



GS-5424G

User Manual

03-2018 / v1.0

Edimax Technology Co., Ltd.

No. 278, Xinhua 1st Rd., Neihu Dist., Taipei City, Taiwan

Email: support@edimax.com.tw

Edimax Technology Europe B.V.

Fijenhof 2, 5652 AE Eindhoven, The Netherlands

Email: support@edimax.nl

Edimax Computer Company

3350 Scott Blvd., Bldg.15 Santa Clara, CA 95054, USA

Live Tech Support: 1(800) 652-6776

Email: support@edimax.com

CONTENTS

I	Introduction	1
I-1	Overview	1
I-2	Package Content.....	1
I-3	Features.....	2
I-4	Product Components.....	2
I-4-1	Ports.....	2
I-4-2	LED Indicators	3
II	Installation.....	4
II-1	Mounting the Switch.....	4
II-1-1	Placement Tips.....	4
II-1-2	Desktop Mounting	5
II-1-3	Rack Mounting.....	5
III	Getting Started	7
III-1	Connecting to Power	7
III-2	Connecting to Network	8
III-3	Starting the Web-based Configuration Utility.....	9
III-3-1	Logging In.....	10
III-3-2	Logging Out.....	11
IV	Web-based Switch Configuration.....	12
IV-1	Status.....	13
IV-1-1	System Information	13
IV-1-2	Logging Message.....	15
IV-1-3	Port	16
IV-1-4	Link Aggregation	21
IV-1-5	MAC Address Table.....	22
IV-2	Network.....	23
IV-2-1	IP Address	23
IV-2-2	System Time	26
IV-3	Port.....	28
IV-3-1	Port Setting.....	28
IV-3-2	Long Range Mode	31
IV-3-3	Error Disable	32
IV-3-4	Link Aggregation	33
IV-3-5	EEE	39

IV-3-6	Jumbo Frame	40
IV-4	VLAN	41
IV-4-1	VLAN	41
IV-4-2	Voice VLAN	49
IV-4-3	MAC VLAN	52
IV-5	MAC Address Table	55
IV-5-1	Dynamic Address	55
IV-5-2	Static Address	55
IV-5-3	Filtering Address	56
IV-6	Spanning Tree.....	57
IV-6-1	Property.....	57
IV-6-2	Port Setting.....	59
IV-6-3	MST Instance	61
IV-6-4	MST Port Setting.....	63
IV-6-5	Statistics.....	65
IV-7	Discovery.....	67
IV-7-1	LLDP	67
IV-8	Multicast	81
IV-8-1	General	81
IV-8-2	IGMP Snooping	86
IV-8-3	MVR	93
IV-9	Security.....	98
IV-9-1	RADIUS.....	98
IV-9-2	Management Access.....	101
IV-9-3	Authentication Manager	107
IV-9-4	Port Security	116
IV-9-5	Protected Port	118
IV-9-6	Storm Control	120
IV-9-7	DoS.....	122
IV-9-8	DHCP Snooping	126
IV-9-9	IP Source Guard	134
IV-10	ACL.....	139
IV-10-1	MAC ACL.....	139
IV-10-2	MAC ACE	140
IV-10-3	IPv4 ACL	142
IV-10-4	IPv4 ACE	143
IV-10-5	ACL Binding	147
IV-11	QoS.....	149
IV-11-1	General.....	149
IV-11-2	Rate Limit	156
IV-12	Diagnostics	159

IV-12-1	Logging	159
IV-12-2	Mirroring	161
IV-12-3	Ping	163
IV-12-4	Traceroute	164
IV-12-5	Copper Test	165
IV-12-6	Fiber Module	166
IV-12-7	UDLD	167
IV-13	Management	171
IV-13-1	User Account	171
IV-13-2	Fireware	173
IV-13-3	Configuration	177
IV-13-4	SNMP	182

Safety and Regulatory

Audience

This guide is for the networking professional managing the standalone PG28CB switch series. It is recommended that only professionals with experience working with Intelligent Technology INC. networking devices who are familiar with the Ethernet and local area networking terminology, should service the equipment.

Conventions

The following conventions are used in this manual to convey instructions and information:

Command descriptions use these conventions:

- Commands and keywords are in boldface text.
- Arguments for which you supply values are in italic.
- Square brackets ([]) mean optional elements.
- Braces ({ }) group required choices, and vertical bars (|) separate the alternative elements.
- Braces and vertical bars within square brackets ({ [|]}) mean a required choice within an optional element.

Interactive examples use these conventions:

- Nonprinting characters, such as passwords or tabs, are in angle brackets (< >). Notes and cautions use the following conventions and symbols:
 - Note
Means additional information. Notes contain additional useful information or references to material available outside of this document.
 - Caution
Indicates that the reader must be careful. In a situation where a Caution is listed, a user may cause equipment damage or loss of data.

I Introduction

Thank you for choosing a Edimax WEB Smart Ethernet Switch. This device is designed to be operational right out-of-the-box as a standard bridge. In the default configuration, it will forward packets between connecting devices after powered up.

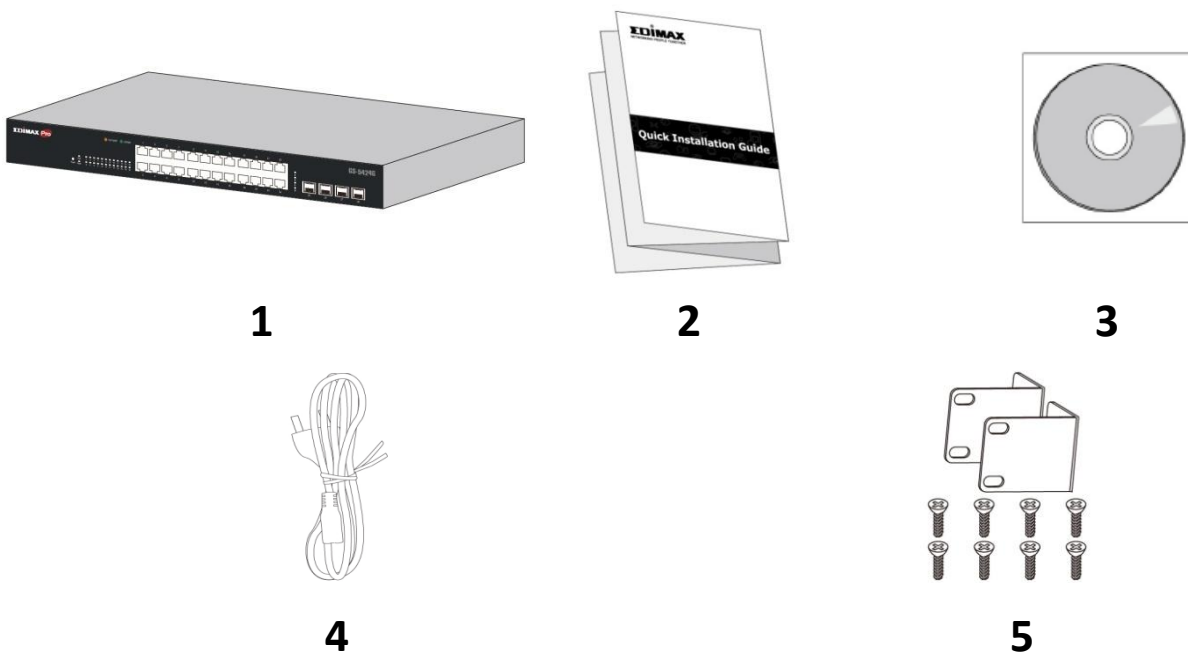
Before you begin installing the switch, make sure you have all of the package contents available, and a PC with a web browser for using web-based system management tools.

I-1 Overview

The Edimax GS-5424G is 24-Port Gigabit Smart Managed Switch with 4 SFP Ports.

I-2 Package Content

Before using the product, check that the items listed below are included and in good condition. If any item does not accord with the table, please contact your dealer immediately.



- 1.** GS-5424G Switch
- 2.** Quick Installation Guide
- 3.** CD
- 4.** Power Cord
- 5.** Rack-Mount Kit & Screws

I-3 Features

- Supports up to 24 10/100/1000Mbps Gigabit Ethernet ports and 4 mini-GBIC/SFP slots
- IEEE 802.1Q VLAN allows network segmentation to enhance performance and security
- Supports Access Control List (ACL)
- Switch capacity: PG28CB: 56Gbps, Forwarding rate: 41.6Mbps
- Supports IGMP Snooping V1 / V2 / V3
- 8K MAC address table and 10K jumbo frames
- 19-inch rack-mountable metal case

I-4 Product Components

I-4-1 Ports

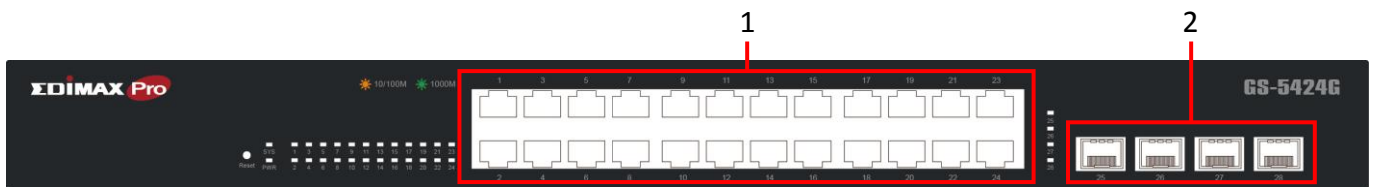


Figure 1 - Front View

No.	Name	Description
1	10/100/1000Mbps RJ-45 ports (1-24)	Designed to connect to network devices with a bandwidth of 10Mbps, 100Mbps or 1000Mbps. Each has a corresponding 10/100/1000Mbps LED.
2	SFP Ports	Designed to install SFP modules to connect to network devices with a bandwidth of 1000Mbps. Each has a corresponding 1000Mbps LED.



Figure 2 - Rear View

No.	Name	Description
1	AC power in	Support AC100 – 240V 50-60Hz.

I-4-2 LED Indicators

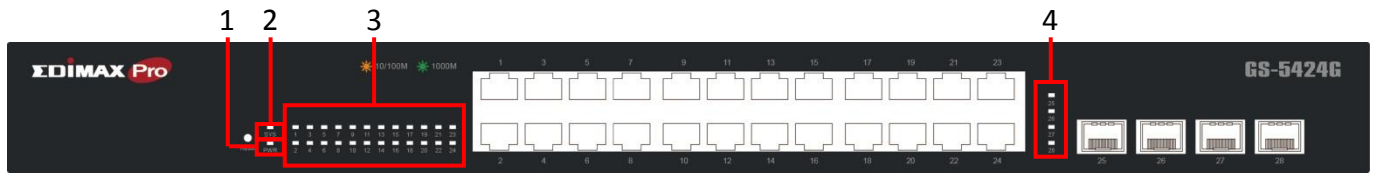


Figure 3 - Front View LED Indicators

No.	Name	Description
1	Power	<ul style="list-style-type: none"> ● Off: power off ● On: power on
2	System	<ul style="list-style-type: none"> ● Off: system not ready ● On: system ready ● Blinking: system boot-up
3	Port LED	<ul style="list-style-type: none"> ● Off: port disconnected or link fail ● Green on: 1000Mbps connected ● Amber on: 10/100Mbps connected ● Blinking: sending or receiving data
4	SFP LED	<ul style="list-style-type: none"> ● Off: port disconnected or link fail ● Green on: 1000Mbps connected

II Installation

This chapter describes how to install and connect your Edimax Switch. Read the following topics and perform the procedures in the correct order. Incorrect installation may cause damage to the product.

II-1 Mounting the Switch

There are two ways to physically set up the switch.

- Place the switch on a flat surface.
- Mount the switch in a standard rack (1 rack unit high).

II-1-1 Placement Tips

- Ambient Temperature — To prevent the switch from overheating, do not operate it in an area that exceeds an ambient temperature of 122°F (50°C).
- Air Flow — Be sure that there is adequate air flow around the switch.
- Mechanical Loading — Be sure that the switch is level and stable to avoid any hazardous conditions.
- Circuit Overloading — Adding the switch to the power outlet must not overload that circuit.

Follow these guidelines to install the switch securely.

- Put the switch in a stable place such as a desktop, to avoid it falling.
- Ensure the switch works in the proper AC input range and matches the voltage labeled.
- Ensure there is proper heat dissipation from and adequate ventilation around the switch.
- Ensure the switch's location can support the weight of the switch and its accessories.

II-1-2 Desktop Mounting

Please install the four rubber feet (included) on the bottom of the switch and place the switch at the desired location.

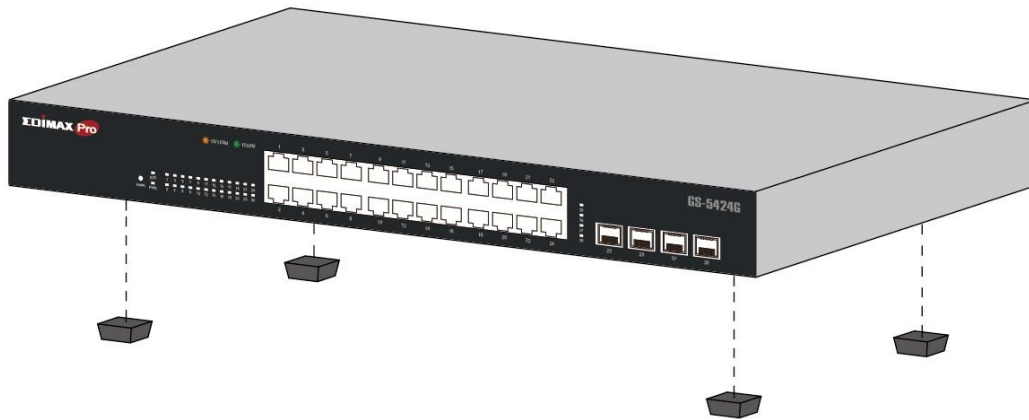


Figure 4 - Desktop Installation

II-1-3 Rack Mounting

You can mount the switch in any standard size, 19-inch (about 48 cm) wide rack. The switch requires 1 rack unit (RU) of space, which is 1.75 inches (44.45 mm) high.

For stability, load the rack from the bottom to the top, with the heaviest devices on the bottom. A top-heavy rack is likely to be unstable and may tip over.

When mounting smaller switch products into a standard 19-inch rack, a pair of extension brackets (sometimes referred to as ears) are needed to adapt the switch to the rack size.

These extension brackets are mounted on the switch using the screws provided in the kit, and have two holes that are used to then screw the switch into the rack.

An example of one type of these extension brackets is shown in the following figure.

A common problem that occurs during rack mounting is the distance between the screw holes on the rack. Some racks are made with a uniform distance between all of the holes, and others have the holes organized into groups (see photo on the next page for an example).

When organized into groups, the switch must be placed in the rack so that the holes in the extension brackets line up correctly.

1. Align the mounting brackets with the mounting holes on the switch's side panels and secure the brackets with the screws provided.

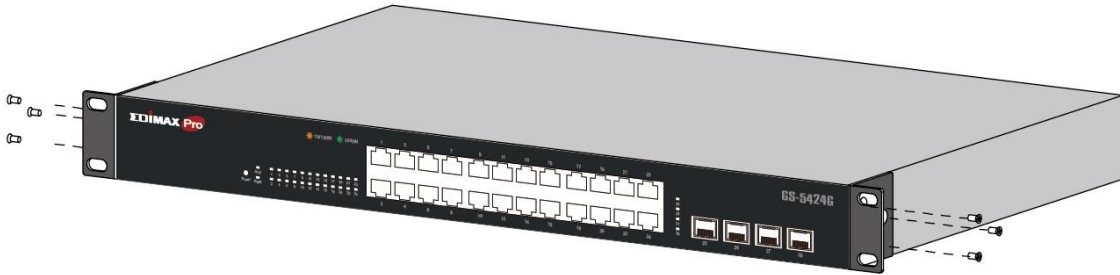


Figure 5 - Bracket Installation

2. Secure the switch on the equipment rack with the screws provided.

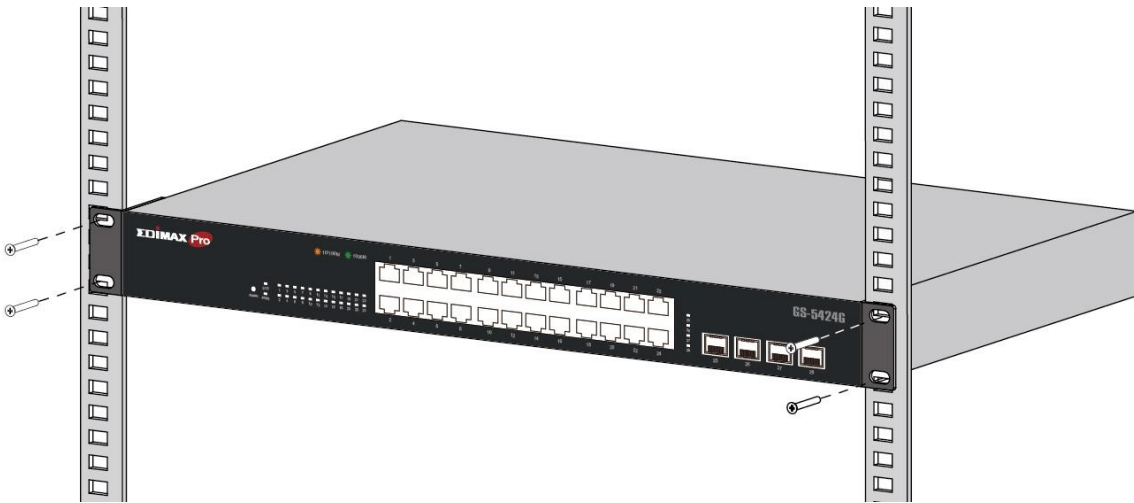


Figure 6 - Rack Installation

III Getting Started

This section provides an introduction to the web-based configuration utility, and covers the following topics:

- Powering on the device
- Connecting to the network
- Starting the web-based configuration utility

III-1 Connecting to Power

Power down and disconnect the power cord before servicing or wiring a switch.

Do not disconnect modules or cabling unless the power is first switched off. The device only supports the voltage outlined in the type plate. Do not use any other power components except those specifically designated for the switch.

Disconnect the power cord before installation or cable wiring.

The switch is powered by the AC 100-240 V 50/60Hz internal high-performance power supply. It is recommended to connect the switch with a single-phase three-wire power source with a neutral outlet, or a multifunctional computer professional source. Connect the AC power connector on the back panel of the switch to the external power source with the included power cord, and check the power LED is on.

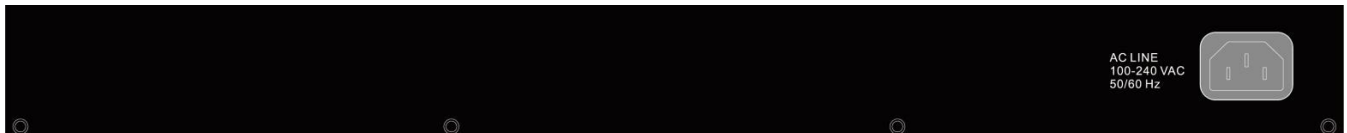


Figure 7 - Rear View AC Power Socket

III-2 Connecting to Network

To connect the switch to the network:

- 1.** Connect an Ethernet cable to the Ethernet port of a computer
- 2.** Connect the other end of the Ethernet cable to one of the numbered Ethernet ports of the switch. The LED of the port lights if the device connected is active.
- 3.** Repeat Step 1 and Step 2 for each device to connect to the switch.

We strongly recommend using CAT-5E or better cable to connect network devices. When connecting network devices, do not exceed the maximum cabling distance of 100 meters (328 feet). It can take up to one minute for attached devices or the LAN to be operational after it is connected. This is normal behavior.

Connect the switch to end nodes using a standard Cat 5/5e Ethernet cable (UTP/STP) to connect the switch to end nodes as shown in the illustration below.

Switch ports will automatically adjust to the characteristics (MDI/MDI-X, speed, duplex) of the device to which the switch is connected.

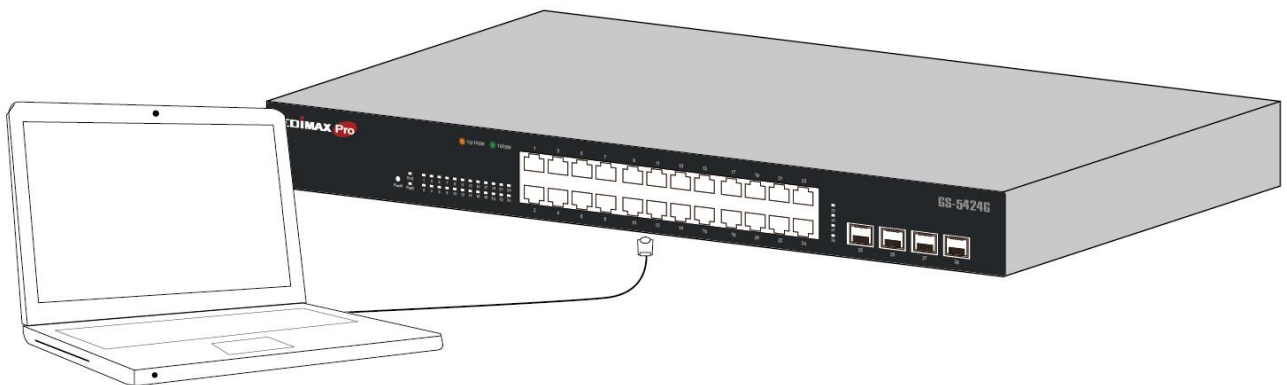


Figure 8 - PC Connect

III-3 Starting the Web-based Configuration Utility

This section describes how to navigate the web-based switch configuration utility. Be sure to disable any pop-up blocker.

Browser Restrictions

- If you are using older versions of Internet Explorer, you cannot directly use an IPv6 address to access the device. You can, however, use the DNS (Domain Name System) server to create a domain name that contains the IPv6 address, and then use that domain name in the address bar in place of the IPv6 address.
- If you have multiple IPv6 interfaces on your management station, use the IPv6 global address instead of the IPv6 link local address to access the device from your browser.

Launching the Configuration Utility

To open the web-based configuration utility:

1. Open a Web browser.
2. Enter the IP address of the device you are configuring in the address bar on the browser (factory default IP address is 192.168.2.1) and then press Enter.

When the device is using the factory default IP address, its power LED flashes continuously. When the device is using a DHCP assigned IP address or an administrator-configured static IP address, the power LED is lit a solid color. Your computer's IP address must be in the same subnet as the switch. For example, if the switch is using the factory default IP address, your computer's IP address can be in the following range: 192.168.2.x (whereas x is a number from 2 to 254).

After a successful connection, the login window displays.



EDIMAX Pro

Model Name GS-5424G

Username:

Password:

Language English ▾

LOGIN

Figure 9 - Login Window

please see the Launching the Configuration Utility section in the Administration Guide for additional information.

III-3-2 Logging Out

By default, the application logs out after ten minutes of inactivity.

To manually logout, click Logout in the top right corner of any page.

When a timeout occurs or you intentionally log out of the system, a message appears and the Login page appears, with a message indicating the logged-out state. After you log in, the application returns to the initial page.

IV Web-based Switch Configuration

The smart switch software provides rich Layer 2 functionality for switches in your networks. This chapter describes how to use the web-based management interface (Web UI) to configure the switch’s features.

For the purposes of this manual, the user interface is separated into four sections, as shown in the following figure:

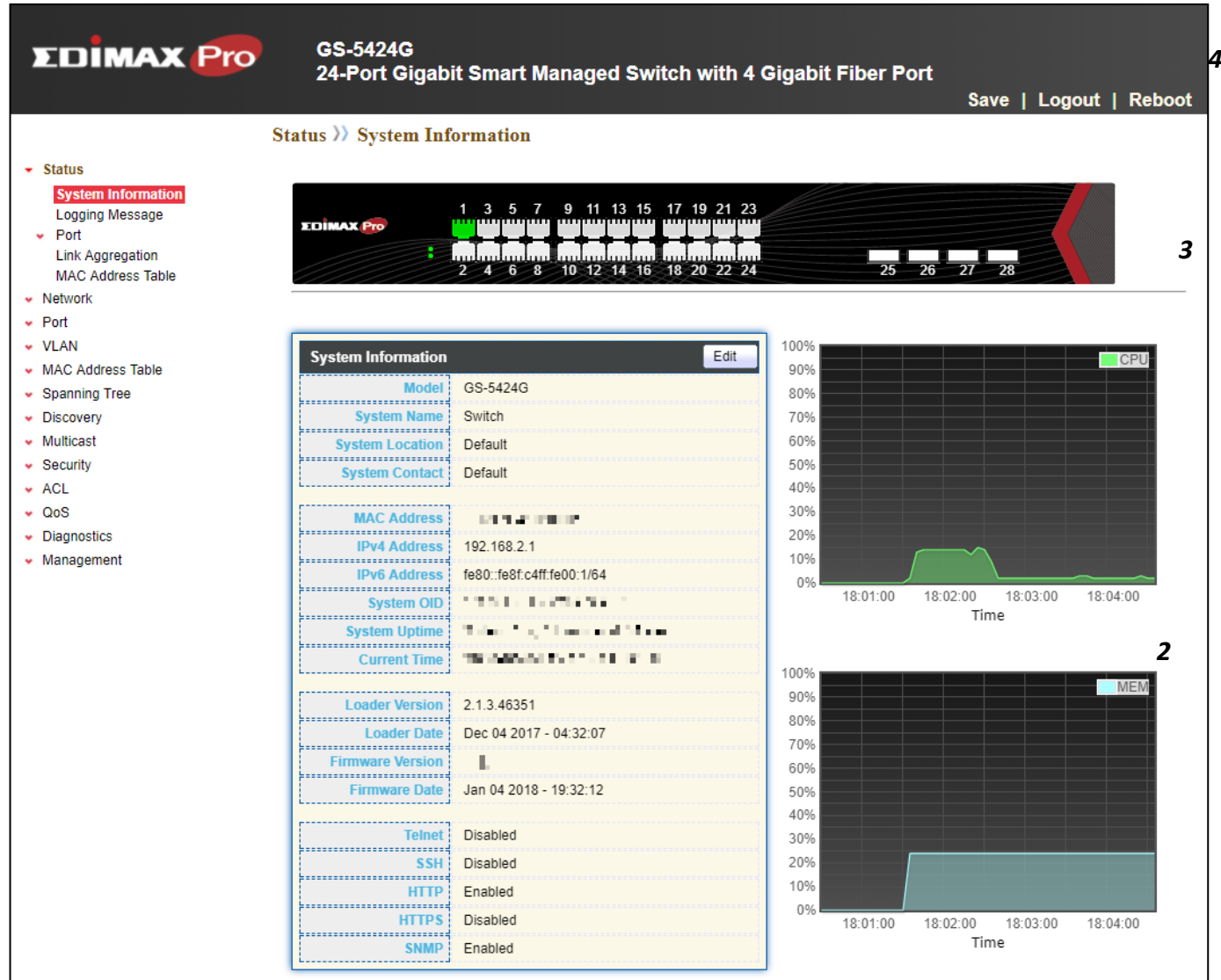


Figure 11 - User Interface

No.	Name	Description
1	Configuration menu	Navigate to locate specific switch functions.
2	Configuration settings	Edit specific function settings.
3	Switch’s current link status	Green squares indicate the port link is up, while black squares indicate the port link is down.
4	Common toolbar	Provides access to frequently used settings.

IV-1 Status

Use the Status pages to view system information and status.

IV-1-1 System Information

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

To display the Device Information web page, click **Status > System Information**.

