2 Gigabit PoE + 2 2.5G SFP Slots
Layer 2 Managed Industrial Ethernet Switch
User Manual

Document Version: 01
Issue Date: 01/12/2022

Preface

This User Manual has introduced this switch:

- Product features
- Product network management configuration
- Overview of related principles of network management

Audience

This manual applies to the following engineers:

- Network administrators
- Technical support engineers
- Network engineer

Text Format Convention

Format	Description
" "	Words with “” represent the interface words. Such as: “Port No.”.
>	Multi-level path is separated by ">". Such as opening the local connection path description: Open "Control Panel> Network Connection> Local Area Connection".
Light Blue Font	It represents the words clicked to achieve hyperlink. The font color is as follows: ‘Light Blue’.

Symbols

Format	Description
 Notice	Remind the announcements in the operation, improper operation may result in data loss or equipment damage.
 Warning	Pay attention to the notes on the mark, improper operation may cause personal injury.
 Note	Make a necessary supplementary instruction for operation description.

Format	Description
 Key	Configuration, operation, or tips for device usage.
 Tips	Pay attention to the operation or information to ensure success device configuration or normal working.

Revision Record

Version No.	Date	Revision note
01	01/12/2022	Product release

Contents

1 Log in the Web Interface

1.1 System Requirements for WEB Browsing

Using the industrial Ethernet switch, the system should meet the following conditions.

Hardware and software	System requirements
CPU	Above Pentium 586
Memory	Above 128MB
Resolution	Above 1024x768
Color	256 color or above
Browser	Internet Explorer 6.0 or above
Operating system	Windows XP/7/8/10

1.2 Setting IP Address of PC

The switch default management as follows:

IP Settings	Default Value
IP Address	192.168.1.254
Subnet mask	255.255.255.0

While configuring the switch via Web:

- Before remote configuration, please make sure the route between computer and switch is reachable.
- Before local configuration, please make sure the IP address of the computer is on the same subnet to the one of switch.

Note:
When the switch is first configured. If it is configured locally, make sure the current computer network segment is 1.

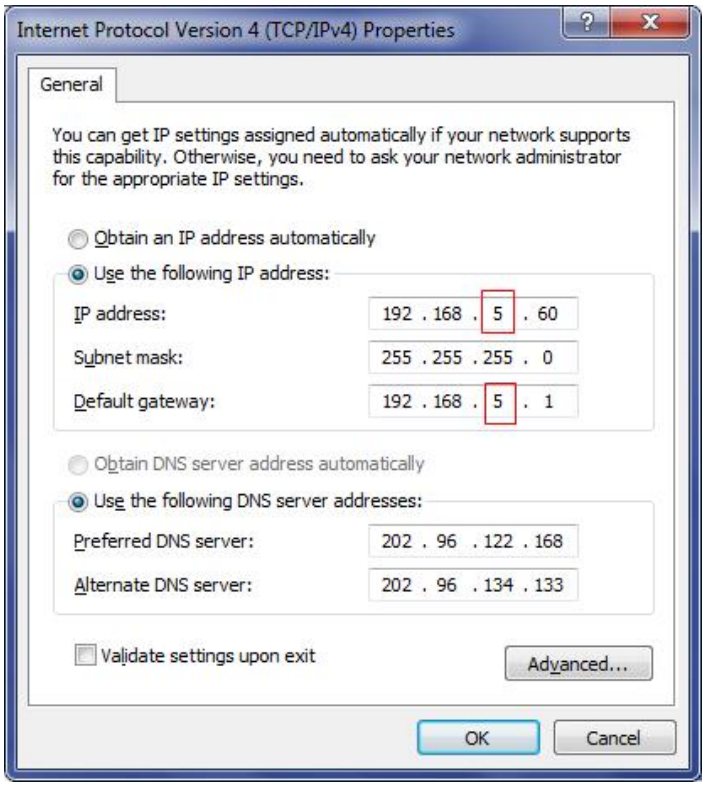
Eg: Assume that the IP address of the current PC is 192.168.5.60, change the network segment "5" of the IP address to "1".

Operation Steps

Amendment steps as follow:

Step 1 Open "Control Panel> Network Connection> Local Area Connection> Properties> Internet Protocol Version 4 (TCP / IPv4)> Properties".

Step 2 Change the selected "5" in red frame of the picture below to "1".



Step 3 Click “OK”, IP address is modified successfully.

Step 4 End.

1.3 Log in the Web Configuration Interface

Operation Steps

The initial password of the default user must be changed when logging in to the device for the first time. Login in the web configuration interface as follow:

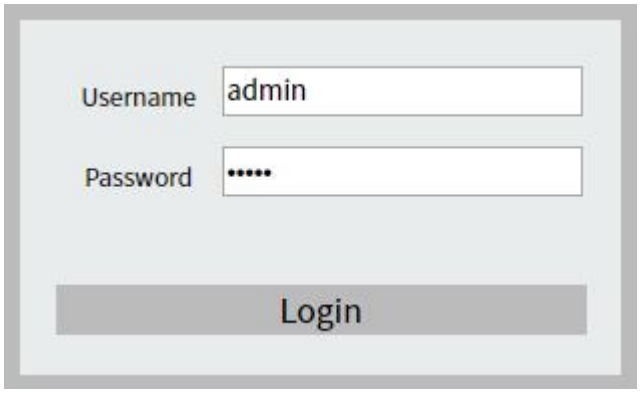
Step 1 Run the computer browser.

Step 2 Enter the address of the switch "http://192.168.1.254" in the address bar of the browser.

Step 3 Click the Enter key.

Step 4 Pop-up dialog box as shown below, enter the user name and password in the login

window.

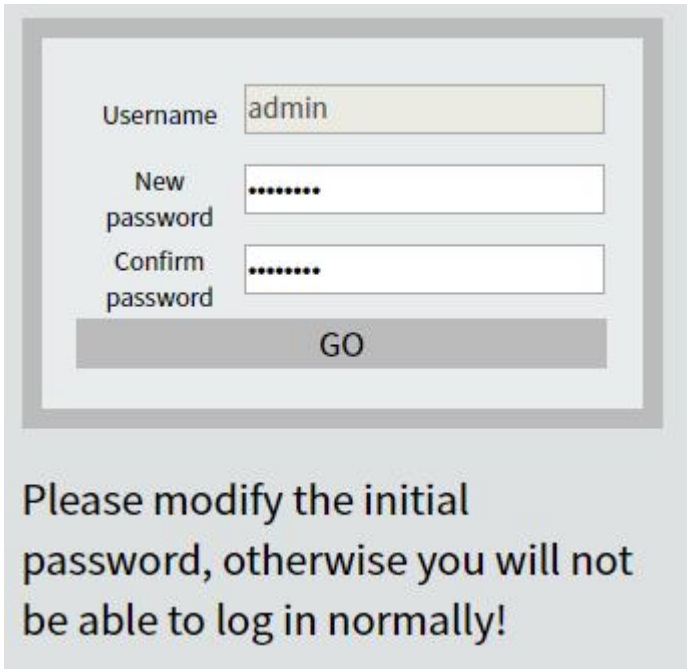


Note:

- This switch supports one default user. This user has administrator privilege and can configure devices via WEB, TELNET, SSH, CLI, etc.
- The default username and password are “admin”; please strictly distinguish capital and small letter while entering.
- If you log in to the device for the first time, you will be prompted to change the default user's initial password. If the password has been modified through the WEB or CLI, the subsequent steps can be ignored and the modified password can be used to log in to the device directly.
- If the number of incorrect login information input reaches 5 times, the system will automatically lock the user for 5 minutes.

Step 5 Click "Login".

Step 6 Pop up a window as the figure below, enter the new password on the login window.



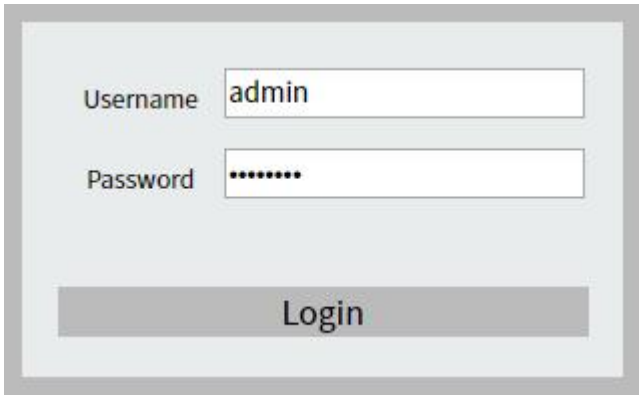
Note:

- The device could be logged in for the first time by default username and initial password; After logging in, the system will prompt you to modify the default user's initial password, and you can log in normally after modification.

- The length of the new password string must be greater than or equal to 8 and be composed of two or more of uppercase letters, lowercase letters, numbers and special characters.
- After changing the password, save the current configuration on the "System Configuration > Save startup-config" page to take effect.

Step 7 Click "OK".

Step 8 Pop up a window as the figure below, enter the user name and new password on the login window.



Step 9 Click the “login” button.

Step 10 End.

After login in successfully, user can configure relative parameters and information according to demands.

Note:

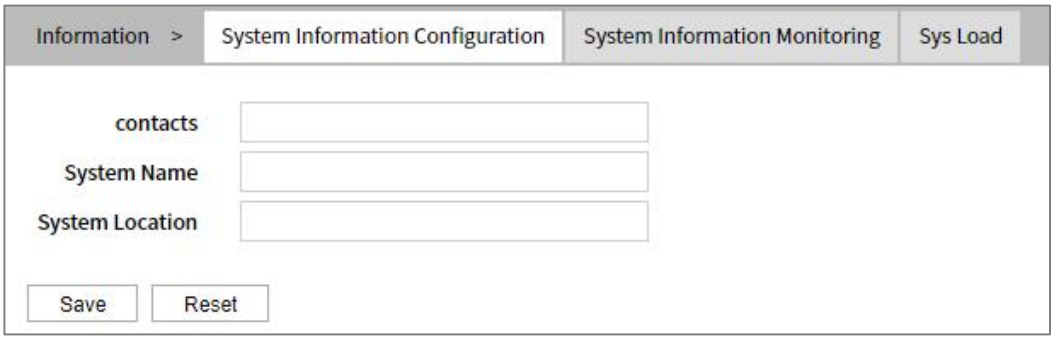
After logging in to the device, you can modify the IP address of the switch as needed.

2 System

2.1 System Information

2.1.1 System Information Configuration

The configuration of switch system information is provided here.



Contact

The textual identification of the contact person for this managed node, together with contact information. The allowed string length of the contact is 0-255, which is composed of letters, numbers, underlines and minus signs. The first character must be a letter, the last character cannot be a minus sign, and spaces are not supported.

System Name

An administratively assigned name for this managed node. The allowed string length of the system name is 0-255, which is composed of Chinese, letters, numbers and underlines. The first character cannot be a number and spaces are not supported.

System Location

The geographical location of this managed node(e.g., telephone closet, 3rd floor). The allowed string length of the system location is 0-255, which is composed of Chinese, letters, numbers and underlines. The first character cannot be a number and spaces are not supported.

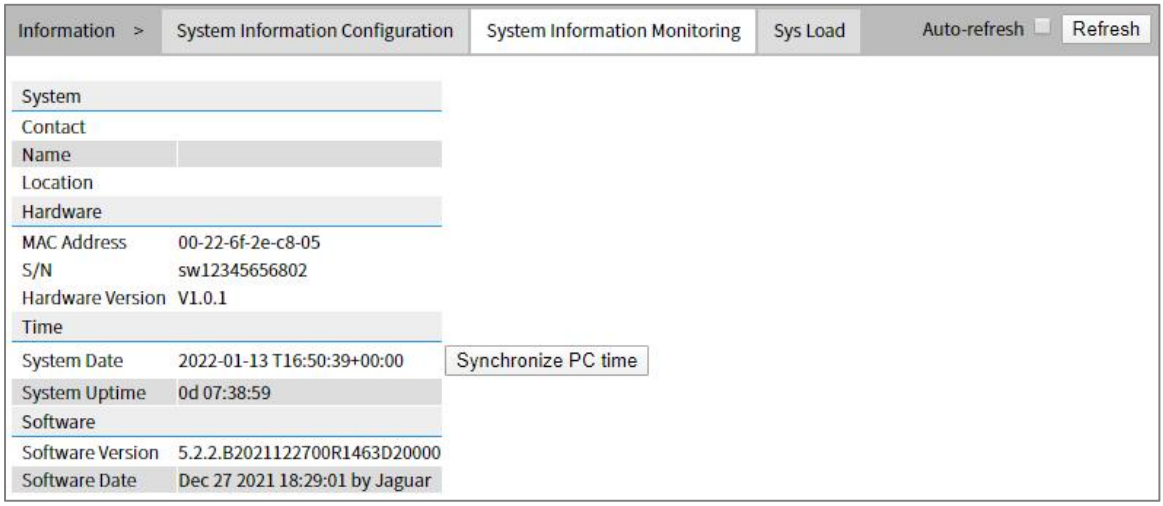
Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

2.1.2 System Information Monitor

The monitoring of switch system information is provided here.



System

- System contacts: System contacts configured by the path "System > System Information > System Information Configuration".
- System name: System name configured by the path "System > System Information > System Information Configuration".
- System location: System location configured by the path "System > System Information > System Information Configuration".

Hardware

- MAC address: The MAC Address of this switch.
- S/N: Device SN.
- Hardware version: hardware version information of the device.

Time

- System date: The system date can be synchronized with the computer through the "Synchronize PC Time" button.

- System run time: the run time of the device after powering on.

Software

- Software version: The software version of this switch.
- Software date: the software compilation date of the device.

Buttons

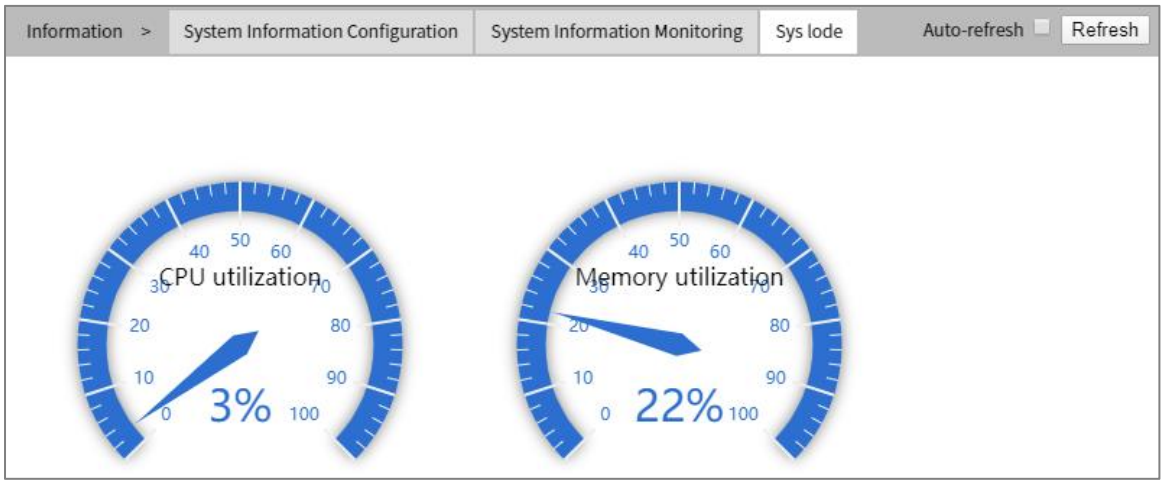
Synchronize PC time: click the system date to synchronize with the computer clock.

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page.

2.1.3 Load

This page displays the CPU utilization and memory utilization of the current device.



CPU Utilization/Memory Utilization

The CPU utilization and memory utilization of the device. CPU utilization and memory utilization are important indicators to measure device performance. If the CPU or memory utilization is too high, it may lead to business exceptions.

Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

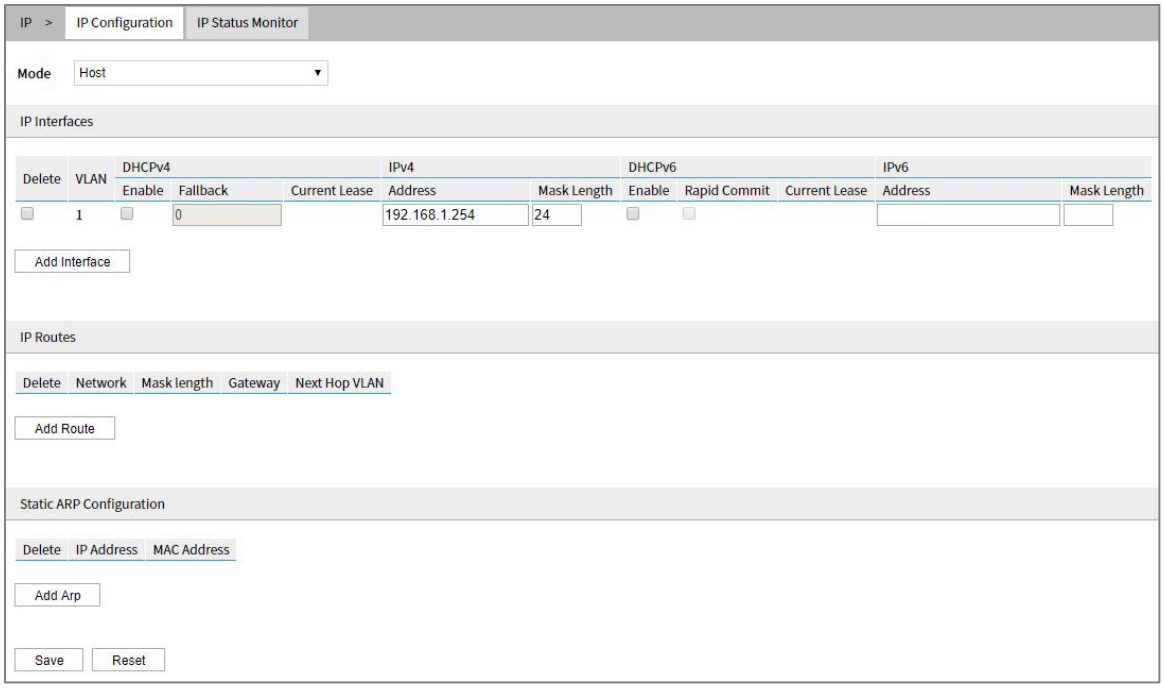
Refresh: Click to refresh the page.

2.2 IP

2.2.1 IP Configuration

Configure IP basic settings, control IP interfaces, IP routes and static ARP configuration.

The maximum number of IP interfaces supported is 8 and the maximum number of static routing entries is 32.



Mode

Configure whether the IP stack should act as a Host or a Router.

- Host: In Host mode, IP traffic between interfaces will not be routed.
- Router: In Router mode, traffic is routed between all interfaces.

IP Interface

Delete

Select this option to delete an existing IP interface.

VLAN

The VLAN associated with the IP interface. Only ports in this VLAN will be able to access the IP interface. This field is only available for input when creating a new interface.

DHCPv4 Enable

Enable the DHCPv4 client by checking this box. If this option is enabled, the system will configure the IPv4 address and mask of the interface using the DHCPv4 protocol. The DHCPv4 client will announce the configured System Name as hostname to provide DNS lookup.

DHCPv4 Fallback Timeout

The number of seconds for trying to obtain a DHCP lease. After this period expires, a configured IPv4 address will be used as IPv4 interface address. A value of zero disables the fallback mechanism, such that DHCP will keep retrying until a valid lease is obtained. Legal values are 0 to 4294967295 seconds.

DHCPv4 Current Lease

For DHCP interfaces with an active lease, this column show the current interface address, as provided by the DHCP server.

IPv4 Address

The IPv4 address of the interface in dotted decimal notation.

If DHCP is enabled, this field configures the fallback address. The field will be left blank if IPv4 operation on the interface is not desired - or no DHCP fallback address is desired.

IPv4 Mask Length

The IPv4 network mask, in number of bits (prefix length). Valid values are between 1 and 30 for a IPv4 address.

If DHCP is enabled, this field configures the fallback address network mask. The field will be left blank if IPv4 operation on the interface is not desired - or no DHCP fallback address is desired.

DHCPv6 Enable

Enable the DHCPv6 client by checking this box. If this option is enabled, the system will configure the IPv6 address of the interface using the DHCPv6 protocol.

DHCPv6 Rapid Commit

Enable the DHCPv6 Rapid-Commit option by checking this box. If this option is enabled, the DHCPv6 client terminates the waiting process as soon as a Reply message with a Rapid Commit option is received.

This option is only manageable when DHCPv6 client is enabled.

DHCPv6 Current Lease

For DHCPv6 interface with an active lease, this column shows the interface address provided by the DHCPv6 server.

IPv6 Address

The IPv6 address of the interface. A IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, fe80:: 215: c5ff: fe03:4dc7。The symbol is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once.

System accepts the valid IPv6 unicast address only, except IPv4-Compatible address and IPv4-Mapped address.

The field may be left blank if IPv6 operation on the interface is not desired.

IPv6-Mask

The IPv6 network mask, in number of bits (prefix length). Valid values are between 1 and 128 bits for a IPv6 address.

The field may be left blank if IPv6 operation on the interface is not desired.

IP Routes

Delete

Select this option to delete an existing IP route.

Internet

The destination IP network or host address of this route. Valid format is dotted decimal notation or a valid IPv6 notation. A default route can use the value 0.0.0.0or IPv6:: notation.

Mask Length

The destination IP network or host mask, in number of bits (prefix length). It defines how much of a network address that must match, in order to qualify for this route. Valid values are between 0 and 32 bits respectively 128 for IPv6 routes. Only a default route will have a mask length of 0 (as it will match anything).

Gateway

The IP address of the IP gateway. Valid format is dotted decimal notation or a valid IPv6 notation. Gateway and Network must be of the same type.

Next Hop VLAN (Only for IPv6)

The VLAN ID (VID) of the specific IPv6 interface associated with the gateway.

The given VID ranges from 1 to 4095 and will be effective only when the corresponding IPv6 interface is valid.

If the IPv6 gateway address is link-local, it must specify the next hop VLAN for the gateway.

If the IPv6 gateway address is not link-local, system ignores the next hop VLAN for the gateway.

Static ARP Configuration

Delete

Select this option to delete an existing entry. It will be deleted during the next Save operation.

IP Address/MAC Address

Allowed Source IPv4 address and Source MAC address in ARP request packets.

Buttons

Add new IP interface: click to add new IP interface. A maximum of 8 interfaces is supported.

Add new IP route: click to add new IP route. A maximum of 32 routes is supported.

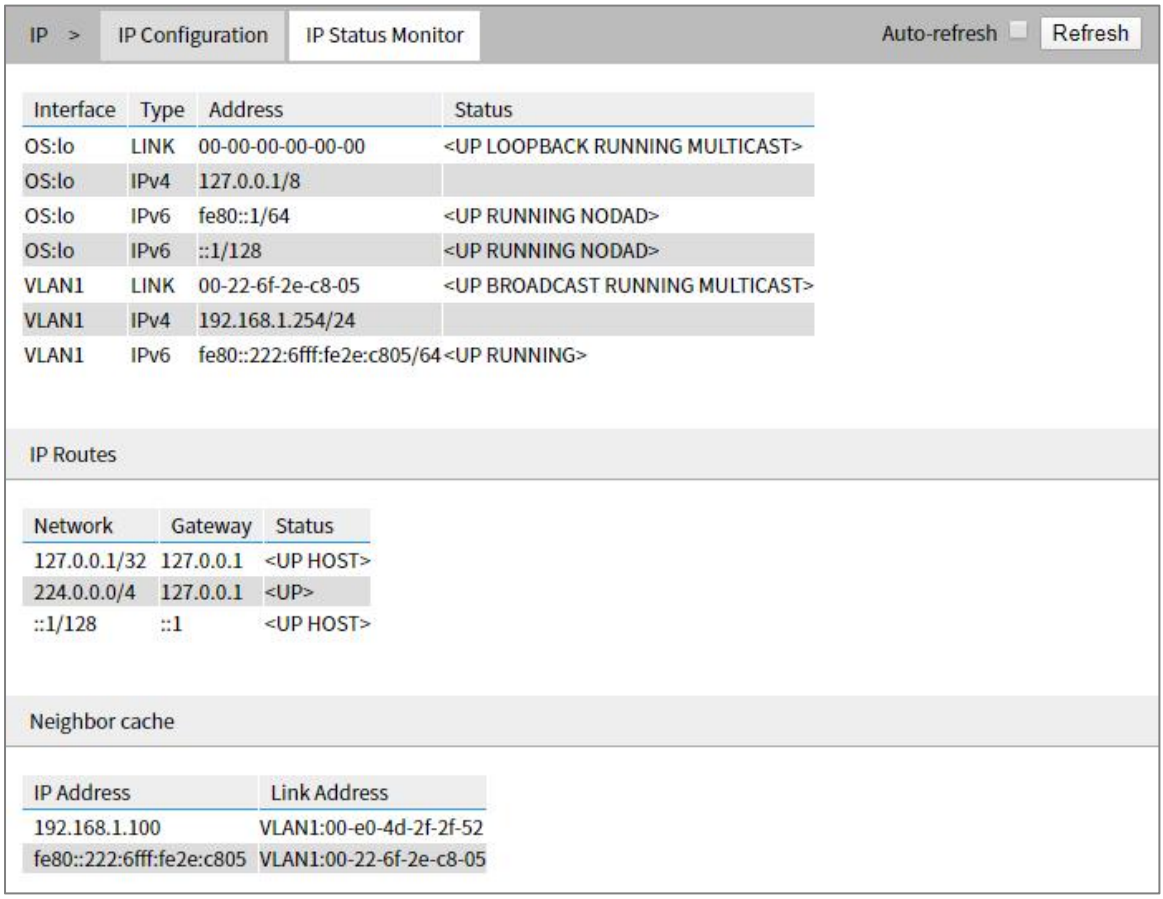
Add Arp: click to add a new entry to the static ARP checklist.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

2.2.2 IP Status Monitoring

This page displays the status of the IP protocol layer. The status is defined by the IP interfaces, the IP routes and the neighbour cache (ARP cache) status.



Interface

Interface name, such as VLAN interface, local loopback lo.

Type

The address type of the entry. This may be LINK, IPv4 or IPv6.

Address

The current address of the interface (of the given type).

Status

The status flags of the interface (and/or address).

IP Routes

Network

The destination IP network or host address of this route.

Gateway

The gateway address of this route.

Status

The status flags of the route.

Neighbour cache

IP Address

The IP address of the entry.

Link Address

The Link (MAC) address for which a binding to the IP address given exist.

Buttons

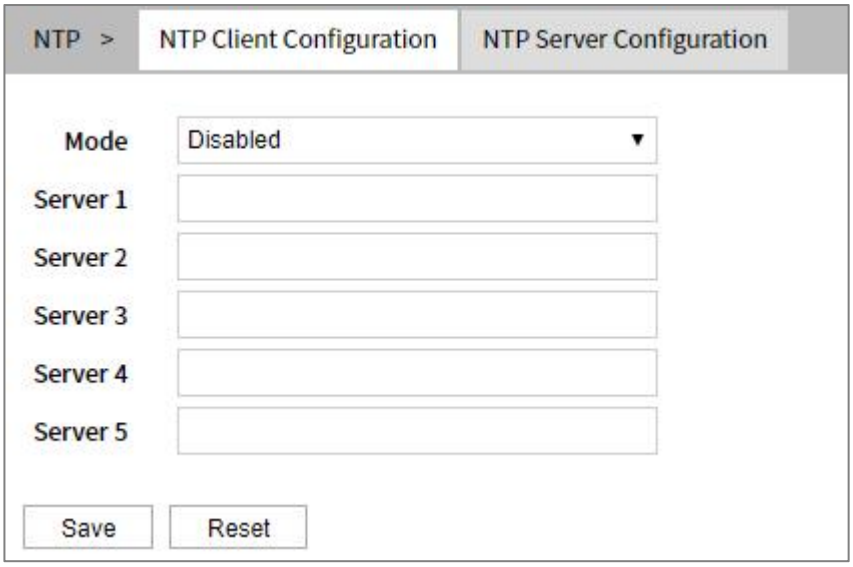
Refresh: Click to refresh the page immediately.

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

2.3 NTP

2.3.1 NTP Client Configuration

Configure NTP client on this page.



Mode

Indicates the NTP mode operation. Possible modes are:

- Enabled: Enable NTP client mode operation.
- Disabled: Disable NTP client mode operation.

Server

Provide the IPv4 address of a NTP server. For example, “192.1.2.34”.

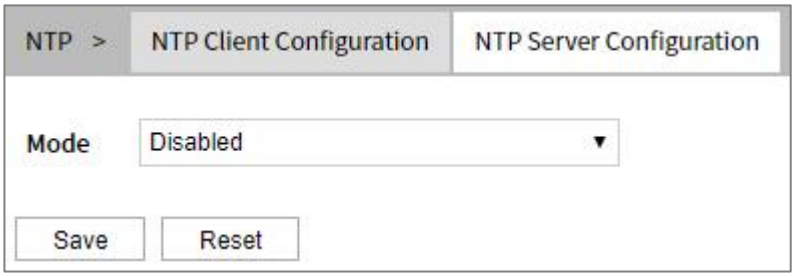
Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

2.3.2 NTP Server Configuration

Configure NTP server on this page.



Mode

Configure the NTP server mode, options are as follows:

- Enable: Enable NTP Server.
- Disable: Disable NTP Server.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

2.4 Time Zone

Time Zone

Lists the various Time Zones worldwide. Select appropriate Time Zone from the drop down and click Save to set.

Acronym

User can set the acronym of the time zone. This is a User configurable acronym to identify the time zone. (Range: Up to 16 characters).

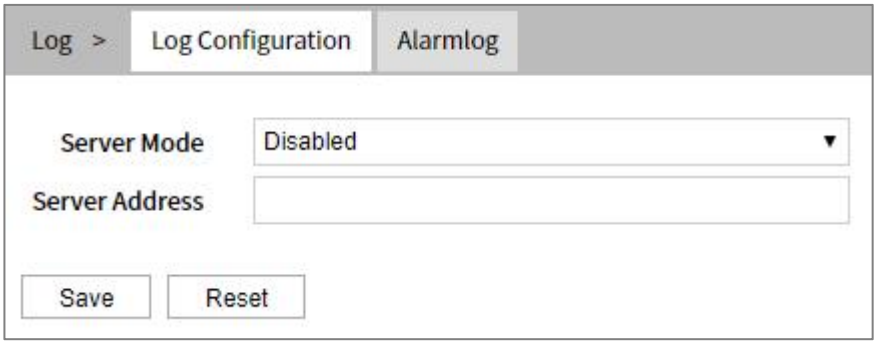
Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

2.5 Log

2.5.1 Log Configuration



Server Mode

Switch Syslog service. When the mode operation is enabled, the Syslog message will send out to the Syslog server. The Syslog protocol is based on UDP communication and received on UDP port 514 and the Syslog server will not send acknowledgments back since UDP is a connectionless protocol and it does not provide acknowledgments. The Syslog packet will always send out even if the Syslog server does not exist. Possible modes are:

- Enabled: Enable server mode operation.
- Disabled: Disable server mode operation.

Server Address

Indicates the IPv4 host address of Syslog server. If the switch provide DNS feature, it also can be a domain name.

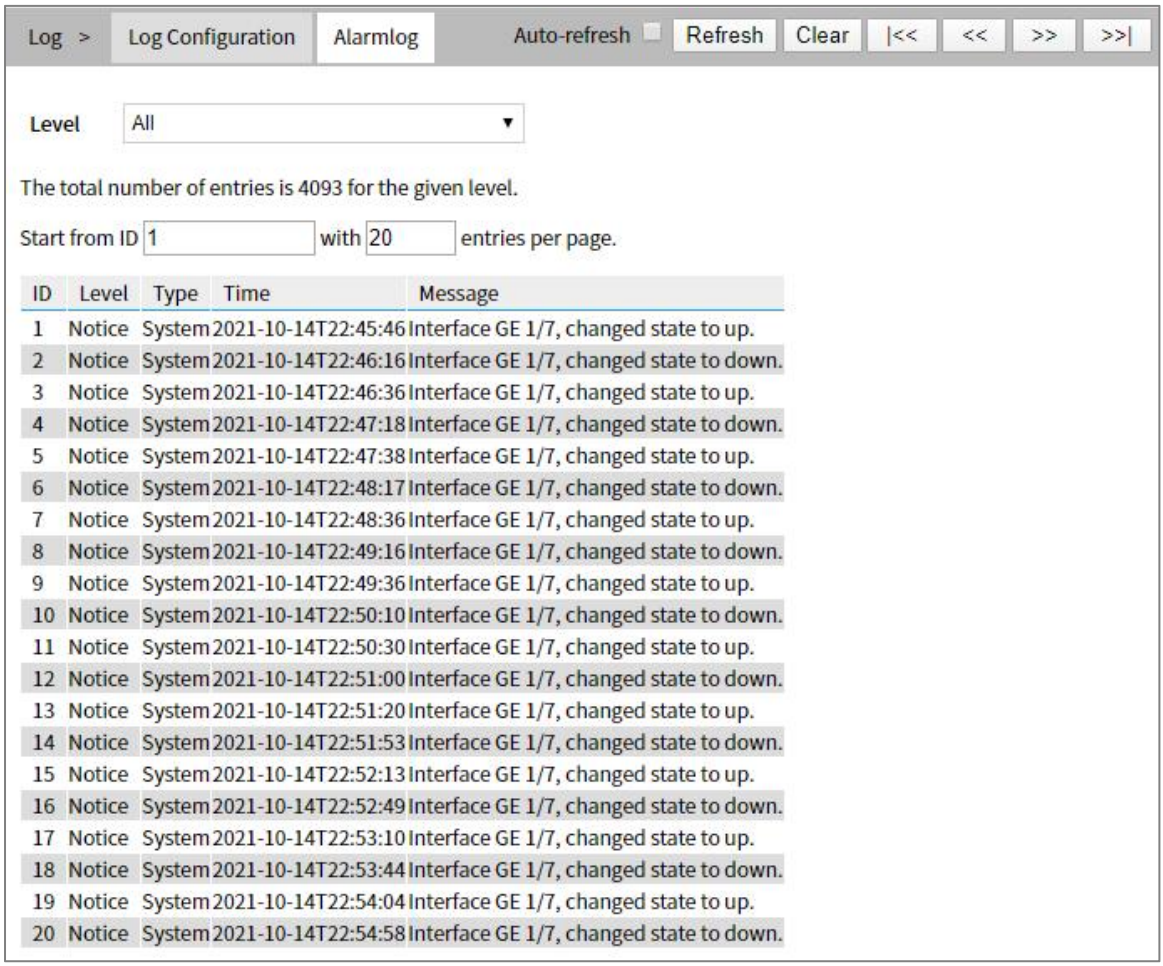
Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

2.5.2 Alert Log

Administrators can view all log information, and ordinary users can only view their own log information. The alarm log interface of switch system is as follows.



Level

The level of the alarm log entry.

- Error: the alarm log entry belongs to the error level.
- Warning: the alarm log entry belongs to the warning level.
- Important: the alarm log entry belongs to the important level.
- Notification: the alarm log entry belongs to the notification level.
- All: All alarm logs.

ID

ID of the log entry (> = 1).

Level

Severity level of the log entry.

Type

Log category, such as system, application and other information.

Time

Log occurrence time.

Message

Details of the log entry. Log information mainly records user operation, system failure, system safety and other information, including user log, security log and diagnostic log.

- User log: records user operations and system operation information.
- Security log: records information including account management, protocol, anti-attack and status.
- Diagnostic log: records information that assists in problem identification.

Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Update the log entry to the current entry ID.

Clear: Clear log statistics information.

| < <: update the log entry to the first available entry ID.

<<: update the log entry to the last available entry ID.

> >: update the log entry to the next available entry ID.

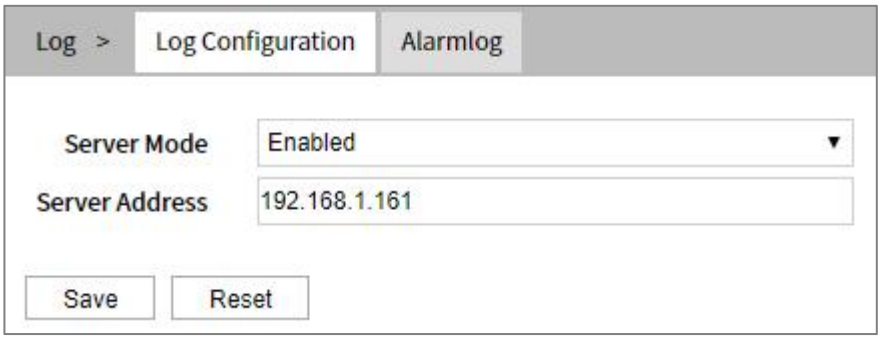
> > |: update the log entry to the last available entry ID.

Configuration Instance

"Visual Sys log Server" is a free open source software for receiving and viewing syslog messages. At present, the host with "Visual Syslog Server" installed is used as the system log server, and the IP address of the host is 192.168.1.161. The device transmits log information to the host server through UDP protocol. The configuration steps are as follows:

Step 1 Log in to the device WEB interface.

Step 2 On the "System > Log > Log Configuration" page, configure relevant parameters, as shown in the following figure:



1 Click the “Server Mode” drop-down list and select “Enable”.

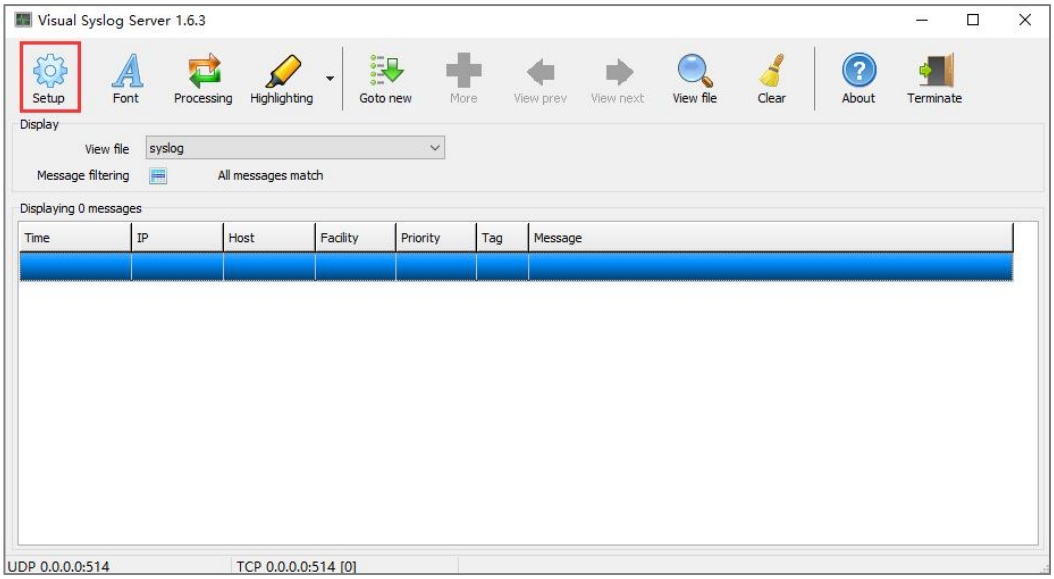
2 In the “Server Address” text box, enter the IP address "192.168.1.161" of the server.

3 Click "Save" button.

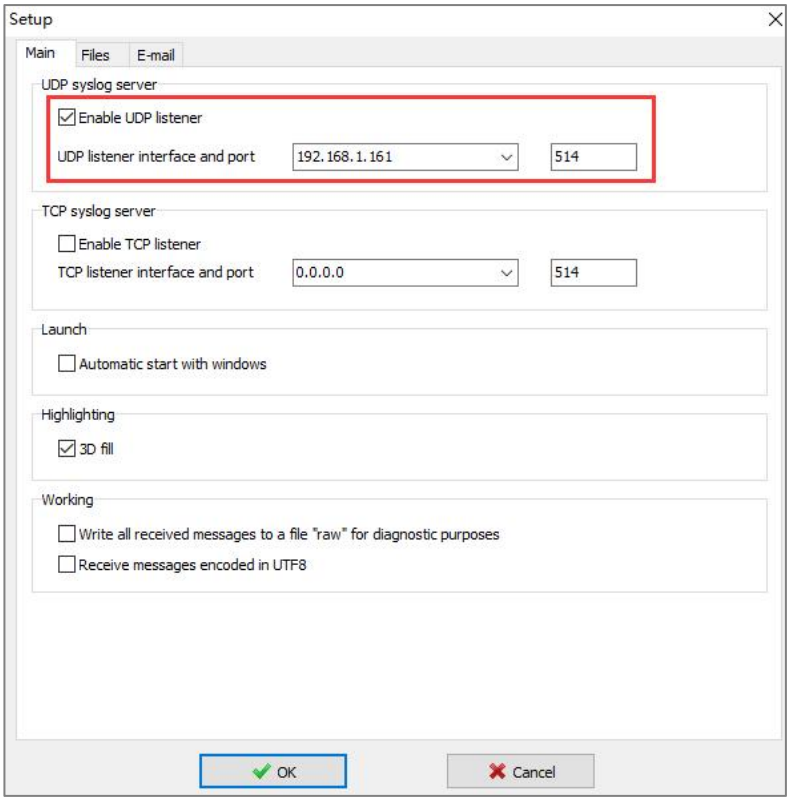
Step 3 Enter "System Configuration > Save startup-config".

Step 4 Click "Apply".

Step 5 Run "Visual Sys log Server" on the host to complete the configuration of relevant parameters, as shown below.



1 Click the "Setup" button, as shown in the above figure;



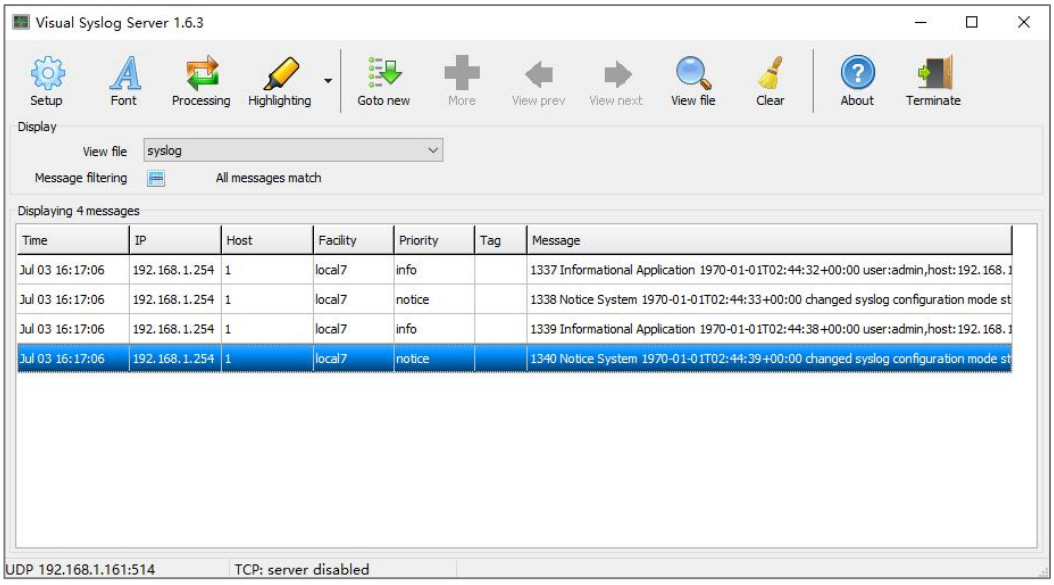
2 On the "Setup" page, in the Main configuration area, check "Enable UDP

Listener", as shown in the above figure;

3 Select the IP address "192.168.1.161" and port number "514" of the server from the "UDP listener interface and port" drop-down list;

4 Click “OK” button.

Step 6 Check the log information in the "Visual Sys log Server" configuration interface, as shown in the following figure.



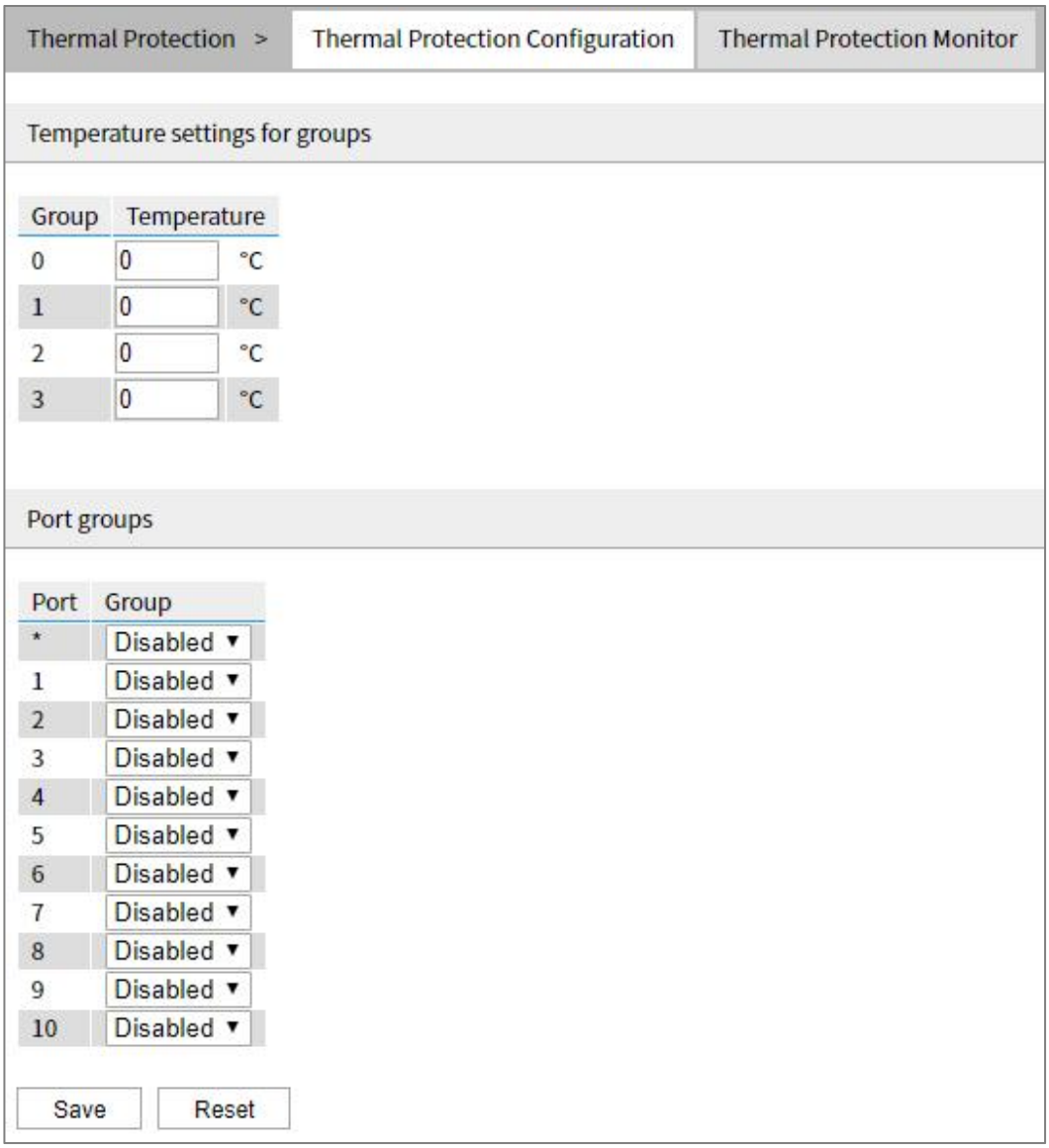
Step 7 End.

2.6 Temperature Protection

2.6.1 Thermal Protection Configuration

This option allows the user to inspect and configure the current setting for controlling thermal protection. Thermal protection is used to protect the chip from getting overheated.

When the temperature exceeds the configured thermal protection temperature, ports will be turned off in order to decrease the power consumption. It is possible to arrange the ports with different groups. Each group can be given a temperature at which the corresponding ports shall be turned off.



Group Temperature Settings

Group

Group ID of the group displayed.

Temperature

Limit the total temperature of port members of the group. Temperatures between 0 and 255 C are supported.

Port groups

Port

The corresponding Ethernet port number of the device.

Port groups

The temperature group to which the port belongs can be selected as follows:

- Disable.
- 0
- 1
- 2
- 3

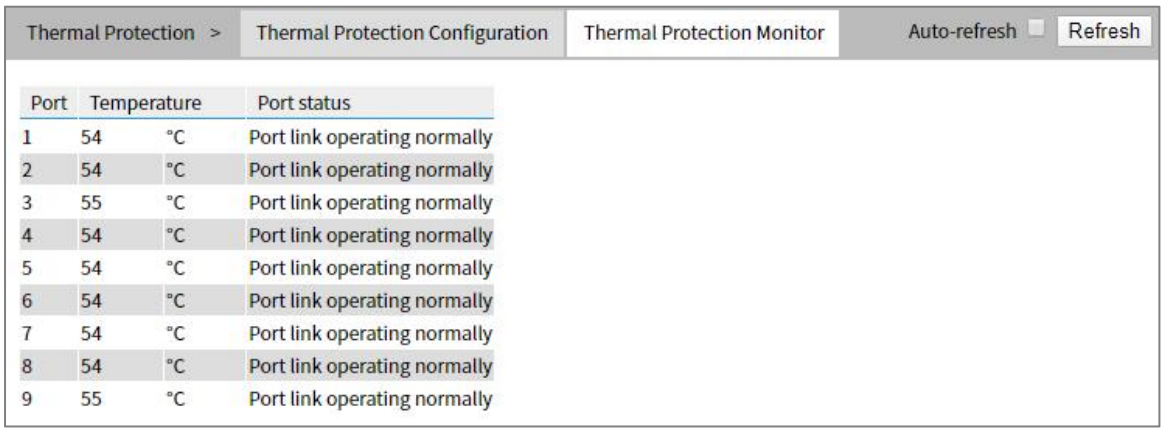
Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

2.6.2 Thermal Protection Monitoring

This page allows the user to inspect status information related to thermal protection.



Port	Temperature		Port status
1	54	°C	Port link operating normally
2	54	°C	Port link operating normally
3	55	°C	Port link operating normally
4	54	°C	Port link operating normally
5	54	°C	Port link operating normally
6	54	°C	Port link operating normally
7	54	°C	Port link operating normally
8	54	°C	Port link operating normally
9	55	°C	Port link operating normally

Port

The switch port number.

Temperature

Shows the current chip temperature in degrees Celsius.

Port Status

Shows if the port is thermally protected (link is down) or if the port is operating normally.

Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

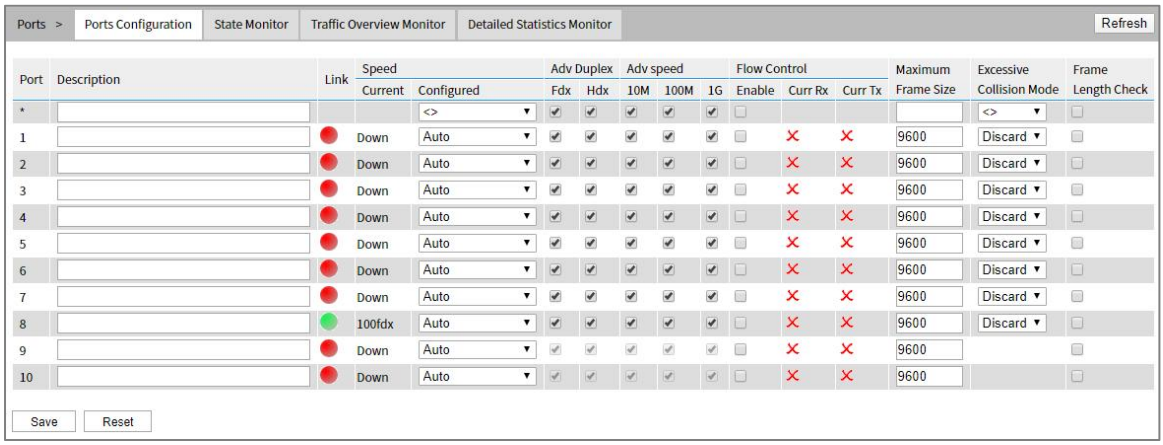
Refresh: Update the log entry to the current entry ID.

3 Port

3.1 Port

3.1.1 Port Configuration

This feature displays current port configurations. Ports can also be configured using this feature.



Port

This is the logical port number for this row.

Description

The description of the port. It is a valid string no longer than 256 characters. The port description can be used to identify the field port wiring, which is convenient for field maintenance.

Link State

The port link state is displayed graphically. Green indicates that the port is connected, and red indicates that the port is not connected.

Link Speed

Rate duplex is divided into current state and forced configuration state.

- The current sate is the current link speed of the port.
- Forced configuration can select any available link speed for the given switch port. Only speeds supported by the specific port is shown. Configured Link Speed are as follows:
  - Disabled: disables the switch port.
  - Auto: the port automatically negotiates the transmission speed and duplex with the connected device, and keeps the highest compatible speed with the connected device.
  - 10Mbps HDX: Forces the cu port in 10 Mbps half duplex mode.
  - 10Mbps FDX: Forces the cu port in 10 Mbps full duplex mode.
  - 100Mbps HDX: Forces the cu port in 100 Mbps half duplex mode.
  - 100Mbps FDX: Forces the port in 100 Mbps full duplex mode.
  - 1Gbps FDX: Forces the port in 1 Gbps full duplex mode.
  - 2.5Gbps FDX: Forces the port in 2.5Gbps full duplex mode.

Advertise Duplex

When duplex is set as auto that is, Autonegotiation, the port will only advertise the specified duplex as either Fdx or Hdx to the link partner.

Advertise Speed

When Speed is set as auto that is, Autonegotiation, the port will only advertise the specified speeds (10M 100M 1G) to the link partner.

Flow Control

When Auto Speed is selected on a port, this section indicates the flow control capability that is advertised to the link partner. When a fixed-speed setting is selected, that is what is used. The “Current Rx” column indicates whether pause frames on the port are obeyed, and the “Current Tx” column indicates whether pause frames on the port are transmitted. The Rx and Tx settings are determined by the result of the last Auto-Negotiation.

Maximum Frame Size

Enter the maximum frame size allowed for the switch port, including FCS. The range is 1518-9600 bytes.

Excessive Collision Mode

Configure port transmit collision behavior.

- Discard: Discard frame after 16 collisions (default).
- Restart: Restart backoff algorithm after 16 collisions.

Frame Length Check

If the frame length in the EtherType/Length field is incorrect, the frame is discarded. The Ethernet frame contains an EtherType/Length field. When the value is 1535 or below, this field is used for indicating the size of the payload frame (in bytes). If the EtherType/Length field is above 1535, it indicates that the field is used as an EtherType (indicating which protocol is encapsulated in the payload of the frame). If "frame length check" is enabled, frames with payload size less than 1536 bytes are dropped, if the EtherType/Length field doesn't match the actually payload length. If "frame length check" is disabled, frames are not dropped due to frame length mismatch. Note: frames discarded due to mismatched frame length are not counted.

Buttons

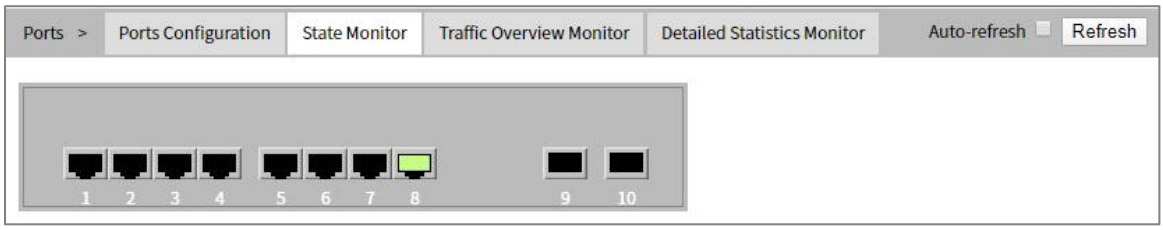
Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Refresh: Click to refresh the page; any changes made locally will be undone.

3.1.2 Status Monitoring

This page provides port state monitoring of the current switch.



The port states are illustrated as follows:

RJ45 port			
SFP ports			
Status	Forced disconnection	Not connected	Connected

Buttons

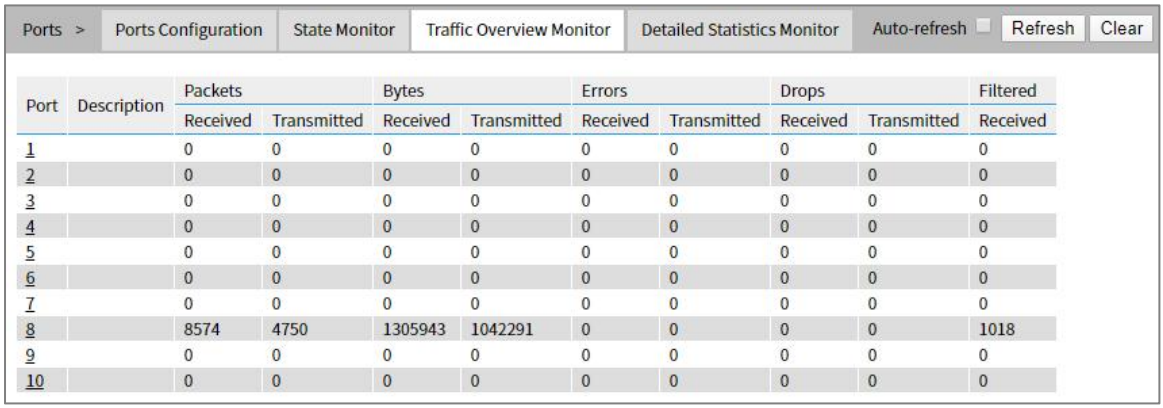
Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page.

3.1.3 Summary Statistical Monitoring

This page provides an overview of general traffic statistics for all switch ports.

The displayed counters are:



Port	Description	Packets		Bytes		Errors		Drops		Filtered
		Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1		0	0	0	0	0	0	0	0	0
2		0	0	0	0	0	0	0	0	0
3		0	0	0	0	0	0	0	0	0
4		0	0	0	0	0	0	0	0	0
5		0	0	0	0	0	0	0	0	0
6		0	0	0	0	0	0	0	0	0
7		0	0	0	0	0	0	0	0	0
8		8574	4750	1305943	1042291	0	0	0	0	1018
9		0	0	0	0	0	0	0	0	0
10		0	0	0	0	0	0	0	0	0

Port

The switch port number. Click the port number link to jump to the "Detailed statistical monitoring" page. See the next section for details.

Description

The description of the port.

Packets

The number of received and transmitted packets per port.

Bytes

The number of received and transmitted bytes per port.

Errors

The number of frames received in error and the number of incomplete transmissions per port.

Drops

The number of frames dropped due to congestion in receiving or transmission.

Filtered

The number of received frames filtered by the forwarding process.

Buttons

Refresh: Click to refresh the page immediately.

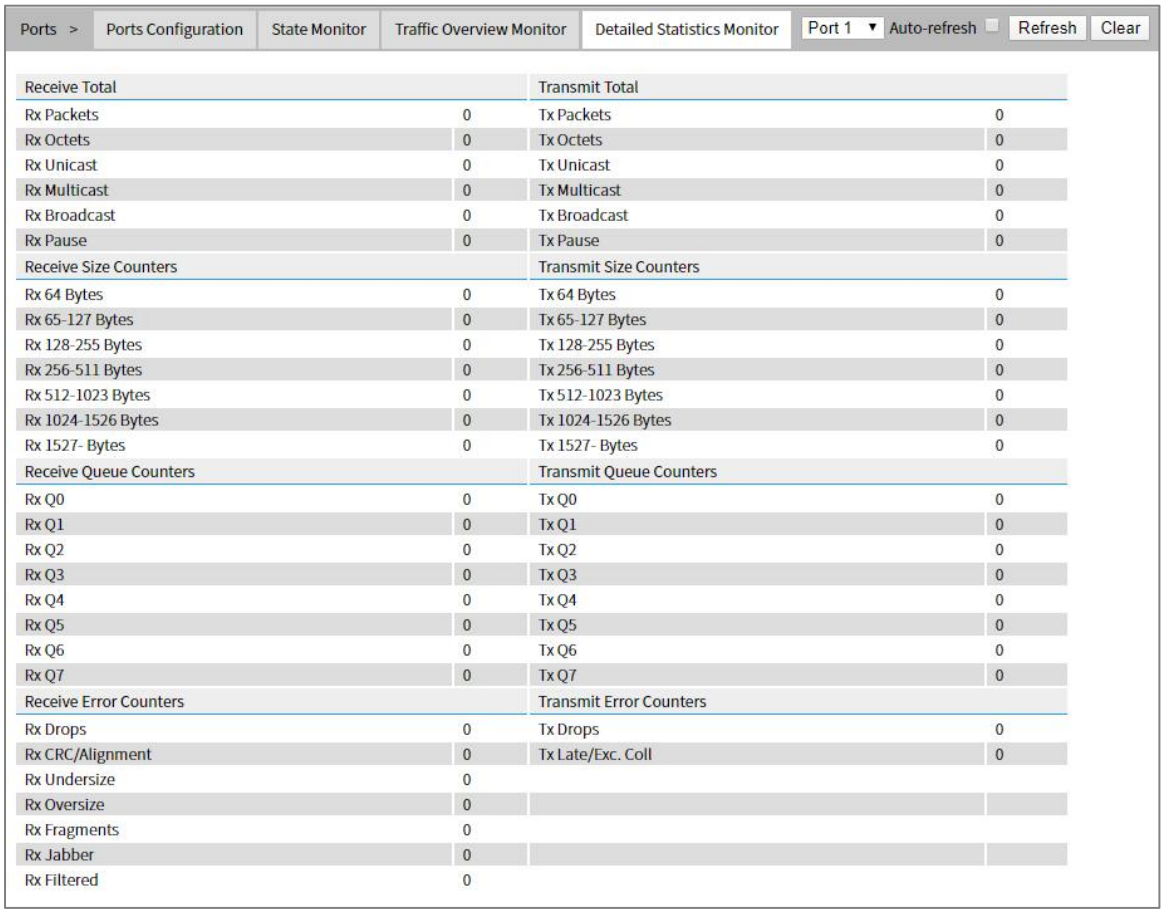
Clear: Clears the counters for all ports.

Auto-refresh: Check this box to enable an automatic refresh. Automatic refresh occurs every 3 seconds.

3.1.4 Detailed Statistical Monitoring

This page provides detailed traffic statistics for a specific switch port. Use the port drop-down list to select which switch port details to display.

Port details include the number of data such as packets sent and received, message length, message queue, error frames, etc.



Receiving statistics and sending statistics

Total receiving and sending data packets

The total number of packets received and sent, including normal and abnormal packets.

Receive Total and Transmit Total

The total number of bytes received and sent, including FCS parity bits.

Receiving and sending unicast packets

The number of unicast packets received and sent, including normal and abnormal unicast packets.

Receiving and Sending Multicast Packets

The number of multicast packets received and sent, including normal and abnormal multicast packets.

Receiving and sending broadcast packets

The number of broadcast packets received and sent, including normal and abnormal broadcast packets.

Receiving and sending Pause frames

A count of MAC control frames received or sent on this port, which have an opcode indicating pause operation.

Receiving and sending message length statistics

Number of packets of different lengths received and sent. They are categorized according to their respective frame sizes.

Receive and Transmit Queue Counters

The number of received and transmitted packets per input and output queue.

Receive Error Counters

Rx Drops

The number of frames dropped due to lack of receive buffers or egress congestion.

Rx CRC/Alignment

The number of frames received with CRC or alignment errors.

Rx Undersize

The number of short 1 frames received with valid CRC.

Rx Oversize

The number of long 2 frames received with valid CRC.

Rx Fragments

The number of short 1 frames received with invalid CRC.

Rx Jabber

The number of long 2 frames received with invalid CRC.

Rx Filtered

The number of received frames filtered by the forwarding process.

Note:

- 1 Short frames are frames that are smaller than 64 bytes.
- Long frame is a frame that exceeds the MTU frame length set by the port.

Transmit Error Counters

Tx Drops

The number of frames dropped due to output buffer congestion.

Tx Late/Exc.Coll

The number of frames dropped due to excessive or late collisions.

Buttons

Port 1 ▼: the port select box determines which port is affected by clicking the buttons.

Refresh: Click to refresh the page immediately.

Clear: Clears the counters for all ports.

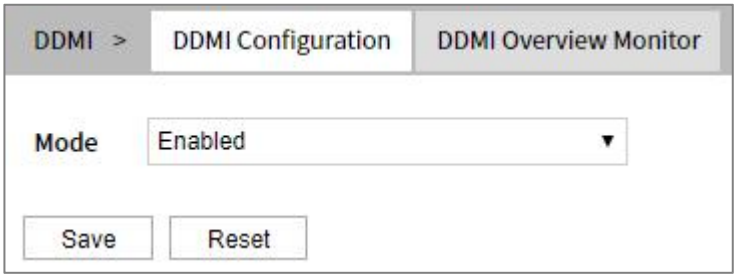
Auto-refresh: Check this box to enable an automatic refresh. Automatic refresh occurs every 3 seconds.

3.2 DDMI

The DDMI (Digital Diagnostic Monitoring Interface) function can monitor the temperature, voltage, optical power and other parameters of the SFP optical module that supports DDM on the SFP interface of the device. This function has greatly facilitated the troubleshooting process of optical fiber link and the cost of on-site debugging.

3.2.1 DDMI Configuration

This page allows you to configure DDMI.



Mode

Display DDMI mode operation. Possible modes are:

- Enable: enable DDMI mode operation.
- Disable: disable DDMI mode operation.

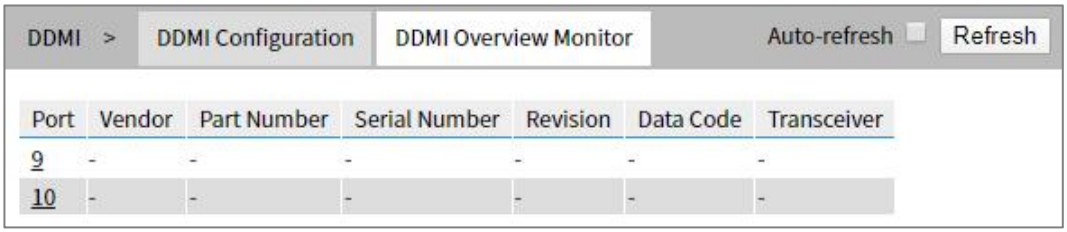
Buttons

Save: Click to save changes.

Reset: Click here to undo any changes made locally and revert to the previously saved values.

3.2.2 DDMI Overview Monitoring

This page displays an overview of DDMI information.



Port

DDMI port. Click the DDMI port number link to enter the "Transceiver Information" page.

Vendor

Display the supplier name.

Component Number

Display the supplier PN component number provided by the SFP supplier.

Sequence Number

Display the serial number of the SFP module provided by the vendor.

Adjustment

Indicate the revision level of the supplier according to the part number provided by the supplier.

Data Code

Display the manufacturing date code of the supplier.

Transceiver

Indicate transceiver compatibility.

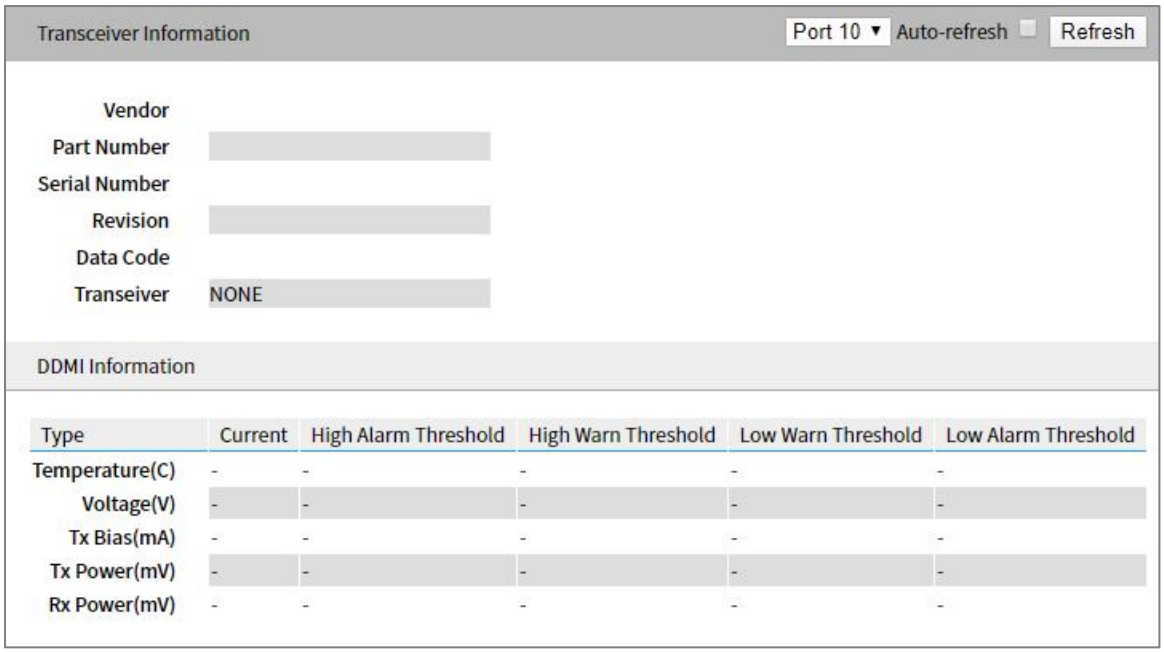
Buttons

Refresh: Click to refresh the page immediately.

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Transceiver Information

Click the port number link that supports DDM to enter the transceiver information page.



Vendor

Indicates Vendor name SFP vendor name.

Part Number

Indicates Vendor PN Part number provided by SFP vendor.

Serial Number

Indicates Vendor SN Serial number provided by vendor.

Revision

Indicates Vendor rev Revision level for part number provided by vendor.

Data Code

Indicates Date code Vendor's manufacturing date code.

Transceiver

Indicates Transceiver compatibility.

DDMI Information

Current

The current value of temperature, voltage, TX bias, TX power, and RX power.

High Alarm Threshold

The high alarm threshold value of temperature, voltage, TX bias, TX power, and RX power.

High Warn Threshold

The high warn threshold value of temperature, voltage, TX bias, TX power, and RX power.

Low Warn Threshold

The low warn threshold value of temperature, voltage, TX bias, TX power, and RX power.

Low Alarm Threshold

The low alarm threshold value of temperature, voltage, TX bias, TX power, and RX power.

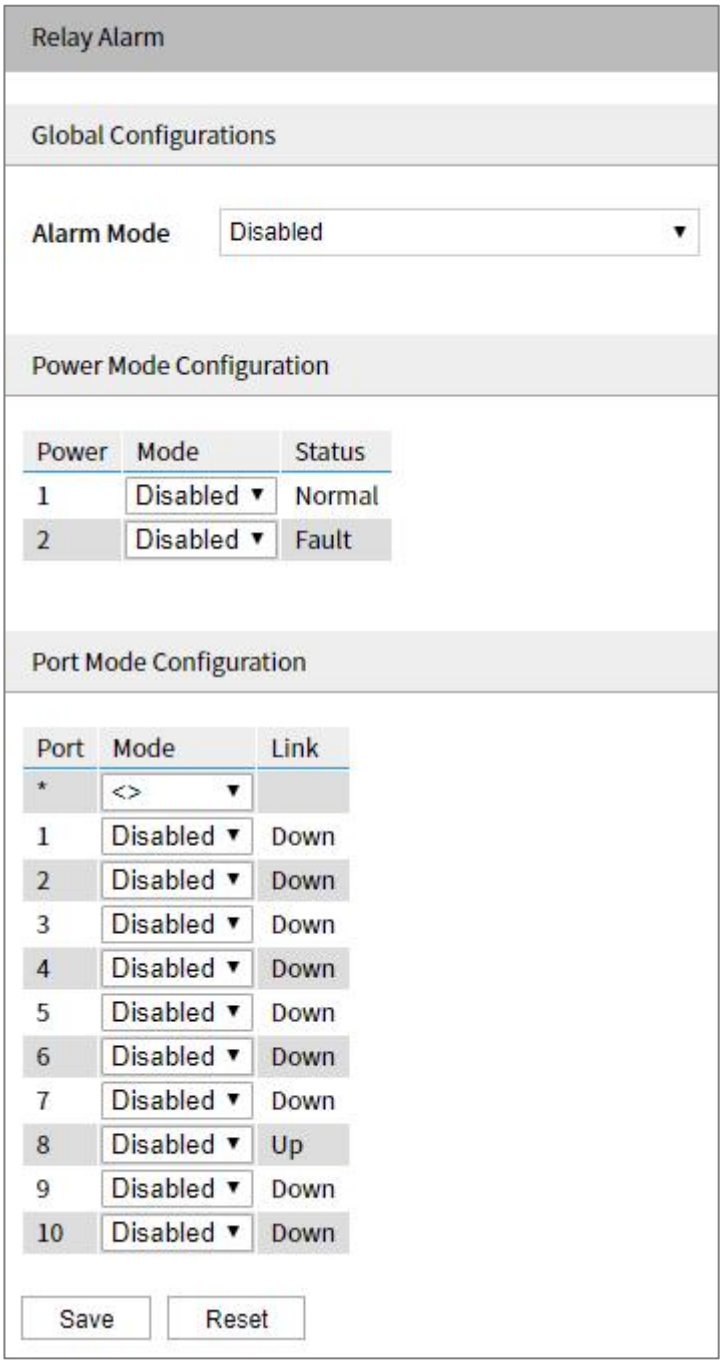
Buttons

Refresh: click to refresh the page immediately.

Auto-refresh: Check this box to enable an automatic refresh. Automatic refresh occurs every 3 seconds.

3.3 Relay Alarm

On the page of “Relay Alarm”, user can enable port alarm, and configure relevant alarm information.



Global Configuration

Alarm Mode

Whether to enable power supply and port fault alarm through relay or ALM indicator, the options are as follows:

- Enable
- Disable

Power Mode Configuration

Only dual-power devices support power alarm.

Power

Display the power supply interface number of the device, value is 1 or 2.

Mode

Enable the power supply alarm or not, options as follows:

- Enable: when the power supply fails, power supply alarm will be triggered.
- Disable

Status

Connection status of power supply, the device will automatically recognize and display, values include:

- Fault
- Normal.

Port Mode Configuration

Port

Displays the port number of the device.

Mode

Enable the port alarm or not, options as follows:

- Enable: when the port is disconnected, port alarm will be triggered.
- Disable

Connection State

Connection status of the port, the device will automatically recognize and display, values include:

- Connection
- Not connected

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4 Safety Device

4.1 Users

This option provides an overview of the current users. Currently, the only way to log in as another user on the web server is to close and reopen the browser.

Username

The name identifying the user. This is also a link to edit a user.

Privilege Level

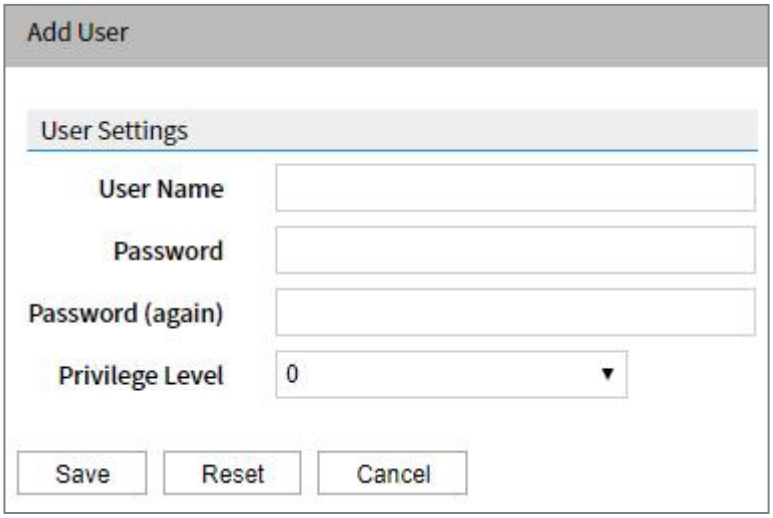
The privilege level of the user. The allowed range is 0 to 15. If the privilege level value is 15, it can access all groups, that is, that is granted the fully control of the device. But the privilege of other value need to refer to each group privilege level. User's privilege should be same or greater than the group privilege level to have the access of that group. By default setting, most groups privilege level 5 has the read-only access and privilege level 10 has the read-write access. And the system maintenance (software upload, factory defaults, and so on) need user privilege level 15. Generally, the privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account and privilege level 5 for a guest account.

Buttons

Add a new user: Click this button to add a new user.

New user

Click “Add new user” to enter the “New user” page.



Username

A string identifying the user name that this entry should belong to. The allowed string length is 1 to 31. The valid user name allows letters, numbers and underscores.

Password

The password of the user. The allowed string length must be greater than or equal to 8. Passwords contain at least two of uppercase letters, lowercase letters, numbers or special characters.

Note:

User name and password cannot be the same.

Confirm password

Enter the password again.

Privilege Level

The privilege level of the user. The allowed range is 0 to 15. If the privilege level value is 15, it can access all groups, i.e. that is granted the fully control of the device. But the privilege of other value need to refer to each group privilege level. User's privilege should be same or greater than the group privilege level to have the access of that group. By default setting, most groups privilege level 5 has the read-only access and privilege level 10 has the read-write access. And the system maintenance (software upload, factory defaults and etc.) need user privilege level 15. Generally, the privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account and privilege level 5 for a guest account.

Buttons

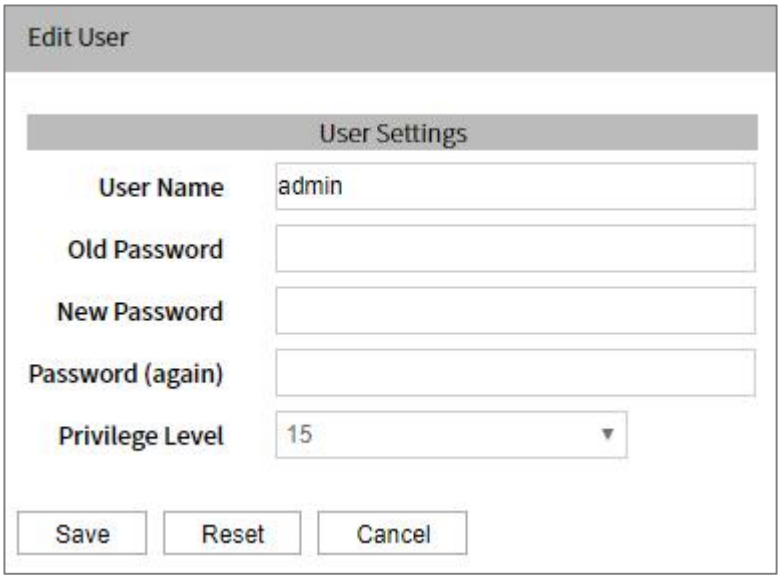
Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Back: Click to undo any changes made locally and return to the Users.

