PROFESSIONAL

NGSM8T2P/NGSM24T4P/NGSM48T4XP

L2 /L3 Management Switch

User Manual

About This Manual

Copyright

Purpose

This manual gives specific information on how to operate and use the management functions of the L2 / L3 management series

Audience

The Manual is intended for use by network administrators who are responsible for operating and maintaining network equipment; consequently, it assumes a basic working knowledge of general switch functions, the Internet Protocol (IP), and web management (HTTP/HTTPs).

Table of Contents

Revision History

Release	Date	Revision
V1.00	2022/07/15	A1
V1.1	2023/11/23	A2

Overview

Niveo L2 / L3 Managed switch is a next-generation Ethernet Switch offering powerful L2 features, and Layer 3 Static routing that delivers the cost-effectively business and transports Ethernet services via fiber or copper connections.It provides high HW performance and environment flexibility for SMBs and Enterprises.

It is ideal to deliver management simplicity, optimum user experience, and lower cost. The embedded Device Managed System is designed to be extremely easy-to-use/manage/install IP Phone, IP Cam, or Wifi-AP for Enterprise Applications.

- L2+ features provide better manageability, security, QoS, and performance.
- Support IPv4/IPv6 dual stack management
- Support SSH/SSL secured management
- Support SNMP v1/v2c/v3
- Support RMON groups 1,2,3,9
- Support sFlow
- Support IGMP v1/v2/v3 Snooping
- Support MLD v1/v2 Snooping
- Support RADIUS and TACACS+ authentication
- Support IP Source Guard
- Support DHCP Relay (Option 82)
- Support DHCP Snooping
- Support ACL and QCL for traffic filtering
- Support 802.1d(STP), 802.1w(RSTP) and 802.1s(MSTP)
- Support LACP and static link aggregation
- Support Q-in-Q double tag VLAN
- Support GVRP dynamic VLAN

Overview of this User Guide

- Chapter 1 “Operation of Web-based Management”
- Chapter 2 “Configuration”
- Chapter 3 “Monitor”
- Chapter 4 “Diagnostics”
- Chapter 5 “Maintenance”

Chapter 1 Operation of Web-based Management

IMPORTANT:

1. It is recommended to use **Chrome, Firefox, Edge and IE** to open a web console with the switch.

2. You should save the configuration changes made on the menus before leaving the web page. Otherwise, your configuration changes will be lost. The save button is located on the upper right corner of the screen.

Initial Configuration

This chapter instructs you how to configure and manage the switch through the web interface. With this facility, you can easily access and monitor through any one port of the switch all the status of the switch, including MIBs status, each port activity, Spanning tree status, port aggregation status, multicast traffic, VLAN and priority status, even illegal access record and so on.

The default IP Address: 192.168.2.1

Default Username:Admin

Default password:system

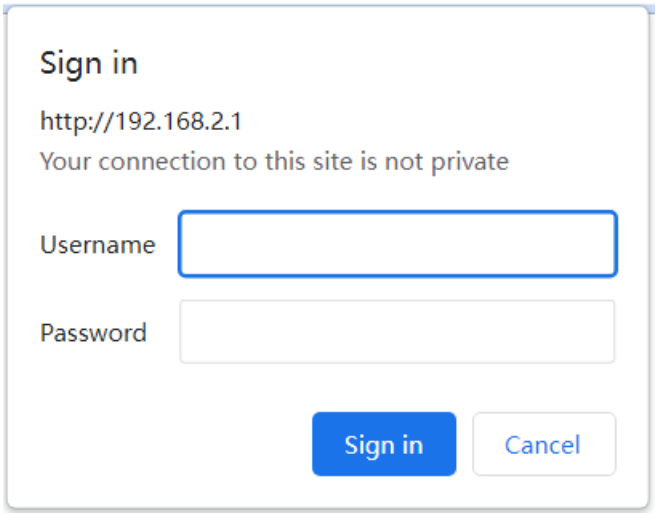


Figure 1: The login page

Chapter 2 Configuration

This chapter describes the entire basic configuration tasks which includes the System Information and any manage of the Switch (e.g. Time, Account, IP, Syslog and NTP.)

2-1 System

You can identify the system by configuring the contact information, name, and location of the switch.

2-1.1 Information

The switch system's contact information is provided here.

Web interface

To configure System Information in the web interface:

1. Click Configuration, System and Information.
2. Write System Contact, System Name, System Location information in this page.
3. Click Save

Figure 2-1.1: System Information

Parameter description:

- **System Contact :**

  The textual identification of the contact person for this managed node, together with information on how to contact this person. The allowed string length is 0 to 128, and the allowed content is the ASCII characters from 32 to 126.

- **System name :**

  An administratively assigned name for this managed node. By convention, this is the node's fully-qualified domain name. A domain name is a text string drawn from the alphabet (A-

Za-z), digits (0-9), minus sign (-). No space characters are permitted as part of a name. The first character must be an alpha character. And the first or last character must not be a minus sign. The allowed string length is 0 to 128.

- **System Location :**

  The physical location of this node(e.g., telephone closet, 3rd floor). The allowed string length is 0 to 128, and the allowed content is the ASCII characters from 32 to 126.

Buttons

- **Save :**

  Click to save changes.

- **Reset :**

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

The IPv4 address for the switch could be obtained via DHCP Server for VLAN 1. To manually configure an address, you need to change the switch's default settings to values that are compatible with your network. You may also need to establish a default gateway between the switch and management stations that exist on another network segment.

Configure the switch-managed IP information on this page

Configure IP basic settings, control IP interfaces and IP routes.

The maximum number of interfaces supported is 128 and the maximum number of routes is 128.

Web Interface

To configure an IP address in the web interface:

1. Click Configuration, System and IP.
2. Click Add Interface then you can create new Interface on the switch.
3. Click Add Route then you can create new Route on the switch.
4. Click Save.

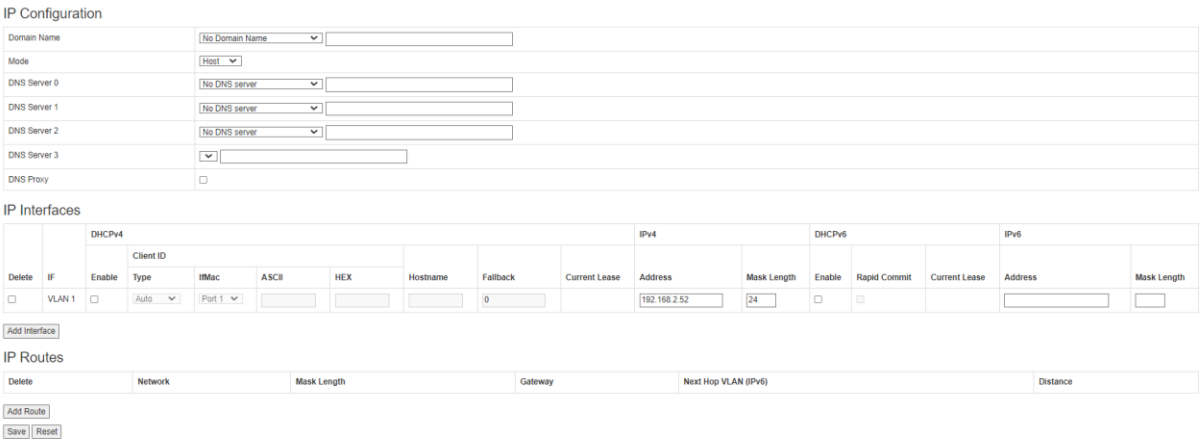


Figure2-1.2: The IP configuration

Parameter description:

IP Configuration

- **Domain Name**

  This setting allows to configure the domain name by switch. The following modes are supported:

  - No Domain name:
  - Configured domain name:
  - From any DHCPv6 interfaces:
  - From this DHCPv6 interface:

- **Mode :**

Configure whether the IP stack should act as a Host or a Router. In Host mode, IP traffic between interfaces will not be routed. In Router mode traffic is routed between all interfaces.

- **DNS Server :**

  This setting controls the DNS name resolution done by the switch. The following modes are supported:

  - From any DHCP interfaces:
    The first DNS server offered from a DHCP lease to a DHCP-enabled interface will be used.
  - No DNS server:
    No DNS server will be used.
  - Configured:
    Explicitly provide the IP address of the DNS Server in dotted decimal notation.
  - From this DHCP interface
    Specify from which DHCP-enabled interface a provided DNS server should be preferred.

- **DNS Proxy :**

  When DNS proxy is enabled, system will relay DNS requests to the currently configured DNS server, and reply as a DNS resolver to the client devices on the network.

IP Interfaces

- **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.

- **IPv4 DHCP Enabled:**

  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.

- **IPv4 DHCP Client Identifier Type:**

  This specified which of the three type below, i.e. IfMac, ASCII or HEX, shall be used for the Client Identifier. See RFC-2132 section 9.14.

- **IPv4 DHCP Client Identifier IfMac:**

  The interface name of DHCP client identifier. When DHCPv4 client is enabled and the client identifier type is 'ifmac', the configured interface's hardware MAC address will be used in the DHCP option 61 field.

- **IPv4 DHCP Client Identifier ASCII :**

  The ASCII string of DHCP client identifier. When DHCPv4 client is enabled and the client identifier type is 'ascii', the ASCII string will be used in the DHCP option 61 field.

- **IPv4 DHCP Client Identifier HEX:**

  The hexadecimal string of DHCP client identifier. When DHCPv4 client is enabled and the client identifier type 'hex', the hexadecimal value will be used in the DHCP option 61 field.

- **IPv4 DHCP Hostname:**

  The hostname of DHCP client. If DHCPv4 client is enabled, the configured hostname will be used in the DHCP option 12 field. When this value is empty string, the field use the configured system name plus the latest three bytes of system MAC addresses as the hostname.

- **IPv4 DHCP 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.

- **IPv4 DHCP 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 may be left blank if IPv4 operation on the interface is not desired - or no DHCP fallback address is desired.

- **IPv4 Mask :**

  The IPv4 network mask, in number of bits (prefix length). Valid values are between 0 and 30 bits for a IPv4 address.
  If DHCP is enabled, this field configures the fallback address network mask. The field may 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:**

  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.

- **Resolving IPv6 DAD :**

  The link-local address is formed from an interface identifier based on the hardware address which is supposed to be uniquely assigned. Once the DAD (Duplicate Address Detection) detects the address duplication, the operation on the interface SHOULD be disabled.
  At this moment, manual intervention is required to resolve the address duplication. For example, check whether the loop occurs in the VLAN or there is indeed other device occupying the same hardware address as the device in the VLAN.
  After making sure the specific link-local address is unique on the IPv6 link in use, delete and then add the specific IPv6 interface to restart the IPv6 operations on this interface.

IP Routes

- **Delete :**

  Select this option to delete an existing IP route.

- **Network :**

  The destination IP network or host address of this route. Valid format is dotted decimal notationor 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 notationor 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 4094 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.

Buttons

- **Add Interface :**

  Click to add a new IP interface. A maximum of 8 interfaces is supported.

- **Add Route :**

  Click to add a new IP route. A maximum of 32 routes is supported.

- **Apply :**

  Click to save changes.

- **Reset :**

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

2-1.3 NTP

NTP is Network Time Protocol and is used to sync the network time based Greenwich Mean Time (GMT). If use the NTP mode and select a built-in NTP time server or manually specify an user-defined NTP server as well as Time Zone, the switch will sync the time in a short after pressing <Apply> button. Though it synchronizes the time automatically, NTP does not update the time periodically without user's processing.

Time Zone is an offset time off GMT. You have to select the time zone first and then perform time sync via NTP because the switch will combine this time zone offset and updated NTP time to come out the local time, otherwise, you will not able to get the correct time. The switch supports configurable time zone from –12 to +13 step 1 hour.

Default NTP is disabled.

Web Interface

To configure NTP in the web interface:

1. Click Configuration, System and NTP.
2. Specify the Time parameter in manual parameters.
3. Click Apply.

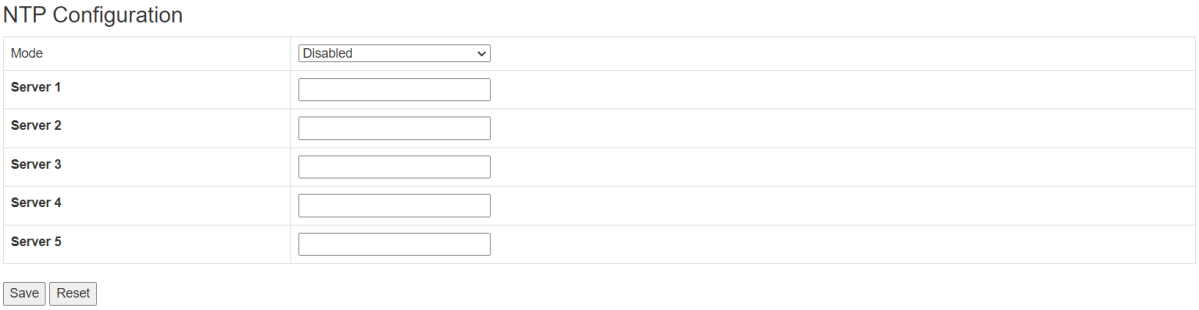


Figure 2-1.3: The NTP configuration

Parameter description:

- **Mode :**

  Indicates the NTP mode operation. Possible modes are:
  Enabled: Enable NTP client mode operation.
  Disabled: Disable NTP client mode operation.

- **Server 1~5:**

  Provide the IPv4 or IPv6 address of a NTP server. 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. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'. In addition, it can also accept a domain name address.

Buttons

- **Save :**

  Click to save changes.

- **Reset :**

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

2-1.4 Time

The switch allows to configure the Time Zone and setup daylight saving time.

Web Interface

To configure Time in the web interface:

1. Click Configuration, System and Time.
2. Specify the Time parameter.
3. Click Save.

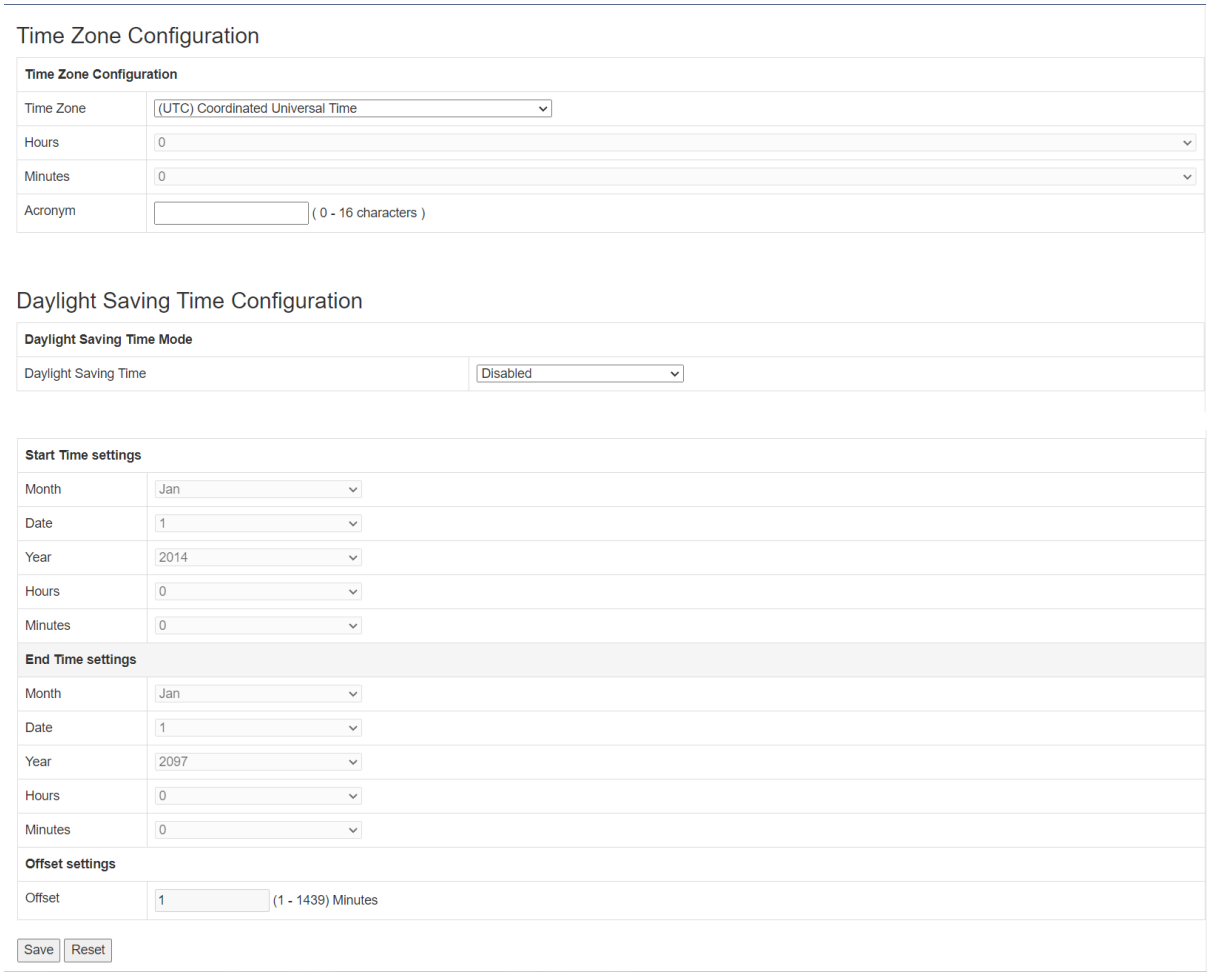


Figure 2-1.4: The time configuration

Parameter description:

Time Zone Configuration

- **Time Zone :**

  Lists various Time Zones world wide. Select appropriate Time Zone from the drop down and click Save to set. The 'Manual Setting' options is used for the specific time zone which is excluded from the options list.

- **Hours:**

  Number of hours offset from UTC. The field only available when time zone manual setting

- **Minutes :**

Number of minutes offset from UTC. The field only available when time zone manual setting.

- **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) Notice the string '' is a special syntax that is reserved for null input.

Daylight Saving Time Configuration

- **Daylight Saving Time :**

  This is used to set the clock forward or backward according to the configurations set below for a defined Daylight Saving Time duration. Select 'Disable' to disable the Daylight Saving Time configuration. Select 'Recurring' and configure the Daylight Saving Time duration to repeat the configuration every year. Select 'Non-Recurring' and configure the Daylight Saving Time duration for single time configuration. (Default: Disabled).

Recurring Configuration

- **Start time settings :**

  Year - Select the starting year.

  Day - Select the starting day.

  Month - Select the starting month.

  Hours - Select the starting hour.

  Minutes - Select the starting minute.

- **End time settings :**

  Year - Select the ending year.

  Day - Select the ending day.

  Month - Select the ending month.

  Hours - Select the ending hour.

  Minutes - Select the ending minute.

- **Offset settings :**

  Offset - Enter the number of minutes to add during Daylight Saving Time. (Range: 1 to 1440)

NOTE: The under “Start Time Settings” and “End Time Settings” was displayed what you set on the “Start Time Settings” and “End Time Settings” field information.

Buttons

- **Save :**

  Click to save changes.

- **Reset :**

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

2-1.5 Log

The log is a standard for logging program messages . It allows separation of the software that generates messages from the system that stores them and the software that reports and analyzes them. It can be used as well a generalized informational, analysis and debugging messages. It is supported by a wide variety of devices and receivers across multiple platforms.

Web Interface

To configure log configuration in the web interface:

1. Click Configuration, System and log.
2. Specify the Server Address.
3. Evoke the Syslog to enable it.
4. Click Save.

Figure2-1.5: The System Log configuration

Parameter description:

- **Server Mode :**

  Indicate the server mode operation. When the mode operation is enabled, the syslog message will send out to 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 sender 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 hosts address of syslog server. If the switch provide DNS feature, it also can be a host name.

- **Syslog Level :**

  Severity levels indicates how important particular messages are. There are 4 severity levels:

  Error: Error condition

  Warning: Warning condition

  Notice: Normal but important event

  Informational: Informational messages

Buttons

- **Save :**

Click to save changes.

- **Reset :**

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

2-2 Green Ethernet

2-2.1 LED

The LED light intensity may be adjusted in a percentage of intensity during programmable time periods.
The maintenance checkbox will bring LED intensity to 100% for 10 seconds in the event of any error (such as link down）.

Web Interface

To configure LED power reduction Configuration in the web interface:

1. Click Configuration, Green Ethernet and LED.
2. Select the start time, end time and intensity.
3. Click Save.

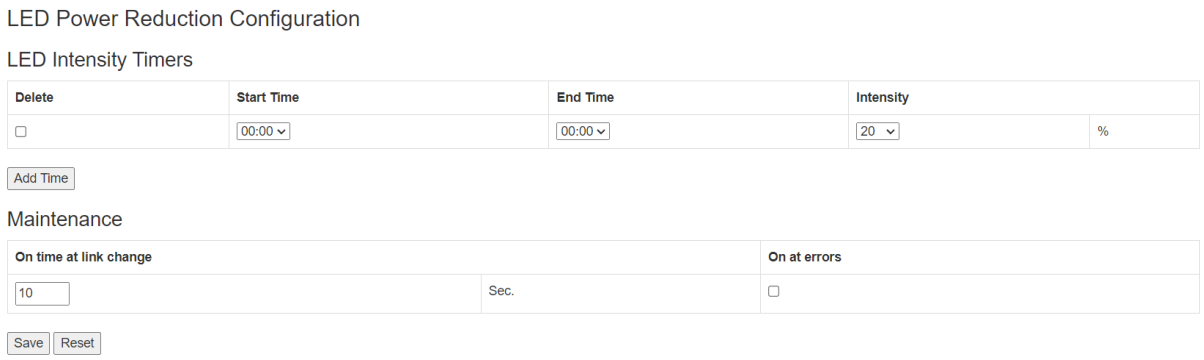


Figure 2-2.1: LED Power Reduction Configuration

Parameter description:

- **Start Time :**

  The time at which the LEDs intensity shall be set to the corresponding intensity.

- **End Time:**

  The time at which the LEDs intensity shall be set to a new intensity. If no intensity is specified for the next hour, the intensity is set to default intensity.

- **Intensity :**

  The LEDs intensity (100% = Full power, 0% = LED off).

- **On time at link change:**

  When a network administrator does maintenance of the switch (e.g. adding or moving users) he might want to have full LED intensity during the maintenance period . Therefore it is possible to specify that the LEDs shall use full intensity a specific period of time. Maintenance Time is the number of seconds that the LEDs will have full intensity after either a port has changed link state, or the LED pushbutton has been pushed. Valid range is from 0 to 65535 seconds.

- **Intensity :**

  In the case where maximum power saving is enabled by turning the LEDs completely off, it might be convenient to indicate to the network administrator that an error has been recorded in the system log. By checking the "On at errors" the LEDs will be turned on at 100% in the case that errors are logged in the system log.

Buttons

- **Add Time**

  Click to add the time configuration

- **Save :**

  Click to save changes.

- **Reset :**

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

2-2.2 Port Power Savings

EEE is a power saving option that reduces the power usage when there is low or no traffic utilization.

EEE works by powering down circuits when there is no traffic. When a port gets data to be transmitted all circuits are powered up. The time it takes to power up the circuits is named wakeup time. The default wakeup time is 17 us for 1Gbit links and 30 us for other link speeds. EEE devices must agree upon the value of the wakeup time in order to make sure that both the receiving and transmitting device has all circuits powered up when traffic is transmitted. The devices can exchange wakeup time information using the LLDP protocol.