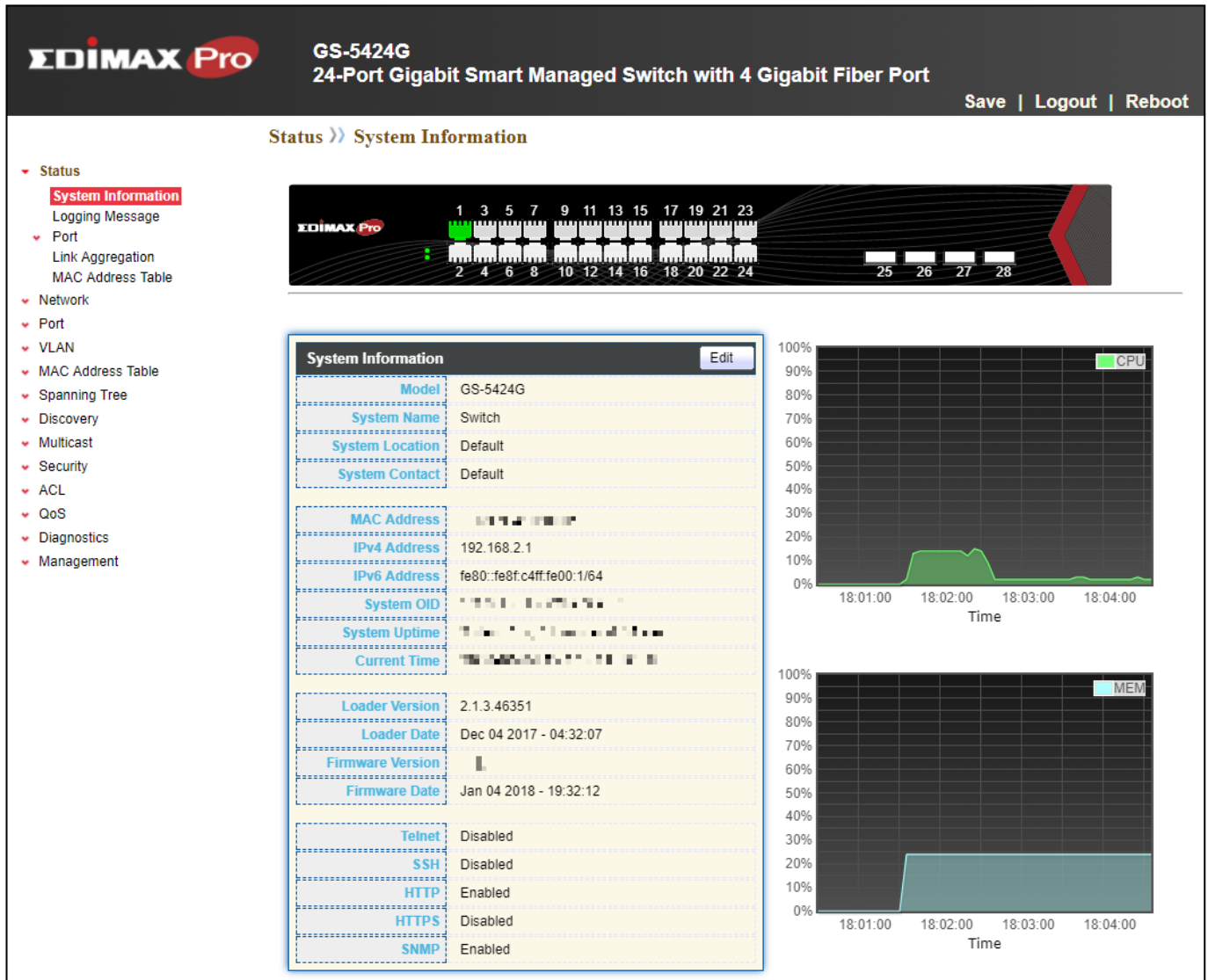


Figure 12 - Status > System Information

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

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

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

The screenshot shows a web-based dialog box titled "Edit System Information". The dialog contains three text input fields stacked vertically. The first field is labeled "System Name" and contains the text "Switch". The second field is labeled "System Location" and contains the text "Default". The third field is labeled "System Contact" and contains the text "Default". Below these fields are two buttons: "Apply" and "Close". The entire dialog is enclosed in a dashed blue border.

Figure 13 - Status > System Information > Edit System Information

Item	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.

IV-1-2 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 4 of 4 entries 🔍

Log ID	Time	Severity	Description
1	Jan 01 2000 00:01:19	notice	New http connection for user admin, source 192.168.2.22 ACCEPTED
2	Jan 01 2000 00:01:01	notice	GigabitEthernet28 link up
3	Jan 01 2000 00:00:58	notice	RESTART: System restarted - Cold Start
4	Jan 01 2000 00:00:58	notice	Logging is enabled

Clear Refresh First Previous **1** Next Last

Figure 14 - Status > Logging Message

Item	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.
Viewing	The logging view including: <ul style="list-style-type: none"> ● RAM: Show the logging messages stored on the RAM. ● Flash: Show the logging messages stored on the Flash.
Clear	Clear the logging messages.
Refresh	Refresh the logging messages.

IV-1-3 Port

IV-1-3-1 Statistics

This page displays standard counters on network traffic from the Interfaces, Ethernet-like and RMONMIB. 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.

To display the Port Flow Chart web page, click **Status > Port > Statistics**.

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

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 15 - Status > Port > Statistics

Item	Description
Port	Select one port to show counter statistics.
MIB Counter	Select the MIB counter to show different counter type <ul style="list-style-type: none"> ● All: All counters. ● Interface: Interface related MIB counters. ● Etherlike: Ethernet-like related MIB counters. ● RMON: RMON related MIB counters.
Refresh Rate	Refresh the web page every period of seconds to get new counter of specified port.

IV-1-3-2 Error Disabled

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

Error Disabled Table

<input type="checkbox"/>	Port	Reason	Time Left (sec)
<input type="checkbox"/>	GE1	---	---
<input type="checkbox"/>	GE2	---	---
<input type="checkbox"/>	GE3	---	---
<input type="checkbox"/>	GE4	---	---
<input type="checkbox"/>	GE5	---	---
<input type="checkbox"/>	GE6	---	---
<input type="checkbox"/>	GE7	---	---
<input type="checkbox"/>	GE8	---	---
<input type="checkbox"/>	GE9	---	---
<input type="checkbox"/>	GE10	---	---
<input type="checkbox"/>	GE11	---	---
<input type="checkbox"/>	GE12	---	---
<input type="checkbox"/>	GE13	---	---
<input type="checkbox"/>	GE14	---	---
<input type="checkbox"/>	GE15	---	---
<input type="checkbox"/>	GE16	---	---
<input type="checkbox"/>	GE17	---	---
<input type="checkbox"/>	GE18	---	---
<input type="checkbox"/>	GE19	---	---
<input type="checkbox"/>	GE20	---	---
<input type="checkbox"/>	GE21	---	---
<input type="checkbox"/>	GE22	---	---
<input type="checkbox"/>	GE23	---	---
<input type="checkbox"/>	GE24	---	---
<input type="checkbox"/>	GE25	---	---
<input type="checkbox"/>	GE26	---	---
<input type="checkbox"/>	GE27	---	---
<input type="checkbox"/>	GE28	---	---
<input type="checkbox"/>	LAG1	---	---
<input type="checkbox"/>	LAG2	---	---
<input type="checkbox"/>	LAG3	---	---

Figure 16 - Status > Port > Error Disabled

Item	Description
<input type="checkbox"/>	Select one or more port to operate.
Port	Interface or port number.
Reason	Port will be disabled by one of the following error reason: <ul style="list-style-type: none"> ● BPDU Guard ● UDLD ● Self Loop ● Broadcast Flood ● Unknown Multicast Flood ● Unicast Flood ● ACL

	<ul style="list-style-type: none"> ● Port Security Violation ● DHCP rate limit ● ARP rate limit
Time Left (sec)	The time left in second for the error recovery.
Refresh	Refresh the current page.
Recover	Recover the selected port status.

IV-1-3-3 Bandwidth Utilization

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

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

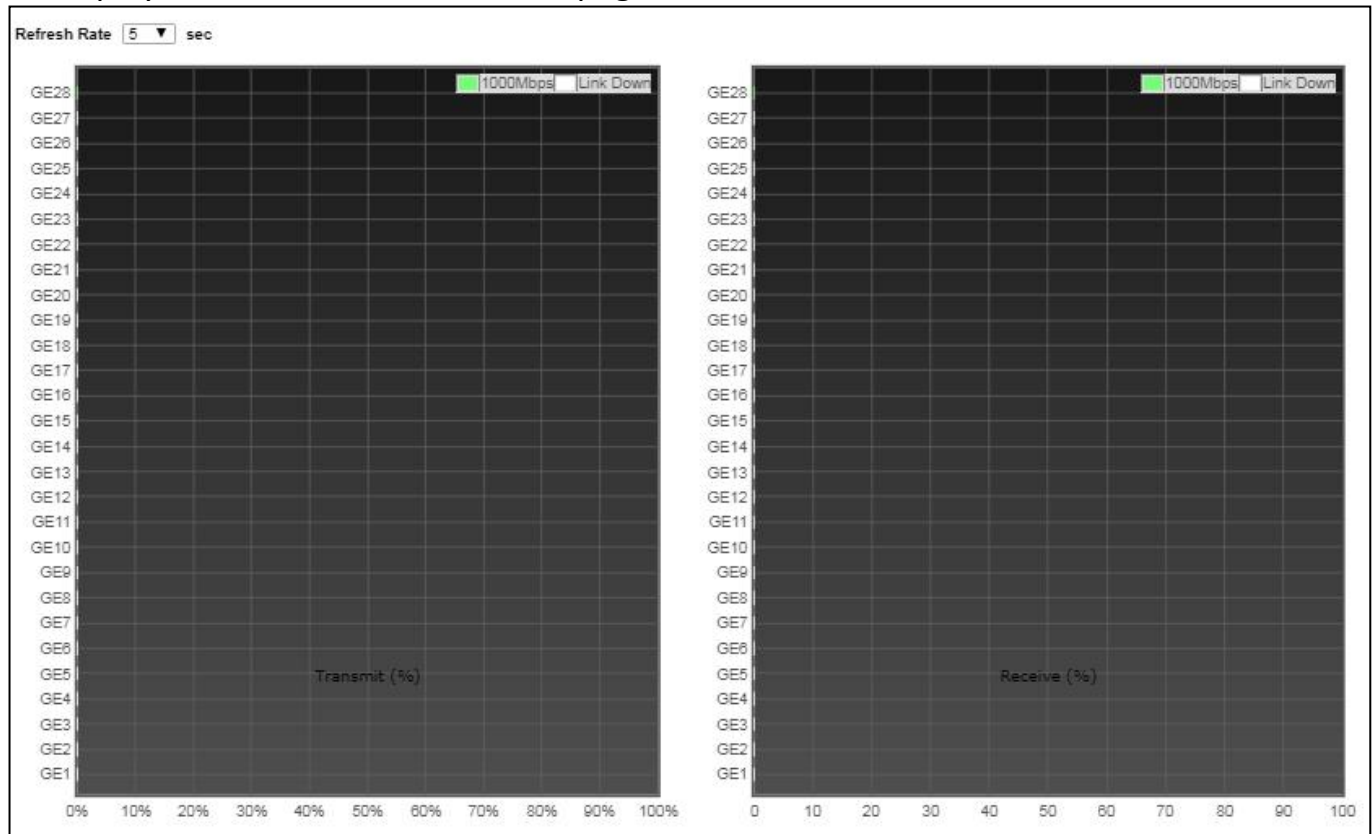


Figure 17 - Status > Port > Bandwidth Utilization

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

IV-1-4 Link Aggregation

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

Link Aggregation Table

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

Figure 18 - Status > Link Aggregation

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

IV-1-5 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.

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

VLAN	MAC Address	Type	Port
1	74:DA:38:17:6E:7A	Management	CPU
1	B8:6B:23:6D:C1:14	Dynamic	GE28

Figure 19 - Status > MAC Address Table

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

IV-2 Network

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

IV-2-1 IP Address

This section allows you to edit the IP address, Netmask, Gateway and DNS server of the switch.

To view the IP Address menu, navigate to **Network > IP Address**.

IPv4 Address	
Address Type	<input checked="" type="radio"/> Static <input type="radio"/> Dynamic
IP Address	192.168.2.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.2.254
DNS Server 1	168.95.1.1
DNS Server 2	168.95.192.1

IPv6 Address	
Auto Configuration	<input checked="" type="checkbox"/> Enable
DHCPv6 Client	<input type="checkbox"/> Enable
IPv6 Address	
Prefix Length	0 (0 - 128)
IPv6 Gateway	
DNS Server 1	
DNS Server 2	

Operational Status	
IPv4 Address	192.168.2.1
IPv4 Default Gateway	192.168.2.254
IPv6 Address	fe80::76da:38ff:fe17:6e7a/64
IPv6 Gateway	::
Link Local Address	fe80::76da:38ff:fe17:6e7a/64

Apply

Figure 20 - Network > IP Address

Item	Description
Address Type	The address type of switch IP configuration including <ul style="list-style-type: none"> ● Static: Static IP configured by users will be used. ● Dynamic: Enable the DHCP to obtain the IP address from a DHCP server.
IP Address	Specify the switch static IP address on the static configuration.
Subnet Mask	Specify the switch subnet mask on the static configuration.
Default Gateway	Specify the default gateway on the static configuration. The

	default gateway must be in the same subnet with switch IP address configuration.
DNS Server 1	Specify the primary user-defined IPv4 DNS server configuration.
DNS Server 2	Specify the secondary user-defined IPv4 DNS server configuration.
Table 3-2: IPv6 Address fields	
IPv4 Address	The operational IPv4 address of the switch.
IPv4 Gateway	The operational IPv4 gateway of the switch.
IPv6 Address v6	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.

IV-2-2 System Time

This page allows 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.

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

Source	<input type="radio"/> SNTP <input type="radio"/> From Computer <input checked="" type="radio"/> Manual Time
Time Zone	UTC +8:00 ▼
SNTP	
Address Type	<input checked="" type="radio"/> Hostname <input type="radio"/> IPv4
Server Address	<input type="text"/>
Server Port	123 (1 - 65535, default 123)
Manual Time	
Date	2000-01-01 YYYY-MM-DD
Time	00:15:47 HH:MM:SS
Daylight Saving Time	
Type	<input checked="" type="radio"/> None <input type="radio"/> Recurring <input type="radio"/> Non-recurring <input type="radio"/> USA <input type="radio"/> European
Offset	60 Min (1 - 1440, default 60)
Recurring	From: Day Sun ▼ Week First ▼ Month Jan ▼ Time <input type="text"/> To: Day Sun ▼ Week First ▼ Month Jan ▼ Time <input type="text"/>
Non-recurring	From: <input type="text"/> YYYY-MM-DD <input type="text"/> HH:MM To: <input type="text"/> YYYY-MM-DD <input type="text"/> HH:MM
Operational Status	
Current Time	2000-01-01 00:15:47 UTC+8
<input type="button" value="Apply"/>	

Figure 21 - Network > System Time

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

IV-3 Port

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

IV-3-1 Port Setting

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

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

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	Down	Auto	Auto	Disabled
<input type="checkbox"/>	9	GE9	1000M Copper		Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	10	GE10	1000M Copper		Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	11	GE11	1000M Copper		Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	12	GE12	1000M Copper		Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	13	GE13	1000M Copper		Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	14	GE14	1000M Copper		Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	15	GE15	1000M Copper		Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	16	GE16	1000M Copper		Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	17	GE17	1000M Copper		Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	18	GE18	1000M Copper		Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	19	GE19	1000M Copper		Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	20	GE20	1000M Copper		Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	21	GE21	1000M Copper		Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	22	GE22	1000M Copper		Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	23	GE23	1000M Copper		Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	24	GE24	1000M Copper		Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	25	GE25	1000M Combo Copper		Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	26	GE26	1000M Combo Copper		Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	27	GE27	1000M Combo Copper		Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	28	GE28	1000M Combo Copper		Enabled	Up	Auto (1000M)	Auto (Full)	Disabled (Disabled)

Figure 22 - Port > Port Setting

Item	Description
Port	Port Name.
Type	Port media type.
Description	Port Description.

State	Port admin state <ul style="list-style-type: none"> ● Enabled: Enable the port. ● Disabled: Disable the port.
Link Status	Current port link status <ul style="list-style-type: none"> ● Up: Port is link up. ● Down: Port is link down.
Speed	Current port speed configuration and link speed status.
Duplex	Current port duplex configuration and link duplex status.
Flow Control	Current port flow control configuration and link flow control status.

Click **“Edit”** button to edit Port Setting menu

Edit Port Setting

Port GE1

Description

State Enable

Speed

Auto 10M
 Auto - 10M 100M
 Auto - 100M 1000M
 Auto - 1000M
 Auto - 10M/100M

Duplex

Auto
 Full
 Half

Flow Control

Auto
 Enable
 Disable

Figure 23 - Port > Port Setting > Port Setting

Item	Description
Port	Selected Port list.
Description	Port media type.
State	Port admin state. <ul style="list-style-type: none"> ● Enabled: Enable the port. ● Disabled: Disable the port.
Speed	Port speed capabilities. <ul style="list-style-type: none"> ● Auto: Auto speed with all capabilities. ● Auto-10M: Auto speed with 10M ability only.

	<ul style="list-style-type: none"> ● Auto-100M: Auto speed with 100M ability only. ● Auto-1000M: Auto speed with 1000M ability only. ● Auto-10M/100M: Auto speed with 10M/100M abilities. ● 10M: Force speed with 10M ability. ● 100M: Force speed with 100M ability. ● 1000M: Force speed with 1000M ability.
Duplex	Port duplex capabilities. <ul style="list-style-type: none"> ● Auto: Auto duplex with all capabilities. ● Half: Auto speed with 10M and 100M ability only. ● Full: Auto speed with 10M/100M/1000M ability only.
Flow Control	Port flow control. <ul style="list-style-type: none"> ● Auto: Auto flow control by negotiation. ● Enabled: Enable flow control ability. ● Disabled: Disable flow control ability.

IV-3-2 Long Range Mode

This page shows port current status and Enable long range mode will double the cabling distance but reduce the speed to 10Mbps.

To display Long Range Mode web page, click **Port > Long Range Mode Setting**.

Long Range Mode Table

Enable long range mode will double the cabling distance but reduce the speed to 10Mbps.

Port	State
GE1	Disable ▼
GE2	Disable ▼
GE3	Disable ▼
GE4	Disable ▼
GE5	Disable ▼
GE6	Disable ▼
GE7	Disable ▼
GE8	Disable ▼
GE9	Disable ▼
GE10	Disable ▼
GE11	Disable ▼
GE12	Disable ▼
GE13	Disable ▼
GE14	Disable ▼
GE15	Disable ▼
GE16	Disable ▼
GE17	Disable ▼
GE18	Disable ▼
GE19	Disable ▼
GE20	Disable ▼
GE21	Disable ▼
GE22	Disable ▼
GE23	Disable ▼
GE24	Disable ▼
GE25	Disable ▼
GE26	Disable ▼
GE27	Disable ▼
GE28	Disable ▼

Apply

Figure 24 - Port > Long Range Mode

IV-3-3 Error Disable

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

The screenshot shows a web interface for configuring error disable settings. At the top, there is a 'Recovery Interval' field with the value '300' and a unit 'Sec (30 - 86400)'. Below this is a list of ten error disable reasons, each with an 'Enable' checkbox. The reasons are: BPDU Guard, UDLD, Self Loop, Broadcast Flood, Unknown Multicast Flood, Unicast Flood, ACL, Port Security, DHCP Rate Limit, and ARP Rate Limit. All checkboxes are currently unchecked. An 'Apply' button is located at the bottom left of the configuration area.

Figure 25 - Port > Error disable

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

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

IV-3-4 Link Aggregation

IV-3-4-1 Group

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

To view the Group menu, navigate to **Port > Link Aggregation > Group**.

Figure 26 - Port > Link Aggregation > Group

Item	Description
Load Balance Algorithm	LAG load balance distribution algorithm <ul style="list-style-type: none"> ● src-dst-mac: Based on MAC address. ● src-dst-mac-ip: Based on MAC address and IP address.
LAG	LAG Name.
Name	LAG port description.
Type	The type of the LAG <ul style="list-style-type: none"> ● Static: The group of ports assigned to a static LAG are always active members. ● LACP: The group of ports assigned to dynamic LAG are candidate ports. LACP determines which candidate ports are active member ports.
Link Status	LAG port link status

Active Member	Active member ports of the LAG.
Inactive Member	Inactive member ports of the LAG.

Click **“Edit”** to edit Link Aggregation Group menu.

Figure 27 - Port > Link Aggregation > Group > Edit Link Aggregation Group

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

IV-3-4-2 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.

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

Port Setting Table

<input type="checkbox"/>	LAG	Type	Description	State	Link Status	Speed	Duplex	Flow Control
<input type="checkbox"/>	LAG 1			Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	LAG 2			Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	LAG 3			Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	LAG 4			Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	LAG 5			Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	LAG 6			Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	LAG 7			Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	LAG 8			Enabled	Down	Auto	Auto	Disabled

Figure 28 - Port > Link Aggregation > Port Setting

Item	Description
LAG	LAG Port Name.
Type	LAG Port media type.
Description	LAG Port description.
State	LAG Port admin state <ul style="list-style-type: none"> ● Enabled: Enable the port. ● Disabled: Disable the port.
Link Status	Current LAG port link status <ul style="list-style-type: none"> ● Up: Port is link up. ● Down: Port is link down.
Speed	Current LAG port speed configuration and link speed status.
Duplex	Current LAG port duplex configuration and link duplex status.
Flow Control	Current LAG port flow control configuration and link flow control status.

Click **“Edit”** to view Edit Port Setting menu.

Figure 29 - Port > Link Aggregation > Port Setting > Edit Port Setting

Item	Description
Port	Selected Port list.
Description	Port description.
State	Port admin state <ul style="list-style-type: none"> ● Enabled: Enable the port. ● Disabled: Disable the port.
Speed	Port speed capabilities <ul style="list-style-type: none"> ● Auto: Auto speed with all capabilities. ● Auto-10M: Auto speed with 10M ability only. ● Auto-100M: Auto speed with 100M ability only. ● Auto-1000M: Auto speed with 1000M ability only. ● Auto-10M/100M: Auto speed with 10M/100M abilities. ● 10M: Force speed with 10M ability. ● 100M: Force speed with 100M ability. ● 1000M: Force speed with 1000M ability.
Flow Control	Port flow control <ul style="list-style-type: none"> ● Auto: Auto flow control by negotiation. ● Enabled: Enable flow control ability. ● Disabled: Disable flow control ability.

IV-3-4-3 LACP

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

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

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

Apply

LACP Port Setting Table

<input type="checkbox"/>	Entry	Port	Port Priority	Timeout
<input type="checkbox"/>	1	GE1	1	Long
<input type="checkbox"/>	2	GE2	1	Long
<input type="checkbox"/>	3	GE3	1	Long
<input type="checkbox"/>	4	GE4	1	Long
<input type="checkbox"/>	5	GE5	1	Long
<input type="checkbox"/>	6	GE6	1	Long
<input type="checkbox"/>	7	GE7	1	Long
<input type="checkbox"/>	8	GE8	1	Long
<input type="checkbox"/>	9	GE9	1	Long
<input type="checkbox"/>	10	GE10	1	Long
<input type="checkbox"/>	11	GE11	1	Long
<input type="checkbox"/>	12	GE12	1	Long
<input type="checkbox"/>	13	GE13	1	Long
<input type="checkbox"/>	14	GE14	1	Long
<input type="checkbox"/>	15	GE15	1	Long
<input type="checkbox"/>	16	GE16	1	Long
<input type="checkbox"/>	17	GE17	1	Long
<input type="checkbox"/>	18	GE18	1	Long
<input type="checkbox"/>	19	GE19	1	Long
<input type="checkbox"/>	20	GE20	1	Long
<input type="checkbox"/>	21	GE21	1	Long
<input type="checkbox"/>	22	GE22	1	Long
<input type="checkbox"/>	23	GE23	1	Long
<input type="checkbox"/>	24	GE24	1	Long
<input type="checkbox"/>	25	GE25	1	Long
<input type="checkbox"/>	26	GE26	1	Long
<input type="checkbox"/>	27	GE27	1	Long
<input type="checkbox"/>	28	GE28	1	Long

Edit

Figure 30 - Port > Link Aggregation > LACP

Item	Description
System Priority	Configure the system priority of LACP. This decides the system priority field in LACP PDU.
Port	Port Name.
Port Priority	LACP priority value of the port.
Timeout	The periodic transmissions type of LACP PDUs. <ul style="list-style-type: none"> ● Long: Transmit LACP PDU with slow periodic (30s). ● Short: Transmit LACPP DU with fast periodic (1s).

Click "**Edit**" button to view Edit LACP Port Setting menu.

Edit LACP Port Setting

Port: GE1

Port Priority: 1 (1 - 65535, default 1)

Timeout: Long Short

Apply Close

Figure 31 - Port > Link Aggregation > LACP > Edit LACP Port Setting

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

IV-3-5 EEE

This page allows user to configure Energy Efficient Ethernet settings.

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

EEE Setting Table

<input type="checkbox"/>	Entry	Port	State	Operational Status
<input type="checkbox"/>	1	GE1	Disabled	Disabled
<input type="checkbox"/>	2	GE2	Disabled	Disabled
<input type="checkbox"/>	3	GE3	Disabled	Disabled
<input type="checkbox"/>	4	GE4	Disabled	Disabled
<input type="checkbox"/>	5	GE5	Disabled	Disabled
<input type="checkbox"/>	6	GE6	Disabled	Disabled
<input type="checkbox"/>	7	GE7	Disabled	Disabled
<input type="checkbox"/>	8	GE8	Disabled	Disabled
<input type="checkbox"/>	9	GE9	Disabled	Disabled
<input type="checkbox"/>	10	GE10	Disabled	Disabled
<input type="checkbox"/>	11	GE11	Disabled	Disabled
<input type="checkbox"/>	12	GE12	Disabled	Disabled
<input type="checkbox"/>	13	GE13	Disabled	Disabled
<input type="checkbox"/>	14	GE14	Disabled	Disabled
<input type="checkbox"/>	15	GE15	Disabled	Disabled
<input type="checkbox"/>	16	GE16	Disabled	Disabled
<input type="checkbox"/>	17	GE17	Disabled	Disabled
<input type="checkbox"/>	18	GE18	Disabled	Disabled
<input type="checkbox"/>	19	GE19	Disabled	Disabled
<input type="checkbox"/>	20	GE20	Disabled	Disabled
<input type="checkbox"/>	21	GE21	Disabled	Disabled
<input type="checkbox"/>	22	GE22	Disabled	Disabled
<input type="checkbox"/>	23	GE23	Disabled	Disabled
<input type="checkbox"/>	24	GE24	Disabled	Disabled
<input type="checkbox"/>	25	GE25	Disabled	Disabled
<input type="checkbox"/>	26	GE26	Disabled	Disabled
<input type="checkbox"/>	27	GE27	Disabled	Disabled
<input type="checkbox"/>	28	GE28	Disabled	Disabled

Figure 32 - Port > EEE

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

Click **“Edit”** to edit the EEE menu.

Figure 33 - Port > EEE > Edit EEE Setting

Item	Description
Port	Port Name
State	Port EEE admin state <ul style="list-style-type: none"> ● Enabled: EEE is enabled. ● Disabled: EEE is disabled.

IV-3-6 Jumbo Frame

This page allows user to configure switch jumbo frame size.

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

Figure 34 - Port > Jumbo Frame

Item	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.

IV-4 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.

IV-4-1 VLAN

Use the VLAN pages to configure settings of VLAN.

IV-4-1-1 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.

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

The screenshot shows the 'Create VLAN' interface. On the left, under 'Available VLAN', there is a list of VLANs: VLAN 2, VLAN 3, VLAN 4, VLAN 5, VLAN 6, VLAN 7, VLAN 8, and VLAN 9. On the right, under 'Created VLAN', there is a list containing 'VLAN 1'. Between the two lists are right and left arrow buttons. Below the lists is an 'Apply' button. Underneath is a 'VLAN Table' with a search bar and a table containing one entry: '1' with name 'default' and type 'Default'. At the bottom of the table are 'Edit' and 'Delete' buttons, and a pagination control showing '1' of 1 entries.

Figure 35 - VLAN > VLAN > Create VLAN

Item	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
VLAN	The VLAN ID.
Name	The VLAN Name.
Type	The VLAN Type. <ul style="list-style-type: none"> ● Static: Port base VLAN. ● Dynamic: 802.1q VLAN.

Click “**Edit**” button to view Edit VLAN Name menu.

Figure 36 - VLAN > VLAN > Create VLAN > Edit VLAN Name

Item	Description
Name	Input VLAN name.

IV-4-1-2 VLAN Configuration

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

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

VLAN Configuration Table

VLAN

Entry	Port	Mode	Membership				PVID
1	GE1	Trunk	<input type="radio"/> Excluded	<input type="radio"/> Forbidden	<input type="radio"/> Tagged	<input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
2	GE2	Trunk	<input type="radio"/> Excluded	<input type="radio"/> Forbidden	<input type="radio"/> Tagged	<input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
3	GE3	Trunk	<input type="radio"/> Excluded	<input type="radio"/> Forbidden	<input type="radio"/> Tagged	<input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
4	GE4	Trunk	<input type="radio"/> Excluded	<input type="radio"/> Forbidden	<input type="radio"/> Tagged	<input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
5	GE5	Trunk	<input type="radio"/> Excluded	<input type="radio"/> Forbidden	<input type="radio"/> Tagged	<input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
6	GE6	Trunk	<input type="radio"/> Excluded	<input type="radio"/> Forbidden	<input type="radio"/> Tagged	<input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
7	GE7	Trunk	<input type="radio"/> Excluded	<input type="radio"/> Forbidden	<input type="radio"/> Tagged	<input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
8	GE8	Trunk	<input type="radio"/> Excluded	<input type="radio"/> Forbidden	<input type="radio"/> Tagged	<input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
9	GE9	Trunk	<input type="radio"/> Excluded	<input type="radio"/> Forbidden	<input type="radio"/> Tagged	<input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
10	GE10	Trunk	<input type="radio"/> Excluded	<input type="radio"/> Forbidden	<input type="radio"/> Tagged	<input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
11	GE11	Trunk	<input type="radio"/> Excluded	<input type="radio"/> Forbidden	<input type="radio"/> Tagged	<input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
12	GE12	Trunk	<input type="radio"/> Excluded	<input type="radio"/> Forbidden	<input type="radio"/> Tagged	<input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
13	GE13	Trunk	<input type="radio"/> Excluded	<input type="radio"/> Forbidden	<input type="radio"/> Tagged	<input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
14	GE14	Trunk	<input type="radio"/> Excluded	<input type="radio"/> Forbidden	<input type="radio"/> Tagged	<input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
15	GE15	Trunk	<input type="radio"/> Excluded	<input type="radio"/> Forbidden	<input type="radio"/> Tagged	<input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
16	GE16	Trunk	<input type="radio"/> Excluded	<input type="radio"/> Forbidden	<input type="radio"/> Tagged	<input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
17	GE17	Trunk	<input type="radio"/> Excluded	<input type="radio"/> Forbidden	<input type="radio"/> Tagged	<input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
18	GE18	Trunk	<input type="radio"/> Excluded	<input type="radio"/> Forbidden	<input type="radio"/> Tagged	<input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
19	GE19	Trunk	<input type="radio"/> Excluded	<input type="radio"/> Forbidden	<input type="radio"/> Tagged	<input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
20	GE20	Trunk	<input type="radio"/> Excluded	<input type="radio"/> Forbidden	<input type="radio"/> Tagged	<input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
21	GE21	Trunk	<input type="radio"/> Excluded	<input type="radio"/> Forbidden	<input type="radio"/> Tagged	<input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
22	GE22	Trunk	<input type="radio"/> Excluded	<input type="radio"/> Forbidden	<input type="radio"/> Tagged	<input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
23	GE23	Trunk	<input type="radio"/> Excluded	<input type="radio"/> Forbidden	<input type="radio"/> Tagged	<input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
24	GE24	Trunk	<input type="radio"/> Excluded	<input type="radio"/> Forbidden	<input type="radio"/> Tagged	<input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
25	GE25	Trunk	<input type="radio"/> Excluded	<input type="radio"/> Forbidden	<input type="radio"/> Tagged	<input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
26	GE26	Trunk	<input type="radio"/> Excluded	<input type="radio"/> Forbidden	<input type="radio"/> Tagged	<input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
27	GE27	Trunk	<input type="radio"/> Excluded	<input type="radio"/> Forbidden	<input type="radio"/> Tagged	<input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
28	GE28	Trunk	<input type="radio"/> Excluded	<input type="radio"/> Forbidden	<input type="radio"/> Tagged	<input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
29	LAG1	Trunk	<input type="radio"/> Excluded	<input type="radio"/> Forbidden	<input type="radio"/> Tagged	<input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>

Figure 37 - VLAN > VLAN > VLAN Configuration

Item	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. <input checked="" type="radio"/> Forbidden: Specify the port is forbidden in the VLAN.