Edit User

Click the user name link to enter the "Edit User" page.



Username

Display the name of the current editing user.

Old password

Enter the password of the current editing user.

New password

Set a new password for the current editing user. The allowed string length of password must be greater than or equal to 8. Passwords contain at least two of uppercase letters, lowercase letters, numbers or special characters.

Note:

User name and password cannot be the same.

Confirm password

Enter the new password again.

Privilege Level

The privilege level of the user. The allowed range is 0 to 15. If the privilege level value is 15, it can access all groups, i.e. that is granted the fully control of the device. But the privilege of other value need to refer to each group privilege level. User's privilege

should be same or greater than the group privilege level to have the access of that group. By default setting, most groups privilege level 5 has the read-only access and privilege level 10 has the read-write access. And the system maintenance (software upload, factory defaults and etc.) need user privilege level 15. Generally, the privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account and privilege level 5 for a guest account.

Buttons

Save: Click to save changes.

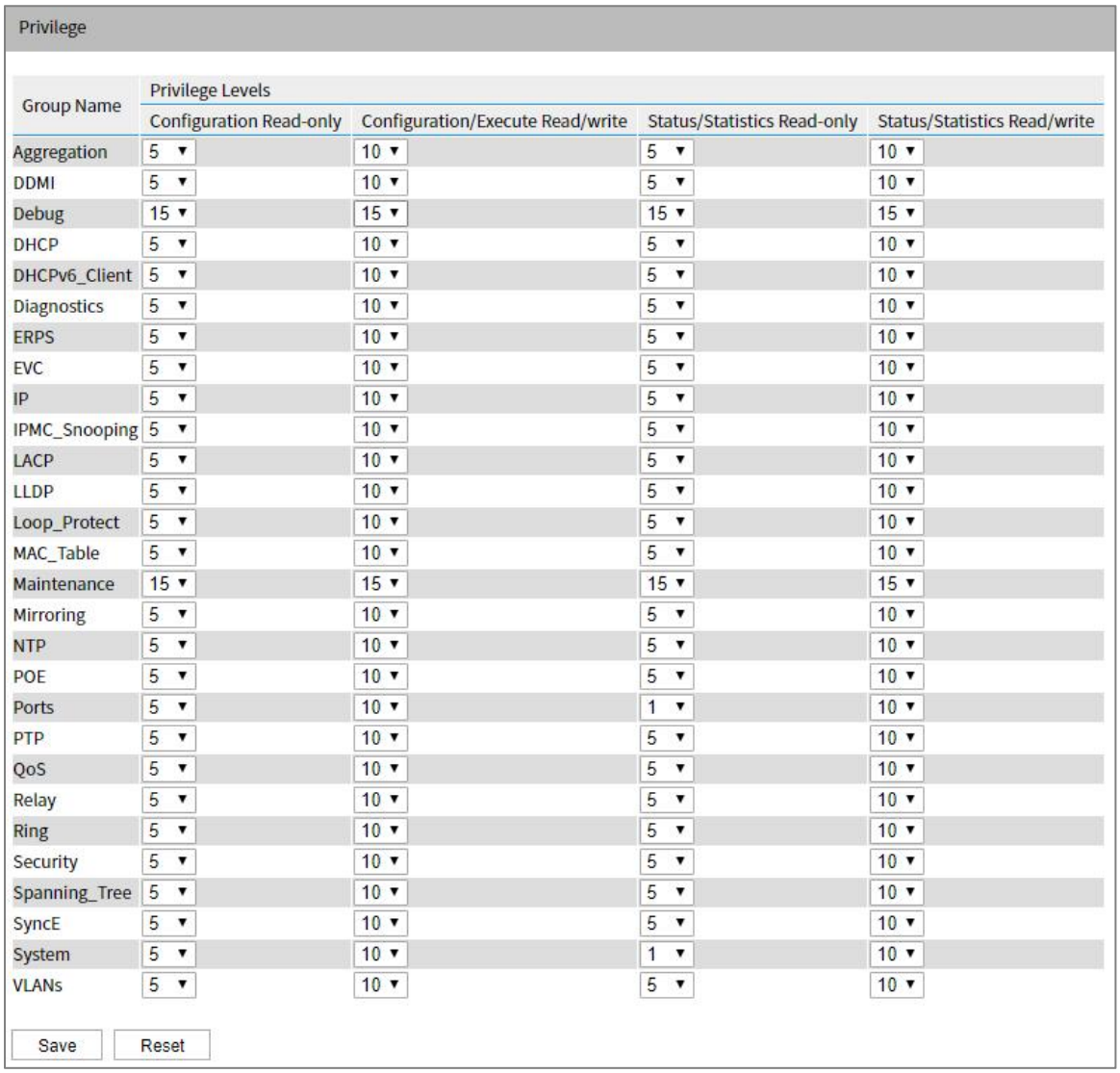
Reset: Click to undo any changes made locally and revert to previously saved values.

Back: Click to undo any changes made locally and return to the Users.

Delete user: Delete the current user. (The default user admin cannot be deleted)

4.2 Privilege Level

This option provides an overview of the privilege levels configuration.



Group Name

The name identifying the privilege group. In most cases, a privilege level group consists of a single module (for example, LACP, VLANs or QoS), but a few of them contains more than one. The following description defines these privilege level groups in details:

- System: time zone, menu bar status.
- Security:DDMI, authentication method, SSH, HTTPS, access management, port limit control, port security, NAS, ACL, RADIUS, TACAS+.
- Diagnostics: Ping and cable detection.
- Maintenance: includes the following contents: device restart, restore factory settings, software upgrade and firmware selection in System Maintenance; Download, upload, activate and delete in System Configuration; System information and logs in System; Users and privilege levels in Safety Devices.
- Debug: Only present in CLI.

Privilege Level

Every group has an authorization Privilege level for the following sub groups: configuration read-only, configuration/execute read-write, status/statistics read-only, status/statistics read-write (for example, for clearing of statistics). User Privilege should be same or greater than the authorization Privilege level to have the access to that group.

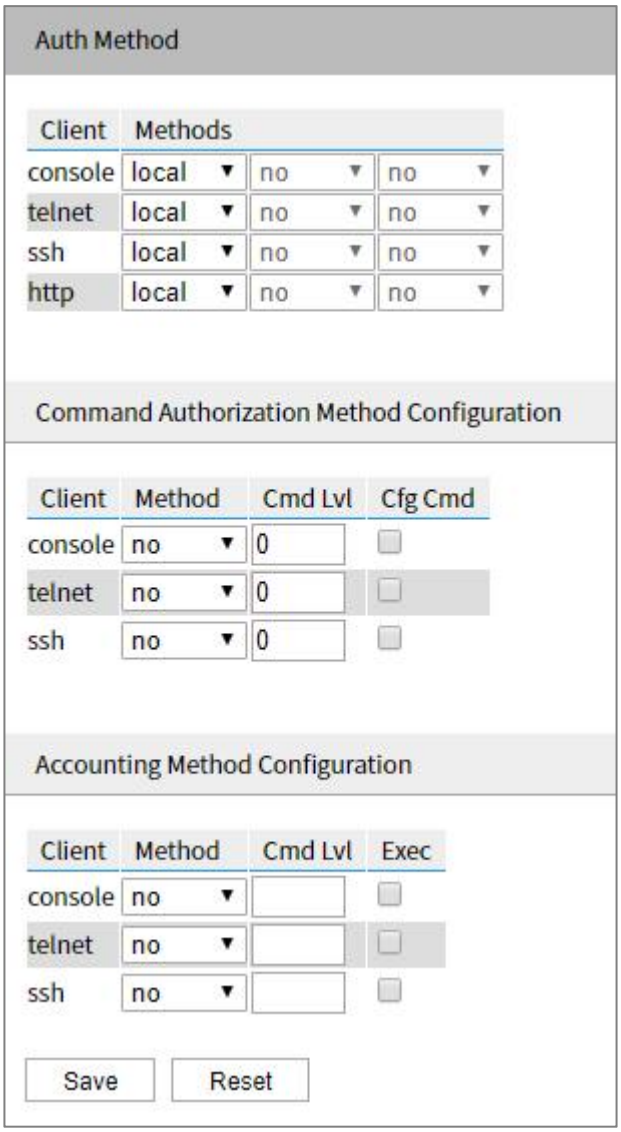
Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.3 Authentication method

This option allows you to configure how a user is authenticated when he logs into the switch via one of the management client interfaces.



The table has one row for each client type and a number of columns which are as follows:

Client

The management client for which the configuration below applies.

- console
- telnet
- ssh
- http

Methods

Method can be set to one of the following values:

- no: Authentication is disabled and login is not possible.
- local: Use the local user database on the switch for authentication.
- radius: Uses one or more of the remote RADIUS servers for authentication.
- tacacs: Uses one or more of the remote TACACS+ servers for authentication.

Methods that involves remote servers are timed out if the remote servers are offline. In this case the next method is tried. Each method is tried from left to right and continues until a method either approves or rejects a user. If a remote server is used for primary authentication it is recommended to configure secondary authentication as local. This will enable the management client to log in via the local user database if none of the configured authentication servers are alive.

Command Authorization Method Configuration

The command authorization section allows you to limit the CLI commands available to a user. The table has one row for each client type and a number of columns which are as follows:

Client

The management client for which the configuration below applies.

- console
- telnet
- ssh

Methods

Method can be set to one of the following values:

- no: disable command authorization. User is granted access to CLI commands according to his privilege level.
- tacacs: Uses one or more of the remote TACACS+ servers for command authorization. If all remote servers are offline, the user is granted access to CLI commands according to his privilege level.

Cmd Lvl

Authorizes all commands with a privilege level higher than or equal to this level. Valid values are in the range 0 to 15.

Cfg Cmd

Also, authorizes configuration commands.

Accounting Method Configuration

The accounting section allows you to configure command and exec (login) accounting. The table has one row for each client type and a number of columns which are as follows:

Client

The management client for which the configuration below applies.

- console
- telnet
- ssh

Methods

Method can be set to one of the following values:

- no: disable authentication.
- tacacs: Uses one or more of the remote TACACS+ servers for accounting.

Cmd Lvl

Enable statistics of all commands with a privilege level higher than or equal to this level. Valid values are in the range 0 to 15. Leave the field empty to disable command accounting.

Exec

Enables exec (login) accounting.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.4 SSH

This option allows you to configure SSH. SSH (Secure Shell) protocol provides secure remote login on insecure network, ensures the integrity, reliability and safe transmission of data. After logging into the device through the SSH, use the command line provided by the device to manage and configure the device. This device supports SSH2.0 Version.

Pattern

The Mode option indicates the SSH mode operation. Possible modes are:

- Enabled: Enables SSH mode operation.
- Disabled: Disables SSH mode operation.

Buttons

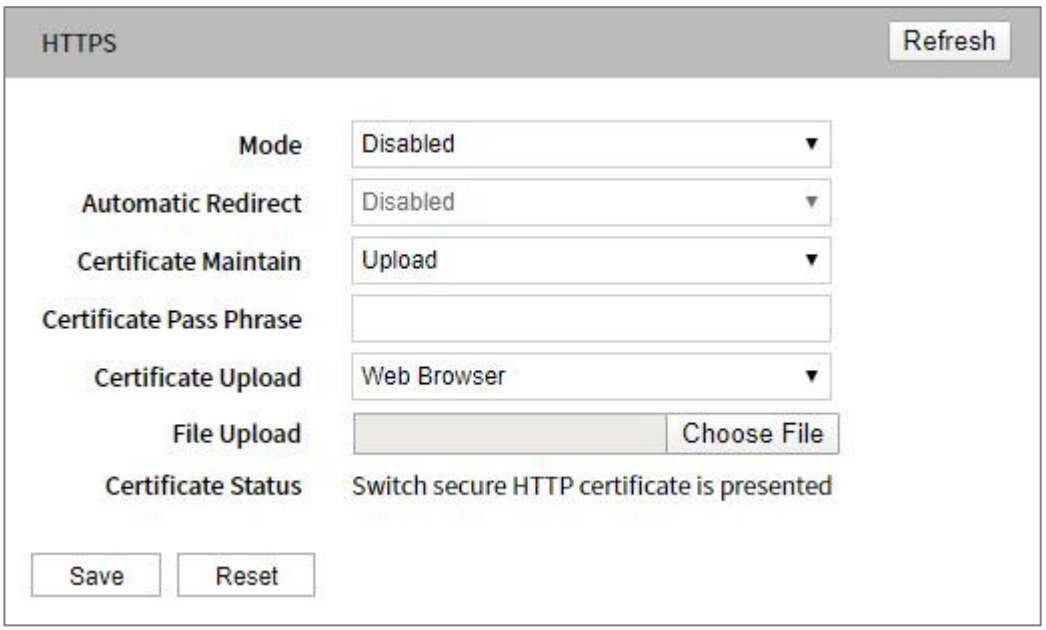
Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.5 HTTPS

HTTPS is short for Secure HTTP. HTTPS using the SSL (Secure Sockets Layer) protocol, encrypt the data that the client interacts with the device, and formulate access control strategy based on attribute certificate for equipment, improve the security and integrity of data transmission, ensure legitimate clients can safely access device, prohibited to illegally client access equipment, so as to realize the management of the safety of the equipment. In order to ensure security, users can reacquire the officially trusted server digital certificate file and key file from CA (Certificate Authority).

This page allows you to configure the HTTPS settings and maintain the current certificate on the switch.



Mode

Indicate the HTTPS mode operation. Possible modes are:

- Enabled: Enable HTTPS mode operation.
- Disabled: Disable HTTPS mode operation.

Automatic Redirect

Indicate the HTTPS redirect mode operation. It is only significant when “Enabled" HTTPS Mode is selected. When the redirect mode is enabled, the HTTP connection will be redirected to HTTPS connection automatically.

Notice that the browser may not allow the redirect operation due to the security consideration unless the switch certificate is trusted to the browser. You need to initialize the HTTPS connection manually for this case.

Possible modes are:

- Enabled: Enable HTTPS redirect mode operation.
- Disabled: Disable HTTPS redirect mode operation.

Certificate Maintain

The operation of certificate maintenance. Possible operations are:

- None: No operation.
- Delete: Delete the current certificate.
- Upload: Upload a certificate PEM file. Possible methods are: Web Browser or URL.
- Generate: Generate a new self-signed RSA certificate.

Certificate Pass Phrase

When "Certificate Maintenance" is "Upload", fields such as "Certificate Passphrase" and "Certificate Upload" appear. Enter the pass phrase in this field if your uploading certificate is protected by a specific passphrase.

Certificate Upload

Upload a certificate PEM file into the switch. The file should contain the certificate and private key together. If you have two separated files for saving certificate and private key. Use the Linux cat command to combine them into a single PEM file. For example, cat my.cert my.key > my.pem

Notice that the RSA certificate is recommended since most of the new version of browsers has removed support for DSA in certificate, e.g. Firefox v37 and Chrome v39.

Possible methods are:

- Web Browser: Upload a certificate via Web browser.
- URL: Upload a certificate via URL, the supported protocols are HTTP, HTTPS, TFTP and FTP. The URL format is <protocol>://[<username>[:<password>]@]<host>[:<port>][/<path>]/<file_name>. E.g. https://username:password@10.10.10.10:443/new_image_path/new_image.dat. A valid file name is a text string drawn from alphabet (A-Z, a-z), digits (09), dot (.), hyphen (-), under score(_). The maximum length is 63 and hyphen must not be first character. The file name content that only contains '.' is not allowed.

File Upload

When "Certificate Upload" is "Web Browser", click the "Select File" button and select a local certificate file to upload.

URL

When "Certificate Upload" is "URL", enter the URL link address of the certificate file here.

Certificate Status

Display the current status of certificate on the switch. There are the following states:

- The device security HTTP certificate has been submitted.
- The device security HTTP certificate has not been submitted.
- The device security HTTP certificate is generating ...

Buttons

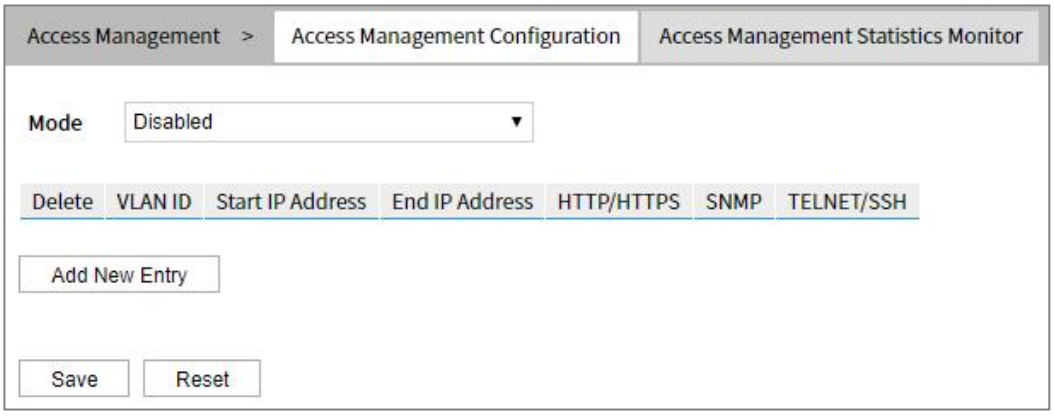
Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.6 Access Management

4.6.1 Access Management Configuration

This option allows you to configure access management. The maximum number of entries is 16. If the type of the application matches any one of the access management entries, it allows access to the switch.



Mode

Indicates the access management mode operation. Possible modes are:

- Enabled: Enables access management mode operation.
- Disabled: Disables access management mode operation.

Delete

Check the corresponding check box to delete an entry. It will be deleted during the next Save operation.

VLAN ID

The VLAN ID for the access management entry.

Start IP address

The start IP address for the access management entry.

Ending IP Address

The end IP address for the access management entry.

HTTP/HTTPS

Indicates that the host can access the switch from HTTP/HTTPS interface if the host IP address matches the IP address range provided in the entry.

SNMP

Indicates that the host can access the switch from SNMP interface if the host IP address matches the IP address range provided in the entry.

TELNET/SSH

Indicates that the host can access the switch from TELNET/SSH interface if the host IP address matches the IP address range provided in the entry.

Buttons

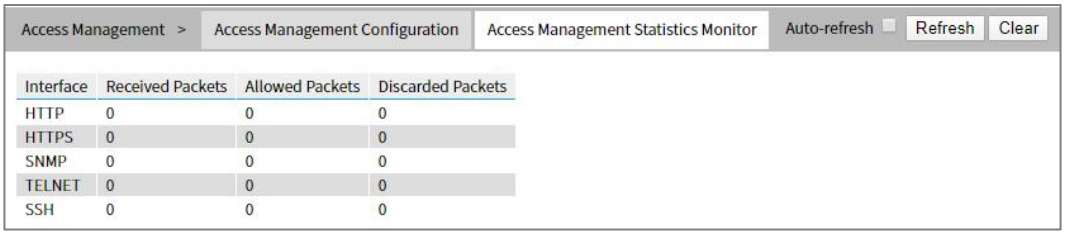
Add new entry: Click to add a new access management entry.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.6.2 Access Management Statistics

This page provides statistics for access management.



Interface

The interface type through which the remote host can access the switch.

Received Packets

Number of received packets from the interface when access management mode is enabled.

Allowed Packets

Number of allowed packets from the interface when access management mode is enabled.

Discarded Packets

Number of discarded packets from the interface when access management mode is enabled.

Buttons

Refresh: Click to refresh the page immediately.

Clear: Clear the counters for all ports.

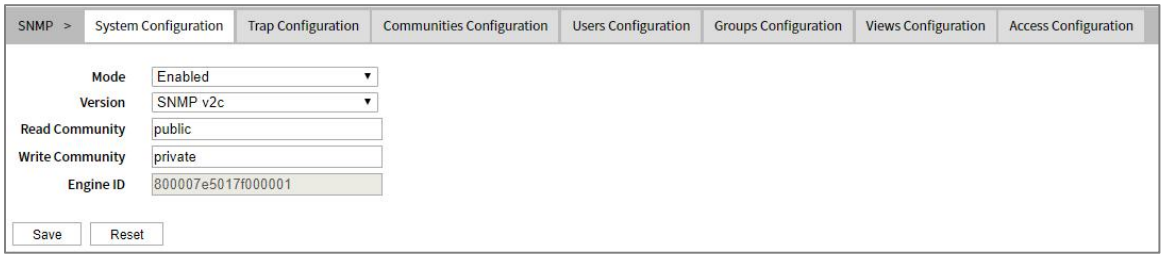
Auto-refresh: Check this box to enable an automatic refresh. Automatic refresh occurs every 3 seconds.

4.7 SNMP

SNMP (Simple Network Management Protocol) is a network management standard protocol widely used in TCP/IP networks. SNMP provides a way to manage devices by running network management software on a central computer (or network management workstation). The device supports SNMPv1/v2c/v3 version and v3 provides authentication encryption based on USM (User Security Module) and access control based on VACM (View-based Access Control Model).

4.7.1 System Configuration

This option allows you to system configure the SNMP feature.



Mode

Indicates the SNMP mode operation. Possible modes are:

- Enabled: Enables SNMP mode operation.
- Disabled: Disables SNMP mode operation.

Version

Indicates the SNMP supported version.

- SNMP v1: Set SNMP supported version 1.
- SNMP v2c: Set SNMP supported version 2c.
- SNMP v3: Set version 3 supported by SNMP.

Read Community

Indicates the community read access string to permit access to SNMP agent. The allowed string length is 1 to 255, and the allowed content is the ASCII characters from 33 to 126. The field is applicable only when SNMP version is SNMPv1 or SNMPv2c. If SNMP version is SNMPv3, the community string is associated with SNMPv3 communities table. It provides more flexibility to configure security name than a

SNMPv1 or SNMPv2c community string. In addition to community string, a particular range of source addresses can be used to restrict source subnet.

Write Community

Indicates the community write access string to permit access to SNMP agent. The allowed string length is 1 to 255, and the allowed content is the ASCII characters from 33 to 126. The field is applicable only when SNMP version is SNMPv1 or SNMPv2c. If SNMP version is SNMPv3, the community string is associated with SNMPv3 communities table. It provides more flexibility to configure security name than a SNMPv1 or SNMPv2c community string. In addition to community string, a particular range of source addresses can be used to restrict source subnet.

Engine ID

Indicates the SNMPv3 engine ID. The string must contain an even number(in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed. Change of the Engine ID will clear all original local users.

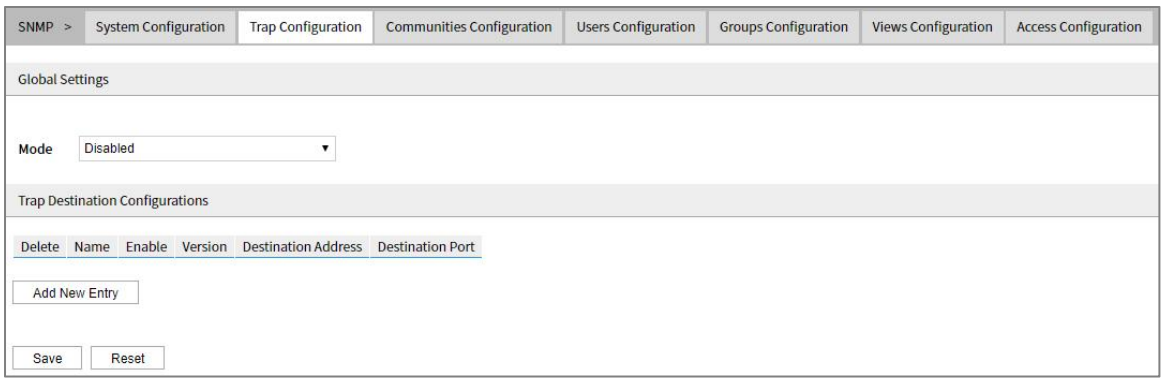
Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.7.2 Trap Configuration

This option allows you to configure the SNMP trap feature. When the device reaches the trigger condition of alarm, it will send a Trap message to NMS through Agent to inform the abnormal situation on the device side, which is convenient for the network administrator to handle in time. For example, after the managed device is warm-started, the Agent will send the Trap of WarmStart to NMS.



Global Settings

Mode

The Trap mode operation. Possible modes are as follows:

- Enabled: Enables SNMP trap mode operation.
- Disabled: Disables SNMP trap mode operation.

Trap Destination Configurations

Delete

Check the corresponding check box to delete an entry. It will be deleted during the next Save operation.

Name

Indicates the name of the Trap configuration.

Mode

The status of Trap mode is displayed as follows:

- Enabled: Enables SNMP trap mode operation.
- Disabled: Disables SNMP trap mode operation.

Version

Indicates the SNMP trap supported version.

Destination Address

Indicates the SNMP trap destination address. It allows a valid IP address in dotted decimal notation ('x.y.z.w') as well as a valid hostname.

Destination Port

Indicates the SNMP trap destination port. SNMP Agent sends an SNMP message via this port. The port range is 1~65535.

Buttons

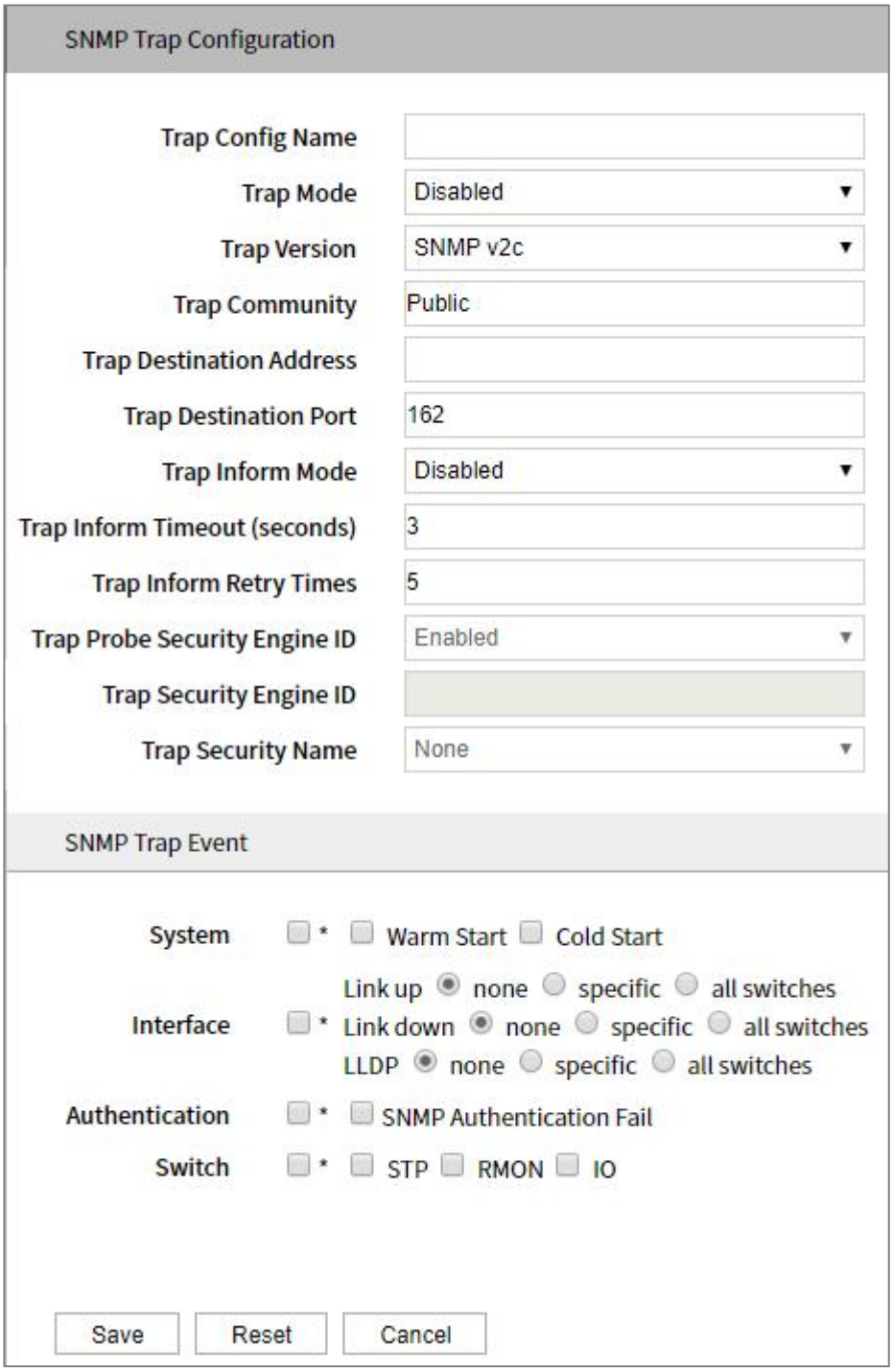
Add new entry: Click to add a new user.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

SNMP Trap Configuration

Click “Add new entry” to enter the “SNMP Trap Configuration” page.



Trap Config Name

Indicates which trap Configuration's name for configuring. The allowed string length is 3 to 15, and the allowed content is ASCII characters from 33 to 126.

Trap Mode

The drop-down list of Trap mode, options as follows:

- Enabled: Enable Trap mode.
- Disabled: Disable Trap mode.

Trap Version

Indicates the SNMP supported version.

Trap Community

Indicates the community access string when sending SNMP trap packet. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126.

Trap Destination Address

SNMP trap destination IP address It allows a valid IP address in dotted decimal notation ('x.y.z.w').

And it also allow a valid hostname.

Trap Destination port

SNMP trap destination port number. SNMP Agent will send SNMP message via this port, the port range is 1~65535.

Trap Inform Mode

Indicates the SNMP trap inform mode operation. Possible modes are:

- Enabled: Enable SNMP trap inform mode operation.
- Disabled: Disable SNMP trap inform mode operation.

Trap Inform Timeout (seconds)

Indicates the SNMP trap inform timeout. The allowed range is 0 to 2147.

Trap Inform Retry Times

Indicates the SNMP trap inform retry times. The allowed range is 0 to 255.

Trap Probe Security Engine ID

Indicates the SNMP trap probe security engine ID mode of operation. Possible modes are:

- Enabled: Enable SNMP trap probe security engine ID mode of operation.
- Disabled: Disable SNMP trap probe security engine ID mode of operation.

Trap Security Engine ID

Indicates the SNMP trap security engine ID. SNMPv3 sends traps and informs using USM for authentication and privacy. A unique engine ID for these traps and informs is needed. When "Trap Probe Security Engine ID" is enabled, the ID will be probed automatically. Otherwise, the ID specified in this field is used. The string must contain an even number(in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed.

Trap Security Name

Indicates the SNMP trap security name. SNMPv3 traps and informs using USM for authentication and privacy. A unique security name is needed when traps and informs are enabled.

SNMP Trap Event

System

Enable/disable the System group's traps. Optional traps are:

- Warm Start: Enable/disable Warm Start Trap.
- Cold Start: Enable/disable Cold Start Trap.

Interface

Indicates that the Interface group's Traps. Possible modes are:

- Link Up: Enable/disable Link up Trap.
- Link Down: Enable/disable Link down Trap.
- LLDP: Enable/disable LLDP Trap.

The interface selection is as follows:

- None: no port selected.
- Specific: select the specified port. After checking, the port-connect / disconnect configuration area is displayed. You can check the port to send trap after connecting / disconnecting.
- All switches: select all switch Ethernet ports.

Certification

Indicates that the authentication group's Traps. Optional traps are:

- SNMP authentication failure: Enable/disable SNMP trap authentication failure trap.

Enable

Indicates that the Switch group's traps. Optional traps are:

- STP: Enable/disable STP trap.
- RMON: Enable/disable RMON trap.
- IO: Enable/disable IO trap. (This function is reserved)

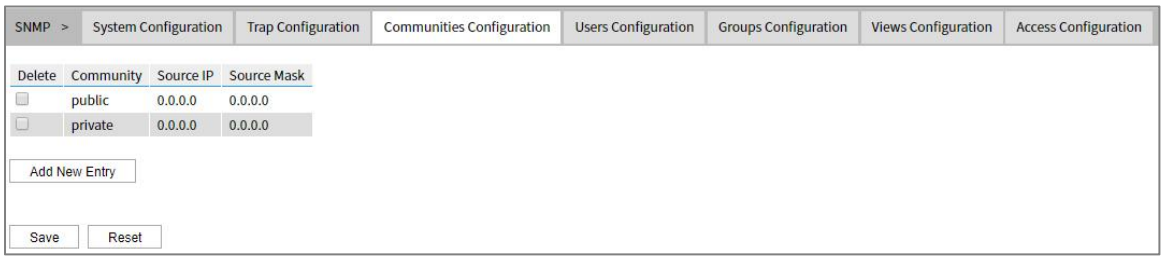
Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.7.3 Community Configuration

This option allows you to configure SNMPv3 community table. The entry index key is Community.



Delete

Check the corresponding check box to delete an entry. It will be deleted during the next Save operation.

Community

Indicates the community access string to permit access to SNMPv3 agent. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126. The community string will be treated as security name and map a SNMPv1 or SNMPv2c community string.

Source IP

Indicates the SNMP access source address. A particular range of source addresses can be used to restrict source subnet when combined with source mask.

Source Mask

Indicates the SNMP access source address mask.

Buttons

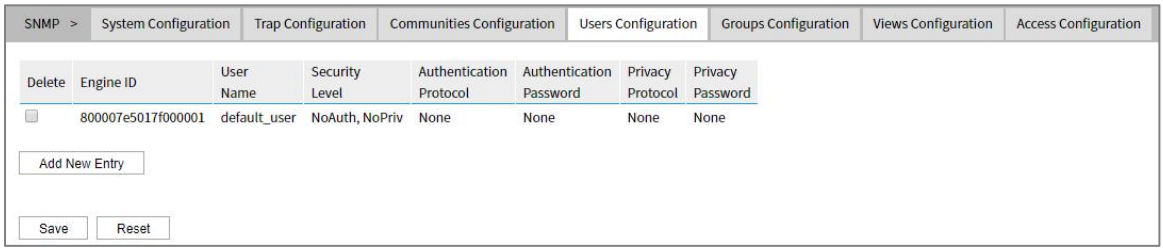
Add new community entry: Click to add a new community entry.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.7.4 User Configuration

This option allows you to configure SNMPv3 user table. The entry index keys are Engine ID and User Name.



Delete

Check the corresponding check box to delete an entry. It will be deleted during the next Save operation.

Engine ID

An hexadecimal string identifying the engine ID that this entry should belong to. The string must contain an even number(in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed. The SNMPv3 architecture uses the User-based Security Model (USM) for message security and the View-based Access Control Model (VACM) for access control. For the USM entry, the usmUserEngineID and usmUserName are the entry's keys. In a simple agent, usmUserEngineID is always that agent's own snmpEngineID value. The value can also take the value of the snmpEngineID of a remote SNMP engine with which this user can communicate. In other words, if user engine ID equal system engine ID then it is a local user; otherwise it is a remote user.

Username

A string identifying the user name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Security Level

Indicates the security model that this entry should belong to. Possible security models are:

- NoAuth, NoPriv: No authentication and no privacy.
- Auth, NoPriv: Authentication and no privacy.
- Auth, Priv: Authentication and privacy.

The value of security level cannot be modified if entry already exists. That means must first ensure that the value is set correctly.

Authentication Mode

Indicates the authentication protocol that this entry should belong to. Possible modes are:

- None: No authentication protocol.
- MD5: An optional flag to indicate that this user uses MD5 authentication protocol. This algorithm has security risks.
- SHA: An optional flag to indicate that this user uses SHA authentication protocol. This algorithm has security risks.

The value of security level cannot be modified if entry already exists. That means must first ensure that the value is set correctly.

Authentication Password

A string identifying the authentication password phrase. For MD5 authentication protocol, the allowed string length is 8 to 32. For SHA authentication protocol, the allowed string length is 8 to 40. The allowed content is ASCII characters from 33 to 126.

Privacy Protocol

Indicates the privacy protocol that this entry should belong to. Possible privacy protocols are:

- None: No privacy protocol.
- DES: An optional flag to indicate that this user uses DES authentication protocol. DES encryption has security risks. It is recommended to use AES encryption mode with high security.
- AES: An optional flag to indicate that this user uses AES authentication protocol.

Privacy Password

A string identifying the privacy password phrase. The allowed string length is 8 to 32, and the allowed content is ASCII characters from 33 to 126.

Buttons

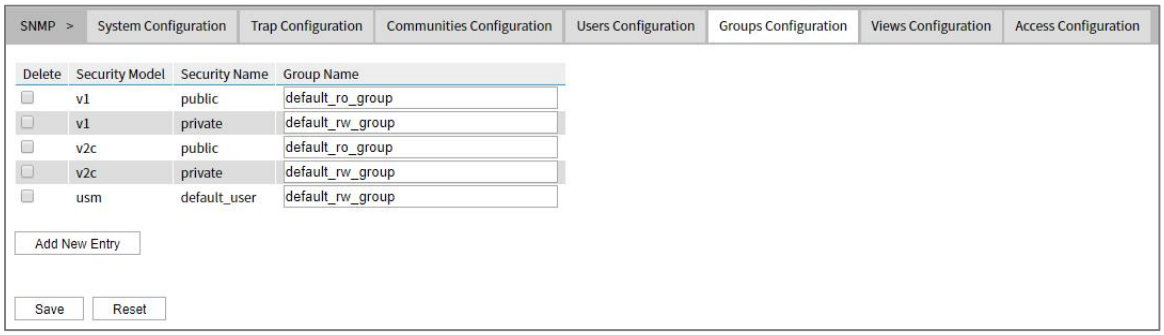
Add New Entry: Click to add new entry.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.7.5 Group Configuration

This option allows you to configure the SNMPv3 group table. The entry index keys are Security Model and Security Name.



Delete

Check the corresponding check box to delete an entry. It will be deleted during the next Save operation.

Security Model

Indicates the security model that this entry should belong to. Possible security models are as follows:

- v1: Reserved for SNMPv1.
- v2c: Reserved for SNMPv2c.
- usm: User-based Security Model (USM).

Security Name

A string identifying the security name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Group Name

A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Buttons

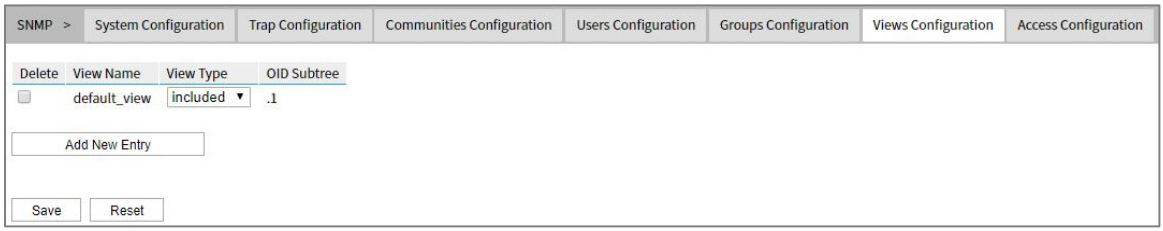
Add new group entry: Click to add a new community entry.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.7.6 View Configuration

Configure SNMPv3 view table on this page. The entry index keys are View Name and OID Subtree.



Delete

Check to delete the entry. It will be deleted during the next save.

View Name

A string identifying the view name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

View Type

Indicates the view type that this entry should belong to. Possible view types are:

- included: An optional flag to indicate that this view subtree should be included.
- excluded: An optional flag to indicate that this view subtree should be excluded.

In general, if a view entry's view type is 'excluded', there should be another view entry existing with view type as 'included' and it's OID subtree should overstep the 'excluded' view entry.

OID Subtree

The OID defining the root of the subtree to add to the named view. The format of MIB subtree OID is ".OID1.OID2.OID3.……". The allowed OID length is 1 to 128. The allowed string content is digital number or asterisk(*).

Buttons

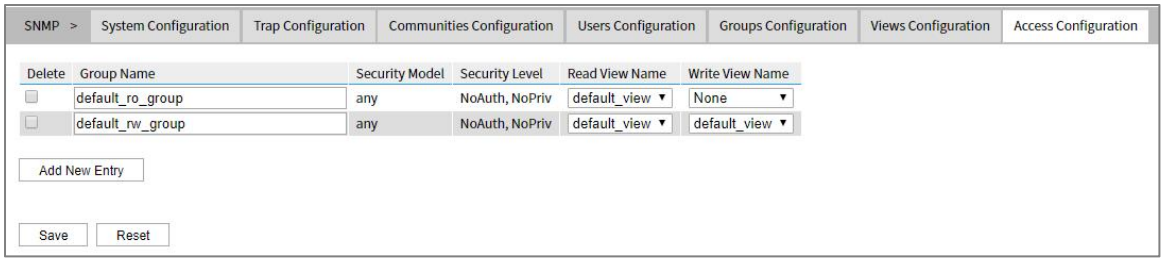
Add new view entry: click to add a new view entry.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.7.7 Access Configuration

Configure SNMPv3 access table on this page. The entry index keys are Group Name, Security Model and Security Level.



Delete

Check to delete the entry. It will be deleted during the next save.

Group Name

A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Security Model

Indicates the security model that this entry should belong to. Possible security models are:

- any: Any security model accepted(v1|v2c|usm).
- v1: Reserved for SNMPv1.
- v2c: Reserved for SNMPv2c.
- usm: User-based Security Model (USM).

Security Level

Indicates the security model that this entry should belong to. Possible security models are:

- NoAuth, NoPriv: No authentication and no privacy.
- Auth, NoPriv: Authentication and no privacy.
- Auth, Priv: Authentication and privacy.

Read View Name

The name of the MIB view defining the MIB objects for which this request may request the current values. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Write View Name

The name of the MIB view defining the MIB objects for which this request may potentially set new values. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Buttons

Add new access entry: click to add a new access entry.

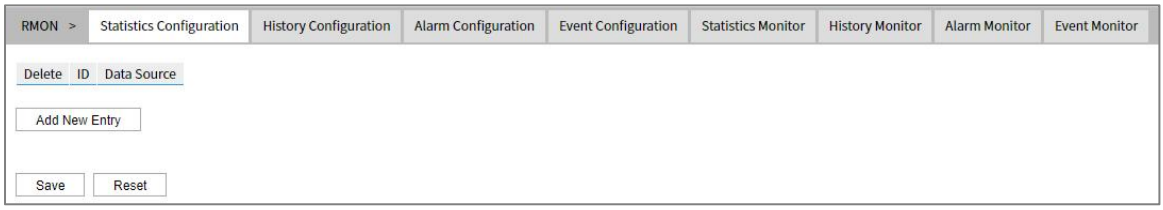
Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.8 RMON

4.8.1 Statistics Configuration

Configure RMON Statistics table on this page. The entry index key is ID.



Delete

Check to delete the entry. It will be deleted during the next save.

ID

Indicates the index of the entry. The range is from 1 to 65535.

Data Source

Indicates the port ID which wants to be monitored. If in stacking switch, the value must add 1000000*(switch ID-1), for example, if the port is switch 3 port 5, the value is 2000005.

Buttons

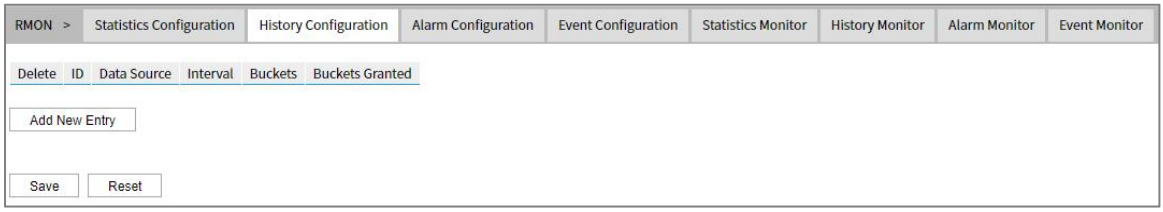
Add new entry: Click to add a new community entry.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.8.2 History Configuration

Configure RMON History table on this page. The entry index key is ID.



Delete

Check to delete the entry. It will be deleted during the next save.

ID

Indicates the index of the entry. The range is from 1 to 65535.

Data Source

Indicates the port ID which wants to be monitored. If in stacking switch, the value must add 1000000*(switch ID-1), for example, if the port is switch 3 port 5, the value is 2000005.

Sampling Interval

Indicates the interval in seconds for sampling the history statistics data. The range is from 1 to 3600, default value is 1800 seconds.

Buckets

Indicates the maximum data entries associated this History control entry stored in RMON. The range is from 1 to 3600, default value is 50.

Buckets Granted

The number of data shall be saved in the RMON.

Buttons

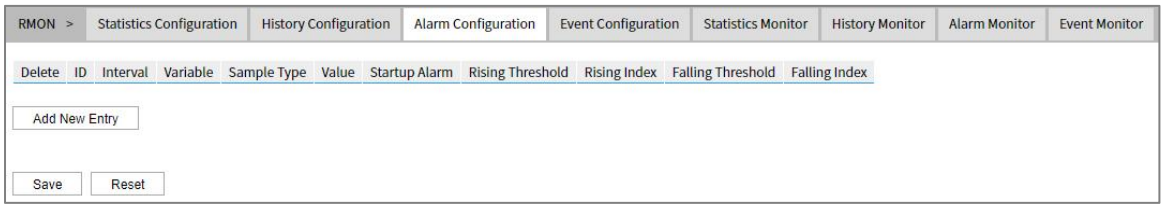
Add new entry: Click to add a new community entry.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.8.3 Alarm Configuration

Configure RMON alarm table on this page. The entry index key is ID.



Delete

Check to delete the entry. It will be deleted during the next save.

ID

Indicates the index of the entry. The range is from 1 to 65535.

Interval

Indicates the interval in seconds for sampling and comparing the rising and falling threshold. The range is from 1 to 2^31-1.

Variable

MIB OID node.

Sample Type

The method of sampling the selected variable and calculating the value to be compared against the thresholds, possible sample types are:

- Absolute: Get the sample directly.
- Delta: Calculate the difference between samples (default).

Variable

The value of the statistic during the last sampling period.

Startup Alarm

The method of sampling the selected variable and calculating the value to be compared against the thresholds, possible sample types are:

- RisingTrigger alarm when the first value is larger than the rising threshold.
- FallingTrigger alarm when the first value is less than the falling threshold.
- RisingOrFallingTrigger alarm when the first value is larger than the rising threshold or less than the falling threshold (default).

Rising Threshold

Rising threshold value (-2147483648-2147483647).

Rising Index

Rising event index (1-65535).

Falling Threshold

Falling threshold value (-2147483648-2147483647).

Falling Index

Falling event index (1-65535).

Buttons

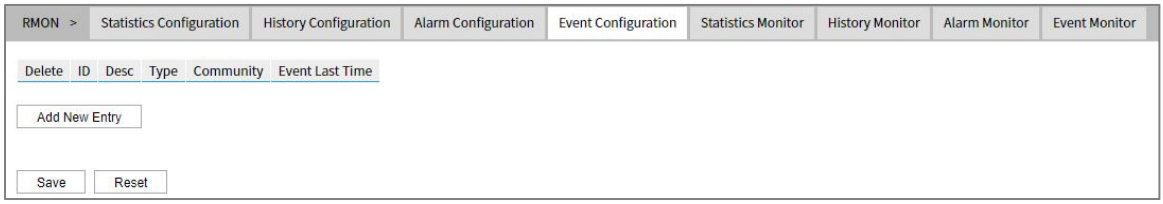
Add new entry: Click to add a new community entry.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.8.4 Link Event Configuration

Configure RMON Event table on this page. The entry index key is ID.



Delete

Check to delete the entry. It will be deleted during the next save.

ID

Indicates the index of the entry. The range is from 1 to 65535.

Description

Indicates this event, the string length is from 0 to 127, default is a null string.

Type

Indicates the notification of the event, the possible types are:

- none: No operations.
- Log: When an event is triggered, create SNMP log entries.
- snmptrap: send SNMP trap when an event is triggered.
- Logandtrap: Create SNMP log entry and send SNMP trap when an event is triggered.

Community

Specify the community when trap is sent, the string length is from 0 to 127, default is "public".

Event Last Time

Indicates the value of sysUpTime at the time this event entry last generated an event.

Buttons

Add new entry: Click to add a new community entry.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

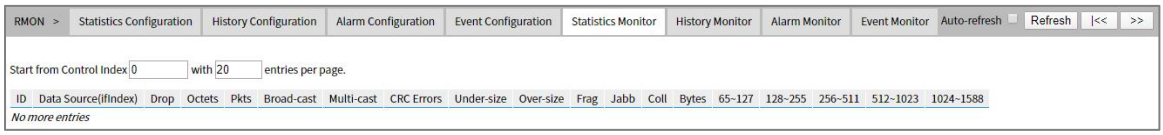
4.8.5 Statistics Monitoring

This page provides an overview of RMON Statistics entries. Each page shows up to 99 entries from the Alarm table, default being 20, selected through the "entries per page" input field. When first visited, the WEB page will show the first 20 entries from the beginning of the Statistics table. The first displayed will be the one with the lowest ID found in the Statistics table.

The "Start from Control Index" allows the user to select the starting point in the Alarm table. Clicking the “Refresh” button will update the displayed table starting from that or the next closest Statistics table match.

This “>>” button will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the “|<<” button to start over.

The displayed counters are:



ID

Indicates the index of Statistics entry.

Data Source(Interface)

The port ID which wants to be monitored.

Discarded Packets

The total number of events in which packets were dropped by the probe due to lack of resources.

Eight-bit Byte

The total number of octets of data (including those in bad packets) received on the network.

Packets

The total number of packets (including bad packets, broadcast packets, and multicast packets) received.

Broadcast

The total number of good packets received that were directed to the broadcast address.

Multicast

The total number of good packets received that were directed to a multicast address.

CRC Error

Total number of packets received. Eight-bit byte with length (excluding the frame part, but including FCS octets) between 64 and 1518, but there is an integer (FCS error) bad frame check sequence (FCS) of eight-bit byte or a bad FCS eight-bit byte which is not an integer (alignment error).

Undersize

The total number of packets received that were less than 64 octets.

Oversize

The total number of packets received that were longer than 1518 octets.

Fragment

The number of frames which size is less than 64 octets received with invalid CRC.

Jabb

The number of frames which size is larger than 64 octets received with invalid CRC.

Conflict

The best estimate of the total number of collisions on this Ethernet segment.

Bytes

The total number of packets (including bad packets) received that were 64 octets in length.

65~127

The total number of packets (including bad packets) received that were between 65 to 127 octets in length.

128~255

The total number of packets (including bad packets) received that were between 128 to 255 octets in length.

256~511

The total number of packets (including bad packets) received that were between 256 to 511 octets in length.

512~1023

The total number of packets (including bad packets) received that were between 512 to 1023 octets in length.

1024~1588

The total number of packets (including bad packets) received that were between 1024 to 1588 octets in length.

Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

|<<: Updates the table starting from the first entry in the Statistics table, i.e. the entry with the lowest ID.

>>: Updates the table, starting with the entry after the last entry currently displayed.

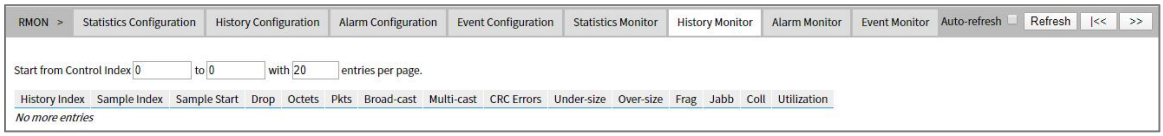
4.8.6 History Monitoring

This page provides an overview of RMON History entries. Each page shows up to 99 entries from the History table, default being 20, selected through the "entries per page" input field. When first visited, the WEB page will show the first 20 entries from the beginning of the History table. The first displayed will be the one with the lowest History Index and Sample Index found in the History table.

“Start from Control Index” allows the user to select a starting point in the history table. Clicking the “Refresh” button will update the displayed table starting from that or the next closest History table match.

This “>>” button will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the “|<<” button to start over.

The displayed fields are:



ID

Indicates the index of History control entry.

Sample Index

Indicates the index of the data entry associated with the control entry.

Sample initial value

Sample SysUpTime value measured at interval time.

Discarded Packets

The total number of events in which packets were dropped by the probe due to lack of resources.

Eight-bit Byte

The total number of octets of data (including those in bad packets) received on the network.

Packets

The total number of packets (including bad packets, broadcast packets, and multicast packets) received.

Broadcast

The total number of good packets received that were directed to the broadcast address.

Multicast

The total number of good packets received that were directed to a multicast address.

CRC Error

Total number of packets received. Eight-bit byte with length (excluding the frame part, but including FCS octets) between 64 and 1518, but there is an integer (FCS error) bad frame check sequence (FCS) of eight-bit byte or a bad FCS eight-bit byte which is not an integer (alignment error).

Undersize

The total number of packets received that were less than 64 octets.

Oversize

The total number of packets received that were longer than 1518 octets.

Fragment

The number of frames which size is less than 64 octets received with invalid CRC.

Jabb

The number of frames which size is larger than 64 octets received with invalid CRC.

Conflict

The best estimate of the total number of collisions on this Ethernet segment.

Application

The best estimate of the mean physical layer network utilization on this interface during this sampling interval, in hundredths of a percent.

Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

|<<: Updates the table starting from the first entry in the Statistics table, i.e. the entry with the lowest ID.

>>: Updates the table, starting with the entry after the last entry currently displayed.

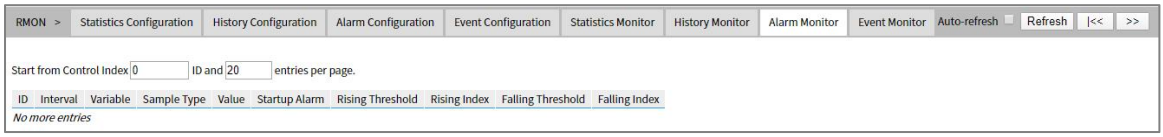
4.8.7 Alarm Monitoring

This page provides an overview of RMON Statistics entries. Each page shows up to 99 entries from the Statistics table, default being 20, selected through the "entries per page" input field. When first visited, the WEB page will show the first 20 entries from the beginning of the Statistics table. The first displayed will be the one with the lowest ID found in the Statistics table.

The "Start from Control Index" allows the user to select the starting point in the Alarm table. Clicking the “Refresh” button will update the displayed table starting from that or the next closest Statistics table match.

This “>>” button will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the “|<<” button to start over.

The displayed fields are:



ID

Indicates the index of Alarm control entry.

Interval

Indicates the interval in seconds for sampling and comparing the rising and falling threshold.

Variable

Indicates the particular variable to be sampled

Sample Type

The method of sampling the selected variable and calculating the value to be compared against the thresholds.

Value

The value of the statistic during the last sampling period.

Startup Alarm

The alarm that may be sent when this entry is first set to valid.

Rising Threshold

Rising threshold value.

Rising Index

Rising event index.

Falling Threshold

Falling threshold value.

Falling index

Falling event index.

Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

|<<: Updates the table starting from the first entry in the Statistics table, i.e. the entry with the lowest ID.

>>: Updates the table, starting with the entry after the last entry currently displayed.

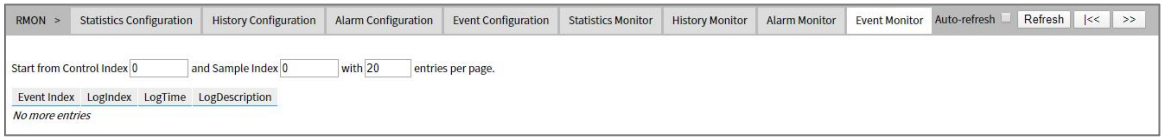
4.8.8 Event Monitoring

This page provides an overview of RMON event entries. Each page shows up to 99 entries from the event table, default being 20, selected through the "entries per page" input field. When first visited, the WEB page will show the first 20 entries from the beginning of the Event table. The first displayed will be the one with the lowest Event Index and Log Index found in the Event table.

The "Start from Control Index and Sample Index" input field allows the user to select a starting point in the Event table. Clicking the “Refresh” button will update the displayed table starting from that or the next closest Event table match.

This “>>” button will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the “|<<” button to start over.

The displayed fields are:



Event Index

Indicates the index of the event entry.

Log Index

Indicates the index of the log entry.

LogTime

Indicates Event log time

LogDescription

Indicates the Event description.

Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

|<<: Updates the table starting from the first entry in the Event Table, i.e. the entry with the lowest Event Index and Log Index.

>>: Updates the table, starting with the entry after the last entry currently displayed.

5 Secure Network

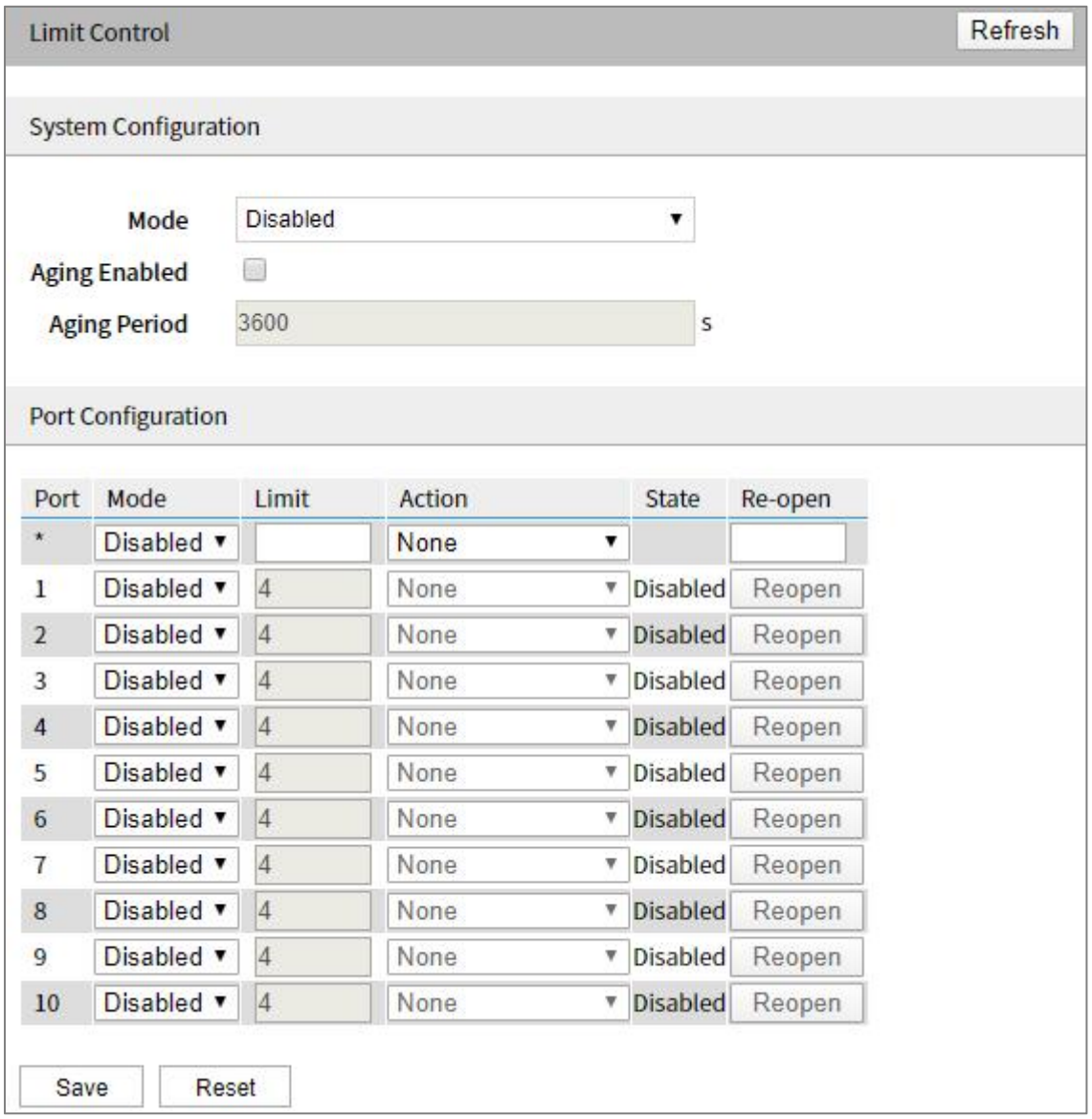
5.1 Port Limit Control

This page allows you to configure the Port Security Limit Control system and port settings.

Limit Control allows for limiting the number of users on a specified port. A user is identified by a MAC address and VLAN ID. If Limit Control is enabled on a port, the limit specifies the maximum number of users on the port. If this number is exceeded, an action is taken. The action can be one of the four different actions as described below.

The Limit Control module utilizes a lower-layer module, Port Security module, which manages MAC addresses learnt on the port.

The Limit Control configuration consists of two sections, a system- and a port-wide.



System Configuration

Mode

Indicates if Limit Control is globally enabled or disabled on the switch. If globally disabled, other modules may still use the underlying functionality, but limit checks and corresponding actions are disabled.

Aging Enabled

If checked, secured MAC addresses are subject to aging as discussed under Aging Period .

Aging Period

If Aging Enabled is checked, then the aging period is controlled with this input. If other modules are using the underlying port security for securing MAC addresses, they may

have other requirements to the aging period. The underlying port security will use the shorter requested aging period of all modules that use the functionality.

The Aging Period can be set to a number between 10 and 10000000 seconds.

To understand why aging may be desired, consider the following scenario: Suppose an end-host is connected to a 3rd party switch or hub, which in turn is connected to a port on this switch on which Limit Control is enabled. The end-host will be allowed to forward if the limit is not exceeded. Now suppose that the end-host logs off or powers down. If it wasn't for aging, the end-host would still take up resources on this switch and will be allowed to forward. To overcome this situation, enable aging. With aging enabled, a timer is started once the end-host gets secured. When the timer expires, the switch starts looking for frames from the end-host, and if such frames are not seen within the next Aging Period, the end-host is assumed to be disconnected, and the corresponding resources are freed on the switch.

Port Configuration

The table has one row for each port on the switch and a number of columns, which are:

Port

The port number for which the configuration below applies.

Mode

Controls whether Limit Control is enabled on this port. Both this and the Global Mode must be set to Enabled for Limit Control to be in effect. Notice that other modules may still use the underlying port security features without enabling Limit Control on a given port.

Limit

The maximum number of MAC addresses that can be secured on this port. This number cannot exceed 1024. If the limit is exceeded, the corresponding action is taken.

The switch is "born" with a total number of MAC addresses from which all ports draw whenever a new MAC address is seen on a Port Security-enabled port. Since all ports draw from the same pool, it may happen that a configured maximum cannot be granted, if the remaining ports have already used all available MAC addresses.

Action

If Limit is reached, the switch can take one of the following actions:

- None: Do not allow more than Limit MAC addresses on the port, but take no further action.

- Trap: If Limit +1 MAC addresses is seen on the port, send an SNMP trap. If Aging is disabled, only one SNMP trap will be sent, but with Aging enabled, new SNMP traps will be sent every time the limit gets exceeded.
- Shutdown: If Limit +1 MAC addresses is seen on the port, shut down the port. This implies that all secured MAC addresses will be removed from the port, and no new address will be learned. Even if the link is physically disconnected and reconnected on the port (by disconnecting the cable), the port will remain shut down. There are three ways to re-open the port:

  1) Boot the switch,

  2) Disable and re-enable Limit Control on the port or the switch,

  3) Click the Reopen button.
- Trap & Shutdown: If Limit + 1 MAC addresses is seen on the port, both the "Trap" and the "Shutdown" actions described above will be taken.

State

This column shows the current state of the port as seen from the Limit Control's point of view. The state takes one of four values:

- Disabled: Limit Control is either globally disabled or disabled on the port.
- Ready: The limit is not yet reached. This can be shown for all actions.
- Limit Reached: Indicates that the limit is reached on this port. This state can only be shown if Action is set to None or Trap.
- Shutdown: Indicates that the port is shut down by the Limit Control module. This state can only be shown if Action is set to Shutdown or Trap & Shutdown.

Re-open Button

If a port is shutdown by this module, you may reopen it by clicking this button, which will only be enabled if this is the case.

Note that clicking the "Reopen" button will refresh the page, so uncommitted changes will be lost.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

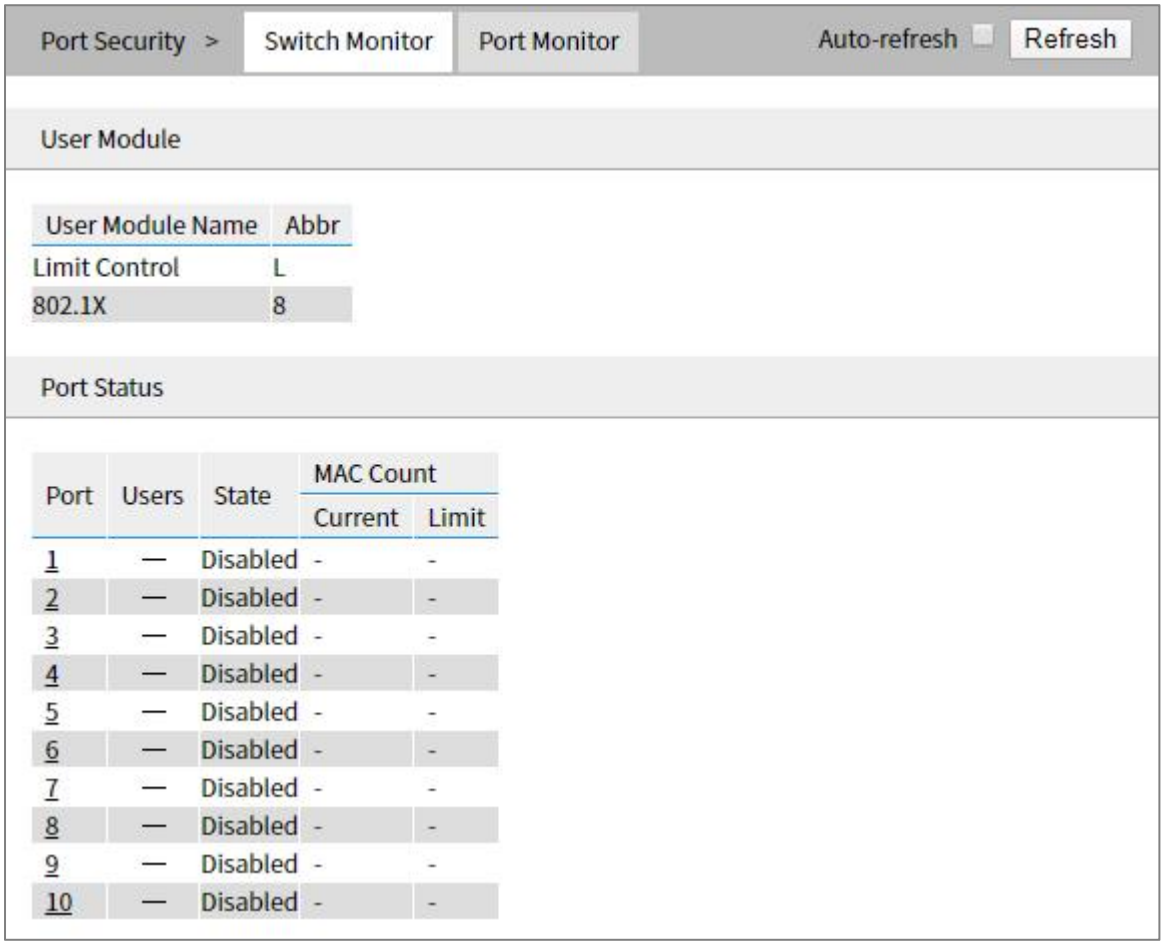
5.2 Port Security

5.2.1 Switch Monitoring

This page shows the Port Security status. Port Security is a module with no direct configuration. Configuration comes indirectly from other modules - the user modules.

When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise.

The status page is divided into two sections - one with a legend of user modules and one with the actual port status.



User Module

This shows all user modules that may request Port Security services.

User Module Name

The full name of a module that may request Port Security services.

Abbr

A one-letter abbreviation of the user module. Used in the user column of the port status table.

Port Status

The table has one row for each port on the switch and a number of columns, which are:

Port

The port number for which the status applies. Click the port number to see the status for this particular port.

User

Each of the user modules has a column that shows whether that module has enabled Port Security or not. '-' means that the corresponding user module is not enabled, whereas a letter indicates that the user module abbreviated by that letter (see Abbr) has enabled port security.

Status

Shows the current state of the port. It can take one of four values:

- Disabled: No user modules are currently using the Port Security service.
- Ready: The Port Security service is in use by at least one user module, and is awaiting frames from unknown MAC addresses to arrive.
- Limit Reached: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is reached and no more MAC addresses should be taken in.
- Shutdown: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is exceeded. No MAC addresses can be learned on the port until it is administratively re-opened on the Limit Control configuration Web-page.

MAC Count (Current, Limit)

The two columns indicate the number of currently learned MAC addresses (forwarding as well as blocked) and the maximum number of MAC addresses that can be learned on the port, respectively.

If no user modules are enabled on the port, the Current column will show a dash (-).

If the restriction control user module is not enabled on the port, the restriction column will display a dash (-).

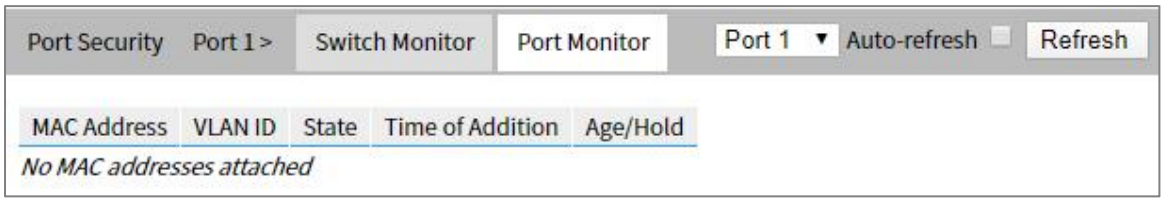
Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

5.2.2 Port Monitoring

This page shows the MAC addresses secured by the Port Security module. Port Security is a module with no direct configuration. Configuration comes indirectly from other modules - the user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise.



MAC Address & VLAN ID

The MAC address and VLAN ID that is seen on this port. If no MAC addresses are learned, a single row stating "No MAC addresses attached" is displayed.

Status

Indicates whether the corresponding MAC address is blocked or forwarding. In the blocked state, it will not be allowed to transmit or receive traffic.

Time of Addition

Shows the date and time when this MAC address was first seen on the port.

Age/Hold

If at least one user module has decided to block this MAC address, it will stay in the blocked state until the hold time (measured in seconds) expires. If all user modules have decided to allow this MAC address to forward, and aging is enabled, the Port Security module will periodically check that this MAC address still forwards traffic. If the age period (measured in seconds) expires and no frames have been seen, the MAC address will be removed from the MAC table. Otherwise a new age period will begin.

If aging is disabled or a user module has decided to hold the MAC address indefinitely, a dash (-) will be shown.

Buttons

Use the port select box to select which port to show status for.

Auto-refresh: Check this box to enable an automatic refresh. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

5.3 NAS

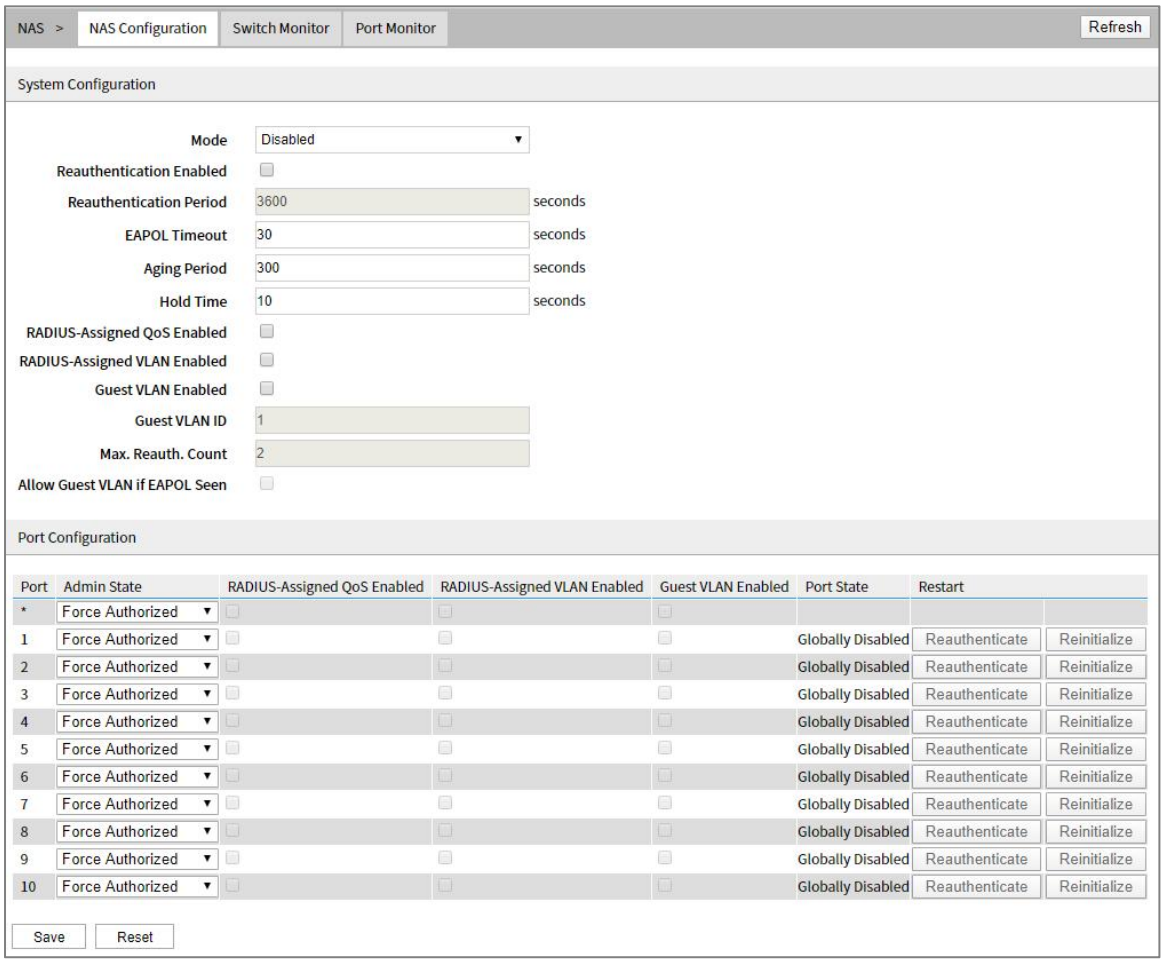
5.3.1 NAS Configuration

This page allows you to configure the IEEE 802.1X and MAC-based authentication system and port settings.

The IEEE 802.1X standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication. One or more central servers, the backend servers, determine whether the user is allowed access to the network. These backend (RADIUS) servers are configured on the "Security Network" page. The IEEE802.1X standard defines port-based operation, but non-standard variants overcome security limitations as shall be explored below.

MAC-based authentication allows for authentication of more than one user on the same port, and doesn't require the user to have special 802.1X supplicant software installed on his system. The switch uses the user's MAC address to authenticate against the backend server. Intruders can create counterfeit MAC addresses, which makes MAC-based authentication less secure than 802.1X authentication.

The NAS configuration consists of two sections, a system- and a port-wide.



System Configuration

Mode

Indicates if NAS is globally enabled or disabled on the switch. If globally disabled, all ports are allowed forwarding of frames.

Reauthentication Enabled

If checked, successfully authenticated supplicants/clients are reauthenticated after the interval specified by the Reauthentication Period. Reauthentication for 802.1X-enabled ports can be used to detect if a new device is plugged into a switch port or if a supplicant is no longer attached.

For MAC-based ports, reauthentication is only useful if the RADIUS server configuration has changed. It does not involve communication between the switch and the client, and therefore doesn't imply that a client is still present on a port (see Aging Period below).

Reauthentication Period

Determines the period, in seconds, after which a connected client must be reauthenticated. This is only active if the Reauthentication Enabled checkbox is checked. Valid values are in the range 1 to 3600 seconds.

EAPOL Timeout

Determines the time for retransmission of Request Identity EAPOL frames.

Valid values are in the range 1 to 65535 seconds. This has no effect for MAC-based ports.

Aging Time

This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses:

- Single 802.1X
- Multi 802.1X
- MAC-Based Auth.

When the NAS module uses the Port Security module to secure MAC addresses, the Port Security module needs to check for activity on the MAC address in question at regular intervals and free resources if no activity is seen within a given period of time. This parameter controls exactly this period and can be set to a number between 10 and 1000000 seconds.

If reauthentication is enabled and the port is in an 802.1X-based mode, this is not so critical, since supplicants that are no longer attached to the port will get removed upon the next reauthentication, which will fail. But if reauthentication is not enabled, the only way to free resources is by aging the entries.

For ports in MAC-based Auth. mode, reauthentication doesn't cause direct communication between the switch and the client, so this will not detect whether the client is still attached or not, and the only way to free any resources is to age the entry.

Hold Time

This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses:

- Single 802.1X
- Multi 802.1X
- MAC-Based Auth.

If a client is denied access - either because the RADIUS server denies the client access or because the RADIUS server request times out - the client is put on hold in the Unauthorized state. The hold timer does not count during an on-going authentication.

In MAC-based Auth. mode, the switch will ignore new frames coming from the client during the hold time.

The Hold Time can be set to a number between 10 and 1000000 seconds.

RADIUS-Assigned QoS Enabled

RADIUS-assigned QoS provides a means to centrally control the traffic class to which traffic coming from a successfully authenticated supplicant is assigned on the switch. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature (see RADIUS-Assigned QoS Enabled below for a detailed description).

The "RADIUS-Assigned QoS Enabled" checkbox provides a quick way to globally enable/disable RADIUS-server assigned QoS Class functionality. When checked, the individual ports' ditto setting determine whether RADIUS-assigned QoS Class is enabled on that port. When unchecked, RADIUS-server assigned QoS Class is disabled on all ports.

