Quant

ELEVATING TECHNOLOGY

POE Web Management Manual

Series Switch Web Management Manual-linux

Q-M-4800-24P-L3-4S-V	Q-M-4800-48P-L3-4S-V	Q-IE-6600-28P-L3-4G-E	Q-IE-6600-48P-L3-4G-E
Q-EP-9300-24P-L3-4G	Q-EP-9300-48P-L3-4G	Q-IE-9600-24P-L3-4G-E	Q-IE-9600-48P-L3-4G-E

Table of Contents

Chapter 1. Product Overview

1.1. Product introduction

The POE38 series product is a high-performance, high-efficiency high-end intelligent rack industrial core three-layer switch. The range includes 4800-24P-L3, 4800-48P-L3 (10/100/1000/100010/100010/1000 supported) and 4-lane 1000 SFP/1010 SFP+ optical ports, 10/100/100/100/1000 SFP(X) Ethernet Standard power interface, four 1000 SFP-SFP/10GbE SFP + optical ports, increased bandwidth improves the communication function of network data, very suitable for large-scale network applications.
This series of products supports IPv4/IPv6 dual-stack platform and supports multiple advanced management functions, such as: POE management, MAC table, VLAN, port isolation, loop protection, IGMP snooping, MLD snooping, ERPS, DHCP client, DHCP snooping, STP/RSTP/MSTP, 802.1x, QoS, port mirroring, LLDP, static routing, NTP, etc., Su connection.

1.2. Product Features

4800-24P-L3 provides 24*10/100/1000Base-T(X) PoE ports, 4*1000Base-X SFP / 10GbE SFP + optical ports
4800-48P-L3 provides 48*10/100/1000Base-T(X) PoE ports, 4*1000Base-X SFP/10GbE SFP + optical port

- Support V-ring network redundancy patent technology, network fault self-repair time is less than 20 ms
- Support POE management, support POE load timing restart, timing switch
- Support IGMP snooping, static multicast filtering and MLD snooping filtering
- Support DHCP snooping, prevent ARP attack, illegal DHCP server access and other attacks
- Support NTP to facilitate real-time synchronization of network time
- Support SNMP v1/v2/v3, a simple network management protocol
- Support LLDP Link Layer Discovery Protocol
- Support ACL function, enhance the flexibility and security of network management
- Support IEEE802.1P QoS function, increase network stability
- Support port mirroring function, easy to debug online
- Support cable detection, easy to check the length of the network cable
- Support STP/RSTP/MSTP to improve network stability
- Support IEEE802.1Q VLAN, IEEE802.1ad QINQ to facilitate network planning
- Support 802.1x port authentication and Mac address authentication to enhance network security
- Layer 3 switching technology supports static routing
- Support working temperature range -10℃~50℃

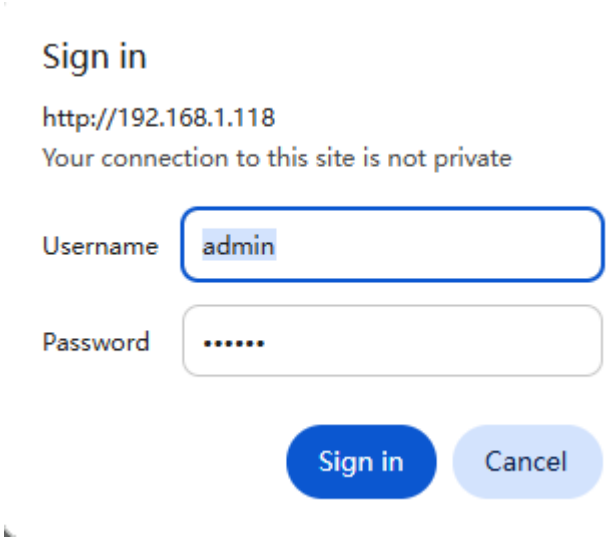
- Support storage temperature range -40°C to 85°C
- Support silent fan, rack mount design

1.3. Login to the network, administrator

Enter the IP address of the device (the address installed on the computer) in the browser to manage the switch. The format of the URL in the address bar is: http://xxx.xxx.xxx.xxx, where xxx represents the IP address of the switch.

Note: The default factory IP address is 192.168.2.1.

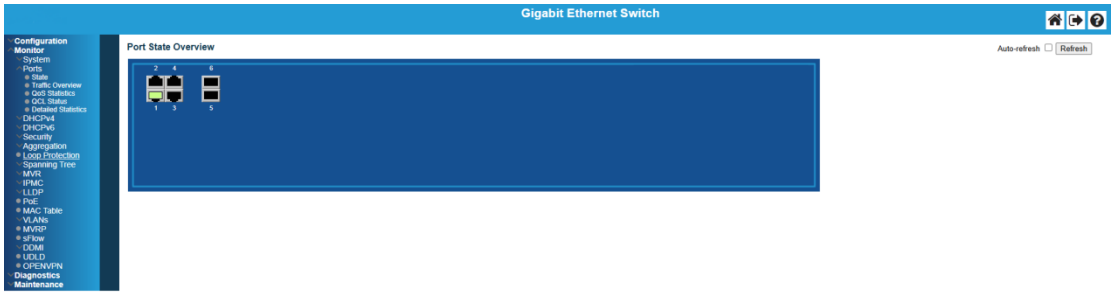
The User Authentication window for the Management Module will pop up.



The username is admin and the password is system. Click OK to open the web-based management user interface.

1.4. Web-based user interface

The user interface provides access to the different configuration and management windows of the switch, allowing users to view performance statistics and monitor system status graphically.
The user interface is divided into three distinct areas.



Area	Function
Area 1	Display manufacturer LOGO, port PoE and Link working status, Chinese and English switching and help.
Area 2	Select the displayed menu or window, and click the hyperlink menu button and subfolder to display the corresponding menu content.
Area 3	According to the user's selection (area 2), display the relevant information and con diagram data items of the switch, this area is the main page of the switch con diagram and status.

1.5. Web pages

When a user connects to the management mode of the switch through a web browser, a login window is displayed. Enter the username and password to access the management interface of the switch.
Below is a list and description of the main folders in the web interface:
information and status - users can view the information and working status of the switch under this menu.
Network Management - Users can con- figure the relevant network management features of the switch in this section.
Port Con Diagram - User can con diagram the port related features of the switch in this section.
PoE - Users can view the PoE-related con diagram and status of the switch in this section.
Advanced Con Diagram - User can con diagram the advanced L2 related features of the switch in this section.
Security Con Diagram - User can con diagram the security related features of the switch in this section.
QoScon Diagram - User can con diagram the QoS related features of the switch in this section.
system diagnostics - In this section the user can con- figure the diagnostics related

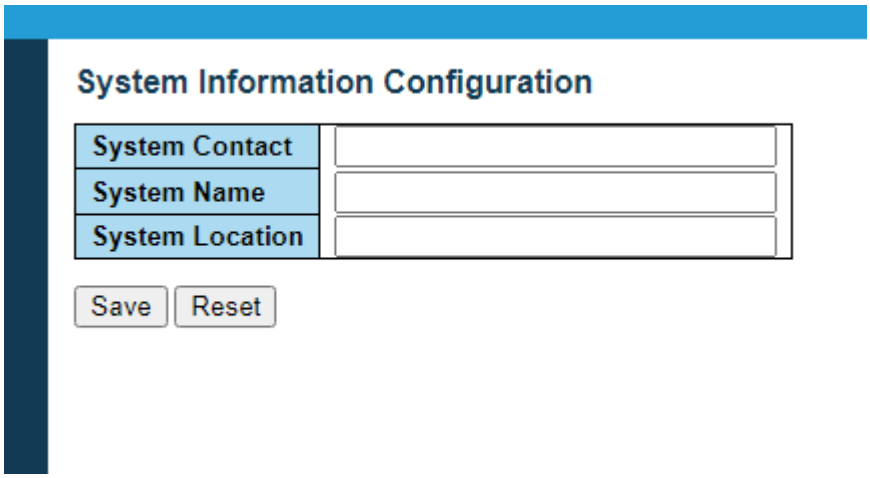
features of the switch.
System Maintenance-Users can view the system maintenance related features of the switch in this part.

Chapter 2. Configuration

2.1. System

2.1.1. Information

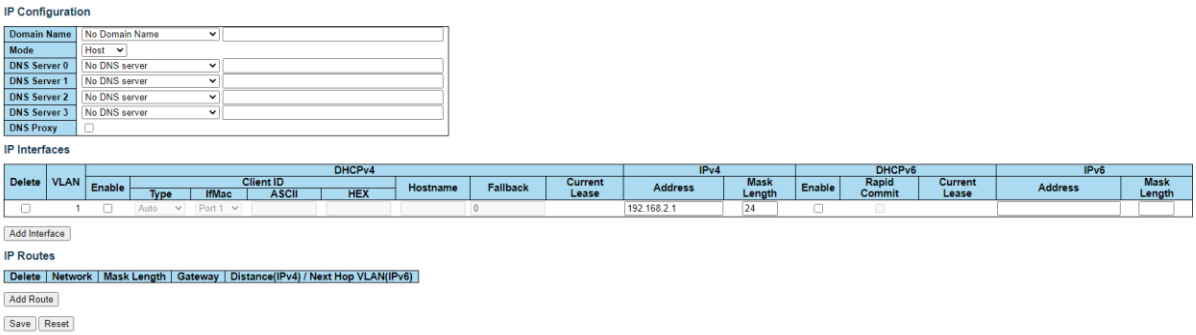
Click "Configuration > System > Information".



Parameters	Explain
Administrative Staff	Administrative Staff
System Name	Enter The Switch Name
System Location	System Location

2.1.2. IP

Note: The factory default IP address of the switch is 192.168.2.1, and the subnet mask is 255.255.255.0 (24) Click "Configuration>System>IP.



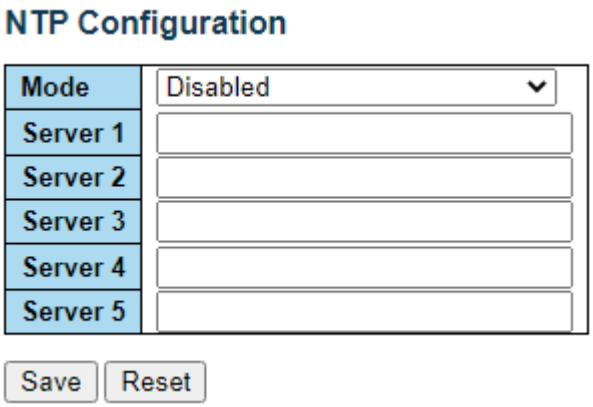
Parameters	Explain
Domain Name	The domain name of the con diagram switch
Mode	Optional Host and router
DNS Server	Optional No DNS server,Configuerd IPV4,From any DHCPv4 interfaces, From this DHCPv4 interfaces
DNS Proxy	DNS proxy
Interface Name	Displays the system interface name.
VLAN	Enter the VLAN used for access and management of the switch.
IPv4 DHCP	If it is enabled, it means that the VLAN interface opens the IPv4 DHCP client to dynamically obtain the IPv4 address of the switch, otherwise the static IPcon diagram of the switch is used Waiting time, which means the waiting time for the switch to try to obtain a dynamic IP address through DHCP (in seconds), 0 means never timeout. Current IP address, indicating the IP address obtained through DHCP.
IPv4	IP address, the static IPv4 address entered by the user. IP mask, the static IPv4 subnet mask entered by the user.
IPv6	IP address, the static IPv6 address entered by the user. IP mask, the static IPv6 subnet mask entered by the user.
IP Routes	Destination network segment, the user enters the IPv4 address of the destination network segment. IP mask, the user enters a static IPv4 subnet mask. Next hop address, the user enters the next IPv4 address

Click "Add" to create a new management VLAN and IP address. Click "Save" for the changes to take effect.

Note: The switch only creates VLAN1 by default. If the user needs to use the management switch of other VLAN, he must first add the VLAN in the VLAN module and add the relevant ports to the VLAN to realize Layer 3 communication between VLAN.

2.1.3. NTP

Simple Network Time Protocol (NTP), a protocol for synchronizing clocks over the Internet. Users can configure the time setting of the switch.
To view this window, click "con diagram >system >NTP".



Parameters	Explanation
Mode	Use the drop-down menu to enable (Enabled) or disable (Disabled) NTP.
NTP Server	The IP address of the NTP server, from which NTP information will be obtained, and multiple NTP servers can be filled in.

Click the "Save" button to accept the changes.

2.1.4. Time zone setting

The time zone setting is to adjust to the time of the corresponding country by setting the time. Users can configure the time setting of the switch.
To view this window, click "con diagram >system >time".

Time Zone Configuration

Time Zone Configuration	
Time Zone	(UTC) Coordinated Universal Time
Hours	0
Minutes	0
Acronym	(0 - 16 characters)

Daylight Saving Time Configuration

Daylight Saving Time Mode	
Daylight Saving Time	Disabled

Start Time settings	
Month	Jan
Date	1
Year	2014
Hours	0
Minutes	0
End Time settings	
Month	Jan
Date	1
Year	2097
Hours	0
Minutes	0
Offset settings	
Offset	1 (1 - 1439) Minutes

Save Reset

Parameters	Explanation
Time Zone Setting	Enter the time that needs to be changed.

Click the "Save" button to accept the changes.

2.1.5. Log con diagram

Users can view the system log of the switch.

Click "con diagram >system >diary",

System Log Configuration

Server Mode	Disabled
Server Address	
Syslog Level	Informational

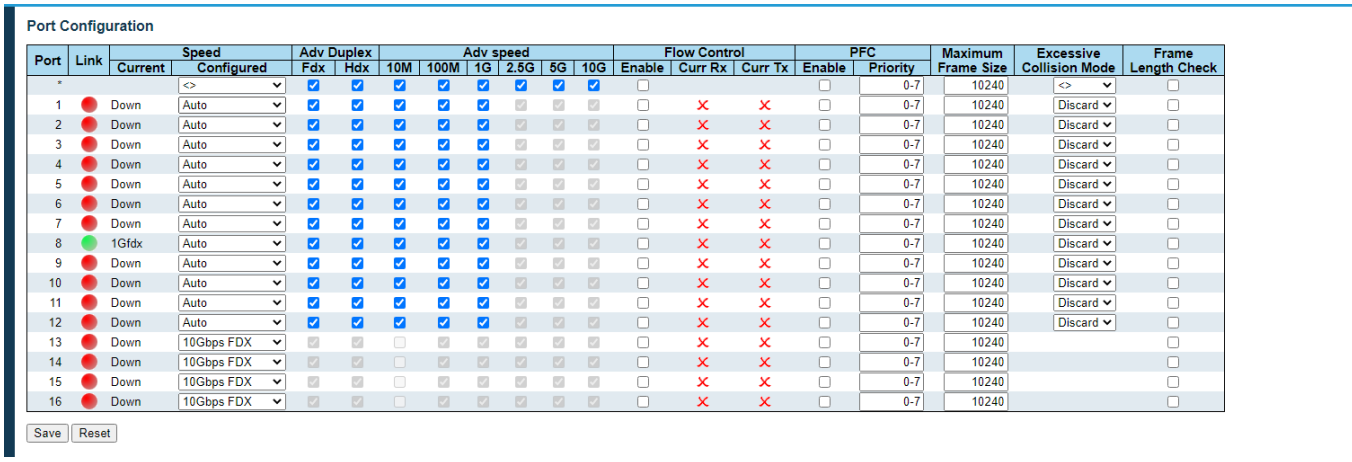
Save Reset

Parameters	Explanation
Mode	Choose to enable or disable the system logging feature. If "Enabled" is selected, the switch will send system logs to the specified log server
Server IP Address	Specify the IP address of the log server
Log Level	Specify the level of the log, the optional level includes: Info: informations, warnings and errors. Warning: warnings and errors. Error: errors.

Click "Save" for the changes to take effect.

2.2. Port con diagram

This page is used to con diagram switch port related features.
Click "Con Diagram > Port".



Parameters	Explanation
Link State	Red means Link Down, green means Link Up
Rate	Select the speed and full-duplex/half-duplex status of the port. Auto means automatically negotiate between 10, 100, 1000Mbps devices in full-duplex (FDX) or half-duplex mode (HDX) (1000mbps is always in full-duplex mode). The Auto setting allows the port to automatically determine the fastest settings for the device connected to the port and apply those settings. 1000X_AMS indicates that the port is photoelectric multiplexed, and the optical port is prioritized. Disabled indicates that the port is disabled. Other options are 10M HDX, 10M FDX, 100M HDX, 100M FDX, 1000M FDX, 1000X.

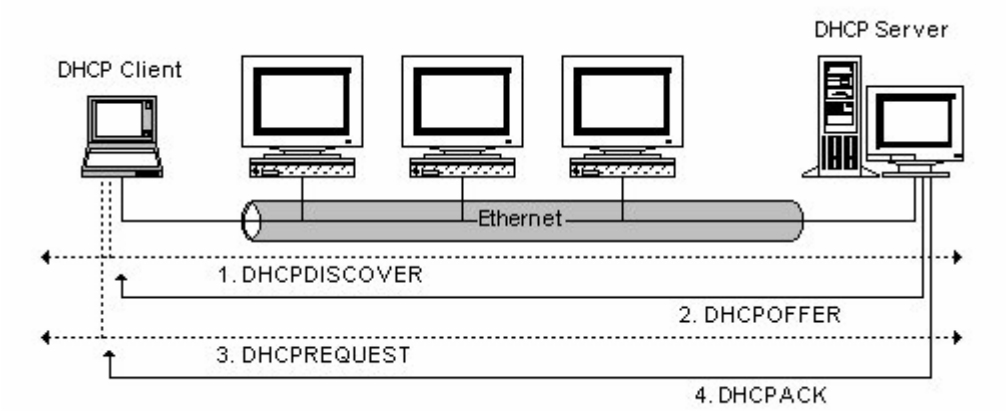
Flow Control	Shows flow control mechanisms used in various port con diagrams. Full-duplex ports use 802.3x flow control, half-duplex ports use back pressure flow control. Disabled by default. Checking User Settings means enabling flow control.
Max Frame Length	It is used to set the maximum frame length of Ethernet, the default setting is 9600, that is, it supports Jumbo frame.

Click "Save" for the changes to take effect.

2.3. DHCPv4

2.3.1. Understanding DHCP

The DHCP protocol is widely used to dynamically allocate reusable network resources, such as IP addresses. A typical process of DHCP obtaining IP.

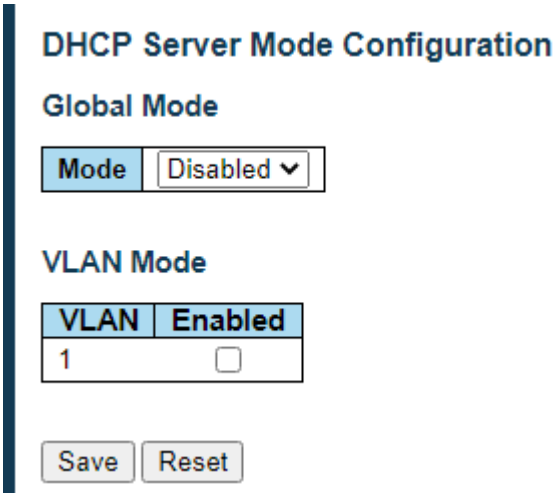


The DHCP Client sends a DHCP DISCOVER broadcast message to the DHCP Server. If the Client does not receive a response from the server within a certain period of time, the DHCP DISCOVER message will be resent.
After receiving the DHCP DISCOVER message, the DHCP Server allocates resources (such as IP addresses) to the Client according to a certain strategy, and then sends a DHCP OFFER message.
After receiving the DHCP OFFER message, the DHCP Client sends out a DHCP REQUEST request to obtain the server lease, and notifies other servers that they have accepted the address assigned by the server.
After receiving the DHCP REQUEST message, the server verifies whether the resource can be allocated. If it can be allocated, it will send a DHCP ACK message; if it cannot be allocated, it will send a DHCP NAK message. After receiving the DHCP ACK message, the DHCP Client starts to use the resources allocated by the server. If a DHCP NAK is received, the DHCP DISCOVER message is resent.

2.3.2. DHCPV4 service

2.3.2.1. Mode

Click on "Con Diagram > DHCPV4 > Service > Mode".

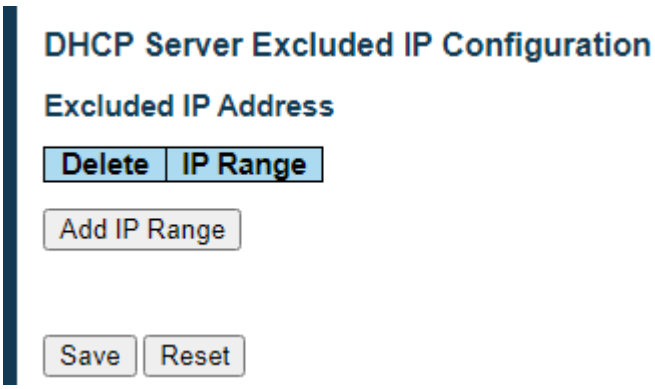


Parameters	Explanation
Global Mode	Disable and enable can be selected
Vlan Mode	Optional check and uncheck

Click "Save" for the changes to take effect.

2.3.2.2. Remove address con map

Click "Con Diagram >DHCPV4>Service>Exclude Address Con Diagram".

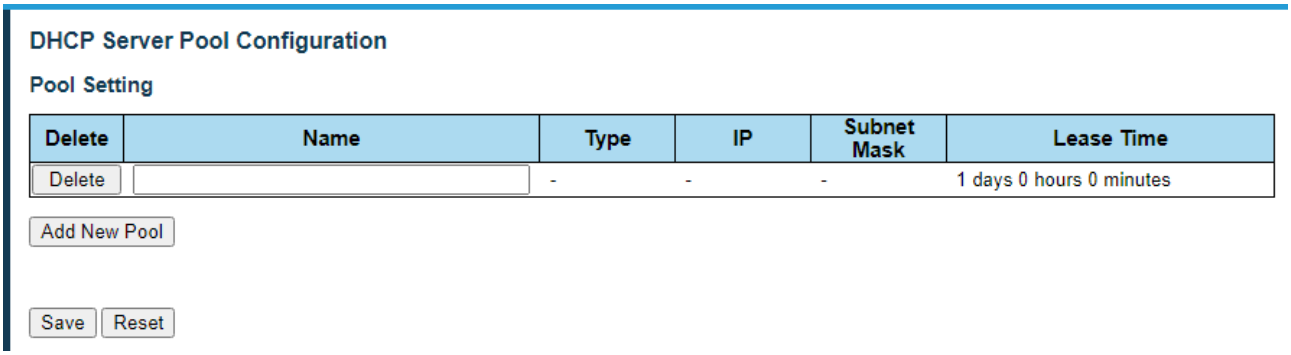


Parameters	Explanation
Add IP Range	Fill in the range of excluded IP addresses

Click "Save" for the changes to take effect.

2.3.2.3. Address pool

Click "con diagram >DHCPV4>service>address pool".



Parameters	Explanation
Add New Pool	Fill in the address pool name

Click "Save" for the changes to take effect.

Click on the pool name to enter the con diagram

DHCP Pool Configuration

Pool

Name	IP

Setting

Pool Name	IP
Type	None
IP	
Subnet Mask	
Lease Time	1 days (0-365) 0 hours (0-23) 0 minutes (0-59)
Domain Name	
Broadcast Address	
Default Router	0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
DNS Server	0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
NTP Server	0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
Tftp Server	
Bootfile Name	
NetBIOS Node Type	None
NetBIOS Scope	
NetBIOS Name Server	0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
NIS Domain Name	
NIS Server	0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
Client Identifier	None
Hardware Address	
Client Name	
Vendor 1 Class Identifier	
Vendor 1 Specific Information	
Vendor 2 Class Identifier	
Vendor 2 Specific Information	
Vendor 3 Class Identifier	
Vendor 3 Specific Information	
Vendor 4 Class Identifier	
Vendor 4 Specific Information	

Save Reset

Parameters	Explanation
Type	Divided into two modes: Host and Network

IP	Enter IP address
Subnet Mask	Enter subnet mask
Lease Term	Set the lease period of the address
Domain Name	Set domain name
Broadcast Address	Set broadcast address
Default Router	Set gateway
DNS Server	Set DNS service
NTP Server	Set NTP service
NetBIOS Node Type	Set NetBIOS type

Click "Save" for the changes to take effect.

2.3.3. Understanding DHCP Snooping

DHCP snooping, by snooping on the DHCP interaction messages between the client and the server,Realize the monitoring of users, and at the same time, DHCP Snooping functions as a DHCP message filtering function, and realizes filtering of illegal servers through a reasonable con diagram. The following explains some terms and functions used in DHCP Snooping:

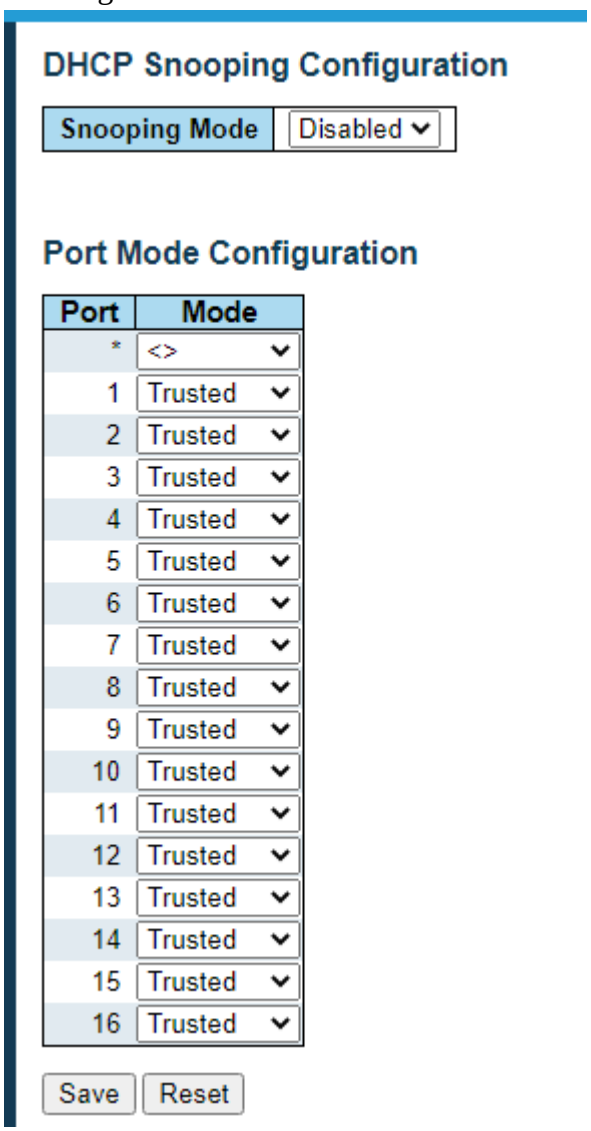
- DHCP Snooping TRUST port: Since DHCP obtains IP interactive messages in the form of broadcast, there are illegal servers that affect users' normal IP acquisition, and what's more, illegal servers are used to cheat and steal user information. In order to prevent illegal The server problem, DHCP Snooping divides the port into two types, TRUST port and UNTRUST port, the device only forwards the DHCP Reply message received by the TRUST port, and discards all DHCP Reply messages from the UNTRUST port, so that we send legal DHCP The port connected to the server is set as TURST port, and the other ports are set as UNTRUST port, so that the illegal DHCP Server can be shielded.
- DHCP Snooping binding database: In the network of DHCP environment, the problem of users setting IP addresses without authorization often occurs. The private setting of IP addresses by users not only makes the network difficult to maintain, but also causes some legitimate users who use DHCP to obtain IPs to fail due to conflicts. If the network cannot be used normally, DHCP Snooping snoops the messages exchanged between Client and Server, and forms a user record entry with IP information obtained by the user, user MAC, VID, PORT, lease time and other information, thus forming a DHCP Snooping The user database, with the use of ARP detection function or ARP CHECK function, so as to achieve the purpose of controlling users to access the Internet.

DHCP Snooping checks the validity of the DHCP messages passing through the device, discards illegal DHCP messages, records user information and generates a DHCP Snooping binding database for other functions to query. The following types of packets are considered illegal DHCP packets:

- The DHCP reply message received by the UNTRUST port, including DHCPACK, DHCPNACK, DHCPOFFER, etc.
- The DHCP request message with the network management information [giaddr] received by the UNTRUST port.
- When mac verification is enabled, the source MAC and the DHCP Client field value carried in the DHCP message are different messages.
- A DHCPRELEASE message in which the user's information exists in the DHCP Snooping binding database, but the port information is inconsistent with the port information stored in the information of the device in the DHCP binding database.

2.3.4. DHCPV4 monitoring

Click "con diagram >DHCPV4>DHCPV4 Snooping" to view the DHCP Snooping con diagram of the switch.

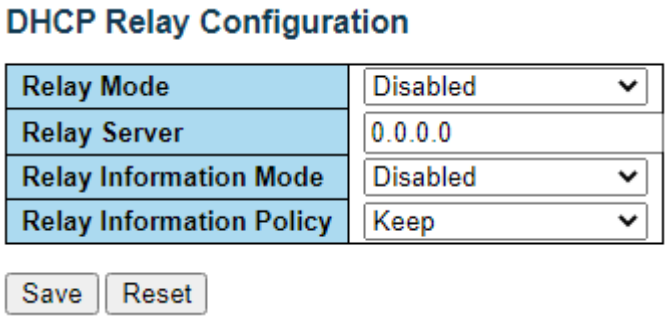


Parameters	Explanation
DHCP Snooping Mode	- Enable or disable DHCP Snooping.
Port Mode	-Indicates the DHCP snooping port mode. Possible port modes are: -Trusted: Con s the port as trusted source of the DHCP messages. -Untrusted: Con s the port as untrusted source of the DHCP messages.

Click "Save" for the changes to take effect.

2.3.5. DHCPV4 Relay

Click on "Con Graph >DHCPV4>DHCPV4 Relay.



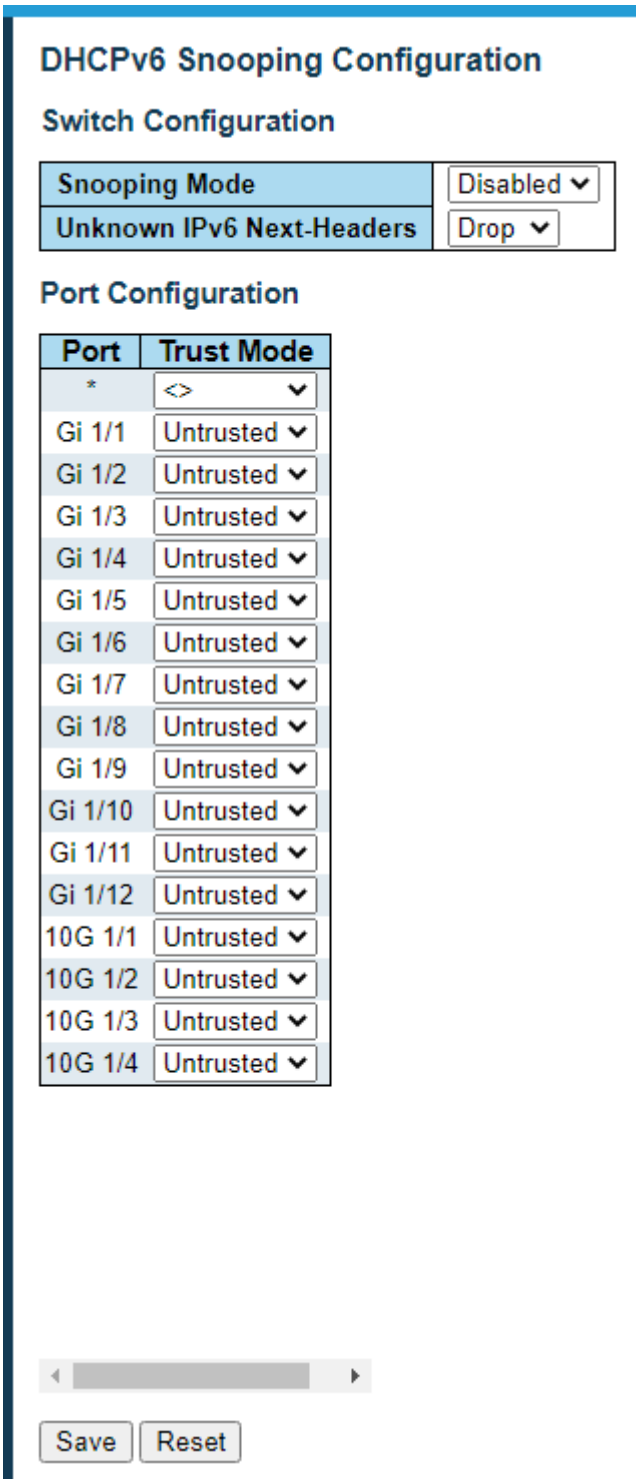
Parameters	Explanation
Repeater Mode	Enable or disable DHCP relay.
Relay Server	Fill in the relay server
Relay Information Mode	Enable or disable relay information mode
Relay Information Strategy	Select relay information strategy (keep and dorp)

Click "Save" for the changes to take effect.

2.4. DHCPv6 snooping

2.4.1. DHCPV6 monitoring

Click "con diagram >DHCPV6>DHCPV6 Snooping" to view the DHCPV6 Snooping con diagram of the switch.



Parameters	Explanation
DHCP Snoopingv6 Mode	Click "Save" for the changes to take effect.
Port Mode	Enable or disable DHCP SnoopingV6. Indicates the DHCP snooping port mode. Possible port modes are: Trusted: Con s the port as trusted source of the DHCP

	messages. Untrusted: Con s the port as untrusted source of the DHCP messages.

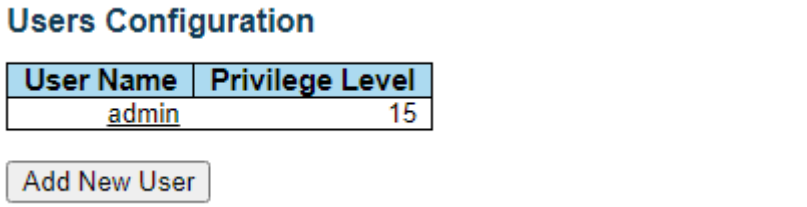
Click "Save" for the changes to take effect.