	<ul style="list-style-type: none"> ● Excluded: Specify the port is excluded in the VLAN. ● Tagged: Specify the port is tagged member in the VLAN. ● Untagged: Specify the port is untagged member in the VLAN.
PVID	Display if it is PVID of interface.

IV-4-1-3 Membership

This page allows user to view membership information for each port and edit membership for specified interface.

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

Membership Table

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	GE11	Trunk	1UP	1UP
<input type="radio"/> 12	GE12	Trunk	1UP	1UP
<input type="radio"/> 13	GE13	Trunk	1UP	1UP
<input type="radio"/> 14	GE14	Trunk	1UP	1UP
<input type="radio"/> 15	GE15	Trunk	1UP	1UP
<input type="radio"/> 16	GE16	Trunk	1UP	1UP
<input type="radio"/> 17	GE17	Trunk	1UP	1UP
<input type="radio"/> 18	GE18	Trunk	1UP	1UP
<input type="radio"/> 19	GE19	Trunk	1UP	1UP
<input type="radio"/> 20	GE20	Trunk	1UP	1UP
<input type="radio"/> 21	GE21	Trunk	1UP	1UP
<input type="radio"/> 22	GE22	Trunk	1UP	1UP
<input type="radio"/> 23	GE23	Trunk	1UP	1UP
<input type="radio"/> 24	GE24	Trunk	1UP	1UP
<input type="radio"/> 25	GE25	Trunk	1UP	1UP
<input type="radio"/> 26	GE26	Trunk	1UP	1UP
<input type="radio"/> 27	GE27	Trunk	1UP	1UP
<input type="radio"/> 28	GE28	Trunk	1UP	1UP
<input type="radio"/> 29	LAG1	Trunk	1UP	1UP
<input type="radio"/> 30	LAG2	Trunk	1UP	1UP

Figure 38 - VLAN > VLAN > Membership

Item	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.

Click "**Edit**" button to view the Edit Port Setting menu

Figure 39 - VLAN > VLAN > Membership > Edit Port Setting

Item	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. Select the time source.</p> <ul style="list-style-type: none"> ● Forbidden: Set VLAN as forbidden VLAN. ● Excluded: This option is always disabled. ● Tagged: Set VLAN as tagged VLAN. ● Untagged: Set VLAN as untagged VLAN. ● PVID: Check this checkbox to select the VLAN ID to be the port-based

	VLAN ID for this port. PVID may auto select or can't select in differ settings.
--	---

IV-4-1-4 Port Setting

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

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

Port Setting Table

Q

<input type="checkbox"/>	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 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	GE11	Trunk	1	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	12	GE12	Trunk	1	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	13	GE13	Trunk	1	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	14	GE14	Trunk	1	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	15	GE15	Trunk	1	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	16	GE16	Trunk	1	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	17	GE17	Trunk	1	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	18	GE18	Trunk	1	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	19	GE19	Trunk	1	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	20	GE20	Trunk	1	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	21	GE21	Trunk	1	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	22	GE22	Trunk	1	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	23	GE23	Trunk	1	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	24	GE24	Trunk	1	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	25	GE25	Trunk	1	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	26	GE26	Trunk	1	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	27	GE27	Trunk	1	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	28	GE28	Trunk	1	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	29	LAG1	Trunk	1	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	30	LAG2	Trunk	1	All	Enabled	Disabled	0x8100

Figure 40 - VLAN > VLAN > Port Setting

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

Click “Edit” button to Edit Port Setting menu.

Figure 41 - VLAN > VLAN > Port Setting > Edit Port Setting

Item	Description
Port	Display selected port to be edited.
Mode	Select the VLAN mode of the interface. <ul style="list-style-type: none"> ● Forbidden: Set VLAN as forbidden VLAN. ● Hybrid: Support all functions as defined in IEEE 802.1Q specification. ● Access: Accepts only untagged frames and join an untagged VLAN. ● Trunk: An untagged member of one VLAN at most, and is a tagged member of zero or more VLANs.
PVID	Specify the port-based VLAN ID (1-4094). It's only available with Hybrid and Trunk mode.
Accepted Type	Specify the acceptable-frame-type of the specified interfaces. It's only available with Hybrid mode.
Ingress	Set checkbox to enable/disable ingress filtering. It's only available with

Filtering	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.

IV-4-2 Voice VLAN

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

IV-4-2-1 Property

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

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

The screenshot displays the configuration interface for Voice VLAN properties. It includes a configuration panel with the following settings:

- State:** Enable
- VLAN:** None (dropdown menu)
- CoS / 802.1p Remarking:** Enable, 6 (dropdown menu)
- Aging Time:** 1440 (text input), Sec (30 - 65536, default 1440)

An **Apply** button is located below the configuration panel.

Port Setting Table

Search:

Entry	Port	State	Mode	QoS Policy	
<input type="checkbox"/>	1	GE1	Disabled	Auto	Voice Packet
<input type="checkbox"/>	2	GE2	Disabled	Auto	Voice Packet
<input type="checkbox"/>	3	GE3	Disabled	Auto	Voice Packet
<input type="checkbox"/>	4	GE4	Disabled	Auto	Voice Packet
<input type="checkbox"/>	5	GE5	Disabled	Auto	Voice Packet
<input type="checkbox"/>	6	GE6	Disabled	Auto	Voice Packet
<input type="checkbox"/>	7	GE7	Disabled	Auto	Voice Packet
<input type="checkbox"/>	8	GE8	Disabled	Auto	Voice Packet
<input type="checkbox"/>	9	GE9	Disabled	Auto	Voice Packet
<input type="checkbox"/>	10	GE10	Disabled	Auto	Voice Packet
<input type="checkbox"/>	11	GE11	Disabled	Auto	Voice Packet
<input type="checkbox"/>	12	GE12	Disabled	Auto	Voice Packet
<input type="checkbox"/>	13	GE13	Disabled	Auto	Voice Packet
<input type="checkbox"/>	14	GE14	Disabled	Auto	Voice Packet
<input type="checkbox"/>	15	GE15	Disabled	Auto	Voice Packet
<input type="checkbox"/>	16	GE16	Disabled	Auto	Voice Packet
<input type="checkbox"/>	17	GE17	Disabled	Auto	Voice Packet
<input type="checkbox"/>	18	GE18	Disabled	Auto	Voice Packet
<input type="checkbox"/>	19	GE19	Disabled	Auto	Voice Packet
<input type="checkbox"/>	20	GE20	Disabled	Auto	Voice Packet

Figure 42 - VLAN > Voice VLAN > Property

Item	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.
Port Setting Table	
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.

Click “**Edit**” button to view Edit Port Setting menu.

Figure 43 - VLAN > Voice VLAN > Property > Edit Port Setting

Item	Description
Port	Display selected port to be edited.
State	Set checkbox to enable/disabled voice VLAN function of interface.
Mode	Select port voice VLAN mode <ul style="list-style-type: none"> ● Auto: Voice VLAN auto detect packets that match OUI table and add received port into voice VLAN ID tagged member. ● Manual: User need add interface to VLAN ID tagged member manually.
QoS Policy	Select port QoS Policy mode <ul style="list-style-type: none"> ● Voice Packet: QoS attributes are applied to packets with OUIs in the source MAC address. ● All: QoS attributes are applied to packets that are classified to Voice VLAN.

IV-4-2-2 Voice OUI

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

To display the Voice OUI Web page, click **VLAN > Voice VLAN > Voice OUI**.

Voice OUI Table

Showing entries Showing 1 to 8 of 8 entries

<input type="checkbox"/>	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

Figure 44 - VLAN > Voice VLAN > Voice OUI

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

Click “Add” or “Edit” button to Add/Edit Voice OUI menu.

Add Voice OUI

OUI: : :

Description:

Edit Voice OUI

OUI: 00:03:6B

Description:

Figure 45 - VLAN > Voice VLAN > Voice OUI > Add/Edit Voice OUI

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

IV-4-3 MAC VLAN

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

IV-4-3-1 MAC Group

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

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

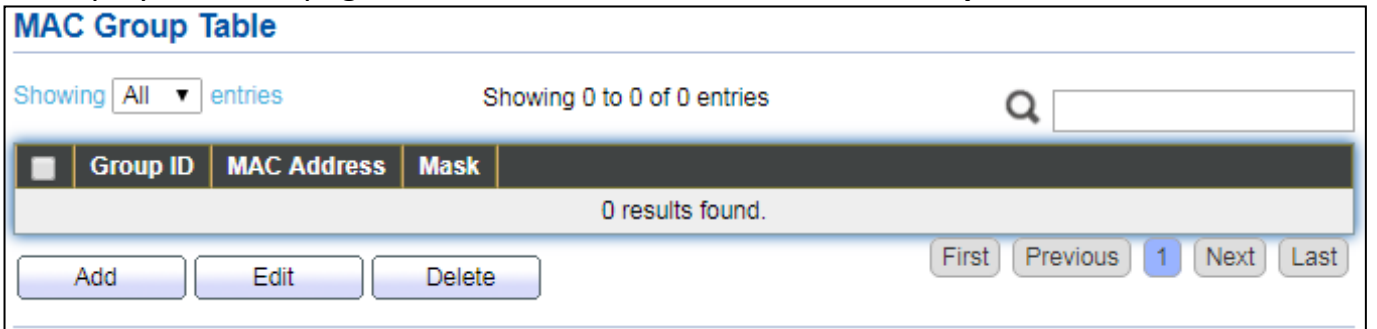


Figure 46 - VLAN > MAC VLAN > MAC Group

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

Click **“Add”** button or **“Edit”** button to view Add/Edit MAC menu.

Add MAC Group

Group ID

MAC Address

Mask

Edit MAC Group

Group ID

MAC Address

Mask

Figure 47 - VLAN > MAC VLAN > MAC Group > Add/Edit MAC

Item	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.

IV-4-3-2 Group Binding

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

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

Group Binding Table

Showing All entries
Showing 0 to 0 of 0 entries

Port	Group ID	VLAN
0 results found.		

1

Figure 48 - VLAN > MAC VLAN > Group Binding

Item	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.

Click “Add” or “Edit” button to view the Add/Edit Group Binding menu.

Add Group Binding

Port

Available Port

Selected Port

➤

➤

➤

Note: Only VLAN Hybrid port can be set MAC VLAN

Group ID

None ▼

VLAN

(1 - 4094)

Apply

Close

Edit Group Binding

Port

Group ID

VLAN

(1 - 4094)

Apply

Close

Figure 49 - VLAN > MAC VLAN > Add/Edit Group Binding

Item	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.

IV-5 MAC Address Table

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

IV-5-1 Dynamic Address

To display the Dynamic Address web page, click **MAC Address Table > Dynamic Address**.

Aging Time Sec (10 - 630, default 300)

Apply

Dynamic Address Table

Showing entries Showing 1 to 1 of 1 entries

<input type="checkbox"/>	VLAN	MAC Address	Port
<input type="checkbox"/>	1	B8:6B:23:6D:C1:14	GE28

First Previous 1 Next Last

Clear Refresh Add Static Address

Figure 50 - MAC Address Table > Dynamic Address

Item	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.

IV-5-2 Static Address

To display the Static Address web page, click **MAC Address Table > Static Address**.

Static Address Table

Showing entries Showing 0 to 0 of 0 entries

<input type="checkbox"/>	VLAN	MAC Address	Port
0 results found.			

First Previous 1 Next Last

Add Edit Delete

Figure 51 - MAC Address Table > Static Address

Item	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.

IV-5-3 Filtering Address

To display the Filtering Address web page, click **MAC Address Table > Filtering Address**.

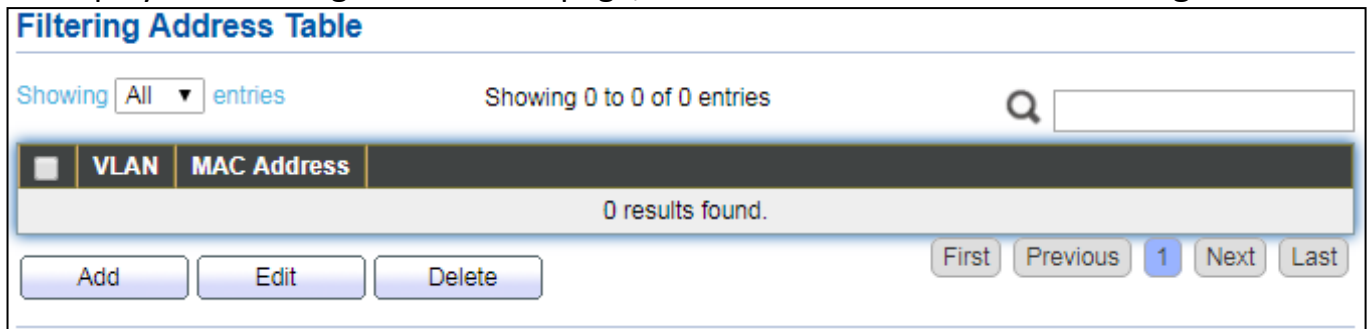


Figure 52 - MAC Address Table > Filtering Address

Item	Description
MAC Address	Specify unicast MAC address in the packets to be dropped.
VLAN	Specify the VLAN to show or clear MAC entries.

IV-6 Spanning Tree

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

IV-6-1 Property

To display the Property web page, click **Spanning Tree > Property**.

State	<input 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	<input type="text" value="32768"/> (0 - 61440, default 32768)
Hello Time	<input type="text" value="2"/> Sec (1 - 10, default 2)
Max Age	<input type="text" value="20"/> Sec (6 - 40, default 20)
Forward Delay	<input type="text" value="15"/> Sec (4 - 30, default 15)
Tx Hold Count	<input type="text" value="6"/> (1 - 10, default 6)
Region Name	<input type="text" value="74:DA:38:17:6E:7A"/>
Revision	<input type="text" value="0"/> (0 - 65535, default 0)
Max Hop	<input type="text" value="20"/> (1 - 40, default 20)
Operational Status	
Bridge Identifier	32768-74:DA:38:17:6E:7A
Designated Root Bridge	0-00:00:00:00:00:00
Root Port	N/A
Root Path Cost	0
Topology Change Count	0
Last Topology Change	0D/0H/0M/0S

Figure 53 - Spanning Tree > Property

Item	Description
State	Enable/disable the STP on the switch.
Operation Mode	Specify the STP operation mode. <ul style="list-style-type: none"> ● STP: Enable the Spanning Tree (STP) operation. ● RSTP: Enable the Rapid Spanning Tree (RSTP) operation. ● MSTP: Enable the Multiple Spanning Tree (MSTP) operation.
Path Cost	Specify the path cost method. <ul style="list-style-type: none"> ● Long: Specifies that the default port path costs are within the range: 1-200,000,000. ● Short: Specifies that the default port path costs are within the range: 1-65,535.
BPDU Handling	Specify the BPDU forward method when the STP is disabled. <ul style="list-style-type: none"> ● Filtering: Filter the BPDU when STP is disabled. ● Flooding: Flood the BPDU when STP is disabled.
Priority	Specify the bridge priority. The valid range is from 0 to 61440, and the value should be the multiple of 4096. It ensures the probability that the switch is selected as the root bridge, and the lower value has the higher priority for the switch to be selected as the root bridge of the topology.
Hello Time	Specify the STP hello time in second to broadcast its hello message to other bridges by Designated Ports. Its valid range is from 1 to 10 seconds.
Max Age	Specify the time interval in seconds for a switch to wait the configuration messages, without attempting to redefine its own configuration.
Forward Delay	Specify the STP forward delay time, which is the amount of time that a port remains in the Listening and Learning states before it enters the Forwarding state. Its valid range is from 4 to 10 seconds.
TX Hold Count	Specify the tx-hold-count used to limit the maximum numbers of packets transmission per second. The valid range is from 1 to 10.
Region Name	The MSTP instance name. Its maximum length is 32 characters. The default value is the MAC address of the switch.
Revision	The MSTP revision number. Its valid range is from 0 to 65535.
Max Hop	Specify the number of hops in an MSTP region before the BPDU is discarded. The valid range is 1 to 40.
Operational Status	
Bridge Identifier	Bridge identifier of the switch.
Designated Root Identifier	Bridge identifier of the designated root bridge.
Root Port	Operational root port of the switch.
Root Path Cost	Operational root path cost.
Topology Change Count	Numbers of the topology changes.

Last Topology Change	The last time for the topology change.
----------------------	--

IV-6-2 Port Setting

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

Port Setting Table

Entry	Port	State	Path Cost	Priority	BPDU Filter	BPDU Guard	Operational Edge	Operational Point-to-Point	Port Role	Port State	Designated Bridge	Designated Port ID	Designated Cost
1	GE1	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-1	20000
2	GE2	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-2	20000
3	GE3	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-3	20000
4	GE4	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-4	20000
5	GE5	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-5	20000
6	GE6	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-6	20000
7	GE7	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-7	20000
8	GE8	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-8	20000
9	GE9	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-9	20000
10	GE10	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-10	20000
11	GE11	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-11	20000
12	GE12	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-12	20000
13	GE13	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-13	20000
14	GE14	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-14	20000
15	GE15	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-15	20000
16	GE16	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-16	20000
17	GE17	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-17	20000
18	GE18	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-18	20000
19	GE19	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-19	20000
20	GE20	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-20	20000
21	GE21	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-21	20000
22	GE22	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-22	20000
23	GE23	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-23	20000
24	GE24	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-24	20000
25	GE25	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-25	20000
26	GE26	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-26	20000
27	GE27	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-27	20000
28	GE28	Enabled	20000	128	Disabled	Disabled	Disabled	Enabled	Disabled	Forwarding	0-00:00:00:00:00:00	128-28	20000
29	LAG1	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-29	20000
30	LAG2	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-30	20000
31	LAG3	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-31	20000

Figure 54 - Spanning Tree > Port Setting

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

Designated Port ID	The designated port ID on the switch.
Designated Cost	The path cost of the designated port on the switch.
Protocol Migration Check	Restart the Spanning Tree Protocol (STP) migration process (re-negotiate with its neighborhood) on the specific interface.

Click "**Edit**" button to view Edit Port Setting menu.

Edit Port Setting

Port: GE1

State: Enable

Path Cost: (0 - 200000000) (0 = Auto)

Priority: ▼

Edge Port: Enable

BPDU Filter: Enable

BPDU Guard: Enable

Point-to-Point: Auto
 Enable
 Disable

Port State: Disabled

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

Designated Port ID: 128-1

Designated Cost: 20000

Operational Edge: False

Operational Point-to-Point: False

Figure 55 - Spanning Tree > Port Setting > Edit Port Setting

Item	Description
Port	Selected port ID.
State	Enable/Disable the STP on the specified port.
Path Cost	Specify the STP path cost on the specified port.
Priority	Specify the STP path cost on the specified port.
Edge Port	Specify the edge mode. <ul style="list-style-type: none"> ● Enable: Force to true state (as link to a host). ● Disable: Force to false state (as link to a bridge).

	In the edge mode, the interface would be put into the Forwarding state immediately upon link up. If the edge mode is enabled for the interface and there are BPDUs received on the interface, the loop might be occurred in the short time before the STP state change.
BPDU Filter	The BPDU Filter configuration avoids receiving / transmitting BPDU from the specified ports. <ul style="list-style-type: none"> ● Enable: Enable BPDU filter function. ● Disable: Disable BPDU filter function.
BPDU Guard	The BPDU Guard configuration to drop the received BPDU directly. <ul style="list-style-type: none"> ● Enable: Enable BPDU guard function. ● Disable: Disable BPDU guard function.
Point-to-Point	Specify the Point-to-Point port configuration: <ul style="list-style-type: none"> ● Auto: The state is depended on the duplex setting of the port ● Enable: Force to true state. ● Disable: Force to false state

IV-6-3 MST Instance

To configure MST instance setting, click **STP > MST Instance**.

MST Instance Table

	MSTI	Priority	Bridge Identifier	Designated Root Bridge	Root Port	Root Path Cost	Remaining Hop	VLAN
<input type="radio"/>	0	32768	32768-74:DA:38:17:6E:7A	0-00:00:00:00:00:00	N/A	0	0	1-4094
<input type="radio"/>	1	32768	32768-74:DA:38:17:6E:7A	0-00:00:00:00:00:00	N/A	0	0	
<input type="radio"/>	2	32768	32768-74:DA:38:17:6E:7A	0-00:00:00:00:00:00	N/A	0	0	
<input type="radio"/>	3	32768	32768-74:DA:38:17:6E:7A	0-00:00:00:00:00:00	N/A	0	0	
<input type="radio"/>	4	32768	32768-74:DA:38:17:6E:7A	0-00:00:00:00:00:00	N/A	0	0	
<input type="radio"/>	5	32768	32768-74:DA:38:17:6E:7A	0-00:00:00:00:00:00	N/A	0	0	
<input type="radio"/>	6	32768	32768-74:DA:38:17:6E:7A	0-00:00:00:00:00:00	N/A	0	0	
<input type="radio"/>	7	32768	32768-74:DA:38:17:6E:7A	0-00:00:00:00:00:00	N/A	0	0	
<input type="radio"/>	8	32768	32768-74:DA:38:17:6E:7A	0-00:00:00:00:00:00	N/A	0	0	
<input type="radio"/>	9	32768	32768-74:DA:38:17:6E:7A	0-00:00:00:00:00:00	N/A	0	0	
<input type="radio"/>	10	32768	32768-74:DA:38:17:6E:7A	0-00:00:00:00:00:00	N/A	0	0	
<input type="radio"/>	11	32768	32768-74:DA:38:17:6E:7A	0-00:00:00:00:00:00	N/A	0	0	
<input type="radio"/>	12	32768	32768-74:DA:38:17:6E:7A	0-00:00:00:00:00:00	N/A	0	0	
<input type="radio"/>	13	32768	32768-74:DA:38:17:6E:7A	0-00:00:00:00:00:00	N/A	0	0	
<input type="radio"/>	14	32768	32768-74:DA:38:17:6E:7A	0-00:00:00:00:00:00	N/A	0	0	
<input type="radio"/>	15	32768	32768-74:DA:38:17:6E:7A	0-00:00:00:00:00:00	N/A	0	0	

Figure 56 - Spanning Tree > MST Instance

Item	Description
MSTI	Designated port number.
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.

Click "Edit" button to view Edit MST Instance menu.

Edit MST Instance Setting

MSTI 1

VLAN

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

Selected VLAN: (empty)

Priority: 32768 (0 - 61440, default 32768)

Bridge Identifier: 32768-74:DA:38:17:6E:7A

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

Root Port: (empty)

Root Path Cost: 0

Remaining Hop: 0

Apply Close

Figure 57 - Spanning Tree > MST Instance > Edit MST Instance Setting

Item	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.

IV-6-4 MST Port Setting

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

MST Port Setting Table

MSTI

Q

Entry	Port	Path Cost	Priority	Port Role	Port State	Mode	Type	Designated Bridge	Designated Port ID	Designated Cost	Remaining Hop	
<input type="checkbox"/>	1	GE1	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-1	20000	20
<input type="checkbox"/>	2	GE2	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-2	20000	20
<input type="checkbox"/>	3	GE3	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-3	20000	20
<input type="checkbox"/>	4	GE4	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-4	20000	20
<input type="checkbox"/>	5	GE5	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-5	20000	20
<input type="checkbox"/>	6	GE6	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-6	20000	20
<input type="checkbox"/>	7	GE7	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-7	20000	20
<input type="checkbox"/>	8	GE8	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-8	20000	20
<input type="checkbox"/>	9	GE9	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-9	20000	20
<input type="checkbox"/>	10	GE10	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-10	20000	20
<input type="checkbox"/>	11	GE11	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-11	20000	20
<input type="checkbox"/>	12	GE12	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-12	20000	20
<input type="checkbox"/>	13	GE13	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-13	20000	20
<input type="checkbox"/>	14	GE14	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-14	20000	20
<input type="checkbox"/>	15	GE15	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-15	20000	20
<input type="checkbox"/>	16	GE16	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-16	20000	20
<input type="checkbox"/>	17	GE17	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-17	20000	20
<input type="checkbox"/>	18	GE18	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-18	20000	20
<input type="checkbox"/>	19	GE19	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-19	20000	20
<input type="checkbox"/>	20	GE20	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-20	20000	20
<input type="checkbox"/>	21	GE21	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-21	20000	20
<input type="checkbox"/>	22	GE22	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-22	20000	20
<input type="checkbox"/>	23	GE23	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-23	20000	20
<input type="checkbox"/>	24	GE24	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-24	20000	20
<input type="checkbox"/>	25	GE25	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-25	20000	20
<input type="checkbox"/>	26	GE26	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-26	20000	20
<input type="checkbox"/>	27	GE27	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-27	20000	20
<input type="checkbox"/>	28	GE28	20000	128	Disabled	Forwarding	RSTP	Boundary	0-00:00:00:00:00:00	128-28	20000	20
<input type="checkbox"/>	29	LAG1	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-29	20000	20
<input type="checkbox"/>	30	LAG2	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-30	20000	20

Figure 58 - Spanning Tree > MST Port Setting

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

	<ul style="list-style-type: none"> ● Internal: The port attaching an MST Bridge to a LAN that is not in the same region.
Designated Bridge	The bridge ID of the designated bridge.
Designated Port ID	The designated port ID on the switch.
Designated Cost	The path cost of the designated port on the switch.
Remaining Hop	The remaining hops count on the specified port.

Click "Edit" button to view Edit MST Port Setting menu.

Edit MST Port Setting

MSTI	0
Port	GE1

Path Cost	<input type="text" value="0"/> (0 - 200000000) (0 = Auto)
Priority	<input type="text" value="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 59 - Spanning Tree > MST Port Setting > Edit MST Port Setting

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

IV-6-5 Statistics

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

Statistics Table

Refresh Rate sec Q

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	GE11	0	0	0	0	0	0
<input type="checkbox"/>	12	GE12	0	0	0	0	0	0
<input type="checkbox"/>	13	GE13	0	0	0	0	0	0
<input type="checkbox"/>	14	GE14	0	0	0	0	0	0
<input type="checkbox"/>	15	GE15	0	0	0	0	0	0
<input type="checkbox"/>	16	GE16	0	0	0	0	0	0
<input type="checkbox"/>	17	GE17	0	0	0	0	0	0
<input type="checkbox"/>	18	GE18	0	0	0	0	0	0
<input type="checkbox"/>	19	GE19	0	0	0	0	0	0
<input type="checkbox"/>	20	GE20	0	0	0	0	0	0
<input type="checkbox"/>	21	GE21	0	0	0	0	0	0
<input type="checkbox"/>	22	GE22	0	0	0	0	0	0
<input type="checkbox"/>	23	GE23	0	0	0	0	0	0
<input type="checkbox"/>	24	GE24	0	0	0	0	0	0
<input type="checkbox"/>	25	GE25	0	0	0	0	0	0
<input type="checkbox"/>	26	GE26	0	0	0	0	0	0
<input type="checkbox"/>	27	GE27	0	0	0	0	0	0
<input type="checkbox"/>	28	GE28	0	0	0	0	0	0
<input type="checkbox"/>	29	LAG1	0	0	0	0	0	0

Figure 60 - Spanning Tree > Statistics

Item	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.

Click "**View**" button to view the STP Port Statistic menu.

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

Receive BPDU

Config	0
TCN	0
MSTP	0

Transmit BPDU

Config	0
TCN	0
MSTP	0

Refresh
Clear
Close

Figure 61 - Spanning Tree > Statistics > STP Port Statistic

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

IV-7 Discovery

Use this section to configure LLDP.

