

# ALL-SG9312M-10G

12-port 10G SFP+ L2 Switch



# **User Manual**

# Default-IP

# 192.168.2.1

Username & Password:

# admin

# **Table of Contents**

Chapter 1 Introduction
1.1 General Description ······8
1.2 The Front Panel ······ 8
1.3 LEDs Definition ······ 8
1.4 The Rear Panel ······ 8
1.5 Hardware Installation 9
Chapter 2 Getting Started
2.1 Preparation for Web Interface10
2.2 System login ······10
2.3 The Graphic User Interface 11
Chapter 3 Status ······14
3.1 System Information14
3.2 Logging Message ·····15
3.3 Port
3.3.1 Statistics
3.3.2 Error Disabled
3.3.3 Bandwidth Utilization 18
3.4 Link Aggregation 19
3.5 MAC Address Table 19
Chapter 4 Network 21
4.1 IP Address
4.2 System Time 22
Chapter 5 Port ······25
5.1 Port Setting
5.2 Error Disabled
5.3 Link Aggregation 27
5.3.1 Trunk Group Setting ·····27
5.3.2 Port Setting
5.3.3 LACP
5.4 Jumbo Frame
Chapter 6 VLAN
6.1 VLAN
6.1.1 Create VLAN
6.1.2 VLAN Configuration ····································
6.1.3 Membership
6.1.4 Port Setting
6.2 Voice VLAN
6.2.1 Property

6.2.2 Voice OUI ·······3	39
6.3 Protocol VLAN ·······4	10
6.3.1 Protocol Group ······4	10
6.3.2 Group Binding ······4	10
6.4 MAC VLAN	11
6.4.1 MAC Group 4	1
6.4.2 Group Binding ······4	12
6.5 Surveillance VLAN ·······4	13
6.5.1 Property	13
6.5.2 Surveillance OUI ···································	4
6.6 GVRP4	15
6.6.1 Property	15
6.6.2 Membership ·······4	16
6.6.3 Statistics ·······4	16
Chapter 7 MAC Address Table ······4	18
7.1 Dynamic Address······4	18
7.2 Static Address 4	18
7.3 Filtering Address······4	19
Chapter 8 Spanning Tree5	50
8.1 Property ·······5	50
8.2 Port Setting ······5	51
8.3 MST Instance ······5	53
8.4 MST Port Setting ······5	55
8.5 Statistics ······5	56
Chapter 9 Discovery 55	58
9.1 LLDP5	58
9.1.1 Property	58
9.1.2 Port Setting ······5	59
9.1.3 MED Network Policy ······6	30
9.1.4 MED Port Setting ·······6	51
9.1.5 Packet View ·······6	32
9.1.6 Local Information ······6	34
9.1.7 Neighbor	34
9.1.8 Statistics ·······6	35
Chapter 10 Multicast ······6	37
10.1 General······6	37
10.1.1 Property ······6	37
10.1.2 Group Address 6	37
10.1.3 Router Port ······6	38
10.1.4 Forward All······6	39

10.1.5 Throttling ······	70
10.1.6 Filtering Protocol ······	···71
10.1.7 Filtering Binding ······	…72
10.2 IGMP Snooping ······	73
10.2.1 Property ·····	73
10.2.2 Querier	…76
10.2.3 Statistics	77
10.3 MLD Snooping ·····	77
10.3.1 Property ·····	···78
10.3.2 Statistics	80
10.4 MVR	···81
10.4.1 Property ·····	···81
10.4.2 Port Setting ······	···81
10.4.3 Group Address	82
Chapter 11 Security ·····	84
11.1 RADIUS ·····	84
11.2 TACACS+	85
11.3 AAA ·····	···87
11.3.1 Method List ·····	···87
11.3.2 Login Authentication	···87
11.4 Management Access ······	88
11.4.1 Management VLAN······	88
11.4.2 Management Service ·····	88
11.4.3 Management ACL ······	89
11.4.4 Management ACE······	90
11.5 Authentication Manager	…91
11.5.1 Property	…91
11.5.2 Port Setting ······	…92
11.5.3 MAC-Based Local Account ·····	93
11.5.4 WEB-Based Local Account	…94
11.5.5 Sessions	…95
11.6 Port Security ·····	…95
11.7 Traffic Segmentation ······	96
11.8 Storm Control	···97
11.9 DoS	98
11.9.1 Property	99
11.9.2 Port Setting ·····	· 100
11.10 Dynamic ARP Inspection	· 100
11.10.1 Property ·····	· 101
11.10.2 Statistics ·····	· 102

11.11 DHCP Snooping ····································	103
11.11.1 Property ····································	103
11.11.2 Statistics ·······	105
11.11.3 Option82 Property ·······	105
11.11.4 Option82 Circuit ID ·······	107
11.12 IP Source Guard ·······	107
11.12.1 Port Setting ····································	108
11.12.2 IMPV Binding ····································	108
11.12.3 Save Database ·······	109
Chapter 12 ACL ······	111
12.1 MAC ACL	111
12.2 MAC ACE	112
12.3 IPv4 ACL	113
12.4 IPv4 ACE	113
12.5 IPv6 ACL	117
12.6 IPv6 ACE	117
12.7 ACL Binding	119
Chapter 13 QoS ······	121
13.1 General······	121
13.1.1 Property ······	121
13.1.2 Queue Scheduling ·······	123
13.1.3 CoS Mapping·······	124
13.1.4 DSCP Mapping ····································	124
13.1.5 IP Precedence Mapping······	125
13.2 Rate Limit ·······	126
13.2.1 Ingress / Egress Port······	126
13.2.2 Egress Queue	127
Chapter 14 Diagnostics ······	130
14.1 Logging ······	130
14.1.1 Property ·······	130
14.1.2 Remote Server ······	131
14.2 Mirroring ······	131
14.3 Ping	132
14.4 Traceroute ······	133
14.5 Fiber Module ····································	133
14.6 UDLD ······	133
14.6.1 Property ·······	134
14.6.2 Neighbor	135
Chapter 15 Management ·······	136
15.1 User Account ······	136

15.2 Firmware
15.2.1 Upgrade / Backup
15.2.2 Active Image 138
15.3 Configuration ······ 139
15.3.1 Upgrade / Backup······ 139
15.3.2 Save Configuration
15.4 SNMP
15.4.1 View
15.4.2 Group ······ 142
15.4.3 Community 144
15.4.4 User ······ 144
15.4.5 Engine ID
15.4.6 Trap Event
15.4.7 Notification ····································
15.5 RMON
15.5.1 Statistics
15.5.2 History
15.5.3 Event ······ 150
15.5.4 Alarm ······ 151

# Chapter 1 Introduction

## **1.1 General Description**

This switch is 12-port 10G SFP+ L2 Switch. The switch provides exceptionally smart Web management features, such as VLAN, QoS, RSTP, IGMP Snooping, LACP, IEEE802.1X, Strom Control...etc. The switch is standard 19" rack-mount design to fit into the rack environment. With these features, the switch is a superb choice for medium or large network environment to strengthen its network connection and efficiency.

## **1.2 The Front Panel**

The following figure shows the front panel of the switch.



This device provides extensive LEDs to show the activities on power, system and ports. See the following description for your reference:

LED	Status	Operation
PWR	Green Off	Power off or fail.
	Green On	Power on.
	Green Off	Power off or fail
SYS	Blinking Green	System booting up.
	Green On	System is ready
AI FRT Red Off Switch is normal condition		Switch is normal condition
/	Red On	Alarm for system failure because of overheat, wrong voltage.
	Off	Port disconnected or link fail
1-12 Port	Steady Green	10Gbps connected.
LED: (SFP+)	Steady Amber	1000Mbps connected
	Blinking	Sending or receiving data.

#### The Reset Button

Reset the switch to its factory default configuration via the RESET button. Press the Reset button for ten seconds and release. The switch automatically reboots and reloads its factory configuration file. The Reset button is on the front panel of the switch.

## 1.4 The Rear Panel

The following figure shows the rear panel of the switch:



#### **Power Receptacle**

To be compatible with the electric service standards around the world, the switch is designed to afford the power supply in the range from 100 to 240 VAC, 50/60 Hz. Please make sure that your outlet standard to be within this range.

To power on the switch, please plug the female end of the power cord firmly into the receptacle of the switch, the other end into an electric service outlet. After the switch powered on, please check if the power LED is lit for a normal power status.

#### 1.5 Hardware Installation

To install this switch, please place it on a large flat surface with a power socket close by. This surface should be clean, smooth, and level. Also, please make sure that there is enough space around this switch for RJ45 cable or fiber cable, power cord and ventilation.

If you're installing this switch on a 19-inch rack, please make sure to use the rack-mount kit (L brackets) and screws come with the product package. ALL screws must be fastened so the rack-mount kit and your product are tightly conjoined before installing it on your 19-inch rack.

#### **SFP Installation**

While install the SFP transceiver, make sure the SFP type of the 2 ends is the same and the transmission distance, wavelength, fiber cable can meet your request. It is suggested to purchase the SFP transceiver with the switch provider to avoid any incompatible issue.

The way to connect the SFP transceiver is to Plug in SFP fiber transceiver fist. The SFP transceiver has 2 plug for fiber cable, one is TX (transmit), the other is RX (receive). Cross-connect the transmit channel at each end to the receive channel at the opposite end.

#### **Rack-mount Installation**

Attach the brackets to the device by using the screws provided in the Rack Mount kit. Mount the device in the 19-inch rack by using four rack-mounting screws provided by the rack manufacturer.

## Chapter 2 Getting Started

## 2.1 Preparation for Web Interface

The web management page allows you to use a standard web-browser such as Microsoft Internet Explorer, Google Chrome or Mozilla Firefox, to configure and interrogate the switch from anywhere on the network.

Before you attempt to use the web user interface to manage switch operation, verify that your switch is properly installed on your network and that every PC on this network can access the switch via the web browser.

- 1. Verify that your network interface card (NIC) is operational, and that your operating system supports TCP/IP protocol.
- 2. Wire the switch power and connect your computer to the switch.
- 3. The switch default IP address is **192.168.2.1**. The Switch and the connected PC should locate within the same IP Subnet.
- 4. Change your computer's IP address to 192.168.2.XX or other IP address which is located in the 192.168.2.x (For example: IP Address: 192.168.2.100; Subnet Mask: 255.255.255.0) subnet.

📱 Local Area Connection Properties	Internet Protocol Version 4 (TCP/IPv4) Properties	? X
Networking Sharing	General	
Connect using:	You can get IP settings assigned automatically if your network s this capability. Otherwise, you need to ask your network adminis for the appropriate IP settings.	upports strator
This connection uses the following item	Obtain an IP address automatically	
<ul> <li>Realtek Teaming Protocol Driv</li> <li>Realtek Vian Protocol Driver ()</li> </ul>	IP address: 192.168.2.100	
Arealtek NDIS Protocol Driver     Arealtek Protocol Version 6 (TQ)	Subnet mask: 255 . 255 . 255 . 0	
Internet Protocol Version 4 (TO Link-Laver Topology Discover	Default gateway:	
Link-Layer Topology Discover	Obtain DNS server address automatically	
	Use the following DNS server addresses:	
Install Uninstall	Preferred DNS server:	
Description Transmission Control Protocol/Intern	Alternate DNS server:	
wide area network protocol that prov across diverse interconnected netwo	Validate settings upon exit	nced
	ОК	Cancel

## 2.2 System login

- 1. Start your web browser.
- 2. Type "http://"and the IP address of the switch (for example, the default management IP address is **192.168.2.1**) in the Location or Address field. Press **[ENTER]**.



3. The login screen appears. The default username and password are "**admin**", so you can click **Login** and go to the web configuration screen directly.



## 2.3 The Graphic User Interface

After the password authorization, the System page shows up. You may click on each folder on the left column of each page to get access to each configuration page. The Graphic User Interface is as follows:

ALLNET*	12 10-Gigabit Fiber Port Full L2 Management Switch		ALL-SG9312-10G Save   Logout   Reboot
	Status >> System I	nformation	
Status     System Information     Logging Message     Port     Link Aggregation     MAC Address Table			
<ul> <li>Network</li> <li>Port</li> <li>VLAN</li> </ul>	System Information		
<ul> <li>MAC Address Table</li> </ul>	Model	ALL-SG9312-10G	
<ul> <li>Spanning Tree</li> </ul>	System Name	Switch	₩ 70%
Discovery     Multicast	System Location	Default	60%
Security	System Contact	Default	50%
✓ ACL			40%
↓ QoS	MAC Address	FC:8F:C4:0D:22:11	20%
<ul> <li>Diagnostics</li> </ul>	IPv4 Address	192.168.2.1	10%
<ul> <li>Management</li> </ul>	IPv6 Address	fe80::fe8f:c4ff:fe0d:2211/64	0%
	System Uptime	1 day, 18 hr, 39 min and 58 sec	11:32:00 11:33:00 11:34:00 11:35:00 11:36:00
	Current Time	1970-01-02 18:39:58 UTC+8	100%

In the navigation panel, click a main link to reveal a list of submenu links shown as the following:

LINKS	Submenu
	System Information. Logging Message
Status	Port - Statistics, Error Disabled, Bandwidth Utilization
	Link Aggregation
	MAC Address Table
Network	IP Address
	System Time
	Port Setting
Port	Error Disabled
	Link Aggregation - Group, Port Setting, LACP
	JUMDO FIAME
	Voice VLAN – Create VLAN, VLAN Configuration, Membership, Port Setting
	Protocol VI AN - Protocol Group, Group Binding
VLAN	MAC VI AN - MAC Group, Group Binding
	Surveillance VI AN - Property, Surveillance OUI
	GVRP - Property, Membership, Statistics
	Dynamic Address
MAC Address Table	Static Address
	Filtering Address
	Property
	Port Setting
Spanning Tree	MST Instance
	MST Port Setting
	Statistics
	Property Deart Setting
	MED Network Policy
	MED Port Setting
Discovery (LLDP)	Packet View
	Neighbor
	Statistics
	General - Property, Group Address, Router Port, Forward All, Throttling,
	Filtering Profile, Filtering Binding
Multicast	IGMP Snooping - Property, Querier, Statistics
	MLD Snooping - Property, Statistics
	MVR - Property, Port Setting, Group Address
	TACACS+
	AAA Method List Login Authontication
	Management Access - Management VI AN Management Service
	Management ACI Management ACE
	Authentication Manager - Property, Port Setting, MAC-Based Local
Security	Account, WEB-Based Local Account, Sessions
	Port Security
	Traffic Segmentation
	Storm Control
	DoS - Property, Port Setting
	Dynamic ARP Inspection - Property, Statistics
	DHCP Snooping - Property, Statistics, Option82 Property, Option82
	Circuit ID

The following table describes the links in the navigation panel.

	IP Source Guard - Port Setting, IMPV Binding, Save Database
	MAC ACL MAC ACE
	IPv4 ACL
ACL	IPv4 ACE
	IPv6 ACL
	IPv6 ACE
	ACL Binding
	General - Property, Queue Scheduling, CoS Mapping, DSCP
QoS	Mapping, IP Precedence Mapping
	Rate Limit - Ingress/Egress Port, Egress Queue
	Logging - Property, Remove Server
	Mirroring
Diagnostics	Ping
Diagnostics	Traceroute
	Fiber Module
	UDLD - Property, Neighbor
	User Account
	Firmware – Upgrade/Backup, Active Image
Managamant	Configuration - Upgrade/Backup, Save Configuration
Management	SNMP - View, Group, Community, User, Engine ID, Trap Event,
	Notification
	RMON - Statistics, History, Event, Alarm

Please note, you have to click **Save** to save the configuration after changing any settings.

# Chapter 3 Status

Use the Status pages to view system information and status.

## 3.1 System Information

#### Click Status > System Information

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

S	Status »> System I	nformation	
✓ Status			
System Information Logging Message Port Link Aggregation MAC Address Table			9 <u>10 11 12</u>
<ul> <li>✓ Network</li> <li>✓ Port</li> </ul>			2 400%
• VLAN	System Information	Edit	5 90%
MAC Address Table     Spanning Tree	Model	ALL-SG9312-10G	2008 jatit
<ul> <li>Discovery</li> </ul>	System Name	Switch	· · · · · · · · · · · · · · · · · · ·
✓ Multicast	System Location	Default	60%
<ul> <li>Security</li> </ul>	System Contact	Default	40%
✓ ACL			30%
✓ QoS	MAC Address	FC:8F:C4:0D:22:11	20%
Diagnostics	IPv4 Address	192.168.2.1	10%
• Management	IPv6 Address	fe80::fe8f:c4ff:fe0d:2211/64	
	System Uptime	1 day, 18 hr, 39 min and 58 sec	11.32.00 11.33.00 11.34.00 11.33.00 11.30.00
	Current Time	1970-01-02 18:39:58 UTC+8	
			100%
	Loader Version	3.6.6.55087	
	Loader Date	Nov 10 2021 - 09:56:22	
	Firmware Version	1.0.1	5 70%
	Firmware Date	Nov 10 2021 - 09:57:26	50%
	Telnet	Disabled	40%
	SSH	Disabled	20%
	HTTP	Enabled	10%
	HTTPS	Disabled	0%
	SNMP	Enabled	12:04:00 12:00:00 12:00:00 12:07:00

Field	Description	
Model	Model name of the switch	
System Name	System name of the switch. This name will also use as CLI prefix of each line	
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

Field	Description
System Name	System name of the switch. This name will also use as CLI prefix of each line.
System Location	Location information of the switch.
System Contact	Contact information of the switch.

## 3.2 Logging Message

Click Status > Logging Message

This page shows logging messages stored on the RAM and Flash.

Status 》 Logging Message						
System Information	Logging Message Table					
Logging Message Port	Viewing RAM V					
Link Aggregation MAC Address Table	Showing All v entries		Showing 1 to 5 of 5 entries	٩		
<ul> <li>Network</li> </ul>	Log ID Time	Severity	Description			
• Port	1 Jan 02 1970 18:39	56 notice	New http connection for user admin, source 192.168.2.202 ACCEPTED			
• VLAN	2 Jan 01 1970 00:01	20 notice	XGigabitEthernet1 link up			
<ul> <li>MAC Address Table</li> </ul>	3 Jan 01 1970 00:01	12 notice	XGigabitEthernet2 link up			
<ul> <li>Spanning Tree</li> </ul>	4 Jan 01 1970 00:00	13 notice	RESTART: System restarted - Cold Start			
<ul> <li>Discovery</li> </ul>	5 Jan 01 1970 00:00	13 notice	Logging is enabled			
<ul> <li>✓ Multicast</li> <li>✓ Security</li> </ul>			Logging to one loo	First Previous 1 Next Last		
• ACL	Clear Refresh	J				
✓ QoS						
<ul> <li>Diagnostics</li> </ul>						
<ul> <li>Management</li> </ul>						

Field	Description				
	The logging view including:				
Viewing	<b>RAM</b> : 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.				
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.				

## 3.3 Port

The port configuration page displays port summary and status information.

### 3.3.1 Statistics

#### Click Status > Port > Statistics

On this page user can get standard counters on network traffic from the interfaces, Ethernet-like and RMON MIB. Interfaces and Ethernet-like counters display errors on the traffic passing through each port. RMON counters provide a total count of different frame types and sizes passing through each port.

	Status >> Port >> St	atistics
✓ Status	Bort 100	
System Information Logging Message Port Statistics Error Disabled	MIB Counter	All Interface Etherlike RMON
Bandwidth Utilization Link Aggregation MAC Address Table V Network	Refresh Rate	None 5 sec 10 sec 30 sec
✤ Port		
• VLAN	Clear	
<ul> <li>MAC Address Table</li> </ul>	Interface	
<ul> <li>Spanning Tree</li> </ul>	Interface	
• Discovery	ifInOctets	11101823
<ul> <li>Multicast</li> </ul>	ifInUcastPkts	0
✓ Security	ifInNUcastPkts	105516
• ACL	ifInDiscards	0
v QoS	ifOutOctets	66795534
Diagnostics	ifOutUcastPkts	0
Management	ifOutNUcastPkts	1028937
	ifOutDiscards	0
	ifInMulticastPkts	99784
	ifInMulticastPkts	99714
	ifInBroadcastPkts	5721
	ifOutMulticastPkts	187113
	ifOutBroadcastPkts	839465

	Status >> Port >> Statistics	
✓ Status		
System Information	Etherlike	1
Logging Message	dot3StatsAlignmentErrors	0
Statistics	dot3StatsFCSErrors	0
Error Disabled	dot3StatsSingleCollisionFrames	0
Bandwidth Utilization	dot3StatsMultipleCollisionFrames	0
Link Aggregation	dot3StatsDeferredTransmissions	0
Network	dot3StatsLateCollisions	0
✓ Port	dot3StatsExcessiveCollisions	0
• VLAN	dot3StatsFrameTooLongs	0
<ul> <li>MAC Address Table</li> </ul>	dot3StatsSymbolErrors	0
<ul> <li>Spanning Tree</li> </ul>	dot3ControllnLinknownOncodes	0
• Discovery	dot3inPausoEramos	0
✓ Multicast		0
<ul> <li>Security</li> </ul>	dot3OutPauseFrames	0
* ACL	RMON	
• QoS	etherStatsDropEvents	0
<ul> <li>Management</li> </ul>	etherStatsOctets	11093772
	etherStatsPkts	105443
	othorStateProadcastBkts	5724
	etter Stats Di Vaucastr Kis	00740
	etherStatsMulticastPkts	997/19
	etherStatsCRCAlignErrors	0
	etherStatsUnderSizePkts	0
	etherStatsOverSizePkts	0
	etherStatsFragments	0
	etherStatsJabbers	0
	etherStatsCollisions	0
	etherStatsPkts64Octets	2532
	etherStatsPkts65to127Octets	95398
	etherStatsPkts128to255Octets	7513
	etherStatsPkts256to511Octets	0
	etherStatsPkte512to1022Octote	0
	etherStatsPkta102/to15420ctets	0
	einerstatsPkts1024to1518Octets	U

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

Field	Description
Port	Select one port to show counter statistics.
	Select the MIB counter to show different count type
	All: All counters.
MIB Counter	Interface: Interface related MIB counters
	Etherlike: Ethernet-like related MIB counters
	RMON : RMON related MIB counters
Bofrach Bata	Refresh the web page every period of seconds to get new counter of
Rellesii Kate	specified port.

#### 3.3.2 Error Disabled

#### Click Status > Port > Error Disabled

Error Disabled is a feature that automatically disables a port on a switch and this feature is designed to inform the administrator when there is a port problem or error. The reasons a switch can go into Error Disabled mode and shutdown a port are many and include: **BPDU Guard**, **UDLD**, **Self Loop**, **Broadcast Flood**, **Unknown Multicast Flood**, **Unicast Flood**, **ACL**, **Port Security**, **DHCP Rate** 

**Limit** and **ARP Rate Limit**. When a port is in Error Disabled state, it is effectively shut down and no traffic is sent or received on that port.

You can observe which port(s) is(are) disabled with the reason here. Click **Recover** to recover the port.

	Statu	s )) Po	ort » Er	ror Disabled	
✓ Status	Erre	or Disab	led Table		
System Information		Dioub			
Logging Message	-				
Port		Port	Reason	Time Left (sec)	
Statistics Error Disabled		10GE1			
Bandwidth Utilization		10GE2			
Link Aggregation		10GE3			
MAC Address Table		10000	20023		
• Network		10055			
✤ Port		10GE5			
✓ VLAN		10GE6			
<ul> <li>MAC Address Table</li> </ul>		10GE7			
<ul> <li>Spanning Tree</li> </ul>		10GE8			
<ul> <li>Discovery</li> </ul>		10GE9			
<ul> <li>Multicast</li> </ul>		10GE10			
<ul> <li>Security</li> </ul>		10GE11			
✓ ACL		10GE12			
✓ QoS		LAG1			
<ul> <li>Diagnostics</li> </ul>		LAG2			
✓ Management		LAG3			
		LAG4			
		LAG5			
		LAG6			
		LAG7			
		LAG8			
	F	Refresh	Recover	]	

#### 3.3.3 Bandwidth Utilization

#### Click Status > Port > Bandwidth Utilization

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



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

# 3.4 Link Aggregation

#### Click Status > Link Aggregation

Display the Link Aggregation status of web page.

	Status)	) Link	( Agg	regation				
System Information	Link Ag	ggrega	tion Ta	able				
Logging Message								
A Port							Q	
Statistics	LAG	Name	Type	Link Status	Active Member	Inactive Member		
EITOI DISabled		Nume	iybe	Enix Otatus	Active member	mactive member		
	LAG 1							
	LAG 2							
	LAG 3							
✓ Network	LAG 4							
✓ Port	LAG 5							
✓ VLAN								
<ul> <li>MAC Address Table</li> </ul>	LAG 6							
<ul> <li>Spanning Tree</li> </ul>	LAG 7							
✤ Discovery	LAG 8							

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

## 3.5 MAC Address Table

Click Status > MAC Address Table

The MAC address table page displays all MAC address entries on the switch including static MAC address created by administrator or auto learned from hardware.

	Status )	MAC Addres	ss Table					
✓ Status								
System Information	MAC A	ddress Table						
Logging Message Port Statistics	Showing	All 🗸 entries	S	Showing 1 to	8 of 8 entries	(	Q	
Error Disabled	VLAN	MAC Address	Туре	Port				
Bandwidth Utilization	1	FC:8F:C4:0D:22:11	Management	CPU				
Link Aggregation	1	00:03:79:08:0D:94	Dynamic	10GE2				
MAC Address Table	1	00:08:54:73:ED:F9	Dynamic	10GE2				
Network	1	00:0E:C6:82:34:98	Dynamic	10GE1				П
✓ Port	1	00:0F:C9:12:34:56	Dynamic	10GE2				
VLAN	1	00:0F:C9:12:34:71	Dynamic	10GE2				
MAC Address Table	1	00:17:16:07:E3:40	Dynamic	10GE2				
Spanning free     Discovery	1	8C:16:45:37:F3:67	Dynamic	10GE4				
<ul> <li>✓ Multicast</li> <li>✓ Security</li> </ul>	Clea	r Refresh	]			First	Previous 1 Next La	st

The "**Clear**" button will clear all dynamic entries and "Refresh" button will retrieve latest MAC address entries and show them on page.

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

# Chapter 4 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.

## 4.1 IP Address

#### Click Network > IP Address

Use the IP Setting screen to configure the switch IP address and the default gateway device. The gateway field specifies the IP address of the gateway (next hop) for outgoing traffic. The switch needs an IP address for it to be managed over the network. The factory default IP address is 192.168.2.1. The subnet mask specifies the network number portion of an IP address. The factory default subnet mask is 255.255.255.0.

Ne	etwork »> IP Addres	SS	
<ul> <li>Status</li> </ul>			
- Network	IPv4 Address		
IP Address System Time	Address Type	Static     Dynamic	
<ul><li>✓ Port</li><li>✓ VLAN</li></ul>	IP Address	192.168.2.1	
<ul> <li>MAC Address Table</li> </ul>	Subnet Mask	255.255.255.0	
Spanning Tree     Discovery	Default Gateway	192.168.2.254	
<ul> <li>Multicast</li> </ul>	DNS Server 1	168.95.1.1	
<ul> <li>Security</li> <li>ACL</li> </ul>	DNS Server 2	168.95.192.1	
✓ QoS	IPv6 Address		
Diagnostics	Auto Configuration	C Enable	
Management	DHCPv6 Client		
	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::fe8f:c4ff:fe0d:2211/64	
	IPv6 Gateway	:	
	Link Local Address	fe80::fe8f:c4ff:fe0d:2211/64	
	Apply		

Field	Description		
IPv4 Address Field			
	Select the address type of IP configuration		
Address Type	•Static: Static IP configured by users will be used.		
	• <b>Dynamic</b> : Enable DHCP to obtain IP information from a DHCP server		
	on the network.		

IP Address	Enter the IP address of your switch in dotted decimal notation for example 192 168 2.1. If static mode is enabled, enter IP address in
	this field.
	Enter the IP subnet mask of your switch in dotted decimal notation for
Subnet Mask	example 255.255.255.0. If static mode is enabled, enter subnet mask
	in this field.
Default Octoor	Specify the default gateway on the static configuration. The default
Default Gateway	configuration
DNS Server 1	If static mode is enabled, enter primary DNS server address in this field.
DNS Server 2	If static mode is enabled, enter secondary DNS server address in this field.
IPv6 Address Field	
Auto Configuration	Select <b>Enable</b> or <b>Disable</b> the IPv6 auto configuration.
	DHCPv6 client state.
DHCPv6 Client	•Enable: Enable DHCPv6 client function.
DHCPv6 Client	•Enable: Enable DHCPv6 client function. •Disable: Disable DHCPv6 client function
DHCPv6 Client IPv6 Address	<ul> <li>•Enable: Enable DHCPv6 client function.</li> <li>•Disable: Disable DHCPv6 client function</li> <li>Specify the IPv6 address, when the IPv6 auto configuration and DHCPv6 client are disabled.</li> </ul>
DHCPv6 Client IPv6 Address IPv6 Prefix	<ul> <li>•Enable: Enable DHCPv6 client function.</li> <li>•Disable: Disable DHCPv6 client function</li> <li>Specify the IPv6 address, when the IPv6 auto configuration and DHCPv6 client are disabled.</li> <li>Specify the prefix for the IPv6 address, when the IPv6 auto configuration and DHCPv6 client are disabled.</li> </ul>
DHCPv6 Client IPv6 Address IPv6 Prefix	<ul> <li>•Enable: Enable DHCPv6 client function.</li> <li>•Disable: Disable DHCPv6 client function</li> <li>Specify the IPv6 address, when the IPv6 auto configuration and DHCPv6 client are disabled.</li> <li>Specify the prefix for the IPv6 address, when the IPv6 auto configuration and DHCPv6 client are disabled.</li> <li>Specify the IPv6 default gateway, when the IPv6 auto configuration</li> </ul>
DHCPv6 Client IPv6 Address IPv6 Prefix Gateway	<ul> <li>•Enable: Enable DHCPv6 client function.</li> <li>•Disable: Disable DHCPv6 client function</li> <li>Specify the IPv6 address, when the IPv6 auto configuration and DHCPv6 client are disabled.</li> <li>Specify the prefix for the IPv6 address, when the IPv6 auto configuration and DHCPv6 client are disabled.</li> <li>Specify the IPv6 default gateway, when the IPv6 auto configuration and DHCPv6 client are disabled.</li> </ul>
DHCPv6 Client IPv6 Address IPv6 Prefix Gateway DNS Server 1	<ul> <li>•Enable: Enable DHCPv6 client function.</li> <li>•Disable: Disable DHCPv6 client function</li> <li>Specify the IPv6 address, when the IPv6 auto configuration and DHCPv6 client are disabled.</li> <li>Specify the prefix for the IPv6 address, when the IPv6 auto configuration and DHCPv6 client are disabled.</li> <li>Specify the IPv6 default gateway, when the IPv6 auto configuration and DHCPv6 client are disabled.</li> <li>Specify the IPv6 default gateway, when the IPv6 auto configuration and DHCPv6 client are disabled.</li> <li>Specify the primary user-defined IPv6 DNS server configuration.</li> </ul>
DHCPv6 Client IPv6 Address IPv6 Prefix Gateway DNS Server 1 DNS Server 2	<ul> <li>•Enable: Enable DHCPv6 client function.</li> <li>•Disable: Disable DHCPv6 client function</li> <li>Specify the IPv6 address, when the IPv6 auto configuration and DHCPv6 client are disabled.</li> <li>Specify the prefix for the IPv6 address, when the IPv6 auto configuration and DHCPv6 client are disabled.</li> <li>Specify the IPv6 default gateway, when the IPv6 auto configuration and DHCPv6 client are disabled.</li> <li>Specify the IPv6 default gateway, when the IPv6 auto configuration and DHCPv6 client are disabled.</li> <li>Specify the primary user-defined IPv6 DNS server configuration.</li> <li>Specify the secondary user-defined IPv6 DNS server configuration.</li> </ul>
DHCPv6 Client IPv6 Address IPv6 Prefix Gateway DNS Server 1 DNS Server 2 Operational Status	<ul> <li>•Enable: Enable DHCPv6 client function.</li> <li>•Disable: Disable DHCPv6 client function</li> <li>Specify the IPv6 address, when the IPv6 auto configuration and DHCPv6 client are disabled.</li> <li>Specify the prefix for the IPv6 address, when the IPv6 auto configuration and DHCPv6 client are disabled.</li> <li>Specify the IPv6 default gateway, when the IPv6 auto configuration and DHCPv6 client are disabled.</li> <li>Specify the primary user-defined IPv6 DNS server configuration.</li> <li>Specify the secondary user-defined IPv6 DNS server configuration.</li> </ul>
DHCPv6 Client IPv6 Address IPv6 Prefix Gateway DNS Server 1 DNS Server 2 Operational Status IPv4 Address	<ul> <li>•Enable: Enable DHCPv6 client function.</li> <li>•Disable: Disable DHCPv6 client function</li> <li>Specify the IPv6 address, when the IPv6 auto configuration and DHCPv6 client are disabled.</li> <li>Specify the prefix for the IPv6 address, when the IPv6 auto configuration and DHCPv6 client are disabled.</li> <li>Specify the IPv6 default gateway, when the IPv6 auto configuration and DHCPv6 client are disabled.</li> <li>Specify the IPv6 default gateway, when the IPv6 auto configuration and DHCPv6 client are disabled.</li> <li>Specify the primary user-defined IPv6 DNS server configuration.</li> <li>Specify the secondary user-defined IPv6 DNS server configuration.</li> </ul>
DHCPv6 Client IPv6 Address IPv6 Prefix Gateway DNS Server 1 DNS Server 2 Operational Status IPv4 Address IPv4 Gateway	<ul> <li>•Enable: Enable DHCPv6 client function.</li> <li>•Disable: Disable DHCPv6 client function</li> <li>Specify the IPv6 address, when the IPv6 auto configuration and DHCPv6 client are disabled.</li> <li>Specify the prefix for the IPv6 address, when the IPv6 auto configuration and DHCPv6 client are disabled.</li> <li>Specify the IPv6 default gateway, when the IPv6 auto configuration and DHCPv6 client are disabled.</li> <li>Specify the IPv6 default gateway, when the IPv6 auto configuration and DHCPv6 client are disabled.</li> <li>Specify the primary user-defined IPv6 DNS server configuration.</li> <li>Specify the secondary user-defined IPv6 DNS server configuration.</li> <li>The operational IPv4 address of the switch.</li> <li>The operational IPv4 gateway of the switch.</li> </ul>
DHCPv6 Client IPv6 Address IPv6 Prefix Gateway DNS Server 1 DNS Server 2 Operational Status IPv4 Address IPv4 Gateway IPv6 Address	<ul> <li>•Enable: Enable DHCPv6 client function.</li> <li>•Disable: Disable DHCPv6 client function</li> <li>Specify the IPv6 address, when the IPv6 auto configuration and DHCPv6 client are disabled.</li> <li>Specify the prefix for the IPv6 address, when the IPv6 auto configuration and DHCPv6 client are disabled.</li> <li>Specify the IPv6 default gateway, when the IPv6 auto configuration and DHCPv6 client are disabled.</li> <li>Specify the primary user-defined IPv6 DNS server configuration.</li> <li>Specify the secondary user-defined IPv6 DNS server configuration.</li> <li>The operational IPv4 address of the switch.</li> <li>The operational IPv6 address of the switch.</li> </ul>
DHCPv6 Client IPv6 Address IPv6 Prefix Gateway DNS Server 1 DNS Server 2 Operational Status IPv4 Address IPv4 Gateway IPv6 Gateway	<ul> <li>•Enable: Enable DHCPv6 client function.</li> <li>•Disable: Disable DHCPv6 client function</li> <li>Specify the IPv6 address, when the IPv6 auto configuration and DHCPv6 client are disabled.</li> <li>Specify the prefix for the IPv6 address, when the IPv6 auto configuration and DHCPv6 client are disabled.</li> <li>Specify the IPv6 default gateway, when the IPv6 auto configuration and DHCPv6 client are disabled.</li> <li>Specify the primary user-defined IPv6 DNS server configuration.</li> <li>Specify the secondary user-defined IPv6 DNS server configuration.</li> <li>The operational IPv4 address of the switch.</li> <li>The operational IPv6 address of the switch.</li> <li>The operational IPv6 gateway of the switch.</li> </ul>

## 4.2 System Time

#### Click Network > System Time

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

Network	⊖ SNTP
IP Address Source Sourc	Ce O From Computer Manual Time
Port Time Zoi	ne UTC +8:00 V
VLAN	
MAC Address Table SNTP	
Spanning Tree Address Typ Discovery	● Hostname ○ IPv4
Multicast Server Addres	SS
ACL Server Po	rt 123 (1 - 65535, default 123)
QoS	
Diagnostics Manual Time	
Management Da	te 1970-01-03 YYYY-MM-DD
Tin	ne 04:30:16 HH:MM:SS
Davlight Saving	1 Time
	None
Туј	<ul> <li>Non-recurring</li> <li>USA</li> <li>Europen</li> </ul>
Offs	et 60 Min (1 - 1440, default 60)
Recurrin	From:     Day     Sun     Week     First     Month     Jan     Time       To:     Day     Sun     Week     First     Month     Jan     Time
Non-recurrin	From: YYYY-MM-DD HH:MM
Operational Sta	To: YYYY-MM-DD HH:MM

Field	Description				
	Select the time source				
	•SNTP: Time sync from NTP server.				
Source	•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					
	Select the mode of daylight saving time.				
	None: Disable daylight saving time.				
	Recurring: Using recurring mode of daylight saving time.				
Туре	Non-Recurring: Using non-recurring mode of daylight saving time.				
	<b>USA</b> : Using daylight saving time in the United States that starts on				
	the second Sunday of March and ends on the first Sunday of				
	November				

	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.
Pocurring From	Specify the starting time of recurring daylight saving time. This field
Recurring From	available when selecting "Recurring" mode.
Pocurring To	Specify the ending time of recurring daylight saving time. This field
Recurring To	available when selecting "Recurring" mode.
Non requiring From	Specify the starting time of non-recurring daylight saving time. This
Non-recurring From	field available when selecting "Non-Recurring" mode.
Non requiring To	Specify the ending time of non-recurring daylight saving time. This
Non-recurring To	field available when selecting "Non-Recurring" mode.