EEE works for ports in auto-negotiation mode, where the port is negotiated to either 1G or 100 Mbit full duplex mode.

For ports that are not EEE-capable the corresponding EEE checkboxes are grayed out and thus impossible to enable EEE for.

When a port is powered down for saving power, outgoing traffic is stored in a buffer until the port is powered up again. Because there are some overhead in turning the port down and up, more power can be saved if the traffic can be buffered up until a large burst of traffic can be transmitted. Buffering traffic will give some latency in the traffic.

Web Interface

To configure a Port Power Saving Configuration in the web interface:

4. Click Configuration, Green Ethernet and Port Power Savings.
5. Evoke to enable or disable the ActiPHY, PerfectReach, EEE and EEE Urgent Queues.
6. Click Apply.

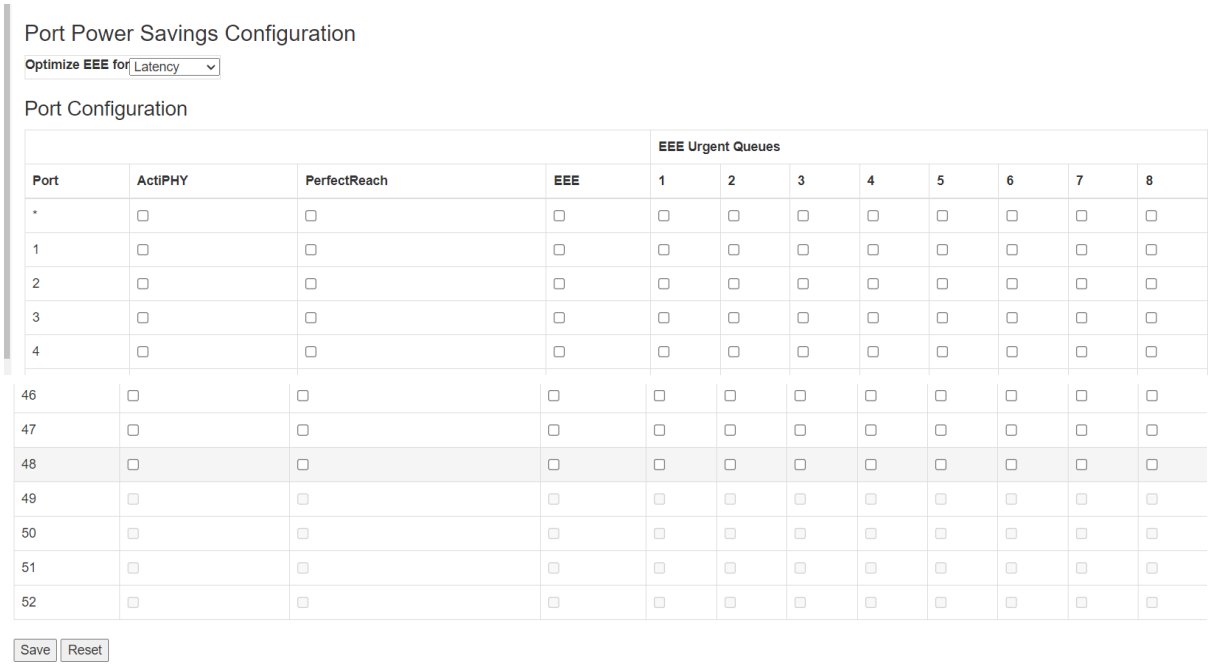


Figure 2-2.2: The Port Power Saving Configuration

Parameter description:

Optimize EEE for :

The switch can be set to optimize EEE for either best power saving or least traffic latency.

- **Port :**

The switch port number of the logical port.

- **EEE :**

  Controls whether EEE is enabled for this switch port.

  For maximizing power savings, the circuit isn't started at once transmit data is ready for a port, but is instead queued until a burst of data is ready to be transmitted. This will give some traffic latency.

  If desired it is possible to minimize the latency for specific frames, by mapping the frames to a specific queue (done with QOS), and then mark the queue as an urgent queue. When an urgent queue gets data to be transmitted, the circuits will be powered up at once and the latency will be reduced to the wakeup time.

- **EEE Urgent Queues :**

  Queues set will activate transmission of frames as soon as data is available. Otherwise the queue will postpone transmission until a burst of frames can be transmitted.

Buttons

- **Save :**

  Click to save changes.

- **Reset :**

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

2-3 Ports Configuration

The section describes to configure the Port detail parameters of the switch. Others you could using the Port configure to enable or disable the Port of the switch. Monitor the ports content or status in the function.

2-3.1 Ports

This page displays current port configurations. Ports can also be configured here.

Web Interface

To configure a Current Port Configuration in the web interface:

1. Click Configuration and Ports.
2. Specify the Speed Configured, Flow Control, Maximum Frame size etc.
3. Click Save.

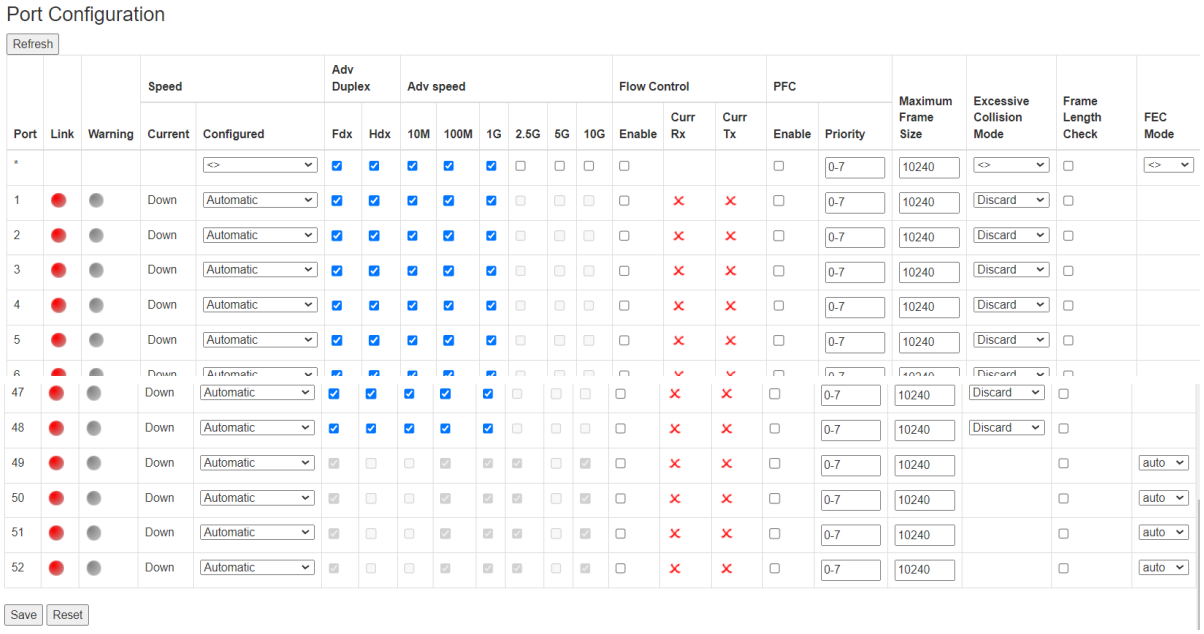


Figure 2-3.1: The Port Configuration

Parameter description:

- **Port :**

  This is the logical port number for this row.

- **Link :**

  The current link state is displayed graphically. Green indicates the link is up and red that it is down.

- **Warning :**

  Operational warnings of the port.

: No warnings

: There are warnings, use tooltip to see.

- **Current Link Speed :**

  Provides the current link speed of the port.

- **Configured Link Speed :**

  Selects any available link speed for the given switch port. Only speeds supported by the specific port is shown. Possible speeds are:

  Disabled - Disables the switch port operation.

  Auto - Port auto negotiating speed with the link partner and selects the highest speed that is compatible with the link partner.

  10Mbps HDX - Forces the cu port in 10Mbps half-duplex mode.

  10Mbps FDX - Forces the cu port in 10Mbps full duplex mode.

  100Mbps HDX - Forces the cu port in 100Mbps half-duplex mode.

  100Mbps FDX - Forces the cu port in 100Mbps full duplex mode.

  1Gbps FDX - Forces the port in 1Gbps full duplex

  2.5Gbps FDX - Forces the Serdes port in 2.5Gbps full duplex mode.

  10Gbps FDX - Forces the port in 10Gbps full duplex

- **Dual-media:**

  If a port is Dual-media, this field selects which of the ports to use. If Auto is selected, both ports can be used, and if both ports has link, the SFP port will be preferred.

- **Advertise Duplex:**

  When duplex is set as auto i.e auto negotiation, the port will only advertise the specified duplex as either Fdx or Hdx to the link partner. By default port will advertise all the supported duplexes if the Duplex is Auto.

- **Advertise Speed :**

  When Speed is set as auto i.e auto negotiation, the port will only advertise the specified speeds (10M 100M 1G 2.5G 5G 10G) to the link partner. By default port will advertise all the supported speeds if speed is set as Auto.

- **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.

  Check the configured column to use flow control. This setting is related to the setting for Configured Link Speed.

  NOTICE: The 100FX standard does not support Auto Negotiation, so when in 100FX mode the flow control capabilities will always be shown as "disabled".

- **Maximum Frame Size :**

  Enter the maximum frame size allowed for the switch port, including FCS. The range is 1518-10240 bytes.

- **PFC (Priority based on flow control) :**

When PFC (802.1Qbb Priority Flow Control) is enabled on a port then flow control on a priority level is enabled. Through the Priority field, range (one or more) of priorities can be configured, e.g. '0-3,7' which equals '0,1,2,3,7'. PFC is not supported through auto negotiation. PFC and Flowcontrol cannot both be enabled on the same port.

- **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 :**

  Configures if frames with incorrect frame length in the EtherType/Length field shall be dropped. An Ethernet frame contains a field EtherType which can be used to indicate the frame payload size (in bytes) for values of 1535 and below. 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 does not match the actually payload length. If "frame length check" is disabled, frames are not dropped due to frame length mismatch. Note: No drop counters count frames dropped due to frame length mismatch

- **FEC (Forwarding Error Correction) Mode :**

  FEC is short for Forward Error Correction. It is a technique for controlling errors over an unreliable link. The idea is that the sender adds some extra bits to the frame that allows a receiver to correct bit errors in the received frame.
  R-FEC (IEEE802.3 clause 74 - sometimes called Firecode). This is meant for 10G. The parameter affects both what is requested during clause 73 aneg and what the port is configured to use if not running clause 73 aneg. If running clause 73 aneg on 10G ports we always tell the link partner that we support R-FEC. What the end user can control with the fec command is whether we request R-FEC. If either us or the link partner requests R-FEC, the port will end up using R-FEC.

  auto: This is the default and means the following:
  If a 10G port runs clause 73, R-FEC will be requested.
  Otherwise, no FEC will be enabled.
  r-fec: If a 10G port runs clause 73, only R-FEC will be requested. If a 10G port does not run clause 73, but is loaded with at least a 10G SFP and the speed is at least 5G, only R-FEC will be enabled. Otherwise, no FEC will be enabled.
  none: If the port is running clause 73, R-FEC will not be requested (but remember that this does not mean that the clause 73 aneg will not result in the port running FEC). Otherwise, the port will not run any FEC.

Buttons

- **Save :**

  Click to save changes.

- **Reset :**

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

- **Upper left icon (Refresh) :**

  Click to refresh the page. Any changes made locally will be undone.

2-4 CFM

The section describes to configure the CFM parameters of the switch.

Ethernet CFM is an end-to-end per-service-instance (per-VLAN) Ethernet layer OAM protocol. It includes proactive connectivity monitoring, fault verification, and fault isolation. End-to-end can be provider-edge-to provider-edge (PE-to-PE) device or customer-edge-to-customer-edge (CE-to-CE) device. Ethernet CFM, as specified by IEEE 802.1ag, is the standard for Layer 2 ping, Layer 2 traceroute, and end-to-end connectivity verification of the Ethernet network.

2-4.1 CFM Global Configuration

This page configures CFM global configuration.

Web Interface

To configure CFM global configuration in the web interface:

1. Click Configuration, CFM and CFM gbobal configuration.
2. Select the sender ID TLV, port status TLV, interface status TLV etc.
3. Click save.

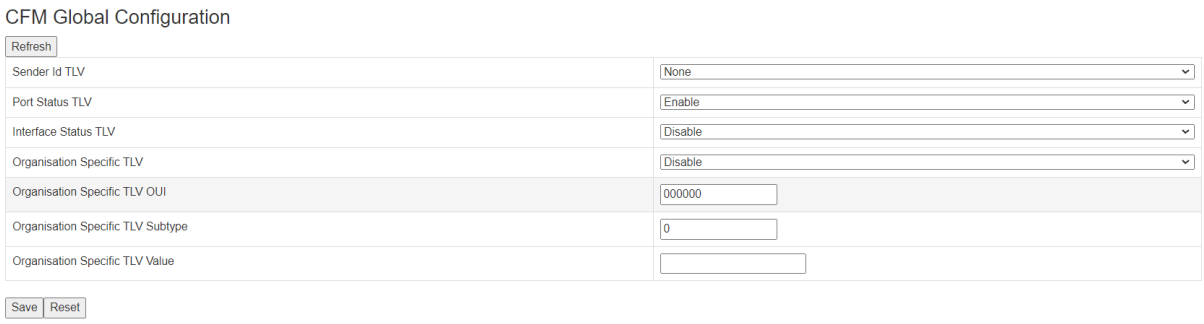


Figure 2-4.1: CFM Global Configuration

Parameter description:

- **Sender ID TLV :**

  Choose whether and what to use as Sender ID TLVs in CCMs generated by this switch. Can be overridden by Domain and Service level configuration.
  None: Do not include Sender ID TLVs.
  Chassis: Enable Sender ID TLV and send Chassis ID (MAC Address).
  Manage: Enable Sender ID TLV and send Management address (IPv4 Address).
  ChassisManage: Enable Sender ID TLV and send both Chassis ID (MAC Address) and Management Address (IPv4 Address).

- **Port Status TLV :**

  Choose whether to send Port Status TLVs in CCMs generated by this switch. Can be overridden by Domain and Service level configuration.
  Enable: Send Port Status TLVs in CCMs generated by this switch.
  Disable: Do not send Port Status TLVs in CCMs generated by this switch

- **Interface Status TLV:**

  Choose whether to send Interface Status TLVs in CCMs generated by this switch. Can be

overridden by Domain and Service level configuration.
Enable: Send Interface Status TLVs in CCMs generated by this switch.
Disable: Do not Send Interface Status TLVs in CCMs generated by this switch.

- **Organisation Specific TLV:**

  Choose whether to send Organisation Specific TLVs in CCMs generated by this switch. Can be overridden by Domain and Service level configuration.
  Enable: Send Organisation Specific TLVs in CCMs generated by this switch.
  Disable: Do not send Organisation Specific TLVs in CCMs generated by this switch.

- **Organisation Specific TLV OUI:**

  This is the three-bytes OUI transmitted with the Organization-Specific TLVs. Enter as 6 characters 0-9, a-f.

- **Organisation Specific TLV Subtype:**

  This is the subtype transmitted with the Organization-Specific TLV. Can be any value in range [0; 255]

- **Organisation Specific TLV Value:**

  This is the value transmitted in the Organization-Specific TLVs. Value is a printable character string of length 0-63.

Buttons

- **Save :**

  Click to save changes.

- **Reset :**

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

2-4.2 Domain

This page configures CFM domain.

Web Interface

To configure CFM domain in the web interface:

1. Click Configuration, CFM and Domain.
2. Enter domain, format, name, level and TLV option.
3. Click save.

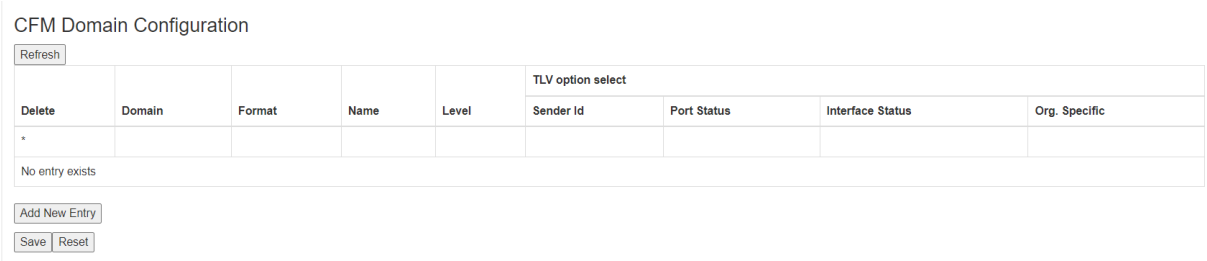


Figure 2-4.2: CFM Domain Configuration

Parameter description:

- **Domain :**

  Enter the name of Domain. Value is a single word which begins with an alphabetic letter A-Z or a-z with length 1-15

- **Format :**

  Select the MD name format. To mimic Y.1731 MEG IDs, Possible modes are:

  None
  String

- **Name:**

  The contents of this pamameter depends on the value of the format member.
  If format is None: Name is not used, but will be set to all-zeros behind the scenes. This format is typically used by Y.1731-kind-of-PDUs.
  If format is String: Name must contain a string from 1 to 43 characters long

- **Level:**

  MD/MEG level of this domain. Valid values are restricted to 0 - 7.

  About leak prevention
  Leak prevention is about discarding OAM PDUs with MEG levels lower than the MEP they hit when the OAM PDUs are ingressing the port on which the MEP resides, and to discard OAM PDUs with MEG levels at or lower than the MEP's when the OAM PDUs are ingressing other ports.
  There are two categories of architectures, when it comes to leak-prevention: Those that use Shared MEG level and those that use Independent MEG level:

  Shared MEG level
  On Shared MEG level architectures, Port Down MEPs always perform level filtering no matter which VLAN ID (VID) OAM PDUs get classified to, unless the same port has a VLAN MEP on the VID in question. So if you have a Port MEP in VID X and a VLAN MEP in VID Y, an OAM frame arriving on the port and gets classified to VID X or VID Z will be handled/level-filtered by the Port MEP, whereas an OAM frame ingressing the port in VID Y will be handled by the

VLAN MEP. Likewise, if the switch has a Port MEP on VID X on Port X and an OAM frame ingresses on VID Y on Port Y, it is subject to level filtering before egressing Port X, unless Port X also has a VLAN MEP on VID Y, in which case the VLAN MEP will take care of level-filtering the OAM PDU.
On Shared MEG level architectures, all Port MEPs must have the same MEG level and any VLAN MEP must have a MEG level higher than the Port MEPs' MEG level.

Independent MEG level
On Independent MEG level architectures, Port Down MEPs never perform level filtering on frames not classified to the MEP's VID. So if you have a Port MEP on VID X and a VLAN MEP on VID Y and an OAM frame ingresses any port on VID Z, it is not subject to handling/level-filtering by any of the two MEPs.

This switch exhibits Independent MEG level.

- **LTV Option Select:**

Sender ID
Default Sender ID TLV format to be used in CCMs generated by this Domain (may be overridden in service)
None: Do not include Sender ID TLVs.
Chassis: Enable Sender ID TLV and send Chassis ID (MAC Address).
Manage: Enable Sender ID TLV and send Management address (IPv4 Address).
ChassisManage: Enable Sender ID TLV and send both Chassis ID (MAC Address) and Management Address (IPv4 Address).
Defer: Let the global configuration decide if Sender ID TLVs shall be included (may be overridden in service).

Port Status:
Include or exclude Port Status TLV in CCMs generated by this Domain or let higher level determine (may be overridden in Service).
Disable: Do not include Port Status TLVs.
Enable: Include Port Status TLVs.
Defer: Let the global configuration decide if Port Status TLVs shall be included (may be overridden in Service).

Interface Status:
Include or exclude Interface Status TLV in CCMs generated by this Domain or let higher level determine (may be overridden in Service).
Disable: Do not include Interface Status TLVs.
Enable: Include Interface Status TLVs.
Defer: Let the global configuration decide if Interface Status TLVs shall be included (may be overridden in Service).

Org. Specific:
Exclude Organization-Specific TLV in CCMs generated by this Domain or let higher level determine (may be overridden in Service).
Disable: Do not include Organization-Specific TLVs.
Defer: Let the global configuration decide if Organization-Specific TLVs shall be included (may be overridden in Service).

Buttons

- **Add New Entry:**

  Click to add a new domain enter level

- **Save :**

  Click to save changes.

- **Reset :**

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

2-4.3 Service

This page configures CFM service parameters.

Web Interface

To configure CFM service in the web interface:

4. Click Configuration, CFM and Service.

5. Enter domain, format, name,VLAN, CCM interval and TLV option.

6. Click save.

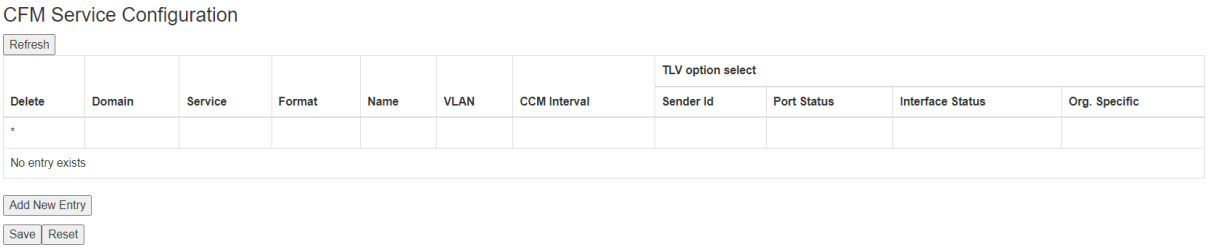


Figure 2-4.3: CFM Service Configuration

Parameter description:

- **Domain :**

  Select he name of Domain under which this Service resides.

- **Service:**

  Enter the name of Service. Value is a single word which begins with an alphabetic letter A-Z or a-z with length 1-15.

- **Format:**

  Select the short Service name format. This decides how the value of the Name parameter will be interpreted. To mimic Y.1731 MEG IDs, create an MD instance with an empty name and use Y1731 ICC or Y1731 ICC CC.
  Possible values are:
  String
  Two Octets
  Y1731 ICC
  Y1731 ICC CC
  Look under Name for explanation.

- **Name:**

  The contents of this parameter depends on the value of the format member. Besides the limitations explained for each of them, the following applies in general:
  If the Domain Format is None, the size of this cannot exceed 45 bytes.
  If the Domain Format is not None, the size of this cannot exceed 44 bytes.

  If Format is String, the following applies:
  length must be in range [1; 44]
  Contents must be in range [32; 126]

  If Format is Two Octets, the following applies:

  Name[0] and Name[1] will both be interpreted as unsigned 8-bit integers (allowing a range

of [0; 255]). Name[0] will be placed in the PDU before Name[1].
The remaining available bytes in name will not be used.

If Format is Y1731 ICC, the following applies:
length must be 13.
Contents must be in range [a-z,A-Z,0-9]
Y.1731 specifies that it is a concatenation of ICC (ITU Carrier Code) and UMC (Unique MEG ID Code):
ICC: 1-6 bytes
UMC: 7-12 bytes
In principle UMC can be any value in range [1; 127], but this API does not allow for specifying length of ICC, so the underlying code doesn't know where ICC ends and UMC starts.
The Domain Format must be None.