RADIUS-Assigned VLAN Enabled

RADIUS-assigned VLAN provides a means to centrally control the VLAN on which a successfully authenticated supplicant is placed on the switch. Incoming traffic will be classified to and switched on the RADIUS-assigned VLAN. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature (see RADIUS-Assigned VLAN Enabled below for a detailed description).

The "RADIUS-Assigned VLAN Enabled" checkbox provides a quick way to globally enable/disable RADIUS-server assigned VLAN functionality. When checked, the individual ports' ditto setting determine whether RADIUS-assigned VLAN is enabled on that port. When unchecked, RADIUS-server assigned VLAN is disabled on all ports.

Guest VLAN Enabled

A Guest VLAN is a special VLAN - typically with limited network access - on which 802.1X-unaware clients are placed after a network administrator-defined timeout. The switch follows a set of rules for entering and leaving the Guest VLAN as listed below.

The "Guest VLAN Enabled" checkbox provides a quick way to globally enable/disable Guest VLAN functionality. When checked, the individual ports' ditto setting determines whether the port can be moved into Guest VLAN. When unchecked, the ability to move to the Guest VLAN is disabled on all ports.

Guest VLAN ID

This is the value that a port's Port VLAN ID is set to if a port is moved into the Guest VLAN. It is only changeable if the Guest VLAN option is globally enabled.

Valid values are in the range [1; 4095].

Max. Reauth. Count

The number of times the switch transmits an EAPOL Request Identity frame without response before considering entering the Guest VLAN is adjusted with this setting. The value can only be changed if the Guest VLAN option is globally enabled.

Valid values are in the range [1; 255].

Allow Guest VLAN if EAPOL Seen

The switch remembers if an EAPOL frame has been received on the port for the life-time of the port. Once the switch considers whether to enter the Guest VLAN, it will first check if this option is enabled or disabled. If disabled (unchecked; default), the switch will only enter the Guest VLAN if an EAPOL frame has not been received on the port for the life-time of the port. If enabled (checked), the switch will consider entering the Guest VLAN even if an EAPOL frame has been received on the port for the life-time of the port.

The value can only be changed if the Guest VLAN option is globally enabled.

Port Configuration

The table has one row for each port on the switch and a number of columns, which are:

Port

The port number for which the configuration below applies.

Admin State

If NAS is globally enabled, this selection controls the port's authentication mode. The following modes are available:

- Force Authorized
  In this mode, the switch will send one EAPOL Success frame when the port link comes up, and any client on the port will be allowed network access without authentication.
- Force Unauthorized
  In this mode, the switch will send one EAPOL Failure frame when the port link comes up, and any client on the port will be disallowed network access.
- Port-based 802.1X
  In the 802.1X-world, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The authenticator acts as the man-in-the-middle, forwarding requests and responses between the supplicant and the authentication server. Frames sent between the supplicant and the switch are special 802.1X frames, known as EAPOL (EAP Over LANs) frames. EAPOL frames encapsulate EAP PDUs (RFC3748). Frames

sent between the switch and the RADIUS server are RADIUS packets. RADIUS packets also encapsulate EAP PDUs together with other attributes like the switch's IP address, name, and the supplicant's port number on the switch. EAP is very flexible, in that it allows for different authentication methods, like MD5-Challenge, PEAP, and TLS. The important thing is that the authenticator (the switch) doesn't need to know which authentication method the supplicant and the authentication server are using, or how many information exchange frames are needed for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it. When authentication is complete, the RADIUS server sends a special packet containing a success or failure indication. Besides forwarding this decision to the supplicant, the switch uses it to open up or block traffic on the switch port connected to the supplicant.

Note:
Suppose two backend servers are enabled and that the server timeout is configured to X seconds (using the AAA configuration page), and suppose that the first server in the list is currently down (but not considered dead). Now, if the supplicant retransmits EAPOL Start frames at a rate faster than X seconds, then it will never get authenticated, because the switch will cancel on-going backend authentication server requests whenever it receives a new EAPOL Start frame from the supplicant. And since the server hasn't yet failed (because the X seconds haven't expired), the same server will be contacted upon the next backend authentication server request from the switch. This scenario will loop forever. Therefore, the server timeout should be smaller than the supplicant's EAPOL Start frame retransmission rate.

- MAC-based Auth.

  Unlike port-based 802.1X, MAC-based authentication is not a standard, but merely a best-practices method adopted by the industry. In MAC-based authentication, users are called clients, and the switch acts as the supplicant on behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by the switch, which in turn uses the client's MAC address as both username and password in the subsequent EAP exchange with the RADIUS server. The 6-byte MAC address is converted to a string on the following form "xx-xx-xx-xx-xx-xx", that is, a dash (-) is used as separator between the lower-cased hexadecimal digits. The switch only supports the MD5-Challenge authentication method, so the RADIUS server must be configured accordingly.

  When authentication is complete, the RADIUS server sends a success or failure indication, which in turn causes the switch to open up or block traffic for that particular client, using the Port Security module. Only then will frames from the client be forwarded on the switch. There are no EAPOL frames involved in this authentication, and therefore, MAC-based Authentication has nothing to do with the 802.1X standard.

The advantage of MAC-based authentication over 802.1X-based authentication is that the clients don't need special supplicant software to authenticate. The disadvantage is that MAC addresses can be spoofed by malicious users - equipment whose MAC address is a valid RADIUS user can be used by anyone. Also, only the MD5-Challenge method is supported. The maximum number of clients that can be attached to a port can be limited using the Port Security Limit Control functionality.

- Single 802.1X
  In port-based 802.1X authentication, once a supplicant is successfully authenticated on a port, the whole port is opened for network traffic. This allows other clients connected to the port (for instance through a hub) to piggy-back on the successfully authenticated client and get network access even though they really aren't authenticated. To overcome this security breach, use the Single 802.1X variant.
  Single 802.1X is really not an IEEE standard, but features many of the same characteristics as does port-based 802.1X. In Single 802.1X, at most one supplicant can get authenticated on the port at a time. Normal EAPOL frames are used in the communication between the supplicant and the switch. If more than one supplicant is connected to a port, the one that comes first when the port's link comes up will be the first one considered. If that supplicant doesn't provide valid credentials within a certain amount of time, another supplicant will get a chance. Once a supplicant is successfully authenticated, only that supplicant will be allowed access. This is the most secure of all the supported modes. In this mode, the Port Security module is used to secure a supplicant's MAC address once successfully authenticated.
- Multi 802.1X
  Multi 802.1X is - like Single 802.1X - not an IEEE standard, but a variant that features many of the same characteristics. In Multi 802.1X, one or more supplicants can get authenticated on the same port at the same time. Each supplicant is authenticated individually and secured in the MAC table using the Port Security module.
  In Multi 802.1X it is not possible to use the multicast BPDU MAC address as destination MAC address for EAPOL frames sent from the switch towards the supplicant, since that would cause all supplicants attached to the port to reply to requests sent from the switch. Instead, the switch uses the supplicant's MAC address, which is obtained from the first EAPOL Start or EAPOL Response Identity frame sent by the supplicant. An exception to this is when no supplicants

are attached. In this case, the switch sends EAPOL Request Identity frames using the BPDU multicast MAC address as destination - to wake up any supplicants that might be on the port.

The maximum number of supplicants that can be attached to a port can be limited using the Port Security Limit Control functionality.

RADIUS-Assigned QoS Enabled

When RADIUS-Assigned QoS is both globally enabled and enabled (checked) on a given port, the switch reacts to QoS Class information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, traffic received on the supplicant's port will be classified to the given QoS Class. If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a QoS Class or it's invalid, or the supplicant is otherwise no longer present on the port, the port's QoS Class is immediately reverted to the original QoS Class (which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned).

This option is only available for single-client modes, i.e.

- Port-based 802.1X
- Single 802.1X

RADIUS attributes used in identifying a QoS Class:

- The User-Priority-Table attribute defined in RFC4675 forms the basis for identifying the QoS Class in an Access-Accept packet.
- Only the first occurrence of the attribute in the packet will be considered, and to be valid, it must follow this rule:
  - • All 8 octets in the attribute value must be identical and consist of ASCII characters in the range '0' - '7', which translates into the desired QoS Class in the range [0; 7].

RADIUS-Assigned VLAN Enabled

When RADIUS-Assigned VLAN is both globally enabled and enabled (checked) for a given port, the switch reacts to VLAN ID information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, the port's Port VLAN ID will be changed to this VLAN ID, the port will be set to be a member of that VLAN ID, and the port will be forced into VLAN unaware mode. Once assigned, all traffic arriving on the port will be classified and switched on the RADIUS-assigned VLAN ID.

If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a VLAN ID or it's invalid, or the supplicant is otherwise no longer present on the port, the port's VLAN ID is immediately reverted to the original VLAN ID (which may be

changed by the administrator in the meanwhile without affecting the RADIUS-assigned).

This option is only available for single-client modes, i.e.

- Port-based 802.1X
- Single 802.1X

RADIUS attributes used in identifying a VLAN ID:

RFC2868 and RFC3580 form the basis for the attributes used in identifying a VLAN ID in an Access-Accept packet. The following criteria are used:

- The Tunnel-Medium-Type, Tunnel-Type, and Tunnel-Private-Group-ID attributes must all be present at least once in the Access-Accept packet.
- The switch looks for the first set of these attributes that have the same Tag value and fulfill the following requirements (if Tag == 0 is used, the Tunnel-Private-Group-ID does not need to include a Tag):
  - Value of Tunnel-Medium-Type must be set to "IEEE-802" (ordinal 6).
  - Value of Tunnel-Type must be set to "VLAN" (ordinal 13).
  - Value of Tunnel-Private-Group-ID must be a string of ASCII chars in the range '0' - '9', which is interpreted as a decimal string representing the VLAN ID. Leading '0's are discarded. The final value must be in the range [1; 4095].

Guest VLAN Enabled

When Guest VLAN is both globally enabled and enabled (checked) for a given port, the switch considers moving the port into the Guest VLAN according to the rules outlined below.

This option is only available for EAPOL-based modes, i.e.:

- Port-based 802.1X
- Single 802.1X
- Multi 802.1X

Guest VLAN Operation:

When a Guest VLAN enabled port's link comes up, the switch starts transmitting EAPOL Request Identity frames. If the number of transmissions of such frames exceeds Max. Reauth. Count and no EAPOL frames have been received in the meanwhile, the switch considers entering the Guest VLAN. The interval between transmission of EAPOL Request Identity frames is configured with EAPOL Timeout. If Allow Guest VLAN if EAPOL Seen is enabled, the port will now be placed in the Guest VLAN. If disabled, the switch will first check its history to see if an EAPOL frame has previously been received on the port (this history is cleared if the port link goes down or the port's Admin State is changed), and if not, the port will be placed in the Guest

VLAN. Otherwise it will not move to the Guest VLAN, but continue transmitting EAPOL Request Identity frames at the rate given by EAPOL Timeout.

Once in the Guest VLAN, the port is considered authenticated, and all attached clients on the port are allowed access on this VLAN. The switch will not transmit an EAPOL Success frame when entering the Guest VLAN.

While in the Guest VLAN, the switch monitors the link for EAPOL frames, and if one such frame is received, the switch immediately takes the port out of the Guest VLAN and starts authenticating the supplicant according to the port mode. If an EAPOL frame is received, the port will never be able to go back into the Guest VLAN if the "Allow Guest VLAN if EAPOL Seen" is disabled.

Port state

The current state of the port. It can undertake one of the following values:

- Globally Disabled: NAS is globally disabled.
- Link Down: NAS is globally enabled, but there is no link on the port.
- Authorized: The port is in Force Authorized or a single-supplicant mode and the supplicant is authorized.
- Unauthorized: The port is in Force Unauthorized or a single-supplicant mode and the supplicant is not successfully authorized by the RADIUS server.
- X Auth/Y Unauth: The port is in a multi-supplicant mode. Currently X clients are authorized and Y are unauthorized.

Restart

Two buttons are available for each row. The buttons are only enabled when authentication is globally enabled and the port's Admin State is in an EAPOL-based or MAC-based mode.

Clicking these buttons will not cause settings changed on the page to take effect.

- Reauthenticate: Schedules a reauthentication whenever the quiet-period of the port runs out (EAPOL-based authentication). For MAC-based authentication, reauthentication will be attempted immediately.

  The button only has effect for successfully authenticated clients on the port and will not cause the clients to get temporarily unauthorized.
- Reinitialize: Forces a reinitialization of the clients on the port and thereby a reauthentication immediately. The clients will transfer to the unauthorized state while the reauthentication is in progress.

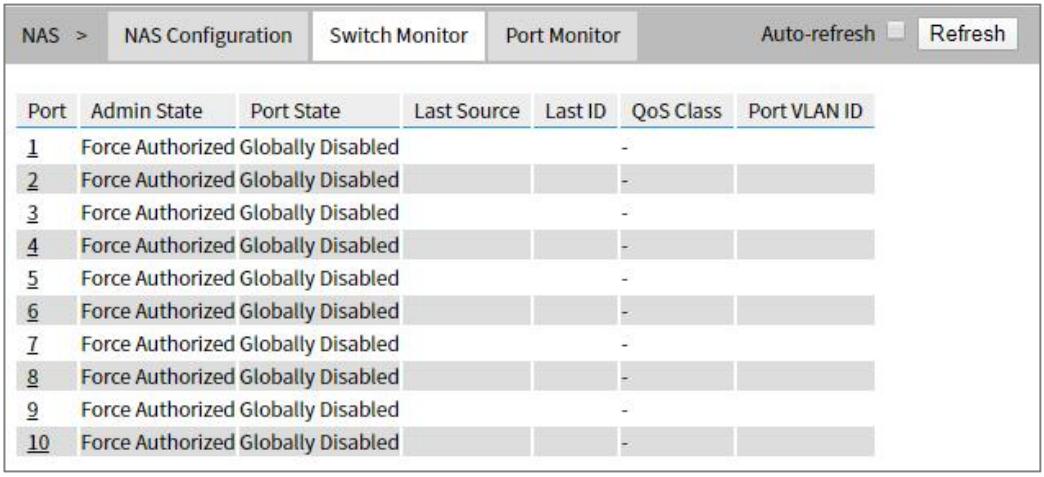
Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

5.3.2 Device Monitoring

This page provides an overview of the current NAS port states.



Port

The switch port number. Click to navigate to detailed NAS statistics for this port.

Admin State

The port's current administrative state. Refer to NAS Admin State for a description of possible values.

Port state

The current state of the port. Refer to NAS Admin State for a description of possible values.

Last Source

The source MAC address carried in the most recently received EAPOL frame for EAPOL-based authentication, and the most recently received frame from a new client for MAC-based authentication.

Last ID

The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame for EAPOL-based authentication, and the source MAC address from the most recently received frame from a new client for MAC-based authentication.

Buttons

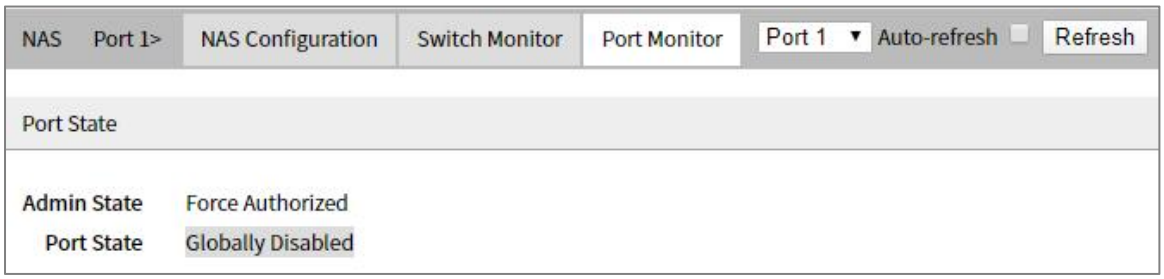
Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

5.3.3 Port Monitoring

This page provides detailed NAS statistics for a specific switch port running EAPOL-based IEEE 802.1X authentication. For MAC-based ports, it shows selected backend server (RADIUS Authentication Server) statistics, only .

Use the port select box to select which port details to be displayed.



Port state

Admin State

The port's current administrative state. Refer to NAS Configuration Admin State for a description of possible values.

Port state

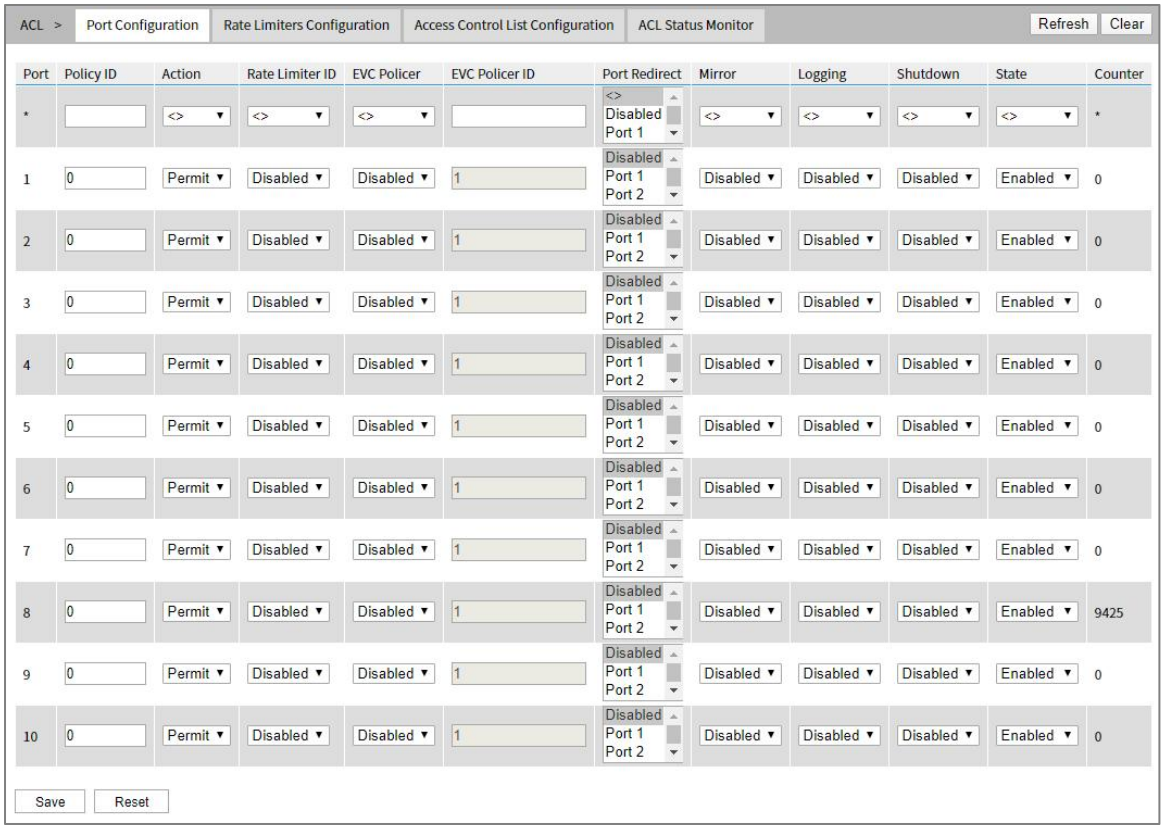
The current state of the port. Refer to NAS Configuration Admin State for a description of possible values.

5.4 ACL

The ACL(Access Control List) is a set composed of one or more rules. The device matches messages based on these rules, which can filter out specific messages and allow or prevent the messages from passing according to the processing strategy of the service module applying ACL.

5.4.1 Port Configuration

Configure the ACL parameters (ACE) of each switch port. These parameters will affect frames received on a port unless the frame matches a specific ACE.



Port

The switch port number.

Policy ID

Select the policy ID to apply to this port. The allowed values are 0 through 255. The default value is 0.

Action

Select whether forwarding is permitted ("Permit") or denied ("Deny"). The default value is "Permit".

Rate Limiter ID

Select which rate limiter ID to apply on this port. The allowed values are Disabled or the values 1 through 16. The default value is "Disabled".

EVC Policer

Select whether EVC policer is enabled or disabled. The default value is "Disabled". Note that ACL rate limiter and EVC policer can not both be enabled.

EVC Policer ID

Select which EVC policer ID to apply on this port. The allowed values are Disabled or the values 1 through 256.

Port Redirect

Select which port frames are redirected on. Frames matching the ACE are redirected to the specified port. The allowed values are “Disabled” or the specified port number. This parameter cannot be set when the operation is set to ”Allowed”. The default value is "Disabled".

Mirroring

Specify the mirror operation of this port. The allowed values are:

- Enabled: Frames received on the port are mirrored. Frames matching the ACE are mirrored to the destination mirror port.
- Disabled: Frames received on the port are not mirrored.

The default value is "Disabled".

Logging

Specify the logging operation of this port. Notice that the logging message doesn't include the 4 bytes CRC. The allowed values are:

- Enabled: Frames matching the ACE received on the port are stored in the Log.
- Disabled: Frames received on the port are not logged.

The default value is "Disabled".

Note:

The logging feature only works when the packet length is less than 1518(without VLAN tags) and the System Log memory size and logging rate is not limited.

Shutdown

Specify the port shut down operation of this port. The allowed values are:

- Enabled: If a frame matching the ACE is received on the port, the port will be disabled.
- Disabled: Port shut down is disabled.

The default value is "Disabled".

Note

Only when the packet length is less than 1518 (without VLAN tag), the port shutdown function is effective.

Status

Specify the port state of this port. The allowed values are:

- Enabled: To reopen ports by changing the volatile port configuration of the ACL user module.
- Disabled: To close ports by changing the volatile port configuration of the ACL user module.

The default value is "Enabled".

Counter

Counts the number of frames that match this ACE.

Buttons

Save: Click to save changes.

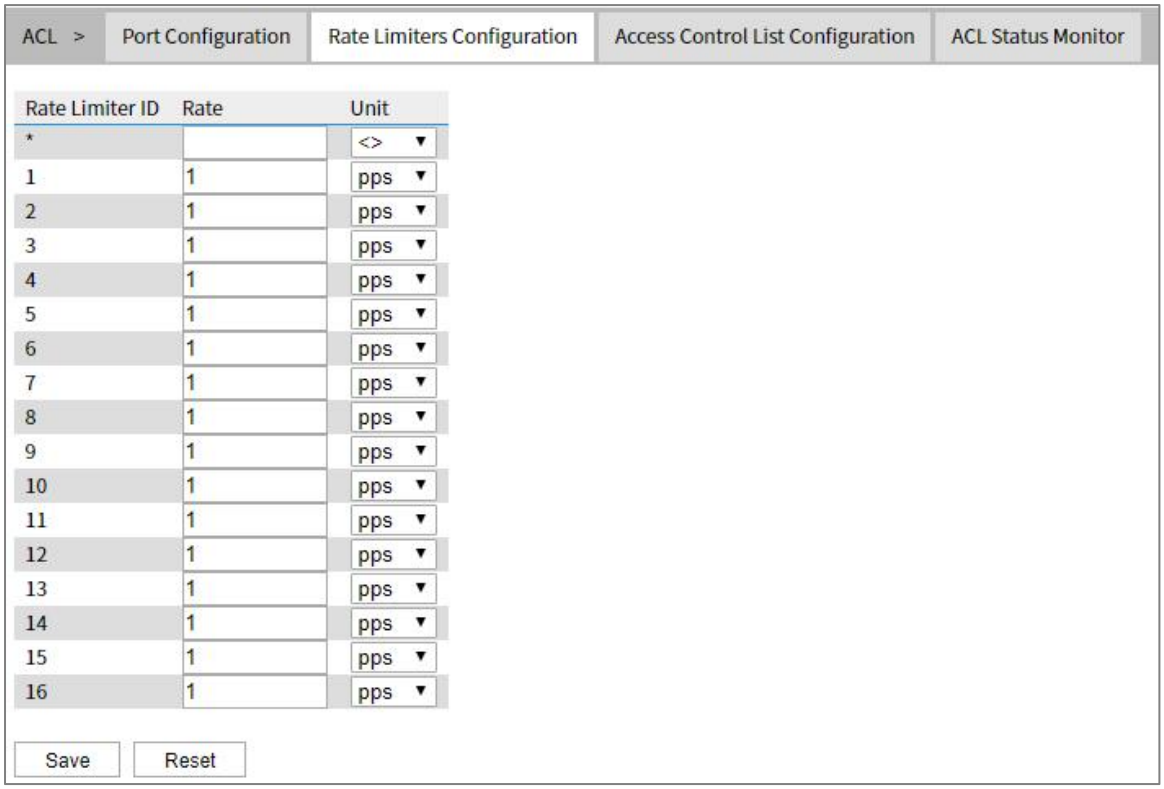
Reset: Click to undo any changes made locally and revert to previously saved values.

Refresh: Click to refresh the page; any changes made locally will be undone.

Clear: Click to clear the counters.

5.4.2 Rate Limiter Configuration

Configure the rate limiter for the ACL of the switch.



Rate Limiter ID

The rate limiter ID for the settings contained in the same row and its range is 1 to 16.

Rate

The valid rate is 0-3276700pps.

Or 0,100,200,300, ..., 1000000kbps.

Unit

Specify the rate unit. The allowed values are:

- pps: packets per second.
- kbps: kbits per second.

Buttons

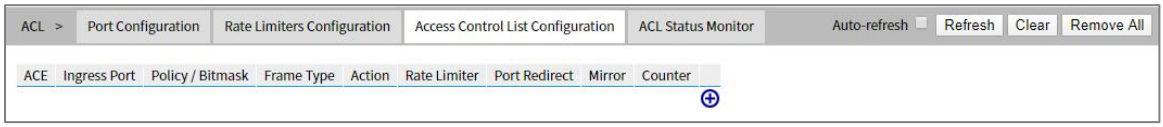
Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

5.4.3 Access Control List Configuration

This page shows the Access Control List (ACL), which is made up of the ACEs defined on this switch. Each row describes the ACE that is defined. The maximum number of ACEs is 256 on each switch.

Click on the lowest plus sign to add a new ACE to the list. The reserved ACEs used for internal protocol, cannot be edited or deleted, the order sequence cannot be changed and the priority is highest.



ACE

Indicates the ACE ID.

Egress Port

The ingress port of the ACE. Possible values are:

- All: The ACE will match all ingress port.
- Port number: The ACE will match a specific ingress port.

Policy / Bitmask

Displays the policy number and bitmask of ACE.

Frame Type

Indicates the frame type of the ACE. Possible values are:

- Any: The ACE will match any frame type.
- EType: The ACE will match Ethernet Type frames.

  Note:
  Ethernet Type based ACE will not get matched by IP and ARP frames.
- ARP: The ACE will match ARP/RARP frames.
- IPv4: The ACE will match all IPv4 frames.
- IPv4/ICMP: The ACE will match IPv4 frames with ICMP protocol.
- IPv4/UDP: The ACE will match IPv4 frames with UDP protocol.
- IPv4/TCP: The ACE will match IPv4 frames with TCP protocol.
- IPv4/Other: The ACE will match IPv4 frames, which are not ICMP/UDP/TCP.

- IPv6: The ACE will match all IPv6 standard frames.

Action

Indicates the forwarding action of the ACE.

- Permit: Frames matching the ACE may be forwarded and learned.
- Deny: Frames matching the ACE are dropped.
- Filter: Frames matching the ACE are filtered.

Rate Limiter

Indicates the rate limiter number of the ACE. The allowed range is 1 to 16. When Disabled is displayed, the rate limiter operation is disabled.

Mirror port

Indicates the port redirect operation of the ACE. Frames matching the ACE are redirected to the port number. The allowed values are Disabled or a specific port number. When Disabled is displayed, the port redirect operation is disabled.

Mirroring

Specify the mirror operation of this port. Frames matching the ACE are mirrored to the destination mirror port. The allowed values are:

- Enabled: Frames received on the port are mirrored.
- Disabled: Frames received on the port are not mirrored.

The default value is "Disabled".

Counter

The counter indicates the number of times the ACE was hit by a frame.

Modification Buttons

You can modify each ACE (Access Control Entry) in the table using the following buttons:

Add: Insert a new ACE before the current row.

Edit: Edit the ACE row.

Up: move ACE up to the list.

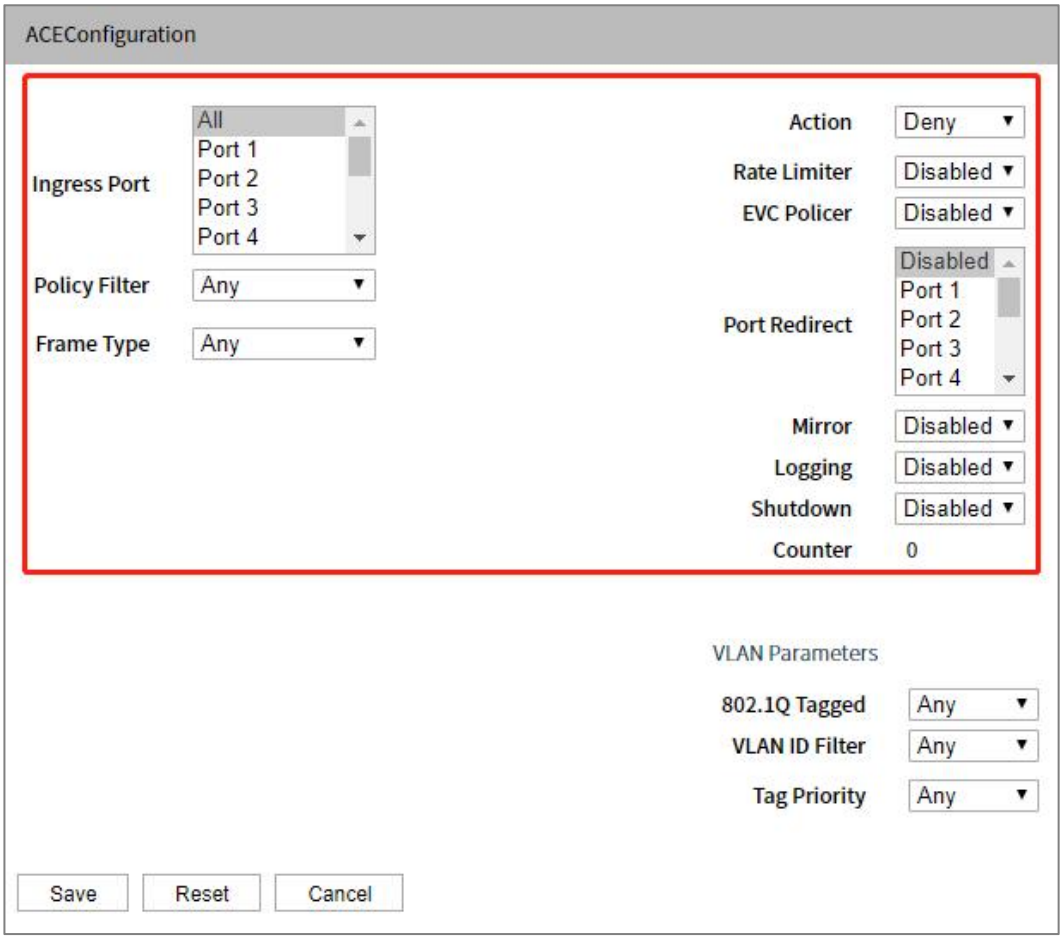
Down: move ACE down to the list.

Delete: delete ACE.

Add: The lowest plus sign adds a new entry at the bottom of the ACE listings.

ACE Configuration

Click the “” icon to enter ACE (Access Control Entry) configuration page.



An ACE consists of several parameters. These parameters vary according to the frame type that you select. First select the ingress port for the ACE, and then select the frame type. Different parameter options are displayed depending on the frame type selected.

A frame that hits this ACE matches the configuration that is defined here.

Ingress Port

Select the ingress port for which this ACE applies.

- All: The ACE applies to all port.
- Port n: The ACE applies to this port number, where n is the number of the switch port.

Policy Filter

Specify the policy number filter for this ACE.

- Any: No policy filter is specified. (policy filter status is "don't-care".)
- Specific: If you want to filter a specific policy with this ACE, choose this value. Two field for entering an policy value and bitmask appears.

Policy Value

When "Specific" is selected for the policy filter, you can enter a specific policy value. The allowed range is 0 to 255.

Policy / Bitmask

When "Specific" is selected for the policy filter, you can enter a specific policy bitmask. The allowed range is 0x0 to 0xff. Notice the usage of bitmask, if the binary bit value is "0", it means this bit is "don't-care". The real matched pattern is [policy_value & policy_bitmask]. For example, if the policy value is 3 and the policy bitmask is 0x10(bit 0 is "don't-care" bit), then policy 2 and 3 are applied to this rule.

Frame Type

Select the frame type for this ACE. These frame types are mutually exclusive.

- Any: Any frame can match this ACE.
- Ethernet Type: Only Ethernet Type frames can match this ACE. The IEEE 802.3 describes the value of Length/Type Field specifications to be greater than or equal to 1536 decimal (equal to 0600 hexadecimal) and the value should not be equal to 0x800(IPv4), 0x806(ARP) or 0x86DD(IPv6).
- ARP: Only ARP frames can match this ACE. Notice the ARP frames won't match the ACE with ethernet type.
- IPv4: Only IPv4 frames can match this ACE. Notice the IPv4 frames won't match the ACE with ethernet type.
- IPv6: Only IPv6 frames can match this ACE. Notice the IPv6 frames won't match the ACE with ethernet type.

Action

Specify the action to take with a frame that hits this ACE.

- Permit: The frame that hits this ACE is granted permission for the ACE operation.
- Deny: The frame that hits this ACE is dropped.
- Filter: Frames matching the ACE are filtered.

Rate Limiter

Specify the rate limiter in number of base units. The allowed range is 1 to 16. “Disabled” indicates that the rate limiter operation is disabled.

EVC Policer

Select whether EVC policer is enabled or disabled. The default value is "Disabled". Note that ACL rate limiter and EVC policer can not both be enabled.

EVC Policer ID

Select which EVC policer ID to apply on this port. The allowed values are Disabled or the values 1 through 256.

Port Redirect

Frames that hit the ACE are redirected to the port number specified here. The rate limiter will affect these ports. The allowed range is the same as the switch port number range. “Disabled” indicates that the port redirect operation is disabled and the specific port number of 'Port Redirect' can't be set when “Action” is “Permit”.

Mirror

Specify the mirror operation of this port. Frames matching the ACE are mirrored to the destination mirror port. The rate limiter will not affect frames on the mirror port. The allowed values are:

- Enabled: Frames received on the port are mirrored.
- Disabled: Frames received on the port are not mirrored.

The default value is “Disabled”.

Logging

Specify the logging operation of the ACE. Notice that the logging message doesn't include the 4 bytes CRC information. The allowed values are:

- Enabled: Frames matching the ACE are stored in the System Log.
- Disabled: Frames matching the ACE are not logged.

  Note:
  The logging feature only works when the packet length is less than 1518(without VLAN tags) and the System Log memory size and logging rate is not limited.

Shutdown

Specify the port shut down operation of the ACE. The allowed values are:

- Enabled: If a frame matches the ACE, the ingress port will be disabled.
- Disabled: Port shut down is disabled for the ACE.

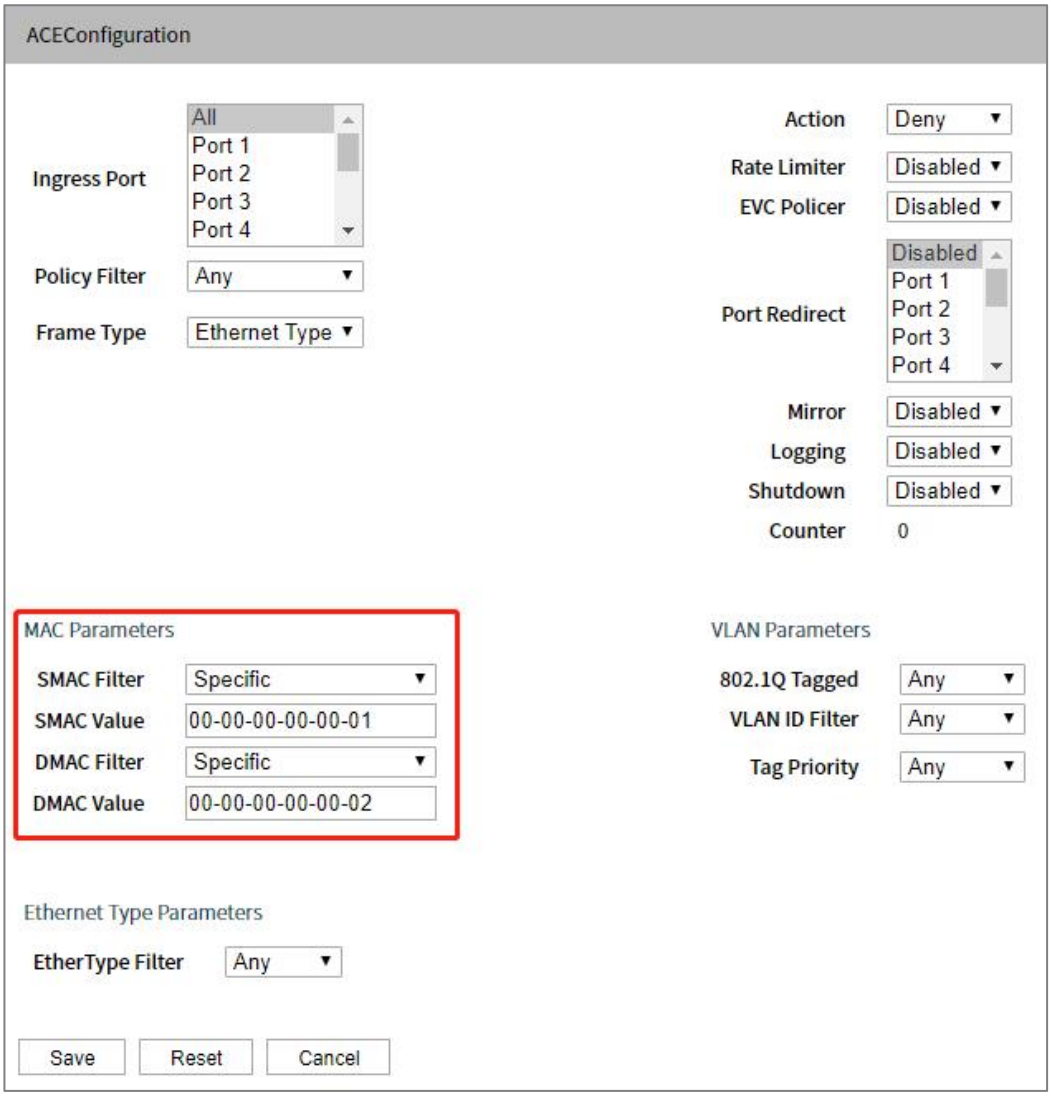
  Note:
  Only when the packet length is less than 1518 (without VLAN tag), the port shutdown function is effective.

Counter

The counter indicates the number of times the ACE was hit by a frame.

MAC Parameters

MAC parameters are displayed only when the frame type is "Ethernet type" or "ARP".



SMAC Filter

Specify the source MAC filter for this ACE.

- Any: No SMAC filter is specified. (SMAC filter status is "don't-care".)
- Specific: If you want to filter a specific source MAC address with this ACE, choose this value. A field for entering an SMAC value appears.

SMAC Value

When "Specific" is selected for the SMAC filter, you can enter a specific source MAC address. The legal format is "xx-xx-xx-xx-xx-xx" or "xx.xx.xx.xx.xx.xx" or "xxxxxxxxxxxx" (x is a hexadecimal digit). A frame that hits this ACE matches this SMAC value.

DMAC Filter

Specify the destination MAC filter for this ACE.

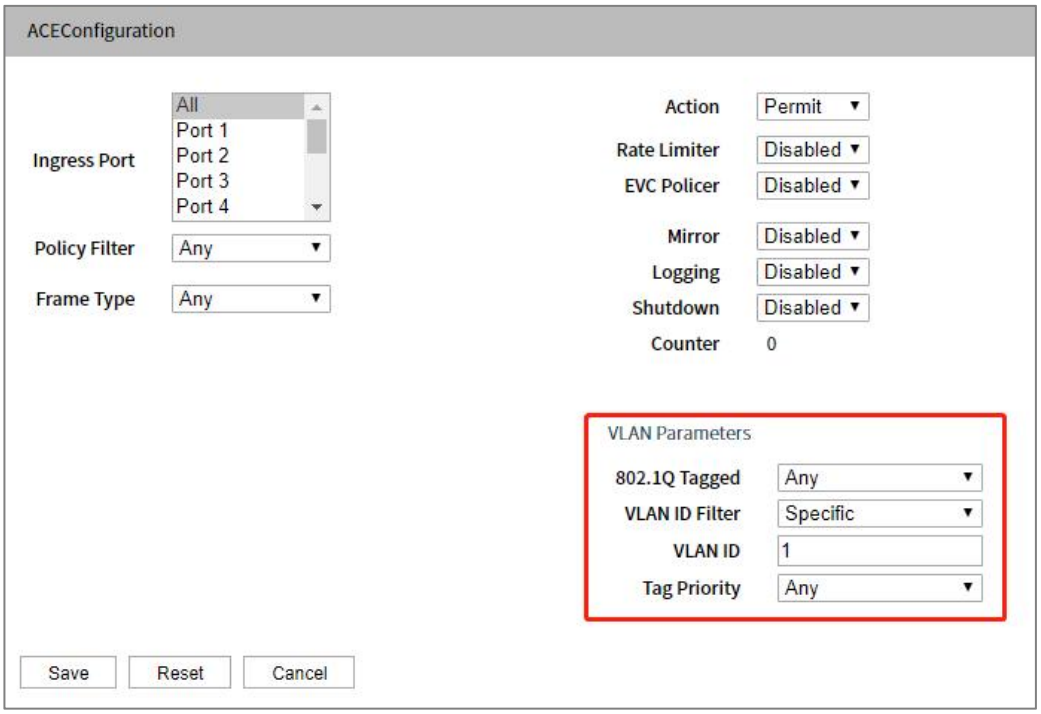
- Any: No DMAC filter is specified. (DMAC filter status is "don't-care".)
- MC: Frame must be multicast.

- BC: Frame must be broadcast.
- UC: Frame must be unicast.
- Specific: If you want to filter a specific destination MAC address with this ACE, choose this value. A field for entering an DMAC value appears.

DMAC Value

When "Specific" is selected for the DMAC filter, you can enter a specific destination MAC address. The legal format is "xx-xx-xx-xx-xx-xx" or "xx.xx.xx.xx.xx.xx" or "xxxxxxxxxxxx" (x is a hexadecimal digit). A frame that hits this ACE matches this DMAC value.

VLAN Parameters



802.1Q Tagged

Specify whether frames can hit the action according to the 802.1Q tagged. The allowed values are:

- Any: Any value is allowed ("don't-care").
- Enabled: tagged frames only.
- Disabled: Untagged frame only.

The default value is 'Any'.

VLAN ID Filter

Specify the VLAN ID filter for this ACE.

- Any: No VLAN ID filter is specified. (VLAN ID filter status is "don't-care".)
- Specific: If you want to filter a specific VLAN ID with this ACE, choose this value.

A field for entering a VLAN ID number appears.

VLAN ID

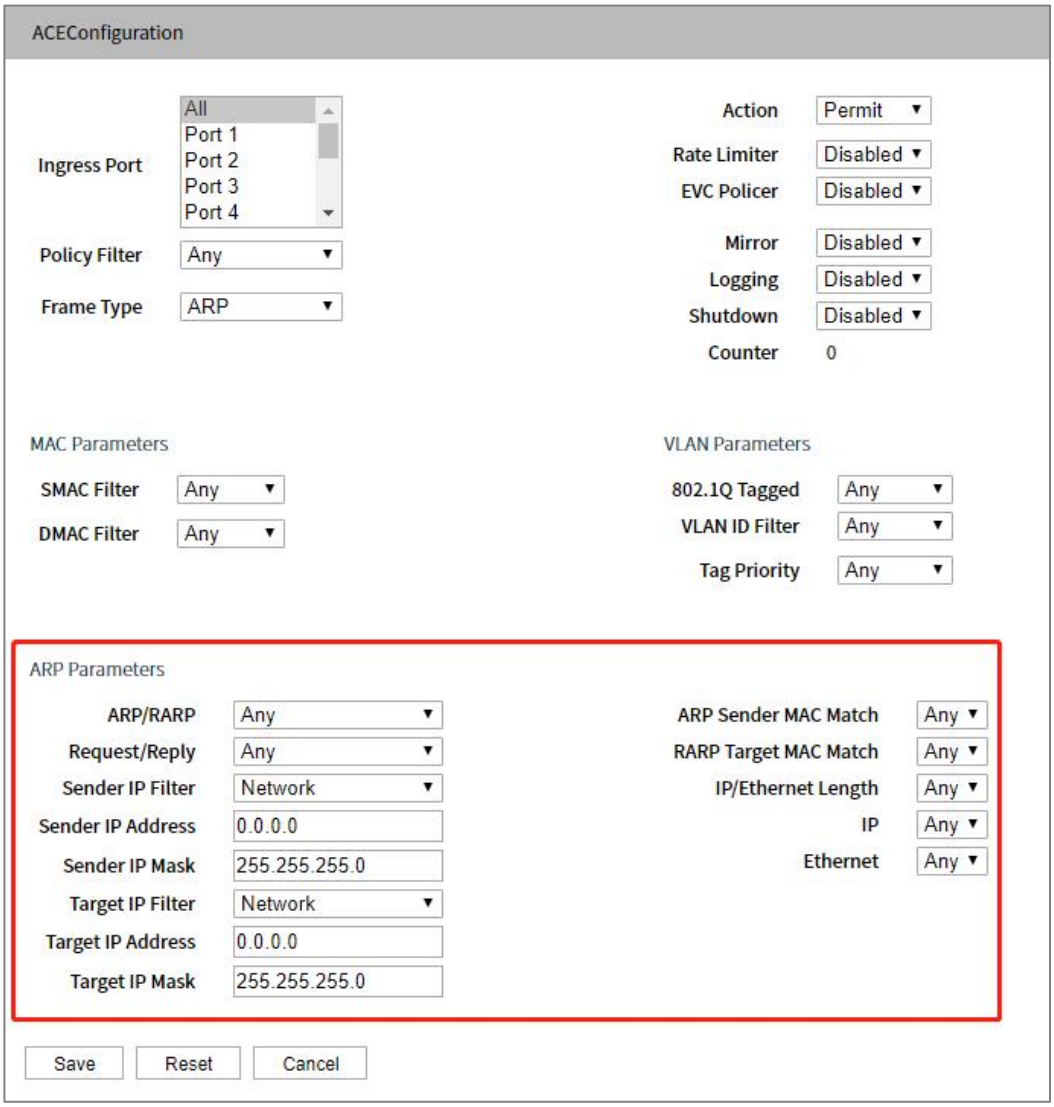
When "Specific" is selected for the VLAN ID filter, you can enter a specific VLAN ID number. The allowed range is 1 to 4095. A frame that hits this ACE matches this VLAN ID value.

Tag Priority

Specify the tag priority for this ACE. A frame that hits this ACE matches this tag priority. The allowed number range is 0 to 7 or range 0-1, 2-3, 4-5, 6-7, 0-3 and 4-7. The value Any means that no tag priority is specified (tag priority is "don't-care".)

ARP Parameters

The ARP parameters can be configured when Frame Type "ARP" is selected.



ARP/RARP

Specify the available ARP/RARP opcode (OP) flag for this ACE.

- Any: no ARP / RARP opcode flag specified. (The opcode is "don't-care".)
- ARP: Frame must have ARP opcode set to ARP.
- RARP: Frame must have RARP opcode set to RARP.
- Other: Frame has unknown ARP/RARP Opcode flag.

Request/Reply

Specify the available Request/Reply opcode (OP) flag for this ACE.

- Any: No Request/Reply OP flag is specified. (OP is "don't-care".)
- Request: Frame must have ARP Request or RARP Request OP flag set.
- Reply: Frame must have ARP Reply or RARP Reply OP flag.

Sender IP Filter

Specify the sender IP filter for this ACE.

- Any: No sender IP filter is specified. (Sender IP filter is "don't-care".)
- Host: Sender IP filter is set to Host. Specify the sender IP address in the Sender IP Address field that appears.
- Network: Sender IP filter is set to Network. Specify the sender IP address and sender IP mask in the "Sender IP Address" and "Sender IP Mask" fields that appear.

Sender IP Address

When "Host" or "Network" is selected for the sender IP filter, you can enter a specific sender IP address in dotted decimal notation. Notice the invalid IP address configuration is acceptable too, for example, 0.0.0.0. Normally, an ACE with invalid IP address will explicitly adding deny action.

Sender IP Mask

When "Network" is selected for the sender IP filter, you can enter a specific sender IP mask in dotted decimal notation.

Target IP Filter

Specify the target IP filter for this specific ACE.

- Any: No target IP filter is specified. (Target IP filter is "don't-care".)
- Host: Target IP filter is set to Host. Specify the target IP address in the "Target IP Address" field that appears.
- Network: Target IP filter is set to "Network". Specify the target IP address and target IP mask in the "Target IP Address" and "Target IP Mask" fields that appear.

Target IP Address

When "Host" or "Network" is selected for the target IP filter, you can enter a specific target IP address in dotted decimal notation. Notice the invalid IP address

configuration is acceptable too, for example, 0.0.0.0. Normally, an ACE with invalid IP address will explicitly adding deny action.

Target IP Mask

When "Network" is selected for the target IP filter, you can enter a specific target IP mask in dotted decimal notation.

ARP Sender MAC Match

Specify whether frames can hit the action according to their sender hardware address field (SHA) settings.

- 0: ARP frames where SHA is not equal to the SMAC address.
- 1: ARP frames where SHA is equal to the SMAC address.
- Any: Any value is allowed ("don't-care").

RARP Target MAC Match

Specify whether frames can hit the action according to their target hardware address field (THA) settings.

- 0: RARP frames where THA is not equal to the target MAC address.
- 1: RARP frames where THA is equal to the target MAC address.
- Any: Any value is allowed ("don't-care").

IP/Ethernet Length

Specify whether frames can hit the action according to their ARP/RARP hardware address length (HLN) and protocol address length (PLN) settings.

- 0: ARP/RARP frames where the HLN is not equal to Ethernet (0x06) or the (PLN) is not equal to IPv4 (0x04).
- 1: ARP/RARP frames where the HLN is equal to Ethernet (0x06) and the (PLN) is equal to IPv4 (0x04).
- Any: Any value is allowed ("don't-care").

IP

Specify whether frames can hit the action according to their ARP/RARP hardware address space (HRD) settings.

- 0: ARP/RARP frames where the HRD is not equal to Ethernet (1).
- 1: ARP/RARP frames where the HRD is equal to Ethernet (1).
- Any: Any value is allowed ("don't-care").

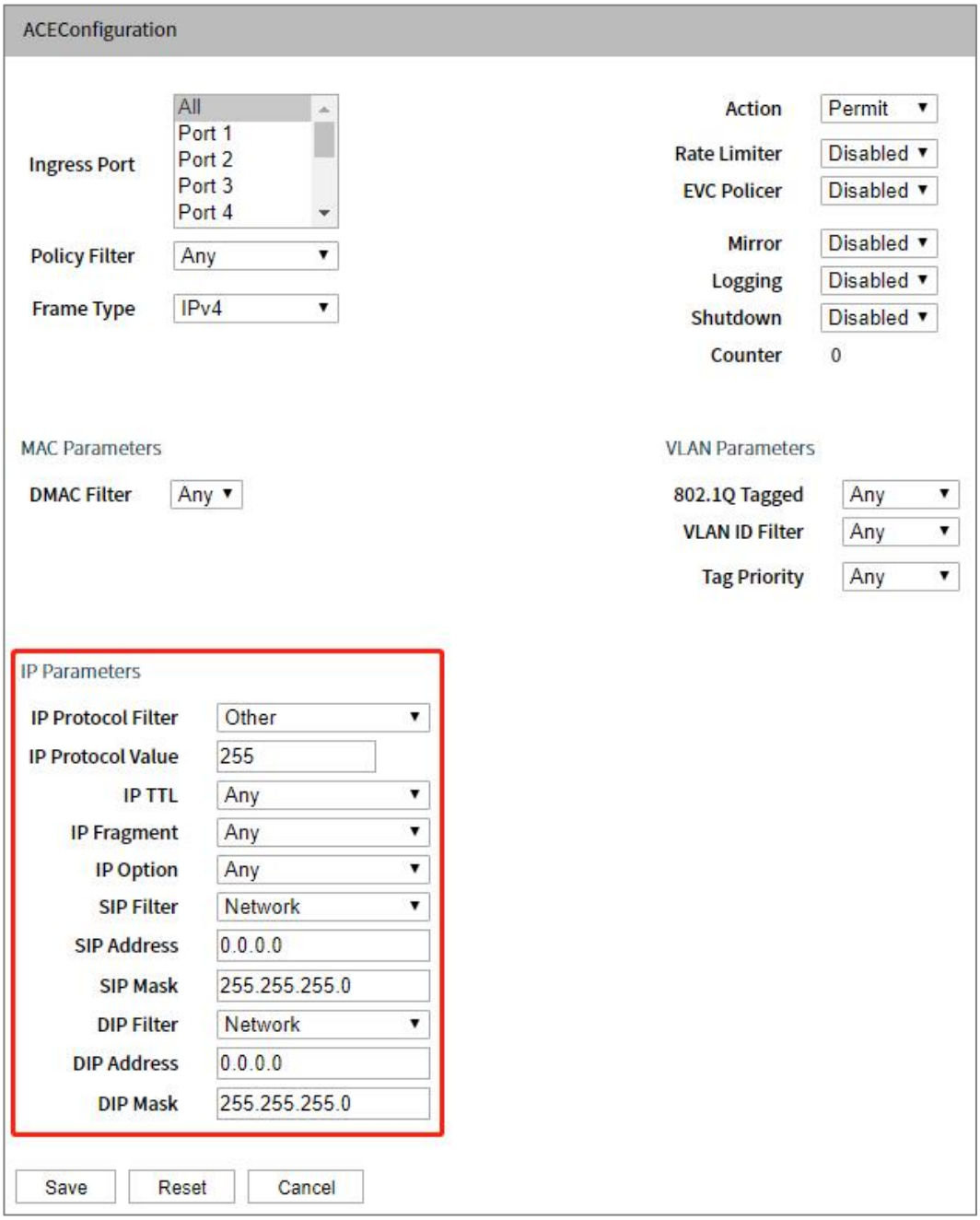
Ethernet

Specify whether frames can hit the action according to their ARP/RARP protocol address space (PRO) settings.

- 0: ARP/RARP frames where the PRO is not equal to IP (0x800).
- 1: ARP/RARP frames where the PRO is equal to IP (0x800).
- Any: Any value is allowed ("don't-care").

IP Parameters

The IP parameters can be configured when Frame Type "IPv4" is selected.



IP Protocol Filter

Specify the IP protocol filter for this ACE.

- Any: No IP protocol filter is specified ("don't-care").
- Other: If you want to filter a specific IP protocol filter with this ACE, choose this value. A field for entering an IP Protocol Value filter appears.
- ICMP: Select ICMP to filter IPv4 ICMP protocol frames. Extra fields for defining ICMP parameters will appear. These fields are explained later in this help file.

- UDP: Select UDP to filter IPv4 UDP protocol frames. Extra fields for defining UDP parameters will appear. These fields are explained later in this help file.
- TCP: Select TCP to filter IPv4 TCP protocol frames. Extra fields for defining TCP parameters will appear. These fields are explained later in this help file.

IP Protocol Value

When "Other" is selected for the IP protocol value, you can enter a specific value. The allowed range is 0 to 255. A frame that hits this ACE matches this IP protocol value.

IP TTL

Specify the Time-to-Live settings for this ACE.

- Zero: IPv4 frames with a Time-to-Live field greater than zero must not be able to match this entry.
- non-zero: IPv4 frames with a Time-to-Live field greater than zero must be able to match this entry.
- Any: Any value is allowed ("don't-care").

IP Fragment

Specify the fragment offset settings for this ACE. This involves the settings for the More Fragments (MF) bit and the Fragment Offset (FRAG OFFSET) field for an IPv4 frame.

- No: IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must not be able to match this entry.
- Yes: IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must be able to match this entry.
- Any: Any value is allowed ("don't-care").

IP Option

Specify the options flag setting for this ACE.

- No: IPv4 frames where the options flag is set must not be able to match this entry.
- Yes: IPv4 frames where the options flag is set must be able to match this entry.
- Any: Any value is allowed ("don't-care").

SIP Filter

Specify the source IP filter for this ACE.

- Any: No source IP filter is specified. (Source IP filter is "don't-care".)
- Host: Source IP filter is set to "Host". Specify the source IP address in the "SIP Address" field that appears.
- Network: Source IP filter is set to "Network". Specify the source IP address and source IP mask in the "SIP Address" and "SIP Mask" fields that appear.

SIP Address

When "Host" or "Network" is selected for the source IP filter, you can enter a specific SIP address in dotted decimal notation. Notice the invalid IP address configuration is acceptable too, for example, 0.0.0.0. Normally, an ACE with invalid IP address will explicitly adding deny action.

SIP Mask

When "Network" is selected for the source IP filter, you can enter a specific SIP mask in dotted decimal notation.

DIP Filter

Specify the destination IP filter for this ACE.

- Any: No destination IP filter is specified. (Destination IP filter is "don't-care".)
- Host: Destination IP filter is set to "Host". Specify the destination IP address in the "DIP Address" field that appears.
- Network: Destination IP filter is set to Network. Specify the destination IP address and destination IP mask in the "DIP Address" and "DIP Mask" fields that appear.

DIP Address

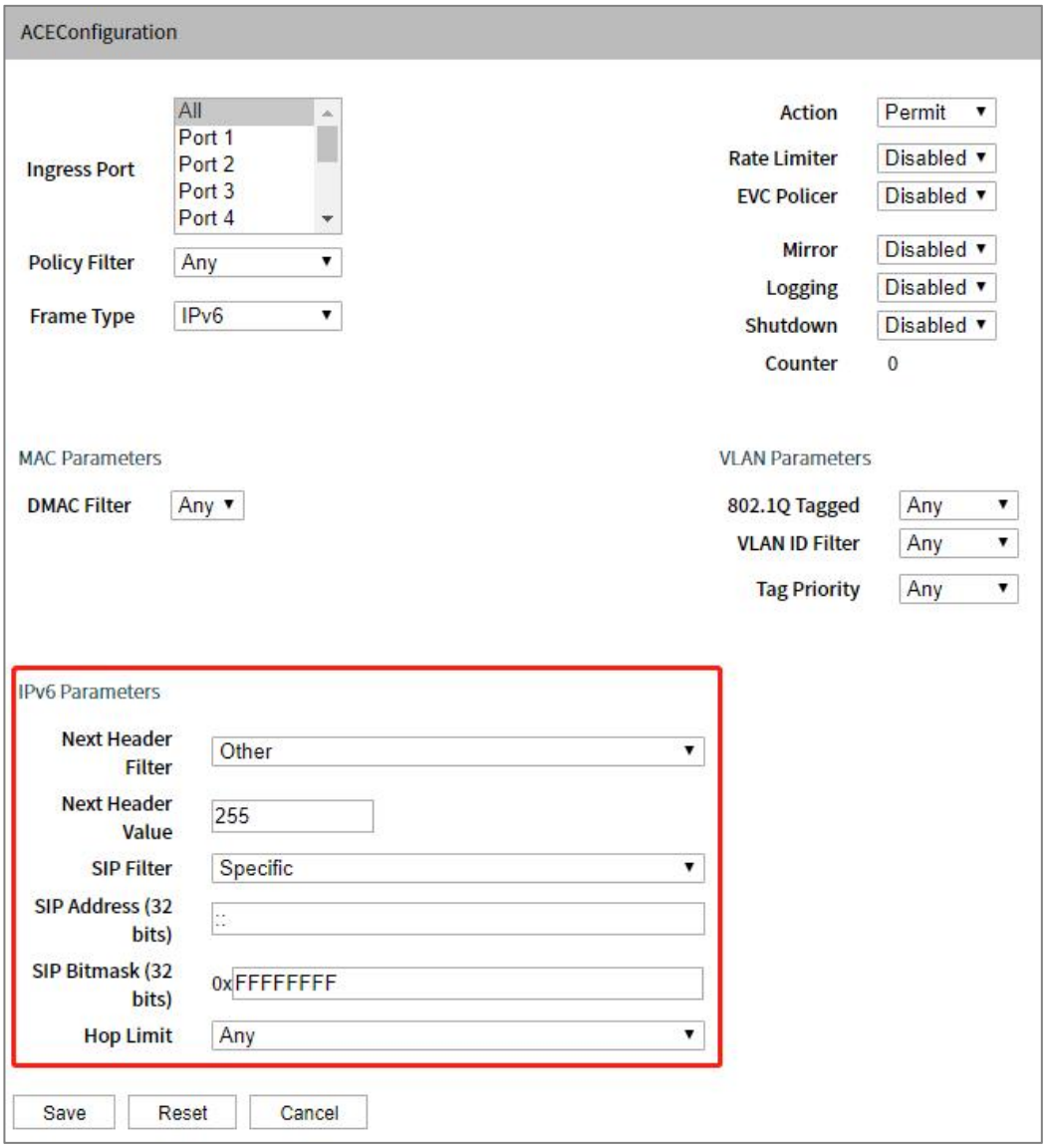
When "Host" or "Network" is selected for the destination IP filter, you can enter a specific DIP address in dotted decimal notation. Notice the invalid IP address configuration is acceptable too, for example, 0.0.0.0. Normally, an ACE with invalid IP address will explicitly adding deny action.

DIP Mask

When "Network" is selected for the destination IP filter, you can enter a specific DIP mask in dotted decimal notation.

IPv6 Parameter

The IPv6 parameters can be configured when Frame Type "IPv6" is selected.



Next Header Filter

Specify the IPv6 Next Header filter for this ACE.

- Any: No IP IPv6 Next Header filter is specified ("don't-care").
- Other: If you want to filter a specific IPv6 Next Header filter with this ACE, choose this value. A field for entering an “IPv6 Next Header” filter appears.
- ICMP: Select ICMP to filter IPv6 ICMP protocol frames. Extra fields for defining ICMP parameters will appear. These fields are explained later in this help file.
- UDP: Select UDP to filter IPv6 UDP protocol frames. Extra fields for defining UDP parameters will appear. These fields are explained later in this help file.
- TCP: Select TCP to filter IPv6 TCP protocol frames. Extra fields for defining TCP parameters will appear. These fields are explained later in this help file.

Next Header Value

You can enter a specified value for IPv6 Next Header when “Other” was selected. The allowed range is 0 to 255. A frame that hits this ACE matches this IPv6 protocol value.

SIP Filter

Specify the source IPv6 filter for this ACE.

- Any: No source IPv6 filter is specified. (Source IPv6 filter is "don't-care".)
- Specific: set source IPv6 filter to network. Specify the source IPv6 address and source IPv6 mask in the "SIP Address" and "SIP Mask" fields that appear.

SIP Address (32bits)

When "Specific" is selected for the SIPv6 filter, you can enter a specific SIPv6 address. Only support the last 32 bits of the IPv6 source address.

SIP Bitmask (32Bits)

When "Specific" is selected for the SIPv6 filter, you can enter a specific SIPv6 bitmask. Only support the last 32 bits of the IPv6 source address. Notice the usage of bitmask, if the binary bit value is "0", it means this bit is "don't-care". The real matched pattern is [sipv6_address & sipv6_bitmask]（ Last 32bits）. E.g. If SIPv6 address is 2001::3, SIPv6 bitmask is 0xFFFFFE (bit 0 is "don't-care" bit), SIPv6 address 2001::2 and 2001::3 will apply this rule.

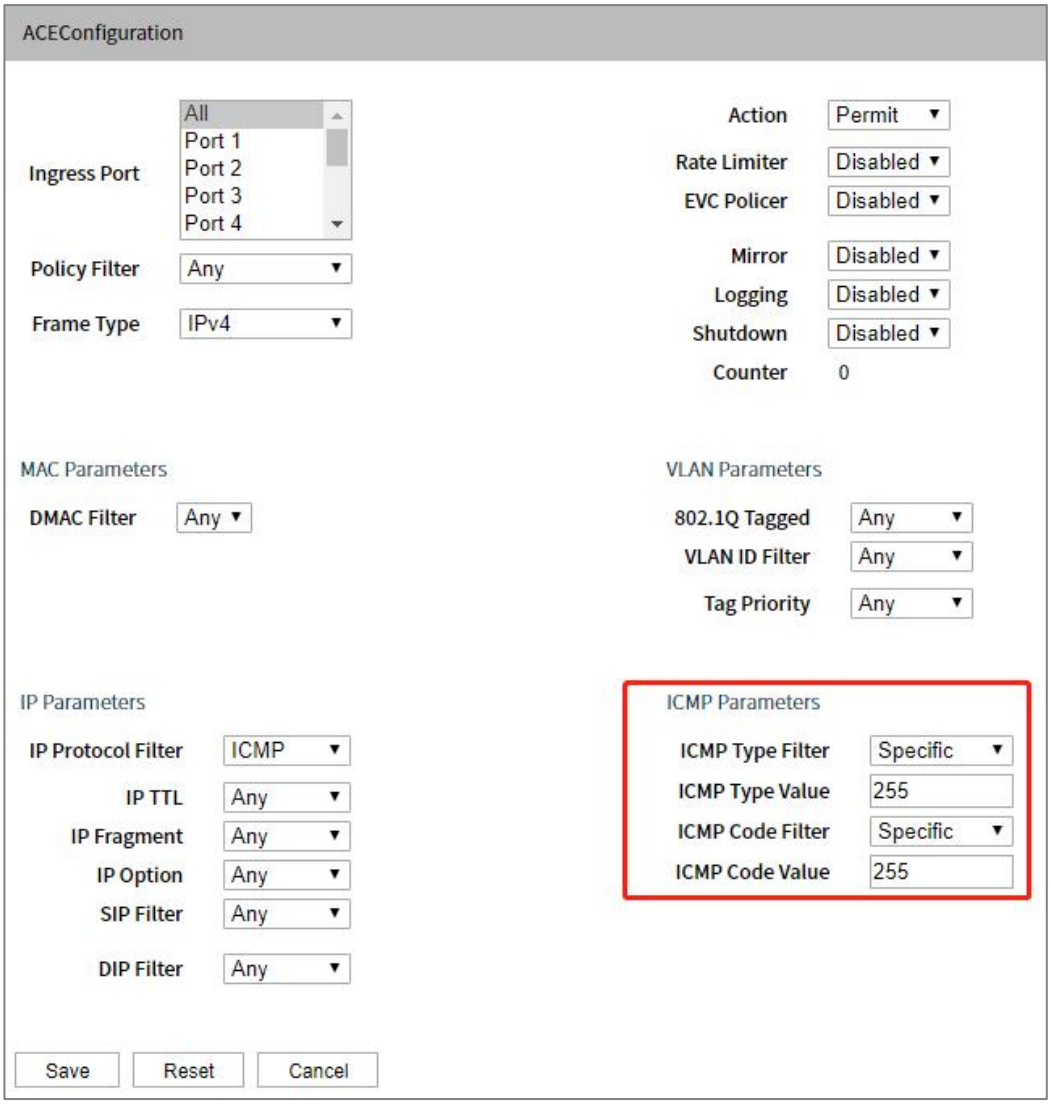
Hop Limit

Specify the Hop limit settings for this ACE.

- 0: Hop limits that IPv6 frames with field greater than zero cannot match this entry.
- 1: Hop limits that IPv6 frames with field greater than zero must match this entry.
- Any: any value is allowed ("don't care").

ICMP Parameters

When "Frame Type" is "IPv4" and "IP Protocol Filter" is "ICMP", the "ICMP Parameter" configuration is displayed.



ICMP Type Filter

Specify the ICMP filter for this ACE.

- Any: No IP protocol ICMP filter is specified (ICMP filter status is "don't-care").
- Specific: If you want to filter a specific ICMP filter with this ACE, you can enter a specific ICMP value. A field for entering a "ICMP Type Value" appears.

ICMP Type Value

When "Specific" is selected for the ICMP filter, you can enter a specific ICMP value. The allowed range is 0 to 255. A frame that hits this ACE matches this ICMP value.

ICMP Code Filter

Specify the ICMP code filter for this ACE.

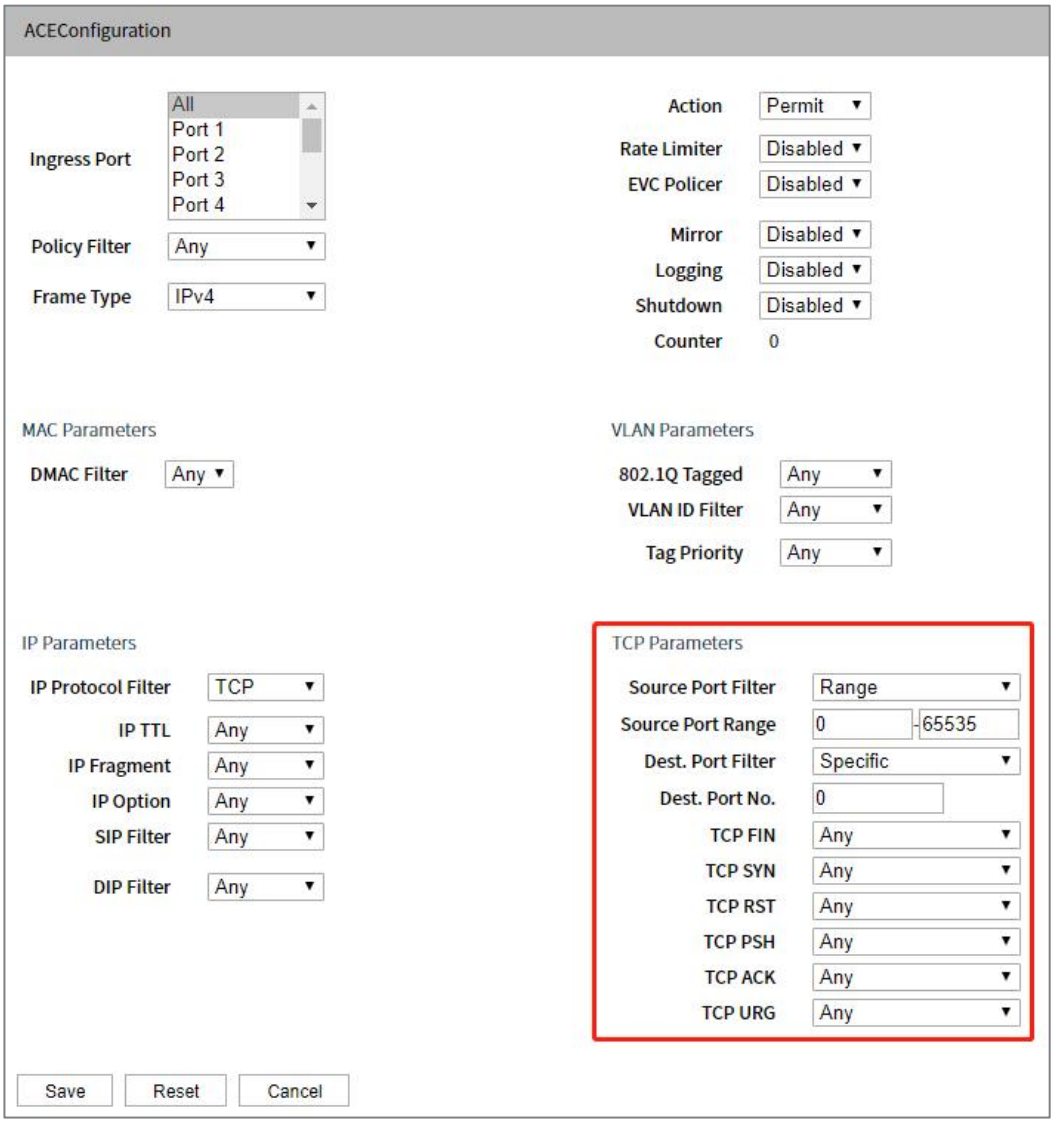
- Any: No ICMP code filter is specified (ICMP code filter status is "don't-care").
- Specific: If you want to filter a specific ICMP code filter with this ACE, you can enter a specific ICMP code value. A field for entering a ICMP Code Value appears.

ICMP Code Value

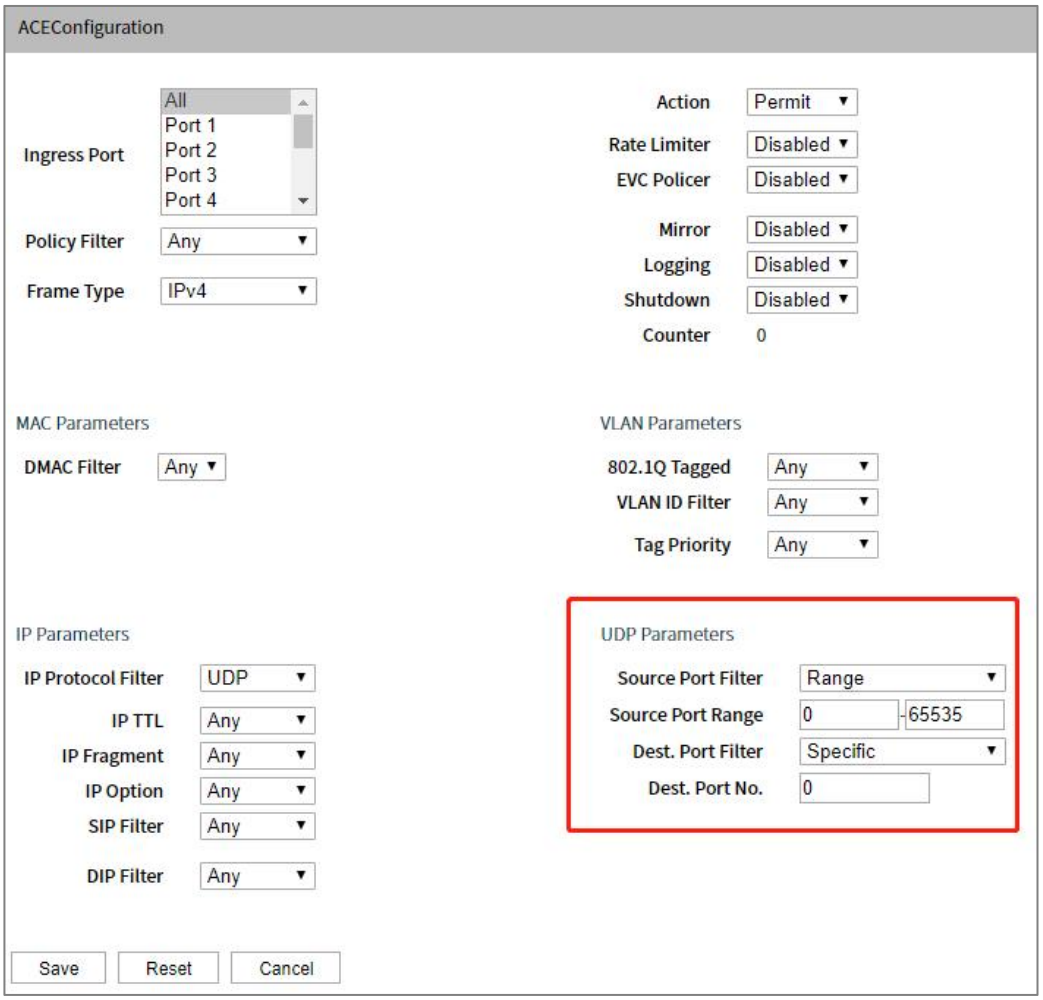
When "Specific" is selected for the ICMP code filter, you can enter a specific ICMP code value. The allowed range is 0 to 255. A frame that hits this ACE matches this ICMP code value.

TCP/UDP Parameters

When "Frame Type" is "IPv4" and "IP Protocol Filter" is "TCP", the "TCP Parameter" configuration is displayed.



When "Frame Type" is "IPv4" and "IP Protocol Filter" is "UDP", the "UDP Parameter" configuration is displayed.



TCP/UDP Source Port Filter

Specify the TCP/UDP source filter for this ACE.

- Any: No TCP/UDP source filter is specified (TCP/UDP source filter status is "don't-care").
- Specific: If you want to filter a specific TCP/UDP source filter with this ACE, you can enter a specific TCP/UDP source value. A field for entering a TCP/UDP source value appears.
- Range: If you want to filter a specific TCP/UDP source range filter with this ACE, you can enter a specific TCP/UDP source range value. A field for entering a TCP/UDP source value appears.

TCP/UDP Source Port No.

When "Specific" is selected for the TCP/UDP source filter, you can enter a specific TCP/UDP source value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP source value.

TCP/UDP Source Port Range

When "Range" is selected for the TCP/UDP source filter, you can enter a specific TCP/UDP source range value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP source value.

TCP/UDP Dest. Port Filter

Specify the TCP/UDP destination filter for this ACE.

- Any: No TCP/UDP destination filter is specified (TCP/UDP destination filter status is "don't-care").
- Specific: If you want to filter a specific TCP/UDP destination filter with this ACE, you can enter a specific TCP/UDP destination value. A field for entering a TCP/UDP destination value appears.
- Range: If you want to filter a specific range TCP/UDP destination filter with this ACE, you can enter a specific TCP/UDP destination range value. A field for entering a TCP/UDP destination value appears.

TCP/UDP Dest. Port No.

When "Specific" is selected for the TCP/UDP destination filter, you can enter a specific TCP/UDP destination value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP destination value.

TCP/UDP Dest. Port Range

When "Range" is selected for the TCP/UDP destination filter, you can enter a specific TCP/UDP destination range value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP destination value.

TCP FIN

Specify the TCP "No more data from sender" (FIN) value for this ACE.

- 0: TCP frames where the FIN field is set must not be able to match this entry.
- 1: TCP frames where the FIN field is set must be able to match this entry.
- Any: Any value is allowed ("don't-care").

TCP SYN

Specify the TCP "Synchronize sequence numbers" (SYN) value for this ACE.

- 0: TCP frames where the SYN field is set must not be able to match this entry.
- 1: TCP frames where the SYN field is set must be able to match this entry.
- Any: Any value is allowed ("don't-care").

TCP RST

Specify the TCP "Reset the connection" (RST) value for this ACE.