# Chapter 5 Port

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

## 5.1 Port Setting

#### Click Port > Port Setting

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

	Port X	) Port	Setting							
✓ Status										
<ul> <li>Network</li> </ul>	Port	Settin	g Table							
✓ Port										
Port Setting										
Error Disabled		Entry	Port	Туре	Description	State	Link Status	Speed	Duplex	Flow Control
Jumbo Frame		1	10GE1	10G Fiber		Enabled	Up	Auto (1000M)	Full (Full)	Disabled (Disabled)
* VLAN		2	10GE2	10G Fiber		Enabled	Up	Auto (1000M)	Full (Full)	Disabled (Disabled)
✤ MAC Address Table		3	10GE3	10G Fiber		Enabled	Down	Auto	Full	Disabled
✓ Spanning Tree		4	10GE4	10G Fiber		Enabled	Up	Auto (1000M)	Full (Full)	Disabled (Disabled)
✤ Discovery		5	10GE5	10G Fiber		Enabled	Down	Auto	Full	Disabled
✓ Multicast		6	10GE6	10G Fiber		Enabled	Down	Auto	Full	Disabled
✤ Security		7	10GE7	10G Fiber		Enabled	Down	Auto	Full	Disabled
* ACL		8	10GE8	10G Fiber		Enabled	Down	Auto	Full	Disabled
≁ QoS		9	10GE9	10G Fiber		Enabled	Down	Auto	Full	Disabled
<ul> <li>Diagnostics</li> </ul>		10	10GE10	10G Fiber		Enabled	Down	Auto	Full	Disabled
<ul> <li>Management</li> </ul>		11	10GE11	10G Fiber		Enabled	Down	Auto	Full	Disabled
		12	10GE12	10G Fiber		Enabled	Down	Auto	Full	Disabled
	-	Edit	ן							

Field	Description
Port	Port Name.
Туре	Allows you to Enable/Disable the port. When Enable is selected, the port can forward the packets normally.
Description	Port description
	Port admin state.
State	Enabled: Enable the port.
	Disabled: Disable the port.
	Current port link status
Link Status	<b>Up</b> : 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.

#### Note:

- 1. The switch can't be managed through the disable port.
- 2. The switch might lose connection temporarily for the specific port (which connect to the management PC) setting. If it happens, refresh WEB GUI can recover the connection.

#### Edit Port Setting

Port	10GE1	
Description		
State	Enable	
Speed	<ul> <li>Auto</li> <li>1000M</li> <li>10G</li> </ul>	
low Control	<ul><li>Enable</li><li>Disable</li></ul>	

Field	Description				
Port	Selected Port list.				
Description	Port description				
	Port admin state.				
State	Enabled: Enable the port.				
	Disabled: Disable the port.				
	Current port link status				
Link Status	<b>Up</b> : Port is link up.				
	Down: Port is link down.				
	Select the Port speed/duplex capabilities for the ports you need:				
	•Auto: Auto-negotiation speed/ duplex with all capabilities.				
Speed	•1000M: Force speed with 1000M ability				
	•10G: Force speed with 10G ability				
	Port flow control capabilities				
Flow Control	•Enabled: Enable flow control ability.				
	•Disabled: Disable flow control ability.				

### 5.2 Error Disabled

#### Click Port > Error Disabled

Error Disabled is a feature that automatically disables a port on a switch and this feature is designed to inform the administrator when there is a port problem or error. The reasons a switch can go into Error Disabled mode and shutdown a port are many and include: **BPDU Guard**, **UDLD**, **Self Loop**, **Broadcast Flood**, **Unknown Multicast Flood**, **Unicast Flood**, **ACL**, **Port Security**, **DHCP Rate Limit** and **ARP Rate Limit**. When a port is in Error Disabled state, it is effectively shut down and no traffic is sent or received on that port.

	Port >>>> Error Disabled	
✓ Status		
• Network	Pecovery Interval	300 Sec (30, 86400)
	Recovery interval	300 300 (30 - 00400)
Port Setting Error Disabled	BPDU Guard	Enable
<ul> <li>Link Aggregation</li> </ul>	UDLD	Enable
Jumbo Frame	Self Loop	Enable
VLAN	Broadcast Flood	Enable
MAC Address Table	Unknown Multicast Flood	
	Unicast Flood	
	Unicast Flood	
✓ Muticast	ACL	Enable
✓ Security	Port Security	Enable
• ACL	DHCP Rate Limit	Enable
✤ QoS	APP Pate Limit	
<ul> <li>Diagnostics</li> </ul>		
<ul> <li>Management</li> </ul>		
	Apply	

Field	Description		
PDDU Guard	Enable STP and enable BPDU Guard. When the port receive the		
BPD0 Guard	BPDU packet.		
UDLD	When UDLD (UniDirectional Link Detection) happened.		
Solfloop	Enable STP and disable BPDU Guard. When the port receive the		
Sell Loop	BPDU from itself.		
Broadcast Flood	The incoming broadcast packets on the port exceed the rate limit set		
BIOAUCAST FIOOU	in Storm Control and set Action to Shutdown.		
Unknown Multicast	The incoming unknown multicast packets on the port exceed the rate		
Flood	limit set in Storm Control and set Action to Shutdown.		
Unicast Flood	The incoming unknown unicast packets on the port exceed the rate		
Officast Flood	limit set in Storm Control and set Action to Shutdown		
ACL	The packets match the rules set in <b>ACL</b> and set <b>Action</b> to <b>Shutdown</b> .		
Bort Socurity	The number of learning MAC addresses in the port exceeds the limit		
Port Security	set in Port Security and set Action to Shutdown.		
DHCB Bata Limit	The incoming DHCP packets on the port exceed the rate limit set in		
	DHCP Snooping.		
APP Pate Limit	The incoming ARP packets on the port exceed the rate limit set in		
	Dynamic ARP Inspection.		

## 5.3 Link Aggregation

#### Click Port > Link Aggregation

The Link Aggregation is used to combine a number of ports together to make a single high-bandwidth data path, which can highly extend the bandwidth.

#### 5.3.1 Trunk Group Setting

#### Click Port > Link Aggregation > Group

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

	Port >> Link Aggregation >> Group					
✓ Status						
<ul> <li>Network</li> </ul>						
- Port	Load Balance Algorithm					
Port Setting						
Error Disabled	Apply					
<ul> <li>Link Aggregation</li> </ul>						
Group						
Port Setting	Link Aggregation Table					
LACP						
Jumbo Frame						
VLAN	LAC Name Type Link Statue Active Member Inactive Member					
<ul> <li>MAC Address Table</li> </ul>						
Spanning Tree	0 LAG1					
<ul> <li>Discovery</li> </ul>	O LAG 2					
Multicast	O LAG 3					
<ul> <li>Security</li> </ul>	O LAG 4					
ACL	O LAG 5					
v QoS	O LAG 6					
<ul> <li>Diagnostics</li> </ul>	O LAG 7					
<ul> <li>Management</li> </ul>	O LAG 8					
	Edit					

Field	Description		
Load Palanaa	LAG load balance distribution algorithm.		
Algorithm	MAC Address: Based on MAC address		
Algorithm	IP-MAC Address: Based on MAC address and IP address		
LAG	LAG (Link Aggregation Group) Name.		
Name	LAG port description		
	The type of the LAG.		
	Static: The group of ports assigned to a static LAG are always active		
Туре	members.		
	<b>LACP</b> : The group of ports assigned to dynamic LAG are candidate ports.		
	LACP determines which candidate ports are active member ports.		
Link Status	LAG port link status.		
Active Member	Active member ports of the LAG.		
Inactive Member	Inactive member ports of the LAG.		

Select Link Aggregation Table and click "**Edit**" button to edit LAG setting. Edit LAG Group Setting

LAG	1	
LAG	1	
Name		
Trino	<ul> <li>Static</li> </ul>	
туре	O LACP	
	Available Port	Selected Port
Member	10GE1 ^	
	10GE2	^
	10GE3	>
	10GE4	
	10GE5	
	10GE6	<
	10GE7	<b>~</b>
	10GE8 🗸	

Field	Description		
LAG	Selected LAG Group ID		
Name	LAG port description		
	The type of the LAG.		
	Static: The group of ports assigned to a static LAG are always active		
Туре	members.		
	<b>LACP</b> : 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.		

## 5.3.2 Port Setting

#### Click Port > Link Aggregation > Port Setting

This page shows LAG port current status and allows user to edit LAG port configurations.

Port Setting Table							
	Туре	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	ן						

Field	Description
LAG	LAG Port Name
Туре	LAG Port media type
Description	LAG port description

	LAG Port admin state.		
State	Enable: Enable the port		
	Disable: Disable the port		
	Current LAG port link status.		
Link Status	<b>Up</b> : 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.		

Select Port Setting Table and click "Edit" button to edit port setting.

Port	LAG1	
Description		
State	✓ Enable	
Speed	0 1000M	
Flow Control	O Enable	
	O Disable	

Field	Description			
Port	Selected port list			
Description	Port description			
	Port admin state			
State	Enable: Enable the port			
	Disable: Disable the port			
	Port speed capabilities.			
Speed	•1000M: Force speed with 1000M ability.			
	•10G: Force speed with 10G ability			
	Port flow control.			
	•Auto: Auto flow control by negotiation.			
Flow Control	•Enabled: Enable flow control ability.			
	•Disabled: Disable flow control ability.			

#### 5.3.3 LACP

Click Port > Link Aggregation > LACP

This page allow user to configure LACP global and port configurations.

System F	Priority 32	2768	(1 - 65	5535, default 32768)
Apply				
LACP Port	Setting T	able		
Entry	Port	Port Priority	Timeout	
1	10GE1	1	Long	

	2	10GE2	1	Long	
	3	10GE3	1	Long	
	4	10GE4	1	Long	
	5	10GE5	1	Long	
	6	10GE6	1	Long	
	7	10GE7	1	Long	
	8	10GE8	1	Long	
	9	10GE9	1	Long	
	10	10GE10	1	Long	
	11	10GE11	1	Long	
	12	10GE12	1	Long	
Edit					

Field	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.
	The periodic transmissions type of LACP PDUs.
Timeout	Long: Transmit LACP PDU with slow periodic (30s).
	Short: Transmit LACP PDU with fast periodic (1s).

Select ports and click "Edit" button to edit port configuration.

Edit		Port	Setting	
Luit	LACI	1 OIL	ocung	

Port	10GE1		
Port Priority	1	(1 - 65535, default 1)	
Timeout	<ul><li>Long</li><li>Short</li></ul>		

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

## 5.4 Jumbo Frame

Click Port > Jumbo Frame

This page allows user to configure switch jumbo frame size.

Port » Jumbo Frame					
✓ Status					
• Network					
→ Port	Jumbo Frame	NOTE: Enable/10240 byte Disable/1522 byte			
Port Setting		NOTE. Enabler 10240 Byte, Disabler 1022 Byte			
Error Disabled					
<ul> <li>Link Aggregation</li> </ul>					
Group					
Port Setting					
LACP					
Jumbo Frame					

Field	Description
	Enable or Disable jumbo frame.
Jumbo Frame	When jumbo frame is enabled, the frame size 10240 will be used.
	When jumbo frame is disabled, default frame size 1522 will be used.

# Chapter 6 VLAN

A virtual local area network (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 configured through software instead of physically relocating devices or connections.

## 6.1 VLAN

Use the VLAN pages to configure settings of VLAN and all VLAN-related protocol.

#### 6.1.1 Create VLAN

#### Click VLAN > VLAN > Create VLAN

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

	VLAN >> VLAN >> Create VLAN					
✓ Status						
<ul> <li>Network</li> </ul>	Available VLAN Created VLAN					
✤ Port						
VLAN	VLAN Z A VLAN Y A					
~ VLAN	VLAN 4					
VI AN Configuration	VLAN VLAN 5					
Membership	VLAN 6					
Port Setting	VLAN 7 VLAN 8					
<ul> <li>Voice VLAN</li> </ul>	VLAN 9 V					
Surveillance VLAN	Apply					
✓ GVRP						
<ul> <li>MAC Address Table</li> </ul>	VLAN Table Showing All - entries Showing 1 to 1 of 1 entries Q					
<ul> <li>Spanning Tree</li> </ul>						
<ul> <li>Discovery</li> </ul>						
<ul> <li>Multicast</li> </ul>						
✓ Security						
V ACL	First Previous 1 Next Last					
<ul> <li>Diagnostics</li> </ul>	Edit Delete					
	Description					
	VLAN has not created yet.					
able VLAN	Select available VLANs from left box then move to right box					
	VLAN had been created.					
	Select created VLANs from right box then move to left box t					

Click "Edit" button to edit VLAN name

Edit VLAN N	ame	 	 
Name	VLAN0100		 
Apply	Close		

Field	Description
Name	Input VLAN name.

## 6.1.2 VLAN Configuration

#### Click VLAN > VLAN > VLAN Configuration

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

۷	LAN X	VLAN	>> VL	AN Configu	uration			
✓ Status		о <i>г</i>						
<ul> <li>Network</li> </ul>	VLAN	Configu	ration	lable				
✓ Port	VLAN	default	~					
VLAN								
<ul> <li>VLAN</li> </ul>								
Create VLAN	Entry	Port	Mode		Membe	rship		PVID
VLAN Configuration	1	10GE1	Trunk	Excluded	Forbidden	Tagged	<ul> <li>Untagged</li> </ul>	
Membership	2	10GE2	Trunk	Excluded	O Forbidden	<ul> <li>Tagged</li> </ul>	Ontagged	$\checkmark$
	3	10GE3	Trunk	Excluded	<ul> <li>Forbidden</li> </ul>	Tagged	<ul> <li>Untagged</li> </ul>	
Protocol VLAN	4	10GE4	Trunk	Excluded	O Forbidden	Tagged	<ul> <li>Untagged</li> </ul>	<ul> <li>Image: A set of the set of the</li></ul>
<ul> <li>MAC VLAN</li> </ul>	5	10GE5	Trunk	Excluded	O Forbidden	Tagged	<ul> <li>Untagged</li> </ul>	
Surveillance VLAN	6	10GE6	Trunk	Excluded	O Forbidden	Tagged	O Untagged	~
✓ GVRP	7	10GE7	Trunk	O Excluded	O Forbidden	O Tagged	O Untagged	
✤ MAC Address Table	8	10GE8	Trunk	O Excluded	O Forbidden	O Tagged	O Untagged	
<ul> <li>Spanning Tree</li> </ul>	9	10GE9	Trunk	O Excluded			Untagged	
✤ Discovery	10	10GE10	Trunk					
✓ Multicast	11	10GE10	Trunk		Eorbidden			
	12	100510	Trunk	O Excluded				
✓ ACL	12	IUGE 12	Trunk	C Excluded				
	13	LAGT	типк		Forbidden			
<ul> <li>Diagnostics</li> </ul>	14	LAG2	Trunk	CExcluded	OForbidden	O Tagged	O Untagged	
<ul> <li>Management</li> </ul>	15	LAG3	Trunk	<ul> <li>Excluded</li> </ul>	<ul> <li>Forbidden</li> </ul>	<ul> <li>Tagged</li> </ul>	<ul> <li>Untagged</li> </ul>	$\checkmark$
	16	LAG4	Trunk	O Excluded	O Forbidden	Tagged	O Untagged	$\checkmark$
	17	LAG5	Trunk	Excluded	Forbidden	Tagged	Ontagged	
	18	LAG6	Trunk	Excluded	Forbidden	Tagged	<ul> <li>Untagged</li> </ul>	$\checkmark$
	19	LAG7	Trunk	Excluded	O Forbidden	Tagged	<ul> <li>Untagged</li> </ul>	
	20	LAG8	Trunk	Excluded	O Forbidden	Tagged	<ul> <li>Untagged</li> </ul>	~
	Арр	ly						

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

## 6.1.3 Membership

Click VLAN > VLAN > Membership

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

VLAN >> VLAN >> Membership						
✓ Status						
<ul> <li>Network</li> </ul>	Mem	bersh	ip Table			
• Port						
VLAN						
VLAN		Entry	Port	Mode	Administrative VLAN	Operational VLAN
Create VLAN	0	1	10GE1	Trunk	1UP	1UP
VLAN Configuration	0	2	10GE2	Trunk	1UP	1UP
Membership Dort Setting	Õ	3	10GE3	Trunk	1UP	1UP
Voice VLAN	0	4	10GE4	Trunk	1UP	1UP
Protocol VLAN	0	5	10GE5	Trunk	11IP	11.IP
MAC VLAN		6	10026	Trunk	1110	1118
<ul> <li>Surveillance VLAN</li> </ul>		7	10020	Trunk		
✓ GVRP	0	1	IUGE/	TTUTIK	TUP	IUP
<ul> <li>MAC Address Table</li> </ul>	0	8	10GE8	Trunk	1UP	1UP
<ul> <li>Spanning Tree</li> </ul>	0	9	10GE9	Trunk	1UP	1UP
<ul> <li>Discovery</li> </ul>	0	10	10GE10	Trunk	1UP	1UP
<ul> <li>Multicast</li> </ul>	0	11	10GE11	Trunk	1UP	1UP
<ul> <li>Security</li> </ul>	0	12	10GE12	Trunk	1UP	1UP
* ACL	0	13	LAG1	Trunk	1UP	1UP
• QoS	0	14	LAG2	Trunk	1UP	1UP
<ul> <li>Diagnostics</li> </ul>	0	15	LAG3	Trunk	1UP	1UP
<ul> <li>Management</li> </ul>	0	16	LAG4	Trunk	1UP	1UP
	0	17	LAG5	Trunk	1UP	1UP
	0	18	LAG6	Trunk	1UP	1UP
	0	19	LAG7	Trunk	1UP	1UP
	0	20	LAG8	Trunk	1UP	1UP
	E	Edit				

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

Click "Edit" button to edit VLAN membership

#### Edit Port Setting

Port	10GE1
Mode	Trunk
	100 ^ 1UP ^
Membership	v v
	<ul> <li>Forbidden</li> <li>Excluded</li> <li>Tagged</li> <li>Untagged</li> </ul>
	PVID
Apply	Close

Field	Description
Port	Display the interface of port entry.
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. <b>Forbidden</b> : Set VLAN as forbidden VLAN.

Excluded: Set option is always disabled.
Tagged: Set VLAN as tagged VLAN.
Untagged: Set VLAN as untagged VLAN.
<b>PVID</b> : Check this checkbox to select the VLAN ID to be the port-based
VLAN ID for this port. PVID may auto select or can't select in differ
settings.

## 6.1.4 Port Setting

#### Click VLAN > VLAN > Port Setting

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

	VLAN	>> VI	AN >>	Port S	Settin	g			
✓ Status	Port	Settin	a Table						
✓ Network		octain	ig iubic						
✤ Port									
✓ VLAN		Fata	Dert	Mada	D\//D	Assent Frame Trees	In grass Filtering	Unlink	TRID
∧ VLAN		Enuy	For	wode	PVID	Accept Frame Type	ingress Filtering	Оринк	
Create VLAN	U	1	10GE1	Trunk	1	All	Enabled	Disabled	0x8100
VLAN Configuration		2	10GE2	Trunk	1	All	Enabled	Disabled	0x8100
Membership		3	10GE3	Trunk	1	All	Enabled	Disabled	0x8100
Port Setting		4	10GE4	Trunk	1	All	Enabled	Disabled	0x8100
Voice VLAN     Protocol VLAN		5	10GE5	Trunk	1	All	Enabled	Disabled	0x8100
<ul> <li>MAC VLAN</li> </ul>		6	10GE6	Trunk	1	All	Enabled	Disabled	0x8100
<ul> <li>Surveillance VLAN</li> </ul>		7	10GE7	Trunk	1	All	Enabled	Disabled	0x8100
✓ GVRP		8	10GE8	Trunk	1	All	Enabled	Disabled	0x8100
<ul> <li>MAC Address Table</li> </ul>		9	10GE9	Trunk	1	All	Enabled	Disabled	0x8100
<ul> <li>Spanning Tree</li> </ul>		10	10GE10	Trunk	1	All	Enabled	Disabled	0x8100
<ul> <li>Discovery</li> </ul>		11	10GE11	Trunk	1	All	Enabled	Disabled	0x8100
Multicast		12	10GE12	Trunk	1	All	Enabled	Disabled	0x8100
✓ Security		13	LAG1	Trunk	1	All	Enabled	Disabled	0x8100
✓ ACL		14	LAG2	Trunk	1	All	Enabled	Disabled	0x8100
		15	LAG3	Trunk	1	All	Enabled	Disabled	0x8100
Management		16	LAG4	Trunk	1	All	Enabled	Disabled	0x8100
		17	LAG5	Trunk	1	All	Enabled	Disabled	0x8100
		18	LAG6	Trunk	1	All	Enabled	Disabled	0x8100
		19	LAG7	Trunk	1	All	Enabled	Disabled	0x8100
		20	LAG8	Trunk	1	All	Enabled	Disabled	0x8100
	E	Edit							

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

Click "Edit" button to edit VLAN port setting
Port	10GE1		
Mode	<ul> <li>Hybrid</li> <li>Access</li> <li>Trunk</li> <li>Tunnel</li> </ul>		
PVID	1	(1 - 4094)	
Accept Frame Type	<ul> <li>All</li> <li>Tag Only</li> <li>Untag Only</li> </ul>		
Ingress Filtering	Enable		
Uplink	Enable		
TPID	0x8100 v		

Field	Description
Port	Display the interface of port entry.
	Select the VLAN mode of the interface.
Mode	<b>Access</b> : Accepts only untagged frames and join an untagged VLAN.
	<b>Trunk</b> : An untagged member of one VLAN at most, and is a tagged member of zero or more VLANs.
PVID	Specify the port-based VLAN ID (1~4094). It's only available with hybrid and Trunk mode.
Accept Frame Type	Specify the acceptable-frame-type of the specified interfaces. It's only available with Hybrid mode.
Ingress Filtering	Specify the status of ingress filtering. It's only available with Hybrid mode.
Uplink	Check to enable Uplink. It's only available with Trunk mode.
TPID	The options are: 0x8100, 0x88a8, 0x9100, 0x9200.

## 6.2 Voice VLAN

## 6.2.1 Property

#### Click VLAN > Voice VLAN > Property

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

			State	Enable	•		
			VLAN	None	~		
				Enable			
AN		CoS	5 / 802.1p				
tv			marking	6 ~			
DUI			ing Time	1440		Min (30 - 6553	36, default 144
VLAN		ontAg	ing nine	Note: Aging Time = Port Aging Time + OUI Aging Time(30 mins)			
N .							
ce VLAN		oply	]				
ss ladie	Port	Settin	g Table				
ree	-						
		Entry	Port	State	Mode	QoS Policy	
		1	10GE1	Disabled	Auto	Voice Packet	
		2	10GE2	Disabled	Auto	Voice Packet	
		3	10GE3	Disabled	Auto	Voice Packet	
		4	10GE4	Disabled	Auto	Voice Packet	
		5	10GE5	Disabled	Auto	Voice Packet	
		6	10GE6	Disabled	Auto	Voice Packet	
		7	10GE7	Disabled	Auto	Voice Packet	
		8	10GE8	Disabled	Auto	Voice Packet	
		9	10GE9	Disabled	Auto	Voice Packet	
		10	10GE10	Disabled	Auto	Voice Packet	
		11	10GE11	Disabled	Auto	Voice Packet	
		12	10GE12	Disabled	Auto	Voice Packet	
		13		Disabled	Auto	Voice Packet	
		14		Disabled	Auto	Voice Packet	
		14	LAG2	Disabled	Auto		
		15	LAGS	Disabled	Auto	Voice Packet	
		16	LAG4	Disabled	Auto	voice Packet	
		17	LAG5	Disabled	Auto	Voice Packet	
		18	LAG6	Disabled	Auto	Voice Packet	
		19	LAG7	Disabled	Auto	Voice Packet	

Field	Description
State	Set checkbox to enable or disable voice VLAN function.
VLAN	Select Voice VLAN ID. Voice VLAN ID cannot be default VLAN.
Cos/802.1p	Set checkbox to enable or disable 1p remarking. If enabled, qualified packets will be remark by this value.
Remarking	Select a value of VPT. Qualified packets will use this VPT value as inner priority. (Range: 0-7; Default: 6)
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.

Field	Description
Port	Display port entry
State	Display enable/disable status of interface.
Mode	Display voice VLAN mode.
QoS Policy	Display voice VLAN remark will effect which kind of packet

Click "Edit" button to edit Property Port.

Port	10GE1	
State	Enable	
Mode	<ul> <li>Auto</li> <li>Manual</li> </ul>	
QoS Policy	Voice Packet     All	

Field	Description
Port	Display selected port to be edited.
State	Set checkbox to enable/disable voice VLAN function of interface.
Mode	Select port voice VLAN mode. <b>Auto</b> : Voice VLAN auto detect packets that match OUI table and add received port into voice VLAN ID tagged member. <b>Manual</b> : User need add interface to VLAN ID tagged member manually.
QoS Policy	Select port QoS Policy mode Voice Packet: QoS attributes are applied to packets with OUIs in the source MAC address. All: QoS attributes are applied to packets that are classified to the Voice VLAN.

## 6.2.2 Voice OUI

#### Click VLAN > Voice VLAN > Voice OUI

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

	VLAN >> Voice VLAN >> Voice OUI	
Status     Network     Port	Voice OUI Table	
VLAN	Showing All v entries Showing 1 to	o 8 of 8 entries
VLAN Voice VLAN	Description OUI OUI Ma	ask
Property	3COM 00:E0:BB:00:00:00 FF-FF-FF-0	00-00-00
Voice OUI	Cisco 00:03:6B:00:00:00 FF-FF-FF-0	00-00-00
Protocol VLAN	Veritel 00:E0:75:00:00:00 FF-FF-0	00-00-00
Surveillance VLAN	Pingtel 00:D0:1E:00:00:00 FF-FF-FF-0	00-00-00
✓ GVRP	Siemens 00:01:E3:00:00:00 FF-FF-FF-0	00-00-00
<ul> <li>MAC Address Table</li> </ul>	NEC/Philips 00:60:B9:00:00:00 FF-FF-F-0	00-00-00
<ul> <li>Spanning Tree</li> </ul>	H3C 00:0F:E2:00:00:00 FF-FF-FF-0	00-00-00
✤ Discovery	Avaya 00:09:6E:00:00:00 FF-FF-FF-0	00-00-00
<ul> <li>Multicast</li> <li>Security</li> </ul>	Add Edit Delete	First Previous 1 Next Last
bld	Description	
JI	Display OUI MAC address.	
scription	Display description of OUI en	try.

Click "Add" or "Edit" buttons to add or edit Voice OUI.

Add Voice OUI	
0	ון ::::::::::::::::::::::::::::::::::::
Descriptio	n 📃
NOTE:16 maxim	Um user defined OUI allowed.
k	Description
	Input OUI MAC address. Can't be edited in edit dialog.
cription	Input description of the specified MAC address to the voice VLAN O

## **6.3 Protocol VLAN**

## 6.3.1 Protocol Group

#### Click VLAN > Protocol VLAN > Protocol Group

table.

This page allows you to add new protocols to Group ID (unique for each Group) mapping entries as well as allow you to see and delete already mapped entries for the selected stack switch unit.

VLAN >> Protocol VLAN >> Protocol Group					
✓ Status					
• Network	Drotocol Crown Table				
• Port					
→ VLAN	Showing All v entries Showing 0 to 0 of 0 entries	0			
VLAN		4			
<ul> <li>Voice VLAN</li> </ul>	Group ID Frame Type Protocol Value				
Protocol VLAN	0 results found.				
Protocol Group Group Binding	Add Edit Delete	First Previous 1 Next Last			
<ul> <li>Surveillance VLAN</li> <li>GVRP</li> </ul>					

Click "Add" or "Edit" button to add or edit Protocol VLAN Group.

Group ID	1 ~			
Frame Type	Ethernet_II	×		
Protocol Value	0x		(0x600 ~ 0xFFFE)	

Field	Description
Group ID	Select Group ID 1 to 8.
Frame Type	Select Frame Type. The options are "Ethernet_II", "IEEE802.3_LL_Other" and "RFC_1042".
Protocol Value	Set Protocol Value. The range is 0x600 to 0xFFFE.

## 6.3.2 Group Binding

Click VLAN > Protocol VLAN > Group Binding

This page allows you to map an already configured Group ID to a VLAN for the selected port.

	VLAN >>> Protocol VLAN	>> Group Binding	
✓ Status			
<ul> <li>Network</li> </ul>	Crewn Binding Table		
✓ Port	Group Binding Table		
VLAN	Showing All v entries	Showing 0 to 0 of 0 entries	0
VLAN	· · · · · ·	-	4
<ul> <li>Voice VLAN</li> </ul>	Port Group ID VLAN		
<ul> <li>Protocol VLAN</li> </ul>		0 results found.	
Protocol Group			First Previous 1 Next Last
Group Binding	Add Edit	Delete	
MAC VLAN			
<ul> <li>Surveillance VLAN</li> </ul>			

Click "Add" or "Edit" button to add or edit Group Binding.

	Available Port	Selected Port	
	^	^	
Port		>	
TOR			
	~	<b>`</b>	
	Note: Only VLAN H	ybrid port can be set Protocol VLAN	
Group ID	1 🗸		
VLAN	(1 -	4094)	

Field	Description
Port	Select the port(s) to set Protocol VLAN.
Group ID	Select the Group ID.
VLAN	Indicates the VLAN ID.

## 6.4 MAC VLAN

## 6.4.1 MAC Group

#### Click VLAN > MAC VLAN > MAC Group

The MAC-based VLAN entries can be configured here. This page allows for adding and deleting MAC-based VLAN entries.

	VLAN >> MAC VLAN >> MAC Group	
<ul> <li>Status</li> <li>Network</li> </ul>		
<ul> <li>Port</li> </ul>	MAC Group Table	
	Showing All v entries Showing 0 to 0 of 0 entries	Q
<ul> <li>VLAN</li> <li>Voice VLAN</li> </ul>	Group ID MAC Address Mask	
Protocol VLAN     MAC VLAN	0 results found.	
MAC Group	Add Edit Delete	First Previous 1 Next Last
Group Binding <ul> <li>Surveillance VLAN</li> </ul>		
✓ GVRP		

Click "Add" or "Edit" button to add or edit MAC VLAN.

Group ID	(1 - 2147483647)
NAC Address	
Mask	(9 - 48)

Field	Description
Group ID	Indicates the Group ID.
MAC Address	Indicates the MAC address.
Mask	Indicates the mask.

## 6.4.2 Group Binding

VLAN

#### Click VLAN > MAC VLAN > Group Binding

This page allows for assigning the MAC Group to different ports.

	VLAN >> MAC VLAN >> Group Binding	
✤ Status		
✤ Network	Group Binding Table	
• Port		
VLAN	Showing All v entries Showing 0 to 0 of 0 entrie	es O
VLAN		4
<ul> <li>Voice VLAN</li> </ul>	Port Group ID VLAN	
<ul> <li>Protocol VLAN</li> </ul>	0 results foun	d.
MAC VLAN		First Previous 1 Next Last
MAC Group	Add Edit Delete	
Group Binding		
<ul> <li>Surveillance VLAN</li> </ul>		
✓ GVRP		

Click "Add" or "Edit" button to add or edit Group Binding.

	Port Group ID T Apply	vailable Port Selected Port
Field		Description
Port		Select the port(s) to set MAC VLAN.
Group ID		Select the Group ID.

Indicates the VLAN ID.

# 6.5 Surveillance VLAN

## 6.5.1 Property

#### Click VLAN > Surveillance VLAN > Property

This page allows user to configure global and per interface setting of surveillance VLAN.

	VLAN	>> Si	urveilla	nce VL/	AN >>	Property	
Status							
Network			State		<b>`</b>		
Port			State				
VLAN			VLAN	None	~		
VLAN		CoS	6 / 802.1p	Enable	9		
Voice VLAN		Re	marking	6 ~			
Protocol VLAN     MAC VLAN				1440		Min (30 - 6553	36. default 1440)
Surveillance VLAN		Port Ag	ing Time	Note: Agin	g Time =	Port Aging Time	e + OUI Aging Time(30 mins)
Property	· · · · · ·						5 5 ( , , , , , , , , , , , , , , , , ,
Surveillance OUI	A	pply					
GVRP		0					
MAC Address Table	Port	Settin	ig lable				
Spanning Tree							Q
Discovery		Entry	Port	Stato	Mode	OoS Boliev	
Multicast		1	10GE1	Disabled	Auto	Video Porket	
Security		1	10052	Disabled	Auto	Video Packet	
		2	10062	Disabled	Auto	Video Packet	
		3	10GE4	Disabled	Auto	Video Packet	
Management		4	10005	Disabled	Auto	Video Packet	
		5	10025	Disabled	Auto	Video Packet	
		0	10GE0	Disabled	Auto	Video Packet	
		/	10GE7	Disabled	Auto	Video Packet	
		8	10GE8	Disabled	Auto	Video Packet	
		9	10GE9	Disabled	Auto	Video Packet	
		10	10GE10	Disabled	Auto	Video Packet	
		11	10GE11	Disabled	Auto	Video Packet	
		12	10GE12	Disabled	Auto	Video Packet	
		13	LAGI	Disabled	Auto	Video Packet	
		14	LAG2	Disabled	Auto	video Packet	
		15	LAG3	Disabled	Auto	Video Packet	
		16	LAG4	Disabled	Auto	video Packet	
		17	LAG5	Disabled	Auto	Video Packet	
		18	LAG6	Disabled	Auto	Video Packet	
		19	LAG7	Disabled	Auto	Video Packet	
		20	LAG8	Disabled	Auto	Video Packet	

Field	Description
State	Set checkbox to enable or disable voice VLAN function.
VLAN	Select Video VLAN ID. Video VLAN ID cannot be default VLAN.
Cos/802.1p Remarking	Set checkbox to enable or disable 1p remarking. If enabled, qualified packets will be remark by this value. Select a value of VPT. Qualified packets will use this VPT value as inner priority. (Range: 0-7; Default: 6)
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.

Field	Description
Port	Display port entry
State	Display enable/disable status of interface.
Mode	Display video VLAN mode.
QoS Policy	Display video VLAN remark will effect which kind of packet

Click "Edit" buttons to edit the Surveillance VLAN.

Port	10GE1	
State	Enable	
Mode	<ul> <li>Auto</li> <li>Manual</li> </ul>	
QoS Policy	<ul> <li>Video Packet</li> <li>All</li> </ul>	

Field	Description
Port	Display selected port to be edited.
State	Set checkbox to enable/disable video VLAN function of interface.
	Select port video VLAN mode.
Mode	Auto: Video 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 Video Packet: QoS attributes are applied to packets with OUIs in the source MAC address. All: QoS attributes are applied to packets that are classified to the Video VLAN.

## 6.5.2 Surveillance OUI

#### Click VLAN > Surveillance VLAN > Surveillance OUI

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

VLAN >>> Surveillance VLAN >>> Surveillance OUI				
✓ Status				
<ul> <li>Network</li> </ul>				
✓ Port				
VLAN	Showing All v entries Showing 0 to 0 of 0 entries			
VLAN				
Voice VLAN	Description OUI OUI Mask			
<ul> <li>Protocol VLAN</li> </ul>	0 results found.			
<ul> <li>MAC VLAN</li> <li>Surveillance VLAN</li> <li>Property</li> </ul>	Add Edit Delete First Previous 1 Next Las			
Surveillance OUI				

Click "Add" or "Edit" buttons to add or edit Surveillance OUI.