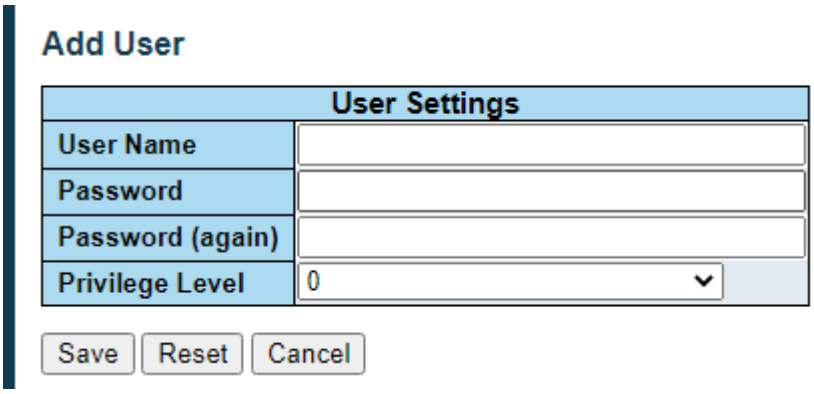
2.5. Security con diagram

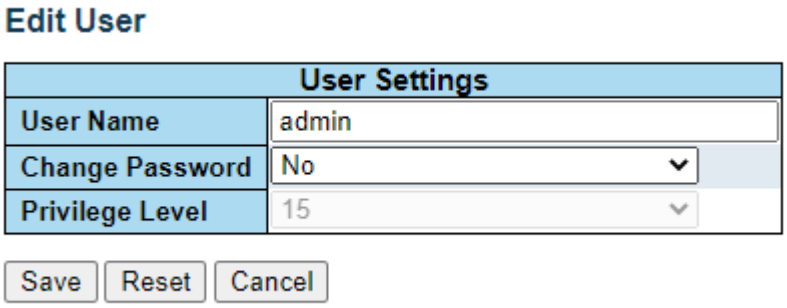
2.5.1. Exchange

2.5.1.1. User

The switch supports modifying the login password.
Click "Con Diagram > Security > Exchange > User".







Parameters	Explanation
Username	Username
Password	Change password
Level	Modify user level

Click "Save" for the changes to take effect.

2.5.1.2. Privilege levels

Click on "Con Diagram > Security > Exchange > Privilege Level".

Privilege Level Configuration

Group Name	Privilege Levels			
	Configuration Read-only	Configuration/Execute Read/write	Status/Statistics Read-only	Status/Statistics Read/write
Aggregation	5	10	5	10
Alarm	5	10	5	10
BOX_SERVICE	5	10	5	10
CLOUD_SERVICE	5	10	5	10
DDMI	5	10	5	10
Debug	15	15	15	15
DHCP	5	10	5	10
DHCPv6_Client	5	10	5	10
Diagnostics	5	10	5	10
EPS	5	10	5	10
ERPS	5	10	5	10
ETH_LINK_OAM	5	10	5	10
EVC	5	10	5	10
Firmware	5	10	5	10
FRR	5	10	5	10
Green_Ethernet	5	10	5	10
HQoS	5	10	5	10
IP	5	10	5	10
IPC_SERVIE	5	10	5	10
IPMC_Snooping	5	10	5	10
LACP	5	10	5	10
LLDP	5	10	5	10
Loop_Protect	5	10	5	10
MAC_Table	5	10	5	10
MEP	5	10	5	10
Miscellaneous	15	15	15	15
MRP	5	10	5	10
MVR	5	10	5	10
NTP	5	10	5	10
Performance_Monitor	5	10	5	10
POE	5	10	5	10
Ports	5	10	1	10
Private_VLANs	5	10	5	10
QoS	5	10	5	10
RFC2544	5	10	5	10
RMirror	5	10	5	10
Security(access)	10	10	5	10
Security(network)	5	10	5	10

Click the "Save" button for the changes to take effect.

2.5.1.3. Authentication method

Click "Con Diagram > Security > Exchange > Authentication Method".

Authentication Method Configuration

Client	Methods		
console	local	no	no
telnet	local	no	no
ssh	local	no	no
http	local	no	no

Command Authorization Method Configuration

Client	Method	Cmd Lvl	Cfg Cmd
console	no	0	☐
telnet	no	0	☐
ssh	no	0	☐

Accounting Method Configuration

Client	Method	Cmd Lvl	Exec
console	no		☐
telnet	no		☐
ssh	no		☐

Save Reset

Click the "Save" button for the changes to take effect.

2.5.1.4. SSH

Click on "Con Diagram > Security > Exchange > SSH".

SSH Configuration

Mode	Enabled

Save Reset

Click the "Save" button for the changes to take effect.

2.5.1.5. HTTPS

Click on "Con Diagram > Security > Exchange > HTTPS"

HTTPS Configuration

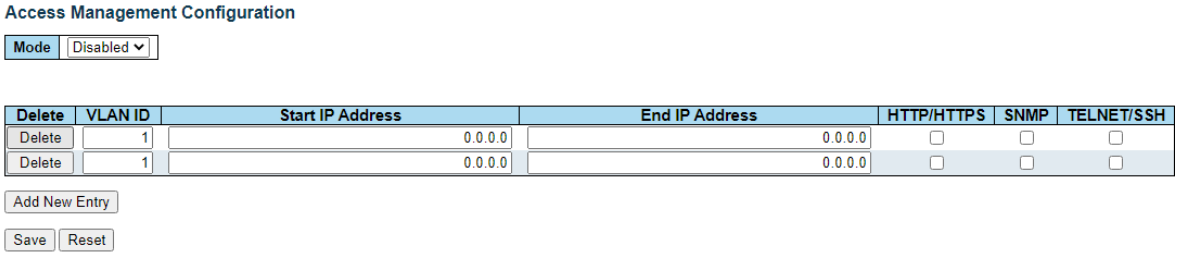
Mode	Disabled
Automatic Redirect	Disabled
Certificate Maintain	None
Certificate Status	Switch secure HTTP certificate is presented

Save Reset

Click the "Save" button for the changes to take effect.

2.5.1.6. Access Management

Click on“Configuration>Security>Switch>Access Management”

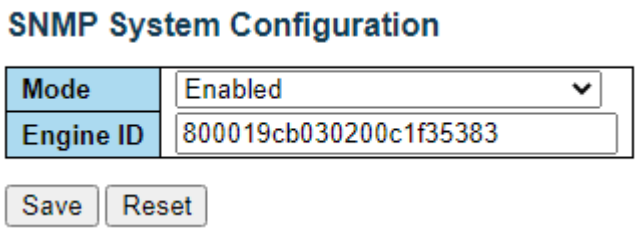


Click the "Save" button for the changes to take effect.

2.5.1.7. SNMP

2.5.1.7.1 system

Click on “Configuration>Security>Switch>SNMP>system ”.

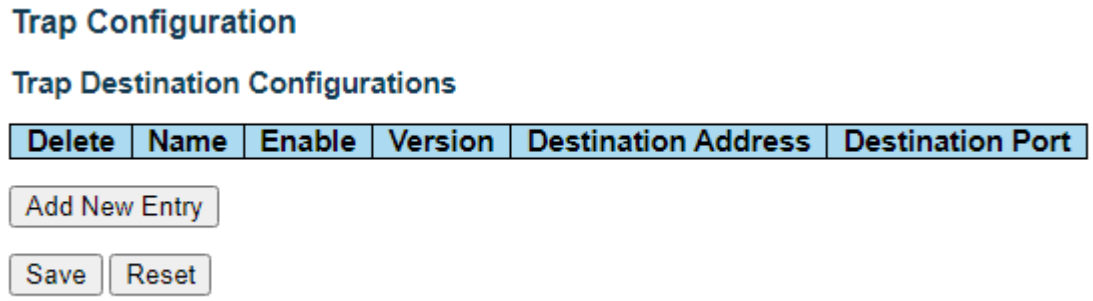


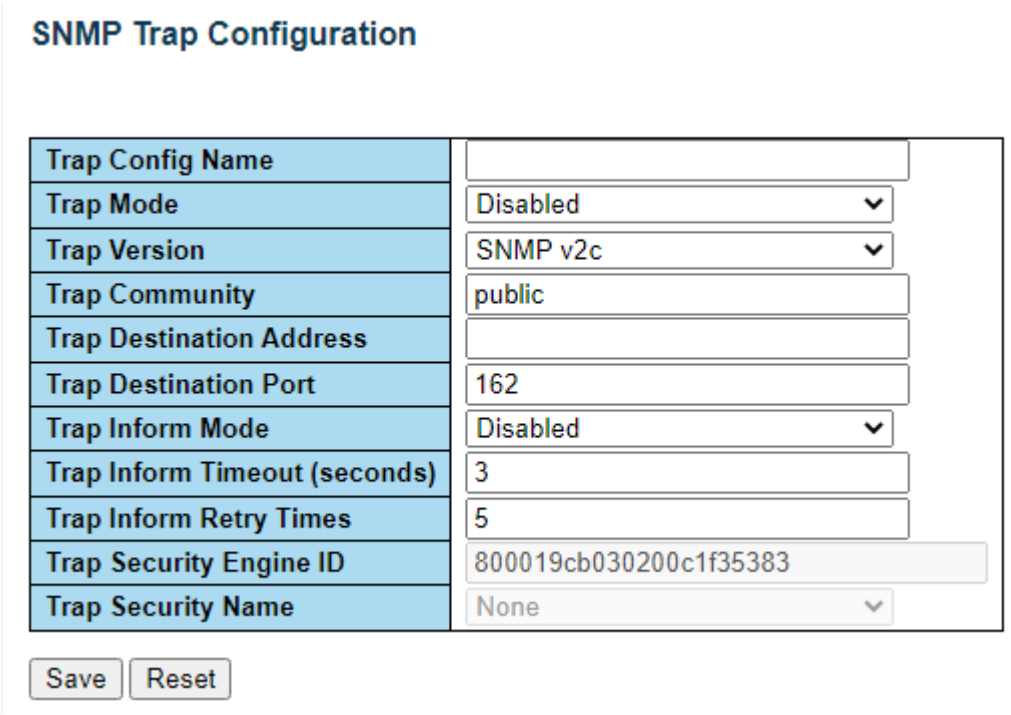
Click the "Save" button for the changes to take effect.

2.5.1.7.2. Trap

Destinations

Click on “Configuration>Security>Switch>SNMP>Trap>Destinations”.

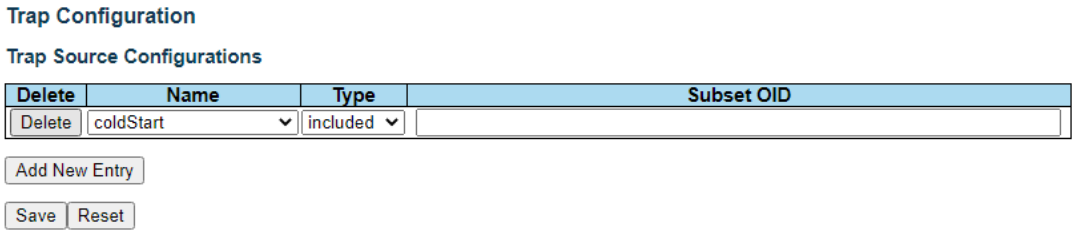




Click the "Save" button for the changes to take effect.

Sources

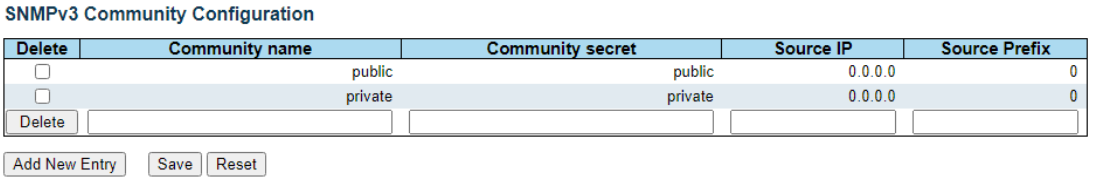
Click on “Configuration>Security>Switch>SNMP>Trap>Sources”.



Click the "Save" button for the changes to take effect.

2.5.1.7.3. Communities

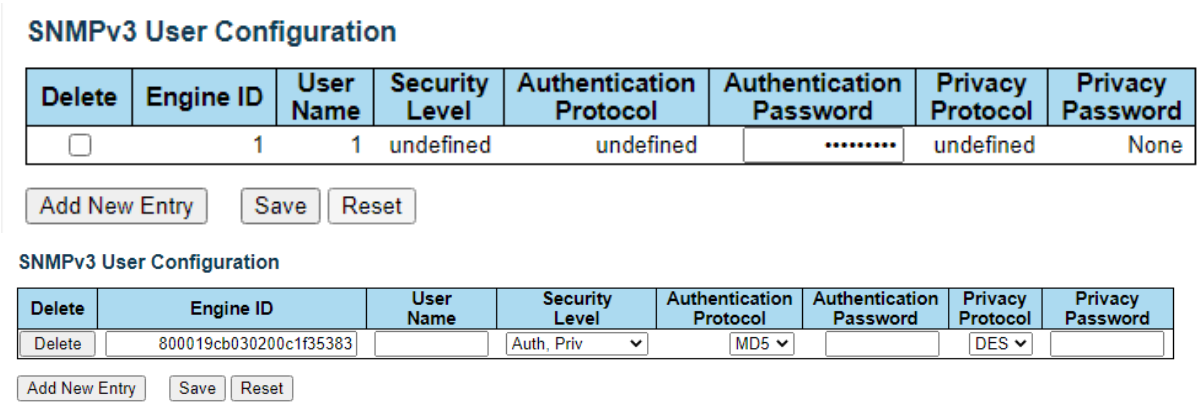
Click on “Configuration>Security>Switch>SNMP>Communities”.



Click the "Save" button for the changes to take effect.

2.5.1.7.4 . Users

Click on “Configuration>Security>Switch>SNMP>Users”.



SNMPv3 User Configuration

Delete	Engine ID	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
☐	1	1	undefined	undefined	•••••••••	undefined	None

Add New Entry | Save | Reset

SNMPv3 User Configuration

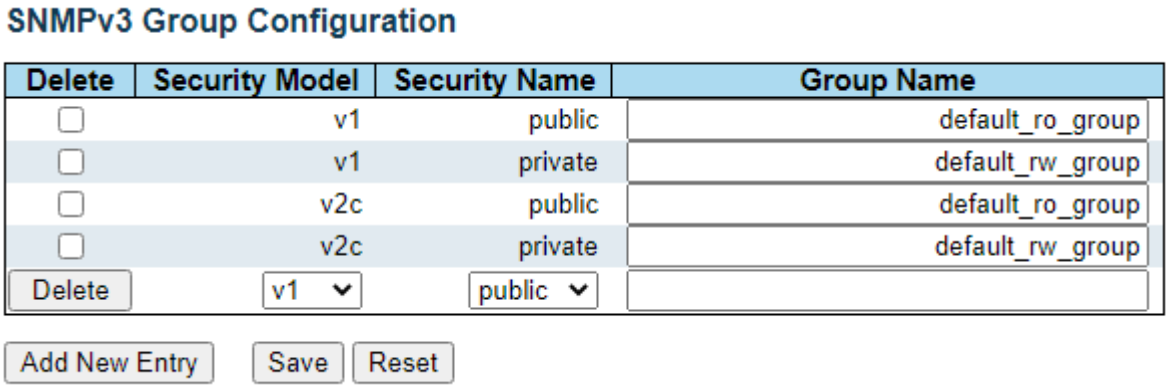
Delete	Engine ID	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
Delete	800019cb030200c1f35383		Auth, Priv	MD5		DES	

Add New Entry | Save | Reset

Click the "Save" button for the changes to take effect.

2.5.1.7.5. Groups

Click on “Configuration>Security>Switch>SNMP>Groups”.



SNMPv3 Group Configuration

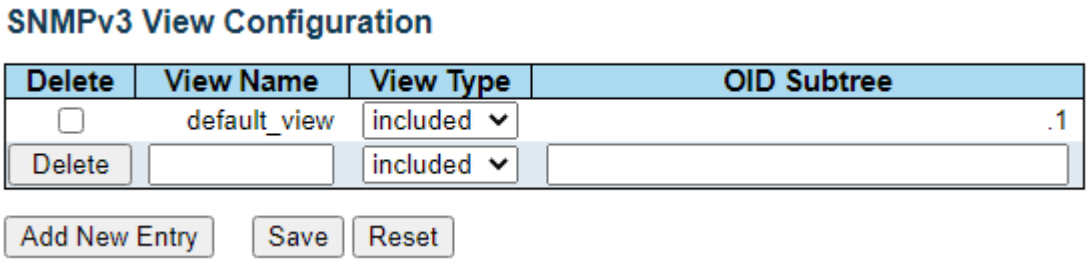
Delete	Security Model	Security Name	Group Name
☐	v1	public	default_ro_group
☐	v1	private	default_rw_group
☐	v2c	public	default_ro_group
☐	v2c	private	default_rw_group
Delete	v1	public	

Add New Entry | Save | Reset

Click the "Save" button for the changes to take effect.

2.5.1.7.6. Views

Click on Configuration>Security>Switch>SNMP>Views.



SNMPv3 View Configuration

Delete	View Name	View Type	OID Subtree
☐	default_view	included	.1
Delete		included	

Add New Entry | Save | Reset

Click "Save" for the changes to take effect.

2.5.1.7.7. Access

Click on“Configuration>Security>Switch>SNMP>Access”.

SNMPv3 Access Configuration

Delete	Group Name	Security Model	Security Level	Read View Name	Write View Name
☐	default_ro_group	any	NoAuth, NoPriv	default_view	None
☐	default_rw_group	any	NoAuth, NoPriv	default_view	default_view
Delete	default_ro_group	any	NoAuth, NoPriv	None	None

Add New Entry | Save | Reset

Click "Save" for the changes to take effect.

2.5.1.8. RMON

2.5.1.8.1. Statistics

Click on“Configuration>Security>Switch>RMON>Statistics”.

RMON Statistics Configuration

Delete	ID	Data Source
Delete		.1.3.6.1.2.1.2.2.1.1. 0

Add New Entry | Save | Reset

Click "Save" for the changes to take effect.

2.5.1.8.2. History

Click on “Configuration>Security>Switch>SNMP>Trap>History”.

RMON History Configuration

Delete	ID	Data Source	Interval	Buckets	Buckets Granted
Delete		.1.3.6.1.2.1.2.2.1.1. 0	1800	50	

Add New Entry | Save | Reset

Click "Save" for the changes to take effect.

2.5.1.8.3. Alarm

Click on “Configuration>Security>Switch>SNMP>Trap>Alarm”.

RMON Alarm Configuration

Delete	ID	Interval	Variable	Sample Type	Value	Startup Alarm	Rising Threshold	Rising Index	Falling Threshold	Falling Index
Delete		30	.1.3.6.1.2.1.2.2.1. 0.0	Delta	0	RisingOrFalling	0	0	0	0

Add New Entry | Save | Reset

Click "Save" for the changes to take effect.

2.5.1.8.4. Event

Click on “Configuration>Security>Switch>SNMP>Trap>Event”.

RMON Event Configuration

Delete	ID	Desc	Type	Event Last Time
Delete			none	0

Add New Entry | Save | Reset

Click "Save" for the changes to take effect.

2.5.2. Network

2.5.2.1. Port Security

Click on“Configuration>Security>Network>Port Security”.

Port Security Configuration

Global Configuration

Aging Enabled	☐
Aging Period	3600 seconds
Hold Time	300 seconds

Port Configuration

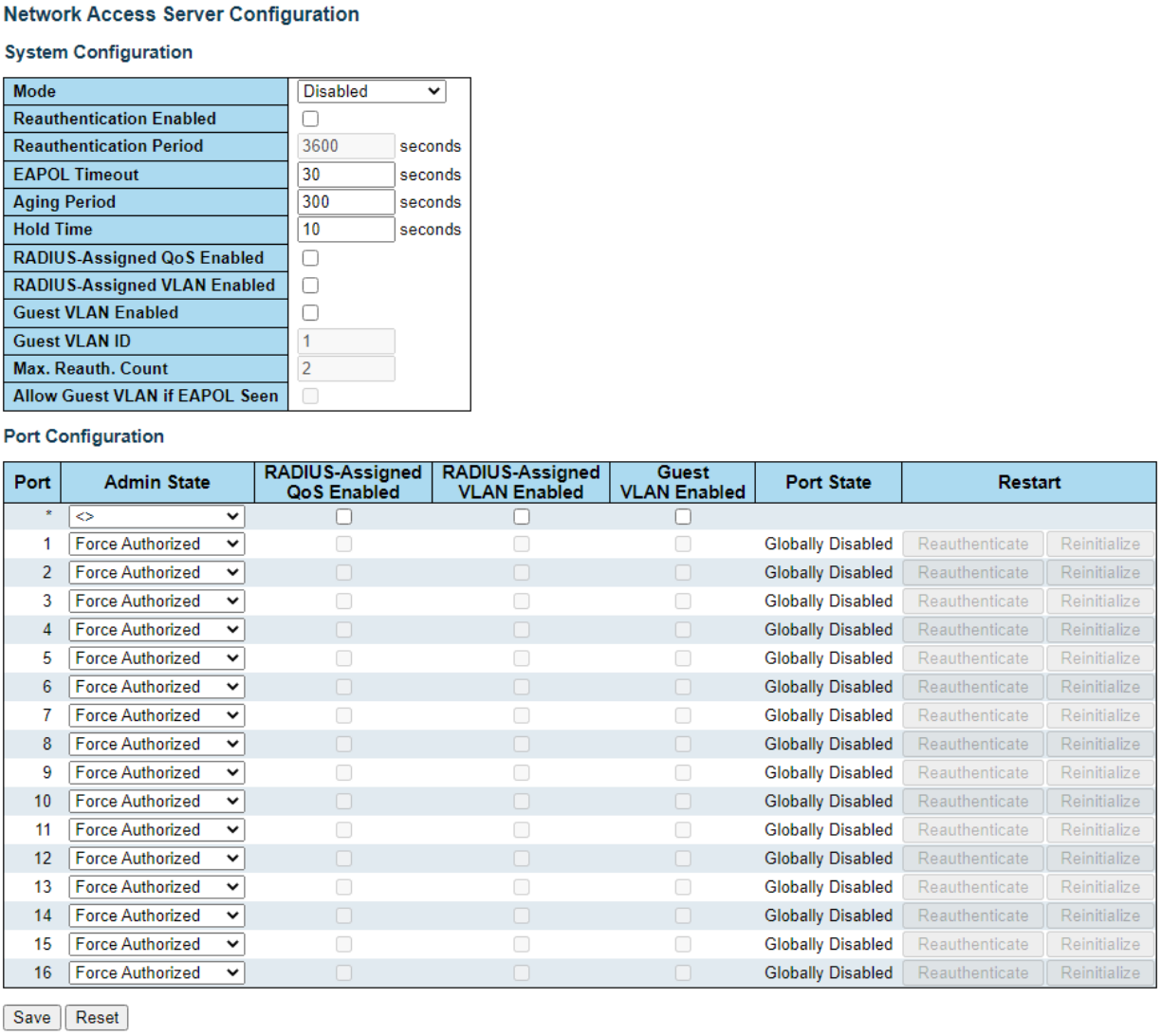
Port	Mode	Limit	Violation Mode	Violation Limit	State
*	<>	4	<>	4	
1	Disabled	4	Protect	4	Disabled
2	Disabled	4	Protect	4	Disabled
3	Disabled	4	Protect	4	Disabled
4	Disabled	4	Protect	4	Disabled
5	Disabled	4	Protect	4	Disabled
6	Disabled	4	Protect	4	Disabled
7	Disabled	4	Protect	4	Disabled
8	Disabled	4	Protect	4	Disabled
9	Disabled	4	Protect	4	Disabled
10	Disabled	4	Protect	4	Disabled
11	Disabled	4	Protect	4	Disabled
12	Disabled	4	Protect	4	Disabled
13	Disabled	4	Protect	4	Disabled
14	Disabled	4	Protect	4	Disabled
15	Disabled	4	Protect	4	Disabled
16	Disabled	4	Protect	4	Disabled

Save | Reset

Click "Save" for the changes to take effect.

2.5.2.2. NAS

Click on“Configuration>Security>Network>NAS”.



Network Access Server Configuration

System Configuration

Mode	Disabled
Reauthentication Enabled	
Reauthentication Period	3600 seconds
EAPOL Timeout	30 seconds
Aging Period	300 seconds
Hold Time	10 seconds
RADIUS-Assigned QoS Enabled	
RADIUS-Assigned VLAN Enabled	
Guest VLAN Enabled	
Guest VLAN ID	1
Max. Reauth. Count	2
Allow Guest VLAN if EAPOL Seen	

Port Configuration

Port	Admin State	RADIUS-Assigned QoS Enabled	RADIUS-Assigned VLAN Enabled	Guest VLAN Enabled	Port State	Restart	
*	<>						
1	Force Authorized				Globally Disabled	Reauthenticate	Reinitialize
2	Force Authorized				Globally Disabled	Reauthenticate	Reinitialize
3	Force Authorized				Globally Disabled	Reauthenticate	Reinitialize
4	Force Authorized				Globally Disabled	Reauthenticate	Reinitialize
5	Force Authorized				Globally Disabled	Reauthenticate	Reinitialize
6	Force Authorized				Globally Disabled	Reauthenticate	Reinitialize
7	Force Authorized				Globally Disabled	Reauthenticate	Reinitialize
8	Force Authorized				Globally Disabled	Reauthenticate	Reinitialize
9	Force Authorized				Globally Disabled	Reauthenticate	Reinitialize
10	Force Authorized				Globally Disabled	Reauthenticate	Reinitialize
11	Force Authorized				Globally Disabled	Reauthenticate	Reinitialize
12	Force Authorized				Globally Disabled	Reauthenticate	Reinitialize
13	Force Authorized				Globally Disabled	Reauthenticate	Reinitialize
14	Force Authorized				Globally Disabled	Reauthenticate	Reinitialize
15	Force Authorized				Globally Disabled	Reauthenticate	Reinitialize
16	Force Authorized				Globally Disabled	Reauthenticate	Reinitialize

Save Reset

Click "Save" for the changes to take effect.

2.5.2.3. ACL

2.5.2.3.1. Ports

Click on“Configuration>Security>Network>ACL>Ports”.

ACL Ports Configuration

Port	Policy ID	Action	Rate Limiter ID	Port Redirect	Mirror	Logging	Shutdown	State	Counter
*	0	<>	<>	Disabled / Port 1 / Port 2	<>	<>	<>	<>	*
1	0	Permit	Disabled	Disabled / Port 1 / Port 2	Disabled	Disabled	Disabled	Enabled	0
2	0	Permit	Disabled	Disabled / Port 1 / Port 2	Disabled	Disabled	Disabled	Enabled	1
3	0	Permit	Disabled	Disabled / Port 1 / Port 2	Disabled	Disabled	Disabled	Enabled	0
4	0	Permit	Disabled	Disabled / Port 1 / Port 2	Disabled	Disabled	Disabled	Enabled	4
5	0	Permit	Disabled	Disabled / Port 1 / Port 2	Disabled	Disabled	Disabled	Enabled	0
6	0	Permit	Disabled	Disabled / Port 1 / Port 2	Disabled	Disabled	Disabled	Enabled	0
7	0	Permit	Disabled	Disabled / Port 1 / Port 2	Disabled	Disabled	Disabled	Enabled	0
8	0	Permit	Disabled	Disabled / Port 1 / Port 2	Disabled	Disabled	Disabled	Enabled	883523
9	0	Permit	Disabled	Disabled / Port 1 / Port 2	Disabled	Disabled	Disabled	Enabled	0
10	0	Permit	Disabled	Disabled / Port 1 / Port 2	Disabled	Disabled	Disabled	Enabled	0
11	0	Permit	Disabled	Disabled / Port 1 / Port 2	Disabled	Disabled	Disabled	Enabled	0
12	0	Permit	Disabled	Disabled / Port 1 / Port 2	Disabled	Disabled	Disabled	Enabled	0
13	0	Permit	Disabled	Disabled / Port 1 / Port 2	Disabled	Disabled	Disabled	Enabled	0
14	0	Permit	Disabled	Disabled / Port 1 / Port 2	Disabled	Disabled	Disabled	Enabled	0
				Disabled					

Click "Save" for the changes to take effect.

2.5.2.3.2. Rate Limiters

Click on“Configuration>Security>Network>ACL>Rate Limiters”.

ACL Rate Limiter Configuration

Rate Limiter ID	Rate	Unit
*	10	<>
1	10	pps
2	10	pps
3	10	pps
4	10	pps
5	10	pps
6	10	pps
7	10	pps
8	10	pps
9	10	pps
10	10	pps
11	10	pps
12	10	pps
13	10	pps
14	10	pps
15	10	pps
16	10	pps

Save Reset

Click "Save" for the changes to take effect.

2.5.2.3.3. Access Control List

Click on“Configuration>Security>Network>ACL>Access Control List”.

Access Control List Configuration

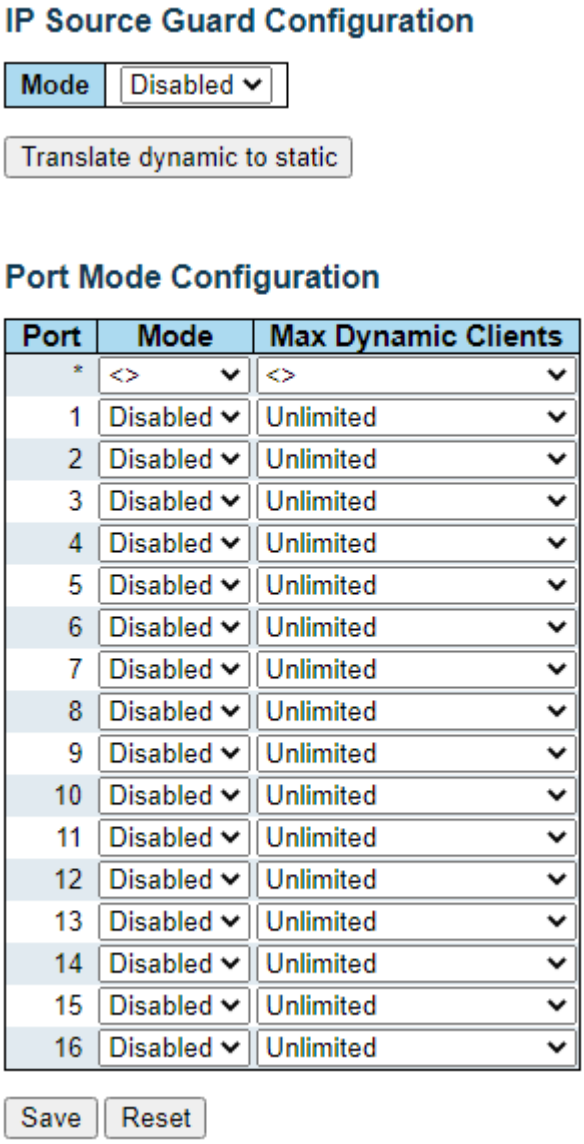
ACE	Ingress Port	Policy / Bitmask	Frame Type	Action	Rate Limiter	Port Redirect	Mirror	Counter	

Click "Save" for the changes to take effect.

2.5.2.4. IP Source Guard

2.5.2.4.1. Configuration

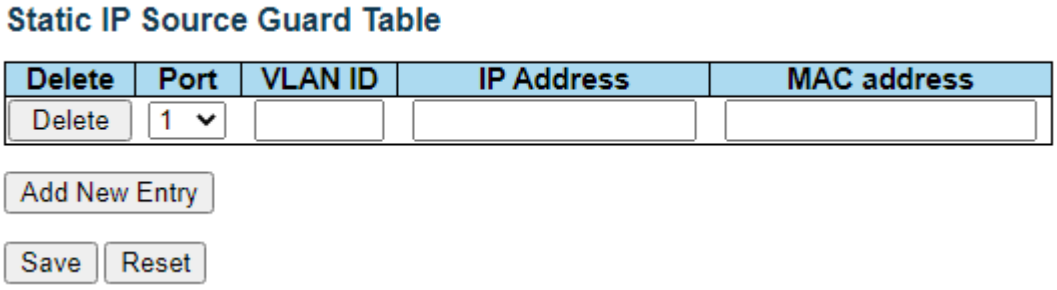
Click on“Configuration>Security>Network>IP Source Guard>Configurationt”.



Click "Save" for the changes to take effect.

2.5.2.4.2. Static Table

Click on“Configuration>Security>Network>IP Source Guard>Static Table”.

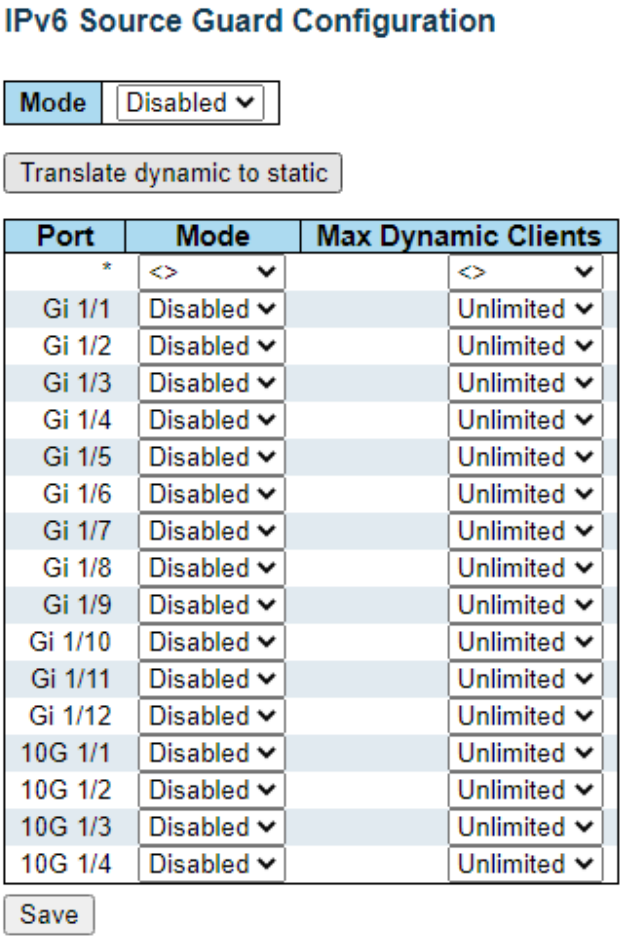


Click "Save" for the changes to take effect.

2.5.2.5. IPv6 Source Guard

2.5.2.5.1. Configuration

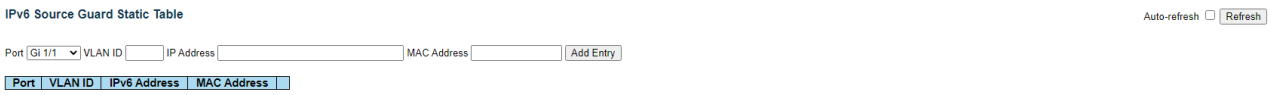
Click on“Configuration>Security>Network>IPv6 Source Guard>Configuration”.



Click "Save" for the changes to take effect.

