

FS-5428X

User Manual

09-2023 / 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

530 Technology Drive Suite 100, Irvine, CA 92618, USA

Email: support@edimax.us

Contents

I. Product Information.....	1
I-1. Package Content	1
I-2. Hardware Overview	1
I-3. LED Status.....	2
II. Installation	2
II-1. Physically Setup.....	2
II-2. Connection	4
III. Web-based Configuration (Login).....	5
IV. Web-based Switch Configuration.....	7
IV-1. Status	7
IV-1-1 System Information	7
IV-1-2 Logging Message.....	9
IV-1-3 Port.....	9
IV-1-3-1 Statistics.....	9
IV-1-3-2 Error Disabled	10
IV-1-3-3 Bandwidth Utilization	11
IV-1-3-4 Link Aggregation	12
IV-1-3-5 MAC Address Table	12
IV-2. Network	13
IV-2-1 IP Address	13
IV-2-2 System Time	15
IV-3. Port.....	18
IV-3-1 Port Setting.....	18
IV-3-2 Error Disable	19
IV-3-3 Link Aggregation	21
IV-3-3-1 Group.....	21
IV-3-3-2 Port Setting.....	22

IV-3-3-3	LACP.....	25
IV-3-4	EEE.....	26
IV-3-5	Jumbo Frame	27
IV-4.	VLAN.....	27
IV-4-1	VLAN	27
IV-4-1-1	Create VLAN	27
IV-4-1-2	VLAN Configuration	29
IV-4-1-3	Membership.....	29
IV-4-1-4	Port Setting	31
IV-4-2	Voice VLAN	33
IV-4-2-1	Property	33
IV-4-2-2	Voice OUI	34
IV-4-3	Protocol VLAN.....	36
IV-4-3-1	Protocol Group.....	36
IV-4-3-2	Group Binding	37
IV-4-4	MAC VLAN	38
IV-4-4-1	MAC Group.....	38
IV-4-4-2	Group Binding	40
IV-5.	MAC Address Table	41
IV-5-1	Dynamic Address	41
IV-5-2	Static Address	42
IV-5-3	Filtering Address.....	42
IV-5-4	Port Security Address	43
IV-6.	Spanning Tree	43
IV-6-1	Property.....	43
IV-6-2	Port Setting.....	45
IV-6-3	MST Instance	48
IV-6-4	MST Port Setting.....	49
IV-6-5	Statistics.....	51
IV-7.	Discovery	53
IV-7-1	LLDP.....	53
IV-7-1-1	Property	54
IV-7-1-2	Port Setting	55
IV-7-1-3	MED Network Policy.....	56
IV-7-1-4	MED Port Setting.....	57
IV-7-1-5	Packet View	59
IV-7-1-6	Local Information	61

IV-7-1-7	Neighbor	64
IV-7-1-8	Statistics	67
IV-8.	Multicast	68
IV-8-1	General	68
IV-8-1-1	Property	69
IV-8-1-2	Group Address.....	69
IV-8-1-3	Router Port.....	71
IV-8-1-4	Forward All	74
IV-8-1-5	Throttling.....	76
IV-8-1-6	Filtering Profile	77
IV-8-1-7	Filtering Binding	79
IV-8-2	IGMP Snooping	80
IV-8-2-1	Property	80
IV-8-2-2	Querier	83
IV-8-2-3	Statistics	85
IV-8-3	MLD Snooping.....	86
IV-8-3-1	Property	86
IV-8-3-2	Statistics	89
IV-8-4	MVR	90
IV-8-4-1	Property	90
IV-8-4-2	Port Setting	91
IV-8-4-3	Group Address.....	92
IV-9.	Routings	94
IV-9-1.	IPv4 Management and Interface.....	94
IV-9-1-1	IPv4 Interface	94
IV-9-1-2	IPv4 Routes.....	95
IV-9-1-3	ARP	96
IV-9-2.	IPv6 Management and Interfaces	96
IV-9-2-1	IPv6 Interface	97
IV-9-2-2	IPv6 Addresses	98
IV-9-2-3	IPv6 Route	99
IV-9-2-4	IPv6 Neighbors	100
IV-10.	Security	101
IV-10-1	RADIUS.....	101
IV-10-2	TACACS+	104
IV-10-3	AAA.....	106
IV-10-3-1	Method List	106
IV-10-3-2	Login Authentication	107

IV-10-4	Management Access	107
IV-10-4-1	Management VLAN	107
IV-10-4-2	Management Service	107
IV-10-4-3	Management ACL	108
IV-10-4-4	Management ACE	109
IV-10-5	Authentication Manager	112
IV-10-5-1	Property	112
IV-10-5-2	Port Setting	116
IV-10-5-3	MAC-Base Local Account	120
IV-10-5-4	WEB-Base Local Account	121
IV-10-5-5	Sessions	122
IV-10-5-6	Port Security	123
IV-10-5-7	Protected Port	125
IV-10-5-8	Storm Control	126
IV-10-6	DoS	128
IV-10-6-1	Property	128
IV-10-6-2	Port Setting	130
IV-10-7	DHCP Snooping	131
IV-10-7-1	Property	131
IV-10-7-2	Statistics	132
IV-10-7-3	Option82 Property	133
IV-10-7-4	Option82 Circuit ID	135
IV-10-8	IP Source Guard	136
IV-10-8-1	Port Setting	136
IV-10-8-2	IMPV Binding	138
IV-10-8-3	Save Database	139
IV-11.	ACL	140
IV-11-1	MAC ACL	140
IV-11-2	MAC ACE	141
IV-11-3	IPv4 ACL	143
IV-11-4	IPv4 ACE	144
IV-11-5	ACL Binding	147
IV-12.	QoS	149
IV-12-1	General	149
IV-12-1-1	Property	149
IV-12-1-2	Queue Scheduling	151
IV-12-1-3	CoS Mapping	152
IV-12-1-4	DSCP Mapping	153
IV-12-1-5	IP Precedence Mapping	153

IV-12-2	Rate Limit.....	154
IV-12-2-1	Ingress/Egress Port.....	155
IV-12-2-2	Egress Queue.....	156
IV-13.	Diagnostics	157
IV-13-1	Logging	157
IV-13-1-1	Property	157
IV-13-1-2	Remote Server.....	158
IV-13-2	Mirroring	159
IV-13-3	Ping.....	161
IV-13-4	Traceroute	162
IV-13-5	Fiber Module	162
IV-13-6	UDLD.....	164
IV-13-6-1	Property	164
IV-13-6-2	Neighbor	166
IV-14.	Management.....	167
IV-14-1	User Account	167
IV-14-2	Firmware.....	169
IV-14-2-1	Upgrade / Backup	169
IV-14-2-2	Active Image	172
IV-14-3	Configuration	173
IV-14-3-1	Upgrade / Backup	173
IV-14-3-2	Save Configuration.....	177
IV-14-4	SNMP	177
IV-14-4-1	View	177
IV-14-4-2	Group	178
IV-14-4-3	Community.....	180
IV-14-4-5	Engine ID	184
IV-14-4-6	Trap Event	187
IV-14-4-7	Notification.....	187
IV-14-5	RMON	191

V. More Information192

VI. Safety Instructions.....192

I. Product Information

- **FS-5428X: 28-Port Gigabit SFP Ports L2+ Switch with 4 SFP+ Ports**

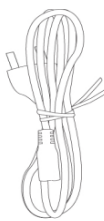
I-1. Package Content



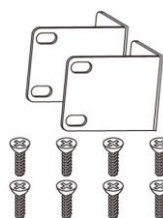
FS-5428X



**Quick Installation
Guide**



Power Cord

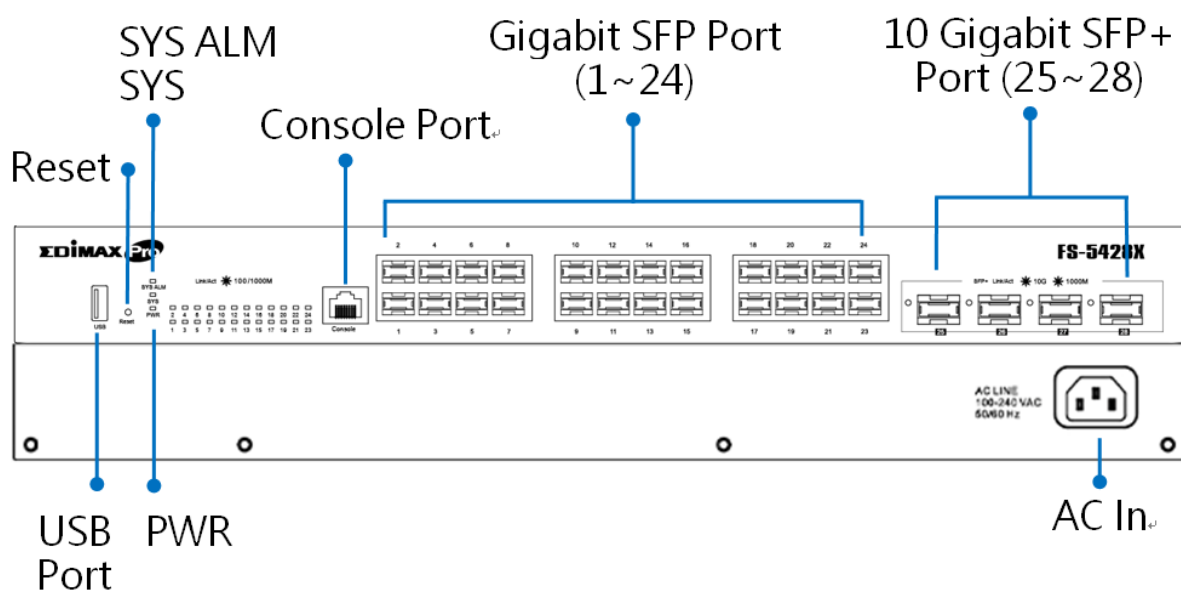


Rack-Mount Kit



Console Cable

I-2. Hardware Overview



I-3. LED Status

Function	Color	Status	Description
PWR	Green	On	Power on
		Off	Power off
SYS	Green	On	Power on
		Blinking	System is booting up
		Off	Power off
SYS ALM	RED	On	System failure (Overheat, crashed, etc.)
		Off	Device in good condition
Link/ACT (1-24 port)	Green	On	Link at 100/1000Mbps
		Blinking	Sending or receiving data
		Off	Port disconnected or link fail
SPF+ (25-28 port)	Green	On	Link at 1000Mbps
		Blinking	Sending or receiving data
		Off	Port disconnected or link fail
	Blue	On	Link at 10Gbps
		Blinking	Sending or receiving data
		Off	Port disconnected or link fail

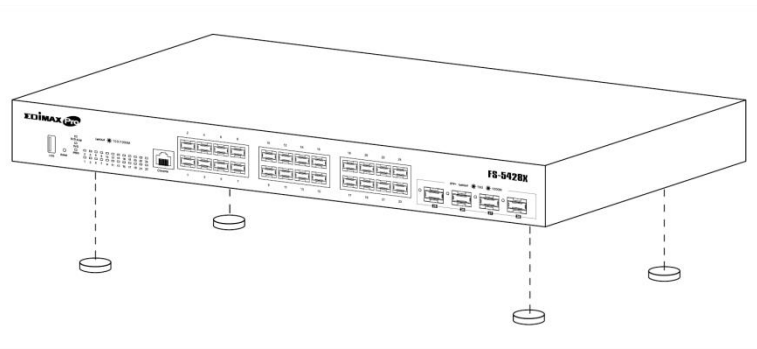
II. Installation

Read the following topics and perform the procedures in the correct order. Incorrect installation may cause damage to the product.

II-1. Physically Setup

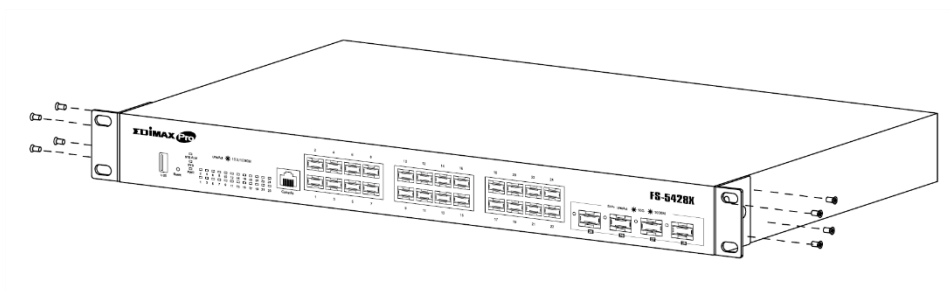
There are two ways to physically set up the switch. No matter how you installed the switch, please keep it with good ventilation.

1. Desktop Placement: Attach the supplied rubber feet to the recessed areas on the bottom of the switch. Place the switch on a flat surface and keep it with good ventilation.

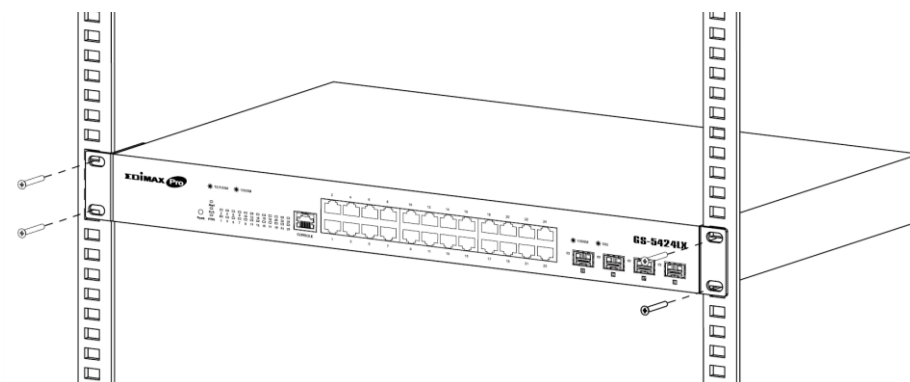


2. **Rack-Mount Installation:** You can mount the switch in any standard size, 19-inch (about 48 cm) wide rack with 1 Rack Unit (1U) of space, which is 1.75 inches (4.45 cm) high.

First, align the mounting brackets with the mounting holes on the switch's side panels and secure the brackets with the screws.



Then secure the switch on the equipment rack and keep it with good ventilation.



II-2. Connection

1. Power on: Connect the power cord to the switch and the power outlet. The switch is powered by the 100-240VAC 50/60Hz external high-performance power supply. (Note: Make sure the PWR LED is green.)
2. Plug the SFP/SFP+ module or DAC/AoC cable into the SFP/SFP+ slot Port 25~28 and connect it to another switch SFP/SFP+ Port.

Note: Make sure that the SFP+/SFP Port LED is blue or green.

These 2 connected SFP+/SFP ports of the switches must be set into the same speed.

If the LED is off, please edit the Speeds of these 2 connected SFP+/SFP ports to be consistent. For more detail, please refer to user manual "Port Setting"

3. Connect a computer: Connect your computer with the switch and get ready for web-based configuration with following "Web-based Configuration Utility".

III. Web-based Configuration (Login)

This section describes how to navigate the web-based switch configuration utility through web browser. Be sure to disable any browser 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

1. Connect your computer with the switch then open a web browser.
2. Enter the IP address of the switch you are configuring in the address bar on the browser (factory default IP address is 192.168.2.1) and then press Enter. Please make sure that your computer's IP address is in the same subnet as this switch. The default IP address is an IP address in the range of 192.168.2.X (X=2-254). You can modify the IP address of your computer if you need.

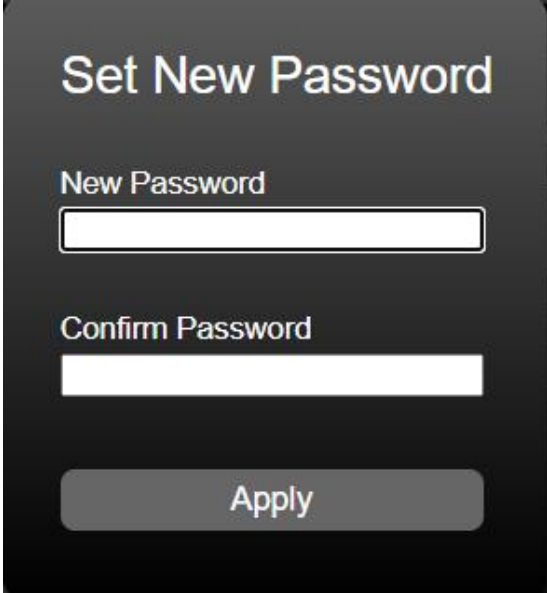
Default IP	192.168.2.1
Default User Name	admin
Default Password	1234

3. The default username is “admin” and the default password is “1234”.



The image shows a login interface for EDIMAX Pro. At the top, the logo "EDIMAX Pro" is displayed. Below it, the "Model Name" is "FS-5428X". There are two input fields: "Username:" and "Password:". Below these is a "Language" dropdown menu set to "English". At the bottom is a "LOGIN" button.

4. **The first time that you log in with the default username and password, you are required to set a new password.**



The image shows a "Set New Password" screen. It has two input fields: "New Password" and "Confirm Password". At the bottom is an "Apply" button.

5. Following the next section for details of Web-based Configuration Utility.

IV. Web-based Switch Configuration

This chapter describes how to use the web-based management interface (Web UI) to configure the switch's features.

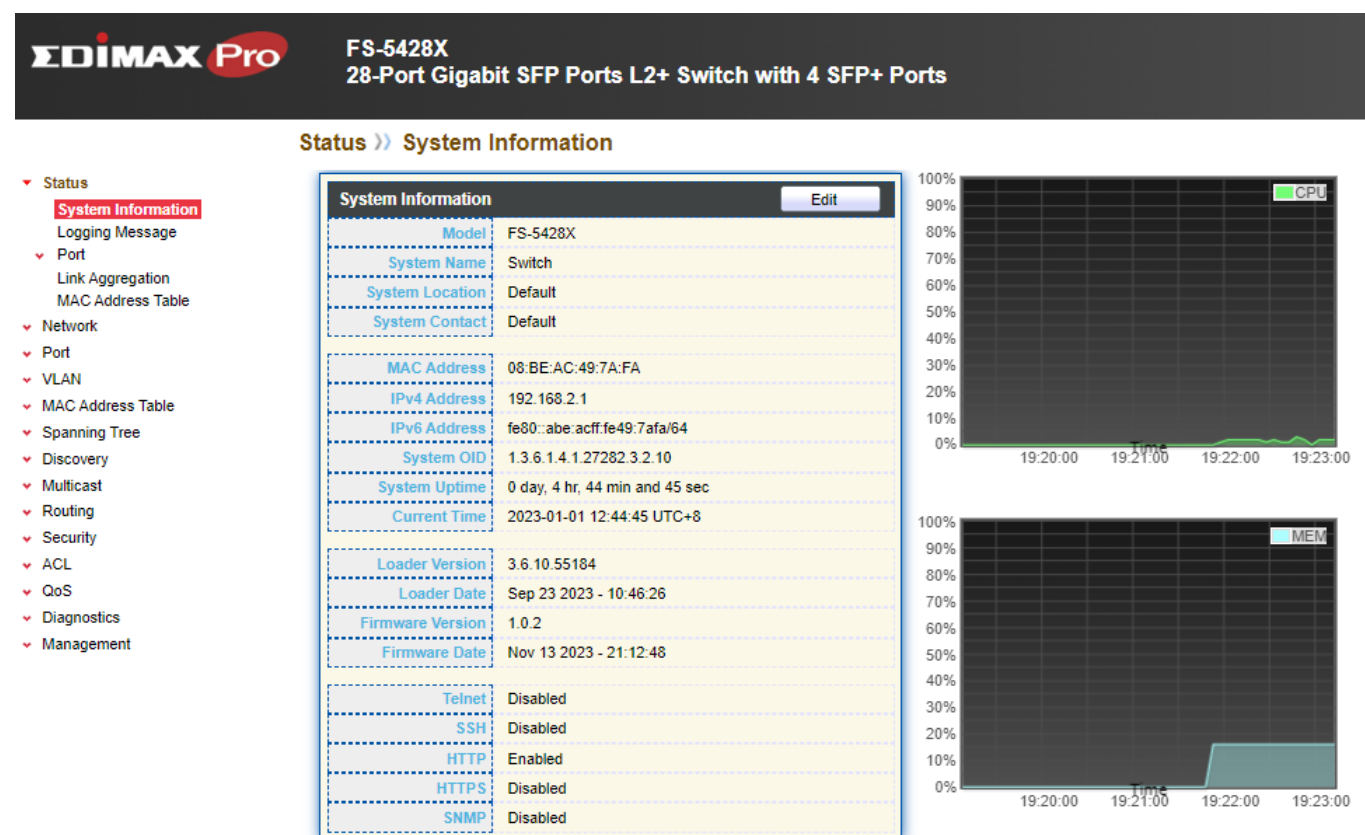
IV-1. Status

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**.