#### Add Surveillance OUI

NOTE:16 maximum user defined OUI allowed.

Apply Close				
Field	Description			
OUI	Input OUI MAC address.			
Description	Input description of the specified MAC address to the video VLAN OUI table.			

# 6.6 GVRP

## 6.6.1 Property

#### Click VLAN > GVRP > Property

GVRP (GARP VLAN Registration Protocol) is a protocol that facilitates control of virtual local area networks (VLANs) within a larger network. GVRP conforms to the IEEE 802.1Q specification, which defines a method of tagging frames with VLAN configuration data. This allows network devices to dynamically exchange VLAN configuration information with other devices.

GVRP provides dynamic registration of VLAN membership; therefore, members can be added or removed from a VLAN at any time, saving the overhead of maintaining static VLAN configuration on switch ports. Additionally, VLAN membership information stays current, limiting the broadcast domain of a VLAN only to the active members of that VLAN.

Status          Status         VLAN         VLAN         VAN         Vote VLAN         Protocol VLAN         Mac VLAN         Stryellance VLAN         OVRP         Property         Mac Address Table         Statustics         Obscovery         1       10GE1         Disabled       Enabled         AOL         AOL         AOL         OOS         Socumy         State         Disabled         State         Disabled         State         Socuming         Tode         Socuming         Tode         Socuming         Tode         Socuming         Tode         Socuming         Socuming         Tole		VLAN	)) G	VRP >>	Proper	ty		
Network     Perit     Perit     Perit     Perit     Perit     VLAN     VLAN     VLAN     VLAN     VLAN     VLAN     Voke VLAN     Discovery     Proporty     Membership     Statistics     Mores     Discovery     Port     Discovery     Tete     Tetet     Tete     Te	Status							
Port       ULAN         VLAN       Operational Timeout         Oute VLAN       0 ms         Protocol VLAN       60 ms         ACC VLAN       0 ms         Overational Timeout       1000 ms         Covery       60 ms         Property       Rembership         Statistics       ACC Address table         Statistics       1000 ms         Matic valuess table       Statistics         Multicast       2 106E2         Discovery       1 100E1         Multicast       3 106E3         Security       3 106E3         ACC       1 100E1         2 106E2       Disabled         3 106E3       Disabled         Coc       5 106E5         Diagnostics       1006E7         Management       7 106E7         1 1 106E11       Disabled         B 106E8       Disabled         B 106E9       Disabled         B 106E7       Disabled         B 106E8       Disabled         B 106E9       Disabled         B 106E10       Disabled         B 106E9       Disabled         B 106E9       Disabled         <	Network		Stat		able			
VLAN         VIAN         Vice VLAN         Protocol VLAN         Survellance VLAN         CVRP         Property         Mac VLAN         Statistics         MAC VLAN         Statistics         Statistics         MAC Address Table         Statistics         Discovery         Multicast         Security         ACL         Cos         Cos         Diagnostics         Management         Management         1006210         Diagnostics         Management         11       100E10         Diabled       Enabled       Normal         Cos       100E50       Disabled       Enabled       Normal         Cos       100E60       Disabled       Enabled       Normal         Cos       100E610       Disabled       Enabled       <	Port		Stat		able			
VLAN Volce VLAN Protocol VLAN Surveillance VLAN Membership Statistics Port State VLAN Creation Registration Port State VLAN Creation Registration Port State VLAN Creation Registration Sourceillance VLAN Membership Statistics Apply Port State VLAN Creation Registration Sourceillance VLAN Apply Port State VLAN Creation Registration Sourceillance VLAN Address Table State VLAN Creation Registration Sourceillance VLAN Note State VLAN Creation Registration Sourceillance VLAN Sourceillance VLAN Note State VLAN Creation Registration Sourceillance VLAN Sourceillance VLAN<	VLAN	O	peration	al Timeou	ıt			
Votco VLAN Protocol VLAN 60 ms 60 ms 60 ms 1000 ms <	VLAN		.loi	n 20 ms				
Protocol VLAN MAC VLAN AVAC VLAN GVPP Property Membership Statistics Statistics Port Setting Table Statistics C Port Setting Table Statistics C Discovery I 1 10GE1 Disabled Enabled Normal ACL Cois Diagnostics Management I 10GE2 Disabled Enabled Normal I 10GE3 Disabled Enabled Normal I 10GE5 Disabled Enabled Normal I 11 10GE1 Disabled Enabled Normal I 12 10GE7 Disabled Enabled Normal I 13 LAG3 Disabled Enabled Normal I 14 LAG2 Disabled Enabled Normal I 14 LAG3 Disabled Enabled Normal I 14 LAG3 Disabled Enabled Normal I 14 LAG3 Disabled Enabled Normal I 14 LAG	<ul> <li>Voice VLAN</li> </ul>			20 110				
MAC VLAN     GVRP     Property     Membership     Statistics     MAC Address Table     Port Setting Table     Port Setting Table     Port State VLAN Creation Registration     Statistics     Multicast     Security     ACL     Go     Go	Protocol VLAN		Leav	e 60 ms				
GVRP       Apply         Property Membership Statistics       Port Setting Table         Site       VLAN Creation       Registration         Discovery       1       100E1       Disabled       Enabled       Normal         Security       3       100E3       Disabled       Enabled       Normal         CoS       1       100E64       Disabled       Enabled       Normal         CoS       5       100E56       Disabled       Enabled       Normal         Bignostics       6       100E64       Disabled       Enabled       Normal         Bignostics       6       100E65       Disabled       Enabled       Normal         Bignostics       6       100E61       Disabled       Enabled       Normal         Bignostics       10       100E10       Disabled       Enabled       Normal         Bignostics       10       100E10       Disabled       Enabled       Normal         Bignostics       10       100E10       Disabled       Enabled       Normal         Bignostics       10       100E110       Disabled       Enabled       Normal         Bignostics       10       100E110       Disabled	MAC VLAN Supreillance VLAN		LeaveA	II 1000 n	ns			
Property Membership Statistics       Port Setting Table         MAC Address Table       Image: Construction of the state of t	GVRP		A	1				
Membership Statelics       Port Setting Table         MAC Address Table	Property		Арріу	J				
Statistics         MAC Address Table       Port       State       VLAN Creation       Registration         Discovery <ul> <li>1</li> <li>10GE1</li> <li>Disabled</li> <li>Enabled</li> <li>Normal</li> </ul> <ul> <li>1</li> <li>10GE5</li> <li>Disabled</li> <li>Enabled</li> <li>Normal</li> </ul> <ul> <li>1</li> <li>10GE5</li> <li>Disabled</li> <li>Enabled</li> <li>Normal</li> </ul> <ul> <li>10GE5</li> <li>Disabled</li> <li>Enabled</li> <li>Normal</li> <li>State</li> <li>Stabled</li> <li>Enabled</li> <li>Normal</li> <li>State</li> <li>Stabled</li> <li>Enabled</li> <li>Normal</li> <li>State</li> <li>Stabled</li> <li>Stabled</li> <li>Enabled</li> <li>Normal</li> <li>Stabled</li> <li>Enabled</li> <li>Normal</li> <li>Stabled</li> <li>Enabled</li> <li>Normal</li> <li>Stabled</li> <li>Enabled</li> <li>Stabled</li> <li>Enabled</li> <li>Normal</li></ul>	Membership	Port	t Settir	ig Table				
MAC Address Table       Pot       State       VLAN Creation       Registration         Discovery <ul> <li>1</li> <li>10GE1</li> <li>Disabled</li> <li>Enabled</li> <li>Normal</li> </ul> Act       2       10GE2       Disabled       Enabled       Normal         Act       3       10GE3       Disabled       Enabled       Normal         CoS       3       10GE5       Disabled       Enabled       Normal         Diagnostics       6       10GE6       Disabled       Enabled       Normal         Banagement       7       10GE7       Disabled       Enabled       Normal         Banagement       9       10GE9       Disabled       Enabled       Normal         Banagement       10       10GE10       Disabled       Enabled       Normal         Banagement       11       10GE10       Disabled       Enabled       Normal	Statistics							0
Spanning TreeImage: stateVLAN CreationRegistrationDiscoveryMulticastSecurityCalCosDiagnosticsDiagnosticsManagementImage TreeImage Tree <th>MAC Address Table</th> <th>_</th> <th></th> <th></th> <th></th> <th></th> <th></th> <th>~</th>	MAC Address Table	_						~
Discovery       1       10GE1       Disabled       Enabled       Normal         Multicast       2       10GE2       Disabled       Enabled       Normal         Security       3       10GE3       Disabled       Enabled       Normal         ACL       3       10GE3       Disabled       Enabled       Normal         GoS       6       10GE6       Disabled       Enabled       Normal         Diagnostics       6       10GE7       Disabled       Enabled       Normal         Management       7       10GE7       Disabled       Enabled       Normal         9       10GE9       Disabled       Enabled       Normal         9       10GE9       Disabled       Enabled       Normal         9       10GE10       Disabled       Enabled       Normal         10       10GE10       Disabled       Enabled       Normal         11       10GE11       Disabled       Enabled       Normal         11       10GE12       Disabled       Enabled       Normal         11       10GE12       Disabled       Enabled       Normal         11       10GE12       Disabled       Enabled	Spanning Tree		Entry	Port	State	VLAN Creation	Registration	
Mulicasi       2       10GE2       Disabled       Enabled       Normal         Security       3       10GE3       Disabled       Enabled       Normal         ACL       4       10GE4       Disabled       Enabled       Normal         Gos       5       10GE5       Disabled       Enabled       Normal         Diagnostics       6       10GE6       Disabled       Enabled       Normal         0       7       10GE7       Disabled       Enabled       Normal         0       6       10GE6       Disabled       Enabled       Normal         0       7       10GE7       Disabled       Enabled       Normal         0       10       10GE10       Disabled       Enabled       Normal         0       10       10GE10       Disabled       Enabled       Normal         0       10       10GE10       Disabled       Enabled       Normal         11       10GE10       Disabled       Enabled       Normal         12       10GE12       Disabled       Enabled       Normal         13       LAG1       Disabled       Enabled       Normal         14       LAG2 <td>Discovery</td> <td></td> <td>1</td> <td>10GE1</td> <td>Disabled</td> <td>Enabled</td> <td>Normal</td> <td></td>	Discovery		1	10GE1	Disabled	Enabled	Normal	
Security       3       10GE3       Disabled       Enabled       Normal         ACL       0.5       10GE5       Disabled       Enabled       Normal         Gos       5       10GE5       Disabled       Enabled       Normal         Management       6       10GE5       Disabled       Enabled       Normal         9       10GE7       Disabled       Enabled       Normal         10       7       10GE7       Disabled       Enabled       Normal         10       10       10GE10       Disabled       Enabled       Normal         10       10GE10       Disabled       Enabled       Normal         11       10GE10       Disabled       Enabled       Normal         12       10GE12       Disabled       Enabled       Normal         13       LG31       Disabled       Enabled       Normal         14       LG2       Disabled       Enabled       Normal         15       LAG3       Disabled       Enabled       Normal         16       LAG4       Disabled       Enabled       Normal         17       LAG5       Disabled       Enabled       Normal	Multicast		2	10GE2	Disabled	Enabled	Normal	
ACL       QoS       GoS       10GE4       Disabled       Enabled       Normal         Diagnostics       6       10GE6       Disabled       Enabled       Normal         Management       7       10GE7       Disabled       Enabled       Normal         0       8       10GE8       Disabled       Enabled       Normal         0       9       10GE7       Disabled       Enabled       Normal         0       9       10GE10       Disabled       Enabled       Normal         0       10       10GE10       Disabled       Enabled       Normal         1       10       10GE10       Disabled       Enabled       Normal         1       10       10GE11       Disabled       Enabled       Normal         1       10       10GE12       Disabled       Enabled       Normal         1       11       10GE12       Disabled       Enabled       Normal         1       14       LG2       Disabled       Enabled       Normal         1       16       LG3       Disabled       Enabled       Normal         1       16       LG3       Disabled       Enabled       Norm	Security		3	10GE3	Disabled	Enabled	Normal	
Clos       5       10GE5       Disabled       Enabled       Normal         Diagnostics       6       10GE6       Disabled       Enabled       Normal         Management       7       10GE7       Disabled       Enabled       Normal         9       10GE9       Disabled       Enabled       Normal         9       10GE9       Disabled       Enabled       Normal         1       10       10GE10       Disabled       Enabled       Normal         1       10       10GE10       Disabled       Enabled       Normal         1       11       10GE10       Disabled       Enabled       Normal         1       11       Disabled       Enabled       Normal         1       11       LAG2       Disabled       Enabled       Normal	ACL		4	10GE4	Disabled	Enabled	Normal	
Diagnositics                6               10GE               Diabled               Normal               Normal          Management              7               10GE               Disabled               Enabled               Normal                 8               10GE               Disabled               Rabled               Normal                 9               10GE               Disabled               Normal               Normal                   10               10GE               Disabled               Normal                   11               10GE               Disabled               Normal                   11               10GE               Disabled               Normal                   11               10GE               Disabled               Normal                   112               10GE               Disabled	Qos		5	10GE5	Disabled	Enabled	Normal	
Maragement       7       10GE7       Disabled       Enabled       Normal         8       10GE8       Disabled       Enabled       Normal         9       10GE9       Disabled       Enabled       Normal         1       10       10GE10       Disabled       Enabled       Normal         1       10       10GE10       Disabled       Enabled       Normal         1       10       10GE10       Disabled       Enabled       Normal         1       11       LAG1       Disabled       Enabled       Normal         1       11       LAG2       Disabled       Enabled <td>Diagnostics</td> <td></td> <td>6</td> <td>10GE6</td> <td>Disabled</td> <td>Enabled</td> <td>Normal</td> <td></td>	Diagnostics		6	10GE6	Disabled	Enabled	Normal	
810GE8DisabledEnabledNormal910GE9DisabledEnabledNormal101010GE10DisabledEnabledNormal111010GE10DisabledEnabledNormal111110GE11DisabledEnabledNormal111210GE12DisabledEnabledNormal1113LAG1DisabledEnabledNormal1114LAG2DisabledEnabledNormal1115LAG3DisabledEnabledNormal1116LAG4DisabledEnabledNormal1117LAG5DisabledEnabledNormal1117LAG6DisabledEnabledNormal1110LAG7DisabledEnabledNormal1210LAG8DisabledEnabledNormal13LAG6DisabledEnabledNormal14LAG5DisabledEnabledNormal15LAG8DisabledEnabledNormal14LAG6DisabledEnabledNormal15LAG8DisabledEnabledNormal15LAG8DisabledEnabledNormal16LAG8DisabledEnabledNormal17LAG8DisabledEnabledNormal16LAG8DisabledEnabledNormal17LAG8Dis	Management		7	10GE7	Disabled	Enabled	Normal	
910GE9DisabledEnabledNormal1010GE10DisabledEnabledNormal1110GE11DisabledEnabledNormal1210GE12DisabledEnabledNormal13LAG1DisabledEnabledNormal14LAG2DisabledEnabledNormal15LAG3DisabledEnabledNormal1616LAG4DisabledNormal17LAG5DisabledEnabledNormal18LAG6DisabledEnabledNormal20LAG8DisabledEnabledNormal			8	10GE8	Disabled	Enabled	Normal	
1010GE10DisabledEnabledNormal1110GE11DisabledEnabledNormal1210GE12DisabledEnabledNormal13LAG1DisabledEnabledNormal14LAG2DisabledEnabledNormal15LAG3DisabledEnabledNormal1616LAG4DisabledEnabledNormal17LAG5DisabledEnabledNormal18LAG6DisabledEnabledNormal20LAG8DisabledEnabledNormal			9	10GE9	Disabled	Enabled	Normal	
1110GE11DisabledEnabledNormal1210GE12DisabledEnabledNormal13LAG1DisabledEnabledNormal14LAG2DisabledEnabledNormal15LAG3DisabledEnabledNormal16LAG4DisabledEnabledNormal17LAG5DisabledEnabledNormal18LAG6DisabledEnabledNormal20LAG8DisabledEnabledNormal			10	10GE10	Disabled	Enabled	Normal	
1210GE12DisabledEnabledNormal13LAG1DisabledEnabledNormal14LAG2DisabledEnabledNormal15LAG3DisabledEnabledNormal16LAG4DisabledEnabledNormal17LAG5DisabledEnabledNormal18LAG6DisabledEnabledNormal19LAG6DisabledEnabledNormal20LAG8DisabledEnabledNormal			11	10GE11	Disabled	Enabled	Normal	
13LAG1DisabledEnabledNormal14LAG2DisabledEnabledNormal15LAG3DisabledEnabledNormal16LAG4DisabledEnabledNormal17LAG5DisabledEnabledNormal18LAG6DisabledEnabledNormal19LAG7DisabledEnabledNormal20LAG8DisabledEnabledNormal			12	10GE12	Disabled	Enabled	Normal	
14LAG2DisabledEnabledNormal15LAG3DisabledEnabledNormal16LAG4DisabledEnabledNormal17LAG5DisabledEnabledNormal18LAG6DisabledEnabledNormal19LAG7DisabledEnabledNormal20LAG8DisabledEnabledNormal			13	LAG1	Disabled	Enabled	Normal	
15       LAG3       Disabled       Enabled       Normal         16       LAG4       Disabled       Enabled       Normal         17       LAG5       Disabled       Enabled       Normal         18       LAG6       Disabled       Enabled       Normal         19       LAG7       Disabled       Enabled       Normal         20       LAG8       Disabled       Enabled       Normal			14	LAG2	Disabled	Enabled	Normal	
16       LAG4       Disabled       Enabled       Normal         17       LAG5       Disabled       Enabled       Normal         18       LAG6       Disabled       Enabled       Normal         19       LAG7       Disabled       Enabled       Normal         20       LAG8       Disabled       Enabled       Normal			15	LAG3	Disabled	Enabled	Normal	
17     LAG5     Disabled     Enabled     Normal       18     LAG6     Disabled     Enabled     Normal       19     LAG7     Disabled     Enabled     Normal       20     LAG8     Disabled     Enabled     Normal			16	LAG4	Disabled	Enabled	Normal	
18     LAG6     Disabled     Enabled     Normal       19     LAG7     Disabled     Enabled     Normal       20     LAG8     Disabled     Enabled     Normal			17	LAG5	Disabled	Enabled	Normal	
19 LAG7 Disabled Enabled Normal     20 LAG8 Disabled Enabled Normal			18	LAG6	Disabled	Enabled	Normal	
20 LAG8 Disabled Enabled Normal			19	LAG7	Disabled	Enabled	Normal	
			20	LAG8	Disabled	Enabled	Normal	
			_0		Disabiod	Entropo		

Click "Edit" buttons to edit GVRP.

Edit Port Settin	ıg
------------------	----

Port	10GE1
State	Enable
VLAN Creation	Enable
Registration	<ul> <li>Normal</li> <li>Fixed</li> <li>Forbidden</li> </ul>

Apply Close

Field	Description			
State	Check to enable GVRP.			
VLAN Creation	Check to enable dynamic VLAN Creation.			
Registration	Select Registration mode. By default GVRP ports are in <b>Normal</b> registration mode. These ports use GVRP join messages from neighboring switches to prune the VLANs running across the 802.1Q trunk link. If the device on the other side is not capable of sending GVRP messages, or if you do not want to allow the switch to prune any of the VLANs, use the <b>Fixed</b> mode. Fixed mode ports will forward for all VLANs that exist in the switch database. Ports in <b>Forbidden</b> mode forward only for VLAN 1.			

## 6.6.2 Membership

#### Click VLAN > GVRP > Membership

This page allow user to view GVRP membership information.

VLAN >> GVRP >> Membership					
<ul> <li>Status</li> </ul>					
<ul> <li>Network</li> </ul>	Membership Table				
✤ Port					
+ VLAN	Showing All v entries Showing 0 to 0 of 0 entries	0			
VLAN		4			
<ul> <li>Voice VLAN</li> </ul>	VLAN Member Dynamic Member Type				
<ul> <li>Protocol VLAN</li> </ul>	0 results found.				
MAC VLAN		First Previous 1 Next Last			
<ul> <li>Surveillance VLAN</li> </ul>					
∧ GVRP					
Property					
Membership					
Statistics					

## 6.6.3 Statistics

Click VLAN > GVRP > Statistics

This page allow user to view GVRP statistics in each port.

V	LAN >> GVRP >	) Statis	stics
<ul> <li>Status</li> </ul>			
<ul> <li>Network</li> </ul>	Bort	10CE1	
✓ Port	FUIL	IUGET	×
VLAN		All Deceiv	
VLAN	Statistics	Received Transr	nit
<ul> <li>Voice VLAN</li> </ul>		O Error	
Protocol VLAN		None	
MAC VLAN Surveillance VLAN	Pofrech Pate	5 sec	
∧ GVRP	Refresh Rate	10 sec	
Property		0 30 sec	
Membership	Clear		
Statistics			
	Receive		
Discovery	Join empty	0	
<ul> <li>Multicast</li> </ul>	Empty	0	
✤ Security		0	
⋆ ACL			
✓ QoS	Join In	0	
<ul> <li>Diagnostics</li> </ul>	Leave In	0	
<ul> <li>Management</li> </ul>	Leave All	0	
	Transmit		
	Join empty	0	
	Empty	0	
	Leave Empty	0	
	Join In	0	
	Leave In	0	
	Leave All	0	
	Error		
	Invalid Pro	tocol ID	0
	Invalid Attribu	te Type	0
	Invalid Attribut	e Value	0
	Invalid Attribute	Length	0
	Invali	d Event	0

# Chapter 7 MAC Address Table

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

## 7.1 Dynamic Address

#### Click MAC Address Table > Dynamic Address

Configure the aging time of the dynamic address. Click **Add Static Address** to add a MAC address to a static MAC address.

	MAC Address Table >> Dynamic Address
<ul> <li>Status</li> <li>Network</li> <li>Port</li> <li>VLAN</li> <li>MAC Address Table</li> <li>Dynamic Address Static Address</li> <li>Filtering Address</li> <li>Spanning Tree</li> </ul>	Aging Time       300       Sec (10 - 630, default 300)         Apply       Dynamic Address Table         Showing All v entries       Showing 1 to 7 of 7 entries
<ul> <li>Discovery</li> <li>Multicast</li> <li>Security</li> <li>ACL</li> <li>QoS</li> <li>Diagnostics</li> <li>Management</li> </ul>	VLAN         MAC Address         Port           1         00:03:79:08:0D:94         10GE2           1         00:08:54:73:ED:F9         10GE2           1         00:0E:C6:82:34:98         10GE1           1         00:0F:C9:12:34:56         10GE2           1         00:0F:C9:12:34:56         10GE2           1         00:0F:C9:12:34:71         10GE2           1         00:0F:C9:12:34:71         10GE2           1         00:0F:C9:12:34:71         10GE2           1         00:17:16:07:E3:40         10GE2           1         8C:16:45:37:F3:67         10GE4
Field	Description
Aging Time	The time in seconds that an entry remains in the MAC address table. Its valid range is from 10 to 630 seconds, and the default value is 300 seconds

## 7.2 Static Address

#### Click MAC Address Table > Static Address

To display the static MAC address. Click **Add**, **Edit** or **Delete** to add, edit or delete a static MAC address.

	MAC Address Table >>> Static Address		
	Static Address Table         Showing All vertices       Showing 0 to 0 of 0 entries         VLAN       MAC Address         Port       0 results found.		
Filtering Address <ul> <li>Spanning Tree</li> </ul>	Add Edit Delete First Previous 1 Next Last		
Field	Description		
MAC Address	The MAC address to which packets will be statically fowarded.		
VLAN	The VLAN ID that MAC address used.		
Port	Interface or port number.		

# 7.3 Filtering Address

#### Click MAC Address Table > Filtering Address

To display the filtering MAC address. Click **Add**, **Edit** or **Delete** to add, edit or delete a filtering MAC address.

	MAC Address Table >> Filtering Address
✓ Status	
<ul> <li>Network</li> </ul>	Filtering Address Table
✓ Port	
✓ VLAN	Showing All v entries Showing 0 to 0 of 0 entries
<ul> <li>MAC Address Table</li> </ul>	
Dynamic Address	VLAN MAC Address
Static Address	0 results found.
Filtering Address	First Previous 1 Next Last
<ul> <li>Spanning Tree</li> </ul>	Add Edit Delete
Field	Description
VLAN	The VLAN ID that MAC address used.
MAC Address	The MAC address to which packets will be filtered.

# Chapter 8 Spanning Tree

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

## 8.1 Property

Click Spanning Tree > Property

Configure and display STP property configuration.

Spanning Tree >> Prop	erty	
• Status		
Network	Enable	
✓ Port		
<ul> <li>VLAN</li> <li>Operation Mode</li> </ul>	RSTP	
MAC Address Table	MSTP	
✓ Spanning Tree	<ul> <li>Long</li> </ul>	
Property Path Cost	<ul> <li>Short</li> </ul>	
MST Instance BPDU Handling MST Port Setting	<ul><li>Filtering</li><li>Flooding</li></ul>	
Statistics  Discovery  Priority	32768	(0 - 61440, default 32768)
Multicast     Hello Time	2	Sec (1 - 10, default 2)
ACL     Max Age	20	Sec (6 - 40, default 20)
✓ QoS Forward Delay	15	Sec (4 - 30, default 15)
Diagnostics		
Management     Tx Hold Count	6	(1 - 10, default 6)
Region Name	FC:8F:C4:0D:22:11	
Revision	0	(0 - 65535, default 0)
Мах Нор	20	(1 - 40, default 20)
Operational Status		
Bridge Identifiter	32768-FC:8F:C4:0D:22	2:11
Designated Root Bridge	32768-00:08:54:73:ED	:F9
Root Port	XGigabitEthernet2	
Root Path Cost	30000	
Topology Change Count	6	
Last Topology Change	0D/1H/26M/29S	
Apply		

Field	Description
State	Enable/Disable the STP on the switch.
Operation Mode	Specify the STP operation mode. <b>STP</b> : Enable the Spanning Tree (STP) operation. <b>RSTP</b> : Enable the Rapid Spanning Tree (RSTP) operation. <b>MSTP</b> : Enable the Multiple Spanning Tree (MSTP) operation.
Path Cost	Specify the path cost method. <b>Long</b> : Specifies that the default port path costs are within the range: 1~200,000,000. <b>Short</b> : 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. <b>Filtering</b> : Filter the BPDU when STP is disabled. <b>Flooding</b> : 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 bridge 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	This name uniquely identifies the MSTI (Multiple Spanning Tree Instance). Enter a descriptive name (up to 32 characters) for an MST region. The default is the MAC address name of the device running MSTP.
Revision	This value, along with the Region Name, identifies the MSTP region configured on the Switch. Devices must have the same revision number to belong to the same region
Мах Нор	Used to set the number of hops between devices in a spanning tree region before the BPDU packet sent by the Switch is discarded. Each Switch on the hop count will reduce the hop count by one until the value reaches zero. The Switch will then discard the BDPU packet and the information held for the port will age out. The user may set a hop count from 1 to 40. The default value is: 20.

#### STP operational status

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

# 8.2 Port Setting

## Click Spanning Tree > Port Setting

Configure and display STP port settings.

#### Spanning Tree >> Port Setting

Port Setting Table

Spanning Tree Property Port Setting

													0	
_													4	<u> </u>
	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	10GE1	Enabled	20000	128	Disabled	Disabled	Disabled	Enabled	Designated	Forwarding	32768-FC:8F:C4:0D:22:11	128-1	20000
	2	10GE2	Enabled	20000	128	Disabled	Disabled	Disabled	Enabled	Root	Forwarding	32768-00:0F:C9:12:34:56	128-2	20000
	3	10GE3	Enabled	2000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-3	2000
	4	10GE4	Enabled	20000	128	Disabled	Disabled	Disabled	Enabled	Designated	Forwarding	32768-FC:8F:C4:0D:22:11	128-4	20000
	5	10GE5	Enabled	2000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-5	2000
	6	10GE6	Enabled	2000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-6	2000
	7	10GE7	Enabled	2000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-7	2000
	8	10GE8	Enabled	2000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-8	2000
	9	10GE9	Enabled	2000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-9	2000
	10	10GE10	Enabled	2000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-10	2000
	11	10GE11	Enabled	2000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-11	2000
	12	10GE12	Enabled	2000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-12	2000
	13	LAG1	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-13	20000
	14	LAG2	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-14	20000
	15	LAG3	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-15	20000
	16	LAG4	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-16	20000
	17	LAG5	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-17	20000
	18	LAG6	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-18	20000
	19	LAG7	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-19	20000
	20	LAG8	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-20	20000

Edit	Protocol Migration Check	
------	--------------------------	--

Field	Description					
Port	Specify the interface ID or the list of interface IDs.					
State	The operational state on the specified port.					
Path Cost	STP path cost on the specified port.					
Priority	STP priority on the specified port.					
BPDU Filter	Control whether a port will transmit and receive BPDUs.					
	Control whether a port will disable itself upon reception of a BPDU.					
BPDU Guard	The port will enter the Error Disabled state, and will be removed from					
	the active topology					
Operational Edge	The operational edge port on the specified port.					
Operational Point-to- Point	The operational edge 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.					

#### STP port setting buttons

<b>v</b>	
Field	Description
Protocol Migration	Restart the Spanning Tree Protocol (STP) migration process (re-
Check	negotiate with its neighborhood) on the specific interface.

Edit STP port setting

**Edit Port Setting** 

Port	10GE1
State	Z Enable
Path Cost	<b>0</b> (0 - 20000000) (0 = Auto)
Priority	128 🗸
Edge Port	Enable
BPDU Filter	Enable
BPDU Guard	Enable
Point-to-Point	Auto     Enable     Disable
Port State	Forwarding
Designated Bridge	32768-FC:8F:C4:0D:22:11
Designated Port ID	128-1
Designated Cost	20000
Operational Edge	False
Operational Point-to-Point	True

Apply Close

Field	Description					
State	Enable/Disable the STP on the specified port					
Path Cost	Specify the STP path cost on the specified port.					
Priority	Specify the STP priority on the specified port.					
	Specify the edge mode.					
	<b>Enable</b> : Force to true state (as link to a host)					
	<b>Disable</b> : Force to false state (as link to a bridge)					
Edge Port	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	Control whether a port will transmit and receive BPDUs.					
	Control whether a port will disable itself upon reception of a BPDU.					
BPDU Guard	The port will enter the Error Disabled state, and will be removed from					
	the active topology					
	Specify the Point-to-Point port configuration:					
Point to Point	Auto: The state is depended on the duplex setting of the port.					
Formeto-Form	Enable: Force to true state.					
	Disable: Force to false state.					

## 8.3 MST Instance

#### Click Spanning Tree > MST Instance

Configure and display MST Instance.

Multiple Spanning Tree Protocol or MSTP enables the grouping of multiple VLANs with the same topology requirements into one Multiple Spanning Tree Instance (MSTI). MSTP then builds an Internal Spanning Tree (IST) for the region containing commonly configured MSTP bridges. Instances are not supported in STP or RSTP. Instead, they have the same spanning tree in common

within the VLAN. MSTP provides the capability to logically divide a Layer 2 network into regions. Every region can contain multiple instances of spanning trees. In MSTP, all of the interconnected bridges that have the same MSTP configuration comprise an MST region.

Spar	nning	Tree ))	MST Instance					
MS	Tineta	nco Tab	le					
Inc	i mata		10					
	MSTI	Priority	Bridge Identifiter	Designated Root Bridge	Root Port	Root Path Cost	Remaining Hop	VLAN
ress Table	0	32768	32768-FC:8F:C4:0D:22:11	32768-00:08:54:73:ED:F9	XGigabitEthernet2	30000	20	1-4094
Tree	) 1	32768	32768-FC:8F:C4:0D:22:11	32768-FC:8F:C4:0D:22:11	XGigabitEthernet2	0	20	
0	2	32768	32768-FC:8F:C4:0D:22:11	32768-FC:8F:C4:0D:22:11	XGigabitEthernet2	0	20	
tting	3	32768	32768-FC:8F:C4:0D:22:11	32768-FC:8F:C4:0D:22:11	XGigabitEthernet2	0	20	
stance	4	32768	32768-EC:8E:C4:0D:22:11	32768-EC:8E:C4:0D:22:11	XGigabitEthernet2	0	20	
	5	32768	32768-EC:8E:C4:0D:22:11	32768-EC:8E:C4:0D:22:11	XGigabitEthernet2	0	20	
	6	32768	32768-FC:8F:C4:0D:22:11	32768-FC:8F:C4:0D:22:11	XGigabitEthernet2	0	20	
	7	32768	32768 EC:8E:C4:0D:22:11	32768_EC:8E:C4:0D:22:11	XGigabitEthernet2	0	20	
		32769	32768 EC:8E:C4:0D:22:11	32768 EC-8E-C4-0D-22-11	XGigabitEthernet2	0	20	
		32769	32768 EC:8E:C4:0D:22:11	32768 EC-8E-C4-0D-22-11	XGigabitEthernet2	0	20	
0	9	32700	32708-FC.8F.C4.0D.22.11	32708-FC.8F.C4.0D.22.11	XGigabitEthemet2	0	20	
0	10	32700	32700-F0.0F:04:0D:22:11	32700-FC.0F:C4:0D:22:11	XGigabitEthemet2	0	20	
nt O	11	32768	32700-FC:0F:C4:0D:22:11	32/00-FC:0F:C4:0D:22:11	XGigabitEthernet2	0	20	
	12	32768	32768-FC:8F:C4:0D:22:11	32768-FC:8F:C4:0D:22:11	XGigabitEthernet2	0	20	
0	) 13	32768	32768-FC:8F:C4:0D:22:11	32768-FC:8F:C4:0D:22:11	XGigabitEthernet2	0	20	
0	14	32768	32768-FC:8F:C4:0D:22:11	32768-FC:8F:C4:0D:22:11	XGigabitEthernet2	0	20	
0	15	32768	32768-FC:8F:C4:0D:22:11	32768-FC:8F:C4:0D:22:11	XGigabitEthernet2	0	20	

#### Edit MST Instance

MSTI	1
VLAN	Available VLAN Selected VLAN
Priority	32768 (0 - 61440, default 32768)
Bridge Identifiter	32768-FC:8F:C4:0D:22:11
Designated Root Bridge	32768-FC:8F:C4:0D:22:11
Root Port	XGigabitEthernet2
Root Path Cost	0
Remaining Hop	20

Field	Description
Available VLAN /	The list of VLANs mapped to the MSTI. A VLAN can only be mapped
Selected VLAN	to one MSTI. An unused MSTI should just be left empty.
	Controls the bridge priority. Lower numeric values have better priority.
Priority	The bridge priority plus the MSTI instance number, concatenated with
_	the 6-byte MAC address of the switch forms a Bridge Identifier.

# 8.4 MST Port Setting

#### Click Spanning Tree > MST Port Setting

This page displays the current MSTI configuration information for the Switch. If a loop occurs, the MSTP function will use the port priority to select an interface to put into the forwarding state. Set a higher priority value for ports you wish to be selected for forwarding first. In instances where the priority value is identical, the MSTP function will implement the lowest MAC address into the forwarding state and other interfaces will be blocked. Note that a lower priority values mean higher priorities for forwarding packets.