2.5.2.5.2. Static Table

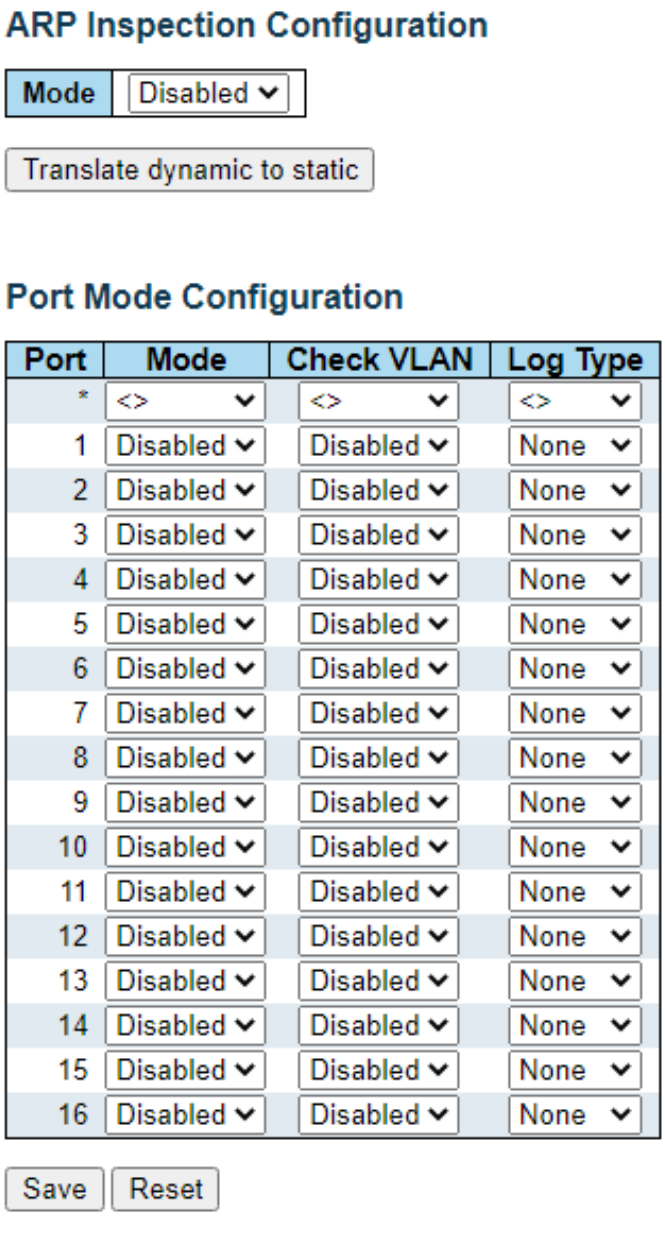
Click on“Configuration>Security>Network>IPv6 Source Guard>Static Table”.



2.5.2.6. ARP Inspection

2.5.2.6.1. Port Configuration

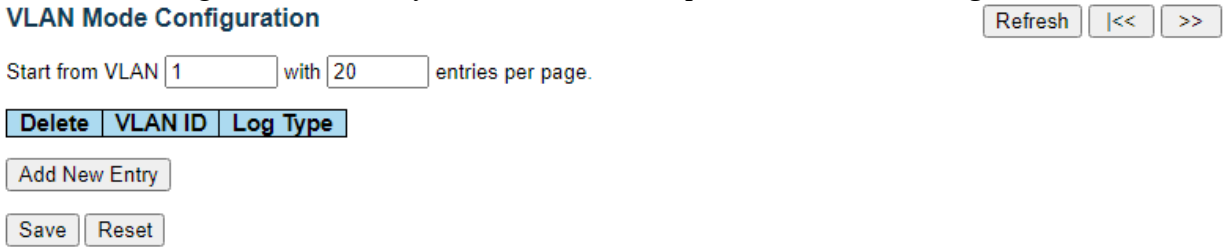
Click on“Configuration>Security>Network>ARP Inspection>Port Configuration”.



Click "Save" for the changes to take effect.

2.5.2.6.2. VLAN Configuration

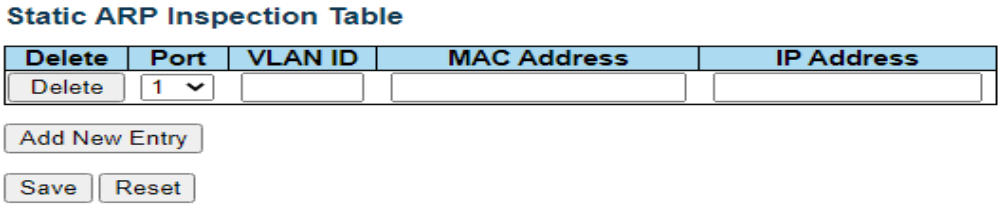
Click on“Configuration>Security>Network>ARP Inspection>VLAN Configuration”.



Click "Save" for the changes to take effect.

2.5.2.6.3. Static Table

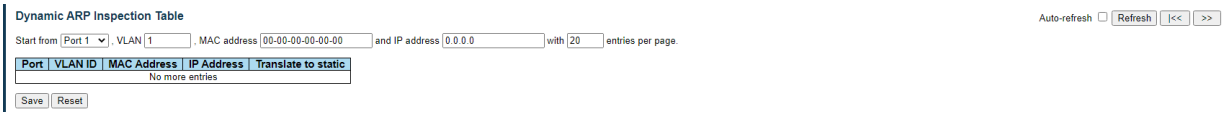
Click on“Configuration>Security>Network>ARP Inspection>Static Table”.



Click "Save" for the changes to take effect.

2.5.2.6.4. Dynamic Table

Click on“Configuration>Security>Network>ARP Inspection>Dynamic Table”.

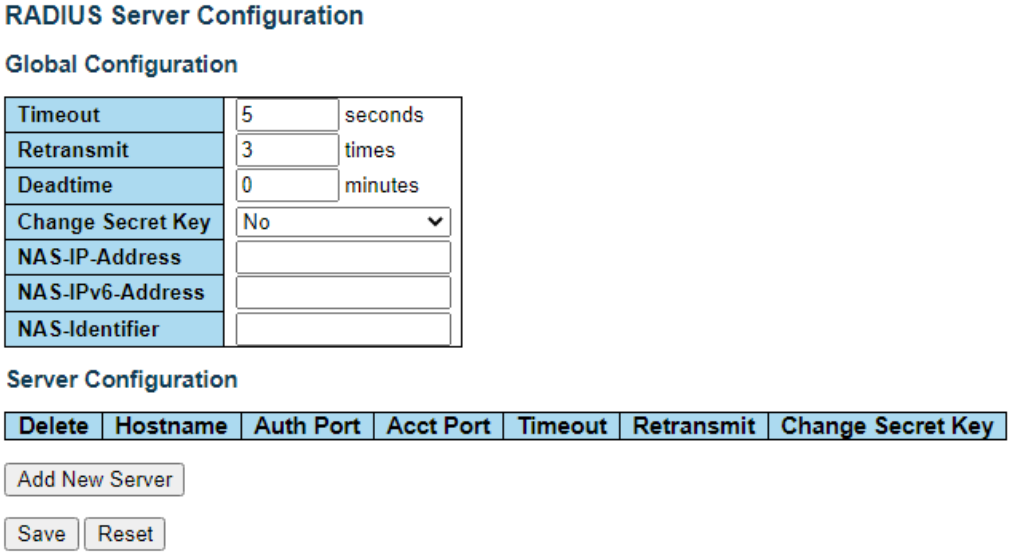


Click "Save" for the changes to take effect.

2.5.3 AAA

2.5.3.1. RADIUS

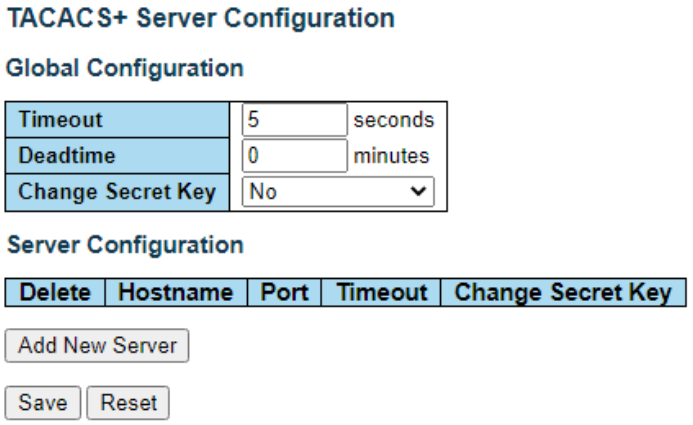
Click on“Configuration>Security>AAA>RADIUS”.



Click "Save" for the changes to take effect.

2.5.3.2. TACACS+

Click on“Configuration>Security>AAA>TACACS+”.

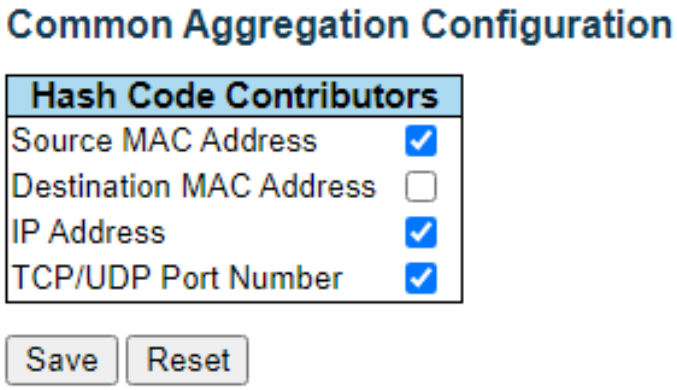


Click "Save" for the changes to take effect.

2.6. Aggregation

2.6.1. Common

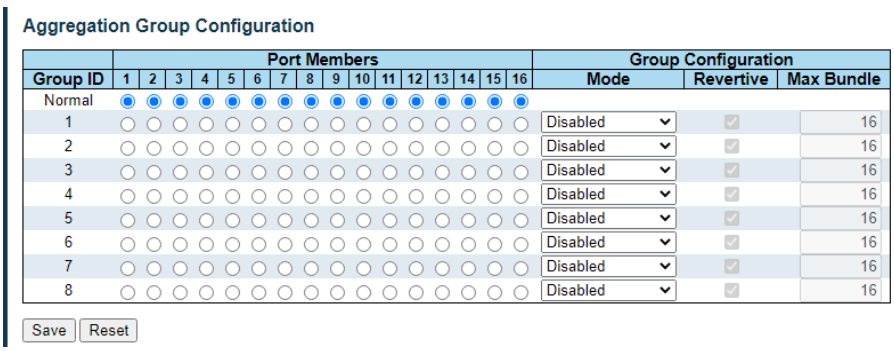
Click on“Configuration>Aggregation>Common”.



Click "Save" for the changes to take effect.

2.6.2. Groups

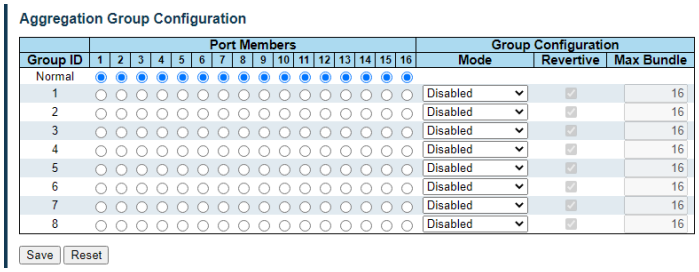
Click on“Configuration>Aggregation>Groups”.



Click "Save" for the changes to take effect.

2.6.3. LACP

Click on“Configuration>Aggregation>LACP”.

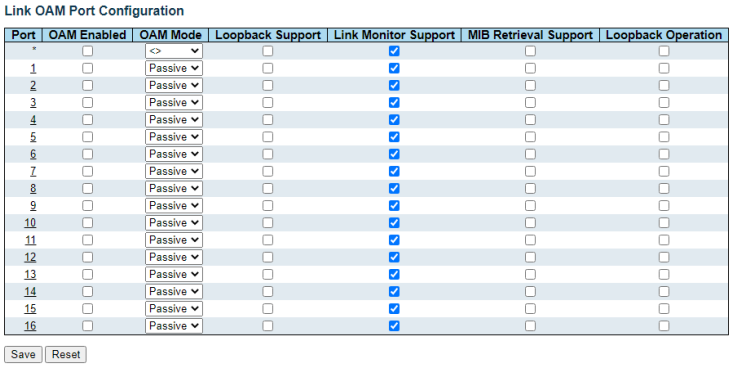


Click "Save" for the changes to take effect.

2.7. Link OAM

2.7.1. Port Settings

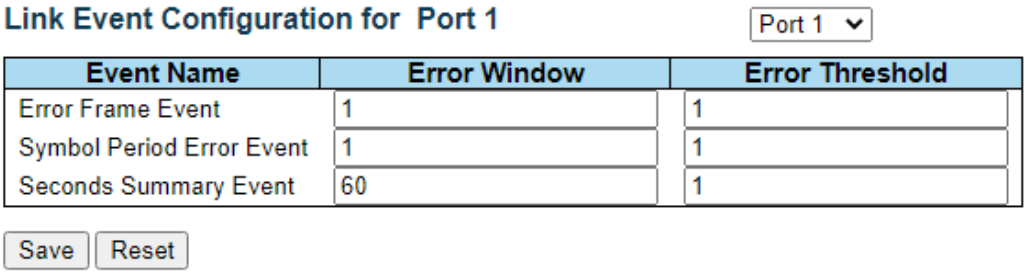
Click on “Configuration>Link OAM>Port Settings”.



Click "Save" for the changes to take effect.

2.7.2. Event Settings

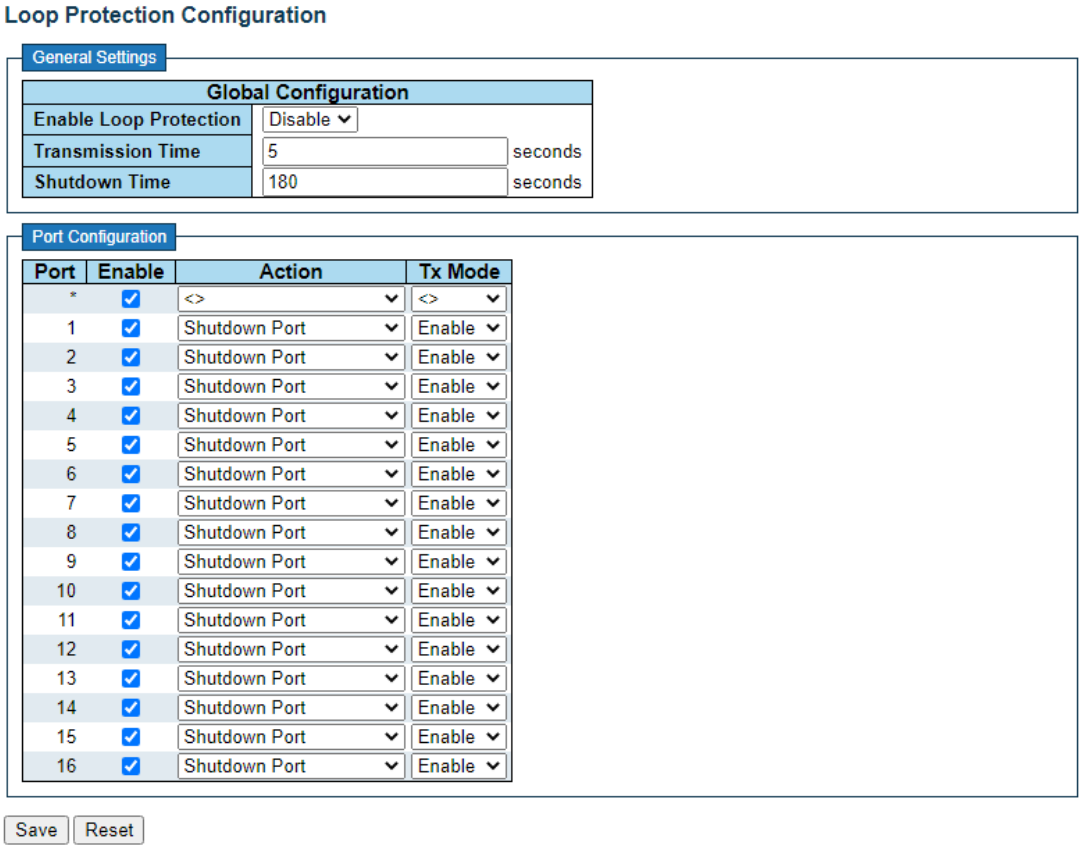
Click on“Configuration>Link OAM>Event Settings”.



Click "Save" for the changes to take effect.

2.8. Loop Protection

Click on“Configuration>Loop Protection>”.

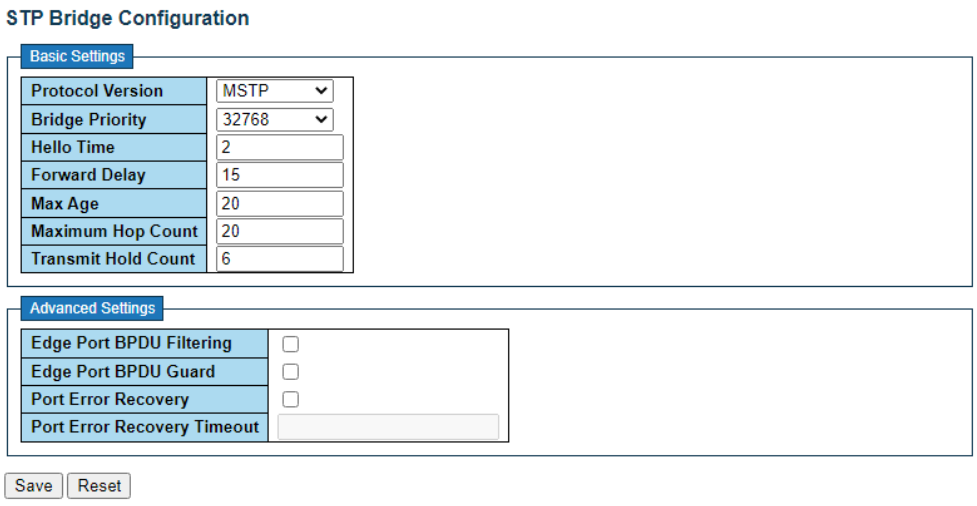


Click "Save" for the changes to take effect.

2.9. Spanning Tree

2.9.1. Bridge Settings

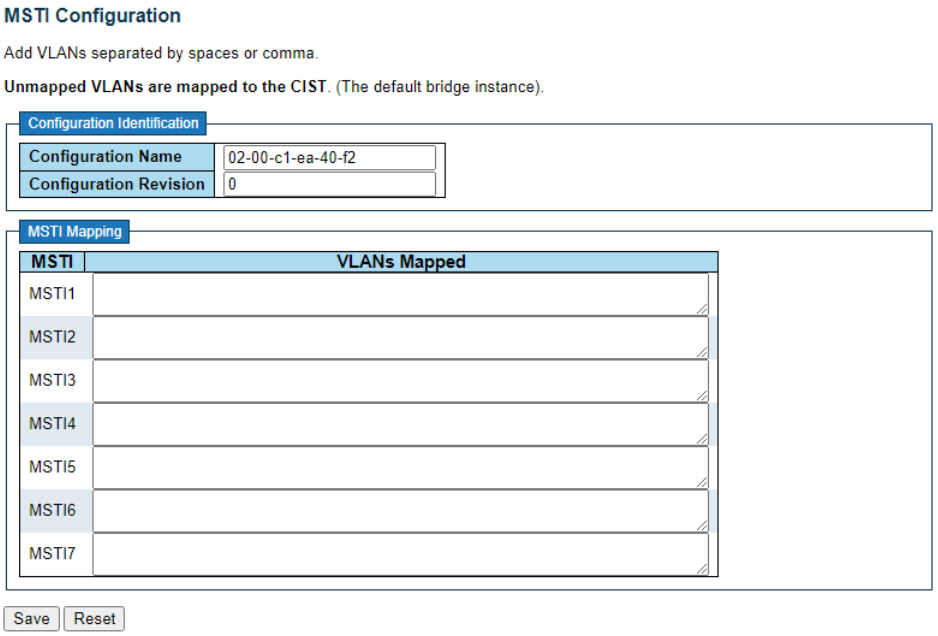
Click on“Configuration>Spanning Tree>Bridge Settings”.



Click "Save" for the changes to take effect.

2.9.2. MSTI Mapping

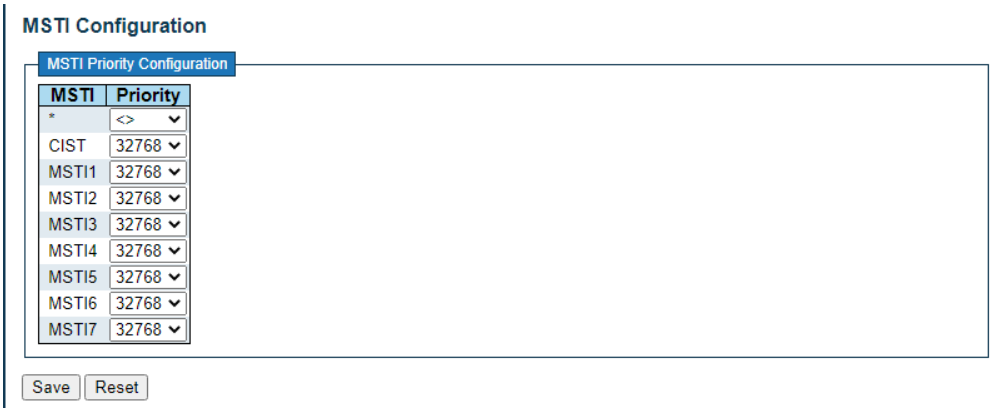
Click on“Configuration>Spanning Tree>MSTI Mapping”.



Click "Save" for the changes to take effect.

2.9.3. MSTI Priorities

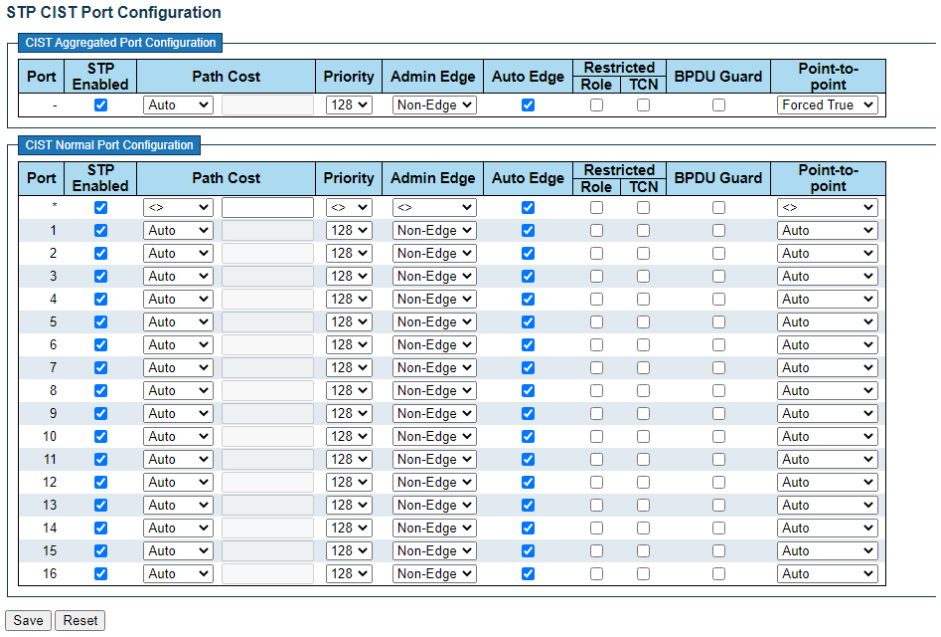
Click on“Configuration>Spanning Tree>MSTI Priorities”.



Click "Save" for the changes to take effect.

2.9.4. CIST Ports

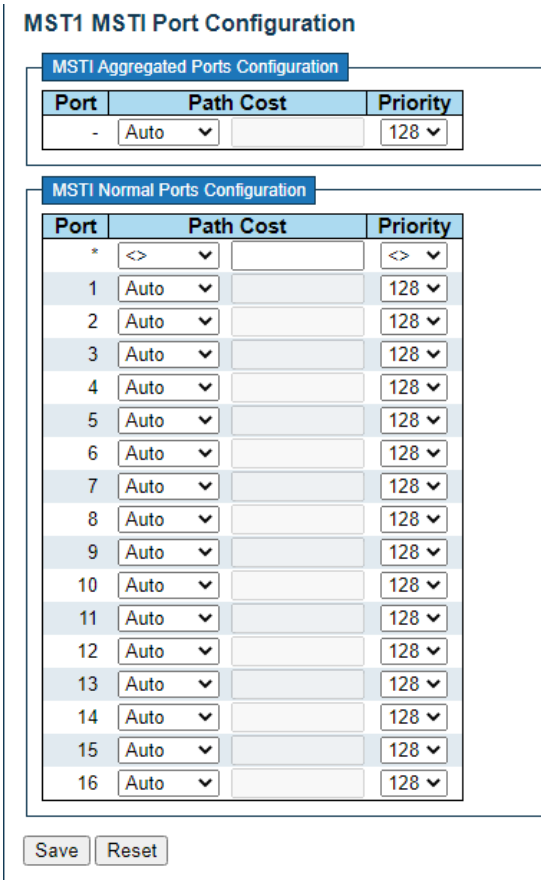
Click on“Configuration>Spanning Tree>CIST Ports”.



Click "Save" for the changes to take effect.

2.9.5. MSTI Ports

Click on“Configuration>Spanning Tree>MSTI Ports”.

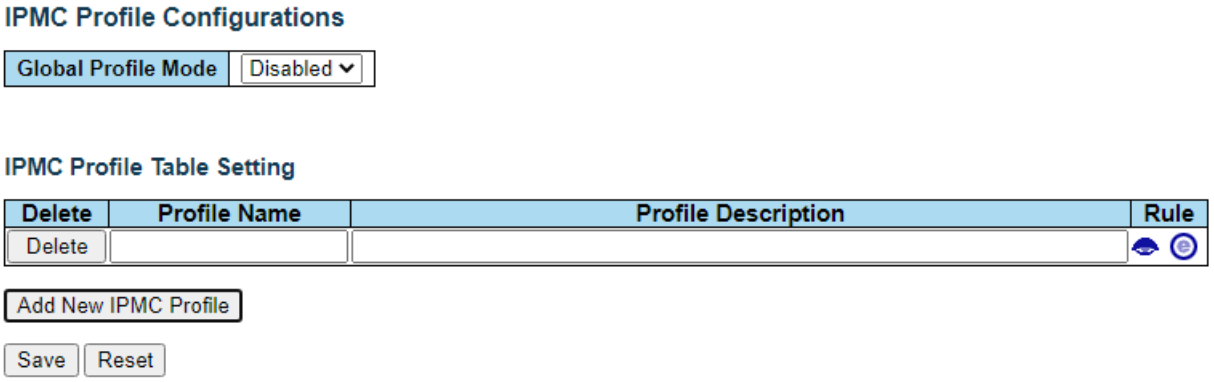


Click "Save" for the changes to take effect.

2.10. IPMC Profile

2.10.1. Profile Table

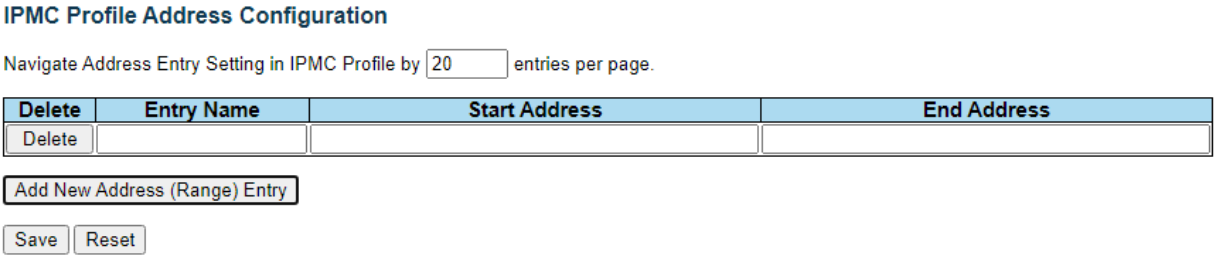
Click on“Configuration>IPMC Profile>Profile Table”.



Click "Save" for the changes to take effect.

2.10.2. Address Entry

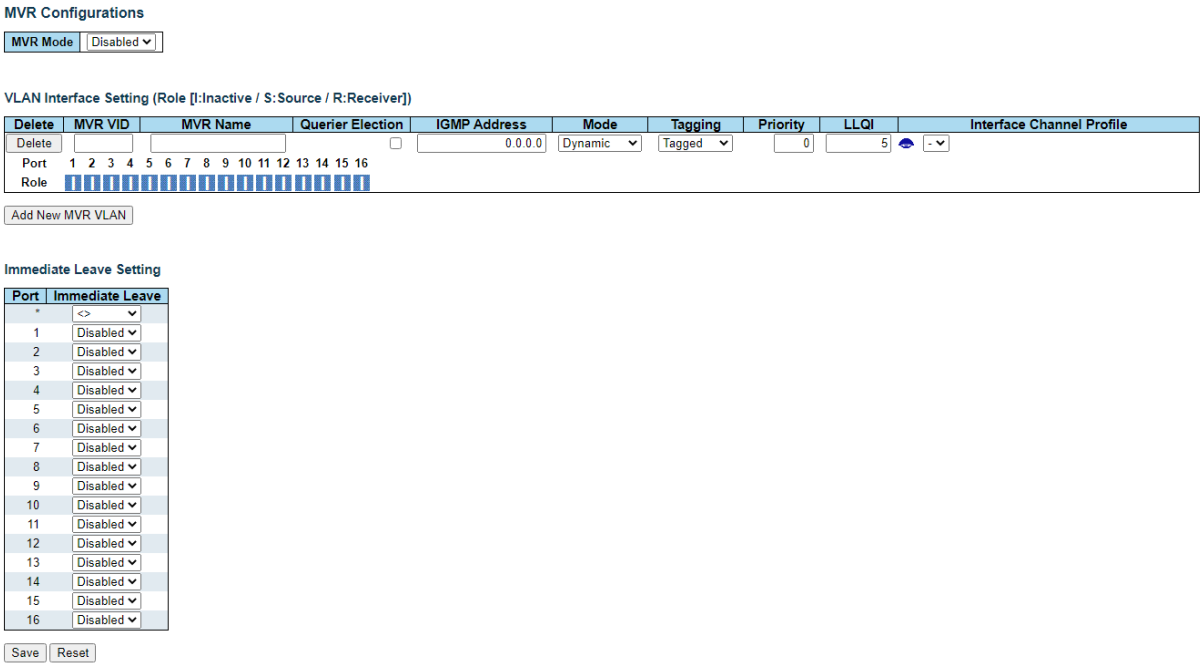
Click on“Configuration>IPMC Profile>Address Entry”.



Click "Save" for the changes to take effect.

2.11. MVR

Click on“Configuration>MVR”.



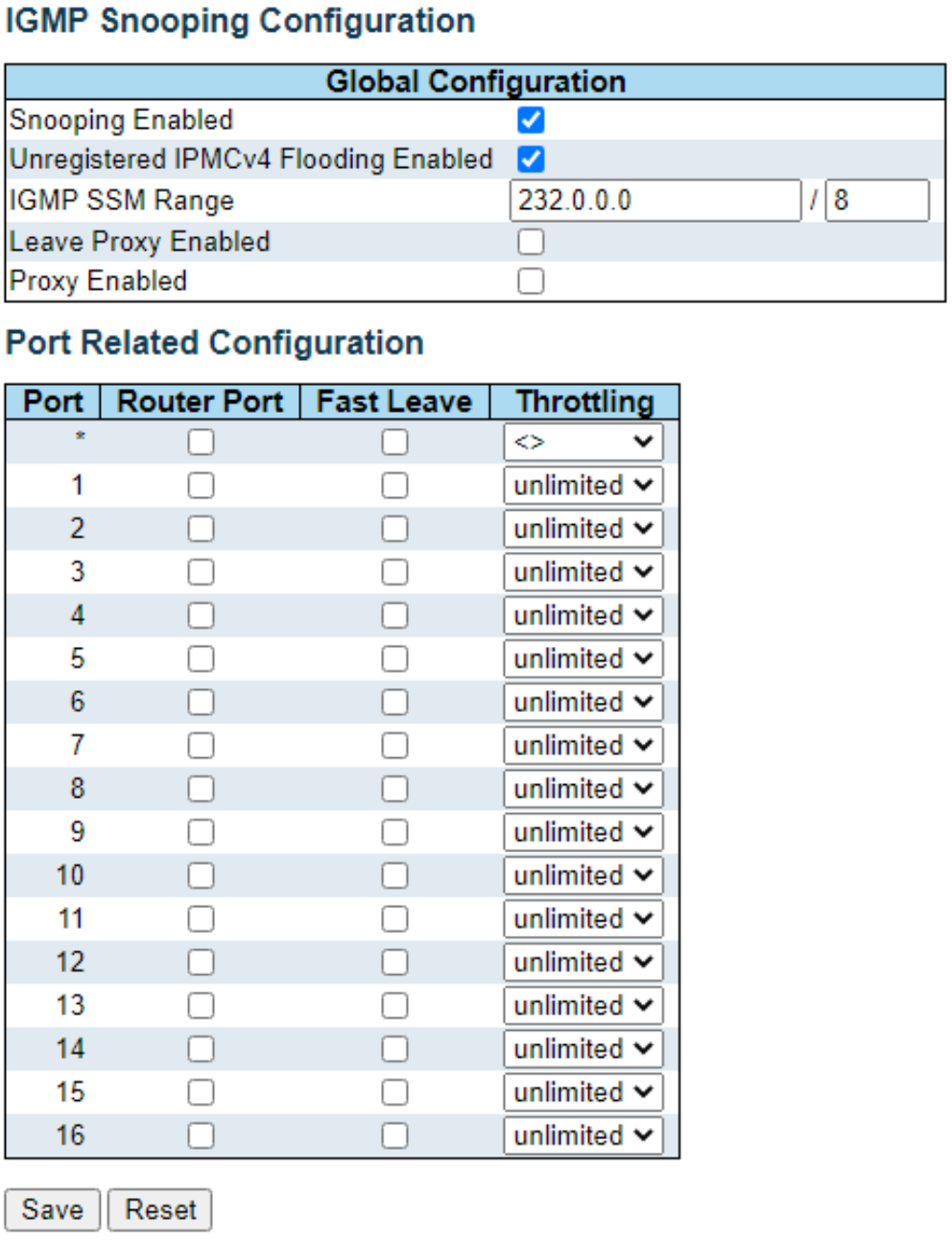
Click "Save" for the changes to take effect.