IV-7-1 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.

IV-7-1-1 Property

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

The screenshot shows the LLDP Property Setting web page. It features a yellow background with a blue border. The top section is titled "LLDP" and contains the following settings:

- State:** Enable
- LLDP Handling:**
 - Filtering
 - Bridging
 - Flooding
- TLV Advertise Interval:** 30 (Sec (5 - 32767, default 30))
- Hold Multiplier:** 4 (2 - 10, default 4)
- Reinitializing Delay:** 2 (Sec (1 - 10, default 2))
- Transmit Delay:** 2 (Sec (1 - 8191, default 2))

The bottom section is titled "LLDP-MED" and contains the following setting:

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

An "Apply" button is located at the bottom left of the page.

Figure 62 - Discovery > LLDP > Property

Item	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"> ● Filtering: Deletes the packet. ● Bridging: (VLAN-aware flooding) Forwards the packet to all VLAN members. ● Flooding: Forwards the packet to all ports
TLV Advertise	Select the interval at which frames are transmitted. The default is 30

Interval	seconds, and the valid range is 5–32767 seconds.
Holdtime Multiplier	Select the multiplier on the transmit interval to assign to TTL (range 2–10, default = 4).
Reinitialization Delay	Select the delay before a re-initialization (range 1–10 seconds, default = 2).
Transmit Delay	Select the delay after an LLDP frame is sent (range 1–8191 seconds, default = 3).
Fast Start Repeat Count	Select fast start repeat count when port link up (range 1–10, default = 3).

IV-7-1-2 Port Setting

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

Port Setting Table

<input type="checkbox"/>	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
<input type="checkbox"/>	11	GE11	Normal	802.1 PVID
<input type="checkbox"/>	12	GE12	Normal	802.1 PVID
<input type="checkbox"/>	13	GE13	Normal	802.1 PVID
<input type="checkbox"/>	14	GE14	Normal	802.1 PVID
<input type="checkbox"/>	15	GE15	Normal	802.1 PVID
<input type="checkbox"/>	16	GE16	Normal	802.1 PVID
<input type="checkbox"/>	17	GE17	Normal	802.1 PVID
<input type="checkbox"/>	18	GE18	Normal	802.1 PVID
<input type="checkbox"/>	19	GE19	Normal	802.1 PVID
<input type="checkbox"/>	20	GE20	Normal	802.1 PVID
<input type="checkbox"/>	21	GE21	Normal	802.1 PVID
<input type="checkbox"/>	22	GE22	Normal	802.1 PVID
<input type="checkbox"/>	23	GE23	Normal	802.1 PVID
<input type="checkbox"/>	24	GE24	Normal	802.1 PVID
<input type="checkbox"/>	25	GE25	Normal	802.1 PVID
<input type="checkbox"/>	26	GE26	Normal	802.1 PVID
<input type="checkbox"/>	27	GE27	Normal	802.1 PVID
<input type="checkbox"/>	28	GE28	Normal	802.1 PVID

Figure 63 - Discovery > LLDP > Port Setting

Item	Description
Port	Port Name.
Mode	The port LLDP mode.
Selectde TLV	The Selected LLDP TLV.

Click "Edit" button to view Edit Port Setting menu.

Figure 64 - Discovery > LLDP > Port Setting > Edit Port Setting

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

802.1 VLAN Name	Select the VLAN Name ID to be carried (multiple selection is allowed).
-----------------	--

IV-7-1-3 Packet View

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

Packet View Table

	Entry	Port	In-Use (Bytes)	Available (Bytes)	Operational Status
<input type="radio"/>	1	GE1	48	1440	Not Overloading
<input type="radio"/>	2	GE2	48	1440	Not Overloading
<input type="radio"/>	3	GE3	48	1440	Not Overloading
<input type="radio"/>	4	GE4	48	1440	Not Overloading
<input type="radio"/>	5	GE5	48	1440	Not Overloading
<input type="radio"/>	6	GE6	48	1440	Not Overloading
<input type="radio"/>	7	GE7	48	1440	Not Overloading
<input type="radio"/>	8	GE8	48	1440	Not Overloading
<input type="radio"/>	9	GE9	48	1440	Not Overloading
<input type="radio"/>	10	GE10	49	1439	Not Overloading
<input type="radio"/>	11	GE11	49	1439	Not Overloading
<input type="radio"/>	12	GE12	49	1439	Not Overloading
<input type="radio"/>	13	GE13	49	1439	Not Overloading
<input type="radio"/>	14	GE14	49	1439	Not Overloading
<input type="radio"/>	15	GE15	49	1439	Not Overloading
<input type="radio"/>	16	GE16	49	1439	Not Overloading
<input type="radio"/>	17	GE17	49	1439	Not Overloading
<input type="radio"/>	18	GE18	49	1439	Not Overloading
<input type="radio"/>	19	GE19	49	1439	Not Overloading
<input type="radio"/>	20	GE20	49	1439	Not Overloading
<input type="radio"/>	21	GE21	49	1439	Not Overloading
<input type="radio"/>	22	GE22	49	1439	Not Overloading
<input type="radio"/>	23	GE23	49	1439	Not Overloading
<input type="radio"/>	24	GE24	49	1439	Not Overloading
<input type="radio"/>	25	GE25	49	1439	Not Overloading
<input type="radio"/>	26	GE26	49	1439	Not Overloading
<input type="radio"/>	27	GE27	49	1439	Not Overloading
<input type="radio"/>	28	GE28	49	1439	Not Overloading

Figure 65 - Discovery > LLDP > Packet View

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

Click "**Detail**" button to view Packet View Detail menu.

Packet View Detail	
Port	GE1
Mandatory TLVs	
Size (Bytes)	21
Operational Status	Transmitted
MED Capabilities	
Size (Bytes)	9
Operational Status	Transmitted
MED Location	
Size (Bytes)	0
Operational Status	Transmitted
MED Network Policy	
Size (Bytes)	10
Operational Status	Transmitted
MED Inventory	
Size (Bytes)	0
Operational Status	Transmitted
MED Extended Power via MDI	
Size (Bytes)	0
Operational Status	Transmitted
802.3 TLVs	
Size (Bytes)	0
Operational Status	Transmitted

Optional TLVs	
Size (Bytes)	0
Operational Status	Transmitted
802.1 TLVs	
Size (Bytes)	8
Operational Status	Transmitted
Total	
In-Use (Bytes)	48
Available (Bytes)	1440

Figure 66 - Discovery > LLDP > Packet View > Packet View Detail

Item	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.

IV-7-1-4 Local Information

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

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

Device Summary

Chassis ID Subtype	MAC address
Chassis ID	FC:8F:C4:00:00:01
System Name	Switch
System Description	24-Port Gigabit Smart Managed Switch with 4 Gigabit Fiber Port
Supported Capabilities	Bridge
Enabled Capabilities	Bridge
Port ID Subtype	Local

Port Status Table

Entry	Port	LLDP State
<input type="radio"/>	1 GE1	Normal
<input type="radio"/>	2 GE2	Normal
<input type="radio"/>	3 GE3	Normal
<input type="radio"/>	4 GE4	Normal
<input type="radio"/>	5 GE5	Normal
<input type="radio"/>	6 GE6	Normal
<input type="radio"/>	7 GE7	Normal
<input type="radio"/>	8 GE8	Normal
<input type="radio"/>	9 GE9	Normal
<input type="radio"/>	10 GE10	Normal
<input type="radio"/>	11 GE11	Normal
<input type="radio"/>	12 GE12	Normal
<input type="radio"/>	13 GE13	Normal
<input type="radio"/>	14 GE14	Normal
<input type="radio"/>	15 GE15	Normal
<input type="radio"/>	16 GE16	Normal
<input type="radio"/>	17 GE17	Normal
<input type="radio"/>	18 GE18	Normal
<input type="radio"/>	19 GE19	Normal
<input type="radio"/>	20 GE20	Normal
<input type="radio"/>	21 GE21	Normal
<input type="radio"/>	22 GE22	Normal
<input type="radio"/>	23 GE23	Normal
<input type="radio"/>	24 GE24	Normal
<input type="radio"/>	25 GE25	Normal
<input type="radio"/>	26 GE26	Normal
<input type="radio"/>	27 GE27	Normal
<input type="radio"/>	28 GE28	Normal

Figure 67 - Discovery > LLDP > Local Information

Item	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	Primary enabled functions of the device.

Enabled	
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.

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

Local Information Detail

Chassis ID Subtype	MAC address
Chassis ID	FC:8F:C4:00:00:01
System Name	Switch
System Description	24-Port Gigabit Smart Managed Switch with 4 Gigabit Fiber Port
Supported Capabilities	Bridge
Enabled Capabilities	Bridge
Port ID	GE1
Port ID Subtype	Local
Port Description	

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

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

802.3 Detail	
802.3 Maximum Frame Size	N/A

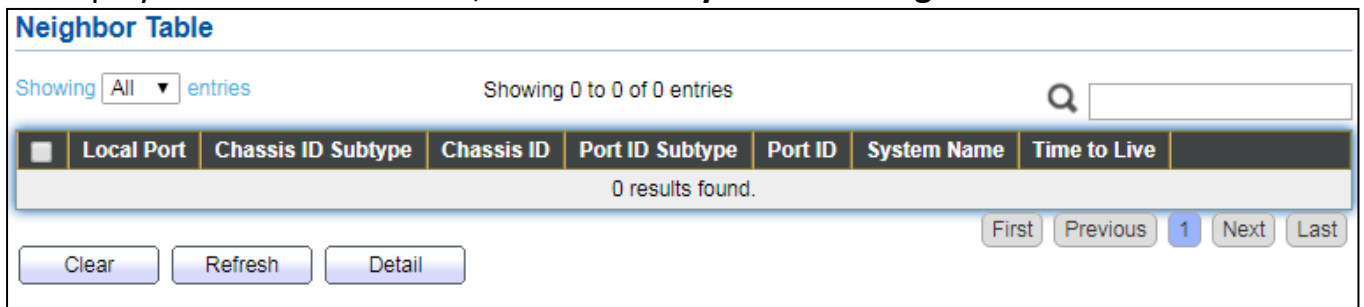
802.3 Link Aggregation	
Aggregation Capability	N/A
Aggregation Status	N/A
Aggregation Port ID	N/A

Figure 68 - Discovery > LLDP > Local Information > Detail

IV-7-1-5 Neighbor

Use the LLDP Neighbor page to view LLDP neighbors information.

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



The screenshot shows a web interface for the LLDP Neighbor table. At the top, it says "Showing All entries" and "Showing 0 to 0 of 0 entries". There is a search bar on the right. The table has the following columns: Local Port, Chassis ID Subtype, Chassis ID, Port ID Subtype, Port ID, System Name, and Time to Live. Below the table, it says "0 results found." and there are navigation buttons: First, Previous, 1, Next, Last. At the bottom, there are buttons for Clear, Refresh, and Detail.

Figure 69 - Discovery > LLDP > Neighbor

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

Click “**detail**” to view selected neighbor detail information

Neighbor Information Detail

Local Port	GE1
------------	-----

Basic Detail

Chassis ID Subtype	MAC address
Chassis ID	A4:4C:C8:16:5C:FB
Port ID Subtype	MAC address
Port ID	A4:4C:C8:16:5C:FB
Port Description	
System Name	
System Description	
Supported Capabilities	N/A
Enabled Capabilities	N/A

Management Address Table

Address Subtype	Address	Interface Subtype	Interface Number
0 results found.			

MAC/PHY Detail

Auto-Negotiation Supported	True
Auto-Negotiation Enabled	True
Auto-Negotiation Advertised Capabilities	1000baseTFD
Operational MAU Type	Other

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

802.1 VLAN and Protocol

PVID	
VLAN Name	N/A

Figure 70 - LLDP Neighbor Detail Page

IV-7-1-6 Statistics

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

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

Global Statistics

Insertions	2
Deletions	1
Drops	0
AgeOuts	0

Clear Refresh

Statistics Table

Q

Entry	Port	Transmit Frame		Receive Frame			Receive TLV		Neighbor Timeout
		Total	Total	Discard	Error	Discard	Unrecognized		
<input type="checkbox"/>	1	GE1	20307	9759	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	0	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
<input type="checkbox"/>	11	GE11	0	0	0	0	0	0	0
<input type="checkbox"/>	12	GE12	0	0	0	0	0	0	0
<input type="checkbox"/>	13	GE13	0	0	0	0	0	0	0
<input type="checkbox"/>	14	GE14	0	0	0	0	0	0	0
<input type="checkbox"/>	15	GE15	0	0	0	0	0	0	0
<input type="checkbox"/>	16	GE16	0	0	0	0	0	0	0
<input type="checkbox"/>	17	GE17	0	0	0	0	0	0	0
<input type="checkbox"/>	18	GE18	0	0	0	0	0	0	0
<input type="checkbox"/>	19	GE19	0	0	0	0	0	0	0
<input type="checkbox"/>	20	GE20	0	0	0	0	0	0	0
<input type="checkbox"/>	21	GE21	0	0	0	0	0	0	0
<input type="checkbox"/>	22	GE22	0	0	0	0	0	0	0
<input type="checkbox"/>	23	GE23	0	0	0	0	0	0	0
<input type="checkbox"/>	24	GE24	0	0	0	0	0	0	0
<input type="checkbox"/>	25	GE25	0	0	0	0	0	0	0
<input type="checkbox"/>	26	GE26	0	0	0	0	0	0	0
<input type="checkbox"/>	27	GE27	0	0	0	0	0	0	0
<input type="checkbox"/>	28	GE28	0	0	0	0	0	0	0

Clear Refresh

Figure 71 - Discovery > LLDP > Statistics

Item	Description
Insertions	The number of times the complete set of information advertised by a particular MAC Service Access Point (MSAP) has been inserted into tables associated with the remote systems.
Deletions	The number of times the complete set of information advertised by MSAP has been deleted from tables associated with the remote systems.
Drops	The number of times the complete set of information advertised by MSAP could not be entered into tables associated with the remote systems because of insufficient resources.
Age Outs	The number of times the complete set of information advertised by MSAP has been deleted from tables associated with the remote systems because the information timeliness interval has expired.

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

IV-8 Multicast

Use this section to configure Multicast.

IV-8-1 General

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

IV-8-1-1 Property

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

The screenshot shows a configuration interface for Multicast settings. It is divided into two main sections. The first section, 'Unknown Multicast Action', contains three radio button options: 'Flood' (which is selected), 'Drop', and 'Forward to Router Port'. The second section, 'Multicast Forward Method', contains two radio button options: 'DMAC-VID' (which is selected) and 'DIP-VID'. Below these sections is an 'Apply' button.

Figure 72 - Multicast > General > Property

Item	Description
Unknown Multicast Action	Set the unknown multicast action <ul style="list-style-type: none">● Flood: flood the unknown multicast data.● Drop: drop the unknown multicast data.● Router port: forward the unknown multicast data to router port.
IPv4	Set the IPv4 multicast forward method. <ul style="list-style-type: none">● MAC-VID: forward method dmac+vid.● DIP-VID: forward method dip+vid.

IV-8-1-2 Group Address

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

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

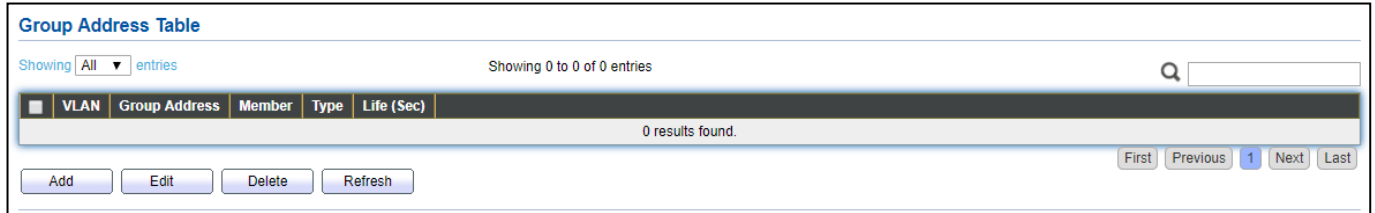


Figure 73 - Multicast > General > Group Address

Item	Description
IP Version	IP Version <ul style="list-style-type: none">● IPv4: ipv4 multicast group● IPv6: ipv6 multicast group
VLAN	The VLAN ID of group.
Group Address	The group IP address.
Member	The member ports of group.
Type	The type of group. Static or Dynamic.
Life(Sec)	The life time of this dynamic group.

Click “Add” or “Edit” button to view Add or Edit Group Address menu.

Add Group Address

VLAN

Group Address

Member

1 ▼

Available Port

- GE1
- GE2
- GE3
- GE4
- GE5
- GE6
- GE7
- GE8

>

<

Selected Port

Apply
Close

Edit Group Address

VLAN

Group Address

Member

1

225.0.0.225

Available Port

- GE2
- GE3
- GE4
- GE5
- GE6
- GE7
- GE8
- GE9

>

<

Selected Port

- GE1

Apply
Close

Figure 74 - Multicast > General > Group Address > Add/Edit Group Address

Item	Description
VLAN	The VLAN ID of group.
Group Address	The group IP address. (Please follow the multicast group address rule)
Member	<p>The member ports of group.</p> <ul style="list-style-type: none"> ● Available Port: Optional port member ● Selected Port: Selected port member <p>Move the Ports by clicking the > and < buttons after selecting a port.</p>

83

IV-8-1-3 Router Port

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

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

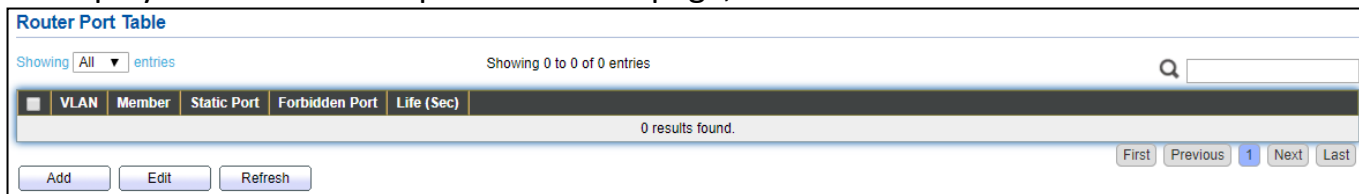


Figure 75 - Multicast > General > Router Port

Item	Description
IP Version	IP Version <ul style="list-style-type: none">● IPv4: ipv4 multicast router● IPv6: ipv6 multicast router
VLAN	The VLAN ID router entry.
Member	Router Port member (include static and learned port member).
Static Port	Static router port member.
Forbidden Port	Forbidden router port member.
Life (Sec)	The expiry time of the router entry.

Click "Add" or "Edit" button to view Add/Edit Router Port menu.

The screenshot shows the 'Add Router Port' configuration interface. It is divided into three sections:

- VLAN:** Contains two lists. 'Available VLAN' is empty. 'Selected VLAN' contains the value '1'. There are right and left arrow buttons between the lists.
- Type:** Contains two radio buttons. 'Static' is selected, and 'Forbidden' is unselected.
- Port:** Contains two lists. 'Available Port' lists GE2, GE3, GE4, GE5, GE6, GE7, GE8, and GE9. 'Selected Port' contains the value GE1. There are right and left arrow buttons between the lists.

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

Figure 76 - Multicast > General > Router Port > Add Router Port

Item	Description
VLAN	The VLAN ID for router entry <ul style="list-style-type: none"> ● Available VLAN: Optional VLAN member ● Selected VLAN: Selected VLAN member.
Type	The router port type <ul style="list-style-type: none"> ● Static: static router port ● Forbidden: forbidden router port, can't learn dynamic router port member
Port	The member ports of router entry. <ul style="list-style-type: none"> ● Available Port: Optional router port member ● Selected Port: Selected router port member

IV-8-2 IGMP Snooping

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

IV-8-2-1 Property

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

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

Figure 77 - Multicast > IGMP Snooping > Property

Item	Description
State	Set the enabling status of IGMP Snooping functionality Enable: If Checked Enable IGMP Snooping, else is Disabled IGMP Snooping.
Version	Set the igmp snooping version <ul style="list-style-type: none"> ● IGMPv2: Only support process igmp v2 packet. ● IGMPv3: Support v3 basic and v2.
Report Suppression	Set the enabling status of IGMP v2 report suppression Enable: If Checked Enable IGMP Snooping v2 report suppression, else Disable the report suppression function.
VLAN	The IGMP entry VLAN ID.
Operation Status	The enable status of IGMP snooping VLAN functionality.
Router Port Auto Learn	The enabling status of IGMP snooping router port auto learning.
Query Robustness	The Query Robustness allows tuning for the expected packet loss on a subnet.

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

Click "Edit" button to Edit VLAN Setting menu.

Edit VLAN Setting

VLAN	1
State	<input type="checkbox"/> Enable
Router Port Auto Learn	<input checked="" type="checkbox"/> Enable
Immediate leave	<input type="checkbox"/> Enable

Query Robustness	<input type="text" value="2"/> (1 - 7, default 2)
Query Interval	<input type="text" value="125"/> Sec (30 - 18000, default 125)
Query Max Response Interval	<input type="text" value="10"/> Sec (5 - 20, default 10)

Last Member Query Counter	<input type="text" value="2"/> (1 - 7, default 2)
Last Member Query Interval	<input type="text" value="1"/> Sec (1 - 25, default 1)

Operational Status

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

Apply
Close

Figure 78 - Multicast > IGMP Snooping > Property > Edit VLAN Setting

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

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

IV-8-2-2 Querier

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

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

Querier Table						
<input type="checkbox"/>	VLAN	State	Operational Status	Version	Querier Address	
<input type="checkbox"/>	1	Disabled	Disabled			

Figure 79 - Multicast > IGMP Snooping > Querier

Item	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.

Click "**Edit**" button to view Edit Querier menu.

Figure 80 - Multicast > IGMP Snooping > Querier > Edit Querier

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

IV-8-2-3 Statistics

This page allows user to clear IGMP snooping statics.

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

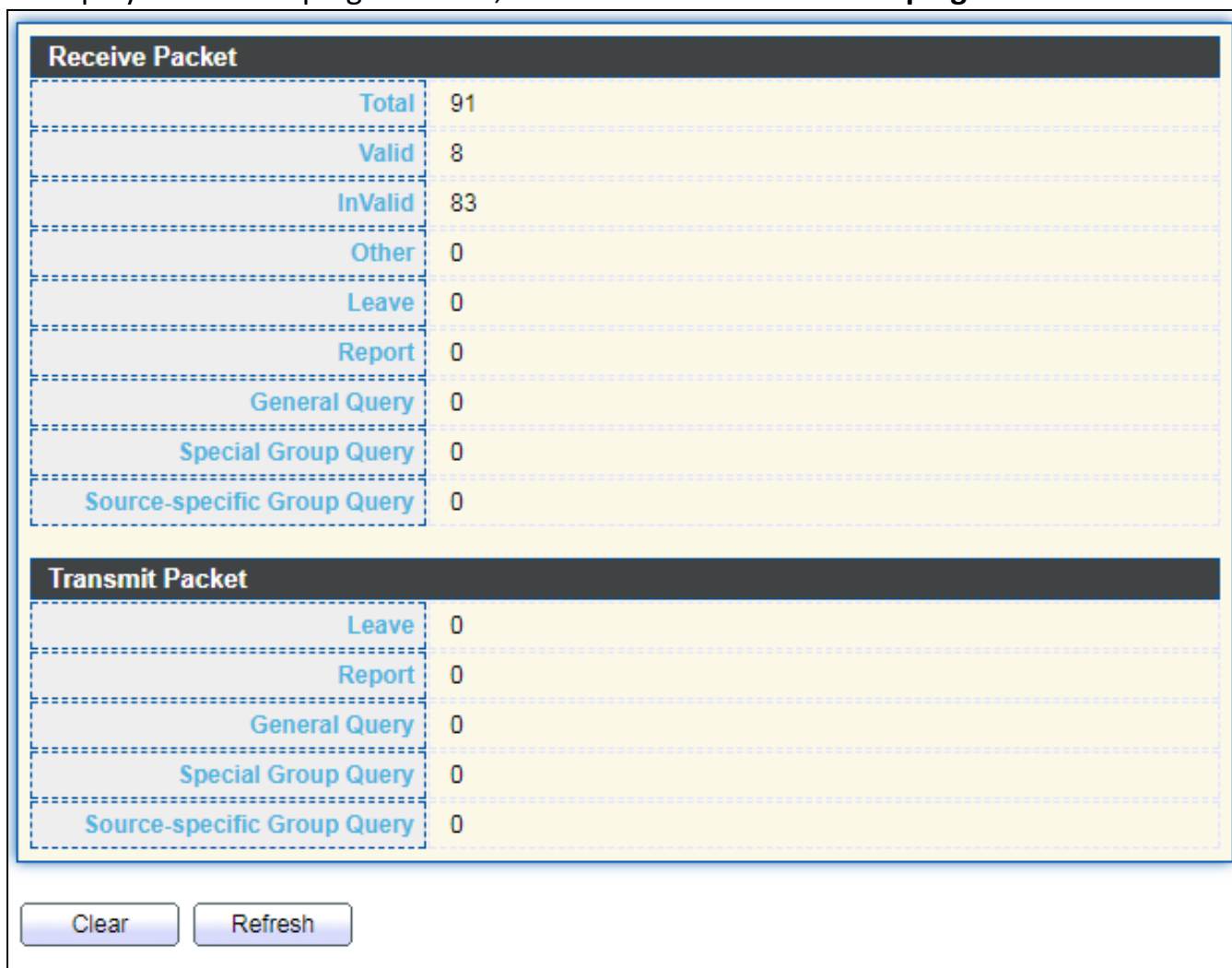


Figure 81 - Multicast > IGMP Snooping > Statistics

Item	Description
Receive Packet	
Total	Total RX igmp packet, include ipv4 multicast data to CPU.
Valid	The valid igmp snooping process packet.
InValid	The invalid igmp snooping process packet.
Other	The ICMP protocol is not 2, and is not ipv4 multicast data packet.
Leave	IGMP leave packet.
Report	IGMP join and report packet.
General Query	IGMP General Query packet.
Special Group Query	IGMP Special Group General Query packet.
Source-specific	IGMP Special Source and Group General Query packet.

Group Query	
Transmit Packet	
Leave	IGMP leave packet
Report	IGMP join and report packet
General Query	IGMP general query packet include querier transmit general query packet.
Special Group Query	IGMP special group query packet include querier transmit special group query packet.
Source-specific Group Query	IGMP Special Source and Group General Query packet.

IV-8-3 MVR

Use the MVR pages to configure settings of MVR function.

IV-8-3-1 Property

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

The screenshot shows the configuration interface for Multicast MVR. It includes the following fields and options:

- State:** Enable
- VLAN:** 1
- Mode:** Compatible, Dynamic
- Group Start:** 0.0.0.0
- Group Count:** 1 (1 - 128)
- Query Time:** 1 Sec (1 - 10)

Operational Group

- Maximum:** 128
- Current:** 0

Apply

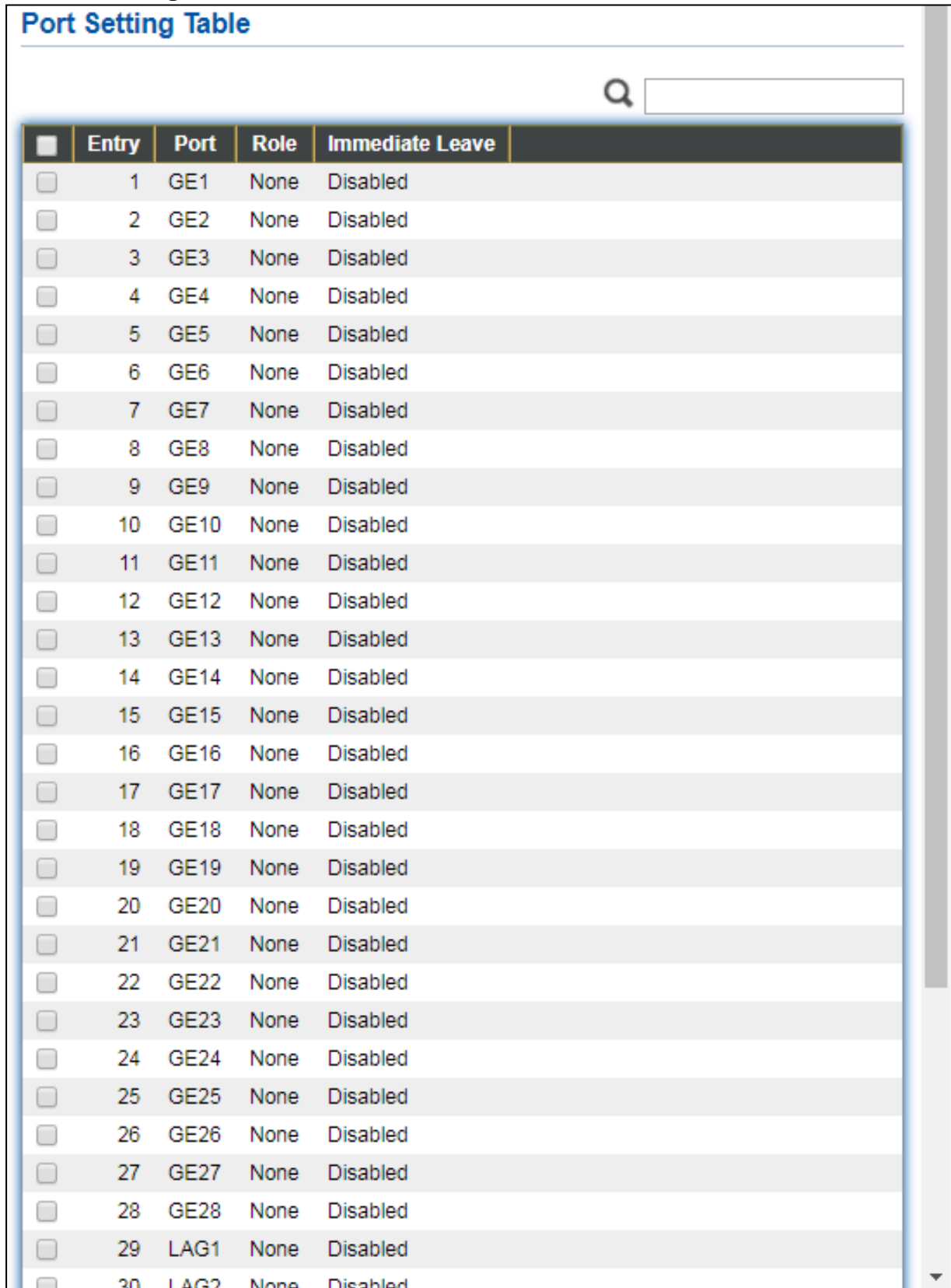
Figure 82 - Multicast > MVR > Property

Item	Description
State	Enable: if checked enable the MVR state, else disable the MVR state.
VLAN	The MVR VLAN ID.
Mode	Set the MVR mode <ul style="list-style-type: none">● Compatible: compatible mode.● Dynamic: learn group member on source port.
Group Start	MVR group range start.
Group Count	MVR group continue count.
Query Time	MVR query time when receive MVR leave MVR group packet.
Maximum	The max number of MVR group database.
Current	The learned MVR group current time

IV-8-3-2 Port Setting

This page allows user to configure port role and port immediate leave.