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.
IPv6 Address	Current system IPv6 address.
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.

Edit System Information

System Name	Switch
System Location	Default
System Contact	Default

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**.

Status >> Logging Message

Showing **All** entries Showing 1 to 14 of 14 entries

Log ID	Time	Severity	Description
1	Jan 01 2023 12:49:49	notice	PORT-0-LINK_UP: Interface GigabitEthernet2 link up, aggregated (1)
2	Jan 01 2023 12:49:51	notice	PORT-5-LINK_DOWN: Interface GigabitEthernet2 link down
3	Jan 01 2023 12:49:49	notice	PORT-5-LINK_UP: Interface GigabitEthernet2 link up
4	Jan 01 2023 12:49:45	notice	PORT-5-LINK_DOWN: Interface GigabitEthernet20 link down
5	Jan 01 2023 12:44:44	notice	AAA-5-CONNECT: New http connection for user admin, source 192.168.2.111 ACCEPTED
6	Jan 01 2023 11:29:16	notice	AAA-5-DISCONNECT: http connection for user admin, source 192.168.2.111 TERMINATED
7	Jan 01 2023 11:16:22	notice	AAA-5-CONNECT: New http connection for user admin, source 192.168.2.111 ACCEPTED
8	Jan 01 2023 09:55:19	warning	AAA-5-USER_REJECT: New http connection for user admin, source 192.168.2.111 REJECTED, aggregated (1)
9	Jan 01 2023 09:53:32	notice	PORT-4-LINK_UP: Interface GigabitEthernet20 link up, aggregated (1)
10	Jan 01 2023 09:55:30	notice	AAA-5-CONNECT: New http connection for user admin, source 192.168.2.111 ACCEPTED
11	Jan 01 2023 09:55:19	warning	AAA-5-USER_REJECT: New http connection for user admin, source 192.168.2.111 REJECTED
12	Jan 01 2023 09:53:34	notice	PORT-4-LINK_DOWN: Interface GigabitEthernet20 link down
13	Jan 01 2023 09:53:32	notice	PORT-5-LINK_UP: Interface GigabitEthernet20 link up
14	Jan 01 2023 00:00:17	notice	SYSTEM-5-WARMSTART: Warm startup

1

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: ● 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.**

Clear

Interface	
ifInOctets	0
ifInUcastPkts	0
ifInNUcastPkts	0
ifInDiscards	0

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

IV-1-3-2 Error Disabled

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

Item	Description
☐	Select one or more port to operate.
Port	Interface or port number.
Reason	Port will be disabled by one of the following error reason: ● BPDU Guard ● UDLD ● Self Loop

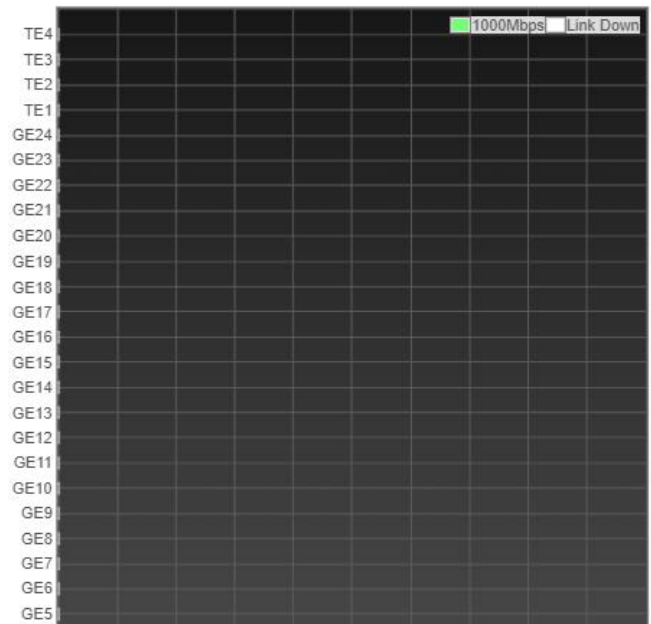
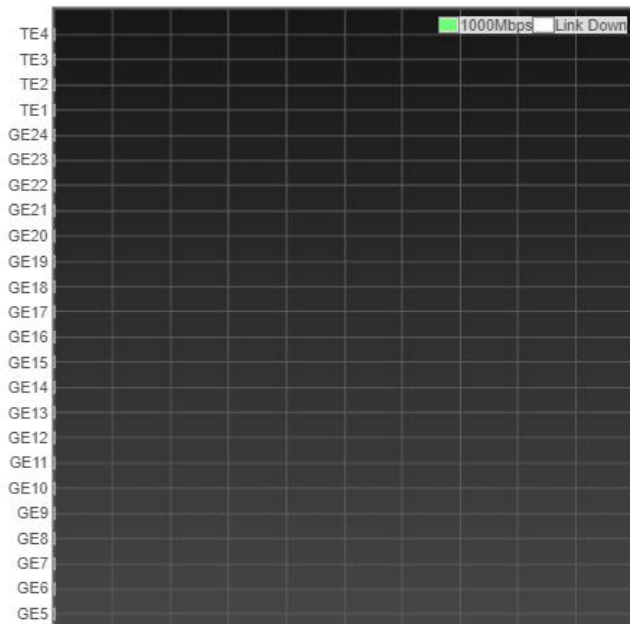
	● Broadcast Flood ● Unknown Multicast Flood ● Unicast Flood ● ACL ● Port Security Violation ● DHCP rate limit ● ARP rate limit
Time Left (sec)	The time left in second for the error recovery.
Refresh	Refresh the current page.
Recover	Recover the selected port status.

IV-1-3-3 Bandwidth Utilization

This page allow 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.**

Refresh Rate sec



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

IV-1-3-4 Link Aggregation

To display the Link Aggregation web page, click **Status > Link Aggregation**.
[Link Aggregation Table](#)

Q

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

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

IV-1-3-5 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**.

MAC Address Table

Showing All entries Showing 1 to 2 of 2 entries

VLAN	MAC Address	Type	Port
1	FC:8F:C4:0D:1E:F7	Management	CPU
1	A4:1F:72:57:57:9E	Dynamic	GE48

Clear Refresh

First Previous 1 Next Last

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

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, Click **Network > IP Address**.

IPv4 Address	
Address Type	☒ Static ☐ 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	☒ Enable
DHCPv6 Client	☐ 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

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

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

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

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

SNTP

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

Manual Time

Date	2021-08-30	YYYY-MM-DD
Time	14:57:44	HH:MM:SS

Daylight Saving Time

Type	☒ None ☐ Recurring ☐ Non-recurring ☐ USA ☐ European	
Offset	60	Min (1 - 1440, default 60)
Recurring	From: Day Sun ▼ Week First ▼ Month Jan ▼ Time	
	To: Day Sun ▼ Week First ▼ Month Jan ▼ Time	
Non-recurring	From: YYYY-MM-DD HH:MM	
	To: YYYY-MM-DD HH:MM	

Operational Status

Current Time	2021-08-30 14:57:44 UTC+8
--------------	---------------------------

Apply

Item	Description
Source	Select the time source. ● SNTP: Time sync from NTP server. ● From Computer: Time set from browser host. ● Manual Time: Time set by manually configure.
Time Zone	Select a time zone difference from listing district.
SNTP	
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. ● 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 >> Port Setting

Port Setting Table

☐	Entry	Port	Type	Description	State	Link Status	Speed	Flow Control
☐	1	GE1	1000M Fiber		Enabled	Down	Auto - 1000M	Disabled
☐	2	GE2	1000M Fiber		Enabled	Up	Auto - 1000M (1000M Full)	Disabled (Off)
☐	3	GE3	1000M Fiber		Enabled	Down	Auto - 1000M	Disabled
☐	4	GE4	1000M Fiber		Enabled	Down	Auto - 1000M	Disabled
☐	5	GE5	1000M Fiber		Enabled	Down	Auto - 1000M	Disabled
☐	6	GE6	1000M Fiber		Enabled	Down	Auto - 1000M	Disabled
☐	7	GE7	1000M Fiber		Enabled	Down	Auto - 1000M	Disabled
☐	8	GE8	1000M Fiber		Enabled	Down	Auto - 1000M	Disabled
☐	9	GE9	1000M Fiber		Enabled	Down	Auto - 1000M	Disabled
☐	10	GE10	1000M Fiber		Enabled	Down	Auto - 1000M	Disabled
☐	11	GE11	1000M Fiber		Enabled	Down	Auto - 1000M	Disabled
☐	12	GE12	1000M Fiber		Enabled	Down	Auto - 1000M	Disabled
☐	13	GE13	1000M Fiber		Enabled	Down	Auto - 1000M	Disabled
☐	14	GE14	1000M Fiber		Enabled	Down	Auto - 1000M	Disabled
☐	15	GE15	1000M Fiber		Enabled	Down	Auto - 1000M	Disabled
☐	16	GE16	1000M Fiber		Enabled	Down	Auto - 1000M	Disabled
☐	17	GE17	1000M Fiber		Enabled	Down	Auto - 1000M	Disabled
☐	18	GE18	1000M Fiber		Enabled	Down	Auto - 1000M	Disabled

Item	Description
Port	Port Name.
Type	Port media type.
Description	Port Description.
State	Port admin state ● Enabled: Enable the port. ● Disabled: Disable the port.

Link Status	Current port link status ● Up: Port is link up. ● Down: Port is link down.
Speed	Current port speed configuration and link speed status.
Duplex	Current port duplex configuration and link duplex status.
Flow Control	Current port flow control configuration and link flow control status.

Click “Edit” button to edit Port Setting menu

Edit Port Setting

Port

GE2

Description

Finace Dept

State

☒ Enable

Speed

☐ 100M/Full
☒ Auto-1000M

Flow Control

☐ Enable
☒ Disable

Apply

Close

Item	Description
Port	Selected Port list.
Description	Port media type.
State	Port admin state. ● Enabled: Enable the port. ● Disabled: Disable the port.
Speed	Port speed capabilities. ● 100M/Full: Speed with 100M ability. ● Auto-1000M: Auto speed with 1000M (Max.)
Flow Control	● Enabled: Enable flow control ability. ● Disabled: Disable flow control ability.

IV-3-2 Error Disable

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

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

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-3-3 Link Aggregation

IV-3-3-1 Group

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

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

Load Balance Algorithm

☒ MAC Address
☐ IP-MAC Address

Apply

Link Aggregation Table

Q

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

Edit

Item	Description
Load Balance Algorithm	LAG load balance distribution algorithm ● src-dst-mac: Based on MAC address. ● src-dst-mac-ip: Based on MAC address and IP address.
LAG	LAG Name.
Name	LAG port description.
Type	The type of the LAG ● Static: The group of ports assigned to a static LAG are always active members. ● LACP: The group of ports assigned to dynamic LAG are candidate ports. LACP determines which candidate ports are active member ports.

Link Status	LAG port link status
Active Member	Active member ports of the LAG.
Inactive Member	Inactive member ports of the LAG.

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

[Edit Link Aggregation Group](#)

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

IV-3-3-2 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

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

Edit

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

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

Edit Port Setting

Port	LAG1
Description	
State	☒ Enable
Speed	☒ Auto ☐ 10M ☐ Auto - 10M ☐ 100M ☐ Auto - 100M ☐ 1000M ☐ Auto - 1000M ☐ Auto - 10M/100M
Flow Control	☐ Auto ☐ Enable ☒ Disable

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

IV-3-3-3 LACP

This page allow 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**.

LACP Port Setting Table

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

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. ● 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

Item	Description
Port	Selected port list.
Port Priority	Enter the LACP priority value of the port

Item	Description
Port	Port Name
State	Port EEE admin state ● Enabled: EEE is enabled. ● Disabled: EEE is disabled.

IV-3-5 Jumbo Frame

This page allow user to configure switch jumbo frame size.

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

Jumbo Frame

☒ Enable

Byte (1518 - 10000, default 1522)

Apply

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

IV-4-1 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.

Use the VLAN pages to configure settings of 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.

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

VLAN

Available VLAN

VLAN 2

VLAN 3

VLAN 4

VLAN 5

VLAN 6

VLAN 7

VLAN 8

VLAN 9

>

<

Created VLAN

VLAN 1

Apply

VLAN Table

Showing All entries

Showing 1 to 1 of 1 entries

	VLAN	Name	Type
☐	1	default	Default

Edit

Delete

First

Previous

1

Next

Last

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. ● Static: Port base VLAN. ● Dynamic: 802.1q VLAN.

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

Edit VLAN Name

Name

VLAN0002

Apply

Close

Item	Description
Name	Input VLAN name.

IV-4-1-2 VLAN Configuration

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

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

Entry	Port	Mode	Membership	PVID
1	GE1	Trunk	☐ Excluded ☐ Forbidden ☐ Tagged ☒ Untagged	☒
2	GE2	Trunk	☐ Excluded ☐ Forbidden ☐ Tagged ☒ Untagged	☒
3	GE3	Trunk	☐ Excluded ☐ Forbidden ☐ Tagged ☒ Untagged	☒
4	GE4	Trunk	☐ Excluded ☐ Forbidden ☐ Tagged ☒ Untagged	☒
5	GE5	Trunk	☐ Excluded ☐ Forbidden ☐ Tagged ☒ Untagged	☒
6	GE6	Trunk	☐ Excluded ☐ Forbidden ☐ Tagged ☒ Untagged	☒
7	GE7	Trunk	☐ Excluded ☐ Forbidden ☐ Tagged ☒ Untagged	☒
8	GE8	Trunk	☐ Excluded ☐ Forbidden ☐ Tagged ☒ Untagged	☒
9	GE9	Trunk	☐ Excluded ☐ Forbidden ☐ Tagged ☒ Untagged	☒
10	GE10	Trunk	☐ Excluded ☐ Forbidden ☐ Tagged ☒ Untagged	☒
11	GE11	Trunk	☐ Excluded ☐ Forbidden ☐ Tagged ☒ Untagged	☒
12	GE12	Trunk	☐ Excluded ☐ Forbidden ☐ Tagged ☒ Untagged	☒
13	GE13	Trunk	☐ Excluded ☐ Forbidden ☐ Tagged ☒ Untagged	☒
14	GE14	Trunk	☐ Excluded ☐ Forbidden ☐ Tagged ☒ Untagged	☒
15	GE15	Trunk	☐ Excluded ☐ Forbidden ☐ Tagged ☒ Untagged	☒
16	GE16	Trunk	☐ Excluded ☐ Forbidden ☐ Tagged ☒ Untagged	☒
17	GE17	Trunk	☐ Excluded ☐ Forbidden ☐ Tagged ☒ Untagged	☒
18	GE18	Trunk	☐ Excluded ☐ Forbidden ☐ Tagged ☒ Untagged	☒
19	GE19	Trunk	☐ Excluded ☐ Forbidden ☐ Tagged ☒ Untagged	☒
20	GE20	Trunk	☐ Excluded ☐ Forbidden ☐ Tagged ☒ Untagged	☒
21	GE21	Trunk	☐ Excluded ☐ Forbidden ☐ Tagged ☒ Untagged	☒
22	GE22	Trunk	☐ Excluded ☐ Forbidden ☐ Tagged ☒ Untagged	☒
23	GE23	Trunk	☐ Excluded ☐ Forbidden ☐ Tagged ☒ Untagged	☒
24	GE24	Trunk	☐ Excluded ☐ Forbidden ☐ Tagged ☒ Untagged	☒

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. ● Forbidden: Specify the port is forbidden in the VLAN. ● Excluded: Specify the port is excluded in the VLAN. ● Tagged: Specify the port is tagged member in the VLAN. ● Untagged: Specify the port is untagged member in the VLAN.
PVID	Display if it is PVID of interface.