2.12. IPMC

2.12.1. IGMP Snooping

2.12.1.1. Basic Configuration

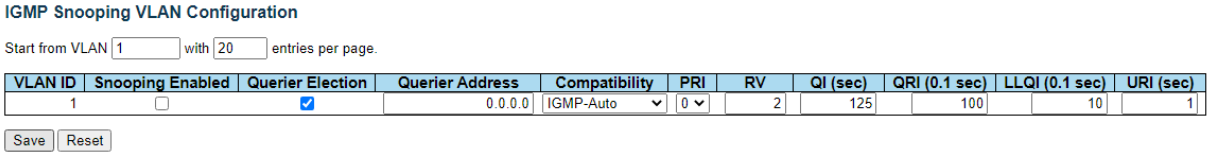
Click on“Configuration>IGMP>IGMP Snooping>Basic Configuration”.



Click "Save" for the changes to take effect.

2.12.1.2. VLAN Configuration

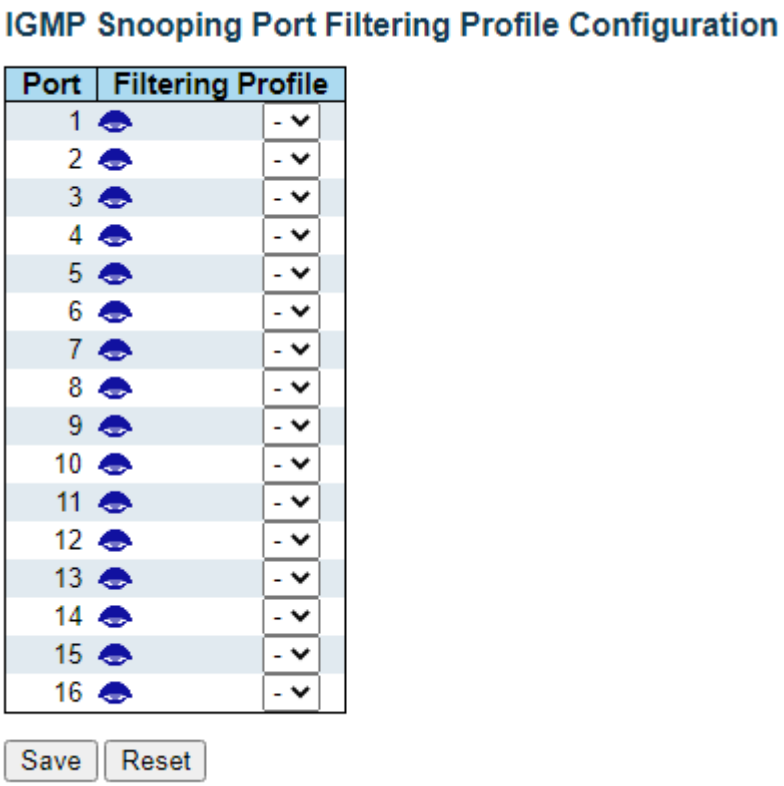
Click on“Configuration>IGMP>IGMP Snooping>VLAN Configuration”.



Click "Save" for the changes to take effect.

2.12.1.3. Port Filtering Profile

Click on“Configuration>IGMP>IGMP Snooping>Port Filtering Profile”.

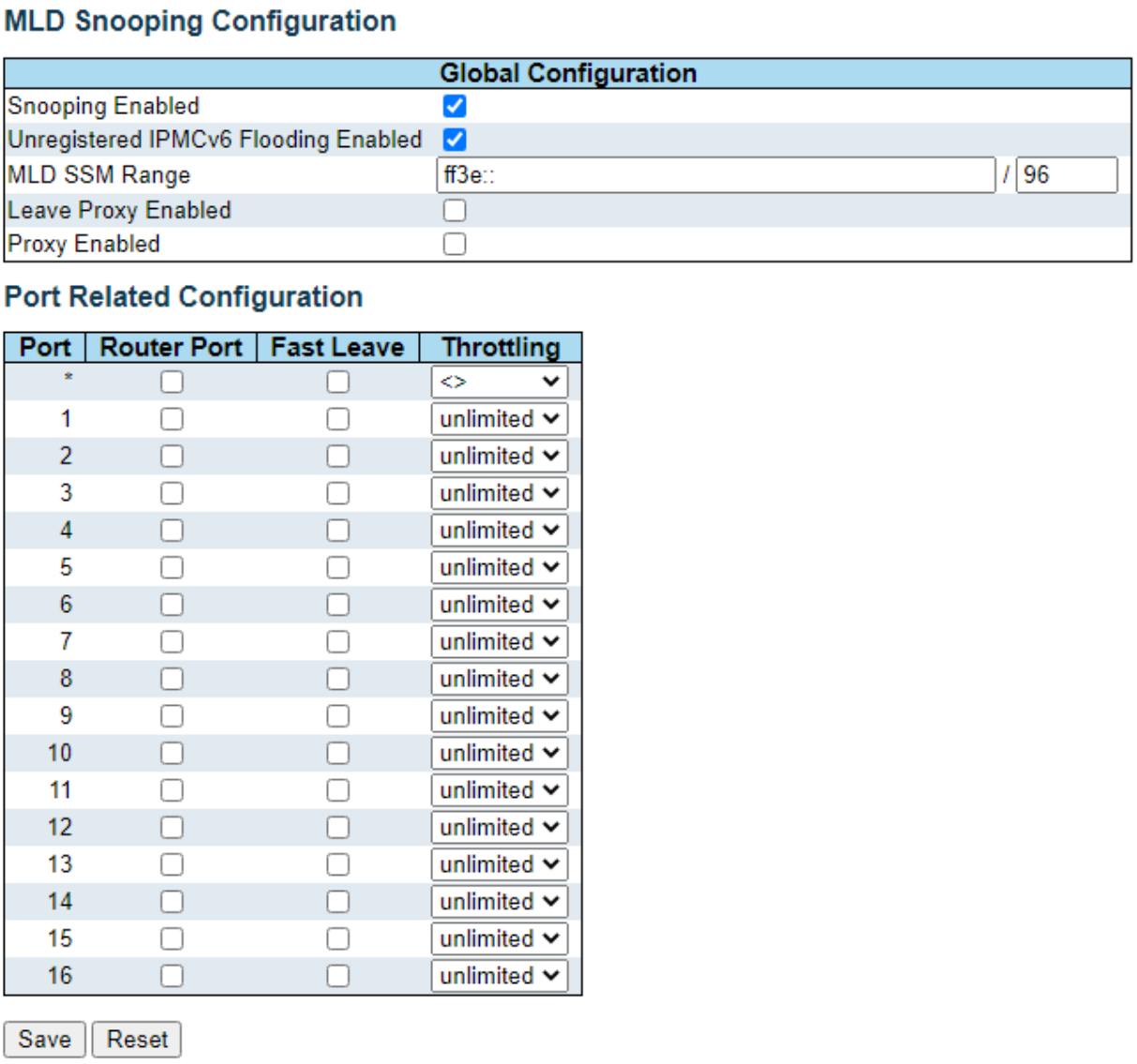


Click "Save" for the changes to take effect.

2.12.2. MLD Snooping

2.12.2.1. Basic Configuration

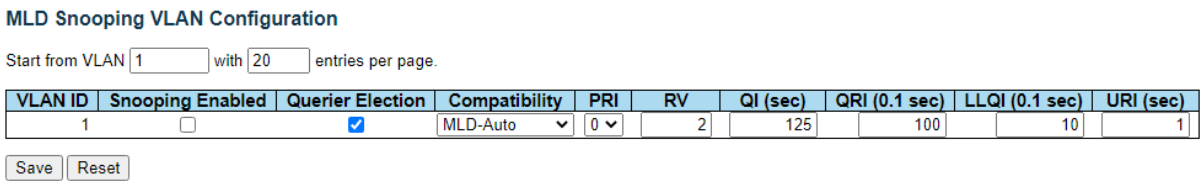
Click on“Configuration>IGMP>MLD Snooping>Basic Configuration”.



Click "Save" for the changes to take effect.

2.12.2.2. VLAN Configuration

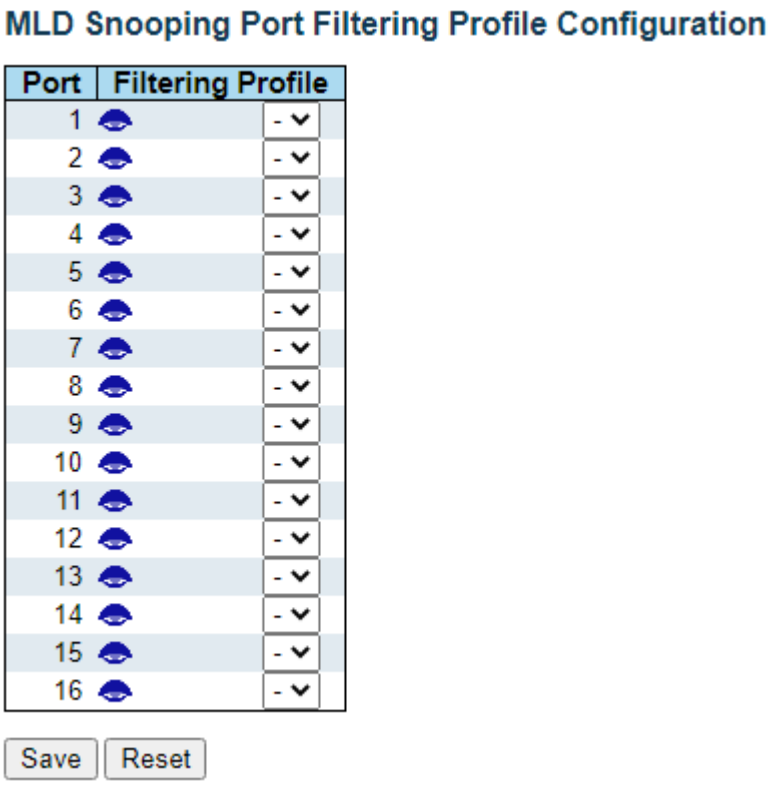
Click on“Configuration>IGMP>MLD Snooping>VLAN Configuration”.



Click "Save" for the changes to take effect.

2.12.2.3. Port Filtering Profile

Click on“Configuration>IGMP>MLD Snooping>Port Filtering Profile”.

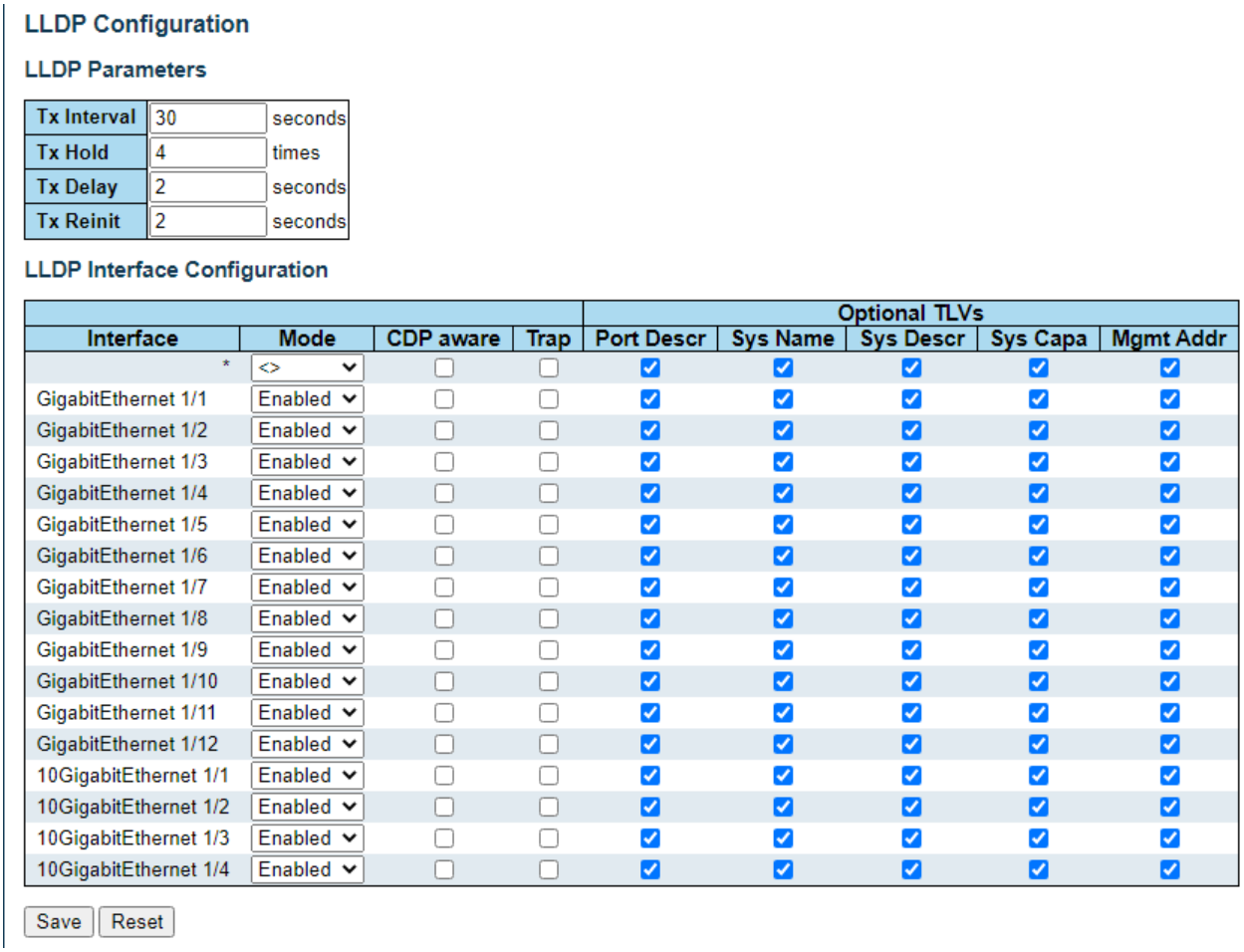


Click "Save" for the changes to take effect.

2.13. LLDP

2.13.1. LLDP

Click on“Configuration>LLDP>LLDP”.



LLDP Configuration

LLDP Parameters

Tx Interval	30	seconds
Tx Hold	4	times
Tx Delay	2	seconds
Tx Reinit	2	seconds

LLDP Interface Configuration

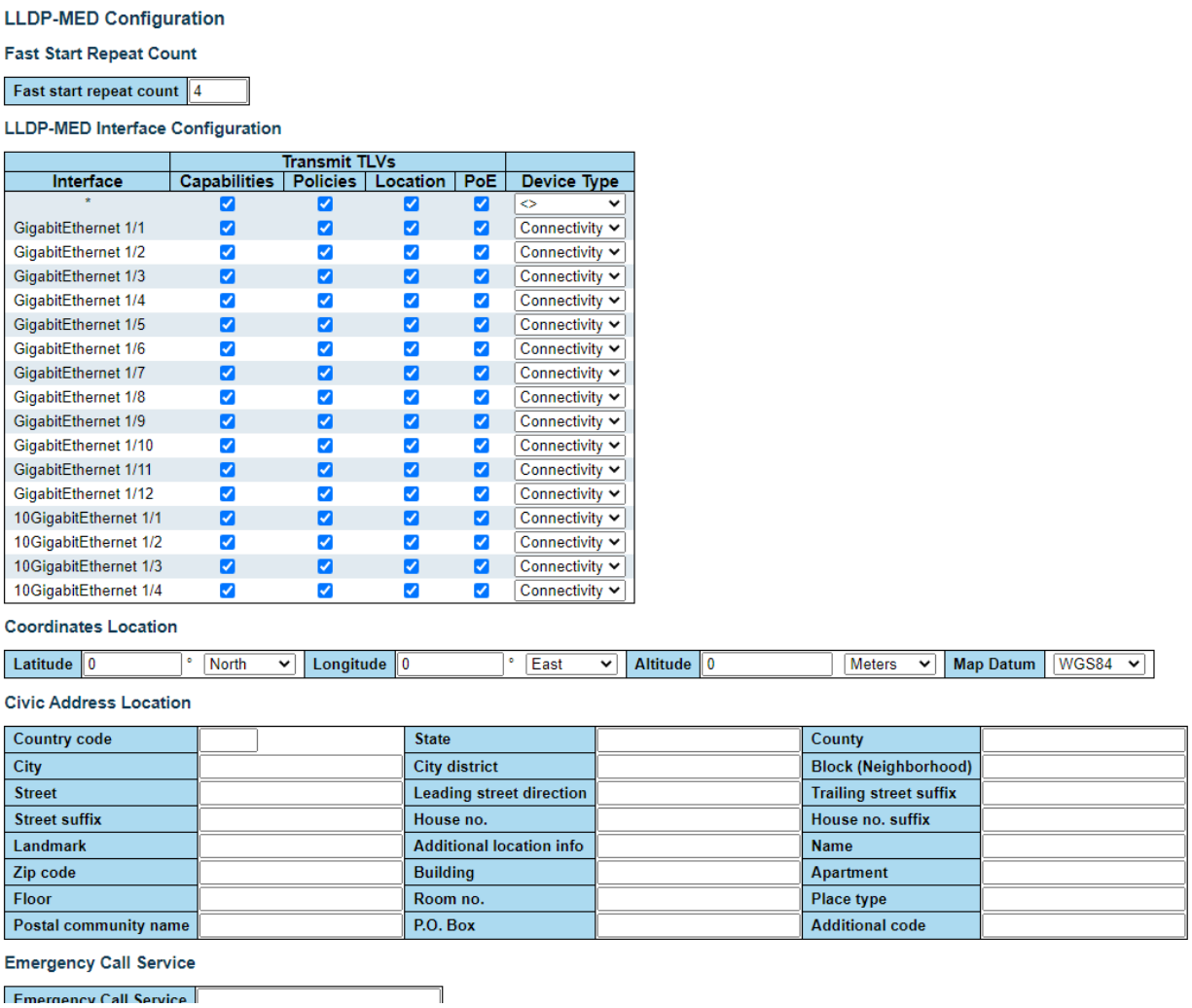
				Optional TLVs				
Interface	Mode	CDP aware	Trap	Port Descr	Sys Name	Sys Descr	Sys Capa	Mgmt Addr
*	<>	☐	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/1	Enabled	☐	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/2	Enabled	☐	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/3	Enabled	☐	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/4	Enabled	☐	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/5	Enabled	☐	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/6	Enabled	☐	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/7	Enabled	☐	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/8	Enabled	☐	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/9	Enabled	☐	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/10	Enabled	☐	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/11	Enabled	☐	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/12	Enabled	☐	☐	☑	☑	☑	☑	☑
10GigabitEthernet 1/1	Enabled	☐	☐	☑	☑	☑	☑	☑
10GigabitEthernet 1/2	Enabled	☐	☐	☑	☑	☑	☑	☑
10GigabitEthernet 1/3	Enabled	☐	☐	☑	☑	☑	☑	☑
10GigabitEthernet 1/4	Enabled	☐	☐	☑	☑	☑	☑	☑

Save Reset

Click "Save" for the changes to take effect.

2.13.2. LLDP-MEO

Click on“Configuration>LLDP>LLDP-MEO”.



LLDP-MED Configuration

Fast Start Repeat Count

Fast start repeat count	4

LLDP-MED Interface Configuration

Interface	Transmit TLVs				
	Capabilities	Policies	Location	PoE	Device Type
*	☑	☑	☑	☑	<>
GigabitEthernet 1/1	☑	☑	☑	☑	Connectivity
GigabitEthernet 1/2	☑	☑	☑	☑	Connectivity
GigabitEthernet 1/3	☑	☑	☑	☑	Connectivity
GigabitEthernet 1/4	☑	☑	☑	☑	Connectivity
GigabitEthernet 1/5	☑	☑	☑	☑	Connectivity
GigabitEthernet 1/6	☑	☑	☑	☑	Connectivity
GigabitEthernet 1/7	☑	☑	☑	☑	Connectivity
GigabitEthernet 1/8	☑	☑	☑	☑	Connectivity
GigabitEthernet 1/9	☑	☑	☑	☑	Connectivity
GigabitEthernet 1/10	☑	☑	☑	☑	Connectivity
GigabitEthernet 1/11	☑	☑	☑	☑	Connectivity
GigabitEthernet 1/12	☑	☑	☑	☑	Connectivity
10GigabitEthernet 1/1	☑	☑	☑	☑	Connectivity
10GigabitEthernet 1/2	☑	☑	☑	☑	Connectivity
10GigabitEthernet 1/3	☑	☑	☑	☑	Connectivity
10GigabitEthernet 1/4	☑	☑	☑	☑	Connectivity

Coordinates Location

Latitude	0	°	North	Longitude	0	°	East	Altitude	0	Meters	Map Datum	WGS84

Civic Address Location

Country code		State		County	
City		City district		Block (Neighborhood)	
Street		Leading street direction		Trailing street suffix	
Street suffix		House no.		House no. suffix	
Landmark		Additional location info		Name	
Zip code		Building		Apartment	
Floor		Room no.		Place type	
Postal community name		P.O. Box		Additional code	

Emergency Call Service

Emergency Call Service	

Emergency Call Service

Emergency Call Service	

Policies

Delete	Policy ID	Application Type	Tag	VLAN ID	L2 Priority	DSCP
No entries present						

Add New Policy

Save Reset

Click "Save" for the changes to take effect.

2.14. POE

Click on“Configuration>POE”.

Power Over Ethernet Configuration

Reserved Power determined by	◉ Class	○ Allocation	○ LLDP-MED
Power Management Mode	◉ Actual Consumption	○ Reserved Power	
Capacitor Detection	◉ Disabled	○ Enabled	

PoE Power Supply Configuration

Primary Power Supply [W]
250

PoE Port Configuration

Port	PoE Mode	Priority	Maximum Power [W]
*	<>	<>	0
1	PoE+	Low	0
2	PoE+	Low	0
3	PoE+	Low	0
4	PoE+	Low	0
5	PoE+	Low	0
6	PoE+	Low	0
7	PoE+	Low	0
8	PoE+	Low	0

Save Reset

Click "Save" for the changes to take effect.

2.15. EPS

Click on“Configuration>EPS”.

Ethernet Protection Switching

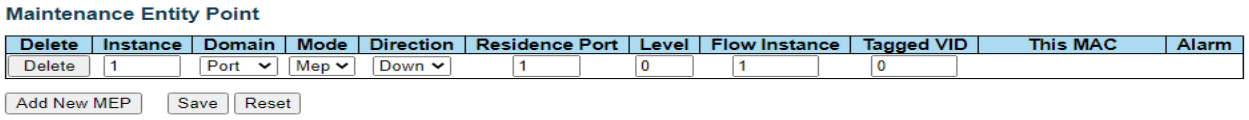
Delete	EPS ID	Domain	Architecture	W Flow	P Flow	W SF MEP	P SF MEP	APS MEP	Alarm
Delete	1	Port	1+1	1	1	1	1	1	

Add New EPS Save Reset

Click "Save" for the changes to take effect.

2.16. MEP

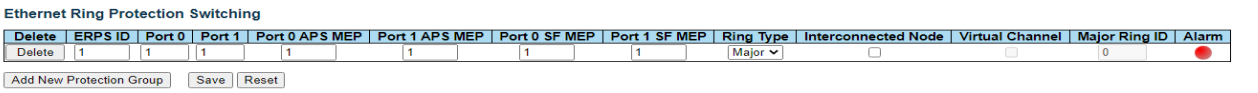
Click on“Configuration>MEP”.



Click "Save" for the changes to take effect.

2.17. ERPS

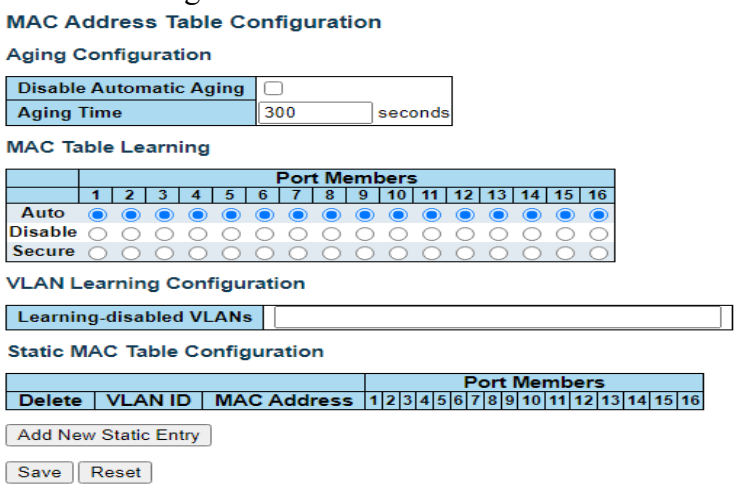
Click on“Configuration>ERPS”.



Click "Save" for the changes to take effect.

2.18. MAC Table

Click on“Configuration>MAC Table”.

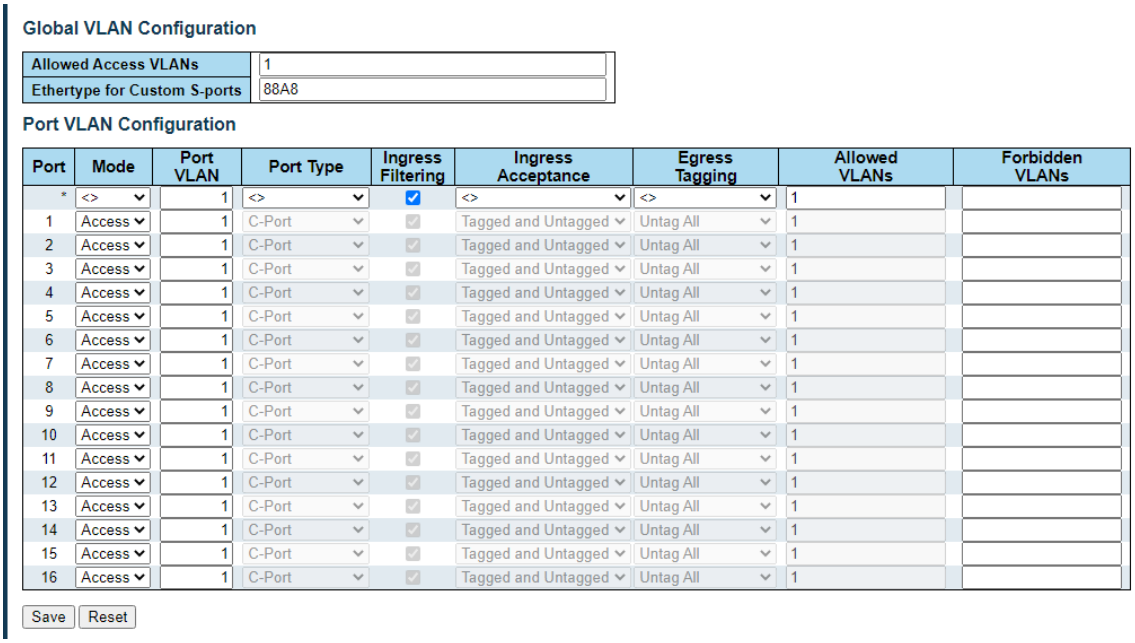


Click "Save" for the changes to take effect.

2.19. VLANS

2.19.1. Configuration

Click on“Configuration>VLANS>Configuration”.



Global VLAN Configuration

Allowed Access VLANs	1
Ethertype for Custom S-ports	88A8

Port VLAN Configuration

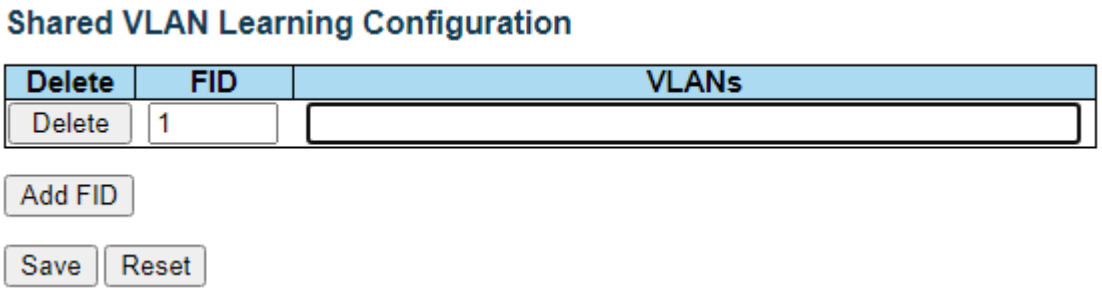
Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<>	1	<>	☑	<>	<>	1	
1	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
2	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
3	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
4	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
5	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
6	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
7	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
8	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
9	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
10	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
11	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
12	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
13	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
14	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
15	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
16	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	

Save Reset

Click "Save" for the changes to take effect.

2.19.2. SVL

Click on“Configuration>VLANS>SVL”.



Shared VLAN Learning Configuration

Delete	FID	VLANs
Delete	1	

Add FID

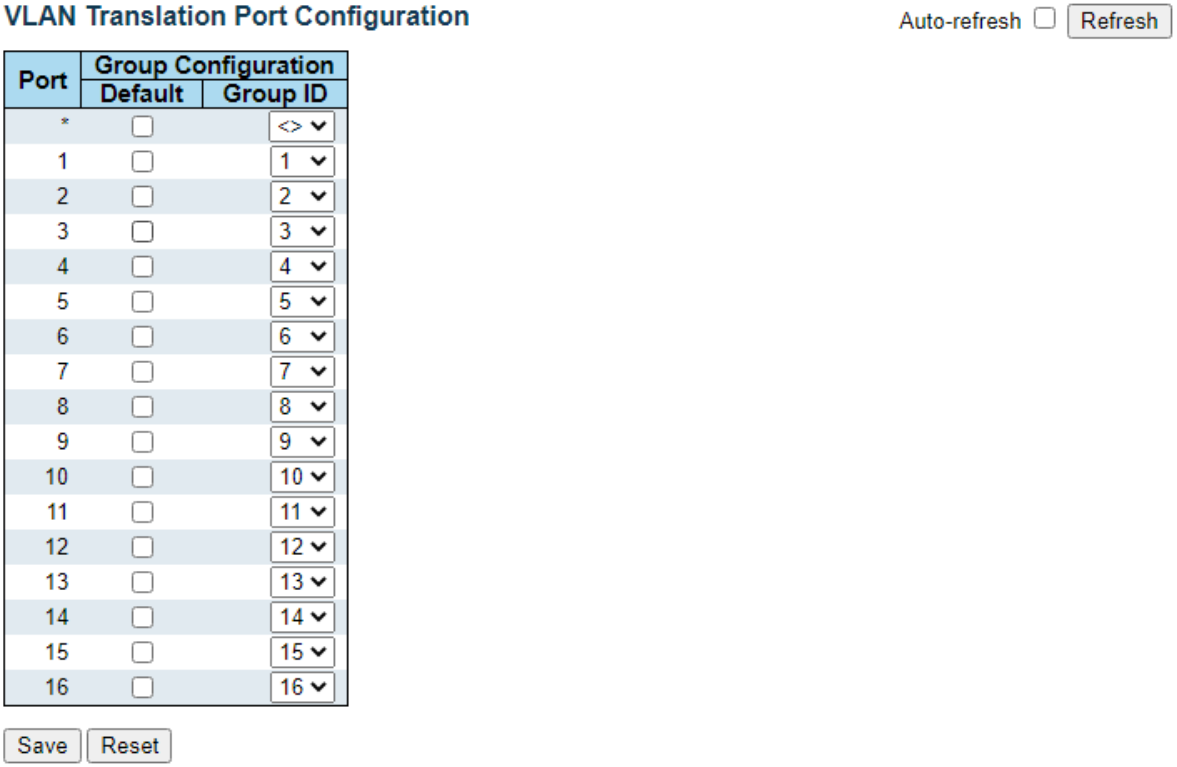
Save Reset

Click "Save" for the changes to take effect.

2.20. VLAN Translation

2.20.1. Port to Group Configuration

Click on“Configuration>VLAN Translation>Port to Group Configuration”.

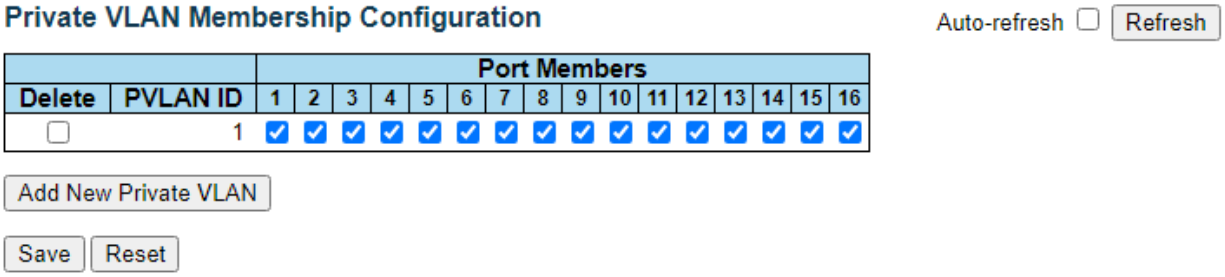


Click "Save" for the changes to take effect.

2.21. Private VLAN

2.21.1. Membership

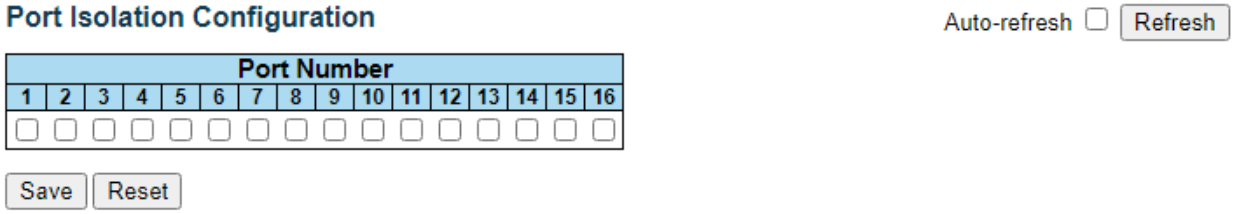
Click on “Configuration>Private VLANs>Membership”.



Click "Save" for the changes to take effect.

2.21.2. Port Isolation

Click on “Configuration>Private VLANs>Port Isolation”.

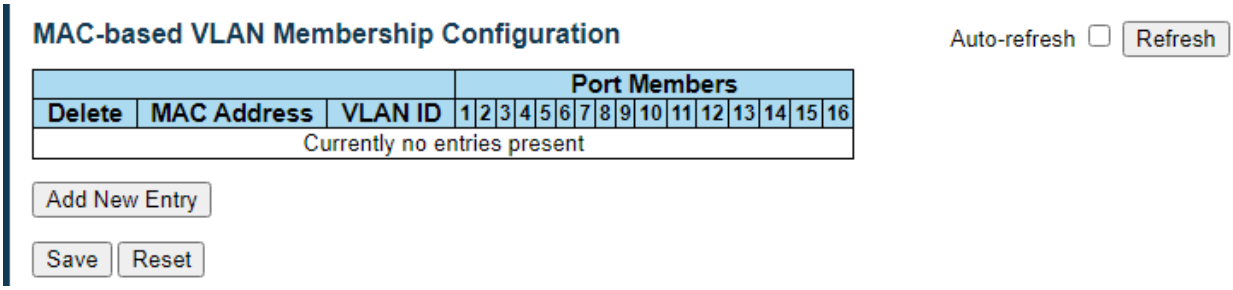


Click "Save" for the changes to take effect.

