Port0 Role: ☒ Normal ☐ master ☐ neighbour ☐ next-neighbour

Port1: N/A

Port1 Role: ☒ Normal ☐ master ☐ neighbour ☐ next-neighbour

Apply Close