IV-4-1-3 Membership

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

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

Entry	Port	Mode	Administrative VLAN	Operational VLAN
1	GE1	Trunk	1UP	1UP
2	GE2	Trunk	1UP	1UP
3	GE3	Trunk	1UP	1UP
4	GE4	Trunk	1UP	1UP
5	GE5	Trunk	1UP	1UP
6	GE6	Hybrid	1U, 3UP	1U, 3UP
7	GE7	Trunk	1UP	1UP
8	GE8	Hybrid	1UP	1UP
9	GE9	Trunk	1UP	1UP
10	GE10	Trunk	1UP	1UP
11	GE11	Trunk	1UP	1UP
12	GE12	Trunk	1UP	1UP
13	GE13	Trunk	1UP	1UP
14	GE14	Trunk	1UP	1UP
15	GE15	Trunk	1UP	1UP
16	GE16	Trunk	1UP	1UP
17	GE17	Trunk	1UP	1UP
18	GE18	Trunk	1UP	1UP
19	GE19	Trunk	1UP	1UP
20	GE20	Trunk	1UP	1UP
21	GE21	Trunk	1UP	1UP
22	GE22	Trunk	1UP	1UP

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

Edit Port Setting

Port GE1

Mode Trunk

Membership

2 1UP

☐ Forbidden
☐ Excluded
☒ Tagged
☐ Untagged
☐ PVID

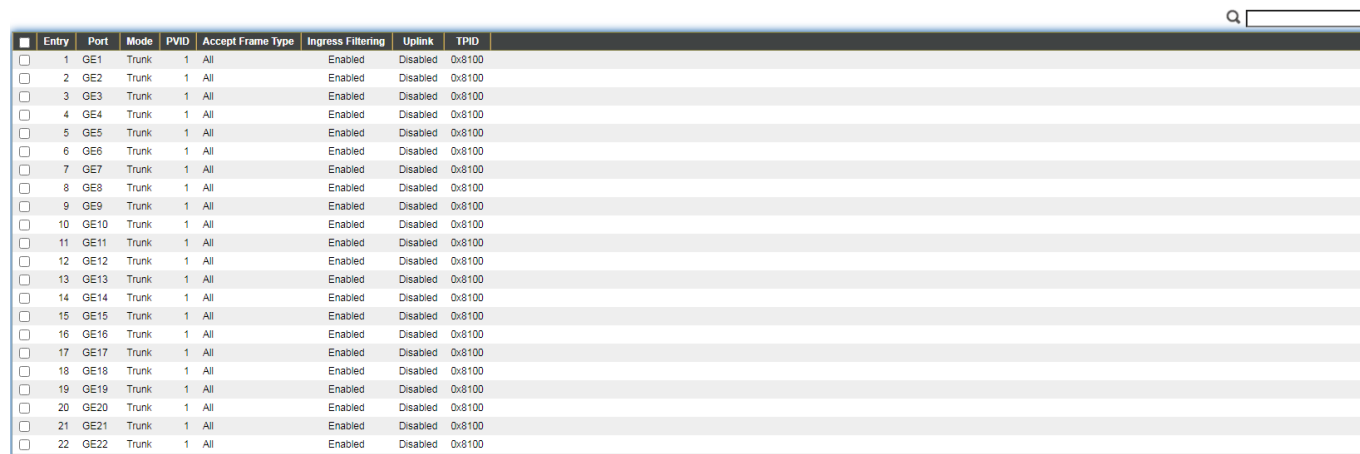
Apply Close

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

IV-4-1-4 Port Setting

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

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



Entry	Port	Mode	PVID	Accept Frame Type	Ingress Filtering	Uplink	TPID
☐	1 GE1	Trunk	1	All	Enabled	Disabled	0x8100
☐	2 GE2	Trunk	1	All	Enabled	Disabled	0x8100
☐	3 GE3	Trunk	1	All	Enabled	Disabled	0x8100
☐	4 GE4	Trunk	1	All	Enabled	Disabled	0x8100
☐	5 GE5	Trunk	1	All	Enabled	Disabled	0x8100
☐	6 GE6	Trunk	1	All	Enabled	Disabled	0x8100
☐	7 GE7	Trunk	1	All	Enabled	Disabled	0x8100
☐	8 GE8	Trunk	1	All	Enabled	Disabled	0x8100
☐	9 GE9	Trunk	1	All	Enabled	Disabled	0x8100
☐	10 GE10	Trunk	1	All	Enabled	Disabled	0x8100
☐	11 GE11	Trunk	1	All	Enabled	Disabled	0x8100
☐	12 GE12	Trunk	1	All	Enabled	Disabled	0x8100
☐	13 GE13	Trunk	1	All	Enabled	Disabled	0x8100
☐	14 GE14	Trunk	1	All	Enabled	Disabled	0x8100
☐	15 GE15	Trunk	1	All	Enabled	Disabled	0x8100
☐	16 GE16	Trunk	1	All	Enabled	Disabled	0x8100
☐	17 GE17	Trunk	1	All	Enabled	Disabled	0x8100
☐	18 GE18	Trunk	1	All	Enabled	Disabled	0x8100
☐	19 GE19	Trunk	1	All	Enabled	Disabled	0x8100
☐	20 GE20	Trunk	1	All	Enabled	Disabled	0x8100
☐	21 GE21	Trunk	1	All	Enabled	Disabled	0x8100
☐	22 GE22	Trunk	1	All	Enabled	Disabled	0x8100

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.

Edit Port Setting

Port

GE1

Mode

☐ Hybrid
☐ Access
☒ Trunk
☐ Tunnel

PVID

(1 - 4094)

Accept Frame Type

☒ All
☐ Tag Only
☐ Untag Only

Ingress Filtering

☒ Enable

Uplink

☐ Enable

TPID

Apply

Close

Item	Description
Port	Display selected port to be edited.
Mode	Select the VLAN mode of the interface. ● 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 Filtering	Set checkbox to enable/disable ingress filtering. It's only available with Hybrid mode.
Uplink	Set checkbox to enable/disable uplink mode. It's only available with trunk mode.
TPID	Select TPID used of interface. It's only available with trunk mode.

IV-4-2 Voice VLAN

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

IV-4-2-1 Property

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

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

State ☐ Enable
VLAN: None
CoS/802.1p ☐ Enable
Port Aging Time: 1440 (Min (30 - 65536, default 1440))
Note: Aging Time = Port Aging Time + QoS Aging Time(30 mins)

Apply

Port Setting Table

Entry	Port	State	Mode	QoS Policy
☐	1 GE1	Disabled	Auto	Voice Packet
☐	2 GE2	Disabled	Auto	Voice Packet
☐	3 GE3	Disabled	Auto	Voice Packet
☐	4 GE4	Disabled	Auto	Voice Packet
☐	5 GE5	Disabled	Auto	Voice Packet
☐	6 GE6	Disabled	Auto	Voice Packet
☐	7 GE7	Disabled	Auto	Voice Packet
☐	8 GE8	Disabled	Auto	Voice Packet
☐	9 GE9	Disabled	Auto	Voice Packet
☐	10 GE10	Disabled	Auto	Voice Packet
☐	11 GE11	Disabled	Auto	Voice Packet
☐	12 GE12	Disabled	Auto	Voice Packet
☐	13 GE13	Disabled	Auto	Voice Packet
☐	14 GE14	Disabled	Auto	Voice Packet
☐	15 GE15	Disabled	Auto	Voice Packet
☐	16 GE16	Disabled	Auto	Voice Packet
☐	17 GE17	Disabled	Auto	Voice Packet
☐	18 GE18	Disabled	Auto	Voice Packet
☐	19 LAG1	Disabled	Auto	Voice Packet

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.

Edit Port Setting

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

Apply

Close

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

IV-4-2-2 Voice OUI

This page allow 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 All entries

Showing 1 to 8 of 8 entries

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

Add

Edit

Delete

First

Previous

1

Next

Last

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

Apply

Close

Edit Voice OUI

OUI

00:03:6B

Description

Cisco

Apply

Close

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 Protocol VLAN

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

IV-4-3-1 Protocol Group

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

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

Protocol Group Table

Showing entries

Showing 0 to 0 of 0 entries

Search

Group ID	Frame Type	Protocol Value
0 results found.		

First Previous 1 Next Last

Item	Description
Group ID	Display group ID of entry.
Frame Type	This function maps packets to protocol-defined VLAN by examining the type octet within the packet header to discover the type of protocol associated with it.
Protocol Value	Display the Ether type of the target protocol.

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

Add Protocol Group

Group ID

Frame Type

Protocol Value 0x (0x600 ~ 0xFFFFE)

Item	Description
Group ID	Input group ID that is a unique ID of group entry. The range from 1 to8. Only available on Add Dialog.
Frame Type	Select a frame type (Ethernet_II, IEEE802.3_LL_C_Other, RFC_1042) for Group ID. - Ethernet_II: Packet type is Ethernet version 2.

	- IEEE802.3_LLC_Other: packet type is 802.3 packet with LLC other header. - RFC_1042: This RFC specifies a standard method of encapsulating the Internet Protocol (IP) datagrams and Address Resolution Protocol (ARP) requests and replies on IEEE 802 Networks to allow compatible and interoperable implementations. This RFC specifies a protocol standard for the Internet community.
Protocol Value	Input the Ether type of the target protocol.

IV-4-3-2 Group Binding

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

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

Group Binding Table

Showing entries

Showing 0 to 0 of 0 entries

Search

Port	Group ID	VLAN
0 results found.		

Item	Description
Port	Display port ID that binding with group entry.
Group ID	Display group ID that port binding with.
VLAN	Display VLAN ID that assigns to packets which match 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 Protocol VLAN

Group ID

VLAN

Apply

Close

Item	Description
Port	Select ports in left box then move to right to binding with group. Or select ports in right box then move to left to unbind with 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 group.

IV-4-4 MAC VLAN

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

IV-4-4-1 MAC Group

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

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

MAC Group Table

Showing All entries

Showing 0 to 0 of 0 entries

☐	Group ID	MAC Address	Mask
0 results found.			
Add Edit Delete First Previous 1 Next Last			

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

 (1 - 2147483647)

MAC Address

Mask

 (9 - 48)

Apply
Close

Edit MAC Group

Group ID

 undefined

MAC Address

Mask

 (9 - 48)

Apply
Close

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-4-4-2 Group Binding

This page allow 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.			
Add Edit Delete First Previous 1 Next Last			

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

VLAN

(1 - 4094)

Apply

Close

Edit Group Binding

Port	
Group ID	
VLAN	(1 - 4094)

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	300 Sec (10 - 630, default 300)
------------	--

Dynamic Address Table

Showing entries

Showing 1 to 1 of 1 entries

☐	VLAN	MAC Address	Port
☐	1	B8:6B:23:6D:C1:14	GE28

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 All ▼ entries Showing 0 to 0 of 0 entries

☐	VLAN	MAC Address	Port
0 results found.			

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**.

Filtering Address Table

Showing All ▼ entries Showing 0 to 0 of 0 entries

☐	VLAN	MAC Address
0 results found.		

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-5-4 Port Security Address

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

Showing All entries

Showing 0 to 0 of 0 entries

☐	VLAN	MAC Address	Type	Port
0 results found.				
AddEditDelete				

Add Port Security Address

MAC Address	
VLAN	(1 - 4094)
Port	GE1 ▼

ApplyClose

Item	Description
MAC Address	Specify The MAC address
VLAN	Specify the VLAN

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	☐ Enable	
Operation Mode	☐ STP ☒ RSTP ☐ MSTP	
Path Cost	☒ Long ☐ Short	
BPDU Handling	☐ Filtering ☒ Flooding	
Priority	32768	(0 - 61440, default 32768)
Hello Time	2	Sec (1 - 10, default 2)
Max Age	20	Sec (6 - 40, default 20)
Forward Delay	15	Sec (4 - 30, default 15)
Tx Hold Count	6	(1 - 10, default 6)
Region Name	74:DA:38:17:6E:7A	
Revision	0	(0 - 65535, default 0)
Max Hop	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	

Item	Description
State	Enable/disable the STP on the switch.
Operation Mode	Specify the STP operation mode. ● STP: Enable the Spanning Tree (STP) operation. ● RSTP: Enable the Rapid Spanning Tree (RSTP) operation. ● MSTP: Enable the Multiple Spanning Tree (MSTP) operation.
Path Cost	Specify the path cost method. ● Long: Specifies that the default port path costs are within the range: 1-200,000,000. ● Short: Specifies that the default port path costs are within the range: 1-65,535.
BPDU Handling	Specify the BPDU forward method when the STP is disabled. ● Filtering: Filter the BPDU when STP is disabled.

	● Flooding: Flood the BPDU when STP is disabled.
Priority	Specify the bridge priority. The valid range is from 0 to 61440, and the value should be the multiple of 4096. It ensures the probability that the switch is selected as the root bridge, and the lower value has the higher priority for the switch to be selected as the root bridge of the topology.
Hello Time	Specify the STP hello time in second to broadcast its hello message to other bridges by Designated Ports. Its valid range is from 1 to 10 seconds.
Max Age	Specify the time interval in seconds for a switch to wait the configuration messages, without attempting to redefine its own configuration.
Forward Delay	Specify the STP forward delay time, which is the amount of time that a port remains in the Listening and Learning states before it enters the Forwarding state. Its valid range is from 4 to 10 seconds.
TX Hold Count	Specify the tx-hold-count used to limit the maximum numbers of packets transmission per second. The valid range is from 1 to 10.
Region Name	The MSTP instance name. Its maximum length is 32 characters. The default value is the MAC address of the switch.
Revision	The MSTP revision number. Its valid range is from 0 to 65535.
Max 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	Enabled	Root	Forwarding	32768-2C:FA:A2:5C:2D:62	128-1	20000
☐	2	GE2	Enabled	200000	128	Disabled	Disabled	Disabled	Enabled	Designated	Forwarding	32768-FC:8F:C4:0D:1A:B5	128-2	200000
☐	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	200000	128	Disabled	Disabled	Disabled	Enabled	Designated	Forwarding	32768-FC:8F:C4:0D:1A:B5	128-16	200000
☐	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

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 (0 - 200000000) (0 = Auto)
Priority	128 ▼
Edge Port	☐ Enable
BPDU Filter	☐ Enable
BPDU Guard	☐ Enable
Point-to-Point	☒ Auto ☐ Enable ☐ Disable
Port State	Disabled
Designated Bridge	0-00:00:00:00:00:00
Designated Port ID	128-1
Designated Cost	20000
Operational Edge	False
Operational Point-to-Point	False

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. ● 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 BPDUs from the specified ports. ● Enable: Enable BPDU filter function.

	● Disable: Disable BPDU filter function.
BPDUGuard	The BPDU Guard configuration to drop the received BPDU directly. ● Enable: Enable BPDU guard function. ● Disable: Disable BPDU guard function.
Point-to-Point	Specify the Point-to-Point port configuration: ● Auto: The state is depended on the duplex setting of the port ● Enable: Force to true state. ● Disable: Force to false state

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
☐	0	32768	32768-74:DA:38:17:6E:7A	0-00:00:00:00:00:00	N/A	0	0	1-4094
☐	1	32768	32768-74:DA:38:17:6E:7A	0-00:00:00:00:00:00	N/A	0	0	
☐	2	32768	32768-74:DA:38:17:6E:7A	0-00:00:00:00:00:00	N/A	0	0	
☐	3	32768	32768-74:DA:38:17:6E:7A	0-00:00:00:00:00:00	N/A	0	0	
☐	4	32768	32768-74:DA:38:17:6E:7A	0-00:00:00:00:00:00	N/A	0	0	
☐	5	32768	32768-74:DA:38:17:6E:7A	0-00:00:00:00:00:00	N/A	0	0	
☐	6	32768	32768-74:DA:38:17:6E:7A	0-00:00:00:00:00:00	N/A	0	0	
☐	7	32768	32768-74:DA:38:17:6E:7A	0-00:00:00:00:00:00	N/A	0	0	
☐	8	32768	32768-74:DA:38:17:6E:7A	0-00:00:00:00:00:00	N/A	0	0	
☐	9	32768	32768-74:DA:38:17:6E:7A	0-00:00:00:00:00:00	N/A	0	0	
☐	10	32768	32768-74:DA:38:17:6E:7A	0-00:00:00:00:00:00	N/A	0	0	
☐	11	32768	32768-74:DA:38:17:6E:7A	0-00:00:00:00:00:00	N/A	0	0	
☐	12	32768	32768-74:DA:38:17:6E:7A	0-00:00:00:00:00:00	N/A	0	0	
☐	13	32768	32768-74:DA:38:17:6E:7A	0-00:00:00:00:00:00	N/A	0	0	
☐	14	32768	32768-74:DA:38:17:6E:7A	0-00:00:00:00:00:00	N/A	0	0	
☐	15	32768	32768-74:DA:38:17:6E:7A	0-00:00:00:00:00:00	N/A	0	0	

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

Priority

(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

Root Path Cost

0

Remaining Hop

0

Apply

Close

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**.

	Entry	Port	Path Cost	Priority	Port Role	Port State	Mode	Type	Designated Bridge	Designated Port ID	Designated Cost	Remaining Hop
☐	1	GE1	20000	128	Root	Forwarding	RSTP	Boundary	32768-2C:FA:A2:5C:2D:62	128-1	20000	20
☐	2	GE2	200000	128	Designated	Forwarding	RSTP	Boundary	32768-FC:8F:C4:0D:1A:B5	128-2	200000	20
☐	3	GE3	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-3	20000	20
☐	4	GE4	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-4	20000	20
☐	5	GE5	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-5	20000	20
☐	6	GE6	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-6	20000	20
☐	7	GE7	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-7	20000	20
☐	8	GE8	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-8	20000	20
☐	9	GE9	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-9	20000	20
☐	10	GE10	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-10	20000	20
☐	11	GE11	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-11	20000	20
☐	12	GE12	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-12	20000	20
☐	13	GE13	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-13	20000	20
☐	14	GE14	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-14	20000	20
☐	15	GE15	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-15	20000	20
☐	16	GE16	200000	128	Designated	Forwarding	RSTP	Boundary	32768-FC:8F:C4:0D:1A:B5	128-16	200000	20
☐	17	GE17	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-17	20000	20
☐	18	GE18	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-18	20000	20
☐	19	GE19	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-19	20000	20
☐	20	GE20	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-20	20000	20
☐	21	GE21	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-21	20000	20
☐	22	GE22	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-22	20000	20
☐	23	GE23	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-23	20000	20
☐	24	GE24	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-24	20000	20
☐	25	XGE1	2000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-25	2000	20
☐	26	XGE2	2000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-26	2000	20
☐	27	XGE3	2000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-27	2000	20
☐	28	XGE4	2000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-28	2000	20
☐	29	LAG1	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-29	20000	20
☐	30	LAG2	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-30	20000	20
☐	31	LAG3	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-31	20000	20
☐	32	LAG4	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-32	20000	20
☐	33	LAG5	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-33	20000	20
☐	34	LAG6	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-34	20000	20
☐	35	LAG7	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-35	20000	20
☐	36	LAG8	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-36	20000	20

Edit

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

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

Edit MST Port Setting

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

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**.

☐	Entry	Port	Receive BPDU			Transmit BPDU			
			Config	TCN	MSTP	Config	TCN	MSTP	
☐	1	GE1	0	0	560479	0	0	36	
☐	2	GE2	0	0	0	0	0	560493	
☐	3	GE3	0	0	0	0	0	0	
☐	4	GE4	0	0	0	0	0	0	
☐	5	GE5	0	0	0	0	0	0	
☐	6	GE6	0	0	0	0	0	188	
☐	7	GE7	0	0	0	0	0	0	
☐	8	GE8	0	0	0	0	0	0	
☐	9	GE9	0	0	0	0	0	0	
☐	10	GE10	0	0	0	0	0	0	
☐	11	GE11	0	0	0	0	0	0	
☐	12	GE12	0	0	0	0	0	0	
☐	13	GE13	0	0	0	0	0	0	
☐	14	GE14	0	0	0	0	0	0	
☐	15	GE15	0	0	0	0	0	0	
☐	16	GE16	0	0	0	0	0	209558	
☐	17	GE17	0	0	0	0	0	0	
☐	18	GE18	0	0	0	0	0	0	

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	☒ None ☐ 5 sec ☐ 10 sec ☐ 30 sec
Receive BPDU	
Config	0
TCN	0
MSTP	0
Transmit BPDU	
Config	0
TCN	0
MSTP	0

RefreshClearClose

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 (Link Layer Discovery Protocol)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 (Link Layer Discovery Protocol-Media Endpoint Discovery)pages.

IV-7-1-1 Property

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

LLDP

State

☒ Enable

LLDP Handling

☐ Filtering
☐ Bridging
☒ Flooding

TLV Advertise Interval

Sec (5 - 32767, default 30)

Hold Multiplier

(2 - 10, default 4)

Reinitializing Delay

Sec (1 - 10, default 2)

Transmit Delay

Sec (1 - 8191, default 2)

LLDP-MED

Fast Start Repeat Count

(1 - 10, default 3)

Apply

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. ● Filtering: Deletes the packet. ● Bridging: (VLAN-aware flooding) Forwards the packet to all VLAN members. ● Flooding: Forwards the packet to all ports
TLV Advertise Interval	Select the interval at which frames are transmitted. The default is 30 seconds, and the valid range is 5–32767 seconds.
Hold Multiplier	Select the multiplier on the transmit interval to assign to TTL (range 2–10, default = 4).
Reinitializing 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**.