- 0: TCP frames where the RST field is set must not be able to match this entry.
- 1: TCP frames where the RST field is set must be able to match this entry.
- Any: Any value is allowed ("don't-care").

TCP PSH

Specify the TCP "Push Function" (PSH) value for this ACE.

- 0: TCP frames where the PSH field is set must not be able to match this entry.
- 1: TCP frames where the PSH field is set must be able to match this entry.
- Any: Any value is allowed ("don't-care").

TCP ACK

Specify the TCP "Acknowledgment field significant" (ACK) value for this ACE.

- 0: TCP frames where the ACK field is set must not be able to match this entry.
- 1: TCP frames where the ACK field is set must be able to match this entry.
- Any: Any value is allowed ("don't-care").

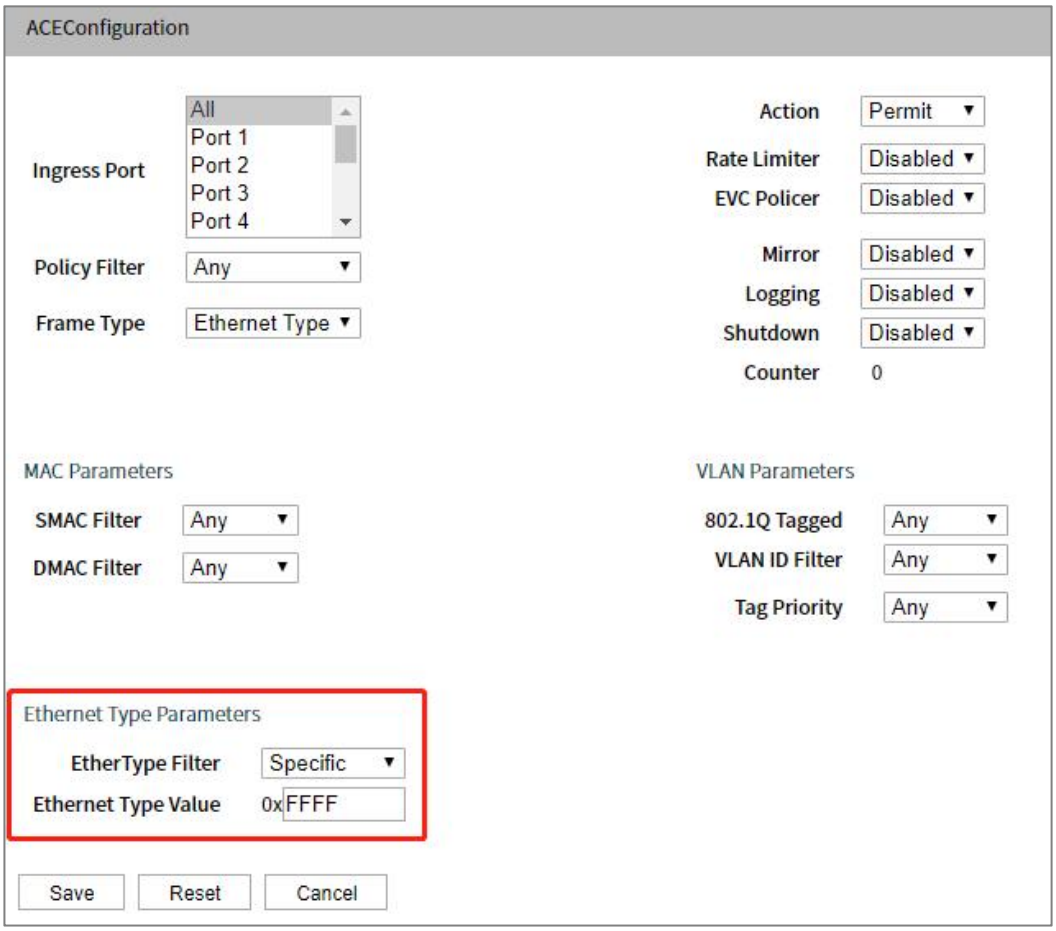
TCP URG

Specify the TCP "Urgent Pointer field significant" (URG) value for this ACE.

- 0: TCP frames where the URG field is set must not be able to match this entry.
- 1: TCP frames where the URG field is set must be able to match this entry.
- Any: Any value is allowed ("don't-care").

Ethernet Type Parameters

The Ethernet Type parameters can be configured when Frame Type "Ethernet Type" is selected.



EtherType Filter

Specify the Ethernet type filter for this ACE.

- Any: No EtherType filter is specified (EtherType filter status is "don't-care").
- Specific: If you want to filter a specific EtherType filter with this ACE, you can enter a specific EtherType value. A field for entering an "Ethernet Type Value" appears.

Ethernet Type Value

When "Specific" is selected for the EtherType filter, you can enter a specific EtherType value. The allowed range is 0x600 to 0xFFFF but excluding 0x800(IPv4), 0x806(ARP) and 0x86DD(IPv6). A frame that hits this ACE matches this EtherType value.

Buttons

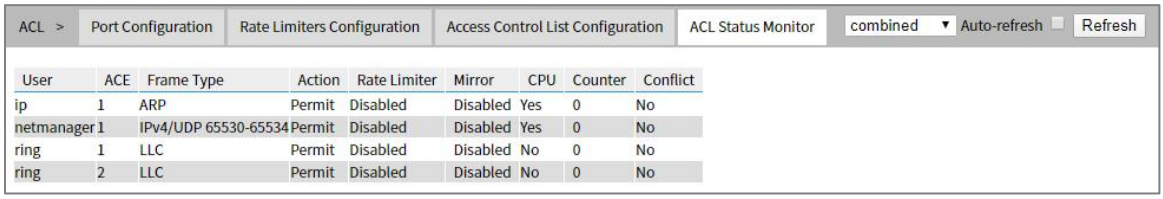
Save: Click to save changes.

Cancel: Click to undo any changes made locally and revert to previously saved values.

Cancel: Return to the previous page.

5.4.4 ACL Status Monitoring

This page shows the ACL status by different ACL users. Each row describes the ACE that is defined. It is a conflict if a specific ACE is not applied to the hardware due to hardware limitations. The maximum number of ACEs is 256 on each switch.



User

Indicates the ACL user. You can filter ACL users through the drop-down list button.

- combined
- static
- ipmc
- evc
- mep
- ptp
- dhcp
- loopProtect
- ring
- mstp
- netmanager
- ip
- conflict

ACE

Indicates the ACE ID on local switch.

Frame Type

Indicates the frame type of the ACE. Possible values are:

- Any: The ACE will match any frame type.
- EType: The ACE will match Ethernet Type frames.

  Note:
  Ethernet Type based ACE will not get matched by IP and ARP frames.
- ARP: The ACE will match ARP/RARP frames.
- IPv4: The ACE will match all IPv4 frames.
- IPv4/ICMP: The ACE will match IPv4 frames with ICMP protocol.
- IPv4/UDP: The ACE will match IPv4 frames with UDP protocol.
- IPv4/TCP: The ACE will match IPv4 frames with TCP protocol.
- IPv4/Other: The ACE will match IPv4 frames, which are not ICMP/UDP/TCP.

- IPv6: The ACE will match all IPv6 standard frames.

Action

Indicates the forwarding action of the ACE.

- Allow: frames matching ACE can be forwarded and learned.
- Reject: frames matching ACE are deleted.
- Filter: Frames matching the ACE are filtered.

Rate Limiter

Indicates the rate limiter number of the ACE. The allowed range is 1 to 16. When Disabled is displayed, the rate limiter operation is disabled.

CPU

Forward packet that matched the specific ACE to CPU.

Counter

The counter indicates the number of times the ACE was hit by a frame.

Conflicts

Indicates the hardware status of the specific ACE. The specific ACE is not applied to the hardware due to hardware limitations.

Buttons

Combined ▼: click this drop-down list to select the ACL user to be displayed.

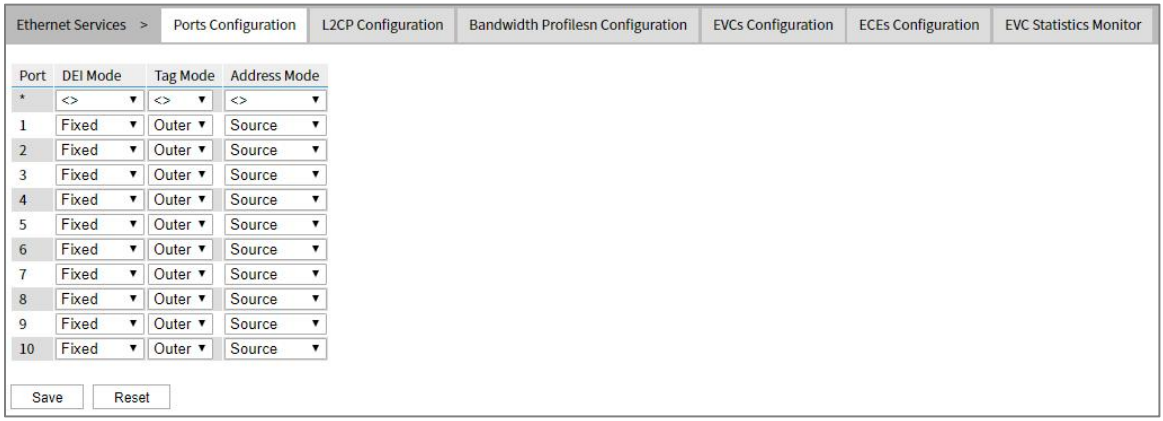
Auto-refresh: Check this box to enable an automatic refresh. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page; any changes made locally will be undone.

5.5 Ethernet Services

5.5.1 Port Configuration

This page displays current EVC port configurations. The settings can also be configured here.



Port

The switch port number.

DEI Mode

The DEI mode for an NNI port determines whether frames transmitted on the port will have the DEI field in the outer tag marked based on the colour of the frame. The allowed values are:

- Coloured: The DEI is 1 for yellow frames and 0 for green frames.
- Fixed: The DEI value is determined by ECE rules.

Tag Mode

The tag mode specifying whether the EVC classification must be based on the outer or inner tag. This can be used on NNI ports connected to another service provider, where an outer "tunnel" tag is added together with the inner tag identifying the EVC. The allowed values are:

- Inner: Enable inner tag in EVC classification.
- Outer: Enable outer tag in EVC classification.

Address Mode

The IP/MAC address mode specifying whether the EVC classification must be based on source (SMAC/SIP) or destination (DMAC/DIP) addresses. The allowed values are:

- Source: Enable SMAC/SIP matching.
- Destination: Enable DMAC/DIP matching.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

5.5.2 L2CP Configuration

This page displays current EVC L2CP configurations. The settings can also be configured here.

Destination MAC Address

The destination BPDU MAC addresses (01-80-C2-00-00-0X) and GARP (01-80-C2-00-00-2X) MAC addresses for the settings contained in the same row.

L2CP Mode

The L2CP mode for the specific port. Possible values are:

- Peer: Allow to peer L2CP frames.
- Forward: Allow to forward L2CP frames.

Buttons

Port 1 ▼: the port select box determines which port is affected by clicking the buttons.

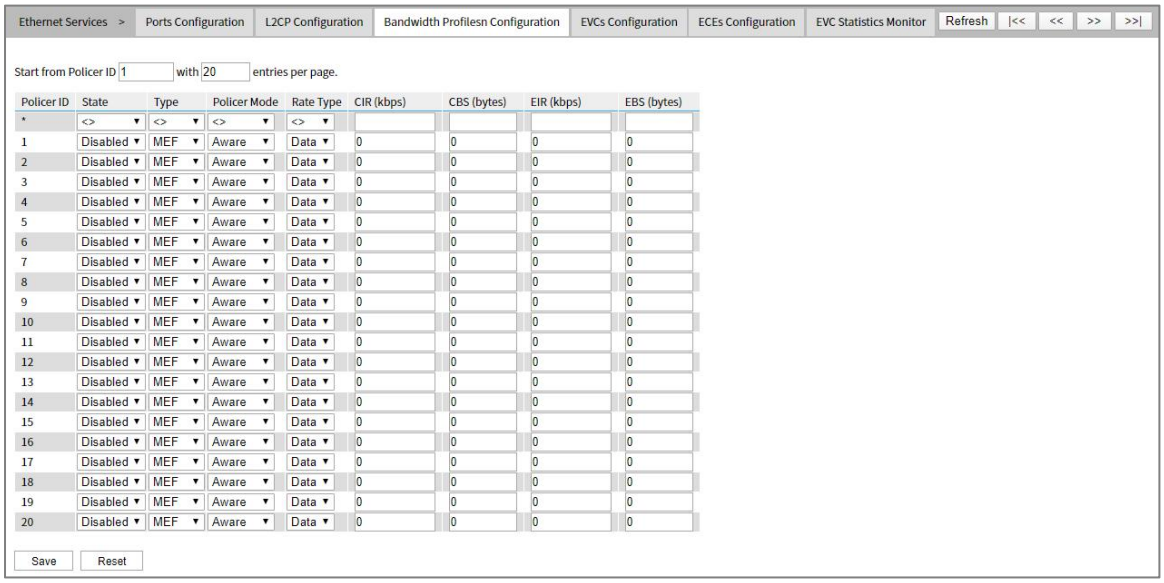
Refresh: Click to refresh the page.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

5.5.3 Bandwidth Limitation Subset

This page displays current EVC ingress bandwidth profile configurations. These policers may be used to limit the traffic received on UNI ports. The settings can also be configured here.



Start from Policer ID

The start Policer ID for displaying the table entries. The allowed range is from 1 through 256.

Entry

The number of entries per page. The allowed range is from 2 through 256.

Policer ID

The Policer ID is used to identify one of the 256 policers.

Status

The administrative state of the bandwidth profile. The allowed values are:

- Enabled: The bandwidth profile enabled.
- Disabled: The bandwidth profile is disabled.

Type

The policer type of the bandwidth profile. The allowed values are:

- MEF: MEF ingress bandwidth profile.
- Single: Single bucket policer.

Pattern

The colour mode of the bandwidth profile. The allowed values are:

- Coupled: Colour-aware mode with coupling enabled.
- Aware: Colour-aware mode with coupling disabled.

Rate Type

The rate type of the bandwidth profile. The allowed values are:

- Data: Specify that this bandwidth profile operates on data rate.
- Line: Specify that this bandwidth profile operates on line rate.

CIR

The Committed Information Rate of the bandwidth profile. The allowed range is from 0 through 10000000 kilobit per second.

CBS

The Committed Burst Size of the bandwidth profile. The allowed range is from 0 through 100000 bytes.

EIR

The Excess Information Rate for MEF type bandwidth profile. The allowed range is from 0 through 10000000 kilobit per second.

EBS

The Excess Burst Size for MEF type bandwidth profile. The allowed range is from 0 through 100000 bytes.

Buttons

Refresh: Refresh the displayed table starting from the input fields.

|<<: Updates the table, starting with the first entry in the table.

<<: Updates the table, ending at the entry before the first entry currently displayed.

>>: Updates the table, starting with the entry after the last entry currently displayed.

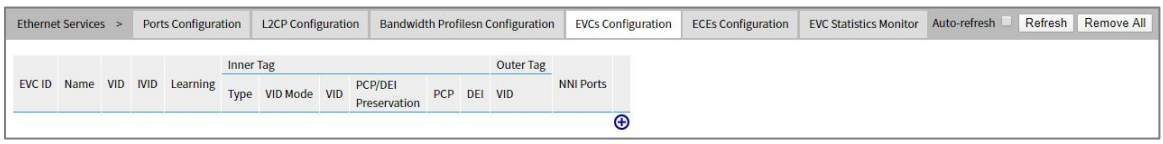
>>|: Updates the table, ending at the last entry in the table.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

5.5.4 EVCs Configuration

This page displays current EVC configurations. On this system, only Provider Bridge based EVCs are supported.



EVC ID

The EVC ID identifies the EVC. The range is from 1 through 256.

Name

The name for the EVC.

VID

The VLAN ID in the PB network. It may be inserted in a C-tag, S-tag or S-custom tag depending on the NNI port VLAN configuration. The range is from 1 through 4095.

IVID

The Internal/classified VLAN ID in the PB network. The range is from 1 through 4095.

Learning

The learning mode for the EVC controls whether source MAC addresses are learned for frames matching the EVC. Learning may be disabled if the EVC only includes two UNI/NNI ports. Possible values are:

- Enabled: Learning is enabled (MAC addresses are learned).
- Disabled: Learning is disabled (MAC addresses are not learned).

Inner Tag Type

The inner tag type is used to determine whether an inner tag is inserted in frames forwarded to NNI ports. Possible values are:

- None: An inner tag is not inserted.
- C-tag: An inner C-tag is inserted.
- S-tag: An inner S-tag is inserted.
- S-custom-tag: An inner tag is inserted and the tag type is determined by the VLAN port configuration of the NNI.

Inner Tag VID Mode

The inner VID Mode affects the VID in the inner and outer tag. Possible values are:

- Normal: The VID of the two outer tags aren't swapped.
- Tunnel: The VID of the two outer tags are swapped, so that the VID of the outer tag is taken from the Inner Tag configuration and the VID of the inner tag is the EVC VID. In this mode, the NNI ports are normally configured to do EVC classification based on the inner tag.

Inner Tag VID

The Inner tag VLAN ID. The allowed range is from 0 through 4095.

Inner Tag PCP/DEI Preservation

The inner tag PCP and DEI preservation. Possible values are:

- Preserved: The inner tag PCP and DEI is preserved.

- Fixed: The inner tag PCP and DEI is fixed.

Inner Tag PCP

The inner tag PCP value. The allowed range is from 0 through 7.

Inner Tag DEI

The inner tag DEI value. The allowed value is 0 or 1.

Outer Tag VID

The EVC outer tag VID for UNI ports. The allowed range is from 0 through 4095.

NNI Ports

The list of Network to Network Interfaces for the EVC.

Modification Buttons

You can modify each EVC in the table using the following buttons:

 Edit the EVC entry.

 Delete the EVC entry.

 Add new EVC entry.

Buttons

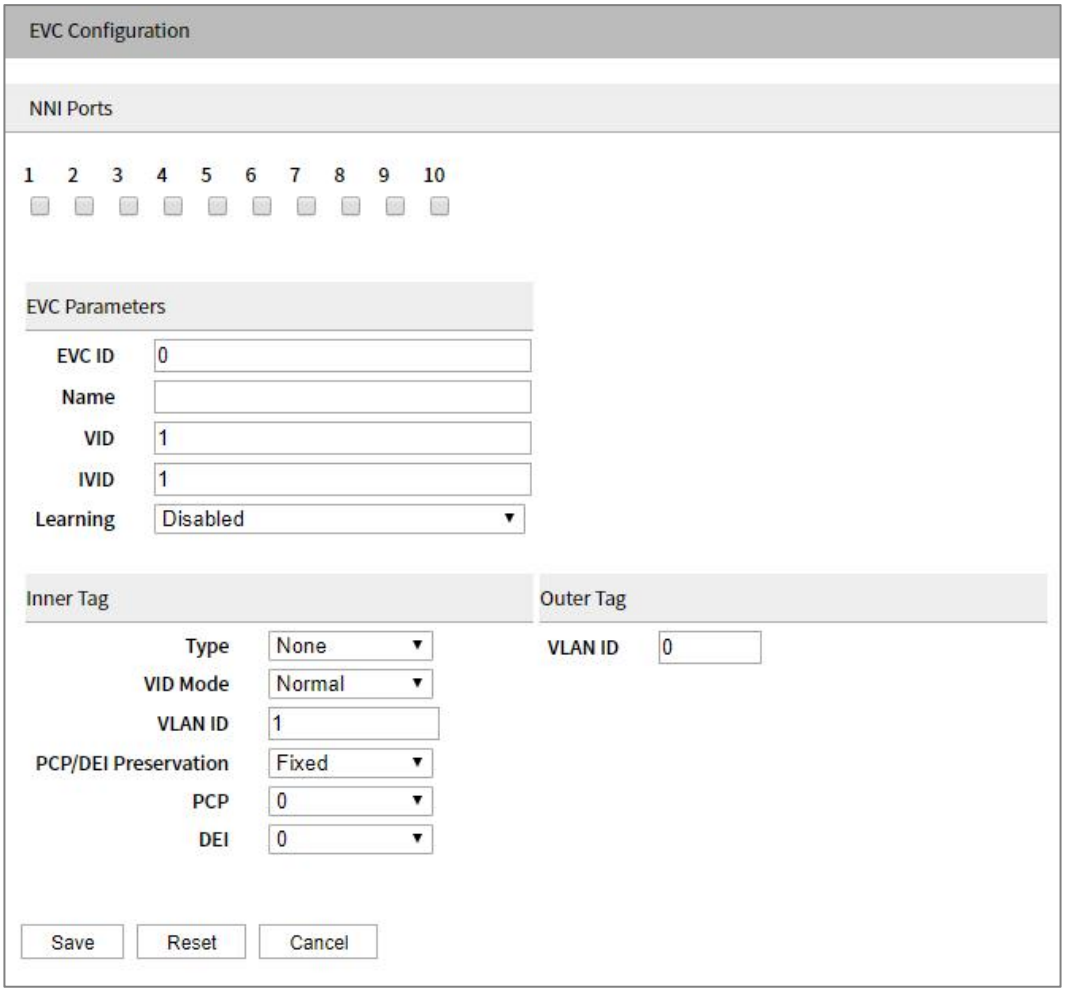
Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page.

Remove all: Click to remove all EVCs.

EVC Configuration

This page displays current EVC configurations. The settings can also be configured here.



NNI Ports

The list of Network to Network Interfaces for the EVC.

EVC Parameters

EVC ID

The EVC ID identifies the EVC. The allowed range is from 1 through 256.

Name

The name for the EVC. It is case sensitive and can contain up to 256 characters combination of alphanumeric and special characters.

VID

The VLAN ID in the PB network. It may be inserted in a C-tag, S-tag or S-custom tag depending on the NNI port VLAN configuration. The allowed range is from 1 through 4095.

IVID

The Internal/classified VLAN ID in the PB network. The allowed range is from 1 through 4095.

Learning

The learning mode for the EVC controls whether source MAC addresses are learned for frames matching the EVC. Learning may be disabled if the EVC only includes two UNI/NNI ports. Possible values are:

- Enabled: Learning is enabled (MAC addresses are learned).
- Disabled: Learning is disabled (MAC addresses are not learned).

Inner Tag

Tag Type

The inner tag type is used to determine whether an inner tag is inserted in frames forwarded to NNI ports. Possible values are:

- None: An inner tag is not inserted.
- C-tag: An inner C-tag is inserted.
- S-tag: An inner S-tag is inserted.
- S-custom-tag: An inner tag is inserted and the tag type is determined by the VLAN port configuration of the NNI.

VID Mode

The inner VID Mode affects the VID in the inner and outer tag. Possible values are:

- Normal: The VID of the two outer tags aren't swapped.
- Tunnel: The VID of the two outer tags are swapped, so that the VID of the outer tag is taken from the Inner Tag configuration and the VID of the inner tag is the EVC VID. In this mode, the NNI ports are normally configured to do EVC classification based on the inner tag.

VLAN ID

The Inner tag VLAN ID. The allowed range is from 1 through 4095.

PCP/DEI Preservation

The inner tag PCP and DEI preservation. Possible values are:

- Preserved: The inner tag PCP and DEI is preserved.
- Fixed: The inner tag PCP and DEI is fixed.

PCP

The inner tag PCP value. The allowed range is from 0 through 7.

DEI

The inner tag DEI value. The allowed value is 0 or 1.

Outer Tag

VLAN ID

The EVC outer tag VID for UNI ports. The allowed range is from 1 through 4095.

Buttons

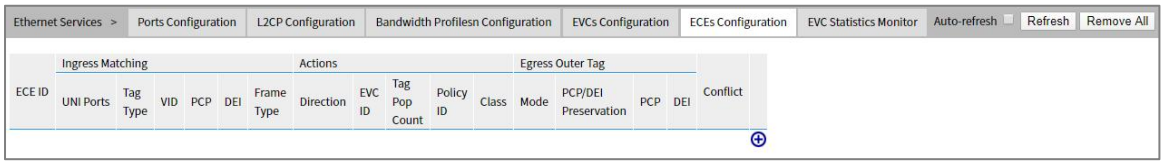
Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Cancel: Return to the previous page; any changes made locally will be undone.

5.5.5 ECEs Configuration

This page displays the current EVC Control Entries (ECEs). The settings can also be configured here.



ECE ID

The ECE ID identifies the ECE. Unique ECE IDs are automatically assigned to ECEs added. The possible range is from 1 through 256.

Ingress Matching

UNI Ports

The list of User Network Interfaces for the ECE.

Tag Type

The tag type for the ECE. Possible values are:

- Any: The ECE will match both tagged and untagged frames.
- Untagged: The ECE will match untagged frames only.
- C-Tagged: The ECE will match custom tagged frames only.
- S-Tagged: The ECE will match service tagged frames only.
- Tagged: The ECE will match tagged frames only.

VID

The VLAN ID for the ECE. It only significant if tag type 'Tagged' is selected. Possible values are:

- Specific: The range is from 0 through 4095.
- Any: The ECE will match any VLAN ID.

PCP

The PCP value for the ECE. It only significant if tag type 'Tagged' is selected. Possible values are:

- Specific: The ECE will match a specific PCP in the range 0 through 7.
- Range: The ECE will match PCP values in the selected range 0-1, 2-3, 4-5, 6-7, 0-3 or 4-7.
- Any: The ECE will match any PCP value.

DEI

The DEI value for the ECE. It only significant if tag type 'Tagged' is selected. The possible values is: 0, 1 or Any.

Frame Type

The frame type for the ECE. Possible values are:

- Any: The ECE will match any frame type.
- IPv4: The ECE will match IPv4 frames only.
- IPv6: The ECE will match IPv6 frames only.

Actions

Direction

The EVCs and ECEs are used to setup flows in one or both directions as determined by the ECE Direction parameter. If the ECE is bidirectional, the ingress rules of the NNI ports will be setup to match the traffic being forwarded to NNI ports. Possible values are:

- Both: Bidirectional.
- UNI-to-NNI: Unidirectional from UNI to NNI.
- NNI-to-UNI: Unidirectional from NNI to UNI.

EVC ID

The EVC ID for the ECE. The ECE is only active when mapping to an existing EVC. Possible values are:

- Specific: The range is from 1 through 256.
- None: The ECE does not map to an EVC.

Tag Pop Count

The ingress tag pop count for the ECE. The possible range is from 0 through 2.

Policy ID

The ACL Policy ID for the ECE. The range is from 0 through 255.

Class

The traffic class for the ECE. The range is from 0 through 7.

Egress Outer Tag

Pattern

The outer tag for nni-to-uni direction for the ECE. Possible values are:

- Enable: Enable outer tag for nni-to-uni direction for the ECE.
- Disable: Disable outer tag for nni-to-uni direction for the ECE.

PEC/DEI Preservation

The outer tag PCP and DEI preservation for the ECE. Possible values are:

- Preserved: The outer tag PCP and DEI are preserved.
- Fixed: The outer tag PCP and DEI are fixed.

PCP

The outer tag PCP value for the ECE. The possible range is from 0 through 7.

DEI

The outer tag DEI value for the ECE. The possible value is 0 or 1.

Conflict

Indicates the hardware status of the specific ECE. The specific ECE is not applied to the hardware due to hardware limitations.

Modification Buttons

You can modify each ECE (EVC Control Entry) in the table using the following buttons:

: Insert a new ECE before the current row.

Edits the ECE row.

: Moves the ECE up the list.

: Moves the ECE down the list.

: delete ECE.

: The lowest plus sign adds a new entry at the bottom of the ECE listings.

Buttons

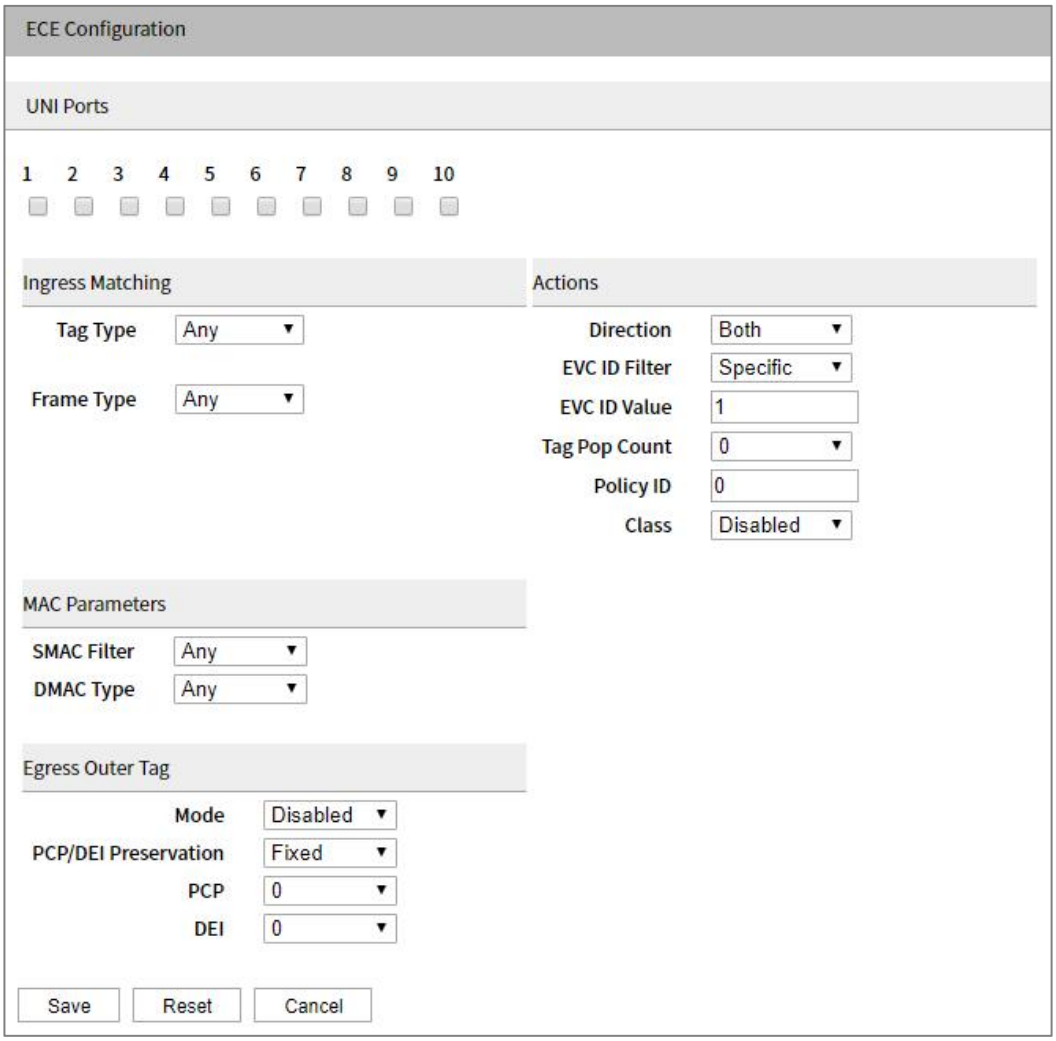
Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page.

Remove all: Click to remove all ECEs.

ECE Configuration

This page displays current ECE configurations. The settings can also be configured here.



UNI Ports

The list of User Network Interfaces for the ECE.

UNI Matching

Tag Type

The tag type for matching the ECE. Possible values are:

- Any: The ECE will match both tagged and untagged frames.
- Untagged: The ECE will match untagged frames only.
- C-Tagged: The ECE will match custom tagged frames only.
- S-Tagged: The ECE will match service tagged frames only.
- Tagged: The ECE will match tagged frames only.

VLAN ID Filter

The VLAN ID filter for matching the ECE. It only significant if tag type 'Tagged' is selected. Possible values are:

- Any: No VLAN ID filter is specified. (VLAN ID filter status is "don't-care".)
- Specific: If you want to filter a specific VLAN ID value with this ECE, choose this

value. A field for entering a specific value appears.

- Range: If you want to filter a specific VLAN ID range filter with this ECE, choose this value. A field for entering a range appears.

VLAN ID Value

When "Specific" is selected for the VLAN ID filter, you can enter a specific value. The allowed value is from 0 through 4095.

VLAN ID Range

When "Range" is selected for the VLAN ID filter, you can enter a specific range. The allowed range is from 0 through 4095.

PCP

The PCP value for matching the ECE. It only significant if tag type 'Tagged' is selected.

Possible values are:

- Any: The ECE will match any PCP value.
- Specific: The ECE will match a specific PCP in the range 0 through 7.
- Range: The ECE will match PCP values in the selected range 0-1, 2-3, 4-5, 6-7, 0-3 or 4-7.

DEI

The DEI value for matching the ECE. It only significant if tag type 'Tagged' is selected.

The allowed value is: 0, 1 or Any.

Frame Type

The frame type for the ECE. Possible values are:

- Any: The ECE will match any frame type.
- IPv4: The ECE will match IPv4 frames only.
- IPv6: The ECE will match IPv6 frames only.

IP Parameters

Protocol

The IP protocol for matching the ECE. Possible values are:

- Any: No protocol filter is specified. (Protocol filter status is "don't-care".)
- UDP: Specify the UDP for matching the ECE.
- TCP: Specify the TCP for matching the ECE.
- Other: If you want to filter a specific protocol value with this ECE, choose this value. A field for entering a specific value appears.

Protocol Value

When "other" is selected for the protocol filter, you can enter a specific value. The allowed value is from 0 through 255.

SIP/DIP Filter

The source/destination IP address for matching the ECE. It depend on by the port address mode, when port address mode is set to 'Source' then the field is used for source address. Similarly when port address mode is set to 'Destination' then the field is used for destination address. Possible values are:

- Any: No SIP/DIP filter is specified. (SIP/DIP filter status is "don't-care".)
- Host: When "IPv4" is selected for the Frame Type, if you want to filter a specific host address with this ECE, choose this value. A field for entering a host address appears.
- Network: When "IPv4" is selected for the Frame Type, if you want to filter a specific network address with this ECE, choose this value. Two fields for entering a specific network address and network mask appears.
- Specific: When "IPv6" is selected for the Frame Type, if you want to filter a specific network address with this ECE, choose this value. Two fields for entering a specific network address and network mask appears.

SIP/ DIP Address

When "IPv4" is selected for the Frame Type and "Host" or "Network" is selected for the SIP/DIP filter, you can enter a specific host or network address. When "IPv6" is selected for the Frame Type, the field only supported 32 bits for IPv6 address.

SIP/DIP Mask

When "IPv4" is selected for the Frame Type and "Host" or "Network" is selected for the SIP/DIP filter, you can enter a specific network mask. When "IPv6" is selected for the Frame Type, the field only supported 32 bits for IPv6 address mask.

DSCP Filter

The DSCP filter for matching the ECE. Possible values are:

- Any: No DSCP filter is specified. (DSCP filter status is "don't-care".)
- Specific: If you want to filter a specific DSCP value with this ECE, choose this value. A field for entering a specific value appears.
- Range: If you want to filter a specific DSCP range filter with this ECE, choose this value. A field for entering a range appears.

DSCP Value

When "Specific" is selected for the DSCP filter, you can enter a specific value. The allowed value is from 0 through 63.

DSCP Range

When "Range" is selected for the DSCP filter, you can enter a specific range. The allowed range is from 0 through 63.

Fragment

The IPv4 Fragment for matching the ECE. This involves the settings for the More Fragments (MF) bit and the Fragment Offset (FRAG OFFSET) field for an IPv4 frame. Possible values are:

- Any: The ECE will match any MF bit.
- Non-Fragment: IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must not be able to match this entry.
- Fragment: IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must be able to match this entry.

UDP/TCP Parameters

Source Port Filter

The TCP/UDP source port for matching the ECE. It only significant if protocol filter 'UDP' or 'TCP' is selected. Possible values are:

- Any: No TCP/UDP source port filter is specified. (Source port filter status is "don't-care".)
- Specific: If you want to filter a specific TCP/UDP source port No. Use this ECE, choose this value. A field for entering a specific No. appears.
- Range: If you want to filter a specific TCP/UDP source port range filter with this ECE, choose this value. A field for entering a range appears.

Source Port No.

When "Specific" is selected for the source port filter, you can enter a specific value. The allowed value is from 0 through 65535.

Source Port Range

When "Range" is selected for the source port filter, you can enter a specific range. The allowed range is from 0 through 65535.

Destination Port Filter

The TCP/UDP destination port for matching the ECE. It only significant if protocol filter 'UDP' or 'TCP' is selected. The possible values are:

- Any: No TCP/UDP destination port filter is specified. (Destination port filter status is "don't-care".)
- Specific: If you want to filter a specific TCP/UDP destination port No. Use this ECE, choose this value. A field for entering a specific No. appears.
- Range: If you want to filter a specific TCP/UDP destination port range filter with this ECE, choose this value. A field for entering a range appears.

Destination Port No.

When "Specific" is selected for the destination port filter, you can enter a specific value. The allowed value is from 0 through 65535.

Destination Port Range

When "Range" is selected for the destination port filter, you can enter a specific range. The allowed range is from 0 through 65535.

MAC Parameters

SMAC Filter

The source MAC address for matching the ECE. Possible values are:

- Any: No SMAC filter is specified. (SMAC filter status is "don't-care".)
- Specific: If you want to filter a specific SMAC value with this ECE, choose this value. A field for entering a specific value appears.

SMAC Value

When "Specific" is selected for the SMAC filter, you can enter a specific value. The legal format is "xx-xx-xx-xx-xx-xx" or "xx.xx.xx.xx.xx.xx" or "xxxxxxxxxxxx" (x is a hexadecimal digit).

DMAC Type

The destination MAC address type for matching the ECE. Possible values are:

- Any: No DMAC type is specified. (DMAC filter status is "don't-care".)
- Unicast: Frame must be unicast.
- Multicast: Frame must be multicast.
- Broadcast: Frame must be broadcast.

Action

Direction

The EVCs and ECEs are used to setup flows in one or both directions as determined by the ECE Direction parameter. If the ECE is bidirectional, the ingress rules of the NNI ports will be setup to match the traffic being forwarded to NNI ports. Possible values are:

- Both: Bidirectional.
- UNI-to-NNI: Unidirectional from UNI to NNI.
- NNI-to-UNI: Unidirectional from NNI to UNI.

EVC ID Filter

The EVC ID for the ECE. The ECE is only active when mapping to an existing EVC. Possible values are:

- Any: No EVC ID filter is specified. (EVC ID filter status is "don't-care".)
- Specific: If you want to filter a specific EVC ID with this ECE, choose this value. A field for entering a specific value appears.

EVC ID Value

When "Specific" is selected for the VLAN ID filter, you can enter a specific value. The allowed value is from 1 through 256.

Tag Pop Count

The ingress tag pop count for the ECE. The allowed range is from 0 through 2.

Policy ID

The ACL Policy ID for the ECE for matching ACL rules. The allowed range is from 0 through 255.

Class

The traffic class for the ECE. The allowed range is from 0 through 7 or disabled.

Egress Outer Tag

Pattern

The outer tag for nni-to-uni direction for the ECE. Possible values are:

- Enable: Enable outer tag for nni-to-uni direction for the ECE.
- Disable: Disable outer tag for nni-to-uni direction for the ECE.

PEC/DEI Preservation

The outer tag PCP and DEI preservation for the ECE. Possible values are:

- Preserved: The outer tag PCP and DEI is preserved.
- Fixed: The outer tag PCP and DEI is fixed.

PCP

The outer tag PCP value for the ECE. The allowed range is from 0 through 7.

DEI

The outer tag DEI value for the ECE. The allowed value is 0 or 1.

Buttons

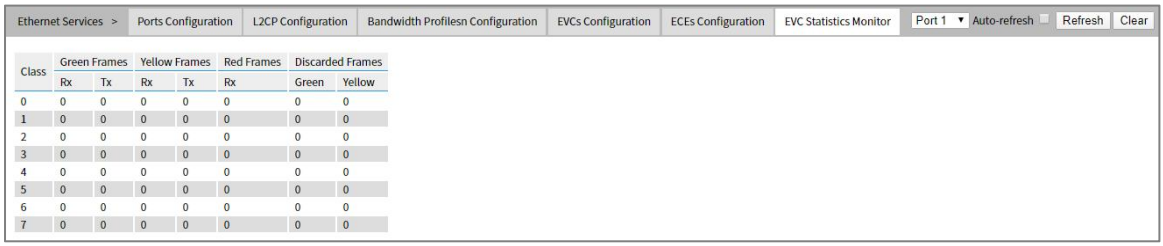
Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Cancel: Return to the previous page; any changes made locally will be undone.

5.5.6 EVC Statistics

This page provides NNI port traffic statistics for the selected EVC. It also shows counters for UNI ports of ECEs mapping to the EVC. And the MPLS Pseudo-Wires counters are included when the PW ID is attached to the selected EVC.



Class

The traffic class for the EVC.

Green Frames Rx

The number of green received.

Green Frames Tx

The number of green transmitted.

Yellow Frames Rx

The number of yellow received.

Yellow Frames Tx

The number of yellow transmitted.

Red Frames Rx

The number of red received.

Discarded Frames Green

The number of discarded in the green color.

Discarded Frames Yellow

The number of discarded in the yellow color.

Buttons

Port 1▼:The port select box determines which port is affected by clicking the buttons.

Auto-refresh: Check this box to enable an automatic refresh. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

Clear: Clears the counters for the selected port.

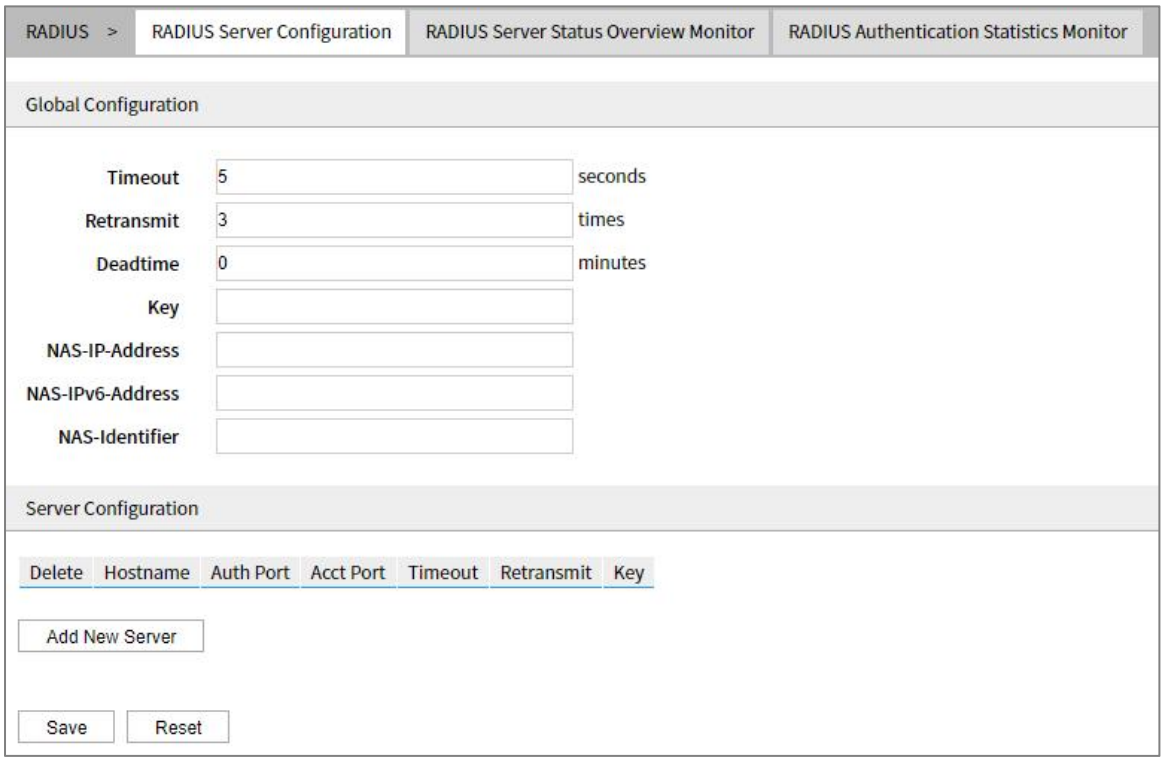
5.6 RADIUS

RADIUS (Remote Authentication Dial-in User Service) is an information interaction protocol with client/server structure, which can protect the network from unauthorized access. It is often used in various network environments that require high security and

allow remote users to access. This protocol defines the RADIUS message format and its transmission mechanism based on UDP(User Datagram Protocol), and specifies UDP Port 1812 and 1813 as authentication and accounting ports, respectively. As a RADIUS client, the device is responsible for transmitting user information to the specified RADIUS server, and then processing it according to the information returned from the server.

5.6.1 RADIUS Server Configuration

This page allows you to configure the RADIUS servers.



Global Configuration

These setting are common for all of the RADIUS servers.

Timeout

Timeout is the number of seconds, in the range 1 to 1000, to wait for a reply from a RADIUS server before retransmitting the request.

Retransmit

Retransmit is the number of times, in the range 1 to 1000, a RADIUS request is retransmitted to a server that is not responding. If the server has not responded after the last retransmit it is considered to be dead.

Deadtime

Deadtime, which can be set to a number between 0 to 1440 分, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead.

Setting the Deadtime to a value greater than 0 (0) will enable this feature, but only if more than one server has been configured.

Key

The secret key - up to 63 characters long - shared between the RADIUS server and the switch.

NAS-IP-Address (Attribute 4)

The IPv4 address to be used as attribute 4 in RADIUS Access-Request packets. If this field is left blank, the IP address of the outgoing interface is used. The IP(Internet Protocol) address of the device carried in the authentication request message sent by the NAS device. If the RADIUS server binds the interface address, it obtains the bound interface address; otherwise, it obtains the interface address that sends message.

NAS-IPv6-Address (Attribute 95)

The IPv6 address to be used as attribute 95 in RADIUS Access-Request packets. If this field is left blank, the IP address of the outgoing interface is used.

NAS-Identifier (Attribute 32)

The NAS-Identifier - up to 253 characters long - to be used as attribute 32 in RADIUS Access-Request packets. If this field is left blank, the NAS-Identifier is not included in the packet. The host name or VLAN ID of the NAS device.

Server Configuration

Delete

To delete a RADIUS server entry, check this box. The entry will be deleted during the next Save.

Hostname

IP address of Radius server.

Note:

The host name must be a valid IPv4 unicast address.

Auth Port

The UDP port to use on the RADIUS server for authentication. Set to 0 to disable authentication.

Acct Port

The UDP port to use on the RADIUS server for accounting. Set to 0 to disable accounting.

Timeout

This optional setting overrides the global timeout value. Leaving it blank will use the global timeout value.

Retransmit

This optional setting overrides the global retransmit value. Leaving it blank will use the global retransmit value.

Key

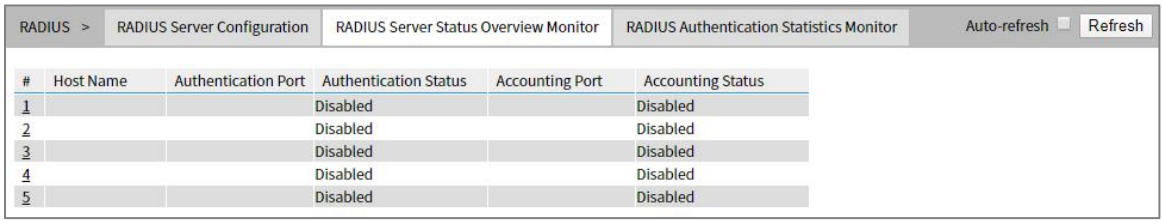
This optional setting overrides the global key. Leaving it blank will use the global key.

Buttons

Add new server: Click to add a new RADIUS server. Up to 5 servers are supported.
Delete: click to undo the addition of the new server.
Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

5.6.2 RADIUS Server Status Overview Monitoring

This page provides an overview of RADIUS server status. This server is configurable on the server configuration page.



#

The RADIUS server number. Click this link to navigate to detailed statistics for this server. See the next section for details.

Hostname

The IP address of this server.

Authentication Port

UDP port number for authentication.

Authentication Status

The current status of the server. This field takes one of the following values:

- Disabled: The server is disabled.
- Not Ready: The server is enabled, but IP communication is not yet up and running.
- Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.
- Dead (X seconds left): Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

Accounting Port

Billing UDP port number.

Accounting Status

The current status of the server. This field takes one of the following values:

- Disabled: The server is disabled.
- Not Ready: The server is enabled, but IP communication is not yet up and running.
- Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.
- Dead (X seconds left): Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

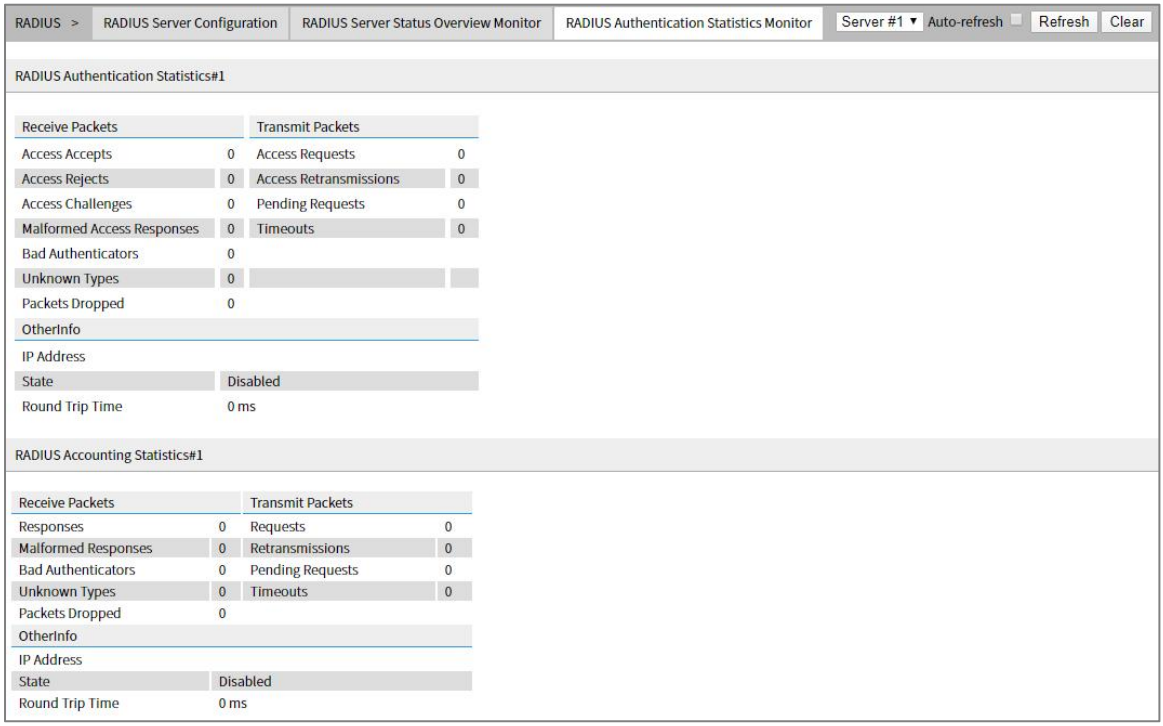
Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

5.6.3 RADIUS Authentication Statistics Link Monitoring

This page provides detailed statistics for a particular RADIUS server.



RADIUS Authentication Statistics

The statistics map closely to those specified in RFC4668 – RADIUS Authentication Client MIB.

Use the server select box to switch between the backend servers to show details for.

Rx and Tx Packets

RADIUS authentication server packet counter. There are seven receive and four transmit counters.

Direction	Name	RFC4668 Name	Note
Received Packets	Receive access	radiusAuthClientExtAccessAccepts	The number of RADIUS Access-Accept packets (valid or invalid) received from the server.
	Deny access	radiusAuthClientExtAccessRejects	The number of RADIUS Access-Reject packets (valid or invalid) received from the server.
	Challenge access	radiusAuthClientExtAccessChallenges	The number of RADIUS Access-Challenge packets (valid or invalid) received from the server.
	Exception access response	radiusAuthClientExtMalformedAccessResponses	The number of malformed RADIUS Access-Response packets received from the server. Malformed packets

Direction	Name	RFC4668 Name	Note
			include packets with an invalid length. Bad authenticators or Message Authenticator attributes or unknown types are not included as malformed access responses.
	Wrong authenticator	radiusAuthClientExtBadAuthenticators	The number of RADIUS Access-Response packets containing invalid authenticators or Message Authenticator attributes received from the server.
	Unknown type	radiusAuthClientExtUnknownTypes	The number of RADIUS packets that were received with unknown types from the server on the authentication port and dropped.
	Discarded Packets	radiusAuthClientExtPacketsDropped	The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.
Tx Packets	Request access	radiusAuthClientExtAccessRequests	The number of RADIUS Access-Request packets sent to the server. This does not include retransmissions.
	Retransmission access	radiusAuthClientExtAccessRetransmissions	The number of RADIUS Access-Request packets retransmitted to the RADIUS authentication server.
	Pending request	radiusAuthClientExtPendingRequests	The number of RADIUS Access-Request packets destined for the server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject, Access-Challenge, timeout, or retransmission.
	timeout	radiusAuthClientExtTi	The number of authentication timeouts

Direction	Name	RFC4668 Name	Note
		meouts	to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.

Other Info

This section contains information about the state of the server and the latest round-trip time.

Name	RFC4668 Name	Description
IP Address	-	IP address and UDP port number of the related authentication server
Status	-	Shows the state of the server. It adopts one of the following values： • Disabled: The selected server is disabled. • Not Ready: The server is enabled, but IP communication is not yet up and running. • Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts. • Dead (X seconds left): Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.
Round-trip time	radiusAuthClientExtRoundTripTime	The time interval (measured in milliseconds) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from the RADIUS

Name	RFC4668 Name	Description
		authentication server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.

RADIUS Accounting Statistics#

The statistics map closely to those specified in RFC4670-RADIUS Accounting Client MIB.

Use the server select box to switch between the backend servers to show details for.

Rx and Tx Packets

RADIUS accounting server packet counter. There are five receive and four transmit counters.

Direction	Name	RFC4670 Name	Description
Rx	Responses	radiusAccClientExtResponses	The number of RADIUS packets (valid or invalid) received from the server.
Rx	Anomaly response	radiusAccClientExtMalformedResponses	The number of malformed RADIUS packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or unknown types are not included as malformed access responses.
Receive	Wrong authentication	radiusAcctClientExtBadAuthenticators	The number of RADIUS packets containing invalid authenticators received from the server.
Receive	Unknown type	radiusAccClientExtUnknownTypes	The number of RADIUS packets of unknown types that were received from the server on the accounting port.
Receive	Discarded Packets	radiusAccClientExtPacketsDropped	The number of RADIUS packets that were received from the server on the accounting port and dropped for some other reason.
Tx	REQUEST	radiusAccClientExtRequests	The number of RADIUS packets sent to the server. This does not include retransmissions.

Direction	Name	RFC4670 Name	Description
Tx	Retransmission	radiusAccClientExtRetransmissions	The number of RADIUS packets retransmitted to the RADIUS accounting server.
Tx	Pending request	radiusAccClientExtPendingRequests	The number of RADIUS packets destined for the server that have not yet timed out or received a response. This variable is incremented when a Request is sent and decremented due to receipt of a Response, timeout, or retransmission.
Tx	timeout	radiusAccClientExtTimeouts	The number of accounting timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.

Other Info

This section contains information about the state of the server and the latest round-trip time.

Name	RFC4670 Name	Description
IP Address	-	IP address and UDP port for the accounting server in question.
Status	-	Shows the state of the server. It takes one of the following values: • Disabled: The selected server is disabled. • Not Ready: The server is enabled, but IP communication is not yet up and running. • Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept accounting attempts. • Dead (X seconds left): Accounting attempts were made to this server, but it

Name	RFC4670 Name	Description
		did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.
Round-trip time	radiusAccClientExtRoundTripTime	The time interval (measured in milliseconds) between the most recent Response and the Request that matched it from the RADIUS accounting server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.

Buttons

Server#1 ▼: The server select the drop-down list determines which server is affected by clicking the buttons.

Auto-refresh: Check this box to enable an automatic refresh. Automatic refresh occurs every 3 seconds.

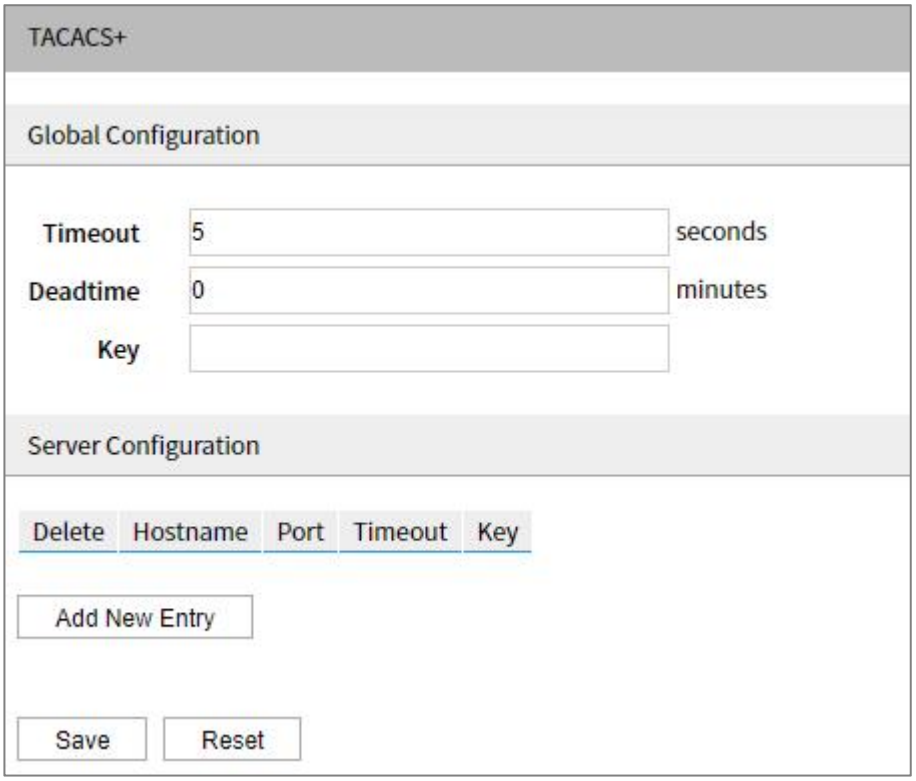
Refresh: Click to refresh the page immediately.

Clear: Clears the counters for the selected server. The "Pending Requests" counter will not be cleared by this operation.

5.7 TACACS+

TACACS+ (Terminal Access Controller Access Control System) is an application based on TCP transmission protocol, which uses client/server mode to realize the communication between NAS(Network Access Server) network access server and TACACS+server. Compared with RADIUS, TACACS+ has more reliable transmission and encryption characteristics and is more suitable for security control.

This page allows you to configure the TACACS+ servers.



Global Configuration

These setting are common for all of the TACACS+ servers.

Timeout

Timeout is the number of seconds, in the range 1 to 1000, to wait for a reply from a TACACS+ server before it is considered to be dead.

Deadtime

Deadtime, which can be set to a number between 0 to 1440 分, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead.

Setting the Deadtime to a value greater than 0 (0) will enable this feature, but only if more than one server has been configured.

Key

The secret key - up to 63 characters long - shared between the TACACS+ server and the switch.

Server Configuration

Delete

To delete a TACACS+ server entry, check this box. The entry will be deleted during the next Save.

Hostname

IP address of TACACS server.

Note:

The host name must be a valid IPv4 unicast address.

Auth Port

The TCP port to use on the TACACS+ server for authentication.

Timeout

This optional setting overrides the global timeout value. Leaving it blank will use the global timeout value.

Key

This optional setting overrides the global key. Leaving it blank will use the global key.

Buttons

Add new server: Click to add a new TACACS + server. Up to 5 servers are supported.

Delete: click to undo the addition of the new server.

Save: Click to save changes.

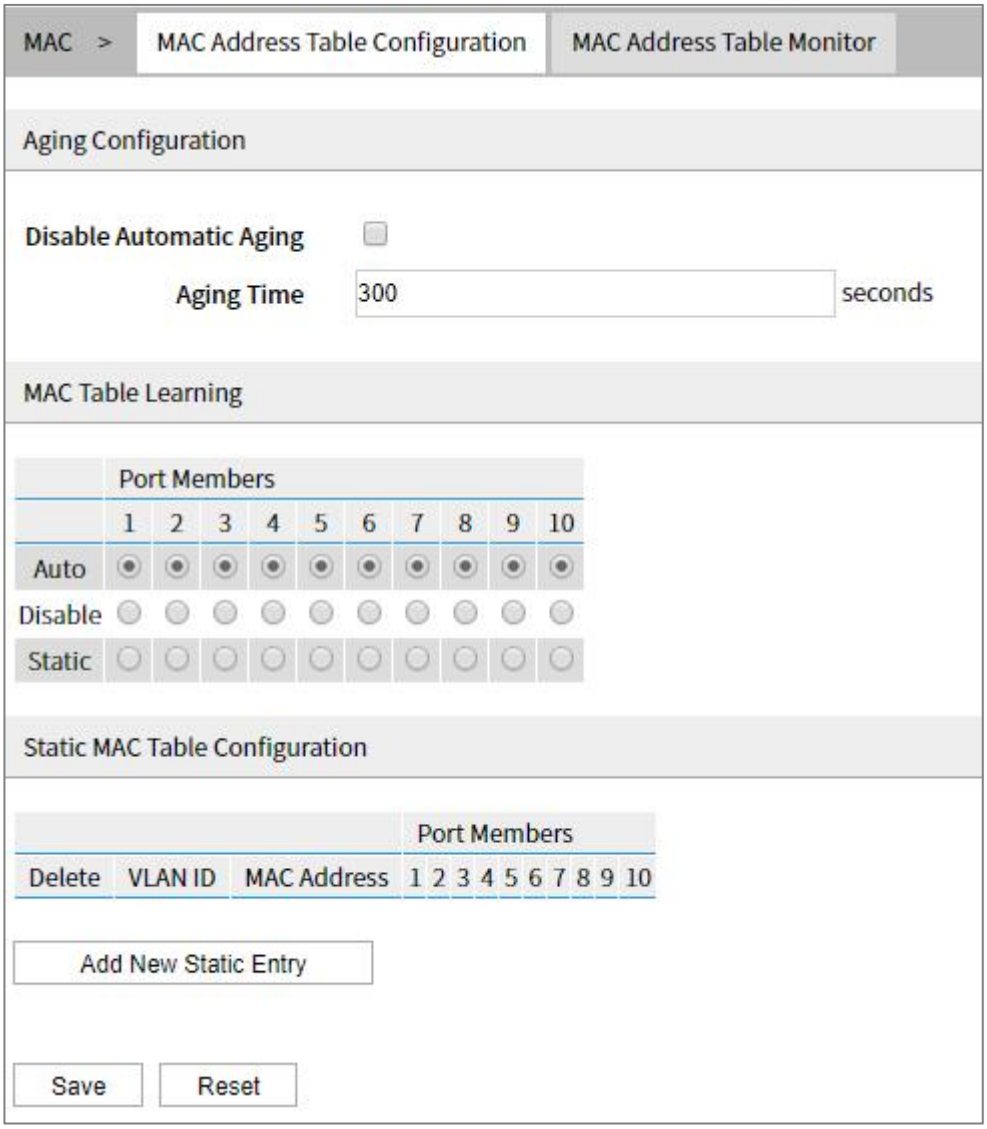
Reset: Click to undo any changes made locally and revert to previously saved values.

6 Layer 2 Protocol

6.1 MAC

Each workstation or server connected to the device has its own unique MAC (Medium Access Control) address. When the device interacts with it, the device will record their MAC address, the interface connecting the device and VLAN ID to guide the unicast forwarding of data.

6.1.1 MAC Address Table Configuration



On this page, you can configure the MAC address aging time in the dynamic MAC table or the static MAC table.

Aging Configuration

Disable Automatic Aging

Disable the automatic aging of dynamic entries by checking Disable Automatic Aging.

Aging Time

Configure aging time by entering a value here in seconds; The allowed range is 10 to 1,000,000 seconds. By default, dynamic entries are removed from the MAC table after 300 seconds. This removal is also called aging.

MAC table learning

If the learning mode for a given port is greyed out, another module is in control of the mode, so that it cannot be changed by the user.

Port Members

Each port of the switch can do learning based upon the following settings:

- Auto: Learning is done automatically as soon as a frame with unknown SMAC is received.
- Disable: No learning is done.
- Static: Only static MAC entries are learned, all other frames are dropped.

Notice:

The static entries in the MAC table are shown in this table. The static MAC table can contain 64 entries.

Static MAC Table Configuration

The static entries in the MAC table are shown in this table. The static MAC table can contain 64 entries.

The MAC table is sorted first by VLAN ID and then by MAC address.

Delete

Check to delete the entry. It will be deleted during the next save.

VLAN

The VLAN ID of the entry.

MAC address;

The MAC address of the entry.

Port Members

Checkmarks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry.

Buttons

Add New Static Entry: Click to add a new MAC table entry.

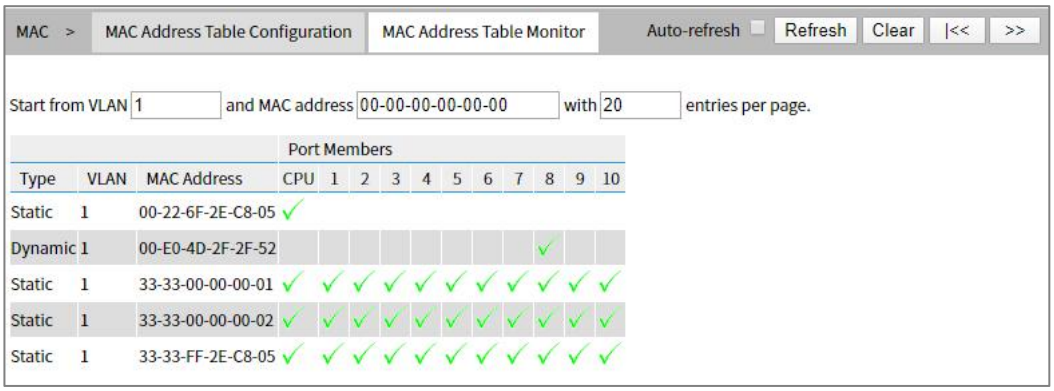
Delete: Click to delete a static entry in the add.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

6.1.2 MAC Address Table Monitoring

Entries in the MAC Table are shown on this page. The MAC Table contains up to 8192 entries, and is sorted first by VLAN ID, then by MAC address.



Each page shows up to 999 entries from the MAC table, default being 20, selected through the "entries per page" input field. When first visited, the Web page will show the first 20 entries from the beginning of the MAC Table. The first displayed will be the one with the lowest VLAN ID and the lowest MAC address found in the MAC Table.

The Start “MAC address" and "VLAN" input fields allow the user to select the starting point in the MAC Table. Clicking the “Refresh” button will update the displayed table starting from that or the closest next MAC Table match. In addition, the two input fields will - upon a “Refresh” button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The “>>” button will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the “|<<” button to start over.

Type

Indicates whether the entry is a static or a dynamic entry.

VLAN

The VLAN ID of the entry.

MAC address;

The MAC address of the entry.

Port Members

The ports that are members of the entry.

Buttons

Auto-refresh: Automatic refresh occurs every 3 seconds.

Refresh: Refreshes the displayed table starting from the "VLAN “ and “MAC address” input fields.

Clear: refresh all dynamic entries.

|<<: Updates the table starting from the first entry in the MAC Table, i.e. the entry with the lowest VLAN ID and MAC address.

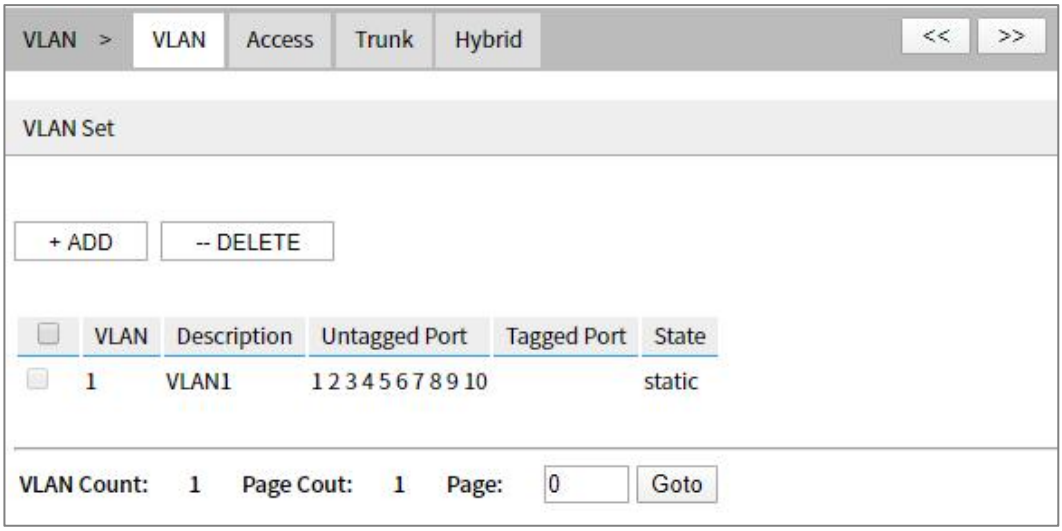
>>: Updates the table, starting with the entry after the last entry currently displayed.

6.2 VLAN

VLAN (Virtual Local Area Network) is a communication technology that logically divides a physical LAN into multiple broadcast domains. Hosts in VLAN can directly communicate with each other, but two VLAN can't directly communicate with each other, which can limit the broadcast message in a VLAN.

6.2.1 VLAN

On this page, users can create VLAN and edit VLAN description.



VLAN Configuration

VLAN configuration can display up to 40 VLAN entries on each page, and the page can be switched through the "Goto", "<<” or ">>" buttons.

VLAN

VLAN ID number, value range is 1-4094.

Description

Description information of VLAN.

Untagged Port

Untagged port member to conduct untagged process to sending data frame.

Tagged Port

Tag port member to conduct tagged process to sending data frame.

Status

Status type:

- Static Configuration
- Dynamic。

Buttons

+Add: click to add new VLAN.

--Delete: Click to delete the selected VLAN. (VLAN1 cannot be deleted)

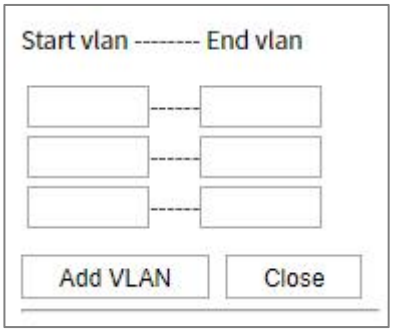
Goto: enter the specified page in “Page” and click “Goto” to jump to the specified page.

<<: Click to display the previous page.

>>: Click to display the next page.

Add

Click the "+ add" button to display the “Add VLAN” input field.



Start VLAN

The start VLAN ID of the new VLAN range, with a value range of 1-4094.

End VLAN

The end VLAN ID of the new VLAN range, with a value range of 1-4094. The start VLAN ID must be less than or equal to the end VLAN ID.

Buttons

Add VLAN: Click to add VLAN within the specified range.

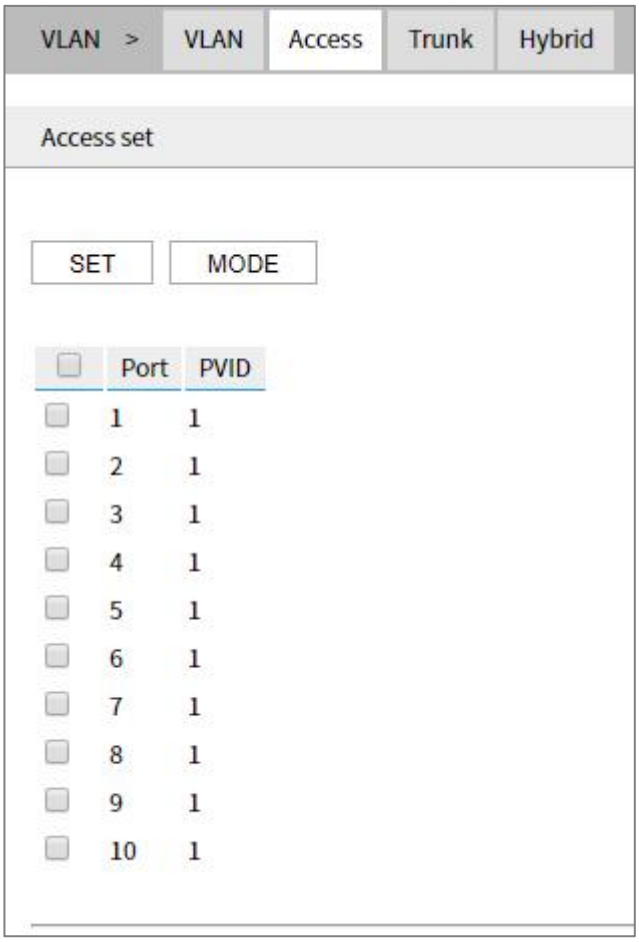
Close: Click to add VLAN.

6.2.2 Access

There are three port modes that the switch supports:

- Access: port only belongs to 1 VLAN(which is the default VLAN), all ports of the switch are Access mode by default and all PVID are 1.
- Trunk: port can belong to multiple VLAN, Trunk port can allow the messages of multiple VLANs to pass with Tag, but only allow the messages of one VLAN to transmit without tag (strip Tag) from this kind of interface. Commonly used in the connection between network devices.
- Hybrid: port can belong to multiple VLANs. Hybrid port allows messages of multiple VLANs to pass with tag, and allows the messages sent from this kind of interface to configure whether the messages of some VLANs is with tag (not strip Tag) or not (strip Tag) . It could be used in the connection between network devices, as well as user devices.

This page allows you to modify the PVID and port mode of the Access port.



Port

The corresponding port name of the device Ethernet port.

Port VLAN ID

PVID value, it defaults to 1, value range is 1-4094. Each port has a PVID property, when the port receives Untag messages, it adds Tag mark on them according to PVID. When the port transmits data message with the same Tag mark as PVID, it would erase the Tag mark and then transmit the message. The PVID of all ports default to 1.

Buttons

Configuration: Click to configure the PVID of the selected port.

Port Mode: Click to configure the port mode of the selected port.

Change Port VLAN

Check the port to be modified, and then click “Configure” to modify the PVID of the port.

Change Port VLAN

Change the PVID number of the specified port, ranging from 1-4094.

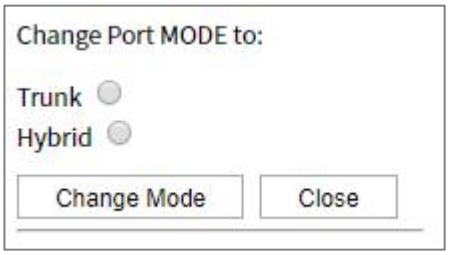
Buttons

Modify VLAN: Click to modify the configuration of the selected port.

Close: Click to cancel the modification.

Change Port Mode

Check the port to be modified, and then click "Mode" to modify the port type.



Change Port Mode

Modify the mode of the specified port. The options are as follows.

- Trunk。
- Hybrid。

If the port mode is set to Trunk or Hybrid, the port display will be updated to the page of “Trunk” or “Hybrid”. Similarly, for "Trunk" or "Hybrid" ports, you can also change the port mode to Access.

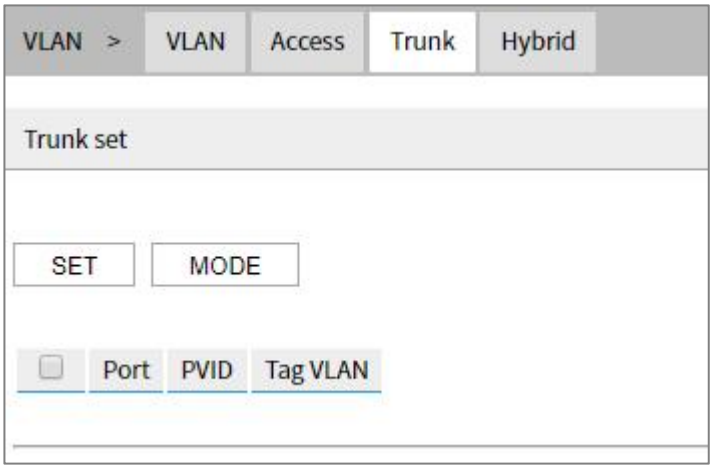
Buttons

Change port type: after selecting the port mode, click to modify the mode of the selected port.

Close: Click to cancel modifying the mode of the selected port.

6.2.3 Trunk

On this page, user can configure the relevant parameters of Trunk port.



Port

The corresponding port name of the device Ethernet port.

Port VLAN ID

VLAN ID number, value range is 1-4094.

TagVLAN

The VLAN ID number that the port allows to pass, a tagged value, a single value or range (the range is indicated by "-"). For example: 9 or 10-15.

Buttons

Set: Check the entries that need to be reconfigured, click “Set” to reset PVID value and TagVLAN parameters.

Port Mode: Click to configure the port mode of the selected port.

Change Port VLAN and AllowVLAN

Check the port to be modified, and then click “Mode” to modify the PVID of the port and the VLAN allowed to pass through.

Change Port VLAN

Change the PVID number of the specified port, ranging from 1-4094.

Change Port AllowVLAN

Modify or configure the VLAN ID that the specified ports allow to pass through. The value range is 1-4094, such as "2-3, 100". VLAN ID value uses "-" to represent a VLAN range, or separated by ",". Chinese symbols are not supported and VLAN should exist.

Buttons

Modify VLAN: Click to modify the configuration of the selected port.

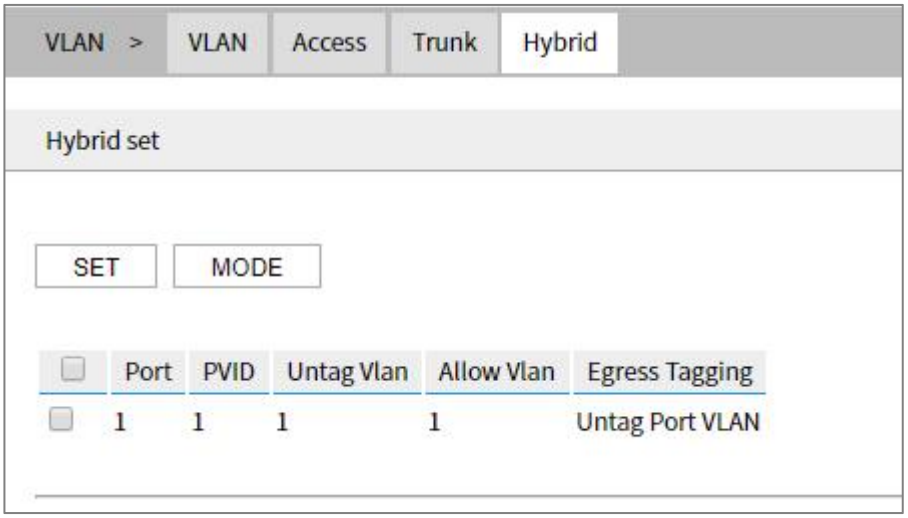
Close: Click to cancel the modification.