If Format is Y1731 ICC CC, the following applies:
length must be 15.
First 2 chars (CC): Must be amongst [A-Z]
Next 1-6 chars (ICC): Must be amongst [a-z,A-Z,0-9]
Next 7-12 chars (UMC): Must be amongst [a-z,A-Z,0-9]
There may be ONE (slash) present in name[3-7].
The Domain format must be None.

- **VLAN:**

  The MA's primary VID. A primary VID of 0 means that all MEPs created within this MA will be created as port MEPs (interface MEPs). There can only be one port MEP per interface. A given port MEP may still be created with tags, if that MEP's VLAN is non-zero."
  A non-zero primary VID means that all MEPs created within this MA will be created as VLAN MEPs. A given MEP may be configured with another VLAN than the MA's primary VID, but it is impossible to have untagged VLAN MEPs.

- **CCM Interval:**

  The CCM rate of all MEPs bound to this Service.

- **TLV Option Select:**

  Sender ID: Default Sender ID TLV format to be used in CCMs generated by this Service.
  None: Do not include Sender ID TLVs.
  Chassis: Enable Sender ID TLV and send Chassis ID (MAC Address).
  Manage: Enable Sender ID TLV and send Management address (IPv4 Address).
  ChassisManage: Enable Sender ID TLV and send both Chassis ID (MAC Address) and Management Address (IPv4 Address).
  Defer: Let the Domain configuration decide if Sender ID TLVs shall be included.

  Port Status: Include or exclude Port Status TLV in CCMs generated by this Service or let higher level determine.
  Disable: Do not include Port Status TLVs.
  Enable: Include Port Status TLVs.
  Defer: Let the Domain configuration decide if Port Status TLVs shall be included.

  Interface Status: Include or exclude Interface Status TLV in CCMs generated by this Service or let higher level determine.
  Disable: Do not include Interface Status TLVs.
  Enable: Include Interface Status TLVs.
  Defer: Let the Domain configuration decide if Interface Status TLVs shall be included.

Org. Specific: Exclude Organization-Specific TLV in CCMs generated by this Service or let higher level determine.
Disable: Do not include Organization-Specific TLVs.
Defer: Let the Domain configuration decide if Organization-Specific TLVs shall be included.

Buttons

- **Add New Entry:**

  Click to add a new service entry

- **Save :**

  Click to save changes.

- **Reset :**

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

Configure CFM MEP parameters on this page.

This switch supports two types of MEP: Port Down-MEPs and VLAN Down-MEPs.

Port Down-MEPs

In 802.1Q terminology, Port MEPs are located below the EISS entity, that is, closest to the physical port. Port MEPs are used by e.g. APS for protection purposes.
Port MEPs are created when the encompassing service has type "Port".
Port MEPs may send OAM PDUs tagged or untagged. An OAM PDU will be sent untagged only if the MEP's VLAN is set to "Inherit" (0). Any other value will cause it to be sent tagged with the port's TPID, whether or not the VLAN matches the port's PVID and that PVID is meant to be sent untagged.

VLAN Down-MEPs

in 802.1Q terminology, VLAN MEPs are located above the EISS entity.
This means that tagging of OAM PDUs will follow the port's VLAN configuration.
Thus, if a VLAN MEP is created on the Port's PVID and PVID is configured to be untagged, OAM PDUs will be transmitted untagged.
VLAN MEPs are created when the encompassing service has type "VLAN".

Down-MEP creation rules

There are a few rules to obey when creating Down-MEPs:

1. There can only be one Port MEP on the same port.
2. There can only be one VLAN MEP on the same port and VLAN.
3. A VLAN MEP must have a higher MD/MEG level than a Port MEP on the same port and VLAN.
4. All Port MEPs must have the same MD/MEG level
5. Any VLAN MEP must have an ME/MEG level higher than a Port MEP

These checks are performed automatically on administratively enabled MEPs when you change a particular MEP, change the Service Type from Port to VLAN or vice versa, or change the domain's MD/MEG level.

Web Interface

To configure CFM MEP in the web interface:

1. Click Configuration, CFM and CFM MEP configuration.
2. Enter domain, service, MEPID, direction, port, LAN, PCP, SMAC, alarm control, state control and remote MEP ID.
3. Click save.

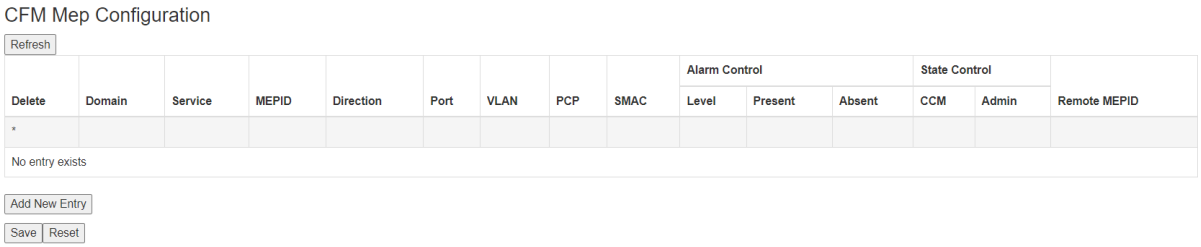


Figure 2-4.4: CFM MEP Configuration

Parameter description:

- **Delect :**

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

- **Domain :**

  Enter the name of Domain under which this MEP resides.

- **Service :**

  Name of Service under which this MEP resides.

- **MEPID:**

  The identification of this MEP. Must be an integer [1..8091]

- **Direction:**

  Set whether this MEP is an Up- or a Down-MEP.

- **Port:**

  Port on which this MEP resides.

- **VLAN:**

  VLAN ID. Use the value 0 to indicate untagged traffic (implies a port MEP)..

- **PCP:**

  Choose PCP value in PDUs' VLAN tag. Not used if untagged.

- **SMAC:**

  Set a Source MAC address to be used in CCM PDUs originating at this MEP. Must be a unicast address. Format is XX:XX:XX:XX:XX:XX. If all-zeros, the switch port's MAC address will be used instead.

- **Alarm Control:**

  Level: If a defect is detected with a priority higher than this level, a fault alarm notification will be generated.
  Valid range is [1; 6] with 1 indicating that any defect will cause a fault alarm and 6 indicating that no defect can cause a fault alarm. See 802.1Q-2018, clause 20.9.5, LowestAlarmPri
  The possible defects and their priorities are:

Short name	Description	Priority
DefRDICCM	Remote Defect Indication	1
DefMACstatus	MAC Status	2

DefRemoteCCM	Remote CCM	3
DefErrorCCM	Error CCM Received	4
DefXconCCM	Cross Connect CCM Received	5

Present: The time in milliseconds that defects must be present before a fault alarm notification is issued. Default is 2500 ms.

Absent: The time in milliseconds that defects must be absent before a fault alarm notification is reset. Default is 10000 ms.

Present: The time in milliseconds that defects must be present before a fault alarm notification is issued. Default is 2500 ms.

Absent: The time in milliseconds that defects must be absent before a fault alarm notification is reset. Default is 10000 ms.

- **State Control:**

  CCM: Enable or disable generation of continuity-check messages (CCMs)
  Admin: Enable or disable this MEP. When this MEP is enabled, it will check received/missing CCMs and can raise defects.

- **Remote MEPID:**

  Specify the Remote MEP that this MEP is expected to receive CCM PDUs from. Must be an integer [0..8091] where 0 means undefined. The value of Remote MEPID must be different from the value of MEPID.

Buttons

- **Add New Entry:**

  Click to add a new MEP entry

- **Save :**

  Click to save changes.

- **Reset :**

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

2-5 ERPS

The section describes to configure the ERPS.

Web Interface

To configure ERPS mode in the web interface:

1. Click Configuration and ERPS.
2. Click ⊕ to add a ERPS
3. Configure the ERPS parameters
4. Click Save.

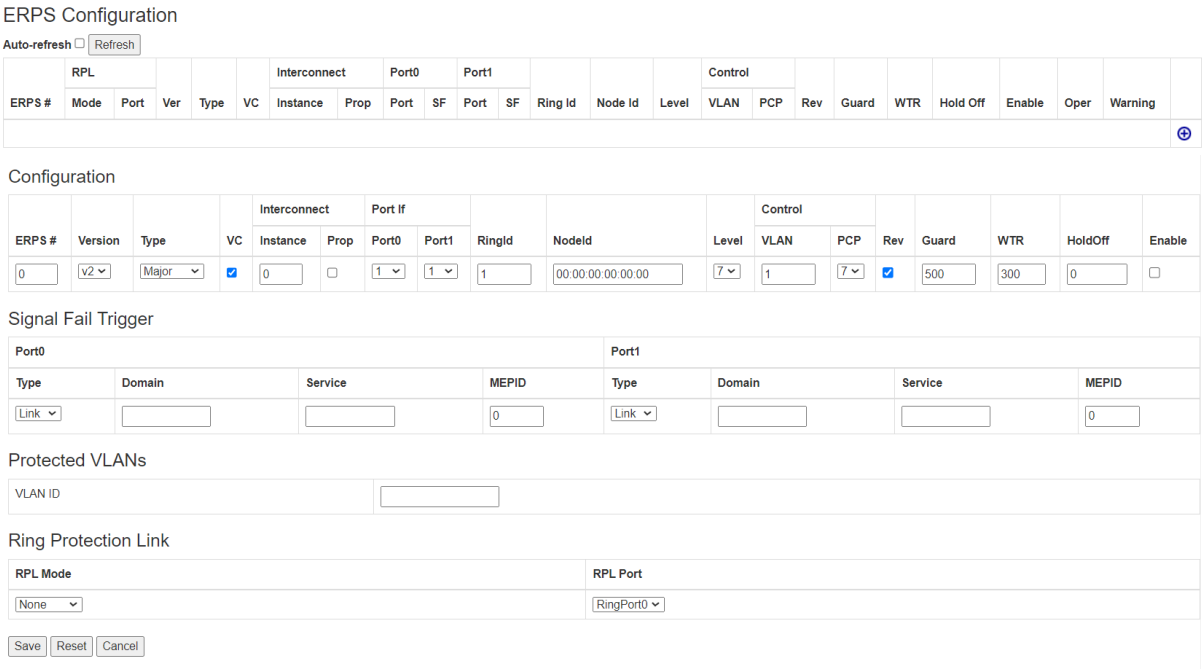


Figure 2-5: The ERPS Configuration

Parameter description:

- **ERPS# :**

  The ID of ERPS. The allowed value is from 1 - 64.

- **ERPS :**

  ERPS protocol version. v1 and v2 are supported.

- **Type :**

  Type of ring. Possible values:

  Major: ERPS major ring (G.8001-2016, clause 3.2.39)

  Sub: ERPS sub-ring (G.8001-2016, clause 3.2.66)

  InterSub: ERPS sub-ring on an interconnection node (G.8001-2016, clause 3.2.66)

- **VC :**

  Controls whether to use a Virtual Channel with a sub-ring.

- **Interconnect Instance:**

For a sub-ring on an interconnection node, this must reference the instance ID of the ring to which this sub-ring is connected.

- **Interconnect Prop:**

  Controls whether the ring referenced by Interconnect Instance shall propagate R-APS flush PDUs whenever this sub-ring's topology changes.

- **Ring ID :**

  The Ring ID is used - along with the control VLAN - to identify R-APS PDUs as belonging to a particular ring.

- **Node ID:**

  The Node ID is used inside the R-APS specific PDU to uniquely identify this node (switch) on the ring.

- **Level :**

  MD/MEG Level of R-APS PDUs we transmit.

- **Control VLAN :**

  The VLAN on which R-APS PDUs are transmitted and received on the ring ports.

- **Control PCP:**

  The PCP value used in the VLAN tag of the R-APS PDUs.

- **Rev:**

  Revertive (true) or Non-revertive (false) mode.

- **Guard :**

  Guard time in ms. Valid range is 10 - 2000 ms.

- **WTR:**

  Wait-to-Restore time in seconds. Valid range 1 - 720 sec.

- **Hold Off :**

  Hold off time in ms. Value is rounded down to 100ms precision. Valid range is 0 - 10000 ms.

- **Enable:**

  The administrative state of this ERPS. Check to make it function normally and uncheck to make it cease functioning.

  Signal Fail Trigger

- **Type :**

  Selects whether Signal Fail (SF) comes from the link state of a given interface, or from a Down-MEP.

- **Domain, Service, MEPID :**

  Identification of the MEP instance to provide Signal Fail, if Type is MEP.

  Protected VLANs

  VLANs which are protected by this ring instance. At least one VLAN must be protected. Specify as a comma separated list of vlan numbers or vlan ranges. Ex.: 1,4,7,30-70

  Ring Protection Link

- **RPL Mode :**

  Ring Protection Link mode. One of

None: This switch doesn't have the RPL port in the ring

Owner: This switch is RPL owner for the ring (G.8001-2016, clause 3.2.61)

Neighbor: This switch is RPL neighbor for the ring (G.8001-2016, clause 3.2.60)

- **RPL Port:**

  Indicates whether it is port0 or port1 that is the Ring Protection Link. Not used if RPL Mode is None.

Configuration Buttons

You can modify each APS in the table using the following buttons:
: Edits the ERPS.
: Deletes the ERPS
: Adds new ERPS

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.

- **Auto-Refresh:**

  Check this box to refresh the page automatically.

- **Refresh:**

  Click to refresh the page immediately.

2-6 MRP

The section describes to configure MRP instances

Web Interface

To configure MRP in the web interface:

1. Click Configuration and MRP.
2. Click ⊕ to add a MRP
3. Select the MRP parameters
4. Click Save.

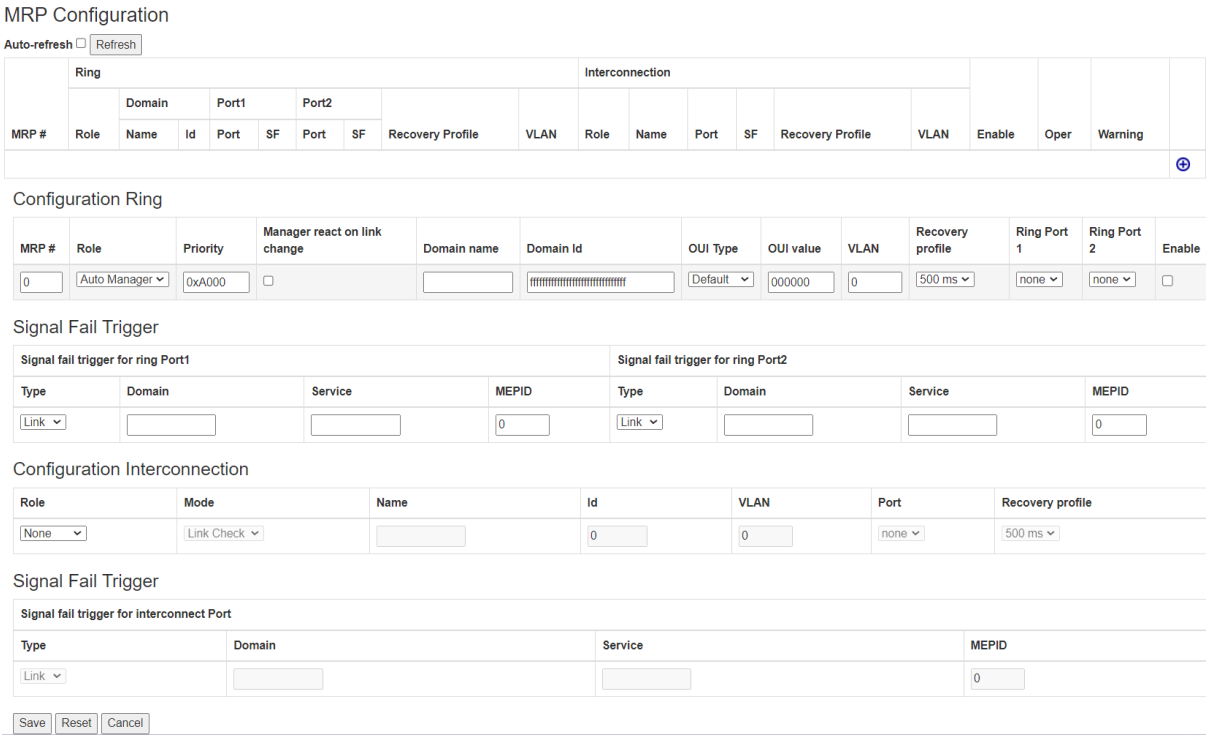


Figure 2-6: The MRP Configuration

Parameter description:

- **MRP#:**

  The ID of MRP. Valid range 1 - 2.

  Configuration Buttons

  You can modify each APS in the table using the following buttons:
  : Edits the ERPS.
  : Deletes the ERPS
  : Adds new ERPS

  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.

- **Auto-Refresh:**

  Check this box to refresh the page automatically.

- **Refresh:**

  Click to refresh the page immediately.

2-7 DHCPv4

The section describes to configure the DHCP Snooping parameters of the switch. The DHCP Snooping can prevent attackers from adding their own DHCP servers to the network.

2-7.1 Server

2-7.1.1 Mode

This page configures global mode and VLAN mode to enable/disable DHCP server per system and per VLAN.

Web Interface

To configure DHCPv4 server mode in the web interface:

5. Click Configuration, DHCPv4, Server and Mode.
6. Select "Enabled" in the Global Mode of DHCP Server Mode Configuration.
7. Add Vlan range.
8. Click Save.

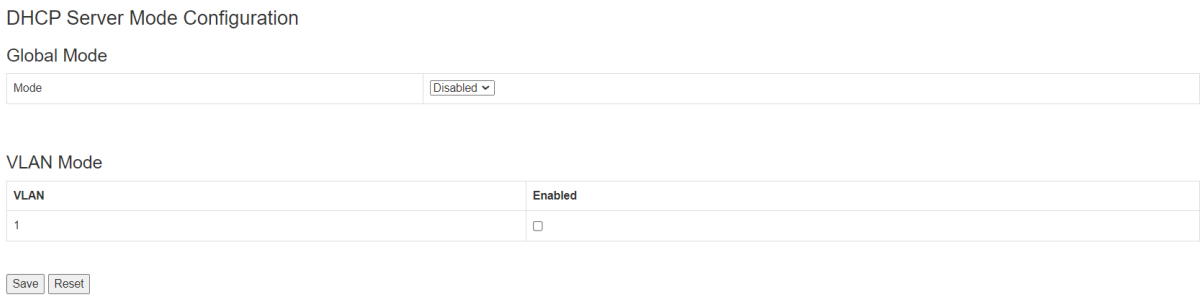


Figure 2-7.1.1: The DHCP server Mode

Parameter description:

- **Mode :**

  Configure the operation mode per system. Possible modes are:
  Enable: Enable DHCP server per system.
  Disable: Disable DHCP server pre system.

- **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 existed VLAN range, then you can follow the steps.

  1. press "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 Apply 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:
Enable: Enable DHCP server per VLAN.
Disable: Disable DHCP server pre VLAN.

Buttons

- **Add VLAN Range :**

  Click to add a new VLAN range.

- **Save :**

  Click to save changes.

- **Reset :**

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

2-7.1.2 Excluded IP

This page configures excluded IP addresses. DHCP server will not allocate these excluded IP addresses to DHCP client.

Web Interface

To configure DHCP server excluded IP in the web interface:

1. Click Configuration, DHCPv4, Server and Excluded IP.
2. Click Add IP Range then you can create new IP Range on the switch.
3. Click Save.

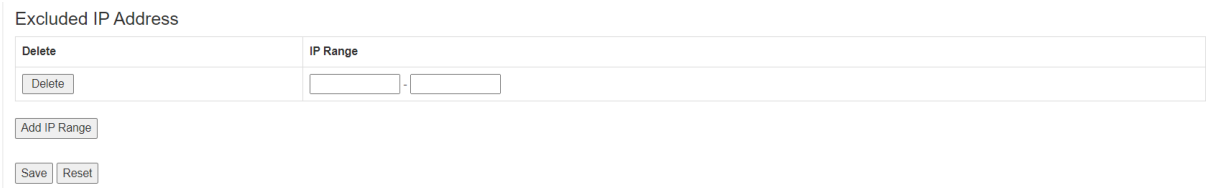


Figure 2-7.1.2: The DHCPv4 server excluded IP

Parameter description:

- **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

- **Delete :**

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

- **Add IP Range :**

  Click to add a new excluded IP range.

- **Save:**

  Click to save changes.

- **Reset :**

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

2-7.1.3 Pool

This page manages DHCP pools. According to the DHCP pool, DHCP server will allocate IP address and deliver configuration parameters to DHCP client.

Web Interface

To configure DHCP server pool in the web interface:

1. Click Configuration, DHCP, Server and Pool.
2. Click Add New Pool then you can create new Pool on the switch.
3. Click Save.

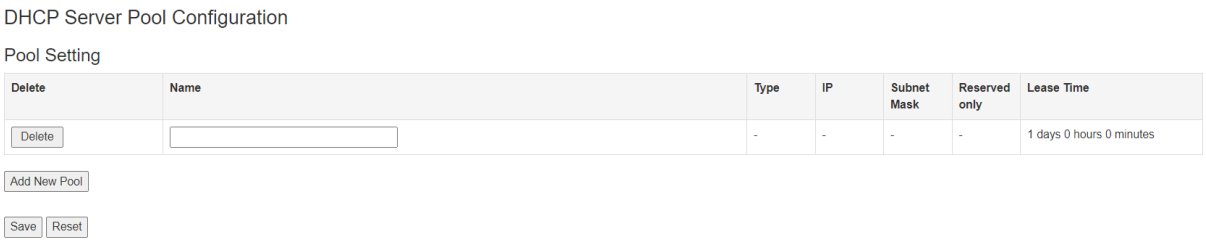


Figure 2-7.1.3: The DHCPv4 server pool

Parameter description:

Pool Setting

Add or delete pools.

Adding a pool and giving a name is to create a new pool with "default" configuration. If you want to configure all settings including type, IP subnet mask and lease time, you can click the pool name to go into the configuration page.

- **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.

- **Reserved Only :**

  If on, Ip addresses optainable from the pool are limited to those entered into the reserved entries table.

- **Lease Time :**

  Display lease time of the pool.

Buttons

- **Delete :**

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

- **Add New Pool :**

  Click to add a new DHCP pool.

- **Save:**

  Click to save changes.

- **Reset :**

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

2-7.2 Snooping

DHCP Snooping is used to block intruder on the untrusted ports of the switch device when it tries to intervene by injecting a bogus DHCP reply packet to a legitimate conversation between the DHCP client and server.

The section describes to configure the DHCP Snooping parameters of the switch. The DHCP Snooping can prevent attackers from adding their own DHCP servers to the network.

Web Interface

To configure DHCP snooping in the web interface:

1. Click Configuration, DHCPv4 and Snooping.
2. Select “Enabled” in the Mode of DHCP Snooping Configuration.
3. Select “Trusted” of the specific port in the Mode of Port Mode Configuration.
4. Click Save.