	Spanning Tree )) MST Port Setting												
<ul> <li>Status</li> </ul>													
<ul> <li>Network</li> </ul>	MS	T Port	Setting T	able									
• Port	MS		1										
✓ VLAN     ✓	1110	10.1											
<ul> <li>MAC Address Table</li> </ul>	_											q	
✓ Spanning Tree		Entry	Port	Path Cost	Priority	Port Role	Port State	Mode	Туре	Designated Bridge	Designated Port ID	Designated Cost	Remaining Hop
Property		1	10GE1	20000	128	Designated	Forwarding	RSTP	Boundary	32768-FC:8F:C4:0D:22:11	128-1	20000	20
Port Setting		2	10GE2	20000	128	Root	Forwarding	RSTP	Boundary	32768-00:0F:C9:12:34:56	128-2	20000	20
MST Instance		3	10GE3	2000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-3	2000	20
MST Port Setting Statistics		4	10GE4	20000	128	Designated	Forwarding	RSTP	Boundary	32768-FC:8F:C4:0D:22:11	128-4	20000	20
Discovery		5	10GE5	2000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-5	2000	20
Multicast		6	10GE6	2000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-6	2000	20
<ul> <li>Security</li> </ul>		7	10GE7	2000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-7	2000	20
✓ ACL		8	10GE8	2000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-8	2000	20
		9	10GE9	2000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-9	2000	20
<ul> <li>Diagnostics</li> </ul>		10	10GE10	2000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-10	2000	20
<ul> <li>Management</li> </ul>		11	10GE11	2000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-11	2000	20
		12	10GE12	2000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-12	2000	20
		13	LAG1	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-13	20000	20
		14	LAG2	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-14	20000	20
		15	LAG3	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-15	20000	20
		16	LAG4	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-16	20000	20
		17	LAG5	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-17	20000	20
		18	LAG6	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-18	20000	20
		19	LAG7	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-19	20000	20
		20	LAG8	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-20	20000	20
		E 49	٦ ٦										

#### Edit MST Port Setting

MSTI	0
Port	10GE1
Path Cost	<b>0</b> (0 - 20000000) (0 = Auto)
Priority	128 ~
Port Role	Designated
Port State	Forwarding
Mode	RSTP
Туре	Boundary
Designated Bridge	32768-FC:8F:C4:0D:22:11
Designated Port ID	128-1
Designated Cost	20000
Remaining Hop	20

Field	Description
Path Cost	Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802 1D recommended values. Using the specific setting, a user-
	defined value can be entered. The path cost is used when establishing

	the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range 1 to 200000000.					
Priority	Controls the port priority. This can be used to control priority of ports having identical port cost.					
Port Role	Each MST bridge port that is enabled is assigned a Port Role for each spanning tree. The Port Role is one of the following values: Root, Designated, Alternate, Backup, Master, or Disabled.					
	Indicates the current STP state of a port. If enabled, the Port State determines what forwarding action is taken regarding traffic. The possible port states are:					
	•Disabled: STP is disabled on the port. The port forwards traffic while					
	learning MAC addresses.					
	•Blocking: The port is blocked and cannot be used to forward traffic					
Port Status	or learn MAC addresses.					
	•Listening: The port is in listening mode. The port cannot forward					
	traffic or learn MAC addresses in this state.					
	•Learning: The port is in learning mode. The port cannot forward					
	traffic. However, it can learn new MAC addresses.					
	•Forwarding: The port is in forwarding mode. The port can forward					
	traffic and learn new MAC addresses in this state					
Mode	The STP mode: Disabled, STP, RSTP or MSTP.					
Туре	The current type of the port.					
Designated Bridge	Displays the Bridge Identifier of the bridge for the Designated Port. It is made up using the bridge priority and the base MAC address of the bridge.					
Designated Port ID	Display the Port ID. It is made up using the priority and the port number.					
Designated Cost	Displays the operation cost of the path from this bridge to the Root Bridge.					
Remaining Hop	The remaining hop number.					

## 8.5 Statistics

Click Spanning Tree > Statistics

To display STP statistics

**Bridge Protocol Data Units (BPDUs)** are frames that contain information about the **Spanning tree protocol (STP)**. Switches send BPDUs using a unique MAC address from its origin port and a multicast address as destination MAC (01:80:C2:00:00:00, or 01:00:0C:CC:CC:CD for Per VLAN Spanning Tree). For STP algorithms to function, the switches need to share information about themselves and their connections. What they share are bridge protocol data units (BPDUs). BPDUs are sent out as multicast frames to which only other layer 2 switches or bridges are listening. If any loops (multiple possible paths between switches) are found in the network topology, the switches will co-operate to disable a port or ports to ensure that there are no loops; that is, from one device to any other device in the layer 2 network, only one path can be taken.

# Status Network Port VLAN MAC Address Table Spanning Tree Property Port Setting MST Instance MST Instance MST Port Setting Statistics Discovery Multicast Security ACL QoS Diagnostics Management

#### Spanning Tree >> Statistics

#### **Statistics Table**

Refresh Rate 0 v sec

_	E natura e	Dent	Rec	eive BF	טסי	Transmit BPDU		
Ч	Entry	Port	Config	TCN	MSTP	Config	TCN	MSTP
	1	10GE1	0	0	0	0	0	6164
	2	10GE2	0	0	31913	0	0	8
	3	10GE3	0	0	0	0	0	0
	4	10GE4	0	0	0	0	0	31928
	5	10GE5	0	0	0	0	0	0
	6	10GE6	0	0	0	0	0	0
	7	10GE7	0	0	0	0	0	0
	8	10GE8	0	0	0	0	0	0
	9	10GE9	0	0	0	0	0	0
	10	10GE10	0	0	0	0	0	0
	11	10GE11	0	0	0	0	0	0
	12	10GE12	0	0	0	0	0	0
	13	LAG1	0	0	0	0	0	0
	14	LAG2	0	0	0	0	0	0
	15	LAG3	0	0	0	0	0	0
	16	LAG4	0	0	0	0	0	0
	17	LAG5	0	0	0	0	0	0
	18	LAG6	0	0	0	0	0	0
	19	LAG7	0	0	0	0	0	0
	20	LAG8	0	0	0	0	0	0

Clear Refresh View

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

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

# Chapter 9 Discovery

## 9.1 LLDP

The **Link Layer Discovery Protocol (LLDP)** is a vendor-neutral link layer protocol in the Internet Protocol Suite used by network devices for advertising their identity, capabilities, and neighbors on an IEEE 802 local area network, principally wired Ethernet. The LLDP is a one-way protocol; there are no request/response sequences. Information is advertised by stations implementing the transmit function, and is received and processed by stations implementing the receive function. The LLDP category contains LLDP and LLDP-MED pages.

## 9.1.1 Property

#### Click **Discovery** > **LLDP** > **Property**

To display LLDP Property Setting web page.

	Discovery >> LLDP >> F	Property							
	~								
<ul> <li>Network</li> </ul>	LLDP								
✓ Port	State	Enable							
VLAN									
<ul> <li>MAC Address Table</li> </ul>	LLDP Handling	O Bridging							
<ul> <li>Spanning Tree</li> </ul>		<ul> <li>Flooding</li> </ul>							
- Discovery	TI V Advertise Interval	30	Sec (5 32767 default 30)						
A LLDP.		20	366 (3 - 32707, deladit 30)						
Property	Hold Multiplier	4	(2 - 10, default 4)						
Port Setting MED Network Policy	Reinitializing Delay	2	Sec (1 - 10, default 2)						
MED Port Setting	remaining bondy	n <mark>duononononon</mark>							
Packet View	Transmit Delay	2	Sec (1 - 8191, default 2)						
Local Information									
Neighbor	LLDP-MED								
Statistics	Fast Start Repeat Count	3	(1 - 10, default 3)						
Multicast									
<ul> <li>Security</li> </ul>	Apply								
* ACL									
Field	Description								
State	Enable/Disable LLD	P protocol	on this switch						
LLDP Handling	Select LLDP PDU ha when LLDP is globa <b>Filtering</b> : Deletes th <b>Bridging</b> : (VLAN-av members. <b>Flooding</b> : Forwards	andling ac Ily disable le packet. vare floodi	tion to be filtered, bridging or flooded d. ng) Forwards the packet to all VLAN et to all ports.						
TLV Advertise Interval	Select the interval at seconds, and the va	t which fra Ilid range i	mes are transmitted. The default is 30 s 5~32767 seconds.	)					
Holdtime Multiplier	Select the multiplier 2~10, default=4).	on the tra	nsmit interval to assign to TTL (range						
Reinitialization Delay	Select the delay before default=2).	ore a re-in	itialization (range 1~10 seconds,						
Transmit Delay	Select the delay after default=3).	er an LLDF	P frame is sent (range 1~8191 second	s,					
Fast Start Repeat Count	Specifies the repeat	count valu	ue (range 1~10, default=3).						

## 9.1.2 Port Setting

#### Click **Discovery > LLDP > Port Setting**

To display LLDP Port Setting.

	Disco	very	>> LLDI	P እ Po	ort Setting		
✓ Status	Der	Cattin	a Tabla				
✓ Network	Pon	Settin	ig lable				
✓ Port						0	
VLAN						 ч	
<ul> <li>MAC Address Table</li> </ul>		Entry	Port	Mode	Selected TLV		
✓ Spanning Tree		1	10GE1	Normal	802.1 PVID		
✓ Discovery		2	10GE2	Normal	802.1 PVID		
∧ LLDP		3	10GE3	Normal	802.1 PVID		
Property		4	10GE4	Normal	802.1 PVID		
Port Setting		5	10GE5	Normal	802.1 PVID		
MED Network Policy		6	10GE6	Normal	802.1 PVID		
Packet View		7	10GE7	Normal	802.1 PVID		
Local Information		8	10GE8	Normal	802.1 PVID		
Neighbor		9	10GE9	Normal	802.1 PVID		
Statistics		10	10GE10	Normal	802.1 PVID		
✓ Multicast		11	10GE11	Normal	802.1 PVID		
✓ Security		12	10GE12	Normal	802.1 PVID		
✓ ACL			-				
✓ QoS		Edit					

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

Port	10GE1		
Mode	<ul> <li>Transmit</li> <li>Receive</li> <li>Normal</li> <li>Disable</li> </ul>		
	Available TLV	Selected TL	v
Optional TLV	System Name		
	System Capabilities 802.3 MAC-PHY	<b>、</b> <	Ŷ
	Available VLAN	Selected VL	AN
02.1 VLAN Name	VLAN 1 VLAN 100		^
		<b>、</b>	~

Field	Description						
Port	Select specified port or all ports to configure LLDP state.						
	Select the transmission state of LLDP port interface.						
	Transmit: Transmit LLDP PDUs only.						
Mode	Receive: Receive LLDP PDUs only.						
	Normal: Transmit and receive LLDP PDUs both.						
	<b>Disable</b> : Disable the transmission of LLDP PDUs.						
	Select the LLDP optional TLVs to be carried (multiple selection is						
Optional TLV	allowed).						
	Port Description						

	System Name
	System Description
	System Capabilities
	802.3 MAC-PHY
	802.3 Link Aggregation
	802.3 Maximum Frame Size
	Management IP Address
	802.1 PVID
802.1 VLAN Name	Select the VLAN Name ID to be carried (multiple selection is allowed)

## 9.1.3 MED Network Policy

#### Click Discovery > LLDP > MED Network Policy

LLDP Media Endpoint Discovery (LLDP MED) is an extension to LLDP. This protocol enables advanced LLDP features in a Voice over IP (VoIP) network. Whereas LLDP enables network discovery between Network Connectivity devices, LLDP-MED enables network discovery between Network Connectivity devices and media Endpoints such as, IP telephones, softphones, VoIP gateways and conference bridges.

Discovery >> LLDP >> MED Network Policy						
✓ Status						
<ul> <li>Network</li> </ul>	MED Network Deliev Table					
✤ Port						
VLAN	Showing All v entries Showing 0 to 0 of 0 entries					
<ul> <li>MAC Address Table</li> </ul>						
<ul> <li>Spanning Tree</li> </ul>	Policy ID         Application         VLAN         VLAN Tag         Priority         DSCP					
✓ Discovery	0 results found.					
∧ LLDP	Add Edit Delete First Previous 1 Next Last					
Property						
Port Setting						
MED Network Policy						
MED Port Setting						

Check "**Enable**" and press "**Apply**" to use "MED Network Policy Voice Auto Mode". Click "**Add**" or "**Edit**" button to add or edit a policy.

Policy ID	1 🗸		
Application	Voice	v	
VLAN		Range (1 - 4094)	
VLAN Tag	<ul> <li>Tagged</li> <li>Untagged</li> </ul>		
Priority	0 ~		
DSCP	0 ×		

Field	Description
Policy ID	Select the number of the policy to be created.
Application	Select the type of application (type of traffic) from the list for which the network policy is being defined: <b>Voice</b>

	Voice Signaling
	Guest Voice
	Guest Voice Signaling
	Softphone Voice
	Video Conferencing
	Streaming Video
	Video Signaling
VLAN	Enter the VLAN ID to which the traffic should be sent.
VLAN Tag	Select whether the traffic is Tagged or Untagged.
Priority	Select the traffic priority applied to traffic defined by this network
FIGHTy	policy.
	Select the DSCP value to associate with application data sent by
DSCP	neighbors. This informs them how they should mark the application
	traffic that they send to the switch.

## 9.1.4 MED Port Setting

#### Click Discovery > LLDP > MED Port Setting

Use the LLDP MED Port Settings page to select the network policies, configured on the LLDP MED Network Policy page, to be advertised on the port, and select the LLDP MED TLVs to be sent inside the LLDP PDU.

Discovery >> LLDP >> MED Port Setting								
✓ Status	MEE	Dent	0	Table .				
✓ Network	MEL	Port	Setting	lable				
✓ Port								
✓ VLAN								
<ul> <li>MAC Address Table</li> </ul>		Entry	Port	State	Netw	ork Policy	Location	Inventory
<ul> <li>Spanning Tree</li> </ul>		Linay	1 on	Clute	Active	Application	Location	inventory
- Discovery		1	10GE1	Enabled	Yes		No	No
∧ LLDP		2	10GE2	Enabled	Yes		No	No
Property		3	10GE3	Enabled	Yes		No	No
Port Setting		4	10GE4	Enabled	Yes		No	No
MED Network Policy		5	10GE5	Enabled	Yes		No	No
Packet View		6	10GE6	Enabled	Yes		No	No
Local Information		7	10GE7	Enabled	Yes		No	No
Neighbor		8	10GE8	Enabled	Yes		No	No
Statistics		9	10GE9	Enabled	Yes		No	No
✓ Multicast		10	10GE10	Enabled	Yes		No	No
• Security		11	10GE11	Enabled	Yes		No	No
✓ ACL		12	10GE12	Enabled	Yes		No	No
♥ QoS	-		~					
		Edit						

Select the port and click "Edit" button to edit.

Port	10GE1				
State	Enable				
	Available TLV		S	elected TLV	
Optional TLV	Location Inventory	^	>	Network Policy	^
		~	<		~
	Available Policy		S	elected Policy	
Network policy		^			^
		~	<		~
ocation					
Coordinate				(16 pairs of hexa	decimal characters)
Civic				(6-160 pairs of he	exadecimal characters
ECS ELIN				(10-25 pairs of he	exadecimal characters

Field	Description
State	Enable or disable LLDP MED on this port.
Optional TLV	Select the TLVs that can be published by the switch, by moving them to the Selected Optional TLVs list.
Network Policy	Select the LLDP MED policies that will be published by LLDP, by moving them to the Selected Policy list. These policies were created on the LLDP MED Network Policy page.
Location	
Coordinate	Enter the coordinate location to be published by LLDP.
Civic	Enter the civic address to be published by LLDP.
ECS ELIN	Enter the Emergency Call Service (ECS) ELIN location to be published by LLDP.

## 9.1.5 Packet View

#### Click Discovery > LLDP > Packet View

To display LLDP packet information.

Discovery >>> LLDP >>> Packet View							
✓ Status	-						
<ul> <li>Network</li> </ul>	Pac	Packet View Table					
✓ Port							
✓ VLAN	-						
<ul> <li>MAC Address Table</li> </ul>		Entry	Port	In-Use (Bytes)	Available (Bytes)	Operational Status	
✓ Spanning Tree	0	1	10GE1	49	1109	Not Overloading	
- Discovery	0	2	10GE2	49	1079	Not Overloading	
∧ LLDP	0	3	10GE3	49	1049	Not Overloading	
Property	0	4	10GE4	49	1019	Not Overloading	
Port Setting	0	5	10GE5	49	989	Not Overloading	
MED Port Setting	0	6	10GE6	49	959	Not Overloading	
Packet View	0	7	10GE7	49	929	Not Overloading	
Local Information	0	8	10GE8	49	899	Not Overloading	
Neighbor	0	9	10GE9	49	869	Not Overloading	
Statistics	0	10	10GE10	50	838	Not Overloading	
	0	11	10GE11	50	808	Not Overloading	
	0	12	10GE12	50	778	Not Overloading	
			<u> </u>			-	
▼ Q05		Detail					

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

If need detail information, select the port, then click Detail.

Port	10GE1
Mandatory TLVs	
Size (Bytes)	22
Operational Status	Overloading
MED Capabilities	
Size (Bytes)	9
Operational Status	Overloading
MED Location	
Size (Bytes)	0
Operational Status	Overloading
MED Network Policy	
Size (Bytes)	10
Operational Status	Transmitted
MED Inventory	
Size (Bytes)	0
Operational Status	Overloading
MED Extended Power	r via MDI
Size (Bytes)	0
Operational Status	Transmitted
802.3 TLVs	
Size (Bytes)	0
Operational Status	Overloading
Optional TLVs	
Size (Bytes)	0
Operational Status	Overloading
802.1 TLVs	
Size (Bytes)	8
Operational Status	Overloading
Total	
In-Use (Bytes)	49
Available (Bytes)	-79

Field	Description
Port	Port Name
Mandatan, TLVa	Total mandatory TLV byte size.
	Status is sent or overloading.
802 3 TI Ve	Total 802.3 TLVs byte size.
802.3 TEVS	Status is sent or overloading.
Optional TLVs	Total Optional TLV byte size.
	Status is sent or overloading.
802 1 TI Ve	Total 802.1 TLVs byte size.
802.1 ILVS	Status is sent or overloading.
Total	Total number of bytes of LLDP information in each packet.

## 9.1.6 Local Information

#### Click **Discovery** > **LLDP** > **Local Information**

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

	Discovery >> LLDP >> Local Information				
<ul><li>✓ Status</li><li>✓ Network</li></ul>	Device Summary				
✓ Port	Chaesis ID Subturns MAC address				
VLAN					
MAC Address Table     Spapping Tree	Suctan Nama Switch				
Discovery	System Description All SC0312 10G				
LLDP	Superted Capabilities Prize				
Property	Supported Capabilities Dide				
Port Setting					
MED Port Setting	Port ID Subtype Local				
Packet View	Port Status Table				
Local Information Neighbor					
Statistics	Setter Part U DR State U DR MED State				
✓ Multicast	Entry Port LLDP State LLDP-MED State				
<ul> <li>Security</li> </ul>	0 2 10GE2 Normal Enabled				
✓ ACL	O 3 10GE3 Normal Enabled				
↓ Qos	0 4 10GE4 Normal Enabled				
Management	O 5 10GE5 Normal Enabled				
Wanagement	6 10GE6 Normal Enabled				
	7 10GE7 Normal Enabled				
	O 8 10GE8 Normal Enabled				
	O 9 10GE9 Normal Enabled				
	O 10 10GE10 Normal Enabled				
	O 11 10GE11 Normal Enabled				
	O 12 10GE12 Normal Enabled				
	Detail				
Field	Description				
Chassis ID Subtype	Type of chassis ID, such as the MAC address.				
	Identifier of chassis Where the chassis ID subtype is a MAC addr	ess			
Chassis ID	the MAC address of the switch is displayed.	000,			
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	The status of LLDP-MED.				

Click "Detail" button on the page to view detail information of the selected port.

## 9.1.7 Neighbor

Click Discovery > LLDP > Neighbor

Use the LLDP Neighbor page to view LLDP neighbors information.

	Discovery >> LL	)P >> Neighbor					
<ul> <li>✓ Status</li> <li>✓ Network</li> <li>✓ Port</li> </ul>	Neighbor Table						
VLAN     MAC Address Table	Showing All v entr	es	Showing 1 to 3 of 3	3 entries		Q	
<ul> <li>Spanning Tree</li> </ul>	Local Port	Chassis ID Subtype	Chassis ID	Port ID Subtype	Port ID	System Name	Time to Live
- Discovery	10GE1	MAC address	8C:16:45:37:F3:67	MAC address	8C:16:45:37:F3:67		3446
▲ LLDP	10GE2	MAC address	00:0F:C9:12:34:56	Local	gi27		115
Property	10GE4	MAC address	00:0E:C6:82:34:98	MAC address	00:0E:C6:82:34:98		2881
Port Setting MED Network Policy MED Port Setting Packet View Local Information Neighbor Statistics	Clear Re	resh Detail				First Previ	us 1 Next Last

Field	Description					
Local Port	Number of the local port to which the neighbor is connected.					
Chassis ID Subtype	Type of chassis ID (for example, MAC address)					
Chassis ID	Identifier of the 802 LAN neighboring device's chassis.					
Port ID Subtype	Type of the port identifier that is shown.					
Port ID	Identifier of port.					
System Name	Published name of the switch.					
Time to Live	Time interval in seconds after which the information for this neighbor is deleted.					

Click "Detail" to view selected neighbor detail information.

#### 9.1.8 Statistics

#### Click Discovery > LLDP > Statistics

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

۵	)isco	very	>> LLDI	> >> Statistic	s					
<ul> <li>Status</li> </ul>										
<ul> <li>Network</li> </ul>	Glo	oal Sta	tistics							
• Port										
VLAN		Insertio	<b>ns</b> 19							
MAC Address Table		Deletio	<b>ns</b> 16							
<ul> <li>Spanning Tree</li> </ul>		Dro	<b>ps</b> 0							
- Discovery		AgeOu	its 0							
▲ LLDP	· · · · · ·									
Property	0	Clear	Refree	sh						
Port Setting										
MED Network Policy	Stat	istics	lable							
Packet View	_									
Local Information		Entra	Bort	Transmit Frame Receive Frame		Receive TLV		Neighbor		
Neighbor		Entry	Port	Total	Total	Discard	Error	Discard	Unrecognized	Timeout
Statistics		1	10GE1	27642	914	2	0	0	0	0
<ul> <li>Multicast</li> </ul>		2	10GE2	31385	31374	0	0	0	0	0
✤ Security		3	10GE3	0	0	0	0	0	0	0
• ACL		4	10GE4	9397	365	4	0	0	0	0
v QoS		5	10GE5	0	0	0	0	0	0	0
<ul> <li>Diagnostics</li> </ul>		6	10GE6	0	0	0	0	0	0	0
<ul> <li>Management</li> </ul>	H	7	10GE7	0	0	0	0	0	0	0
		, 8	10058	0	0	0	0	0	0	0
		0	10050	0	0	0	0	0	0	0
		9	10029	0	0	0	0	0	0	0
		10	10GE10	0	0	0	0	0	0	0
		11	10GE11	0	0	0	0	0	0	0
		12	10GE12	0	0	0	0	0	0	0
		Clear	Refre	sh						

Field	Description
Insertions	The number of times the complete set of information advertised by a particular MAC Service Access Point (MSAP) has been inserted into tables associated with the remote systems.
Deletions	The number of times the complete set of information advertised by MSAP has been deleted from tables associated with the remote systems.
Drops	The number of times the complete set of information advertised by MSAP could not be entered into tables associated with the remote systems because of insufficient resources.
Age Outs	The number of times the complete set of information advertised by MSAP has been deleted from tables associated with the remote system because the information timeliness interval has expired.
Port	Interface or port number.
Transmit Frame Total	Number of LLDP frames transmitted on the corresponding port.
Receive Frame Total	Number of LLDP frames received by this LLDP agent on the corresponding port, while the LLDP agent is enabled.
Receive Frame Discard	Number of LLDP frames discarded for any reason by the LLDP agent on the corresponding port.
Receive Frame Error	Number of invalid LLDP frames received by the LLDP agent on the corresponding port, while the LLDP agent is enabled.
Receive TLV Discard	Number of TLVs of LLDP frames discarded for any reason by the LLDP agent on the corresponding port.
Receive TLV	Number of TLVs of LLDP frames that are unrecognized while the
Unrecognized	LLDP agent is enabled.
Neighbor Timeout	Number of age out LLDP frames.

# Chapter 10 Multicast

## 10.1 General

Use the General pages to configure setting of IGMP snooping property and group and router setting function.

## 10.1.1 Property

#### Click Multicast > General > Property

This page allows user to set multicast forwarding method and unknown multicast action.

		Multicast >> General >> Property			
	<ul> <li>Status</li> </ul>				
	<ul> <li>Network</li> </ul>				
	✓ Port	Unknown Multicast			
	✓ VLAN	Action Forward to Router Port			
	<ul> <li>MAC Address Table</li> </ul>				
	<ul> <li>Spanning Tree</li> </ul>	Multicast Forward Method			
	<ul> <li>Discovery</li> </ul>	IPv4 O DMAC-VID			
	<ul> <li>Multicast</li> </ul>	O DIP-VID			
	General	Anniv			
	Property Group Address	Арру			
	Router Port				
	Forward All				
	Throttling				
	Filtering Profile				
	Filtering Binding				
Field		Description			
		Set the unknown multicast action			
Unknown	Multicast	<b>Drop</b> : drop the unknown multicast data.			
Action		Flood flood the unknown multicast data			
,		Deuter next ferward the unknown multicest date to reviter next			
		<b>Router port</b> : forward the unknown multicast data to router			
		Set the IPv4 multicast forward method.			
IPv4		MAC-VID: forward method dmac+vid.			
		DIP VID: forward method din+vid			
<b>DIP-VID</b> : Iorward method dip+vid.					

## 10.1.2 Group Address

#### Click Multicast > General > Group Address

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

Multicast >> General >> Group Address						
✓ Status						
<ul> <li>Network</li> </ul>	Crown Address Table					
✓ Port	Group Address Table					
▼ VLAN	Showing All v entries Showing 0 to 0 of 0 entries	0				
<ul> <li>MAC Address Table</li> </ul>		4				
<ul> <li>Spanning Tree</li> </ul>	VLAN Group Address Member Type Life (Sec)					
<ul> <li>Discovery</li> </ul>	0 results found.					
✓ Multicast		First Previous 1 Next Last				
→ General	Add Edit Delete Refresh					
Property						
Group Address						
Router Port						
Forward All						
Throttling						
Filtering Profile						
Filtering Binding						

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

#### Click "Add/Edit" to add/edit Group Address.

VLAN	1 ~	
Group Address		
Member	Available Port Selected Port	

Field	Description
VLAN	The VLAN ID of group.
Group Address	The group IP address.
	The member ports of group.
Member	Available Port: Optional port member
	Selected Port: Selected port member

## 10.1.3 Router Port

#### Click Multicast > General > Router Port

A Multicast router (Mrouter) port is a port that connects to a Multicast router. The switch includes the Mrouter port(s) when it forwards Multicast streams and IGMP/ MLD registration messages. It is required in order for all Mrouters can, in turn, forward the Multicast streams and propagate the registration messages to other subnets.

Use the Multicast Router Port page to statically configure or see dynamically detected ports connected to Mrouters.

Multicast >> General >> Router Port							
✓ Status							
<ul> <li>Network</li> </ul>	Deuter Deut Tehle						
✤ Port	Router Port Table						
VLAN	IP Version IPv4 V						
<ul> <li>MAC Address Table</li> </ul>							
<ul> <li>Spanning Tree</li> </ul>	Showing All v entries Showing 0 to 0 of 0 entries	Q					
• Discovery	VLAN Member Static Port Forbidden Port Life (Sec)						
✓ Multicast	O results found						
▲ General		First Deviews ( Next Lest					
Property		First Previous 1 Next Last					
Group Address	Add Edit Refresh						
Router Port							
Forward All							
Throttling							
Filtering Profile							
Filtering Binding							

Click "Add/Edit" to add/edit Router Port.

1							
1	•						
100			^				
	>						
	<						
	<u> </u>		~				
· · · · ·	•	,					
IPv4 v							
Statio							
<ul> <li>Static</li> <li>Forbidden</li> </ul>							
Available Port		Selected P	Port				
10051	T						
10GE1 P			^				
10GE3							
10GE4							
10GE5							
10GE6	<						
10GE7							
	<ul> <li>IPv4 </li> <li>Static</li> <li>Forbidden</li> <li>Available Port</li> <li>10GE1</li> <li>10GE3</li> <li>10GE4</li> <li>10GE5</li> <li>10GE6</li> <li>10GE7</li> </ul>	IPv4 ~ Static Forbidden Available Port 10GE1 10GE2 10GE3 10GE4 10GE5 10GE6 10GE6 10GE7	IPv4 ~ Static Forbidden Available Port 10GE1 10GE2 10GE3 10GE4 10GE5 10GE6 10GF7	IPv4 v Static Forbidden Available Port 10GE1 10GE2 10GE3 10GE4 10GE5 10GE6 10GE7	IPv4 v Static Forbidden Available Port 10GE1 10GE2 10GE3 10GE4 10GE5 10GE6 10GE6 10GE7	IPv4 V Static Forbidden Available Port Selected Port 10GE1 10GE2 10GE3 10GE5 10GE6 10GE6 10GE7	IPv4 ~ Static Forbidden Available Port Selected Port 10GE1 10GE2 10GE5 10GE5 10GE5 10GE6

Field	Description
VLAN	Select the VLAN ID for the router ports
IP Version	IPv4 or IPv6
Туре	For each interface, select its association type. The options are: <b>Static</b> : The port is statically configured as a Multicast router port. <b>Forbidden</b> : This port is not to be configured as a Multicast router port, even if IGMP or MLD queries are received on this port.
Port	Select the port(s) for the router ports

#### 10.1.4 Forward All

#### Click Multicast > General > Forward ALL

Use the Forward All page to configure the ports or LAGs to receive Multicast streams from a specific VLAN. You can statically configure a port to Forward All if the devices connecting to the port do not support IGMP or MLD.

Multicast >> General >> Forward All					
✓ Status					
<ul> <li>Network</li> </ul>	Ferryard All Table				
✓ Port	Forward All Table				
VLAN	Showing All v entries Showing 0 to 0 of 0 entries	0			
<ul> <li>MAC Address Table</li> </ul>		4			
<ul> <li>Spanning Tree</li> </ul>	ULAN Static Port Forbidden Port				
✤ Discovery	0 results found.				
✓ Multicast		First Previous 1 Next Last			
▲ General					
Property					
Group Address					
Router Port					
Forward All					
Throttling					
Filtering Profile					
Filtering Binding					

Click "Add/Edit" to add/edit Forward ALL table.

VLAN	Available VLAN	Selected VLAN
IP Version	V	
Туре	<ul> <li>Static</li> <li>Forbidden</li> </ul>	
Port	Available Port           10GE1           10GE2           10GE3           10GE4           10GE5           10GE6           10GE7           10GE8	Selected Port

Apply Close

Field	Description
VLAN	Select the VLAN ID.
IP Version	IPv4 or IPv6
Туре	Select the interface that is to be defined as Forward All by using the following methods: <b>Static</b> : The port receives all registered Multicast streams. <b>Forbidden</b> : The port cannot receive any registered Multicast streams, even if IGMP/MLD snooping designated the port to join a Multicast group.
Port	Select the port(s) for the Forward ALL.

## 10.1.5 Throttling

#### Click Multicast > General > Throttling

Use the Throttling page to configure the maximum number of Multicast groups that are allowed on each interface and specify the action when the limit reaches.

	Multio	cast )	Gene	ral 💙 Thre	ottling	
Status	_					
Network	Thro	ottling	Table			
Port						
VLAN	_					Q
MAC Address Table		Entry	Port	Max Group	Exceed Action	
Spanning Tree		1	10GE1	256	Deny	
Discovery		2	10GE2	256	Deny	
Multicast		3	10GE3	256	Deny	
<ul> <li>General</li> </ul>		4	10GE4	256	Deny	
Property		5	10GE5	256	Deny	
Group Address Pouter Port		6	10GE6	256	Deny	
Forward All		7	10GE7	256	Deny	
Throttling		8	10GE8	256	Deny	
Filtering Profile		9	10GE9	256	Denv	
Filtering Binding		10	10GE10	256	Denv	
IGMP Snooping     MLD Spooping		11	10GE11	256	Denv	
<ul> <li>MED Shooping</li> <li>MVR</li> </ul>		12	10GE12	256	Deny	
Security		13	LAG1	256	Deny	
ACL		14	LAG2	256	Deny	
QoS		15	LAG3	256	Deny	
Diagnostics		16	LAGA	256	Deny	
Management		17	LAG5	256	Deny	
		10	LAGE	200	Deny	
		10	LAGO	200	Deny	
		19	LAGI	206	Deny	
		20	LAG8	256	Deny	

Select port and click "Edit" to edit Throttling.

Port	10GE1		
Max Group	256	(0 - 256)	
Exceed Action	<ul> <li>Deny</li> <li>Replace</li> </ul>		

Field	Description
Max Group	Enter the maximum number of IGMP groups that are allowed on the interface.
Exceed Action	<b>Deny</b> or <b>Replace</b> the existing group with the new group for which the IGMP report was received when the limit is reached.

## 10.1.6 Filtering Protocol

#### Click Multicast > General > Filtering Protocol

A Multicast filter profile permits or denies a range of Multicast groups to be learned when the join group matches the filter profile IP group range.

Multicast >> General >> Filtering Profile					
✓ Status					
<ul> <li>Network</li> </ul>	Elferies Berfle Table				
✓ Port	Filtering Profile Table				
✓ VLAN	Showing All v entries Showing 0 to 0 of 0 entries				
<ul> <li>MAC Address Table</li> </ul>					
<ul> <li>Spanning Tree</li> </ul>	Profile ID Start Address End Address Action				
✤ Discovery	0 results found.				
✓ Multicast	First Previous 1 Nex	kt Last			
▲ General					
Property					
Group Address					
Router Port					
Forward All					
Throttling					
Filtering Profile					
Filtering Binding					

Click "Add/Edit" to add/edit a filtering profile.

Profile ID		(1 - 128)	
Start Address			
End Address			
Action	Allow		

Field	Description
Profile ID	Enter the sequence number for the profile.
IP Version	Select ether IPv4 or IPv6 to apply the filter profile to IPv4 or IPv6
	Multicast traffic.
Start Address Enter the starting Multicast group address.	
End Address	Enter the ending Multicast group address.
Action	Allow or Deny Multicast frames when the join group matches the
	profile IP group range.

## 10.1.7 Filtering Binding

#### Click Multicast > General > Filtering Binding

To assign a Multicast filter profile to an interface to deny or permit the Multicast group when the join group matches the filter profile
	Multica	ast )> G	eneral ))	Filtering Bi	nding			
<ul> <li>Status</li> </ul>	Filter	ing Bind	ing Table					
<ul> <li>Network</li> </ul>		ing bind	ing indic					
<ul> <li>Port</li> </ul>							0	
VLAN						 	 ~	
<ul> <li>MAC Address Table</li> </ul>		Entry	Port	Profile ID				
<ul> <li>Spanning Tree</li> </ul>		1	10GE1					
<ul> <li>Discovery</li> </ul>		2	10GE2					
🗕 Multicast		3	10GE3					
- General		4	10GE4					
Property		5	10GE5					
Group Address		6	10GE6					
Router Port		7	10GE7					
Forward All Throttling		8	10GE8					
Filtering Profile		9	10GE9					
Filtering Binding		10	10GE10					
<ul> <li>IGMP Snooping</li> </ul>		11	10GE11					
<ul> <li>MLD Snooping</li> </ul>		12	10GE12					
MVR		13	LAG1					
<ul> <li>Security</li> </ul>		14	LAG2					
• ACL		14	LAC2					
▼ QoS		15	LAGS					
<ul> <li>Diagnostics</li> </ul>		16	LAG4					
Management		17	LAGS					
		18	LAG6					
		19	LAG7					
		20	LAG8					
	E	lit						

Select port and click "Edit" to assign Filter profile.

Port	10GE1
B	Enable
Profile ID	v

Field	Description
Profile ID	Check Enable and select filter profile.

# 10.2 IGMP Snooping

Use the IGMP Snooping pages to configure setting of IGMP snooping function

# 10.2.1 Property

#### Click Multicast > IGMP Snooping > Property

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

I	Multica	st ))	IGMP Snoop	ing )〉Pro	perty					
	Ri App	eport Su bly Settin	State Version Version Ppression I Er	nable MPv2 MPv3 nable						
<ul> <li>MLD Snooping</li> <li>MVR</li> </ul>	<b>     </b>	/LAN (	Operational Status	Router Port Auto Learn	Query Robustness	Query Interval	Query Max Response Interval	Last Member Query Counter	Last Member Query Interval	Immediate Leave
✓ Security		1	Disabled	Enabled	2	125	10	2	1	Disabled
✓ ACL		100	Disabled	Enabled	2	125	10	2	1	Disabled
<ul> <li>Diagnostics</li> </ul>	Ed	it								
Field		De	escription	า						
State		Se Er Sr	et the ena <b>1able</b> : If C 10oping.	bling st Checked	atus of d Enable	IGMF e IGN	? Snooping 1P Snoopir	function ng, else is	ality s Disable	ed IGMP
Version		Se IG IG	et the IGN MPv2: Or MPv3: St	IP Snoo nly supp upport v	oping ve port pro /3 basic	ersion cess and	IGMP v2 p v2.	oacket.		
Report Suppression	on	Se Er els	et the ena <b>1able</b> : If C se Disable	bling st Checkeo e the re	atus of d Enable port sup	IGMF e IGN opres	9 v2 report 1P Snoopir sion functio	suppress ng v2 rep on.	sion. ort supp	ression,
VLAN		Th	ne IGMP e	entry VL	AN ID.					
<b>Operation Status</b>		Th	ne enable	status	of IGMF	o Sno	oping VLA	N functio	nality.	
Router Port Auto Learn		Th	ne enablin	g statu	s of IGN	/IP Sr	nooping ro	uter port	auto lear	ning
Query Robustness	S	Th as	ne Query l subnet.	Robusti	ness all	ows t	uning for tl	ne expec	ted pack	et lose on
Query Interval		Th	ne interval	of que	ry to se	nd ge	eneral quer	у.		
Query Max Respo	nse	In	Members	hip Qu	ery Mes	sage	s, it specifi	ies the m	aximum	allowed
Interval		tin	ne before	sending	g a resp	ondii	ng report ir	n units of	1/10 sec	cond.
Last Member Que	ry	Th	ne count t	nat Que	erier-sw	itch s	ends Grou	p-Specifi	ic Querie	s when it
count		re	ceives <u>a</u> L	eave C	Group m	<u>essa</u>	ge for a gr	oup.		
Last Member Que	ry	Th	ne interval	that Q	uerier-s	witch	sends Gro	oup-Spec	ific Quer	ies when it
Interval	-	re	<u>ceive</u> s a L	eave C	Broup m	essa	ge for a gr	oup.		
Immediate Leave		Th re	ne immedi ceive IGN	ate lea IP Leav	ve statu /e mess	s of t age.	he group v	vill imme	diate lea	ve when

Click "Edit" to edit VLAN Setting.

|--|

VLAN	100	
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)	

Apply Close

Field	Description
VLAN	The selected VLAN List
State	Set the enabling status of IGMP Snooping VLAN functionality <b>Enable</b> : If Checked Enable IGMP Snooping router VLAN, else is Disabled IGMP Snooping VLAN.
Router Port Auto Learn	Set the enabling status of IGMP Snooping router port learning. <b>Enable</b> : 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. <b>Enable</b> : 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**

Field	Description
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.