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



<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	GE11	None	Disabled
<input type="checkbox"/>	12	GE12	None	Disabled
<input type="checkbox"/>	13	GE13	None	Disabled
<input type="checkbox"/>	14	GE14	None	Disabled
<input type="checkbox"/>	15	GE15	None	Disabled
<input type="checkbox"/>	16	GE16	None	Disabled
<input type="checkbox"/>	17	GE17	None	Disabled
<input type="checkbox"/>	18	GE18	None	Disabled
<input type="checkbox"/>	19	GE19	None	Disabled
<input type="checkbox"/>	20	GE20	None	Disabled
<input type="checkbox"/>	21	GE21	None	Disabled
<input type="checkbox"/>	22	GE22	None	Disabled
<input type="checkbox"/>	23	GE23	None	Disabled
<input type="checkbox"/>	24	GE24	None	Disabled
<input type="checkbox"/>	25	GE25	None	Disabled
<input type="checkbox"/>	26	GE26	None	Disabled
<input type="checkbox"/>	27	GE27	None	Disabled
<input type="checkbox"/>	28	GE28	None	Disabled
<input type="checkbox"/>	29	LAG1	None	Disabled
<input type="checkbox"/>	30	LAG2	None	Disabled

Figure 83 - Multicast > MVR > Port Setting

Item	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.

Click "**Edit**" button to view Edit Port Setting menu.

The screenshot shows the 'Edit Port Setting' dialog box. It contains the following fields and options:

- Port:** GE1
- Role:**
 - None
 - Receiver
 - Source
- Immediate Leave:** Enable

Buttons: Apply, Close

Figure 84 - Multicast > MVR > Port Setting > Edit Port Setting

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

IV-8-3-3 Group Address

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

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

Figure 85 - Multicast > MVR > Group Address

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

Click "**Add**" button to view Add/Edit Group Address Table menu.

Figure 86 - Multicast > MVR > Group Address > Add Group Address

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

IV-9 Security

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

IV-9-1 RADIUS

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

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

Figure 87 - Security > RADIUS

Item	Description
Retry	Set default retry number.
Timeout	Set default timeout value.
Key String	Set default RADIUS key string
RADIUS Table	
Server Address	RADIUS server address.
Server Port	RADIUS server port.
Priority	RADIUS server priority (smaller value has higher priority). RADIUS session will try to establish with the server setting which has highest priority. If failed, it will try to connect to the server with next higher priority.
Retry	RADIUS server retry value. If it is fail to connect to server, it will keep trying until timeout with retry times.
Timeout	RADIUS server timeout value. If it is fail to connect to server, it will

	keep trying until timeout.
Usage	RADIUS server usage type Login: For login authentication. 802.1x: For 802.1x authentication. All: For all types.

Click "Add" or "Edit" button to view Add/Edit RADIUS Server menu.

Add RADIUS Server

Address Type	<input checked="" type="radio"/> Hostname <input type="radio"/> IPv4 <input type="radio"/> IPv6
Server Address	<input style="width: 100%;" type="text"/>
Server Port	<input style="width: 80%;" type="text" value="1812"/> (0 - 65535, default 1812)
Priority	<input style="width: 80%;" type="text"/> (0 - 65535)
Key String	<input checked="" type="checkbox"/> Use Default <input style="width: 100%;" type="text"/>
Retry	<input checked="" type="checkbox"/> Use Default <input style="width: 80%;" type="text" value="3"/> (1 - 10, default 3)
Timeout	<input checked="" type="checkbox"/> Use Default <input style="width: 80%;" type="text" value="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	undefined
Server Port	<input type="text" value="0"/> (0 - 65535, default 1812)
Priority	<input type="text" value="-1"/> (0 - 65535)
Key String	<input type="checkbox"/> Use Default <input type="text"/>
Retry	<input type="checkbox"/> Use Default <input type="text" value="0"/> (1 - 10, default 3)
Timeout	<input type="checkbox"/> Use Default <input type="text" value="0"/> Sec (1 - 30, default 3)
Usage	<input checked="" type="radio"/> Login <input type="radio"/> 802.1X <input type="radio"/> All

Figure 88 - Security > RADIUS > Add/Edit RADIUS Server

Item	Description
Address Type	In add dialog, user need to specify server Address Type <ul style="list-style-type: none"> ● Hostname: Use domain name as server address. ● IPv4: Use IPv4 as server address. ● IPv6: Use IPv6 as server address.
Server Address	In add dialog, user need to input server address based on address type. In edit dialog, it shows current edit server address.
Server Port	Set RADIUS server port.
Priority	Set RADIUS server priority (smaller value has higher priority). RADIUS session will try to establish with the server setting which has highest priority. If failed, it will try to connect to the server with next higher priority.
Retry	Set RADIUS server retry value. If it is fail to connect to server, it will keep trying until timeout with retry times.
Timeout	Set RADIUS server timeout value. If it is fail to connect to server, it will keep trying until timeout.
Usage	Set RADIUS server usage type <ul style="list-style-type: none"> ● Login: For login authentification. ● 802.1x: For 802.1x authentication. ● All: For all types.

IV-9-2 Management Access

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

IV-9-2-1 Management Service

This page allows user to change management services related configurations.

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

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 checked="" type="checkbox"/> 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 89 - Security > Management Access > Management Service

Item	Description
Management Service	Management service admin state. <ul style="list-style-type: none"> ● Telnet: Connect CLI through telnet. ● SSH: Connect CLI through SSH. ● HTTP: Connect WEBUI through HTTP. ● HTTPS: Connect WEBUI through HTTPS. ● SNMP: Manage switch through SNMP.
Session Timeout	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.

IV-9-2-2 Management ACL

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

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

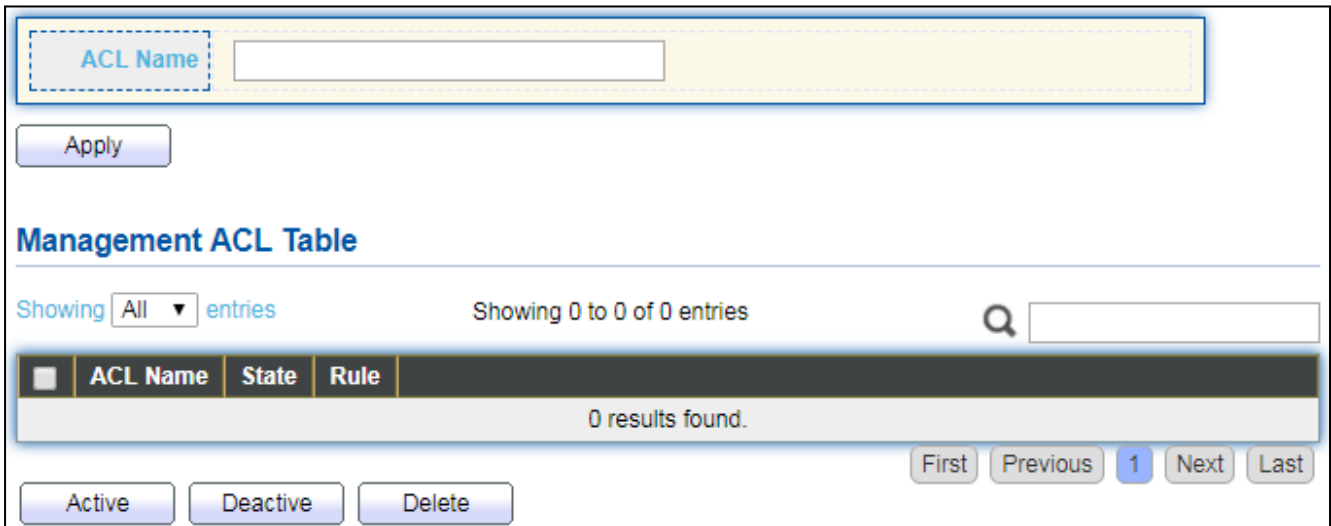


Figure 90 - Security > Management Access > Management ACL

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

IV-9-2-3 Management ACE

This page allows 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

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

Management ACE Table

ACL Name

Showing entries Showing 0 to 0 of 0 entries

<input type="checkbox"/>	Priority	Action	Service	Port	Address / Mask
0 results found.					

Figure 91 - Security > Management Access > Management ACE

Item	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.

Click "Add" or "Edit" button to view Add/Edit Management ACE menu.

Add Management ACE

ACL Name	manage	
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	Selected Port
	GE1 GE2 GE3 GE4 GE5 GE6 GE7 GE8	
IP Version	<input checked="" type="radio"/> All <input type="radio"/> IPv4 <input type="radio"/> IPv6	
IPv4	/ 255.255.255.255	
IPv6	/ 128 (1 - 128)	

Apply Close

Edit Management ACE

ACL Name	manage	
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 GE3 GE4 GE5 GE6 GE7 GE8 GE9	Selected Port GE1
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 92 - Security > Management Access > Add/Edit Management ACE

Item	Description
ACL Name	Display the ACL name to which an ACE is being added.
Priority	Specify the priority of the ACE. ACEs with higher sequence are processed first (1 is the highest priority). Only available on Add Dialog.
Service	Select the type service of rule. <ul style="list-style-type: none"> ● All: All services. ● HTTP: Only HTTP service. ● HTTPS: Only HTTPS service. ● SNMP: Only SNMP service. ● SSH: Only SSH service. ● Telnet: Only Telnet service.
Action	Select the action after ACE match packet. <ul style="list-style-type: none"> ● Permit: Forward packets that meet the ACE criteria.

	<ul style="list-style-type: none"> ● Deny: Drop packets that meet the ACE criteria.
Port	Select ports which will be matched.
IP Version	Select the type of source IP address. <ul style="list-style-type: none"> ● All: All IP addresses can access. ● IPv4: Specify IPv4 address ca access. ● IPv6: Specify IPv6 address ca access.
IPv4	Enter the source IPv4 address value and mask to which will be matched.
IPv6	Enter the source IPv6 address value and mask to which will be matched.

IV-9-3 Authentication Manager

IV-9-3-1 Property

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

To display authentication manager Property web page, click **Security > Authentication Manager > Property**.

Authentication Type

 802.1x

Guest VLAN

 Enable

MAC-Based User ID Format

Port Mode Table

Entry	Port	Authentication Type	Host Mode	Method	Guest VLAN	VLAN Assign Mode	
		802.1x					
<input type="checkbox"/>	1	GE1	Disabled	Multiple Authentication	RADIUS	Disabled	Static
<input type="checkbox"/>	2	GE2	Disabled	Multiple Authentication	RADIUS	Disabled	Static
<input type="checkbox"/>	3	GE3	Disabled	Multiple Authentication	RADIUS	Disabled	Static
<input type="checkbox"/>	4	GE4	Disabled	Multiple Authentication	RADIUS	Disabled	Static
<input type="checkbox"/>	5	GE5	Disabled	Multiple Authentication	RADIUS	Disabled	Static
<input type="checkbox"/>	6	GE6	Disabled	Multiple Authentication	RADIUS	Disabled	Static
<input type="checkbox"/>	7	GE7	Disabled	Multiple Authentication	RADIUS	Disabled	Static
<input type="checkbox"/>	8	GE8	Disabled	Multiple Authentication	RADIUS	Disabled	Static
<input type="checkbox"/>	9	GE9	Disabled	Multiple Authentication	RADIUS	Disabled	Static
<input type="checkbox"/>	10	GE10	Disabled	Multiple Authentication	RADIUS	Disabled	Static
<input type="checkbox"/>	11	GE11	Disabled	Multiple Authentication	RADIUS	Disabled	Static
<input type="checkbox"/>	12	GE12	Disabled	Multiple Authentication	RADIUS	Disabled	Static
<input type="checkbox"/>	13	GE13	Disabled	Multiple Authentication	RADIUS	Disabled	Static
<input type="checkbox"/>	14	GE14	Disabled	Multiple Authentication	RADIUS	Disabled	Static
<input type="checkbox"/>	15	GE15	Disabled	Multiple Authentication	RADIUS	Disabled	Static
<input type="checkbox"/>	16	GE16	Disabled	Multiple Authentication	RADIUS	Disabled	Static
<input type="checkbox"/>	17	GE17	Disabled	Multiple Authentication	RADIUS	Disabled	Static
<input type="checkbox"/>	18	GE18	Disabled	Multiple Authentication	RADIUS	Disabled	Static
<input type="checkbox"/>	19	GE19	Disabled	Multiple Authentication	RADIUS	Disabled	Static
<input type="checkbox"/>	20	GE20	Disabled	Multiple Authentication	RADIUS	Disabled	Static
<input type="checkbox"/>	21	GE21	Disabled	Multiple Authentication	RADIUS	Disabled	Static
<input type="checkbox"/>	22	GE22	Disabled	Multiple Authentication	RADIUS	Disabled	Static
<input type="checkbox"/>	23	GE23	Disabled	Multiple Authentication	RADIUS	Disabled	Static
<input type="checkbox"/>	24	GE24	Disabled	Multiple Authentication	RADIUS	Disabled	Static
<input type="checkbox"/>	25	GE25	Disabled	Multiple Authentication	RADIUS	Disabled	Static
<input type="checkbox"/>	26	GE26	Disabled	Multiple Authentication	RADIUS	Disabled	Static
<input type="checkbox"/>	27	GE27	Disabled	Multiple Authentication	RADIUS	Disabled	Static
<input type="checkbox"/>	28	GE28	Disabled	Multiple Authentication	RADIUS	Disabled	Static

Figure 93 - Security > Authentication Manager > Property

Item	Description
Authentication Type	Set checkbox to enable/disable following authentication types ● 802.1x: Use IEEE 802.1x to do authentication
Guest VLAN	Set checkbox to enable/disable guest VLAN, if guest VLAN is enabled, you need to select one available VLAN ID to be guest VID.
MAC-Based User ID Format	Select mac-based authentication RADIUS username/password ID format.

	<ul style="list-style-type: none"> ● XXXXXXXXXXXX ● Xxxxxxxxxxxxxx ● XX:XX:XX:XX:XX:XX ● xx:xx:xx:xx:xx:xx ● XX-XX-XX-XX-XX-XX ● xx-xx-xx-xx-xx-xx ● XX.XX.XX.XX.XX.XX ● xx.xx.xx.xx.xx.xx ● XXXX:XXXX:XXXX ● xxxx:xxxx:xxxx ● XXXX-XXXX-XXXX ● XXXX-XXXX-XXXX ● XXXX.XXXX.XXXX ● XXXX.XXXX.XXXX ● XXXXXX:XXXXXX ● XXXXXX:XXXXXX ● XXXXXX-XXXXXX ● XXXXXX-XXXXXX
--	--

Port Mode Table

Port	Port Name.
Authentication Type (802.1X)	802.1X authentication type state <ul style="list-style-type: none"> ● Enabled: 802.1X is enabled. ● Disabled: 802.1X is disabled.
Method	Support following authentication method order combinations. These orders only available on MAC-Based authentication and WEB-Based authentication. 802.1x only support Radius method. <ul style="list-style-type: none"> ● Local: Use DUT’s local database to do authentication ● Radius: Use remote RADIUS server to do authentication ● Local Radius ● Radius Local
Guest VLAN	Port guest VLAN enable state <ul style="list-style-type: none"> ● Enabled: Guest VLAN is enabled on port. ● Disabled: Guest VLAN is disabled on port.
VLAN Assign Mode	Support following VLAN assign mode and only apply when source is RADIUS <ul style="list-style-type: none"> ● Disable: Ignore the VLAN authorization result and keep original VLAN of host. ● Reject: If get VLAN authorized information, just use it. However, if there is no VLAN authorized information, reject the host and make it unauthorized. ● Static: If get VLAN authorized information, just use it. If there is no VLAN authorized information, keep original VLAN of host.

Click **“Edit”** button to view the Edit Port Mode menu.

Figure 94 - Security > Authentication Manager > Property > Edit Port Mode

Item	Description
Port	Selected port list.
Authentication Type	Set checkbox to enable/disable authentication types.
Host Mode	<p>Select authenticating host mode</p> <ul style="list-style-type: none"> ● Multiple Authentication: In this mode, every client need to pass authenticate procedure individually. ● Multiple Hosts: In this mode, only one client need to be authenticated and other clients will get the same access accessibility. Web-auth cannot be enabled in this mode. ● Single Host: In this mode, only one host is allowed to be authenticated. It is the same as Multi-auth mode with max hosts number configure to be 1.
Method	<p>Support following authentication method order combinations. These orders only available on MAC-Based authentication and WEB-Based authentication. 802.1x only support Radius method.</p> <ul style="list-style-type: none"> ● Local: Use DUT’s local database to do authentication. ● Radius: Use remote RADIUS server to do authentication. ● Local Radius. ● Radius Local.
Guest VLAN	Set checkbox to enable/disable guest VLAN.

VLAN Assign Mode	<p>Support following VLAN assign mode and only apply when source is RADIUS</p> <ul style="list-style-type: none">● Disable: Ignore the VLAN authorization result and keep original VLAN of host.● Reject: If get VLAN authorized information, just use it. However, if there is no VLAN authorized information, reject the host and make it unauthorized.● Static: If get VLAN authorized information, just use it. If there is no VLAN authorized information, keep original VLAN of host.
------------------	---

IV-9-3-2 Port Setting

This page allows user to configure authentication manger port settings

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

Port Setting Table

Entry	Port	Port Control	Reauthentication	Max Hosts	Common Timer			802.1x Parameters				
					Reauthentication	Inactive	Quiet	TX Period	Supplicant Timeout	Server Timeout	Max Request	
<input type="checkbox"/>	1	GE1	Disabled	Disabled	256	3600	60	60	30	30	30	2
<input type="checkbox"/>	2	GE2	Disabled	Disabled	256	3600	60	60	30	30	30	2
<input type="checkbox"/>	3	GE3	Disabled	Disabled	256	3600	60	60	30	30	30	2
<input type="checkbox"/>	4	GE4	Disabled	Disabled	256	3600	60	60	30	30	30	2
<input type="checkbox"/>	5	GE5	Disabled	Disabled	256	3600	60	60	30	30	30	2
<input type="checkbox"/>	6	GE6	Disabled	Disabled	256	3600	60	60	30	30	30	2
<input type="checkbox"/>	7	GE7	Disabled	Disabled	256	3600	60	60	30	30	30	2
<input type="checkbox"/>	8	GE8	Disabled	Disabled	256	3600	60	60	30	30	30	2
<input type="checkbox"/>	9	GE9	Disabled	Disabled	256	3600	60	60	30	30	30	2
<input type="checkbox"/>	10	GE10	Disabled	Disabled	256	3600	60	60	30	30	30	2
<input type="checkbox"/>	11	GE11	Disabled	Disabled	256	3600	60	60	30	30	30	2
<input type="checkbox"/>	12	GE12	Disabled	Disabled	256	3600	60	60	30	30	30	2
<input type="checkbox"/>	13	GE13	Disabled	Disabled	256	3600	60	60	30	30	30	2
<input type="checkbox"/>	14	GE14	Disabled	Disabled	256	3600	60	60	30	30	30	2
<input type="checkbox"/>	15	GE15	Disabled	Disabled	256	3600	60	60	30	30	30	2
<input type="checkbox"/>	16	GE16	Disabled	Disabled	256	3600	60	60	30	30	30	2
<input type="checkbox"/>	17	GE17	Disabled	Disabled	256	3600	60	60	30	30	30	2
<input type="checkbox"/>	18	GE18	Disabled	Disabled	256	3600	60	60	30	30	30	2
<input type="checkbox"/>	19	GE19	Disabled	Disabled	256	3600	60	60	30	30	30	2
<input type="checkbox"/>	20	GE20	Disabled	Disabled	256	3600	60	60	30	30	30	2
<input type="checkbox"/>	21	GE21	Disabled	Disabled	256	3600	60	60	30	30	30	2
<input type="checkbox"/>	22	GE22	Disabled	Disabled	256	3600	60	60	30	30	30	2
<input type="checkbox"/>	23	GE23	Disabled	Disabled	256	3600	60	60	30	30	30	2
<input type="checkbox"/>	24	GE24	Disabled	Disabled	256	3600	60	60	30	30	30	2
<input type="checkbox"/>	25	GE25	Disabled	Disabled	256	3600	60	60	30	30	30	2
<input type="checkbox"/>	26	GE26	Disabled	Disabled	256	3600	60	60	30	30	30	2
<input type="checkbox"/>	27	GE27	Disabled	Disabled	256	3600	60	60	30	30	30	2
<input type="checkbox"/>	28	GE28	Disabled	Disabled	256	3600	60	60	30	30	30	2

Edit

Figure 95 - Security > Authentication Manager > Port Setting

Item	Description
Port	Port
Port Control	<p>Support following authentication port control types.</p> <ul style="list-style-type: none"> ● Disable: Disable authentication function and all clients have network accessibility. ● Force Authorized: Port is force authorized and all clients have network accessibility. ● Force Unauthorized: Port is force unauthorized and all clients have no network accessibility. ● Auto: Need passing authentication procedure to get network accessibility.
Reauthentication	<p>Reautheticate state</p> <ul style="list-style-type: none"> ● Enabled: Host will be reauthenticated after reauthentication period. ● Disabled: Host will not be reauthenticated after reauthentication

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

Click "Edit" button to view Edit Port Setting menu.

Edit Port Setting

Port	GE1	
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	<input type="text" value="256"/>	(1 - 256, default 256)
Common Timer		
Reauthentication	<input type="text" value="3600"/>	Sec (300 - 4294967294, default 3600)
Inactive	<input type="text" value="60"/>	Sec (60 - 65535, default 60)
Quiet	<input type="text" value="60"/>	Sec (0 - 65535, default 60)
802.1x Parameters		
TX Period	<input type="text" value="30"/>	Sec (1 - 65535, default 30)
Supplicant Timeout	<input type="text" value="30"/>	Sec (1 - 65535, default 30)
Server Timeout	<input type="text" value="30"/>	Sec (1 - 65535, default 30)
Max Request	<input type="text" value="2"/>	(1 - 10, default 2)

Figure 96 - Security > Authentication Manager > Port Setting > Edit Port Setting

Item	Description
Port	Port Name.
Port Control	Support following authentication port control types. <ul style="list-style-type: none"> ● Disable: Disable authentication function and all clients have network accessibility. ● Force Authorized: Port is force authorized and all clients have network accessibility. ● Force Unauthorized: Port is force unauthorized and all clients have no network accessibility. ● Auto: Need passing authentication procedure to get network accessibility.
Reauthentication	Set checkbox to enable/disable reauthentication.
Max Hosts	In Multiple Authentication mode, total host number cannot not exceed max hosts number.
Common Timer	
Reauthentication	After re-authenticate period, host will return to initial state and need

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

IV-9-3-3 Sessions

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

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

Figure 97 - Security > Authentication Manager > Sessions

Item	Description
Session ID	Session ID is unique of each session.
Port	Port name which the host located.
MAC Address	Host MAC address.
Current Type	Show current authenticating type ● 802.1x: Use IEEE 802.1X to do authenticating
Status	Show host authentication session status IP version (IPv4, IPv6)

	<ul style="list-style-type: none"> ● Disable: This session is ready to be deleted ● Running: Authentication process is running ● Authorized: Authentication is passed and getting network accessibility. ● Unauthorized: Authentication is not passed and not getting network accessibility. ● Locked: Host is locked and do not allow to do authenticating until quiet period. ● Guest: Host is in the guest VLAN.
Operational (VLAN)	Shows host operational VLAN ID.
Operational (Session Time)	In "Authorized" state, it shows total time after authorized.
Operational (Inactived)	In "Authorized" state, it shows how long the host do not send any packet.
Operational (Quiet Time)	In "Locked" state, it shows total time after locked.
Authorized (VLAN)	Shows VLAN ID given from authorized procedure.
Authorized (Reauthentication Period)	Shows reauthentication period given from authorized procedure.
Authorized (Inactive Timeouts)	Shows inactive timeout given from authorized procedure.

IV-9-4 Port Security

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

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

Entry	Port	State	MAC Address	Action
1	GE1	Disabled	1	Discard
2	GE2	Disabled	1	Discard
3	GE3	Disabled	1	Discard
4	GE4	Disabled	1	Discard
5	GE5	Disabled	1	Discard
6	GE6	Disabled	1	Discard
7	GE7	Disabled	1	Discard
8	GE8	Disabled	1	Discard
9	GE9	Disabled	1	Discard
10	GE10	Disabled	1	Discard
11	GE11	Disabled	1	Discard
12	GE12	Disabled	1	Discard
13	GE13	Disabled	1	Discard
14	GE14	Disabled	1	Discard
15	GE15	Disabled	1	Discard
16	GE16	Disabled	1	Discard
17	GE17	Disabled	1	Discard
18	GE18	Disabled	1	Discard
19	GE19	Disabled	1	Discard
20	GE20	Disabled	1	Discard
21	GE21	Disabled	1	Discard
22	GE22	Disabled	1	Discard
23	GE23	Disabled	1	Discard
24	GE24	Disabled	1	Discard
25	GE25	Disabled	1	Discard
26	GE26	Disabled	1	Discard
27	GE27	Disabled	1	Discard
28	GE28	Disabled	1	Discard
29	LAG1	Disabled	1	Discard
30	LAG2	Disabled	1	Discard
31	LAG3	Disabled	1	Discard
32	LAG4	Disabled	1	Discard
33	LAG5	Disabled	1	Discard
34	LAG6	Disabled	1	Discard
35	LAG7	Disabled	1	Discard
36	LAG8	Disabled	1	Discard

Figure 98 - Security > Port Security

Item	Description
State	Enable/Disable the port security function.
Port	Select one or multiple ports to configure.
State	Select the status of port security <ul style="list-style-type: none"> ● Disable: Disable port security function. ● Enable: Enable port security function.
MAC Address	Specify the number of how many mac addresses can be learned.

Action	<p>Select the action if learned mac addresses</p> <ul style="list-style-type: none"> ● Forward: Forward this packet whose SMAC is new to system and exceed the learning-limit number. ● Discard: Discard this packet whose SMAC is new to system and exceed the learning-limit number. ● Shutdown: Shutdown this port when receives a packet whose SMAC is new to system and exceed the learning limit number.
--------	---

Click "Edit" button to view Edit Port Security menu.

Figure 99 - Security > Port Security > Edd Port Security

Item	Description
Port	Select one or multiple ports to configure.
State	Select the status of port security Disable: Disable port security function. Enable: Enable port security function.
MAC Address	Specify the number of how many mac addresses can be learned.
Action	<p>Select the action if learned mac addresses</p> <ul style="list-style-type: none"> ● Forward: Forward this packet whose SMAC is new to system and exceed the learning-limit number. ● Discard: Discard this packet whose SMAC is new to system and exceed the learning-limit number. ● Shutdown: Shutdown this port when receives a packet whose SMAC is new to system and exceed the learning limit number.

IV-9-5 Protected Port

This page allows 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.