Entry	Port	Mode	Selected TLV
☐	1 GE1	Normal	802.1 PVID
☐	2 GE2	Normal	802.1 PVID
☐	3 GE3	Normal	802.1 PVID
☐	4 GE4	Normal	802.1 PVID
☐	5 GE5	Normal	802.1 PVID
☐	6 GE6	Normal	802.1 PVID
☐	7 GE7	Normal	802.1 PVID
☐	8 GE8	Normal	802.1 PVID
☐	9 GE9	Normal	802.1 PVID
☐	10 GE10	Normal	802.1 PVID
☐	11 GE11	Normal	802.1 PVID
☐	12 GE12	Normal	802.1 PVID
☐	13 GE13	Normal	802.1 PVID
☐	14 GE14	Normal	802.1 PVID
☐	15 GE15	Normal	802.1 PVID
☐	16 GE16	Normal	802.1 PVID

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

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

Edit Port Setting

Port

Mode

Optional TLV

802.1 VLAN Name

GE1

Transmit

Receive

Normal

Disable

Available TLV

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

Selected TLV

802.1 PVID

Available VLAN

VLAN 1
VLAN 2

Selected VLAN

Apply

Close

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

IV-7-1-3 MED Network Policy

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

Edit MED Network Policy

Policy ID	undefined
Application	Voice
VLAN	2 Range (1 - 4094)
VLAN Tag	☐ Tagged ☒ Untagged
Priority	0
DSCP	0

Apply Close

Item	Description
Policy ID	Showing the MED Network is defined or undefined.
Application	Define an application for LLDP. ● Voice ● Voice Signaling ● Guest Voice ● Guest Voice Signaling ● Softphone Voice ● Video Conferencing ● Streaming Video ● Video Signaling
VLAN	Configure VLAN (Valid values are from 1 to 4094)
VLAN Tag	Define VLAN Tag (Tagged/Untagged). VLAN tagging is used to tell which packet belongs to which VLAN on the other side. To make recognition easier, a packet is tagged with a VLAN tag in the Ethernet frame.
Priority	Define the priority
DSCP	Enter a Differentiated Services Code Point (DSCP)

IV-7-1-4 MED Port Setting

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

MED Port Setting Table

	Entry	Port	State	Network Policy		Location	Inventory
				Active	Application		
☐	1	GE1	Enabled	Yes		No	No
☐	2	GE2	Enabled	Yes		No	No
☐	3	GE3	Enabled	Yes		No	No
☐	4	GE4	Enabled	Yes		No	No
☐	5	GE5	Enabled	Yes		No	No
☐	6	GE6	Enabled	Yes		No	No
☐	7	GE7	Enabled	Yes		No	No
☐	8	GE8	Enabled	Yes		No	No
☐	9	GE9	Enabled	Yes		No	No
☐	10	GE10	Enabled	Yes		No	No
☐	11	GE11	Enabled	Yes		No	No
☐	12	GE12	Enabled	Yes		No	No
☐	13	GE13	Enabled	Yes		No	No
☐	14	GE14	Enabled	Yes		No	No
☐	15	GE15	Enabled	Yes		No	No
☐	16	GE16	Enabled	Yes		No	No
☐	17	GE17	Enabled	Yes		No	No
☐	18	GE18	Enabled	Yes		No	No
☐	19	GE19	Enabled	Yes		No	No
☐	20	GE20	Enabled	Yes		No	No

Item	Description
Entry	Entry of number.
Port	Port Name.
State	Status of LLDP (Enabled or Disabled).
Network Policy	Display LLDP whether active.
Location	MED location.
Inventory	MED Inventory.

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

Edit MED Port Setting

Port
GE1

State
☒ Enable

Optional TLV

Available TLV

Location
Extended Power-via-MDI
Inventory

>
<

Selected TLV

Network Policy

Network policy

Available Policy

>
<

Selected Policy

Location

Coordinate

(16 pairs of hexadecimal characters)

Civic

(6-160 pairs of hexadecimal characters)

ECS ELIN

(10-25 pairs of hexadecimal characters)

Apply

Close

Item	Description
Port	Port Name.
State	Enable/ Disable MED Port on this switch.
Optional TLV	Select the LLDP optional TLVs to be carried (multiple selection is allowed). ● Location ● Extended Power-via-MDI ● Inventory

	● Network Policy
Network Policy	Select the Network Policy to be carried
Coordinate	Configures a coordinate-based location for an endpoint device.
Civic	Configures a civic-address-based location for Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED)
ECS ELIN	Configures an Emergency Call Service (ECS) based location for Link Layer Discovery Protocol Media Endpoint Device (LLDP-MED)

IV-7-1-5 Packet View

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

Entry	Port	In-Use (Bytes)	Available (Bytes)	Operational Status
1	GE1	48	1440	Not Overloading
2	GE2	48	1440	Not Overloading
3	GE3	48	1440	Not Overloading
4	GE4	48	1440	Not Overloading
5	GE5	48	1440	Not Overloading
6	GE6	48	1440	Not Overloading
7	GE7	48	1440	Not Overloading
8	GE8	48	1440	Not Overloading
9	GE9	48	1440	Not Overloading
10	GE10	49	1439	Not Overloading
11	GE11	49	1439	Not Overloading
12	GE12	49	1439	Not Overloading
13	GE13	49	1439	Not Overloading
14	GE14	49	1439	Not Overloading
15	GE15	49	1439	Not Overloading
16	GE16	49	1439	Not Overloading
17	GE17	49	1439	Not Overloading
18	GE18	65	1423	Not Overloading
19	GE19	49	1439	Not Overloading
20	GE20	49	1439	Not Overloading
21	GE21	49	1439	Not Overloading
22	GE22	49	1439	Not Overloading
23	GE23	49	1439	Not Overloading
24	GE24	49	1439	Not Overloading
25	XGE1	49	1439	Not Overloading
26	XGE2	49	1439	Not Overloading
27	XGE3	49	1439	Not Overloading
28	XGE4	49	1439	Not Overloading

Detail

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

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-7-1-6 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:C4:0D:1D:EC
System Name	Switch
System Description	CG 5040PL-C

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

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 Enabled	Primary enabled functions of the device.
Port ID Subtype	Type of the port identifier that is shown.
LLDP Status	LLDP Tx and Rx abilities.
LLDP Med Status	LLDP MED enable state.

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

Local Information Detail

Chassis ID Subtype	MAC address
Chassis ID	74:DA:38:17:6E:7A
System Name	Switch
System Description	24-Port Gigabit PoE+ Smart Managed Switch with 4 RJ45/SFP Combo Ports
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

MED Detail

Capabilities Supported	Capabilities , Network policy
Current Capabilities	Capabilities , Network policy
Device Class	Network Connectivity
PoE Device Type	N/A
PoE Power Source	N/A
PoE Power Priority	N/A
PoE Power Value	N/A
Hardware Revision	N/A
Firmware Revision	N/A
Software Revision	N/A
Serial Number	N/A
Manufacturer Name	N/A
Model Name	N/A
Asset ID	N/A

Location Information

Civic	N/A
Coordinate	N/A
ECS ELIN	N/A

Network Policy Table

Application Type	VLAN	VLAN Type	Priority	DSCP
0 results found.				

Close

IV-7-1-7 Neighbor

Use the LLDP Neighbor page to view LLDP neighbors information.

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

Neighbor Table

Showing All entries
Showing 0 to 0 of 0 entries

Q

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

Clear

Refresh

Detail

First

Previous

1

Next

Last

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

Basic Detail

Chassis ID Subtype	Unknown
Chassis ID	
Port ID Subtype	Unknown
Port ID	
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	N/A
Auto-Negotiation Enabled	N/A
Auto-Negotiation Advertised Capabilities	N/A
Operational MAU Type	N/A

802.3 Power via MDI		
	MDI Power Support Port Class	N/A
	PSE MDI Power Support	N/A
	PSE MDI Power State	N/A
	PSE Power Pair Control Ability	N/A
	PSE Power Pair	N/A
	PSE Power Class	N/A
	Power Type	N/A
	Power Source	N/A
	Power Priority	N/A
	PD Request Power Value	N/A
	PSE Allocated Power Value	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
802.1 VLAN and Protocol		
	PVID	
	VLAN Name	N/A
MED Detail		
	Capabilities Supported	N/A
	Current Capabilities	N/A
	Device Class	N/A
	PoE Device Type	N/A
	PoE Power Source	N/A
	PoE Power Priority	N/A
	PoE Power Value	N/A
	Hardware Revision	N/A
	Firmware Revision	N/A
	Software Revision	N/A
	Serial Number	N/A
	Manufacturer Name	N/A
	Model Name	N/A
	Asset ID	N/A

Location Information

Civic	N/A
Coordinate	N/A
ECS ELIN	N/A

Network Policy Table

Application Type	VLAN	VLAN Type	Priority	DSCP
0 results found.				

Close

IV-7-1-8 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	4
Deletions	2
Drops	0
AgeOuts	0

Clear

Refresh

Entry	Port	Transmit Frame		Receive Frame				Receive TLV			Neighbor Timeout
		Total	Total	Total	Discard	Error	Discard	Unrecognized			
☐	1 GE1	112157	74775	0	0	0	0	0	0	0	0
☐	2 GE2	112169	0	0	0	0	0	0	0	0	0
☐	3 GE3	0	0	0	0	0	0	0	0	0	0
☐	4 GE4	0	0	0	0	0	0	0	0	0	0
☐	5 GE5	0	0	0	0	0	0	0	0	0	0
☐	6 GE6	39	0	0	0	0	0	0	0	0	0
☐	7 GE7	0	0	0	0	0	0	0	0	0	0
☐	8 GE8	0	0	0	0	0	0	0	0	0	0
☐	9 GE9	0	0	0	0	0	0	0	0	0	0
☐	10 GE10	0	0	0	0	0	0	0	0	0	0
☐	11 GE11	0	0	0	0	0	0	0	0	0	0
☐	12 GE12	0	0	0	0	0	0	0	0	0	0
☐	13 GE13	0	0	0	0	0	0	0	0	0	0
☐	14 GE14	0	0	0	0	0	0	0	0	0	0
☐	15 GE15	0	0	0	0	0	0	0	0	0	0
☐	16 GE16	41974	0	0	0	0	0	0	0	0	0
☐	17 GE17	0	0	0	0	0	0	0	0	0	0
☐	18 GE18	0	0	0	0	0	0	0	0	0	0
☐	19 GE19	0	0	0	0	0	0	0	0	0	0
☐	20 GE20	0	0	0	0	0	0	0	0	0	0
☐	21 GE21	0	0	0	0	0	0	0	0	0	0
☐	22 GE22	0	0	0	0	0	0	0	0	0	0
☐	23 GE23	0	0	0	0	0	0	0	0	0	0
☐	24 GE24	0	0	0	0	0	0	0	0	0	0
☐	25 XGE1	0	0	0	0	0	0	0	0	0	0
☐	26 XGE2	0	0	0	0	0	0	0	0	0	0
☐	27 XGE3	0	0	0	0	0	0	0	0	0	0
☐	28 XGE4	0	0	0	0	0	0	0	0	0	0

Clear

Refresh

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.**

Unknown Multicast Action

☒ Flood
☐ Drop
☐ Forward to Router Port

Multicast Forward Method

IPv4 ☒ DMAC-VID ☐ DIP-VID

IPv6 ☒ DMAC-VID ☐ DIP-VID

Apply

Item	Description
Unknown Multicast Action	Set the unknown multicast action ● 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. ● MAC-VID: forward method dmac+vid. ● DIP-VID: forward method dip+vid.
IPv6	Set the ipv6 multicast forward method. ● MAC-VID: forward method dmac+vid. ● DIP-VID: forward method dip+vid(dip is ipv6 low 32 bit).

IV-8-1-2 Group Address

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

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

Group Address Table

IP Version IPv4 ▼

Showing All ▼ entries

Showing 0 to 0 of 0 entries

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

First Previous **1** Next Last

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

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

Add Group Address

VLAN

1 ▼

IP Version

IPv4 ▼

Group Address

Member

Available Port

GE1
GE2
GE3
GE4
GE5
GE6
GE7
GE8

>
<

Selected Port

Edit Group Address

VLAN	1
Group Address	225.0.0.1
Member	Available Port Selected Port GE2 GE3 GE4 GE5 GE6 GE7 GE8 GE9 > GE1 <

Apply Close

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

IV-8-1-3 Router Port

This page allow 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**.

Router Port Table

IP Version IPv4 ▼

Showing All ▼ entries

Showing 0 to 0 of 0 entries

☐	VLAN	Member	Static Port	Forbidden Port	Life (Sec)
0 results found.					

First Previous 1 Next Last

Add Edit Refresh

Item	Description
IP Version	IP Version ● IPv4: ipv4 multicast router ● IPv6: ipv6 multicast router
VLAN	The VLAN ID router entry.
Member	Router Port member (include static and learned port member).
Static Port	Static router port member.
Forbidden	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.

Add Router Port

VLAN	Available VLAN	Selected VLAN
	1	
IP Version	IPv4	
Type	☒ Static ☐ Forbidden	
Port	Available Port	Selected Port
	GE1	
	GE2	
	GE3	
	GE4	
	GE5	
	GE6	
	GE7	
	GE8	

ApplyClose

Edit Router Port

VLAN	1	
IP Version	IPv4	
Type	☒ Static ☐ Forbidden	
Port	Available Port	Selected Port
	GE2	GE1
	GE3	
	GE4	
	GE5	
	GE6	
	GE7	
	GE8	
	GE9	

ApplyClose

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

IV-8-1-4 Forward All

This page allow user to browse all forward port information.

Forward All Table

IP Version IPv4 ▾

Showing All ▾ entries Showing 0 to 0 of 0 entries Q

☐	VLAN	Static Port	Forbidden Port
0 results found.			

Add
Edit
Delete
First
Previous
1
Next
Last

Item	Description
IP Version	IP Version ● IPv4 ● IPv6
VLAN	The VLAN ID entry.
Static Port	Static port member.
Forbidden	Forbidden port member.

Click "**Add**" or "**Edit**" button to view Add/Edit Forward All menu

Add Forward All

VLAN	Available VLAN 1 Selected VLAN
IP Version	IPv4 ▼
Type	☒ Static ☐ Forbidden
Port	Available Port GE1 GE2 GE3 GE4 GE5 GE6 GE7 GE8 Selected Port

Apply Close

Item	Description
VLAN	The VLAN ID for forwarding entry ● Available VLAN: Optional VLAN member ● Selected VLAN: Selected VLAN member.
IP Version	IP Version ● IPv4 ● IPv6
Type	The router port type ● Static ● Forbidden
Port	The member ports of forward port entry. ● Available Port: Optional port member ● Selected Port: Selected port member

IV-8-1-5 Throttling

This page allow user to browse throttling port information.

Multicast throttling sets a maximum number of multicast groups that a port can join at the same time. When the maximum number of groups is reached on a port, the switch can take one of two actions; either “deny” or “replace”. If the action is set to deny, any new multicast join reports will be dropped. If the action is set to replace, the switch randomly removes an existing group and replaces it with the new multicast group.

Throttling Table

IP Version IPv4

	Entry	Port	Max Group	Exceed Action
☐	1	GE1	256	Deny
☐	2	GE2	256	Deny
☐	3	GE3	256	Deny
☐	4	GE4	256	Deny
☐	5	GE5	256	Deny
☐	6	GE6	256	Deny
☐	7	GE7	256	Deny
☐	8	GE8	256	Deny
☐	9	GE9	256	Deny
☐	10	GE10	256	Deny
☐	11	GE11	256	Deny
☐	12	GE12	256	Deny
☐	13	GE13	256	Deny
☐	14	GE14	256	Deny
☐	15	GE15	256	Deny
☐	16	GE16	256	Deny
☐	17	GE17	256	Deny

Item	Description
IP Version	IP Version ● IPv4 ● IPv6
Entry	Port number
Port	Port name
Max Group	Display the maximum number of multicast groups an interface can join at the same time.
Exceed action	Display the status of the action to take when the maximum number of multicast groups for the interface has been exceeded.

Click "**Add**" or "**Edit**" button to view Add/Edit Throttling Port menu

Edit Throttling

Port

GE1

IP Version

IPv4

Max Group

256

(0 - 256)

Exceed Action

☒ Deny

☐ Replace

Apply

Close

Item	Description
Port	Port name
IP Version	P Version ● IPv4 ● IPv6
Max Group	Sets the maximum number of multicast groups an interface can join at the same time. Range: 0-256 Default: 256
Exceed action	Sets the action to take when the maximum number of multicast groups for the interface has been exceeded. Deny: The new multicast group join report is dropped Replace: The new multicast group replaces an existing group

IV-8-1-6 Filtering Profile

This page allow user to browse filtering profile information.

Filtering Profile Table

IP Version

IPv4

Showing

All

entries

Showing 0 to 0 of 0 entries

Q

☐

Profile ID

Start Address

End Address

Action

0 results found.

Add

Edit

Delete

First

Previous

1

Next

Last

Item	Description
IP Version	IP Version ● IPv4 ● IPv6
Profile ID	Display the current ID.
Start Address	Display the current Start Address.
End Address	Display the current End Address.
Action	Display the current action.

Click "**Add**" or "**Edit**" button to view Add/Edit Filtering Profile menu.

Add Profile

Profile ID

 (1 - 128)

IP Version

IPv4 ▾

Start Address

End Address

Action

☒ Allow
 ☐ Deny

Apply

Close

Item	Description
Profile ID	Enter the ID of this particular profile
IP Version	IP Version ● IPv4 ● IPv6
Start Address	Specify a multicast group range by entering a start IP address.
End Address	Specify a multicast group range by entering an end IP address.

Action	Sets the access mode of the profile either Allow or Deny. Allow: Multicast join reports are processed when a multicast group falls within the controlled range. Deny: When the access mode is set to, multicast join reports are only processed when the multicast group is not in the controlled range.
--------	---

IV-8-1-7 Filtering Binding

This page allow user to browse filtering binding information.

Filtering Binding Table

IP Version IPv4

Q

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

Item	Description
IP Version	IP Version ● IPv4 ● IPv6
Entry	Display the port number.
Port	Display the current port.
Profile ID	Display the current filter profile ID.

Click "**Add**" or "**Edit**" button to view Add/Edit Filtering Binding menu.

Edit Filtering Binding

Port	GE1
IP Version	IPv4
Profile ID	☐ Enable ▼

Apply Close

Item	Description
Port	Display the current port.
IP Version	IP Version ● IPv4 ● IPv6
Profile ID	Enable/Disable Profile ID.

IV-8-2 IGMP Snooping

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

IV-8-2-1 Property

This page allow 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**.

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

VLAN Setting Table

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

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

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 allow 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

Q

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

Edit

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	The IGMP Snooping querier operational version.
Querier IP	The operational Querier IP address on the VLAN.

Click "Edit" button to view Edit Querier menu.

Edit Querier

VLAN

1

State

☐ Enable

Version

☒ IGMPv2

☐ IGMPv3

Apply

Close

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 - IGMPv2: Querier version 2. - IGMPv3: Querier version 3. (IGMP Snooping version should be IGMPv3)

IV-8-2-3 Statistics

This page allow user to clear IGMP snooping statics.

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

Receive Packet		
Total	91	
Valid	8	
InValid	83	
Other	0	
Leave	0	
Report	0	
General Query	0	
Special Group Query	0	
Source-specific Group Query	0	
Transmit Packet		
Leave	0	
Report	0	
General Query	0	
Special Group Query	0	
Source-specific Group Query	0	

Clear

Refresh

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	Other data packet.
Leave	IGMP leave packet.
Report	IGMP join and report packet.
General Query	IGMP General Query packet.
Special Group Query	IGMP Special Group General Query packet.