## 10.2.2 Querier

### Click Multicast > IGMP Snooping > Querier

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

		Multic	ast ))	IGMP	Snooping )> Q	uerier			
<ul><li>Status</li><li>Network</li></ul>	_								
<ul><li>✓ Port</li><li>✓ VLAN</li></ul>		Quei	rier la	DIE				<u> </u>	
<ul> <li>MAC Address Table</li> <li>Spanning Tree</li> </ul>			VLAN	State	Operational Status	Version	Querier Address		-
<ul> <li>Discovery</li> <li>Multicast</li> </ul>			1 100	Disabled Disabled	Disabled Disabled			•	
General     IGMP Snooping     Property     Querier     Statistics     MLD Snooping     MVR			dit	)					
	Desc	ripti	on						

Field	Description
VLAN	IGMP Snooping querier entry VLAN ID.
State	The IGMP Snooping querier Admin State.
<b>Operational Status</b>	The IGMP Snooping querier operational status.
Querier Version	The IGMP Snooping querier operational version.
Querier IP	The operational querier IP address on the VLAN.

Click "Edit" to edit IGMP Snooping Querier.

#### Edit Querier

VLAN	100
State	Enable
Version	<ul> <li>IGMPv2</li> <li>IGMPv3</li> </ul>

Field	Description
VLAN	The selected Edit IGMP Snooping querier VLAN list.
State	Set the enabling status of IGMP Querier Election on the chose VLANs. <b>Enabled</b> : 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)

## 10.2.3 Statistics

### Click Multicast > IGMP Snooping > Statistics

This page allows user to display IGMP Snooping Statistics and clear IGMP Snooping statistics.

atus		
etwork	Receive Packet	
	Total	7059
AC Address Table	Valid	143
anning Tree	InValid	6916
covery	Other	0
lticast	Leave	0
Seneral	Report	0
Property	General Query	0
Querier	Special Group Query	0
Statistics	Source-specific Group Query	0
MVR		
curity	Transmit Packet	
L	Leave	0
S	Report	0
gnostics	General Query	0
nagement	Special Group Query	0
	Source-specific Group Query	0

#### **Receive Packet**

Field	Description
Total	Total RX IGMP packet, include IPv4 multicast data to CPU.
Valid	The valid IGMP Snooping process packet.
InValid	The invalid IGMP Snooping process packet.
Other	The ICMP protocol is not 2, and is not IPv4 multicast data packet.
Leave	IGMP leave packet.
Report	IGMP join and report packet.
General Query	IGMP general query packet
Special Group Query	IGMP special group general query packet
Source-specific Group Query	IGMP special source and group general query packet

#### **Transmit Packet**

Field	Description
Leave	IGMP leave packet
Report	IGMP join and report packet
General Query	IGMP general query packet includes 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.

# 10.3 MLD Snooping

Multicast Listener Discovery (MLD) Snooping operates on the IPv6 traffic level for discovering

multicast listeners on a directly attached port and performs a similar function to IGMP Snooping for IPv4. MLD snooping allows the Switch to examine MLD packets and make forwarding decisions based on content. MLD Snooping limits IPv6 multicast traffic by dynamically configuring the Switch port so that multicast traffic is forwarded only to those ports that wish to receive it. This reduces the flooding of IPv6 multicast packets in the specified VLANs. Both IGMP and MLD Snooping can be active at the same time

### 10.3.1 Property

#### Click Multicast > MLD Snooping > Property

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

	Multi	cast ))	MLD Snoopii	ng እ Prop	erty					
<ul> <li>Network</li> </ul>			State 🗆 Er	able						
✤ Port	_									
VLAN			Version M	LDV1 LDv2						
<ul> <li>MAC Address Table</li> </ul>		Denort (	unnraasian 🗖 E							
<ul> <li>Spanning Tree</li> </ul>		Report		lable						
<ul> <li>Discovery</li> </ul>		Apply	1							
✓ Multicast		-ppiy	J							
✓ General										
<ul> <li>IGMP Snooping</li> </ul>	VLA	N Sett	ing Table							
MLD Snooping										
Property										
Statistics				Router Port	Query	Query	Query Max	Last Member	Last Member	
<ul> <li>Security</li> </ul>		VLAN	Operational Status	Auto Learn	Robustness	Interval	Response Interval	Query Counter	Query Interval	Immediate Leave
✓ ACL		1	Disabled	Enabled	2	125	10	2	1	Disabled
✓ QoS		100	Disabled	Enabled	2	125	10	2	1	Disabled
· Diagnostics										
<ul> <li>Management</li> </ul>		Edit								
			-							
Field		1	Description	n						

Field	Description
State	Check to enable MLD Snooping.
Version	Select either MLDv1 or MLDv2.
Report Suppression	Enable or disable MLD Snooping report suppression. Disabling this
	feature will forward all MLDv1 reports to Multicast routers.

Click "Edit" to edit VLAN Setting.

VLAN	100		
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)	
perational Status			
Status	Disabled		
Query Robustness	2		
Query Interval	125 (Sec)		
Query Max Response Interval	10 (Sec)		
Last Member Query Counter	2		
Last Member Query Interval	1 (Sec)		

Apply Close

Field	Description
VLAN	The selected VLAN List
State	Set the enabling status of IGMP Snooping VLAN functionality <b>Enable</b> : If checked Enable MLD Snooping router VLAN, else is Disabled MLD Snooping VLAN.
Router Port Auto Learn	Set the enabling status of MLD Snooping router port learning. <b>Enable</b> : 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. <b>Enable</b> : 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.

Field	Description
Status	Operational MLD Snooping status, must both MLD Snooping global
Status	and MLD Snooping enable the status will be enable.
Query Robustness	Operational Query Robustness.
Query Interval	Operational Query Interval.
Query Max Response Interval	Operational Query Max Response Interval.

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

### 10.3.2 Statistics

### Click Multicast > MLD Snooping > Statistics

This page allows user to display IMLD Snooping Statistics and clear MLD Snooping statistics.

ľ	Aulticast >> MLD Snooping	g >> Statistics
Status		
Network	Receive Packet	
Port	Total	0
/LAN		
IAC Address Table	Valid	U
Spanning Tree	InValid	0
Discovery	Other	0
Multicast	Leave	0
General	Report	0
IGMP Snooping	General Query	Ο
Property	Encoded Crown Owene	
Statistics	Special Group Query	U
MVR	Source-specific Group Query	0
Security	Transmit Backat	
ACL	Iransmit Packet	
QoS	Leave	0
Diagnostics	Report	0
Management	General Query	0
	Special Group Query	0
	Source-specific Group Query	0

#### **Receive Packet**

Field	Description
Total	Total RX MLD packet, include IPv6 multicast data to CPU.
Valid	The valid MLD Snooping process packet.
InValid	The invalid IMLD Snooping process packet.
Other	The ICMP protocol is not 2, and is not IPv6 multicast data packet.
Leave	MLD leave packet.
Report	MLD join and report packet.
General Query	MLD general query packet
Special Group Query	MLD special group general query packet
Source-specific Group Query	MLD special source and group general query packet

### Transmit Packet

Field	Description
Leave	MLD leave packet
Report	MLD join and report packet
General Query	MLD general query packet includes querier transmit general query packet.
Special Group Query	MLD special group query packet include querier transmit special group query packet.

# 10.4 MVR

### 10.4.1 Property

### Click Multicast > MVR > Property

Multicast VLAN Registration (MVR) allows multicast traffic to be dedicated to a specific VLAN across a multicast domain so that receivers in other VLANs can join the sources in the dedicated VLAN and received multicast traffic.

And and the last test to the last test to a last to a last to a						
ole mode. MVR						
s In <b>Dynamic</b> mode						
o. In <b>Dynamic</b> mode						
het will be used as a						
The starting IPV4/IPV6 Multicast Group Address that will be used as a						
streaming channel.						
rt memberships on a						
rt memberships on a ast group						

## 10.4.2 Port Setting

### Click Multicast > MVR > Port Setting

This page allows user to configure MVR role in each port.

	Multio	ast X	MVR	>> Po	rt Setting		
<ul> <li>Status</li> </ul>	Port	Port Setting Table					
<ul> <li>Network</li> </ul>							
✤ Port							
VLAN		-					
<ul> <li>MAC Address Table</li> </ul>		Entry	Ροπ	Role	Immediate Leave		
<ul> <li>Spanning Tree</li> </ul>		1	10GE1	None	Disabled		
Discovery		2	10GE2	None	Disabled		
✓ Multicast		3	10GE3	None	Disabled		
<ul> <li>General</li> </ul>		4	10GE4	None	Disabled		
<ul> <li>IGMP Snooping</li> </ul>		5	10GE5	None	Disabled		
<ul> <li>MLD Snooping</li> <li>MVP</li> </ul>		6	10GE6	None	Disabled		
Property		7	10GE7	None	Disabled		
Port Setting		8	10GE8	None	Disabled		
Group Address		9	10GE9	None	Disabled		
<ul> <li>Security</li> </ul>		10	10GE10	None	Disabled		
✤ ACL		11	10GE11	None	Disabled		
♥ QoS		12	10GE12	None	Disabled		
<ul> <li>Diagnostics</li> </ul>		13	LAG1	None	Disabled		
✤ Management		14	LAG2	None	Disabled		
		15	LAG3	None	Disabled		
		16	LAG4	None	Disabled		
		17	LAG5	None	Disabled		
		18	LAG6	None	Disabled		
		19	LAG7	None	Disabled		
		20	LAG8	None	Disabled		
		Edit					

Check the port and click "Edit" to edit Port Setting.

Port	10GE1	
Role	None     Receiver     Source	
Immediate Leave	Enable	

Field	Description
Port	The selected port.
Role	<ul> <li>None: The designated port does not participate MVR operations.</li> <li>Receiver: Configure a port as a receiver port if it is a subscriber port and should only receive multicast data. It does not receive data unless it becomes a member of the multicast group by issuing IGMP/MLD messages.</li> <li>Source: Configure uplink ports that receive and send multicast data as source ports. Subscribers cannot be directly connected to source ports.</li> </ul>
Immediate Leave	Check to enable the fast leave on the port.

# 10.4.3 Group Address

### Click Multicast > MVR > Group Address

This page allows user to assign the port(s) to group address.

	Multicast >> MVR >> Group Address		
✓ Status			
<ul> <li>Network</li> </ul>	Group Address Table		
✤ Port	Group Address Table		
✓ VLAN	Showing All v entries Showing (	to 0 of 0 entries	
<ul> <li>MAC Address Table</li> </ul>			4
	VLAN Group Address Member Type	Life (Sec)	
<ul> <li>Discovery</li> </ul>		0 results found.	
✓ Multicast			First Previous 1 Next Last
✓ General	Add Edit Delete Refresh		
<ul> <li>IGMP Snooping</li> </ul>			
<ul> <li>MLD Snooping</li> </ul>			
▲ MVR			
Property			
Port Setting			
Group Address			

Click "Add" or "Edit" to add or edit Group Address.

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

Field	Description
VLAN	The multicast VLAN ID.
Group Address	Specify the group address.
Member	Select the port(s) to be the group member.

# Chapter 11 Security

Use the security pages to configure setting for the switch security features.

# 11.1 RADIUS

#### Click Security > RADIUS

**Remote Authentication Dial-In User Service** (**RADIUS**) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for users who connect and use a network service.

This page allows user to set up RADIUS server.

Security » RADIUS								
✓ Status								
<ul> <li>Network</li> </ul>	Use Default Parameter							
✓ Port	Deter			40 1-6-				
VLAN	Retry	3	(1 -	10, defau	ult 3)			
<ul> <li>MAC Address Table</li> </ul>	Timeout	3	Sec	(1 - 30, c	default 3)			
<ul> <li>Spanning Tree</li> </ul>	Koy String							
• Discovery	Key String							
✓ Multicast								
✓ Security	Apply							
RADIUS TACACS+	RADIUS Table	•						
Management Access	Showing All ~	entries	Showi	ng 0 to 0	of 0 entries	5	0	
Authentication Manager	Q							
Port Security	Server Add	ress Server I	Port Priority	Retry	Timeout	Usage		
Traffic Segmentation	0 results found.							
DoS	Add	Edit	Delete				First Previous 1	Next Last
Field	Descrip	tion						
Botm.	Enter the number of transmitted requests sent to the Radius server							
Retry	before a failure occurs. The default is 3.							
	Enter the	amount	of time th	ne de	vice w	aits fo	r an answer from th	e
Timeout	Padius Server before switching to the payt server. The default value is				valua is			
imeout	2		iore switt	, ing		HOAL 3		
	3.	14 01		-			· · ·	
Key String	Enter the Key String used for encrypting all Radius communication							
	between	the device	ce and the	e Rad	dius se	rver.		

Click "Add" or "Edit" to add or edit RADIUS server.

Address Type	<ul> <li>Hostname</li> <li>IPv4</li> <li>IPv6</li> </ul>	
Server Address		
Server Port	1812	(0 - 65535, default 1812)
Priority		(0 - 65535)
Key String	✓ Use Default	
Retry	✓ Use Default	(1 - 10, default 3)
Timeout	✓ Use Default 3	Sec (1 - 30, default 3)
Usage	<ul> <li>Login</li> <li>802.1X</li> <li>All</li> </ul>	

Field	Description
Address Type	Specify the address type to "Hostname", "IPv4", or "IPv6".
Server Address	Specify the Hostname/IPv6/IPv4 address for the RADIUS server.
Server Port	Enter the server port number. The default port is 1812.
Key String	Enter the Key String used for encrypting all Radius communication
	between the device and the Radius server.
Potry	Enter the number of transmitted requests sent to the Radius server
Reliy	before a failure occurs. The default is 3.
	Enter the amount of time the device waits for an answer from the
Timeout	Radius Server before switching to the next server. The default value is
	3.
Usage	Select the usage: Login, 802.1X, All.

# 11.2 TACACS+

Click Security > TACACS+

**Terminal Access Controller Access-Control System Plus** (**TACACS+**) is a protocol developed by Cisco. TACACS+ handles authentication, authorization, and accounting (AAA) services. This page allows user to set up TACACS+ server.

	Security >> TACACS+			
✓ Status				
✓ Network	Use Default Parameter			
Port     VLAN     MAC Address Table	Timeout         5         Sec (1 - 30, default 5)			
Spanning Tree     Discovery     Multicast	Apply			
Security      RADIUS      TACACS+      the security	TACACS+ Table       Showing All v entries       Showing 0 to 0 of 0 entries			
AAA     Management Access     Authentication Manager     Port Security     Traffic Segmentation     Storm Control	Server Address     Server Port     Priority     Timeout       0 results found.       Add     Edit     Delete			
Field	Description			
Timeout	Enter the amount of time the device waits for an answer from the TACACS+ Server before switching to the next server. The default value is 3.			
Key String	Enter the Key String used for encrypting all TACACS+ communication between the device and the TACACS+ server.			

Click "Add" or "Edit" to add or edit TACACS+ server.

Address Type	<ul> <li>Hostname</li> <li>IPv4</li> <li>IPv6</li> </ul>	
Server Address		
Server Port	49	(0 - 65535, default 49)
Priority		(0 - 65535)
Key String	✓ Use Default	
<b>T</b> ime	✓ Use Default	
Timeout	5	Sec (1 - 30, default 5)

Field	Description	
Address Type	Specify the address type to "Hostname", "IPv4", or "IPv6".	
Server Address	Specify the Hostname/IPv6/IPv4 address for the TACACS+ server.	
Server Port	Enter the server port number. The default port is 49.	
Key String	Enter the Key String used for encrypting all TACACS+ communication between the device and the TACACS+ server.	
Timeout	Enter the amount of time the device waits for an answer from the TACACS+ Server before switching to the next server. The default value is 5.	

# 11.3 AAA

## 11.3.1 Method List

### Click Security >AAA > Method List

This page allows user to change Method List.

	Security >> AAA >> Method List
Status  Network  Port  VLAN  MAC Address Table  Spanning Tree  Discovery  Nutrieset	Method List Table Showing All  entries Showing 1 to 1 of 1 entries Name Sequence default (1) Local First Provision 1 Next Last
	Add Edit Delete

Click "Add" or "Edit" to add or edit Method List.

Name	
Method 1	<ul> <li>Empty</li> <li>None</li> <li>Local</li> <li>Enable</li> <li>RADIUS</li> <li>TACACS+</li> </ul>
Method 2	<ul> <li>Empty</li> <li>None</li> <li>Local</li> <li>Enable</li> <li>RADIUS</li> <li>TACACS+</li> </ul>
Method 3	Empty     None     Local     Enable     RADIUS     TACACS+
Method 4	Empty     None     Local     Enable     RADIUS     TACACS+

## 11.3.2 Login Authentication

#### Click Security >AAA > Login Authentication

This page allows user to change Login Authentication. User can change the login authentication method for "Console", "Telnet", "SSH", "HTTP" and "HTTPS".

	Security >> A	AAA >> Login Authentication
✓ Status		
• Network	Console	
✓ Port	Console	
VLAN	Telnet	default v (1) Local
✓ MAC Address Table	SSH	default 🗸 (1) Local
<ul> <li>Spanning Tree</li> </ul>	UTTD	
✤ Discovery	nur	
✓ Multicast	HTTPS	default v (1) Local
✓ Security		
RADIUS	Apply	
TACACS+		
AAA		
Method List		
Login Authentication		

# **11.4 Management Access**

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

### 11.4.1 Management VLAN

#### Click Security > Management Access > Management VLAN

This page allow user to change Management VLAN connection.

		Security >> Management Access >> Management VLAN
	MAC Address Table     Spanning Tree     Discovery	Management VLAN 1 - default Note: Change Management VLAN may cause connection interrupted
	Konstant Security RADIUS TACACS+ AAA Management Access Management VLAN Management VLAN Management ACL	Apply
Field	Management ACE	Description

	Salast management V/I AN in antian list
	Select management VLAN in option list.
Management VLAN	Management connection, such as http, https, SNMP etc, has the same VLAN of management VLAN are allow connecting to device. Others will be dropped.

### 11.4.2 Management Service

#### Click Security > Management Access > Management Service

This page allows user to change management services related configurations.

S	ecurity )) N	lanagement	Access >> Management Service	
Status				
Network	Managemen	t Service		
Port	Teinet			
VLAN				
MAC Address Table	331			
Spanning Tree	HTTP	Enable		
Discovery	HTTPS	Enable		
Multicast	SNMP	Enable		
Security				
RADIUS	Session Tim	leout		
	Console	10	Min (0 - 65535, default 10)	
Management Access	Teinet	10	Min (0 - 65535, default 10)	
Management Service	SSH	10	Min (0 - 65535, default 10)	
Management ACE	HTTP	10	Min (0 - 65535, default 10)	
Authentication Manager Port Security	HTTPS	10	Min (0 - 65535, default 10)	
Storm Control	Password R	etry Count		
DoS	Console	3	(0 - 120, default 3)	
	Teinet	3	(0 - 120, default 3)	
	SSH	3	(0 - 120, default 3)	
	Silent Time			
	Console	0	Sec (0 - 65535, default 0)	
	Teinet	0	Sec (0 - 65535, default 0)	
	SSH	0	Sec (0 - 65535, default 0)	
	Apply			

Field	Description	
	Management Service admin state.	
	Telnet: Connect CLI through Telnet.	
Managament Samiaa	SSH: Connect CLI through SSH.	
Management Service	HTTP: Connect Web UI through HTTP.	
	HTTPS: Connect Web UI through HTTPS.	
	SNMP: Manage switch through SNMP.	
Section Timeout	Set session timeout minutes for user access to user interface. 0	
Session Timeout	minute means never timeout.	
Password Retry	Sat password rates against for upor appage to upor interface	
Count	Set password retry count for user access to user interface.	
Silent Time	Set silent time for user access to user interface.	

# 11.4.3 Management ACL

Click Security > Management Access > Management ACL

This page displays the currently-defined Management ACLs profiles. To add a new ACL, enter the name of the new ACL and click **Apply**.

	Security >> Management Access >> Management ACL
✓ Status	
Vetwork	A CL Name
✓ Port	
VLAN	
<ul> <li>MAC Address Table</li> </ul>	Арріу
<ul> <li>Spanning Tree</li> </ul>	
<ul> <li>Discovery</li> </ul>	Management ACL Table
✓ Multicast	
- Security	Showing Air V entries Showing 0 to 0 of 0 entries Q
RADIUS	ACL Name State Rule
TACACS+	0 results found.
AAA Managamant Assass	First Previous 1 Next Last
Management VLAN	Active Deactive Delete
Management Service	
Management ACL	
Management ACE	

# 11.4.4 Management ACE

### Click Security > Management Access > Management ACE

Use this page to view and add rules to Management ACLs

	Security >>> Management Access >>>> Management AC	E
✓ Multicast		
✓ Security	Management ACE Table	
RADIUS		
TACACS+	ACL Name test v	
V AAA		
<ul> <li>Management Access</li> </ul>	Showing All v entries Showing 0 to 0 of 0 entries	0
Management VLAN	-	4
Management Service	Priority Action Service Port Address / Mask	
Management ACL	0 results found.	
Management ACE		First Previous 1 Next Last
Authentication Manager	Add Edit Delete	First Frevious I IVext Last
Port Security		

Select an ACL Name and click "Add/Edit" to add/edit ACE. Check and click Delete to delete ACEs.

ACL Name	test			
Priority	1 (1 -	65535)		
Service	<ul> <li>All</li> <li>Http</li> <li>Https</li> <li>Snmp</li> <li>SSH</li> <li>Telnet</li> </ul>			
Action	<ul><li>Permit</li><li>Deny</li></ul>			
Port	Available Port 10GE1 10GE2 10GE3 10GE4 10GE5 10GE6 10GE7 10GE8	se Se	lected Port	
P Version	<ul> <li>All</li> <li>IPv4</li> <li>IPv6</li> </ul>			
IPv4			/ 255.255.255.255	
IPv6			/ 128	(1 - 128)

Field	Description
ACL Name	The selected ACL.
Priority	Set priority for the rule.
Service	Select service.
Action	Select the action: Permit or Deny.
Port	Select the port.
IP Version	Select the IP version.

# **11.5 Authentication Manager**

# 11.5.1 Property

Click Security > Authentication Manager > Property

This page allows user to change Authentication Type and Property.

	Secu	ırity እ	Authe	nticatio	n Manage	r )> Prope	rty				
<ul> <li>Network</li> </ul>	1				D 902.1v						
✓ Port					002.1x						
<ul> <li>VLAN</li> </ul>			Authentic	ation Type	MAC-Bas	ed					
<ul> <li>MAC Address Table</li> </ul>					WEB-Bas	ed					
<ul> <li>Spanning Tree</li> </ul>					Enable						
Discovery			Gu	lest VLAN	1 ×						
<ul> <li>Multicast</li> </ul>						<u></u>					
- Security		MAC-B	ased User	ID Format	XXXXXXXX	XXXX ~					
RADIUS	_										
TACACS+		Apply									
~ AAA	Po	rt Mode	Table								
Management Access											
<ul> <li>Authentication Manager</li> </ul>					Authentication	Туре					
Property		Entry	Port	802.1x	MAC-Based	WEB-Based	Host Mode	Order	Method	Guest VLAN	VLAN Assign Mode
Port Setting		1	10GE1	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
MAC-Based Local Account		2	10GE2	Disabled	Disabled	Disabled	Multiple Authentication	802 1x	RADIUS	Disabled	Static
WED-Dased Local Account Sessions		2	10052	Disabled	Disabled	Disabled	Multiple Authentication	902.1x	PADILIS	Disabled	Static
Port Security		3	10023	Disabled	Disabled	Disabled	Multiple Authentication	002.1x	RADIUS	Disabled	Static
Traffic Segmentation		4	10GE4	Disabled	Disabled	Disabled	Multiple Authentication	802.1X	RADIUS	Disabled	Static
Storm Control		5	10GE5	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
V DoS		6	10GE6	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
		7	10GE7	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
		8	10GE8	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
		9	10GE9	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
		10	10GE10	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
		11	10GE11	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
		12	10GE12	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static

Select the ports in Port Mode Table and click "Edit" to edit Property.

Port	10GE1	
	□ 802.1x	
Authentication Type	MAC-Based	
	U WEB-Based	
Host Mode	Multiple Authentication     Multiple Hosts	
	O Single Host	
	Available Type Select Type	
	MAC-Based A 802.1x A	
Order	WEB-Based	
	Available Method Select Method	
	Local	
Method		
Guest VLAN	Enable	
VI AN Assign Mode	O Disable	
A A A SSIGN MODE	• Static	

## 11.5.2 Port Setting

### Click Security > Authentication Manager > Port Setting

This page allows user to change Port Setting.

	Secu	rity ))	Authe	ntication I	/lanager ))Po	rt Setting	I								
<ul> <li>Network</li> </ul>															
✓ Port	Por	t setti	ng lable	•											
VLAN															
<ul> <li>MAC Address Table</li> </ul>															_
<ul> <li>Spanning Tree</li> </ul>		Entry	Port	Port Control	Reauthentication	Max Hosts	Commo	n Timer			802.1x Pa	rameters		Web-Based Parameter	5
<ul> <li>Discovery</li> </ul>		Linuy	For	Fort control	Readmentication	Max Hosts	Reauthentication	Inactive	Quiet	TX Period	Supplicant Timeout	Server Timeout	Max Request	Max Login	
<ul> <li>Multicast</li> </ul>		1	10GE1	Disabled	Disabled	256	3600	60	60	30	30	30	2		3
👻 Security		2	10GE2	Disabled	Disabled	256	3600	60	60	30	30	30	2	:	3
RADIUS		3	10GE3	Disabled	Disabled	256	3600	60	60	30	30	30	2	:	3
TACACS+		4	10GE4	Disabled	Disabled	256	3600	60	60	30	30	30	2		3
V AAA		5	10GE5	Disabled	Disabled	256	3600	60	60	30	30	30	2	3	3
Management Access		6	10GE6	Disabled	Disabled	256	3600	60	60	30	30	30	2		3
Property		7	10GE7	Disabled	Disabled	256	3600	60	60	30	30	30	2	:	3
Port Setting		8	10GE8	Disabled	Disabled	256	3600	60	60	30	30	30	2		3
MAC-Based Local Account		9	10GE9	Disabled	Disabled	256	3600	60	60	30	30	30	2		3
WEB-Based Local Account		10	10GE10	Disabled	Disabled	256	3600	60	60	30	30	30	2		3
Sessions Doct Coourthy		11	10GE11	Disabled	Disabled	256	3600	60	60	30	30	30	2		3
Traffic Segmentation		12	10GE12	Disabled	Disabled	256	3600	60	60	30	30	30	2		3
Storm Control		12	-	0.040/04	Citabled	200	3000	00	00	50	50	50	2		-
✓ DoS		Edit													

Select the ports in Port Setting Table and click "Edit" to edit Port Setting.

Edit Port Setting

Port	10GE1					
Port Control	<ul> <li>Disabled</li> <li>Force Authorized</li> <li>Force Unauthorized</li> <li>Auto</li> </ul>					
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)				
02.1x 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)				
Veb-Based Parameter	'S					
May Login						
Max Login	3	(3 - 10, default 3)				

## 11.5.3 MAC-Based Local Account

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

This page allows user to add MAC-Based account.

	Secu	rity እ Auth	enticat	ion M	anager )) MA	C-Base	d Local Account
- Security							
RADIUS	MAG	C-Based Loca	al Accou	unt Tab	le		
TACACS+							
× AAA	Show	ring All 🗸 entr	ries			Showing	0 to 0 of 0 entries
<ul> <li>Management Access</li> </ul>							
Authentication Manager		MAC Address	Control	VIAN	Timeout (Se	ec)	
Property		MAG Address	Control	VLAN	Reauthentication	Inactive	
Port Setting							0 results found.
MAC-Based Local Account							
WEB-Based Local Account		Add E	Edit	Dele	te		
Sections							

Click "Add" or "Edit" to add or edit a MAC-based account.

MAC Address		
Port Control	<ul><li>Force Authorized</li><li>Force Unauthorized</li></ul>	
VLAN	User Defined	(1 - 4094)
ssigned Timer		
Reauthentication	User Defined	Sec (300 - 4294967294)
Inactive	User Defined	Sec (60 - 65535)

## 11.5.4 WEB-Based Local Account

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

This page allows user to add WEB-Based account.

S	Security >> Authentication Manage	er >> WEB-Based Local Account
Security     RADIUS	WEB-Based Local Account Table	
TACACS+ AAA Management Access	Showing All v entries	Showing 0 to 0 of 0 entries
Authentication Manager Property	Username VLAN Timeout (Sec Reauthentication	) Inactive
Port Setting MAC-Based Local Account		0 results found.
WEB-Based Local Account Sessions	Add Edit Delete	

Click "Add" or "Edit" to add or edit a WEB-based account.

Username			
Password			
Confirm Password			
	User Defined		
VLAN	1	(1 - 4094)	
ssigned Timer			
Basythantiastion	User Defined		
Reauthentication	3600	Sec (300 - 4294967294)	
I	User Defined		
Inactive	60	Sec (60 - 65535)	

## 11.5.5 Sessions

### Click Security > Authentication Manager > Sessions

This page allows user to monitor Sessions.

	Secu	rity እ Au	then	tication Ma	nager )) S	ession	S							
Multicast														
Security     RADIUS     TACACS+	Ses: Show	sions Tabl	e entries			Show	ving 0 to (	0 of 0 entrie	es					
AAA Management Access Authentication Manager		Session ID	Port	MAC Address	Current Type	Status	c	Operationa Session	I Information	n Quiet		Authorized Informat	ion	
Property							VLAN	Time	Time	Time	VLAN	Period	Timeout	
Port Setting MAC-Based Local Account								0 res	sults found.					
WEB-Based Local Account Sessions		Clear	Refres	h									Fir	st
Port Security														

# **11.6 Port Security**

### Click Security > Port Security

Network security can be increased by limiting access on a specific port to users with specific MAC addresses. Port Security prevents unauthorized device to the Switch prior to stopping auto-learning processing.

S	ecur	ity »	Port S	ecurity			
* VLAN	_						
MAC Address Table		State	Enable	• • • • • • • • • • • • • • • • • • •			
<ul> <li>Spanning Tree</li> </ul>							
✤ Discovery	A	pply					
✓ Multicast	Port	Soow	ity Tabl				
✓ Security	FUIL	Secu	πγ ταριά	7			
RADIUS						C	2
TACACS+		Entry	Port	State	MAC Address	Action	
AAA     Management Access		1	10GE1	Disabled	1	Discard	
Authentication Manager		2	10GE2	Disabled	1	Discard	
Port Security		3	10GE3	Disabled	1	Discard	
Traffic Segmentation		4	10GE4	Disabled	1	Discard	
Storm Control		5	10GE5	Disabled	1	Discard	
DoS     Dynamic APP Inspection		6	10GE6	Disabled	1	Discard	
DHCP Snooping		7	10GE7	Disabled	1	Discard	
IP Source Guard		8	10GE8	Disabled	1	Discard	
✓ ACL		9	10GE9	Disabled	1	Discard	
✓ QoS		10	10GE10	Disabled	1	Discard	
<ul> <li>Diagnostics</li> </ul>		11	10GE11	Disabled	1	Discard	
✓ Management		12	10GE12	Disabled	1	Discard	
		13	LAG1	Disabled	1	Discard	
		14	LAG2	Disabled	1	Discard	
		15	LAG3	Disabled	1	Discard	
		16	LAG4	Disabled	1	Discard	
		17	LAG5	Disabled	1	Discard	
		18	LAG6	Disabled	1	Discard	
		19	LAG7	Disabled	1	Discard	
		20	LAG8	Disabled	1	Discard	
	-	dit	٦				

Select port and click "Edit" to edit port security.

Port	10GE1	
State	Enable	
MAC Address	1	(0 - 255, default 1)
Action	<ul> <li>Forward</li> <li>Discard</li> <li>Shutdown</li> </ul>	

Field	Description
Port	The selected port.
State	Check to Enable for the port security feature for the selected port
MAC Address	Enter the maximum number of MAC Address that can be learned on the port. The range is from 0-255.
Action	Select the action: <b>Forward</b> , <b>Discard</b> or <b>Shutdown</b> when exceeded the maximum number of MAC Address.

# **11.7 Traffic Segmentation**

### Click Security > Traffic Segmentation

Traffic Segmentation prohibits ports to communicate with each other directly, on other manufacturers' switches, this function is called Protected Ports, Port Isolation, etc.

	Security >> Traffic Segmentation					
Status     Network     Port     VI.AN	Traffic Segmentation Settings					
<ul> <li>MAC Address Table</li> </ul>	Port List (e.g. GE1,GE2-5,10GE1-2)	All Ports				
✓ Spanning Tree	Forward Port List (e.g. GE1.GE2-5,10GE1-2)	All Ports				
<ul> <li>Discovery</li> </ul>						
<ul> <li>Multicast</li> </ul>	Apply					
- Security	The file One was to file Table					
TACACS+						
Management Access	Entry Port Forward Port List					
Port Security	1 10GE1 xGE1-12,lag1-8					
Traffic Segmentation	2 10GE2 xGE1-12,lag1-8					
Storm Control	3 10GE3 xGE1-12,lag1-8					
DoS	4 10GE4 xGE1-12,lag1-8					
DHCP Snooping	5 10GE5 xGE1-12,lag1-8					
V IP Source Guard	6 10GE6 xGE1-12,lag1-8					
✓ ACL	7 10GE7 xGE1-12,lag1-8					
	8 10GE8 xGE1-12,lag1-8					
	9 10GE9 xGE1-12,lag1-8					
	10 10GE10 xGE1-12,lag1-8					
	11 10GE11 xGE1-12,lag1-8					
	12 10GE12 XGE1-12,lag1-8					
ld	Description					
rt List	Enter the source port (eg. xGE1, xGE2-xGE12)					
rward Port List	Enter the forwarding ports (eg. xGE1, xGE2–xGE12, LAG1-LAG8)					

# **11.8 Storm Control**

### Click Security > Storm Control

To display Storm Control global setting web page.

	Secu	ity ))	Storm	Contro							
	_										
✓ Network			O Packe	t / Sec							
✓ Port		Mode	<ul> <li>Kbits /</li> </ul>	Sec							
✓ VLAN			<ul> <li>Exclusion</li> </ul>	1e							
<ul> <li>MAC Address Table</li> </ul>		IFG		e							
<ul> <li>Spanning Tree</li> </ul>	· · · · · ·	f									
✓ Discovery	Apply										
✓ Multicast	Dent	0.41									
✓ Security	Port	Settin	ig lable								
RADIUS					-						
TACACS+		Entry	Port	State	Bro	adcast	Unknow	n Multicast	Unkno	wn Unicast	Action
~ AAA					State	Rate (Kbps)	State	Rate (Kbps)	State	Rate (Kbps)	
Authentication Manager		1	10GE1	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
Port Security		2	10GE2	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
Traffic Segmentation		3	10GE3	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
Storm Control		4	10GE4	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
✓ DoS		5	10GE5	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
Dynamic ARP Inspection		6	10GE6	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
DHCP Snooping		7	10GE7	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
* ACL		8	10GE8	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
• 00S		9	10GE9	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
		10	10GE10	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
		11	10GE11	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
		12	10GE12	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
		Edit									

Field	Description
	Select the unit of storm control
Unit	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.
	<b>Included</b> : include preamble & IFG (20 bytes) when count ingress storm
	control rate.