Change Port Mode

Check the port to be modified, and then click "Mode" to set the port mode to Access or Hybrid. Changing the port mode page configuration is similar to access and will not be repeated here.

6.2.4 Hybrid

On this page, user can configure the relevant parameters of Hybrid port mode.



Port

The corresponding port name of the device Ethernet port.

Port VLAN ID

VLAN ID number, value range is 1-4094.

Untag Vlan

The VLAN ID number that the port allows to pass without tags.

Allow Vlan

The VLAN ID number that the port allows to pass, a single value or range (the range is indicated by "-"). For example: 9 or 10-15.

Egress Tagging

Processing mode of Hybrid interface for marking of exit message;

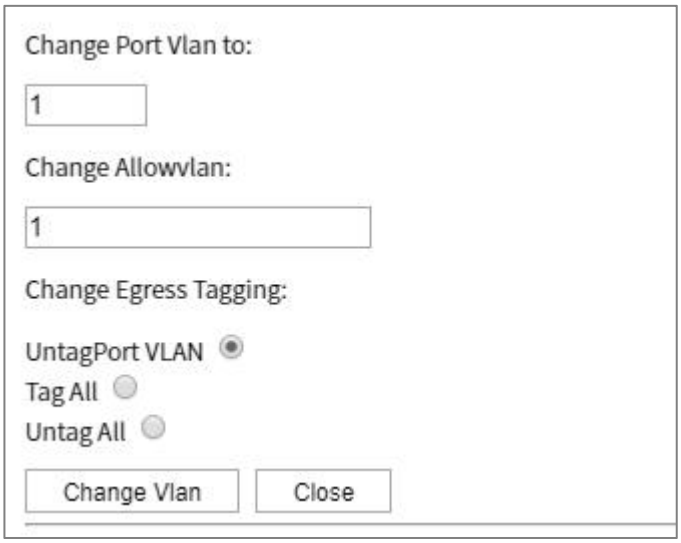
- UntagPortVLAN：PVID is not tagged;
- TagAll: Tag all VLAN;
- UntagAll: Untag all VLAN.

Buttons

- Set: Check the entries that need to be reconfigured, click “Set” to reset PVID value and VLAN parameters.
- Port Mode: Click to configure the port mode of the selected port.

Change Port VLAN, AllowVLAN, and Egress Tag Type

Check the port to be modified, and then click “Mode” to modify the PVID of the port, the VLAN allowed to pass through and the processing of egress tags.



Change Port VLAN

Change the PVID number of the specified port, ranging from 1-4094.

Change AllowVLAN

Modify or configure the VLAN ID that the specified ports allow to pass through. The value range is 1-4094, such as "2-3, 100". VLAN ID value uses "-" to represent a VLAN range, or separated by ",". Chinese symbols are not supported and VLAN should exist.

Change Egress Tag Type

Modify or configure the processing method of the interface for egress message tags:

- UntagPortVLAN：PVID is not tagged;
- TagAll: Tag all VLAN;
- UntagAll: Untag all VLAN.

Buttons

Modify VLAN: Click to modify the configuration of the selected port.

Close: Click to cancel the modification.

Change Port Mode

Check the port to be modified, and then click "Port Mode" to set the port mode to Access or Trunk. Changing the port mode page configuration is similar to access and will not be repeated here.

Process for Port Receiving Message

Interface type	Process for Receiving Untagged Message	Process for Receiving Tagged Message
Access	Receive this message and tag it with default VLAN ID.	• Receive the message when the VLAN ID is the same as default

Interface type	Process for Receiving Untagged Message	Process for Receiving Tagged Message
		VLAN ID. • Discard the message when the VLAN ID is different from the default VLAN ID.
Trunk	Receive this message and tag it with default VLAN ID.	• Receive this message when the VLAN ID is in the list of VLAN ID that allow to pass through the interface. • Discard this message when the VLAN ID is not in the list of VLAN ID that allow to pass through the interface.
Hybrid		

Process for Port Sending Message

Interface type	The process of transmit frame
Access	Strip the PVID Tag of the message first, then transmit it.
Trunk	• When the VLAN ID is the same as the default VLAN ID, and it is the VLAN ID allowed to pass through the interface, it would strip the Tag and send this message. • When the VLAN ID is different from the default VLAN ID, and it's the VLAN ID allowed to pass through the interface, it would remain its original Tag and send the message.
Hybrid	When the VLAN ID is the one allowed to pass through the interface, it would send this message. It could be set to whether to carry Tag during transmission.

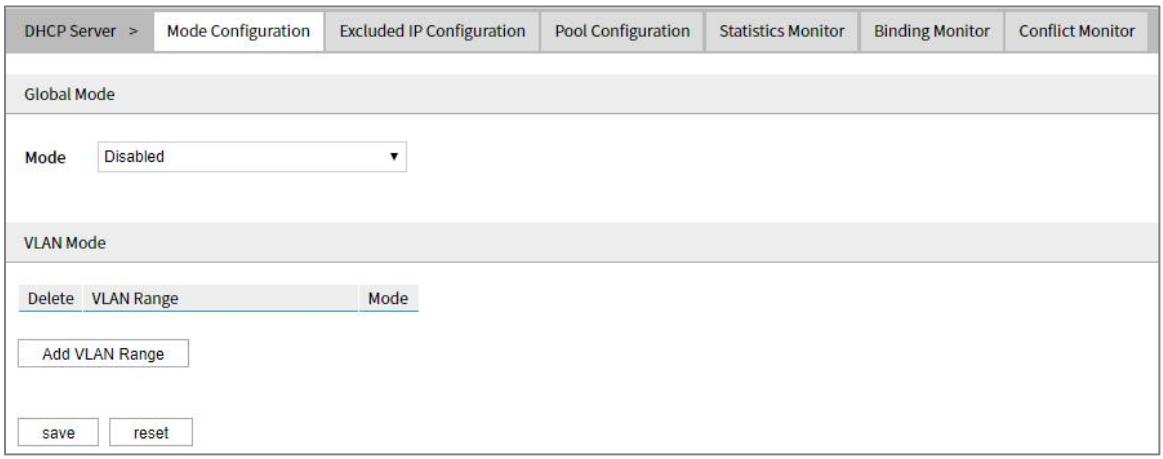
6.3 DHCP server

DHCP (Dynamic Host Configuration Protocol) is a technology used for centralized and dynamic user IP address management and configuration.

DHCP adopts client/server communication mode that the DHCP client submits configuration application to the DHCP server, then the server returns the configuration information (including IP address, default gateway, DNS) allocated for the client. This can realize the dynamic allocation of IP addresses and centralized configuration management of other network parameters.

6.3.1 Mode Setting

This page configures global mode and VLAN mode to enable/disable DHCP server per system and per VLAN.



Global Mode

Pattern

Configure operation mode to enable/disable DHCP server per system. Possible modes are:

- Enabled: Enable DHCP server per system.
- Disabled: Disable DHCP server per system.

VLAN

Configure operation mode to enable/disable DHCP server per VLAN.

Delete

Click the “Delete” button to undo the entry being added.

VLAN Range

Indicate the VLAN range in which DHCP server is enabled or disabled. The first VLAN ID must be smaller than or equal to the second VLAN ID. BUT, if the VLAN range contains only 1 VLAN ID, then you can just input it into either one of the first and second VLAN ID or both.

On the other hand, if you want to disable/delete existed VLAN range, then you can follow the steps.

1 Click “Add VLAN Range” to add a new VLAN range.

2 Input the VLAN range that you want to disable.

3 Choose Mode to be disabled.

4 Press “Save” to apply the change.

Then, you will see the disabled VLAN range is removed from the DHCP Server mode configuration page.

Mode

Indicate the operation mode per VLAN. Possible modes are:

- Enabled: Enable DHCP server per VLAN.
- Disabled: Disable DHCP server per VLAN.

Buttons

Add VLAN range: click to add new VLAN range.

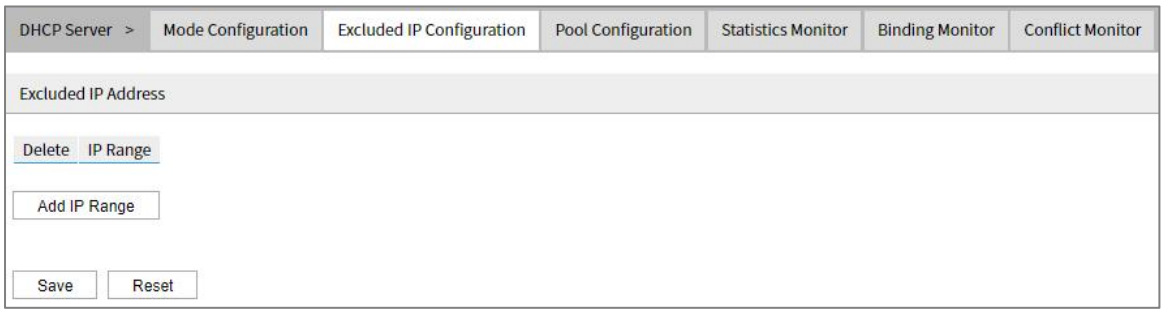
Delete: Click to undo the entry being added.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

6.3.2 Reserve IP Address Configuration

This page configures excluded IP addresses. DHCP server will not allocate these excluded IP addresses to DHCP client.



Excluded IP Address

Delete

Select this check box and click the “Save” button to delete the corresponding entry.

IP Range

Define the IP range to be excluded IP addresses. The first excluded IP must be smaller than or equal to the second excluded IP. BUT, if the IP range contains only 1 excluded IP, then you can just input it to either one of the first and second excluded IP or both.

Buttons

Add IP range: Click to add a new excluded IP range.

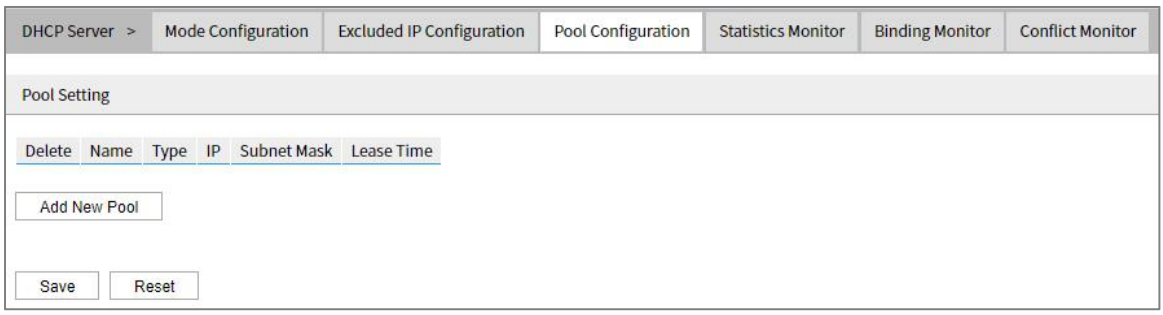
Delete: Click to undo the entry being added.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

6.3.3 DHCP Pool Configuration

This page manages DHCP pools. According to the DHCP pool, DHCP server will allocate IP address and deliver configuration parameters to DHCP client.



Pool Setting

Delete

Select this check box and click the “Save” button to delete the corresponding entry.

Name

Configure the pool name that accepts all printable characters, except white space. If you want to configure the detail settings, you can click the pool name to go into the configuration page.

Type

Display which type of the pool is.

- Network: the pool defines a pool of IP addresses to service more than one DHCP client.
- Host: the pool services for a specific DHCP client identified by client identifier or hardware address.
- -: If "-" is displayed, it means not defined.

IP

Display network number of the DHCP address pool.

If "-" is displayed, it means not defined.

Subnet Mask

Display subnet mask of the DHCP address pool.

If "-" is displayed, it means not defined.

Lease Time

Display lease time of the pool.

Buttons

Add new address pool: click to add a DHCP pool.

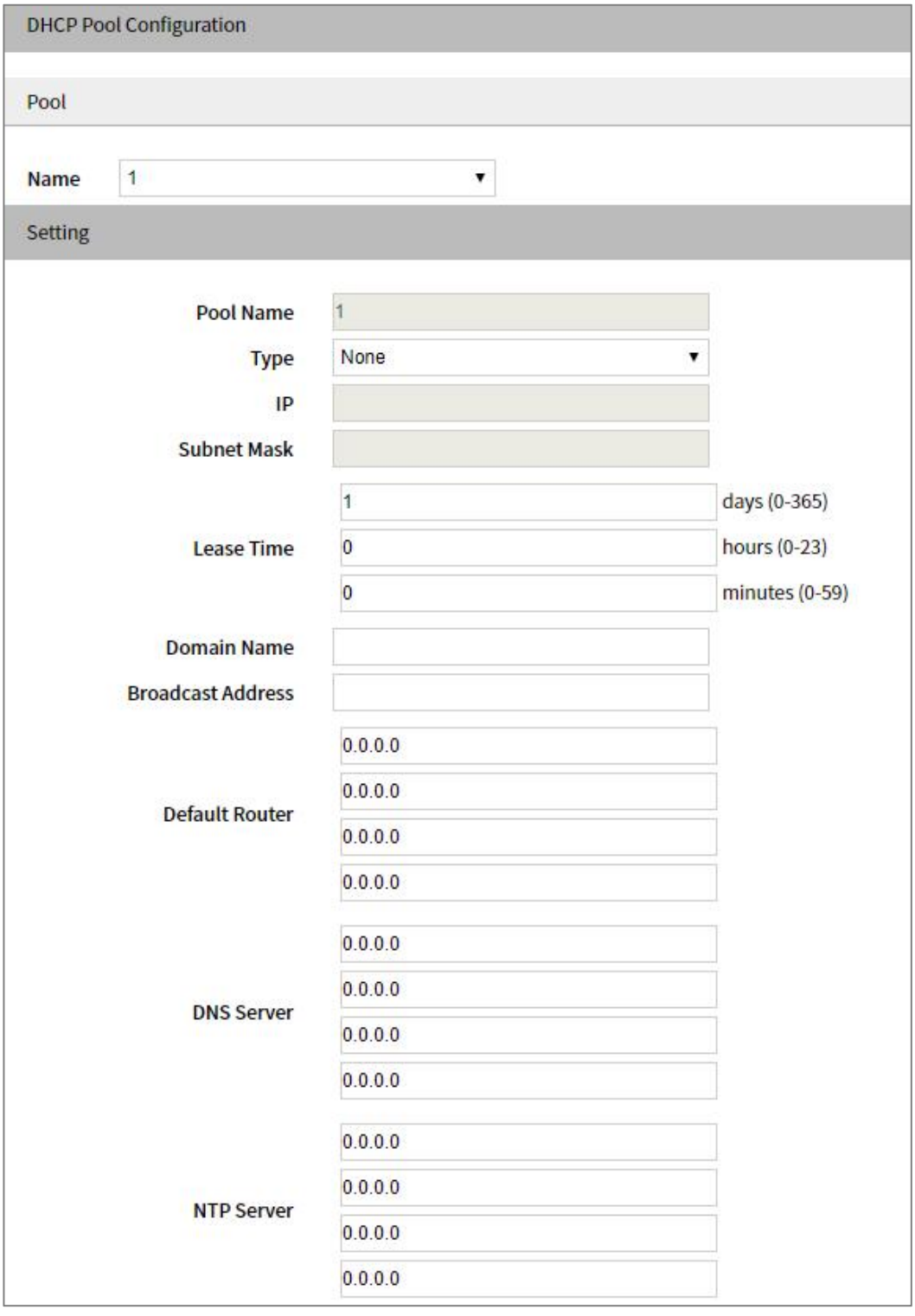
Delete: Click to undo the entry being added.

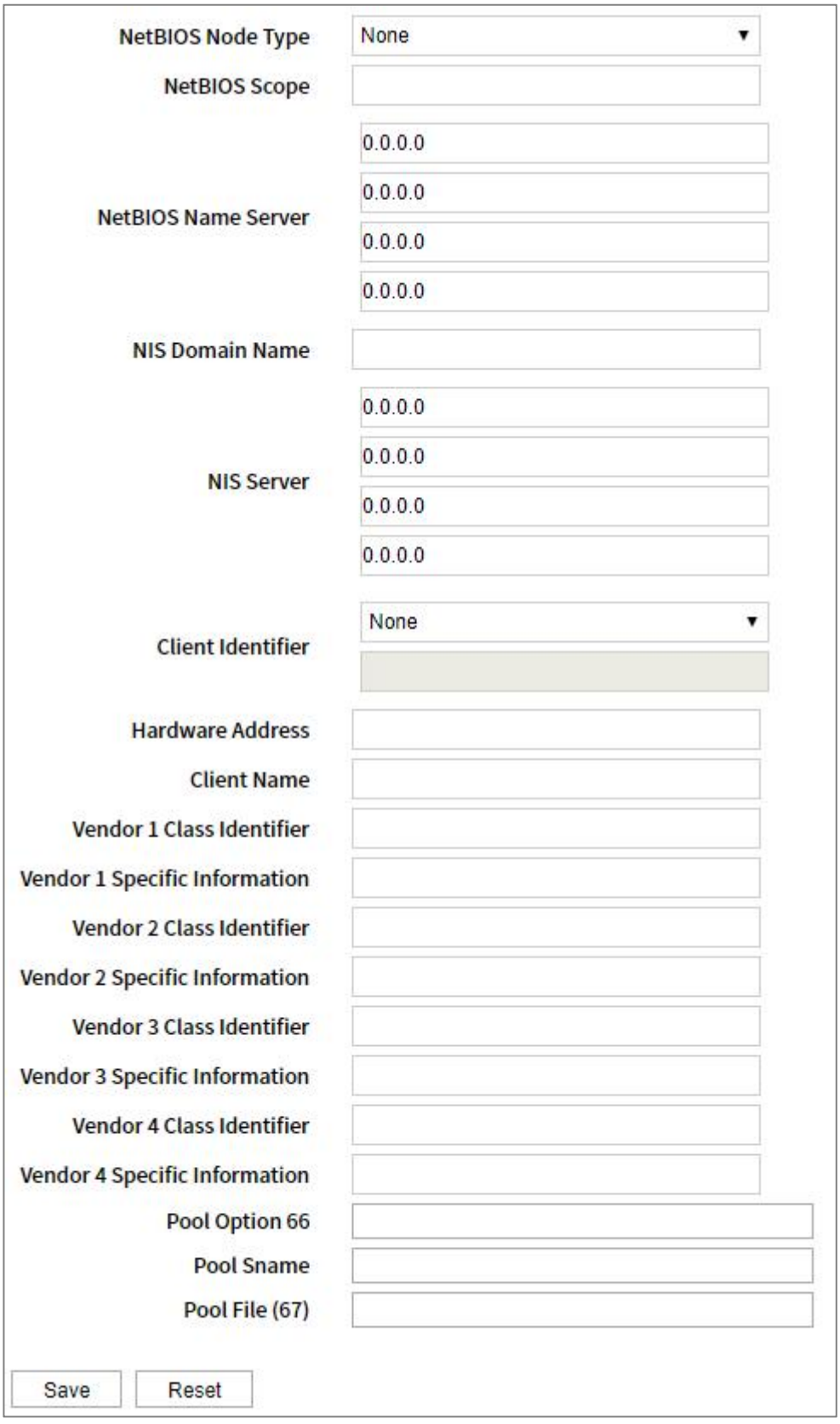
Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

DHCP Pool Configuration

Click the address pool name link to enter the “DHCP address pool configuration” page.


DHCP Pool Configuration
Pool
Name
1
Setting
Pool Name
1
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



Name

Select a pool to configure the settings.

Name

Select a pool by pool name.

Setting

Configure pool settings.

Name

Display the selected pool name.

Type

Specify which type of the pool is.

- None
- Network: the pool defines a pool of IP addresses to service more than one DHCP client.
- Host: the pool services for a specific DHCP client identified by client identifier or hardware address.

IP

Specify network number of the DHCP address pool.

Subnet Mask

DHCP option 1.

Specify subnet mask of the DHCP address pool.

Lease Time

DHCP option 51, 58 and 59.

Specified Lease Time. Allow the client to request a lease time for the IP address. If all are 0, then it means the lease time is infinite.

Domain Name

DHCP option 15.

Specify domain name that client should use when resolving hostname via DNS.

Broadcast Address

DHCP option 28.

Specify the broadcast address in use on the client's subnet.

Default Router

DHCP option 3.

Specify a list of IP addresses for routers on the client's subnet.

DNS Server

DHCP option 6.

Specify a list of Domain Name System name servers available to the client.

NTP Server

DHCP option 42.

Specify a list of IP addresses indicating NTP servers available to the client.

NetBIOS Node Type

DHCP option 46.

Specify NetBIOS node type option to allow Netbios over TCP/IP clients which are configurable to be configured as described in RFC 1001/1002.

NetBIOS Scope

DHCP option 47.

Specify the NetBIOS over TCP/IP scope parameter for the client as specified in RFC 1001/1002.

NetBIOS Server

DHCP option 44.

Specify a list of NBNS name servers listed in order of preference.

NIS Domain Name

DHCP option 40.

Specify the name of the client's NIS domain.

NIS Server

DHCP option 41.

Specify a list of IP addresses indicating NIS servers available to the client.

Client Identifier

DHCP option 61.

Specify client's unique identifier to be used when the pool is the type of host.

Hardware Address

Specify client's hardware(MAC) address to be used when the pool is the type of host.

Client Name

DHCP option 12.

Specify the name of client to be used when the pool is the type of host.

Vendor # Class Identifier

DHCP option 60.

Specify to be used by DHCP client to optionally identify the vendor type and configuration of a DHCP client. DHCP server will deliver the corresponding option 43 specific information to the client that sends option 60 vendor class identifier.

Vendor # Specific Information

DHCP option 43.

Specify vendor specific information according to option 60 vendor class identifier.

Pool Option 66

This option identifies the TFTP server when the "Sname" field in the DHCP header is used as a DHCP option. Set TFTP server IP address for specifying the address of the TFTP server assigned to the client.

Pool Sname

This field indicates the name of the server from which a client obtains configuration information. Specifies a TFTP server name allocated to DHCP clients.

Pool File（67）

DHCP option 67.

Set boot filename option to specify the boot filename assigned to the client.

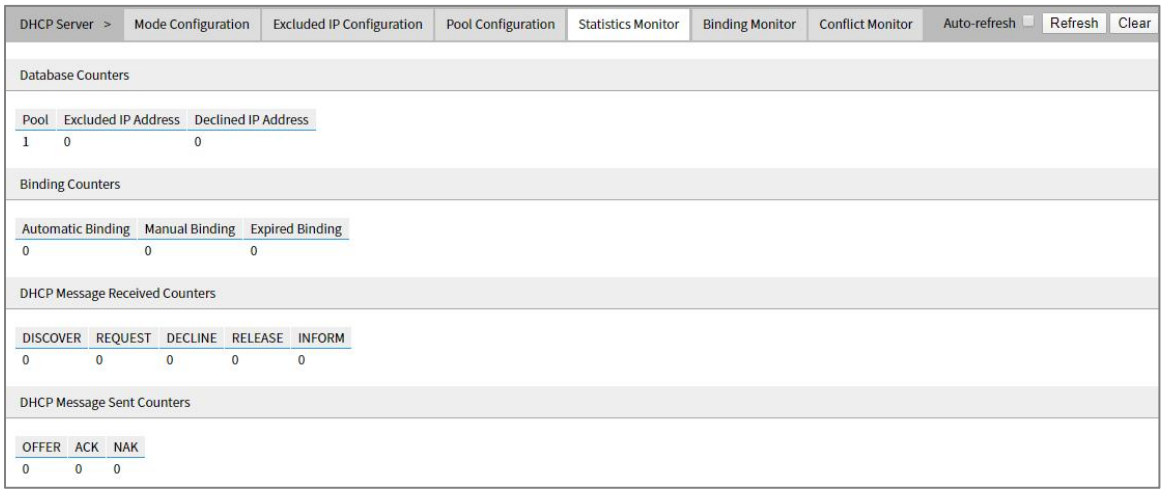
Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

6.3.4 Statistics Monitoring

This page displays the database counters and the number of DHCP messages sent and received by DHCP server.



Database Counters

Display counters of various databases.

Pool

Number of pools.

Excluded IP Address

Number of excluded IP address ranges.

Declined IP Address

Number of declined IP addresses.

Binding Counters

Display counters of various databases.

Automatic Binding

Number of bindings with Network-type pools.

Manual Binding

Number of bindings that administrator assigns an IP address to a client. That is, the pool is of Host type.

Expired Binding

Number of bindings that their lease time expired or they are cleared from Automatic/Manual type bindings.

DHCP Message Received Counters

Display counters of DHCP messages received by DHCP server.

DISCOVER

Number of DHCP DISCOVER messages received.

REQUEST

Number of DHCP REQUEST messages received.

DECLINE

Number of DHCP DECLINE messages received.

RELEASE

Number of DHCP RELEASE messages received.

INFORM

Number of DHCP INFORM messages received.

DHCP Message Sent Counters

Display counters of DHCP messages sent by DHCP server.

OFFER

Number of DHCP OFFER messages sent.

ACK

Number of DHCP ACK messages sent.

NAK

Number of DHCP NAK messages sent.

Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

Clear: Click to clear the statistics information.

6.3.5 Binding Monitoring

This page displays bindings generated for DHCP clients.

Binding IP Address

Display all bindings.

IP

IP address allocated to DHCP client.

Type

Type of binding. Possible types are Automatic, Manual, Expired.

Status

State of binding. Possible states are Committed, Allocated, Expired.

Pool Name

The pool that generates the binding.

Server ID

Server IP address to service the binding.

Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

Clear selected: click to clear selected bindings. If the selected binding is Automatic or Manual, then it is changed to be Expired. If the selected binding is Expired, then it is freed.

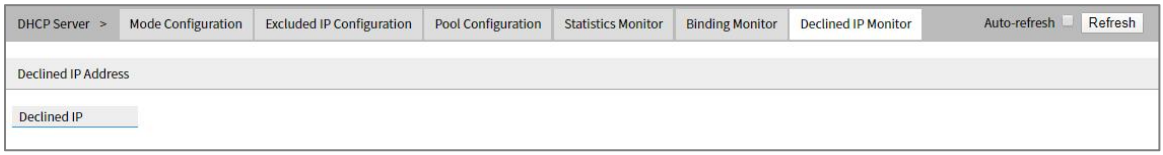
Clear Automatic: Click to clear all automatic bindings and change them to expired bindings.

Clear Manual: Click to clear all manual bindings and change them to expired bindings.

Clear Expired: Click to clear all expired bindings and free them.

6.3.6 Conflict Monitoring

This page displays declined IP addresses.



Conflicting IP addresses

Conflicting IP

List of IP addresses declined.

Buttons

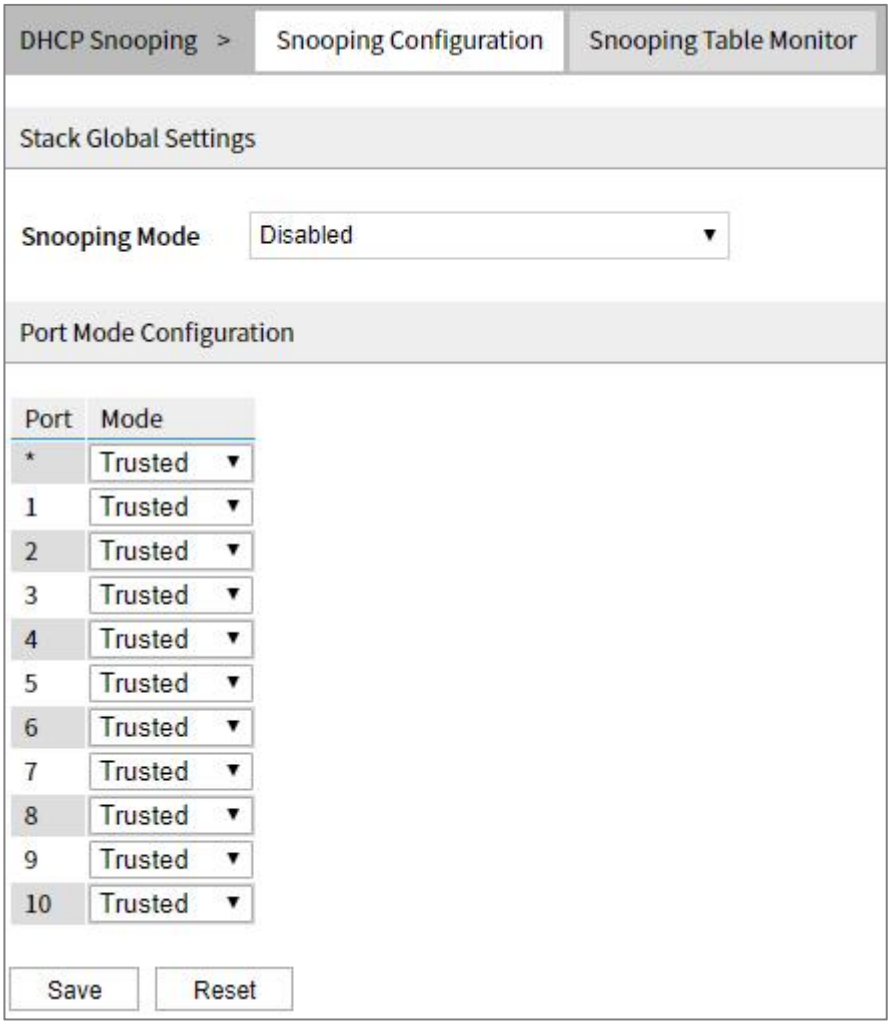
Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

6.4 DHCP Snooping

6.4.1 Listening Configuration

Configure DHCP Snooping on this page.



Stack Global Settings

Snooping Mode

Indicates the DHCP snooping mode operation. Possible modes are:

- Enabled: Enable DHCP snooping mode operation. When DHCP snooping mode operation is enabled, the DHCP request messages will be forwarded to trusted ports and only allow reply packets from trusted ports.
- Disabled: Disable DHCP snooping mode operation.

Port Mode Configuration

Pattern

Indicates the DHCP snooping port mode. Possible port modes are:

- Trusted: Configures the port as trusted source of the DHCP messages.
- Untrusted: Configures the port as untrusted source of the DHCP messages.

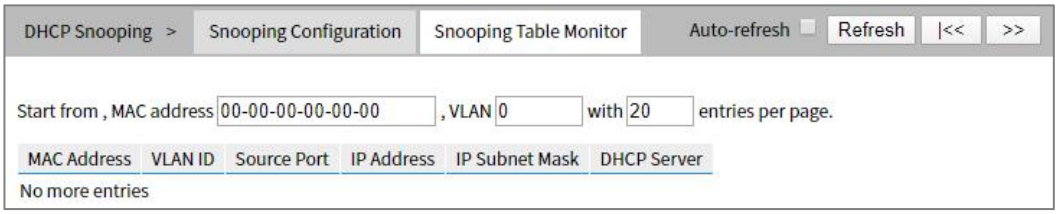
Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

6.4.2 Listening Table Monitoring

This page display the dynamic IP assigned information after DHCP Snooping mode is disabled. All DHCP clients obtained the dynamic IP address from the DHCP server will be listed in this table except for local VLAN interface IP addresses. Entries in the Dynamic DHCP snooping Table are shown on this page.



Each page shows up to 99 entries from the Dynamic DHCP snooping table, default being 20, selected through the "per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Dynamic DHCP snooping Table.

The "MAC address" and "VLAN" input fields allows the user to select the starting point in the Dynamic DHCP snooping Table. Clicking the “Refresh” button will update the displayed table starting from that or the closest next Dynamic DHCP snooping Table match. In addition, the two input fields will - upon a “Refresh” button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

“>>” will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the “|<<” button to start over.

MAC address

User MAC address of the entry.

VLAN

VLAN-ID in which the DHCP traffic is permitted.

Source Port

Switch Port Number for which the entries are displayed.

IP Address

User IP address of the entry.

IP Subnet Mask

User IP subnet mask of the entry.

DHCP Server

DHCP Server address of the entry.

Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Refresh the displayed table starting from the input fields.

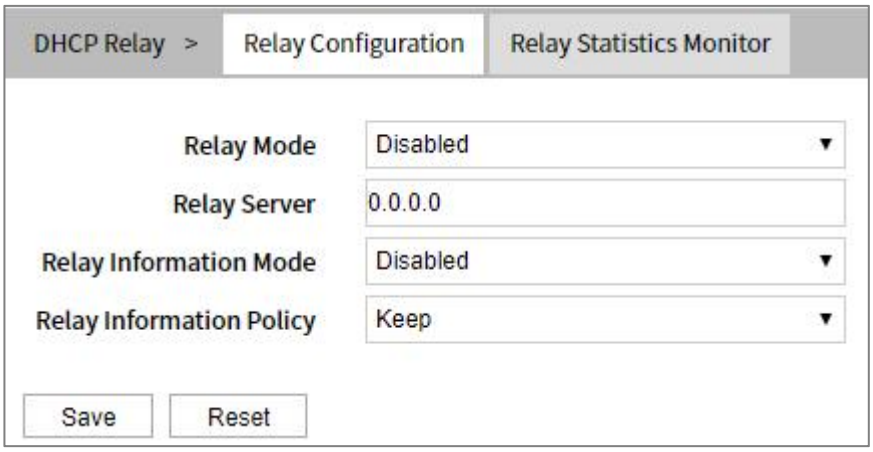
|<<: Updates the table starting from the first entry in the Dynamic DHCP snooping Table.

>>: Updates the table, starting with the entry after the last entry currently displayed.

6.5 DHCP Relay

6.5.1 Relay Configuration

A DHCP relay agent is used to forward and to transfer DHCP messages between the clients and the server when they are not in the same subnet domain. It stores the incoming interface IP address in the GIADDR field of the DHCP packet. The DHCP server can use the value of GIADDR field to determine the assigned subnet. For such condition, please make sure the switch configuration of VLAN interface IP address and PVID (Port VLAN ID) correctly.



Relay Mode

Indicates the DHCP relay mode operation. Possible modes are:

- Enabled: Enable DHCP relay mode operation. When DHCP relay mode operation is enabled, the agent forwards and transfers DHCP messages between the clients and the server when they are not in the same subnet domain. And the DHCP broadcast message won't be flooded for security considerations.

- Disabled: Disable DHCP relay mode operation.

Relay Server

Indicates the DHCP relay server IP address.

Relay Information Mode

Indicates the DHCP relay information mode option operation. The option 82 circuit ID format as "[vlan_id][module_id][port_no]". The first four characters represent the VLAN ID, the fifth and sixth characters are the module ID(in standalone device it always equal 0, in stackable device it means switch ID), and the last two characters are the port number. For example, "00030108" means the DHCP message receive form VLAN ID 3, switch ID 1, port No 8. And the option 82 remote ID value is equal the switch MAC address.

Possible modes are:

- Enabled: Enable DHCP relay information mode operation. When DHCP relay information mode operation is enabled, the agent inserts specific information (option 82) into a DHCP message when forwarding to DHCP server and removes it from a DHCP message when transferring to DHCP client. It only works when DHCP relay operation mode is enabled.
- Disabled: Disable DHCP relay information mode operation.

Relay Information Policy

Indicates the DHCP relay information option policy. When DHCP relay information mode operation is enabled, if the agent receives a DHCP message that already contains relay agent information it will enforce the policy. The 'Replace' policy is invalid when relay information mode is disabled. Possible policies are:

- Replace: Replace the original relay information when a DHCP message that already contains it is received.
- Keep: Keep the original relay information when a DHCP message that already contains it is received.
- Drop: Drop the package when a DHCP message that already contains relay information is received.

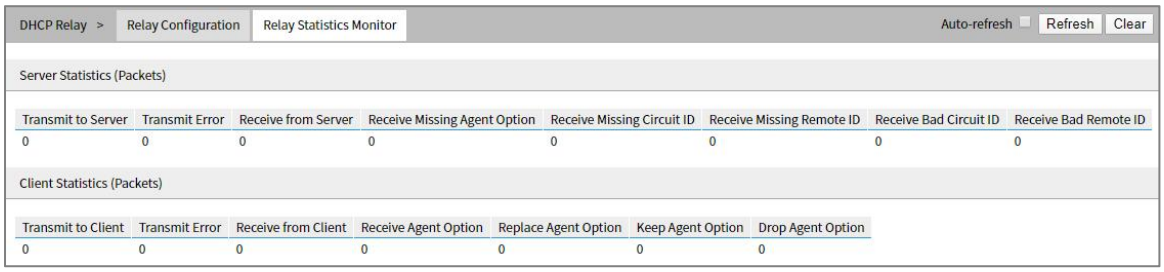
Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

6.5.2 Relay Statistics Monitoring

This page provides statistics for DHCP relay.



Server Statistics

Send to Server

The number of packets that are relayed from client to server.

Send Error

The number of packets that resulted in errors while being sent to clients.

Receive from Server

The number of packets received from server.

Receive No Agent Option

The number of packets received without agent information options.

Receive No Circuit ID

The number of packets received with the Circuit ID option missing.

Receive No Remote ID

The number of packets received with the Remote ID option missing.

The received Circuit ID does not match

The number of packets whose Circuit ID option did not match known circuit ID.

The receive Remote ID does not match

The number of packets whose Remote ID option did not match known Remote ID.

Client Statistics

Send to Client

The number of relayed packets from server to client.

Transmit Error

The number of packets that resulted in error while being sent to servers.

Receive from Client

The number of received packets from server.

Receive Agent Option

The number of received packets with relay agent information option.

Replace Agent Option

The number of packets which were replaced with relay agent information option.

Retain Agent Option

The number of packets whose relay agent information was retained.

Discard Agent Option

The number of packets that were dropped which were received with relay agent information.

Buttons

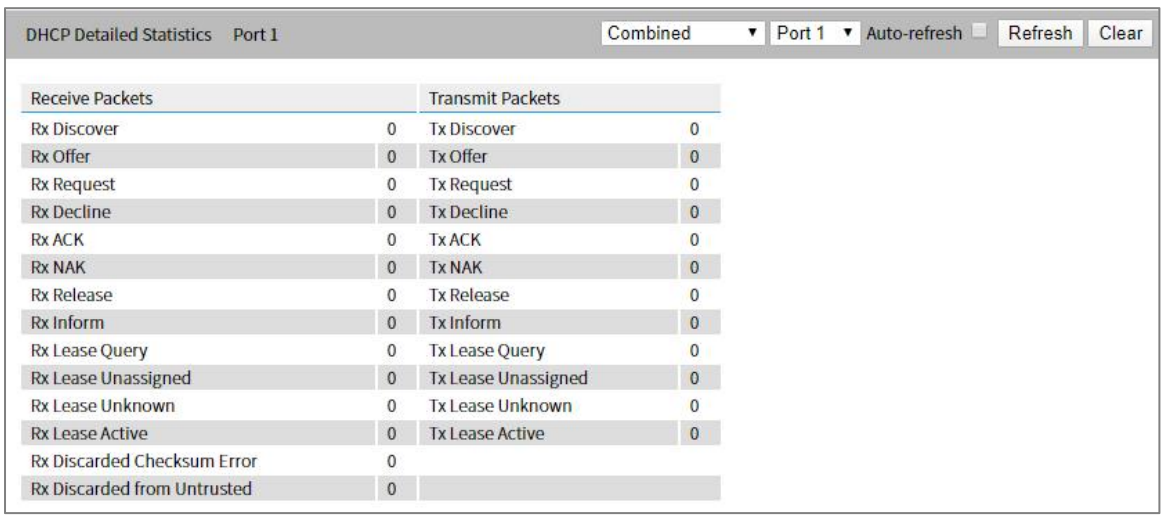
Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

Clear: : Clear all statistics.

6.6 DHCP Detailed Statistics

This page provides statistics for DHCP snooping. Notice that the normal forward per-port TX statistics isn't increased if the incoming DHCP packet is done by L3 forwarding mechanism. And clear the statistics on specific port may not take effect on global statistics since it gathers the different layer overview.



Receive and Transmit Packets

Rx and Tx Discover

The number of Discover (option 53 with value 1) packets received and transmitted.

Rx and Tx Offer

The number of Offer (option 53 with value 2) packets received and transmitted.

Rx and Tx Request

The number of Request (option 53 with value 3) packets received and transmitted.

Rx and Tx Decline

The number of Decline (option 53 with value 4) packets received and transmitted.

Rx and Tx ACK

The number of ACK (option 53 with value 5) packets received and transmitted.

Rx and Tx NAK

The number of NAK (option 53 with value 6) packets received and transmitted.

Rx and Tx Release

The number of Release (option 53 with value 7) packets received and transmitted.

Rx and Tx Inform

The number of Inform (option 53 with value 8) packets received and transmitted.

Rx and Tx Lease Query

The number of lease query (option 53 with value 10) packets received and transmitted.

Rx and Tx Lease Unassigned

The number of lease unassigned (option 53 with value 11) packets received and transmitted.

Rx and Tx Lease Unknown

The number of lease unknown (option 53 with value 12) packets received and transmitted.

Rx and Tx Lease Active

The number of lease active (option 53 with value 13) packets received and transmitted.

Rx Discarded checksum error

The number of discard packet that IP/UDP checksum is error.

Rx Discarded from Untrusted

The number of discarded packet that are coming from untrusted port.

Buttons

Combined ▼: the DHCP user select box determines which user is affected by clicking the buttons. Options are as follows:

- Combined
- Normal Forward
- Server
- Client
- Snooping
- Relay

Port 1 ▼: the port select box determines which port is affected by clicking the buttons.

Auto-refresh: Check this box to enable an automatic refresh. Automatic refresh occurs every 3 seconds.

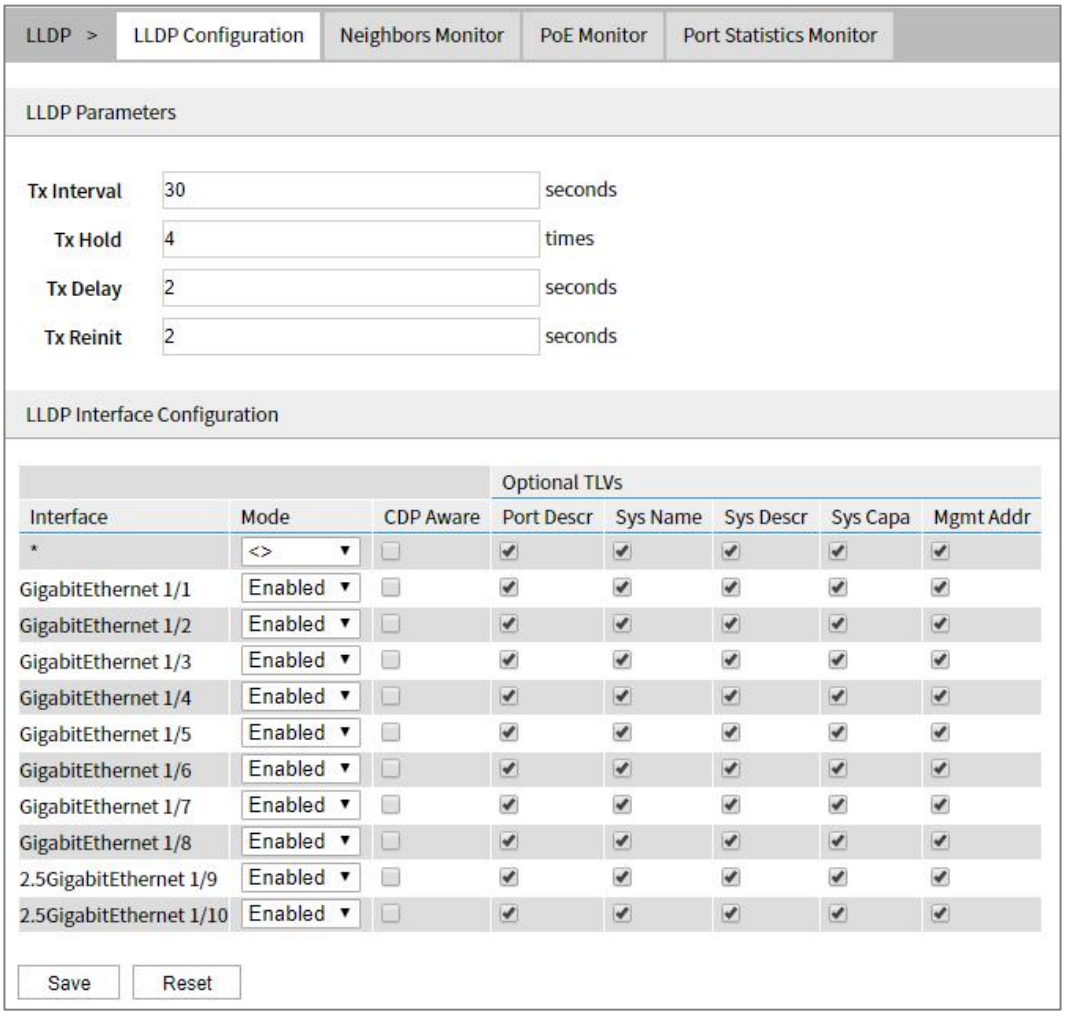
Refresh: Click to refresh the page immediately.

Clear: clear the counters of all ports.

6.7 LLDP

6.7.1 LLDP Configuration

This page allows the user to inspect and configure the current LLDP interface settings.



LLDP Parameters

Tx Interval

The switch periodically transmits LLDP frames to its neighbors for having the network discovery information up-to-date. The interval between each LLDP frame is determined by the Tx Interval value. Valid values are restricted to 5 - 32768 seconds.

Tx Hold

Each LLDP frame contains information about how long time the information in the LLDP frame shall be considered valid. The LLDP information valid period is set to Tx Hold multiplied by Tx Interval seconds. Valid values are restricted to 2 - 10 times.

Tx Delay

If some configuration is changed (e.g. the IP address) a new LLDP frame is transmitted, but the time between the LLDP frames will always be at least the value of Tx Delay seconds. Tx Delay cannot be larger than 1/4 of the Tx Interval value. Valid values are restricted to 1 - 8192 seconds.

Tx Reinit

When a interface is disabled, LLDP is disabled or the switch is rebooted, a LLDP shutdown frame is transmitted to the neighboring units, signaling that the LLDP information isn't valid anymore. Tx Reinit controls the amount of seconds between the shutdown frame and a new LLDP initialization. Valid values are restricted to 1 - 10 seconds.

LLDP Interface Configuration

Interface

The switch interface name of the logical LLDP interface.

Pattern

Select LLDP mode.

- Rx only: The switch will not send out LLDP information, but LLDP information from neighbor units is analyzed.
- Tx only: The switch will drop LLDP information received from neighbors, but will send out LLDP information.
- Disabled: The switch will not send out LLDP information, and will drop LLDP information received from neighbors.
- Tx and Rx: The switch will send out LLDP information, and will analyze LLDP information received from neighbors.

CDP Aware

Select CDP awareness.

The CDP operation is restricted to decoding incoming CDP frames (The switch doesn't transmit CDP frames). CDP frames are only decoded if LLDP on the interface is enabled.

Only CDP TLVs that can be mapped to a corresponding field in the LLDP neighbors table are decoded. All other TLVs are discarded (Unrecognized CDP TLVs and discarded CDP frames are not shown in the LLDP statistics.). CDP TLVs are mapped onto LLDP neighbors' table as shown below.

- CDP TLV "Device ID" is mapped to the LLDP "Chassis ID" field.
- CDP TLV "Address" is mapped to the LLDP "Management Address" field. The CDP address TLV can contain multiple addresses, but only the first address is shown in the LLDP neighbors table.
- CDP TLV Port ID is mapped to the LLDP Port ID field.
- CDP TLV Version and Platform is mapped to the LLDP System Description field.

Both the CDP and LLDP support system capabilities, but the CDP capabilities cover capabilities that are not part of the LLDP. These capabilities are shown as others in the LLDP neighbors table.

If all interfaces have CDP awareness disabled the switch forwards CDP frames received from neighbor devices. If at least one interface has CDP awareness enabled all CDP frames are terminated by the switch.

Note:

When CDP awareness on an interface is disabled the CDP information isn't removed immediately, but gets removed when the hold time is exceeded.

Port Description

Optional TLV: When checked the "port description" is included in LLDP information transmitted.

System Name

Optional TLV: When checked the "system name" is included in LLDP information transmitted.

System description

Optional TLV: When checked the "system description" is included in LLDP information transmitted.

System Capabilities

Optional TLV: When checked the "system capability" is included in LLDP information transmitted.

Management address

Optional TLV: When checked the "management address" is included in LLDP information transmitted.

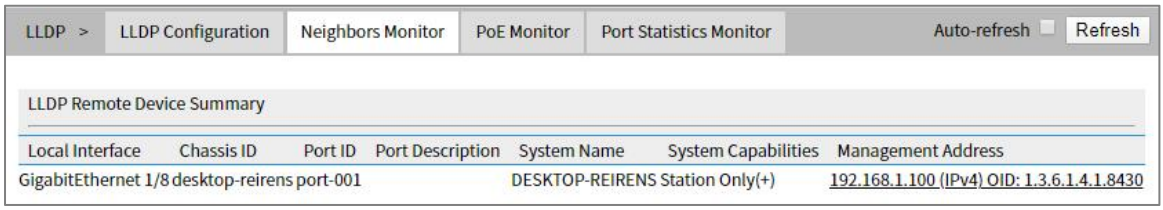
Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

6.7.2 LLDP Neighbor Information

This page provides a status overview for all LLDP neighbors. The displayed table contains a row for each interface on which an LLDP neighbor is detected. The columns hold the following information:



Local Interface

The interface on which the LLDP frame was received.

Chassis ID

The chassis ID is the identification of the neighbor LLDP frame.

Port ID

The port ID is the identification of the neighbor port.

Port description

Port Description is the port description advertised by the neighbor unit.

System name

System Name is the name advertised by the neighbor unit.

System function

System Capabilities describes the neighbor unit's capabilities. The possible capabilities are:

- Other
- Repeater
- Bridge
- WLAN Access Point
- Router
- Telephone
- DOCSIS cable device
- Station only
- Reserved

When a function is enabled, the function is followed by (+). If the function is disabled, the function is followed by (-).

Management address

Management Address is the neighbor unit's address that is used for higher layer entities to assist discovery by the network management. This could for instance hold the neighbor's IP address.

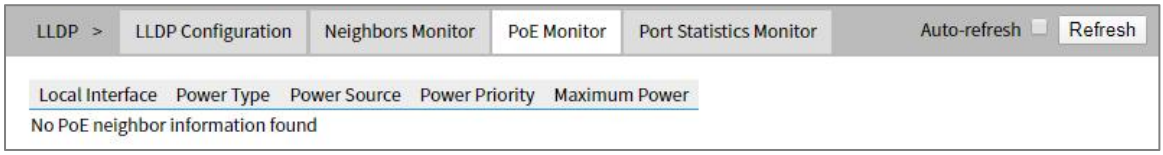
Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page.

6.7.3 PoE Monitoring

This page provides a status overview for all LLDP PoE neighbors. The displayed table contains a row for each interface on which an LLDP PoE neighbor is detected. The columns hold the following information:



Local Interface

The interface for this switch on which the LLDP frame was received.

Power Type

The Power Type represents whether the device is a Power Sourcing Entity (PSE) or Power Device (PD).

If the Power Type is unknown it is represented as "Reserved".

Energy source

The Power Source represents the power source being utilized by a PSE or PD device.

If the device is a PSE device it can either run on its Primary Power Source or its Backup Power Source. If it is unknown whether the PSE device is using its Primary Power Source or its Backup Power Source it is indicated as "Unknown"

If the device is a PD device it can either run on its local power supply or it can use the PSE as power source. It can also use both its local power supply and the PSE.

If it is unknown what power supply the PD device is using it is indicated as "Unknown"

Power Priority

Power Power Priority represents the priority of the PD device, or the power priority associated with the PSE type device's interface that is sourcing the power. There are three levels of power priority. The three levels are: Critical, High and Low.

If the power priority is unknown it is indicated as "Unknown"

Max Value

The Maximum Power Value contains a numerical value that indicates the maximum power in watts required by a PD device from a PSE device, or the minimum power a

PSE device is capable of sourcing over a maximum length cable based on its current configuration.

The maximum allowed value is 102.3 W. If the device indicates value higher than 102.3 W, it is represented as "reserved"

Buttons

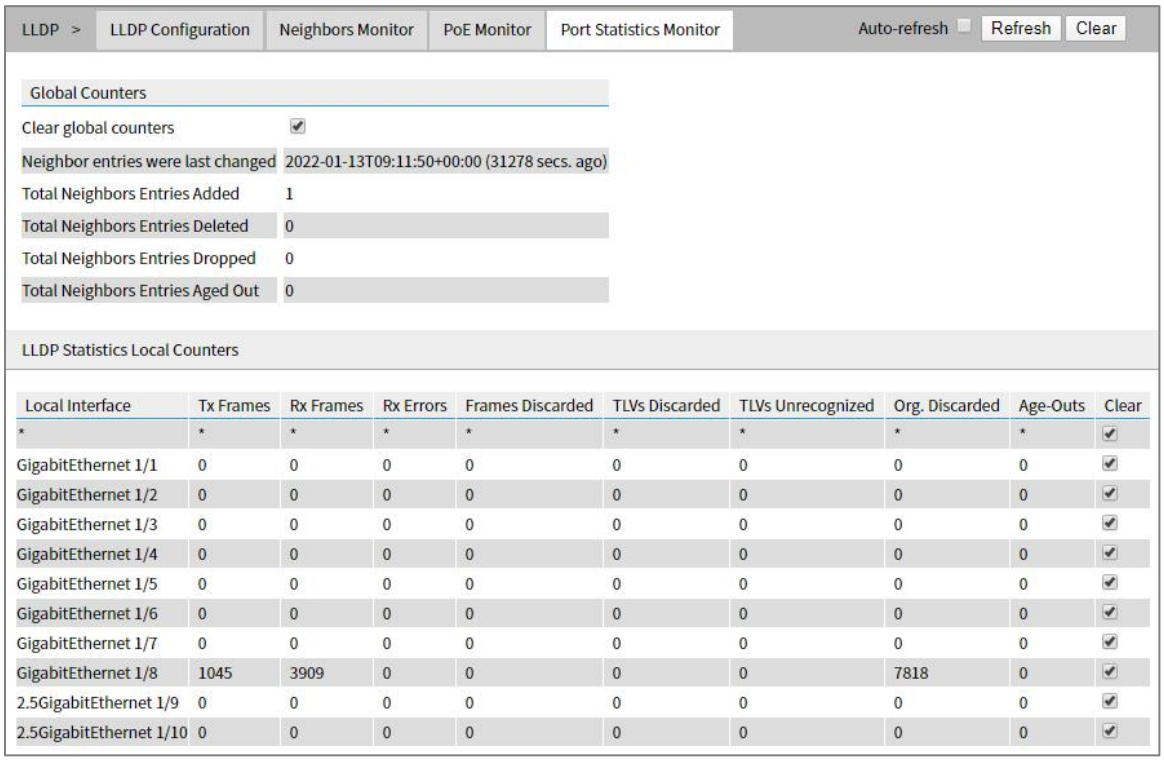
Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page.

6.7.4 Port Statistics Monitoring

This page provides an overview of all LLDP traffic.

Two types of counters are shown. Global counters are counters that refer to the whole switch, while local counters refer to per interface counters for the currently selected switch.



Global counter

Clear global counters

If checked the global counters are cleared when “Clear” is clicked.

Recently changed neighbor entry

Shows the time when the last entry was last deleted or added. It also shows the time elapsed since the last change was detected.

Total Neighbors Entries Added

Shows the number of new entries added since switch reboot.

Total Neighbors Entries Deleted

Shows the number of new entries deleted since switch reboot.

Number of discarded neighbor entries

Shows the number of LLDP frames dropped due to the entry table being full.

Number of expired neighbor entries

Shows the number of entries deleted due to Time-To-Live expiring.

LLDP Statistics Local Counter

The displayed table contains a row for each interface. The columns hold the following information:

Local Interface

The interface at which LLDP frames are received or transmitted.

Tx Frames

The number of LLDP frames transmitted on the interface.

Rx Frames

The number of LLDP frames received on the interface.

Rx Errors

The number of received LLDP frames containing some kind of error.

Frames Discarded

If a LLDP frame is received on a interface, and the switch's internal table has run full, the LLDP frame is counted and discarded. This situation is known as "Too Many Neighbors" in the LLDP standard. LLDP frames require a new entry in the table when the Chassis ID or Remote Port ID is not already contained within the table. Entries are removed from the table when a given interface's link is down, an LLDP shutdown frame is received, or when the entry ages out.

TLVs Discarded

Each LLDP frame can contain multiple pieces of information, known as TLVs (TLV is short for "Type Length Value"). If a TLV is malformed, it is counted and discarded.

TLVs Unrecognized

The number of well-formed TLVs, but with an unknown type value.

Org. Discarded

If LLDP frame is received with an organizationally TLV, but the TLV is not supported the TLV is discarded and counted.

Age-Outs

Each LLDP frame contains information about how long time the LLDP information is valid (age-out time). If no new LLDP frame is received within the age out time, the LLDP information is removed, and the Age-Out counter is incremented.

Clear

If checked the counters for the specific interface are cleared when “Clear” is clicked.

Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

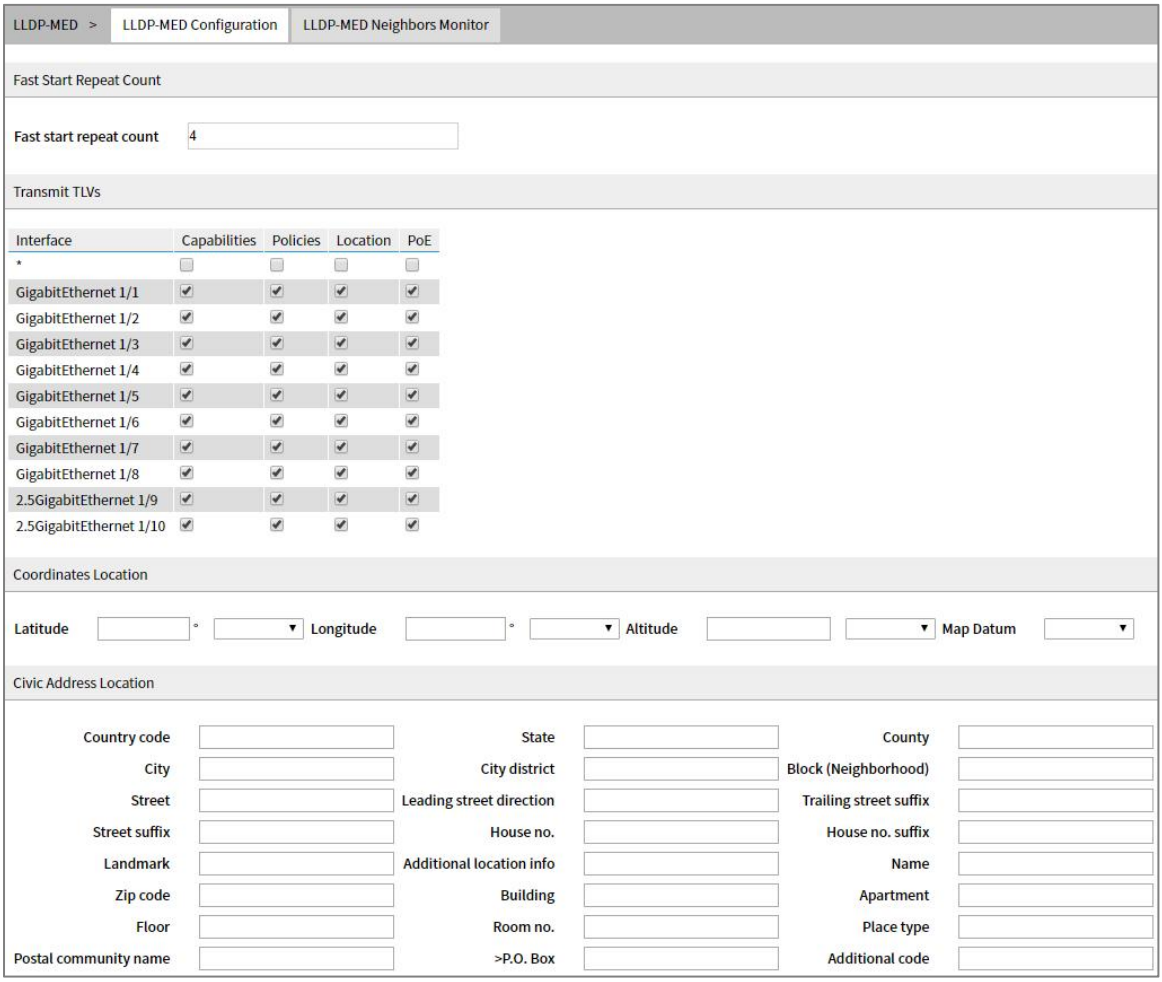
Refresh: Click to refresh the page.

Clear: Clear the counters which have the corresponding checkbox checked.

6.8 LLDP-MED

6.8.1 LLDP-MED Configuration

This page allows you to configure the LLDP-MED. This function applies to VoIP devices which support LLDP-MED.



Fast Message Number

Fast Message Number

Rapid startup and Emergency Call Service Location Identification Discovery of endpoints is a critically important aspect of VoIP systems in general. In addition, it is best to advertise only those pieces of information which are specifically relevant to particular endpoint types (for example only advertise the voice network policy to permitted voice-capable devices), both in order to conserve the limited LLDPU space

and to reduce security and system integrity issues that can come with inappropriate knowledge of the network policy.

With this in mind LLDP-MED defines an LLDP-MED Fast Start interaction between the protocol and the application layers on top of the protocol, in order to achieve these related properties. Initially, a Network Connectivity Device will only transmit LLDP TLVs in an LLDPDU. Only after an LLDP-MED Endpoint Device is detected, will an LLDP-MED capable Network Connectivity Device start to advertise LLDP-MED TLVs in outgoing LLDPDUs on the associated interface. The LLDP-MED application will temporarily speed up the transmission of the LLDPDU to start within a second, when a new LLDP-MED neighbor has been detected in order share LLDP-MED information as fast as possible to new neighbors.

Because there is a risk of an LLDP frame being lost during transmission between neighbors, it is recommended to repeat the fast start transmission multiple times to increase the possibility of the neighbors receiving the LLDP frame. With Fast start repeat count it is possible to specify the number of times the fast start transmission would be repeated. The recommended value is 4 times, given that 4 LLDP frames with a 1 second interval will be transmitted, when an LLDP frame with new information is received.

It should be noted that LLDP-MED and the LLDP-MED Fast Start mechanism is only intended to run on links between LLDP-MED Network Connectivity Devices and Endpoint Devices, and as such does not apply to links between LAN infrastructure elements, including Network Connectivity Devices, or other types of links.

Transmit TLVs

It is possible to select which LLDP-MED information that shall be transmitted to the neighbors. When the checkbox is checked the information is included in the frame transmitted to the neighbor.

Interface

The interface name to which the configuration applies.

Capabilities

When checked the switch's capabilities is included in LLDP-MED information transmitted.

Policy

When checked the configured policies for the interface is included in LLDP-MED information transmitted.

Device Address

When checked the configured location information for the switch is included in LLDP-MED information transmitted.

PoE

When checked the configured PoE (Power Over Ethernet) information for the interface is included in LLDP-MED information transmitted.

Coordinates Location

Latitude

Latitude SHOULD be normalized to within 0-90 degrees with a maximum of 4 digits.

It is possible to specify the direction to either North of the equator or South of the equator.

Longitude

Longitude SHOULD be normalized to within 0-180 degrees with a maximum of 4 digits.

It is possible to specify the direction to either East of the prime meridian or West of the prime meridian.

Altitude

Altitude SHOULD be normalized to within -2097151.9 to 2097151.9 with a maximum of 1 digits.

It is possible to select between two altitude types (floors or meters).

- Meters: Representing meters of Altitude defined by the vertical datum specified.
- Floors: Representing altitude in a form more relevant in buildings which have different floor-to-floor dimensions. An altitude = 0.0 is meaningful even outside a building, and represents ground level at the given latitude and longitude. Inside a building, 0.0 represents the floor level associated with ground level at the main entrance.

Map Datum

The Map Datum is used for the coordinates given in these options:

- WGS84: (Geographical 3D) - World Geodesic System 1984, CRS Code 4327, Prime Meridian Name:
- NAD83/NAVD88: North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; The associated vertical datum is the North American Vertical Datum of 1988 (NAVD88). This datum pair is to be used when referencing locations on land, not near tidal water (which would use Datum = NAD83/MLLW).
- NAD83/MLLW: North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; The associated vertical datum is Mean Lower Low Water (MLLW). This datum pair is to be used when referencing locations on water/sea/ocean.

Civic Address Location

IETF Geopriv Civic Address based Location Configuration Information (Civic Address LCI). The total number of characters for the combined civic address information must not exceed 250 characters.

A couple of notes to the limitation of 250 characters.

1) A non-empty city address location will use two extra characters outside the city address location text.

2) The 2-letter country code is not part of the 250-character limit.

Country code

The two-letter ISO 3166 country code in capital ASCII letters - Example: DK, DE or US.

State

National subdivisions.

County

County.

City

City, township.

City District

City division.

Block (Neighborhood)

Neighborhood, block.

Street

Street.

Leading street direction

Leading street direction.

Trailing street suffix

Trailing street suffix

Street suffix

Street suffix.

House number

House no.

House no. suffix

House no. suffix.

Landmark

Landmark.

Other Location Information

Other location info.

Name

Name.

Zip code

Zip code.

Building

Building.

Apartment

Unit.

Floor

Floor.

Room no.

Room number.

Place Type

Place type.

Postal Community Name

Postal community name.

P.O. Box

P.O. Box.

Other Info

Other Info.

Emergency Call Service

Emergency Call Service (e.g. E911 and others), such as defined by TIA or NENA.

Emergency Call Service

Emergency Call Service ELIN identifier data format is defined to carry the ELIN identifier as used during emergency call setup to a traditional CAMA or ISDN

trunk-based PSAP. This format consists of a numerical digit string, corresponding to the ELIN to be used for emergency calling.

Policy

Network Policy Discovery enables the efficient discovery and diagnosis of mismatch issues with the VLAN configuration, along with the associated Layer 2 and Layer 3 attributes, which apply for a set of specific protocol applications on that port. Improper network policy configurations are a very significant issue in VoIP environments that frequently result in voice quality degradation or loss of service.

Policies are only intended for use with applications that have specific 'real-time' network policy requirements, such as interactive voice and/or video services.

The network policy attributes advertised are:

1Layer 2 VLAN ID (IEEE 802.1Q-2003)

2Layer 2 priority value (IEEE 802.1D-2004)

3Layer 3 Diffserv code point (DSCP) value (IETF RFC 2474)

This network policy is potentially advertised and associated with multiple sets of application types supported on a given port. The application types specifically addressed are:

1Voice

2Guest Voice

3Softphone Voice

4Video Conferencing

5Streaming Video

6Control / Signaling (conditionally support a separate network policy for the media types above)

A large network may support multiple VoIP policies across the entire organization, and different policies per application type. LLDP-MED allows multiple policies to be advertised per port, each corresponding to a different application type. Different ports on the same Network Connectivity Device may advertise different sets of policies, based on the authenticated user identity or port configuration.

It should be noted that LLDP-MED is not intended to run on links other than between Network Connectivity Devices and Endpoints, and therefore does not need to advertise the multitude of network policies that frequently run on an aggregated link interior to the LAN.

Delete

Check to delete the policy. It will be deleted during the next save.

Policy ID

This is auto generated and shall be used when selecting the policies that shall be mapped to the specific interfaces.

Application Type

Intended use of the application types:

- Voice - for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications.
- Voice Signaling - for use in network topologies that require a different policy for the voice signaling than for the voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Voice application policy.
- Guest Voice - support a separate 'limited feature-set' voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services.
- Guest Voice Signaling-use in network topologies that require a different policy for the guest voice signaling than for the guest voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Guest Voice application policy.
- Softphone Voice - for use by softphone applications on typical data centric devices, such as PCs or laptops. This class of endpoints frequently does not support multiple VLANs, if at all, and are typically configured to use an 'untagged' VLAN or a single 'tagged' data specific VLAN. When a network policy is defined for use with an 'untagged' VLAN (see Tagged flag below), then the L2 priority field is ignored and only the DSCP value has relevance.
- Video Conferencing - for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services.
- Streaming Video - for use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type.
- Video Signaling - for use in network topologies that require a separate policy for the video signaling than for the video media. This application type should not be advertised if all the same network policies apply as those advertised in the Video Conferencing application policy.

TAG

Tag indicating whether the specified application type is using a ‘tagged’ or an ‘untagged’ VLAN.

- Untagged: indicates that the device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003. In this case, both the VLAN ID and the Layer 2 priority fields are ignored and only the DSCP

value has relevance.

- Tagged: indicates that the device is using the IEEE 802.1Q tagged frame format, and that both the VLAN ID and the Layer 2 priority values are being used, as well as the DSCP value. The tagged format includes an additional field, known as the tag header. The tagged frame format also includes priority tagged frames as defined by IEEE 802.1Q-2003.

VLAN ID

VLAN identifier (VID) for the interface as defined in IEEE 802.1Q-2003.

L2 Priority

L2 Priority is the Layer 2 priority to be used for the specified application type. L2 Priority may specify one of eight priority levels (0 through 7), as defined by IEEE 802.1D-2004. A value of 0 represents use of the default priority as defined in IEEE 802.1D-2004.

DSCP

DSCP value to be used to provide Diffserv node behaviour for the specified application type as defined in IETF RFC 2474. DSCP may contain one of 64 code point values (0 through 63). A value of 0 represents use of the default DSCP value as defined in RFC 2475.

Policies Interface Configuration

Every interface may advertise a unique set of network policies or different attributes for the same network policies, based on the authenticated user identity or interface configuration.

Interface

The interface name to which the configuration applies.

Policy ID

The set of policies that shall apply to a given interface. The set of policies is selected by check marking the checkboxes that corresponds to the policies.

Buttons

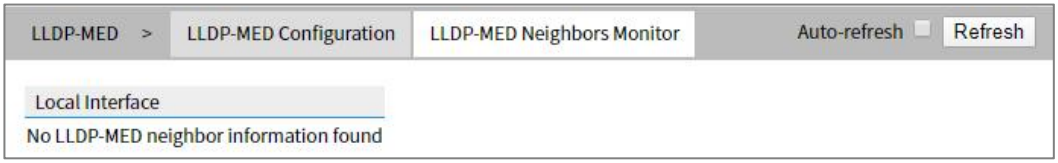
Add a new policy: Click to add a new policy. Specify the Application type, Tag, VLAN ID, L2 Priority and DSCP for the new policy. Click "Save". The number of policies supported is 32

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

6.8.2 LLDP-MED Neighbor Information

This page provides a status overview of all LLDP-MED neighbors. The displayed table contains a row for each interface on which an LLDP neighbor is detected. This function applies to VoIP devices which support LLDP-MED. The columns hold the following information:



Local Interface

The interface on which the LLDP frame was received.

Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page.

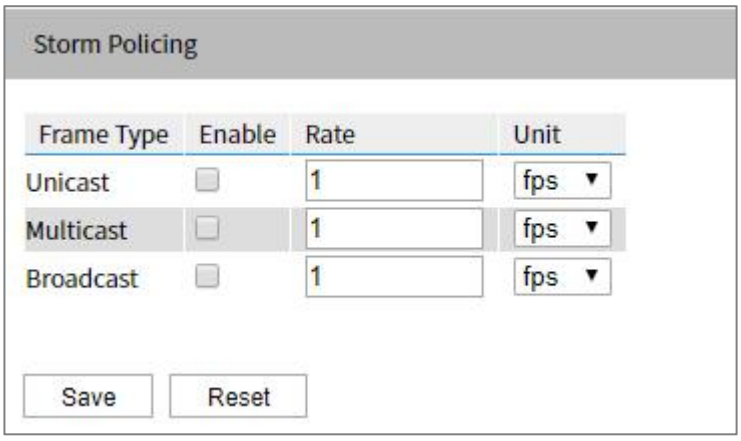
6.9 Storm Control

Storm suppression is a security technology used to control broadcast, unknown multicast and unknown unicast messages to prevent broadcast storms caused by these three types of messages. It mainly limits traffic by configuring thresholds.

Global storm policers for the switch are configured on this page.

These only affect flooding frames, that is, (VLAN ID, DMAC) paired frames do not exist in the MAC address table.

The displayed settings are:



Frame Type

The frame type for which the configuration below applies.

- Unicast: unknown unicast message, that is, unicast message whose destination MAC address is not learned by the device.
- Multicast.
- Broadcast.

Enable

Enable or disable the global storm policer for the given frame type.

Rate

Controls the rate for the global storm policer. This value is restricted to 1-1024000 when "Unit" is fps, and 1-1024 when "Unit" is kfps. The rate is internally rounded up to the nearest value supported by the global storm policer.

Unit

Controls the unit of measure for the global storm policer rate as fps or kfps.

Buttons

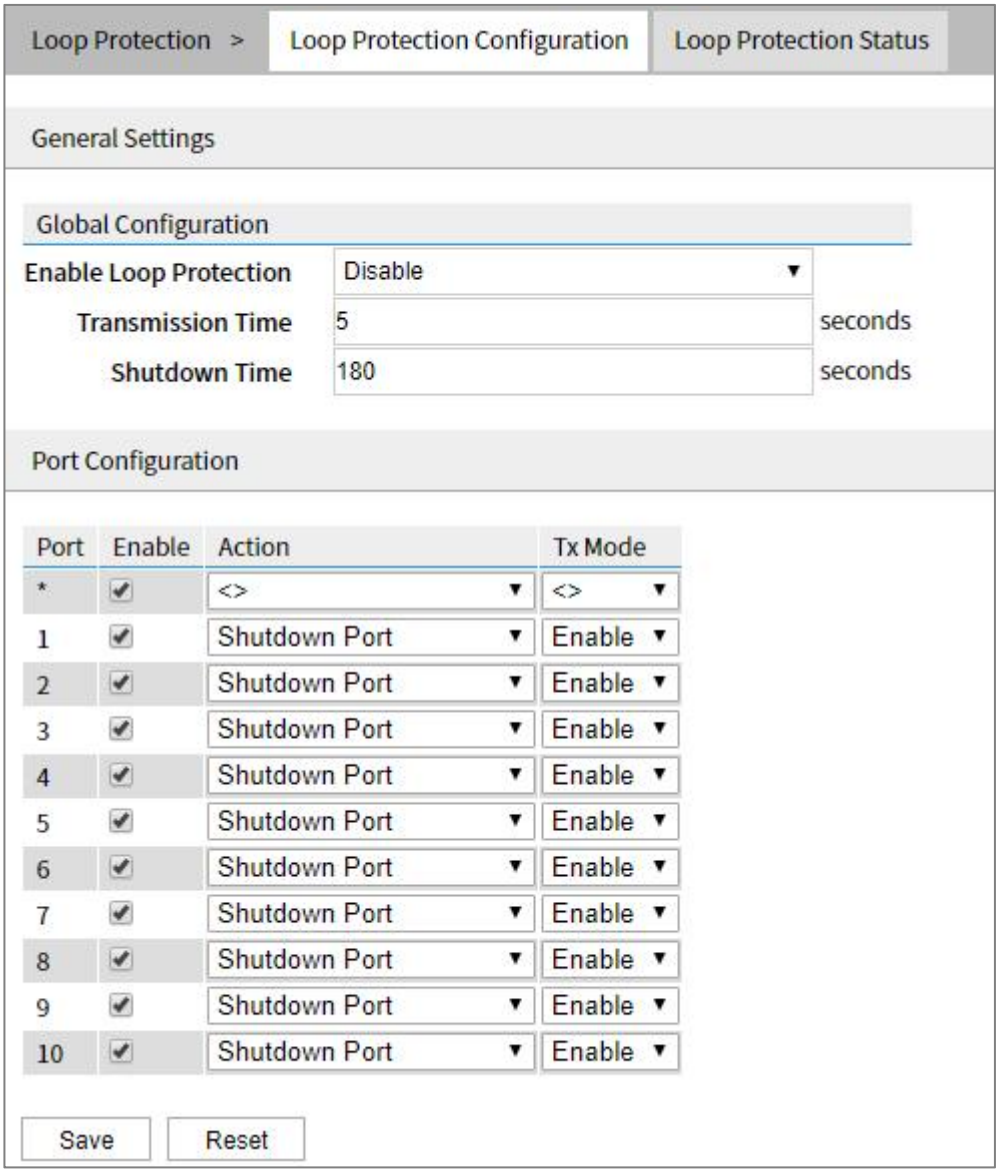
Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

6.10 Loop Protection

6.10.1 Loop Protection Configuration

This page allows the user to inspect the current Loop Protection configurations, and possibly change them as well.



General Settings

Enable Loop Protection

Controls whether loop protections is enabled (as a whole).

Transmission Time

The interval between each loop protection PDU sent on each port. Valid values are 1 to 10 seconds. Default value is 5 seconds.

Shutdown Time

The period (in seconds) for which a port will be kept disabled in the event of a loop is detected (and the port action shuts down the port). Valid values are 0 to 604800 seconds (7 days). A value of zero will keep a port disabled (until next device restart). Default value is 180 seconds.

Port Configuration

Port

The switch port number.

Switch

Controls whether loop protection is enabled on this switch port.

Action

Configures the action performed when a loop is detected on a port. Valid values are

- Shutdown Port
- Shutdown Port and Log
- Log Only

Active Protection

Controls whether the port is actively generating loop protection PDU's, or whether it is just passively looking for looped PDU's.