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

Protected Port Table

Q

<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	GE11	Unprotected
<input type="checkbox"/>	12	GE12	Unprotected
<input type="checkbox"/>	13	GE13	Unprotected
<input type="checkbox"/>	14	GE14	Unprotected
<input type="checkbox"/>	15	GE15	Unprotected
<input type="checkbox"/>	16	GE16	Unprotected
<input type="checkbox"/>	17	GE17	Unprotected
<input type="checkbox"/>	18	GE18	Unprotected
<input type="checkbox"/>	19	GE19	Unprotected
<input type="checkbox"/>	20	GE20	Unprotected
<input type="checkbox"/>	21	GE21	Unprotected
<input type="checkbox"/>	22	GE22	Unprotected
<input type="checkbox"/>	23	GE23	Unprotected
<input type="checkbox"/>	24	GE24	Unprotected
<input type="checkbox"/>	25	GE25	Unprotected
<input type="checkbox"/>	26	GE26	Unprotected
<input type="checkbox"/>	27	GE27	Unprotected
<input type="checkbox"/>	28	GE28	Unprotected

Edit

Figure 100 - Security > Protected Port

Item	Description
Port	Port Name.
State	Port protected admin state. <ul style="list-style-type: none"> ● Protected: Port is protected. ● Unprotected: Port is unprotected

Click "**Edit**" button to view Edit Protected Port menu.

Figure 101 - Security > Protected Port > Edit Protected Port

Item	Description
Port	Selected port list.
State	Port protected admin state. <ul style="list-style-type: none"> ● Protected: Enable protecting function. ● Unprotected: Disable protecting function.

IV-9-6 Storm Control

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

The screenshot displays the Storm Control configuration interface. At the top, there are two sections: 'Mode' and 'IFG'. The 'Mode' section has two radio buttons: 'Packet / Sec' (unselected) and 'Kbits / Sec' (selected). The 'IFG' section has two radio buttons: 'Exclude' (selected) and 'Include' (unselected). Below these is an 'Apply' button. The main part of the page is the 'Port Setting Table', which includes a search bar and a table with the following columns: Entry, Port, State, Broadcast (State, Rate (Kbps)), Unknown Multicast (State, Rate (Kbps)), Unknown Unicast (State, Rate (Kbps)), and Action. The table contains 23 rows, each representing a port from GE1 to GE23. All ports are currently in a 'Disabled' state, and the broadcast, unknown multicast, and unknown unicast settings are also disabled with a rate of 10000 Kbps. The action for all ports is 'Drop'.

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
<input type="checkbox"/>	11	GE11	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
<input type="checkbox"/>	12	GE12	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
<input type="checkbox"/>	13	GE13	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
<input type="checkbox"/>	14	GE14	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
<input type="checkbox"/>	15	GE15	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
<input type="checkbox"/>	16	GE16	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
<input type="checkbox"/>	17	GE17	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
<input type="checkbox"/>	18	GE18	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
<input type="checkbox"/>	19	GE19	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
<input type="checkbox"/>	20	GE20	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
<input type="checkbox"/>	21	GE21	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
<input type="checkbox"/>	22	GE22	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
<input type="checkbox"/>	23	GE23	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop

Figure 102 - Security > Storm Control

Item	Description
Mode(Unit)	Select the unit of storm control <ul style="list-style-type: none"> ● Packet / Sec: storm control rate calculates by packet-based ● Kbits / Sec: storm control rate calculates by octet-based.
IFG	Select the rate calculates w/o preamble & IFG (20 bytes) <ul style="list-style-type: none"> ● Excluded: exclude preamble & IFG (20 bytes) when count ingress storm control rate.

	<ul style="list-style-type: none"> ● Included: include preamble & IFG (20 bytes) when count ingress storm control rate.
--	--

Click "Edit" button to view Edit Port Setting menu.

Edit Port Setting

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

Figure 103 - Security > Storm Control > Edit Port Setting

Item	Description
Port	Select the setting ports.
State	Select the state of setting Enable: Enable the storm control function.
Broadcast	Enable: Enable the storm control function of Broadcast packet. Value of storm control rate, Unit: pps (packet per-second, range 1- 262143) or Kbps (Kbits per-second, range16 - 1000000) depends on global mode setting.
Unknown Multicast	Enable: Enable the storm control function of Unknown multicast packet. Value of storm control rate, Unit: pps (packet per-second, range 1- 262143) or Kbps (Kbits per-second, range16 - 1000000) depends on global mode setting.
Unknown Unicast	Enable: Enable the storm control function of Unknown unicast packet. Value of storm control rate, Unit: pps (packet per-second, range 1 - 262143) or Kbps (Kbits per-second, range16 - 1000000) depends on global mode setting.
Action	Select the state of setting <ul style="list-style-type: none"> ● Drop: Packets exceed storm control rate will be dropped. ● Shutdown: Port will be shutdown when packets exceed storm control rate.

IV-9-7 DoS

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

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

IV-9-7-1 Property

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 <input type="text" value="512"/> Byte (0 - 65535, default 512)
TCP Min Hdr size	<input checked="" type="checkbox"/> Enable <input type="text" value="20"/> Byte (0 - 31, default 20)
IPv6 Min Fragment	<input checked="" type="checkbox"/> Enable <input type="text" value="1240"/> Byte (0 - 65535, default 1240)
Smurf Attack	<input checked="" type="checkbox"/> Enable <input type="text" value="0"/> Netmask Length (0 - 32, default 0)

Figure 104 - Security > DoS > Property

Item	Description
POD	Avoids ping of death attack.
Land	Drops the packets if the source IP address is equal to the destination IP address.
UDP Blat	Drops the packets if the UDP source port equals to the UDP

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

IV-9-7-2 Port Setting

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

Port Setting Table

Q

<input type="checkbox"/>	Entry	Port	State
<input type="checkbox"/>	1	GE1	Disabled
<input type="checkbox"/>	2	GE2	Disabled
<input type="checkbox"/>	3	GE3	Disabled
<input type="checkbox"/>	4	GE4	Disabled
<input type="checkbox"/>	5	GE5	Disabled
<input type="checkbox"/>	6	GE6	Disabled
<input type="checkbox"/>	7	GE7	Disabled
<input type="checkbox"/>	8	GE8	Disabled
<input type="checkbox"/>	9	GE9	Disabled
<input type="checkbox"/>	10	GE10	Disabled
<input type="checkbox"/>	11	GE11	Disabled
<input type="checkbox"/>	12	GE12	Disabled
<input type="checkbox"/>	13	GE13	Disabled
<input type="checkbox"/>	14	GE14	Disabled
<input type="checkbox"/>	15	GE15	Disabled
<input type="checkbox"/>	16	GE16	Disabled
<input type="checkbox"/>	17	GE17	Disabled
<input type="checkbox"/>	18	GE18	Disabled
<input type="checkbox"/>	19	GE19	Disabled
<input type="checkbox"/>	20	GE20	Disabled
<input type="checkbox"/>	21	GE21	Disabled
<input type="checkbox"/>	22	GE22	Disabled
<input type="checkbox"/>	23	GE23	Disabled
<input type="checkbox"/>	24	GE24	Disabled
<input type="checkbox"/>	25	GE25	Disabled
<input type="checkbox"/>	26	GE26	Disabled
<input type="checkbox"/>	27	GE27	Disabled
<input type="checkbox"/>	28	GE28	Disabled

Figure 105 - Security > DoS > Port Setting

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

IV-9-8 DHCP Snooping

Use the DHCP Snooping pages to configure settings of DHCP Snooping.

IV-9-8-1 Property

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

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

State Enable

Available VLAN Selected VLAN

VLAN 1

VLAN

Apply

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
<input type="checkbox"/> 9	GE9	Disabled	Disabled	Unlimited
<input type="checkbox"/> 10	GE10	Disabled	Disabled	Unlimited
<input type="checkbox"/> 11	GE11	Disabled	Disabled	Unlimited
<input type="checkbox"/> 12	GE12	Disabled	Disabled	Unlimited
<input type="checkbox"/> 13	GE13	Disabled	Disabled	Unlimited
<input type="checkbox"/> 14	GE14	Disabled	Disabled	Unlimited
<input type="checkbox"/> 15	GE15	Disabled	Disabled	Unlimited
<input type="checkbox"/> 16	GE16	Disabled	Disabled	Unlimited
<input type="checkbox"/> 17	GE17	Disabled	Disabled	Unlimited
<input type="checkbox"/> 18	GE18	Disabled	Disabled	Unlimited
<input type="checkbox"/> 19	GE19	Disabled	Disabled	Unlimited

Figure 106 - Security > DHCP Snooping > Property

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

Click "**Edit**" button to view Edit Port Setting menu.

Figure 107 - Security > DHCP Snooping > Property > Edit Port Setting

Item	Description
Port	Display selected port to be edited
Trust	Set checkbox to enable/disabled trust of interface. All DHCP packet will be forward directly if enable trust. Default is disabled.
Verify Chaddr	Set checkbox to enable or disable chaddr validation of interface. All DHCP packets will be checked whether client hardware mac address is same as source mac in Ethernet header if enable chaddr validation. Default is disabled.
Rate Limit	Input rate limitation of DHCP packets. The unit is pps. 0 means unlimited. Default is unlimited.

IV-9-8-2 Statistics

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

To view the Statistics menu, navigate to **Security > DHCP Snooping > Statistics**.

Statistics Table

<input type="checkbox"/>	Entry	Port	Forward	Chaddr Check Drop	Untrust Port Drop	Untrust Port with Option82 Drop	Invalid Drop
<input type="checkbox"/>	1	GE1	0	0	0	0	0
<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
<input type="checkbox"/>	8	GE8	0	0	0	0	0
<input type="checkbox"/>	9	GE9	0	0	0	0	0
<input type="checkbox"/>	10	GE10	0	0	0	0	0
<input type="checkbox"/>	11	GE11	0	0	0	0	0
<input type="checkbox"/>	12	GE12	0	0	0	0	0
<input type="checkbox"/>	13	GE13	0	0	0	0	0
<input type="checkbox"/>	14	GE14	0	0	0	0	0
<input type="checkbox"/>	15	GE15	0	0	0	0	0
<input type="checkbox"/>	16	GE16	0	0	0	0	0
<input type="checkbox"/>	17	GE17	0	0	0	0	0
<input type="checkbox"/>	18	GE18	0	0	0	0	0
<input type="checkbox"/>	19	GE19	0	0	0	0	0
<input type="checkbox"/>	20	GE20	0	0	0	0	0
<input type="checkbox"/>	21	GE21	0	0	0	0	0
<input type="checkbox"/>	22	GE22	0	0	0	0	0
<input type="checkbox"/>	23	GE23	0	0	0	0	0
<input type="checkbox"/>	24	GE24	0	0	0	0	0
<input type="checkbox"/>	25	GE25	0	0	0	0	0
<input type="checkbox"/>	26	GE26	0	0	0	0	0
<input type="checkbox"/>	27	GE27	0	0	0	0	0
<input type="checkbox"/>	28	GE28	0	0	0	0	0
<input type="checkbox"/>	29	LAG1	0	0	0	0	0

Figure 108 - Security > DHCP Snooping > Statistics

Item	Description
Port	Display port ID.
Forwarded	Display how many packets forwarded normally.

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

IV-9-8-3 Option82 Property

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

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

The screenshot displays the configuration interface for DHCP Option82. At the top, there is a 'Remote ID' section with a 'User Defined' checkbox and an empty text input field. Below this is the 'Operational Status' section, which shows the current Remote ID as '74:da:38:17:6e:7a (Switch Mac in Byte Order)'. An 'Apply' button is located below the status section. The main part of the page is the 'Port Setting Table', which is a table with 22 rows and 5 columns: Entry, Port, State, and Allow Untrust. All ports (GE1 to GE22) are currently 'Disabled' and set to 'Drop'.

Entry	Port	State	Allow Untrust
1	GE1	Disabled	Drop
2	GE2	Disabled	Drop
3	GE3	Disabled	Drop
4	GE4	Disabled	Drop
5	GE5	Disabled	Drop
6	GE6	Disabled	Drop
7	GE7	Disabled	Drop
8	GE8	Disabled	Drop
9	GE9	Disabled	Drop
10	GE10	Disabled	Drop
11	GE11	Disabled	Drop
12	GE12	Disabled	Drop
13	GE13	Disabled	Drop
14	GE14	Disabled	Drop
15	GE15	Disabled	Drop
16	GE16	Disabled	Drop
17	GE17	Disabled	Drop
18	GE18	Disabled	Drop
19	GE19	Disabled	Drop
20	GE20	Disabled	Drop
21	GE21	Disabled	Drop
22	GE22	Disabled	Drop

Figure 109 - Security > DHCP Snooping > Option82 Property

Item	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.
Port Setting Table	
Port	Display port ID.
State	Display option82 enable/disable status of interface.
Allow untrusted	Display allow untrusted action of interface.

Click "Edit" button to view Edit Port Setting menu.

Figure 110 - DHCP Snooping > Option82 Property > Edit Port Setting

Item	Description
Port	Display selected port to be edited
State	Set checkbox to enable/disable option82 function of interface.
Allow untrusted	Select the action perform when untrusted port receive DHCP packet has option82 filed. Default is drop. <ul style="list-style-type: none"> ● Keep: Keep original option82 content. ● Replace: Replace option82 content by switch setting ● Drop: Drop packets with option82

IV-9-8-4 Option82 Circuit ID

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

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

Figure 111 - Security > DHCP Snooping > Option82 Circuit ID

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

Click **"Add"** button or **"Edit"** button to view the Add/Edit Option82 Circuit ID menu.

Figure 112 - Security > DHCP Snooping > Option82 Circuit ID > Add/Edit Option82 Circuit ID

Item	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.

IV-9-9 IP Source Guard

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

IV-9-9-1 Port Setting

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

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

Port Setting Table

Q

<input type="checkbox"/>	Entry	Port	State	Verify Source	Current Entry	Max Entry
<input type="checkbox"/>	1	GE1	Disabled	IP	0	Unlimited
<input type="checkbox"/>	2	GE2	Disabled	IP	0	Unlimited
<input type="checkbox"/>	3	GE3	Disabled	IP	0	Unlimited
<input type="checkbox"/>	4	GE4	Disabled	IP	0	Unlimited
<input type="checkbox"/>	5	GE5	Disabled	IP	0	Unlimited
<input type="checkbox"/>	6	GE6	Disabled	IP	0	Unlimited
<input type="checkbox"/>	7	GE7	Disabled	IP	0	Unlimited
<input type="checkbox"/>	8	GE8	Disabled	IP	0	Unlimited
<input type="checkbox"/>	9	GE9	Disabled	IP	0	Unlimited
<input type="checkbox"/>	10	GE10	Disabled	IP	0	Unlimited
<input type="checkbox"/>	11	GE11	Disabled	IP	0	Unlimited
<input type="checkbox"/>	12	GE12	Disabled	IP	0	Unlimited
<input type="checkbox"/>	13	GE13	Disabled	IP	0	Unlimited
<input type="checkbox"/>	14	GE14	Disabled	IP	0	Unlimited
<input type="checkbox"/>	15	GE15	Disabled	IP	0	Unlimited
<input type="checkbox"/>	16	GE16	Disabled	IP	0	Unlimited
<input type="checkbox"/>	17	GE17	Disabled	IP	0	Unlimited
<input type="checkbox"/>	18	GE18	Disabled	IP	0	Unlimited
<input type="checkbox"/>	19	GE19	Disabled	IP	0	Unlimited
<input type="checkbox"/>	20	GE20	Disabled	IP	0	Unlimited
<input type="checkbox"/>	21	GE21	Disabled	IP	0	Unlimited
<input type="checkbox"/>	22	GE22	Disabled	IP	0	Unlimited
<input type="checkbox"/>	23	GE23	Disabled	IP	0	Unlimited
<input type="checkbox"/>	24	GE24	Disabled	IP	0	Unlimited
<input type="checkbox"/>	25	GE25	Disabled	IP	0	Unlimited
<input type="checkbox"/>	26	GE26	Disabled	IP	0	Unlimited
<input type="checkbox"/>	27	GE27	Disabled	IP	0	Unlimited
<input type="checkbox"/>	28	GE28	Disabled	IP	0	Unlimited
<input type="checkbox"/>	29	LAG1	Disabled	IP	0	Unlimited
<input type="checkbox"/>	30	LAG2	Disabled	IP	0	Unlimited
<input type="checkbox"/>	31	LAG3	Disabled	IP	0	Unlimited

Figure 113 Security > IP Source Guard > Port Setting

Item	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.

Click "**Edit**" button to view the Edit Port Setting menu.

Figure 114 - Security > IP Source Guard > Port Setting > Edit Port Setting

Item	Description
Port	Display selected port to be edited.
Status	Set checkbox to enable or disable IP Source Guard function. Default is disabled.
Verify Source	Select the mode of IP Source Guard verification <ul style="list-style-type: none"> ● IP: Only verify source IP address of packet. ● IP-MAC: Verify source IP and source MAC address of packet.
Max 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.

IV-9-9-2 IMPV Binding

This page allows 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.

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

The screenshot shows a web interface for managing IP-MAC-Port-VLAN Binding. At the top, it says "IP-MAC-Port-VLAN Binding Table". Below this, there is a search bar and a dropdown menu set to "All" entries. The text "Showing 0 to 0 of 0 entries" is displayed. A table with the following columns is shown: Port, VLAN, MAC Address, IP Address, Binding, Type, and Lease Time. Below the table, it says "0 results found." At the bottom, there are buttons for "Add", "Edit", "Delete", "First", "Previous", "Next", and "Last".

Figure 115 - Security > IP Source Guard > IMPV Binding

Item	Description
Port	Display port ID of entry.
VLAN	Display VLAN ID of entry.
MAC Address	Display MAC address of entry. Only available of IP-MAC binding entry.
IP Address	Display IP address of entry. Mask always to be 255.255.255.255 for IP-MAC binding. IP binding entry display user input.
Binding	Display binding type of entry.
Type	Type of existing binding entry <ul style="list-style-type: none"> ● Static: Entry added by user. ● Dynamic: Entry learned by DHCP snooping.
Lease Time	Lease time of DHCP Snooping learned entry. After lease time entry will be deleted. Only available of dynamic entry.

Click "Add" or "Edit" button to view the Add/Edit IP-MAC-Port-VLAN Binding menu.

Add IP-MAC-Port-VLAN Binding

Port	GE1 ▾
VLAN	<input type="text" value=""/> (1 - 4094)
Binding	<input checked="" type="radio"/> IP-MAC-Port-VLAN <input type="radio"/> IP-Port-VLAN
MAC Address	<input type="text" value=""/>
IP Address	<input type="text" value=""/> / <input type="text" value="255.255.255.255"/>

Edit IP-MAC-Port-VLAN Binding

Port	GE1 ▾
VLAN	20
Binding	IP-MAC-Port-VLAN
MAC Address	00:11:22:33:44:55
IP Address	<input type="text" value="192.168.2.33"/> / <input type="text" value="255.255.255.255"/>

Figure 116 - Security > IP Source Guard > Add/Edit IP-MAC-Port-VLAN Binding

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

IV-9-9-3 Save Database

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

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

Figure 117 - Security > IP Source Guard > Save Database

Item	Description
Type	Select the type of database agent. <ul style="list-style-type: none"> ● None: Disable database agent service. ● Flash: Save DHCP dynamic binding entries to flash. ● TFTP: Save DHCP dynamic binding entries to remote TFTP server.
Filename	Input filename for backup file. Only available when selecting type "flash" and "TFTP".
Address Type	Select the type of TFTP server. <ul style="list-style-type: none"> ● Hostname: TFTP server address is hostname. ● IPv4: TFTP server address is IPv4 address ● IPv6: TFTP server address is IPv6 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.

IV-10 ACL

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

IV-10-1 MAC ACL

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

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

ACL Name

Apply

ACL Table

Showing All entries Showing 0 to 0 of 0 entries

ACL Name Rule Port

0 results found.

First Previous 1 Next Last

Delete

Figure 118 - ACL > MAC ACL

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

IV-10-2 MAC ACE

This page allows 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.

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

Figure 119 - ACL > MAC ACE

Item	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.

Click **“Edit”** button to view the Edit ACE menu.

Figure 120 - ACL > Edit ACE

Item	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. <ul style="list-style-type: none"> ● Permit: Forward packets that meet the ACE criteria. ● Deny: Drop packets that meet the ACE criteria. ● Shutdown: Drop packets that meet the ACE criteria, and disable the port from where the packets were received. Such ports can be reactivated from the Port Settings page.
Source MAC	Select the type for source MAC address. <ul style="list-style-type: none"> ● Any: All source addresses are acceptable. ● User Defined: Only a source address or a range of source addresses which users define are acceptable. Enter the source MAC address and mask to which will be matched.
Destination MAC	Select the type for Destination MAC address.

	<ul style="list-style-type: none"> ● Any: All destination addresses are acceptable. ● User Defined: Only a destination address or a range of destination addresses which users define are acceptable. Enter the destination MAC address and mask to which will be matched.
Ethertype	<p>Select the type for Ethernet frame type.</p> <ul style="list-style-type: none"> ● Any: All Ethernet frame type is acceptable. ● User Defined: Only an Ethernet frame type which users define is acceptable. Enter the Ethernet frame type value to which will be matched.
VLAN	<p>Select the type for VLAN ID.</p> <ul style="list-style-type: none"> ● Any: All VLAN ID is acceptable. ● User Defined: Only a VLAN ID which users define is acceptable. Enter the VLAN ID to which will be matched.
802.1p	<p>Select the type for 802.1p value.</p> <ul style="list-style-type: none"> ● Any: All 802.1p value is acceptable. ● User Defined: Only an 802.1p value or a range of 802.1p value which users define is acceptable. Enter the 802.1p value and mask to which will be matched.

IV-10-3 IPv4 ACL

This page allows user to add or delete IPv4 ACL rule. A rule cannot be deleted if under binding.

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

Figure 121 - ACL > IPv4 ACL

Item	Description
ACL Name	Input IPv4 ACL name.
ACL Name	Display IPv4 ACL name.
Rule	Display the number ACE rule of ACL.
Port	Display the port list that bind this ACL.

IV-10-4 IPv4 ACE

This page allows 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.

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

The screenshot shows the 'ACE Table' interface. At the top, there is a search bar and a filter for 'ACL Name' set to 'None'. Below that, it says 'Showing All entries' and 'Showing 0 to 0 of 0 entries'. The table has the following columns: Sequence, Action, Protocol, Source IP (Address, Mask), Destination IP (Address, Mask), Source Port, Destination Port, TCP Flags, Type of Service (DSCP, IP Precedence), and ICMP (Type, Code). The table is currently empty, displaying '0 results found.' and navigation buttons for 'First', 'Previous', '1', 'Next', and 'Last'.

Figure 122 - ACL > IPv4 ACE

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

Click "Add" or "Edit" button to view the Add/Edit ACE menu.

Edit ACE

ACL Name	777
Sequence	888
Action	<input checked="" type="radio"/> Permit <input type="radio"/> Deny <input type="radio"/> Shutdown
Protocol	<input checked="" type="radio"/> Any <input type="radio"/> Select <input type="text" value="ICMP"/> <input type="radio"/> Define <input type="text" value=""/> (0 - 255)
Source IP	<input checked="" type="checkbox"/> Any <input type="text" value=""/> / <input type="text" value=""/> (Address / Mask)
Destination IP	<input checked="" type="checkbox"/> Any <input type="text" value=""/> / <input type="text" value=""/> (Address / Mask)
Type of Service	<input checked="" type="radio"/> Any <input type="radio"/> DSCP <input type="text" value=""/> (0 - 63) <input type="radio"/> IP Precedence <input type="text" value=""/> (0 - 7)
Source Port	<input checked="" type="radio"/> Any <input type="radio"/> Single <input type="text" value=""/> (0 - 65535) <input type="radio"/> Range <input type="text" value=""/> - <input type="text" value=""/> (0 - 65535)
Destination Port	<input checked="" type="radio"/> Any <input type="radio"/> Single <input type="text" value=""/> (0 - 65535) <input type="radio"/> Range <input type="text" value=""/> - <input type="text" value=""/> (0 - 65535)
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 <input type="text" value="Echo Reply"/> <input type="radio"/> Define <input type="text" value=""/> (0 - 255)
ICMP Code	<input checked="" type="radio"/> Any <input type="radio"/> Define <input type="text" value=""/> (0 - 255)

Figure 123 - ACL > Add/Edit ACE

Item	Description
ACL Name	Display the ACL name to which an ACE is being added.
Sequence	Specify the sequence of the ACE. ACEs with higher sequence are processed first (1 is the highest sequence). Only available on Add dialog.
Action	Select the action for a match. <ul style="list-style-type: none"> ● Permit: Forward packets that meet the ACE criteria. ● Deny: Drop packets that meet the ACE criteria. ● Shutdown: Drop packets that meet the ACE criteria, and disable the port from where the packets were received. Such ports can be reactivated from the Port Settings page.
Protocol	Select the type of protocol for a match. <ul style="list-style-type: none"> ● Any (IP): All IP protocols are acceptable. ● Select from list: Select one of the following protocols from the drop-down list. ICMP/IPinIP/TCP/EGP/IGP/UDP/HMP/RDP/IPV6/IPV6:ROUT/IPV6:F RAG/ RSVP/IPV6:ICMP/OSPF/PIM/L2TP ● Protocol ID to match: Enter the protocol ID.
Source IP	Select the type for source IP address. <ul style="list-style-type: none"> ● Any: All source addresses are acceptable. ● User Defined: Only a source address or a range of source addresses which users define are acceptable. Enter the source IP address value and mask to which will be matched.
Destination IP	Select the type for destination IP address. <ul style="list-style-type: none"> ● Any: All destination addresses are acceptable. ● User Defined: Only a destination address or a range of destination addresses which users define are acceptable. Enter the destination IP address value and mask to which will be matched.
Source Port	Select the type of protocol for a match. Only available when protocol is TCP or UDP. <ul style="list-style-type: none"> ● Any: All source ports are acceptable. ● Single: Enter a single TCP/UDP source port to which packets are matched. ● Range: Select a range of TCP/UDP source ports to which the packet is matched. There are eight different port ranges that can be configured (shared between source and destination ports). TCP and UDP protocols each have eight port ranges.
Destination Port	Select the type of protocol for a match. Only available when protocol is TCP or UDP. <ul style="list-style-type: none"> ● Any: All source ports are acceptable. ● Single: Enter a single TCP/UDP source port to which packets are matched. ● Range: Select a range of TCP/UDP source ports to which the packet is matched. There are eight different port ranges that can be

	configured (shared between source and destination ports). TCP and UDP protocols each have eight port ranges.
TCP Flags	Select one or more TCP flags with which to filter packets. Filtered packets are either forwarded or dropped. Filtering packets by TCP flags increases packet control, which increases network security. Only available when protocol is TCP.
Type of Service	Select the type of service for a match. <ul style="list-style-type: none"> ● Any: All types of service are acceptable. ● DSCP to match: Enter a Differentiated Services Code Point (DSCP) to match. ● IP Precedence to match: Enter a IP Precedence to match.
ICMP Type	Either select the message type by name or enter the message type number. Only available when protocol is ICMP. <ul style="list-style-type: none"> ● Any: All message types are acceptable. ● Select from list: Select message type by name. ● Protocol ID to match: Enter the number of message type.
ICMP Code	Select the type for ICMP code. Only available when protocol is ICMP. <ul style="list-style-type: none"> ● Any: All codes are acceptable. ● User Defined: Enter an ICMP code to match.

IV-10-5 ACL Binding

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

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

The screenshot shows the 'ACL Binding Table' interface. At the top right, there is a search icon and a search input field. The table below has the following structure:

Entry	Port	MAC ACL	IPv4 ACL
<input type="checkbox"/>	1	GE1	
<input type="checkbox"/>	2	GE2	
<input type="checkbox"/>	3	GE3	
<input type="checkbox"/>	4	GE4	
<input type="checkbox"/>	5	GE5	
<input type="checkbox"/>	6	GE6	
<input type="checkbox"/>	7	GE7	
<input type="checkbox"/>	8	GE8	
<input type="checkbox"/>	9	GE9	
<input type="checkbox"/>	10	GE10	
<input type="checkbox"/>	11	GE11	
<input type="checkbox"/>	12	GE12	
<input type="checkbox"/>	13	GE13	
<input type="checkbox"/>	14	GE14	
<input type="checkbox"/>	15	GE15	
<input type="checkbox"/>	16	GE16	
<input type="checkbox"/>	17	GE17	
<input type="checkbox"/>	18	GE18	
<input type="checkbox"/>	19	GE19	
<input type="checkbox"/>	20	GE20	
<input type="checkbox"/>	21	GE21	
<input type="checkbox"/>	22	GE22	
<input type="checkbox"/>	23	GE23	
<input type="checkbox"/>	24	GE24	
<input type="checkbox"/>	25	GE25	
<input type="checkbox"/>	26	GE26	
<input type="checkbox"/>	27	GE27	
<input type="checkbox"/>	28	GE28	
<input type="checkbox"/>	29	LAG1	
<input type="checkbox"/>	30	LAG2	
<input type="checkbox"/>	31	LAG3	
<input type="checkbox"/>	32	LAG4	
<input type="checkbox"/>	33	LAG5	
<input type="checkbox"/>	34	LAG6	
<input type="checkbox"/>	35	LAG7	
<input type="checkbox"/>	36	LAG8	

Below the table, there are three buttons: 'Bind', 'Unbind', and 'Edit'.

Figure 124 - ACL > ACL Binding

Item	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.

Click “**Edit**” button to view the Edit ACL Binding menu.

Edit ACL Binding

Port GE1
Note: ACL without any rules cannot be bound

MAC ACL None ▼

IPv4 ACL None ▼

Apply Close

Figure 125 - ACL > Edit ACL Binding

Item	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.