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

IV-8-3 MLD Snooping

This page provides MLD Snooping related configuration. Most of the settings are global, whereas the Router Port configuration is related to the current unit, as reflected by the page header.

IV-8-3-1 Property

State	☐ Enable
Version	☒ MLDv1 ☐ MLDv2
Report Suppression	☒ Enable

Apply

Item	Description
State	Set the enabling status of MLD Snooping functionality Enable: If Checked Enable MLD Snooping, else is Disabled MLD Snooping.
Version	Set the MLD Snooping version ● IGMPv2: Only support process igmp v2 packet. ● IGMPv3: Support v3 basic and v2.
Report Suppression	Limits the membership report traffic sent to multicast-capable routers. When you disable report suppression, all MLD reports are sent as is to multicast-capable routers.

VLAN Setting Table

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

Item	Description
VLAN	Display the current entry number
Operational Status	Display the current MLD snooping operation status
Router Port Auto Learn	Display the current router ports auto learning
Query Robustness	Display the current query robustness
Query Interval	Display the current query interval
Query Max Response Interval	Display the current query max response interval
Last Member Query Counter	Display the current last member query count
Last Member Query Interval	Display the current last member query interval
Immediate Leave	Display the current immediate leave

Click “**Edit**” button to edit parameter.

Edit VLAN Setting

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

Item	Description
VLAN	The selected VLAN List.
State	Set the enabling status of MLD Snooping VLAN functionality Enable: If Checked Enable MLD Snooping VLAN, else is Disabled MLD Snooping VLAN.
Router Port Auto Learn	Set the enabling status of MLD Snooping router port learning Enable: If checked Enable learning router port by query and PIM, DVRMP, else Disable the learning router port.
Immediate leave	Immediate Leave the group when receive MLD Leave message. Enable: If checked Enable immediate leave, else disable immediate leave.
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	The Admin query max response interval , In Membership

Response Interval	Query Messages, it specifies the maximum allowed time before sending a responding report in units of 1/10 second.
Last Member Query Counter	The Admin last member query count that Querier-switch sends Group-Specific Queries when it receives a Leave Group message for a group.
Last Member Query Interval	The Admin last member query interval that Querier-switch sends Group-Specific Queries when it receives a Leave Group message for a group.
Operational Status	
Status	Operational MLD snooping status , must both MLD snooping global and 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-8-3-2 Statistics

State	☐ Enable
Version	☒ MLDv1 ☐ MLDv2
Report Suppression	☒ Enable

Apply

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

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

Clear

Refresh

IV-8-4 MVR

Use the MVR pages to configure settings of MVR function.

IV-8-4-1 Property

State	☐ Enable
Version	☒ MLDv1 ☐ MLDv2
Report Suppression	☒ Enable

Apply

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

State	☐ Enable
VLAN	1 ▼
Mode	☒ Compatible ☐ Dynamic
Group Start	0.0.0.0
Group Count	1 (1 - 128)
Query Time	1 Sec (1 - 10)

Operational Group	
Maximum	128
Current	0

Apply

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 ● 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-8-4-2 Port Setting

This page allow 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**.

Entry	Port	Role	Immediate Leave
1	GE1	None	Disabled
2	GE2	None	Disabled
3	GE3	None	Disabled
4	GE4	None	Disabled
5	GE5	None	Disabled
6	GE6	None	Disabled
7	GE7	None	Disabled
8	GE8	None	Disabled
9	GE9	None	Disabled
10	GE10	None	Disabled
11	GE11	None	Disabled
12	GE12	None	Disabled
13	GE13	None	Disabled
14	GE14	None	Disabled
15	GE15	None	Disabled
16	GE16	None	Disabled
17	GE17	None	Disabled
18	GE18	None	Disabled
19	GE19	None	Disabled
20	GE20	None	Disabled
21	GE21	None	Disabled

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.

Edit Port Setting

Port

GE1

Role

☒ None
☐ Receiver
☐ Source

Immediate Leave

☐ Enable

Apply

Close

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

IV-8-4-3 Group Address

This page allow 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**.

Group Address Table

Showing All entries

Showing 0 to 0 of 0 entries

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

First Previous **1** Next Last

[Add](#) [Edit](#) [Delete](#) [Refresh](#)

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.

Add Group Address

VLAN	1
Group Address	(0.0.0.0 - 0.0.0.0)
Member	Available Port Selected Port ➤ ➤

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

Item	Description
VLAN	The VLAN ID of MVR group.
Group Address	The MVR group IP address.
Member	The member ports of MVR group.

	● Available Port: Optional port member, it is only receiver port when MVR mode is compatible, it include source port when mode is dynamic. ● Selected Port: Selected port member
--	---

IV-9. Routings

IV-9-1. IPv4 Management and Interface

IV-9-1-1 IPv4 Interface

Static routing is a form of routing that occurs when a router uses a manually-configured routing entry, rather than information from dynamic routing traffic. In many cases, static routes are manually configured by a network administrator by adding in entries into a routing table, though this may not always be the case.

IPv4 Interface Table

☐	Interface	IP Address Type	IP Address	Mask	Status
Add Delete					

Click “Add” to configure Static routing functions

Add IPv4 Interface

Interface

VLAN

10

Address Type

☐ Dynamic
☒ Static

IP Address

10.10.10.36

Mask

☒ Network Mask

255.255.0.0

☐ Prefix Length (8 - 30)

Apply

Close

☐	Interface	IP Address Type	IP Address	Mask	Status
☐	VLAN 10	Static	10.10.10.36	255.255.0.0	Valid

Item	Description
VLAN	The VLAN ID you have created
Address Type	Dynamic or Static IP address
IP Address	IP address for static routing
Mask	Mask for static routing
Prefix Length	Prefix Length from 8 to 30

IV-9-1-2 IPv4 Routes

Static Routing Settings

Add IPv4 Static Route

IP Address	10.10.10.0
Mask	☐ Network Mask ☒ Prefix Length 16 (0 - 32)
Next Hop Router IP Address	10.10.10.254
Metric	1 (1 - 255, default 1)

IPv4 Routing Table

☐	Destination IP Prefix	Prefix Length	Route Type	Next Hop Router IP Address	Metric	Administrative Distance	Outgoing Interface
☐	10.10.0.0	16	Static	10.10.10.254	1	1	inactive
☐	192.168.2.0	24	Directly Connected				MGMT VLAN*

Item	Description
IP Address	Enter IP address
Mask	Network Mask Enter the Network Mask, eg. 255.255.255.0
	Prefix Length Range: 0~32

Next Hop Router IP address	Enter the IP Address
Metric	Range: 1~255

IV-9-1-3 ARP

Address Resolution Protocol (ARP) is the method for finding a host's Link Layer (MAC) address when only its IP address is known. The ARP table is used to maintain a correlation between each MAC address and its corresponding IP address. The ARP table can be manually entered by the user. User entries are not aged out.

Routing >> IPv4 Management and Interfaces >> ARP

It

Al

On

Cl

Er

Edit ARP

Interface

VLAN10

IP Address

10.10.10.20

MAC Address

80:1f:02:d6:d1:cf

Apply

Close

ARP Table

It

IP

N

☐	Interface	IP Address	MAC Address	Status
☐	VLAN 1	192.168.2.111	8c:04:ba:0c:37:79	Dynamic

Add

Edit

Delete

Lengthn

-

Next Hop Router IP address

Enter the IP Address

Metric

Range: 1~255

IV-9-2. IPv6 Management and Interfaces

Typically in IPv6, engineers choose prefix lengths that are multiples of four. That makes the prefix easier to understand without using a subnet calculator. Look at the example in figure 6, each additional 4 in the prefix length moves the network portion of the address one hexadecimal digit to the right.

IV-9-2-1 IPv6 Interface

Enable and apply

IPv6 Unicast Routing

☒ Enable

Apply

Cancel

IPv6 Interface Table

☐	Interface	DHCPv6 Client			Auto Configuration	DAD Attempts	
		Stateless	Information Refresh Time	Minimum Information Refresh Time			
0 results found.							
Add		Edit		Delete			

Click “Add” to configure IPv6

Add IPv6 Interface

Interface

VLAN

10

Auto Configuration

☒ Enable

DAD Attempts

1

(0 - 600, default 1)

DHCPv6 Client

Stateless

☐ Enable

Information Refresh Time

86400

(86400 - 4294967294, default 86400)

Minimum Information Refresh Time

600

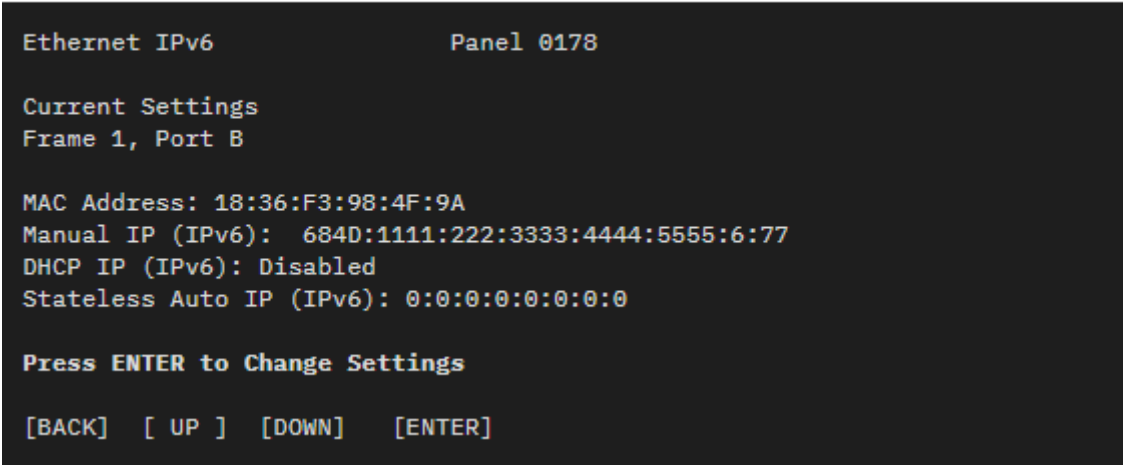
(600 - 4294967294, default 600)

Apply

Close

Item	Description	
Interface	VLAN ID Selection	
Auto Configuration	Checkbox for enabling	
DAD Attempts	Range: 0~600	
DHCP Client	Stateless	Checkbox for enabling
	Info. Refresh Time	Range:86400~4294967294
	Max. Info. Refresh Time	Range:600~4294967294

The following example shows a screen that uses IPv6 addresses:



IV-9-2-2 IPv6 Addresses

☒	IPv6 Address Type	IPv6 Address	IPv6 Prefix Length	DAD Status	
☐	Multicast	ff05::2			
☐	Multicast	ff01::2			
☐	Multicast	ff02::2			
☐	Multicast	ff02::1			
☐	Multicast	ff01::1			
AddDelete					

Add IPv6 Interface

Interface

undefined

IPv6 Address Type

Global

Link Local

IPv6 Address

Prefix Length

(3 - 128)

EUI-64

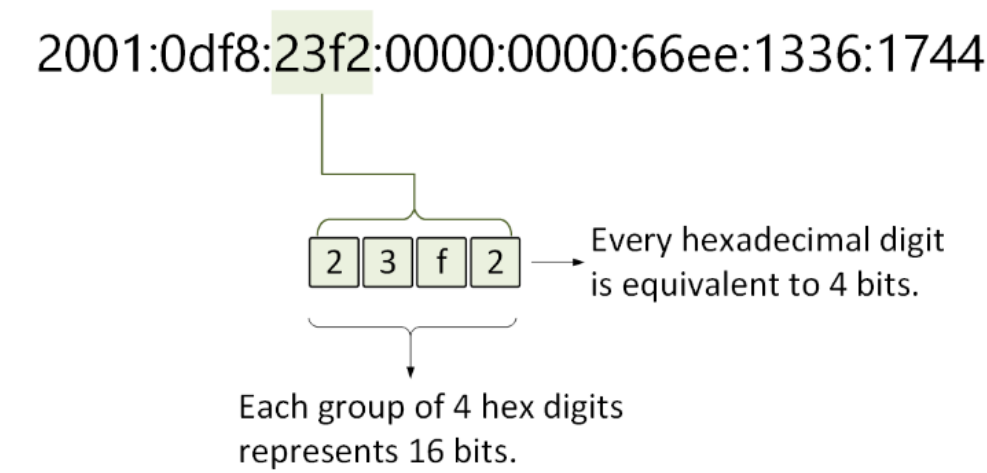
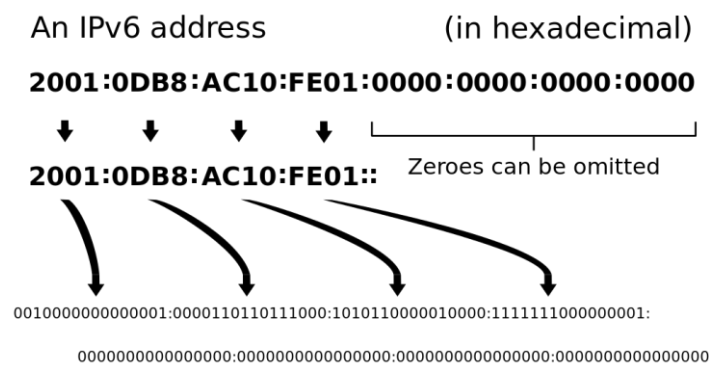
Enable

Apply

Close

Item	Description
IPv6 Address Type	Global or Link Local
IPv6 Address	IPv6 IP address
Prefix Length	Range: 3~128
EUI-64	Checkbox for enabling

IV-9-2-3 IPv6 Route



Add IPv6 Static Route

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

Item	Description
IPv6 Prefix	eg. 2001:1111:2222:3333::/64
IPv6 Prefix Length	Range : 0~128
Next Hop Router IP Address	Range: 3~128
Metric	Range : 1~ 255

Prefix Length	Network Portion	Total Addresses
/4	2::	2 ¹²⁴

Prefix Length	Network Portion	Total Addresses
/8	20::	2 ¹²⁰
/12	200::	2 ¹¹⁶
/16	2001::	2 ¹¹²
/20	2001:0::	2 ¹⁰⁸
/24	2001:0d::	2 ¹⁰⁴
/28	2001:0df::	2 ¹⁰⁰
/32	2001:0df8::	2 ⁹⁶
/36	2001:0df8:0::	2 ⁹²
/40	2001:0df8:00::	2 ⁸⁸
/44	2001:0df8:00f::	2 ⁸⁴
/48	2001:0df8:00f2::	2 ⁸⁰
/52	2001:0df8:00f2:0::	2 ⁷⁶
/56	2001:0df8:00f2:00::	2 ⁷²
/60	2001:0df8:00f2:000::	2 ⁶⁸
/64	2001:0df8:00f2:0000::	2 ⁶⁴

IV-9-2-4 IPv6 Neighbors

Clear Neighbor Table

☐ All
☐ Dynamic
☐ Static
☒ N/A

Apply

Cancel

Item	Description	
Clear Neighbors Table	All	All Neighbors Tables are cleared.
	Dynamic	Only dynamic Neighbors Tables are cleared.
	Static	Only static Neighbors Tables are cleared
	N/A	N/A

IPv6 Neighbor Table

☐	Interface	IPv6 Address	MAC Address	Status	Router
0 results found.					
Add Edit Delete					

Click “Add”

Add Neighbor

Interface	VLAN 10 ▼
IP Address	2001:0db8:85a3:0000:0000:8
MAC Address	80:1F:02:D6:D1:CF
Apply Close	

Item	Description
Interface	Select VLAN ID
IPv6 Prefix Length	IPv6 IP Address eg. 2001:0db8:85a3:0000:0000:8a2e:0370:7334
MAC Address	MAC Address eg. XX:XX:XX:XX:XX:XX

IV-10. Security

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

IV-10-1 RADIUS

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

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

Use Default Parameter

Retry

(1 - 10, default 3)

Timeout

Sec (1 - 30, default 3)

Key String

Apply

RADIUS Table

Showing All entries
Showing 0 to 0 of 0 entries

☐	Server Address	Server Port	Priority	Retry	Timeout	Usage
0 results found.						

Add Edit Delete
First Previous 1 Next Last

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

Edit RADIUS Server

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

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

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

IV-10-2 TACACS+

This page is to configure the TACACS+ server connection session parameters. TACACS+ which stands for Terminal Access Controller Access Control Server is a security protocol used in the AAA framework to provide centralized authentication for users who want to gain access to the network.

Use Default Parameter

Timeout

5

Sec (1 - 30, default 5)

Key String

Apply

Item	Description
Timeout	Set the timeout in the range 1 to 30, a TACACS+ request is retransmitted to a server that is not responding. If the server has not responded after the last retransmit it is considered to be dead.
Key String	Define the key between the TACACS+ server and the switch.

TACACS+ Table

Showing All entries

Showing 0 to 0 of 0 entries

☐	Server Address	Server Port	Priority	Timeout
0 results found.				
Add	Edit	Delete	First Previous 1 Next Last	

Click **"Add"** or **"Edit"** button to view Add/Edit TACACS+ Server menu.

Add TACACS+ Server

Address Type	☒ Hostname ☐ IPv4 ☐ IPv6	
Server Address		
Server Port	49	(0 - 65535, default 49)
Priority		(0 - 65535)
Key String	☒ Use Default 	
Timeout	☒ Use Default 5 Sec (1 - 30, default 5)	

Item	Description
Address Type	In add dialog, user need to specify server Address Type ● Hostname: Use domain name as server address. ● IPv4: Use IPv4 as server address. ● IPv6: Use IPv6 as server address.
Server Address	In add dialog, user need to input server address based on address type. In edit dialog, it shows current edit server address.
Server Port	Set TACACS+ server port.
Priority	Set TACACS+ server priority (smaller value has higher priority). TACACS+ session will try to establish with the server setting which has highest priority. If failed, it will try to connect to the server with next higher priority.
Retry	Set TACACS+ server retry value. If it is fail to connect to server, it will keep trying until timeout with retry times.
Key String	Set the key- shared between the TACACS+ Authentication Server and the switch.
Timeout	Set TACACS+ server timeout value. If it is fail to connect to server, it will keep trying until timeout.

IV-10-3 AAA

Authentication, Authorization, and Accounting (AAA) is a security framework that controls access to computer resources, enforces policies, and audits usage. AAA and its combined processes play a major role in network management and cyber security by screening users and keeping track of their activity while they are connected.

IV-10-3-1 Method List

Indicates the host can define different methods from **Empty/None/Local/Enable/RADIUS/TACACS+**.

Method List Table

Showing

All

 entries

Showing 1 to 1 of 1 entries

Q

☐	Name	Sequence
☐	default	(1) Local

Add

Edit

Delete

First

Previous

1

Next

Last

Click **"Add"** or **"Edit"** button to view Add/Edit Method List.

Add Method List

Name

Method 1

☒ Empty

☐ None

☐ Local

☐ Enable

☐ RADIUS

☐ TACACS+

Method 2

☒ Empty

☐ None

☐ Local

☐ Enable

☐ RADIUS

☐ TACACS+

Method 3

☒ Empty

☐ None

☐ Local

☐ Enable

☐ RADIUS

☐ TACACS+

Method 4

☒ Empty

☐ None

☐ Local

☐ Enable

☐ RADIUS

☐ TACACS+

Apply

Close

IV-10-3-2 Login Authentication

This section is to control the access of the Managed Switch, including the different access methods – Console, Telnet, SSH, HTTP and HTTPS.