Click "Edit" to edit the storm control port setting web page.

Port	10GE1	
State	Enable	
<b>B</b>	Enable	
Broadcast	10000	Kbps (16 - 10000000, default 10000)
Unknown Multicast	Enable	
	10000	Kbps (16 - 10000000, default 10000)
	Enable	
Unknown Unicast	10000	Kbps (16 - 10000000, default 10000)
Action	<ul><li>Drop</li></ul>	

Field	Description
Port	Select the setting ports
Stato	Select the state of setting.
State	Enable: Enable the storm control function.
	<b>Enable</b> : Enable the storm control function of broadcast packet.
Broadcast	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.
	<b>Enable</b> : Enable the storm control function of unknown multicast packet.
Unknown Multicast	Value of storm control rate, Unit: pps (packet per-second, range
	1~262143) or Kbps (Kbits per-second, range16~1000000) depends on
	<b>Enable</b> : Enable the storm control function of unknown unicast packet
	Value of storm control rate. Unit: pps (packet per-second range
Unknown Unicast	1~262143) or Kbps (Kbits per-second, range16~1000000) depends on
	global mode setting.
	Select the state of setting.
Action	<b>Drop</b> : Packets exceed storm control rate will be dropped.
ACUUII	Shutdown: Port will be shutdown when packets exceed storm control
	rate.

# 11.9 DoS

A Denial of Service (DoS) attack is a hacker attempt to make a device unavailable to its users. DoS

attacks saturate the device with external communication requests, so that it cannot respond to legitimate traffic. These attacks usually lead to a device CPU overload.

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

## 11.9.1 Property

### Click Security > DoS > Property

To display DoS Global Setting web page.

	Security >> DoS >> P	roperty					
✓ Status							
<ul> <li>Network</li> </ul>	POD	Enable					
✤ Port	Land	Enable					
✓ VLAN	UDP Blat						
MAC Address Table							
Spanning Tree							
Multicast	DMAC = SMAC	Enable					
Security	Null Scan Attack						
RADIUS	Y Maa Caan Attack						
TACACS+		Enable					
~ AAA	TCP SYN-FIN Attack	Enable					
Management Access	TCP SYN-RST Attack	Enable					
Port Security							
Traffic Segmentation							
Storm Control	TCP-SYN						
DoS		Note: Source Port	t < 1024				
Property Port Setting	TCP Fragment	Enable					
Dynamic ARP Inspection	. e. r agneni	Note: Offset = 1					
DHCP Snooping							
IP Source Guard							
	Ping Max Size						
		512	Byte (0 - 65535, default 512)				
		🔽 Enable					
	TCP Min Hdr size	20	Byte (0 - 31, default 20)				
	IPv6 Min Fragment						
		1240	Byte (0 - 65535, default 1240)				
		Enable					
	Smurf Attack	0	Netmask Length (0 - 32, default 0)				
		1-					

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

TCP-SYN(SPORT <1024)	Drops SYN packets with sport less than 1024.
TCP Fragment (Offset=1)	Drops the TCP fragment packets with offset equals to one.
Ping Max Size	Specify the maximum size of the ICMPv4/ICMPv6 ping packets. The valid range is from 0 to 65535 bytes, and the default value is 512 bytes.
IPv4 Ping Max Size	Checks the maximum size of ICMP ping packets, and drops the packets larger than the maximum packet size.
IPv6 Ping Max Size	Checks the maximum size of ICMPv6 ping packets, and drops the packets larger than the maximum packet size
TCP Min Hdr Size	Checks the minimum TCP header and drops the TCP packets with the header smaller than the minimum size. The length range is from 0 to 31 bytes, and default length is 20 bytes.
IPv6 Min Fragment	Checks the minimum size of IPv6 fragments, and drops the packets smaller than the minimum size. The valid range is from 0 to 65535 bytes, and default value is 1240 bytes.
Smurf Attack	Avoid smurf attack. The length range of the netmask is from 0 to 323 bytes, and default length is 0 bytes.

## 11.9.2 Port Setting

### Click Security > DoS > Port Setting

To configure and display the state of DoS protection for interfaces.

	Se	ecuri	ty እን	DoS ))	Port S	Setting
✓ Status	^					
		Port 9	Sottin	a Tabla		
✤ Port		FUIL	Settin	y lable		
✓ VLAN						0
<ul> <li>MAC Address Table</li> </ul>						~
<ul> <li>Spanning Tree</li> </ul>			Entry	Port	State	
✤ Discovery			1	10GE1	Disabled	
✓ Multicast			2	10GE2	Disabled	
✓ Security			3	10GE3	Disabled	
RADIUS			4	10GE4	Disabled	
TACACS+			5	10GE5	Disabled	
· AAA			6	10GE6	Disabled	
Authentication Manager			7	10GE7	Disabled	
Port Security			8	10GE8	Disabled	
Traffic Segmentation			9	10GE9	Disabled	
Storm Control			10	10GE10	Disabled	
∧ DoS			11	10GE11	Disabled	
Property Port Setting			12	10GE12	Disabled	
Dynamic ARP Inspection				~		
<ul> <li>DHCP Snooping</li> </ul>		Ec	dit	J		
ield	Desc	cript	ion			
Port	Inter	face	or p	ort nu	mber.	
state	Enat	ole/D	isab	le the	DoS p	protection on the interface.

# 11.10 Dynamic ARP Inspection

Dynamic ARP inspection (DAI) protects switching devices against ARP spoofing.

DAI inspects Address Resolution Protocol (ARP) packets on the LAN and uses the information in the DHCP snooping database on the switch to validate ARP packets and to protect against ARP

spoofing (also known as ARP poisoning or ARP cache poisoning). ARP requests and replies are compared against entries in the DHCP snooping database, and filtering decisions are made based on the results of those comparisons. When an attacker tries to use a forged ARP packet to spoof an address, the switch compares the address with entries in the database. If the MAC address or IP address in the ARP packet does not match a valid entry in the DHCP snooping database, the packet is dropped.

## 11.10.1 Property

#### Click Security > Dynamic ARP Inspection > Property

State Enable Available VLAN Selected VLAN VIAN 1 Security **VLAN 100** > TACACS+ VLAN Management Access Authentication Manage < Fraffic Segmentation Apply ARP Inspection Port Setting Table Property Q P Source Guard Entry Port Trust Source MAC Address Destination MAC Address IP Address Rate Limit 1 10GE1 Disabled Disabled Disabled Disabled Unlimited 2 10GE2 Disabled Disabled Disabled Disabled Unlimited 3 10GE3 Disabled Disabled Disabled Unlimited Disabled Management 10GE4 Disabled Disabled Disabled Disabled Unlimited 4 5 10GE5 Disabled Disabled Disabled Disabled Unlimited Disabled 6 10GE6 Disabled Disabled Disabled Unlimited 7 10GE7 Disabled Disabled Disabled Disabled Unlimited 8 10GE8 Disabled Disabled Disabled Disabled Unlimited 9 10GE9 Disabled Disabled Disabled Disabled Unlimited 10 10GE10 Disabled Disabled Disabled Disabled Unlimited Disabled 11 10GE11 Disabled Disabled Disabled Unlimited 10GE12 Disabled Disabled Disabled Disabled 12 Unlimited Disabled Disabled 13 LAG1 Disabled Disabled Unlimited П 14 LAG2 Disabled Disabled Disabled Disabled Unlimited 15 LAG3 Disabled Disabled Disabled Disabled Unlimited 16 LAG4 Disabled Disabled Disabled Disabled Unlimited 17 LAG5 Disabled Disabled Disabled Disabled Unlimited Disabled 18 LAG6 Disabled Disabled Disabled Unlimited 19 LAG7 Disabled Disabled Disabled Disabled Unlimited Disabled 20 LAG8 Disabled Disabled Disabled Unlimited Edit

To configure and display the state of Dynamic ARP Inspection for interfaces.

Select port and click "Edit" to edit DAI for that port.

#### **Edit Port Setting**

Port	10GE1					
Trust	Enable					
Source MAC Address	Enable					
Destination MAC Address	Enable					
IP Address	<ul><li>Enable</li><li>Allow Zere</li></ul>	p (0.0.0)				
Rate Limit	0	pps (0 - 50, default 0), 0 is Unlimited				

Field	Description
Port	The selected port.
Trust	Check to set the port to <b>Trust</b> state. DAI associates a trust state with each interface on the switch. Packets arriving on trusted interfaces bypass all DAI validation checks, and those arriving on untrusted interfaces undergo the DAI validation process.
Source MAC Address	Check this option; DAI will check Source MAC Address.
Destination MAC Address	Check this option; DAI will check Destination MAC Address.
IP Address	Check this option; DAI will check IP Address. And if check Allow Zero, DAI will allow 0.0.0.0 IP address to pass through.
Rate Limit	Set the rate limit on untrusted interfaces. The rate is unlimited on all trusted interfaces.

## 11.10.2 Statistics

### Click Security > Dynamic ARP Inspection > Statistics

To display the statistics of Dynamic ARP Inspection.

S	ecur	ity እ	Dynam	nic ARP	Inspectio	n )) Statistics	5		
ddress Table									
Tree									
	Stat	ISTICS	lable						
								0	
								ų	
		Entry	Port	Forward	Source MAC	Destination MAC	Source IP	Destination IP	IP-MAC
		Linuy	1 011	Torward	Failure	Failure	Validation Failure	Validation Failure	Mismatch Failur
		1	10GE1	0	0	0	0	0	
		2	10GE2	0	0	0	0	0	
		3	10GE3	0	0	0	0	0	
n de la companya de la		4	10GE4	0	0	0	0	0	
		5	10GE5	0	0	0	0	0	
		6	10026	0	0	0	0	0	
n		7	10000	0	0	0	0	0	
		1	10GE7	0	0	0	0	0	
		8	10GE8	0	0	0	0	0	
		9	10GE9	0	0	0	0	0	
		10	10GE10	0	0	0	0	0	
		11	10GE11	0	0	0	0	0	
		12	10GE12	0	0	0	0	0	
		13	LAG1	0	0	0	0	0	
V		14	LAG2	0	0	0	0	0	
		15	LAG3	0	0	0	0	0	
		16	LAG4	0	0	0	0	0	
		17	LAG5	0	0	0	0	0	
		18	LAG6	0	0	0	0	0	
		19	LAG7	0	0	0	0	0	
		20		0	0	0	0	0	

# 11.11 DHCP Snooping

You can use DHCP snooping to help avoid the Denial of Service attacks that result from unauthorized users adding a DHCP server to the network that then provides invalid configuration data to other DHCP clients on the network. DHCP snooping accomplishes this by allowing you to distinguish between trusted ports connected to a DHCP server or switch and untrusted ports connected to end-users. DHCP packets are forwarded between trusted ports without inspection. DHCP packets received on other switch ports are inspected before being forwarded. Packets from untrusted sources are dropped.

## 11.11.1 Property

### Click Security > DHCP Snooping > Property

To configure and display the state of DHCP Snooping for interfaces.

	Securit	y // DHC	Shoop	ing // Prop	erty	
<ul> <li>Discovery</li> </ul>	^					
<ul> <li>Multicast</li> </ul>		tata 🗖 Eau	bla			
✓ Security	3		DIE			
RADIUS		Availab	e VLAN	Selected VLAN	1	
TACACS+		VLAN	1 ^			
✓ AAA		VLAN	100	,	^	
<ul> <li>Management Access</li> </ul>						
Authentication Manager	VL			_		
Port Security						
I raffic Segmentation						
				· ·	<b>~</b>	
Dynamic ARP Inspection			*			
DHCP Snooping						
Property	App	bly				
Statistics	Port S	etting Tab	e			
Option82 Property		oung ius				
Option82 Circuit ID						Q
<ul> <li>IP Source Guard</li> </ul>		ntry Port	Trust	Verify Chaddr	Rate Limit	
✓ ACL		1 10GE1	Disabled	Disabled	Linlimited	
✓ QoS		0 40050	Disabled	Disabled	Unlimited	
<ul> <li>Diagnostics</li> </ul>		2 10GE2	Disabled	Disabled	Unimited	
<ul> <li>Management</li> </ul>	$\sim$	3 10GE3	Disabled	Disabled	Unlimited	
		4 10GE4	Disabled	Disabled	Unlimited	
		5 10GE5	Disabled	Disabled	Unlimited	
		6 10GE6	Disabled	Disabled	Unlimited	
		7 10GE7	Disabled	Disabled	Unlimited	
		8 10GE8	Disabled	Disabled	Unlimited	
		9 10GE9	Disabled	Disabled	Unlimited	
		10 10GE1	0 Disabled	Disabled	Unlimited	
		11 10GE1	1 Disabled	Disabled	Unlimited	
		12 10GE1	2 Disabled	Disabled	Unlimited	
		12 10021	Disabled	Disabled	Unlimited	
		13 LAGT	Disabled	Disabled	Unimited	
		14 LAG2	Disabled	Disabled	Unimited	
		15 LAG3	Disabled	Disabled	Unlimited	
		16 LAG4	Disabled	Disabled	Unlimited	
		17 LAG5	Disabled	Disabled	Unlimited	
		18 LAG6	Disabled	Disabled	Unlimited	
		19 LAG7	Disabled	Disabled	Unlimited	
		20 LAG8	Disabled	Disabled	Unlimited	
	Ed	it				

DUOD

Select port and click "Edit" to edit DHCP Snooping for that port.

Port	10GE1	
Trust	Enable	
Verify Chaddr	Enable	
Rate Limit	pps (0 - 300, default 0), 0 is Unlimited	

Field	Description
Port	The selected port.
	Check to set the port to <b>Trust</b> state.
Trust	The DHCP snooping feature determines whether traffic sources are
	trusted or untrusted. An untrusted source may initiate traffic attacks or
	other hostile actions. To prevent such attacks, the DHCP snooping
	feature filters messages and rate-limits traffic from untrusted sources.
	Check to enable Verify Chaddr.
Verify Chaddr	DHCP snooping drops DHCP packets received on untrusted ports
	when the check address (chaddr) field in the DHCP header does not
	match the source MAC address of the packet.

Pato Limit	Set the rate limit on untrusted interfaces. The rate is unlimited on all
	trusted interfaces.

## 11.11.2 Statistics

### Click Security > DHCP Snooping > Statistics

To display the statistics of DHCP Snooping.

	Secu	ity ))	DHCP	Snoopi	ng እ Statis	tics			
Discovery									
<ul> <li>Multicast</li> </ul>	Stat	istics	Table						
- Security									
RADIUS	_							4	
TACACS+					Chaddr Check	Untrust Port	Untrust Port	Invalid	
<ul> <li>AAA</li> <li>Management Access</li> </ul>		Entry	Port	Forward	Drop	Drop	with Option82	Drop	
Authentication Manager					2.00	2.00	Drop	2.00	
Port Security		1	10GE1	0	0	0	0	0	
Traffic Segmentation		2	10GE2	0	0	0	0	0	
Storm Control		3	10GE3	0	0	0	0	0	
• DoS		4	10GE4	0	0	0	0	0	
Dynamic ARP Inspection		5	10GE5	0	0	0	0	0	
Property		6	10GE6	0	0	0	0	0	
Statistics		7	10GE7	0	0	0	0	0	
Option82 Property		8	10GE8	0	0	0	0	0	
Option82 Circuit ID		9	10GE9	0	0	0	0	0	
VIP Source Guard		10	10GE10	0	0	0	0	0	
✓ ACL		11	10GE11	0	0	0	0	0	
▼ QoS		12	10GE12	0	0	0	0	0	
Diagnostics		13	LAG1	0	0	0	0	0	
Management		14	LAG2	0	0	0	0	0	
		15	LAG3	0	0	0	0	0	
		16	LAG4	0	0	0	0	0	
		17	LAG5	0	0	0	0	0	
		18	LAG6	0	0	0	0	0	
		19	LAG7	0	0	0	0	0	
		20	LAG8	0	0	0	0	0	
		Clear	Refre	sh					

# 11.11.3 Option82 Property

Click Security > DHCP Snooping > Option82 Property

To configure and display Option82 property.

Monitorial         Monitorial         Accord         AA         AA         AA         A Athenication Management Access         Athenication Mac		S	ecuri	ty እ	DHCP	Snoopi	ng እ Optio	n82 Propert	у		
• Mudual         • Security           PADIUS         TACACS*           • AA         • Management Access           • Initic Segmentation         Both Control           • Security         Table           • Data         • Control           • Data         • Control           • Options2 Property         Point Security           • Point Security         • Table           • Options2 Property         Options2 Property           • Pointe Cault         • Options2 Property           • Options2 Property         Options2 Property           • Pointe Cault         • Options2 Property           • Options2 Property         Options2 Property           • Options2 Property         Options2 Property           • Add         • Options2 Property           • Options2 Property         Options2 Property           • Desprosition         • Optingte Desprop           • I ogtio Destab	<ul> <li>Discovery</li> </ul>	^	_								
Security     Remote ID	<ul> <li>Multicast</li> </ul>					User Defined					
RADUS         CACACE         A AN         A Hubenkalon Manage         Property         Statelics         Optionas 2 Property         Statelics         Optionas 2 Property         Statelics         Optionas 2 Property         Statelics         Optionas 2 Property         Statelics         Diginoacis         T 106E1 Disabled       Drop         I 106E8 Disabled       Drop	- Security		Remote ID								
Image: Processor in the second status         Name         AAA         Management Access         Pot Security         Table Segmentation         Stom Control         DoS         Dynamic ARP Inspector         DidS Display         Poperty         Statissics         Options 2 Property         Disabled Drop         10 106E1 Disa	RADIUS										
eld          Observed to       Description         eld       Description         eld       Description         enter to       Displeted for defining the MAC address of the switch that added the corp	AAA		Ope	ration	al Status						
<ul> <li>Authentication Manager Port Security Trafic Segmentation Storm Control</li> <li>DoS</li> <li>Dynamic ARP Inspection</li> <li>DHCP Security Option82 Circuit ID</li> <li>P Source Guard</li> <li>Stote Codd</li>     &lt;</ul>	Management Access		P	emote	D fc:8f	c4·0d·22·11	(Switch Mac in By	rte Order)			
Pot Security       Apply         Dod       Pot Setting Table         Dispersive       Options2 Property         Options2 Property       1 100E1 Disabled       Drop         Quite Security       1 100E1 Disabled       Drop         Quite Security       2 100E2 Disabled       Drop         Quite Security       3 100E3 Disabled       Drop         Quite Security       1 100E1 Disabled       Drop         Quite Security       1 100E1 Disabled       Drop         Quite Security       1 100E5 Disabled       Drop         Management       1 100E5 Disabled       Drop         Management       1 100E5 Disabled       Drop         Imagement       1 1 100E5 Disabled       Drop         Imagement       LAG	Authentication Manager		<b>`</b>	emote	10.01.	04.00.22.11	(Owner Mae In By				
Iradic Segmentation         • DoS         •	Port Security		Ap	ply							
• Dols       Option Science       Option Scienc	Storm Control		Port 9	Sottin	a Tabla						
Optimic ARP Inspection         DHCP Shooping         Property         Options2 Property         Mariagement         Vio Disabled       Drop         1 1 006E1 Disabled       Drop         1 1 1 106E1 Disabled       Drop         1 1 1 016E1 Disabled       Drop         1 1 1 016E1 Disabled       Drop         1 1 1 016E1 Disabled       Drop<	<ul> <li>DoS</li> </ul>		Ports	settin	y lable						
	<ul> <li>Dynamic ARP Inspection</li> </ul>									Q	
Property Statistics Option82 Property Option82 Proper	DHCP Snooping			Entry	Port	State	Allow Untrust				
Option82 Property Option82 Circuit ID       2       106E2       Disabled       Drop         • ACL       Gas       6       106E5       Disabled       Drop         • ACL       Gas       6       106E5       Disabled       Drop         • Management       0       6       106E5       Disabled       Drop         • Management       0       0       0       Disabled       Drop         • 10       10.0E7       Disabled       Drop       0       0       Disabled       Drop         • 10       10.0E10       Disabled       Drop       0       11       10       Disabled       Drop         • 11       10.0E10       Disabled       Drop       0       12       10       Drop         • 13       LAG1       Disabled       Drop       0       14       LAG2       Disabled       Drop         • 14       LAG2       Disabled       Drop       0       <	Property			1	10GE1	Disabled	Drop				
Optione2 Circuit ID       3       10GE3       Disabled       Drop         • ACL       • OGS       • OGS       • OGS       • OGS       • OGS         • Diagnostics       • Official Disabled       Drop       • Official Disabled       Drop         • Minagement       • OGE       • OGE       • OGE       • OGE         • Minagement       • OGE       • OGE       Disabled       Drop         • 10       10GE3       Disabled       Drop         • 10       10GE3       Disabled       Drop         • 10       10GE3       Disabled       Drop         • 10       10GE1       Disabled       Drop         • 11       10GE1       Disabled       Drop         • 12       10GE3       Disabled       Drop         • 14       LAG2       Disabled       Drop         • 14       LAG3       Disabled       Drop         • 14       LAG3       Disabled       Drop         • 14       LAG3       Disabled       Drop         • 14       LAG4       Disabled       Drop         • 15       LAG3       Disabled       Drop         • 15       LAG3       Disabled       Drop </th <th>Option82 Property</th> <th></th> <th></th> <th>2</th> <th>10GE2</th> <th>Disabled</th> <th>Drop</th> <th></th> <th></th> <th></th> <th></th>	Option82 Property			2	10GE2	Disabled	Drop				
Image: P Source Guard       4       10GE4       Disabled       Drop         Image: Source Guard       5       10GE5       Disabled       Drop         Image: Source Guard       6       10GE6       Disabled       Drop         Image: Source Guard       7       10GE7       Disabled       Drop         Image: Source Guard       8       10GE8       Disabled       Drop         Image: Source Guard       8       10GE7       Disabled       Drop         Image: Source Guard       8       10GE8       Disabled       Drop         Image: Source Guard       8       10GE8       Disabled       Drop         Image: Source Guard       9       10GE9       Disabled       Drop         Image: Source Guard       9       10GE10       Disabled       Drop         Image: Source Guard       10       10       LAG2       Disabled       Drop         Image: Source Guard       10       LAG2       Disabled <th>Option82 Circuit ID</th> <th></th> <th></th> <th>3</th> <th>10GE3</th> <th>Disabled</th> <th>Drop</th> <th></th> <th></th> <th></th> <th></th>	Option82 Circuit ID			3	10GE3	Disabled	Drop				
• AcL       • Gos         • Diagnostics       • O         • Management       • O         • O       • O         • Management       • O         • Management       • O         • Management       • O         • O       • O         • O       • O         • Management       • O         • O       • O	IP Source Guard			4	10GE4	Disabled	Drop				
• OoS       • Diaghostics       • T 10GE7 Disabled       Drop         • Management       • 10GE8       Disabled       Drop         • 9       10GE9       Disabled       Drop         • 10       10GE1       Disabled       Drop         • 11       10GE1       Disabled       Drop         • 12       10GE12       Disabled       Drop         • 14       LAG2       Disabled       Drop         • 15       LAG3       Disabled       Drop         • 16       LAG4       Disabled       Drop         • 18       LAG6       Disabled       Drop         • 18       LAG6       Disabled       Drop         • 18       LAG6       Disabled       Drop         • 19       LAG7       Disabled       Drop         • 10       LAG8       Disabled       Drop         • 14       LAG2       Disabled       Drop         • 14       LAG2       Disabled       Drop         • 14       LAG2       Disabled       Drop         • 14       LAG4       Disabled       Drop         • 18       LAG6       Disabled       Drop         • 19       LAG	✓ ACL			5	10GE5	Disabled	Drop				
• Diagnostics       - 7       10GE7       Disabled       Drop         • Management       - 8       10GE3       Disabled       Drop         - 10       10GE10       Disabled       Drop         - 11       10GE11       Disabled       Drop         - 12       10GE12       Disabled       Drop         - 13       LAG1       Disabled       Drop         - 14       LAG2       Disabled       Drop         - 15       LAG3       Disabled       Drop         - 16       LAG4       Disabled       Drop         - 17       LAG5       Disabled       Drop         - 18       LAG6       Disabled       Drop         - 18       LAG6       Disabled       Drop         - 19       LAG7       Disabled       Drop         - 20       LAG8       Disabled       Drop				6	10GE6	Disabled	Drop				
Image: Next Sector S	✤ Diagnostics			7	10GE7	Disabled	Drop				
emote ID       9       10GE9       Disabled       Drop         9       10GE10       Disabled       Drop         11       10GE11       Disabled       Drop         12       10GE12       Disabled       Drop         13       LAG1       Disabled       Drop         14       LAG2       Disabled       Drop         15       LAG3       Disabled       Drop         16       LAG4       Disabled       Drop         17       LAG5       Disabled       Drop         18       LAG6       Disabled       Drop         19       LAG7       Disabled       Drop         20       LAG8       Disabled       Drop         20       LAG8       Disabled       Drop         Edit       Description       Used for defining the MAC address of the switch that added the set of the set of the switch that added the set of the set of the switch that added the set of the set of the switch that added the set of the se	<ul> <li>Management</li> </ul>	$\sim$		8	10GE8	Disabled	Drop				
Image: second				9	10GE9	Disabled	Drop				
Image: state of the system				10	10GE10	Disabled	Drop				
Image: state in the second state in				11	10GE11	Disabled	Drop				
Image: state of the system				12	10GE12	Disabled	Drop				
Image: state of the sector				13	LAG1	Disabled	Drop				
Image: state in the second state in				14	LAG2	Disabled	Drop				
Image: Second state in the second s				15	LAG3	Disabled	Drop				
Image: state of the sector				16	LAG4	Disabled	Drop				
Image: Second state in the second s				17	LAG5	Disabled	Drop				
Image:				18	LAG6	Disabled	Drop				
Image: Description       Image: D				19	LAG7	Disabled	Drop				
Edit       Description       Used for defining the MAC address of the switch that added the option       Option				20	LAG8	Disabled	Drop				
enote ID Continue 00 information			-		1						
eld         Description           emote ID         Used for defining the MAC address of the switch that added the Outline 00 information			E	dit	J						
emote ID Used for defining the MAC address of the switch that added the	ield	De	scri	ptic	on						
emote ID		Us	ed fo	or d	efinir	na the	MAC ad	dress of	the swi	tch that a	dded th
	iemote ID	On	tion	82	infor	nation	יי ו				

Select port and click "Edit" to edit Option82 property for that port.

Close

Edit Port Setting Port 10GE1 State Enable О Кеер Allow Untrust O Drop Replace Apply

Field Description Port The selected port. Check to set the port to Trust state. State Configures DHCP snooping behavior when forwarding a DHCP packet from an untrusted port that already contains DHCP relay information (Option 82). Keep: The packet is forwarded without replacing the option **Allow Untrust** information. **Drop**: The packet is dropped. Replace: The existing option is replaced with a new Option 82 generated by the switch.

## 11.11.4 Option82 Circuit ID

### Click Security > DHCP Snooping > Option82 Circuit ID

To configure and display Option82 Circuit ID.

	Security 🕨 DHCP Snoor	oing >> Option82 Circuit II	)
Discovery			
<ul> <li>Multicast</li> </ul>			
✓ Security	Option82 Circuit ID Table		
RADIUS TACACS+	Showing All v entries	Showing 0 to 0 of 0 entries	Q
~ AAA	Port VLAN Circuit ID		
Management Access		0 results found.	
<ul> <li>Authentication Manager</li> <li>Port Security</li> </ul>	Add Edit	Delete	First Previous 1 Next Last
Traffic Segmentation			
Storm Control			
✓ DoS			
Dynamic ARP Inspection			
DHCP Snooping			
Statistics			
Ontion82 Property			
Option82 Circuit ID			
IP Source Guard			

Click "Add" or "Edit" to add or edit an Option82 Circuit ID.

Port	10GE1 ×
VLAN	(1 - 4094) (Keep empty to set without VLAN)
Circuit ID	
Apply	Close
Field	Description
Port	Select the port to add Circuit ID.
VLAN	Specify the VLAN ID.
Circuit ID	Used for defining the switch port and VLAN number of the port user(s)

# 11.12 IP Source Guard

IP Source Guard is a security feature that restricts IP traffic on untrusted Layer 2 ports by filtering traffic based on the DHCP snooping binding database or manually configured IP source bindings. This feature helps prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host. Any IP traffic coming into the interface with a source IP address other than that assigned (via DHCP or static configuration) will be filtered out on the untrusted Layer 2 ports.

The IP Source Guard feature is enabled in combination with the DHCP snooping feature on untrusted Layer 2 interfaces. It builds and maintains an IP source binding table that is learned by DHCP snooping or manually configured (static IP source bindings). An entry in the IP source binding table contains the IP address and the associated MAC and VLAN numbers. The IP Source Guard is

supported on Layer 2 ports only, including access and trunk ports.

## 11.12.1 Port Setting

### Click Security > IP Source Guard > Port Setting

	Secur	ity »	IP Sou	rce Gua	ard 》Port	Setting		
<ul> <li>Spanning Tree</li> </ul>								
<ul> <li>Discovery</li> </ul>	Port	Settin	g Table					
✓ Multicast								
✓ Security								Q
RADIUS		Entry	Port	State	Verify Source	Current Entry	Max Entry	,
TACACS+		1	10GE1	Disabled	IP	0	Unlimited	
~ AAA		2	10GE2	Disabled	IP	0	Unlimited	
Authentication Manager		2	10022	Disabled		0	Unlimited	
Port Security		3	10GE3	Disabled	IP	0	Unimited	
Traffic Segmentation		4	10GE4	Disabled	IP	0	Uniimited	
Storm Control		5	10GE5	Disabled	IP	0	Unlimited	
✓ DoS		6	10GE6	Disabled	IP	0	Unlimited	
<ul> <li>Dynamic ARP Inspection</li> </ul>		7	10GE7	Disabled	IP	0	Unlimited	
DHCP Snooping		8	10GE8	Disabled	IP	0	Unlimited	
P Source Guard      Port Sotting		9	10GE9	Disabled	IP	0	Unlimited	
IMPV/ Binding		10	10GE10	Disabled	IP	0	Unlimited	
Save Database		11	10GE11	Disabled	IP	0	Unlimited	
▼ ACL		12	10GE12	Disabled	IP	0	Unlimited	
▼ QoS		13	LAG1	Disabled	IP	0	Unlimited	
<ul> <li>Diagnostics</li> </ul>		14	LAG2	Disabled	IP	0	Unlimited	
Management	n n	15	LAG3	Disabled	IP	0	Unlimited	
		16	LAG4	Disabled	IP	0	Unlimited	
		17	LAG5	Disabled	IP	0	Unlimited	
		18		Disabled	IP	0	Unlimited	
		10		Disabled	" ID	0	Unlimited	
		19		Disabled	IF ID	0	Unlineited	
		20	LAG8	Disabled	IP	0	Unlimited	
		Edit						

Check the port and click "Edit" to edit IP Source Guard for that port.

	Edit Port Setting						
	;;						
	Port	10GE1					
	State	Enable					
	Verify Source	<ul> <li>IP</li> <li>IP-MAC</li> </ul>					
	Max Entry	0 (0 - 50, default 0), 0 is Unlimited					
	Apply C	lose					
Field		Description					
Port		Selected port.					
State		Check to Enable IP Source Guard.					
Verify Sou	urce	Select method: IP or IP-MAC.					
Max Entry	,	Specify the maximum number of dynamic clients that can be learned on given port. This value can be 0-50 (0 means unlimited).					

### 11.12.2 IMPV Binding

Click Security > IP Source Guard > IMPV Binding
	Security » IP Source Guard » IMPV Binding
Discovery     Multicast     Security     RADIUS	IP-MAC-Port-VLAN Binding Table
TACACS+ AAA Management Access	Port VLAN MAC Address IP Address Binding Type Lease Time     O results found.
Port Security Traffic Segmentation	Add Edit Delete First Previous 1 Next Last
Storm Control     DoS     Dynamic ARP Inspection	
<ul> <li>DHCP Snooping</li> <li>IP Source Guard</li> <li>Port Setting</li> </ul>	
IMPV Binding Save Database	

Click "Add" or "Edit" to add or edit a Binding rule.

Port	10GE1 ~	
VLAN		(1 - 4094)
Binding	<ul> <li>IP-MAC-Port-VLAN</li> <li>IP-Port-VLAN</li> </ul>	
MAC Address		]
IP Address		1 255.255.255.255

Field	Description
Port	Select the port.
VLAN	The VLAN ID for the settings.
Binding	Select the binding method: IP-MAC-Port-VLAN or IP-Port-VLAN.
MAC Address	Allowed Source MAC address.
IP Address	Allowed Source IP address.

## 11.12.3 Save Database

Click Security > IP Source Guard > Save Database

	Security >> IP So	urce Guard )>	Save Database	
★ Discovery     ▲				
✓ Multicast		None		
✓ Security	Туре	Flash		
RADIUS		O TETP		
TACACS+ ~ AAA	Filename			
Management Access     Authentication Manager	Address Type	<ul><li>Hostname</li><li>IPv4</li></ul>		
Port Security Traffic Segmentation	Server Address			
Storm Control	Write Delay	300	Sec (15 - 86400, default 300)	
Dynamic ARP Inspection	Timeout	300	Sec (0 - 86400, default 300)	
IP Source Guard     Port Setting     IMPV Binding     Save Database	Apply			

Field	Description
Туре	Select type: None, Flash or TFTP.
Filename	Enter the filename to save database If using TFTP method.
Address Type	Enter the address type to save database If using TFTP method.
Server Address	Enter the server address to save database If using TFTP method.
Write Delay	Specify the write delay time.
Timeout	Specify the timeout.

# Chapter 12 ACL

An Access Control List (ACL) allows you to define classification rules or establish criteria to provide security to your network by blocking unauthorized users and allowing authorized users to access specific areas or resources. ACLs can provide basic security for access to the network by controlling whether packets are forwarded or blocked at the Switch ports. Access Control Lists (ACLs) are filters that allow you to classify data packets according to a particular content in the packet header, such as the source address, destination address, source port number, destination port number, and more. Packet classifiers identify flows for more efficient processing.

Each filter defines the conditions that must match for inclusion in the filter. ACLs (Access Control Lists) provide packet filtering for IP frames (based on the protocol, TCP/UDP port number or frame type) or layer 2 frames (based on any destination MAC address for unicast, broadcast, or multicast, or based on VLAN ID or VLAN tag priority). ACLs can be used to improve performance by blocking unnecessary network traffic or to implement security controls by restricting access to specific network resources or protocols.

Policies can be used to differentiate service for client ports, server ports, network ports, or guest ports. They can also be used to strictly control network traffic by only allowing incoming frames that match the source MAC and source IP address on a specific port. ACLs are composed of Access Control Entries (ACEs), which are rules that determine traffic classifications. Each ACE is a considered as a single rule, and up to 512 rules may be defined on ACLs. ACLs are used to provide traffic flow control, restrict contents of routing updates, and determine which types of traffic are forwarded or blocked. This criterion can be specified on a basis of the MAC address or IP address.

# 12.1 MAC ACL

#### Click ACL > MAC ACL

This page displays the currently-defined MAC-based ACLs profiles. To add a new ACL, enter the name of the new ACL and click **Apply**.

	ACL >> MAC ACL		
✓ Status			
✓ Network			
✓ VLAN			
<ul> <li>MAC Address Table</li> </ul>	Apply		
<ul> <li>Spanning Tree</li> </ul>			
<ul> <li>Discovery</li> </ul>	ACL Table		
✓ Multicast			
✓ Security		Showing 0 to 0 of 0 entries	Q
✓ ACL	ACL Name Rule Port		
MAC ACL		0 results found.	
MAC ACE			First Previous 1 Next Last
IPv4 ACL	Delete		
IPv4 ACE	Delete		
IPv6 ACL			
IPv6 ACE			
ACL Binding			

# 12.2 MAC ACE

#### Click ACL > MAC ACE

Use this page to view and add rules to MAC-based ACLs

		ACE									
✓ Status											
<ul> <li>Network</li> </ul>											
✓ Port	ACE Table										
✓ VLAN	ACL Name test	~									
<ul> <li>MAC Address Table</li> </ul>		1									
<ul> <li>Spanning Tree</li> </ul>	Showing All ~	entries	:	Showing	g 0 to 0 of 0	entries		Q			
<ul> <li>Discovery</li> </ul>			Source M	/AC	Destination MAC	Ethertype V		802.1	D		
✓ Multicast	Sequence Action	Address	Mask	Address	Mask		VLAN Value	Value M	/lask		
✓ Security			<u> </u>		0 results fr	Jund					
→ ACL						Juna.	First	Dravi		Mayt	Last
MAC ACL	Add	Edit	Delete				FIIS	Flevi		Nexi	Lasi
MAC ACE											
IPv4 ACL											
IPv4 ACE											
IPv6 ACL											
IPv6 ACE											
ACL Binding											

Select an ACL Name and click "Add/Edit" to add/edit ACE. Check and click Delete to delete ACEs.