IV-11 QoS

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

IV-11-1 General

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

IV-11-1-1 Property

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

State Enable
Trust Mode CoS IP Precedence

Port Setting Table

Entry	Port	CoS	Trust	Remarking		
				CoS	IP Precedence	
<input type="checkbox"/>	1	GE1	0	Enabled	Disabled	Disabled
<input type="checkbox"/>	2	GE2	0	Enabled	Disabled	Disabled
<input type="checkbox"/>	3	GE3	0	Enabled	Disabled	Disabled
<input type="checkbox"/>	4	GE4	0	Enabled	Disabled	Disabled
<input type="checkbox"/>	5	GE5	0	Enabled	Disabled	Disabled
<input type="checkbox"/>	6	GE6	0	Enabled	Disabled	Disabled
<input type="checkbox"/>	7	GE7	0	Enabled	Disabled	Disabled
<input type="checkbox"/>	8	GE8	0	Enabled	Disabled	Disabled
<input type="checkbox"/>	9	GE9	0	Enabled	Disabled	Disabled
<input type="checkbox"/>	10	GE10	0	Enabled	Disabled	Disabled
<input type="checkbox"/>	11	GE11	0	Enabled	Disabled	Disabled
<input type="checkbox"/>	12	GE12	0	Enabled	Disabled	Disabled
<input type="checkbox"/>	13	GE13	0	Enabled	Disabled	Disabled
<input type="checkbox"/>	14	GE14	0	Enabled	Disabled	Disabled
<input type="checkbox"/>	15	GE15	0	Enabled	Disabled	Disabled
<input type="checkbox"/>	16	GE16	0	Enabled	Disabled	Disabled
<input type="checkbox"/>	17	GE17	0	Enabled	Disabled	Disabled
<input type="checkbox"/>	18	GE18	0	Enabled	Disabled	Disabled
<input type="checkbox"/>	19	GE19	0	Enabled	Disabled	Disabled
<input type="checkbox"/>	20	GE20	0	Enabled	Disabled	Disabled
<input type="checkbox"/>	21	GE21	0	Enabled	Disabled	Disabled
<input type="checkbox"/>	22	GE22	0	Enabled	Disabled	Disabled
<input type="checkbox"/>	23	GE23	0	Enabled	Disabled	Disabled
<input type="checkbox"/>	24	GE24	0	Enabled	Disabled	Disabled
<input type="checkbox"/>	25	GE25	0	Enabled	Disabled	Disabled
<input type="checkbox"/>	26	GE26	0	Enabled	Disabled	Disabled
<input type="checkbox"/>	27	GE27	0	Enabled	Disabled	Disabled
<input type="checkbox"/>	28	GE28	0	Enabled	Disabled	Disabled
<input type="checkbox"/>	29	LAG1	0	Enabled	Disabled	Disabled
<input type="checkbox"/>	30	LAG2	0	Enabled	Disabled	Disabled
<input type="checkbox"/>	31	LAG3	0	Enabled	Disabled	Disabled
<input type="checkbox"/>	32	LAG4	0	Enabled	Disabled	Disabled
<input type="checkbox"/>	33	LAG5	0	Enabled	Disabled	Disabled
<input type="checkbox"/>	34	LAG6	0	Enabled	Disabled	Disabled
<input type="checkbox"/>	35	LAG7	0	Enabled	Disabled	Disabled
<input type="checkbox"/>	36	LAG8	0	Enabled	Disabled	Disabled

Figure 126 - QoS > General > Property

Item	Description
State	Set checkbox to enable/disable QoS.
Trust	Select QoS trust mode <ul style="list-style-type: none"> ● CoS: Traffic is mapped to queues based on the CoS field in the VLAN tag, or based on the per-port default CoS value (if there is no VLAN tag on the incoming packet), the actual mapping of the CoS to queue can be configured on port setting dialog. ● IP Precedence: Traffic is mapped to queues based on the IP precedence. The actual mapping of the IP precedence to queue can be configured on the IP Precedence mapping page.

Port Setting Table	
Port	Port name
CoS	Port default CoS priority value for the selected ports.
Trust	Port trust state <ul style="list-style-type: none"> ● Enabled: Traffic will follow trust mode in global setting ● Disabled: Traffic will always use best efforts
Remarking (CoS)	Set checkbox to enable/disable port CoS remarking. <ul style="list-style-type: none"> ● Enabled: CoS remarking is enabled ● Disabled: CoS remarking is disabled
Remarking (IP Precedence)	Set checkbox to enable/disable port IP Precedence remarking. <ul style="list-style-type: none"> ● Enabled: DSCP remarking is enabled ● Disabled: DSCP remarking is disabled

Click "**Edit**" button to view the Edit Port Setting menu.

Figure 127 - Qos > General > Property

Item	Description
Port	Selected 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 (IP Precedence)	Set checkbox to enable/disable port IP Precedence remarking.

IV-11-1-2 Queue Scheduling

The switch supports eight queues for each interface. Queue number 8 is the highest priority queue.

Queue number 1 is the lowest priority queue. There are two ways of determining how traffic in queues is handled, Strict Priority (SP) and Weighted Round Robin (WRR).

- **Strict Priority (SP)**—Egress traffic from the highest priority queue is transmitted first. Traffic from the lower queues is processed only after the highest queue has been transmitted, which provide the highest level of priority of traffic to the highest numbered queue.
- **Weighted Round Robin (WRR)**—In WRR mode the number of packets sent from the queue is proportional to the weight of the queue (the higher the weight, the more frames are sent).

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

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

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

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

Apply

Figure 128 - QoS > General > Queue Scheduling

Item	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.

IV-11-1-3 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.

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

CoS to Queue Mapping

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

Queue to CoS Mapping

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

Figure 129 - QoS > General > Cos Mapping

Item	Description
CoS to Queue Mapping	
CoS	CoS value.
Queue	Select queue id for the CoS value.
Queue to CoS Mapping	
Queue	Queue ID
CoS	Select CoS value for the queue id.

IV-11-1-4 IP Precedence Mapping

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

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

IP Precedence to Queue Mapping

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

Queue to IP Precedence Mapping

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

Figure 130 - QoS > General > IP Precedence Mapping

Item	Description
IP Precedence to Queue Mapping	
IP Precedence	IP Precedence value.
Queue	Queue value which IP Precedence is mapped.
Queue to IP Precedence Mapping	
Queue	Queue ID.
IP Precedence	IP Precedence value which queue is mapped.

IV-11-2 Rate Limit

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

IV-11-2-1 Ingress/Egress Port

This page allows 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.

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

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	
<input type="checkbox"/>	11	GE11	Disabled		Disabled	
<input type="checkbox"/>	12	GE12	Disabled		Disabled	
<input type="checkbox"/>	13	GE13	Disabled		Disabled	
<input type="checkbox"/>	14	GE14	Disabled		Disabled	
<input type="checkbox"/>	15	GE15	Disabled		Disabled	
<input type="checkbox"/>	16	GE16	Disabled		Disabled	
<input type="checkbox"/>	17	GE17	Disabled		Disabled	
<input type="checkbox"/>	18	GE18	Disabled		Disabled	
<input type="checkbox"/>	19	GE19	Disabled		Disabled	
<input type="checkbox"/>	20	GE20	Disabled		Disabled	
<input type="checkbox"/>	21	GE21	Disabled		Disabled	
<input type="checkbox"/>	22	GE22	Disabled		Disabled	
<input type="checkbox"/>	23	GE23	Disabled		Disabled	
<input type="checkbox"/>	24	GE24	Disabled		Disabled	
<input type="checkbox"/>	25	GE25	Disabled		Disabled	
<input type="checkbox"/>	26	GE26	Disabled		Disabled	
<input type="checkbox"/>	27	GE27	Disabled		Disabled	
<input type="checkbox"/>	28	GE28	Disabled		Disabled	

Q

Figure 131 - QoS > Rate Limit > Ingress / Egress Port

Item	Description
Port	Port name.
Ingress (State)	Port ingress rate limit state <ul style="list-style-type: none"> ● Enabled: Ingress rate limit is enabled ● Disabled: Ingress rate limit is disabled
Ingress (Rate)	Port ingress rate limit value if ingress rate state is enabled.
IP Precedence	IP Precedence value which queue is mapped.
Egress (State)	Port egress rate limit state

	<ul style="list-style-type: none"> ● Enabled: Egress rate limit is enabled ● Disabled: Egress rate limit is disabled
Egress (Rate)	Port egress rate limit value if egress rate state is enabled.

Click "**Edit**" button to view the Ingress / Egress Port menu.

The screenshot shows a configuration window titled "Edit Ingress / Egress Port". The window contains a form with the following fields:

- Port:** GE1
- Ingress:**
 - Enable:
 - Rate Limit: 1000000 Kbps (16 - 1000000)
- Egress:**
 - Enable:
 - Rate Limit: 1000000 Kbps (16 - 1000000)

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

Figure 132 - QoS > Rate Limit > Ingress / Egress Port

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

IV-12 Diagnostics

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

IV-12-1 Logging

IV-12-1-1 Property

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

The screenshot shows the configuration interface for logging services. It is organized into four main sections, each with a title bar and two sub-sections: 'State' and 'Minimum Severity'.
 1. **Global Logging**: The 'State' checkbox is checked, labeled 'Enable'.
 2. **Console Logging**: The 'State' checkbox is checked, labeled 'Enable'. The 'Minimum Severity' dropdown is set to 'Notice'. A note below reads: 'Note: Emergency, Alert, Critical, Error, Warning, Notice'.
 3. **RAM Logging**: The 'State' checkbox is checked, labeled 'Enable'. The 'Minimum Severity' dropdown is set to 'Notice'. A note below reads: 'Note: Emergency, Alert, Critical, Error, Warning, Notice'.
 4. **Flash Logging**: The 'State' checkbox is unchecked, labeled 'Enable'. The 'Minimum Severity' dropdown is set to 'Notice'. A note below reads: 'Note: Emergency, Alert, Critical, Error, Warning, Notice'.
 At the bottom of the form is an 'Apply' button.

Figure 133 - Diagnostics > Logging > Property

Item	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.
Console Logging	
State	Enable/Disable the console logging service
Minimum Severity	The minimum severity for the console logging.
RAM Logging	
State	Enable/Disable the RAM logging service.
Minimum Severity	The minimum severity for the RAM logging.
Flash Logging	

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

IV-12-1-2 Remote Server

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

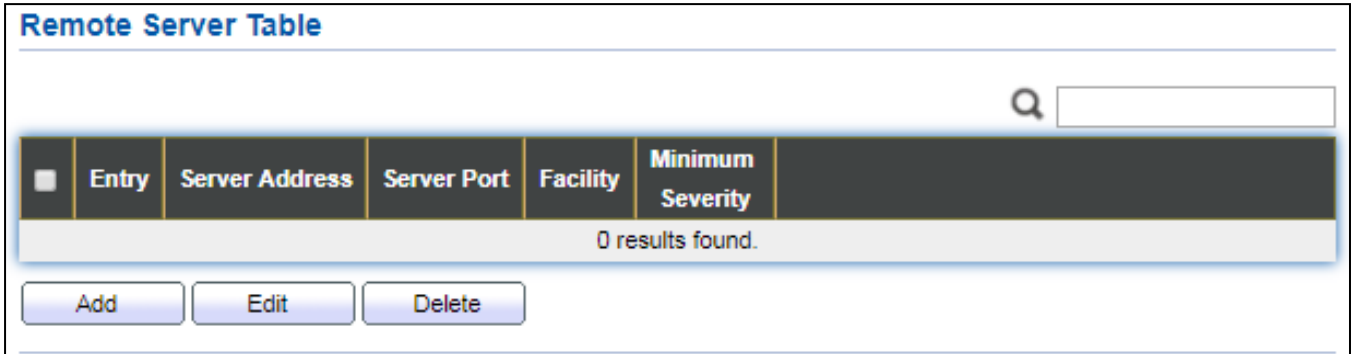


Figure 134 - Diagnostics > Logging > Remote Server

Item	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.
Minimum Severity	<ul style="list-style-type: none"> ● Emergence: System is not usable. ● Alert: Immediate action is needed. ● Critical: System is in the critical condition. ● Error: System is in error condition ● Warning: System warning has occurred ● Notice: System is functioning properly, but a system notice has occurred. ● Informational: Device information. ● Debug: Provides detailed information about an event.

IV-12-2 Mirroring

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

Mirroring Table

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

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

Figure 135 - Diagnostics > Mirroring

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

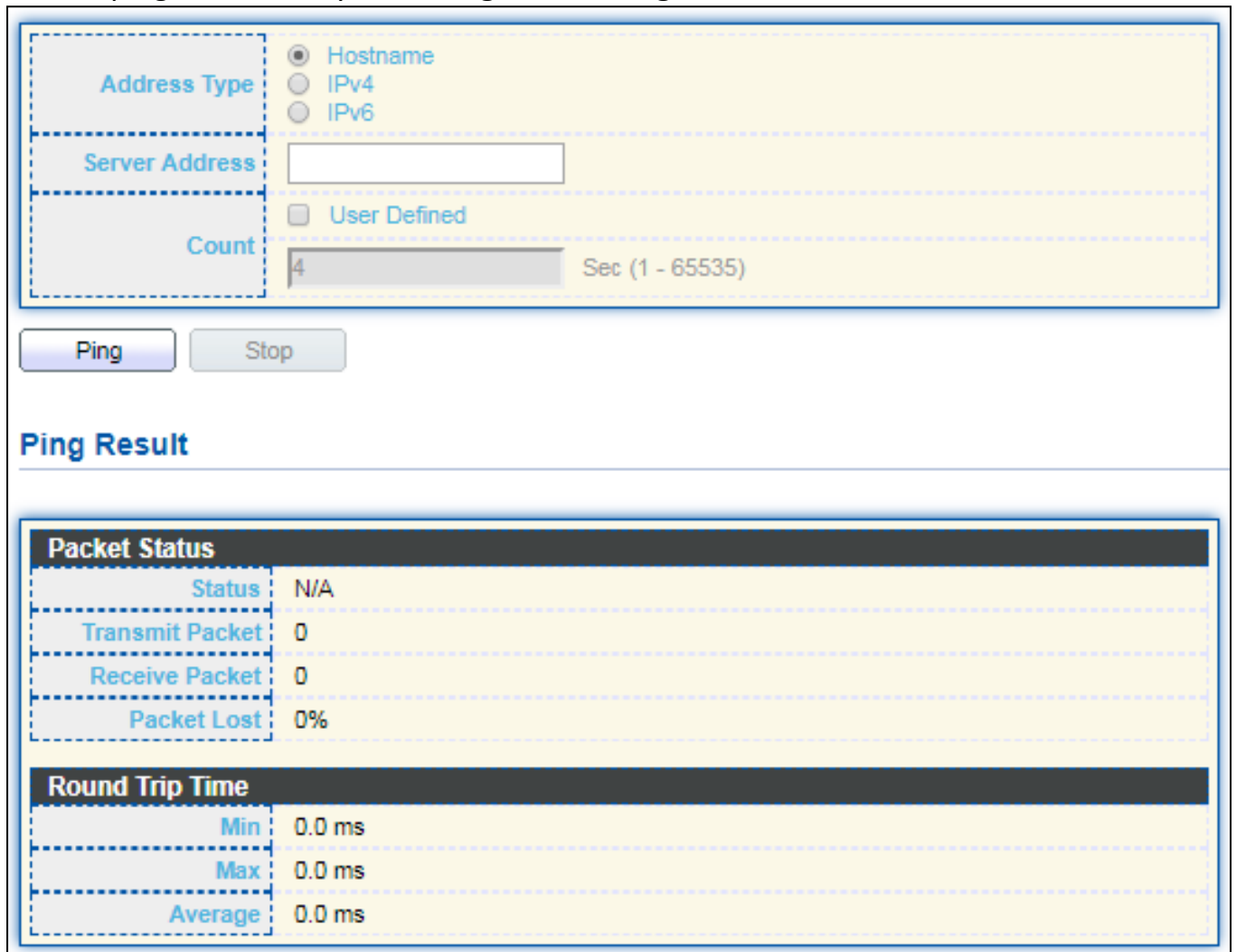
Click "Edit" button to view the Edit Mirroring menu.

Figure 136 - Diagnostics > Mirroring > Edit Mirroring

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

IV-12-3 Ping

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



The screenshot shows a web-based diagnostic tool for ping. It has a configuration area with three sections: 'Address Type' with radio buttons for 'Hostname' (selected), 'IPv4', and 'IPv6'; 'Server Address' with an empty text input field; and 'Count' with a checkbox for 'User Defined' and a numeric input field set to '4', with a timer 'Sec (1 - 65535)'. Below the configuration are 'Ping' and 'Stop' buttons. The 'Ping Result' section contains two tables. The first table, 'Packet Status', shows: Status: N/A, Transmit Packet: 0, Receive Packet: 0, and Packet Lost: 0%. The second table, 'Round Trip Time', shows: Min: 0.0 ms, Max: 0.0 ms, and Average: 0.0 ms.

Figure 137 - Diagnostics > Ping

Item	Description
Address Type	Specify the address type to "Hostname" or "IPv4".
Server Address	Specify the Hostname/IPv4 address for the remote logging server.
Count	Specify the numbers of each ICMP ping request.

IV-12-4 Traceroute

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

The screenshot shows a configuration panel for a traceroute tool. It includes three main input sections: 'Address Type' with radio buttons for 'Hostname' (selected) and 'IPv4'; 'Server Address' with an empty text box; and 'Time to Live' with a checkbox for 'User Defined' (unchecked) and a numeric input field set to '30' (range 2-255, default 30). Below the inputs are 'Apply' and 'Stop' buttons. A section titled 'Traceroute Result' contains a large empty rectangular area for displaying the results.

Figure 138 - Diagnostics > Traceroute

Item	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.

IV-12-5 Copper Test

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

The screenshot shows a web interface for a Copper Test. At the top, there is a 'Port' dropdown menu with 'GE1' selected. Below this is a 'Copper Test' button. The main content area is titled 'Copper Test Result' and contains a table with the following data:

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

Figure 139 - Diagnostics > Logging>Copper Test

Item	Description
Port	Specify the interface for the copper test.
Copper Test Result	
Port	The interface for the copper test.
Result	The status of copper test. It include: <ul style="list-style-type: none"> ● OK: Correctly terminated pair. ● Short Cable: Shorted pair. ● Open Cable: Open pair, no link partner. ● Impedance Mismatch: Terminating impedance is not in the reference range.
Length	Distance in meter from the port to the location on the cable where the fault was discovered.

IV-12-6 Fiber Module

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

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

Fiber Module Table								
	Port	Temperature (C)	Voltage (V)	Current (mA)	Output Power (mW)	Input Power (mW)	OE Present	Loss of Signal
<input type="radio"/>	GE25	N/A	N/A	N/A	N/A	N/A	Remove	Loss
<input type="radio"/>	GE26	N/A	N/A	N/A	N/A	N/A	Remove	Loss
<input type="radio"/>	GE27	N/A	N/A	N/A	N/A	N/A	Remove	Loss
<input type="radio"/>	GE28	N/A	N/A	N/A	N/A	N/A	Remove	Loss

Refresh Detail

Figure 140 - Diagnostics > Logging>Fiber Module

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

Click "Detail" button to view the Fiber Module Status menu

Fiber Module Status

Port	GE25
OE Present	N/A
Loss of Signal	N/A
Transceiver Type	N/A
Connector Type	N/A
Ethernet Compliance Code	N/A
Transmission Media	N/A
Wavelength	N/A
Bitrate	N/A
Vendor OUI	N/A
Vendor Name	N/A
Vendor PN	N/A
Vendor Revision	N/A
Vendor SN	N/A
Date Code	N/A
Temperature (C)	N/A
Voltage (V)	N/A
Current (mA)	N/A
Output Power (mW)	N/A
Input Power (mW)	N/A

Refresh Close

Figure 141 - Diagnostics > Logging>Fiber Module>Fiber Module Status

IV-12-7 UDLD

Use the UDLD pages to configure settings of UDLD function.

IV-12-7-1 Property

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

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

Message Time Sec (1 - 90, default 15)

Port Setting Table

<input type="checkbox"/>	Entry	Port	Mode	Bidirectional State	Operational Status	Neighbor
<input type="checkbox"/>	1	GE1	Disabled	Unknown		0
<input type="checkbox"/>	2	GE2	Disabled	Unknown		0
<input type="checkbox"/>	3	GE3	Disabled	Unknown		0
<input type="checkbox"/>	4	GE4	Disabled	Unknown		0
<input type="checkbox"/>	5	GE5	Disabled	Unknown		0
<input type="checkbox"/>	6	GE6	Disabled	Unknown		0
<input type="checkbox"/>	7	GE7	Disabled	Unknown		0
<input type="checkbox"/>	8	GE8	Disabled	Unknown		0
<input type="checkbox"/>	9	GE9	Disabled	Unknown		0
<input type="checkbox"/>	10	GE10	Disabled	Unknown		0
<input type="checkbox"/>	11	GE11	Disabled	Unknown		0
<input type="checkbox"/>	12	GE12	Disabled	Unknown		0
<input type="checkbox"/>	13	GE13	Disabled	Unknown		0
<input type="checkbox"/>	14	GE14	Disabled	Unknown		0
<input type="checkbox"/>	15	GE15	Disabled	Unknown		0
<input type="checkbox"/>	16	GE16	Disabled	Unknown		0
<input type="checkbox"/>	17	GE17	Disabled	Unknown		0
<input type="checkbox"/>	18	GE18	Disabled	Unknown		0
<input type="checkbox"/>	19	GE19	Disabled	Unknown		0
<input type="checkbox"/>	20	GE20	Disabled	Unknown		0
<input type="checkbox"/>	21	GE21	Disabled	Unknown		0
<input type="checkbox"/>	22	GE22	Disabled	Unknown		0
<input type="checkbox"/>	23	GE23	Disabled	Unknown		0
<input type="checkbox"/>	24	GE24	Disabled	Unknown		0
<input type="checkbox"/>	25	GE25	Disabled	Unknown		0
<input type="checkbox"/>	26	GE26	Disabled	Unknown		0
<input type="checkbox"/>	27	GE27	Disabled	Unknown		0
<input type="checkbox"/>	28	GE28	Disabled	Unknown		0

Figure 142 - Diagnostics > UDLD >Property

Item	Description
Message Time	Input the interval for sending message. Range is 1 -90 seconds.
Port	Display port ID of entry.
Mode	Display UDLD running mode of interface.
Bidirectional State	Display bidirectional state of interface.
Operational Status	Display operational status of interface.
Neighbor	Display the number of neighbor of interface.

Click "**Edit**" button to view the Fiber Module Status menu

Figure 143 - Diagnostics > UDLD>Property>Edit

Item	Description
Port	Display selected port to be edited.
Mode	<p>Select UDLD running mode of interface.</p> <ul style="list-style-type: none"> ● Disabled: Disable UDLD function. ● Normal: Running on normal mode that port goes to Link Up One phase after last neighbor ages out. ● Aggressive: Running on aggressive mode that port goes to Re-Establish phase after last neighbor ages out.

IV-12-7-2 Neighbor

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

Figure 144 - Diagnostics > UDLD>Neighbor

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

IV-13 Management

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

IV-13-1 User Account

The default username/password is admin/1234. Default account is unable 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.

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

The screenshot shows the 'User Account' management interface. At the top, it says 'Showing All entries' and 'Showing 1 to 1 of 1 entries'. Below this is a table with columns for 'Username' and 'Privilege'. The table contains one row with 'admin' and 'Admin'. Below the table are buttons for 'Add', 'Edit', and 'Delete'. On the right side, there are navigation buttons: 'First', 'Previous', '1', 'Next', and 'Last'. A search bar is located on the right side of the table.

Figure 145 - Management > User Account

Item	Description
Username	User name of the account.
Privilege	Select privilege level for new account. <ul style="list-style-type: none">● Admin: Allow to change switch settings. Privilege value equals to 15.● User: See switch settings only. Not allow to change it. Privilege level equals to 1.

Click "Add" or "Edit" button to view the Add/Edit User Account menu.

The screenshot shows the 'Add User Account' dialog box. It has a title bar 'Add User Account'. Inside, there are four input fields: 'Username', 'Password', 'Confirm Password', and 'Privilege'. The 'Privilege' field has two radio buttons: 'Admin' (selected) and 'User'. At the bottom, there are two buttons: 'Apply' and 'Close'.

Edit User Account

Username	admin
Password	<input type="text"/>
Confirm Password	<input type="text"/>
Privilege	<input checked="" type="radio"/> Admin <input type="radio"/> User

Apply Close

Figure 146 - Management > User Account > Add/Edit User Account

Item	Description
Username	User name of the account.
Password	Set password of the account.
Confirm Password	Set the same password of the account as in "Password" field.
Privilege	Select privilege level for new account. <ul style="list-style-type: none"> ● Admin: Allow to change switch settings. Privilege value equals to 15. ● User: See switch settings only. Not allow to change it. Privilege level equals to 1.

IV-13-2 Fireware

IV-13-2-1 Upgrade / Backup

This page allows user to upgrade or backup firmware image through HTTP or TFTP server.

For **Upgrade** action and **HTTP** method:

The screenshot shows a configuration panel for upgrading firmware via HTTP. It features three sections: 'Action' with radio buttons for 'Upgrade' (selected) and 'Backup'; 'Method' with radio buttons for 'TFTP' and 'HTTP' (selected); and 'Filename' with a 'Choose File' button and a text field containing 'No file chosen'. An 'Apply' button is located at the bottom left.

Figure 147 - Management > Firmware > Upgrade (Default Method: HTTP)

Item	Description
Action	Firmware operations <ul style="list-style-type: none"> ● Upgrade: Upgrade firmware from remote host to DUT. ● Backup: Backup firmware image from DUT to remote host.
Method	Firmware upgrade / backup method. <ul style="list-style-type: none"> ● TFTP: Using TFTP to upgrade/backup firmware. ● HTTP: Using WEB browser to upgrade/backup firmware.
Filename	Use browser to upgrade firmware, you should select firmware image file on your host PC.

For **Upgrade** action and **TFTP** method:

The screenshot shows a configuration panel for upgrading firmware via TFTP. It features five sections: 'Action' with radio buttons for 'Upgrade' (selected) and 'Backup'; 'Method' with radio buttons for 'TFTP' (selected) and 'HTTP'; 'Address Type' with radio buttons for 'Hostname' (selected), 'IPv4', and 'IPv6'; 'Server Address' with an empty text input field; and 'Filename' with an empty text input field. An 'Apply' button is located at the bottom left.

Figure 148 - Management > Firmware > Upgrade (Method: TFTP)

Item	Description
Action	Firmware operations <ul style="list-style-type: none"> ● Upgrade: Upgrade firmware from remote host to DUT ● Backup: Backup firmware image from DUT to remote host
Method	Firmware upgrade / backup method <ul style="list-style-type: none"> ● TFTP: Using TFTP to upgrade/backup firmware. ● HTTP: Using WEB browser to upgrade/backup firmware.
Address Type	Specify TFTP server address type <ul style="list-style-type: none"> ● Hostname: Use domain name as server address ● IPv4: Use IPv4 as server address ● IPv6: Use IPv6 as server address
Server Address	Specify TFTP server address.
Filename	Firmware image file name on remote TFTP server

For **Backup** action and **HTTP** method:

The screenshot shows a configuration window with three sections: Action, Method, and Firmware. Each section has radio buttons for different 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.

Figure 149 - Management > Firmware > Backup (Method: HTTP)

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

For **Backup** action and **TFTP** method:

The screenshot shows a configuration interface for firmware backup. It includes the following fields and options:

- Action:** Radio buttons for Upgrade and Backup. Backup is selected.
- Method:** Radio buttons for TFTP and HTTP. TFTP is selected.
- Firmware:** Radio buttons for Image0 and Image1. Image0 is selected.
- Address Type:** Radio buttons for Hostname, IPv4, and IPv6. Hostname is selected.
- Server Address:** A text input field.
- Filename:** A text input field.
- Apply:** A button at the bottom left.

Figure 150 - Management > Firmware > Backup (Method: TFTP)

Item	Description
Action	Firmware operations <ul style="list-style-type: none"> ● Upgrade: Upgrade firmware from remote host to DUT ● Backup: Backup firmware image from DUT to remote host
Method	Firmware upgrade / backup method <ul style="list-style-type: none"> ● TFTP: Using TFTP to upgrade/backup firmware. ● HTTP: Using WEB browser to upgrade/backup firmware.
Firmware	Firmware partition need to backup <ul style="list-style-type: none"> ● Image0: Firmware image in flash partition 0. ● Image1: Firmware image in flash partition 1.
Address Type	Specify TFTP server address type <ul style="list-style-type: none"> ● Hostname: Use domain name as server address. ● IPv4: Use IPv4 as server address. ● IPv6: Use IPv6 as server address.
Server Address	Specify TFTP server address address.
Filename	File name saved on remote TFTP server.

IV-13-2-2 Active Image

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

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

The screenshot shows a web interface for selecting a firmware image. At the top, there is a section titled "Active Image" with two radio buttons: "Image0" (unselected) and "Image1" (selected). Below this, a note states: "Note: the image was selected for the next boot".

Below the selection area, there are two detailed sections:

- Active Image:**
 - Firmware: Image1
 - Version: 1.1.1
 - Name: Edimax_GS-5424G_V1.1.1_r451_vmlinux_web.bix
 - Size: 6377396 Bytes
 - Created: 2018-01-04 19:32:12
- Backup Image:**
 - Firmware: Image0
 - Version: 1.00.08
 - Name: (empty)
 - Size: 6377963 Bytes
 - Created: 2017-12-04 04:32:24

At the bottom of the form is an "Apply" button.