2.22. VCL

2.22.1. MAC-based VLAN

Click on “Configuration>VCL>MAC-based VLAN”.

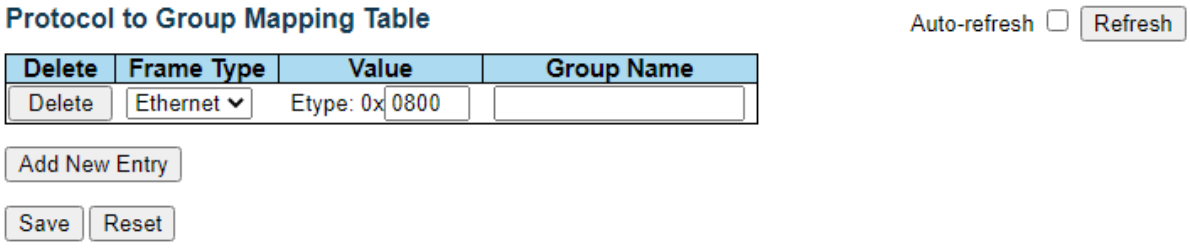


Click "Save" for the changes to take effect.

2.22.2. Protocol-based VLAN

2.22.2.1. Protocol to Group

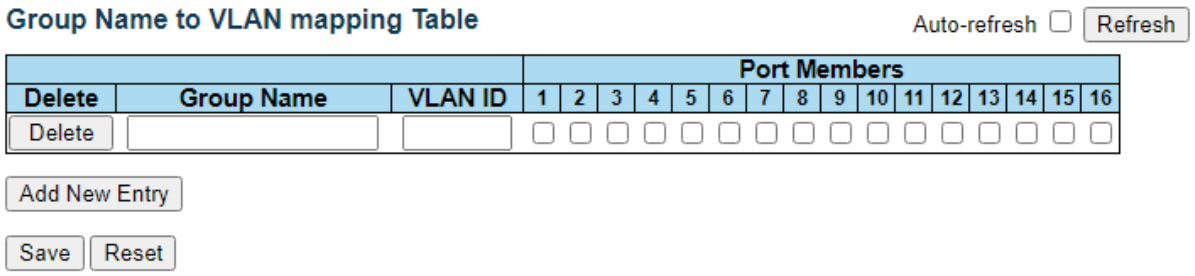
Click on “Configuration>VCL>Protocol-based VLAN>rotocol to Group”.



Click "Save" for the changes to take effect.

2.22.2.2. Group to VLAN

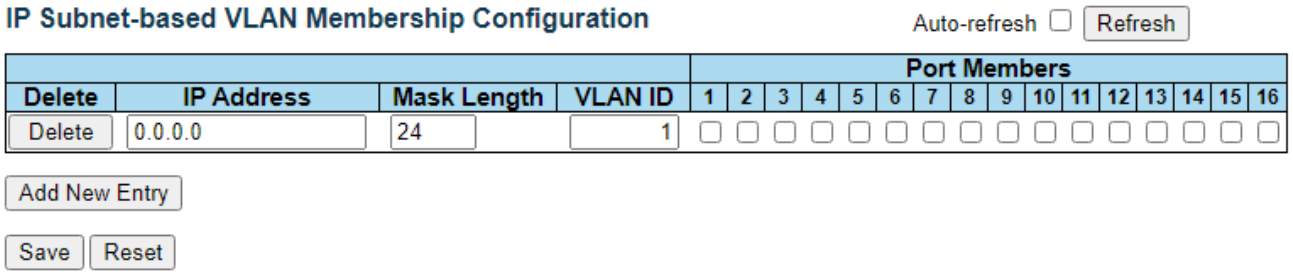
Click on “Configuration>VCL>Protocol-based VLAN>Group to VLAN”.



Click "Save" for the changes to take effect.

2.22.3. IP Subnet-based VLAN

Click on “Configuration>VCL>IP Subnet-based VLAN”.



Click "Save" for the changes to take effect.

2.23. Voice VLAN

2.23.1. Configuration

Click on “Configuration>Voice VLAN>Configuration”.

Voice VLAN Configuration

Mode	Disabled
VLAN ID	1000
Aging Time	86400 seconds
Traffic Class	7 (High)

Port Configuration

Port	Mode	Security	Discovery Protocol
*	<>	<>	<>
1	Disabled	Disabled	OUI
2	Disabled	Disabled	OUI
3	Disabled	Disabled	OUI
4	Disabled	Disabled	OUI
5	Disabled	Disabled	OUI
6	Disabled	Disabled	OUI
7	Disabled	Disabled	OUI
8	Disabled	Disabled	OUI
9	Disabled	Disabled	OUI
10	Disabled	Disabled	OUI
11	Disabled	Disabled	OUI
12	Disabled	Disabled	OUI
13	Disabled	Disabled	OUI
14	Disabled	Disabled	OUI
15	Disabled	Disabled	OUI
16	Disabled	Disabled	OUI

Save Reset

Click "Save" for the changes to take effect.

2.23.2. OUI

Click on “Configuration>Voice VLAN>OUI”.

Voice VLAN OUI Table

Delete	Telephony OUI	Description
☐	00-01-e3	Siemens AG phones
☐	00-03-6b	Cisco phones
☐	00-0f-e2	H3C phones
☐	00-60-b9	Philips and NEC AG phones
☐	00-d0-1e	Pingtel phones
☐	00-e0-75	Polycom phones
☐	00-e0-bb	3Com phones

Add New Entry

Save Reset

Click "Save" for the changes to take effect.

2.24. Ethernet Services

2.24.1. L2CP

Click on “Configuration>Ethernet Services>L2CP”.

L2CP Port Configuration

Port 1 | Refresh

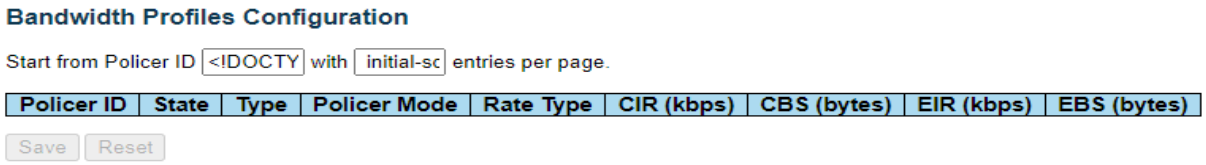
DMAC	L2CP Mode	CoS ID
*	<>	<>
01-80-C2-00-00-00	Peer	Disabled
01-80-C2-00-00-01	Peer	Disabled
01-80-C2-00-00-02	Peer	Disabled
01-80-C2-00-00-03	Peer	Disabled
01-80-C2-00-00-04	Peer	Disabled
01-80-C2-00-00-05	Peer	Disabled
01-80-C2-00-00-06	Peer	Disabled
01-80-C2-00-00-07	Peer	Disabled
01-80-C2-00-00-08	Peer	Disabled
01-80-C2-00-00-09	Peer	Disabled
01-80-C2-00-00-0A	Peer	Disabled
01-80-C2-00-00-0B	Peer	Disabled
01-80-C2-00-00-0C	Peer	Disabled
01-80-C2-00-00-0D	Peer	Disabled
01-80-C2-00-00-0E	Peer	Disabled
01-80-C2-00-00-0F	Peer	Disabled
01-80-C2-00-00-20	Forward	Disabled
01-80-C2-00-00-21	Forward	Disabled
01-80-C2-00-00-22	Forward	Disabled
01-80-C2-00-00-23	Forward	Disabled
01-80-C2-00-00-24	Forward	Disabled
01-80-C2-00-00-25	Forward	Disabled
01-80-C2-00-00-26	Forward	Disabled
01-80-C2-00-00-27	Forward	Disabled
01-80-C2-00-00-28	Forward	Disabled
01-80-C2-00-00-29	Forward	Disabled
01-80-C2-00-00-2A	Forward	Disabled
01-80-C2-00-00-2B	Forward	Disabled
01-80-C2-00-00-2C	Forward	Disabled
01-80-C2-00-00-2D	Forward	Disabled
01-80-C2-00-00-2E	Forward	Disabled
01-80-C2-00-00-2F	Forward	Disabled

Save | Reset

Click "Save" for the changes to take effect.

2.24.2. Bandwidth Profiles

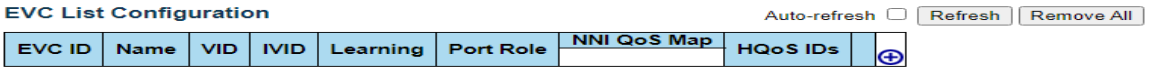
Click on “Configuration>Ethernet Services>Bandwidth Profiles”.



Click "Save" for the changes to take effect.

2.24.3. EVC

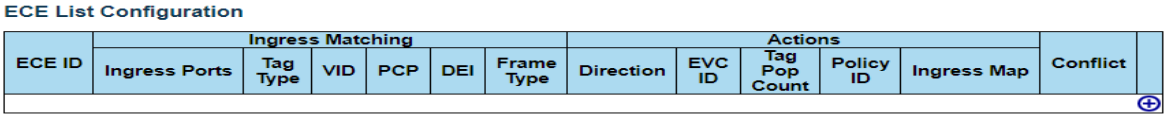
Click on “Configuration>Ethernet Services>EVC”.



Click "Save" for the changes to take effect.

2.24.4. ECE

Click on “Configuration>Ethernet Services>ECE”.

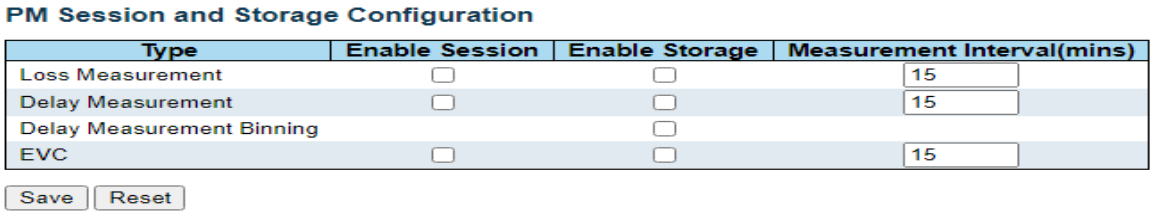


Click "Save" for the changes to take effect.

2.25. Performance Monitor

2.25.1. Configuration

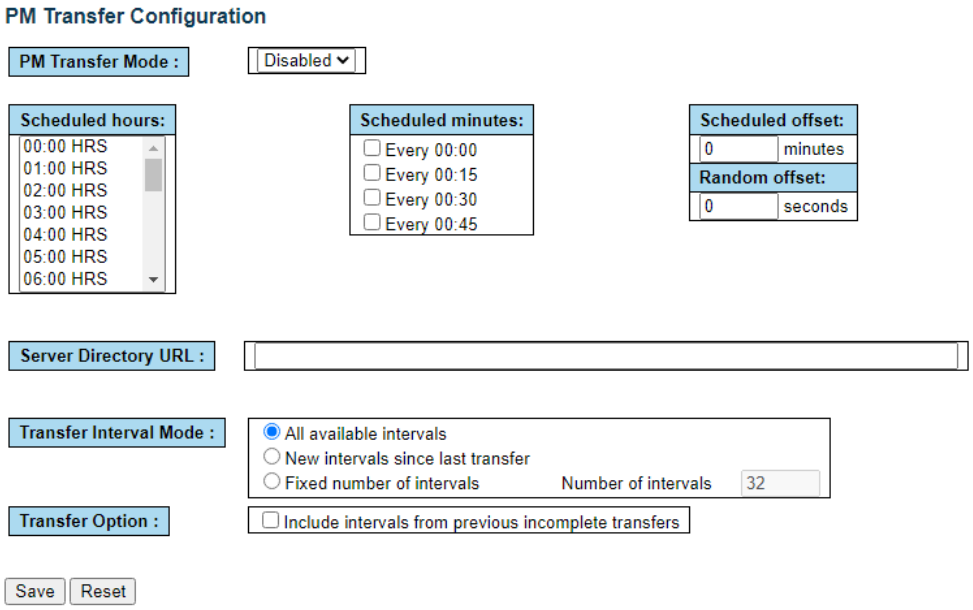
Click on “Configuration>Performance Monitor>Configuration”.



Click "Save" for the changes to take effect.

2.25.2. Transfer Mode

Click on “Configuration>Performance Monitor>Transfer Mode”.

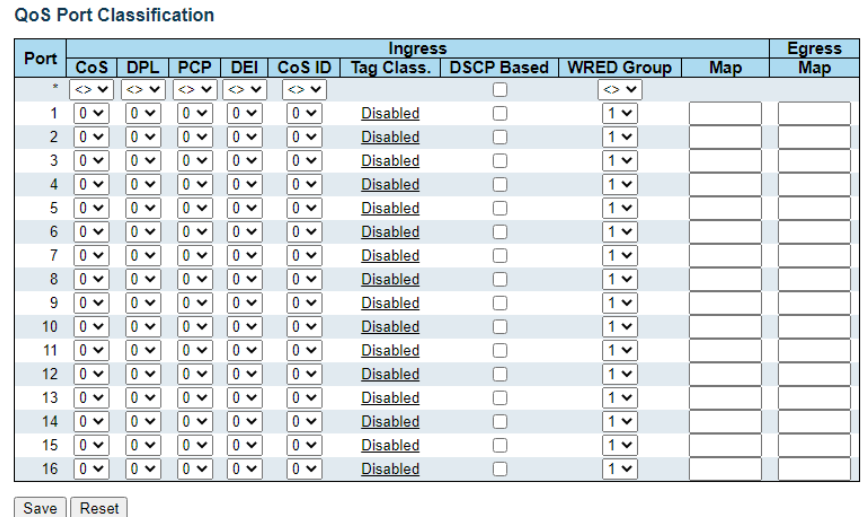


Click "Save" for the changes to take effect.

2.26. QoS

2.26.1 Port Classification

Click on “Configuration>QoS>Port Classification”.



Click "Save" for the changes to take effect.

2.26.2. Port Policing

Click on “Configuration>QoS>Port Policing”.

QoS Ingress Port Policers

Port	Enable	Rate	Unit	Flow Control
*	☐	500	<>	☐
1	☐	500	kbps	☐
2	☐	500	kbps	☐
3	☐	500	kbps	☐
4	☐	500	kbps	☐
5	☐	500	kbps	☐
6	☐	500	kbps	☐
7	☐	500	kbps	☐
8	☐	500	kbps	☐
9	☐	500	kbps	☐
10	☐	500	kbps	☐
11	☐	500	kbps	☐
12	☐	500	kbps	☐
13	☐	500	kbps	☐
14	☐	500	kbps	☐
15	☐	500	kbps	☐
16	☐	500	kbps	☐

Save Reset

Click "Save" for the changes to take effect.

2.26.3. Queue Policing

Click on “Configuration>QoS>Queue Policing”.

QoS Ingress Queue Policers

Port	Queue 0 Enable	Queue 1 Enable	Queue 2 Enable	Queue 3 Enable	Queue 4 Enable	Queue 5 Enable	Queue 6 Enable	Queue 7 Enable
*	☐	☐	☐	☐	☐	☐	☐	☐
1	☐	☐	☐	☐	☐	☐	☐	☐
2	☐	☐	☐	☐	☐	☐	☐	☐
3	☐	☐	☐	☐	☐	☐	☐	☐
4	☐	☐	☐	☐	☐	☐	☐	☐
5	☐	☐	☐	☐	☐	☐	☐	☐
6	☐	☐	☐	☐	☐	☐	☐	☐
7	☐	☐	☐	☐	☐	☐	☐	☐
8	☐	☐	☐	☐	☐	☐	☐	☐
9	☐	☐	☐	☐	☐	☐	☐	☐
10	☐	☐	☐	☐	☐	☐	☐	☐
11	☐	☐	☐	☐	☐	☐	☐	☐
12	☐	☐	☐	☐	☐	☐	☐	☐
13	☐	☐	☐	☐	☐	☐	☐	☐
14	☐	☐	☐	☐	☐	☐	☐	☐
15	☐	☐	☐	☐	☐	☐	☐	☐
16	☐	☐	☐	☐	☐	☐	☐	☐

Save Reset

Click "Save" for the changes to take effect.

2.26.4. Port Scheduler

Click on “Configuration>QoS>Queue Policing”.

QoS Egress Port Schedulers

Port	Mode	Weight							
		Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7
1	Strict Priority	-	-	-	-	-	-	-	-
2	Strict Priority	-	-	-	-	-	-	-	-
3	Strict Priority	-	-	-	-	-	-	-	-
4	Strict Priority	-	-	-	-	-	-	-	-
5	Strict Priority	-	-	-	-	-	-	-	-
6	Strict Priority	-	-	-	-	-	-	-	-
7	Strict Priority	-	-	-	-	-	-	-	-
8	Strict Priority	-	-	-	-	-	-	-	-
9	Strict Priority	-	-	-	-	-	-	-	-
10	Strict Priority	-	-	-	-	-	-	-	-
11	Strict Priority	-	-	-	-	-	-	-	-
12	Strict Priority	-	-	-	-	-	-	-	-
13	Strict Priority	-	-	-	-	-	-	-	-
14	Strict Priority	-	-	-	-	-	-	-	-
15	Strict Priority	-	-	-	-	-	-	-	-
16	Strict Priority	-	-	-	-	-	-	-	-

Click "Save" for the changes to take effect.

2.26.5. Port Shaping

Click on “Configuration>QoS>Port Shaping”.

QoS Egress Port Shapers

Port	Shapers								
	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Port
1	-	-	-	-	-	-	-	-	-
2	-	-	-	-	-	-	-	-	-
3	-	-	-	-	-	-	-	-	-
4	-	-	-	-	-	-	-	-	-
5	-	-	-	-	-	-	-	-	-
6	-	-	-	-	-	-	-	-	-
7	-	-	-	-	-	-	-	-	-
8	-	-	-	-	-	-	-	-	-
9	-	-	-	-	-	-	-	-	-
10	-	-	-	-	-	-	-	-	-
11	-	-	-	-	-	-	-	-	-
12	-	-	-	-	-	-	-	-	-
13	-	-	-	-	-	-	-	-	-
14	-	-	-	-	-	-	-	-	-
15	-	-	-	-	-	-	-	-	-
16	-	-	-	-	-	-	-	-	-

Click "Save" for the changes to take effect.

2.26.6. Port Tag Remarking

Click on “Configuration>QoS>Port Tag Remarking”.

QoS Egress Port Tag Remarking

Port	Mode
1	Classified
2	Classified
3	Classified
4	Classified
5	Classified
6	Classified
7	Classified
8	Classified
9	Classified
10	Classified
11	Classified
12	Classified
13	Classified
14	Classified
15	Classified
16	Classified

Click "Save" for the changes to take effect.

2.26.7. Port DSCP

Click on “Configuration>QoS>Port DSCP”.

QoS Port DSCP Configuration

Port	Ingress		Egress
	Translate	Classify	Rewrite
*	☐	<>	<>
1	☐	Disable	Disable
2	☐	Disable	Disable
3	☐	Disable	Disable
4	☐	Disable	Disable
5	☐	Disable	Disable
6	☐	Disable	Disable
7	☐	Disable	Disable
8	☐	Disable	Disable
9	☐	Disable	Disable
10	☐	Disable	Disable
11	☐	Disable	Disable
12	☐	Disable	Disable
13	☐	Disable	Disable
14	☐	Disable	Disable
15	☐	Disable	Disable
16	☐	Disable	Disable

Save Reset

Click "Save" for the changes to take effect.

2.26.8. DSCP-Based QoS

Click on “Configuration>QoS>DSCP-Based QoS”.

DSCP-Based QoS Ingress Classification

DSCP	Trust	CoS	DPL
*	☐	<>	<>
0 (BE)	☐	0	0
1	☐	0	0
2	☐	0	0
3	☐	0	0
4	☐	0	0
5	☐	0	0
6	☐	0	0
7	☐	0	0
8 (CS1)	☐	0	0
9	☐	0	0
10 (AF11)	☐	0	0
11	☐	0	0
12 (AF12)	☐	0	0
13	☐	0	0
14 (AF13)	☐	0	0
15	☐	0	0
16 (CS2)	☐	0	0
17	☐	0	0
18 (AF21)	☐	0	0
19	☐	0	0
20 (AF22)	☐	0	0
21	☐	0	0
22 (AF23)	☐	0	0
23	☐	0	0
24 (CS3)	☐	0	0
25	☐	0	0
26 (AF31)	☐	0	0
27	☐	0	0
28 (AF32)	☐	0	0
29	☐	0	0
30 (AF33)	☐	0	0
31	☐	0	0

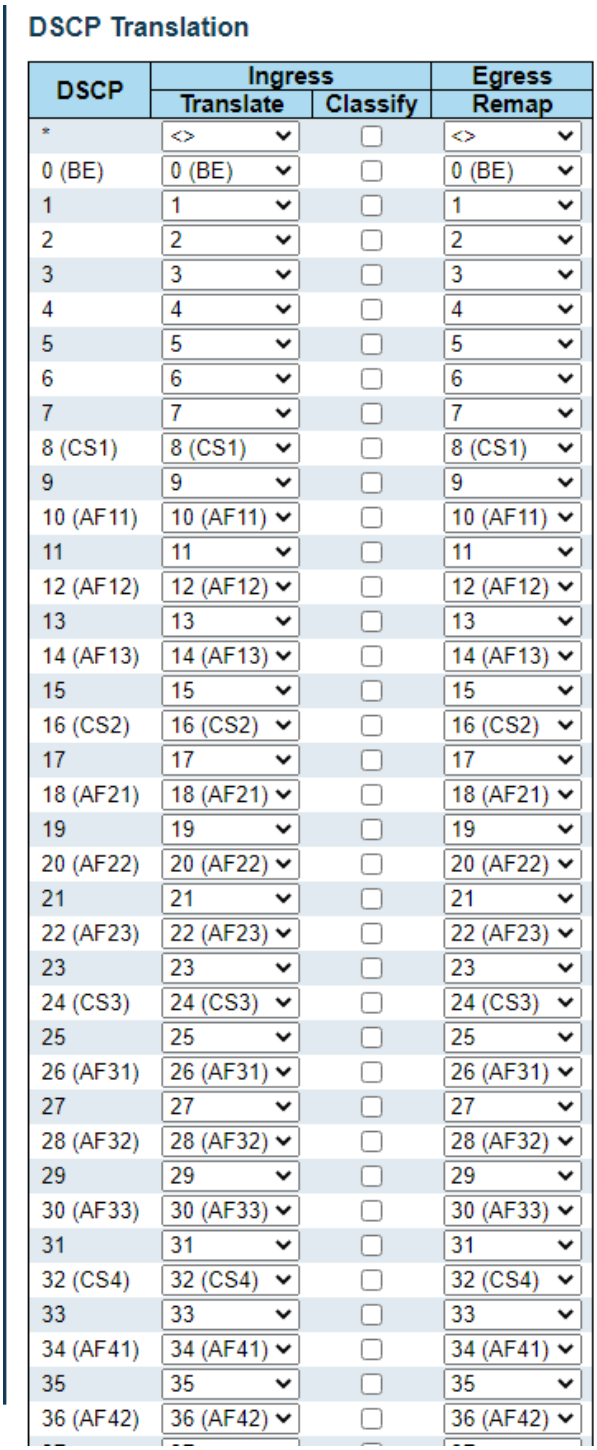
31	☐	0	0
32 (CS4)	☐	0	0
33	☐	0	0
34 (AF41)	☐	0	0
35	☐	0	0
36 (AF42)	☐	0	0
37	☐	0	0
38 (AF43)	☐	0	0
39	☐	0	0
40 (CS5)	☐	0	0
41	☐	0	0
42	☐	0	0
43	☐	0	0
44	☐	0	0
45	☐	0	0
46 (EF)	☐	0	0
47	☐	0	0
48 (CS6)	☐	0	0
49	☐	0	0
50	☐	0	0
51	☐	0	0
52	☐	0	0
53	☐	0	0
54	☐	0	0
55	☐	0	0
56 (CS7)	☐	0	0
57	☐	0	0
58	☐	0	0
59	☐	0	0
60	☐	0	0
61	☐	0	0
62	☐	0	0
63	☐	0	0

Save Reset

Click "Save" for the changes to take effect.

2.26.9. DSCP Translation

Click on “Configuration>QoS>DSCP Translation”.



DSCP Translation

DSCP	Ingress		Egress
	Translate	Classify	Remap
*	<>	☐	<>
0 (BE)	0 (BE)	☐	0 (BE)
1	1	☐	1
2	2	☐	2
3	3	☐	3
4	4	☐	4
5	5	☐	5
6	6	☐	6
7	7	☐	7
8 (CS1)	8 (CS1)	☐	8 (CS1)
9	9	☐	9
10 (AF11)	10 (AF11)	☐	10 (AF11)
11	11	☐	11
12 (AF12)	12 (AF12)	☐	12 (AF12)
13	13	☐	13
14 (AF13)	14 (AF13)	☐	14 (AF13)
15	15	☐	15
16 (CS2)	16 (CS2)	☐	16 (CS2)
17	17	☐	17
18 (AF21)	18 (AF21)	☐	18 (AF21)
19	19	☐	19
20 (AF22)	20 (AF22)	☐	20 (AF22)
21	21	☐	21
22 (AF23)	22 (AF23)	☐	22 (AF23)
23	23	☐	23
24 (CS3)	24 (CS3)	☐	24 (CS3)
25	25	☐	25
26 (AF31)	26 (AF31)	☐	26 (AF31)
27	27	☐	27
28 (AF32)	28 (AF32)	☐	28 (AF32)
29	29	☐	29
30 (AF33)	30 (AF33)	☐	30 (AF33)
31	31	☐	31
32 (CS4)	32 (CS4)	☐	32 (CS4)
33	33	☐	33
34 (AF41)	34 (AF41)	☐	34 (AF41)
35	35	☐	35
36 (AF42)	36 (AF42)	☐	36 (AF42)

31	31	☐	31
32 (CS4)	32 (CS4)	☐	32 (CS4)
33	33	☐	33
34 (AF41)	34 (AF41)	☐	34 (AF41)
35	35	☐	35
36 (AF42)	36 (AF42)	☐	36 (AF42)
37	37	☐	37
38 (AF43)	38 (AF43)	☐	38 (AF43)
39	39	☐	39
40 (CS5)	40 (CS5)	☐	40 (CS5)
41	41	☐	41
42	42	☐	42
43	43	☐	43
44	44	☐	44
45	45	☐	45
46 (EF)	46 (EF)	☐	46 (EF)
47	47	☐	47
48 (CS6)	48 (CS6)	☐	48 (CS6)
49	49	☐	49
50	50	☐	50
51	51	☐	51
52	52	☐	52
53	53	☐	53
54	54	☐	54
55	55	☐	55
56 (CS7)	56 (CS7)	☐	56 (CS7)
57	57	☐	57
58	58	☐	58
59	59	☐	59
60	60	☐	60
61	61	☐	61
62	62	☐	62
63	63	☐	63

Save Reset

Click "Save" for the changes to take effect.

2.26.10. DSCP Classification

Click on “Configuration>QoS>DSCP Classification”.

DSCP Classification

CoS	DSCP DP0	DSCP DP1	DSCP DP2	DSCP DP3
*	<>	<>	<>	<>
0	0 (BE)	0 (BE)	0 (BE)	0 (BE)
1	0 (BE)	0 (BE)	0 (BE)	0 (BE)
2	0 (BE)	0 (BE)	0 (BE)	0 (BE)
3	0 (BE)	0 (BE)	0 (BE)	0 (BE)
4	0 (BE)	0 (BE)	0 (BE)	0 (BE)
5	0 (BE)	0 (BE)	0 (BE)	0 (BE)
6	0 (BE)	0 (BE)	0 (BE)	0 (BE)
7	0 (BE)	0 (BE)	0 (BE)	0 (BE)

Save Reset

Click "Save" for the changes to take effect.

2.26.11. Ingress Map

Click on “Configuration>QoS>Ingress Map”.

QoS Ingress Map Configuration

Map ID	Key-Type	Action-Type						
		CoS	DPL	PCP	DEI	DSCP	CoS ID	Path CoS ID

Ingress Map Configuration

Ingress Map ID

MAP ID	0

Ingress Map Key

Map Key	PCP

Ingress Map Action

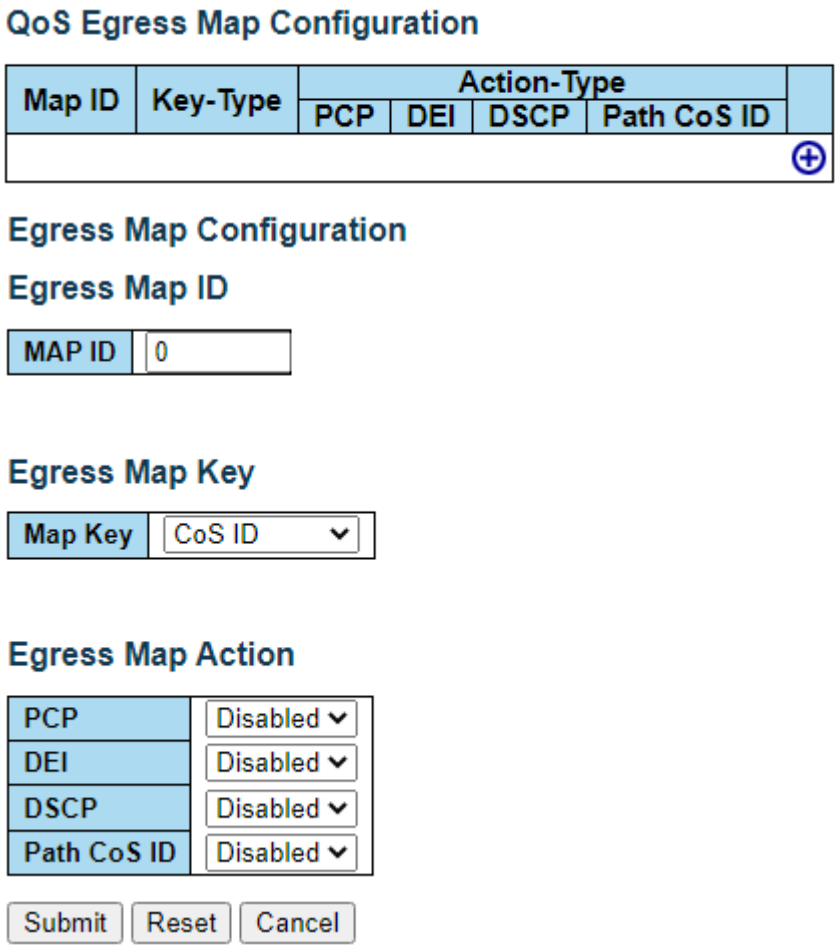
CoS	Disabled
DPL	Disabled
PCP	Disabled
DEI	Disabled
DSCP	Disabled
CoS ID	Disabled
Path CoS ID	Disabled

Submit Reset Cancel

Click "Save" for the changes to take effect.

2.26.12. Egress Map

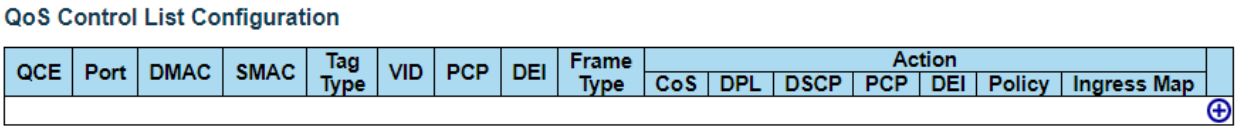
Click on “Configuration>QoS>Egress Map”.



Click "Save" for the changes to take effect.

2.26.13. QoS Control List

Click on “Configuration>QoS>QoS Control List”.



QCE Configuration

Port Members															
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

Key Parameters

DMAC	Any
SMAC	Any
Tag	Any
VID	Any
PCP	Any
DEI	Any
Inner Tag	Any
Inner VID	Any
Inner PCP	Any
Inner DEI	Any
Frame Type	Any

Action Parameters

CoS	0
DPL	Default
DSCP	Default
PCP	Default
DEI	Default
Policy	
Ingress Map ID	

Save Reset Cancel

Click "Save" for the changes to take effect.

2.26.14. Storm Policing

Click on “Configuration>QoS>Storm Policing”.

Global Storm Policer Configuration

Frame Type	Enable	Rate	Unit
Unicast	☐	10	fps
Multicast	☐	10	fps
Broadcast	☐	10	fps

Port Storm Policer Configuration

Port	Unicast Frames			Broadcast Frames			Unknown Frames		
	Enable	Rate	Unit	Enable	Rate	Unit	Enable	Rate	Unit
*	☐	500	<>	☐	500	<>	☐	500	<>
1	☐	500	kbps	☐	500	kbps	☐	500	kbps
2	☐	500	kbps	☐	500	kbps	☐	500	kbps
3	☐	500	kbps	☐	500	kbps	☐	500	kbps
4	☐	500	kbps	☐	500	kbps	☐	500	kbps
5	☐	500	kbps	☐	500	kbps	☐	500	kbps
6	☐	500	kbps	☐	500	kbps	☐	500	kbps
7	☐	500	kbps	☐	500	kbps	☐	500	kbps
8	☐	500	kbps	☐	500	kbps	☐	500	kbps
9	☐	500	kbps	☐	500	kbps	☐	500	kbps
10	☐	500	kbps	☐	500	kbps	☐	500	kbps
11	☐	500	kbps	☐	500	kbps	☐	500	kbps
12	☐	500	kbps	☐	500	kbps	☐	500	kbps
13	☐	500	kbps	☐	500	kbps	☐	500	kbps
14	☐	500	kbps	☐	500	kbps	☐	500	kbps
15	☐	500	kbps	☐	500	kbps	☐	500	kbps
16	☐	500	kbps	☐	500	kbps	☐	500	kbps

Save Reset

Click "Save" for the changes to take effect.

2.26.15. WRED

Click on “Configuration>QoS>WRED”.