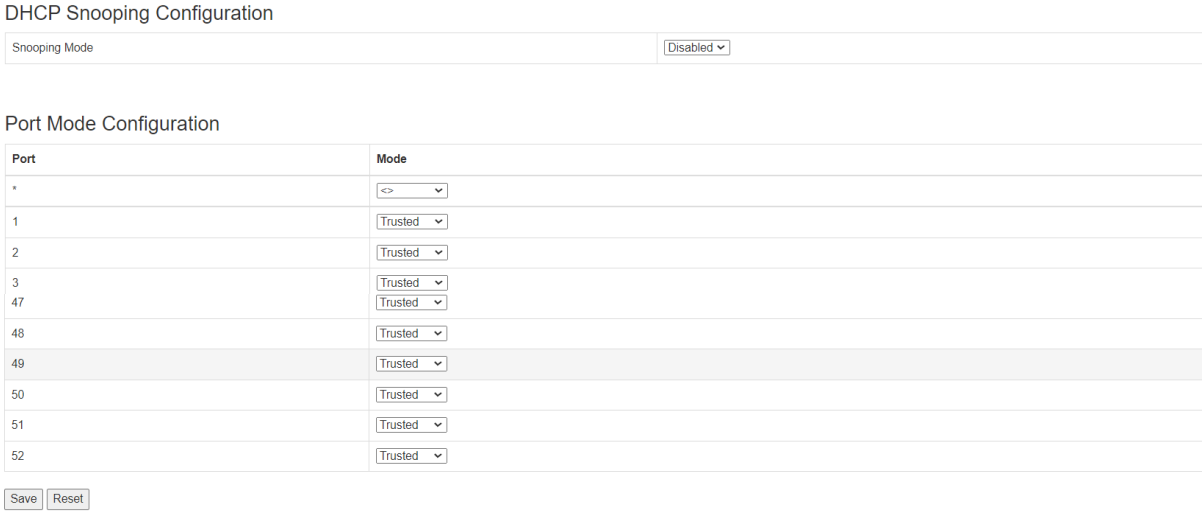


Figure 2-7.2: The DHCPv4 Snooping Configuration

Parameter description:

- **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**

  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.

2-7.3 Relay

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.

Web Interface

To configure DHCP Relay in the web interface:

1. Click Configuration, DHCPv4 and Relay
2. Specify the Relay Mode, Relay server, Relay Information Mode, Relay Information police.
3. Click Save.

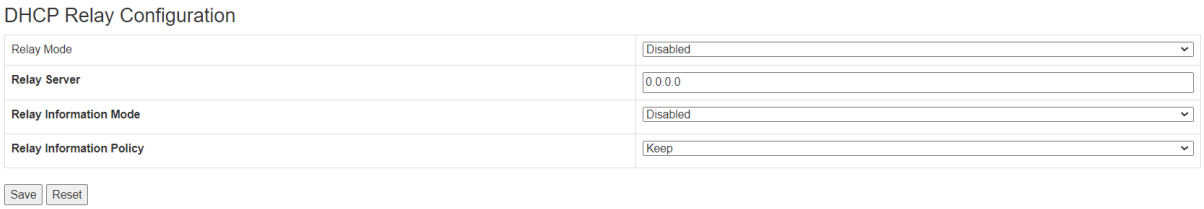


Figure 2-7.3: The DHCPv4 Relay Configuration

Parameter description:

- **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.

2-8 DHCPv6

The section describes to configure the DHCPv6 Snooping parameters of the switch. The DHCP Snooping can prevent attackers from adding their own DHCP servers to the network.

2-8.1 Snooping

Configure DHCPv6 (aka. DHCP over IPv6) Snooping on this page.

Web Interface

To configure DHCP snooping in the web interface:

1. Click Configuration, DHCPv6 and Snooping.
2. Select “Enabled” in the Mode of DHCP Snooping Configuration.
3. Select to drop/ allow the unknown IPv6 Next-Headers
4. Select “Trusted” of the specific port in the Mode of Port Mode Configuration.
5. Click Save.

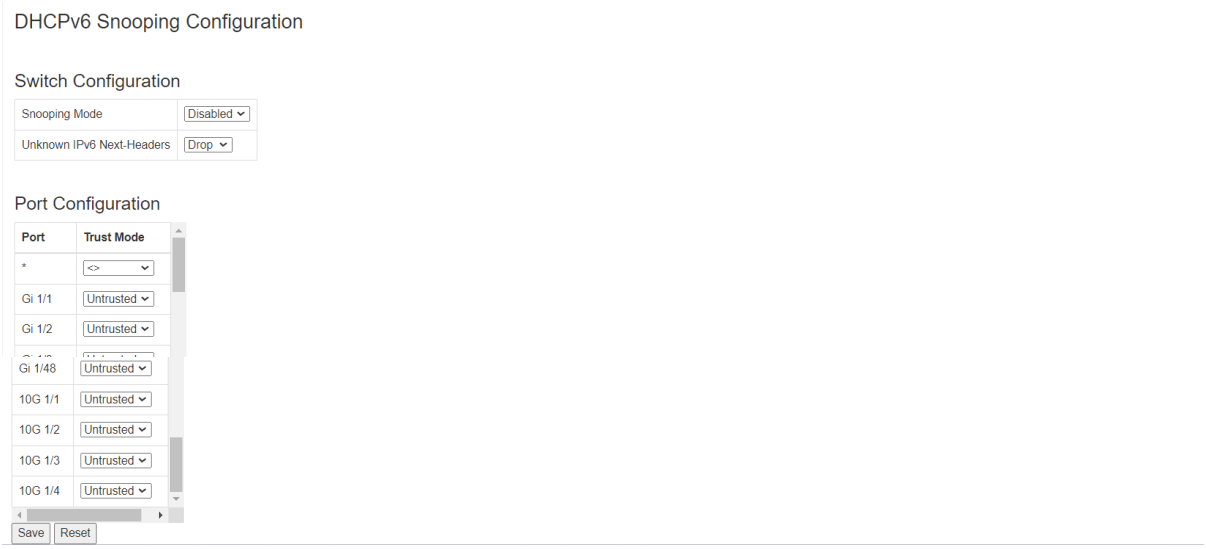


Figure 2-8.1: The DHCP Snooping Configuration

Parameter description:

- **Snooping Mode :**

  Indicates the DHCPv6 snooping mode operation.
  Possible modes are:
  Enabled: Enable DHCPv6 snooping mode operation. When DHCPv6 snooping mode operation is enabled, the DHCPv6 client request messages will be forwarded to trusted ports and only allow reply packets from trusted ports.
  Disabled: Disable DHCP snooping mode operation.

- **Unknown IPv6 Next-Headers:**

  Indicates how Unknown IPv6 Next-Header values should be treated. The switch needs to parse all IPv6 packets to a DHCPv6 client to determine if it is in fact a DHCPv6 message. If an unknown IPv6 extension header is encountered the parsing cannot continue. See RFC 7610, section 5, item 3 for details.
  Possible options are:
  Drop: Drop packets with unknown IPv6 extension headers. This is the most secure option but may result in traffic disruptions.
  Allow: Allow packets with unknown IPv6 extension headers. This is a less secure option but prevents traffic disruptions.

- **Port Mode Configuration**

  Indicates the DHCPv6 snooping port mode.
  Possible port modes are:
  Trusted: Configures the port as trusted source of the DHCPv6 messages.
  Untrusted: Configures the port as untrusted source of the DHCPv6 messages.

Buttons

- **Save :**

  Click to save changes.

- **Reset :**

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

2-8.2 Relay

In this page it is possible to configure DHCPv6 Relay for a specific vlan.

Web Interface

To configure DHCPv6 Relay in the web interface:

1. Click Configuration, DHCPv6 and Relay
2. Clikc “Add New Entry’ to add a relay configuration
3. Specify the interface, relay interface and relay desitination
4. Click Save.

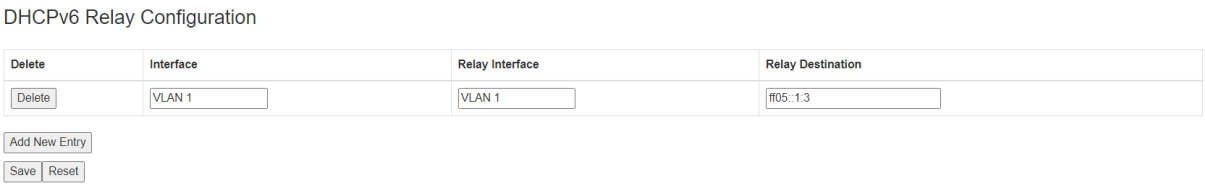


Figure 2-8.2: The DHCPv6 Relay Configuration

Parameter description:

- **Interface :**

  Interface identification.

- **Relay Interface :**

  Interface identification. The id of the interface used for relaying.

- **Relay Destination :**

  An IPv6 address represented as human readable test as specified in RFC5952. The IPv6 address of the DHCPv6 server that requests shall be relayed to. The default value 'ff05::1:3' mans 'any DHCP server'.

Buttons

- **Add New Entry :**

  Click to add a new entry.

- **Save:**

  Click to save changes.

- **Reset :**

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

2-9 Security

This section shows you to configure the Port Security settings of the Switch. You can use the Port Security feature to restrict input to an interface by limiting and identifying MAC addresses.

2-9.1 Switch

2-9.1.1 Users

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

Web Interface

To configure User in the web interface:

1. Click Configuration, Security, Switch and Users.
2. Click Add new user
3. Specify the User Name parameter.
4. Click Save.

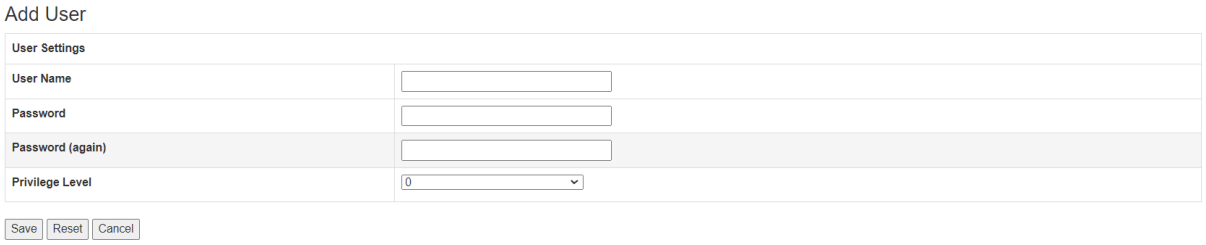


Figure 2-9.1.1: The Users configuration

Parameter description:

- **User Name :**

  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 is 0 to 31. Any printable characters including space is accepted.

- **Password (again) :**

  To type the password again. You must type the same password again in the field.

- **Privilege Level :**

  The privilege level of the user. The allowed range is 0 to 5. If the privilege level value is 5, it can access all groups, i.e. that is granted the fully control of the device. But others 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 1 has the read-only access and privilege level 3 has the read-write access. And the system maintenance (software upload, factory defaults and etc.) need user privilege level 5. Generally, the privilege level 5 can be used for an administrator account, privilege level 3 for a standard user account and privilege level 1 for a guest account.

Buttons

- **Save :**

  Click to save changes.

- **Reset :**

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

- **Cancel :**

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

- **Delete User :**

  Delete the current user. This button is not available for new configurations (Add new user)

This page provides an overview of the privilege levels. The switch provides user set Account, Aggregation, Diagnostics, EEE, GARP, GVRP,IP, IPMC Snooping LACP LLDP LLDP MED MAC Table MRP MVR MVRP Maintenance Mirroring Ports Private VLANs QoS SMTP SNMP Security Spanning Tree System Trap Event VCL VLANs Voice VLAN Privilege Levels from 1 to 15 .

Web Interface

To configure Privilege Level in the web interface:

1. Click Configuration, Security, Switch and Privilege Levels.
2. Specify the Privilege parameter.
3. Click Save.

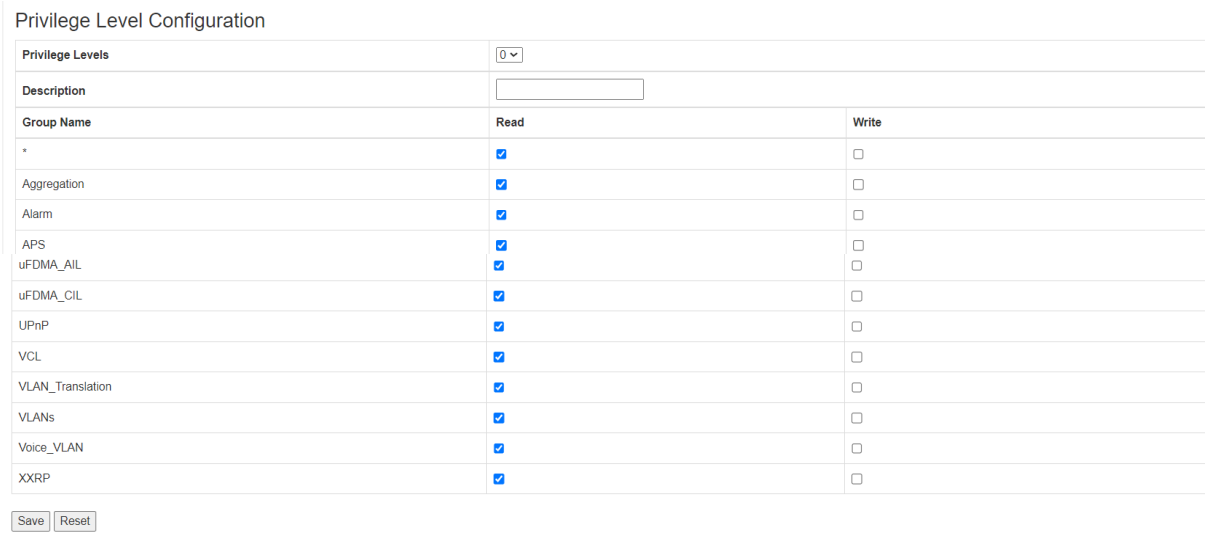


Figure2-9.1.2: The Privilege Level configuration

Parameter description:

- **Group Name :**

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

  System: Contact, Name, Location, Timezone, Daylight Saving Time, Log.

  Security: Authentication, System Access Management, Port (contains Dot1x port, MAC based and the MAC Address Limit), ACL, HTTPS, SSH, ARP Inspection, IP source guard.

  IP: Everything except 'ping'.

  Port: Everything except 'VeriPHY'.

  Diagnostics: 'ping' and 'VeriPHY'.

  Maintenance: CLI- System Reboot, System Restore Default, System Password, Configuration Save, Configuration Load and Firmware Load. Web- Users, Privilege Levels and everything in Maintenance.

Debug: Only present in CLI.

- **Privilege Levels :**

  The Privilege Levels can be configured between 0 to 5 (where 0 is lowest level and 5 is highest level) Every group has an authorization Privilege level for the following sub groups: read and write(e.g. for clearing of statistics). User Privilege should be same or greater than the authorization Privilege level to have the access to that group.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

This page shows how to configure a user with authenticated when he logs into the switch via one of the management client interfaces.

Web Interface

To configure an Authentication Method Configuration in the web interface:

1. Click Configuration, Security, Switch and Auth Method.
2. Specify the Client (console, telent, ssh, http) which you want to monitor.
3. Specify the command Authentication Method
4. Specif accounting method.
5. Click Save

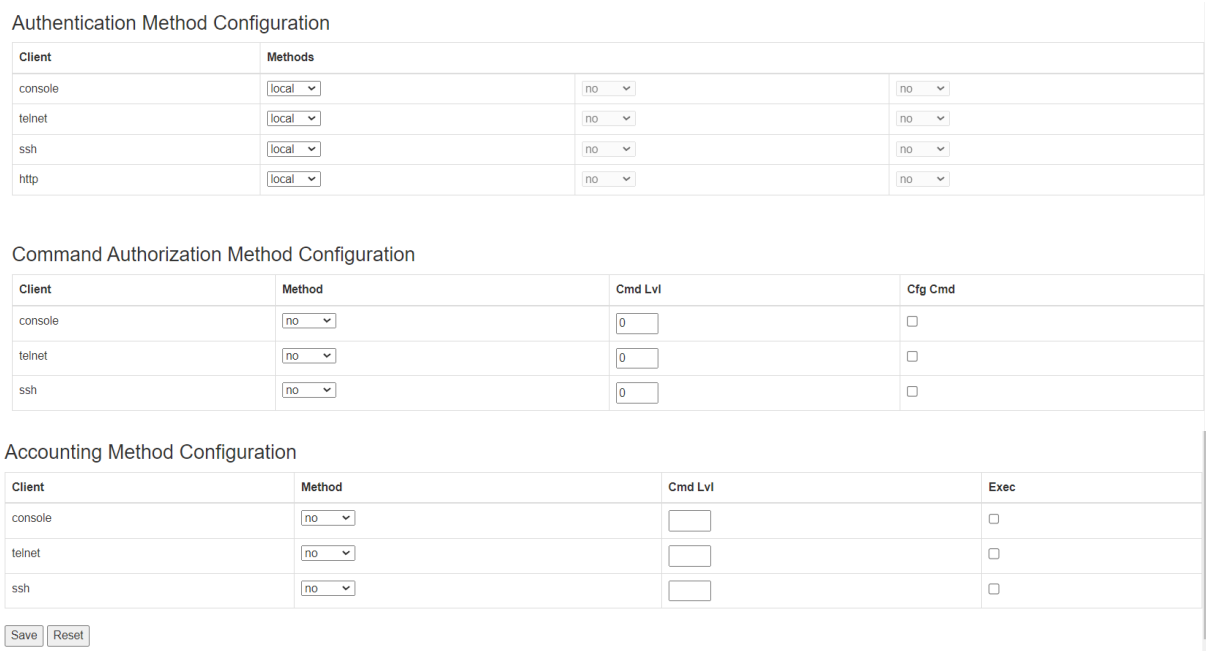


Figure 2-9.1.3: The Authentication Method Configuration

Parameter description:

Authentication Method Configuration Help

- **Client :**

  The management client for which the configuration below applies.

- **Authentication Method :**

  Authentication 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 : use a remote RADIUS server for authentication.
  - tacacs : use a remote TACACS+ server 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 login via the local user database if none of the configured authentication servers are alive.

Command Authorization Method Configuration Help

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:

- **Client :**

  The management client for which the configuration below applies.

- **Method:**

  Method can be set to one of the following values:

  no: Command authorization is disabled. User is granted access to CLI commands according to his privilege level.

  tacacs: Use remote TACACS+ server(s) for command authorization. If all remote servers are offline, the user is granted access to CLI commands according to his privilege level.

- **Cmd Lvl:**

  Authorize 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 authorize configuration commands.

Accounting Method Configuration Help

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:

- **Client :**

  The management client for which the configuration below applies.

- **Method:**

  Method can be set to one of the following values:

  no: Accounting is disabled.

  tacacs: Use remote TACACS+ server(s) for accounting.

- **Cmd Lvl:**

  Enable accounting 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.Enable accounting 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 :**

  Enable exec (login) accounting.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

This section shows you to configure SSH of the Switch.

Web Interface

To configure an SSH in the web interface:

1. Click Configuration, Security, Switch and SSH.
2. Select “Enabled” in the Mode of SSH
3. Click Save.

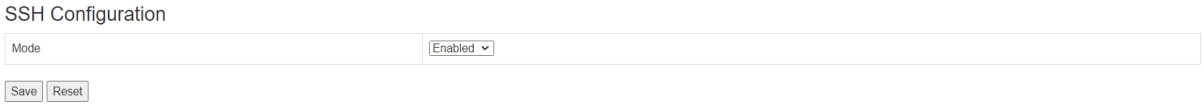


Figure 2-9.1.4: The SSH Configuration

Parameter description:

- **Mode :**

  Indicates the SSH mode operation. Possible modes are:
  Enabled: Enable SSH mode operation.
  Disabled: Disable SSH mode operation

Buttons

- **Save :**

  Click to save changes.

- **Reset :**

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

2-9.1.5 HTTPS

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

Web Interface

To configure an Access Management Configuration in the web interface:

1. Click Configuration, Security, Switch and HTTPS.
2. Select “Enabled” in the Mode.
3. Select “Enabled/Disabled” the automatic redirect
4. Select the certificate maintain mode
5. Click Save

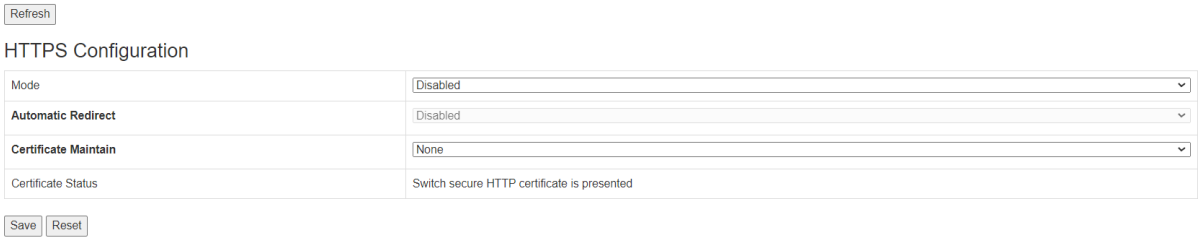


Figure 2-9.1.5,: The HTTPS Configuration

Parameter description:

- **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 "HTTPS Mode Enabled" 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 :**

  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>. For example, tftp://10.10.10.10/new_image_path/new_image.dat, http://username:password@10.10.10.10:80/new_image_path/new_image.dat. A valid file name is a text string drawn from alphabet (A-Za-z), digits (0-9), 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.

- **Certificate Status:**

  Display the current status of certificate on the switch.Possible statuses are:
  Switch secure HTTP certificate is presented.
  Switch secure HTTP certificate is not presented.
  Switch secure HTTP certificate is generating ....

Buttons

- **Refresh :**

  Click to refresh the page. Any changes made locally will be undone.

- **Apply :**

  Click to save changes.

- **Reset :**

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

This section shows you to configure access management table of the Switch including HTTP/HTTPS, SNMP, and TELNET/SSH. You can manage the Switch over an Ethernet LAN, or over the Internet. The maximum number of entries is 16. If the application's type match any one of the access management entries, it will allow access to the switch.

Web Interface

To configure an Access Management Configuration in the web interface:

1. Click Configuration, Security, Switch and Access Management.
2. Select “Enabled” in the Mode of Access Management Configuration.
3. Click “Add new entry”.
4. Specify the Start IP Address, End IP Address.
5. Checked Access Management method (HTTP/HTTPS, SNMP, and TELNET/SSH) in the entry.
6. Click Sa e.

Figure 2-9.1.6: The Access Management Configuration

Parameter description:

- **Mode :**

  Indicates the access management mode operation. Possible modes are:

  Enabled: Enable access management mode operation.

  Disabled: Disable access management mode operation.

- **VLAN ID :**

  Indicates the VLAN ID for the access management entry.

- **Start IP address :**

  Indicates the start IP address for the access management entry.

- **End IP address :**

  Indicates 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

- **Delete :**

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

- **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.

2-9.1.7 SNMP

Any Network Management System (NMS) running the Simple Network Management Protocol (SNMP) can manage the Managed devices equipped with SNMP agent, provided that the Management Information Base (MIB) is installed correctly on the managed devices. The SNMP is a protocol that is used to govern the transfer of information between SNMP manager and agent and traverses the Object Identity (OID) of the management Information Base (MIB), described in the form of SMI syntax. SNMP agent is running on the switch to response the request issued by SNMP manager.