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

Apply

IV-10-4 Management Access

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

IV-10-4-1 Management VLAN

Management VLAN	1 - default ▼
-----------------	---------------

Note: Change Management VLAN may cause connection interrupted

Apply

Note: Change Management VLAN may cause connection interrupted

IV-10-4-2 Management Service

This page allow user to change management services related configurations.

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

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

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

Password Retry Count		
Console	3	(0 - 120, default 3)
Telnet	3	(0 - 120, default 3)
SSH	3	(0 - 120, default 3)

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

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

IV-10-4-3 Management ACL

This page allow 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**.

ACL Name

Apply

Management ACL Table

Showing

All ▼

 entries
Showing 0 to 0 of 0 entries

Q

☐	ACL Name	State	Rule
0 results found.			

Active

Deactive

Delete

First

Previous

1

Next

Last

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-10-4-4 Management ACE

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

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

Management ACE Table

ACL Name

manage ▼

Showing

All ▼

 entries
Showing 0 to 0 of 0 entries

Q

☐	Priority	Action	Service	Port	Address / Mask
0 results found.					

Add

Edit

Delete

First

Previous

1

Next

Last

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 Managemet ACE

ACL Name	manage		
Priority	1	(1 - 65535)	
Service	☐ All ☐ Http ☐ Https ☒ Snmp ☐ SSH ☐ Telnet		
Action	☐ Permit ☒ Deny		
Port	Available Port GE1 GE2 GE3 GE4 GE5 GE6 GE7 GE8	➤ ➤ ➤ ➤ ➤ ➤ ➤ ➤	Selected Port
IP Version	☒ All ☐ IPv4 ☐ IPv6		
IPv4	/ 255.255.255.255		
IPv6	/ 128 (1 - 128)		

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

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

IPv6	Enter the source IPv6 address value and mask to which will be matched.
------	--

IV-10-5 Authentication Manager

IV-10-5-1. Property

This page allow 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

Guest VLAN

MAC-Based User ID Format

☒ 802.1x
☐ Enable

1

XXXXXXXXXXXX

Apply

Port Mode Table

Entry	Port	Authentication Type	Host Mode	Method	Guest VLAN	VLAN Assign Mode
		802.1x				
☐	1 GE1	Disabled	Multiple Authentication	RADIUS	Disabled	Static
☐	2 GE2	Disabled	Multiple Authentication	RADIUS	Disabled	Static
☐	3 GE3	Disabled	Multiple Authentication	RADIUS	Disabled	Static
☐	4 GE4	Disabled	Multiple Authentication	RADIUS	Disabled	Static
☐	5 GE5	Disabled	Multiple Authentication	RADIUS	Disabled	Static
☐	6 GE6	Disabled	Multiple Authentication	RADIUS	Disabled	Static
☐	7 GE7	Disabled	Multiple Authentication	RADIUS	Disabled	Static
☐	8 GE8	Disabled	Multiple Authentication	RADIUS	Disabled	Static
☐	9 GE9	Disabled	Multiple Authentication	RADIUS	Disabled	Static
☐	10 GE10	Disabled	Multiple Authentication	RADIUS	Disabled	Static
☐	11 GE11	Disabled	Multiple Authentication	RADIUS	Disabled	Static
☐	12 GE12	Disabled	Multiple Authentication	RADIUS	Disabled	Static
☐	13 GE13	Disabled	Multiple Authentication	RADIUS	Disabled	Static
☐	14 GE14	Disabled	Multiple Authentication	RADIUS	Disabled	Static
☐	15 GE15	Disabled	Multiple Authentication	RADIUS	Disabled	Static
☐	16 GE16	Disabled	Multiple Authentication	RADIUS	Disabled	Static
☐	17 GE17	Disabled	Multiple Authentication	RADIUS	Disabled	Static
☐	18 GE18	Disabled	Multiple Authentication	RADIUS	Disabled	Static
☐	19 GE19	Disabled	Multiple Authentication	RADIUS	Disabled	Static
☐	20 GE20	Enabled	Multiple Authentication	RADIUS	Disabled	Static
☐	21 GE21	Disabled	Multiple Authentication	RADIUS	Disabled	Static
☐	22 GE22	Disabled	Multiple Authentication	RADIUS	Disabled	Static

Item	Description
Authentication Type	Set checkbox to enable/disable following authentication types 802.1x: Use IEEE 802.1x to do authentication - MAC-Based: Use MAC address to do authentication - WEB-Based: Prompt authentication web page for user to do authentication

Guest VLAN	Set checkbox to enable/disable guest VLAN, if guest VLAN is enabled, you need to select one available VLAN ID to be guest VID.
MAC-Based User ID Format	Select mac-based authentication RADIUS username/password ID format. ● XXXXXXXXXXXX ● 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 ● Enabled: 802.1X is enabled. ● Disabled: 802.1X is disabled.
Authentication Type (MAC-Based)	MAC-Based authentication type state ● Enabled: MAC-Based authentication is enabled ● Disabled: MAC-Based authentication is disabled
Authentication Type (WEB-Based)	WEB-Based authentication type state ● Enabled: WEB-Based authentication is enabled ● Disabled: WEB-Based authentication is disabled
Host Mode	Authenticating host mode ● Multiple Authentication: In this mode, every client need to pass authenticate procedure individually. ● Multiple Hosts: In this mode, only one client need to be authenticated and other clients will get the same access accessibility. Web-auth cannot be enabled in this mode. ● Single Host: In this mode, only one host is allowed to be authenticated. It is the same as Multi-auth mode with max

	hosts number configure to be 1.
Order	Support following authentication type order combinations. Web Authentication should always be the last type. The authentication manager will go to next type if current type is not enabled or authenticated fail. ● 802.1x ● MAC-Based ● WEB-Based ● 802.1x MAC-Based ● 802.1x WEB-Based ● MAC-Based 802.1x ● WEB-Based 802.1x ● 802.1x MAC-Based WEB-Based ● 802.1x WEB-Based MAC-Based
Method	Support following authentication method order combinations. These orders only available on MAC-Based authentication and WEB-Based authentication. 802.1x only support Radius method. ● Local: Use DUT's local database to do authentication ● Radius: Use remote RADIUS server to do authentication ● Local Radius ● Radius Local
Guest VLAN	Port guest VLAN enable state ● Enabled: Guest VLAN is enabled on port. ● Disabled: Guest VLAN is disabled on port.
VLAN Assign Mode	Support following VLAN assign mode and only apply when source is RADIUS ● Disable: Ignore the VLAN authorization result and keep original VLAN of host. ● Reject: If get VLAN authorized information, just use it. However, if there is no VLAN authorized information, reject the host and make it unauthorized. ● Static: If get VLAN authorized information, just use it. If there is no VLAN authorized information, keep original VLAN of host.

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

Edit Port Mode

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

Apply

Close

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

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

IV-10-5-2. Port Setting

This page allow 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	
☐	1	GE1	Disabled	Disabled	256	3600	60	60	30	30	30	2	
☐	2	GE2	Disabled	Disabled	256	3600	60	60	30	30	30	2	
☐	3	GE3	Disabled	Disabled	256	3600	60	60	30	30	30	2	
☐	4	GE4	Disabled	Disabled	256	3600	60	60	30	30	30	2	
☐	5	GE5	Disabled	Disabled	256	3600	60	60	30	30	30	2	
☐	6	GE6	Disabled	Disabled	256	3600	60	60	30	30	30	2	
☐	7	GE7	Disabled	Disabled	256	3600	60	60	30	30	30	2	
☐	8	GE8	Disabled	Disabled	256	3600	60	60	30	30	30	2	
☐	9	GE9	Disabled	Disabled	256	3600	60	60	30	30	30	2	
☐	10	GE10	Disabled	Disabled	256	3600	60	60	30	30	30	2	
☐	11	GE11	Disabled	Disabled	256	3600	60	60	30	30	30	2	
☐	12	GE12	Disabled	Disabled	256	3600	60	60	30	30	30	2	
☐	13	GE13	Disabled	Disabled	256	3600	60	60	30	30	30	2	
☐	14	GE14	Disabled	Disabled	256	3600	60	60	30	30	30	2	
☐	15	GE15	Disabled	Disabled	256	3600	60	60	30	30	30	2	
☐	16	GE16	Disabled	Disabled	256	3600	60	60	30	30	30	2	
☐	17	GE17	Disabled	Disabled	256	3600	60	60	30	30	30	2	
☐	18	GE18	Disabled	Disabled	256	3600	60	60	30	30	30	2	
☐	19	GE19	Disabled	Disabled	256	3600	60	60	30	30	30	2	
☐	20	GE20	Force Authorized	Enabled	256	3600	60	60	30	30	30	2	
☐	21	GE21	Disabled	Disabled	256	3600	60	60	30	30	30	2	
☐	22	GE22	Disabled	Disabled	256	3600	60	60	30	30	30	2	
☐	23	GE23	Disabled	Disabled	256	3600	60	60	30	30	30	2	

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

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

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

Edit Port Setting

Port

GE1

Port Control

☒ Disabled
☐ Force Authorized
☐ Force Unauthorized
☐ Auto

Reauthentication

☐ Enable

Max Hosts

256 (1 - 256, default 256)

Common Timer

Reauthentication

3600 Sec (300 - 4294967294, default 3600)

Inactive

60 Sec (60 - 65535, default 60)

Quiet

60 Sec (0 - 65535, default 60)

802.1x Parameters

TX Period

30 Sec (1 - 65535, default 30)

Supplicant Timeout

30 Sec (1 - 65535, default 30)

Server Timeout

30 Sec (1 - 65535, default 30)

Max Request

2 (1 - 10, default 2)

Web-Based Parameters

Max Login

☐ Infinite
3 (3 - 10, default 3)

Apply

Close

Item	Description
Port	Port #
Port Control	Support following authentication port control types. ● Disable: Disable authentication function and all clients have network accessibility. Force Authorized: Port is force authorized and all clients have network accessibility. ● Force Unauthorized: Port is force unauthorized and all clients have no network accessibility. ● Auto: Need passing authentication procedure to get network accessibility.
Reauthentication	Set checkbox to enable/disable reauthentication.
Max Hosts	In Multiple Authentication mode, total host number cannot not exceed max hosts number.
Common Timer	
Reauthentication	After re-authenticate period, host will return to initial state and need to pass authentication procedure again.
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 Parameters	
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.
Web-Based Parameters	
Max Login	Set checkbox to set max login number to be infinite or specify max login number.

IV-10-5-3. MAC-Base Local Account

Click "Edit" or "Add" button to view Edit MAC-Based Local Account menu.

MAC-Based Local Account Table

Showing All entries Showing 0 to 0 of 0 entries

MAC Address	Control	VLAN	Timeout (Sec)
			Reauthentication Inactive
0 results found.			

Add Edit Delete

First Previous 1 Next Last

Add MAC-Based Local Account

MAC Address	
Port Control	☐ Force Authorized ☒ Force Unauthorized
VLAN	☐ User Defined 1 (1 - 4094)
Assigned Timer	
Reauthentication	☐ User Defined 3600 Sec (300 - 4294967294)
Inactive	☐ User Defined 60 Sec (60 - 65535)

Apply Close

Item	Description
MAC Address	Enter the MAC Address
Port Control	Support following authentication port control types. ● Disable: Disable authentication function and all clients have network accessibility. Force Authorized: Port is force authorized and all clients have network accessibility. ● Force Unauthorized: Port is force unauthorized and all clients have no network accessibility. ● Auto: Need passing authentication procedure to get network accessibility.
VLAN	Set the VLAN (1~4094)
Assigned 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.
----------	--

IV-10-5-4. WEB-Base Local Account

WEB-Based Local Account Table

Showing All entries Showing 0 to 0 of 0 entries Q

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

Add Edit Delete First Previous 1 Next Last

Click **"Edit"** or **"Add"** button to view Edit MAC-Based Local Account menu.

Add WEB-Based Local Account

Username

Password

Confirm Password

VLAN

☐ User Defined

1 (1 - 4094)

Assigned Timer

Reauthentication

Inactive

☐ User Defined
3600 Sec (300 - 4294967294)

☐ User Defined
60 Sec (60 - 65535)

Apply

Close

Item	Description
Username	Enter the username.
Password	Enter the password.
Confirm Password	Re-enter the password.
VLAN	Set the VLAN (1~4094)
Assigned 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.

IV-10-5-5. 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**.

Sessions Table

Showing All ▾ [entries](#)

Showing 0 to 0 of 0 entries

Session ID

Port

MAC Address

Current Type

Status

VLAN

Session Time

Inactivated Time

Quiet Time

VLAN

Reauthentication Period

Inactive Timeout

0 results found.

Clear

Refresh

First

Previous

1

Next

Last

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 ● MAC-Based: Use MAC-Based authentication to do authenticating. ● WEB-Based: Use WEB-Based authentication to do authenticating.
Status	Show host authentication session status IP version (IPv4, IPv6) ● 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-10-5-6. Port Security

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

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

Port Security Table

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 XGE1	Disabled	1	Discard
☐	26 XGE2	Disabled	1	Discard
☐	27 XGE3	Disabled	1	Discard
☐	28 XGE4	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

Edit

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

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

Edit Port Security

Port
State
MAC Address
Action

GE1
☐ Enable
 (0 - 255, default 1)
☐ Forward
☒ Discard
☐ Shutdown

Apply
Close

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	Select the action if learned mac addresses ● Forward: Forward this packet whose SMAC is new to system and exceed the learning-limit number. ● Discard: Discard this packet whose SMAC is new to system and exceed the learning-limit number. ● Shutdown: Shutdown this port when receives a packet whose SMAC is new to system and exceed the learning limit number.

IV-10-5-7. Protected Port

Some applications require that no traffic be forwarded at Layer 2 between ports on the same switch so that one neighbor does not see the traffic generated by another neighbor. In such an environment, the use of protected ports ensures that there is no exchange of unicast, broadcast, or multicast traffic between these ports on the switch.

Protected Port Table

☐	Entry	Port	State
☒	1	GE1	Unprotected
☐	2	GE2	Unprotected
☐	3	GE3	Unprotected
☐	4	GE4	Unprotected
☐	5	GE5	Unprotected
☐	6	GE6	Unprotected
☐	7	GE7	Unprotected
☐	8	GE8	Unprotected
☐	9	GE9	Unprotected
☐	10	GE10	Unprotected
☐	11	GE11	Unprotected
☐	12	GE12	Unprotected

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

Edit Protected Port

Port	GE1
State	☒ Protected

Check "**State**" checkbox, and Click "**Apply**" button to enable Protected Port you selected.

IV-10-5-8. Storm Control

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

When Broadcast, unknown Multicast, or unknown Unicast frames are received, they are duplicated, and a copy is sent to all possible egress ports. This means that in practice they are sent to all ports belonging to the relevant VLAN. In this way, one ingress frame is turned into many, creating the potential for a storm.

Storm protection enables you to limit the number of frames entering the switch and to define the types of frames that are counted towards this limit.

When the rate of Broadcast, unknown Multicast, or unknown Unicast frames is higher than the user-defined threshold, frames received beyond the threshold are discarded or the interface shuts down.

Mode

☐ Packet / Sec
☒ Kbits / Sec

IFG

☒ Exclude
☐ Include

Apply

Port Setting Table



	Entry	Port	State	Broadcast		Unknown Multicast		Unknown Unicast		Action
				State	Rate (Kbps)	State	Rate (Kbps)	State	Rate (Kbps)	
☐	1	GE1	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
☐	2	GE2	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
☐	3	GE3	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
☐	4	GE4	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
☐	5	GE5	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
☐	6	GE6	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
☐	7	GE7	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
☐	8	GE8	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
☐	9	GE9	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
☐	10	GE10	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
☐	11	GE11	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
☐	12	GE12	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
☐	13	GE13	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
☐	14	GE14	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
☐	15	GE15	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
☐	16	GE16	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
☐	17	GE17	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
☐	18	GE18	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
☐	19	GE19	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop

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

Note: Bandwidth capacity on an Ethernet interface is consumed not only by frames of traffic but also by a preamble before each frame and a minimum length of Inter-Frame Gap (IFG),

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

Edit Port Setting

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

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, range 16 - 1000000) depends on global mode setting.
Unknown	Enable: Enable the storm control function of Unknown multicast

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

IV-10-6 DoS

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

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

IV-10-6-1 Property

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

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

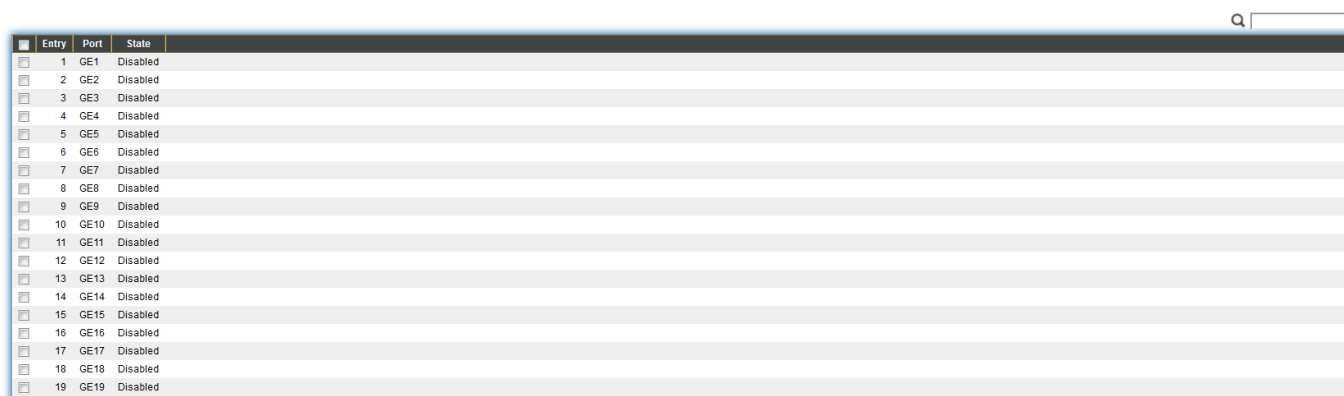
Apply

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 Attach	Drops the packets with NULL scan.
X-Mas Scan Attack	Drops the packets if the sequence number is zero, and the FIN, URG and PSH bits are set.

TCP SYN-FIN Attack	Drops the packets with SYN and FIN bits set.
TCP SYN-RST Attack	Drops the packets with SYN and RST bits set
ICMP Fragment	Drops the fragmented ICMP packets.
TCP SYN (SPORT<1024)	Drops SYN packets with sport less than 1024.
TCP Fragment (Offset = 1)	Drops the TCP fragment packets with offset equals to one.
Ping Max Size	Specify the maximum size of the ICMPv4/ICMPv6 ping packets. The valid range is from 0 to 65535 bytes, and the default value is 512 bytes.
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-10-6-2 Port Setting

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



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

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

IV-10-7 DHCP Snooping

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

IV-10-7-1 Property

This page allow 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

Apply

Port Setting Table

						Q	
☐	Entry	Port	Trust	Verify Chaddr	Rate Limit		
☐	1	GE1	Disabled	Disabled	Unlimited		
☐	2	GE2	Disabled	Disabled	Unlimited		
☐	3	GE3	Disabled	Disabled	Unlimited		
☐	4	GE4	Disabled	Disabled	Unlimited		
☐	5	GE5	Disabled	Disabled	Unlimited		
☐	6	GE6	Disabled	Disabled	Unlimited		
☐	7	GE7	Disabled	Disabled	Unlimited		
☐	8	GE8	Disabled	Disabled	Unlimited		
☐	9	GE9	Disabled	Disabled	Unlimited		
☐	10	GE10	Disabled	Disabled	Unlimited		

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.