Figure 151 - Management > Firmware > Active Image

Item	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.

IV-13-3 Configuration

IV-13-3-1 Upgrade / Backup

This page allows user to upgrade or backup configuration file through HTTP or TFTP server.

For **Upgrade** action and **HTTP** method:

The screenshot shows a web interface for configuration management. It is divided into four sections by dashed lines:

- Action:** Radio buttons for 'Upgrade' (selected) and 'Backup'.
- Method:** Radio buttons for 'TFTP' and 'HTTP' (selected).
- Configuration:** Radio buttons for 'Running Configuration' (selected), 'Startup Configuration', 'Backup Configuration', 'RAM Log', and 'Flash Log'.
- Filename:** A 'Choose File' button and a text field containing 'No file chosen'.

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

Figure 152 - Management > Configuration > Upgrade (Default Method: HTTP)

Item	Description
Action	Configuration operations <ul style="list-style-type: none">● Upgrade: Upgrade firmware from remote host to DUT● Backup: Backup firmware image from DUT to remote host
Method	Configuration upgrade / backup method <ul style="list-style-type: none">● TFTP: Using TFTP to upgrade/backup firmware● HTTP: Using WEB browser to upgrade/backup firmware
Configuration	Configuration types <ul style="list-style-type: none">● Running Configuration: Merge to current running configuration file● Startup Configuration: Replace startup configuration file● Backup Configuration: Replace backup configuration file
Filename	Use browser to upgrade configuration, you should select configuration file on your host PC.

For **Upgrade** action and **TFTP** method:

The screenshot shows a configuration interface for upgrading firmware. It features several sections with radio button options and text input fields. The 'Action' section has 'Upgrade' selected. The 'Method' section has 'TFTP' selected. The 'Configuration' section has 'Running Configuration' selected. The 'Address Type' section has 'Hostname' selected. There are two empty text input fields for 'Server Address' and 'Filename'. An 'Apply' button is located at the bottom left of the configuration area.

Figure 153 - Management > Configuration > Upgrade (Method: TFTP)

Item	Description
Action	Configuration operations <ul style="list-style-type: none"> ● Upgrade: Upgrade firmware from remote host to DUT ● Backup: Backup firmware image from DUT to remote host
Method	Configuration upgrade / backup method <ul style="list-style-type: none"> ● TFTP: Using TFTP to upgrade/backup firmware ● HTTP: Using WEB browser to upgrade/backup firmware
Configuration	Configuration types <ul style="list-style-type: none"> ● Running Configuration: Merge to current running configuration file ● Startup Configuration: Replace startup configuration file ● Backup Configuration: Replace backup configuration file
Address Type	Specify TFTP server address type <ul style="list-style-type: none"> ● Hostname: Use domain name as server address ● IPv4: Use IPv4 as server address ● IPv6: Use IPv6 as server address
Server Address	Specify TFTP server address address
Filename	File name saved on remote TFTP server

For **Backup** action and **HTTP** method:

The screenshot shows a configuration window with a yellow background. It is divided into three sections by dashed lines:

- Action:** Contains two radio buttons: 'Upgrade' (unselected) and 'Backup' (selected).
- Method:** Contains two radio buttons: 'TFTP' (unselected) and 'HTTP' (selected).
- Configuration:** Contains five radio buttons: 'Running Configuration' (selected), 'Startup Configuration' (unselected), 'Backup Configuration' (unselected), 'RAM Log' (unselected), and 'Flash Log' (unselected).

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

Figure 154 - Management > Configuration > Backup (Method: HTTP)

Item	Description
Action	<p>Configuration operations</p> <ul style="list-style-type: none"> ● Upgrade: Upgrade firmware from remote host to DUT ● Backup: Backup firmware image from DUT to remote host
Method	<p>Configuration upgrade / backup method</p> <ul style="list-style-type: none"> ● TFTP: Using TFTP to upgrade/backup firmware ● HTTP: Using WEB browser to upgrade/backup firmware
Configuration	<p>Configuration types</p> <ul style="list-style-type: none"> ● Running Configuration: Backup running configuration file. ● Startup Configuration: Backup start configuration file. ● Backup Configuration: Backup backup configuration file. ● RAM Log: Backup log file stored in RAM. ● Flash Log: Backup log files store in Flash.

For **Backup** action and **TFTP** method:

The screenshot shows a configuration window for Backup operations. It is divided into several sections by dashed lines:

- Action:** Radio buttons for Upgrade and Backup. Backup is selected.
- Method:** Radio buttons for TFTP and HTTP. TFTP is selected.
- Configuration:** Radio buttons for Running Configuration, Startup Configuration, Backup Configuration, RAM Log, and Flash Log. Running Configuration is selected.
- Address Type:** Radio buttons for Hostname, IPv4, and IPv6. Hostname is selected.
- Server Address:** An empty text input field.
- Filename:** An empty text input field.

An "Apply" button is located at the bottom left of the configuration area.

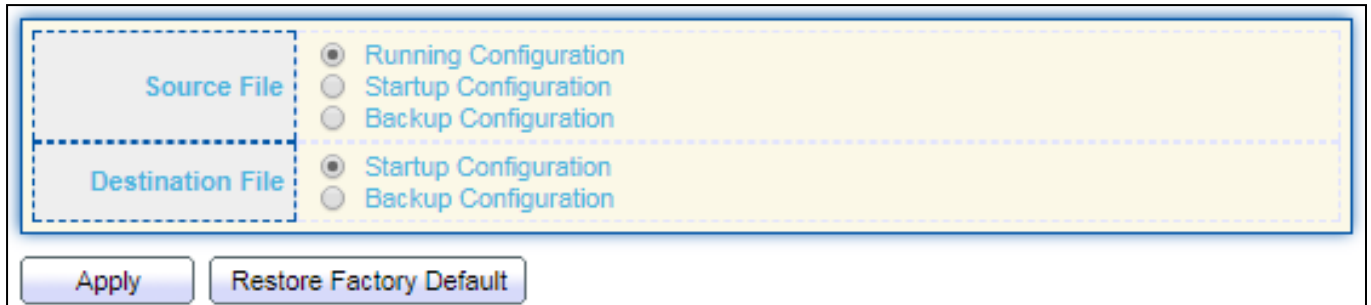
Figure 155 - Management > Configuration > Backup (Method: TFTP)

Item	Description
Action	Configuration operations <ul style="list-style-type: none"> ● Upgrade: Upgrade firmware from remote host to DUT ● Backup: Backup firmware image from DUT to remote host
Method	Configuration upgrade / backup method <ul style="list-style-type: none"> ● TFTP: Using TFTP to upgrade/backup firmware ● HTTP: Using WEB browser to upgrade/backup firmware
Configuration	Configuration types <ul style="list-style-type: none"> ● Running Configuration: Backup running configuration file. ● Startup Configuration: Backup start configuration file. ● Backup Configuration: Backup backup configuration file. ● RAM Log: Backup log file stored in RAM. ● Flash Log: Backup log files store in Flash.
Address Type	Specify TFTP server address type <ul style="list-style-type: none"> ● Hostname: Use domain name as server address ● IPv4: Use IPv4 as server address ● IPv6: Use IPv6 as server address
Server Address	Specify TFTP server address address.
Filename	File name saved on remote TFTP server.

IV-13-3-2 Save Configuration

This page allows user to manage configuration file saved on DUT and click “**Restore Factory Default**” button to restore factory defaults.

To display the Save Configuration web page, click **Management > Configuration > Save Configuration**.



The screenshot shows a web interface for saving configuration. It features two sections: 'Source File' and 'Destination File'. The 'Source File' section has three radio button options: 'Running Configuration' (which is selected), 'Startup Configuration', and 'Backup Configuration'. The 'Destination File' section has two radio button options: 'Startup Configuration' (which is selected) and 'Backup Configuration'. Below these sections are two buttons: 'Apply' and 'Restore Factory Default'.

Figure 156 - Management > Configuration > Save Configuration

Item	Description
Source File	Source file types <ul style="list-style-type: none">● Running Configuration: Copy running configuration file to destination.● Startup Configuration: Copy startup configuration file to destination.● Backup Configuration: Copy backup configuration file to destination
Destination File	Destination file <ul style="list-style-type: none">● Startup Configuration: Save file as startup configuration.● Backup Configuration: Save file as backup configuration.

IV-13-4 SNMP

IV-13-4-1 View

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

View Table

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

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

First Previous **1** Next Last

Figure 157 - Management > SNMP > View

Item	Description
View	The SNMP view name. Its maximum length is 30 characters
OID Subtree	Specify the ASN.1 subtree object identifier (OID) to be included or excluded from the SNMP view
Type	Include or exclude the selected MIBs in the view

IV-13-4-2 Group

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

Group Table

Showing **All** entries Showing 0 to 0 of 0 entries

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

First Previous **1** Next Last

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

Figure 158 - Management > SNMP > Group

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

Security Level	Specify SNMP security level <ul style="list-style-type: none"> ● No Security: Specify that no packet authentication is performed. ● Authentication: Specify that no packet authentication without encryption is performed. ● Authentication and Privacy: Specify that no packet authentication with encryption is performed.
View	
Read	Group read view name.
Write	Group write view name.
Notify	The view name that sends only traps with contents that is included in SNMP view selected for notification.

Click "Add" or "Edit" button to view the Add/Edit Group menu.

Add Group

Group	<input style="width: 90%;" type="text"/>
Version	<input checked="" type="radio"/> SNMPv1 <input type="radio"/> SNMPv2 <input type="radio"/> SNMPv3
Security Level	<input checked="" type="radio"/> No Security <input type="radio"/> Authentication <input type="radio"/> Authentication and Privacy
View	<input checked="" type="checkbox"/> Read <input type="checkbox"/> Write <input type="checkbox"/> Notify

Apply
Close

Edit Group

Group	1
Version	<input checked="" type="radio"/> SNMPv1 <input type="radio"/> SNMPv2 <input type="radio"/> SNMPv3
Security Level	<input checked="" type="radio"/> No Security <input type="radio"/> Authentication <input type="radio"/> Authentication and Privacy
View	<input checked="" type="checkbox"/> Read <input type="checkbox"/> Write <input type="checkbox"/> Notify

Apply
Close

Figure 159 - Management > SNMP > Group > Add/Edit Group

Item	Description
Group	Specify SNMP group name, and the maximum length is 30 characters.
Version	Specify SNMP version <input checked="" type="radio"/> SNMPv1: SNMP Version 1.

	<ul style="list-style-type: none"> ● SNMPv2: Community-based SNMP Version 2. ● SNMPv3: User security model SNMP version 3.
Security Level	Specify SNMP security level <ul style="list-style-type: none"> ● No Security : Specify that no packet authentication is performed. ● Authentication: Specify that no packet authentication without encryption is performed. ● Authentication and Privacy: Specify that no packet authentication with encryption is performed.
View	
Read	Select read view name if Read is checked.
Write	Select write view name, if Write is checked.
Notify	Select notify view name, if Notify is checked.

IV-13-4-3 Community

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

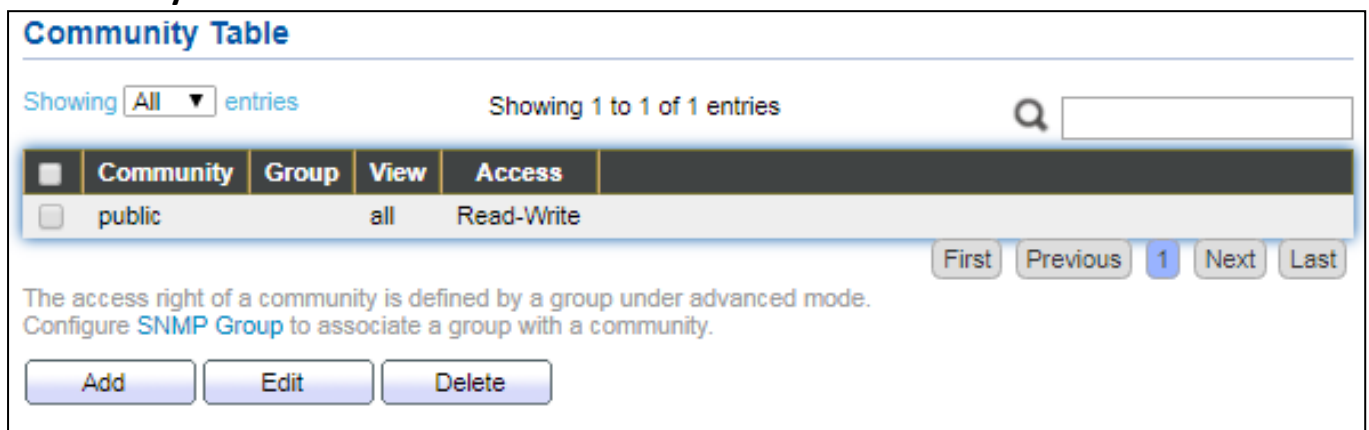


Figure 160 - Management > SNMP > Community

Item	Description
Community	The SNMP community name. Its maximum length is 20 characters.
Group	Specify the SNMP group configured by the command snmp group to define the object available to the community.
View	Specify the SNMP view to define the object available to the community.
Access	SNMP access mode <ul style="list-style-type: none"> ● Read-Only: Read only. ● Read-Write: Read and write.

Click "Add" or "Edit" button to view the Add/Edit Community menu.

The image displays two screenshots of a network management interface for configuring SNMP communities. The top screenshot is titled "Add Community" and shows a form with the following fields: "Community" (an empty text box), "Type" (radio buttons for "Basic" and "Advanced", with "Basic" selected), "View" (a dropdown menu set to "all"), "Access" (radio buttons for "Read-Only" and "Read-Write", with "Read-Only" selected), and "Group" (a dropdown menu set to "1"). Below the form are "Apply" and "Close" buttons. The bottom screenshot is titled "Edit Community" and shows the same form with the following values: "Community" is "public", "Type" is "Basic", "View" is "all", "Access" is "Read-Write", and "Group" is "1". It also has "Apply" and "Close" buttons.

Figure 161 - Management > SNMP > Group > Add/Edit Community

Item	Description
Community	The SNMP community name. Its maximum length is 20 characters.
Type	SNMP Community mode <ul style="list-style-type: none"> ● Basic: SNMP community specifies view and access right. ● Advanced: SNMP community specifies group.
View	Specify the SNMP view to define the object available to the community.
Access	SNMP access mode <ul style="list-style-type: none"> ● Read-Only: Read only. ● Read-Write: Read and write.
Group	Specify the SNMP group configured by the command snmp group to define the object available to the community.

IV-13-4-4 User

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

User Table

Showing **All** entries Showing 0 to 0 of 0 entries

<input type="checkbox"/>	User	Group	Security Level	Authentication Method	Privacy Method
0 results found.					

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

Figure 162 - Management > SNMP > User

Item	Description
User	Specify the SNMP user name on the host that connects to the SNMP agent. The max character is 30 characters. For the SNMP v1 or v2c, the user name must match the community name.
Group	Specify the SNMP group to which the SNMP user belongs.
Security Level	SNMP privilege mode <ul style="list-style-type: none"> ● No Security: Specify that no packet authentication is performed. ● Authentication: Specify that no packet authentication without encryption is performed. ● Authentication and Privacy: Specify that no packet authentication with encryption is performed.
Authentication Method	Authentication Protocol which is available when Privilege Mode is Authentication or Authentication and Privacy. <ul style="list-style-type: none"> ● None: No authentication required. ● MD5: Specify the HMAC-MD5-96 authentication protocol. ● SHA: Specify the HMAC-SHA-96 authentication protocol
Privacy Method	Encryption Protocol <ul style="list-style-type: none"> ● None: No privacy required. ● DES: DES algorithm

Click "Add" or "Edit" button to view Add/Edit User menu.

Add User

User	<input type="text"/>
Group	11 ▼
Security Level	<input checked="" type="radio"/> No Security <input type="radio"/> Authentication <input type="radio"/> Authentication and Privacy

Authentication

Method	<input checked="" type="radio"/> None <input type="radio"/> MD5 <input type="radio"/> SHA
Password	<input type="password"/>

Privacy

Method	<input checked="" type="radio"/> None <input type="radio"/> DES
Password	<input type="password"/>

Apply Close

Edit User

User	22
Group	11 ▼
Security Level	<input checked="" type="radio"/> No Security <input type="radio"/> Authentication <input type="radio"/> Authentication and Privacy

Authentication

Method	<input checked="" type="radio"/> None <input type="radio"/> MD5 <input type="radio"/> SHA
Password	<input type="password"/>

Privacy

Method	<input checked="" type="radio"/> None <input type="radio"/> DES
Password	<input type="password"/>

Apply Close

Figure 163 - Management > SNMP > User > Add/Edit User

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

IV-13-4-5 Engine ID

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

Figure 164 - Management > SNMP > Engine ID

Item	Description
Local Engine ID	
Engine ID	If checked "User Defined", the local engine ID is configure by user, else use the default Engine ID which is made up of MAC and Enterprise ID. The user defined engine ID is range 10 to 64 hexadecimal characters, and the hexadecimal number must be divided by 2.
Remote Engine ID Table	
Table	
Server Address	Remote host.
Engine ID	Specify Remote SNMP engine ID. The engine ID is range10 to 64 hexadecimal characters, and the hexadecimal number must be divided by 2.

Click "**Add**" button to view Add Remote Engine ID menu.

Figure 165 - Management > SNMP > Add Engine ID

Item	Description
Address Type	Remote host address type for Hostname/IPv4/IPv6.
Server Address	Remote host.
Engine ID	Specify Remote SNMP engine ID. The engine ID is range 10 to 64 hexadecimal characters, and the hexadecimal number must be divided by 2.

Click "**Edit**" button to view Edit Remote Engine ID menu.

Figure 166 - Management > SNMP > Edit Engine ID

Item	Description
Server Address	Edit Remote host address
Engine ID	Specify Remote SNMP engine ID. The engine ID is range 10 to 64 hexadecimal characters, and the hexadecimal number must be divided by 2.

IV-13-4-6 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 checked="" type="checkbox"/>	Enable
Warm Start	<input checked="" type="checkbox"/>	Enable

Apply

Figure 167 - Management > SNMP > Trap Event

Item	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.

IV-13-4-7 Notification

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

Notification Table

Showing All entries Showing 0 to 0 of 0 entries

<input type="checkbox"/>	Server Address	Server Port	Timeout	Retry	Version	Type	Community / User	Security Level
0 results found.								

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 168 - Management > SNMP > Notification

Item	Description
Server Address	IP address or the hostname of the SNMP trap recipients.
Server Port	Recipients server UDP port number.
Timeout	Specify the SNMP informs timeout.
Retry	Specify the retry counter of the SNMP informs.
Version	Specify SNMP notification version <ul style="list-style-type: none"> ● SNMPv1: SNMP Version 1 notification.

	<ul style="list-style-type: none"> ● SNMPv2: SNMP Version 2 notification. ● SNMPv3: SNMP Version 3 notification.
Type	<p>Notification Type</p> <ul style="list-style-type: none"> ● Trap: Send SNMP traps to the host. ● Inform: Send SNMP informs to the host.
Community/User	SNMP community/user name for notification. If version is SNMPv3 the name is user name, else is community name.
UDP Port	Specify the UDP port number.
Timeout	Specify the SNMP informs timeout.
Security Level	<p>SNMP trap packet security level</p> <ul style="list-style-type: none"> ● No Security: Specify that no packet authentication is performed. ● Authentication: Specify that no packet authentication without encryption is performed. ● Authentication and Privacy: Specify that no packet authentication with encryption is performed.

Click "**Add**" button to view the Notification menu.

Add Notification

Address Type	<input checked="" type="radio"/> Hostname <input type="radio"/> IPv4 <input type="radio"/> IPv6
Server Address	<input style="width: 100%;" type="text"/>
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	<input style="width: 100%;" type="text" value="public"/>
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 style="width: 100%;" type="text" value="162"/> (1 - 65535, default 162)
Timeout	<input checked="" type="checkbox"/> Use Default <input style="width: 100%;" type="text" value="15"/> Sec (1 - 300, default 15)
Retry	<input checked="" type="checkbox"/> Use Default <input style="width: 100%;" type="text" value="3"/> (1 - 255, default 3)

Apply

Close

Figure 169 - Management > SNMP > Notification > Add Notification

Item	Description
Address Type	Notify recipients host address type.
Server Address	IP address or the hostname of the SNMP trap recipients.
Version	Specify SNMP notification version <ul style="list-style-type: none"> ● SNMPv1: SNMP Version 1 notification. ● SNMPv2: SNMP Version 2 notification. ● SNMPv3: SNMP Version 3 notification.
Type	Notification Type <ul style="list-style-type: none"> ● Trap: Send SNMP traps to the host. ● Inform: Send SNMP informs to the host.(version 1 have no inform)
Community/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 <ul style="list-style-type: none"> ● No Security: Specify that no packet authentication is performed. ● Authentication: Specify that no packet authentication without encryption is performed. ● Authentication and Privacy: Specify that no packet authentication with encryption is performed.
Server Port	Recipient 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.

Click "Edit" button to view the Edit Notification menu.

Figure 170 - Management > SNMP > Notification > Edit Notification

Item	Description
Server Address	Edit SNMP notify recipients address
Version	Specify SNMP notification version <ul style="list-style-type: none"> ● SNMPv1: SNMP Version 1 notification. ● SNMPv2: SNMP Version 2 notification. ● SNMPv3: SNMP Version 3 notification.
Type	Notification Type <ul style="list-style-type: none"> ● Trap: Send SNMP traps to the host. ● Inform: Send SNMP informs to the host.(version 1 have no inform)
Community/User	SNMP community/user name for notification. If version is SNMPv3 the name is user name, else is community name.
Community Level	SNMP notification packet security level, the security level must less than or equal to the community/user name <ul style="list-style-type: none"> ● No Security: Specify that no packet authentication is performed. ● Authentication: Specify that no packet authentication without encryption is performed. ● Authentication and Privacy: Specify that no packet authentication with encryption is performed.
Server Port	Recipients server UDP port number, if "use default" checked the value

	is 162, else user configure.
Timeout	Specify the SNMP informs timeout, if “use default” checked the value is 15, else user configure.
Retry	Specify the SNMP informs retry count, if “use default” checked the value is 3, else user configure.

COPYRIGHT

Copyright © Edimax Technology Co., Ltd. all rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise, without the prior written permission from Edimax Technology Co., Ltd.

Edimax Technology Co., Ltd. makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties, merchantability, or fitness for any particular purpose. Any software described in this manual is sold or licensed as is. Should the programs prove defective following their purchase, the buyer (and not this company, its distributor, or its dealer) assumes the entire cost of all necessary servicing, repair, and any incidental or consequential damages resulting from any defect in the software. Edimax Technology Co., Ltd. reserves the right to revise this publication and to make changes from time to time in the contents hereof without the obligation to notify any person of such revision or changes.

The product you have purchased and the setup screen may appear slightly different from those shown in this QIG. The software and specifications are subject to change without notice. Please visit our website www.edimax.com for updates. All brand and product names mentioned in this manual are trademarks and/or registered trademarks of their respective holders.

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio technician for help.

FCC Caution

This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter. This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation. Any changes or modifications not expressly approved by the party responsible for compliance could void the authority to operate equipment.

Federal Communications Commission (FCC) Radiation Exposure Statement

This equipment complies with FCC radiation exposure set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 2.5cm (1 inch) during normal operation.

Federal Communications Commission (FCC) RF Exposure Requirements

This EUT is compliance with SAR for general population/uncontrolled exposure limits in ANSI/IEEE C95.1-1999 and had been tested in accordance with the measurement methods and procedures specified in OET Bulletin 65 Supplement C. The equipment version marketed in US is restricted to usage of the channels 1-11 only. This equipment is restricted to *indoor* use when operated in the 5.15 to 5.25 GHz frequency range.

R&TTE Compliance Statement

This equipment complies with all the requirements of DIRECTIVE 2014/30/EU OF THE EUROPEAN PARLIAMENT AND THE COUNCIL of March 9, 1999 on radio equipment and telecommunication terminal equipment and the mutual recognition of their conformity (R&TTE). The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) As of April 8, 2000.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

EU Countries Intended for Use

The ETSI version of this device is intended for home and office use in Austria, Belgium, Bulgaria, Cyprus, Czech, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Turkey, and United Kingdom. The ETSI version of this device is also authorized for use in EFTA member states: Iceland, Liechtenstein, Norway, and Switzerland.

EU Countries Not Intended for Use

None

EU Declaration of Conformity

- English:** This equipment is in compliance with the essential requirements and other relevant provisions of Directive 2014/30/EU.
- Français:** Cet équipement est conforme aux exigences essentielles et autres dispositions de la directive 2014/30/EU.
- Čeština:** Toto zařízení je v souladu se základními požadavky a ostatními příslušnými ustanoveními směrnic 2014/30/EU.
- Polski:** Urządzenie jest zgodne z ogólnymi wymaganiami oraz szczególnymi warunkami określonymi Dyrektywą UE 2014/30/EU.
- Română:** Acest echipament este în conformitate cu cerințele esențiale și alte prevederi relevante ale Directivei 2014/30/EU.
- Русский:** Это оборудование соответствует основным требованиям и положениям Директивы 2014/30/EU.
- Magyar:** Ez a berendezés megfelel az alapvető követelményeknek és más vonatkozó irányelveknek (2014/30/EU).
- Türkçe:** Bu cihaz 2014/30/EU. direktifleri zorunlu istekler ve diğer hükümlerle ile uyumludur.
- Українська:** Обладнання відповідає вимогам і умовам директиви 2014/30/EU.
- Slovenčina:** Toto zariadenie spĺňa základné požiadavky a ďalšie príslušné ustanovenia smerníc 2014/30/EU.
- Deutsch:** Dieses Gerät erfüllt die Voraussetzungen gemäß den Richtlinien 2014/30/EU.
- Español:** El presente equipo cumple los requisitos esenciales de la Directiva 2014/30/EU.
- Italiano:** Questo apparecchio è conforme ai requisiti essenziali e alle altre disposizioni applicabili della Direttiva 2014/30/EU.
- Nederlands:** Dit apparaat voldoet aan de essentiële eisen en andere van toepassing zijnde bepalingen van richtlijn 2014/30/EU.
- Português:** Este equipamento cumpre os requisitos essenciais da Directiva 2014/30/EU.
- Norsk:** Dette utstyret er i samsvar med de viktigste kravene og andre relevante regler i Direktiv 2014/30/EU.
- Svenska:** Denna utrustning är i överensstämmelse med de väsentliga kraven och övriga relevanta bestämmelser i direktiv 2014/30/EU.
- Dansk:** Dette udstyr er i overensstemmelse med de væsentligste krav og andre relevante forordninger i direktiv 2014/30/EU.
- suomen kieli:** Tämä laite täyttää direktiivien 2014/30/EU. oleelliset vaatimukset ja muut asiaankuuluvat määräykset.

FOR USE IN 



WEEE Directive & Product Disposal



At the end of its serviceable life, this product should not be treated as household or general waste. It should be handed over to the applicable collection point for the recycling of electrical and electronic equipment, or returned to the supplier for disposal.

Declaration of Conformity

We, Edimax Technology Co., Ltd., declare under our sole responsibility, that the equipment described below complies with the requirements of the European R&TTE directives.

Equipment: 24-port Gigabit Ethernet+4 SFP Lite Web Smart Switch
Model No.: GS-5424G

The following European standards for essential requirements have been followed:

Directives 2014/30/EU

EMC : EN 55032:2015
EN 61000-3-2:2014 Class A
EN 61000-3-3:2013
EN 55024:2015
Safety (LVD) : EN 60950-1:2006 + A11:2009 + A1:2010 + A12:2011+A2:2013

Edimax Technology Europe B.V.
Fijenhof 2,
5652 AE Eindhoven,
The Netherlands

a company of :
Edimax Technology Co., Ltd.
No. 278, Xinhu 1st Rd.,
Neihu Dist., Taipei City,
Taiwan

Signature:

Printed Name: Vivian Ma
Title: Director
Edimax Technology Europe B.V.



Date of Signature: March, 2018

Signature:

A handwritten signature in black ink, appearing to read 'Albert Chang', written over a horizontal line.

Printed Name:

Albert Chang

Title:

Director

Edimax Technology Co., Ltd.

Notice According to GNU General Public License Version 2

This product includes software that is subject to the GNU General Public License version 2. The program is free software and distributed without any warranty of the author. We offer, valid for at least three years, to give you, for a charge no more than the costs of physically performing source distribution, a complete machine-readable copy of the corresponding source code.

Das Produkt beinhaltet Software, die den Bedingungen der GNU/GPL-Version 2 unterliegt. Das Programm ist eine sog. „Free Software“, der Autor stellt das Programm ohne irgendeine Gewährleistungen zur Verfügung. Wir bieten Ihnen für einen Zeitraum von drei Jahren an, eine vollständige maschinenlesbare Kopie des Quelltextes der Programme zur Verfügung zu stellen – zu nicht höheren Kosten als denen, die durch den physikalischen Kopiervorgang anfallen.

GNU GENERAL PUBLIC LICENSE Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc. 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA
Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep

intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

- a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
- b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
- c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

- a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
- b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
- c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.