Basically, it is passive except issuing the trap information. The switch supports a switch to turn on or off the SNMP agent. If you set the field SNMP "Enable", SNMP agent will be started up. All supported MIB OIDs, including RMON MIB, can be accessed via SNMP manager. If the field SNMP is set "Disable", SNMP agent will be de-activated, the related Community Name, Trap Host IP Address, Trap and all MIB counters will be ignored.

2-9.1.7.1 System

This section describes how to configure SNMP System on the switch. This function is used to configure SNMP settings, community name, trap host and public traps as well as the throttle of SNMP. A SNMP manager must pass the authentication by identifying both community names, then it can access the MIB information of the target device. So, both parties must have the same community name. Once completing the setting, click <Apply> button, the setting takes effect.

Web Interface

To configure the configure SNMP System in the web interface:

1. Click Configuration, Security, Switch, SNMP and System.
2. Evoke SNMP State to enable or disable the SNMP function.
3. Specify the Engine ID
4. Click Save.

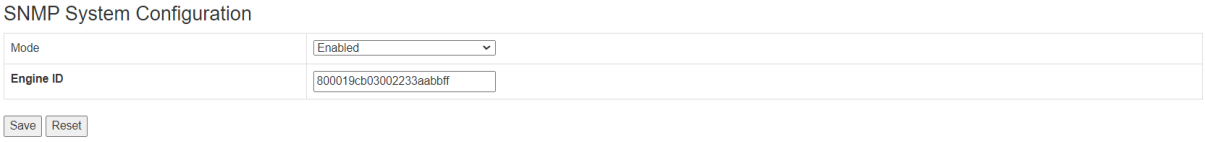


Figure 2-9.1.7.1: The SNMP System Configuration

Parameter description:

- **Mode :**

  Indicates the SNMP mode operation. Possible modes are:

  Enabled: Enable SNMP mode operation.

  Disabled: Disable SNMP mode operation.

- **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.

2-9.1.7.2 Trap

Configure SNMP trap on this page.

2-9.1.7.2.1

Configure trap destination on this page

Web Interface

To configure the configure SNMP Trap Configuration in the web interface:

1. Click Configuration, Security, Switch, SNMP, Trap and Destination.
2. Click Add New Entry then you can create new SNMP Trap on the switch.
3. Click Save

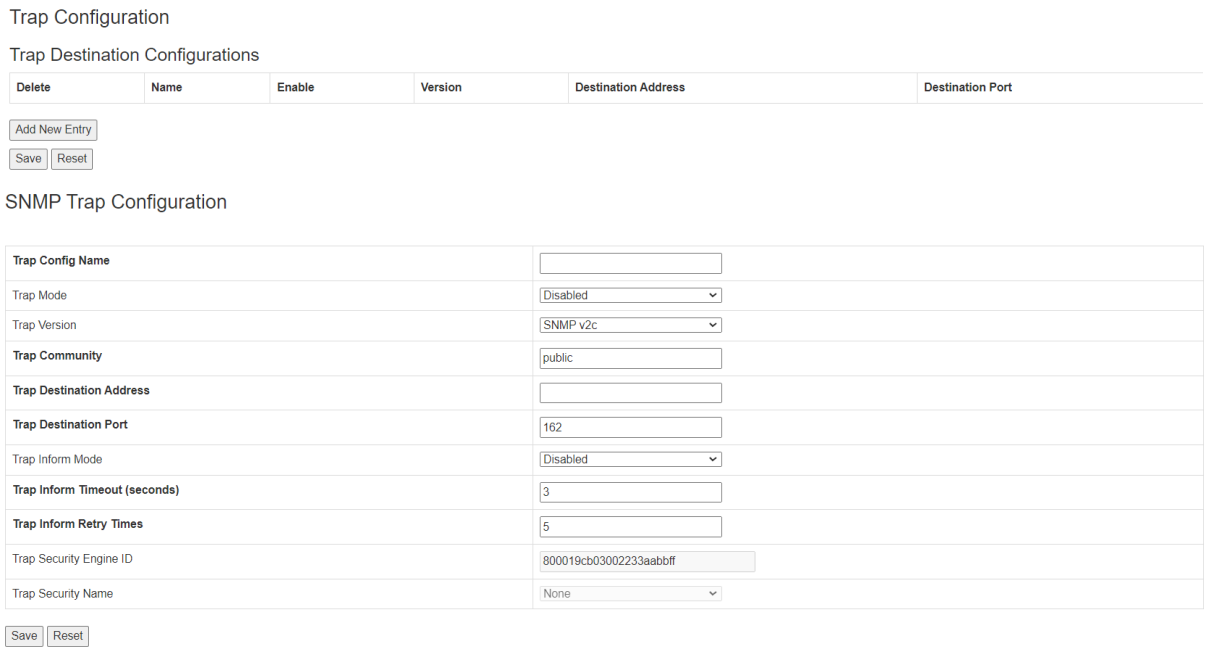


Figure 2-9.1.7.2.1: The SNMP Trap Configuration

Parameter description:

- **Name :**

  Indicates the trap Configuration's name. Indicates the trap destination's name.

- **Enable :**

  Indicates the trap destination mode operation. Possible modes are:
  Enabled: Enable SNMP trap mode operation.
  Disabled: Disable SNMP trap mode operation.

- **Version :**

  Indicates the SNMP trap supported version. Possible versions are:
  SNMPv1: Set SNMP trap supported version 1.
  SNMPv2c: Set SNMP trap supported version 2c.

  SNMPv3: Set SNMP trap supported version 3.

- **Destination Address :**

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

  And it also allow a valid hostname. A valid hostname is a string drawn from the alphabet (A-Za-z), digits (0-9), dot (.), dash (-). Spaces are not allowed, the first character must be an alpha character, and the first and last characters must not be a dot or a dash.

  Indicates the SNMP trap destination IPv6 address. 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. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.

- **Destination port :**

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

Buttons

- **Delete :**

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

- **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.

2-9.1.7.2.2

This page provides SNMP trap source configurations. A trap is sent for the given trap source if at least one filter with filter type included matches the filter, and no filters with filter type excluded matches.

The maximum entry count is 32.

Web Interface

To configure the configure SNMP Trap Configuration in the web interface:

1. Click Configuration, Security, Switch, SNMP Trap and source.
2. Click Add New Entry then you can create new SNMP Trap source on the switch.
3. Click Save

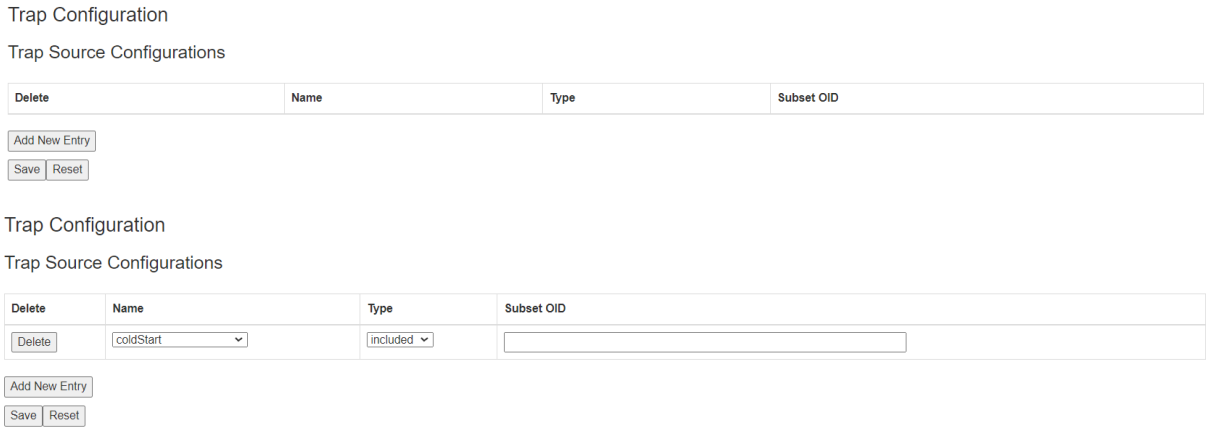


Figure 2-9.1.7.2.2: The SNMP Trap Configuration

Parameter description:

- **Name :**

  Indicates the name for the entry.

- **Type :**

  The filter type for the entry. Possible types are:
  included: An optional flag to indicate a trap is sent for the given trap source is matched.
  excluded: An optional flag to indicate a trap is not sent for the given trap source is matched.

- **Subset OID:**

  The subset OID for the entry. The value should depend on the what kind of trap name. For example, the ifIdex is the subset OID of linkUp and linkDown. A valid subset OID is one or more digital number(0-4294967295) or asterisk(*) which are separated by dots(.). The first character must not begin withasterisk(*) and the maximum of OID count must not exceed 128.

Buttons

- **Delete :**

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

- **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.

2-9.1.7.3 Communities

The function is used to configure SNMPv3 communities. The entry index key is Community.

Web Interface

To configure the SNMP Communities in the web interface:

1. Click Configuration, Security, Switch, SNMP and Communities.
2. Click Add new Entry.
3. Specify the SNMP community parameters.
4. Click Save.
5. If you want to modify or clear the setting then click Reset.

Figure 2-9.1.7.3: The SNMPv3 Communities Security Configuration

Parameter description:

- **Community Name :**

  Indicates the security name to map the community to the SNMP Groups configuration. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

- **Community Secret :**

  .Indicates the community secret (access string) to permit access using SNMPv1 and SNMPv2c to the SNMP agent. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

- **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 Prefix:**

  SNMP access source address prefix.

Buttons

- **Delete :**

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

- **Add New Entry :**

  Click to add a new entry.

- **Save :**

  Click to save changes.

- **Reset :**

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

2-9.1.7.4 Users

Configure SNMPv3 user table on this page. The entry index keys are Engine ID and User Name.

Web Interface

To configure the SNMP Users in the web interface:

1. Click Configuration, Security, Switch, SNMP and Users.
2. Click Add new Entry.
3. Specify the Privilege parameter.
4. Click Save.

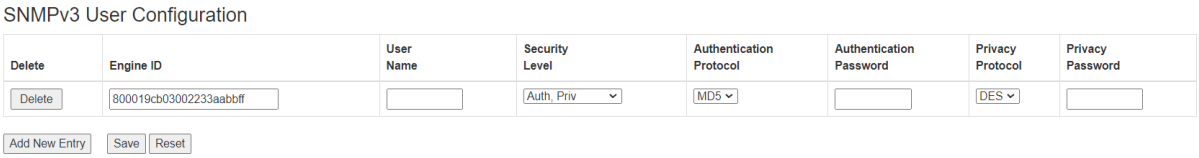


Figure 2-9.1.7.4: The SNMP Users Configuration

Parameter description:

- **Engine ID :**

  An octet 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 local user; otherwise it's remote user.

- **User Name :**

  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 it must first be ensured that the value is set correctly.

- **Authentication Protocol :**

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

  None: No authentication protocol.

  MD5: An optional flag to indicate that this user uses MD5 authentication protocol.

SHA: An optional flag to indicate that this user uses SHA authentication protocol.

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.

  AES: When available, 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

- **Delete :**

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

- **Add New Entry :**

  Click to add a new entry.

- **Save :**

  Click to save changes.

- **Reset :**

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

2-9.1.7.5 Groups

Configure SNMPv3 group table on this page. The entry index keys are Security Model and Security Name.

Web Interface

To configure the SNMP Groups in the web interface:

1. Click Configuration, Security, Switch, SNMP and Groups.
2. Click Add new Entry.
3. Specify the Privilege parameter.
4. Click Save.

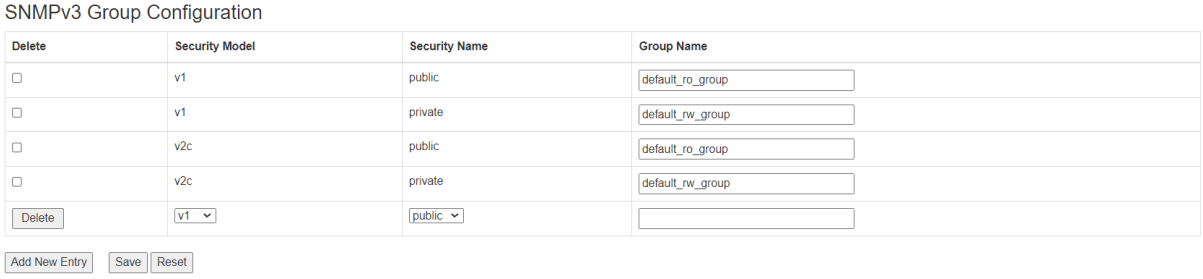


Figure 2-9.1.7.5: The SNMP Groups Configuration

Parameter description:

- **Security Model :**

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

  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

- **Delete :**

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

- **Add New Entry :**

  Click to add a new entry.

- **Save :**

  Click to save changes.

- **Reset :**

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

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

Web Interface

To configure the SNMP views in the web interface:

1. Click Configuration, Security, Switch, SNMP and Views.
2. Click Add New Entry.
3. Specify the SNMP View parameters.
4. Click Save.
5. If you want to modify or clear the setting then click Reset.

Figure 2-9.1.7.6: The SNMP Views Configuration

Parameter description:

- **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 allowed OID length is 1 to 128. The allowed string content is digital number or asterisk(*).

Buttons

- **Delete :**

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

- **Add New Entry :**

  Click to add a new entry.

- **Save :**

  Click to save changes.

- **Reset :**

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

The function is used to configure SNMPv3 access table on this page.The entry index keys are Group Name, Security Model and Security Level.

Web Interface

To configure the SNMP Access in the web interface:

1. Click Configuration, Security, Switch, SNMP and Accesses.
2. Click Add new Access.
3. Specify the SNMP Access parameters.
4. Click Save.
5. If you want to modify or clear the setting then click Reset.

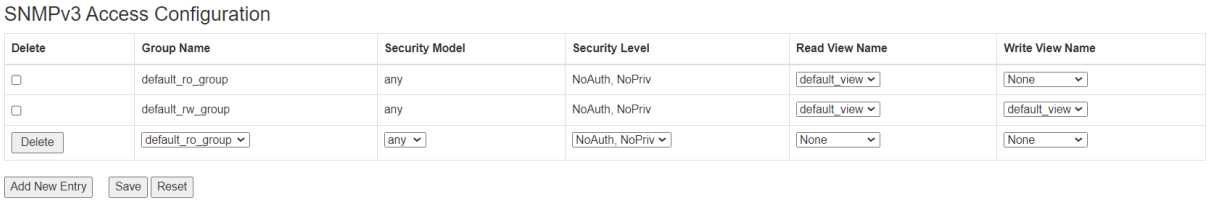


Figure 2-10.1.7.7: The SNMP Accesses Configuration

Parameter description:

- **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

- **Delete :**

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

- **Add New Entry :**

  Click to add a new entry.

- **Save :**

  Click to save changes.

- **Reset :**

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

2-9.1.6 RMON

An RMON implementation typically operates in a client/server model. Monitoring devices contain RMON software agents that collect information and analyze packets. These probes act as servers and the Network Management applications that communicate with them act as clients.

2-10.1.6.1 Statistics

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

Web Interface

To configure the RMON configuration in the web interface:

1. Click Configuration, Security, Switch, RMON and Statistics.
2. Click Add New Entry.
3. Specify the ID parameters.
4. Click Save.

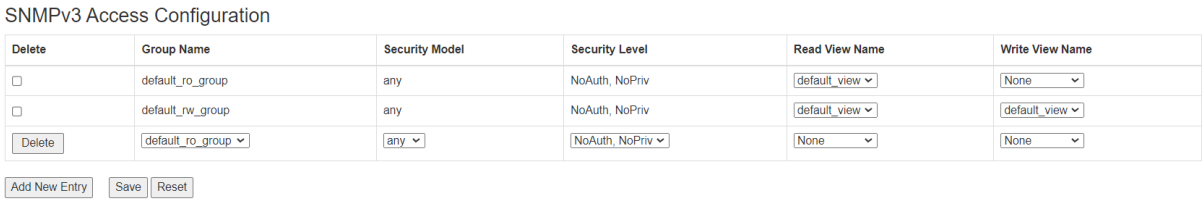


Figure 2-9.1.6.1: The RMON Statistics Configuration

Parameter description:

- **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 1000*(switch ID-1), for example, if the port is switch 3 port 5, the value is 2005

Buttons

- **Delete :**

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

- **Add New Entry :**

  Click to add a new entry.

- **Apply :**

  Click to save changes.

- **Reset :**

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

2-9.1.6.2 History

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

Web Interface

the RMON History in the web interface:

1. Click Configuration, Security, Switch, RMON and History.
2. Click Add New Entry.
3. Specify the ID parameters.
4. Click Save.

Figure 2-9.1.6.2: The RMON History Configuration

Parameter description:

- **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.

- **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

- **Delete :**

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

- **Add New Entry :**

  Click to add a new entry.

- **Save :**

  Click to save changes.

- **Reset :**

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

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

Web Interface

To display the configure RMON Alarm in the web interface:

1. Click Configuration, Security, Switch, RMON and Alarm.
2. Click Add New Entry.
3. Specify the ID parameters.
4. Click Save.

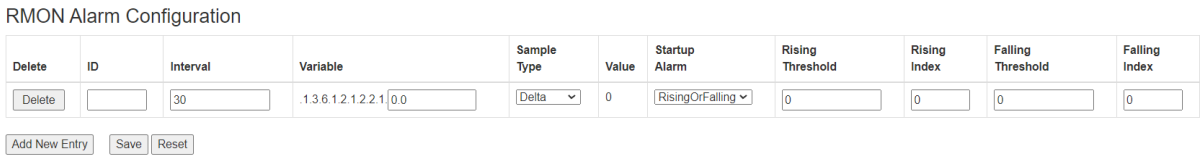


Figure 2-9.1.6.3: The RMON Alarm Configuration

Parameter description:

- **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 :**

  Indicates the particular variable to be sampled, the possible variables are:

  InOctets: The total number of octets received on the interface, including framing characters.

  InUcastPkts: The number of uni-cast packets delivered to a higher-layer protocol.

  InNUcastPkts: The number of broad-cast and multi-cast packets delivered to a higher-layer protocol.

  InDiscards: The number of inbound packets that are discarded even the packets are normal.

  InErrors: The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.

  InUnknownProtos:the number of the inbound packets that were discarded because of the unknown or un-support protocol.

  OutOctets: The number of octets transmitted out of the interface , including framing characters.

  OutUcastPkts: The number of uni-cast packets that request to transmit.

  OutNUcastPkts: The number of broad-cast and multi-cast packets that request to transmit.

  OutDiscards: The number of outbound packets that are discarded event the packets is normal.

  OutErrors: The The number of outbound packets that could not be transmitted because of

errors.

OutQLen: The length of the output packet queue (in packets).

- **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).

- **Value :**

  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).If this value is zero, no associated event will be generated, as zero is not a valid event index.

- **Falling Threshold :**

  Falling threshold value (-2147483648-2147483647)

- **Falling Index :**

  Falling event index (1-65535).If this value is zero, no associated event will be generated, as zero is not a valid event index.

Buttons

- **Delete :**

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

- **Add New Entry :**

  Click to add a new entry.

- **Save :**

  Click to save changes.

- **Reset :**

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

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

Web Interface

To display the configure RMON Event in the web interface:

1. Click Configuration, Security, Switch, RMON and Event.
2. Click Add New Entry.
3. Specify the ID parameters.
4. Click Save.

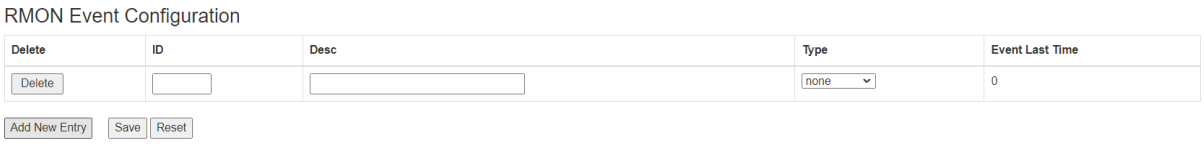


Figure 2-9.1.6.4: The RMON Event Configuration

Parameter description:

- **ID :**

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

- **Desc :**

  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 SNMP log is created, no SNMP trap is sent.

  Log: Create SNMP log entry when the event is triggered.

  Snmp trap: Send SNMP trap when the event is triggered.

  Log and trap: Create SNMP log entry and sent SNMP trap when the 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

- **Delete :**

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

- **Add New Entry :**

  Click to add a new entry.

- **Save :**

  Click to save changes.

- **Reset :**

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

2-9.2 Network

2-9.2.1 Port Security

Port security defines three types of MAC addresses, of which static and sticky can be added and removed on this page:

Dynamic: A MAC address learned through learn frames coming to the Port Security module while the interface in qeustion is not in sticky mode. Dynamic entries disappear if it ages out or if the interface link goes down.

Static: A MAC address added by end-user through management. Static MAC addresses are not subject to aging and will be added to the MAC address table once Port Security gets enabled on the interface.

Static entries are part of the running-config and will survive interface link state changes and reboots if saved to startup-config. Static entries can be added to the running-config at any time whether or not Port Security is enabled.

Sticky: When the interface is in sticky mode, all entries that would otherwise have been learned as dynamic are learned as sticky.

Like static entries, sticky entries are part of the running-config and will survive interface link state changes and reboots if saved to the startup-config.

Though not the intention with Sticky entries, they can be added by management to the running-config at any time whether or not Port Security is enabled on the interface, as long as the interface is in Sticky mode. Sticky entries will disappear if the interface is taken out of Sticky mode.

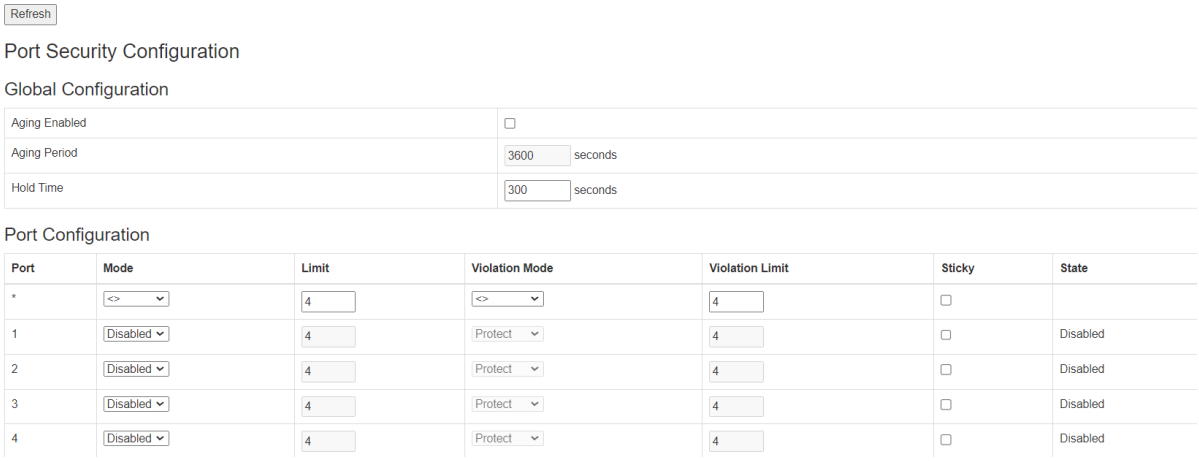
Web Interface

To configure global configuration of port security in the web interface:

1. Select “Enabled” in the Mode of System Configuration.
2. Checked Aging Enabled.
3. Set Aging Period (Default is 3600 seconds).