Edit Port Setting

Port

GE1

Trust

☐ Enable

Verify Chaddr

☐ Enable

Rate Limit

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

Apply

Close

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-10-7-2 Statistics

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

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

	Entry	Port	Forward	Chaddr Check Drop	Untrust Port Drop	Untrust Port with Option82 Drop	Invalid Drop
☐	1	GE1	0	0	0	0	0
☐	2	GE2	0	0	0	0	0
☐	3	GE3	0	0	0	0	0
☐	4	GE4	0	0	0	0	0
☐	5	GE5	0	0	0	0	0
☐	6	GE6	0	0	0	0	0
☐	7	GE7	0	0	0	0	0
☐	8	GE8	0	0	0	0	0
☐	9	GE9	0	0	0	0	0
☐	10	GE10	0	0	0	0	0
☐	11	GE11	0	0	0	0	0
☐	12	GE12	0	0	0	0	0
☐	13	GE13	0	0	0	0	0
☐	14	GE14	0	0	0	0	0
☐	15	GE15	0	0	0	0	0
☐	16	GE16	0	0	0	0	0
☐	17	GE17	0	0	0	0	0
☐	18	GE18	0	0	0	0	0
☐	19	GE19	0	0	0	0	0
☐	20	GE20	0	0	0	0	0
☐	21	GE21	0	0	0	0	0
☐	22	GE22	0	0	0	0	0
☐	23	GE23	0	0	0	0	0
☐	24	GE24	0	0	0	0	0
☐	25	XGE1	0	0	0	0	0

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-10-7-3 Option82 Property

This page allow 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**.

Remote ID
☐ User Defined

Operational Status

Remote ID 74:da:38:17:6e:7a (Switch Mac in Byte Order)

Apply

Port Setting Table



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

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.

Edit Port Setting

Port	GE1
State	☐ Enable
Allow Untrust	☐ Keep ☒ Drop ☐ Replace

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. ● Keep: Keep original option82 content. ● Replace: Replace option82 content by switch setting ● Drop: Drop packets with option82

IV-10-7-4 Option82 Circuit ID

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

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

Option82 Circuit ID Table

Showing All entries Showing 0 to 0 of 0 entries

☐	Port	VLAN	Circuit ID
0 results found.			

1

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.

Add Option82 Circuit ID

Port	GE1 ▾
VLAN	(1 - 4094) (Keep empty to set without VLAN)
Circuit ID	

Apply

Close

Edit Option82 Circuit ID

Port	
VLAN	
Circuit ID	

Apply

Close

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-10-8 IP Source Guard

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

IV-10-8-1 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**.

Entry	Port	State	Verify Source	Current Entry	Max Entry
1	GE1	Disabled	IP	0	1
2	GE2	Disabled	IP	0	Unlimited
3	GE3	Disabled	IP	0	Unlimited
4	GE4	Disabled	IP	0	Unlimited
5	GE5	Disabled	IP	0	Unlimited
6	GE6	Disabled	IP	0	Unlimited
7	GE7	Disabled	IP	0	Unlimited
8	GE8	Disabled	IP	0	Unlimited
9	GE9	Disabled	IP	0	Unlimited
10	GE10	Disabled	IP	0	Unlimited
11	GE11	Disabled	IP	0	Unlimited
12	GE12	Disabled	IP	0	Unlimited
13	GE13	Disabled	IP	0	Unlimited
14	GE14	Disabled	IP	0	Unlimited
15	GE15	Disabled	IP	0	Unlimited
16	GE16	Disabled	IP	0	Unlimited
17	GE17	Disabled	IP	0	Unlimited
18	GE18	Disabled	IP	0	Unlimited
19	GE19	Disabled	IP	0	Unlimited
20	GE20	Disabled	IP	0	Unlimited
21	GE21	Disabled	IP	0	Unlimited
22	GE22	Disabled	IP	0	Unlimited
23	GE23	Disabled	IP	0	Unlimited
24	GE24	Disabled	IP	0	Unlimited
25	XGE1	Disabled	IP	0	Unlimited
26	VLAN	Disabled	IP	0	Unlimited

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.

Edit Port Setting

Port

GE1

State

☐ Enable

Verify Source

☒ IP
☐ IP-MAC

Max Entry

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

Apply

Close

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 ● 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-10-8-2 IMPV Binding

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

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

IP-MAC-Port-VLAN Binding Table

Showing All ▾ entries Showing 0 to 0 of 0 entries

☐	Port	VLAN	MAC Address	IP Address	Binding	Type	Lease Time
0 results found.							

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 ● 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	(1 - 4094)
Binding	☒ IP-MAC-Port-VLAN ☐ IP-Port-VLAN
MAC Address	
IP Address	/ 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	192.168.2.33	/ 255.255.255.255

ApplyClose

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-10-8-3 Save Database

This page allow 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.**

The screenshot shows a configuration window for DHCP dynamic binding. It includes the following fields and options:

- Type:** Radio buttons for None (selected), Flash, and TFTP.
- Filename:** A text input field.
- Address Type:** Radio buttons for Hostname (selected) and IPv4.
- Server Address:** A text input field.
- Write Delay:** A text input field with the value 300. The range is Sec (15 - 86400, default 300).
- Timeout:** A text input field with the value 300. The range is Sec (0 - 86400, default 300).
- Apply:** A button at the bottom left.

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

IV-11. ACL

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

IV-11-1 MAC ACL

This page allow 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

Q

ACL Name

Rule

Port

0 results found.

First

Previous

1

Next

Last

Delete

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-11-2 MAC ACE

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

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

ACE Table

ACL Name

None

Showing

All

entries
Showing 0 to 0 of 0 entries

Q

Sequence

Action

Source MAC

Destination MAC

Ethertype

VLAN

802.1p

Address

Mask

Address

Mask

Value

Mask

0 results found.

First

Previous

1

Next

Last

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	Display the destination MAC address and mask of ACE.

MAC	
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.

Edit ACE

ACL Name	666
Sequence	555
Action	☒ Permit ☐ Deny ☐ Shutdown
Source MAC	☒ Any / (Address / Mask)
Destination MAC	☒ Any / (Address / Mask)
Ethertype	☒ Any 0x (0x600 ~ 0xFFFF)
VLAN	☒ Any (1 - 4094)
802.1p	☒ Any / (Value / Mask) (0 - 7)

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

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

IV-11-3 IPv4 ACL

This page allow 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**.

ACL Name

ACL Table

Showing

All ▼

 entries
Showing 0 to 0 of 0 entries

☐	ACL Name	Rule	Port
0 results found.			

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-11-4 IPv4 ACE

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

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

ACE Table

ACL Name

None ▼

Showing

All ▼

 entries
Showing 0 to 0 of 0 entries

☐	Sequence	Action	Protocol	Source IP		Destination IP		Source Port	Destination Port	TCP Flags	Type of Service		ICMP	
				Address	Mask	Address	Mask				DSCP	IP Precedence	Type	Code
0 results found.														

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

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. ● Permit: Forward packets that meet the ACE criteria. ● Deny: Drop packets that meet the ACE criteria. ● Shutdown: Drop packets that meet the ACE criteria, and disable the port from where the packets were received. Such ports can be reactivated from the Port Settings page.
Protocol	Select the type of protocol for a match. ● Any (IP): All IP protocols are acceptable. ● Select from list: Select one of the following protocols from the drop-down list. ICMP/IPinIP/TCP/EGP/IGP/UDP/HMP/RDP/IPV6/IPV6:ROUT/IPV6: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. ● Any: All source addresses are acceptable. ● User Defined: Only a source address or a range of source addresses which users define are acceptable. Enter the source IP address value and mask to which will be matched.
Destination IP	Select the type for destination IP address. ● Any: All destination addresses are acceptable. ● User Defined: Only a destination address or a range of destination addresses which users define are acceptable. Enter the destination IP address value and mask to which will be matched.
Source Port	Select the type of protocol for a match. Only available when protocol is TCP or UDP. ● Any: All source ports are acceptable. ● Single: Enter a single TCP/UDP source port to which packets are matched. ● Range: Select a range of TCP/UDP source ports to which the packet is matched. There are eight different port ranges that can be configured (shared between source and destination ports). TCP and UDP protocols each have eight port ranges.
Destination Port	Select the type of protocol for a match. Only available when protocol is TCP or UDP. ● Any: All source ports are acceptable. ● Single: Enter a single TCP/UDP source port to which packets are

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

IV-11-5 ACL Binding

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

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

Q

Entry	Port	MAC ACL	IPv4 ACL
☐	1 GE1		
☐	2 GE2		
☐	3 GE3		
☐	4 GE4		
☐	5 GE5		
☐	6 GE6		
☐	7 GE7		
☐	8 GE8		
☐	9 GE9		
☐	10 GE10		
☐	11 GE11		
☐	12 GE12		
☐	13 GE13		
☐	14 GE14		
☐	15 GE15		
☐	16 GE16		
☐	17 GE17		
☐	18 GE18		
☐	19 GE19		
☐	20 GE20		
☐	21 GE21		
☐	22 GE22		
☐	23 GE23		
☐	24 GE24		
☐	25 XGE1		
☐	26 XGE2		
☐	27 XGE3		
☐	28 XGE4		
☐	29 LAG1		
☐	30 LAG2		
☐	31 LAG3		
☐	32 LAG4		
☐	33 LAG5		
☐	34 LAG6		
☐	35 LAG7		
☐	36 LAG8		

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.
IPv6 ACL	Display ipv6 ACL name that bound of interface. Empty means no rule bound.

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

Add ACL Binding

Port

GE1

Note: ACL without any rules cannot be bound

MAC ACL

None ▼

IPv4 ACL

None ▼

IPv6 ACL

None ▼

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.
IPv6 ACL	Select IPv6 ACL name from list to bind.

IV-12. QoS

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

IV-12-1 General

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

IV-12-1-1 Property

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

Entry	Port	CoS	Trust	Remarking	
				CoS	IP Precedence
1	GE1	0	Enabled	Disabled	Disabled
2	GE2	0	Enabled	Disabled	Disabled
3	GE3	0	Enabled	Disabled	Disabled
4	GE4	0	Enabled	Disabled	Disabled
5	GE5	0	Enabled	Disabled	Disabled
6	GE6	0	Enabled	Disabled	Disabled
7	GE7	0	Enabled	Disabled	Disabled
8	GE8	0	Enabled	Disabled	Disabled
9	GE9	0	Enabled	Disabled	Disabled
10	GE10	0	Enabled	Disabled	Disabled
11	GE11	0	Enabled	Disabled	Disabled
12	GE12	0	Enabled	Disabled	Disabled
13	GE13	0	Enabled	Disabled	Disabled
14	GE14	0	Enabled	Disabled	Disabled
15	GE15	0	Enabled	Disabled	Disabled
16	GE16	0	Enabled	Disabled	Disabled
17	GE17	0	Enabled	Disabled	Disabled
18	GE18	0	Enabled	Disabled	Disabled
19	GE19	0	Enabled	Disabled	Disabled
20	GE20	0	Enabled	Disabled	Disabled
21	GE21	0	Enabled	Disabled	Disabled
22	GE22	0	Enabled	Disabled	Disabled
23	GE23	0	Enabled	Disabled	Disabled
24	GE24	0	Enabled	Disabled	Disabled

Item	Description
State	Set checkbox to enable/disable QoS.
Trust	Select QoS trust mode - CoS: Traffic is mapped to queues based on the CoS field in the VLAN tag, or based on the per-port default CoS value (if there is no VLAN tag on the incoming packet), the actual mapping of the CoS to queue can be configured on port setting dialog. - CoS-DSCP: Uses the trust CoS mode for non-IP traffic and trust DSCP mode for IP traffic. - IP Precedence: Traffic is mapped to queues based on the IP precedence. The actual mapping of the IP precedence to queue can be configured on the IP Precedence mapping page.

Port Setting Table	
Port	Port name
CoS	Port default CoS priority value for the selected ports.
Trust	Port trust state ● Enabled: Traffic will follow trust mode in global setting ● Disabled: Traffic will always use best efforts
Remarking (CoS)	Set checkbox to enable/disable port CoS remarking. ● Enabled: CoS remarking is enabled ● Disabled: CoS remarking is disabled
Remarking (IP Precedence)	Set checkbox to enable/disable port IP Precedence remarking. ● Enabled: DSCP remarking is enabled ● Disabled: DSCP remarking is disabled

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

Edit Port Setting

Port

GE1

CoS

0 (0 - 7)

Trust

☒ Enable

Remarking

CoS

☐ Enable

DSCP

☐ Enable

IP Precedence

☐ Enable

Apply

Close

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-12-1-2 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 Scheduling Table

Queue	Method			
	Strict Priority	WRR	Weight	WRR Bandwidth (%)
1	☒	☐	1	
2	☒	☐	2	
3	☒	☐	3	
4	☒	☐	4	
5	☒	☐	5	
6	☒	☐	9	
7	☒	☐	13	
8	☒	☐	15	

Apply

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-12-1-3 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 ▼

Apply

Queue to CoS Mapping

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

Apply

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-12-1-4 DSCP Mapping

DSCP to Queue Mapping

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

Apply

IV-12-1-5 IP Precedence Mapping

This page allow 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 ▼

Apply

Queue to IP Precedence Mapping

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

Apply

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-12-2 Rate Limit

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

IV-12-2-1 Ingress/Egress Port

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

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

	Entry	Port	Ingress		Egress	
			State	Rate (Kbps)	State	Rate (Kbps)
☐	1	GE1	Enabled	10000	Enabled	10000
☐	2	GE2	Disabled		Disabled	
☐	3	GE3	Disabled		Disabled	
☐	4	GE4	Disabled		Disabled	
☐	5	GE5	Disabled		Disabled	
☐	6	GE6	Disabled		Disabled	
☐	7	GE7	Disabled		Disabled	
☐	8	GE8	Disabled		Disabled	
☐	9	GE9	Disabled		Disabled	
☐	10	GE10	Disabled		Disabled	
☐	11	GE11	Disabled		Disabled	
☐	12	GE12	Disabled		Disabled	
☐	13	GE13	Disabled		Disabled	
☐	14	GE14	Disabled		Disabled	
☐	15	GE15	Disabled		Disabled	
☐	16	GE16	Disabled		Disabled	
☐	17	GE17	Disabled		Disabled	
☐	18	GE18	Disabled		Disabled	

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

Edit Ingress / Egress Port

Port

GE1

Ingress

☒ Enable

Kbps (16 - 1000000)

Egress

☒ Enable

Kbps (16 - 1000000)

Apply

Close

Item	Description
Port	Port #
Ingress (State)	Port ingress rate limit state ● Enabled: Ingress rate limit is enabled ● Disabled: Ingress rate limit is disabled
Ingress (Rate)	Port ingress rate limit value if ingress rate state is enabled.
IP Precedence	IP Precedence value which queue is mapped.
Egress (State)	Port egress rate limit state

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

IV-12-2-2 Egress Queue

To display Ingress / Egress Queue web page,
Click **QoS > Rate Limit > Ingress / Egress Queue**

Egress Queue Table

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

Click **"Edit"** button to edit the Egress queue

Edit Egress Queue

Port	GE1-GE3	
Queue 1	☒ Enable	1000000 Kbps (16 - 1000000)
Queue 2	☒ Enable	800000 Kbps (16 - 1000000)
Queue 3	☒ Enable	700000 Kbps (16 - 1000000)
Queue 4	☒ Enable	1000000 Kbps (16 - 1000000)
Queue 5	☒ Enable	1000000 Kbps (16 - 1000000)
Queue 6	☒ Enable	1000000 Kbps (16 - 1000000)
Queue 7	☒ Enable	1000000 Kbps (16 - 1000000)
	☐ Enable	

Each Queue: 16~10000,000 kbps

IV-13. Diagnostics

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

IV-13-1 Logging

IV-13-1-1 Property

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

State☒ Enable

Console Logging

State☒ Enable

Minimum Severity

Notice

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

RAM Logging

State☒ Enable

Minimum Severity

Notice

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

Flash Logging

State☐ Enable

Minimum Severity

Notice

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

Apply

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	

157

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 logging.

IV-13-1-2 Remote Server

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

Remote Server Table

☐	Entry	Server Address	Server Port	Facility	Minimum Severity
0 results found.					

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	● 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-13-2 Mirroring

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

Mirroring Table

Q

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

Edit

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

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

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

Edit Mirroring

Session ID	1	
State	☐ Enable	
Monitor Port	GE1 ▼ ☐ Send or Receive Normal Packet	
Ingress Port	Available Port GE1 GE2 GE3 GE4 GE5 GE6 GE7 GE8	Selected Port (Empty)
Egress Port	Available Port GE1 GE2 GE3 GE4 GE5 GE6 GE7 GE8	Selected Port (Empty)

Apply Close

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

IV-13-3 Ping

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

Address Type

Server Address

Count

☒ Hostname

☐ IPv4

☐ IPv6

☐ User Defined

4

Sec (1 - 65535)

Ping

Stop

Ping Result

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

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-13-4 Traceroute

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

Address Type

Server Address

Time to Live

☒ Hostname
☐ IPv4

(2 - 255, default 30)

☐ User Defined

Apply

Stop

Traceroute Result

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-13-5 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
☐	GE25	N/A	N/A	N/A	N/A	N/A	Remove	Loss
☐	GE26	N/A	N/A	N/A	N/A	N/A	Remove	Loss
☐	GE27	N/A	N/A	N/A	N/A	N/A	Remove	Loss
☐	GE28	N/A	N/A	N/A	N/A	N/A	Remove	Loss

Refresh

Detail

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

IV-13-6 UDLD

Use the UDLD pages to configure settings of UDLD function.

IV-13-6-1 Property

This page allow 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)

Apply

Entry	Port	Mode	Bidirectional State	Operational Status	Neighbor
☐	1	GE1	Disabled	Unknown	0
☐	2	GE2	Disabled	Unknown	0
☐	3	GE3	Disabled	Unknown	0
☐	4	GE4	Disabled	Unknown	0
☐	5	GE5	Disabled	Unknown	0
☐	6	GE6	Disabled	Unknown	0
☐	7	GE7	Disabled	Unknown	0
☐	8	GE8	Disabled	Unknown	0
☐	9	GE9	Disabled	Unknown	0
☐	10	GE10	Disabled	Unknown	0
☐	11	GE11	Disabled	Unknown	0
☐	12	GE12	Disabled	Unknown	0
☐	13	GE13	Disabled	Unknown	0
☐	14	GE14	Disabled	Unknown	0
☐	15	GE15	Disabled	Unknown	0
☐	16	GE16	Disabled	Unknown	0
☐	17	GE17	Disabled	Unknown	0
☐	18	GE18	Disabled	Unknown	0
☐	19	GE19	Normal	Unknown	0
☐	20	GE20	Normal	Unknown	0
☐	21	GE21	Disabled	Unknown	0
☐	22	GE22	Disabled	Unknown	0
☐	23	GE23	Disabled	Unknown	0
☐	24	GE24	Disabled	Unknown	0
☐	25	XGE1	Disabled	Unknown	0
☐	26	XGE2	Disabled	Unknown	0
☐	27	XGE3	Disabled	Unknown	0
☐	28	XGE4	Disabled	Unknown	0

Edit

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.