Buttons

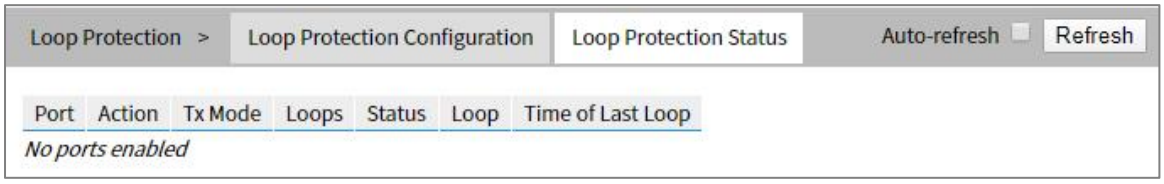
Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

6.10.2 Loop Protection Status

This page displays the loop protection port status the ports of the switch.

Loop protection port status is:



Port

The switch port number of the logical port.

Action

The currently configured port action.

Active Protection

Status of port active protection.

Loops

The number of loops detected on this port.

Status

The current loop protection status of the port.

Loop

Whether a loop is currently detected on the port.

Time of Last Loop

The time of the last loop event detected.

Buttons

Refresh: Click to refresh the page immediately.

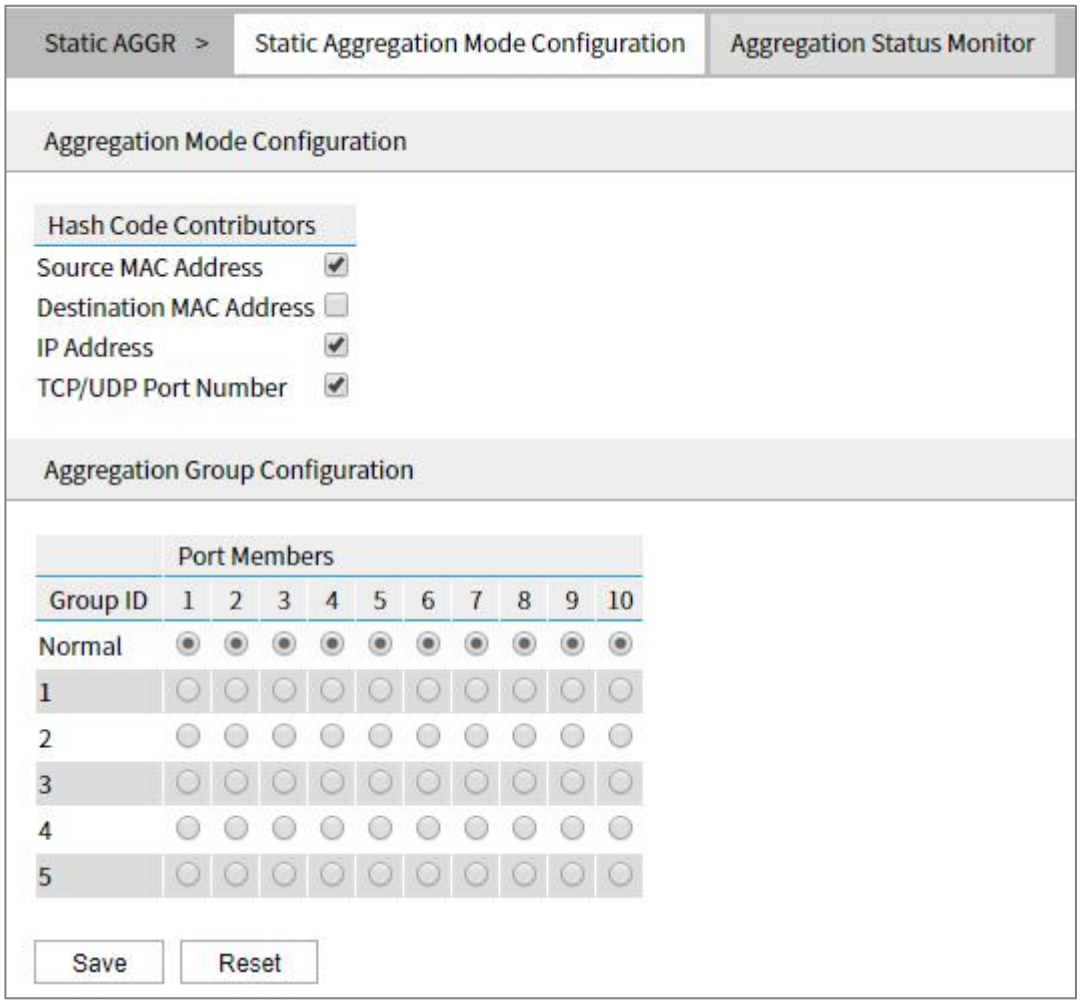
Auto-refresh: Check this box to enable an automatic refresh of the page at regular intervals.

6.11 Static Aggregation

Link aggregation is to bundle multiple Ethernet links into a logical link. By configuring link aggregation, the purpose of increasing bandwidth, improving reliability and load sharing can be realized. According to whether the LACP (Link Aggregation Control Protocol) is enabled, link aggregation is divided into manual mode (static aggregation) and LACP mode (dynamic aggregation).

6.11.1 Static Link Aggregation Mode Configuration

This page is used to configure the Aggregation hash routing algorithm and the aggregation group.



Aggregation Mode Configuration

Hash Algorithm

In order to avoid the disorder of data packets, the HASH-KEY value is generated through the hash algorithm according to the address in the data frame, and then the corresponding egress interface is found in the link aggregation forwarding table according to this value to ensure that the frames in the same data flow are forwarded on the same physical link, so as to realize the load sharing of traffic on each physical link in the aggregation group.

- Source MAC address: The Source MAC address can be used to calculate the destination port for the frame. Check to enable the use of the Source MAC address, or uncheck to disable. By default, Source MAC Address is enabled.
- Destination MAC Address: The Destination MAC Address can be used to calculate the destination port for the frame. Check to enable the use of the Destination MAC Address, or uncheck to disable. By default, Destination MAC Address is disabled.
- IP address: The IP address can be used to calculate the destination port for the

frame. Check to enable the use of the IP Address, or uncheck to disable. By default, IP Address is enabled.

- TCP/UDP port number: The TCP/UDP port number can be used to calculate the destination port for the frame. Check to enable the use of the TCP/UDP Port Number, or uncheck to disable. By default, TCP/UDP Port Number is enabled.

Aggregation Group Configuration

Group ID

Indicates the group ID for the settings contained in the same row. Group ID "Normal" indicates there is no aggregation. Only one group ID is valid per port.

Port Members

Each switch port is listed for each group ID. Select a radio button to include a port in an aggregation, or clear the radio button to remove the port from the aggregation. By default, no ports belong to any aggregation group. Only full duplex ports can join an aggregation and ports must be in the same speed in each group.

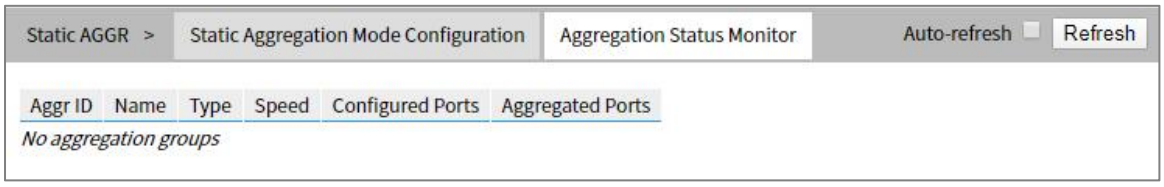
Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

6.11.2 Link Aggregation Status Monitoring

This page is used to see the status of ports in Aggregation group.



Aggr ID

The Aggregation ID associated with this aggregation instance.

Group Name

Name of the Aggregation group ID.

Type

Type of the Aggregation group(Static or LACP).

Speed

Speed of the Aggregation group.

Configured ports

Configured member ports of the Aggregation group.

Aggregated ports

Aggregated member ports of the Aggregation group.

Buttons

Refresh: Click to refresh the page immediately.

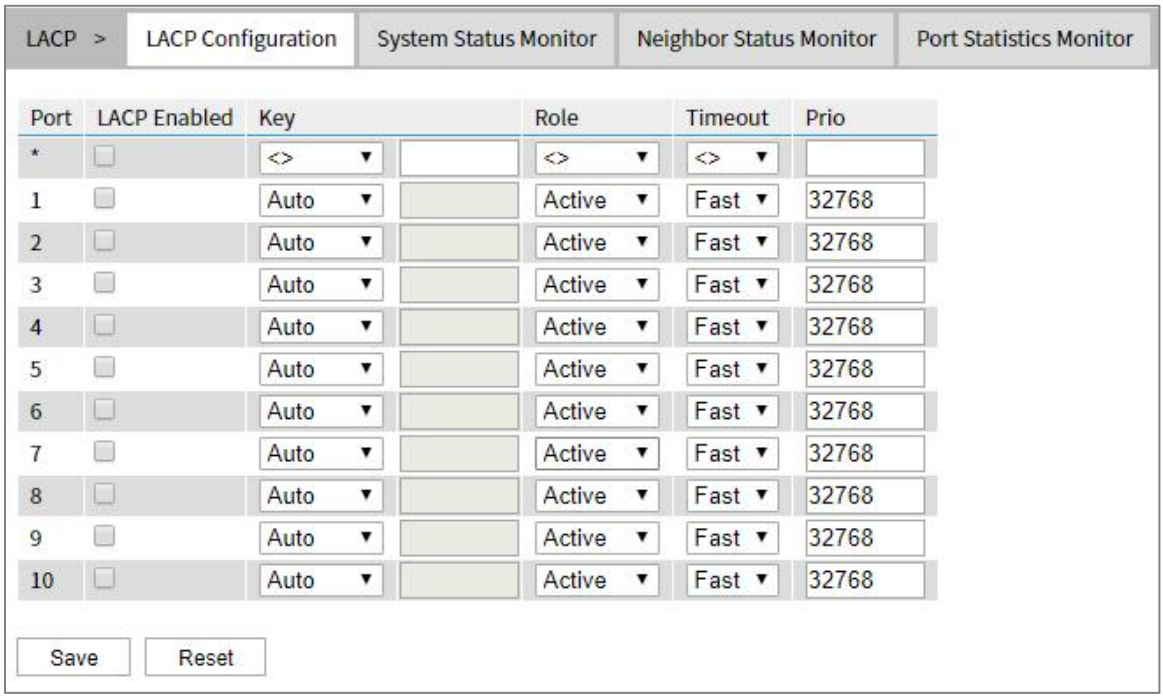
Auto-refresh : Automatic refresh occurs every 3 seconds.

6.12 LACP

LACP (Link Aggregation Control Protocol) provides a standard negotiation mode for data switching devices to automatically form an aggregation link according to their own configuration and enable the aggregation link to send and receive data. After the aggregation link is formed, LACP is responsible for maintaining the link state and automatically adjusting or dissolving the link aggregation when the aggregation conditions change.

6.12.1 LACP Configuration

This page allows the user to inspect the current LACP port configurations, and possibly change them as well.



Port

The switch port number.

Enable

Controls whether LACP is enabled on this switch port. LACP will form an aggregation when 2 or more ports are connected to the same partner.

Key

The Key value incurred by the port, range 1-65535. The Auto setting will set the key as appropriate by the physical link speed, 10Mb=1, 100mb=2, 1gb=3. Using the Specific setting, a user-defined value can be entered. Ports with the same Key value can participate in the same aggregation group, while ports with different keys cannot.

Role

The Role shows the LACP activity status. The Active will transmit LACP packets each second, while Passive will wait for a LACP packet from a partner (speak if spoken to).

timeout

Timeout controls the period between BPDU transmissions. Fast will transmit LACP packets each second, while Slow will wait for 30 seconds before sending a LACP packet.

Prio

The priority of the control port, range 1-65535. If the LACP partner wants to form a larger group than is supported by this device then this parameter will control which ports will be active and which ports will be in a backup role. Lower number means greater priority.

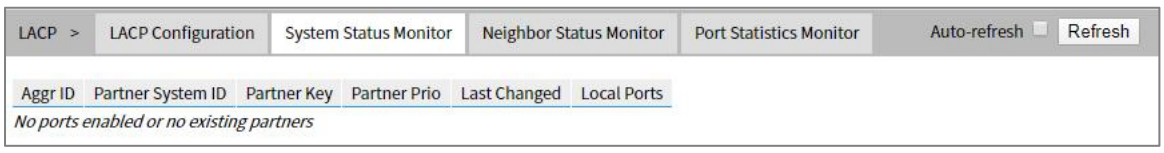
Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

6.12.2 System Status Monitoring

This page provides a status overview for all LACP instances.



Aggr ID

The Aggregation ID associated with this aggregation instance.

Partner System ID

The system ID (MAC address) of the aggregation partner.

Partner Key

The key that the partner has assigned to this aggregation ID.

Partner Prio

Port priority of aggregation partner.

Last changed

The time since this aggregation changed.

Local Ports

Shows which ports are a part of this aggregation for this switch.

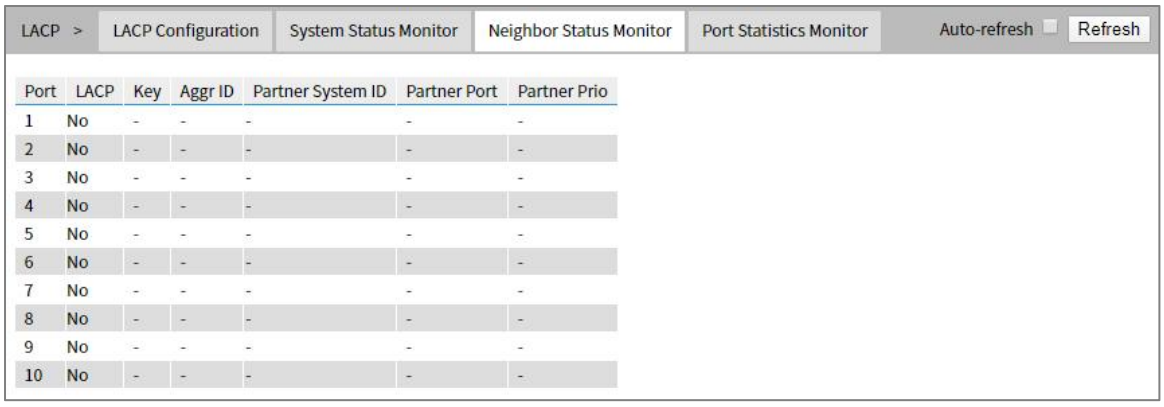
Buttons

Refresh: Click to refresh the page immediately.

Auto-refresh : Automatic refresh occurs every 3 seconds.

6.12.3 Neighbor Status Monitoring

This page provides a status overview for LACP status for all ports.



Port

The switch port number.

LACP

'Yes' means that LACP is enabled and the port link is up. 'No' means that LACP is not enabled or that the port link is down. 'Backup' means that the port could not join the

aggregation group but will join if other port leaves. Meanwhile it's LACP status is disabled.

Key

The key assigned to this port. Only ports with the same key can aggregate together.

Aggr ID

The Aggregation ID assigned to this aggregation group.

Partner System ID

The system ID (MAC address) of the partner.

Partner Port

The partner's port number connected to this port.

Partner Prio

The partner's port priority.

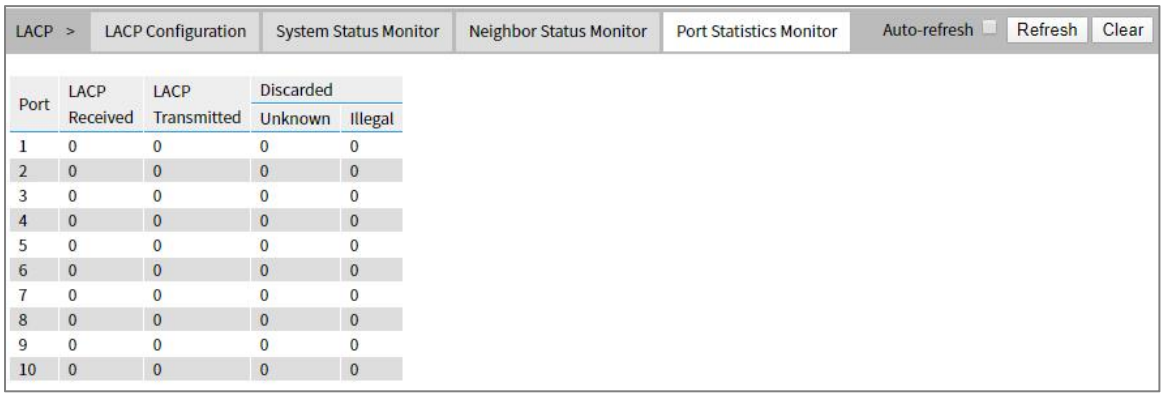
Buttons

Refresh: Click to refresh the page immediately.

Auto-refresh : Automatic refresh occurs every 3 seconds.

6.12.4 Port Statistics Monitoring

This page provides an overview for LACP statistics for all ports.



Port	LACP Received	LACP Transmitted	Discarded	
			Unknown	Illegal
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0
9	0	0	0	0
10	0	0	0	0

Port

The switch port number.

LACP Received

Shows how many LACP frames have been received at each port.

LACP Transmitted

Shows how many LACP frames have been sent from each port.

Discarded Packets

Shows how many unknown or illegal LACP frames have been discarded at each port.

Buttons

Auto-refresh: Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

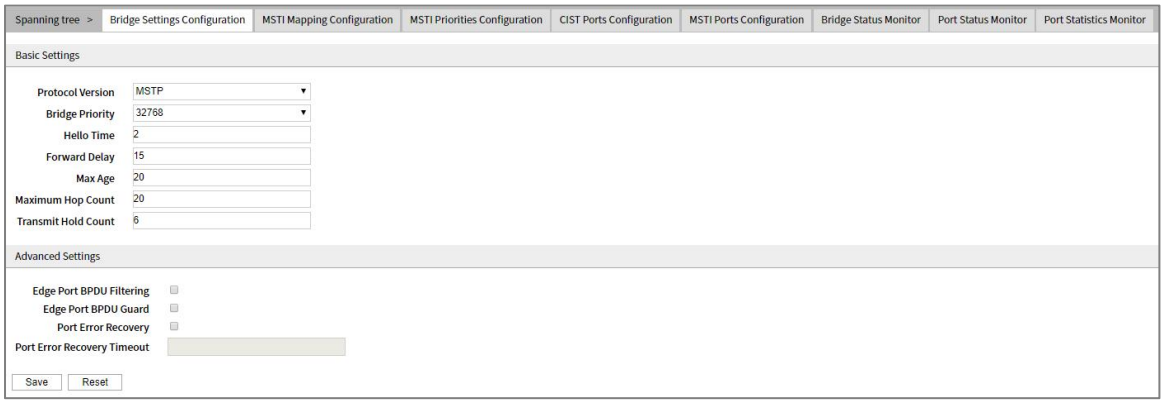
Clear: Clears the counters for all ports.

6.13 Spanning Tree

Equipments running STP (Spanning Tree Protocol) find the loop in the network by interact information, and congest the ports selectively to cut the ring network structure to a non-loop tree network structure, thus preventing message cycle in the ring network and the decline in processing capacity of the device due to the repetitive receiving of the same message. RSTP (Rapid Spanning Tree Protocol) has made improvement on the basis of STP, which has achieved quick topological convergence of network. To address the limitation of STP and RSTP, MSTP (Multiple Spanning Tree Protocol) allows fast convergence and provides multiple paths to load balance VLAN traffic during data forwarding.

6.13.1 Bridge Setting Configuration

This page allows you to configure STP system settings. The settings are used by all STP Bridge instances in the Switch.



Basic Settings

Protocol Version

The MSTP/RSTP/STP protocol version setting. Valid values are STP, RSTP and MSTP.

Bridge Priority

Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier.

For MSTP operation, this is the priority of the CIST. Otherwise, this is the priority of the STP/RSTP bridge.

Hello Time

The interval between sending STP BPDU's. Valid values are in the range 1 to 10 seconds, default is 2 seconds.

Note

Changing this parameter from the default value is not recommended, and may have adverse effects on your network.

Forward Delay

The delay used by STP Bridges to transit Root and Designated Ports to Forwarding (used in STP compatible mode). Valid values are in the range 4 to 30 seconds.

Aging Time

The maximum age of the information transmitted by the Bridge when it is the Root Bridge. Valid values are in the range 6 to 40 seconds, and MaxAge must be <= (FwdDelay-1)*2.

Maximum Hop Count

This defines the initial value of remaining Hops for MSTI information generated at the boundary of an MSTI region. It defines how many bridges a root bridge can distribute its BPDU information to. Valid values are in the range 6 to 40 hops.

Transmit Hold Count

The number of BPDU's a bridge port can send per second. When exceeded, transmission of the next BPDU will be delayed. Valid values are in the range 1 to 10 BPDU's per second.

Advanced Settings

Edge Port BPDU Filtering

Control whether a port explicitly configured as Edge will transmit and receive BPDUs.

BPDU Guard

Control whether a port explicitly configured as Edge will disable itself upon reception of a BPDU. The port will enter the error-disabled state, and will be removed from the active topology.

Port Error Recovery

Control whether a port in the error-disabled state automatically will be enabled after a certain time. If recovery is not enabled, ports have to be disabled and re-enabled for normal STP operation. The condition is also cleared by a system reboot.

Port Error Recovery Timeout

The time to pass before a port in the error-disabled state can be enabled. Valid values are between 30 and 86400 seconds (24 hours).

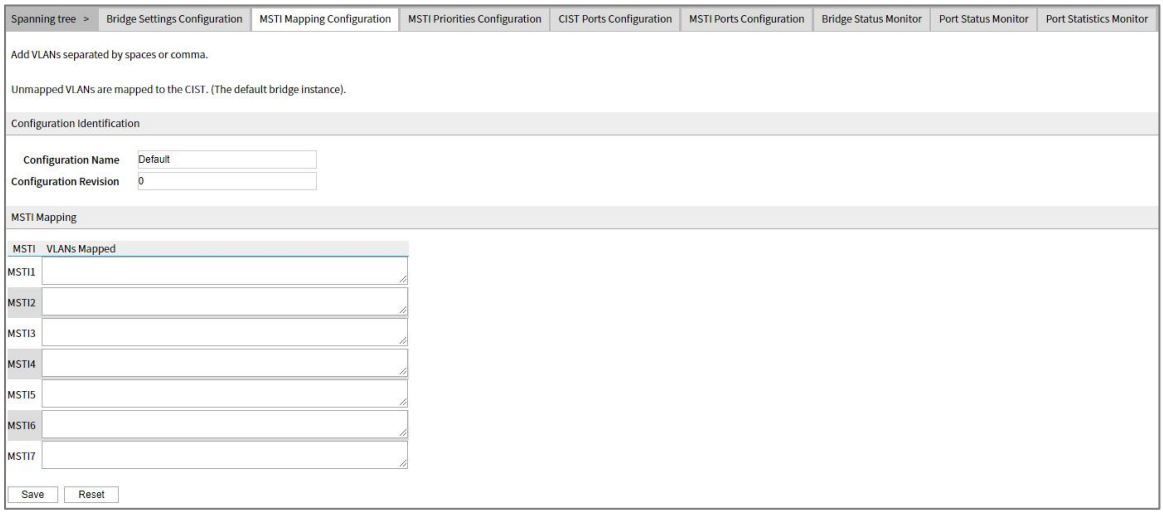
Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

6.13.2 MSTI Mapping Configuration

This page allows the user to inspect the current STP MSTI bridge instance priority configurations, and possibly change them as well.



Configuration Identification

Domain Name

The name identifying the VLAN to MSTI mapping. Bridges must share the name and revision (see below), as well as the VLAN-to-MSTI mapping configuration in order to share spanning trees for MSTI's (Intra-region). The name is at most 32 characters.

Configuration Revision

The revision of the MSTI configuration named above. This must be an integer between 0 and 65535.

MSTI Mapping

MSTI

The Bridge Instance. The CIST is not available for explicit mapping, as it will receive the VLANs not explicitly mapped.

VLANs Mapped

The list of VLANs mapped to the MSTI. The VLANs can be given as a single (xx, xx being between 1 and 4094) VLAN, or a range (xx-yy), each of which must be separated with comma and/or space. A VLAN can only be mapped to one MSTI. An unused MSTI should just be left empty. (I.e. not having any VLANs mapped to it.) Example: 2, 5, 20-40.

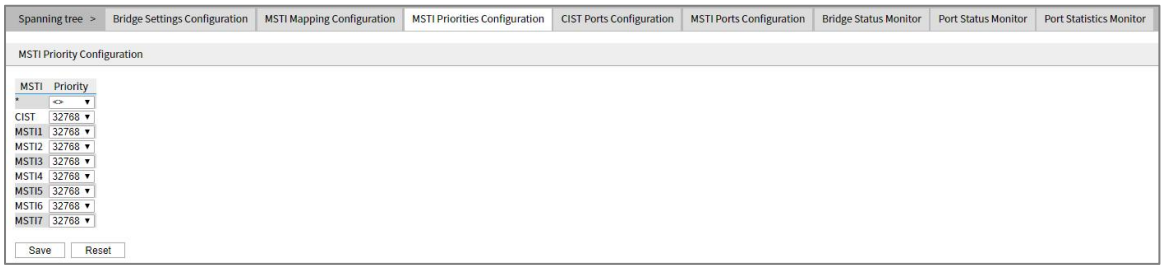
Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

6.13.3 MSTI Priority Configuration

This page allows the user to inspect the current STP MSTI bridge instance priority configurations, and possibly change them as well.



MSTI Priority Configuration

MSTI

The Bridge Instance. The CIST is the default instance, which is always active.

Priority

Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier.

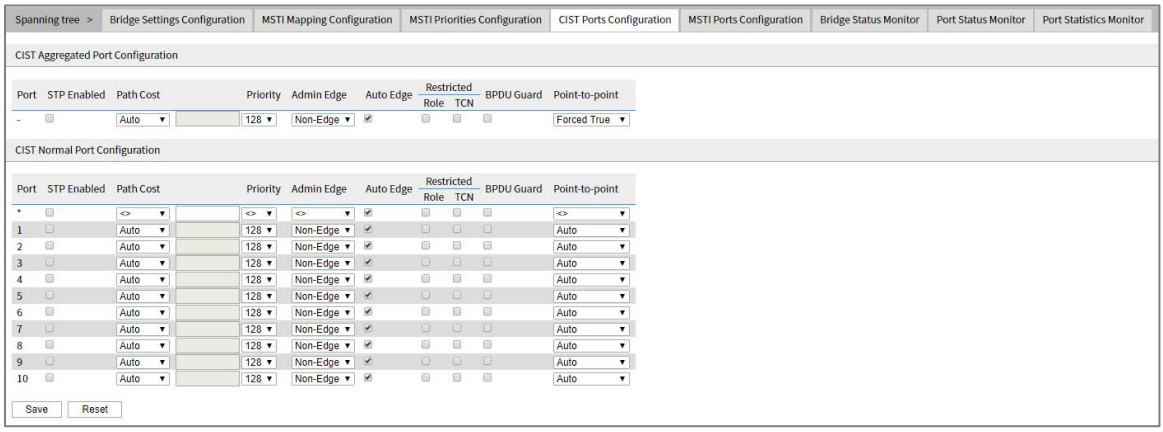
Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

6.13.4 CIST Port Configuration

This page allows the user to inspect the current STP CIST port configurations, and possibly change them as well.



Configuration of CIST Aggregation Port and CIST Physical Port

Port

The switch port number.

STP Enabled

Controls whether STP is enabled on this switch port.

Path Cost

Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favour of higher path cost ports. Valid values are in the range 1 to 200000000.

Priority

Controls the port priority. This can be used to control priority of ports having identical port cost.

Edge management

Controls whether the operEdge flag should start as set or cleared. (The initial operation edge state when a port is initialized).

AutoEdge

Controls whether the bridge should enable automatic edge detection on the bridge port. This allows operEdge to be derived from whether BPDU's are received on the port or not.

Restriction Role

If enabled, causes the port not to be selected as Root Port for the CIST or any MSTI, even if it has the best spanning tree priority vector. Such a port will be selected as an Alternate Port after the Root Port has been selected. If set, it can cause lack of spanning tree connectivity. It can be set by a network administrator to prevent bridges external to a core region of the network influence the spanning tree active topology, possibly because those bridges are not under the full control of the administrator. This feature is also known as Root Guard.

Restriction TCN

If enabled, causes the port not to propagate received topology change notifications and topology changes to other ports. If set it can cause temporary loss of connectivity after changes in a spanning tree's active topology as a result of persistently incorrect learned station location information. It is set by a network administrator to prevent bridges external to a core region of the network, causing address flushing in that region, possibly because those bridges are not under the full control of the administrator or the physical link state of the attached LANs transits frequently.

BPDU Guard

If enabled, causes the port to disable itself upon receiving valid BPDU's. Contrary to the similar bridge setting, the port Edge status does not effect this setting.

A port entering error-disabled state due to this setting is subject to the bridge Port Error Recovery setting as well.

Point-to-Point

Controls whether the port connects to a point-to-point LAN rather than to a shared medium. This can be automatically determined, or forced either true or false.

Transition to the forwarding state is faster for point-to-point LANs than for shared media.

Buttons

Save: Click to save changes.

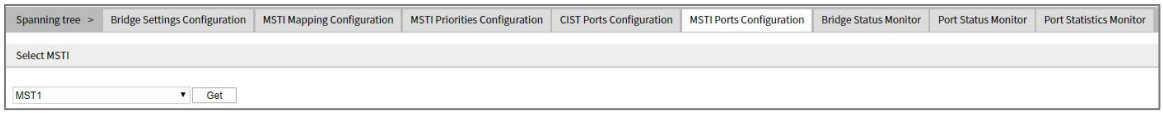
Reset: Click to undo any changes made locally and revert to previously saved values.

6.13.5 MSTI port configuration

This page allows the user to inspect the current STP MSTI port configurations, and possibly change them as well.

An MSTI port is a virtual port, which is instantiated separately for each active CIST (physical) port for each MSTI instance configured on and applicable to the port. The MSTI instance must be selected before displaying actual MSTI port configuration options.

This page contains MSTI port settings for physical and aggregated ports.



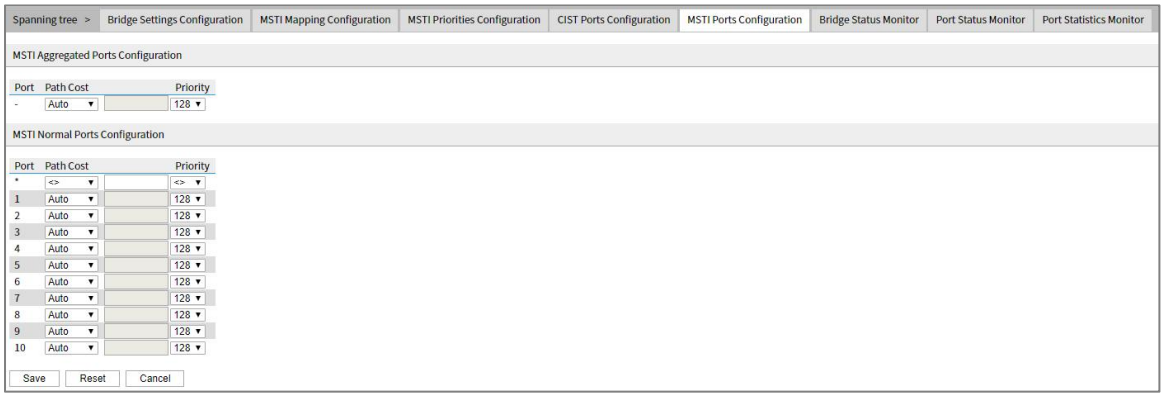
Select MSTI

Buttons

Get: Click to retrieve settings for a specific MSTI.

MSTI port configuration

Select MSTI port and click "Get" to enter MSTI aggregation port and MSTI common port configuration page.



Configuration of MSTI Aggregation Port and Common Port

Port

The switch port number of the corresponding STP CIST (and MSTI) port.

Path Cost

Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favour of higher path cost ports. Valid values are in the range 1 to 200000000.

Priority

Controls the port priority. This can be used to control priority of ports having identical port cost.

Buttons

Save: Click to save changes.

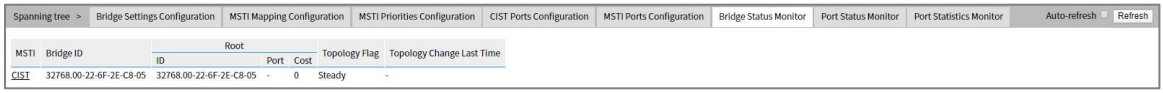
Reset: Click to undo any changes made locally and revert to previously saved values.

Back: go back to the select MSTI page.

6.13.6 Bridge Status Monitoring

This page provides a status overview of all STP bridge instances.

The displayed table contains a row for each STP bridge instance, where the column displays the following information:



MSTI

The Bridge Instance. This is also a link to the STP Detailed Bridge Status.

Bridge ID

The Bridge ID of this Bridge instance.

Root ID

The Bridge ID of the currently elected root bridge.

Root Port

The switch port currently assigned the root port role.

Root Cost

Root Path Cost. For the Root Bridge this is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge.

Topology Flag

The current state of the Topology Change Flag of this Bridge instance.

Topology Change Last

The time since last Topology Change occurred.

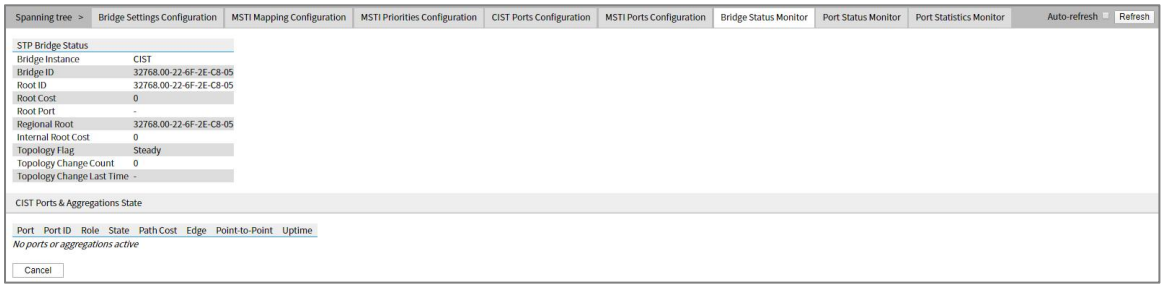
Buttons

Refresh: Click to refresh the page immediately.

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Bridge Status Monitoring

Click the MSTI port link to view the detailed status of the bridge.



STP Bridge Status

Bridge Instance

Bridge Instance -CIST, MST1, ……

Bridge ID

The Bridge ID of this Bridge instance.

Root ID

The Bridge ID of the currently elected root bridge.

Root Cost

Root Path Cost. For the Root Bridge this is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge.

Root Port

The switch port currently assigned the root port role.

Regional Root

The Bridge ID of the currently elected regional root bridge, inside the MSTP region of this bridge. (For the CIST instance only).

Internal Root Cost

The Regional Root Path Cost. For the Regional Root Bridge this is zero. For all other CIST instances in the same MSTP region, it is the sum of the Internal Port Path Costs on the least cost path to the Internal Root Bridge. (For the CIST instance only).

Topology Flag

The current state of the Topology Change Flag of this Bridge instance.

Topology Change Count

The number of times where the topology change flag has been set (during a one-second interval).

Topology Change Last

The time passed since the Topology Flag was last set.

CSTI port and aggregation state

Port

The switch port number.

Port ID

The port id as used by the STP protocol. This is the priority part and the logical port index of the bridge port.

Role

The current STP port role. The port role can be one of the following values： Alternate Port, Backup Port, Root Port, Designated Port.

Status

The current STP port state. The port state can be one of the following values: Discarding Learning Forwarding.

Path Cost

The current STP port path cost. This will either be a value computed from the Auto setting, or any explicitly configured value.

Edge

The current STP port (operational) Edge Flag. An Edge Port is a switch port to which no Bridges are attached. The flag may be automatically computed or explicitly

configured. Each Edge Port transits directly to the Forwarding Port State, since there is no possibility of it participating in a loop.

Point-to-Point

The current STP port point-to-point flag. A point-to-point port connects to a non-shared LAN media. The flag may be automatically computed or explicitly configured. The point-to-point properties of a port affect how fast it can transit to STP state.

Uptime

The time since the bridge port was last initialized.

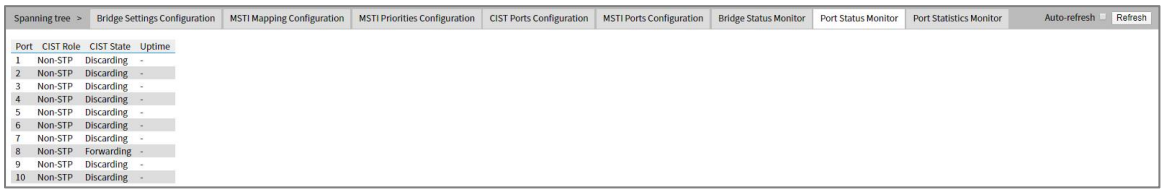
Buttons

Refresh: Click to refresh the page immediately.

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

6.13.7 Port State Monitoring

This page displays the STP CIST port status for physical ports of the switch. STP port state:



Port

The switch port number.

Role

The current STP port role of the CIST port. The port role can be one of the following values: AlternatePort, BackupPort, RootPort DesignatedPort and DisabledPort .

Port state

The current STP port state of the CIST port. The port state can be one of the following values: Discarding Learning Forwarding.

Uptime

The time since the bridge port was last initialized.

Buttons

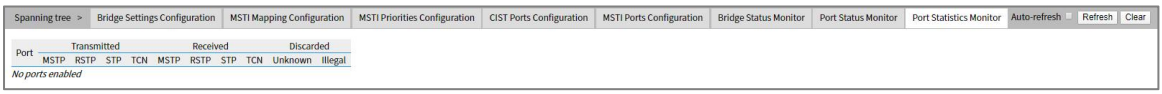
Refresh: Click to refresh the page immediately.

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

6.13.8 Port Statistics Monitoring

This page displays the STP port statistics counters of bridge ports in the switch.

The STP port statistics counters are:



Port

The switch port number.

Tx and Rx

- MSTP: The number of MSTP BPDU's received/transmitted on the port.
- RSTP: The number of RSTP BPDU's received/transmitted on the port.
- STP: The number of legacy STP Configuration BPDU's received/transmitted on the port.
- TCN: The number of (legacy) Topology Change Notification BPDU's received/transmitted on the port.

Discarded Unknown

The number of unknown Spanning Tree BPDU's received (and discarded) on the port.

Discarded Illegal

The number of illegal Spanning Tree BPDU's received (and discarded) on the port.

Buttons

Refresh: Click to refresh the page immediately.

Clear: click to reset the counts.

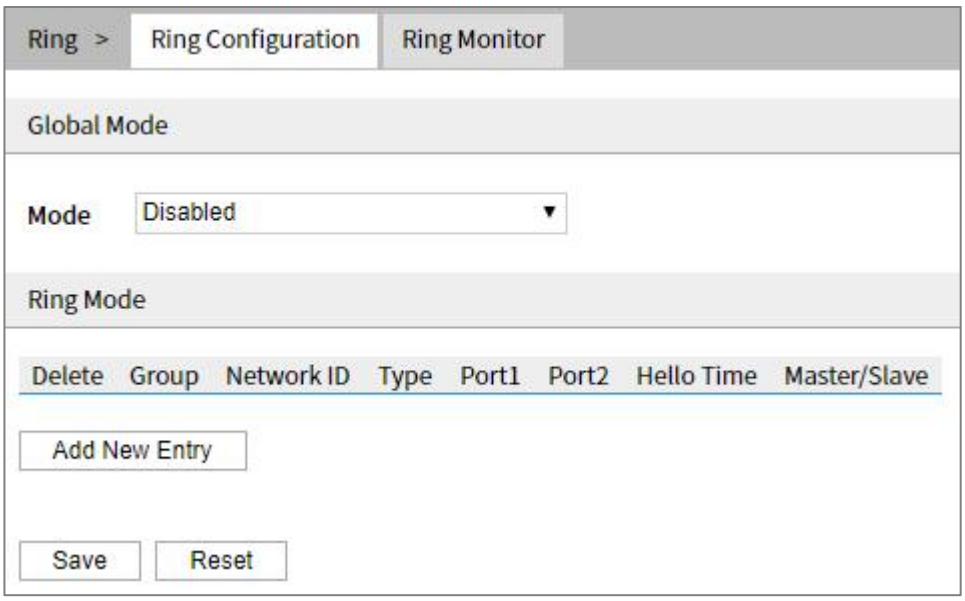
Auto-refresh: Check this box to enable an automatic refresh. Automatic refresh occurs every 3 seconds.

6.14 Ring

6.14.1 Ring Configuration

This page provides ring related configurations.

It provides automatic recovery and reconnection mechanism for the disconnected Ethernet network, which has link redundancy and self-recovery ability in case of network interruption or network failure.



Global Mode

Pattern

Enable/Disable the Global mode.

The ring configuration only takes effect when the global mode is enabled.

Ring Mode

Delete

Check the corresponding check box to delete an entry. It will be deleted during the next Save operation.

Groups

Support ring group 1-4, it can create 4 ring networks at the same time.

Network ID

When multiple switch devices constitute a ring network, the current ring identification of the ring is network identification; the network identifications of different ring network are different.

Type

According to the scene environment requirement, choose different ring type.

- Single: Single ring, it adopts a continuous ring to connect each device together.
- Couple: Coupling ring is a redundant structure proposed to connect two independent networks.

- Chain: The chain, it enhances the flexibility that user builds any type of redundant network topology structure via a kind of advanced software technology.
- Dual-homing: Two adjacent rings share a switch; users can carry the same switch on two different networks or two different switching devices on the same network.

Port1

The network port 1 on the switch device used to form the ring network.

Port2

The network port 2 on the switch device used to form the ring network.

Hello time

Hello_time is the sending time interval of Hello packet; via the ring port, CPU sends information packet to adjacent device for confirming the connection is normal or not.

Master-slave relationship

Single ring has master/slave device option. One-Master Multi-Slave mode is recommended in one single ring. When the device is set as master device and one end of it is backup link, it can enable backup link to ensure the normal operation of the network when failure occurs in ring network.

Buttons

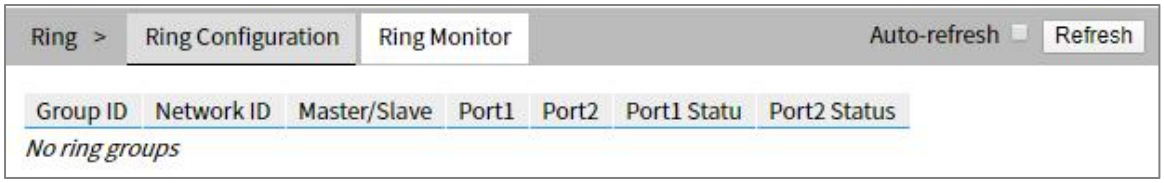
Add new entry: Click to add a new loop entry. Specify the ID and configure the new entry. Click "Save".

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

6.14.2 Loop Monitoring

This page displays the ring status.



Group ID

Group ID of the ring network.

Network ID

The current ring identification of the ring is network ID.

Master and Slave

Single ring has master/slave device option. One-Master Multi-Slave mode is recommended in one single ring. When the device is set as master device and one end of it is backup link, it can enable backup link to ensure the normal operation of the network when failure occurs in ring network.

Port1

The network port 1 on the switch device used to form the ring network.

Port2

The network port 2 on the switch device used to form the ring network.

Port1 Status

The status of network port 1 on the switch device used to form the ring network.

Port2 Status

The status of network port 2 on the switch device used to form the ring network.

Buttons

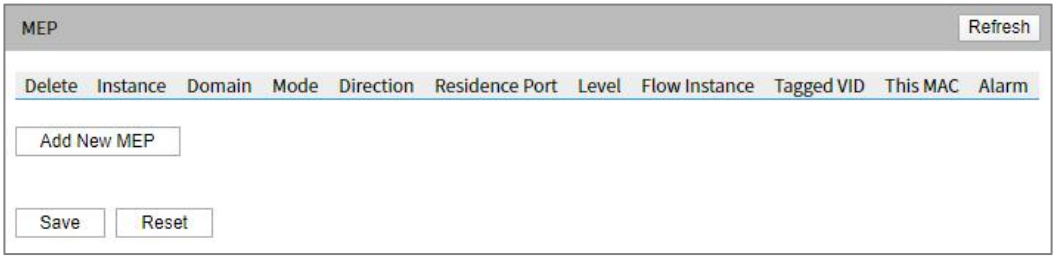
Auto-refresh: Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

6.15 MEP

The MEP (Maintenance Association End Point) determines the scope and boundary of the maintenance domain and is the edge node of the MA (Maintenance Association). The MA (Maintenance Association) and maintenance domain to which the MEP (Maintenance Association End Point) belongs determine the service and level of the message sent by the MEP. The level of the MEP determines the level of the message it can handle. The level of the message sent by the maintenance endpoint is the level of the maintenance endpoint. When the maintenance endpoint receives a message higher than its own level, it will not process it, but forward it according to the original path; When the maintenance endpoint receives a message less than or equal to its own level, it will process it.

The Maintenance Entity Point instances are configured here.



Delete

This box is used to mark a MEP for deletion in next Save operation.

Instance ID

The ID of the MEP. Click on the ID of a MEP to enter the configuration page. The range is from 1 through 100.

Domain

- Port: This is a MEP in the Port Domain.
- EVC: This is a MEP in the EVC Domain. “Instance Flow Control” is a EVC. The EVC must be created
- VLAN: This is a MEP in the VLAN Domain. “Instance Flow Control” is a VLAN. In case of Up-MEP the VLAN must be created.

Pattern

- MEP: This is a Maintenance Entity End Point.
- MIP: This is a Maintenance Entity Intermediate Point.

Direction

- Down: this is an egress OAM and flow of downlink MEP-monitoring "monitoring port".
- Up: this is an egress OAM and flow of uplink MEP-monitoring "monitoring port".

Residence Port

The port where MEP is monitoring - see 'Direction'. For a VLAN MEP the port must be a VLAN member. For a EVC MEP the port must be a port in the EVC.

Level

The MEG level of MEP is an integer within the value range of 0-7. The higher the value, the higher the level.

Flow Instance

The MEP is related to this flow - See 'Domain'. This is not relevant and not shown in case of Port MEP.

Tagged VID

- Port MEP: An outer C/S-tag (depending on VLAN Port Type) is added with this

VID. Entering '0' means no TAG added.

- VLAN MEP: This is not used.
- EVC MEP: This is not used.
- EVC MIP: On Serval, this is the Subscriber VID that identifies the subscriber flow in this EVC where the MIP is active.

This MAC

The MAC of this MEP - can be used by other MEP when unicast is selected (Info only).

Alarm

There is an active alarm on the MEP.

Buttons

Add new MEP: Click to add a new MEP entry.

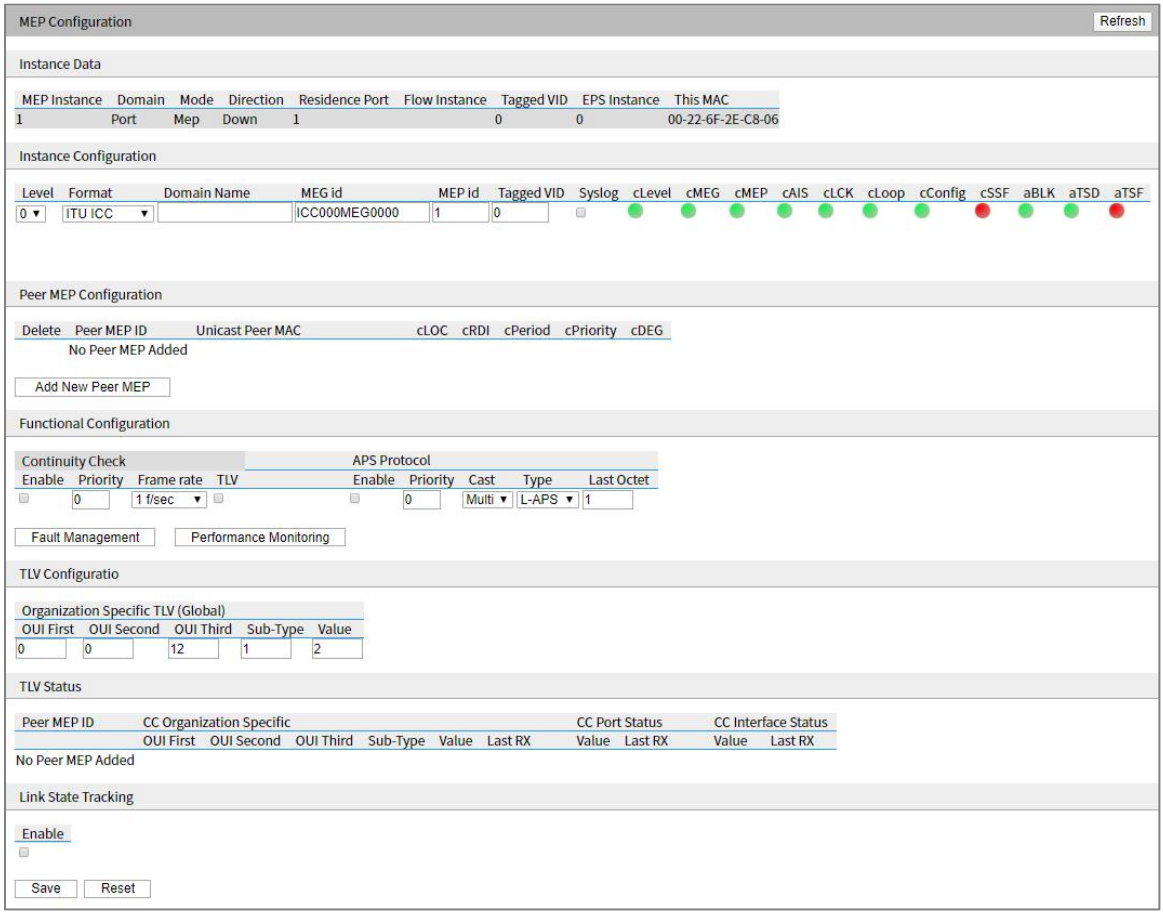
Refresh: Click to refresh the page immediately.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

6.15.1 MEP Configuration

Click the instance ID link to enter the MEP configuration page.



Instance Data

MEP Instance

The ID of the MEP.

Domain

- Port: This is a MEP in the Port Domain.
- EVC: This is a MEP in the EVC Domain. “Instance Flow Control” is a EVC. The EVC must be created
- VLAN: This is a MEP in the VLAN Domain. “Instance Flow Control” is a VLAN. In case of Up-MEP the VLAN must be created.

Pattern

- MEP: This is a Maintenance Entity End Point.
- MIP: This is a Maintenance Entity Intermediate Point.

Direction

- Down: this is an egress OAM and flow of downlink MEP-monitoring "monitoring port".
- Up: this is an egress OAM and flow of uplink MEP-monitoring "monitoring port".

Residence Port

The port where MEP is monitoring - see 'Direction'. For a VLAN MEP the port must be a VLAN member. For a EVC MEP the port must be a port in the EVC.

Flow Instance

The MEP is related to this flow - See 'Domain'. This is not relevant and not shown in case of Port MEP.

Tagged VID

- Port MEP: An outer C/S-tag (depending on VLAN Port Type) is added with this VID. Entering '0' means no TAG added.
- VLAN MEP: This is not used.
- EVC MEP: This is not used.
- EVC MIP: On Serval, this is the Subscriber VID that identifies the subscriber flow in this EVC where the MIP is active.

EPS Instance

The ID of the EPS.

This MAC

The MAC of this MEP - can be used by other MEP when unicast is selected (Info only).

Instance Configuration

Level

The MEG level of this MEP.

Format

This is the configuration of the two possible Maintenance Association Identifier formats.

- ITU ICC: This is defined by ITU (Y1731 Fig. A3). 'Domain Name' is not used. 'MEG id' must be max. 13 char.
- IEEE String: This is defined by IEEE (802.1ag Section 21.6.5). 'Domain Name' can be max. 16 char. 'MEG id' (Short MA Name) can be max. 16 char.
- ITU CC ICC: This is defined by ITU (Y1731 Fig. A5). 'Domain Name' is not used. 'MEG id' must be max. 15 char.

Domain Name

This is the IEEE Maintenance Domain Name and is only used in case of 'IEEE String' format. This string can be empty giving Maintenance Domain Name Format 1 - Not present. This can be max 16 char.

MEG Id

This is either ITU MEG ID or IEEE Short MA Name - depending on 'Format'. See 'Format'. In case of ITU ICC format this must be 13 char. In case of ITU CC ICC format this must be 15 char. In case of IEEE String format this can be max 16 char.

MEP Id

This value will become the transmitted two byte CCM MEP ID.

Tagged VID

This value will be the VID of a TAG added to the OAM PDU.

Syslog

Syslog record.

cLevel

Fault Cause indicating that a CCM is received with a lower level than the configured for this MEP.

cMEG

Fault Cause indicating that a CCM is received with a MEG ID different from configured for this MEP.

cMEP

Fault Cause indicating that a CCM is received with a MEP ID different from all 'Peer MEP ID' configured for this MEP.

cAIS

Fault Cause indicating that AIS PDU is received.

cLCK

Fault Cause indicating that LCK PDU is received.

cLoop

Indicates the failure reason of receiving port loopback.

cConfig

Identifies the failure reason of receiving configuration error.

cSSF

Fault Cause indicating that server layer is indicating Signal Fail.

aBLK

The consequent action of blocking service frames in this flow is active.

aTSD

The consequent action of indicating Trail Signal Degrade is calculated.

aTSF

The consequent action of indicating Trail Signal Fail to-wards protection is active.

Peer MEP Configuration

Delete

This box is used to mark a Peer MEP for deletion in next Save operation.

Peer MEP ID

This value will become an expected MEP ID in a received CCM - see 'cMEP'.

Unicast Peer MAC

This MAC will be used when unicast is selected with this peer MEP. Also this MAC is used to create HW checking of receiving CCM PDU (LOC detection) from this MEP.

cLOC

Fault Cause indicating that no CCM has been received (in 3,5 periods) - from this peer MEP.

cRDI

Fault Cause indicating that a CCM is received with Remote Defect Indication - from this peer MEP.

cPeriod

Fault Cause indicating that a CCM is received with a period different what is configured for this MEP - from this peer MEP.

cPriority

Fault Cause indicating that a CCM is received with a priority different what is configured for this MEP - from this peer MEP.

cDEG

Fault Cause indicating that server layer is indicating Signal Degraded.

Buttons

Add New Peer MEP: Click to add a new peer MEP.

Function Configuration

Continuity Check

- Enable: Continuity Check based on transmitting/receiving CCM PDU can be enabled/disabled. The CCM PDU is always transmitted as Multi-cast Class 1.
- Priority: The priority to be inserted as PCP bits in TAG (if any). In case of enable

of Continuity Check and Loss Measurement both implemented on SW based CCM, 'Priority' has to be the same.

- Frame rate: The frame rate of CCM PDU. This is the inverse of transmission period as described in Y.1731.: This value has the following uses:
  - *The transmission rate of the CCM PDU.
  - *Fault Cause cLOC is declared if no CCM PDU has been received within 3.5 periods - see 'cLOC'.
  - * Fault Cause cPeriod is declared if a CCM PDU has been received with different period - see 'cPeriod'.

  Selecting 300f/sec or 100f/sec will configure HW based CCM (if possible). Selecting other frame rates will configure SW based CCM. In case of enable of Continuity Check and Loss Measurement both implemented on SW based CCM, 'Frame Rate' has to be the same.
- TLV: Enable/disable of TLV insertion in the CCM PDU.

APS Protocol

- Enable: Automatic Protection Switching protocol information transportation based on transmitting/receiving R-APS/L-APS PDU can be enabled/disabled. Must be enabled to support ERPS/ELPS implementing APS. This is only valid with one Peer MEP configured.
- Priority: The priority to be inserted as PCP bits in TAG (if any).
- Cast: Selection of APS PDU transmitted unicast or multi-cast. The unicast MAC will be taken from the 'Unicast Peer MAC' configuration. Unicast is only valid for L-APS - see 'Type'. The R-APS PDU is always transmitted with multi-cast MAC described in G.8032.
- Type:
  - R-APS: APS PDU is transmitted as R-APS - this is for ERPS.
  - L-APS: APS PDU is transmitted as L-APS - this is for ELPS.
- Last Octet: This is the last octet of the transmitted and expected RAPS multi-cast MAC. In G.8031(03/2010), RAPS multicast MAC is defined as 01-19-A7-00-00-XX. In current standard the value for this last octet is '01' and the usage of other values is for further study.

Buttons

Fault management: Click to enter Fault Management page.

Performance Monitoring: Click to go to Performance Monitor page.

TLV Configuration

Configuration of the OAM PDU TLV. Currently only TLV in the CCM is supported.

Organization Specific TLV（Global）

- OUI First: The transmitted first value in the OS TLV OUI field.

- OUI Second: The transmitted second value in the OS TLV OUI field.
- OUI Third: The transmitted third value in the OS TLV OUI field.
- Sub-Type: The transmitted value in the OS TLV Sub-Type field.
- Value: The transmitted value in the OS TLV Value field.

TLV Status

Display of the last received TLV. Currently only TLV in the CCM is supported.

Peer MEP ID

Peer MEP ID.

CC Organization Specific

- OUI First: The last received first value in the OUI field.
- OUI Second: The last received second value in the OS TLV OUI field.
- OUI Third: The last received third value in the OS TLV OUI field.
- Sub-Type: The last received value in the OS TLV Sub-Type field.
- Value: The last received value in the OS TLV Value field.
- Last RX: OS TLV was received in the last received CCM PDU.

CC Port Status

- Value: The last received value in the PS TLV Value field.
- Last RX: PS TLV was received in the last received CCM PDU.

CC Interface Status

- Value: The last received value in the IS TLV Value field.
- Last RX: IS TLV was received in the last received CCM PDU.

Link State Tracking

Enable

When LST is enabled in an instance, Local SF or received 'isDown' in CCM Interface Status TLV, will bring down the residence port. Only valid in Up-MEP. The CCM rate must be 1 f/s or faster.

Buttons

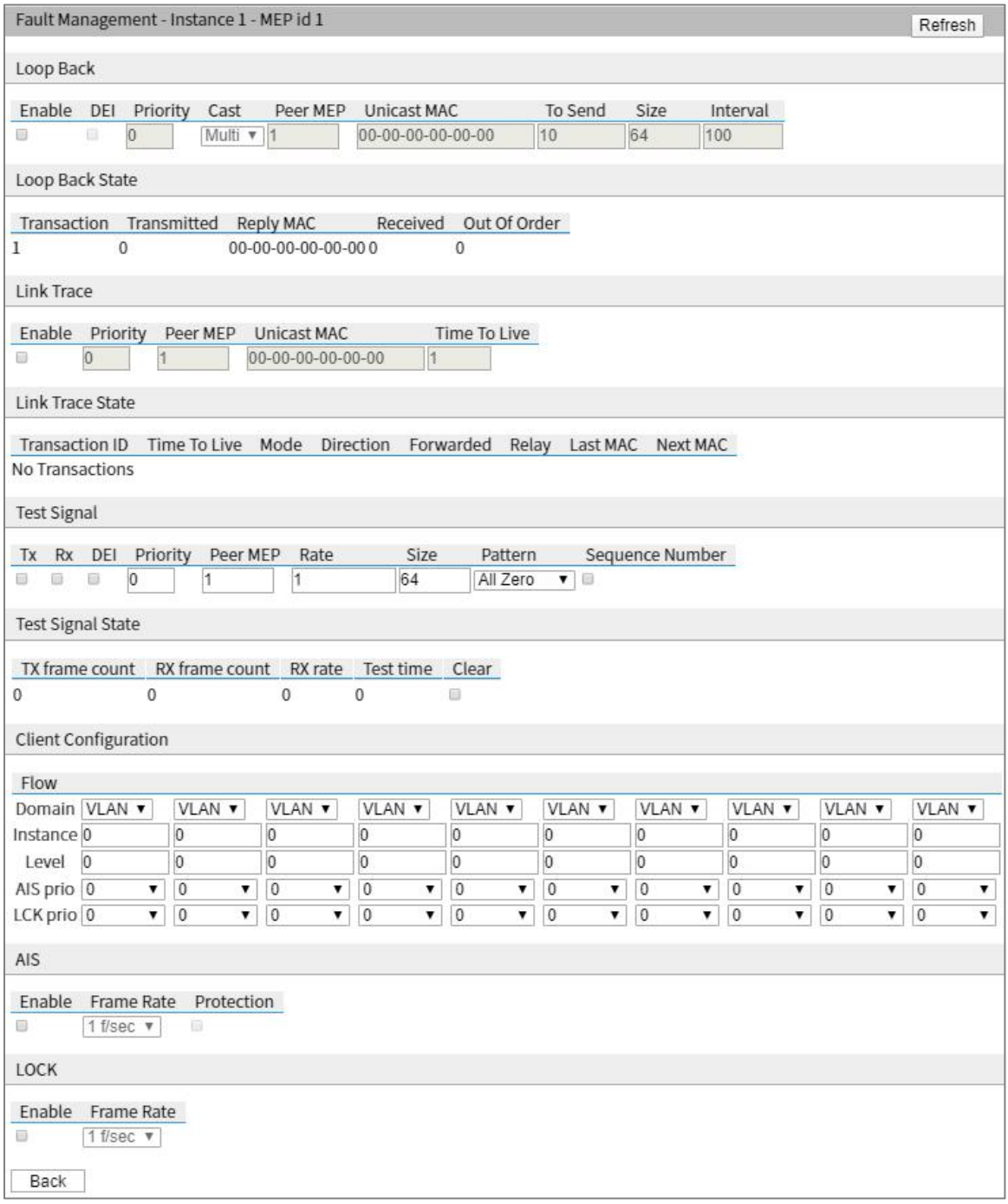
Refresh: Click to refresh the page immediately.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

6.15.2 Fault Management

Click “Fault Management” in “Function Configuration” of “MEP Configuration” page to enter fault management configuration page. This page allows the user to inspect and configure the Fault Management of the current MEP Instance.



Loop Back

Enable

Loop Back based on transmitting/receiving LBM/LBR PDU can be enabled/disabled. Loop Back is automatically disabled when all 'To Send' LBM PDU has been transmitted - waiting 5 sec. for all LBR from the end.

DEI

The DEI to be inserted as PCP bits in TAG (if any).

Prio

The priority to be inserted as PCP bits in TAG (if any).

Cast

Selection of LBM PDU transmitted unicast or multi-cast. The unicast MAC will be configured through 'Peer MEP' or 'Unicast Peer MAC'. To-wards MIP only unicast Loop Back is possible.

Peer MEP

This is only used if the 'Unicast MAC' is configured to all zero. The LBM unicast MAC will be taken from the 'Unicast Peer MAC' configuration of this peer.

Unicast MAC

This is only used if NOT configured to all zero. This will be used as the LBM PDU unicast MAC. This is the only way to configure Loop Back to-wards a MIP.

Tx

The number of LBM PDU to send in one loop test. The value 0 indicate infinite transmission (test behaviour). This is HW based LBM/LBR and Requires VOE.

Size

The LBM frame size. This is entered as the wanted size (in bytes) of a un-tagged frame containing LBM OAM PDU - including CRC (four bytes).
Example when 'Size' = 64 => Un-tagged frame size = DMAC(6) + SMAC(6) + TYPE(2) + TST PDU LENGTH(46) + CRC(4) = 64 bytes
The transmitted frame will be four bytes longer for each tag added - 8 bytes in case of a tunnel EVC.
There are two frame MAX sizes to consider.
Switch RX frame MAX size: The MAX frame size (all inclusive) accepted on the switch port of 9600 Bytes
CPU RX frame MAX size: The MAX frame size (all inclusive) possible to copy to CPU of 1526 Bytes
Consider that the Peer MEP must be able to handle the selected frame size. Consider that In case of SW based MEP, the received LBR PDU must be copied to CPU
Warning will be given if selected frame size exceeds the CPU RX frame MAX size
Frame MIN Size is 64 Bytes.

Interval

The interval between transmitting LBM PDU. In 10 ms. If 'To Send' != 0 (max 100 - '0' is as fast as possible) in 1us. If ‘To Send’ == 0 (max 10.000).

Loop Back State

Transaction ID

The transaction id of the first LBM transmitted. For each LBM transmitted the transaction ID in the PDU is incremented.

Tx

The total number of LBM PDU transmitted.

Reply MAC

The MAC of the replying MEP/MIP. In case of multicast LBM, replies from all peer MEP in the group can be received. This MAC is not shown in case of 'To Send' == 0.

Rx

The total number of LBR PDU received from this 'Reply MAC'.

Out Of Order

The number of LBR PDU received from this 'Reply MAC' with incorrect 'Transaction ID'.

Link Tracking

Enable

Link Trace based on transmitting/receiving LTM/LTR PDU can be enabled/disabled. Link Trace is automatically disabled when all 5 transactions are done with 5 sec. interval - waiting 5 sec. for all LTR in the end. The LTM PDU is always transmitted as Multi-cast Class 2.

Priority

The priority to be inserted as PCP bits in TAG (if any).

Peer MEP

This is only used if the 'Unicast MAC' is configured to all zero. The Link Trace Target MAC will be taken from the 'Unicast Peer MAC' configuration of this peer.

Unicast MAC

This is only used if NOT configured to all zero. This will be used as the Link Trace Target MAC. This is the only way to configure a MIP as Target MAC.

Time To Live

This is the LTM PDU TTL value as described in Y.1731. This value is decremented each time forwarded by a MIP. Will not be forwarded reaching zero.

Link Trace State

Transaction ID

The transaction id is incremented for each LTM send. This value is inserted the transmitted LTM PDU and is expected to be received in the LTR PDU. Received LTR with wrong transaction id is ignored. There are five transactions in one Link Trace activated.

Time To Live

This is the TTL value taken from the LTM received by the MIP/MEP sending this LTR - decremented as if forwarded.

Mode

Indicating if is was a MEP/MIP sending this LTR.

Direction

Indicating if MEP/MIP sending this LTR is ingress/egress.

Forwarded

Indicating if MEP/MIP sending this LTR has forwarded the LTM.

Relay

The Relay action can be one of the following:

- MAC: This is a hit on the LT Target MAC.
- FDB: LTM is forwarded based on hit in the Filtering DB.
- MFDB: LTM is forwarded based on hit in the MIP CCM DB.

Last MAC

The MAC identifying the last sender of the LBM causing this LTR - initiating MEP or previous MIP forwarding.

Next MAC

The MAC identifying the next sender of the LBM causing this LTR - MIP forwarding or terminating MEP.

Test Signal

Tx

Sending Test Signal based on TST PDU can be enabled/disabled.

Rx

Receiving Test Signal based on TST PDU can be enabled/disabled.

DEI

The DEI to be inserted as PCP bits in TAG (if any).

Prio

The priority to be inserted as PCP bits in TAG (if any).

Peer MEP

The TST frame destination MAC will be taken from the 'Unicast Peer MAC' configuration of this peer.

Speed

The TST frame transmission bit rate - in Mega bits pr. second. Limit is 400 Mbps. This is the bit rate of a standard frame without any encapsulation. If 1 Mbps rate is selected in a EVC MEP, the added tag will give a higher bitrate on the wire.

Size

The TST frame size. This is entered as the wanted size (in bytes) of a un-tagged frame containing TST OAM PDU - including CRC (four bytes).
Example when 'Size' = 64 => Un-tagged frame size = DMAC(6) + SMAC(6) + TYPE(2) + TST PDU LENGTH(46) + CRC(4) = 64 bytes
The transmitted frame will be four bytes longer for each tag added - 8 bytes in case of a tunnel EVC.
There are two frame MAX sizes to consider.

Switch RX frame MAX size: The MAX frame size (all inclusive) accepted on the switch port of 9600 Bytes
CPU RX frame MAX size: The MAX frame size (all inclusive) possible to copy to CPU of 1526 Bytes
Consider that the Peer MEP must be able to handle the selected frame size. Consider that in order to calculate the 'RX rate' a received TST PDU must be copied to CPU.
Warning will be given if selected frame size exceeds the CPU RX frame MAX size
Frame MIN Size is 64 Bytes.

Mode

The 'empty' TST PDU has the size of 12 bytes. In order to achieve the configured frame size a data TLV will be added with a pattern.
Example when 'Size' = 64 => Un-tagged frame size = DMAC(6) + SMAC(6) + TYPE(2) + TST PDU LENGTH(46) + CRC(4) = 64 bytes
The TST PDU needs to be 46 bytes so a pattern of 46-12=34 bytes will be added.

- All Zero: Pattern will be '00000000'
- All one: Pattern will be '11111111'

- 10101010: Pattern will be '10101010'

Test Signal State

TX frame count

The number of transmitted TST frames since last 'Clear'.

RX frame count

The number of received TST frames since last 'Clear'.

RX rate

The current received TST frame bit rate in Kbps. This is calculated on a 1 s. basis, starting when first TST frame is received after 'Clear'. The frame size used for this calculation is the first received after 'Clear'

Test time

The number of seconds passed since first TST frame received after last 'Clear'.

Clear

This will clear all Test Signal State. Transmission of TST frame will be restarted. Calculation of 'Rx frame count', 'RX rate' and 'Test time' will be started when receiving first TST frame.

Client Configuration

Only a Port MEP is able to be a server MEP with flow configuration. The Priority in the client flow is always the highest priority configured in the EVC.

Flow

- Domain: The domain of the client layer flow.
- Instance: Client layer flow instance numbers.
- Level: Client layer level - AIS and LCK PDU transmitted in this client layer flow will be on this level.
- AIS Prio: The priority to be used when transmitting AIS in each client flow. Priority resulting in highest possible PCP can be selected.
- LCK Prio: The priority to be used when transmitting LCK in each client flow. Priority resulting in highest possible PCP can be selected.

AIS

Enable

Insertion of AIS signal (AIS PDU transmission) in client layer flows, can be enable/disabled.

Frame rate

Selecting the frame rate of AIS PDU. This is the inverse of transmission period as described in Y.1731.:

Protection

Selecting this means that the first 3 AIS PDU is transmitted as fast as possible - in case of using this for protection in the end point.

LOCK

Enable

Insertion of LOCK signal (LCK PDU transmission) in client layer flows, can be enable/disabled.

Frame rate

The frame rate of LCK PDU. This is the inverse of transmission period as described in Y.1731.:

Buttons

Back: Click to go back to this MEP instance main page.

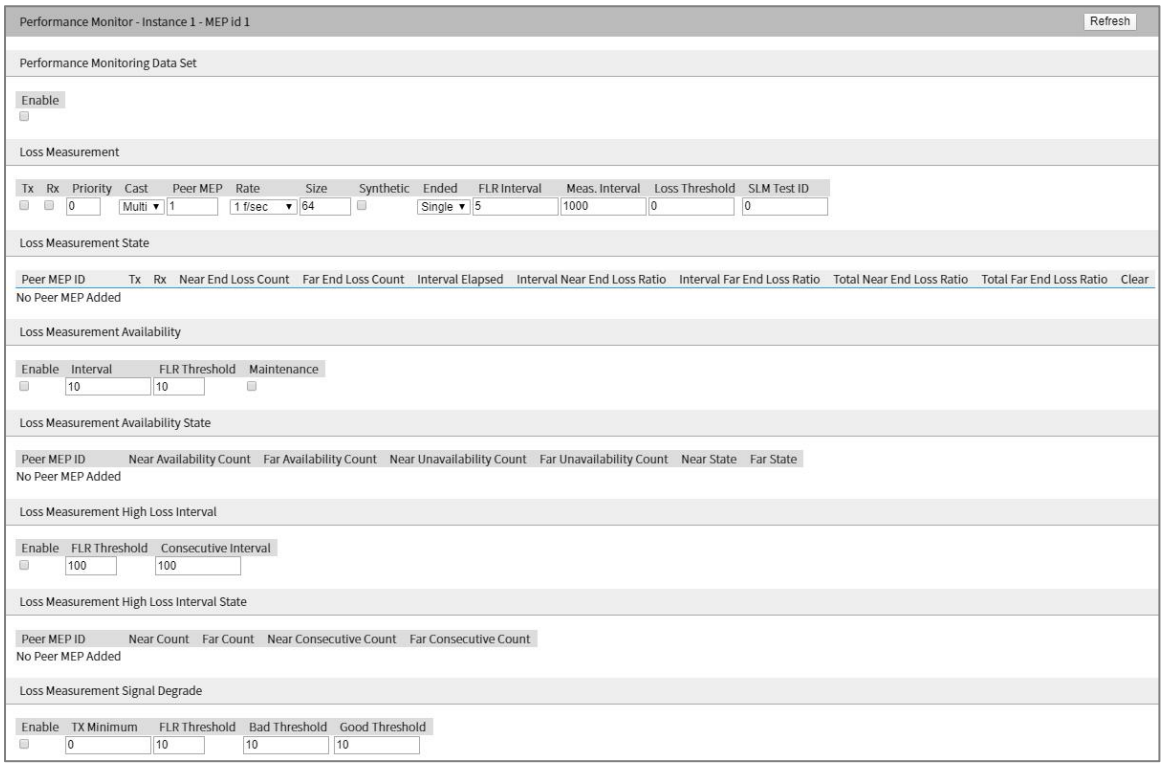
Save: Click to save changes.

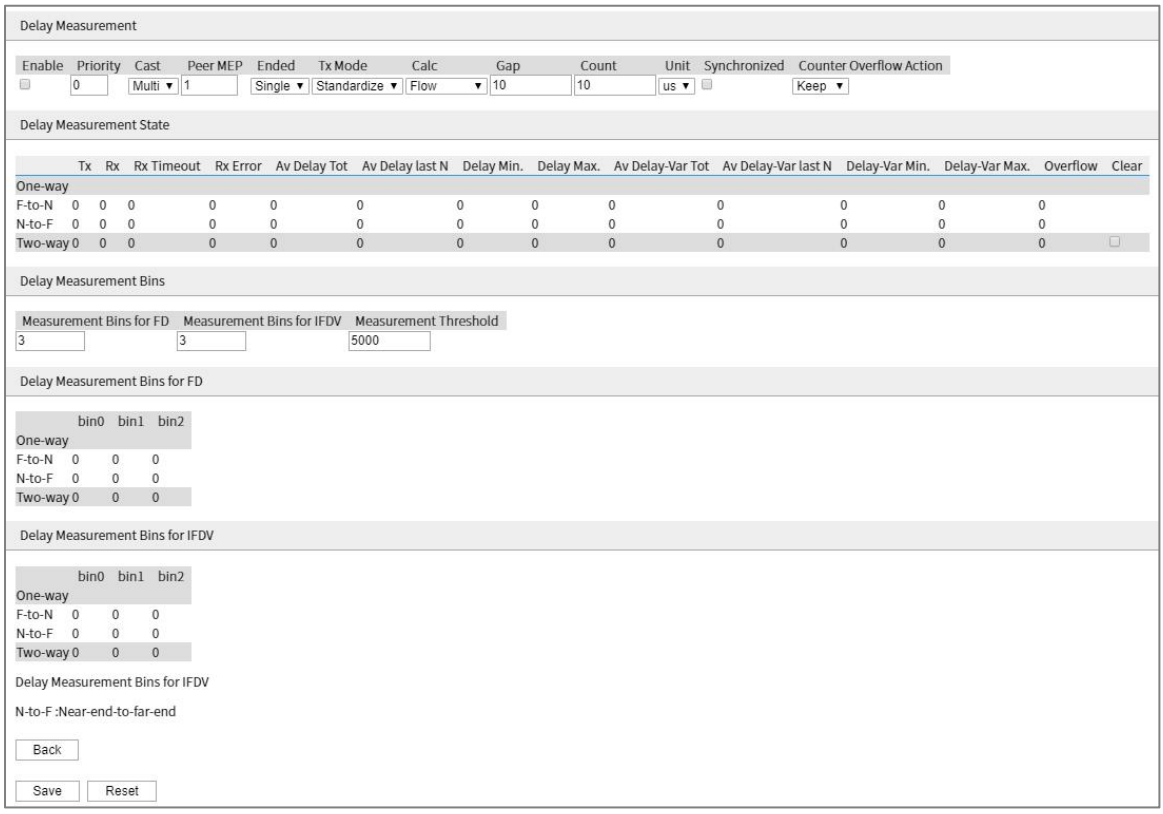
Reset: Click to undo any changes made locally and revert to previously saved values.

6.15.3 Performance Monitoring

Click “Performance Monitoring” in “Function Configuration” of “MEP Configuration” page to enter performance monitoring page.

This page allows the user to inspect and configure the performance monitor of the current MEP Instance.





Performance Monitoring Data Set

Enable

When enabled this MEP instance will contribute to the 'PM Data Set' gathered by the PM Session.

Loss Measurement

Tx

Loss Measurement initiator is enabled/disabled. Initiator is transmitting/receiving CCM or LMM/LMR or SLM/SLR/1SL PDUs - see 'Synthetic' and 'Ended'.
Service frame LM (not 'Synthetic') is only allowed with one Peer MEP configured.
Synthetic frame LM is allowed with multiple Peer MEPs configured.

Rx

Enable loss calculation when receiving LM PDUs (LMM/SLM/1SL). This is ignored when LM initiator is enabled.

Priority

The priority to be inserted as PCP bits in TAG (if any). In case of enable of Continuity Check and Loss Measurement both implemented on SW based CCM, 'Priority' has to be the same.

Cast

Selection of LM PDU transmitted unicast or multicast. The unicast MAC will be taken from the 'Unicast Peer MAC' database. In case of enable of Continuity Check and dual ended Loss Measurement both implemented on SW based CCM, 'Cast' has to be the same.

Peer MEP

Peer MEP-ID for unicast LM. The MAC is taken from the 'Unicast Peer MAC' database. Only used in case of multiple peers ('Synthetic' LM).

Rate

Selecting the frame rate of LM PDU. This is the inverse of transmission period as described in Y.1731
Selecting 100f/sec is only valid in case of 'Synthetic' LM.
Selecting 6f/min is not valid in case of dual ended 'Service frame' LM (CCM PDU based).
In case of enable of Continuity Check and Loss Measurement both implemented on SW based CCM, 'Frame Rate' has to be the same.

Size

The 'Synthetic' SLM/1SL frame size. This is entered as the wanted size (in bytes) of a un-tagged frame containing LM OAM PDU - including CRC (four bytes).