To configure a static and sticky MAC addresses in the web interface:

1. Click “Add New MAC Entry” to add a new MAC
2. Specify parameters
3. Click Save.



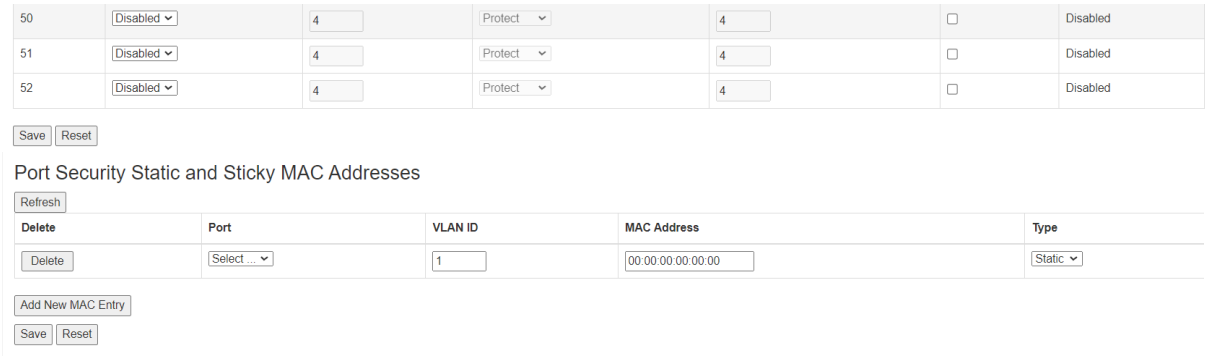


Figure 2-9.2.1: The Port Security Configuration

Parameter description:

System Configuration

- **Delect :**

  Press this button to remove the entry from the MAC address table (if present) and the running-config.
  Notice that dynamic entries may be removed all-together on an interface through "Monitor→Security→Port Security→Switch" and one-by-one through "Monitor→Security→Port Security→Port"

- **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 10,000,000 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 :**

  The port number to which this MAC address is bound.

- **VLAN ID & MAC Address:**

  The VLAN ID and MAC address in question.

- **Type:**

  Indicates the type of entry and may be either Static or Sticky (see description above).

Buttons

- **Add New MAC Entry :**

Click this button will add a new row to the table. This new row allows for adding a static or sticky MAC address to a particular interface. Once satisfied, click the Save-button to save the changes to running-config.
Notice that sticky entries are normally added automatically through learning on the interface.

- **Refresh :**

  You can click them for refresh the Port Security information by manual.

- **Save :**

  Click to save changes.

- **Reset :**

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

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 "Configuration→Security→AAA" 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.

Web Interface

To configure a Network Access Server in the web interface:

1. Click Configuration, Security, Network and NAS.
2. Select “Enabled” in the Mode of Network Access Server Configuration.
3. Checked Reauthentication Enabled.
4. Set Reauthentication Period (Default is 3600 seconds).
5. Set EAPOL Timeout (Default is 30 seconds).
6. Set Aging Period (Default is 300 seconds).
7. Set Hold Time (Default is 10 seconds).
8. Checked RADIUS-Assigned QoS Enabled.
9. Checked RADIUS-Assigned VLAN Enabled.
10. Checked Guest VLAN Enabled.
11. Specify Guest VLAN ID.
12. Specify Max. Reauth. Count.
13. Checked Allow Guest VLAN if EAPOL Seen.
14. Click Save.

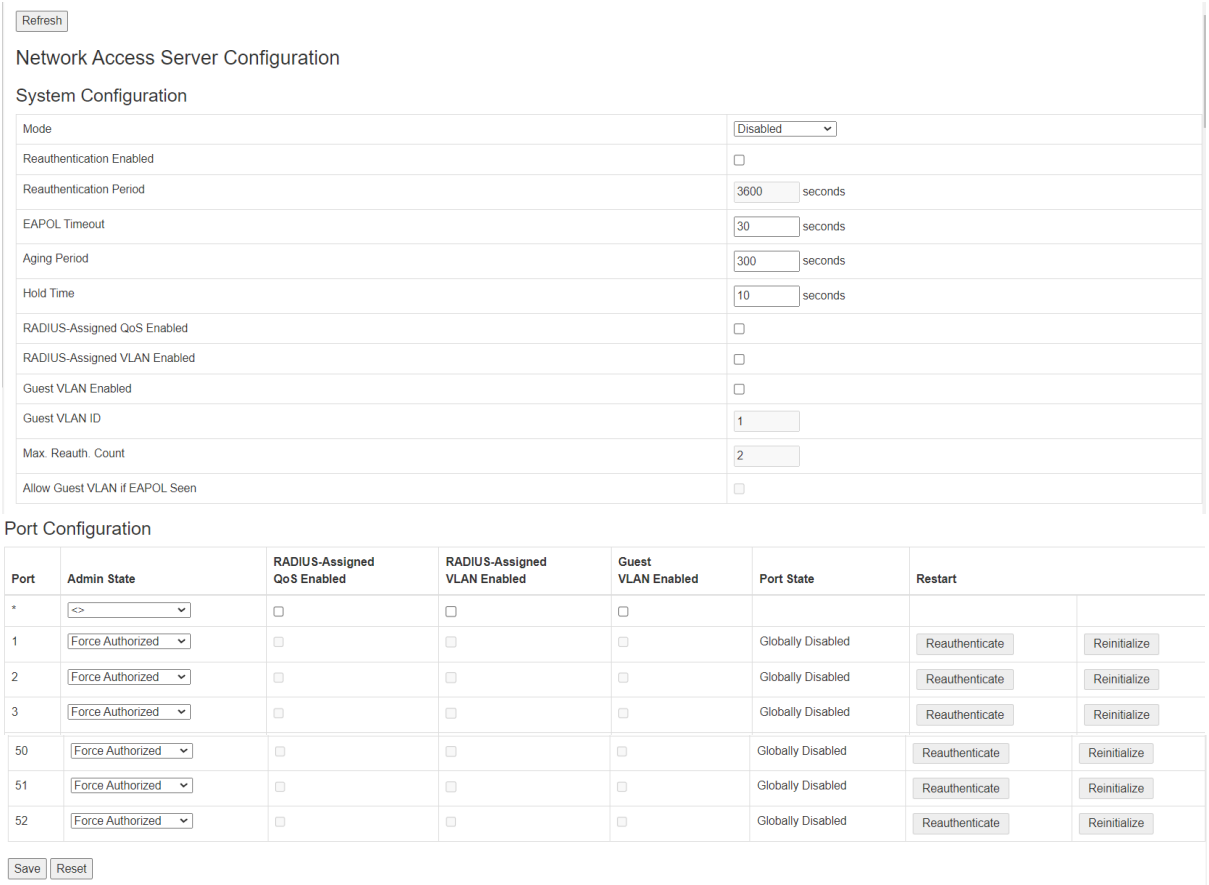


Figure 2-9.2.2: The Network Access Server Configuration

Parameter description:

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 255 seconds. This has no effect for MAC-based ports.

- **Aging Period :**

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 re-authentication, which will fail. But if re-authentication 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 (according to the timeout specified on the "Configuration→Security→AAA" page) - the client is put on hold in the Un-authorized 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 selected 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.

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 :

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 Multi 802.1X variant.

Multi 802.1X is really not an IEEE standard, but features many of the same characteristics as does port-based 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.

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 port-based 802.1X is that several clients can be connected to the same port (e.g. through a 3rd party switch or a hub) and still require individual authentication, and that the clients don't need special supplicant software to authenticate. 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.

- **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:

Refer to the written documentation for a description of the RADIUS attributes needed in order to successfully identify 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's value must be identical and consist of ASCII characters in the range '0' - '3', which translates into the desired QoS Class in the range [0; 3].

- **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

  For trouble-shooting VLAN assignments, use the "Monitor→VLANs→VLAN Membership and VLAN Port" pages. These pages show which modules have (temporarily) overridden the current Port VLAN configuration.

  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 fulfil 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**

For trouble-shooting VLAN assignments, use the "Monitor→VLANs→VLAN Membership and VLAN Port" pages. These pages show which modules have (temporarily) overridden the current Port VLAN configuration.

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 transmissions 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.

  Re-authenticate: Schedules a re-authentication whenever the quiet-period of the port runs out (EAPOL-based authentication). For MAC-based authentication, re-authentication 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 re-initialization of the clients on the port and thereby a re-authentication immediately. The clients will transfer to the unauthorized state while the re-authentication is in progress.

Buttons

- **Refresh :**

  You can click them for refresh the NAS Configuration by manual.

- **Save :**

  Click to save changes.

- **Reset :**

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

2-9.2.3 ACL

The access control list (ACL) is probably the most commonly used object in the IOS. It is used for packet filtering but also for selecting types of traffic to be analyzed, forwarded, or influenced in some way. The ACLs are divided into Ether Types. IPv4, ARP protocol, MAC and VLAN parameters etc. Here we will just go over the standard and extended access lists for TCP/IP. As you create ACEs for ingress classification, you can assign a policy for each port, the policy number is 1-8, and however, each policy can be applied to any port. This makes it very easy to determine what type of ACL policy you will be working with.

2-9.2.3.1 Ports

The section describes how to configure the ACL parameters (ACE) of the each switch port. These parameters will affect frames received on a port unless the frame matches a specific ACE

Web Interface

To configure the ACL Ports Configuration in the web interface:

1. Click Configuration, Security, Network, ACL and Ports.
2. To scroll the specific parameter value to select the correct value for port ACL setting.
3. Click the save to save the setting
4. If you want to cancel the setting then you need to click the reset button. It will revert to previously saved values.
5. After you configure complete then you could see the Counter of the port. Then you could click refresh to update the counter or Clear the information.

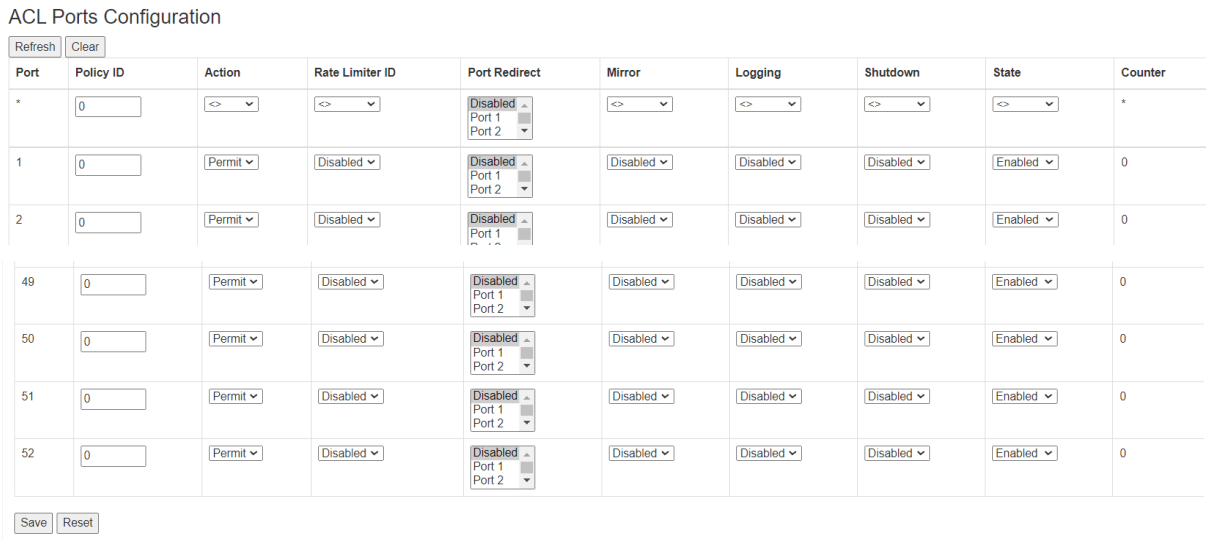


Figure 2-9.2.3.1: The ACL Ports Configuration

Parameter description:

- **Port :**

  The logical port for the settings contained in the same row.

- **Policy ID :**

  Select the policy to apply to this port. The allowed values are 1 through 127. 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 to apply on this port. The allowed values are Disabled or the values 1 through 16. The default value is "Disabled".

- **Port Redirect :**

  Select which port frames are redirected on. The allowed values are Disabled or a specific port number and it can't be set when action is permitted. The default value is "Disabled".

- **Mirror :**

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

  Enabled: Frames received on the port are stored in the System Log.

  Disabled: Frames received on the port are not logged.

  The default value is "Disabled". Please note that the System Log memory size and logging rate is limited.

- **Shutdown :**

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

  Enabled: If a frame is received on the port, the port will be disabled.

  Disabled: Port shut down is disabled.

  The default value is "Disabled".

- **State :**

  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

- **Refresh :**

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

- **Clear :**

  Click to clear the counters.

- **Save :**

  Click to save changes.

- **Reset :**

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

The section describes how to configure the switch's ACL Rate Limiter parameters. The Rate Limiter Level from 1 to 16 that allow user to set rate limiter value and units with pps.

Web Interface

To configure ACL Rate Limiter in the web interface:

1. Click Configuration, Security, Network, ACL and Rate Limiter.
2. To specific the Rate field.
3. Click the Save to save the setting
4. If you want to cancel the setting then you need to click the reset button. It will revert to previously saved values.

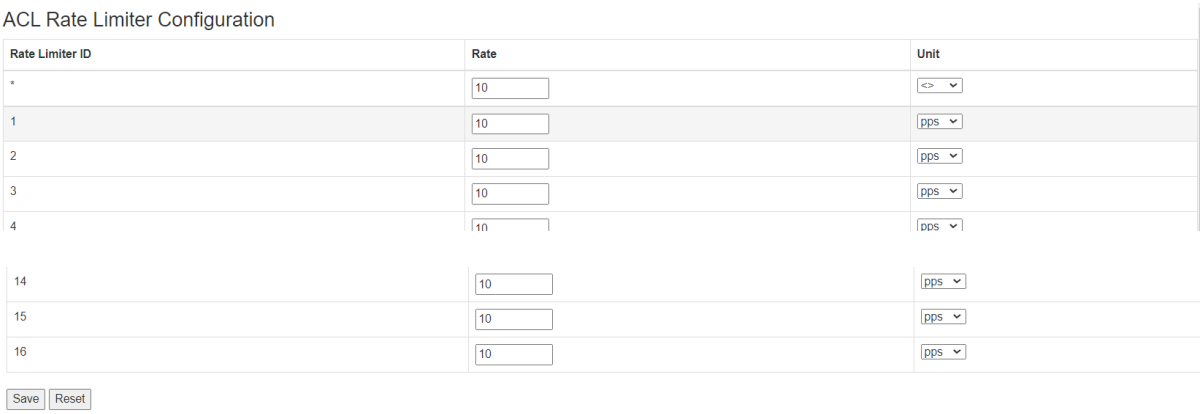


Figure 2-9.2.3.2: The ACL Rate Limiter Configuration

Parameter description:

- **Rate Limiter ID :**

  The rate limiter ID for the settings contained in the same row.

- **Rate :**

  The valid rate is 0, 10, 20, 30, ..., 5000000 in pps or 0, 25, 50, 75, ..., 10000000 in kbps.

Buttons

- **Save :**

  Click to save changes.

- **Reset :**

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

The section describes how to configure Access Control List rule. An Access Control List (ACL) is a sequential list of permit or deny conditions that apply to IP addresses, MAC addresses, or other more specific criteria. This switch tests ingress packets against the conditions in an ACL one by one. A packet will be accepted as soon as it matches a permit rule, or dropped as soon as it matches a deny rule. If no rules match, the frame is accepted. Other actions can also be invoked when a matching packet is found, including rate limiting, copying matching packets to another port or to the system log, or shutting down a port.

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 the priority is highest.

Web Interface

To configure Access Control List in the web interface:

1. Click Configuration, Security, Network, ACL and Access Control List.
2. Click the  button to add a new ACL, or use the other ACL modification buttons to specify the editing action
3. To specific the parameter of the ACE
4. Click the save to save the setting
5. If you want to cancel the setting then click the reset button. It will revert to previously saved values.
6. When editing an entry on the ACE Configuration page, note that the Items displayed depend on various selections, such as Frame Type and IP Protocol Type. Specify the relevant criteria to be matched for this rule, and set the actions to take when a rule is matched (such as Rate Limiter, Port Copy, Logging, and Shutdown).

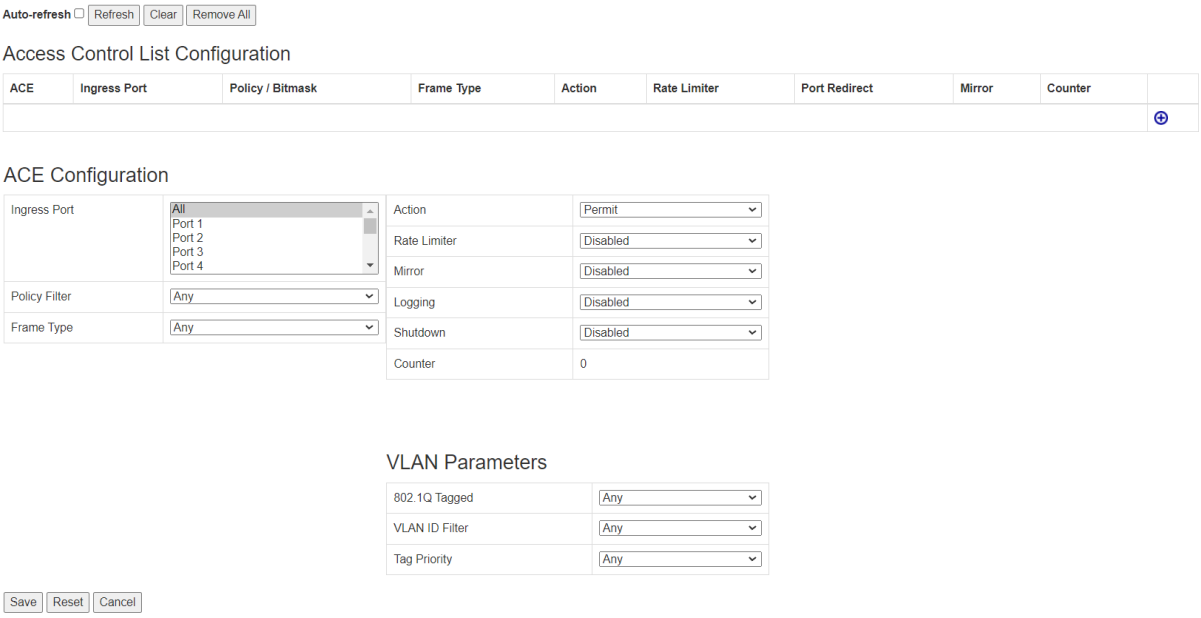


Figure 2-9.2.3.3: The ACL Rate Limiter Configuration

Parameter description:

- **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 Bitmask :**

  When "Specific" is selected for the policy filter, you can enter a specific policy bitmask. The allowed range is 0x0 to 0x7f. 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 :**

  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.

- **Port Redirect :**

  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.

- **Mirror :**

  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".

- **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 limited.

- **Counter :**

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

- **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: The shutdown feature only works when the packet length is less than 1518(without VLAN tags).

MAC Parameter

- **SMAC Filter :**

  (Only displayed when the frame type is Ethernet Type or ARP.)

  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 a 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 frame 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 OP flag is specified. (OP 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 SIP Address field that appears.

  Network: Sender IP filter is set to Network. Specify the sender IP address and sender IP mask in the SIP Address and SIP 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.

- **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.

- **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").

- **Ethernet :**

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

  0: ARP/RARP frames where the HLD is not equal to Ethernet (1).

  1: ARP/RARP frames where the HLD is equal to Ethernet (1).

Any: Any value is allowed ("don't-care").

- **IP :**

  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").

  Specific: If you want to filter a specific IP protocol filter with this ACE, choose this value. A field for entering an IP protocol 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 "Specific" 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 Parameters

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 IPv6 next header filter is specified ("don't-care").

  Specific: 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 :**

  When "Specific" is selected for the IPv6 next header value, you can enter a specific value. 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: Source IPv6 filter is set to Network. Specify the source IPv6 address and source IPv6 mask in the SIP Address fields that appear.

- **SIP Address :**

  When "Specific" is selected for the source IPv6 filter, you can enter a specific SIPv6 address. The field only supported last 32 bits for IPv6 address.

- **SIP BitMask :**

  When "Specific" is selected for the source IPv6 filter, you can enter a specific SIPv6 mask. The field only supported last 32 bits for IPv6 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 32 bits). For example, if the SIPv6 address is 2001::3 and the SIPv6 bitmask is 0xFFFFFFFE(bit 0 is "don't-care" bit), then SIPv6 address 2001::2 and 2001::3 are applied to this rule.

- **Hop Limit :**

  Specify the hop limit settings for this ACE.

  zero: IPv6 frames with a hop limit field greater than zero must not be able to match this entry.

  non-zero: IPv6 frames with a hop limit field greater than zero must be able to match this entry.

  Any: Any value is allowed ("don't-care").

ICMP Parameters

- **ICMP Type Filter :**

  Specify the ICMP filter for this ACE.

  Any: No 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 an ICMP 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 an 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

- **TCP/UDP Source 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 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 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 Destination 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 Destination Number :**

  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 Destination 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 a EtherType 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.

- **Reset :**

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

- **Auto-refresh :**

  To evoke the auto-refresh to refresh the information automatically.

- **Refresh, clear, Remove All :**

  You can click them for refresh the ACL configuration or clear them by manual. Others remove all to clean up all ACL configurations on the table.

- **Cancel :** Return to the previous page.

2-9.2.4 IP Source Guard

The section describes to configure the IP Source Guard detail parameters of the switch. You could use the IP Source Guard configure to enable or disable with the Port of the switch.

2-9.2.4.1 Configuration

This section describes how to configure IP Source Guard setting including:
Mode (Enabled and Disabled)
Maximum Dynamic Clients (0, 1, 2, Unlimited)

Web Interface

To configure an IP Source Guard Configuration in the web interface:

1. Click Configuration, Security, Network, IP Source Guard and Configuration.
2. Select “Enabled” in the Mode of IP Source Guard Configuration.
3. Select “Enabled” of the specific port in the Mode of Port Mode Configuration.
4. Select Maximum Dynamic Clients (0, 1, 2, Unlimited) of the specific port in the Mode of Port Mode Configuration.
5. Click Save.

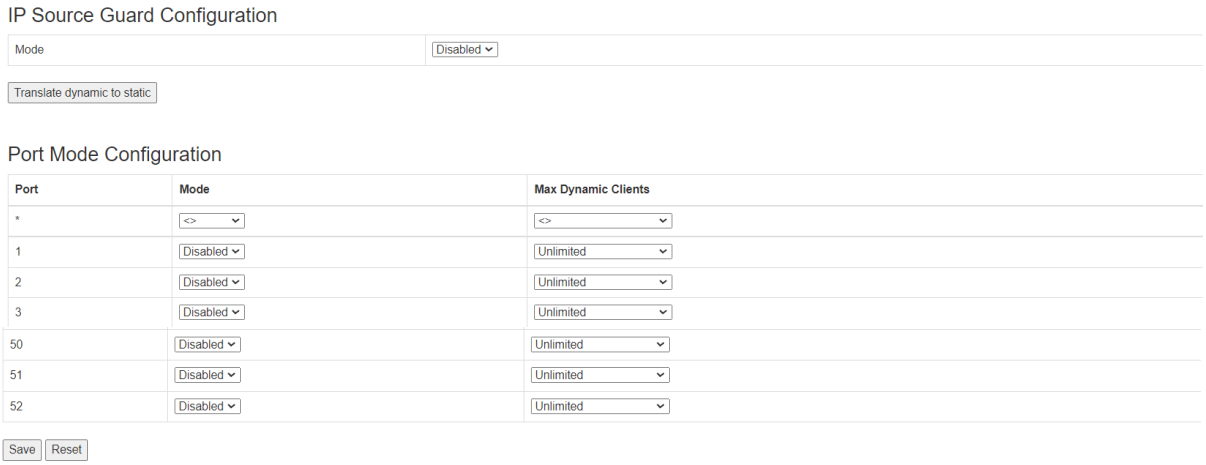


Figure 2-9.2.4.1: The IP Source Guard Configuration

Parameter description:

- **Mode of IP Source Guard Configuration :**

  Enable the Global IP Source Guard or disable the Global IP Source Guard. All configured ACEs will be lost when the mode is enabled.