Weighted Random Early Detection Configuration

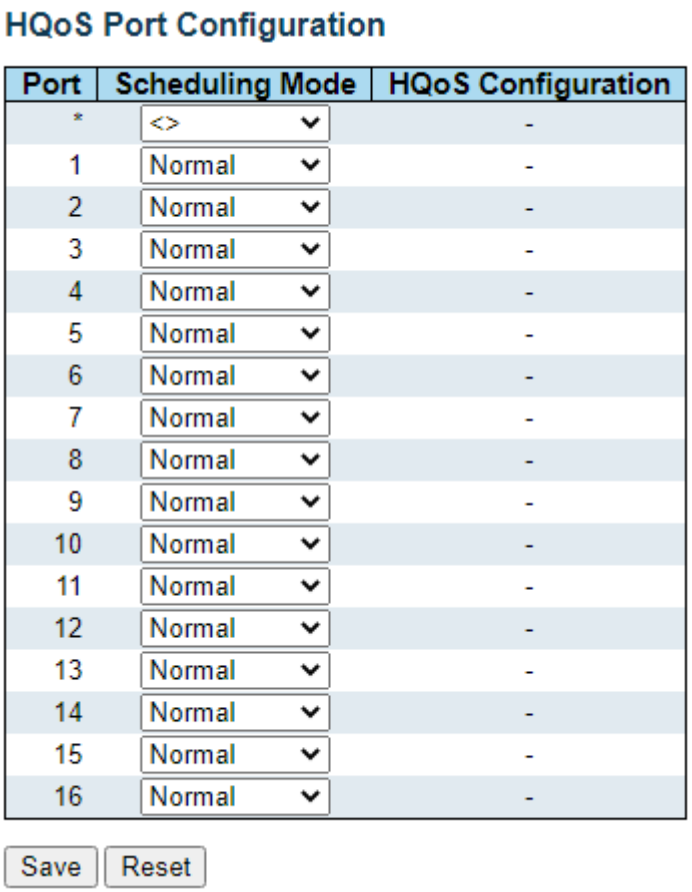
Group	Queue	DPL	Enable	Min	Max	Max Unit
1	0	1	☐	0	50	Drop Probability
1	0	2	☐	0	50	Drop Probability
1	0	3	☐	0	50	Drop Probability
1	1	1	☐	0	50	Drop Probability
1	1	2	☐	0	50	Drop Probability
1	1	3	☐	0	50	Drop Probability
1	2	1	☐	0	50	Drop Probability
1	2	2	☐	0	50	Drop Probability
1	2	3	☐	0	50	Drop Probability
1	3	1	☐	0	50	Drop Probability
1	3	2	☐	0	50	Drop Probability
1	3	3	☐	0	50	Drop Probability
1	4	1	☐	0	50	Drop Probability
1	4	2	☐	0	50	Drop Probability
1	4	3	☐	0	50	Drop Probability
1	5	1	☐	0	50	Drop Probability
1	5	2	☐	0	50	Drop Probability
1	5	3	☐	0	50	Drop Probability
1	6	1	☐	0	50	Drop Probability
1	6	2	☐	0	50	Drop Probability
1	6	3	☐	0	50	Drop Probability
1	7	1	☐	0	50	Drop Probability
1	7	2	☐	0	50	Drop Probability
1	7	3	☐	0	50	Drop Probability
2	0	1	☐	0	50	Drop Probability
2	0	2	☐	0	50	Drop Probability
2	0	3	☐	0	50	Drop Probability
2	1	1	☐	0	50	Drop Probability
2	1	2	☐	0	50	Drop Probability
2	1	3	☐	0	50	Drop Probability
2	2	1	☐	0	50	Drop Probability
2	2	2	☐	0	50	Drop Probability
2	2	3	☐	0	50	Drop Probability
2	3	1	☐	0	50	Drop Probability
2	3	2	☐	0	50	Drop Probability
2	3	3	☐	0	50	Drop Probability
2	4	1	☐	0	50	Drop Probability
2	4	2	☐	0	50	Drop Probability
2	4	3	☐	0	50	Drop Probability

Click "Save" for the changes to take effect.

2.27. HQoS

2.27.1. Ports

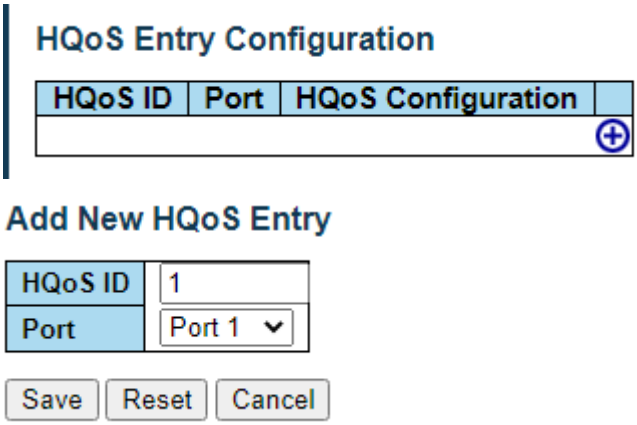
Click on “Configuration>HQoS>Ports”.



Click "Save" for the changes to take effect.

2.27.2. HQoS Entries

Click on “Configuration>HQoS>HQoS Entries”.



Click "Save" for the changes to take effect.

2.28. Mirroring

Click on “Configuration>Mirroring”.

Mirror & RMirror Configuration Table

Refresh

Session ID	Mode	Type	VLAN ID	Reflector Port
1	Disabled	Mirror	-	-
2	Disabled	Mirror	-	-
3	Disabled	Mirror	-	-
4	Disabled	Mirror	-	-
5	Disabled	Mirror	-	-

2.29. UPnP

Click on “Configuration>UPnP”.

UPnP Configuration

Mode	Disabled
TTL	4
Advertising Duration	100
IP Addressing Mode	Dynamic
Static VLAN Interface ID	1

Save Reset

Click "Save" for the changes to take effect.

2.30. MRP

2.30.1. Ports

Click on “Configuration>MRP>Ports”.

MRP Overall Port Configuration

Auto-refresh Refresh

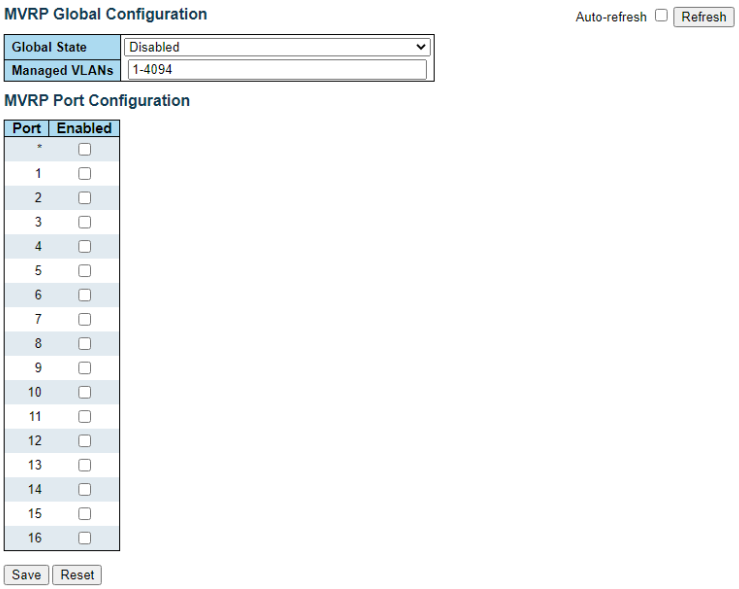
Port	Join Timeout	Leave Timeout	LeaveAll Timeout	Periodic Transmission
*	20	60	1000	
1	20	60	1000	
2	20	60	1000	
3	20	60	1000	
4	20	60	1000	
5	20	60	1000	
6	20	60	1000	
7	20	60	1000	
8	20	60	1000	
9	20	60	1000	
10	20	60	1000	
11	20	60	1000	
12	20	60	1000	
13	20	60	1000	
14	20	60	1000	
15	20	60	1000	
16	20	60	1000	

Save Reset

Click "Save" for the changes to take effect.

2.30.2. MVRP

Click on “Configuration>MRP>MVRP”.

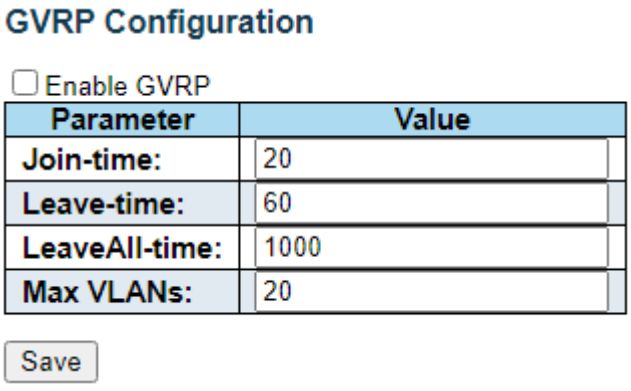


Click "Save" for the changes to take effect.

2.31. GVRP

2.31.1 Global config

Click on “Configuration>GVRP>Global config”.



Click "Save" for the changes to take effect.

2.31.2. Port config

Click on “Configuration>GVRP>Port config”.

GVRP Port Configuration

Port	Mode
*	<>
1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled
9	Disabled
10	Disabled
11	Disabled
12	Disabled
13	Disabled
14	Disabled
15	Disabled
16	Disabled

Save Reset

Click "Save" for the changes to take effect.

2.32. sFlow

Click on “Configuration>sFlow”.

sFlow Configuration Refresh

Agent Configuration

IP Address	127.0.0.1

Receiver Configuration

Owner	<none>	Release
IP Address/Hostname	0.0.0.0	
UDP Port	6343	
Timeout	0	seconds
Max. Datagram Size	1400	bytes

Port Configuration

Port	Flow Sampler			Counter Poller	
	Enabled	Sampling Rate	Max. Header	Enabled	Interval
*	☐	0	128	☐	0
1	☐	0	128	☐	0
2	☐	0	128	☐	0
3	☐	0	128	☐	0
4	☐	0	128	☐	0
5	☐	0	128	☐	0
6	☐	0	128	☐	0
7	☐	0	128	☐	0
8	☐	0	128	☐	0
9	☐	0	128	☐	0
10	☐	0	128	☐	0
11	☐	0	128	☐	0
12	☐	0	128	☐	0
13	☐	0	128	☐	0
14	☐	0	128	☐	0
15	☐	0	128	☐	0
16	☐	0	128	☐	0

Save Reset

Click "Save" for the changes to take effect.

2.33. Traffic Test

2.33.1. Y.1564

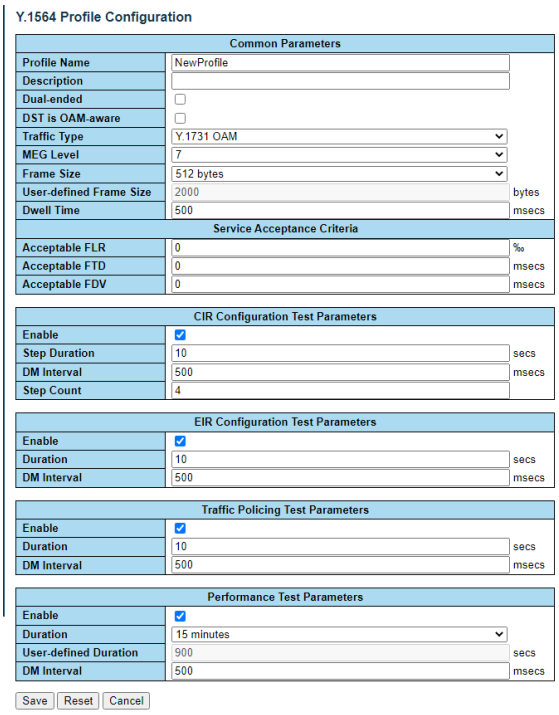
2.33.1.1. Profiles

Click on “Configuration>Traffic Test>Y.1564> Profiles”.

Y.1564 Profile Overview

Delete	Name	Description
<No profiles>		

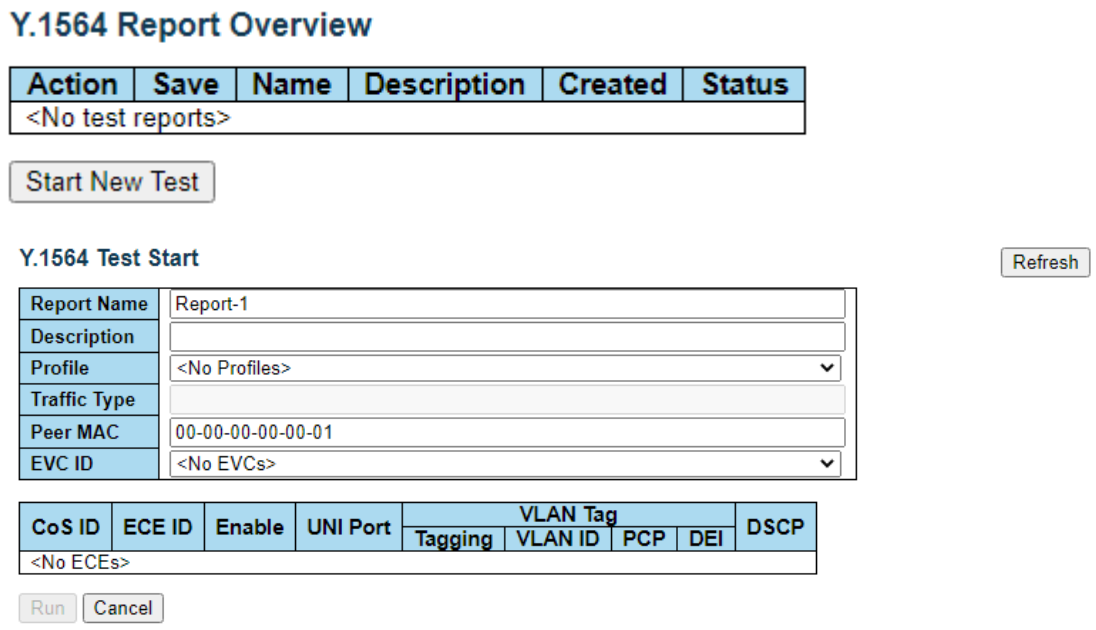
Add New Profile



Click "Save" for the changes to take effect.

2.33.1.2. Reports

Click on “Configuration>Traffic Test>Y.1564> Reports”.

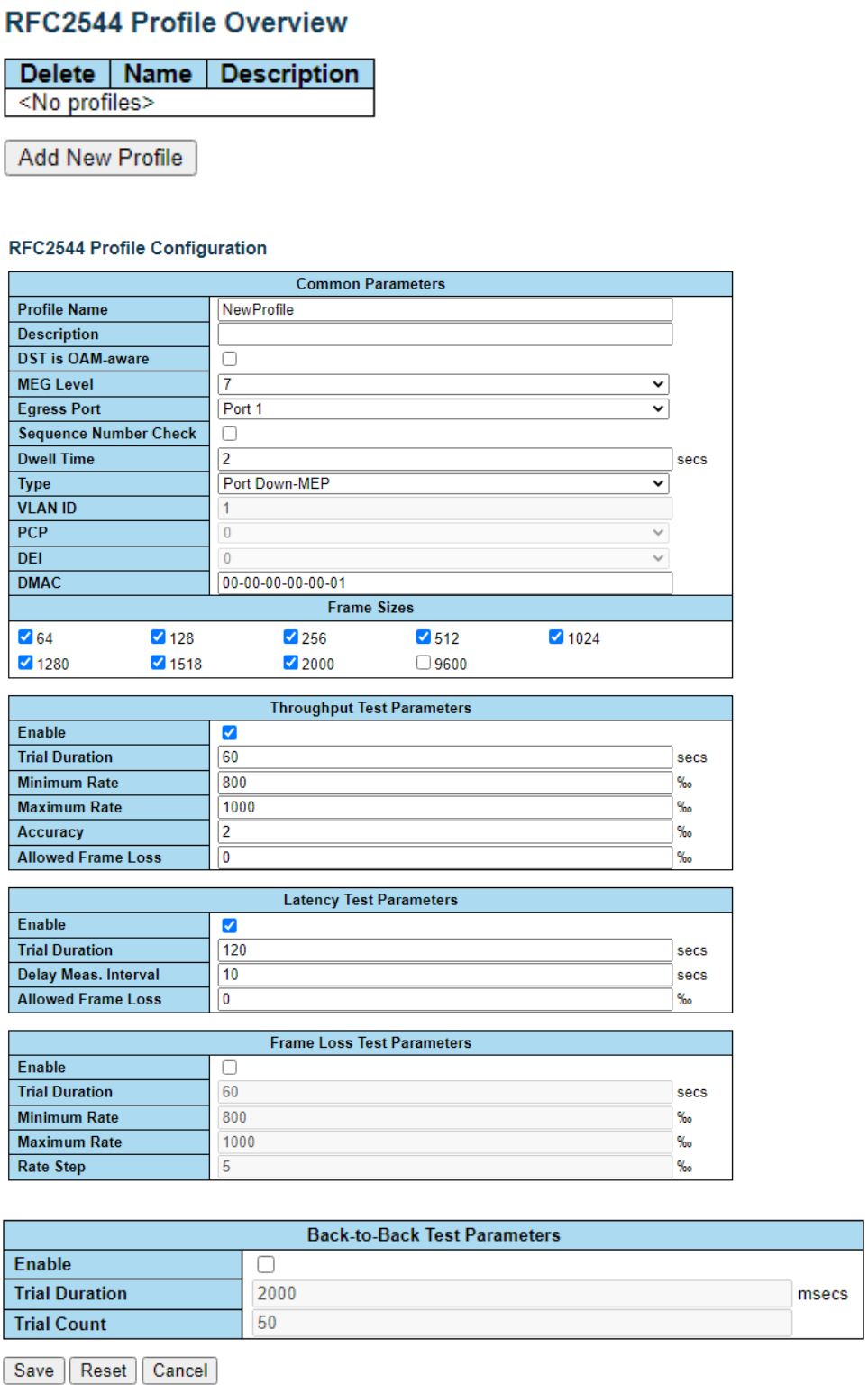


Click "Save" for the changes to take effect.

2.33.2. RFC2544

2.33.2.1. Profiles

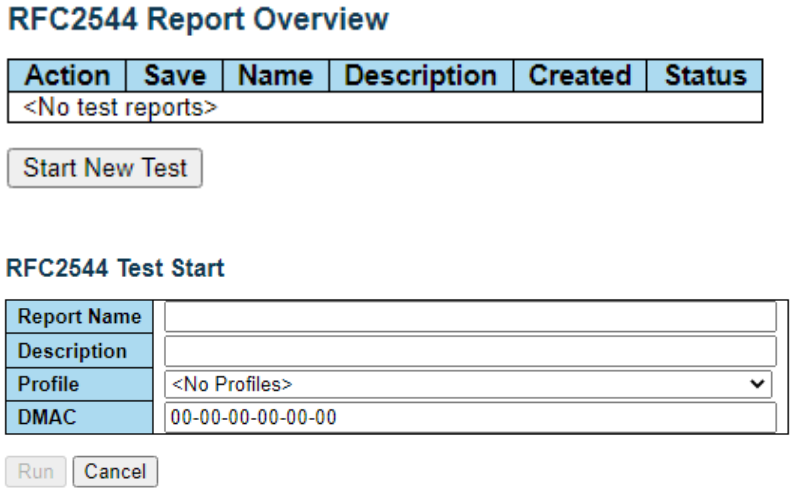
Click on “Configuration>Traffic Test>RFC2544> Profiles”.



Click "Save" for the changes to take effect.

2.33.2.2. Reports

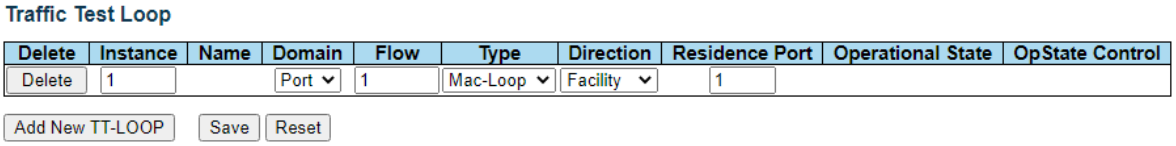
Click on “Configuration>Traffic Test>RFC2544> Reports”.



Click "Save" for the changes to take effect.

2.33.3. Loop

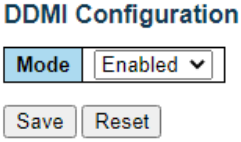
Click on “Configuration>Traffic Test>Loop”.



Click "Save" for the changes to take effect.

2.34. DDMI

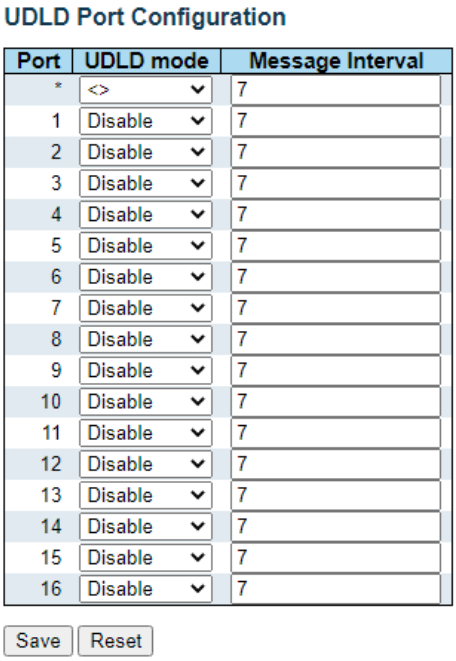
Click on “Configuration>DDMI”.



Click "Save" for the changes to take effect.

2.35. UDLD

Click on “Configuration>UDLD”.



Click "Save" for the changes to take effect.

2.38. OSPF

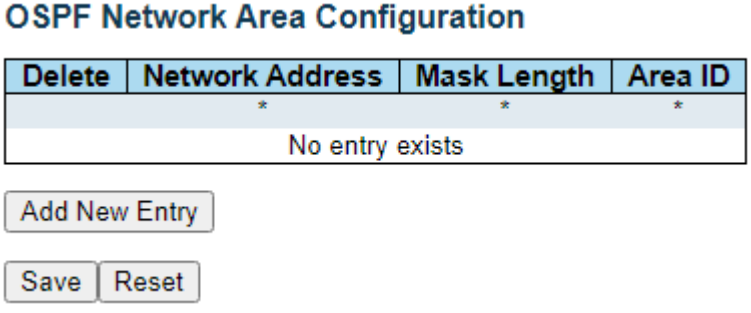
2.38.1. Configuration

Click on “Configuration>OSPF>Configuration”.

Click "Save" for the changes to take effect.

2.38.2. Network Area

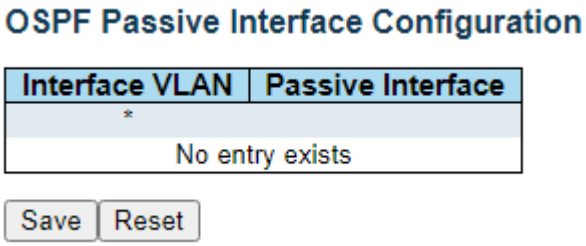
Click on “Configuration>OSPF>Network Area”.



Click "Save" for the changes to take effect.

2.38.3. Passive Interface

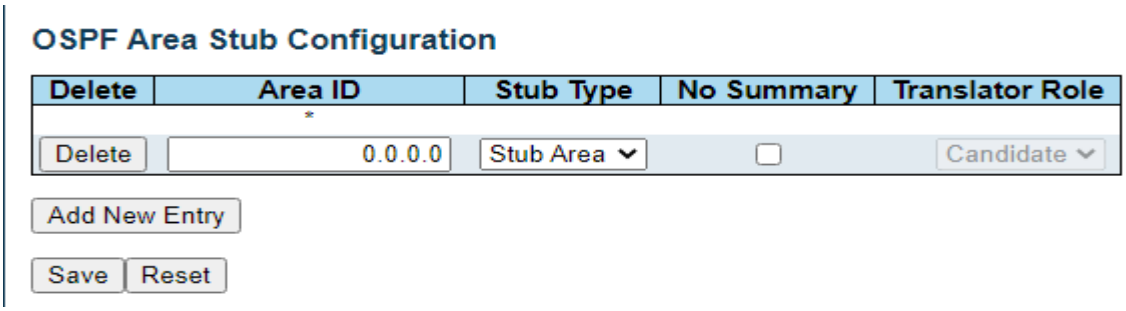
Click on “Configuration>OSPF>Passive Interface”.



Click "Save" for the changes to take effect.

2.38.4. Stub Area

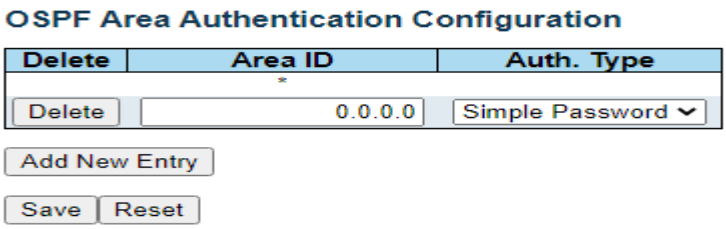
Click on “Configuration>OSPF>Stub Area”.



Click "Save" for the changes to take effect.

2.38.5. Area Authentication

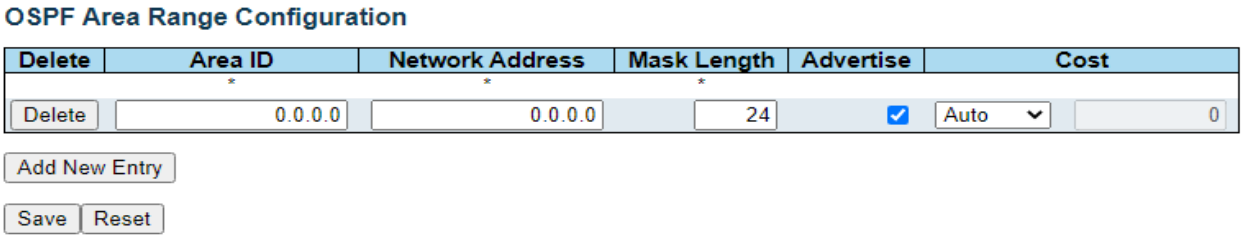
Click on “Configuration>OSPF>Area Authentication”.



Click "Save" for the changes to take effect.

2.38.6. Area Range

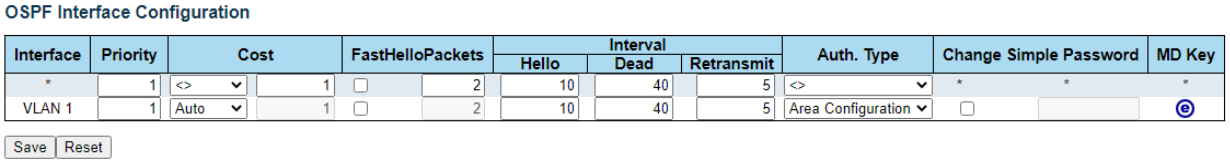
Click on “Configuration>OSPF>Area Range”.



Click "Save" for the changes to take effect.

2.38.7. Interfaces

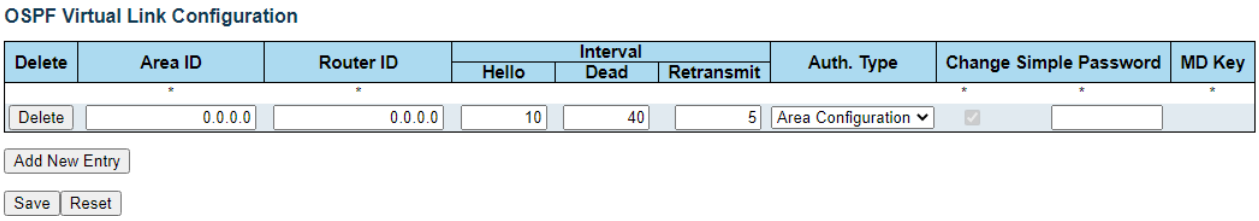
Click on “Configuration>OSPF>Interfaces”.



Click "Save" for the changes to take effect.

2.38.8. Virtual Link

Click on “Configuration>OSPF>Virtual Link”.



Click "Save" for the changes to take effect.

Chapter 3. Monitor

3.1. System

3.1.1. Information

Click on “Monitor>system >Information”.

System Information

System	
Contact	
Name	
Location	
Hardware	
MAC Address	02-00-c1-db-b0-3c
Chip ID	VSC7449
Time	
System Date	1970-01-01T03:11:55+00:00
System Uptime	0d 03:11:55
Software	
Software Version	12GE-4GF-L3 dev-build by root@ieslabsz-Aspire-TC-705 2022-11-07T17:25:11+08:00 Config:ce_sparxIV_90_48 Profile:ce_sparxIV_90_48 SDK:2018.02-011-smb
Software Date	2022-11-07T17:25:11+08:00
Code Revision	Enviroment variable 'CODE_REVISION' not set during compile
Acknowledgments	Details

3.1.2. LED status

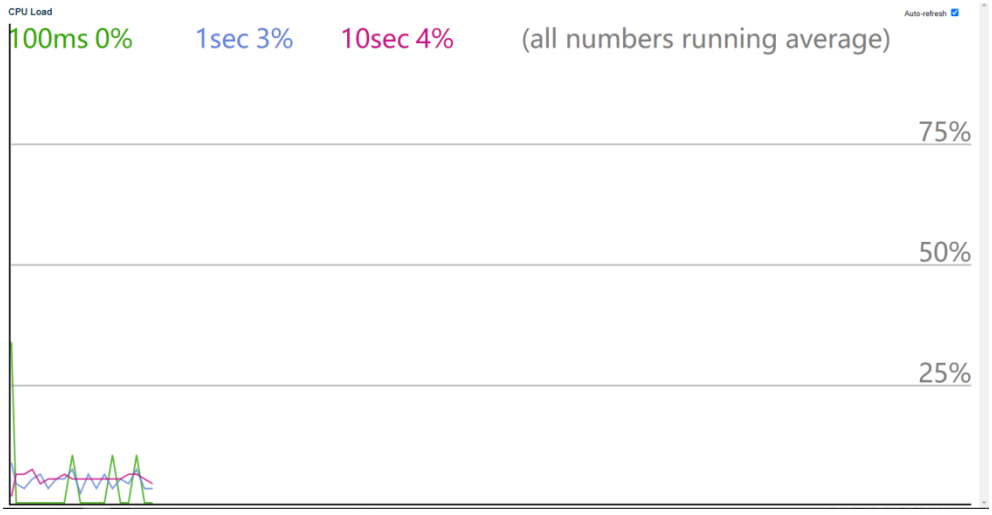
Click on “Monitor>system >LED status”.

System LED Status

Clear Type	All
Description	System LED: green, solid, normal indication.

3.1.3. CPU Load

Click on “Monitor>system >CPU Load”.



3.1.4. IP Status

Click on “Monitor>system >IP Status”.

IP Interfaces

Interface	Type	Address	Status
VLAN1	LINK	02-00-c1-db-b0-3c	<UP BROADCAST MULTICAST>
VLAN1	IPv4	192.168.2.112/24	
VLAN1	IPv6	fe80::c1ff:fedb:b03c/64	

IPv6 Routes

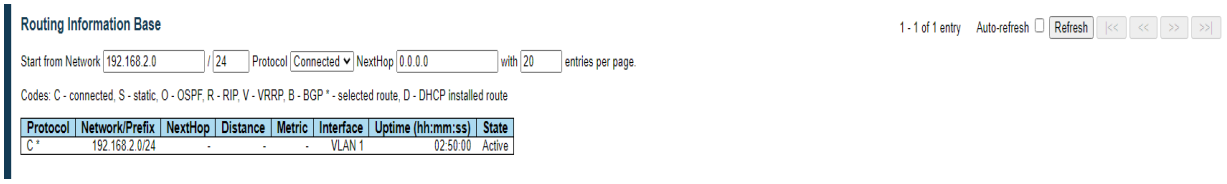
Network	Gateway	Status

Neighbour cache

IP Address	Link Address
169.254.210.149	VLAN1:6c-4b-90-ae-ed-07
192.168.1.1	VLAN1:ec-60-73-32-1e-22
192.168.1.62	VLAN1:6c-4b-90-ae-ed-07
192.168.1.64	VLAN1:42-e3-2c-e7-5c-f1
192.168.1.67	VLAN1:20-77-59-04-ae-f0
192.168.1.71	VLAN1:f4-bf-80-6b-21-c3
192.168.1.72	VLAN1:72-60-b1-70-b6-b0
192.168.1.73	VLAN1:52-c4-31-75-de-80
192.168.1.77	VLAN1:92-cd-1a-19-30-7f
192.168.1.79	VLAN1:ea-c0-96-41-13-aa
192.168.1.87	VLAN1:8e-42-44-0a-44-a1
192.168.1.89	VLAN1:ae-75-c3-82-bf-e6
192.168.1.90	VLAN1:5a-07-9d-89-31-b5
192.168.1.91	VLAN1:12-16-de-f3-4f-d1
192.168.1.92	VLAN1:bc-6e-e2-eb-32-82
192.168.1.93	VLAN1:22-45-aa-69-00-34
192.168.1.94	VLAN1:8c-c8-4b-ea-7b-c9
192.168.1.96	VLAN1:82-77-30-c2-95-e3
192.168.1.97	VLAN1:38-ba-f8-87-cd-8c
192.168.1.98	VLAN1:6c-4b-90-98-90-b3
192.168.1.99	VLAN1:20-77-59-04-ae-f0
192.168.1.105	VLAN1:e4-aa-ea-98-5a-c9
192.168.1.107	VLAN1:c0-b5-d7-83-ef-3d
192.168.1.123	VLAN1:20-77-59-0a-09-62
192.168.1.135	VLAN1:40-5b-d8-a8-5b-53
192.168.1.139	VLAN1:94-08-53-9c-fa-89
192.168.2.1	VLAN1:20-77-59-0a-09-62
192.168.2.118	VLAN1:d4-5d-64-44-0e-fe
192.168.2.151	VLAN1:c0-56-e3-73-d0-6c
192.168.2.160	VLAN1:e0-50-8b-79-fc-a2

3.1.5. Routing Info. Base

Click on “Monitor>system >Routing Info. Base”.



3.1.6. Log

Click on “Monitor>system >Log”.

System Log Information

Level	All
Clear Level	All

The total number of entries is 36 for the given level.

Start from ID 1 with 20 entries per page.