ACL Name	test			
Sequence			(1 - 2147483647)	
Action	<ul> <li>Permit</li> <li>Deny</li> <li>Shutdo</li> </ul>	wn		
Source MAC	Any		1	(Address / Mask)
Destination MAC	✓ Any		1	(Address / Mask)
Ethertype	Any Ox		(0x600 ~ 0xFFFF)	
VLAN	Any	(1 - 4094)		
802.1p	Any		1	(Value / Mask) (0 - 7

Field	Description
ACL Name	The ACL name
Sequence	Enter the sequence number which signifies the order of the specified ACL relative to other ACLs assigned to the selected interface. The valid range is from 1-2147483647, 1 being processed first.
Action	Select what action taken if a packet matches the criteria.

	<ul> <li>Permit – Forward packets that meet the ACL criteria.</li> </ul>
	•Deny – Drops packets that meet the ACL criteria.
	•Shutdown – Shutdown the port that meet the ACL criteria.
Source MAC	Enter a MAC address mask for the source MAC address. A mask of 00:00:00:00:00:00 means the bits must be matched exactly; ff:ff:ff:ff:ff:ff:ff means the bits are irrelevant. Any combination of 0s and ffs can be used.
Destination MAC	Enter a MAC address mask for the destination MAC address. A mask of 00:00:00:00:00:00 means the bits must be matched exactly; ff:ff:ff:ff:ff:ff means the bits are irrelevant. Any combination of 0s and ffs can be used.
Ethertype	Selecting this option instructs the Switch to examine the Ethernet type value in each frame's header. This option can only be used to filter Ethernet II formatted packets. A detailed listing of Ethernet protocol types can be found in RFC 1060. A few of the more common types include 0800 (IP), 0806 (ARP), and 8137 (IPX).
VLAN	Enter the VLAN ID to which the MAC address is attached in MAC ACE. The range is from 1-4094.
802.1p	Enter the 802.1p value. The range is from 0-7.

# 12.3 IPv4 ACL

#### Click ACL > IPv4 ACL

This page displays the currently-defined IPv4-based ACLs profiles. To add a new ACL, enter the name of the new ACL and click **Apply**.

	ACL >>> IPv4 ACL		
✓ Status			
<ul> <li>Network</li> </ul>			
✤ Port			
VLAN			
<ul> <li>MAC Address Table</li> </ul>	Apply		
<ul> <li>Spanning Tree</li> </ul>			
<ul> <li>Discovery</li> </ul>	ACL Table		
✓ Multicast			
✓ Security	Showing All 🗸 entries	Showing 0 to 0 of 0 entries	Q
+ ACL	ACL Name Rule Port		
MAC ACL	the second s	0 results found.	
MAC ACE			First Previous 1 Next Last
IPv4 ACL	Delete		
IPv4 ACE	Delete		
IPv6 ACL			
IPv6 ACE			
ACL Binding			

# 12.4 IPv4 ACE

Click ACL > IPv4 ACE

Use this page to view and add rules to IPv4-based ACLs.

	ACL >> IPv4 ACE
✓ Status	
<ul> <li>Network</li> </ul>	
✓ Port	ACE Table
✓ VLAN	ACL Name allnet V
<ul> <li>MAC Address Table</li> </ul>	
<ul> <li>Spanning Tree</li> </ul>	Showing All v entries Showing 0 to 0 of 0 entries
<ul> <li>Discovery</li> </ul>	Source IP Destination IP Type of Service ICMP
<ul> <li>Multicast</li> </ul>	Source Port Destination Port TCP Flags
<ul> <li>Security</li> </ul>	O results found
↓ ACL	Understandig for the second statement of the second st
MAC ACL	Add Edit Delete
MAC ACE	
IPv4 ACL	
IPv4 ACE	
IPv6 ACL	
IPv6 ACE	
ACL Binding	

Select an ACL Name and click "Add/Edit" to add/edit ACE. Check and click Delete to delete ACEs.

ACL Name	allnet		
Sequence	(1	- 2147483647)	
Action	<ul> <li>Permit</li> <li>Deny</li> <li>Shutdown</li> </ul>		
	Any		
Protocol	O Select ICMP V		
	O Define	(0 - 255)	
	✓ Any		
Source IP	<i>I</i>	(Add	ress / Mask)
	✓ Any		
Destination IP	1	(Add	ress / Mask)
	<ul> <li>Any</li> </ul>		
Type of Service	O DSCP	(0 - 63)	
	O IP Precedence	(0 - 7)	
	<ul> <li>Any</li> </ul>		
Source Port	O Single	(0 - 65535)	
	O Range	-	(0 - 65535)
	<ul> <li>Any</li> </ul>		
Destination Port	O Single	(0 - 65535)	
		_	(0 - 65535)
	Ura: O Set O Unset O I	) Don't care	(,
	Ack: O Set O Unset O I	Don't care	
	Psh: O Set O Unset O	Don't care	
TCP Flags	Rst: 🔿 Set 🔿 Unset 💿 [	Don't care	
	Syn: 🔿 Set 🔿 Unset 💿	Don't care	
	Fin: 🔵 Set 🔵 Unset 💽 🛛	)on't care	
	Any		
ІСМР Туре	O Select Echo Reply	~	
	O Define	(0 - 255)	
ICMB Code	Any		
ICMP Code	O Define	(0 - 255)	

Field	Description					
ACL Name	The ACL name					
Sequence	Enter the sequence number which signifies the order of the specified ACL relative to other ACLs assigned to the selected interface. The valid range is from 1-2147483647, 1 being processed first.					
	Select what action taken if a packet matches the criteria.					
	•Permit – Forward packets that meet the ACL criteria.					
Action	•Deny – Drops packets that meet the ACL criteria.					
	•Shutdown – Shutdown the port that meet the ACL criteria.					
	Select Any, Define, or from the list in the drop down menu.					
Protocol	•Any – Check Any to use any protocol.					
	•Define – Enter the protocol in the ACE to which the packet is matched.					

	<ul> <li>•ICMP – Internet Control Message Protocol (ICMP). The ICMP enables the gateway or destination host to communicate with the source host.</li> <li>•IP in IP – Encapsulates IP packets to create tunnels between two routers. This ensures that IP in IP tunnel appears as a single interface, rather than several separate interfaces. IP in IP enables tunnel intranets occur the internet, and provides an alternative to source routing.</li> <li>•TCP – Transmission Control Protocol (TCP) enables two hosts to communicate and exchange data streams. TCP guarantees packet delivery, and guarantees that packets are transmitted and received in the order they are sent.</li> <li>•EGP – Exterior Gateway Protocol (EGP) permits exchanging routing information between two neighboring gateway hosts in an autonomous systems network.</li> <li>•IDP – Interior Gateway Protocol (IGP) enables a routing information exchange between gateways within an autonomous network.</li> <li>•UDP – User Datagram Protocol (UDP) is a communication protocol that transmits packets but does not guarantee their delivery.</li> <li>•HMP – The Host Mapping Protocol (HMP) collects network information from various networks hosts. HMP monitors hosts spread over the internet as well as hosts in a single network.</li> </ul>
	service for packet-based applications.
	•IPv6 – Matches the packet to the IPv6 protocol.
	·IFV6: FDAC
	•IPV6: FRAG - Fragment Header for IPv6.
	•RVSP – Matches the packet to the ReServation Protocol(RSVP).
	•IPV6: ICMP – The Internet Control Message Protocol (ICMP) allows
	•OSPE – The Open Shortest Path First (OSPE) protocol is a link-state
	hierarchical interior gateway protocol (IGP) for network routing Layer Two (2) Tunneling Protocols. It is an extension to the PPP protocol that enables ISPs operate Virtual Private Networks (VPNs).
	• <b>PIM</b> – Matches the packet to Protocol Independent Multicast (PIM).
	•L2TP – Matches the packet to Internet Protocol (L2TP).
Source IP	Enter the source IP address.
	Select Any DSCP or IP Proceedings from the list. The DSCP range is
Type of Service	from 0-63. The <b>IP Precedence</b> range is from 0-7.
Source Port	Select <b>Any</b> , <b>Single</b> or <b>Range</b> from the list. Enter the source port that is matched to packets. The range is from 0-65535.
Destination Port	Select <b>Any</b> , <b>Single</b> or <b>Range</b> from the list. Enter the destination port that is matched to packets. The range is from 0-65535.
TCP Flags	Set the TCP Flags.
ICMP Type	Select the ICMP Type.
ICMP Code	Enter the ICMP code. The range is from 0-255.

# 12.5 IPv6 ACL

#### Click ACL > IPv6 ACL

This page displays the currently-defined IPv6-based ACLs profiles. To add a new ACL, enter the name of the new ACL and click **Apply**.

	ACL >> IPv6 ACL					
✓ Status						_
✓ Network	ACI Nama					
✓ Port						
<ul> <li>VLAN</li> </ul>	- Annha					
<ul> <li>MAC Address Table</li> </ul>	Арріу					
<ul> <li>Spanning Tree</li> </ul>						
<ul> <li>Discovery</li> </ul>	ACL Table					
<ul> <li>Multicast</li> </ul>	Showing All optrion					
<ul> <li>Security</li> </ul>		Showing 0 to 0 of 0 entries	Q			
→ ACL	ACL Name Rule Port					
MAC ACL		0 results found.				
	-		First Previo	us 1	Next	Last
	Delete					
IPv6 ACL						
IPv6 ACE						
ACL Binding						

# 12.6 IPv6 ACE

#### Click ACL > IPv6 ACE

Use this page to view and add rules to IPv6-based ACLs.

	ACL >> IPv6 ACE
✓ Status	
<ul> <li>Network</li> </ul>	
✓ Port	
<ul> <li>VLAN</li> </ul>	ACL Name test1 ~
<ul> <li>MAC Address Table</li> </ul>	
<ul> <li>Spanning Tree</li> </ul>	Showing All v entries Showing 0 to 0 of 0 entries
<ul> <li>Discovery</li> </ul>	Source IP Destination IP Type of Service ICMP
✓ Multicast	Sequence Action Protocol Address Prefix Address Prefix Source Port Destination Port TCP Flags
<ul> <li>Security</li> </ul>	
✓ ACL	
MAC ACL	Add Edit Delete
MAC ACE	
IPv4 ACL	
IPv4 ACE	
IPv6 ACL	
IPv6 ACE	
ACL Binding	

Select an ACL Name and click "Add/Edit" to add/edit ACE. Check and click Delete to delete ACEs.

#### Add ACE

ACL Name	test1		
Sequence	(1 - 21474	183647)	
Action	<ul> <li>Permit</li> <li>Deny</li> <li>Shutdown</li> </ul>		
Protocol	Any     Select TCP	_	
Source IP	Define     Any	(0 - 255)	(Address / Prefix (0 - 128
Destination IP	✓ Any		(Address / Prefix (0 - 128
Type of Service	Any     DSCP     IP Precedence	(0 - 63)	
Source Port	Any     Single     Range	(0 - 65535)	(0 - 65535)
Destination Port	Any     Single     Range	(0 - 65535)	(0 - 65535)
TCP Flags	Urg:       Set       Unset       Don't ca         Ack:       Set       Unset       Don't ca         Psh:       Set       Unset       Don't ca         Rst:       Set       Unset       Don't ca         Syn:       Set       Unset       Don't ca         Fin:       Set       Unset       Don't ca	are are re are are	
ІСМР Туре	Any     Select Destination Unreachable     Define	(0 - 255)	
ICMP Code	Any     Define	(0 - 255)	

Field	Description					
ACL Name	The ACL name					
Sequence	Enter the sequence number which signifies the order of the specified ACL relative to other ACLs assigned to the selected interface. The valid range is from 1-2147483647, 1 being processed first.					
	Select what action taken if a packet matches the criteria.					
	•Permit – Forward packets that meet the ACL criteria.					
Action	•Deny – Drops packets that meet the ACL criteria.					
	•Shutdown – Shutdown the port that meet the ACL criteria.					

	Select Any, Define, or from the list in the drop down menu.
Protocol	•Any – Check Any to use any protocol.
	•Define – Enter the protocol in the ACE to which the packet is matched.
Source IP	Enter the source IP address.
Destination IP	Enter the destination IP address.
Type of Service	Select Any, DSCP or IP Precedence from the list. The DSCP range is
	from 0-63. The IP Precedence range is from 0-7.
Source Dort	Select Any, Single or Range from the list. Enter the source port that
Source Fort	is matched to packets. The range is from 0-65535.
Dostination Port	Select Any, Single or Range from the list. Enter the destination port
Destination Port	that is matched to packets. The range is from 0-65535.
TCP Flags	Set the TCP Flags.
ІСМР Туре	Select the ICMP Type.
ICMP Code	Enter the ICMP code. The range is from 0-255.

# 12.7 ACL Binding

#### Click ACL > ACL Binding

When an ACL is bound to an interface, all the rules that have been defined for the ACL are applied to that interface. Whenever an ACL is assigned on a port or LAG, flows from that ingress or egress interface that do not match the ACL, are matched to the default rule of dropping unmatched packets. To bind an ACL to an interface, simply select an interface and select the ACL(s) you wish to bind.

	ACL ))		L Bindi	ng				
<ul> <li>Status</li> </ul>								
<ul> <li>Network</li> </ul>	ACL	Bindi	ng Table	•				
✤ Port							~	
✓ VLAN	_						Q,	
<ul> <li>MAC Address Table</li> </ul>		Entry	Port	MAC ACL	IPv4 ACL	IPv6 ACL		
<ul> <li>Spanning Tree</li> </ul>		1	10GE1					
<ul> <li>Discovery</li> </ul>		2	10GE2					
✓ Multicast		3	10GE3					
✤ Security		4	10GE4					
+ ACL		5	10GE5					
MAC ACL		6	10GE6					
		7	10GE7					
		8	10GE8					
IPv6 ACL		9	10GE9					
IPv6 ACE		10	10GE10					
ACL Binding		11	10GE11					
♥ QoS		12	10GE12					
<ul> <li>Diagnostics</li> </ul>		13	LAG1					
<ul> <li>Management</li> </ul>		14	LAG2					
		15	LAG2					
		16	LAG4					
		17	LAG5					
		18	LAG6					
		10	LAGZ					
		20	LAGS					
		20	LAGO					
	В	ind	Unb	nd E	Edit			

Field	Description
Port	Select the port for which the ACLs are bound to.
MAC ACL	The ACL is MAC address based.
IPv4 ACL	The ACL is IPv4 based.
IPv6 ACL	The ACL is IPv6 based.

# Chapter 13 QoS

QoS (Quality of Service) functions to provide different quality of service for various network applications and requirements and optimize the bandwidth resource distribution so as to provide a network service experience of a better quality

# 13.1 General

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

## 13.1.1 Property

#### Click QoS > General > Property

To display QoS property web page.

Q	oS )	) Ger	neral እ	Prop	perty			
✓ Status								
✤ Network		C.	tato 🗖	Enable				
+ Port								
VLAN			0	COS DSCP				
<ul> <li>MAC Address Table</li> </ul>		Trust M	ode O	CoS-DS	SCP			
<ul> <li>Spanning Tree</li> </ul>			Õ	IP Prec	edence			
Discovery	_							
Multicast	4	Apply	J					
Security	Port	t Settin	g Table					
ACL			0					-
QoS								Q
Reperty		Entra	Bort	Cos	Truet		Remark	ing
Queue Scheduling		Entry	Port	Cos	Irust	CoS	DSCP	IP Precedence
CoS Mapping		1	10GE1	0	Enabled	Disabled	Disabled	Disabled
DSCP Mapping		2	10GE2	0	Enabled	Disabled	Disabled	Disabled
IP Precedence Mapping		3	10GE3	0	Enabled	Disabled	Disabled	Disabled
Rate Limit		4	10GE4	0	Enabled	Disabled	Disabled	Disabled
Management		5	10GE5	0	Enabled	Disabled	Disabled	Disabled
Management		6	10GE6	0	Enabled	Disabled	Disabled	Disabled
		7	10GE7	0	Enabled	Disabled	Disabled	Disabled
		8	10GE8	0	Enabled	Disabled	Disabled	Disabled
		9	10GE9	0	Enabled	Disabled	Disabled	Disabled
		10	10GE10	0	Enabled	Disabled	Disabled	Disabled
		11	10GE11	0	Enabled	Disabled	Disabled	Disabled
		12	10GE12	0	Enabled	Disabled	Disabled	Disabled
		13	LAG1	0	Enabled	Disabled	Disabled	Disabled
		14	LAG2	0	Enabled	Disabled	Disabled	Disabled
		15	LAG3	0	Enabled	Disabled	Disabled	Disabled
		16	LAG4	0	Enabled	Disabled	Disabled	Disabled
		17	LAG5	0	Enabled	Disabled	Disabled	Disabled
		18	LAG6	0	Enabled	Disabled	Disabled	Disabled
			1.4.07	0	Enabled	Disabled	Disabled	Disabled
		19	LAG7	U	Enterprote			

Field	Description
State	Set checkbox to enable/disable QoS.

Trust Mode	Select QoS trust mode. <b>CoS</b> : Traffic is mapped to queues based on the CoS field in the VLAN tag, or based on the per-port default CoS value (if there is no VLAN tag on the incoming packet), the actual mapping of the CoS to queue can be configured on port setting dialog. <b>DSCP</b> : All IP traffic is mapped to queues based on the DSCP field in the IP header. The actual mapping of the DSCP to queue can be configured on the DSCP mapping page. If traffic is not IP traffic, it is mapped to the best effort queue. <b>CoS-DSCP</b> : 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.
Field	Description
Port	Port name
CoS	Port default CoS priority value for the selected ports.
Trust	Port trust state <b>Enable</b> : Traffic will follow trust mode in global setting. <b>Disable</b> : Traffic will always use best efforts.
Remarking (CoS)	Port CoS remarking admin state. Enable: CoS remarking is enabled Disable: CoS remarking is disabled
Remarking (DSCP)	Port DSCP remarking admin state. Enable: DSCP remarking is enabled Disable: DSCP remarking is disabled
Remarking (IP Precedence)	Port IP Precedence remarking admin state. <b>Enable</b> : IP Precedence remarking is enabled <b>Disable</b> : IP Precedence remarking is disabled

### Click "Edit" to edit the QoS port setting.

Edit Port Setting

Port	10GE1
CoS	0 (0 - 7)
Trust	Enable
Remarking CoS	
DSCP	
IP Precedence	Enable

	Close
--	-------

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

## 13.1.2 Queue Scheduling

#### Click QoS > General > Queue Scheduling

To display Queue Scheduling web page.

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 mode 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).

C	QoS »	General 🔀	Queu	e Sche	duling		
<ul> <li>Status</li> </ul>							
<ul> <li>Network</li> </ul>	0	Cohoduling '	Tabla				
✓ Port							
• VLAN				Method			
<ul> <li>MAC Address Table</li> </ul>	Queue	Strict Priority	WRR	Weight	WRR Bandwidth (%)		
<ul> <li>Spanning Tree</li> </ul>	1	۲	0	1			
<ul> <li>Discovery</li> </ul>	2	0	0	2			
<ul> <li>Multicast</li> </ul>	3	0	0	3			
✤ Security	4	0	0	4			
✓ ACL	5	0	0	5			
→ QoS	6	0	0	9			
General	7	0	õ	13			
Property Queue Scheduling	8	0	0	15			
CoS Mapping		<u> </u>	0	1.000			
DSCP Mapping	Appl	у					
IP Precedence Mapping							
✓ Rate Limit							
Field	Des	scription					

Field	Description
Queue	Queue ID to configure
Strict Priority	Set queue to strict priority type
WRR	Set queue to Weight Round Robin type.
Weight	If the queue type is WRR, set the queue weight for the queue.

## 13.1.3 CoS Mapping

#### Click QoS > General > CoS Mapping

To display CoS Mapping web page.

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

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

	QoS >> General >> CoS Mapping					
✓ Status	CoS to Queue Manning					
<ul> <li>Network</li> </ul>	Cos to Queue Mapping					
✓ Port	CoS Queue					
VLAN	0 2 -					
MAC Address Table	1 1 -					
Spanning Tree	2 3 ~					
<ul> <li>Discovery</li> <li>Multicast</li> </ul>	3 4 ~					
Security	4 5 ~					
ACL	5 6 ~					
- QoS	6 7 -					
General	7 8 -					
Property	Apply					
Queue Scheduling	, app y					
DSCP Mapping	Queue to CoS Mapping					
IP Precedence Mapping						
<ul> <li>Rate Limit</li> </ul>	Queue CoS					
<ul> <li>Diagnostics</li> </ul>	1 1 -					
<ul> <li>Management</li> </ul>	2 0 ~					
	3 2 -					
	4 3 ~					
	5 4 -					
	6 <u>5</u> ~					
	7 6 -					
	8 7 ~					
	Apply					
Field	Description					
CoS	CoS value					
Queue	Select queue ID for the CoS value					
Field	Description					
Queue	Queue ID					
CoS	Select CoS value for the queue ID					

## 13.1.4 DSCP Mapping

#### Click QoS > General > DSCP Mapping

To display DSCP Mapping web page.

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

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

	QoS >> General >>	DSCP Mapp	ing		
• Status	DSCP to Queue M	lapping			
Network		apping			
• Port	DSCP Queue	DSCP Queue	DSCP Queue	DSCP (	Queue
VLAN	0 [CS0] 1 🗸	16 [CS2] 3 🗸	32 [CS4] 5 🗸	48 [CS6]	7 🗸
MAC Address Table     Spapping Tree	1 1 -	17 3 🗸	33 5 ~	49	7 🗸
	2 1 -	18 [AF21] 3 🗸	34 [AF41] 5 🗸	50	7 v
• Discovery	3 1 -	19 3 🗸	35 5 ~	51	7 🗸
Security	4 1 - 3	20 [AF22] 3 🗸	36 [AF42] 5 🗸	52	7 🗸
<ul> <li>ACI</li> </ul>	5 1 - 2	21 3 ~	37 5 ~	53	7 🗸
- 00S	6 1 🗸 🖯	22 [AF23] 3 🗸	38 [AF43] 5 🗸	54	7 🗸
General	7 1 🗸	23 3 ~	39 5 ~	55	7 🗸
Property	8 [CS1] 2 🗸 🗧	24 [CS3] 4 🗸	40 [CS5] 6 v	56 [CS7]	8 🗸
Queue Scheduling	9 2 🗸	25 4 ~	41 6 ~	57	8 🗸
CoS Mapping	10 [AF11] 2 🗸 🗧	26 [AF31] 4 🗸	42 6 🗸	58	8 🗸
DSCP Mapping	11 2 - 2	27 4 🗸	43 6 ~	59	8 🗸
Rate Limit	12 [AF12] 2 🗸	28 [AF32] 4 🗸	44 6 ~	60	8 🗸
Diagnostics	13 2 - 2	29 4 🗸	45 6 ~	61	8 🗸
<ul> <li>Management</li> </ul>	14 [AF13] 2 🗸 🗧	30 [AF33] 4 🗸	46 [EF] 6 🗸	62	8 🗸
	15 2 -	31 4 🗸	47 6 🗸	63	8 🗸
	Apply           Queue to DSCP M           1         0 [CS0]           2         8 [CS1]           3         16 [CS2]           4         24 [CS3]           5         32 [CS4]           6         40 [CS5]           7         48 [CS6]           8         56 [CS7]           Apply	lapping			
	Description				
	DSCP value				
e	Select Queue I	D for DSC	P value.		
	Description				

## 13.1.5 IP Precedence Mapping

Field Queue

DSCP

### Click QoS > General > IP Precedence Mapping

Queue ID

To display IP Precedence Mapping web page.

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

Select DSCP value for Queue ID.

	QoS >> General >> IP Precedence Mapping						
Status							
Network	IP Precedence to Queue Mapping						
• Port	IP Precedence Queue						
VLAN							
MAC Address Table							
<ul> <li>Spanning Tree</li> </ul>							
Discovery	2 3 3						
Multicast	3 4 ~						
Security	4 5 ~						
ACL	5 6 ~						
QoS	6 7 -						
General	7 8 ~						
Property							
Queue Scheduling	Apply						
CoS Mapping							
DSCP Mapping	Queue to IP Precedence Mapping						
IP Precedence Mapping							
	Ououo IB Procodonco						
<ul> <li>Rate Limit</li> </ul>							
Rate Limit Diagnostics							
Rate Limit Diagnostics Management							
Rate Limit Diagnostics Management	1 0 v 2 1 v 3 2 v						
Rate Limit Diagnostics Management	$ \begin{array}{c ccccccccccccccccccccccccccccccccccc$						
Rate Limit Diagnostics Management	$ \begin{array}{c ccccccccccccccccccccccccccccccccccc$						
Rate Limit Diagnostics Management	$ \begin{array}{c ccccc} 1 & 0 & \cdot \\ \hline 1 & 0 & \cdot \\ 2 & 1 & \cdot \\ 3 & 2 & \cdot \\ 4 & 3 & \cdot \\ 5 & 4 & \cdot \\ 6 & 5 & \cdot \\ \end{array} $						
Rate Limit     Diagnostics     Management	$ \begin{array}{c ccccc} 1 & 0 & \cdot \\ \hline 1 & 0 & \cdot \\ 2 & 1 & \cdot \\ 3 & 2 & \cdot \\ 4 & 3 & \cdot \\ 5 & 4 & \cdot \\ 6 & 5 & \cdot \\ 7 & 6 & \times \\ \end{array} $						
Rate Limit     Diagnostics     Management	$ \begin{array}{c ccccccccccccccccccccccccccccccccccc$						
Rate Limit     Diagnostics     Management	$ \begin{array}{c ccccccccccccccccccccccccccccccccccc$						

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

# 13.2 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.

## 13.2.1 Ingress / Egress Port

### Click QoS > Rate Limit > Ingress/Egress

To display Ingress/Egress Port web page.

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

QoS » Rate Limit » Ingress / Egress Port									
✤ Status	Ingrass / Egrass Port Table								
Network	Ingress / Egress Fort lable								
✓ Port							0		
✓ VLAN							4		
<ul> <li>MAC Address Table</li> </ul>		Entry	Port	In	gress	E	gress		
<ul> <li>Spanning Tree</li> </ul>		,	1 on	State	Rate (Kbps)	State	Rate (Kbps)		
<ul> <li>Discovery</li> </ul>		1	10GE1	Disabled		Disabled			
<ul> <li>Multicast</li> </ul>		2	10GE2	Disabled		Disabled			
<ul> <li>Security</li> </ul>		3	10GE3	Disabled		Disabled			
✓ ACL		4	10GE4	Disabled		Disabled			
		5	10GE5	Disabled		Disabled			
✓ General		6	10GE6	Disabled		Disabled			
Rate Limit		7	10GE7	Disabled		Disabled			
Egress Queue		8	10GE8	Disabled		Disabled			
		9	10GE9	Disabled		Disabled			
<ul> <li>Management</li> </ul>		10	10GE10	Disabled		Disabled			
- Management		11	10GE10	Disabled		Disabled			
		12	10GE12	Disabled		Disabled			
		12	IUGE12	Disabled		Disabled			
	E E	Edit							

Field	Description
Port	Port name
	Port ingress rate limit state
Ingress (State)	Enable: Ingress rate limit is enabled.
_	Disable: Ingress rate limit is disabled.
Ingress (Rate)	Port ingress rate limit value if ingress rate state is enabled.
	Port egress rate limit state
Egress (State)	Enable: Egress rate limit is enabled.
	Disable: Egress rate limit is disabled.
Egress (Rate)	Port egress rate limit value if egress rate state is enabled.

Click "Edit" to edit Ingress/Egress Port.

Port	10GE1		
narooo	Enable		
ngress	1000000	Kbps (16 - 1000000)	
_	Enable		
Egress	1000000	Kbps (16 - 1000000)	

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

# 13.2.2 Egress Queue

Click QoS > Rate Limit > Egress Queue

To display Egress Queue web page.

Egress rate limiting is performed by shaping the output load.

QoS >> Rate Limit >> Egress Queue																			
<ul> <li>Status</li> <li>Network</li> </ul>	Egress Queue Table																		
✓ Port								Q											
MAC Address Table		Entry	Port	Qu	ieue 1	Qu	eue 2	Qu	eue 3	Qu	eue 4	Qu	eue 5	Qu	eue 6	Qu	eue 7	Qu	eue 8
<ul> <li>Spanning Tree</li> </ul>		Linuy	TOIL	State	CIR (Kbps)														
<ul> <li>Discovery</li> </ul>		1	10GE1	Disabled															
<ul> <li>Multicast</li> </ul>		2	10GE2	Disabled															
<ul> <li>Security</li> </ul>		3	10GE3	Disabled															
⋆ ACL		4	10GE4	Disabled															
✓ QoS		5	10GE5	Disabled															
<ul> <li>General</li> </ul>		6	10GE6	Disabled															
<ul> <li>Rate Limit</li> </ul>		7	10GE7	Disabled															
Ingress / Egress Port		8	10GE8	Disabled															
Egress Quede		9	10GE9	Disabled															
Management		10	10GE10	Disabled															
Management		11	10GE11	Disabled															
		12	10GE12	Disabled															
		Edit																	

Field	Description
Port	Port name
	Port egress queue 1 rate limit state.
Queue 1 (State)	Enable: Egress queue rate limit is enable.
	<b>Disable</b> : Egress queue rate limit is disable.
Queue 1 (CIR)	Queue 1 egress committed information rate.
	Port egress queue 2 rate limit state.
Queue 2 (State)	Enable: Egress queue rate limit is enable.
	<b>Disable</b> : Egress queue rate limit is disable.
Queue 2 (CIR)	Queue 2 egress committed information rate.
	Port egress queue 3 rate limit state.
Queue 3 (State)	Enable: Egress queue rate limit is enable.
	<b>Disable</b> : Egress queue rate limit is disable.
Queue 3 (CIR)	Queue 3 egress committed information rate.
	Port egress queue 4 rate limit state.
Queue 4 (State)	Enable: Egress queue rate limit is enable.
	<b>Disable</b> : Egress queue rate limit is disable.
Queue 4 (CIR)	Queue 4 egress committed information rate.
	Port egress queue 5 rate limit state.
Queue 5 (State)	Enable: Egress queue rate limit is enable.
	<b>Disable</b> : Egress queue rate limit is disable.
Queue 5 (CIR)	Queue 5 egress committed information rate.
	Port egress queue 6 rate limit state.
Queue 6 (State)	Enable: Egress queue rate limit is enable.
	<b>Disable</b> : Egress queue rate limit is disable.
Queue 6 (CIR)	Queue 6 egress committed information rate.
	Port egress queue 7 rate limit state.
Queue 7 (State)	<b>Enable</b> : Egress queue rate limit is enable.
	<b>Disable</b> : Egress queue rate limit is disable.
Queue 7 (CIR)	Queue 7 egress committed information rate.
	Port egress queue 8 rate limit state.
Queue 8 (State)	<b>Enable</b> : Egress queue rate limit is enable.
	<b>Disable</b> : Egress queue rate limit is disable.
Queue 8 (CIR)	Queue 8 egress committed information rate.

Port	10GE1		
	Enable		
Queue 1	1000000	Kbps (16 - 1000000)	
_	Enable		
Queue 2	1000000	Kbps (16 - 1000000)	
	Enable		
Queue 3	1000000	Kbps (16 - 1000000)	
	Enable		
Queue 4	1000000	Kbps (16 - 1000000)	
	Enable		
Queue 5	1000000	Kbps (16 - 1000000)	
	Enable		
Queue 6	1000000	Kbps (16 - 1000000)	
	Enable		
Queue 7	1000000	Kbps (16 - 1000000)	
	Enable		
Queue 8	1000000	Kbps (16 - 1000000)	

Apply Close

Field	Description
Port	Select port list
0	Set checkbox to enable/disable egress queue 1 rate limit. If egress rate
Queue	limit is enabled, rate limit value need to be assigned.
0	Set checkbox to enable/disable egress queue 2 rate limit. If egress rate
Queue 2	limit is enabled, rate limit value need to be assigned.
0	Set checkbox to enable/disable egress queue 3 rate limit. If egress rate
Queue 5	limit is enabled, rate limit value need to be assigned.
	Set checkbox to enable/disable egress queue 4 rate limit. If egress rate
Queue 4	limit is enabled, rate limit value need to be assigned.
	Set checkbox to enable/disable egress queue 5 rate limit. If egress rate
Queue 5	limit is enabled, rate limit value need to be assigned.
	Set checkbox to enable/disable egress queue 6 rate limit. If egress rate
Queue o	limit is enabled, rate limit value need to be assigned.
	Set checkbox to enable/disable egress queue 7 rate limit. If egress rate
Queue /	limit is enabled, rate limit value need to be assigned.
	Set checkbox to enable/disable egress queue 8 rate limit. If egress rate
	limit is enabled, rate limit value need to be assigned.

# Chapter 14 Diagnostics

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

# 14.1 Logging

## 14.1.1 Property

#### Click Diagnostics > Logging > Property

To display the Logging Service web page.

	Diagnostics >>> Logging >>> Property
✓ Status	
<ul> <li>Network</li> </ul>	State V Enable
✓ Port	
• VLAN	Console Logging
<ul> <li>MAC Address Table</li> </ul>	State 🗹 Enable
<ul> <li>Spanning Tree</li> </ul>	Minimum Notice ×
<ul> <li>Discovery</li> </ul>	Severity
✓ Multicast	Note: Emergency, Alert, Critical, Error, Warning, Notice
✤ Security	RAM Logging
✤ ACL	
♥ QoS	
✓ Diagnostics	Minimum Notice V
<ul> <li>Logging</li> </ul>	Note: Emergency, Alert, Critical, Error, Warning, Notice
Property	
Remote Server	Flash Logging
Pina	State Enable
Traceroute	Minimum Notice V
Fiber Module	Severity
✓ UDLD	Hote: Energeney, Alert, Shadar, Errol, Hanning, House
<ul> <li>Management</li> </ul>	Apply
ld [	Description
ite E	Enable/Disable the global logging services. When the logging services enabled, logging configuration of each destination rule can be ndividually configured. If the logging service is disabled, no messawill be sent to these destinations.

#### Console Logging

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

#### RAM Logging

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

Flash Logging

Field	Description

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

## 14.1.2 Remote Server

Click Diagnostics > Logging > Remote Server

To display the Remote Logging Server web page.

	Diagnostics >> Logging >> Remote Server							
✓ Status								
<ul> <li>Network</li> </ul>	Remote Server Table							
• Port								
VLAN	Q							
MAC Address Table     Spapping Tree								
Discovery	Entry Server Address Server Port Facility Severity							
<ul> <li>✓ Multicast</li> </ul>	0 results found.							
✓ ACL								
♥ QoS								
✓ Diagnostics								
Logging								
Property Remote Server								
Field	Description							
	The ID eddress of the remete langing company							
Server Address	The P address of the remote logging server.							
Server Ports	The point number of the leading meanages. It can be one of the following							
Facility	values: local0, local1, local2, local3, local4, local5, local6, and local7.							
	The 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.							
Sovority	Warning: System warning has occurred.							
Severity	Warning: System warning has occurred.							
Severity	<b>Warning</b> : System warning has occurred. <b>Notice</b> : System is functioning properly, but a system notice has							
Severity	Warning: System warning has occurred. Notice: System is functioning properly, but a system notice has occurred.							
Severity	<ul> <li>Warning: System warning has occurred.</li> <li>Notice: System is functioning properly, but a system notice has occurred.</li> <li>Informational: Device information.</li> </ul>							

# 14.2 Mirroring

#### Click **Diagnostics > Mirroring**

To display the Port Mirroring web page.

Diagnostics » Mirroring						
✓ Status						
✓ Network	Minu	ania a Tabl	_			
✤ Port	WIIII	oring labi	e			
✓ VLAN						0
<ul> <li>MAC Address Table</li> </ul>	_					4
<ul> <li>Spanning Tree</li> </ul>		Session ID	State	Monitor Port	Ingress Port	Egress Port
• Discovery	0	1	Disabled			
✓ Multicast	0	2	Disabled			
✤ Security	0	3	Disabled			
• ACL	0	4	Disabled			
		)				
- Diagnostics		Edit				
Logging     Mirroring     Bicc		*" Allow the m	onitor port to	o send or receive	normal packets	

Field	Description
Session ID	Select mirror session ID
	Select mirror session state : port-base mirror or disable
State	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.

# 14.3 Ping

## Click Diagnostics > Ping

To display the Diagnostic Ping functionality web page.