- **Port Mode Configuration :**

  Specify IP Source Guard is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, IP Source Guard is enabled on this given port.

- **Max Dynamic Clients :**

  Specify the maximum number of dynamic clients that can be learned on given port. This value can be 0, 1, 2 or unlimited. If the port mode is enabled and the value of max dynamic

client is equal to 0, it means only allow the IP packets forwarding that are matched in static entries on the specific port.

Buttons

- **Translate dynamic to static :**

  Click to translate all dynamic entries to static entries.

- **Save :**

  Click to save changes.

- **Reset :**

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

2-9.2.4.2 Static Table

The section describes to configure the Static IP Source Guard Table parameters of the switch. You could use the Static IP Source Guard Table configure to manage the entries.

Web Interface

To configure a Static IP Source Guard Table Configuration in the web interface:

1. Click Configuration, Security, Network, IP Source Guard and Static Table.
2. Click “Add New Entry”.
3. Specify the Port, VLAN ID, IP Address, and MAC address in the entry.
4. Click Save

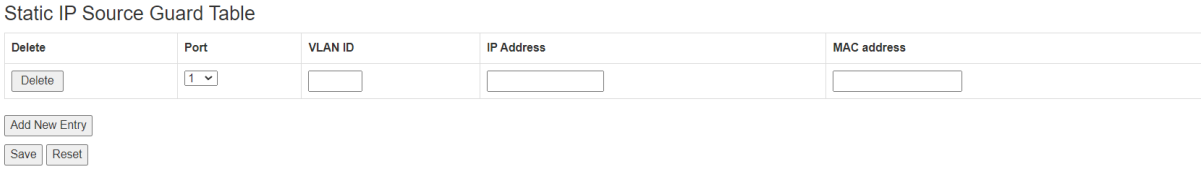


Figure 2-9.2.4.2: The Static IP Source Guard Table

Parameter description:

- **Port :**

  The logical port for the settings.

- **VLAN ID :**

  The VLAN id for the settings.

- **IP Address :**

  Allowed Source IP address.

- **MAC address :**

  Allowed Source MAC address.

Buttons

- **Adding new entry :**

  Click to add a new entry to the Static IP Source Guard table. Specify the Port, VLAN ID, IP address, and IP Mask for the new entry. Click "Save".

- **Save:**

  Click to save changes.

- **Reset :**

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

- **Delete :**

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

2-9.2.5 IPv6 Source Guard

The section describes to configure the IPv6 Source Guard detail parameters of the switch. You could use the IPv6 Source Guard configure to enable or disable with the Port of the switch.

2-9.2.5.1 Configuration

This page shows the static IPv6 Source Guard entries. The maximum number of entries is 112 on the switch.

Web Interface

To configure an IP Source Guard Configuration in the web interface:

1. Click Configuration, Security, Network, IPv6 Source Guard and Configuration.
2. Select “Enabled” in the Mode of IPv6 Source Guard Configuration.
3. Select “Enabled” of the specific port in the Mode of Port Mode Configuration.
4. Select Maximum Dynamic Clients of the specific port in the Mode of Port Mode Configuration.
5. Click Save.

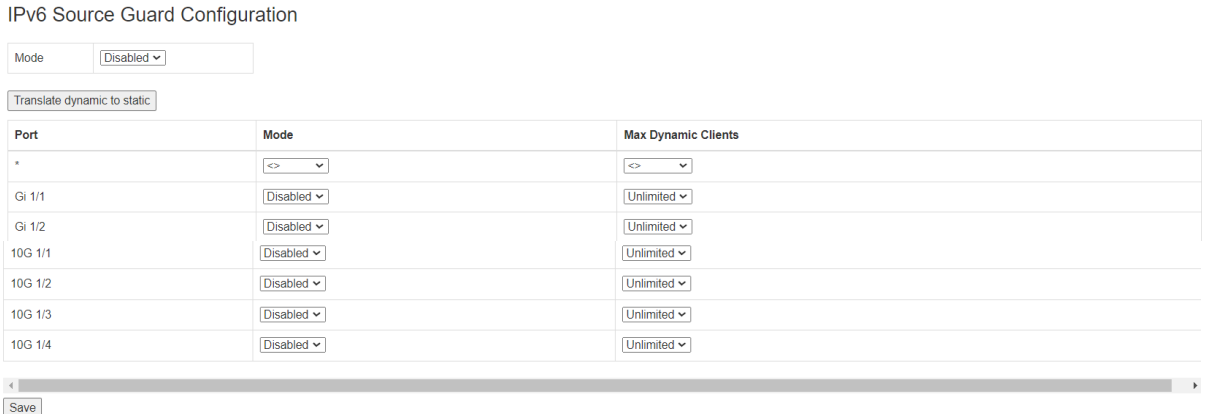


Figure 2-9.2.4.1: The IPv6 Source Guard Configuration

Parameter description:

- **IPv6 Source Guard ConfigurationMode :**

  Enable or disable the IPv6 Source Guard globally.

- **Port Mode Configuration :**

  The table shows all ports on the device. There IPv6 Source Guard can be enabled/disabled on individual ports. Only when both Global Mode and Port Mode on a given port are enabled, IPv6 Source Guard is enabled on this given port.

- **Max Dynamic Clients :**

  Specify the maximum number of dynamic clients that can be learned on given port. This value can be 0, 1, 2 or unlimited. If the port mode is enabled and the value of max dynamic client is equal to 0, only IPv6 packets that are matched in static entries on the specific port are forwarded.

Buttons

- **Translate dynamic to static :**

  Click to translate all dynamic entries to static entries.

- **Save :**

  Click to save changes.

2-9.2.5.2 Static Table

This page shows the static IPv6 Source Guard entries. The maximum number of entries is 112 on the switch.

Web Interface

To configure a Static IPv6 Source Guard Table Configuration in the web interface:

1. Click Configuration, Security, Network, IPv6 Source Guard and Static Table.
2. Specify the Port, VLAN ID, IP Address, and MAC address in the entry.
3. Click Add Entry

Figure 2-9.2.5.2: The Static IPv6 Source Guard Table

Parameter description:

- **Port :**

  The logical port the entry is bound to.

- **VLAN ID :**

  The VLAN Id for the entry. If no VLAN Id is associated with the entry, this field shows 0.

- **IPv6 Address :**

  Allowed Source IPv6 address.

- **Prefix Size:**

  Prefix size of the IPv6 address.

- **MAC address :**

  Allowed Source MAC address.

Buttons

- **Gi 1/1 :**

  Toggle to select entry port.

- **Adding Entry :**

  Click to add a new entry to the Static IPv6 Source Guard table. .

- **Refresh:**

  Refreshes the display table.

- **Auto-refresh :**

  Check this box to refresh the page automatically.

2-9.2.6 ARP Inspection

The section describes to configure the ARP Inspection parameters of the switch. You could use the ARP Inspection configure to manage the ARP table.

2-9.2.6.1 Port Configuration

This section describes how to configure ARP Inspection setting including:
Mode (Enabled and Disabled)
Port (Enabled and Disabled)

Web Interface

To configure an ARP Inspection Configuration in the web interface:

1. Click Configuration, Security, Network, ARP Inspection and Configuration.
2. Select “Enabled” in the Mode of ARP Inspection Configuration.
3. Select “Enabled” of the specific port in the Mode of Port Mode Configuration.
4. Specify “Check VLAN” and “Log Type”
5. Click Save.

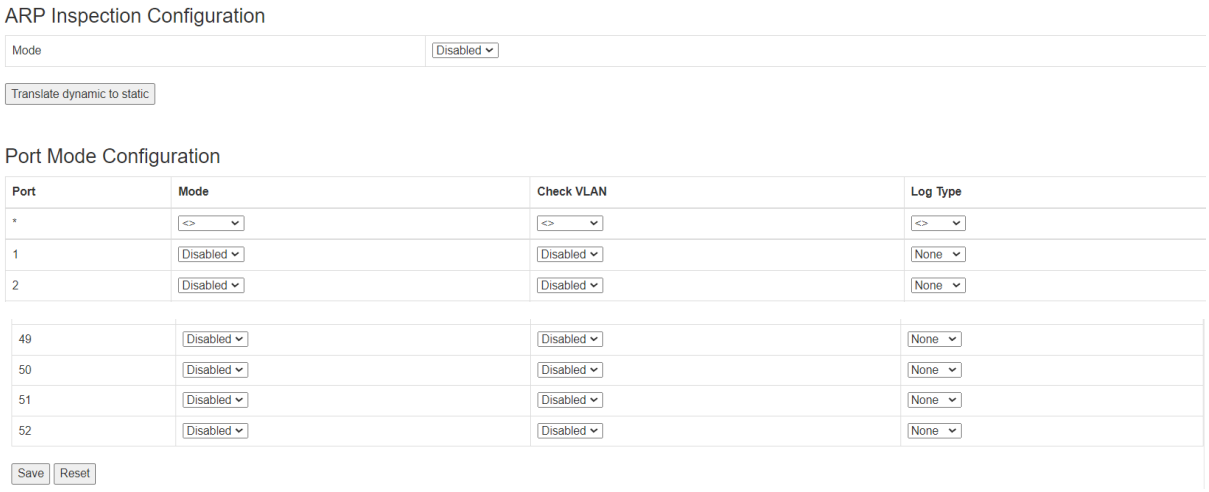


Figure 2-9.2.6.1: The ARP Inspection Configuration.

Parameter description:

- **Mode of ARP Inspection Configuration :**

  Enable the Global ARP Inspection or disable the Global ARP Inspection.

- **Port Mode Configuration :**

  Specify ARP Inspection is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port. Possible modes are:
  Enabled: Enable ARP Inspection operation.
  Disabled: Disable ARP Inspection operation.
  If you want to inspect the VLAN configuration, you have to enable the setting of "Check

VLAN". The default setting of "Check VLAN" is disabled. When the setting of "Check VLAN" is disabled, the log type of ARP Inspection will refer to the port setting. And the setting of "Check VLAN" is enabled, the log type of ARP Inspection will refer to the VLAN setting.
Possible setting of "Check VLAN" are:
Enabled: Enable check VLAN operation.
Disabled: Disable check VLAN operation.
Only the Global Mode and Port Mode on a given port are enabled, and the setting of "Check VLAN" is disabled, the log type of ARP Inspection will refer to the port setting.
There are four log types and possible types are:
None: Log nothing.
Deny: Log denied entries.
Permit: Log permitted entries.
ALL: Log all entries.

Buttons

- **Translate dynamic to static :**

  Click to translate all dynamic entries to static entries.

- **Apply :**

  Click to save changes.

- **Reset :**

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

Each page shows up to 9999 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 button will update the displayed table starting from that or the closest next VLAN Table match. The will use the next entry of the currently displayed VLAN entry as a basis for the next lookup. When the end is reached the warning message is shown in the displayed table. Use the button to start over.

Web Interface

To configure a VLAN Mode Configuration in the web interface:

1. Click Configuration, Security, Network, ARP Inspection and VLAN Mode Configuration.
2. Click “Add new entry”.
3. Specify the VLAN ID, Log Type
4. Click Save.

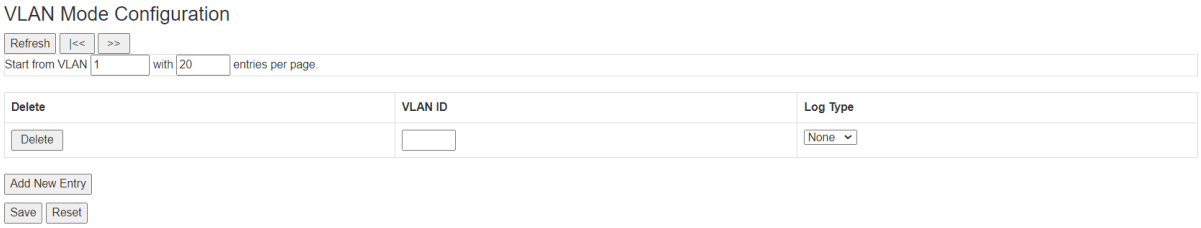


Figure 2-9.2.6.2: The VLAN Mode Configuration

Parameter description:

- **VLAN Mode Configuration :**

  Specify ARP Inspection is enabled on which VLANs. First, you have to enable the port setting on Port mode configuration web page. Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port. Second, you can specify which VLAN will be inspected on VLAN mode configuration web page. The log type also can be configured on per VLAN setting.
  Possible types are:
  None: Log nothing.
  Deny: Log denied entries.
  Permit: Log permitted entries.
  ALL: Log all entries.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

- **Add New Entry :**

  Click to add a new VLAN to the ARP Inspection VLAN table.

2-9.2.6.3 Static Table

This page shows the static ARP Inspection rules. The maximum number of rules is 256 on the switch.

Web Interface

To configure a Static ARP Inspection Table Configuration in the web interface:

1. Click Configuration, Security, Network, ARP Inspection and Static Table.
2. Click “Add New Entry”.
3. Specify the Port, VLAN ID, IP Address, and MAC address in the entry.
4. Click Save.

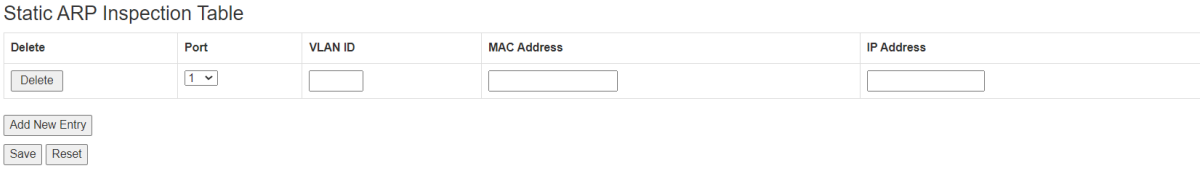


Figure 2-9.2.6.3: The Static ARP Inspection Table

Parameter description:

- **Port :**

  The logical port for the settings.

- **VLAN ID :**

  The vlan id for the settings.

- **MAC Address :**

  Allowed Source MAC address in ARP request packets.

- **IP Address :**

  Allowed Source IP address in ARP request packets.

Buttons

- **Delete :**

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

- **Save :**

  Click to save changes.

- **Reset :**

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

- **Add New Entry :**

  Click to add a new entry to the Static ARP Inspection table.

2-9.2.6.4 Dynamic Table

Entries in the Dynamic ARP Inspection Table are shown on this page. The Dynamic ARP Inspection Table contains up to 256 entries, and is sorted first by port, then by VLAN ID, then by MAC address, and then by IP address. All dynamic entries are learning from DHCP Snooping.

Navigating the ARP Inspection Table
Each page shows up to 99 entries from the Dynamic ARP Inspection 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 Dynamic ARP Inspection Table.
The "Start from port address", "VLAN", "MAC address" and "IP address" input fields allow the user to select the starting point in the Dynamic ARP Inspection Table. Clicking the button will update the displayed table starting from that or the closest next Dynamic ARP Inspection 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.
The 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.

Web Interface

To configure a Dynamic ARP Inspection Table Configuration in the web interface:

1. Click Configuration, Security, Network, ARP Inspection and Dynamic Table.
2. Select “Port” in the Mode of Dynamic ARP Inspection Table.
3. Click Apply.

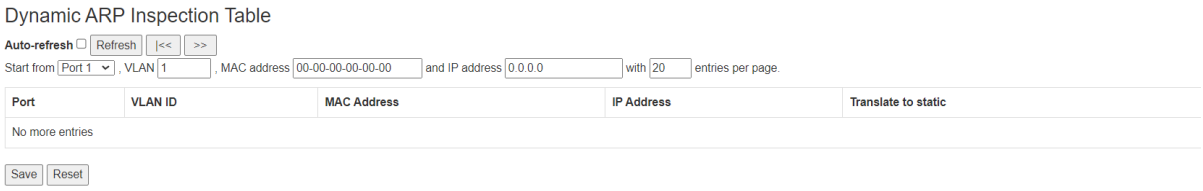


Figure 2-9.2.6.4: The Dynamic ARP Inspection Table

Parameter description:

- **Port :**

  Switch Port Number for which the entries are displayed.

- **VLAN ID :**

  VLAN-ID in which the ARP traffic is permitted.

- **MAC Address :**

  User MAC address of the entry.

- **IP Address :**

  User IP address of the entry.

- **Translate to static :**

  Select the checkbox to translate the entry to static entry.

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 refresh the page automatically. Automatic refresh occurs every 3 seconds.

- **Refresh :**

  Refreshes the displayed table starting from the input fields.

- **Save :**

  Click to save changes.

- **<< :**

  Updates the table starting from the first entry in the Dynamic ARP Inspection Table.

- **>> :**

  Updates the table, starting with the entry after the last entry currently displayed

2-9.3 AAA

This section shows you to use an AAA (Authentication, Authorization, and Accounting) server to provide access control to your network. The AAA server can be a TACACS+ or RADIUS server to create and manage objects that contain settings for using AAA servers.

2-10.3.1 RADIUS

Web Interface

To configure a Common Configuration of AAA, RADIUS in the web interface:

1. Click Configuration, Security, AAA and RADIUS.
2. Specify the global configuration.
3. Click "Add New Server".
4. Specify the Hostname, Auth Port, Acct Port, Timeout, Retransmit and Key in the server.
5. Click Save.

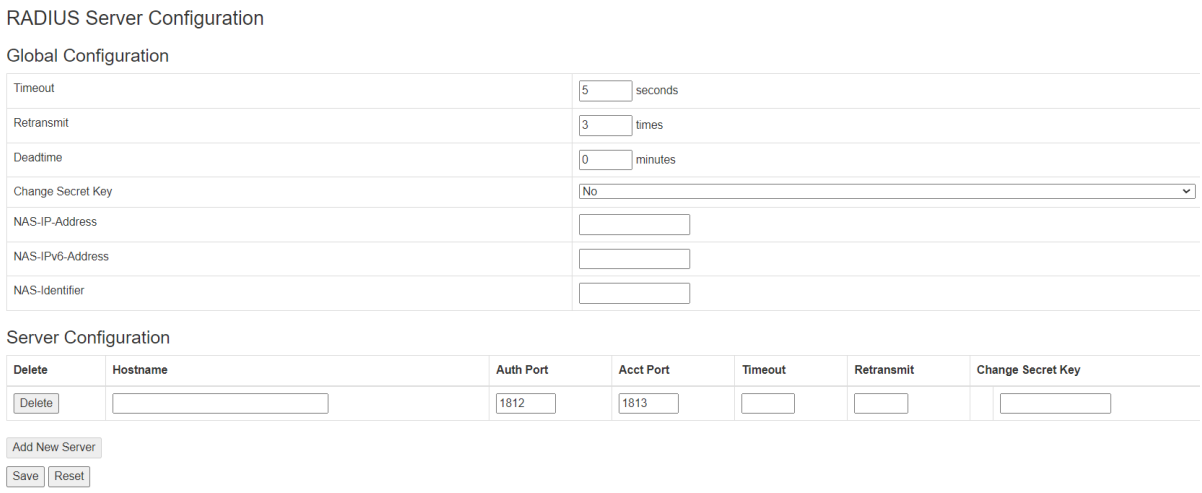


Figure 2-9.3.1: The RADIUS Server Configuration

Parameter description:

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 minutes, 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 (zero) will enable this feature, but only if more than one server has been configured.

- **Change Secret Key :**

  Specify to change the secret key or not. When "Yes" is selected for the option, you can change 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.

- **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 identifier - up to 255 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.

Server Configuration

The table has one row for each RADIUS server and a number of columns, which are:

- **Hostname :**

  The IP address or hostname of the RADIUS server.

- **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.

- **Change Secret Key :**

  When the checkbox is checked, you can change the setting overrides the global key. Leaving it blank will use the global key.

Buttons

- **Delete :**

  This button can be used to undo the addition of the new server.

- **Add New Server :**

  Click to add a new RADIUS server. An empty row is added to the table, and the RADIUS server can be configured as needed. Up to 5 servers are supported.

The button can be used 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.

This page allows you to configure the TACACS+ servers.

Web Interface

To configure the TACACS+ servers in the web interface:

1. Click Configuration, Security, AAA and TACACS+.
2. Specify the global configuration
3. Click “Add New Server”.
4. Specify the Hostname, Port, Timeout and Key in the server.
5. Click Save.

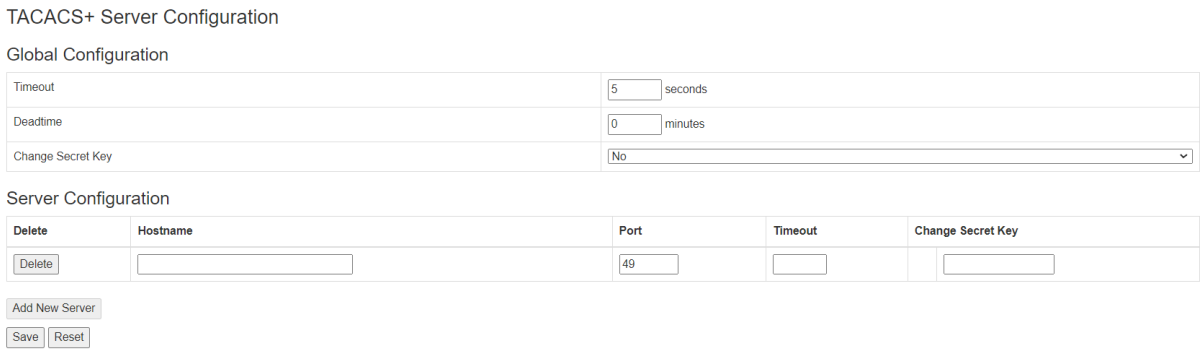


Figure 2-9.3.2: The TACACS+ Server Configuration

Parameter description:

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 minutes, 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 (zero) will enable this feature, but only if more than one server has been configured.

- **Change Secret Key :**

  Specify to change the secret key or not. When "Yes" is selected for the option, you can change the secret key - up to 63 characters long - shared between the TACACS+ server and the switch.

Server Configuration

The table has one row for each TACACS+ server and a number of columns, which are:

- **Delete :**

To delete a TACACS+ server entry, check this box. The entry will be deleted during the next Save.

- **Hostname :**

  The IP address or hostname of the TACACS+ server.

- **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.

- **Change Secret Key :**

  Specify to change the secret key or not. When the checkbox is checked, you can change the setting overrides the global key. Leaving it blank will use the global key.

Buttons

- **Delete :**

  This button can be used to undo the addition of the new server.