ID	Level	Time	Message
1	Notice	1970-01-01T00:00:30+00:00	LINK-CHANGED: Interface GigabitEthernet 1/1, changed state to down .
2	Notice	1970-01-01T00:00:30+00:00	LINK-CHANGED: Interface GigabitEthernet 1/2, changed state to down .
3	Notice	1970-01-01T00:00:30+00:00	LINK-CHANGED: Interface GigabitEthernet 1/3, changed state to down .
4	Notice	1970-01-01T00:00:30+00:00	LINK-CHANGED: Interface GigabitEthernet 1/4, changed state to down .
5	Notice	1970-01-01T00:00:31+00:00	LINK-CHANGED: Interface GigabitEthernet 1/6, changed state to up .
6	Notice	1970-01-01T00:00:31+00:00	LINK-CHANGED: Interface GigabitEthernet 1/9, changed state to down .
7	Notice	1970-01-01T00:00:31+00:00	LINK-CHANGED: Interface GigabitEthernet 1/10, changed state to down .
8	Notice	1970-01-01T00:00:31+00:00	LINK-CHANGED: Interface GigabitEthernet 1/11, changed state to down .
9	Notice	1970-01-01T00:00:31+00:00	LINK-CHANGED: Interface GigabitEthernet 1/12, changed state to down .
10	Notice	1970-01-01T00:00:31+00:00	LINK-CHANGED: Interface 10GigabitEthernet 1/1, changed state to down .
11	Informational	1970-01-01T00:00:37+00:00	SYS-BOOTING: Switch just made a cold boot.
12	Notice	1970-01-01T00:00:40+00:00	LINK-UPDOWN: Interface Vlan 1, changed state to up.
13	Notice	1970-01-01T00:00:40+00:00	LINK-UPDOWN: Interface Vlan 1, changed state to up.
14	Notice	1970-01-01T00:00:41+00:00	LINK-UPDOWN: Interface Vlan 1, changed state to down.
15	Notice	1970-01-01T00:00:44+00:00	LINK-UPDOWN: Interface Vlan 1, changed state to up.
16	Notice	1970-01-01T00:00:46+00:00	LINK-CHANGED: Interface GigabitEthernet 1/1, changed state to up (MEP).
17	Notice	1970-01-01T00:00:46+00:00	LINK-CHANGED: Interface GigabitEthernet 1/2, changed state to up (MEP).
18	Notice	1970-01-01T00:00:46+00:00	LINK-CHANGED: Interface GigabitEthernet 1/3, changed state to up (MEP).
19	Notice	1970-01-01T00:00:46+00:00	LINK-CHANGED: Interface GigabitEthernet 1/4, changed state to up (MEP).
20	Notice	1970-01-01T00:00:46+00:00	LINK-CHANGED: Interface GigabitEthernet 1/5, changed state to up (MEP).

3.1.7. Detailed Log

Click on “Monitor>system >Information”.

Detailed System Log Information

ID	1

Message

Level	Notice
Time	1970-01-01T00:00:30+00:00
Message	LINK-CHANGED: Interface GigabitEthernet 1/1, changed state to down .

3.2. Ports

3.2.1. State

Click on “Monitor>Ports>State”.

Port State Overview

3.2.2. Traffic Overview

Click on “Monitor>Ports>Traffic Overview”.

Port Statistics Overview

Port	Packets		Bytes		Errors		Drops		Filtered
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1	2	0	6050	0	2	0	0	0	0
2	3	0	10396	0	3	0	0	0	0
3	0	0	0	0	0	0	0	0	0
4	17	0	38689	0	17	0	0	0	0
5	0	0	0	0	0	0	0	0	0
6	878083	12739	107325439	2230591	20	0	0	0	336840
7	0	0	0	0	0	0	0	0	0
8	2	0	2374	0	2	0	0	0	0
9	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0	0

3.2.3. QoS Statistics

Click on “Monitor>Ports>QoS Statistics”.

Queuing Counters

Port	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q7	
	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	878189	2888	0	0	0	0	0	0	0	0	0	0	0	0	0	9897
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

3.2.4. QCL Status

Click on “Monitor>Ports>QCL Status”.

QoS Control List Status

User	QCE	Port	Frame Type	Action							Conflict
				CoS	DPL	DSCP	PCP	DEI	Policy	Ingress Map	
No entries											

3.2.5. Detailed Statistics

Click on “Monitor>Ports>Detailed Statistics”.

Detailed Port Statistics Port 1

Port 1 Auto-refresh Refresh Clear

Receive Total		Transmit Total	
Rx Packets	2	Tx Packets	0
Rx Octets	6050	Tx Octets	0
Rx Unicast	0	Tx Unicast	0
Rx Multicast	0	Tx Multicast	0
Rx Broadcast	0	Tx Broadcast	0
Rx Pause	0	Tx Pause	0
Receive Size Counters		**Transmit Size Counters**	
Rx 64 Bytes	0	Tx 64 Bytes	0
Rx 65-127 Bytes	0	Tx 65-127 Bytes	0
Rx 128-255 Bytes	0	Tx 128-255 Bytes	0
Rx 256-511 Bytes	0	Tx 256-511 Bytes	0
Rx 512-1023 Bytes	0	Tx 512-1023 Bytes	0
Rx 1024-1526 Bytes	0	Tx 1024-1526 Bytes	0
Rx 1527- Bytes	2	Tx 1527- Bytes	0
Receive Queue Counters		**Transmit Queue Counters**	
Rx Q0	0	Tx Q0	0
Rx Q1	0	Tx Q1	0
Rx Q2	0	Tx Q2	0
Rx Q3	0	Tx Q3	0
Rx Q4	0	Tx Q4	0
Rx Q5	0	Tx Q5	0
Rx Q6	0	Tx Q6	0
Rx Q7	0	Tx Q7	0
Receive Error Counters		**Transmit Error Counters**	
Rx Drops	0	Tx Drops	0
Rx CRC/Alignment	0	Tx Late/Exc. Coll.	0
Rx Undersize	0		
Rx Oversize	0		
Rx Fragments	0		
Rx Jabber	0		
Rx Filtered	0		

3.3. Link OAM

3.3.1. Statistics

Click on “Monitor>Link OAM>Statistics”.

Detailed Link OAM Statistics for Port 1

Port 1 Auto-refresh Refresh Clear

Receive Total		Transmit Total	
Rx OAM Information PDU's	0	Tx OAM Information PDU's	0
Rx Unique Error Event Notification	0	Tx Unique Error Event Notification	0
Rx Duplicate Error Event Notification	0	Tx Duplicate Error Event Notification	0
Rx Loopback Control	0	Tx Loopback Control	0
Rx Variable Request	0	Tx Variable Request	0
Rx Variable Response	0	Tx Variable Response	0
Rx Org Specific PDU's	0	Tx Org Specific PDU's	0
Rx Unsupported Codes	0	Tx Unsupported Codes	0
Rx Link Fault PDU's	0	Tx Link Fault PDU's	0
Rx Dying Gasp	0	Tx Dying Gasp	0
Rx Critical Event PDU's	0	Tx Critical Event PDU's	0

3.3.2. Port Status

Click on “Monitor>Link OAM>Ports Status”.

Detailed Link OAM Status for Port 1

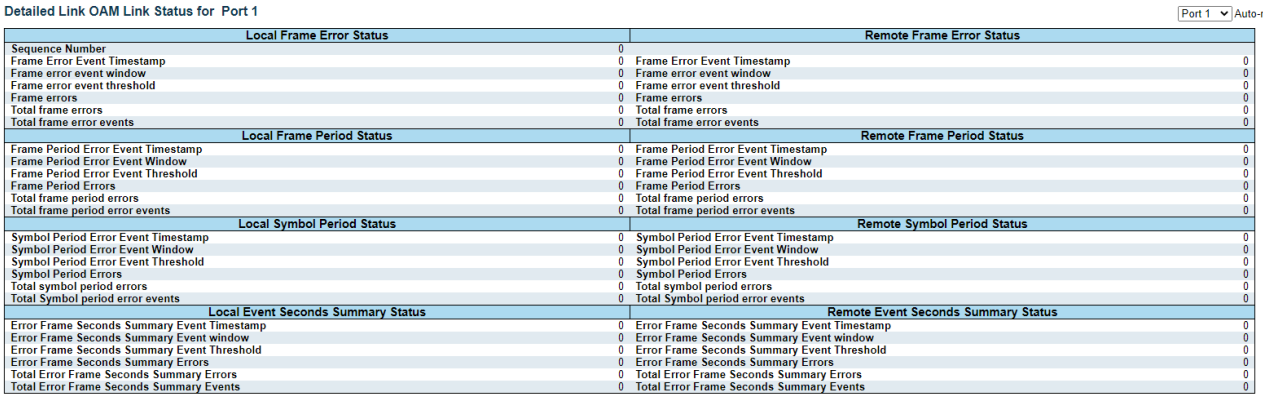
Port 1 Auto-refresh Refr

PDU Permission	Receive only
Discovery State	Fault state
Peer MAC Address	------

Local		Peer	
Mode	Passive	Mode	------
Unidirectional Operation Support	Disabled	Unidirectional Operation Support	------
Remote Loopback Support	Disabled	Remote Loopback Support	------
Link Monitoring Support	Enabled	Link Monitoring Support	------
MIB Retrieval Support	Disabled	MIB Retrieval Support	------
MTU Size	1500	MTU Size	------
Multiplexer State	Forwarding	Multiplexer State	------
Parser State	Forwarding	Parser State	------
Organizational Unique Identification	02-00-c1	Organizational Unique Identification	------
PDU Revision	0	PDU Revision	------

3.3.3. Event Status

Click on “Monitor>Link OAM>Event Status”.



Detailed Link OAM Link Status for Port 1

Port 1 Auto-refresh Refre

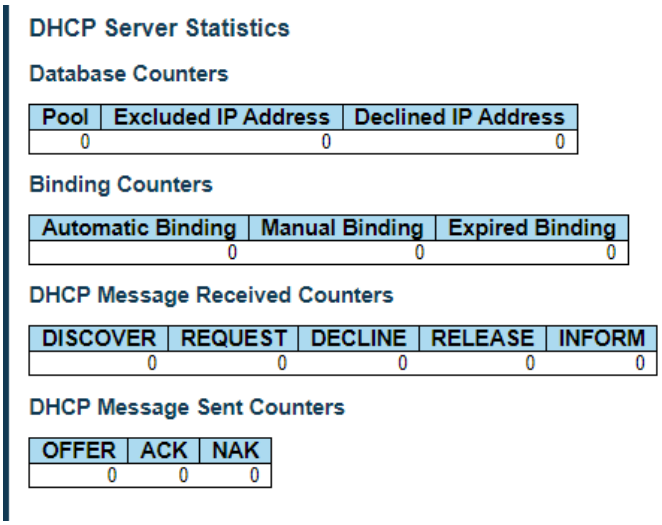
Local Frame Error Status		Remote Frame Error Status	
Sequence Number	0		
Frame Error Event Timestamp	0	Frame Error Event Timestamp	0
Frame error event window	0	Frame error event window	0
Frame error event threshold	0	Frame error event threshold	0
Frame errors	0	Frame errors	0
Total frame errors	0	Total frame errors	0
Total frame error events	0	Total frame error events	0
Local Frame Period Status		**Remote Frame Period Status**	
Frame Period Error Event Timestamp	0	Frame Period Error Event Timestamp	0
Frame Period Error Event Window	0	Frame Period Error Event Window	0
Frame Period Error Event Threshold	0	Frame Period Error Event Threshold	0
Frame Period Errors	0	Frame Period Errors	0
Total frame period errors	0	Total frame period errors	0
Total frame period error events	0	Total frame period error events	0
Local Symbol Period Status		**Remote Symbol Period Status**	
Symbol Period Error Event Timestamp	0	Symbol Period Error Event Timestamp	0
Symbol Period Error Event Window	0	Symbol Period Error Event Window	0
Symbol Period Error Event Threshold	0	Symbol Period Error Event Threshold	0
Symbol Period Errors	0	Symbol Period Errors	0
Total symbol period errors	0	Total symbol period errors	0
Total Symbol period error events	0	Total Symbol period error events	0
Local Event Seconds Summary Status		**Remote Event Seconds Summary Status**	
Error Frame Seconds Summary Event Timestamp	0	Error Frame Seconds Summary Event Timestamp	0
Error Frame Seconds Summary Event window	0	Error Frame Seconds Summary Event window	0
Error Frame Seconds Summary Event Threshold	0	Error Frame Seconds Summary Event Threshold	0
Error Frame Seconds Summary Errors	0	Error Frame Seconds Summary Errors	0
Total Error Frame Seconds Summary Errors	0	Total Error Frame Seconds Summary Errors	0
Total Error Frame Seconds Summary Events	0	Total Error Frame Seconds Summary Events	0

3.4. DHCPv4

3.4.1. Server

3.4.1.1. Statistics

Click on “Monitor>DHCP4>Server>Statistics”.



DHCP Server Statistics

Database Counters

Pool	Excluded IP Address	Declined IP Address
0	0	0

Binding Counters

Automatic Binding	Manual Binding	Expired Binding
0	0	0

DHCP Message Received Counters

DISCOVER	REQUEST	DECLINE	RELEASE	INFORM
0	0	0	0	0

DHCP Message Sent Counters

OFFER	ACK	NAK
0	0	0

3.4.1.2. Binding

Click on “Monitor>DHCP4>Server>Binding”.

DHCP Server Binding IP

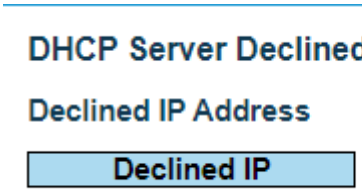
Auto-refresh Refresh Clear Selected Clear Automatic Clear Manual Clear Expired

Binding IP Address

Delete	IP	Type	State	Pool Name	Server ID

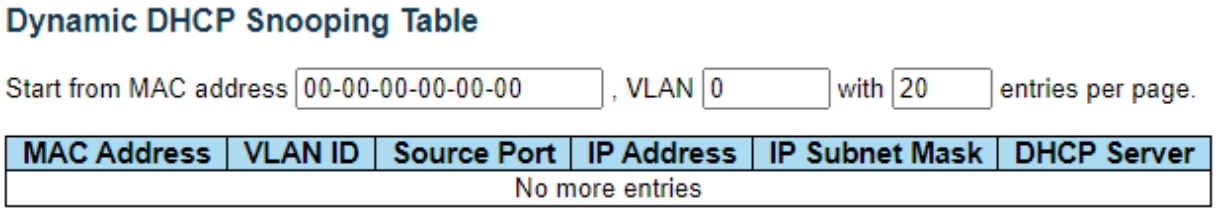
3.4.1.3. Declined IP

Click on “Monitor>DHCP4>Server>Declined IP”.



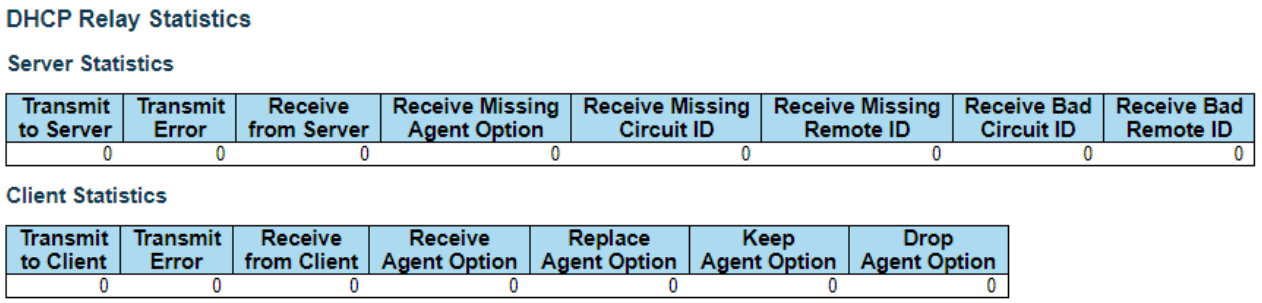
3.4.2. Snooping Table

Click on “Monitor>DHCP4>Snooping Table”.



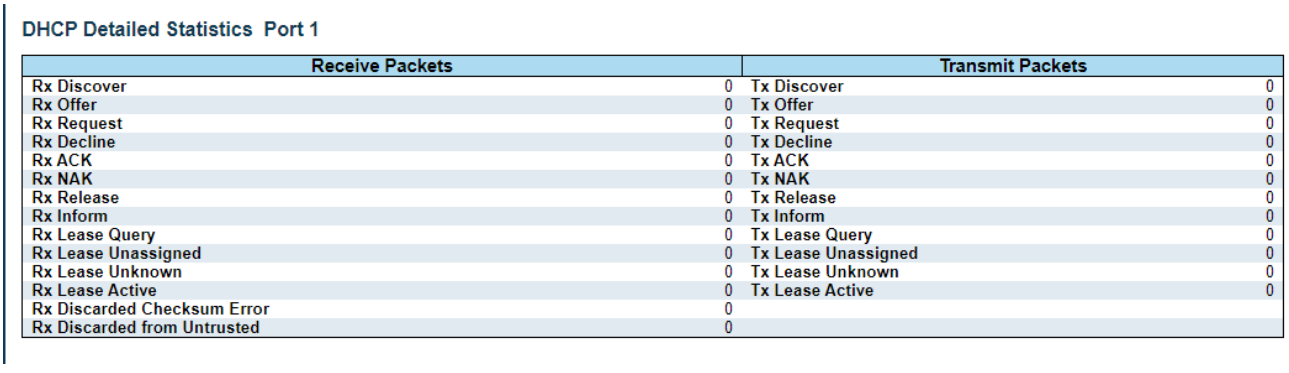
3.4.3. Relay Statistics

Click on “Monitor>DHCP4>Relay Statistics”.



3.4.4. Detailed Statistics

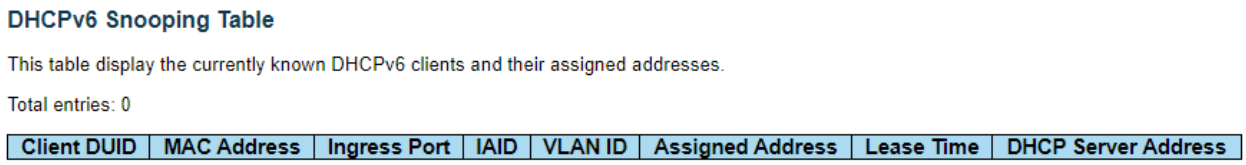
Click on “Monitor>DHCP4>Detailed Statistics”.



3.5. DHCPv6

3.5.1. Snooping Table

Click on “Monitor>DHCPv6>Snooping Table”.



DHCPv6 Snooping Table

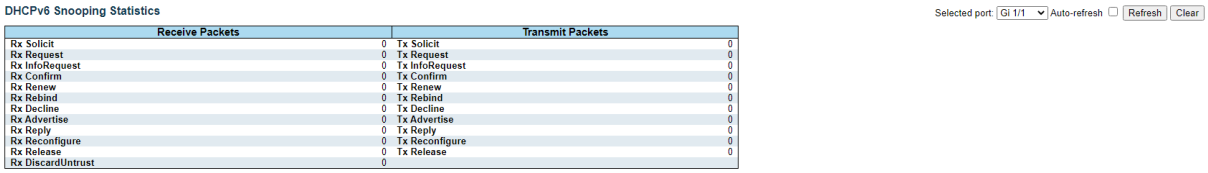
This table display the currently known DHCPv6 clients and their assigned addresses.

Total entries: 0

Client DUID	MAC Address	Ingress Port	IAID	VLAN ID	Assigned Address	Lease Time	DHCP Server Address

3.5.2. Snooping

Click on “Monitor>DHCPv6>Snooping”.



DHCPv6 Snooping Statistics

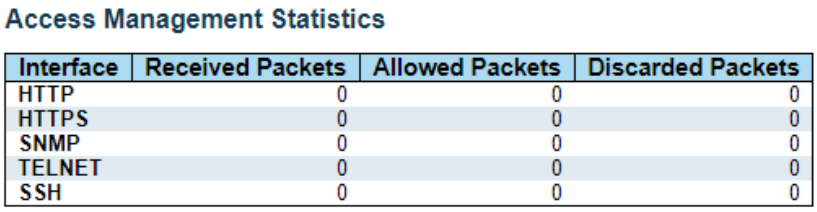
Selected port: Gi 1/1 Auto-refresh Refresh Clear

Receive Packets		Transmit Packets	
Rx Solicit	0	Tx Solicit	0
Rx Request	0	Tx Request	0
Rx InfoRequest	0	Tx InfoRequest	0
Rx Confirm	0	Tx Confirm	0
Rx Renew	0	Tx Renew	0
Rx Rebind	0	Tx Rebind	0
Rx Decline	0	Tx Decline	0
Rx Advertise	0	Tx Advertise	0
Rx Reply	0	Tx Reply	0
Rx Reconfigure	0	Tx Reconfigure	0
Rx Release	0	Tx Release	0
Rx DiscardUntrust	0		

3.6. Security

3.6.1. Access Management Statistics

Click on “Monitor>Security>Access Management Statistics”.



Access Management Statistics

Interface	Received Packets	Allowed Packets	Discarded Packets
HTTP	0	0	0
HTTPS	0	0	0
SNMP	0	0	0
TELNET	0	0	0
SSH	0	0	0

3.6.2. Network

3.6.2.1. Port Security

3.6.2.1.1. Overview

Click on “Monitor>Security>Network>Port Security>Overview”.

Port Security Switch Status

User Module Legend

User Module Name	Abbr
Port Security (Admin)	P
802.1X	8
Voice VLAN	V

Port Status

Clear	Port	Users	Violation Mode	State	MAC Count		
					Current	Violating	Limit
Clear	1	---	Disabled	Disabled	-	-	-
Clear	2	---	Disabled	Disabled	-	-	-
Clear	3	---	Disabled	Disabled	-	-	-
Clear	4	---	Disabled	Disabled	-	-	-
Clear	5	---	Disabled	Disabled	-	-	-
Clear	6	---	Disabled	Disabled	-	-	-
Clear	7	---	Disabled	Disabled	-	-	-
Clear	8	---	Disabled	Disabled	-	-	-
Clear	9	---	Disabled	Disabled	-	-	-
Clear	10	---	Disabled	Disabled	-	-	-
Clear	11	---	Disabled	Disabled	-	-	-
Clear	12	---	Disabled	Disabled	-	-	-
Clear	13	---	Disabled	Disabled	-	-	-
Clear	14	---	Disabled	Disabled	-	-	-
Clear	15	---	Disabled	Disabled	-	-	-
Clear	16	---	Disabled	Disabled	-	-	-

3.6.2.1.2. Details

Click on “Monitor>Security>Network>Port Security>Details”.

Port Security Port Status Port 1

Clear	VLAN ID	MAC Address	State	Age/Hold
No MAC addresses attached				

3.6.2.2.NAS

3.6.2.2.1 Switch

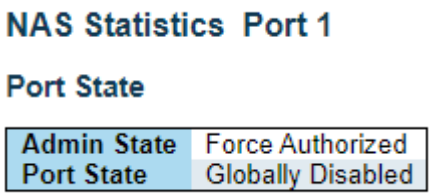
Click on “Monitor>Security>Network>NAS>Switch”.

Network Access Server Switch Status

Port	Admin State	Port State	Last Source	Last ID	QoS Class	Port VLAN ID
1	Force Authorized	Globally Disabled			-	
2	Force Authorized	Globally Disabled			-	
3	Force Authorized	Globally Disabled			-	
4	Force Authorized	Globally Disabled			-	
5	Force Authorized	Globally Disabled			-	
6	Force Authorized	Globally Disabled			-	
7	Force Authorized	Globally Disabled			-	
8	Force Authorized	Globally Disabled			-	
9	Force Authorized	Globally Disabled			-	
10	Force Authorized	Globally Disabled			-	
11	Force Authorized	Globally Disabled			-	
12	Force Authorized	Globally Disabled			-	
13	Force Authorized	Globally Disabled			-	
14	Force Authorized	Globally Disabled			-	
15	Force Authorized	Globally Disabled			-	
16	Force Authorized	Globally Disabled			-	

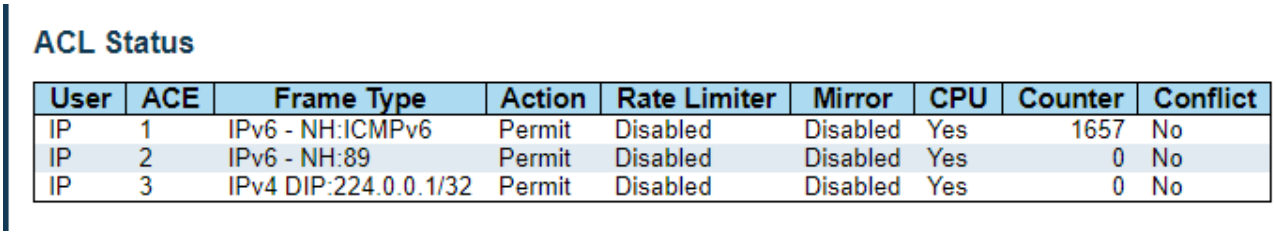
3.6.2.2. Port

Click on “Monitor>Security>Network>NAS>Port”.



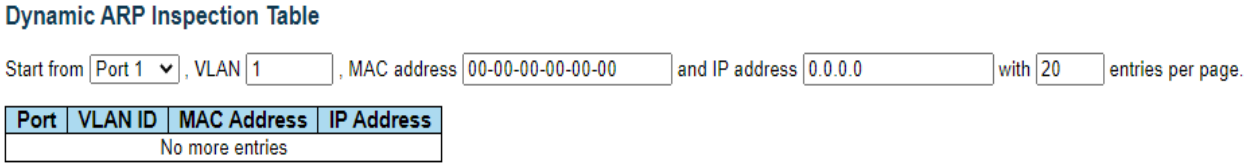
3.6.2.3. ACL Status

Click on “Monitor>Security>Network>ACL Status”.



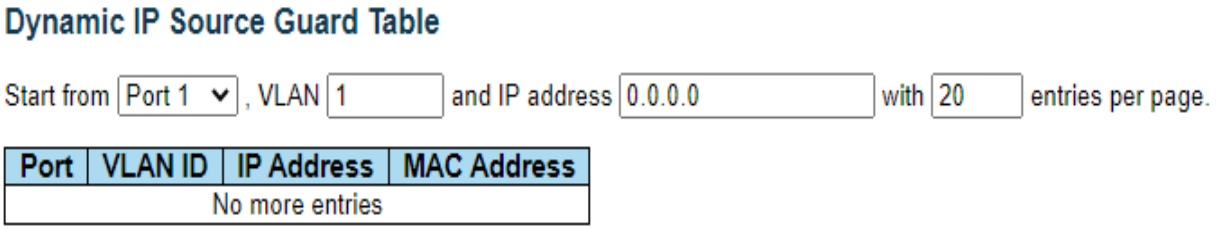
3.6.2.4. ARP Inspection

Click on “Monitor>Security>Network>ARP Inspection”.



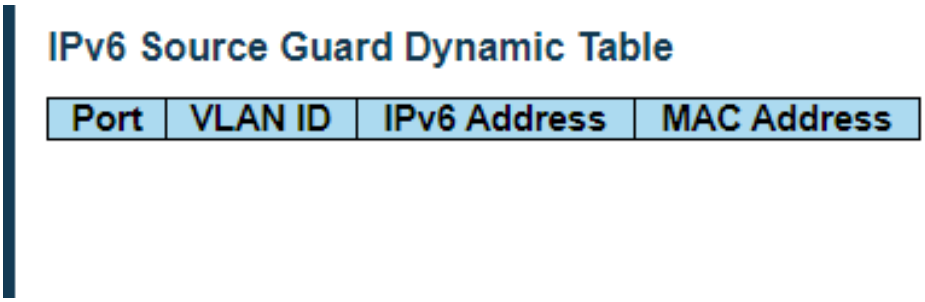
3.6.2.5. IP Source Guard

Click on “Monitor>Security>Network>IP Source Guard”.



3.6.2.6. IPv6 Source Guard

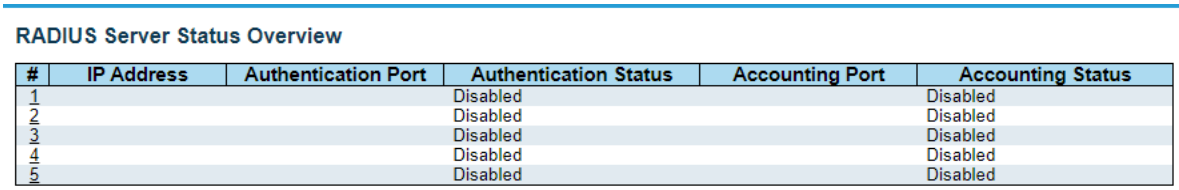
Click on “Monitor>Security>Network>IPv6 Source Guard”.



3.6.3. AAA

3.6.3.1. RADIUS Overview

Click on “Monitor>Security>AAA>RADIUS Overview”.



RADIUS Server Status Overview

#	IP Address	Authentication Port	Authentication Status	Accounting Port	Accounting Status
1			Disabled		Disabled
2			Disabled		Disabled
3			Disabled		Disabled
4			Disabled		Disabled
5			Disabled		Disabled

3.6.3.2. RADIUS Details

Click on “Monitor>Security>AAA>RADIUS Details”.

RADIUS Authentication Statistics for Server #1

Receive Packets		Transmit Packets	
Access Accepts	0	Access Requests	0
Access Rejects	0	Access Retransmissions	0
Access Challenges	0	Pending Requests	0
Malformed Access Responses	0	Timeouts	0
Bad Authenticators	0		
Unknown Types	0		
Packets Dropped	0		
Other Info			
IP Address			
State			Disabled
Round-Trip Time			0 ms

RADIUS Accounting Statistics for Server #1

Receive Packets		Transmit Packets	
Responses	0	Requests	0
Malformed Responses	0	Retransmissions	0
Bad Authenticators	0	Pending Requests	0
Unknown Types	0	Timeouts	0
Packets Dropped	0		
Other Info			
IP Address			
State			Disabled
Round-Trip Time			0 ms

3.6.4. Switch

3.6.4.1. RMON

3.6.4.1.1 Statistics

Click on “Monitor>Security>Switch>RMON>Statistics”.

RMON Statistics Status Overview

Start from Control Index 0 with 20 entries per page.

ID	Data Source (ifIndex)	Drop	Octets	Pkts	Broad-cast	Multi-cast	CRC Errors	Under-size	Over-size	Frag.	Jabb.	Coll.	64 Bytes	65 ~ 127	128 ~ 255	256 ~ 511	512 ~ 1023	1024 ~ 1588
No more entries																		

3.6.4.1.2. History

Click on “Monitor>Security>Switch>RMON>History”.

RMON History Overview

Start from Control Index 0 and Sample Index 0 with 20 entries per page.

History Index	Sample Index	Sample Start	Drop	Octets	Pkts	Broad-cast	Multi-cast	CRC Errors	Under-size	Over-size	Frag.	Jabb.	Coll.	Utilization
No more entries														

3.6.4.1.3. Alarm

Click on “Monitor>Security>Switch>RMON>Alarm”.

RMON Alarm Overview

Start from Control Index 0 with 20 entries per page.

ID	Interval	Variable	Sample Type	Value	Startup Alarm	Rising Threshold	Rising Index	Falling Threshold	Falling Index
No more entries									

3.6.4.1.4 Event

Click on “Monitor>Security>Switch>RMON>Event”.

RMON Event Overview

Start from Control Index 0 and Sample Index 0 with 20 entries per page.

Event Index	LogIndex	LogTime	LogDescription
No more entries			

3.7. Aggregation

3.7.1. Status

Click on “Monitor>Aggregation>Status”.

Aggregation Status

Aggr ID	Name	Type	Speed	Configured Ports	Aggregated Ports
No aggregation groups					

3.7.2. LACP

3.7.2.1. System Status

Click on “Monitor>Aggregation>LACP>system Status”.

LACP System Status

Local System ID

Priority	MAC Address
32768	02-00-c1-b9-15-19

Partner System Status

Aggr ID	Partner System ID	Partner Prio	Partner Key	Last Changed	Local Ports
No ports enabled or no existing partners					

3.7.2.2. Internal Status

Click on “Monitor>Aggregation>LACP>Internal Status”.

LACP Internal Port Status

Port	State	Key	Priority	Activity	Timeout	Aggregation	Synchronization	Collecting	Distributing	Defaulted	Expired
No LACP ports enabled											

3.7.2.3. Neighbor Status

Click on “Monitor>Aggregation>LACP>Neighbor Status”.

LACP Neighbor Port Status

Port	State	Aggr ID	Partner Key	Partner Port	Partner Port Prio	Activity	Timeout	Aggregation	Synchronization	Collecting	Distributing	Defaulted	Expired
No LACP neighbor status available													

3.7.2.4. Port Statistics

Click on “Monitor>Aggregation>LACP>Port Statistics”.

LACP Statistics

Port	LACP Received	LACP Transmitted	Discarded	
			Unknown	Illegal
No ports enabled				

3.8. Loop Protection

Click on “Monitor>Loop Protection”.

Loop Protection Status

Port	Action	Transmit	Loops	Status	Loop	Time of Last Loop
No ports enabled						

3.9. Spanning Tree

3.9.1. Bridge Status

Click on “Monitor>Spanning Tree>Bridge Status”.

STP Bridges

MSTI	Bridge ID	Root			Topology Flag	Topology Change Last
		ID	Port	Cost		
CIST	32768.02-00-C1-B9-15-19	32768.02-00-C1-B9-15-19	-	0	Steady	-

3.9.2. Port Status

Click on “Monitor>Spanning Tree>Port Status”.

STP Port Status

Port	CIST Role	CIST State	Uptime
1	Disabled	Discarding	-
2	Disabled	Discarding	-
3	Disabled	Discarding	-
4	DesignatedPort	Forwarding	0d 00:13:48
5	Disabled	Discarding	-
6	Disabled	Discarding	-
7	Disabled	Discarding	-
8	Disabled	Discarding	-
9	Disabled	Discarding	-
10	Disabled	Discarding	-
11	Disabled	Discarding	-
12	Disabled	Discarding	-
13	Disabled	Discarding	-
14	Disabled	Discarding	-
15	Disabled	Discarding	-
16	Disabled	Discarding	-

3.9.3. Port Statistics

Click on “Monitor>Spanning Tree>Port Statistics”.

STP Statistics

Port	Transmitted				Received				Discarded	
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
4	418	0	0	0	0	0	0	0	0	0

3.10. MVR

3.10.1. Statistics

Click on “Monitor>MVR>Statistics”.

MVR Statistics

VLAN ID	IGMP/MLD Queries Received	IGMP/MLD Queries Transmitted	IGMPv1 Joins Received	IGMPv2/MLDv1 Reports Received	IGMPv3/MLDv2 Reports Received	IGMPv2/MLDv1 Leaves Received
No more entries						

3.10.2. MVR Channel Groups

Click on “Monitor>MVR>MVR Channel Groups”.

MVR Channels (Groups) Information

Start from VLAN 1 and Group Address :: with 20 entries per page.

		Port Members														
VLAN ID	Groups	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
No more entries																	

3.10.3. MVR SFM Information

Click on “Monitor>MVR>MVR SFM Information”.

MVR SFM Information

Start from VLAN 1 and Group Address :: with 20 entries per page.

VLAN ID	Group	Port	Mode	Source Address	Type	Hardware Filter/Switch
No more entries						

3.11. IPMC

3.11.1. IGMP Snooping

3.11.1.1. Status

Click on “Monitor>IPMC>IGMP Snooping>Status”.

IGMP Snooping Status

Statistics

VLAN ID	Querier Version	Host Version	Querier Status	Queries Transmitted	Queries Received	V1 Reports Received	V2 Reports Received	V3 Reports Received	V2 Leaves Received

Router Port

Port	Status
1	-
2	-
3	-
4	-
5	-
6	-
7	-
8	-
9	-
10	-
11	-
12	-
13	-
14	-
15	-
16	-

3.11.1.2. Groups Information

Click on “Monitor>IPMC>IGMP Snooping>Groups Information”.

IGMP Snooping Group Information

Start from VLAN 1 and group address 224.0.0.0 with 20 entries per page.