	Diagnostics )) Ping						
<ul> <li>Status</li> </ul>							
<ul> <li>Network</li> </ul>							
<ul> <li>Port</li> </ul>	Address Type O IPv4						
✓ PoE	IPv6						
<ul> <li>VLAN</li> </ul>	Sarvar Addrass						
<ul> <li>MAC Address Table</li> </ul>							
<ul> <li>Spanning Tree</li> </ul>	User Defined						
<ul> <li>Discovery</li> </ul>	4 Sec (1 - 65535)						
<ul> <li>Multicast</li> </ul>							
<ul> <li>Security</li> </ul>	Ping Stop						
<ul> <li>ACL</li> </ul>							
<ul> <li>QoS</li> </ul>	Ping Result						
<ul> <li>Logging</li> </ul>	Dackot Status						
Mirroring							
Traceroute	Status IV/A						
Copper Test	Transmit Packet 0						
Fiber Module	Receive Packet 0						
<ul> <li>UDLD</li> </ul>	Packet Lost 0%						
<ul> <li>Management</li> </ul>							
	Round Trip Time						
	Min 0.0 ms						
	Max 0.0 ms						
	Δverage 0.0 ms						
	Average 0.0 ms						
Field	Description						
Address Type	Specify the address type to "Hostname", "IPv4", or "IPv6".						
Server Address	Specify the Hostname/IPv4/IPv6 address for ping diagnostics.						
Count	Specify the numbers of each ICMP ning request						

# 14.4 Traceroute

#### Click Diagnostics > Traceroute

To display the Diagnostic Traceroute functionality web page.

	Diagnostics )) Traceroute					
✓ Status						
Vetwork	Hostname					
✤ Port	Address Type					
VLAN	Server Address					
MAC Address Table						
<ul> <li>Spanning Tree</li> <li>Discovery</li> </ul>	Time to Live					
<ul> <li>Discovery</li> <li>Multicast</li> </ul>	30 (2 - 255, default 30)					
Security	Anth					
* ACL	Appiy					
↓ QoS	Traceroute Result					
- Diagnostics						
Logging						
Mirroring						
Traceroute						
Fiber Module						
v UDLD						
ield	Description					
Address Type	Specify the address type to "Hostname" or "IPv4".					
Server Address	Specify the Hostname/IPv4 address for traceroute diagnostics					
Fime to Live	Specify the numbers of Time to Live					

# 14.5 Fiber Module

#### Click Diagnostics > Fiber Module

To display the fiber module.

	Diagnostics >> Fiber Module									
✓ Status		Eiha	r Madul	a Tabla						
<ul> <li>Network</li> </ul>		FIDe	rwodul	e lable						
✤ Port									0	
✓ VLAN									4	
<ul> <li>MAC Address Table</li> </ul>			Port	Temperature (C)	Voltage (V)	Current (mA)	Output Power (mW)	Input Power (mW)	OE Present	Loss of Signal
<ul> <li>Spanning Tree</li> </ul>		0	10GE1	N/S	N/S	N/S	N/S	N/S	Insert	Normal
✤ Discovery		0	10GE2	N/S	N/S	N/S	N/S	N/S	Insert	Normal
<ul> <li>Multicast</li> </ul>		0	10GE3	N/A	N/A	N/A	N/A	N/A	Remove	Loss
<ul> <li>Security</li> </ul>		0	10GE4	N/S	N/S	N/S	N/S	N/S	Insert	Normal
* ACL		0	10GE5	N/A	N/A	N/A	N/A	N/A	Remove	Loss
♥ QoS		0	10GE6	N/A	N/A	N/A	N/A	N/A	Remove	Loss
		0	10GE7	N/A	N/A	N/A	N/A	N/A	Remove	Loss
<ul> <li>Logging</li> </ul>		0	10GE8	N/A	N/A	N/A	N/A	N/A	Remove	Loss
Mirroring		0	10GE9	N/A	N/A	N/A	N/A	N/A	Remove	Loss
Ping Traceroute		0	10GE10	N/A	N/A	N/A	N/A	N/A	Remove	Loss
Fiber Module		0	10GE11	N/A	N/A	N/A	N/A	N/A	Remove	Loss
VDLD		0	10GE12	N/A	N/A	N/A	N/A	N/A	Remove	Loss
<ul> <li>Management</li> </ul>		_								
		R	efresh	Detail						



# 14.6 UDLD

**Unidirectional Link Detection (UDLD)** is a data link layer protocol from Cisco Systems to monitor the physical configuration of the cables and detect unidirectional links.

Unidirectional Link failure can cause "traffic blackholing" and loop in the Switch topology.

In order to detect the unidirectional links before the forwarding loop is created, UDLD works by exchanging protocol packets between the neighboring devices. In order for UDLD to work, both switch devices on the link must support UDLD and have it enabled on respective ports.

## 14.6.1 Property

#### Click Diagnostics > UDLD > Property

To view the UDLD status and set up UDLD mode.

	Diagn	iostic	s » UC	DLD >> P	Property			
✓ Status								
✓ Network	-			45	0			
✓ Port		wessag	e lime	15	Sec (1 - 90	J, delault 15)		
✓ VLAN			ו					
<ul> <li>MAC Address Table</li> </ul>		ърру	J					
<ul> <li>Spanning Tree</li> </ul>								
<ul> <li>Discovery</li> </ul>	Port	Settir	ng Table					
<ul> <li>Multicast</li> </ul>							0	
✓ Security							Q	
✓ ACL		Entry	Port	Mode	Bidirectional State	Operational Status	Neighbor	
v QoS		1	10GE1	Disabled	Unknown		0	
✓ Diagnostics		2	10GE2	Disabled	Unknown		0	
<ul> <li>Logging</li> <li>Missocia -</li> </ul>		3	10GE3	Disabled	Unknown		0	
Ping		4	10GE4	Disabled	Unknown		0	
Traceroute		5	10GE5	Disabled	Unknown		0	
Fiber Module		6	10GE6	Disabled	Unknown		0	
<ul> <li>UDLD</li> </ul>		7	10GE7	Disabled	Unknown		0	
Property		8	10GE8	Disabled	Unknown		0	
Management		9	10GE9	Disabled	Unknown		0	
• management		10	10GE10	Disabled	Unknown		0	
		11	10GE11	Disabled	Unknown		0	
		12	10GE12	Disabled	Unknown		0	
		<b>F</b> 111	7					
		Edit						
d	Desc	cript	ion					
	Agin	d of	ם וסט	inforr	nation hann	ens when th	e nort	that runs UDI
	doco	not	rocci		D packete t	from the nei	abbor	ort for duratio
	ubes		Tecel					
ssage Time	hold	time	. The	hold ti	me for the p	ort is dictate	ed by tl	ne remote por
sage mile	depe	ends	on the	e Mes	sage Time a	at the remot	e side.	The shorter t
	Mess	sade	Time	. the s	horter the h	old time and	I the fa	ster the detec
	The	rana			na Tima is fr	om 1 00 Dr	foult ic	15 seconds
	Ine	rang		เธรรฐกิ		0111 1-90. DE	siduit IS	s to seconds.

Check and click "Edit" to edit UDLD mode.

t Port Se	tting
Port	10GE1
Mode	<ul> <li>Disabled</li> <li>Normal</li> <li>Aggressive</li> </ul>
Apply	Close

Field	Description
Port	The interface for UDLD.

	<b>Disabled</b> : The UDLD function is disabled. <b>Normal</b> : In normal mode, if the link state of the port was determined to be bi-directional and the UDLD information times out, no action is taken
Mode	by UDLD. The port state for UDLD is marked as undetermined. The port behaves according to its STP state. <b>Aggressive</b> : In aggressive mode, if the link state of the port is determined to be bi-directional and the UDLD information times out while the link on the port is still up UDLD tries to re-establish the state
	of the port. If not successful, the port is put into the Error Disabled state.

# 14.6.2 Neighbor

## Click **Diagnostics** > **UDLD** > **Neighbor**

To view the UDLD neighbor status.

	Diagno	stics )> U	IDLD >> Neighbor						
Status     Network     Port	Neighl	bor Table							
<ul> <li>VLAN</li> <li>MAC Address Table</li> </ul>							Q		
Spanning Tree     Discovery	Entry	Expiration Time	Current Neighbor State	Device ID	Device Name	Port ID	Message Interval	Timeout Interval	
<ul> <li>Multicast</li> </ul>				0 results	found.	,		· /	
<ul> <li>Security</li> <li>ACL</li> <li>QoS</li> </ul>	Refre	esh							
Diagnostics     Logging     Mirroring     Ping     Traceroute     Fiber Module									
Property Neighbor									

# Chapter 15 Management

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

# 15.1 User Account

#### Click Management > User Account

The default username/password is admin/admin. And default account is not able to be deleted. Use this page to add additional users that are permitted to manage the switch or to change the passwords of existing users.

	Management )) User Account
✓ Network	Hear Assount
<ul> <li>Port</li> </ul>	User Account
VLAN	Showing All v entries Showing 1 to 1 of 1 entries
<ul> <li>MAC Address Table</li> </ul>	
<ul> <li>Spanning Tree</li> </ul>	Username Privilege
Discovery	admin Admin
Multicast	First Previous 1 Next La
Security	Add Edit Delete
ACL	
v QoS	
<ul> <li>Diagnostics</li> </ul>	
✓ Management	
User Account	
<ul> <li>Firmware</li> </ul>	
Configuration	
- SNMP - BMON	

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

Click "Add" or "Edit" to add/edit User Account.

ld User Account	
Username	
Password	
Confirm Password	
Privilege	<ul> <li>Admin</li> <li>User</li> </ul>

Apply Close

Field	Description	
Username	User name of the account.	
Password	Set password of the account.	
<b>Confirm Password</b> Set the same password of the account as in "Password" field		
	Select privilege level for new account.	
Privilago	Admin: Allow to change switch settings. Privilege value equals to 15.	
Flivliege	<b>User</b> : See switch settings only. Not allow to change it. Privilege level	
	equals to 1.	

# 15.2 Firmware

# 15.2.1 Upgrade / Backup

### Click Management > Firmware > Upgrade/Backup

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

	Management )) Firmware )) Upgrade / Backup	
<ul> <li>Status</li> </ul>		
<ul> <li>Network</li> </ul>	Upgrade	1
• Port	Action Backup	
• VLAN	■ TETP	1000
<ul> <li>MAC Address Table</li> </ul>	Method   HTTP	
<ul> <li>Spanning Tree</li> </ul>	Filename Deserve Ma file selected	1
<ul> <li>Discovery</li> </ul>	BIOWSE No life selected.	
<ul> <li>Multicast</li> </ul>	Annly	
<ul> <li>Security</li> </ul>		
✤ ACL		
👻 QoS		
<ul> <li>Diagnostics</li> </ul>		
<ul> <li>Management</li> </ul>		
User Account		
Firmware		
Upgrade / Backup		
Active Image		
SNMP		
RMON		

#### Upgrade Firmware through HTTP

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

### Upgrade Firmware through TFTP.

Field	Description
	Firmware operations
Action	<b>Upgrade</b> : Upgrade firmware from remote host to DUT.
	Backup: Backup firmware image from DUT to remote host.
	Firmware upgrade/backup method
Method	<b>TFTP</b> : Using TFTP to upgrade/backup firmware.
	HTTP: Using WEB browser to upgrade/backup firmware.
	Specify TFTP server address type
Address Type	Hostname: Use domain name as server address.
Address Type	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

#### Backup Firmware through HTTP

	Field	Description

	Firmware operations
Action	<b>Upgrade</b> : Upgrade firmware from remote host to DUT.
	Backup: Backup firmware image from DUT to remote host.
	Firmware upgrade/backup method
Method	<b>TFTP</b> : Using TFTP to upgrade/backup firmware.
	HTTP: Using WEB browser to upgrade/backup firmware.
	Select which image file to backup.
Firmware	Image0: backup image0.
	Image1: backup image1.

Field	Description
	Firmware operations
Action	<b>Upgrade</b> : Upgrade firmware from remote host to DUT.
	Backup: Backup firmware image from DUT to remote host.
	Firmware upgrade/backup method
Method	<b>TFTP</b> : Using TFTP to upgrade/backup firmware.
	HTTP: Using WEB browser to upgrade/backup firmware.
	Select which image file to backup.
Firmware	Image0: backup image0.
	Image1: backup image1.
	Specify TFTP server address type
Addross Type	Hostname: Use domain name as server address
Address Type	IPv4: Use IPv4 as server address
	IPv6: Use IPv6 as server address
Server Address	Specify TFPT server address
Filename	File name saved on remote TFTP server

# 15.2.2 Active Image

## Click Management > Firmware > Active Image

This page allows user to select firmware image.

Active Image	Image0     Image1
Active Image	Image0     Image1
Active Image	Image1
	Note: the image was selected for the next boot
Active Image	
Firmware	Image0
Version	1.0.1
Name	
Size	8627/13/ Butee
Size	002/454 Bytes
Created	2021-11-10 09:57:26
Backup Image	
Firmware	Image1
Version	1.0.1
Name	
Size	8627434 Butes
Created	0021 40 4 000-57-26
Created	2021-11-10 09:57:26
Apply	
cription	
	Size Created Backup Image Firmware Version Name Size Created

	<b>Firmware</b> : Image0 or Image1 <b>Version</b> : The firmware version of this image.
Active/Backup Image	Name: The filename of this image.
	Size: The file size of this image.
	Created: The date when this image created.

# **15.3 Configuration**

## 15.3.1 Upgrade / Backup

### Click Management > Configuration > Upgrade/Backup

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

nagement >>	Configuration >> Upgrade / Backup
Action	Opgrade
ACUUII	🔘 Backup
Method	◎ TFTP
Metilou	ITTP
	Running Configuration
Configuration	Startup Configuration
	Backup Configuration     BAM Log
	Slash Log
Filonomo	
riiename	Browse No file selected.
Anntu	
Арріу	
	Action Method Configuration Filename

### Upgrade Configuration through HTTP

Field	Description		
	Configuration operations		
Action	<b>Upgrade</b> : Upgrade Configuration from remote host to DUT.		
	Backup: Backup Configuration image from DUT to remote host.		
Method	Configuration upgrade/backup method		
	<b>TFTP</b> : Using TFTP to upgrade/backup Configuration.		
	HTTP: Using WEB browser to upgrade/backup Configuration.		
	Configuration types		
Configuration	Running Configuration: Merge to current running configuration file.		
Configuration	<b>Startup Configuration</b> : Replace the startup configuration file.		
	Backup Configuration: Replace the backup configuration file.		
Filonomo	Use browser to upgrade Configuration, you should select		
Гпепапе	Configuration image file on your host PC.		

#### Upgrade Configuration through TFTP.

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

Configuration	Configuration types <b>Running Configuration</b> : Merge to current running configuration file <b>Startup Configuration</b> : Replace the startup configuration file. <b>Backup Configuration</b> : Replace the backup configuration file.		
Address Type         Dackup Comgutation: Replace the backup comigutation           Address Type         Specify TFTP server address type           Hostname: Use domain name as server address.         IPv4: Use IPv4 as server address			
IPv6: Use IPv6 as server address           Server Address         Specify TFTP server address.			
Filename	Configuration image file name on remote TFTP server		

## Backup Configuration through HTTP

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

### Backup Configuration through TFTP.

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

# 15.3.2 Save Configuration

Click Management > Configuration > Save Configuration

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

	Management >> Configuration >> Save Configuration
	Running Configuration
✓ Port	Source File Startup Configuration
VLAN	Backup Configuration
• MAC Address Table	Startup Configuration
<ul> <li>Spanning Tree</li> </ul>	Destination File Backup Configuration
<ul> <li>Discovery</li> </ul>	
✓ Multicast	Apply Restore Factory Default
<ul> <li>Security</li> </ul>	
• ACL	
<ul> <li>Diagnostics</li> </ul>	
- Management	
User Account	
<ul> <li>Firmware</li> </ul>	
<ul> <li>Configuration</li> </ul>	
Upgrade / Backup	
Save Configuration	
Field	Description
	Source file types
	<b>Running Configuration:</b> Copy running configuration file to destination
Source File	Startup Configuration Copy startup configuration file to destination
	Backup Configuration: Copy backup configuration file to destination
	Destination file
Destination File	Startun Configuration: Save file on startun configuration
	<b>Startup Configuration</b> . Save me as startup configuration.

# 15.4 SNMP

### 15.4.1 View

#### Click Management > SNMP > View

SNMP uses an extensible design, where the available information is defined by Management Information bases (MIBs). MIBs describe the structure of the management data of a device subsystem; they use a hierarchical namespace containing Object Identifiers (OID) to organize themselves. Each OID identifies a variable that can be read or set via SNMP. The SNMP View List is created for the SNMP management station to manage MIB objects.

	Management >> SNMP >> View
VLAN	
<ul> <li>MAC Address Table</li> </ul>	View Table
<ul> <li>Spanning Tree</li> </ul>	
• Discovery	Showing All v entries Showing 1 to 1 of 1 entries
✤ Multicast	
✤ Security	
✤ ACL	
▼ QoS	Add Delete Pirst Previous T Next Last
<ul> <li>Diagnostics</li> </ul>	
✓ Management	
User Account	
<ul> <li>Firmware</li> </ul>	
<ul> <li>Configuration</li> </ul>	
∧ SNMP	
View	
Group	

Click "Add" to add a new OID Subtree.

View		
OID Subtree		
Туре	Included     Excluded	

Field	Description		
View	Enter the view name. The view name can contain up to 30 alphanumeric characters.		
OID Subtree	Enter the Object Identifier (OID) Subtree. The OID identifies an object tree (MIB tree) that will be included or excluded from access by an SNMP manager. Note that the first character must be a period (.). Wild cards can be used to mask a specific portion of the OID string using a period (.).		
Туре	Select whether the defined OID branch within MIB tree will be included or excluded from the selected SNMP view. Generally, if the view type of an entry is <b>Excluded</b> , another entry of view type <b>Included</b> should exist and its OID subtree should overlap the <b>Excluded</b> view entry.		

## 15.4.2 Group

#### Click Management > SNMP > Group

Configure SNMP Groups to control network access on the Switch by providing users in various groups with different management rights via the Read View, Write View, and Notify View options.

	Manageme	nt )> SN	MP >> Grou	р			
VLAN     MAC Address Table     Spanning Tree	Group Tab	le					
✤ Discovery	Showing All	Showing All v entries Showing 0 to 0 of 0 entries					
Multicast     Security	Group	Version	Security Level	Read	View Write	Notify	
<ul><li>ACL</li><li>QoS</li></ul>	0 results found.						
<ul> <li>Diagnostics</li> <li>Management</li> </ul>	Configure SNM	1P View to a	associate a non-de	fault viev	v with a	group.	
User Account Firmware	Add	Edit	Delete				
Configuration SNMP							
view Group Community							

Click "Add" or "Edit" to add or edit a group.

Group	
Version	<ul> <li>SNMPv1</li> <li>SNMPv2</li> <li>SNMPv3</li> </ul>
Security Level	<ul> <li>No Security</li> <li>Authentication</li> <li>Authentication and Privacy</li> </ul>
	☑ Read     all ✓     Write
View	Image: Second

Apply	Close
Field	Description
Group	Enter the group name that access control rules are applied to. The group name can contain up to 30 alphanumeric characters.
Version	Selects the SNMP version (v1, v2c, v3) associated with the group.
Security Level	Select the security level for the group. Security levels apply to SNMPv3 only.
	•No Security – Neither authentication nor the privacy security levels
	are assigned to the group.
	<ul> <li>Authentication – Authenticates SNMP messages.</li> </ul>
	<ul> <li>Authentication and Privacy – Encrypts SNMP messages.</li> </ul>
View	•Read View: Management access is restricted to read-only.
	•Write View: Select a SNMP to allow SNMP write privileges to the
	Switch's SNMP agent.
	•Notify View: Select a SNMP group to receive SNMP trap messages
	generated by the Switch's SNMP agent.

## 15.4.3 Community

#### Click Management > SNMP > Community

In SNMPv1 and SNMPv2c, user authentication is accomplished using types of passwords called Community Strings, which are transmitted in clear text and not supported by authentication. It is important to note that the community name can limit access to the SNMP agent from the SNMP network management station, functioning as a password.

Management >> SNMP >> Community				
VLAN				
<ul> <li>MAC Address Table</li> </ul>	Community Table			
<ul> <li>Spanning Tree</li> </ul>				
✓ Discovery	Showing All v entries Showing 0 to 0 of 0 entries Q			
✓ Multicast	Community Group View Access			
<ul> <li>Security</li> </ul>				
✓ ACL				
✓ QoS	The access right of a community is defined by a group upder advanced mode			
<ul> <li>Diagnostics</li> </ul>	Configure SNMP Group to associate a group with a community.			
✓ Management				
User Account				
✓ Firmware				
Configuration				
* SNMP				
View				
Community				
User				

Click "Add" or "Edit" to add or edit a community.

Community		
Туре	<ul> <li>Basic</li> <li>Advanced</li> </ul>	
View	all v	
Access	<ul> <li>Read-Only</li> <li>Read-Write</li> </ul>	

Field	Description
Community	The SNMP community name. Its maximum length is 20 characters.
Туре	Select <b>Basic</b> or <b>Advance</b> . Select the <b>Advance</b> attached to the SNMP
	group.
View	Select the view name from a list.
	SNMP access mode
Access Right	Read-Only: Read only
_	Read-Write: Read and Write.
Group	Select the SNMP group from a list.

## 15.4.4 User

Click Management > SNMP > User
Use the User page to create SNMP users for authentication with managers using SNMP v3 to associate them to SNMP groups. Click Add to add a new user.

Management >> SNMP >> User						
VLAN     MAC Address Table     Spanning Tree	User Table					
Discovery     Multicast     Security	Showing All ventries Showing 0 to 0 of 0 entries Q User Group Security Level Authentication Method Privacy Method 0 results found.					
ACL     QoS     Diagnostics     Management	First         Previous         1         Next         Last           Configure SNMP Group to associate an SNMPv3 group with an SNMPv3 user.         Add         Edit         Delete					
User Account Firmware Configuration SNMP						
View Group Community User Engine ID						

Click "Add" or "Edit" to add or edit a user.

User	
Group	test v
Security Level	<ul> <li>No Security</li> <li>Authentication</li> <li>Authentication and Privacy</li> </ul>
uthentication	
Method	<ul> <li>None</li> <li>MD5</li> <li>SHA</li> </ul>
Password	
rivacy	
Method	<ul><li>None</li><li>DES</li></ul>
Password	

Field	Description					
User	The SNMP user name. Its maximum length is 30 characters.					
Group	Select the SNMP group from a list.					
	Select the security level for the user.					
	•No Security – Neither authentication nor the privacy security levels					
Security Level	are assigned to the user.					
	<ul> <li>Authentication – Authenticates SNMP messages.</li> </ul>					
	<ul> <li>Authentication and Privacy – Encrypts SNMP messages.</li> </ul>					
Authentication Field						
Method	Select the method used to authenticate users.					
	•MD5 – Using the HMACMD5 algorithm.					
	•SHA – Using the HMACSHA-96 authentication level.					

	Enter the SHA password and the HMAC-SHA-96 password to be used for authentication.
Password	Enter MD5 password and the HMAC-MD5-96 password to be used for authentication.
Privacy Field	
	Select the method used to authenticate users.
Method	•None – No user authentication is used.
	•DES – Using the Data Encryption Standard algorithm.
Password	Enter the Data Encryption Standard key.

### 15.4.5 Engine ID

#### Click Management > SNMP > Engine ID

The Engine ID is only used by SNMPv3 entities to uniquely identify them. An SNMP agent is considered an authoritative SNMP engine. This means that the agent responds to incoming messages (Get, GetNext, GetBulk, Set), and sends trap messages to a manager.

Each SNMP agent maintains local information that is used in SNMPv3 message exchanges. The default SNMP Engine ID is comprised of the enterprise number and the default MAC address. The SNMP Engine ID must be unique for the administrative domain, so that no two devices in a network have the same Engine ID.

Local information is stored in four MIB variables that are read-only (snmpEngineId, snmpEngineBoots, snmpEngineTime, and snmpEngineMaxMessageSize).

	Management >> SNMP >> Engine ID			
<ul> <li>VLAN</li> <li>MAC Address Table</li> <li>Spanning Tree</li> <li>Discovery</li> <li>Multicast</li> <li>Security</li> <li>ACL</li> <li>QoS</li> <li>Diagnostics</li> <li>Management</li> <li>User Account</li> <li>Firmware</li> <li>Configuration</li> <li>SNMP</li> <li>View</li> <li>Group</li> <li>Community</li> <li>User</li> <li>Engine ID</li> <li>Trap Event</li> <li>Notification</li> </ul>	Local Engine ID       User Defined         Engine ID       90006a9203fc8fc40d22         Apply         Remote Engine ID Table         Showing All v entries       Showing 0 to 0 of 0 entries         Server Address       Engine ID         0 results found.       First         Add       Edit			
Field	Description			
Engine ID	<ul> <li>User Defined – Enter the local device Engine ID. The field value is a hexadecimal string (range: 10 to 64). Each byte in the hexadecimal character strings is represented by two hexadecimal digits. The default Engine ID is based on the switch MAC address, and is defined per standard as:</li> <li>•First 4 octets – First bit = 1, the rest is the IANA enterprise number.</li> </ul>			

•Fifth octet – Set to 3 to indicate the MAC address that follows.
<ul> <li>Last 6 octets – MAC address of the switch.</li> </ul>

Click "Add" or "Edit" to add or edit a remote Engine ID.

	Add Remote Engir	ie ID			
	Address Typ	e Hostname O IPv4 O IPv6			
	Server Addres	s (10 - 64 Hexadecimal Characters)			
eld	Apply	Description			
Server Address Enter the IP address or domain name of the remote server the traps		Enter the IP address or domain name of the remote server that receives the traps			
igine ID		Enter the Engine ID.			

# 15.4.6 Trap Event

#### Click Management > SNMP > Trap Event

To display and configure the SNMP trap event.

	Management >> SNMP >> Trap Event				
✓ VLAN					
<ul> <li>MAC Address Table</li> </ul>	Authentication Failure 🗹 Enable				
<ul> <li>Spanning Tree</li> </ul>	Link Up / Down 🔽 Enable				
✤ Discovery	Cold Start 🔽 Enable				
✤ Multicast	Warm Start 🔽 Enable				
✓ Security					
✓ ACL	New Root Chable				
♥ QoS	Topology Change 🔽 Enable				
<ul> <li>Diagnostics</li> </ul>					
<ul> <li>Management</li> </ul>	Apply				
User Account					
✓ Firmware					
Configuration					
View					
Group					
Community					
User					
Engine ID					
Trap Event					
Notification					
Field	Description				
Authentication	SNMP authentication failure trap, when community not match or user				

Authentication	SNMP authentication failure trap, when community not match or user					
Failure	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					

## 15.4.7 Notification

Click Management > SNMP > Notification

To configure the hosts to receive SNMP v1/v2/v3 notification.

	Management >> S	NMP >> No	tificatio	n				
VLAN     MAC Address Table	Notification Table							
Spanning Tree     Discovery	Showing All v entrie	s	Showing	0 to 0 of	0 entries		Q	
<ul> <li>Multicast</li> <li>Security</li> </ul>	Server Address	Server Port	Timeout	Retry	Version	Туре	Community / User	Security Level
• ACL • QoS	For SNMPv1,2 Notificatio	n, SNMP Comm	unity needs	0 resul	ned.		First Previou	s 1 Next Last
Diagnostics     Management     User Account	For SNMPv3 Notification,	SNMP User mu	st be created	1.				
<ul> <li>Firmware</li> <li>Configuration</li> </ul>								
<ul> <li>SNMP</li> <li>View</li> <li>Group</li> </ul>								
Community User								
Engine ID Trap Event Notification								
RMON V								

Click "Add" or "Edit" to add or edit a host.

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

Field	Description					
Server Address	IP address or the hostname of the SNMP trap recipients.					
Version	Specify SNMP notification version.					
	Notification Type					
Туре	<b>Trap</b> : Send SNMP traps to the host.					
	Inform: Send SNMP informs to the host.					
Community	SNMP community name for notification.					
	Select the security level for the host. Security level apply to SNMPv3					
	only.					
Security Level	•No Security – Neither authentication nor the privacy security levels					
	are assigned to the group.					
	<ul> <li>Authentication – Authenticates SNMP messages.</li> </ul>					
	<ul> <li>Authentication and Privacy – Encrypts SNMP messages.</li> </ul>					

Server Port	Enter the UDP port used to send notifications. The default is 162.
Timoout	Configurable only if the notify type is Informs. Enter the amount of time
Timeout	the device waits before re-sending. The default is 15 seconds.
	Configurable only if the notify type is Informs. Enter the amount of time
Retry	the device waits before re-sending an inform request. The default is 3
	times.

# 15.5 RMON

Remote Network Monitoring or RMON is used for support monitoring and protocol analysis of LANS by enabling various network monitors and console systems to exchange network-monitoring data through the Switch.

# 15.5.1 Statistics

#### Click Management > RMON > Statistics

To display RMON statistics.

	Mana	igeme	nt 🕅 RM	ION )> St	atistics	;															
• Status																					-
<ul> <li>Network</li> </ul>																					
✓ Port	Sta	tistics	lable																		
• VLAN	Refr	esh Rate	0 × 8	RC																	
<ul> <li>MAC Address Table</li> </ul>																			0		4
<ul> <li>Spanning Tree</li> </ul>	_												_	_					4		_
· Discovery		Entry	Port	Bytes	Drop	Packets	Broadcast	Multicast	CRC & Align	Undersize	Oversize	Fragments	Jabbers	Collisions	Frames of	Frames of	Frames of	Frames of	Frames of	Frames Greater	1
<ul> <li>Multicast</li> </ul>		,		Received	Events	Received	Packets	Packets	Errors	Packets	Packets				64 Bytes	65 to 127 Bytes	128 to 255 Bytes	256 to 511 Bytes	512 to 1023 Bytes	than 1024 Bytes	Ц
<ul> <li>Security</li> </ul>		1	10GE1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
✓ ACL		2	10GE2	8201242	0	127853	114392	13442	0	0	0	0	0	0	126589	1264	0	0	0	0	
v QoS		3	10GE3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
<ul> <li>Diagnostics</li> </ul>		4	10GE4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
✓ Management		5	10GE5	279999	0	1893	428	1385	0	0	0	0	0	0	559	308	1026	0	0	0	
User Account		6	10GE6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
<ul> <li>Firmware</li> </ul>		7	10GE7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
Configuration		8	10GE8	1307445	0	6218	84	2010	0	0	0	0	0	0	2311	954	1358	1435	160	0	
<ul> <li>SNMP</li> <li>BMON</li> </ul>		9	10GE9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
Statistics		10	10GE10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
History		11	10GE11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
Event		12	10GE12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
Alarm		13	LAG1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
		14	LAG2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
		15	LAG3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
		16	LAG4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
		17	LAG5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
		18	LAG6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
		19	LAG7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
		20	LAG8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
		Clear	Refres	h Vie	w																

# 15.5.2 History

Click Management > RMON > History

The RMON History contains information about samples of data taken from the ports.

Ν	Manageme	nt )>	RMON	I 💙 His	story							
✓ Status												
<ul> <li>Network</li> </ul>												
✓ Port	History Ia	ble										
<ul> <li>VLAN</li> </ul>	Showing All	∽ en	tries		Showing 0 to	0 of 0 entr	ies					
<ul> <li>MAC Address Table</li> </ul>	gi							<u>ч</u>				
<ul> <li>Spanning Tree</li> </ul>	C Entry Bost Interval			Owner	Sam							
<ul> <li>Discovery</li> </ul>		1 on	mervar	Owner	Maximum	Current						
<ul> <li>Multicast</li> </ul>					0	results four	nd.					
<ul> <li>Security</li> </ul>								First	Previous	1 N	lext	Last
✓ ACL	Add	Edit	Delet	te Vi	ew							
✓ QoS												
<ul> <li>Diagnostics</li> </ul>												
✓ Management												
User Account												
<ul> <li>Firmware</li> </ul>												
Configuration												
✓ SNMP												
RMON												
Statistics												
History												
Alorm												
Alarm												

Click "Add" or "Edit" to add or edit a history.

#### Add History

Entry	1	
Port	10GE1 ~	
Max Sample	50	(1 - 50, default 50)
Interval	1800	(1 - 3600, default 1800)
Owner		

Field	Description
Entry	The entry number for History.
Port	Select the port from which the history samples were taken.
Max Sample	Enter the number of samples to be saved. The range is from 1- 50.
Interval	Enter the time that samples are taken from the ports. The field range is from 1-3600.
Owner	Enter the RMON user that requested the RMON information. The range is from 0-32 characters.

## 15.5.3 Event

Click Management > RMON > Event

The Event page defines RMON events on the Switch.

	Management >> RMON >> Event	
<ul> <li>Status</li> </ul>		
<ul> <li>Network</li> </ul>		
✓ Port	Event Table	
✓ VLAN	Showing All v entries Showing 0 to 0 of 0 entries	4
<ul> <li>MAC Address Table</li> </ul>	Q	
<ul> <li>Spanning Tree</li> </ul>	Entry Community Description Notification Time Owner	П
<ul> <li>Discovery</li> </ul>	0 results found.	
<ul> <li>Multicast</li> </ul>	First Previous 1 Next Las	t)
<ul> <li>Security</li> </ul>	Add Edit Delete View	
• ACL		
✓ QoS		
<ul> <li>Diagnostics</li> </ul>		
✓ Management		
User Account		
<ul> <li>Firmware</li> </ul>		
<ul> <li>Configuration</li> </ul>		
✓ SNMP		
A RMON		
Statistics		
History		
Event		
Alarm		

Click "Add" or "Edit" to add or edit an event.

Entry	1	
Notification	<ul> <li>None</li> <li>Event Log</li> <li>Trap</li> <li>Event Log and Trap</li> </ul>	
Community	Default Community	
Description	Default Description	
Owner		

Field	Description
Entry	The entry number for Event.
	Select the event type.
	•Event Log – The event is a log entry.
Notification	•Trap – The event is a trap.
	•Event Log and Trap – The event is both a log entry and a trap.
Community	Enter the community to which the event belongs.
Description	Displays the number of good broadcast packets received on the
Description	interface.
Owner	Enter the switch that defined the event.

### 15.5.4 Alarm

#### Click Management > RMON > Alarm

You can configure Network alarms to occur when a network problem is detected. Choose your preferences for the alarm from the drop-down boxes.

	Manageme	nt ))	RMON	<b>&gt;&gt;</b> /	Alarm							
<ul> <li>Status</li> </ul>												
<ul> <li>Network</li> </ul>												
	Alarm Tab	le										
• VLAN	Showing All	v er	ntries		Show	ina 0 to 0 o	f 0 entries			~		
<ul> <li>MAC Address Table</li> </ul>					0.101		r o onaroo			<sup>U</sup>	L	
<ul> <li>Spanning Tree</li> </ul>	Entry	Port	Coun	ter	Sampling	Interval	Owner	Triggor	Rising		Falling	
• Discovery		Name Value	Value	sampling	mervar	Owner	mgger	Threshold	Event	Threshold	Event	
✓ Multicast						0 res	sults found	I.				
<ul> <li>Security</li> </ul>	-								Fin	st	vious 1 N	lext Last
✓ ACL	Add		Edit	D	elete							
▼ QoS												
<ul> <li>Diagnostics</li> </ul>												
✓ Management												
User Account												
<ul> <li>Firmware</li> </ul>												
Configuration												
SNMP ■ PMON												
Statistics												
History												
Event												
Alarm												

Click "**Add**" or "**Edit**" to add or edit an alarm.

Entry	1
Port	10GE1 v
Counter	Drop Events v
Sampling	Absolute     Delta
Interval	100 Sec (1 - 2147483647, default 100)
Owner	
Trigger	Rising     Falling     Rising and Falling
lising	
Threshold	100 (0 - 2147483647, default 100)
Event	1 - Default Description V
alling	
	20 (0 - 2147483647, default 20)
Threshold	

Field	Description
Entry	The entry number for Alarm.
Port	Select the port from which the alarm samples were taken.
Counter	Select the variable of samples for the specified alarm sample.
	Select the sampling method for the selected variable and comparing the value against the thresholds.
Sampling	•Absolute – Compares the values with the thresholds at the end of the sampling interval.
	•Delta – Subtracts the last sampled value from the current value.
Interval	Enter the alarm interval time.
Owner	Enter the Switch that defined the alarm.

Trigger	<ul> <li>The method of sampling the selected variable and calculating the value to be compared against the thresholds, possible sample types are:</li> <li><b>Rising</b> Trigger alarm when the first value is larger than the rising threshold.</li> <li><b>Falling</b> Trigger alarm when the first value is less than the falling threshold.</li> <li><b>Rising and Falling</b> Trigger alarm when the first value is larger than the falling threshold.</li> </ul>
Rising Field	
Threshold	Enter the rising number that triggers the rising threshold alarm.
Event	Select the event number by the rising alarm is reported.
Falling Field	
Threshold	Enter the rising number that triggers the falling threshold alarm.
Event	Select the event number by the falling alarm is reported.