Edit Port Setting

Port

GE1

Mode

☒ Disabled

☐ Normal

☐ Aggressive

Apply

Close

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

IV-13-6-2 Neighbor

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

Neighbor Table



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

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-14. Management

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

IV-14-1 User Account

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

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

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

User Account

Showing **All** entries

Showing 1 to 1 of 1 entries



☐	Username	Privilege
☐	admin	Admin

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

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

Add User Account

Username	
Password	
Confirm Password	
Privilege	☒ Admin ☐ User

Edit User Account

Username	admin
Password	
Confirm Password	
Privilege	☒ Admin ☐ User

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. ● 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-14-2 Firmware

IV-14-2-1 Upgrade / Backup

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

To display firmware upgrade or backup web page, click **Management > Firmware > Upgrade/Backup**.

The screenshot shows a web form for firmware operations. It is divided into three main sections by dashed lines. The first section, labeled 'Action', contains two radio buttons: 'Upgrade' (which is selected) and 'Backup'. The second section, labeled 'Method', contains two radio buttons: 'TFTP' and 'HTTP' (which is selected). The third section, labeled 'Filename', contains a 'Choose File' button and a text box that currently displays 'No file chosen'. Below the entire form is a single 'Apply' button.

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

To display firmware upgrade or backup web page, click **Management > Firmware > Upgrade/Backup.**

Active Image

☐ Image0
☒ Image1

Note: the image was selected for the next boot

Active Image

Firmware	Image1
Version	1.00.07
Name	Edimax_PG28CB_V1.00.07_r380_vmlinux_web.bix
Size	6417775 Bytes
Created	2017-11-21 14:54:59

Backup Image

Firmware	Image0
Version	1.00.06
Name	Edimax_PG28CB_V1.00.06_r373_vmlinux_web.bix
Size	6413996 Bytes
Created	2017-11-08 20:00:06

Apply

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

To display firmware upgrade or backup web page, click **Management > Firmware > Upgrade/Backup.**

Action

☐ Upgrade
☒ Backup

Method

☐ TFTP
☒ HTTP

Firmware

☒ Image0
☐ Image1

Apply

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

To display the Firmware Upgrade/Backup web page, click Management > Firmware > Upgrade/Backup.

Action

☐ Upgrade
☒ Backup

Method

☒ TFTP
☐ HTTP

Firmware

☒ Image0
☐ Image1

Address Type

☒ Hostname
☐ IPv4
☐ IPv6

Server Address

Filename

Apply

Item	Description
Action	Firmware operations ● Upgrade: Upgrade firmware from remote host to DUT ● Backup: Backup firmware image from DUT to remote host
Method	Firmware upgrade / backup method ● TFTP: Using TFTP to upgrade/backup firmware. ● HTTP: Using WEB browser to upgrade/backup firmware.
Firmware	Firmware partition need to backup ● Image0: Firmware image in flash partition 0. ● Image1: Firmware image in flash partition 1.
Address Type	Specify TFTP server address type ● Hostname: Use domain name as server address. ● IPv4: Use IPv4 as server address. ● IPv6: Use IPv6 as server address.
Server Address	Specify TFTP server address address.
Filename	File name saved on remote TFTP server.

IV-14-2-2 Active Image

This page allow 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**.

Active Image

☐ Image0
☒ Image1

Note: the image was selected for the next boot

Active Image

Firmware	Image1
Version	1.00.07
Name	Edimax_PG28CB_V1.00.07_r380_vmlinux_web.bix
Size	6417775 Bytes
Created	2017-11-21 14:54:59

Backup Image

Firmware	Image0
Version	1.00.06
Name	Edimax_PG28CB_V1.00.06_r373_vmlinux_web.bix
Size	6413996 Bytes
Created	2017-11-08 20:00:06

Apply

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-14-3 Configuration

IV-14-3-1 Upgrade / Backup

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

To display firmware upgrade or backup web page, click **Management > Configuration > Upgrade/Backup**.

Action	☒ Upgrade ☐ Backup
Method	☐ TFTP ☒ HTTP
Configuration	☒ Running Configuration ☐ Startup Configuration ☐ Backup Configuration ☐ RAM Log ☐ Flash Log
Filename	Choose File No file chosen

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

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

To display firmware upgrade or backup web page, click **Management > Configuration > Upgrade/Backup**.

The screenshot shows a web interface for configuring firmware upgrade or backup. It features a yellow background with a blue border. The interface is divided into several sections by dashed lines:

- Action:** Radio buttons for "Upgrade" (selected) and "Backup".
- Method:** Radio buttons for "TFTP" (selected) and "HTTP".
- Configuration:** Radio buttons for "Running Configuration" (selected), "Startup Configuration", "Backup Configuration", "RAM Log", and "Flash Log".
- Address Type:** Radio buttons for "Hostname" (selected), "IPv4", and "IPv6".
- Server Address:** A text input field.
- Filename:** A text input field.
- Apply:** A button at the bottom left.

Item	Description
Action	Configuration operations ● Upgrade: Upgrade firmware from remote host to DUT ● Backup: Backup firmware image from DUT to remote host
Method	Configuration upgrade / backup method ● TFTP: Using TFTP to upgrade/backup firmware ● HTTP: Using WEB browser to upgrade/backup firmware
Configuration	Configuration types ● Running Configuration: Merge to current running configuration file ● Startup Configuration: Replace startup configuration file ● Backup Configuration: Replace backup configuration file
Address Type	Specify TFTP server address type

	● Hostname: Use domain name as server address ● IPv4: Use IPv4 as server address ● IPv6: Use IPv6 as server address
Server Address	Specify TFTP server address
Filename	File name saved on remote TFTP server

To display firmware upgrade or backup web page, click **Management > Configuration > Upgrade/Backup.**

The screenshot shows a web interface for configuring firmware upgrade or backup. It features three main sections: **Action**, **Method**, and **Configuration**. In the **Action** section, the **Backup** radio button is selected. In the **Method** section, the **HTTP** radio button is selected. In the **Configuration** section, the **Running Configuration** radio button is selected. An **Apply** button is located at the bottom left of the configuration area.

Item	Description
Action	Configuration operations ● Upgrade: Upgrade firmware from remote host to DUT ● Backup: Backup firmware image from DUT to remote host
Method	Configuration upgrade / backup method ● TFTP: Using TFTP to upgrade/backup firmware ● HTTP: Using WEB browser to upgrade/backup firmware
Configuration	Configuration types ● Running Configuration: 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.

To display firmware upgrade or backup web page, click **Management > Configuration > Upgrade/Backup**

Action	☒ Upgrade ☐ Backup
Method	☒ TFTP ☐ HTTP
Configuration	☒ Running Configuration ☐ Startup Configuration ☐ Backup Configuration ☐ RAM Log ☐ Flash Log
Address Type	☒ Hostname ☐ IPv4 ☐ IPv6
Server Address	
Filename	

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

IV-14-3-2 Save Configuration

This page allow 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**.

Source File

- ☒ Running Configuration
- ☐ Startup Configuration
- ☐ Backup Configuration

Destination File

- ☒ Startup Configuration
- ☐ Backup Configuration

Apply Restore Factory Default

Item	Description
Source File	Source file types ● Running Configuration: Copy running configuration file to destination. ● Startup Configuration: Copy startup configuration file to destination. ● Backup Configuration: Copy backup configuration file to destination
Destination File	Destination file ● Startup Configuration: Save file as startup configuration. ● Backup Configuration: Save file as backup configuration.

IV-14-4 SNMP

IV-14-4-1 View

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

Showing All entries Showing 1 to 1 of 1 entries

View	OID Subtree	Type
☐ all	.1	Included

Add Delete First Previous 1 Next Last

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-14-4-2 Group

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

Group Table

Showing **All** entries

Showing 0 to 0 of 0 entries

☐	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.

Add

Edit

Delete

Item	Description
Group	Specify SNMP group name, and the maximum length is 30 characters.
Version	Specify SNMP version ● SNMPv1: SNMP Version 1. ● SNMPv2: Community-based SNMP Version 2. ● SNMPv3: User security model SNMP version 3.
Security Level	Specify SNMP security level ● No Security: Specify that no packet authentication is performed. ● Authentication: Specify that no packet authentication without encryption is performed. ● Authentication and Privacy: Specify that no packet authentication with encryption is performed.
View	
Read	Group read view name.
Write	Group write view name.
Notify	The view name that sends only traps with contents that is included in SNMP view selected for notification.

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

Add Group

Group	
Version	☒ SNMPv1 ☐ SNMPv2 ☐ SNMPv3
Security Level	☒ No Security ☐ Authentication ☐ Authentication and Privacy
View	☒ Read ☐ Write ☐ Notify

all ▼

all ▼

all ▼

Apply Close

Edit Group

Group	1
Version	☒ SNMPv1 ☐ SNMPv2 ☐ SNMPv3
Security Level	☒ No Security ☐ Authentication ☐ Authentication and Privacy
View	☒ Read ☐ Write ☐ Notify

all ▼

all ▼

all ▼

Apply Close

Item	Description
Group	Specify SNMP group name, and the maximum length is 30 characters.
Version	Specify SNMP version ● SNMPv1: SNMP Version 1. ● SNMPv2: Community-based SNMP Version 2. ● SNMPv3: User security model SNMP version 3.
Security Level	Specify SNMP security level ● No Security: Specify that no packet authentication is performed.

	● Authentication: Specify that no packet authentication without encryption is performed. ● Authentication and Privacy: Specify that no packet authentication with encryption is performed.
View	
Read	Select read view name if Read is checked.
Write	Select write view name, if Write is checked.
Notify	Select notify view name, if Notify is checked.

IV-14-4-3 Community

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

Community Table

Showing **All** entries

Showing 1 to 1 of 1 entries

☐	Community	Group	View	Access
☐	public		all	Read-Write

First Previous **1** Next Last

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

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 ● Read-Only: Read only. ● Read-Write: Read and write.

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

Add Community

Community	
Type	☒ Basic ☐ Advanced
View	all
Access	☒ Read-Only ☐ Read-Write
Group	1

Apply

Close

Edit Community

Community	public
Type	☒ Basic ☐ Advanced
View	all
Access	☐ Read-Only ☒ Read-Write
Group	1

Apply

Close

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

IV-14-4-4 User

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

User Table

Showing **All** entries

Showing 0 to 0 of 0 entries

☐	User	Group	Security Level	Authentication Method	Privacy Method
0 results found.					

First Previous **1** Next Last

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

Add

Edit

Delete

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

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

Add User

User	
Group	11 ▼
Security Level	☒ No Security ☐ Authentication ☐ Authentication and Privacy
Authentication	
Method	☒ None ☐ MD5 ☐ SHA
Password	
Privacy	
Method	☒ None ☐ DES
Password	

Edit User

User	22
Group	11 ▼
Security Level	☒ No Security ☐ Authentication ☐ Authentication and Privacy
Authentication	
Method	☒ None ☐ MD5 ☐ SHA
Password	
Privacy	
Method	☒ None ☐ DES
Password	

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

IV-14-4-5 Engine ID

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

Local Engine ID

☐ User Defined

Engine ID

80006a920374da38176e7 (10 - 64 Hexadecimal Characters)

Apply

Remote Engine ID Table

Showing All entries

Showing 0 to 0 of 0 entries

	Server Address	Engine ID
0 results found.		
Add	Edit	Delete
First	Previous	1
Next	Last	

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.

Add Remote Engine ID

Address Type

☒ Hostname
☐ IPv4
☐ IPv6

Server Address

Engine ID

(10 - 64 Hexadecimal Characters)

Apply

Close

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 range10 to 64 hexadecimal characters, and the hexadecimal number must be divided by 2.

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

Edit Remote Engine ID

Server Address

123.4.5.6

Engine ID

12345abcde (10 - 64 Hexadecimal Characters)

Apply

Close

Item	Description
Server Address	Edit Remote host address
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.

IV-14-4-6 Trap Event

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

Authentication Failure	☒ Enable
Link Up / Down	☒ Enable
Cold Start	☒ Enable
Warm Start	☒ Enable

Apply

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-14-4-7 Notification

To configure the hosts to receive SNMPv1/v2c/v3 notification, click **Management > SNMP > Notification**.

Notification Table

Showing All entries

Showing 0 to 0 of 0 entries

	Server Address	Server Port	Timeout	Retry	Version	Type	Community / User	Security Level
0 results found.								

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

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 ● SNMPv1: SNMP Version 1 notification. ● SNMPv2c: SNMP Version 2 notification. ● SNMPv3: SNMP Version 3 notification.
Type	Notification Type ● Trap: Send SNMP traps to the host. ● Inform: Send SNMP informs to the host.
Community/User	SNMP community/user name for notification. If version is SNMPv3 the name is user name, else is community name.
UDP Port	Specify the UDP port number.
Timeout	Specify the SNMP informs timeout.
Security Level	SNMP trap packet security level ● No Security: Specify that no packet authentication is performed. ● Authentication: Specify that no packet authentication without encryption is performed. ● Authentication and Privacy: Specify that no packet authentication with encryption is performed.

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

Add Notification

Address Type	☒ Hostname ☐ IPv4 ☐ IPv6
Server Address	
Version	☒ SNMPv1 ☐ SNMPv2 ☐ SNMPv3
Type	☒ Trap ☐ Inform
Community / User	public
Security Level	☒ No Security ☐ Authentication ☐ Authentication and Privacy
Server Port	☒ Use Default 162 (1 - 65535, default 162)
Timeout	☒ Use Default 15 Sec (1 - 300, default 15)
Retry	☒ Use Default 3 (1 - 255, default 3)

Apply

Close

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

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

Edit Notification

Server Address	123.4.5.6	
Version	☒ SNMPv1 ☐ SNMPv2 ☐ SNMPv3	
Type	☒ Trap ☐ Inform	
Community / User	public ▼	
Security Level	☒ No Security ☐ Authentication ☐ Authentication and Privacy	
Server Port	☒ Use Default 162	(1 - 65535, default 162)
Timeout	☒ Use Default 15	Sec (1 - 300, default 15)
Retry	☒ Use Default 3	(1 - 255, default 3)

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

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

IV-14-5 RMON

RMON (Remote Network Monitoring) is a standard monitoring specification that defines a set of statistics and functions that can be exchanged between RMON-compliant console systems and network probes. RMON provides you with comprehensive network-fault diagnosis, planning, and performance-tuning information.

FS-5428X supported RMON Statistics group, History group , Events group and Alarm group.

RMON 1 Group	Function	Elements
Statistics	Contains statistics measured by the RMON probe for each monitored interface on this device.	Packets dropped, packets sent, bytes sent (octets), broadcast packets, multicast packets, CRC errors, runts, giants, fragments, jabbers, collisions, and counters for packets ranging from 64 to 128, 128 to 256, 256 to 512, 512 to 1024, and 1024 to 1518 bytes.
History	Records periodic statistical samples from a network and stores them for later retrieval.	Sample period, number of samples, items sampled.
Alarms	Periodically takes statistical samples from variables in the probe and compares them with previously configured thresholds. If the monitored variable crosses a threshold, an event is generated.	Includes the alarm table: alarm type, interval, starting threshold, stop threshold. Note: The Alarms group requires the implementation of the Events group.
Events	Controls the generation and notification of events from this device.	Event type, description, the last time the event was sent.

V. More Information

For detailed instructions, you can find user manual and all supporting documents from the link below or via the QR code:

<https://www.edimax.com/download/>

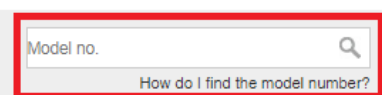


Please search the model number to enter the referred page.

Download

To select your product and find related download materials, enter the model number into the search box on the right side or follow the simple steps below:

*Feel free to contact us anytime if you need help or if you can't find your product.

A screenshot of a web search interface. It features a search box with the placeholder text 'Model no.' and a magnifying glass icon on the right. Below the search box is a link that reads 'How do I find the model number?'. The entire search area is highlighted with a red rectangular border.

VI. Safety Instructions

The following general safety guidelines are provided to help ensure your own personal safety and protect your product from potential damage. Remember to consult the product user instructions for more details.

- This product is designed for indoor use only.
- Static electricity can be harmful to electronic components. Discharge static electricity from your body (i.e. touching grounded bare metal) before touching the product.
- The device contains no user serviceable parts. Do not attempt to service the product and never disassemble the product.
- Do not spill food or liquid on your product and never push any objects into the openings of your product.
- Do not use this product near water, areas with high humidity, or condensation.
- Keep the product away from radiators and other heat sources.
- This device is not designed to be operated by children.
- Always unplug the product from mains power before cleaning and use a dry lint free cloth only.

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 A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

FCC Radiation Exposure Statement

This device complies with FCC radiation exposure limits set forth for an uncontrolled environment and it also complies with Part 15 of the FCC RF Rules. This equipment must be installed and operated in accordance with provided instructions and the antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter. End-users and installers must be provided with antenna installation instructions and consider removing the no-collocation statement.

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.

Caution!

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

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, Croatia, 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 direktiivin 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 Gb Fiber + 4 Port SFP+ L3 Management Switch
Model No.: FS-5428X

The following European standards for essential requirements have been followed:

Directives 2014/30/EU

EMC : EN 55032:2015/A1:2020
EN IEC 61000-3-2:2019+A1:2021
EN 61000-3-3:2013+A2:2021
EN 55035:2017/A11:2020

Directives 2014/35/EU

Safety (LVD) : EN IEC 62368-1:2020+A11:2020

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

Date & Place of Issue: 28/Sep./2023, Eindhoven

Signature: 

Printed Name: David Huang

Title: Director

a company of:

Edimax Technology Co., Ltd.
No. 278, Xinhua 1st Rd., Neihu Dist.,
Taipei City, Taiwan

Date & Place of Issue: 28/Sep./2023, Taipei

Signature: 

Printed Name: Hunter Chen

Title: Director



Declaration of Conformity

We, Edimax Technology Co., Ltd., declare under our sole responsibility, that the equipment described below complies with the requirements of the United Kingdom EMC and Safety directives.

Equipment: 24-port Gb Fiber + 4 Port SFP+ L3 Management Switch
Model No.: FS-5428X

The following European standards for essential requirements have been followed:

Electromagnetic Compatibility Regulations 2016 (S.I. 2016/1091)

EMC : EN 55032:2015/A1:2020
EN IEC 61000-3-2:2019+A1:2021
EN 61000-3-3:2013+A2:2021
EN 55035:2017/A11:2020

Electrical Equipment (Safety) Regulations 2016 (S.I. 2016/1101)

Safety (LVD) : EN IEC 62368-1:2020+A11:2020

Edimax Technology Europe B.V.

Fijenhof 2,

5652 AE Eindhoven,

The Netherlands

Date & Place of Issue: 28/Sep./2023, Eindhoven

Signature: 

Printed Name: David Huang

Title: Director

a company of:

Edimax Technology Co., Ltd.

No. 278, Xinhua 1st Rd., Neihu Dist.,

Taipei City, Taiwan

Date & Place of Issue: 28/Sep./2023, Taipei

Signature: 

Printed Name: Hunter Chen

Title: Director