Example when 'Size' = 64 => Un-tagged frame size = DMAC(6) + SMAC(6) + TYPE(2) + TST PDU LENGTH(46) + CRC(4) = 64 bytes.
The transmitted frame will be four bytes longer for each tag added - 8 bytes in case of a tunnel EVC.
There are two frame MAX sizes to consider.
Switch RX frame MAX size: The MAX frame size (all inclusive) accepted on the switch port of Bytes
CPU RX frame MAX size: The MAX frame size (all inclusive) possible to copy to CPU of Bytes.
Consider that the Peer MEP must be able to handle the selected frame size. Consider that the received SLR PDU must be copied to CPU
Warning will be given if selected frame size exceeds the CPU RX frame MAX size
Frame MIN Size is 64 Bytes.

Synthetic

Synthetic frame LM is enable. This is SLM/SLR/1SL PDU based LM.

Ended

Single: Single ended Loss Measurement implemented on LMM/LMR or SLM/SLR.
Dual: Dual ended Loss Measurement implemented on SW based CCM or 1SL.

FLR Interval

This is the interval in number of measurement intervals where the interval Frame Loss Ratio is calculated.

Meas. Interval

This is the 'synthetic' LM measurement interval in milliseconds. This must be a whole number of the LM PDU transmission interval (inverse 'Rate'). This is the interval in time where the loss and FLR is calculated based on the counted number of SL OAM PDUs. It is in this interval that the calculated FLR is checked against availability, high loss and degraded FLR threshold.
Example: 'Rate' = 100f/sec => 'Meas Interval' = N*10 milliseconds.
Example: 'Rate' = 10f/sec => 'Meas Interval' = N*100 milliseconds.
In case of service frame based LM this attribute is not used and the measurement interval is always the LM PDU transmission interval.

Loss Threshold

Far end loss threshold count is incremented if a loss measurement is above this threshold.

SLM Test ID

Test ID value used in SLM PDUs. The default value is 0.

Loss Measurement State

Peer MEP

The Peer MEP ID that the following state relates to.

Tx

The accumulated transmitted LM PDUs - since last 'clear'.

Rx

The accumulated received LM PDUs - since last 'clear'.

Near End Loss Count

The accumulated near end frame loss count - since last 'clear'.

Far End Loss Count

The accumulated far end frame loss count - since last 'clear'.

Interval Elapsed

The accumulated number of 'FLR Interval' elapsed - since last 'clear'.

Interval Near End Loss Ratio

The near end frame loss ratio calculated based on the near end frame loss count and far end frame transmitted - in the latest 'FLR Interval'. This is shown in (Loss/Tx)*10000. Same as 1/100 Percent.

Interval Far End Loss Ratio

The far end frame loss ratio calculated based on the far end frame loss count and near end frame transmitted - in the latest 'FLR Interval'. This is shown in (Loss/Tx)*10000. Same as 1/100 Percent.

Total Near End Loss Ratio

The near end frame loss ratio calculated based on the near end frame loss count and far end frame transmitted - since last 'clear'. This is shown in (Loss/Tx)*10000. Same as 1/100 Percent.

Total Far End Loss Ratio

The far end frame loss ratio calculated based on the far end frame loss count and near end frame transmitted - since last 'clear'. This is shown in (Loss/Tx)*10000. Same as 1/100 Percent.

Clear

Set of this check and save will clear the accumulated counters and restart ratio calculation.

Loss Measurement Availability

Enable

Enable/disable of loss measurement availability.

Interval

Availability interval - number of measurements with same availability in order to change availability state.

FLR Threshold

Availability frame loss ratio threshold in per mile.

Maintenance

Enable/disable of loss measurement availability maintenance.

Loss Measurement Availability Status

Peer MEP ID

Peer MEP ID.

Near Availability Count

Near end availability count.

Far Availability Count

Far end availability count.

Near Unavailability Count

Near end unavailability count.

Far Unavailability Count

Far end unavailability count.

Near State

Near end availability state.

Far State

Far end availability state.

Loss Measurement High Loss Interval

Enable

Enable/disable of loss measurement high loss interval.

FLR Threshold

High Loss Interval frame loss ratio threshold in per mile.

Consecutive Interval

High Loss Interval consecutive interval (number of measurements).

Loss Measurement High Loss Interval Status

Peer MEP ID

Peer MEP ID.

Near Count

Near end high loss interval count (number of measurements where availability state is available and FLR is above high loss interval FLR threshold.

Far Count

Far end high loss interval count (number of measurements where availability state is available and FLR is above high loss interval FLR threshold.

Near Consecutive Count

Near end high loss interval consecutive count.

Far Consecutive Count

Far end high loss interval consecutive count.

Loss Measurement Signal Degrade

Enable

Enable/disable of loss measurement signal degrade.

TX Minimum

Minimum number of frames that must be transmitted in a measurement before frame loss ratio is tested against loss ratio threshold.

FLR Threshold

Signal Degraded frame loss ratio threshold in per mile.

Bad Threshold

Number of consecutive bad interval measurements required to set degrade state.

Good Threshold

Number of consecutive good interval measurements required to clear degrade state.

Delay Measurement

Enable

Delay Measurement based on transmitting 1DM/DMM PDU can be enabled/disabled. Delay Measurement based on receiving and handling 1DM/DMR PDU is always enabled.

Priority

The priority to be inserted as PCP bits in TAG (if any).

Cast

Selection of 1DM/DMM PDU transmitted unicast or multicast. The unicast MAC will be configured through 'Peer MEP'.

Peer MEP

This is only used if the 'Cast' is configured to Uni. The 1DM/DMR unicast MAC will be taken from the 'Unicast Peer MAC' configuration of this peer.

Ended

- Single: Single ended Delay Measurement implemented on DMM/DMR.
- Dual: Dual ended Delay Measurement implemented on 1DM.

Tx Mode

- Standardize: Y.1731 standardize way to transmit 1DM/DMR.
- Proprietary： Proprietary way with follow-up packets to transmit 1DM/DMR.

Calc

This is only used when "Ended" is configured as single ended.

- Round trip: The frame delay calculated by the transmitting and receiving timestamps of initiators. Frame Delay = RxTimeb-TxTimeStampf.
- Flow: The frame delay calculated by the transmitting and receiving timestamps of initiators and remotes. Frame Delay = (RxTimeb-TxTimeStampf)-(TxTimeStampb-RxTimeStampf).

Gap

The gap between transmitting 1DM/DMM PDU in 10ms. The range is 10 to 65535.

Count

The number of last records to calculate. The range is 10 to 2000.

Unit

The time resolution.

Synchronized

Enable to use DMM/DMR packet to calculate dual ended DM. If the option is enabled, the following action will be taken. When DMR is received, two-way delay (roundtrip or flow) and both near-end-to-far-end and far-end-to-near-end one-way delay are

calculated. When DMM or 1DM is received, only far-end-to-near-end one-way delay is calculated.

Counter Overflow Action

The action to counter when overflow happens.

Delay Measurement State

One-way

One-way delay.

- F-to-N: The one-way delay is from remote devices to the local devices. Here are the conditions to calculate this delay.
  - 1DM receive.
  - DMM received with Synchronized enabled.
  - DMR received with Synchronized enabled.
- N-to-F: The one-way delay is from the local devices to remote devices. The only case to calculate this delay is below. DMR received with Synchronized enabled.

Two-way

Two-way delay.

Tx

The accumulated transmit count - since last 'clear'.

Rx

The accumulated receive count - since last 'clear'.

Rx Timeout

The accumulated receive timeout count for two-way only - since last 'clear'.

Rx Error

The accumulated receive error count - since last 'clear'. This is counting if the frame delay is larger than 1 second or if far end residence time is larger than the round trip time.

Av Delay Tot

The average total delay - since last 'clear'.

Av Delay last N

The average delay of the last n packets - since last 'clear'.

Delay Min.

The minimum delay - since last 'clear'.

Delay Max.

The maximum delay - since last 'clear'.

Av Delay-Var Tot

The average total delay variation - since last 'clear'.

Av Delay-Var last N

The average delay variation of the last n packets - since last 'clear'.

Delay-Var Min.

The minimum delay variation - since last 'clear'.

Delay-Var Max.

The maximum delay variation - since last 'clear'.

Overflow

The number of counter overflow - since last 'clear'.

Clear

Set of this check and save will clear the accumulated counters.

Delay Measurement Bins

A Measurement Bin is a counter that stores the number of delay measurements falling within a specified range, during a Measurement Interval.

Measurement Bins for FD

Configurable number of Frame Delay Measurement Bins per Measurement Interval.

The minimum number of FD Measurement Bins per Measurement Interval supported is 2.

The maximum number of FD Measurement Bins per Measurement Interval supported is 10.

The default number of FD Measurement Bins per Measurement Interval supported is 3.

Measurement Bins for IFDV

Configurable number of Inter-Frame Delay Variation Measurement Bins per Measurement Interval.

The minimum number of FD Measurement Bins per Measurement Interval supported is 2.

The maximum number of FD Measurement Bins per Measurement Interval supported is 10.

The default number of FD Measurement Bins per Measurement Interval supported is 2.

Measurement Threshold

Configurable the Measurement Threshold for each Measurement Bin.

The unit for a measurement threshold is in microseconds (us).

The default configured measurement threshold for a Measurement Bin is an increment of 5000 us.

Delay Measurement Bins for FD

One-way

One-way delay.

- F-to-N: The one-way delay is from remote devices to the local devices. Here are the conditions to calculate this delay.
  - 1DM receive.
  - DMM received with Synchronized enabled.
  - DMR received with Synchronized enabled.
- N-to-F: The one-way delay is from the local devices to remote devices. The only case to calculate this delay is below. DMR received with Synchronized enabled.

Two-way

Two-way delay.

Bin#

A Measurement Bin is a counter that stores the number of delay measurements falling within a specified range, during a Measurement Interval.

If the measurement threshold is 5000 us and the total number of Measurement Bins is four, we can give an example as follows.

Bin	Threshold	Range
bin0	0 us	0 us <= measurement < 5,000 us
bin1	5,000 us	5,000 us <= measurement < 10,000 us
bin2	10,000 us	10,000 us <= measurement < 15,000 us
bin3	15,000 us	15,000 us <= measurement < infinite us

Delay Measurement Bins for IFDV

One-way

One-way delay.

- F-to-N: The one-way delay is from remote devices to the local devices. Here are the conditions to calculate this delay.
  - 1DM receive.

- DMM received with Synchronized enabled.
- DMR received with Synchronized enabled.

- N-to-F: The one-way delay is from the local devices to remote devices. The only case to calculate this delay is below. DMR received with Synchronized enabled.

Two-way

Two-way delay.

Bin#

A Measurement Bin is a counter that stores the number of delay measurements falling within a specified range, during a Measurement Interval.

If the measurement threshold is 5000 us and the total number of Measurement Bins is four, we can give an example as follows.

Bin	Threshold	Range
bin0	0 us	0 us <= measurement < 5,000 us
bin1	5,000 us	5,000 us <= measurement < 10,000 us
bin2	10,000 us	10,000 us <= measurement < 15,000 us
bin3	15,000 us	15,000 us <= measurement < infinite us

Buttons

Back: Click to go back to this MEP instance main page.

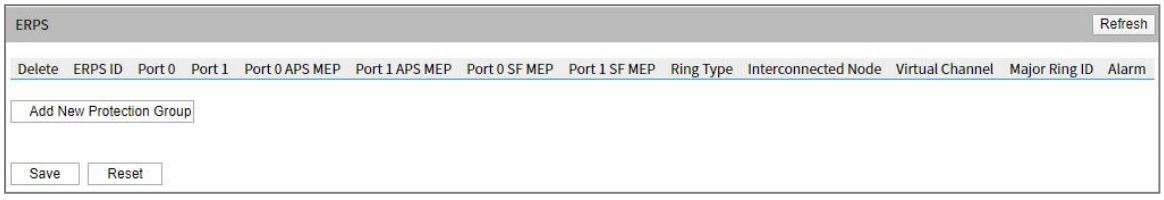
Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

6.16 ERPS

ERPS (Ethernet Ring Protection Switching) supports V1 and V2 versions. ERPS is a broken standard protocol issued by ITU-T. Its convergence speed can meet the requirements of carrier class, effectively prevent the generation of broadcast storm and realize the rapid migration of traffic.

The ERPS instances are configured here.



Delete

This box is used to mark an ERPS for deletion in next save operation.

ERPS ID

The ID of the created Protection group, It must be an integer value between 1 and 64. The maximum numbers of ERPS Protection Groups that can be created are 64. Click on the ID of a Protection group to enter the configuration page.

Port 0

This will create "Port 0" of the switch in the Ring.

Port 1

This will create "Port 1" of the switch in the Ring. As interconnected sub-ring will have only one ring port, "Port 1" is configured as "0" for interconnected sub-ring. "0" in this field indicates that no "Port 1" is associated with this instance

Port 0 APS MEP

The Port 0 APS PDU handling MEP.

Port 1 APS MEP

The Port 1 APS PDU handling MEP. As only one APS MEP is associated with interconnected sub-ring without virtual channel, it is configured as "0" for such ring instances. "0" in this field indicates that no Port 1 APS MEP is associated with this instance.

Port 0 SF MEP

The Port 0 Signal Fail reporting MEP.

Port 1 SF MEP

The Port 1 Signal Fail reporting MEP. As only one SF MEP is associated with interconnected sub-ring without virtual channel, it is configured as "0" for such ring instances. "0" in this field indicates that no Port 1 APS MEP is associated with this instance.

Ring Type

Type of Protecting ring. It can be either major ring or sub-ring.

Interconnected Node

Interconnected Node indicates that the ring instance is interconnected. Click on the checkbox to configure this. "Yes" indicates it is an interconnected node for this instance. "No" indicates that the configured instance is not interconnected.

Virtual Channel

Sub-rings can either have virtual channel or not on the interconnected node. This is configured using "Virtual Channel" checkbox. "Yes" indicates it is a sub-ring with virtual channel. "No" indicates, sub-ring doesn't have virtual channel.

Major Ring ID

Major ring group ID for the interconnected sub-ring. It is used to send topology change updates on major ring. If ring is major, this value is same as the protection group ID of this ring.

Alarm

There is an active alarm on the ERPS.

Buttons

Add new protection group: Click to add a new protection group entry.

Refresh: Click to refresh the page immediately.

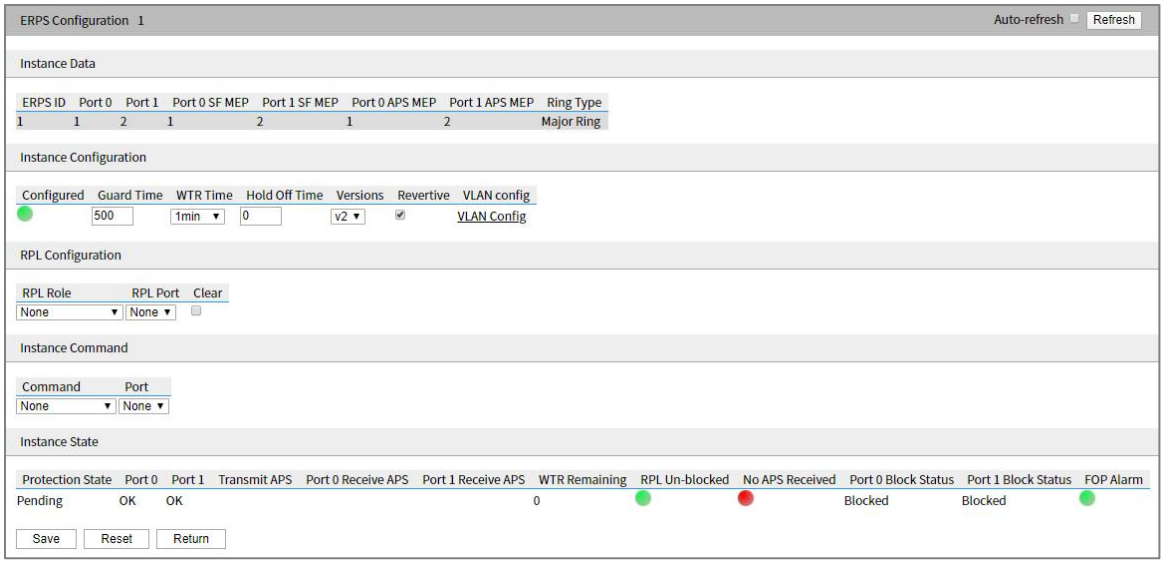
Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

ERPS Instance Configuration

Click the ERPS ID link to enter the ERPS instance configuration page.

This page allows the user to inspect and configure the current ERPS Instance.



Instance Data

ERPS ID

Indicates the ERPS ID.

Port 0

Display the switch ERPS ring port Port 0.

Port 1

Display the switch ERPS ring port Port 1. "Port 1" of the interconnection node is "0", which means that there is no "Port 1" associated with this instance.

Port 0 SF MEP

The Port 0 Signal Fail reporting MEP.

Port 1 SF MEP

The Port 1 Signal Fail reporting MEP. As only one SF MEP is associated with interconnected sub-ring without virtual channel, it is configured as "0" for such ring instances. "0" in this field indicates that no Port 1 APS MEP is associated with this instance.

Port 0 APS MEP

The Port 0 APS PDU handling MEP.

Port 1 APS MEP

The Port 1 APS PDU handling MEP. As only one APS MEP is associated with interconnected sub-ring without virtual channel, it is configured as "0" for such ring instances. "0" in this field indicates that no Port 1 APS MEP is associated with this instance.

Ring Type

Type of Protecting ring. It can be either major ring or sub-ring.

Instance Configuration

Configuration

Red: This ERPS is only created and has not yet been configured - is not active.

Green: This ERPS is configured - is active.

Guard Time

Guard timeout value to be used to prevent ring nodes from receiving outdated R-APS messages.

The period of the guard timer can be configured in 10 ms steps between 10 ms and 2 seconds. The default value is 500 ms.

WTR Time

The Wait To Restore timing value to be used in revertive switching.

The period of the WTR time can be configured by the operator in 1 minute steps between 5 and 12 minutes. The default value is 5 minutes.

Hold Time

The timing value to be used to make persistent check on Signal Fail before switching. The range of the hold off timer is 0 to 10 seconds in steps of 100 ms.

Version

ERPS Protocol Version - v1 or v2

Revertive

In Revertive mode, after the conditions causing a protection switch has cleared, the traffic channel is restored to the working transport entity, i.e., blocked on the RPL.

In Non-Revertive mode, the traffic channel continues to use the RPL, if it is not failed, after a protection switch condition has cleared.

VLAN config

VLAN configuration of the Protection Group. Click on the "VLAN Config" link to configure VLANs for this protection group.

RPL Configuration

RPL Role

It can be either RPL owner or RPL Neighbor.

RPL-Port

This allows to select the east port or west port as the RPL block.

Clear

If the owner has to be changed, then the clear check box allows to clear the RPL owner for that ERPS ring.

Sub-Ring Configuration

This field is displayed when the ring type is Sub Ring.

Sub Ring

Clicking this checkbox indicates that the topology changes in the sub-ring are propagated in the major ring.

Instance Command

Command

Administrative command. A port can be administratively configured to be in either manual switch or forced switch state.

- Forced Switch: Forced Switch command forces a block on the ring port where the command is issued.
- Manual Switch: In the absence of a failure or FS, Manual Switch command forces a block on the ring port where the command is issued.

- Clear: The Clear command is used for clearing an active local administrative command (e.g., Forced Switch or Manual Switch).

Port

Port selection - Port0 or Port1 of the protection Group on which the command is applied.

Instance State

Protection State

ERPS state according to State Transition Tables in G.8032.

Port 0

- OK: State of East port is ok.
- SF: State of East port is Signal Fail

Port1

- OK: State of West port is ok.
- SF: State of West port is Signal Fail.

Transmit APS

The transmitted APS according to State Transition Tables in G.8032.

Port 0 Receive APS

The received APS on Port 0 according to State Transition Tables in G.8032.

Port 1 Receive APS

The received APS on Port 1 according to State Transition Tables in G.8032.

WTR Remaining

Remaining WTR timeout in milliseconds.

RPL Un-blocked

APS is received on the working flow.

No APS Received

RAPS PDU is not received from the other end.

Port 0 Block Status

Block status for Port 0 (Both traffic and R-APS block status). R-APS channel is never blocked on sub-rings without virtual channel.

Port 1 Block Status

Block status for Port 1 (Both traffic and R-APS block status). R-APS channel is never blocked on sub-rings without virtual channel.

FOP Alarm

Failure of Protocol Defect(FOP) status. If FOP is detected, red LED glows; else green LED glows.

Buttons

Save: Click to save changes.

Auto-refresh: Check this box to enable an automatic refresh. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

Reset: Click to undo any changes made locally and revert to previously saved values.

ERPS VLAN Configuration

Click the “VLAN Config” link to enter the ERPS VLAN configuration page.

Delete

To delete a VLAN entry, check this box. The entry will be deleted during the next Save.

VLAN ID

Indicates the ID of this particular VLAN.

Buttons

Add New Entry: Click to add a new VLAN ID. Legal values for a VLAN ID are 1 through 4095. The VLAN is enabled when you click “save”. A VLAN without any port members will be deleted when you click "Save".

Delete: Click to delete the added VLAN.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Back: Click here to return to the previous page.

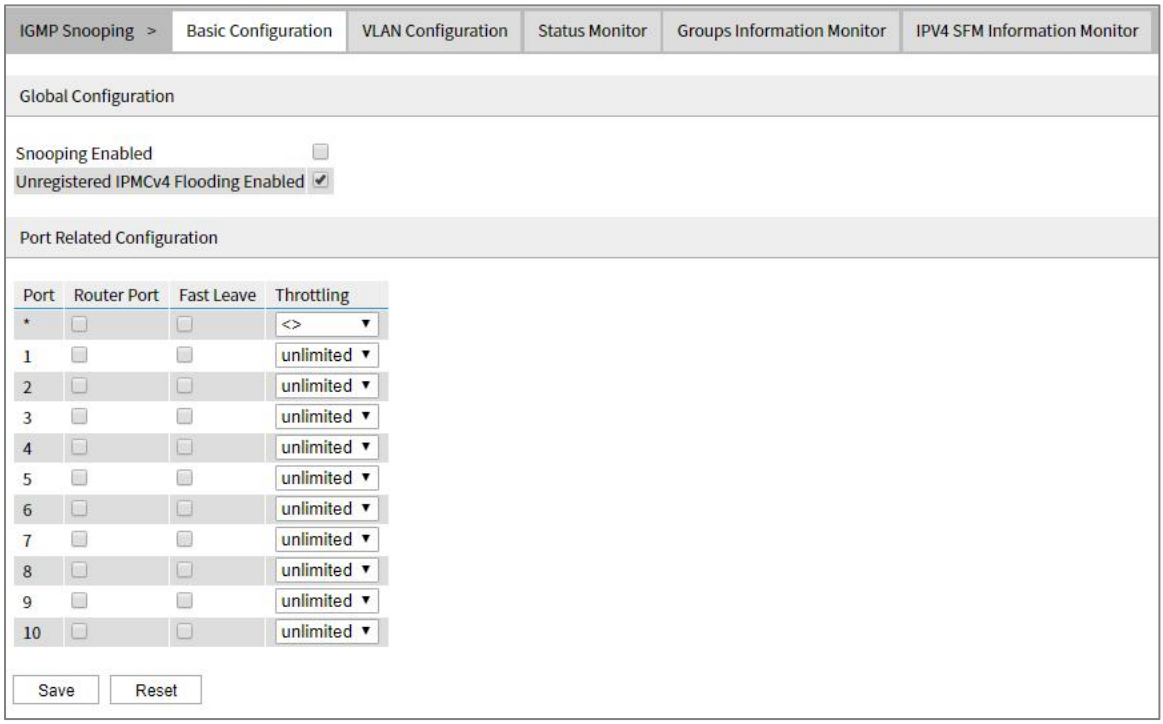
Refresh: Refreshes the displayed table starting from the "VLAN ID" input fields.

7 Multicast

7.1 IGMP Snooping

7.1.1 Basic Configuration

This page provides IGMP Snooping related configuration.



Global Configuration

Snooping Enabled

Enable the Global IGMP Snooping.

Unregistered IPMCv4 Flooding Enabled

Enable unregistered IPMCv4 traffic flooding.

The flooding control takes effect only when IGMP Snooping is enabled.

When IGMP Snooping is disabled, unregistered IPMCv4 traffic flooding is always active in spite of this setting.

Port-related Configuration

Router Port

Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier.

If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.

Fast Leave

Enable the fast leave on the port.

Throttling

Enable to limit the number of multicast groups to which a switch port can belong.

Buttons

Save: Click to save changes.

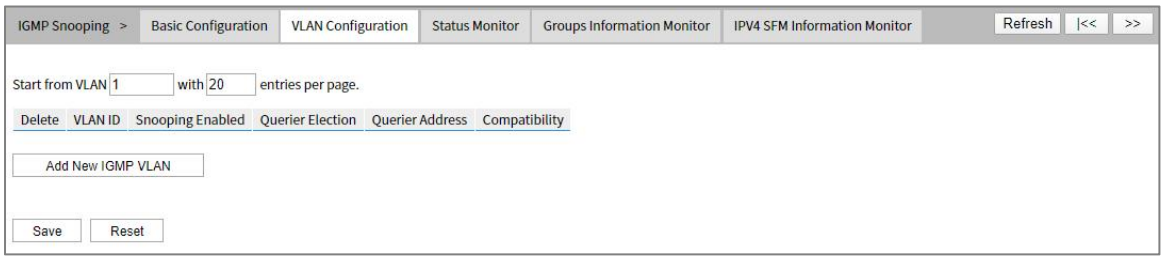
Reset: Click to undo any changes made locally and revert to previously saved values.

7.1.2 VLAN Configuration

Each page shows up to 99 entries from the VLAN table, default being 20, selected through the "__ entries per page" input field. When first visited, the WEB page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table.

The "VLAN" input fields allow the user to select the starting point in the VLAN Table. Clicking the “Refresh” button will update the displayed table starting from that or the closest next VLAN Table match. In addition, the two input fields will - upon a button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

Pressing the “>>” button will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the “|<<” button to start over.



Delete

Check to delete the entry. The designated entry will be deleted during the next save.

VLAN ID

The VLAN ID of the entry.

Enable Listening

Enable the per-VLAN IGMP Snooping. Up to 32 VLANs can be selected for IGMP Snooping.

Querier Election

Enable to join IGMP Querier election in the VLAN. Disable to act as an IGMP Non-Querier.

Querier Address

Define the IPv4 address as source address used in IP header for IGMP Querier election.

When the Querier address is not set, system uses IPv4 management address of the IP interface associated with this VLAN.

When the IPv4 management address is not set, system uses the first available IPv4 management address.

Otherwise, system uses a pre-defined value. By default, this value will be 192.0.2.1.

IGMP Versions

Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of IGMP operating on hosts and routers within a network.

The allowed selection is IGMP-Auto, Forced IGMPv1, Forced IGMPv2, Forced IGMPv3, default compatibility value is IGMP-Auto.

Buttons

Refresh: Refreshes the displayed table starting from the "VLAN" input fields.

|<<: Updates the table starting from the first entry in the VLAN Table, i.e. the entry with the lowest VLAN ID.

>>: Updates the table, starting with the entry after the last entry currently displayed.

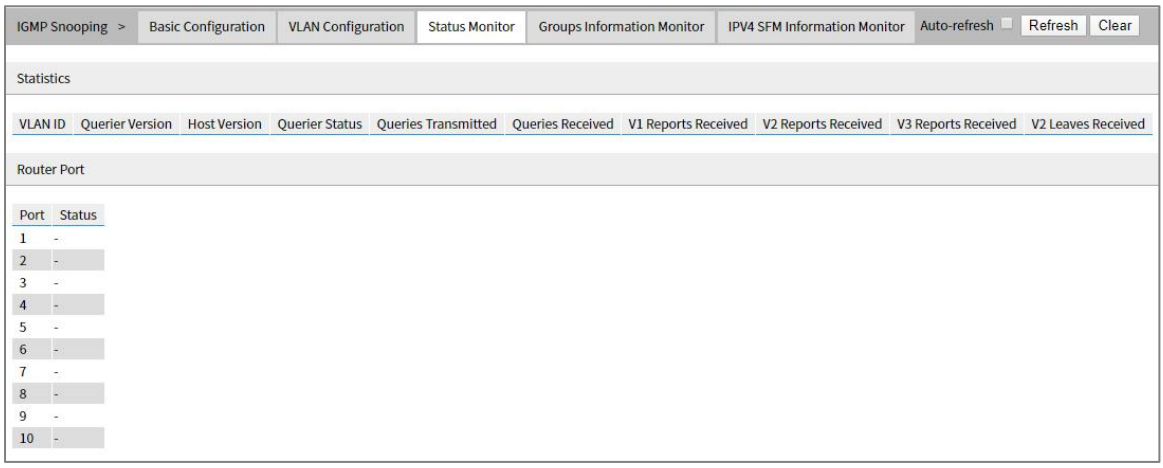
Add New IGMP VLAN: click here to add new IGMP VLAN. Specify the VID and configure the new entry. Click "Save". The specific IGMP VLAN starts working after the corresponding static VLAN is also created.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

7.1.3 Status Monitoring

This page provides IGMP Snooping status.



VLAN ID

The VLAN ID of the entry.

Querier Version

Working Querier Version currently.

Host Version

Working Host Version currently.

Query Status

Shows the Querier status is "ACTIVE" or "IDLE".

"DISABLE" denotes the specific interface is administratively disabled.

Number of Transmitted Inquiry Messages

The number of Transmitted Queries.

Queries Received

The number of Received Queries.

V1 Reports Received

The number of Received V1 Reports.

V2 Reports Received

The number of Received V2 Reports.

V3 Reports Received

The number of Received V3 Reports.

V2 Leaves Received

The number of Received V2 Leaves.

Router Port

Display which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or MLD querier.

Static denotes the specific port is configured to be a router port.

Dynamic denotes the specific port is learnt to be a router port.

Both denote the specific port is configured or learnt to be a router port.

Port

The switch port number.

Status

Indicate whether specific port is a router port or not.

Buttons

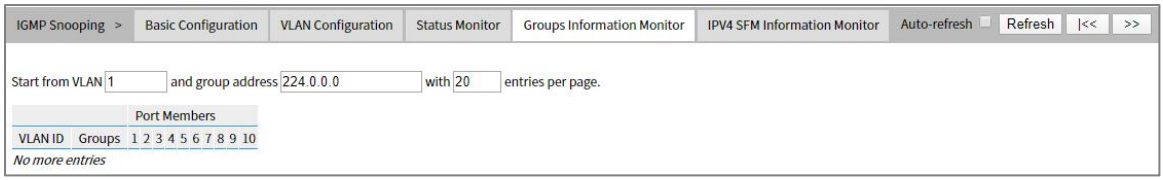
Auto-refresh: Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

Clear: Clears all Statistics counters.

7.1.4 Group Information Monitoring

Entries in the IGMP Group Table are shown on this page. The IGMP Group Table is sorted first by VLAN ID, and then by group.



Each page shows up to 99 entries from the IGMP Group table, default being 20, selected through the "__ entries per page" input field. When first visited, the WEB page will show the first 20 entries from the beginning of the IGMP Group Table.

The "Start from VLAN__", and "group" input fields allow the user to select the starting point in the IGMP Group Table. Clicking the “Refresh” button will update the displayed table starting from that or the closest next IGMP Group Table match. In addition, the two input fields will - upon a “Refresh” button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

“>>” will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the “|<<” button to start over.

VLAN ID

VLAN ID of the group.

Group

Group address of the group displayed.

Port Members

Ports under this group.

Buttons

Auto-refresh: Automatic refresh occurs every 3 seconds.

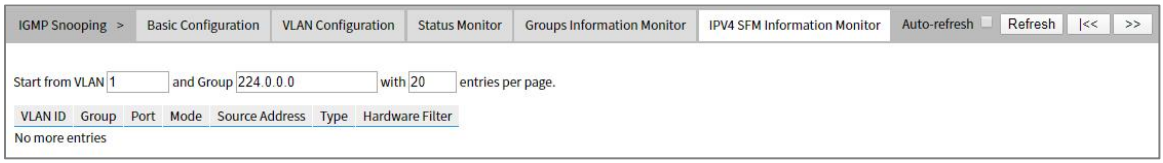
Refresh: Refresh the displayed table starting from the input fields.

|<<: Updates the table, starting with the first entry in the IGMP Group Table.

>>: Updates the table, starting with the entry after the last entry currently displayed.

7.1.5 IPv4 SFM Information Monitoring

Entries in the IGMP SFM Information Table are shown on this page. The IGMP SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses belong to the same group are treated as single entry.



Each page shows up to 99 entries from the IGMP SFM Information Table, default being 20, selected through the "entries per page" input field. When first visited, the WEB page will show the first 20 entries from the beginning of the IGMP SFM Information Table.

The "Start from VLAN__and Group__" input fields allow the user to select the starting point in the IGMP SFM Information Table. Clicking the “Refresh” button will update the displayed table starting from that or the closest next IGMP SFM Information Table match. In addition, the two input fields will - upon a “Refresh” button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

“>>” will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the “|<<” button to start over.

VLAN ID

VLAN ID of the group.

Group

Group address of the group displayed.

Port

The switch port number.

Pattern

Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.

Source Address

IP Address of the source.

Currently, the maximum number of IPv4 source address for filtering (per group) is 8.

When there is no any source filtering address, the text "None" is shown in the Source Address field.

Type

Indicates the Type. It can be either Allow or Deny.

Hardware Filter/Switch

Indicates whether data plane destined to the specific group address from the source IPv4 address could be handled by chip or not.

Buttons

Auto-refresh: Automatic refresh occurs every 3 seconds.

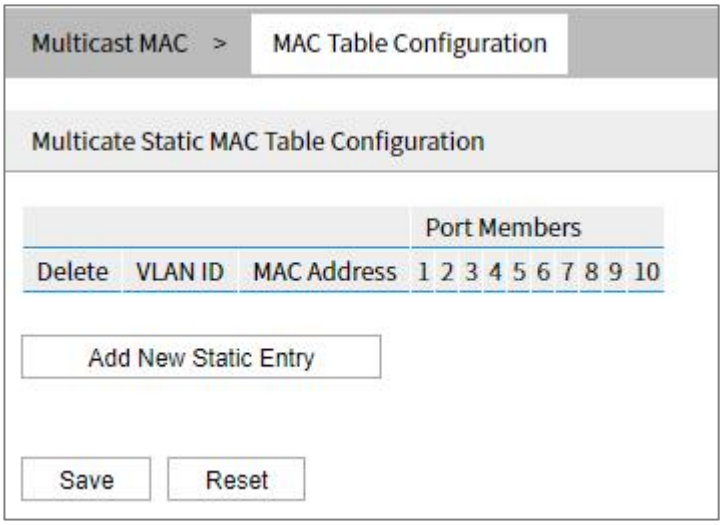
Refresh: Refresh the displayed table starting from the input fields.

|<<: Updates the table starting from the first entry in the IGMP SFM Information Table.

>>: Updates the table, starting with the entry after the last entry currently displayed.

7.2 Multicast MAC

Static multicast MAC address could be added on this page.



Delete

Click the "Delete" button to delete the the current entry.

VLAN

The VLAN ID of the entry.

MAC address;

The multicast MAC address of the entry, such as “01-00-5E-XX-XX-XX”.

Port Members

The ports that are members of the entry.

Buttons

Add new static entry: click to add a new static multicast MAC address entry.

Save: Click to save changes.

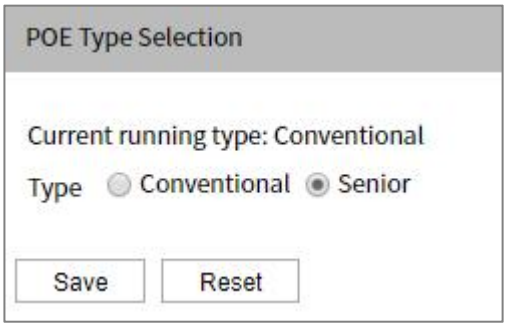
Reset: Click to undo any changes made locally and revert to previously saved values.

8 PoE

POE (Power over Ethernet) refers to power supply through Ethernet network. Poe allows electric power to be transmitted to terminal device through network cable, which greatly saves power wiring cost and provides a simple and convenient power installation mode.

8.1 Type Configuration

This page allows user to select PoE work type.



The current Run type

Display the current PoE type.

Type

Radiobox of PoE type, options are as follows:

- General: In the general type, general configuration of PoE port is supported, such as total power, port priority, port power, port PoE enable, etc.
- Advanced: In the advanced type, in addition to general functions, it also supports functions such as power mode, PoE status monitoring, capacitance detection, power supply delay, policy configuration, automatic check, etc.

PoE type switching takes effect after saving the configuration and restarting the device.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

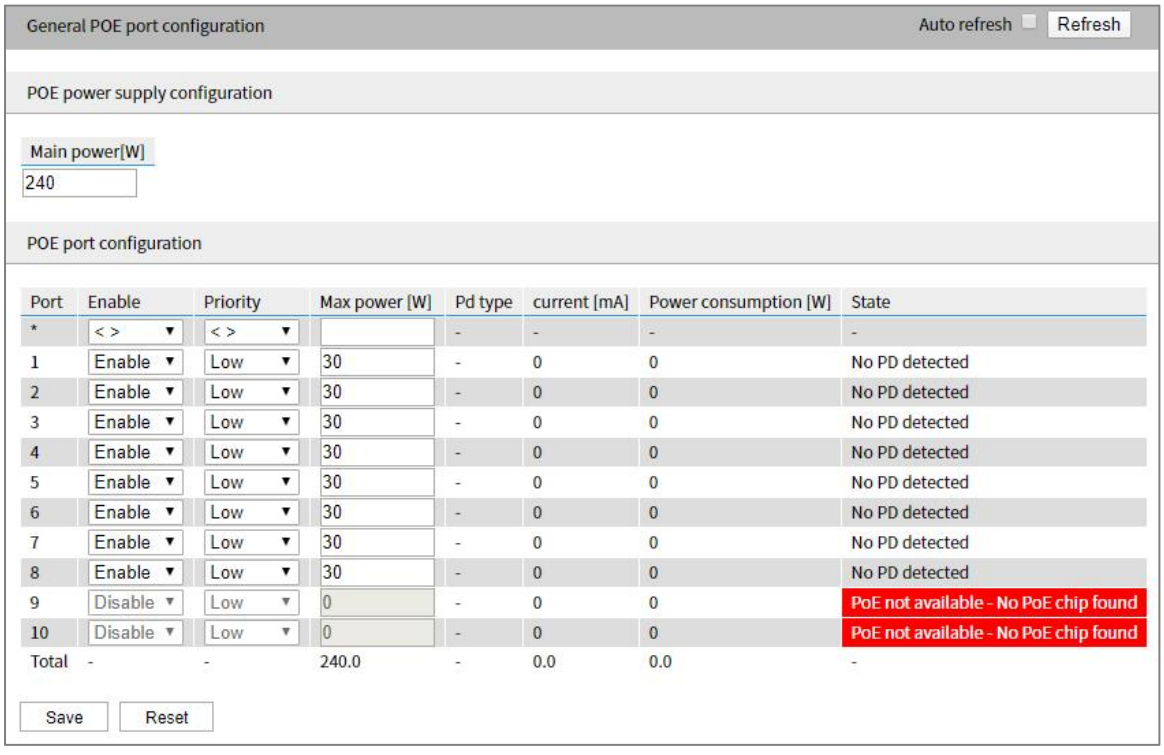
8.2 Global Configuration

In the general type, the global configuration supports PoE normal port configuration.

In the advanced type, the global configuration supports PoE configuration and PoE status monitoring.

8.2.1 POE Normal Port Configuration

This page allows users to check and configure PoE-related parameters under the general type of PoE.



Power Supply Configuration

Primary Power Supply [W]

For being able to determine the amount of power the PD may use, it must be defined what amount of power a power source can deliver.

Valid values are in the range 0 to 240W.

PoE Port Configuration

Port

This is the logical port number for this row.

Ports that are not PoE-capable are grayed out and thus impossible to configure PoE for.

Enable

Enable means PoE enable control of the port.

- Disabled: PoE disabled for the port.
- On: enable PoE/PoE+.

Prio

The Priority represents the ports priority. There are three levels of power priority named Low, High and Critical.

The priority is used in the case where the remote device requires more power than the power supply can deliver. In this case the port with the lowest priority will be turn off starting from the port with the highest port number.

Max power (W)

The Maximum Power value contains a numerical value that indicates the maximum power in watts that can be delivered to a remote device.

The maximum allowed value is 30 W.

PD Class

Each PD is classified according to a class that defines the maximum power the PD will use. The PD Class shows the five classes:

- Class 0: the maximum supported power is 15.4W.
- Class 1: the maximum supported power is 4.0W.
- Class 2: the maximum supported power is 7.0W.
- Class 3: the maximum supported power is 15.4W.
- Class 4: the maximum supported power is 30.0W.

The current [mA]

The Power Used shows how much current the PD currently is using.

Power Used [W]

The Power Used shows how much power the PD currently is using.

Status

Display port status. The status can be one of the following values:

- PoE not available - No PoE chip found
- PoE turned OFF - PoE disabled
- PoE turned OFF - Power budget exceeded - The total requested or used power by the PDs exceeds the maximum power the Power Supply can deliver, and port(s) with the lowest priority is/are powered down.
- No PD detected
- PoE turned OFF - PD overload - The PD has requested or used more power than the port can deliver, and is powered down.
- PoE turned OFF
- Invalid PD - PD detected, but is not working correctly.

Buttons

Save: Click to save changes.

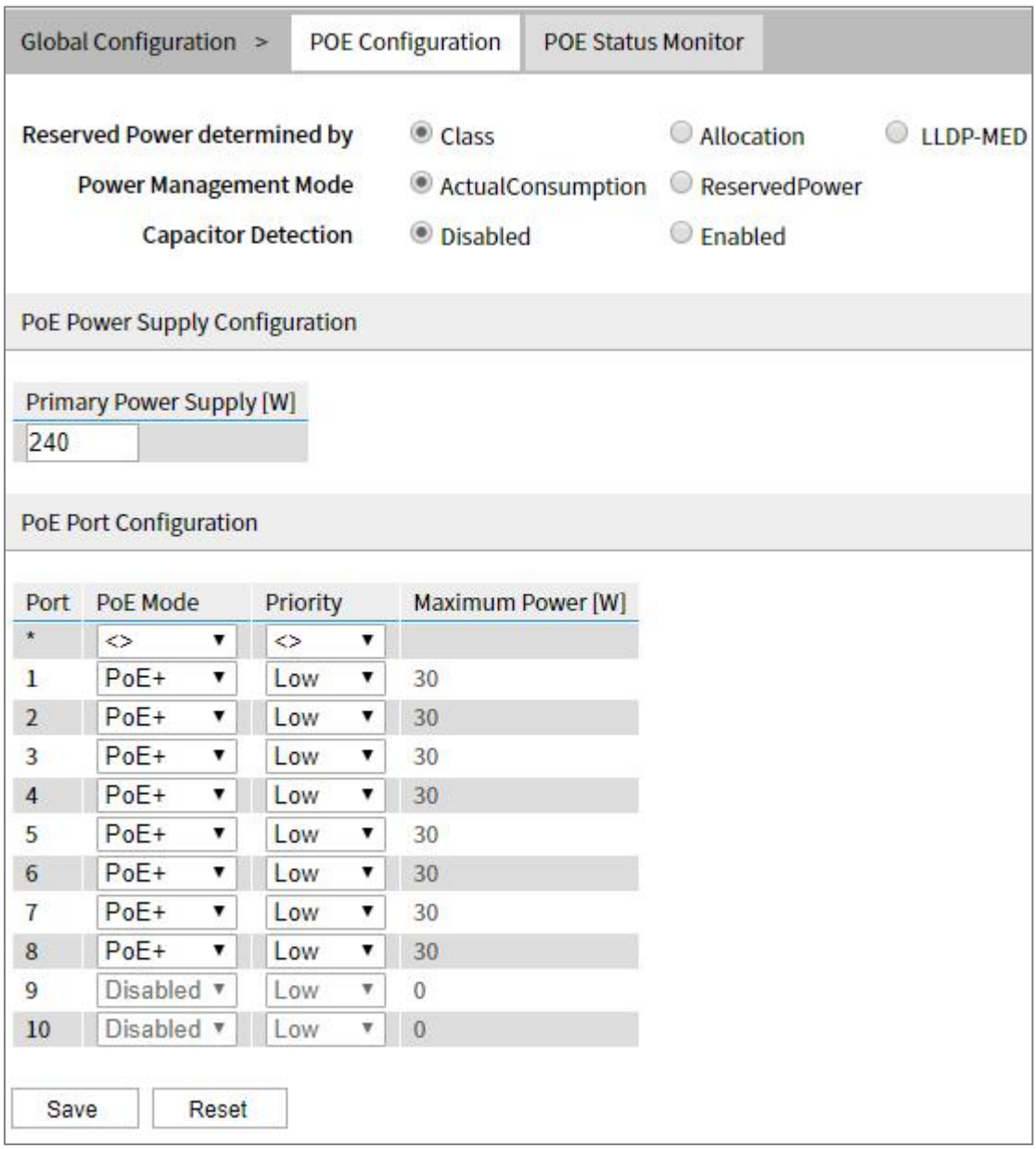
Reset: Click to undo any changes made locally and revert to previously saved values.

Auto-refresh: Check this box to enable an automatic refresh. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page.

8.2.2 PoE Configuration

This page allows the user to inspect and configure the current PoE port settings in PoE advanced type.



Reserved Power determined by

There are three modes for configuring how the ports/PDs may reserve power.

- Allocated mode: In this mode the user allocates the amount of power that each port may reserve. The allocated/reserved power for each port/PD is specified in the Maximum Power fields.
- Class mode: In this mode each port automatically determines how much power to reserve according to the class the connected PD belongs to, and reserves the power accordingly. Four different port classes exist and one for 4, 7, 15.4 or 30 Watts. In this mode the Maximum Power fields have no effect.
- LLDP-MED mode: This mode is similar to the Class mode expect that each port determine the amount power it reserves by exchanging PoE information using the LLDP protocol and reserves power accordingly. If no LLDP information is available for a port, the port will reserve power using the class mode In this mode

the Maximum Power fields have no effect

For all modes: If a port uses more power than the reserved power for the port, the port is shut down.

Power Management Mode

There are 2 modes for configuring when to shut down the ports:

- Actual Consumption: In this mode the ports are shut down when the actual power consumption for all ports exceeds the amount of power that the power supply can deliver or if the actual power consumption for a given port exceeds the reserved power for that port. The ports are shut down according to the ports priority. If two ports have the same priority the port with the highest port number is shut down.
- Reserved Power: In this mode the ports are shut down when total reserved powered exceeds the amount of power that the power supply can deliver. In this mode the port power is not turned on if the PD requests more power than available from the power supply.

Capacitor Detection

Controls capacitor detection for legacy PD devices.

- Disabled: This feature is disabled.
- Enabled: This feature is enabled.

Power Supply Configuration

Primary Power Supply [W]

For being able to determine the amount of power the PD may use, it must be defined what amount of power a power source can deliver.

Valid values are in the range 0 to 240 Watts.

PoE Port Configuration

Port

This is the logical port number for this row.

Ports that are not PoE-capable are grayed out and thus impossible to configure PoE for.

PoE Mode

The PoE Mode represents the PoE operating mode for the port.

- Disabled: PoE disabled for the port.
- PoE: Enables PoE IEEE 802.3af (Class 4 PDs limited to 15.4W)
- PoE+: Enables PoE+ IEEE 802.3at (Class 4 PDs limited to 30W)

Prio

The Priority represents the ports priority. There are three levels of power priority named Low, High and Critical.

The priority is used in the case where the remote device requires more power than the power supply can deliver. In this case the port with the lowest priority will be turn off starting from the port with the highest port number.

Maximum Supported Power [W]

The Maximum Power value contains a numerical value that indicates the maximum power in watts that can be delivered to a remote device.

The maximum allowed value is 30 W.

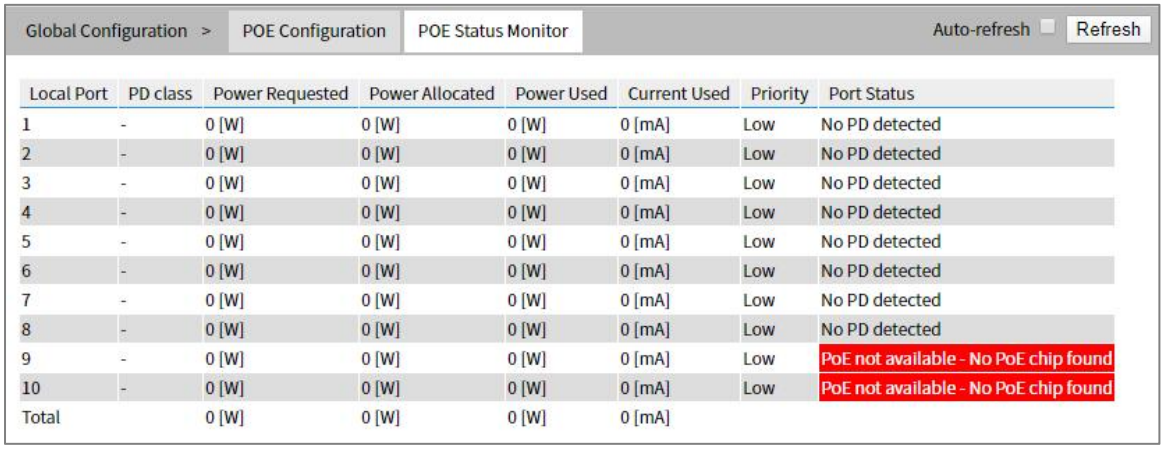
Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

8.2.3 Power Over Ethernet Status

This page allows the user to inspect the current status for all PoE ports.



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
9	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE not available - No PoE chip found
10	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE not available - No PoE chip found
Total		0 [W]	0 [W]	0 [W]	0 [mA]		

Local Port

This is the logical port number for this row.

PD Class

Each PD is classified according to a class that defines the maximum power the PD will use. The PD Class shows the five classes:

- Class 0: the maximum supported power is 15.4W.
- Class 1: the maximum supported power is 4.0W.
- Class 2: the maximum supported power is 7.0W.
- Class 3: the maximum supported power is 15.4W.
- Class 4: the maximum supported power is 30.0W.

Power Requirement

The Power Requested shows the requested amount of power the PD wants to be reserved.

Power Allocated

The Power Allocated shows the amount of power the switch has allocated for the PD.

Power Used

The Power Used shows how much power the PD currently is using.

Current Used

The Power Used shows how much current the PD currently is using.

Priority

The Priority shows the port's priority configured by the user.

Port Status

The Port Status shows the port's status. The status can be one of the following values:

- PoE not available - No PoE chip found
- PoE turned OFF - PoE disabled
- PoE turned OFF - Power budget exceeded - The total requested or used power by the PDs exceeds the maximum power the Power Supply can deliver, and port(s) with the lowest priority is/are powered down.
- No PD detected
- PoE turned OFF - PD overload - The PD has requested or used more power than the port can deliver, and is powered down.
- PoE turned OFF
- Invalid PD - PD detected, but is not working correctly.

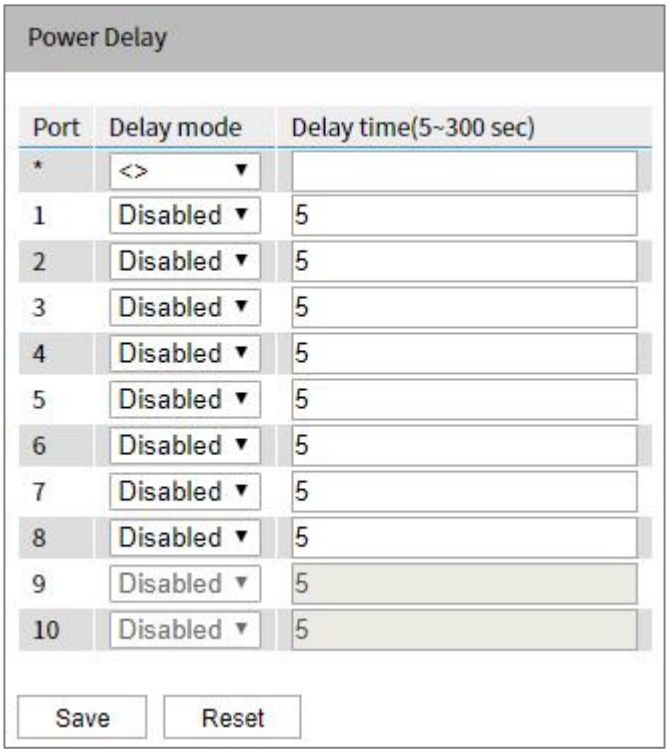
Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page.

8.3 PoE power delay

This page is used to set PoE power supply delay time, which can prevent the instant power supply shock when the device is powered on. After the device is powered on, the PoE port first waits for Delay Time, and then powers the PD.



Delay Mode

Enable Delay Mode or not, options as follows:

- Enable
- Disable

Delay time (5~300sec)

Delay power supply of PoE port.

Buttons

Save: Click to save changes.

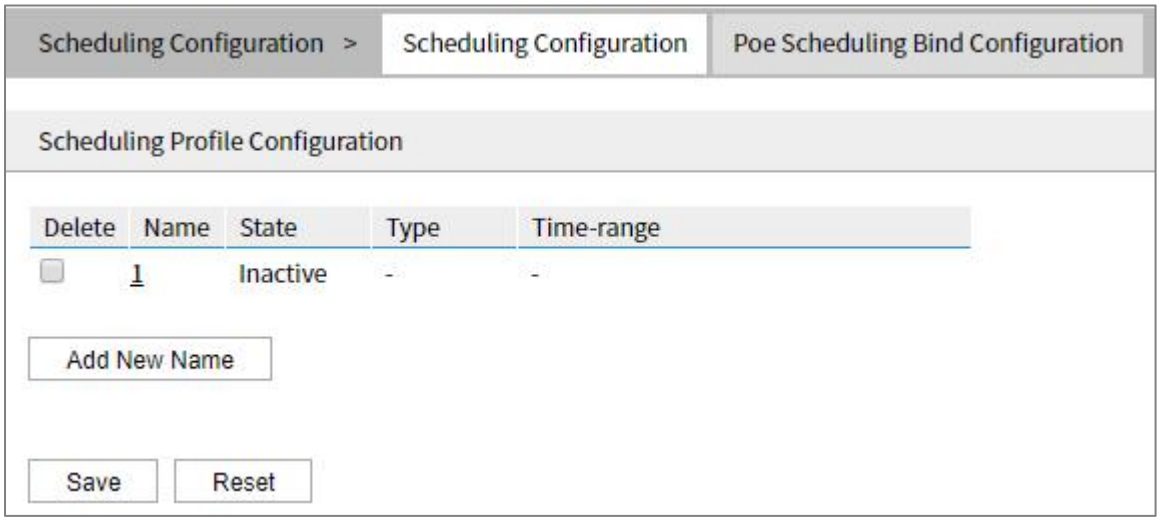
Reset: Click to undo any changes made locally and revert to previously saved values.

8.4 Policy Configuration

8.4.1 Policy Configuration

When PoE scheduling rule is valid only for a certain period of time, user can set time-based scheduling configuration. Therefore, first user can configure one or more time periods, and then reference the time periods in the rule, the rule will be valid only for the specified time period.

Users that adopt the same name can configure multiple time segments with different contents. After gain the union of each cycle time period and each absolute time period, the intersection of each union will become the final valid time range.



Delete

Delete one scheduling user record.

Name

Username. This is also a link to edit a name. Click the user name to enter the policy subset configuration page.

Status

User's current status, it could be Inactive or active.

Type

The type of scheduling policy, Periodic scheduling or Absolute scheduling.

Time-range

Plan time.

Buttons

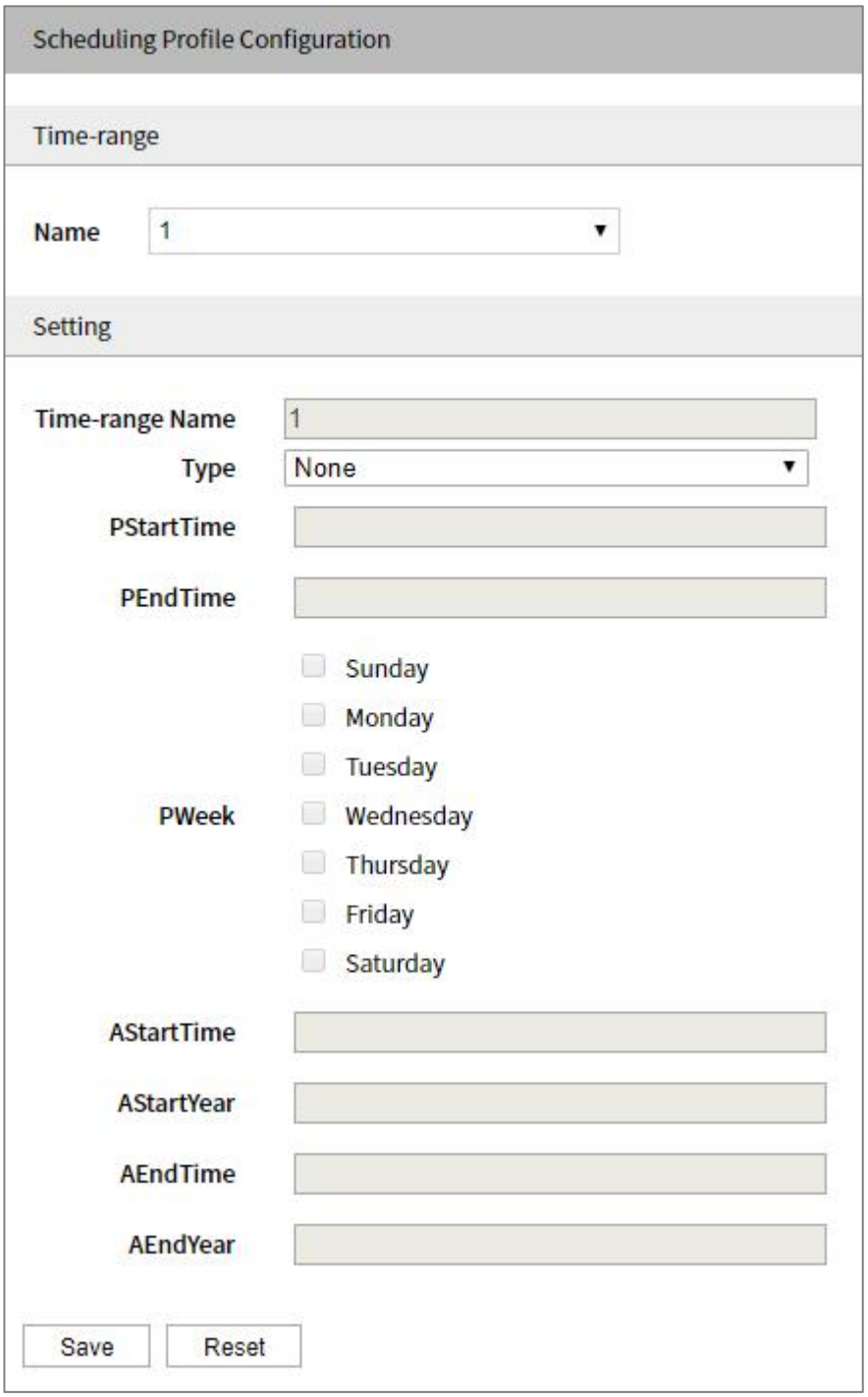
Add new name: click to add new name.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Scheduling Profile Configuration

Click the name link to enter the policy configuration page.



Policy Name

Name

Click the drop-down list of name to switch policies.

Setting

Policy Name

Display the current policy name.

Type

The type of scheduling policy, Periodic scheduling or Absolute scheduling.

PStartTime

Start time of relative time, format: HH:MM (Hour: Minute).

PEndtime

End time of relative time, format: HH:MM (Hour: Minute).

PWeek

Cycle date of relative time, take one week as a cycle.

AStartTime

Start time of absolute time, format: HH:MM (Hour: Minute).

AStartYear

Start date of absolute time, format: YYYY-MM-DD (Year-month-day).

AEndTime

End time of absolute time, format: HH:MM (Hour: Minute).

AEndYear

End date of absolute time, format: YYYY-MM- DD (Year-month-day).

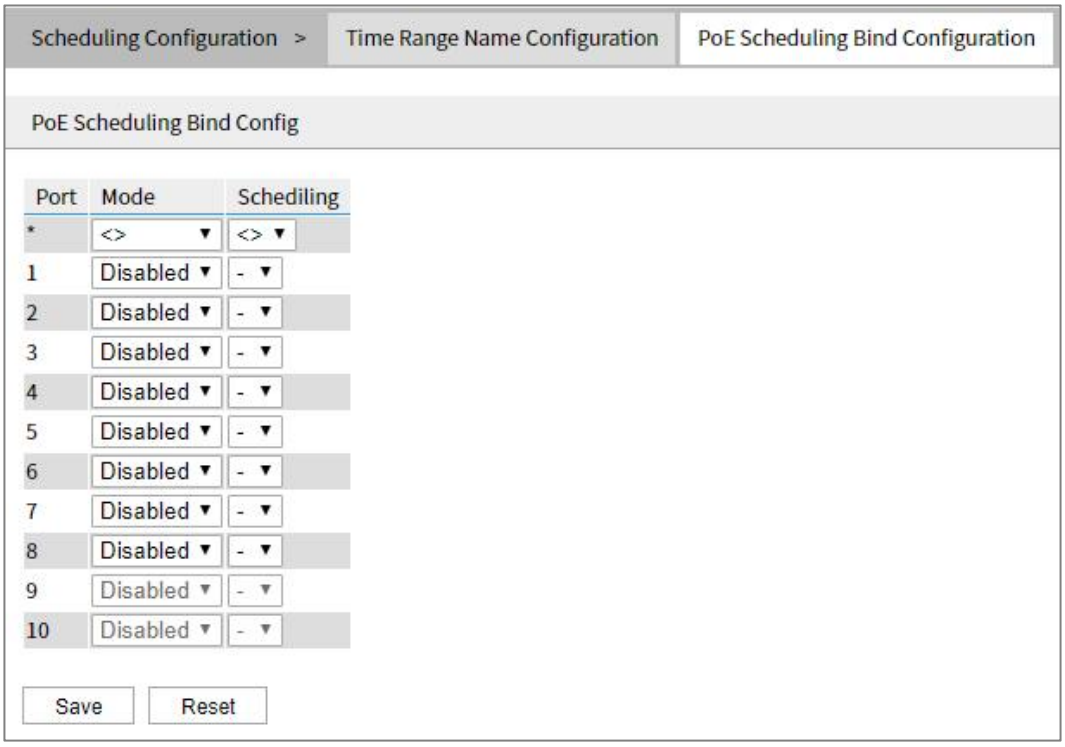
Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

8.4.2 PoE Policy Binding Configuration

This page can configure the port to bind PoE scheduling scheme.



PoE Schedualing Bind Configuration

Pattern

Enable Mode or not, options as follows:

- Disable
- Open

Policy

Select an existing scheduling scheme and bind it to the port.

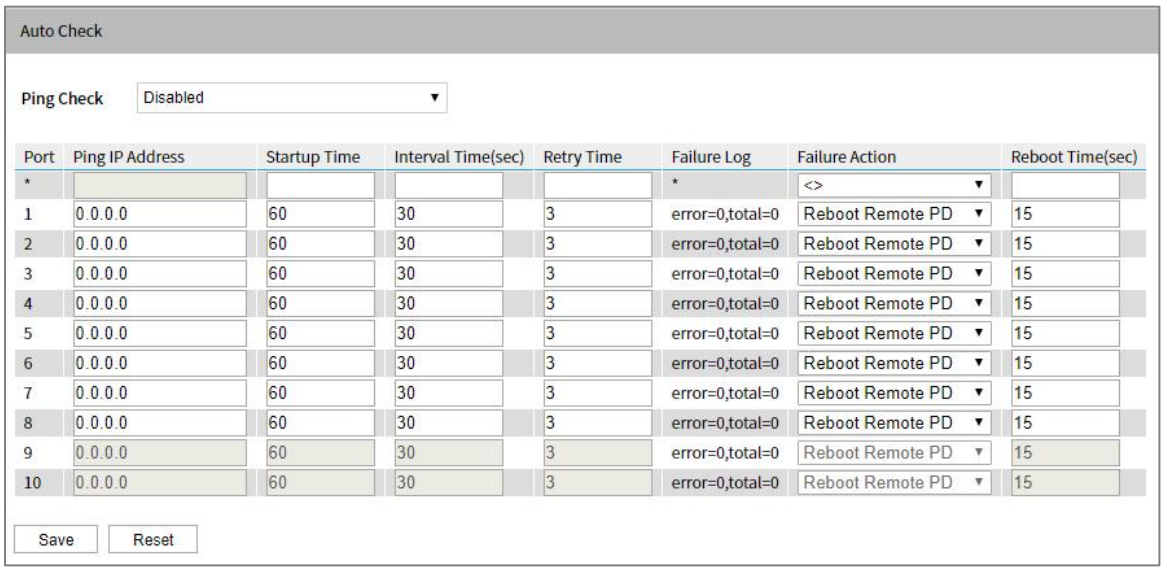
Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

8.5 Auto Check

This page can automatically monitor the PoE status of the port.



Ping Check

The global configuration of PoE port status detection switch. The options are as follows:

- Disable.
- Enable.

IP Address

Ping the IP address of the remote device.

Startup Time

Startup time (reserved, not enabled).

Test period

Test period.

The number of retries

Retry times.

Failure Log

Failure log.

Failure Action

Troubleshooting.

- Ignore.
- Restart the remote PD.

Reboot delay

Reboot delay.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

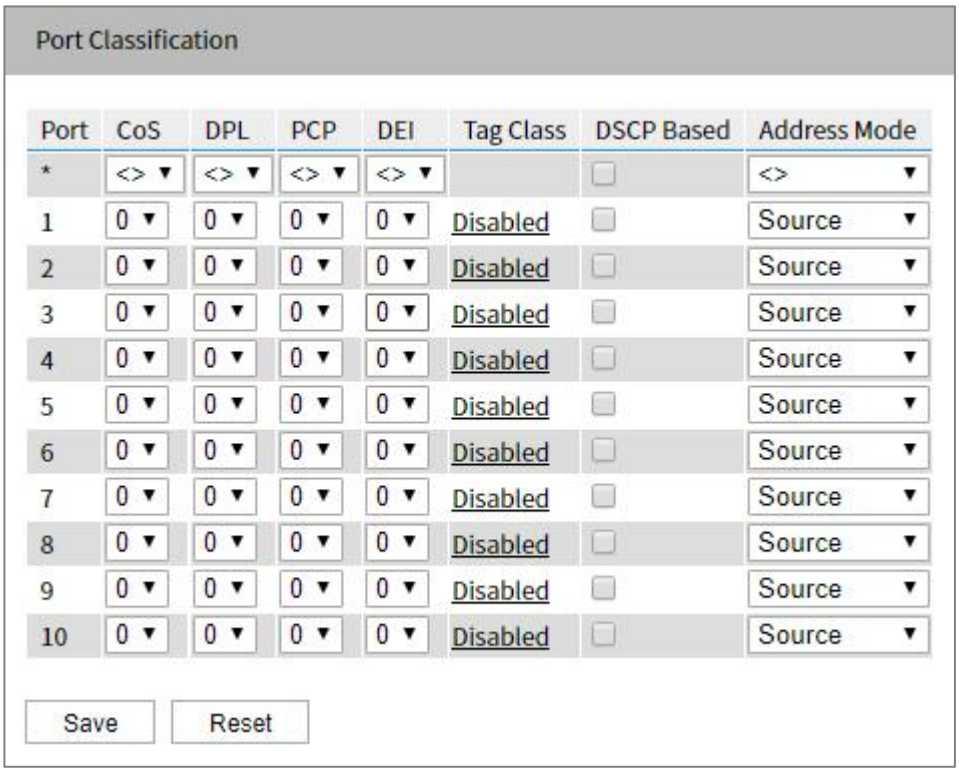
9 Service Quality

QoS (Quality of Service) provides end-to-end service quality guarantee based on the requirements of different services. By configuring QoS, the network traffic can be regulated, network congestion can be avoided and managed, and the loss rate of messages can be reduced. At the same time, it can also provide dedicated bandwidth for users or provide differential services for different services (voice, video, data, etc.).

9.1 Port Classification

This page allows you to configure the basic QoS Ingress Classification settings for all switch ports.

The displayed settings are:



Port

The port number for which the configuration below applies.

CoS

Controls the default class of service.

All frames are classified to a CoS. There is a one to one mapping between CoS, queue and priority. A CoS of 0 (zero) has the lowest priority.

If the port is VLAN aware, the frame is tagged and Tag Class. is enabled, then the frame is classified to a CoS that is mapped from the PCP and DEI value in the tag. Otherwise the frame is classified to the default CoS.

The classified CoS can be overruled by a QCL entry.

Note:

If the default CoS has been dynamically changed, then the actual default CoS is shown in parentheses after the configured default CoS.

DPL

Controls the default drop precedence level.

All frames are classified to a drop precedence level.

If the port is VLAN aware, the frame is tagged and Tag Class. is enabled, then the frame is classified to a DPL that is mapped from the PCP and DEI value in the tag. Otherwise the frame is classified to the default DPL.

The classified DPL can be overruled by a QCL entry.

PCP

Controls the default PCP value.

All frames are classified to a PCP value.

If the port is VLAN aware and the frame is tagged, then the frame is classified to the PCP value in the tag. Otherwise the frame is classified to the default PCP value.

DEI

Controls the default DEI value.

All frames are classified to a DEI value.

If the port is VLAN aware and the frame is tagged, then the frame is classified to the DEI value in the tag. Otherwise the frame is classified to the default DEI value.

Tag Classification

Display the classification mode of label frames on this port. Display the label classification of tagged frames on this port.

- Disabled: Use default CoS and DPL for tagged frames.
- Enabled: Use mapped versions of PCP and DEI for tagged frames.

Click on the mode in order to configure the mode and/or mapping.

Note:

This setting has no effect if the port can't identify VLAN. Tagged frames received on VLAN unaware ports are always classified to the default CoS and DPL.

DSCP-based Classification

Click to Enable DSCP Based QoS Ingress Port Classification.

Address Mode

The IP/MAC address mode specifying whether the QCL classification must be based on source (SMAC/SIP) or destination (DMAC/DIP) addresses on this port. The allowed values are:

- Source: Enable SMAC/SIP matching.
- Destination: Enable DMAC/DIP matching.

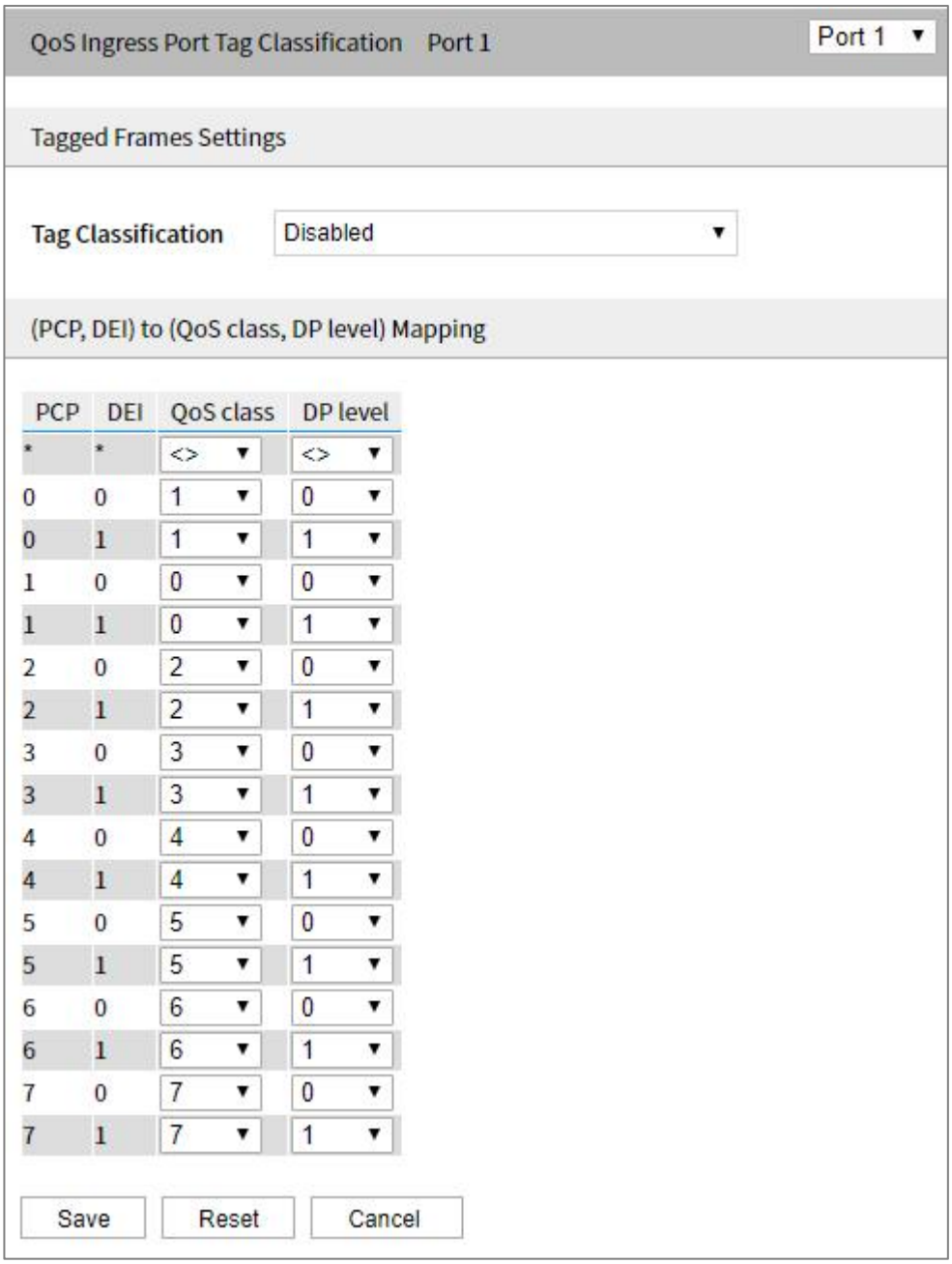
Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

QoS Ingress Port Tag Classification

On the port classification page, click the "Label Classification" link to enter the "QoS egress port label classification" page. The classification mode for tagged frames are configured on this page.



Tag Frame Settings

Tag Classification

Controls the classification mode for tagged frames on this port.

- Disabled: Use default QoS class and Drop Precedence Level for tagged frames.
- Enabled: Use mapped versions of PCP and DEI for tagged frames.

(PCP, DEI) to (QoS Level, DP Level) Mapping

When “Label Classification” is set to “Enabled”, the mapping of classification (PCP, DEI) to (QoS Level, DP Level) value is controlled.

PCP

Display the value of PCP (Priority Code Point).

DEI

Display the value of DEI (Drop Eligible Indicator).

QoS Class

The drop-down list of QoS level, with optional values of 0-7. QoS level mapped by PCP value and DEI value.

DP Level

The drop-down list of DP level, with optional values of 0-1. DP level mapped by PCP value and DEI value.

Buttons

Save: Click to save changes.

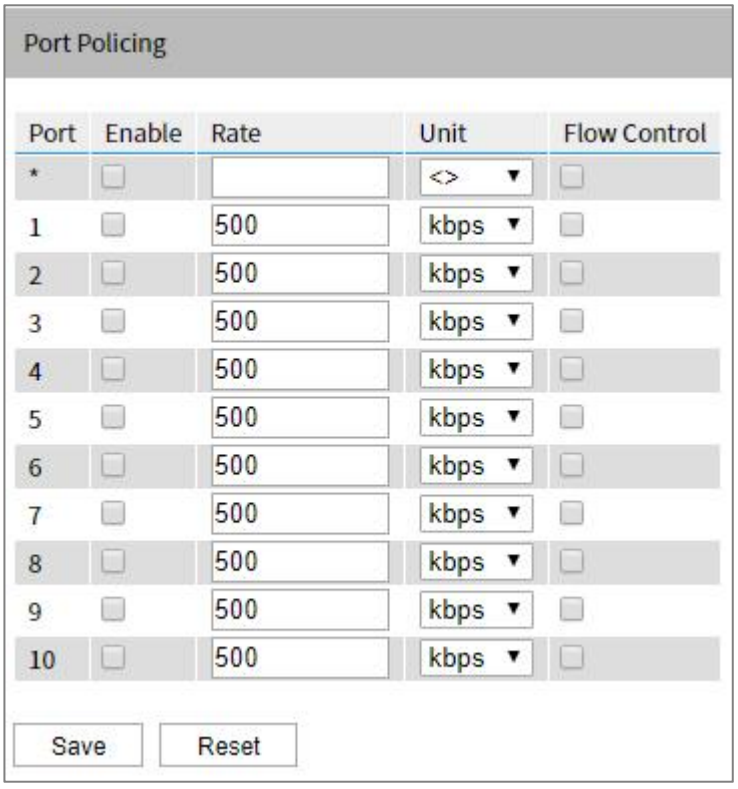
Reset: Click to undo any changes made locally and revert to previously saved values.

Return: Click to undo any changes made locally and return to the previous page.

9.2 Ingress Policy

This page allows you to configure the Policer settings for all switch ports.

The displayed settings are:



Port

The port number for which the configuration below applies.

Enable

Enable or disable the port policer for this switch port.

Rate

Controls the rate for the port policer. This value is restricted to 100-3276700 when "Unit" is kbps or fps, and 1-3276 when "Unit" is Mbps or kfps. The rate is internally rounded up to the nearest value supported by the port policer.

Unit

Controls the unit of measure for the port policer rate as kbps, Mbps, fps or kfps.

Flow Control

If flow control is enabled and the port is in flow control mode, then pause frames are sent instead of discarding frames.