		Port Members														
VLAN ID	Groups	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
No more entries																	

3.11.1.3. IPv4 SFM Information

Click on “Monitor>IPMC>IGMP Snooping>Ipv4 SFM Information”.

IGMP SFM Information

Start from VLAN 1 and Group 224.0.0.0 with 20 entries per page.

VLAN ID	Group	Port	Mode	Source Address	Type	Hardware Filter/Switch
No more entries						

3.11.2. MLD Snooping

3.11.2.1. Status

Click on “Monitor>IPMC>MLD Snooping>Status”.

MLD Snooping Status

Statistics

VLAN ID	Querier Version	Host Version	Querier Status	Queries Transmitted	Queries Received	V1 Reports Received	V2 Reports Received	V1 Leaves Received

Router Port

Port	Status
1	-
2	-
3	-
4	-
5	-
6	-
7	-
8	-
9	-
10	-
11	-
12	-
13	-
14	-
15	-
16	-

3.11.2.2. Groups Information

Click on “Monitor>IPMC>MLD Snooping>Groups Information”.

MLD Snooping Group Information

Start from VLAN 1 and group address ff00:: with 20 entries per page.

		Port Members														
VLAN ID	Groups	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
No more entries																	

3.11.2.3. Ipv6 SFM Information

Click on “Monitor>IPMC>MLD Snooping>Ipv6 SFM Information”.

MLD SFM Information

Start from VLAN 1 and Group ff00:: with 20 entries per page.

VLAN ID	Group	Port	Mode	Source Address	Type	Hardware Filter/Switch
No more entries						

3.12. LLDP

3.12.1. Neighbors

Click on “Monitor>LLDP>Neighbors”.

LLDP Neighbor Information

LLDP Remote Device Summary						
Local Interface	Chassis ID	Port ID	Port Description	System Name	System Capabilities	Management Address
GigabitEthernet 1/4	20-77-59-88-88-88	6	GigabitEthernet 1/6	Switch	Bridge(+)	192.168.8.188 (IPv4) - if-index:0

3.12.2. LLDP-MED Neighbors

Click on “Monitor>LLDP>LLDP-MED Neighbors”.

LLDP-MED Neighbor Information

Local Interface
No LLDP-MED neighbor information found

3.12.3. PoE

Click on “Monitor>LLDP>PoE”.

LLDP Neighbor Power Over Ethernet Information

Local Interface	Power Type	Power Source	Power Priority	Maximum Power
GigabitEthernet 1/4	PSE Device	Primary Power Supply	Low	0 [W]

3.12.4. EEE

Click on “Monitor>LLDP>EEE”.

LLDP Neighbors EEE Information

Local Interface	Tx Tw	Rx Tw	Fallback Receive Tw	Echo Tx Tw	Echo Rx Tw	Resolved Tx Tw	Resolved Rx Tw	EEE in Sync
GigabitEthernet 1/4	EEE not enabled for this interface							

3.12.5. Port Statistics

Click on “Monitor>LLDP>Port Statistics”.

LLDP Global Counters

Global Counters	
Clear global counters	☑
Neighbor entries were last changed	1970-01-01T00:01:03+00:00 (1180 secs. ago)
Total Neighbors Entries Added	1
Total Neighbors Entries Deleted	0
Total Neighbors Entries Dropped	0
Total Neighbors Entries Aged Out	0

LLDP Statistics Local Counters

Local Interface	Tx Frames	Rx Frames	Rx Errors	Frames Discarded	TLVs Discarded	TLVs Unrecognized	Org. Discarded	Age-Outs	Clear
*	*	*	*	*	*	*	*	*	☑
GigabitEthernet 1/1	0	0	0	0	0	0	0	0	☑
GigabitEthernet 1/2	0	0	0	0	0	0	0	0	☑
GigabitEthernet 1/3	0	0	0	0	0	0	0	0	☑
GigabitEthernet 1/4	40	40	0	0	0	0	0	0	☑
GigabitEthernet 1/5	0	0	0	0	0	0	0	0	☑
GigabitEthernet 1/6	0	0	0	0	0	0	0	0	☑
GigabitEthernet 1/7	0	0	0	0	0	0	0	0	☑
GigabitEthernet 1/8	0	0	0	0	0	0	0	0	☑
GigabitEthernet 1/9	0	0	0	0	0	0	0	0	☑
GigabitEthernet 1/10	0	0	0	0	0	0	0	0	☑
GigabitEthernet 1/11	0	0	0	0	0	0	0	0	☑
GigabitEthernet 1/12	0	0	0	0	0	0	0	0	☑
10GigabitEthernet 1/1	0	0	0	0	0	0	0	0	☑
10GigabitEthernet 1/2	0	0	0	0	0	0	0	0	☑
10GigabitEthernet 1/3	0	0	0	0	0	0	0	0	☑
10GigabitEthernet 1/4	0	0	0	0	0	0	0	0	☑

3.13. Ethernet Services

3.13.1. EVC Statistics

Click on “Monitor>Ethernet Services>EVC Statistics”.

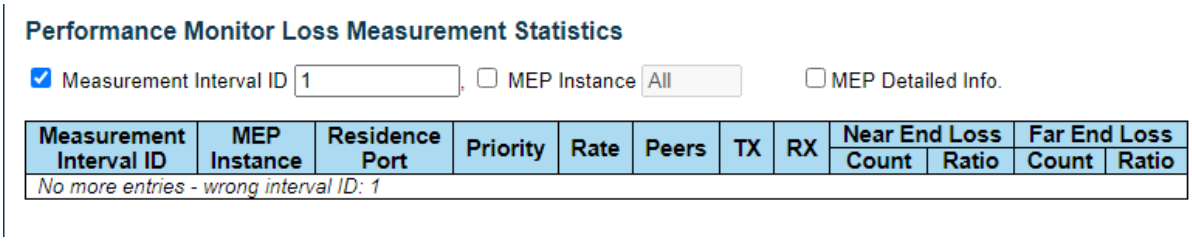
EVC Statistics

Clear	Port	Green Frames		Yellow Frames		Red Frames	Discarded Frames	
		Rx	Tx	Rx	Tx	Rx	Rx	Tx
0	0	0	0	0	0	0	0	
1	0	0	0	0	0	0	0	
2	0	0	0	0	0	0	0	
3	0	0	0	0	0	0	0	
4	0	0	0	0	0	0	0	
5	0	0	0	0	0	0	0	
6	0	0	0	0	0	0	0	
7	0	0	0	0	0	0	0	

3.14. Performance Monitor

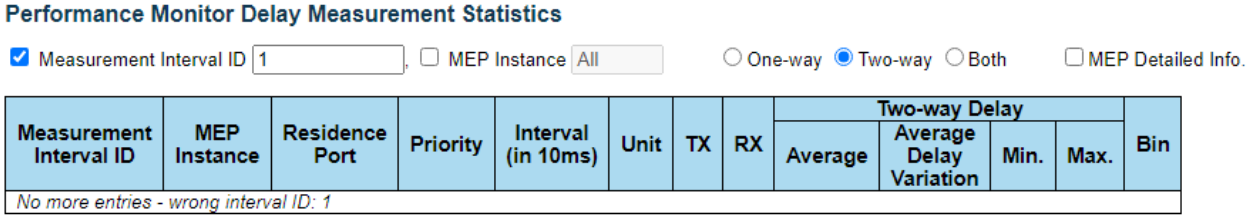
3.14.1. LM Statistics

Click on “Monitor>Performance Monitor>LM Statistics”.



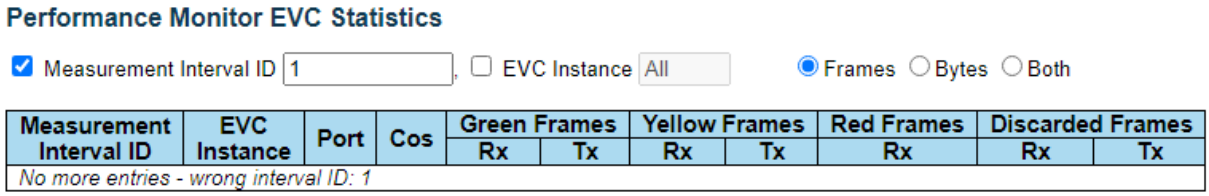
3.14.2. DM Statistics

Click on “Monitor>Performance Monitor>DM Statistics”.



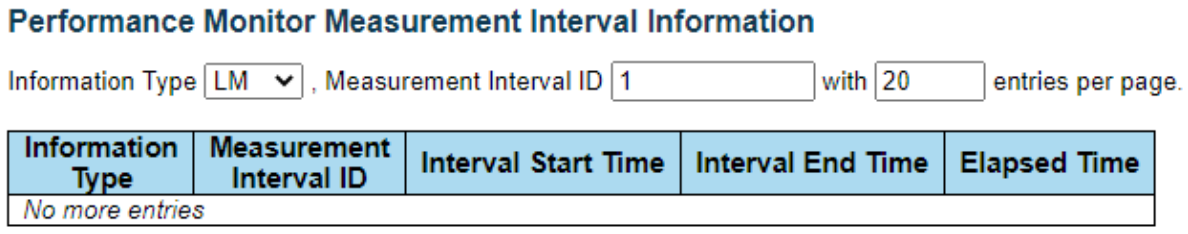
3.14.3. EVC Statistics

Click on “Monitor>Performance Monitor>EVC Statistics”.



3.14.4. Interval Information

Click on “Monitor>Performance Monitor>Interval Information”.



3.15. PoE

Click on “Monitor>PoE”.

Power Over Ethernet Status

Local Port	PD class	Power Requested	Power Allocated	Power Used	Current Used	Priority	Port Status
1	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
2	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
3	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
4	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
5	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
6	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
7	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
8	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
Total		0 [W]	0 [W]	0 [W]	0 [mA]		

3.16. MAC Table

Click on “Monitor>MAC Table”.

MAC Address Table

Start from VLAN 1 and MAC address 00-00-00-00-00-00 with 20 entries per page.

			Port Members															
Type	VLAN	MAC Address	CPU	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Dynamic	1	00-0C-29-6A-7C-32					✓												
Dynamic	1	00-0C-29-C9-25-3D					✓												
Dynamic	1	00-50-56-89-5C-6E					✓												
Dynamic	1	02-0A-C6-DA-32-85					✓												
Dynamic	1	04-D9-F5-03-A6-F4					✓												
Dynamic	1	08-97-98-69-9C-5A					✓												
Dynamic	1	10-90-27-E7-89-27					✓												
Dynamic	1	12-16-DE-F3-4F-D1					✓												
Dynamic	1	12-20-22-E1-55-E8					✓												
Dynamic	1	1C-69-7A-4A-1B-6A					✓												
Dynamic	1	20-77-59-04-AE-F0					✓												
Dynamic	1	20-77-59-88-88-8E					✓												
Dynamic	1	20-F4-78-2E-A4-08					✓												
Dynamic	1	22-3F-30-B4-E8-FC					✓												
Dynamic	1	22-45-AA-69-00-34					✓												
Dynamic	1	2C-4D-54-67-4C-1D					✓												
Dynamic	1	2C-59-E5-D4-56-7A					✓												
Dynamic	1	30-9C-23-C3-9F-84					✓												
Dynamic	1	30-9C-23-F7-70-C8					✓												
Static	1	33-33-00-00-00-01	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

3.17. VLANs

3.17.1. Membership

Click on “Monitor>VLANs>Membership”.

VLAN Membership Status for Combined users

Start from VLAN 1 with 20 entries per page. |<< >>

VLAN ID	Port Members															
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

3.17.2. Ports

Click on “Monitor>VLANs>Ports”.

VLAN Port Status for Combined users

Port	Port Type	Ingress Filtering	Frame Type	Port VLAN ID	Tx Tag	Untagged VLAN ID	Conflicts
1	C-Port	☑	All	1	Untag All		No
2	C-Port	☑	All	1	Untag All		No
3	C-Port	☑	All	1	Untag All		No
4	C-Port	☑	All	1	Untag All		No
5	C-Port	☑	All	1	Untag All		No
6	C-Port	☑	All	1	Untag All		No
7	C-Port	☑	All	1	Untag All		No
8	C-Port	☑	All	1	Untag All		No
9	C-Port	☑	All	1	Untag All		No
10	C-Port	☑	All	1	Untag All		No
11	C-Port	☑	All	1	Untag All		No
12	C-Port	☑	All	1	Untag All		No
13	C-Port	☑	All	1	Untag All		No
14	C-Port	☑	All	1	Untag All		No
15	C-Port	☑	All	1	Untag All		No
16	C-Port	☑	All	1	Untag All		No

3.18. MVRP

Click on “Monitor>MVRP”.

MVRP Statistics

Port	Failed Registrations	Last PDU Origin
1	0	00-00-00-00-00-00
2	0	00-00-00-00-00-00
3	0	00-00-00-00-00-00
4	0	00-00-00-00-00-00
5	0	00-00-00-00-00-00
6	0	00-00-00-00-00-00
7	0	00-00-00-00-00-00
8	0	00-00-00-00-00-00
9	0	00-00-00-00-00-00
10	0	00-00-00-00-00-00
11	0	00-00-00-00-00-00
12	0	00-00-00-00-00-00
13	0	00-00-00-00-00-00
14	0	00-00-00-00-00-00
15	0	00-00-00-00-00-00
16	0	00-00-00-00-00-00

3.19. SFlow

Click on “Monitor>SFLow”.

sFlow Statistics

Receiver Statistics

Owner	<none>
IP Address/Hostname	0.0.0.0
Timeout	0
Tx Successes	0
Tx Errors	0
Flow Samples	0
Counter Samples	0

Port Statistics

Port	Flow Samples	Counter Samples
1	0	0
2	0	0
3	0	0
4	0	0
5	0	0
6	0	0
7	0	0
8	0	0
9	0	0
10	0	0
11	0	0
12	0	0
13	0	0
14	0	0
15	0	0
16	0	0

3.20. DDMI

3.20.1.Overview

Click on “Monitor>DDMI>Overview”.

DDMI Overview

Port	Vendor	Part Number	Serial Number	Revision	Data Code	Transceiver
13	-	-	-	-	-	-
14	-	-	-	-	-	-
15	-	-	-	-	-	-
16	-	-	-	-	-	-

3.20.2.Detailed

Click on “Monitor>DDMI>Detailed”.

Transceiver Information

Vendor	-
Part Number	-
Serial Number	-
Revision	-
Data Code	-
Transeiver	-

DDMI Information

++ : high alarm, + : high warning, - : low warning, -- : low alarm.
Tx: transmit, Rx: receive, mA: milliamperes, mW: milliwatts.

Type	Current	High Alarm Threshold	High Warn Threshold	Low Warn Threshold	Low Alarm Threshold
Temperature(C)	-	-	-	-	-
Voltage(V)	-	-	-	-	-
Tx Bias(mA)	-	-	-	-	-
Tx Power(mW)	-	-	-	-	-
Rx Power(mW)	-	-	-	-	-

3.21. UDLD

Click on “Monitor>UDLD”.

Detailed UDLD Status for Port 1

UDLD status	
UDLD Admin state	Disable
Device ID(local)	02-00-C1-B9-15-19
Device Name(local)	-
Bidirectional State	Indeterminant

Neighbour Status

Port	Device Id	Link Status	Device Name
No Neighbour ports enabled or no existing partners			

3.22. OSPF

3.22.1. Status

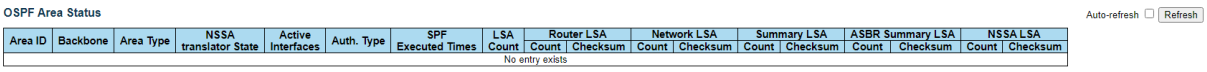
Click on“Monitor>OSPF>Status”.

OSPF Global Status

OSPF is disabled

3.22.2. Area

Click on“Monitor>OSPF>Area”.


OSPF Area Status

Auto-refresh Refresh

Area ID	Backbone	Area Type	NSSA translator State	Active Interfaces	Auth. Type	SPF Executed Times	LSA Count	Router LSA		Network LSA		Summary LSA		ASBR Summary LSA		NSSA LSA	
								Count	Checksum	Count	Checksum	Count	Checksum	Count	Checksum	Count	Checksum
No entry exists																	

3.22.3. Neighbor

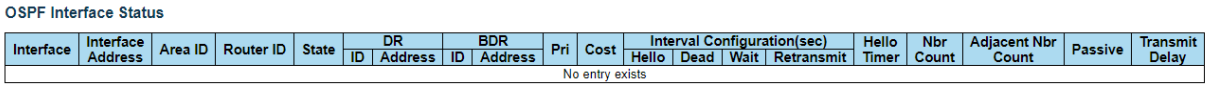
Click on“Monitor>OSPF>Neighbor”.

OSPF Neighbor Status

Neighbor ID	Priority	State	Dead Time	Interface Address	Interface
No entry exists					

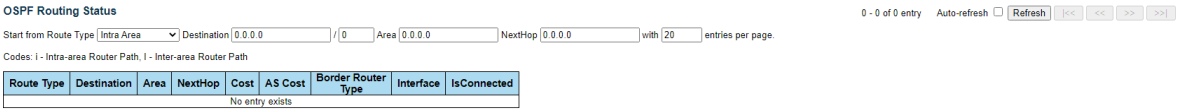
3.22.4. Interface

Click on“Monitor>OSPF>Interface”.



3.22.5. Routing

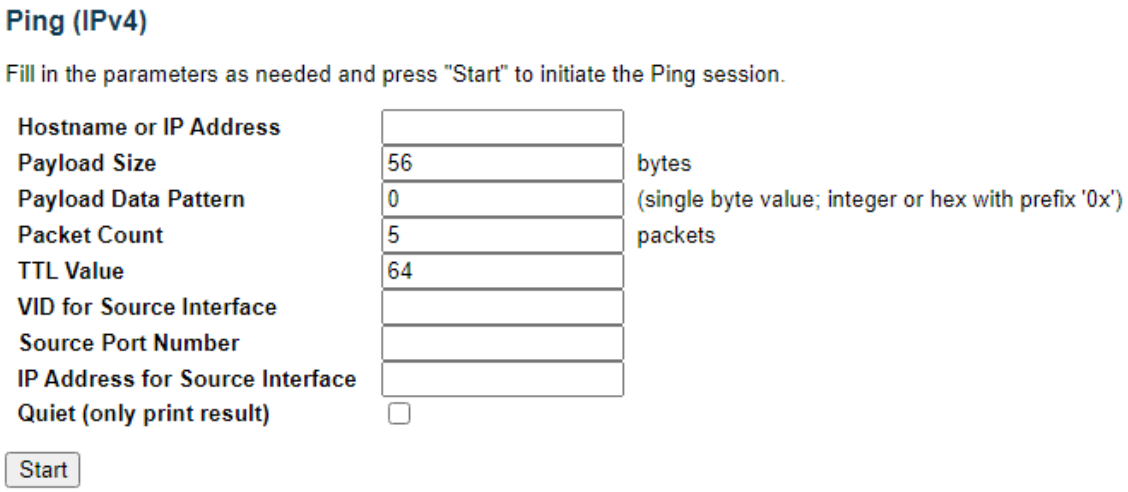
Click on“Monitor>OSPF>Routing”.



Chapter 4. Diagnostics

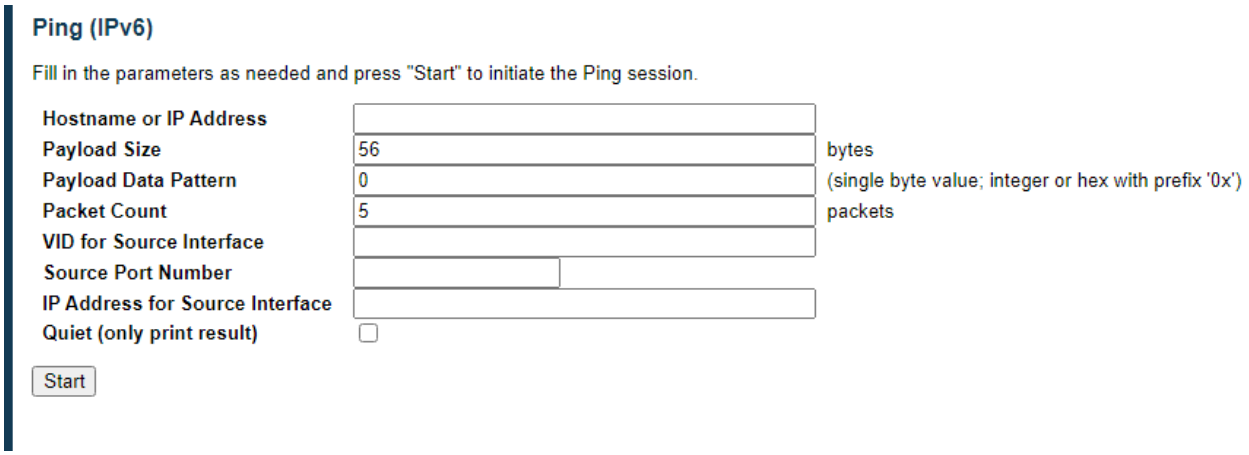
4.1. Ping (IPv4)

Click on“Diagnostics>Ping (IPv4)”.



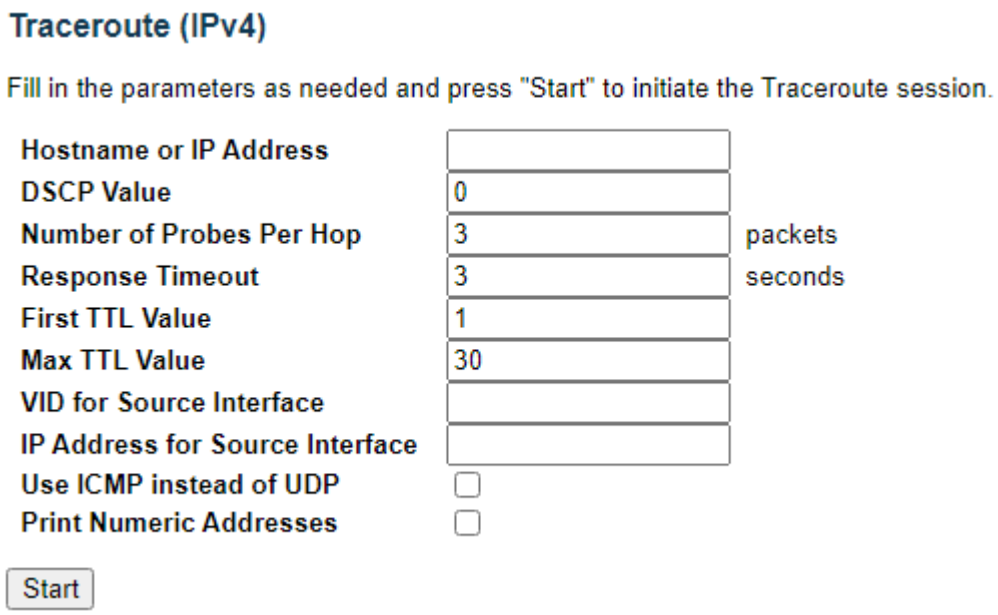
4.2. Ping (IPv6)

Click on“Diagnostics>Ping (IPv6)”.



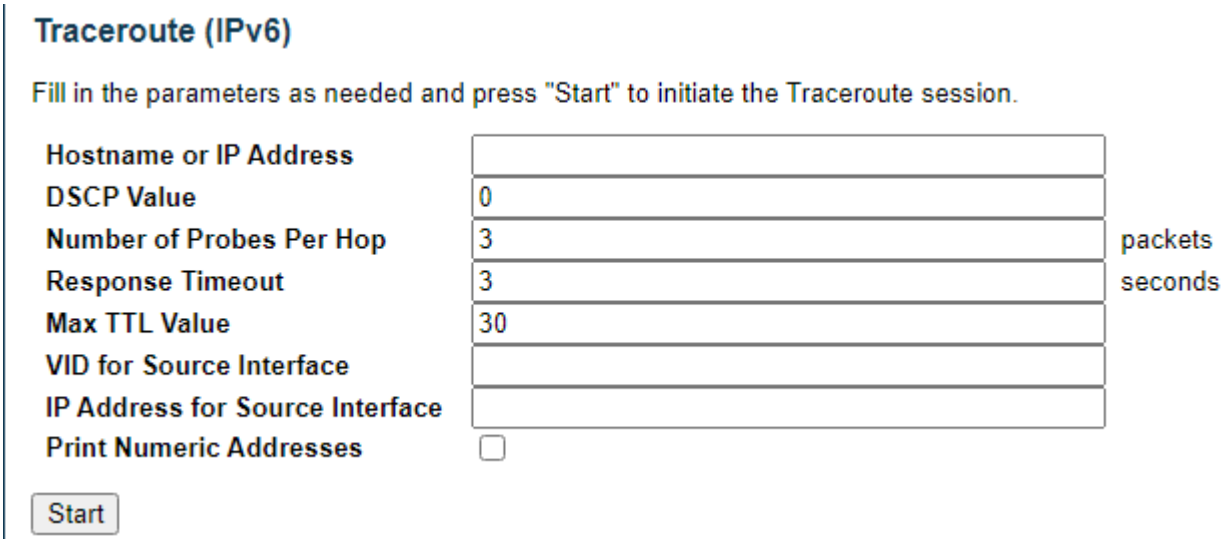
4.3. Traceroute (IPv4)

Click on“Diagnostics>Traceroute (IPv4)”.



4.4. Traceroute (IPv6)

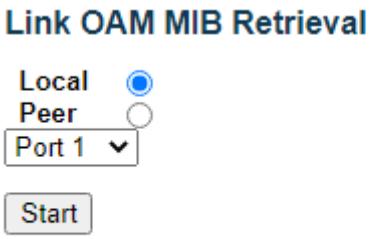
Click on“Diagnostics>Traceroute (IPv6)”.



4.5. Link OAM

4.5.1. MIB Retrieval

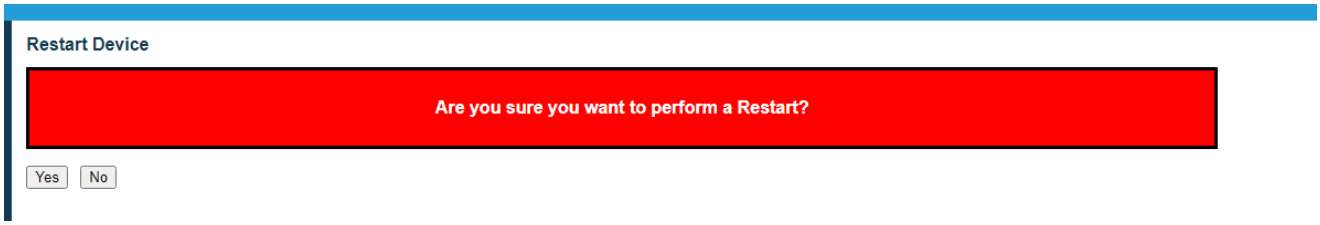
Click on“Diagnostics>Link OAM>MIB Retrieval”.



Chapter 5. Maintenance

5.1. Restart Device

Click on“Maintenance>Restart Device”.



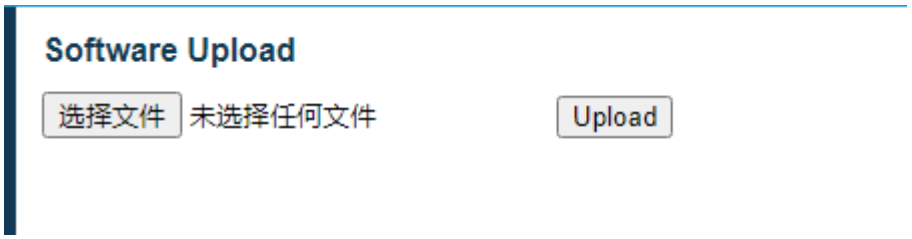
5.2. Factory Defaults

Click on“Maintenance>Factory Defaults”.

5.3. Software

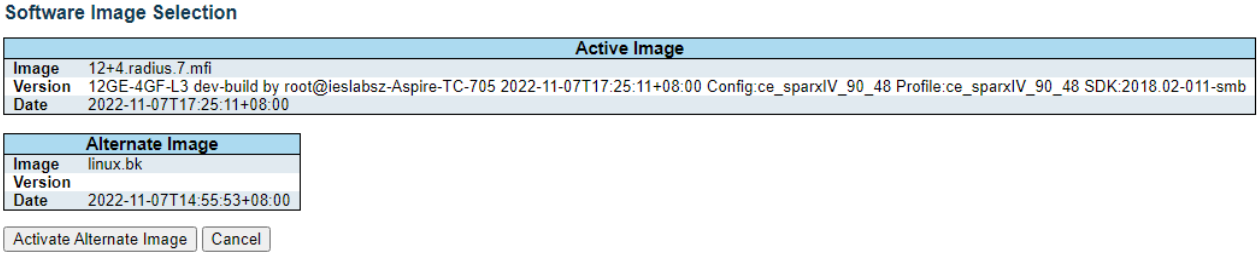
5.3.1. Upload

Click on“Maintenance>Software>Upload”.



5.3.2. Image Select

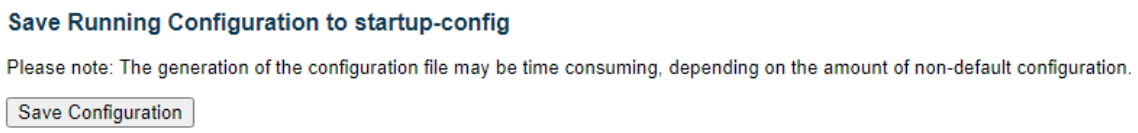
Click on“Maintenance>Software>Image Select”.



5.4.Configuration

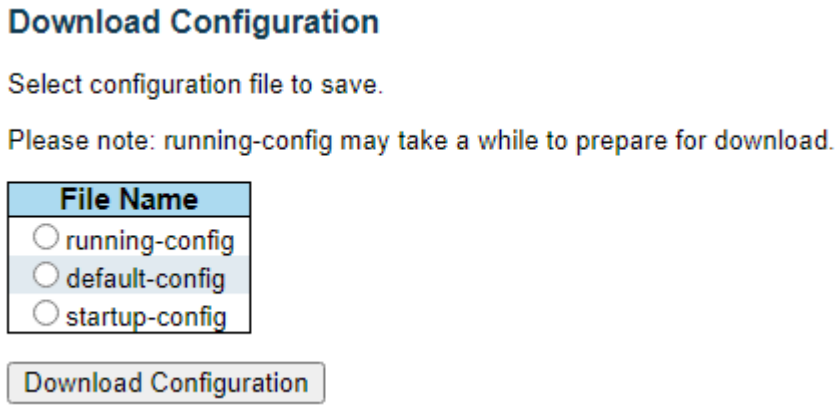
5.4.1. Save startup-config

Click on“Maintenance>Configuration>Save startup-config”.



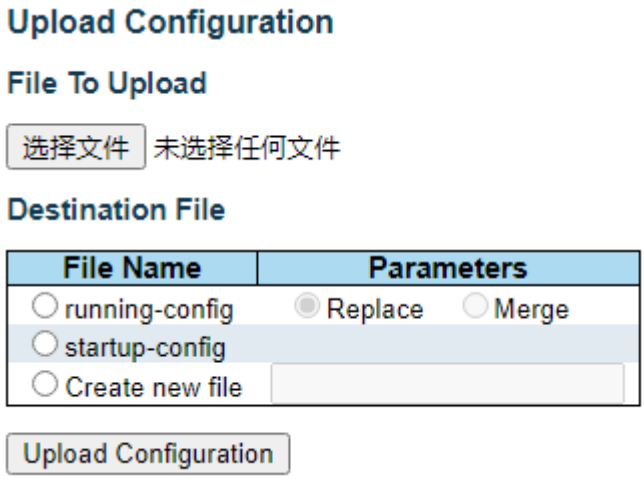
5.4.2. Download

Click on“Maintenance>Configuration>Download”.



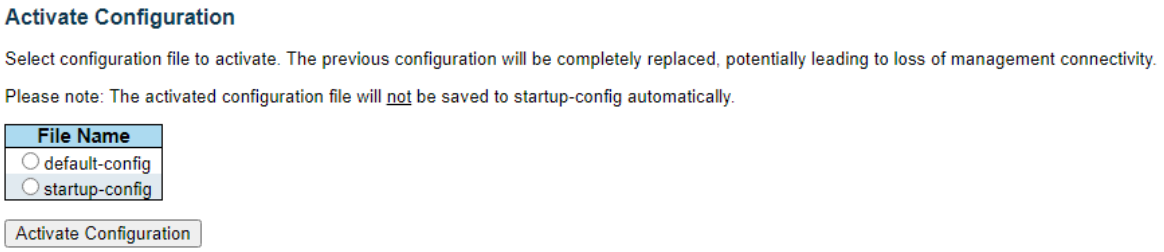
5.4.3. Upload

Click on“Maintenance>Configuration>Upload”.



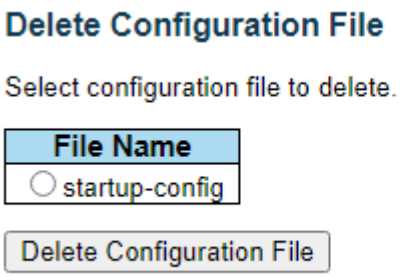
5.4.4. Activate

Click on“Maintenance>Configuration>Activate”.



5.4.5. Delete

Click on“Maintenance>Configuration>Delete”.



Appendix 1.

FAQ

Why is the page displayed abnormally when browsing the con diagram through the WEB?

Answer: Before accessing the WEB, please clear the cache and cookies of IE. Otherwise, the web page may not be displayed normally.

2. What should I do if I forget the login password?

Answer: If you forget the login password, you can initialize the password by restoring the factory settings, and press and hold the button for 10 seconds to initialize the password. Initial username "admin" and password "system".

3. Is the con diagram through the WEB browser equivalent to the con diagram through the CLI command line?

Answer: The con diagrams of the two are the same and do not conflict.

4. Why can't the bandwidth be increased after the Trunking function is completed in the con diagram?

Answer: Check whether the port properties of the port set as Trunking are consistent, including speed, duplex mode, VLAN and other properties.

5. How to solve the problem that some ports of the switch are unreachable?
Answer: When some ports on the switch are unreachable, it may be that the network cable is faulty, the network card is faulty, or the switch port is faulty, and the following tests can be passed.
Locating faults:
1. The connected computer and switch ports remain unchanged, and other network cables are replaced;
2. The connected network cable and switch port remain unchanged, and other computers are replaced;
3. The connected network cable and computer remain unchanged, and other switch ports are replaced;
4. If it is confirmed that the switch port is faulty, please contact the factory for repair;
6. What is the sequence of port adaptive state detection?
Answer: The port detects the status in the following order: 1000Mbps full duplex, 100Mbps full duplex, 100Mbps half duplex, 10Mbps full duplex, 10Mbps half duplex, detect in sequence from high to low, and automatically The highest speed connection supported.