Buttons

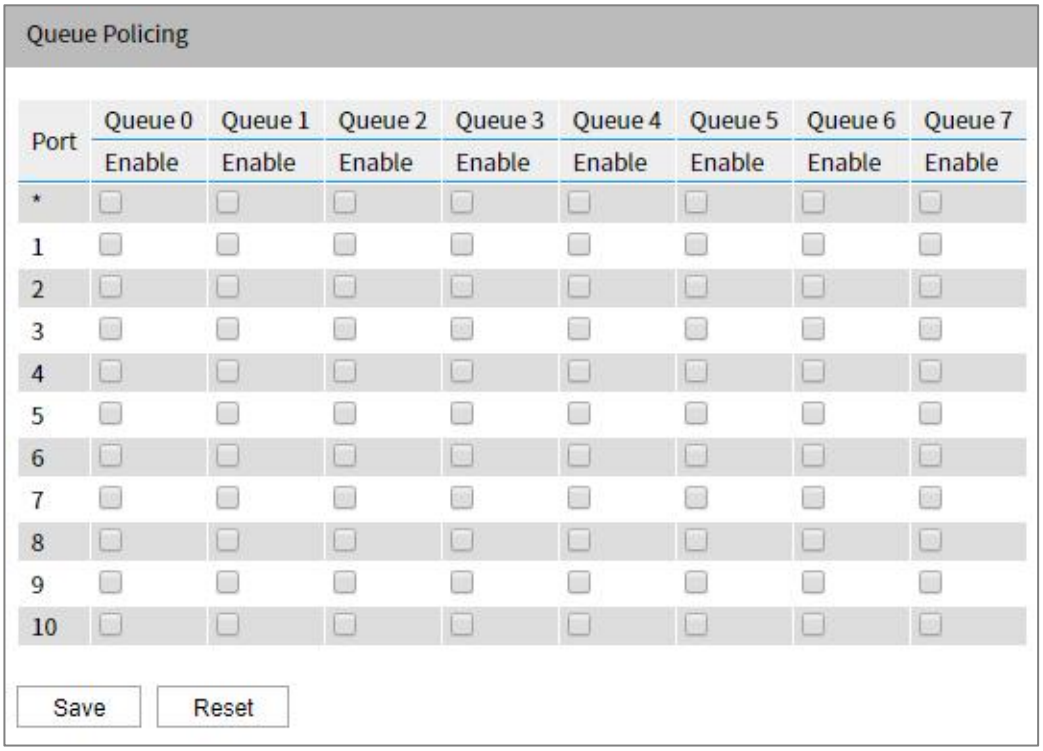
Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

9.3 Queue Strategy

This page allows you to configure the Queue Policer settings for all switch ports.

The displayed settings are:



Port

The port number for which the configuration below applies.

Enable

Enable or disable the queue policer for this switch port. When the check box is checked, the "Rate" and "Unit" configuration items will appear.

Rate

Controls the rate for the queue policer. This value is restricted to 100-3276700 when "Unit" is kbps, and 1-3276 when "Unit" is Mbps. The rate is internally rounded up to the nearest value supported by the queue policer.

This field is only shown if at least one of the queue policers are enabled.

Unit

Controls the unit of measure for the queue policer rate as kbps or Mbps.

This field is only shown if at least one of the queue policers are enabled.

Buttons

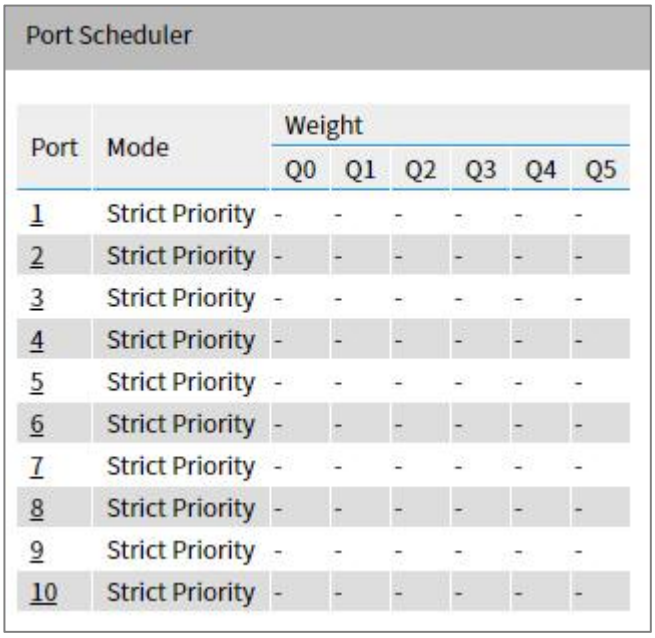
Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

9.4 Egress Scheduling

This page provides an overview of QoS Egress Port Schedulers for all switch ports.

The displayed settings are:



Port Scheduler

Port	Mode	Weight					
		Q0	Q1	Q2	Q3	Q4	Q5
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	-	-	-	-	-	-

Port

The switch port number.

Click on the port number in order to configure the schedulers.

Mode

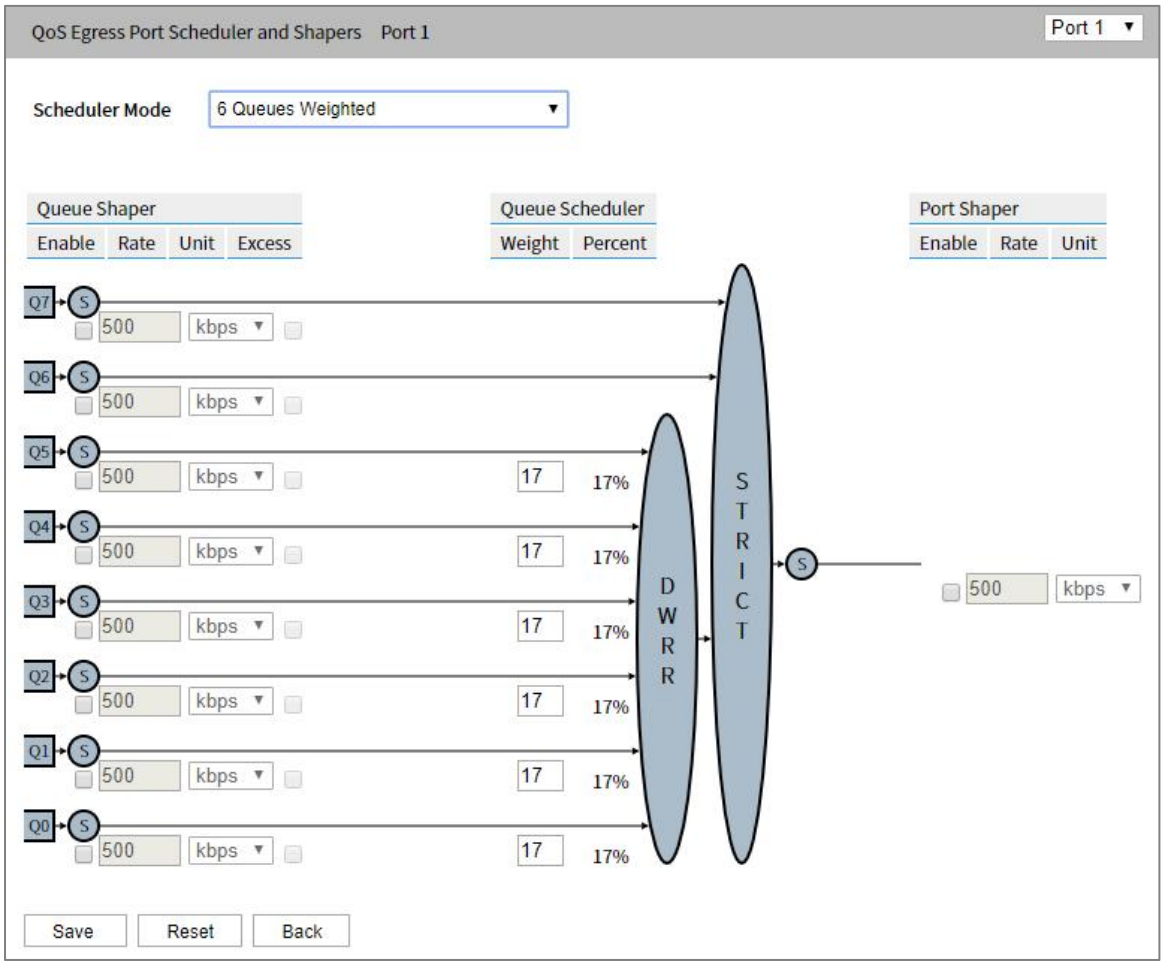
Shows the scheduling mode for this port.

Qn

Shows the weight for this queue and port.

QoS Egress Port Scheduler and Shapers

Click the port link to enter the “QoS egress port scheduling and shaping” page. This page allows you to configure the Scheduler and Shapers for a specific port. The settings relate to the currently selected stack unit.



The displayed settings are:

Scheduler Mode

Controls how many of the queues are scheduled as strict and how many are scheduled as weighted on this switch port.

- Strict Priority.
- 6 Queues Weighted.

Queue Shaper

- Enable: Controls whether the queue shaper is enabled for this queue on this switch port. Ports in Basic or Hierarchical Scheduling Mode (HQoS setting) only have queue shapers on queue 6 and 7.
- Rate: Controls the rate for the queue shaper. This value is restricted to 100-3281943 when "Unit" is kbps, and 1-3281 when "Unit" is Mbps. Ports in Basic or Hierarchical Scheduling Mode (HQoS setting) only have queue shapers on queue 6 and 7. The rate is internally rounded up to the nearest value supported by the queue shaper.
- Unit: Controls the unit of measure for the queue policer rate as kbps or Mbps. Ports in Basic or Hierarchical Scheduling Mode (HQoS setting) only have queue

shapers on queue 6 and 7.

- Excess: Controls whether the queue is allowed to use excess bandwidth. Not shown for ports in Basic or Hierarchical Scheduling Mode (HQoS setting).

Queue Scheduler

When the “Scheduler Mode” is "6 queue weight", the queue scheduling parameters are displayed.

- Weight: Controls the weight for this queue. This value is restricted to 1-100. This parameter is only shown if "Scheduler Mode" is set to "6 Queues Weighted".
- Percent: Shows the weight in percent for this queue. This parameter is only shown if "Scheduler Mode" is set to "6 Queues Weighted".

Port Shaper

- Enable: Controls whether the port shaper is enabled for this switch port. Only shown for Non-service configuration.
- Rate: Controls the rate for the port shaper. This value is restricted to 100-3281943 when "Unit" is kbps, and 1-3281 when "Unit" is Mbps. Only shown for Non-service configuration. The rate is internally rounded up to the nearest value supported by the port shaper.
- Unit: Controls the unit of measure for the port shaper rate as kbps or Mbps. Only shown for Non-service configuration.

Buttons

Save: Click to save changes.

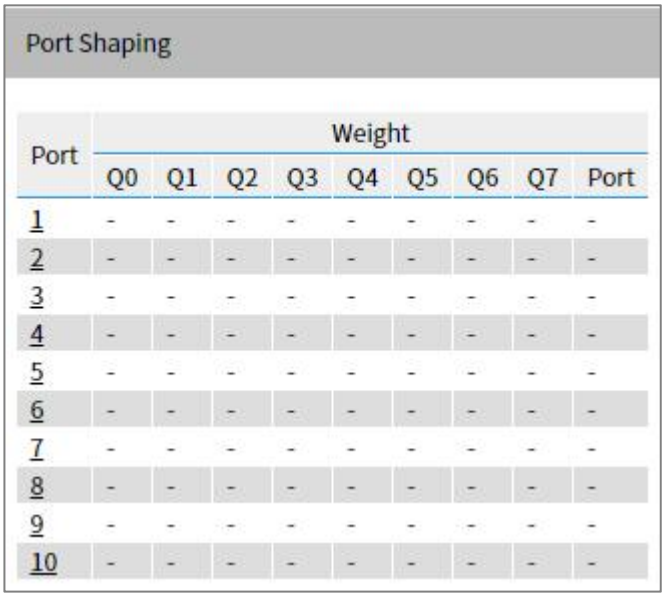
Cancel: Click to undo any changes made locally and revert to previously saved values.

Return: Click to undo any changes made locally and return to the previous page.

9.5 Egress Shaping

This page provides an overview of QoS Egress Port Shapers for all switch ports.

The displayed settings are:



Port

The switch port number.

Click on the port number in order to configure the shapers.

Qn

- Q0-Q7: Shows "-" for disabled or actual queue shaper rate - e.g. "800 Mbps".
- Port: Shows "-" for disabled or actual port shaper rate - e.g. "800 Mbps".

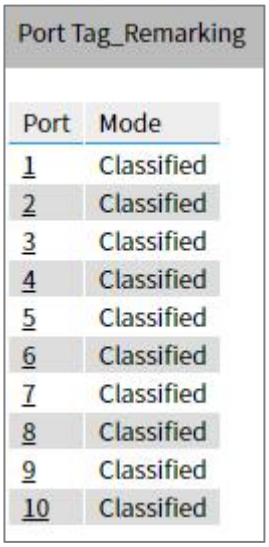
QoS Egress Port Scheduler and Shapers

Click the port link to enter the “QoS egress port scheduling and shaping” page. See "QoS egress port scheduling and shaping" page in the previous section for details.

9.6 Egress Relabeling

This page provides an overview of QoS Egress Port Tag Remarking for all switch ports.

The displayed settings are:



Port

The switch port number.

Click on the port number in order to configure tag remarking.

Mode

Shows the tag remarking mode for this port.

- Classified: Use classified PCP/DEI values.
- Default: Use default PCP/DEI values.
- Mapped: Use mapped versions of QoS class and DP level.

QoS Egress Port Tag Remarking

Click the port link to enter the "QoS egress port retag" page. The QoS Egress Port Tag Remarking for a specific port are configured on this page.

Pattern

Controls the tag remarking mode for this port.

- Classified: Use classified PCP/DEI values.
- Default: Use default PCP/DEI values.
- Mapped: Use mapped versions of QoS class and DP level. PCP/DEI Configuration Controls the default PCP and DEI values used when the mode is set to Default. (QoS class, DP level) to (PCP, DEI) Mapping controls the mapping

of the classified (QoS class, DP level) to (PCP, DEI) values when the mode is set to Mapped.

Buttons

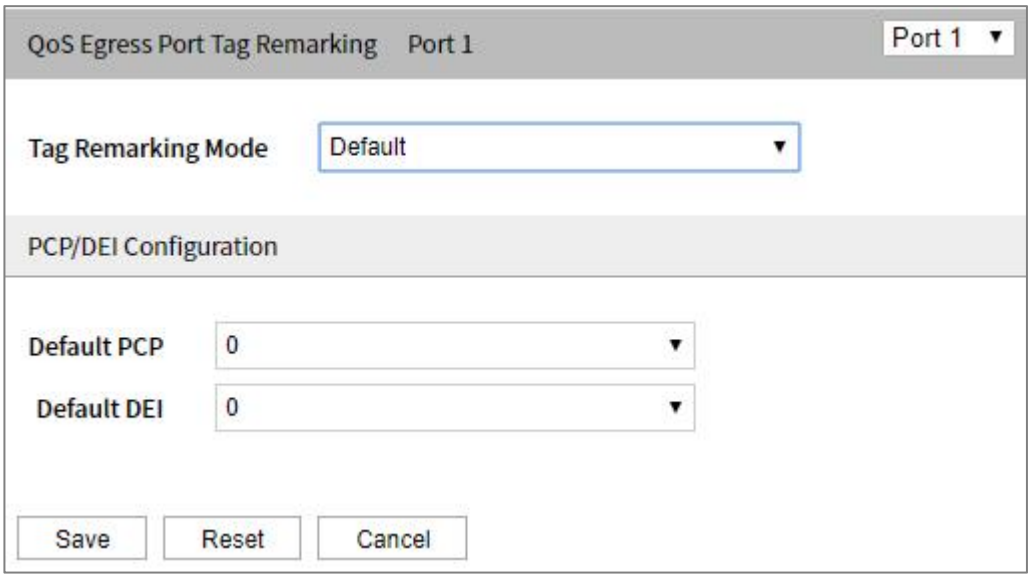
Save: Click to save changes.

Cancel: Click to undo any changes made locally and revert to previously saved values.

Return: Click to undo any changes made locally and return to the previous page.

PCP/DEI Configuration

When "Mode" is "Default", PCP/DEI configuration information is displayed.



Default PCP

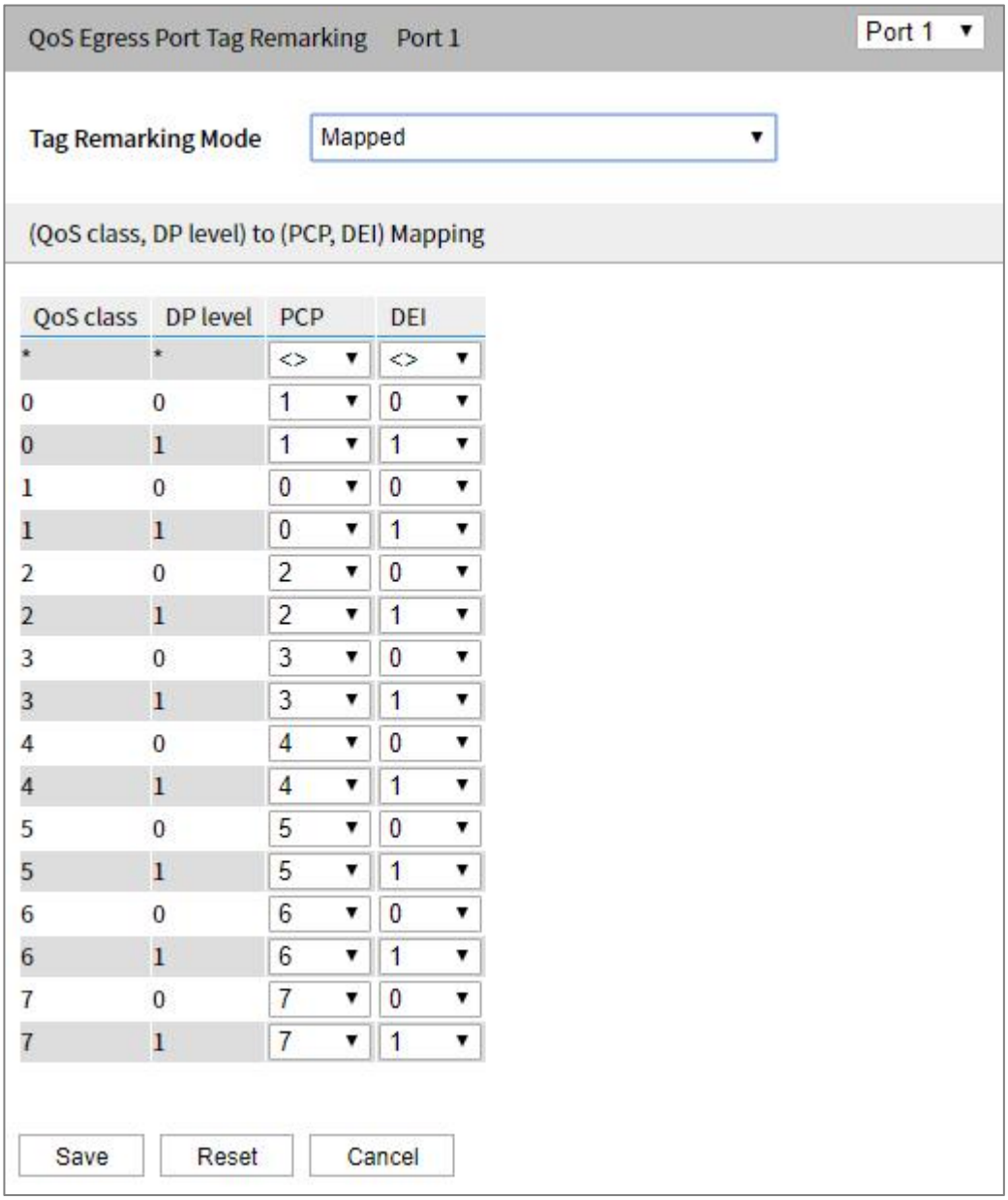
The drop-down list of PCP value, with optional value range 0-7.

Default DEI

The drop-down list of DEI value, with optional value range 0-1.

(QoS Class, DP level) to (PCP, DEI) Mapping

When "Mode" is "Mapping", the (QoS Class, DP level) to (PCP, DEI) mapping information will display.



QoS Class

Display the QoS class.

DP Level

Display the DP level.

PCP

The drop-down list of PCP (Priority Code Point), with optional values of 0-7. PCP value mapped by QoS class and DP level.

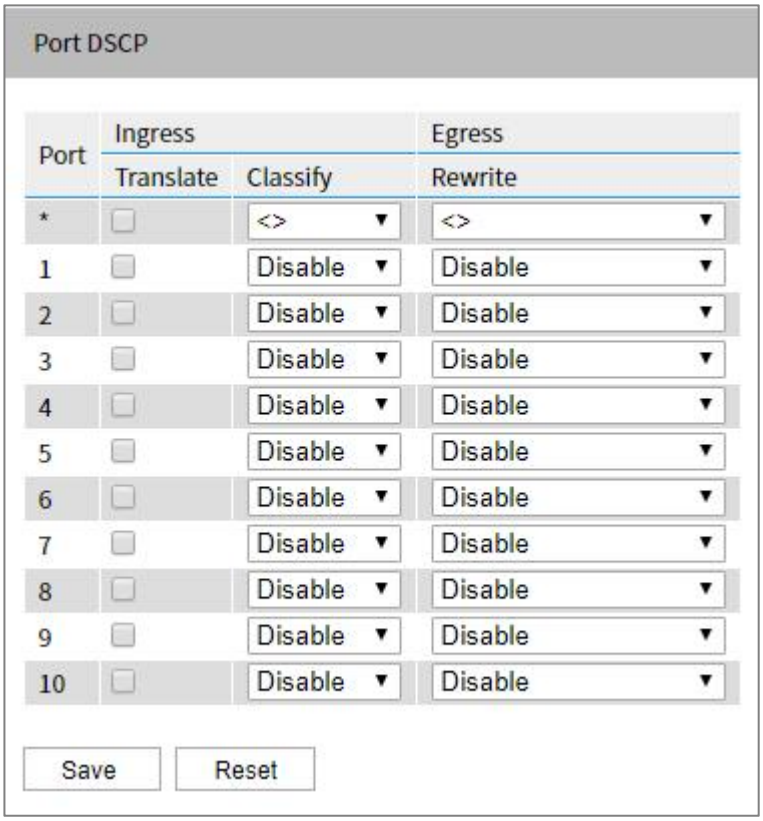
DEI

The drop-down list of DEI (Drop Eligible Indicator), with optional values of 0-1. DEI value mapped by QoS class and DP level.

9.7 Port DSCP

This page allows you to configure the basic QoS Port DSCP Configuration settings for all switch ports.

The displayed settings are:



Port

The Port column shows the list of ports for which you can configure DSCP ingress and egress settings.

Ingress

In Ingress settings you can change ingress translation and classification settings for individual ports.

There are two configuration parameters available in Ingress:

- Translate: To Enable the Ingress Translation click the checkbox.
- Classify: Classification for a port have 4 different values.
  - Disable: no ingress DSCP Classification.
  - DSCP=0: Classify if incoming (or translated if enabled) DSCP is 0.
  - Selected: Classify only selected DSCP for which classification is enabled as specified in DSCP Translation window for the specific DSCP.
  - All: all DSCP are classified.

Egress

Port Egress Rewriting can be one of:

- Disabled: no egress rewrite.
- Enable: enable rewrite without remapping.
- Remap DP Unaware: DSCP from analyzer is remapped and frame is remarked with remapped DSCP value. The remapped DSCP value is always taken from the “DSCP Conversion > Egress Remap DP0” table.
- Remap DP Aware: DSCP from analyzer is remapped and frame is remarked with remapped DSCP value. According to the DP level of the frame, the remapped DSCP value can be obtained from either the “DSCP Conversion > Egress Remap DP0” table or the “DSCP Conversion > Egress Remap DP1” table.

Buttons

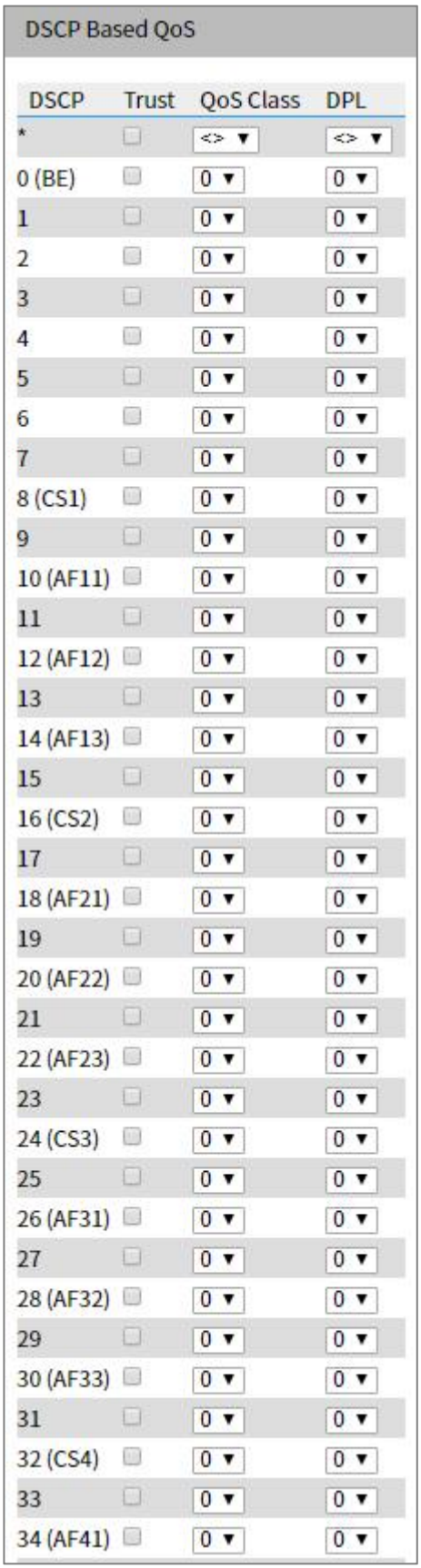
Save: Click to save changes.

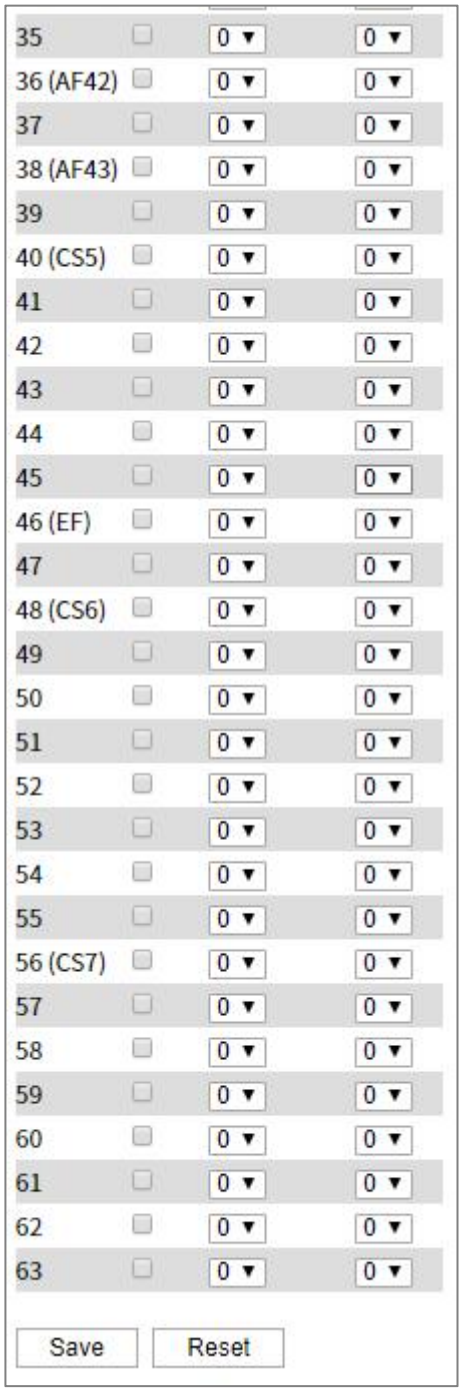
Reset: Click to undo any changes made locally and revert to previously saved values.

9.8 DSCP-based QoS

This page allows you to configure basic QoS DSCP ingress classification settings based on QoS DSCP for all switches.

The displayed settings are:


DSCP Based QoS
DSCP
Trust
QoS Class
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
32 (CS4)
0
0
33
0
0
34 (AF41)
0
0



DSCP

Maximum number of supported DSCP values are 64.

Trust

Controls whether a specific DSCP value is trusted. Only frames with trusted DSCP values are mapped to a specific QoS class and Drop Precedence Level. Frames with untrusted DSCP values are treated as a non-IP frame.

QoS Class

QoS class value can be any of (0-7).

DPL

Drop Precedence Level (0-1).

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

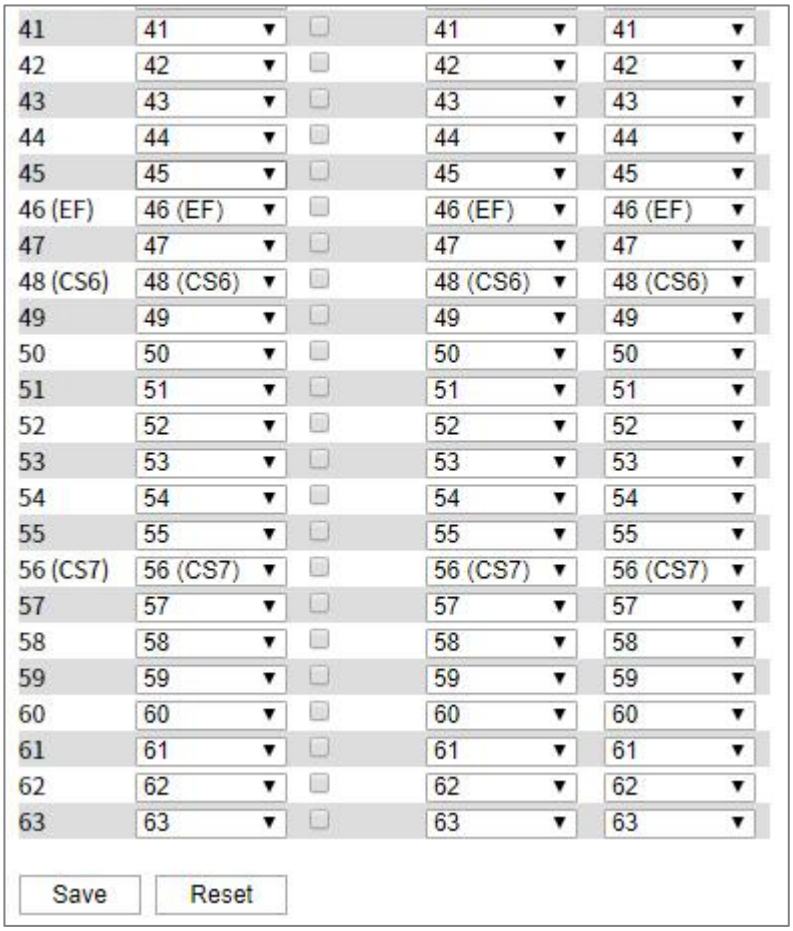
9.9 DSCP Conversion

This page allows you to configure the basic QoS DSCP Translation settings for all switches. DSCP translation can be done in Ingress or Egress.

The displayed settings are:

DSCP Translation

DSCP	Ingress		Egress	
	Translate	Classify	Remap DP0	Remap DP1
*	<>		<>	<>
0 (BE)	0 (BE)		0 (BE)	0 (BE)
1	1		1	1
2	2		2	2
3	3		3	3
4	4		4	4
5	5		5	5
6	6		6	6
7	7		7	7
8 (CS1)	8 (CS1)		8 (CS1)	8 (CS1)
9	9		9	9
10 (AF11)	10 (AF11)		10 (AF11)	10 (AF11)
11	11		11	11
12 (AF12)	12 (AF12)		12 (AF12)	12 (AF12)
13	13		13	13
14 (AF13)	14 (AF13)		14 (AF13)	14 (AF13)
15	15		15	15
16 (CS2)	16 (CS2)		16 (CS2)	16 (CS2)
17	17		17	17
18 (AF21)	18 (AF21)		18 (AF21)	18 (AF21)
19	19		19	19
20 (AF22)	20 (AF22)		20 (AF22)	20 (AF22)
21	21		21	21
22 (AF23)	22 (AF23)		22 (AF23)	22 (AF23)
23	23		23	23
24 (CS3)	24 (CS3)		24 (CS3)	24 (CS3)
25	25		25	25
26 (AF31)	26 (AF31)		26 (AF31)	26 (AF31)
27	27		27	27
28 (AF32)	28 (AF32)		28 (AF32)	28 (AF32)
29	29		29	29
30 (AF33)	30 (AF33)		30 (AF33)	30 (AF33)
31	31		31	31
32 (CS4)	32 (CS4)		32 (CS4)	32 (CS4)
33	33		33	33
34 (AF41)	34 (AF41)		34 (AF41)	34 (AF41)
35	35		35	35
36 (AF42)	36 (AF42)		36 (AF42)	36 (AF42)
37	37		37	37
38 (AF43)	38 (AF43)		38 (AF43)	38 (AF43)
39	39		39	39
40 (CS5)	40 (CS5)		40 (CS5)	40 (CS5)



DSCP

Maximum number of supported DSCP values are 64 and valid DSCP value ranges from 0 to 63.

Ingress

Before using DSCP to realize QoS class and DPL mapping, the DSCP at the entrance can be converted into a new DSCP.

There are two configuration parameters for DSCP mapping:

- Translate: DSCP at Ingress side can be translated to any of (0-63) DSCP values.
- Classify: Click to enable Classification at Ingress side.

Egress

There are the following configurable parameters for Egress side:

- Remap DP0: Controls the remapping for frames with DP level 0. Select the DSCP value from select menu to which you want to remap. DSCP value ranges from 0 to 63.
- Remap DP1: Controls the remapping for frames with DP level 1. Select the DSCP value from select menu to which you want to remap. DSCP value ranges from 0 to 63.

Buttons

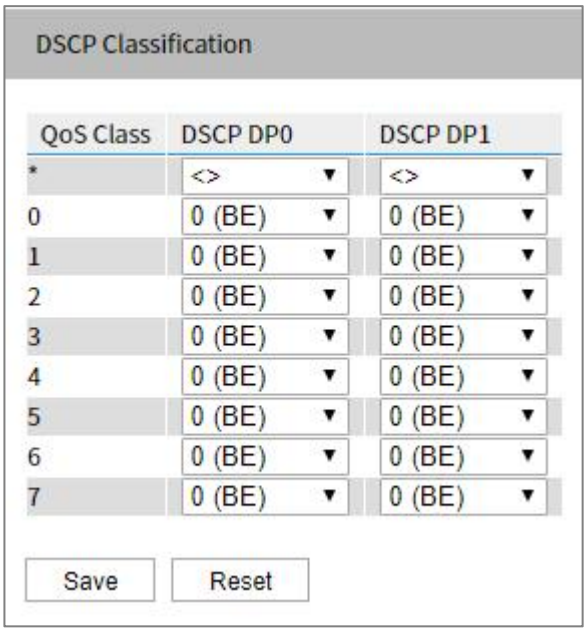
Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

9.10 DSCP Classification

This page allows you to configure the mapping of QoS class and Drop Precedence Level to DSCP value.

The displayed settings are:



QoS Class

Actual QoS class.

DSCP DP0

Select the classified DSCP value (0-63) for Drop Precedence Level 0.

DSCP DP1

Select the classified DSCP value (0-63) for Drop Precedence Level 1.

Buttons

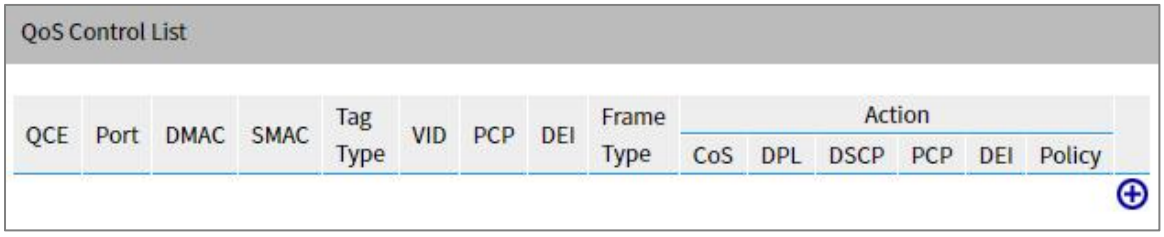
Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

9.11 QoS Control List

This page shows the QoS Control List(QCL), which is made up of the QCEs. Each row describes a QCE that is defined. The maximum number of QCEs is 256 on each switch.

Click on the lowest plus sign to add a new QCE to the list.



QCE

Indicates the QCE id.

Port

Indicates the list of ports configured with the QCE or 'Any'.

DMAC

Indicates the destination MAC address. The possible values are:

- Any: Match any DMAC.
- Unicast: Match unicast DMAC.
- Multicast: Match multicast DMAC.
- Broadcast: Match broadcast DMAC.

The default value is 'Any'.

SMAC

Match specific source MAC address or 'Any'.

If a port is configured to match on destination addresses, this field indicates the DMAC.

Tag Type

Indicates tag type. The possible values are:

- Any: Match tagged and untagged frames.
- Untagged: Match untagged frames.
- Tagged: Match tagged frames.

The default value is 'Any'.

VID

Indicates (VLAN ID), either a specific VID or range of VIDs. VID can be in the range 1-4095 or 'Any'

PCP

Priority Code Point： Valid values of PCP are specific (0, 1, 2, 3, 4, 5, 6, 7) or range (0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'.

DEI

Drop Eligible Indicator: Valid value of DEI are 0, 1 or 'Any'.

Frame Type

Indicates the type of frame. The possible values are:

- Any: Match any frame type.
- Ethernet: Match EtherType frames.
- LLC: Match (LLC) frames.
- SNAP: Match (SNAP) frames.
- IPv4: Match IPv4 frames.
- IPv6: Match IPv6 frames.

Action

Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content.

Possible actions are:

- CoS: Classify Class of Service.
- DPL: Classify Drop Precedence Level.
- DSCP: Classify DSCP value.
- PCP: Classify PCP value.
- DEI: Classify DEI value.
- Policy: Classify ACL Policy number.

Buttons

You can modify each QCE (QoS Control Entry) in the table using the following buttons:

：Insert a new QCE before the current row.

：Edit QCE.

: move QCE entry up.

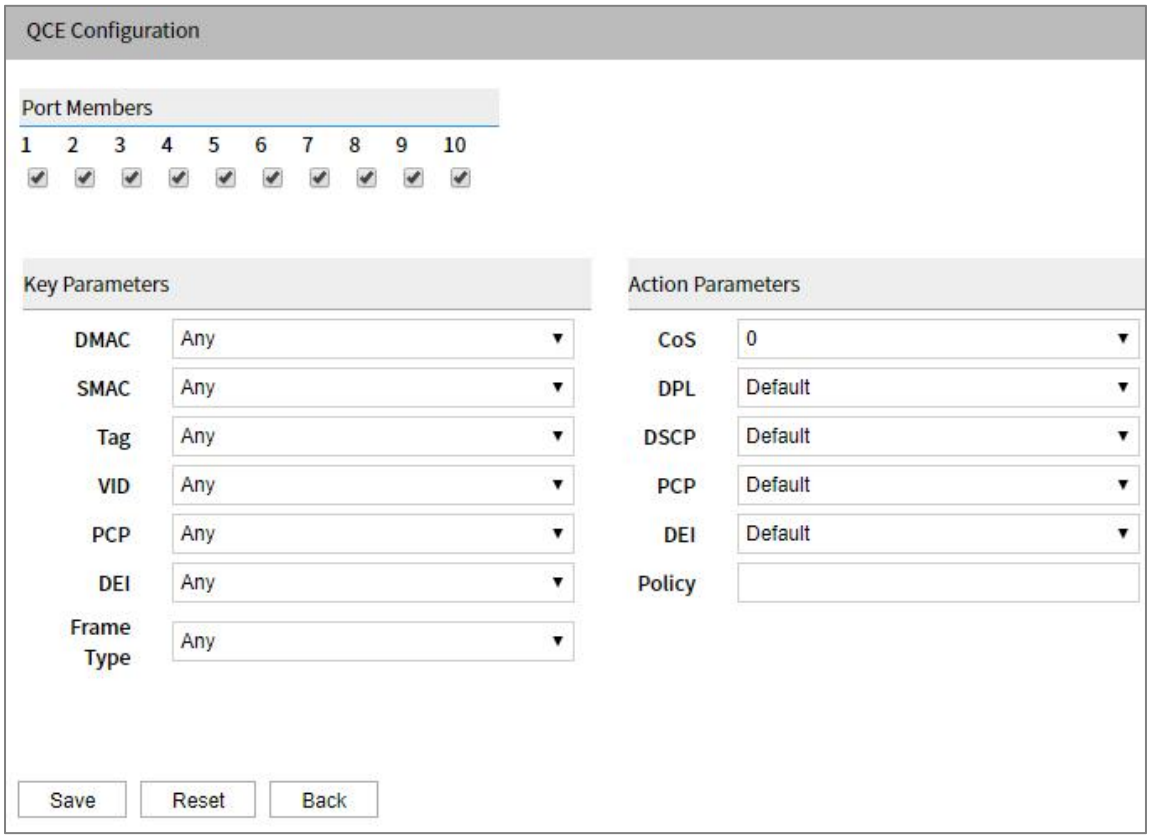
: move QCE entry down.

: delete QCE.

: add new QCE entries at the bottom of the QCE list.

QCE Configuration

Click “⊕” to add a new QCE entry. This page allows to edit|insert a single QoS Control Entry at a time. A QCE consists of several parameters. These parameters vary according to the frame type that you select.



Port Members

Check the checkbox button to include the port in the QCL entry. By default all ports are included.

Key Parameters

Key configuration is described as below:

- DMAC: the destination MAC address can be "Unicast", "Multicast", "Broadcast" or "Any".
- SMAC: Source MAC address: xx-xx-xx-xx-xx-xx or 'Any'. If a port is configured to match on DMAC/DIP, this field is the Destination MAC address.
- Tag: Value of Tag field can be 'Untagged', 'Tagged', 'C-Tagged', 'S-Tagged' or 'Any'.
- VID: Valid value of VLAN ID can be any value in the range 1-4095 or 'Any'; user can enter either a specific value or a range of VIDs.
- PCP: Valid value PCP are specific (0, 1, 2, 3, 4, 5, 6, 7) or range (0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'.

- DEI: Valid value of DEI can be '0', '1' or 'Any'.
- Frame Type: Frame Type can have any of the following values:
  - Any
  - EtherType
  - LLC
  - SNAP
  - IPv4
  - IPv6

These parameters vary according to the frame type that you select. The configuration parameters involved in all frame types will be explained below.

Frame Type	Interface Parameters	Note
Any	—	Allow all types of frames.
EtherType	EtherType	Valid Ether Type can be 0x600-0xFFFF excluding 0x800(IPv4) and 0x86DD(IPv6) or 'Any'.
LLC	DSAP Address	Valid DSAP(Destination Service Access Point) can vary from 0x00 to 0xFF or 'Any'.
	SSAP Address	Valid SSAP(Source Service Access Point) can vary from 0x00 to 0xFF or 'Any'.
	Control	Valid Control field can vary from 0x00 to 0xFF or 'Any'.
SNAP	PID	Valid PID(a.k.a Ether Type) can be 0x0000-0xFFFF or 'Any'.
IPv4	Protocol	IP Protocol (0-255, 'TCP' or 'UDP') or 'Any'.
	SIP	Specific Source IP address in value/mask format or 'Any'. IP and Mask are in the format x.y.z.w where x, y, z, and w are decimal numbers between 0 and 255. When Mask is converted to a 32-bit binary string and read from left to right, all bits following the first zero must also be zero. If a port is configured to match on DMAC/DIP, this field is the Destination IP address.
	IP Fragment	IPv4 frame segment options: “Yes”, “No”, or “Any”.
	DSCP	Diffserv Code Point value (DSCP). It can be a specific value, range of values or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or

Frame Type	Interface Parameters	Note
		AF11-AF43.
	Sport	Source TCP/UDP port (0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.
	Dport	Destination TCP/UDP port (0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.
IPv6	Protocol	IP Protocol (0-255, 'TCP' or 'UDP') or 'Any'.
	SIP	Source IP 32 LS bits of IPv6 source address in value/mask format or 'Any'. If a port is configured to match on DMAC/DIP, this field is the Destination IP address.
	DSCP	Diffserv Code Point value (DSCP). It can be a specific value, range of values or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43.
	Sport	Source TCP/UDP port (0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.
	Dport	Destination TCP/UDP port (0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.

Action Parameters

- CoS: classification of service (0-7) or "Default".
- DP: discard priority (0-1) or "Default".
- DSCP: (0-63, BE, CS1-CS7, EF or AF11-AF43) or 'Default'.
- PCP: (0-7) or 'Default'.

  Note:
  PCP and DEI cannot be set individually.
- DEI: (0-1) or 'Default'.
- Policy: ACL policy number (0-255) or "Default" (empty field).

'Default' means that the default classified value is not modified by this QCE.

Buttons

Save: Click to save the configuration and move to main QCL page.

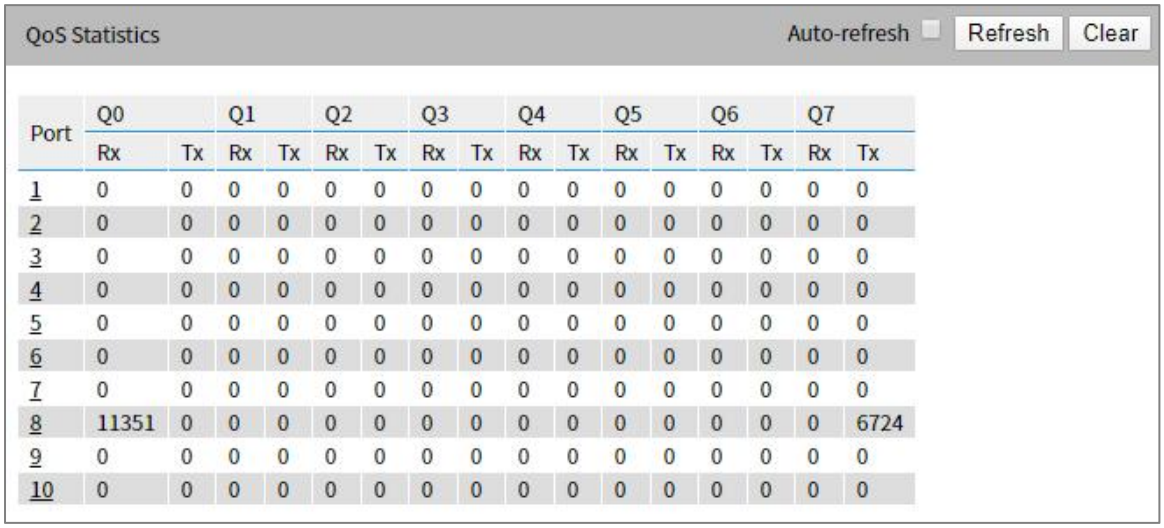
Reset: Click to undo any changes made locally and revert to previously saved values.

Cancel: Return to the previous page without saving the configuration change.

9.12 QoS Statistics

This page provides statistics for the different queues for all switch ports.

The displayed counters are:



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	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	11351	0	0	0	0	0	0	0	0	0	0	0	0	0	0	6724
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

Port

The switch port number. Click the port link to enter the "Port > Detailed Statistical Monitoring" page.

Qn

There are 8 QoS queues per port. Q0 is the lowest priority queue.

- Tx: The number of transmitted packets per queue.
- Rx: The number of received packets per queue.

Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

Clear: Clears the counters for all ports.

9.13 QCL Status

This page shows the QCL status by different QCL users. Each row describes the QCE that is defined. It is a conflict if a specific QCE is not applied to the hardware due to hardware limitations. The maximum number of QCEs is 256 on each switch.

User

Indicates the QCL user.

QCE

Indicates the QCE id.

Port

Indicates the list of ports configured with the QCE.

Frame Type

Indicates the type of frame. The possible values are:

- Any: Match any frame type.
- Ethernet: Match EtherType frames.
- LLC: Match (LLC) frames.
- SNAP: Match (SNAP) frames.
- IPv4: Match IPv4 frames.
- IPv6: Match IPv6 frames.

Action

Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content.

Possible actions are:

- CoS: Classify Class of Service.
- DPL: Classify Drop Precedence Level.
- DSCP: Classify DSCP value.
- PCP: Classify PCP value.
- DEI: Classify DEI value.
- Policy: Classify ACL Policy number.

Conflict

Displays Conflict status of QCL entries. As H/W resources are shared by multiple applications. It may happen that resources required to add a QCE may not be available, in that case it shows conflict status as 'Yes', otherwise it is always 'No'.

Please note that conflict can be resolved by releasing the H/W resources required to add QCL entry on pressing 'Resolve Conflict' button.

Buttons

Combined ▼: Select the QCL status from this drop down list.

- Combined
- Static
- Voice VLAN
- Conflict

Auto-refresh: Check this box to enable an automatic refresh. Automatic refresh occurs every 3 seconds.

Resolve Conflict: Click to release the resources required to add QCL entry, in case the conflict status for any QCL entry is 'yes'.

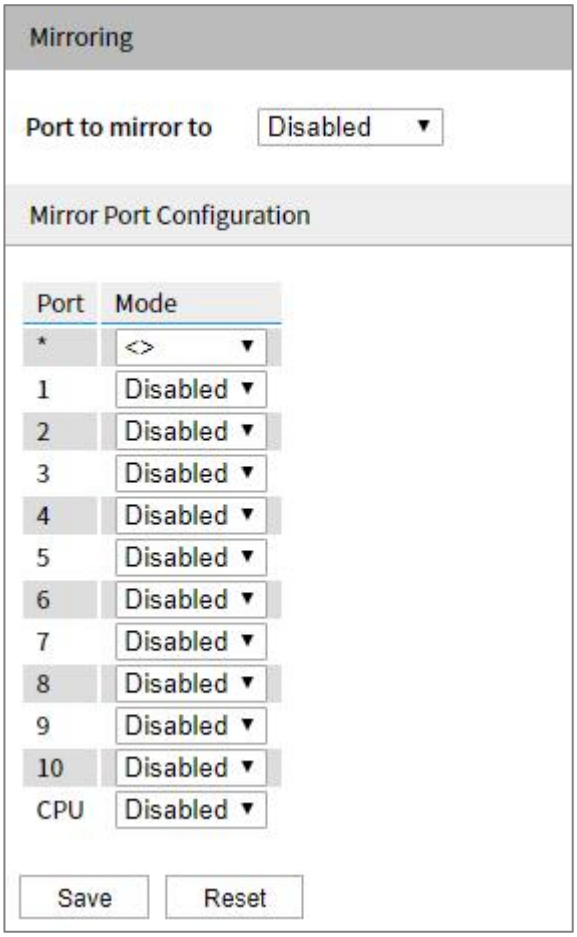
Refresh: Click to refresh the page.

10 System Diagnosis

10.1 Mirroring

Mirroring is a feature for switched port analyzer. The administrator can use the Mirroring to debug network problems. The selected traffic can be mirrored or copied on a destination port where a network analyzer can be attached to analyze the network traffic.

If you want to get the tagged mirrored traffic, you have to set VLAN egress tagging as "Tag All" on the reflector port. On the other hand, if you want to get untagged mirrored traffic, you have to set VLAN egress tagging as "Untag ALL" on the reflector port.



From port mirroring to

This checkbox is designed for selecting destination port.

The destination port is a switched port that you receive a copy of traffic from the source port.

Notice:

- On mirror mode, the device only supports one destination port.
- The destination port needs to disable MAC Table learning.

Mirror port configuration

Port

The switch port number.

Mode

Enable/disable Mirroring function.

- Disable
- Rx
- Tx
- Both

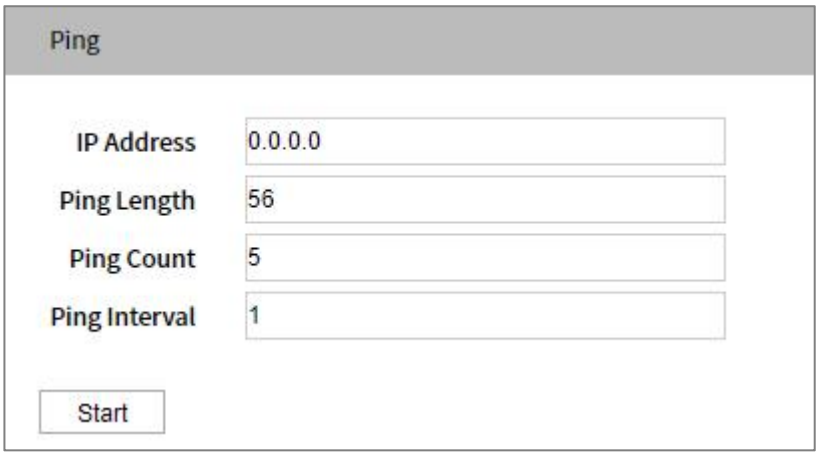
Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

10.2 Ping

This page allows you to issue ICMP PING packets to troubleshoot IP connectivity issues.



After pressing “Start”, ICMP packet is sent, and serial number and round trip time are displayed after receiving reply. The amount of data received in an IP packet of ICMP ECHO_REPLY type is always 8 bytes more than the requested data space (ICMP header). The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

PING server 10.10.132.20, 56 byte data.

64 bytes from 10.10.132.20: icmp_seq=0, time =0ms

64 bytes from 10.10.132.20: icmp_seq=1, time =0ms

64 bytes from 10.10.132.20: icmp_seq=2, time =0ms

64 bytes from 10.10.132.20: icmp_seq=3, time =0ms

64 bytes from 10.10.132.20: icmp_seq=4, time =0ms

Send 5 data packets, receive 5 OK, 0 bad packet

You can configure the following properties of ICMP packets:

Destination IP

The destination IP Address.

Length of Transmission Message

The payload size of the ICMP packet. Values range from 2 bytes to 1452 bytes.

Send Count

The count of the ICMP packet. Values range from 1 time to 60 times.

Time interval

The interval of the ICMP packet. Values range from 0 second to 30 seconds.

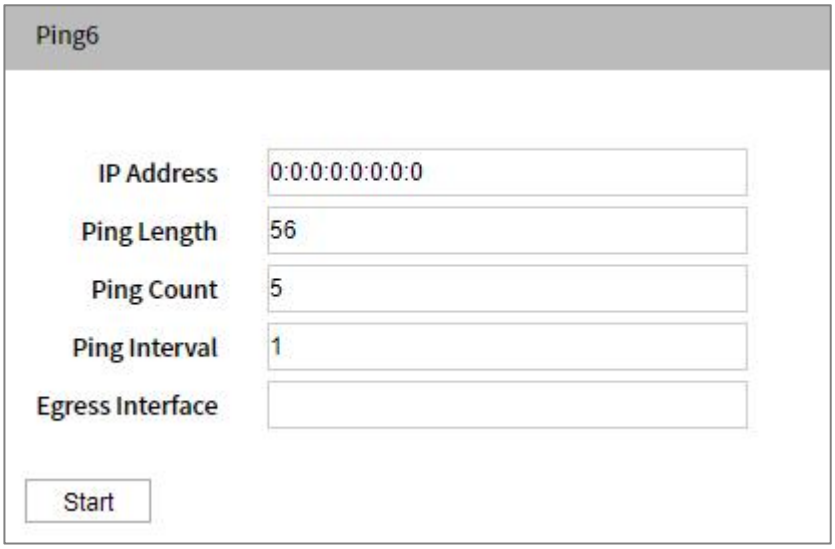
Buttons

Start: Click Start to send ICMP data package.

New Ping: Click to restart diagnostics with PING.

10.3 Ping6

This page allows you to issue ICMPv6 PING packets to troubleshoot IPv6 connectivity issues.



After pressing “Start”, ICMPv6 packet is sent, and serial number and round trip time are displayed after receiving reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

PING6 server ff02::2, 56 bytes of data.

64 bytes from fe80::219:5bff:fe2f:b47: icmp_seq=0, time=10ms

64 bytes from fe80::215:58ff:feed:69dd: icmp_seq=0, time=10ms

64 bytes from fe80::219:5bff:fe2f:b47: icmp_seq=1, time=0ms

64 bytes from fe80::215:58ff:feed:69dd: icmp_seq=1, time=0ms

64 bytes from fe80::219:5bff:fe2f:b47: icmp_seq=2, time=0ms

64 bytes from fe80::215:58ff:feed:69dd: icmp_seq=2, time=0ms

64 bytes from fe80::219:5bff:fe2f:b47: icmp_seq=3, time=0ms

64 bytes from fe80::215:58ff:feed:69dd: icmp_seq=3, time=0ms

64 bytes from fe80::219:5bff:fe2f:b47: icmp_seq=4, time=0ms

64 bytes from fe80::215:58ff:feed:69dd: icmp_seq=4, time=0ms

Send 5 data packets, receive 10 OK, 0 bad packet

You can configure the following properties of the issued ICMP packets:

Destination IP

The destination IP Address.

Length of Transmission Message

The payload size of the ICMP packet. Values range from 2 bytes to 1452 bytes.

Send Count

The count of the ICMP packet. Values range from 1 time to 60 times.

Time interval

The interval of the ICMP packet. Values range from 0 second to 30 seconds.

Egress interface

The VLAN ID (VID) of the specific egress IPv6 interface which ICMP packet goes.

The given VID ranges from 1 to 4094 and will be effective only when the corresponding IPv6 interface is valid.

When the egress interface is not given, PING6 finds the best match interface for destination.

Do not specify egress interface for loopback address.

Do specify egress interface for link-local or multicast address.

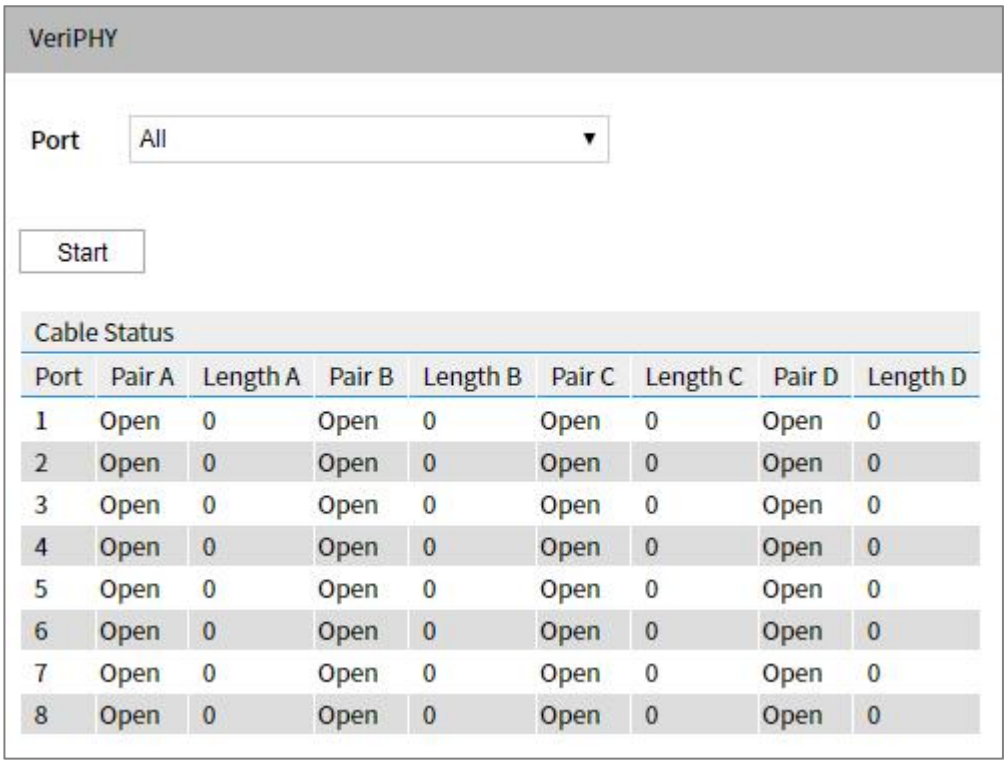
Buttons

Start: Click Start to send ICMP data package.

New Ping: Click to restart diagnostics with PING.

10.4 Cable Detection

This page is used for running the VeriPHY Cable Diagnostics for 10/100 and 1G copper ports.



Press "Start" to run diagnostics. This will take approximately 5 seconds. If all ports are selected, this can take approximately 15 seconds. When completed, the page refreshes automatically, and you can view the cable diagnostics results in the cable status table. Please note that cable detection is only applicable to cables with a length of 7-140m.

10 and 100 Mbps ports will be linked down while running VeriPHY. Therefore, running cable detection on a 10 or 100 Mbps management port will cause the switch to stop responding until cable detection is complete.

Port

The port where you are requesting VeriPHY Cable Diagnostics.

Cable Status

- Port: Switch port number.
- Pair A-D: The status of the cable pair.
  - OK: Correctly terminated pair
  - Open: Open pair
  - Short: Shorted pair
  - Short A: Cross-pair short to pair A
  - Short B: Cross-pair short to pair B
  - Short C: Cross-pair short to pair C
  - Short D: Cross-pair short to pair D

  - Cross A: Abnormal cross-pair coupling with pair A
  - Cross B: Abnormal cross-pair coupling with pair B
  - Cross C: Abnormal cross-pair coupling with pair C
  - Cross D: Abnormal cross-pair coupling with pair D
- Length A-D: Length of cable pair (m). The test results cannot guarantee the accuracy of the network cables produced by all manufacturers, and are only for reference.

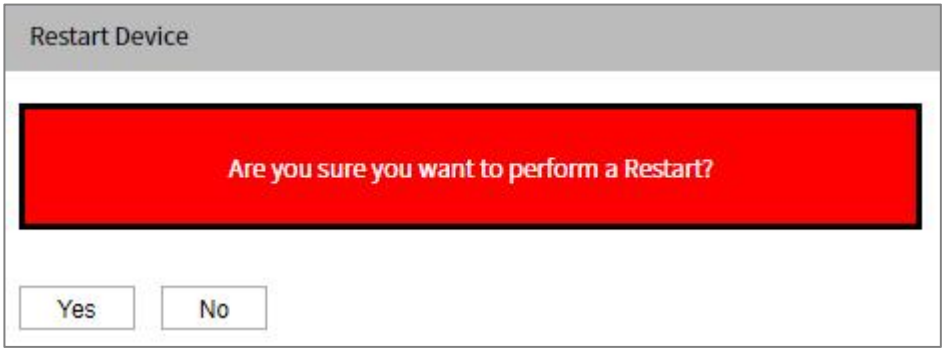
Buttons

Start: click start for port cable detection.

11 System Maintenance

11.1 Restart Device

You can restart the switch on this page. After restart, the switch will boot normally.



Buttons

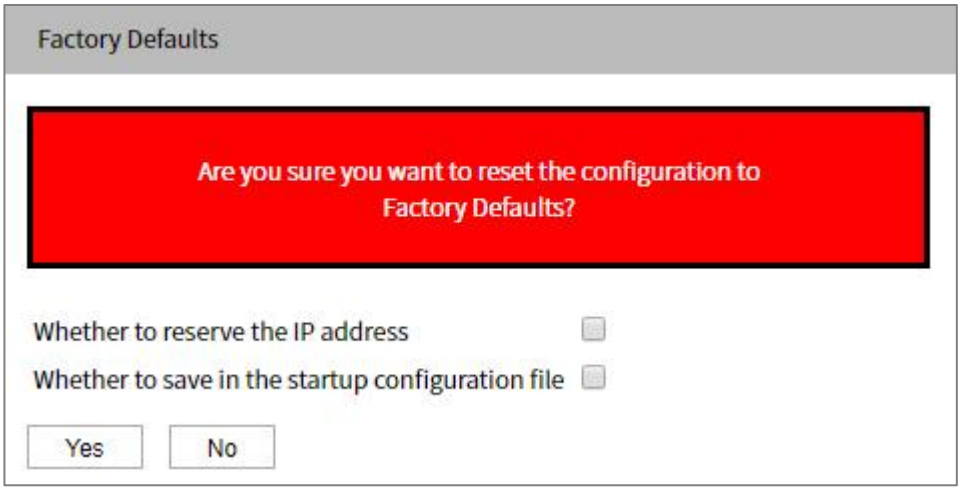
Yes: Click to restart the device.

No: Click to return to the port status page without restarting.

11.2 Restore Factory Settings

You can reset the configuration of the switch on this page.

The new configuration is available immediately, which means that no restart is necessary.



Whether to Reserve the IP Address

When the check box of “Whether to Reserve the IP Address” is checked, the device can keep the current IP address information after restoring the factory settings.

Whether to Save in the Startup Configuration File

When the check box of “Whether to to Save in the Startup Configuration File” is checked, the device can keep the startup information after restoring the factory settings.

Buttons

Yes: Click to reset the configuration to factory default settings.

No: Click to return to the port status page without reconfiguration.

11.3 Upgrade

This page facilitates an update of the firmware controlling the switch.

Click “Choose File” to the location of a software image and click “Upload”.

After uploading the software firmware, the page will announce to start the firmware update. After about a minute, the firmware is updated and the switch restarts.

Warning:

When firmware is being updated, network access is unavailable. Do not restart or power off the device while the firmware update is in progress or the switch may fail to function

afterwards.

Buttons

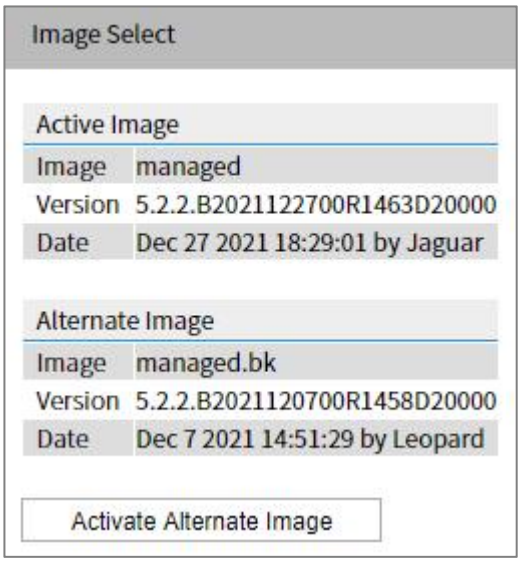
Select File: Click to select the software program to be upgraded.

Update: Click to start upgrading the software.

11.4 Firmware Selection

This page provides information about the active and standby (backup) firmware in the device, and allows recovery to the standby firmware.

The WEB page displays two tables containing information about the active firmware and the standby firmware.



Active Firmware / Standby Firmware

- Firmware: the file name of the firmware.
- Version: The version of the firmware.
- Date: The date where the firmware was produced.

Buttons

Activate alternate image: click to use alternate image.

12 System Configuration

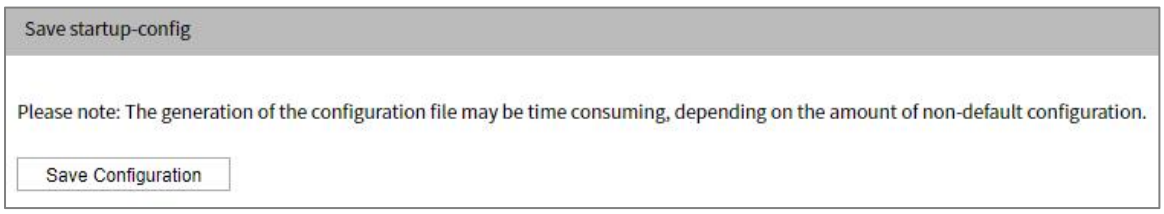
The switch stores its configuration in a number of text files in CLI format. These files are either virtual (based on RAM) or stored in Flash on the switch.

Available documents are:

- running-config: representing the virtual file currently configured by the activity on the switch. This file is volatile.
- startup-config: the startup configuration of the switch, which is read at startup. If this file doesn't exist at boot time, the switch will start up in default configuration.
- default-config: a read-only file with vendor-specific configuration. This file is read when the system is restored to default settings.
- Up to 31 other files, typically used for configuration backups or alternative configurations.

12.1 Save startup-config

This will copy running-config to startup-config, thus ensuring that the currently active configuration will be used on the next restart.



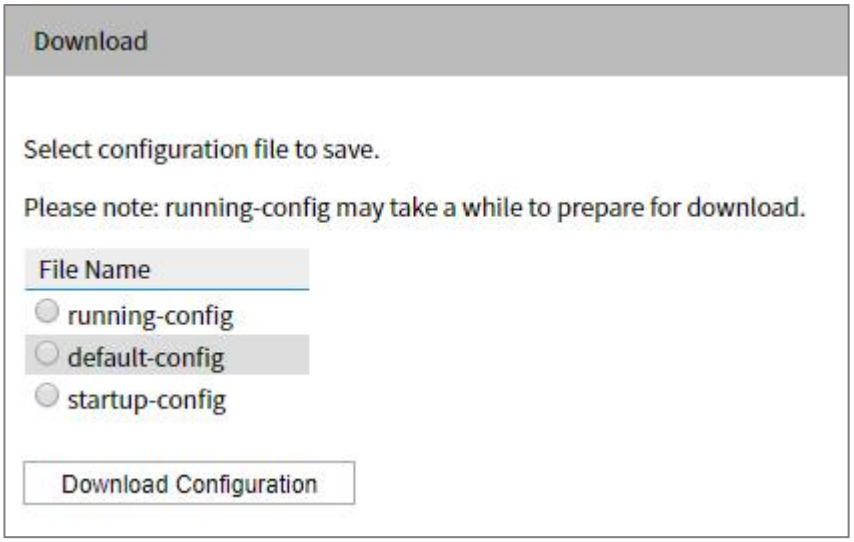
Buttons

Save configuration: Click to save the current running configuration to the startup configuration file.

12.2 Download

It is possible to download any of the files on the switch to the web browser. Select the file and click “Download Configuration File”.

running-config download may take some time to complete, because files must be prepared for download.



File Name

- running-config: representing the virtual file currently configured by the activity on the switch.
- default-config: a read-only file with vendor-specific configuration.
- startup-config: the startup configuration of the switch, which is read at startup.

Note:

If there are other files uploaded, they will also be displayed here.

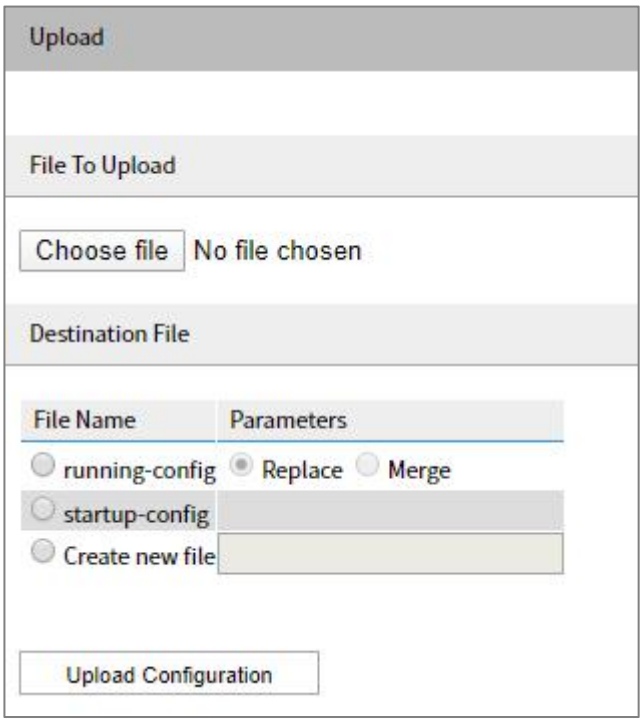
Buttons

Download profile: Click to download the selected profile.

12.3 Upload

It is possible to upload a file from the web browser to all the files on the switch, except default-config which is read-only.

Select the file to upload, select the target file on the target file, and then click “Upload Configuration”.



File to Upload

Buttons

Choose file: click to select the configuration file to be uploaded.

Target File

File Name

- running-config: representing the virtual file currently configured by the activity on the switch.
- startup-config: the startup configuration of the switch, which is read at startup.
- Create new file: Up to 31 other files, typically used for configuration backups or alternative configurations.

Parameter

If the target is running-config, the file will be applied to the switch configuration. This can be achieved in two ways:

- Replace mode: the current configuration is completely replaced with the configuration in the uploaded file.
- Merge mode: the uploaded files are merged into running-config.

When creating a new file, the name of the new file can be configured. It supports up to 63 valid characters, letters, numbers, dots, minus signs and underscores. The minus sign cannot be the first character and cannot contain only dots. If the Flash file system is full (that is, it contains the default configuration and 32 other files, usually including

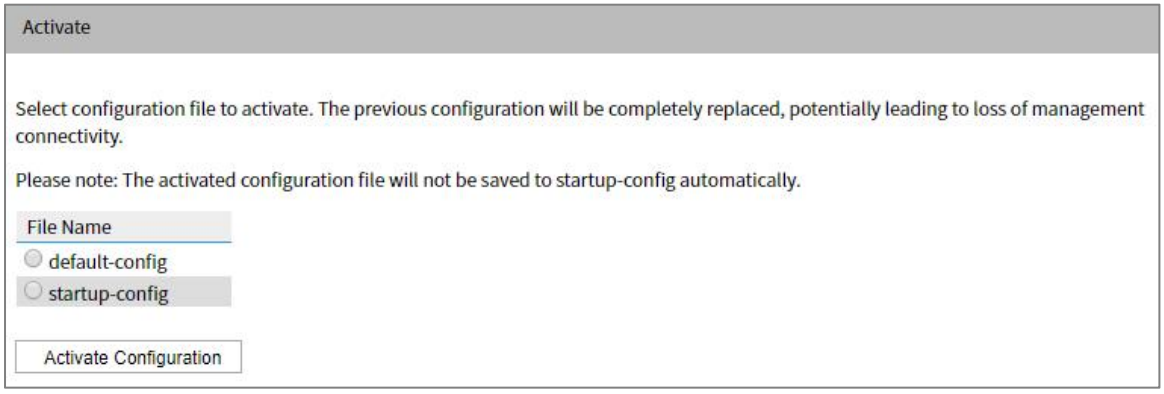
startup-config), it is impossible to create a new file. Instead an existing file must be overwritten or another file must be deleted.

Buttons

Upload configuration: Click start to upload the configuration file.

12.4 Activate

You can activate any configuration file on the switch, except that running-config represents the currently active configuration.



Select the file to activate and click “Activate Configuration”. This will initiate the process of completely replacing the existing configuration with that of the selected file.

File name

- default-config: a read-only file with vendor-specific configuration.
- startup-config: the startup configuration of the switch, which is read at startup.

Note:

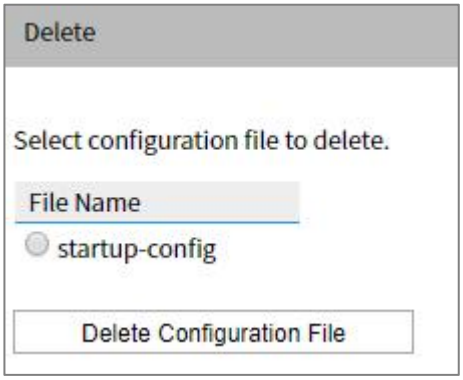
If there are other files uploaded, they will also be displayed here.

Buttons

Activate configuration: Click to activate the selected configuration file into the current running configuration.

12.5 Delete

It is possible to delete any of the writable files stored in Flash, including startup-config. If this is done and the switch is rebooted without a prior Save operation, this effectively resets the switch to default configuration.



File name

- startup-config: the startup configuration of the switch, which is read at startup.

Note:

If there are other files uploaded, they will also be displayed here.

Buttons

Delete profile: Click to delete the selected profile.

13 FAQ

13.1 Sign in Problems

1. **Why the web page display abnormally when browsing the configuration via WEB?**
   Before accessing the WEB, please eliminate IE cache buffer and cookies. Otherwise, the web page will display abnormally.

2. **What should I do if I forget my login password?**
   If you forget the login password, you can initialize the password by restoring the factory settings, and the device can restore the factory settings through the network management software or DIP switch. Both of the initial user name and password are "admin".

13.2 Configuration Problem

1. **Why the bandwidth can't be increased after configuring Trunking (port aggregation) function?**
   Check whether the port attributes set to Trunking are consistent, such as rate, duplex mode, VLAN and other attributes.

2. **How to deal with the problem that part of switch ports are impassable?**
   When some ports on the switch are impassable, it may be network cable, network adapter and switch port faults. User can locate the faults via following tests:
   - Keep connected computer and switch ports unchanged, change other network cables;

- Keep connected network cable and switch port unchanged, change other computers;
- Keep connected network cable and computer unchanged, change other switch port;
- If the switch port faults are confirmed, please contact supplier for maintenance.

3. **How about the order of port self-adaption state detection?**

   The port self-adaption state detection is conducted according to following order: 1000Mbps full duplex, 100Mbps full duplex, 100Mbps half-duplex, 10Mbps full duplex, 10Mbps half-duplex, detect from high to low, connect automatically in supported highest speed.

13.3 Indicator Problem

1. **Why is the power supply indicator off?**

   Possible reasons include:

   - Not connected to the power socket; troubleshooting, connected to the power socket.
   - Power supply or indicators faults; troubleshooting, change the power supply or device test.
   - Power supply voltage can't meet the device requirements; troubleshooting, configure the power supply voltage according to the device manual.

2. **Why is the Link/Act indicator off?**

   Possible reasons include:

   - The network cable portion of Ethernet copper port is disconnected or bad contact; troubleshooting, connect the network cable again.
   - Ethernet terminal device or network card works abnormally; troubleshooting, eliminate the terminal device fault.
   - Not connected to the power socket; troubleshooting, connected to the power socket.
   - Interface rate doesn't match the pattern; troubleshooting, examine whether the device transmission speed matches the duplex mode.

3. **Ethernet copper port and fiber port indicator are connected normally, but can't transmit data, what's the reason?**

When the system is power on or network configuration changes, the device and switch configuration in the network will need some time. Troubleshooting, after the device and switch configuration are completed, Ethernet data can be transmitted; if it's impassable, power off the system, and power on again.

4. **Why does the communication crashes after a period of time, namely, it cannot communicate, and it returns to normal after restarting?**

   Reasons may include:

   - Surrounding environment disturbs the product; troubleshooting, product grounding adopts shielding line or shields the interference source.
   - Site wiring is not normative; Troubleshooting, optical fiber, network cable, optical cable cannot be arranged with power line and high-voltage line.
   - Network cable is disturbed by static electricity or surge; Troubleshooting, change the shielded cable or install a lightning protector.
   - High and low temperature influence; troubleshooting, check the device temperature usage range.