- **Add New Server :**

  Click to add a new TACACS+ server. An empty row is added to the table, and the TACACS+ server can be configured as needed. Up to 5 servers are supported.

- **Save :**

  Click to save changes.

- **Reset :**

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

2-10 Aggregation

2-10.1 Common

This page is used to configure the Aggregation hash mode. This mode applies to the whole network element.

Web Interface

To configure common aggregation configuration in the web interface:

1. Click Configuration, Aggregation and Common.
2. Specify the parameters.
3. Click Save to save the setting.
4. If you want to cancel the setting then you need to click the reset button. It will revert to previously saved values.

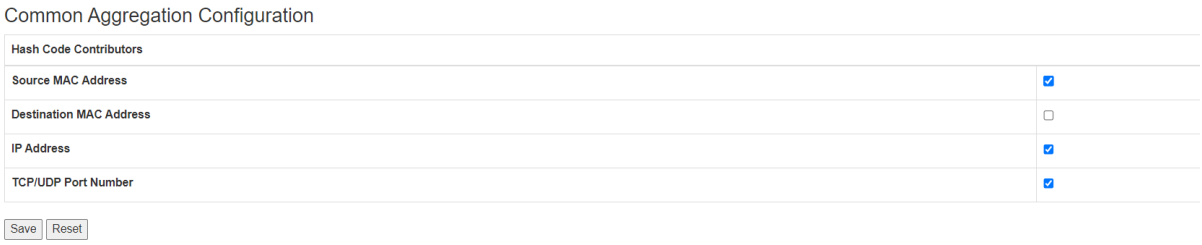


Figure 2-10.1: The Aggregation Mode Configuration

Parameter description:

- **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.

Buttons

- **Save :**

  Click to save changes.

- **Reset :**

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

2-10.2 Groups

This page is used to configure the aggregation groups.

Web Interface

To configure the aggregation group in the web interface:

1. Click Configuration, Aggregation and Groups
2. Evoke Aggregation Group ID Port members and group configuration.
3. Click Save to save the setting.
4. If you want to cancel the setting then you need to click the reset button. It will revert to previously saved values.

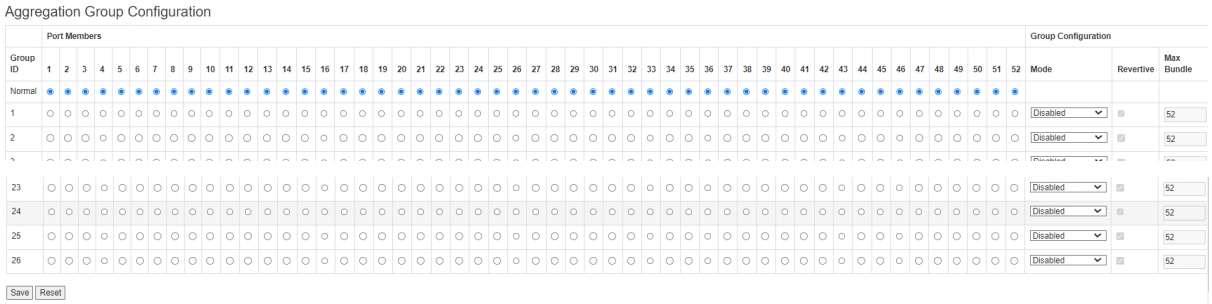


Figure 2-10.2: The Aggregation Mode Configuration

Parameter description:

- **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.

- **Mode :**

  This parameter determines the mode for the aggregation group.

  Disabled: The group is disabled.

  Static: The group operates in static aggregation mode.

  LACP (Active): The group operates in LACP active aggregation mode. See IEEE 801.AX-2014, section 6.4.1 for details.

  LACP (Passive): The group operates in LACP passive aggregation mode. See IEEE 801.AX-2014, section 6.4.1 for details.

- **Revertive:**
  This parameter only applies to LACP-enabled groups. It determines if the group will perform automatic link (re-)calculation when links with higher priority becomes available.

- **Max Bundle:**

  This parameter only applies to LACP-enabled groups. It determines the maximum number of active bundled LACP ports allowed in an aggregation.

Buttons

- **Save :**

  Click to save changes.

- **Reset :**

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

2-10.3 LACP

This page allows the user to inspect the current LACP port configurations, and possibly change them as well.

Web Interface

To configure the LACP Port Configuration in the web interface:

1. Click Configuration, Aggregation and LACP.
2. Specify parameters
3. Click Apply to save the setting.
4. If you want to cancel the setting then you need to click the reset button. It will revert to previously saved values.

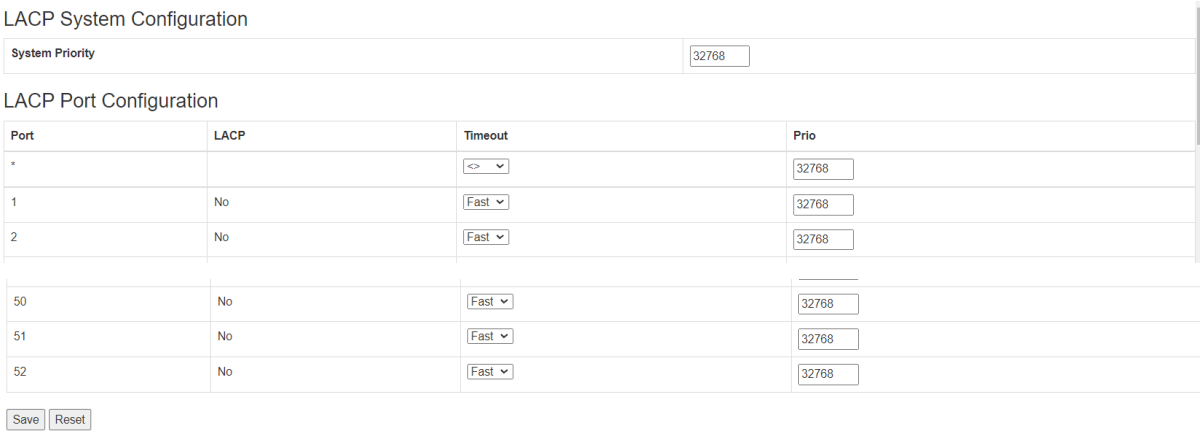


Figure 2-10.3: The LACP Port Configuration

Parameter description:

- **Port :**

  The switch port number.

- **LACP:**

  Show whether LACP is currently enabled on this switch port.

- **Timeout :**

  The 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 Prio controls the priority of the port. 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.

2-11 Link OAM

2-11-1 Port Settings

This page allows the user to inspect the current Link OAM port configurations, and change them as well.

Web Interface

To configure the link OAM port setting parameters in the web interface:

1. Click Configuration, Link OAM and Port Settings.
2. Evoke to specify the parameters
3. Click the Save to save the setting.
4. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.

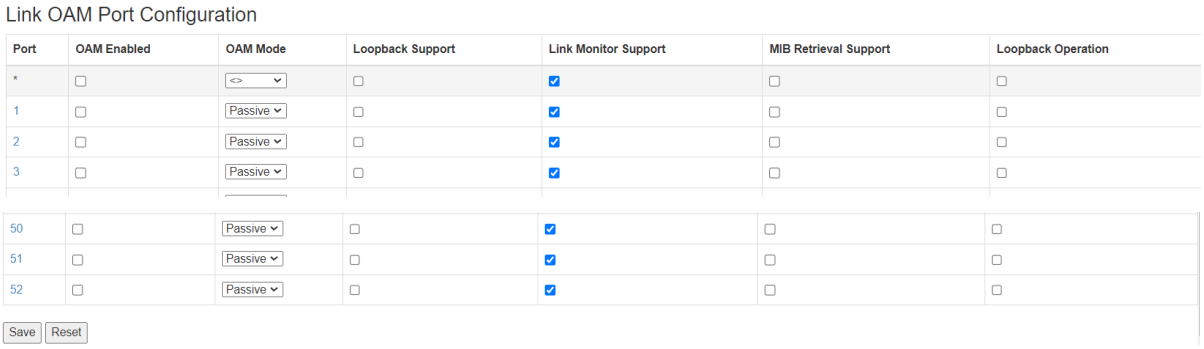


Figure 2-11-1: The Port Setting Configuration

Parameter description:

- **Port :**

  The switch port number.

- **OAM Enabled :**

  Controls whether Link OAM is enabled on this switch port. Enabling Link OAM provides the network operators the ability to monitor the health of the network and quickly determine the location of failing links or fault conditions.

- **OAM Mode:**

  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). Configures the OAM Mode as Active or Passive. The default mode is Passive.

  Active mode: DTE's configured in Active mode initiate the exchange of Information OAMPDUs as defined by the Discovery process. Once the Discovery process completes, Active DTE's are permitted to send any OAMPDU while connected to a remote OAM peer entity in Active mode. Active DTE's operate in a limited respect if the remote OAM entity is operating in Passive mode. Active devices should not respond to OAM remote loopback commands and variable requests from a Passive peer.

  Passive mode: DTE's configured in Passive mode do not initiate the Discovery process.

Passive DTE's react to the initiation of the Discovery process by the remote DTE. This eliminates the possibility of passive to passive links. Passive DTE's shall not send Variable Request or Loopback Control OAMPDUs.

- **Loopback Support :**

  Controls whether the loopback support is enabled for the switch port. Link OAM remote loopback can be used for fault localization and link performance testing. Enabling the loopback support will allow the DTE to execute the remote loopback command that helps in the fault detection.

- **Link Monitor Support :**

  Controls whether the Link Monitor support is enabled for the switch port. On enabling the Link Monitor support, the DTE supports event notification that permits the inclusion of diagnostic information.

- **MIB Retrieval Support :**

  Controls whether the MIB Retrieval Support is enabled for the switch port. On enabling the MIB retrieval support, the DTE supports polling of various Link OAM based MIB variables' contents.

- **Loopback Operation :**

  If the Loopback support is enabled, enabling this field will start a loopback operation for the port.

Buttons

- **Save :**

  Click to save changes.

- **Reset :**

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

This page allows the user to inspect the current Link OAM Link Event configurations, and change them as well.

Web Interface

To configure the link OAM event setting parameters in the web interface:

1. Click Configuration, Link OAM and Event Settings.
2. Select the Port number
3. Specify the Error Window and Error Threshold
4. Click the Save to save the setting.
5. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.

Figure 2-11-2: The Event Setting Configuration

Parameter description:

- **Port :**

  The switch port number of the port.

- **Event Name:**

  Name of the Link Event which is being configured.

- **Action :**

  Configures the action performed when a loop is detected on a port. Valid values are Shutdown Port, Shutdown Port and Log or Log Only.

- **Error Window :**

  Represents the window period in the order of 1 sec for the observation of various link events.

- **Error Threshold :**

  Represents the threshold value for the window period for the appropriate Link event so as to notify the peer of this error.

- **Error Frame Event :**

  The Errored Frame Event counts the number of errored frames detected during the specified period. The period is specified by a time interval (Window in order of 1 sec). This event is generated if the errored frame count is equal to or greater than the specified threshold for that period (Period Threshold). Errored frames are frames that had transmission errors as detected at the Media Access Control sublayer. Error Window for 'Error Frame Event' must

be an integer value between 1-60 and its default value is '1'. Whereas Error Threshold must be between 0-4294967295 and its default value is '1'.

- **Symbol Period Error Event :**

  The Errored Symbol Period Event counts the number of symbol errors that occurred during the specified period. The period is specified by the number of symbols that can be received in a time interval on the underlying physical layer. This event is generated if the symbol error count is equal to or greater than the specified threshold for that period. Error Window for 'Symbol Period Error Event' must be an integer value between 1-60 and its default value is '1'. Whereas Error Threshold must be between 0-4294967295 and its default value is '1'.

- **Seconds Summary Event :**

  specified threshold for that period. An errored frame second is a one second interval wherein at least one frame error was detected. Errored frames are frames that had transmission errors as detected at the Media Access Control sublayer. Error Window for 'Seconds Summary Event' must be an integer value between 10-900 and its default value is '60'. Whereas Error Threshold must be between 0-65535 and its default value is '1'.

Buttons

- **Save:**

  Click to save changes.

- **Reset :**

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

2-12 Loop Protection

This page allows the user to inspect the current Loop Protection configurations, and possibly change them as well.

Web Interface

To configure the Loop Protection parameters in the web interface:

1. Click Configuration, Loop Protection.
2. Evoke to select enable or disable the port loop Protection.
3. Click the Save to save the setting.
4. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.

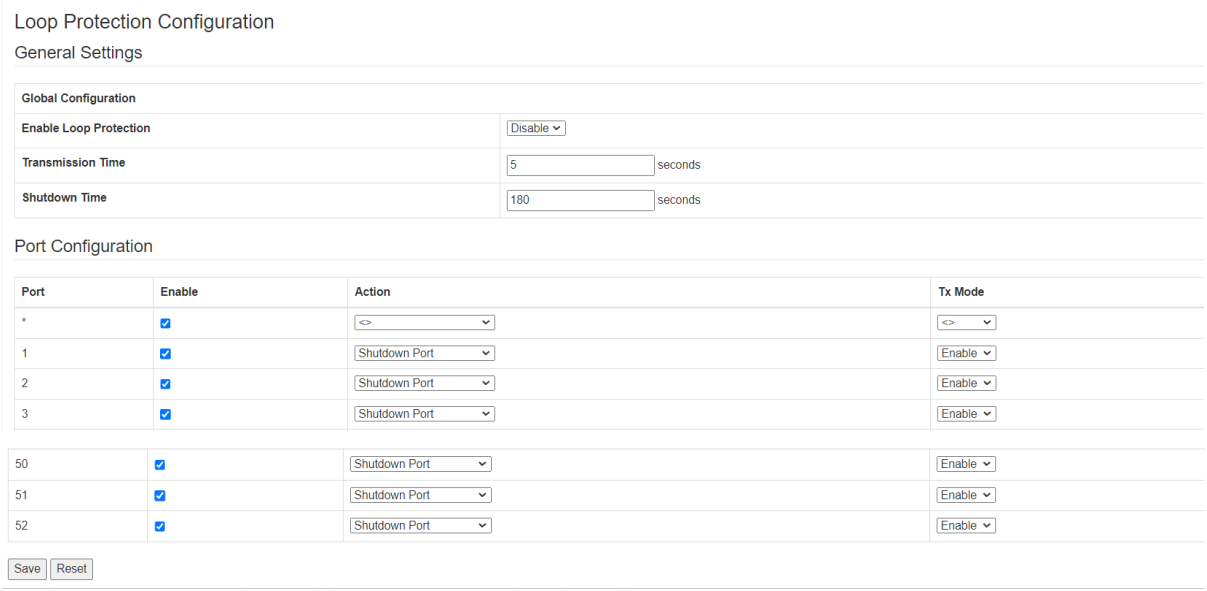


Figure 2-12: The Loop Protection Configuration

Parameter description:

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).

Port Configuration

- **Port No :**

The switch port number of the port.

- **Enable :**

  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 or Log Only.

- **Tx Mode :**

  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.

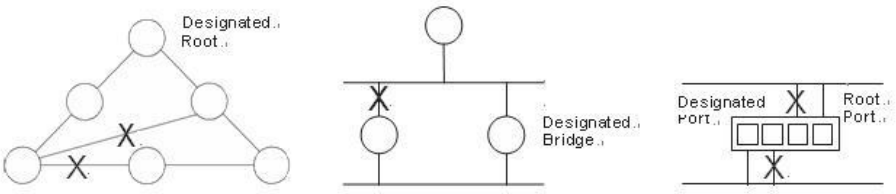
- **Reset :**

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

2-13 Spanning Tree

The Spanning Tree Protocol (STP) can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices (that is, an STP-compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down.

STP - STP uses a distributed algorithm to select a bridging device (STP- compliant switch, bridge or router) that serves as the root of the spanning tree network. It selects a root port on each bridging device (except for the root device) which incurs the lowest path cost when forwarding a packet from that device to the root device. Then it selects a designated bridging device from each LAN which incurs the lowest path cost when forwarding a packet from that LAN to the root device. All ports connected to designated bridging devices are assigned as designated ports. After determining the lowest cost spanning tree, it enables all root ports and designated ports, and disables all other ports. Network packets are therefore only forwarded between root ports and designated ports, eliminating any possible network loops.



Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the Root Bridge. If a bridge does not get a Hello BPDU after a predefined interval (Maximum Age), the bridge assumes that the link to the Root Bridge is down. This bridge will then initiate negotiations with other bridges to reconfigure the network to reestablish a valid network topology.

2-13.1 Bridge Setting

The section describes that how to configure the Spanning Tree Bridge and STP System settings. It allows you to configure STP System settings are used by all STP Bridge instance in the switch.

Web Interface

To configure the Spanning Tree Bridge Settings parameters in the web interface:

1. Click Configuration, Spanning Tree, Bridge Settings.
2. Scroll to select the parameters and write down available value of parameters in blank field in Basic Settings.
3. Evoke to enable or disable the parameters and write down available value of parameters in blank field in Advanced settings.
4. Click the Save to save the setting.
5. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.

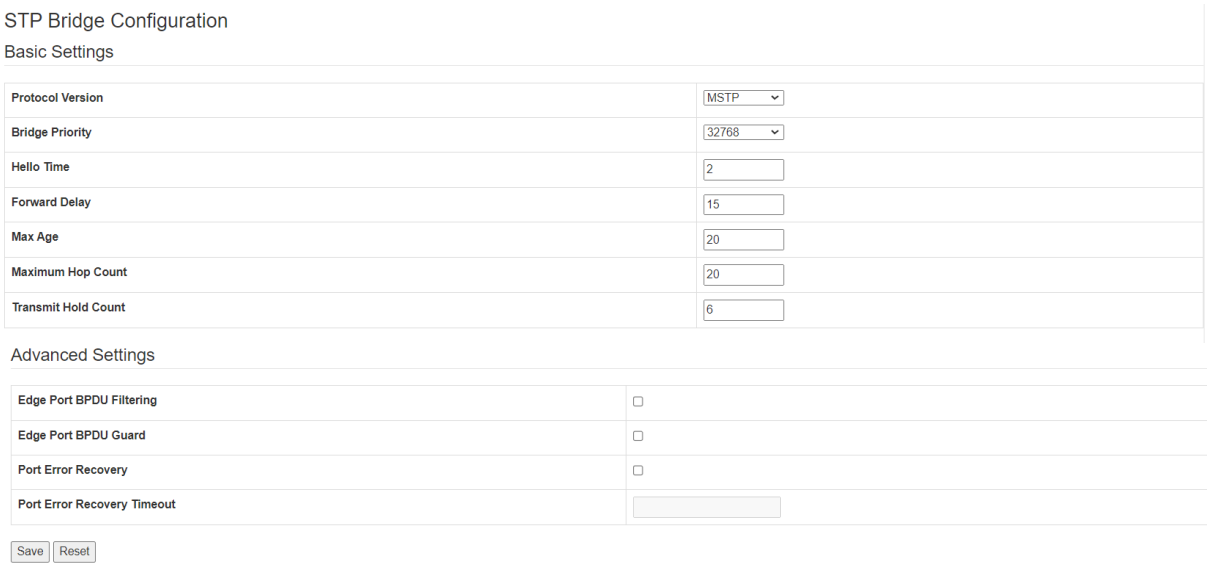


Figure 2-13.1: The STP Bridge Configuration

Parameter description:

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.

- **Max Age :**

  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.

- **Edge Port 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.

When you implement a Spanning Tree protocol on the switch that the bridge instance. The CIST is not available for explicit mapping, as it will receive the VLANs not explicitly mapped. Due to the reason that you need to set the list of VLANs mapped to the MSTI. The VLANs 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.)

This section describes it allows the user to inspect the current STP MSTI bridge instance priority configurations, and possibly change them as well.

Web Interface

To configure the Spanning Tree MSTI Mapping parameters in the web interface:

1. Click Configuration, Spanning Tree, MSTI Mapping.
2. Specify the configuration identification parameters in the field. Specify the VLANs Mapped blank field.
3. Click the Save to save the setting.
4. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.

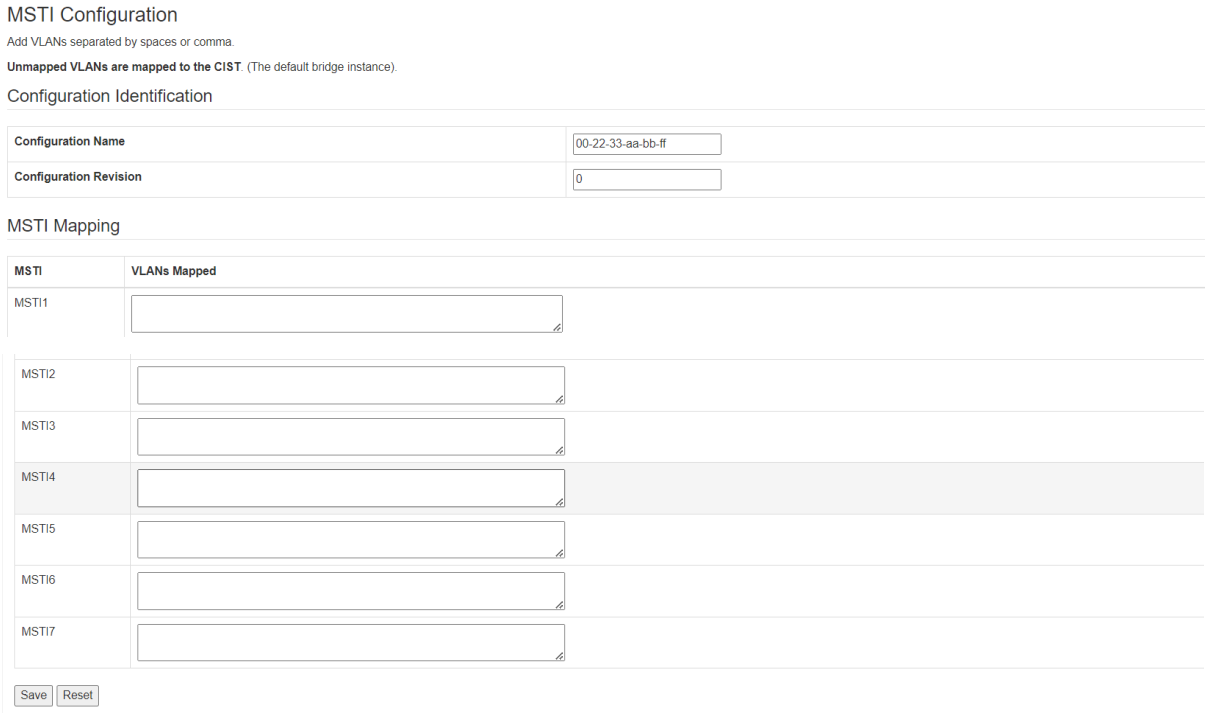


Figure 2-13.2: The MSTI Configuration

Parameter description:

Configuration Identification

- **Configuration 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.

When you implement a Spanning Tree protocol on the switch that the bridge instance. The CIST is the default instance which is always active. For 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

The section describes it allows the user to inspect the current STP MSTI bridge instance priority configurations, and possibly change them as well.

Web Interface

To configure the Spanning Tree MSTI Priorities parameters in the web interface:

1. Click Configuration, Spanning Tree, MSTI Priorities.
2. Scroll the Priority.
3. Click the Save to save the setting.
4. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.

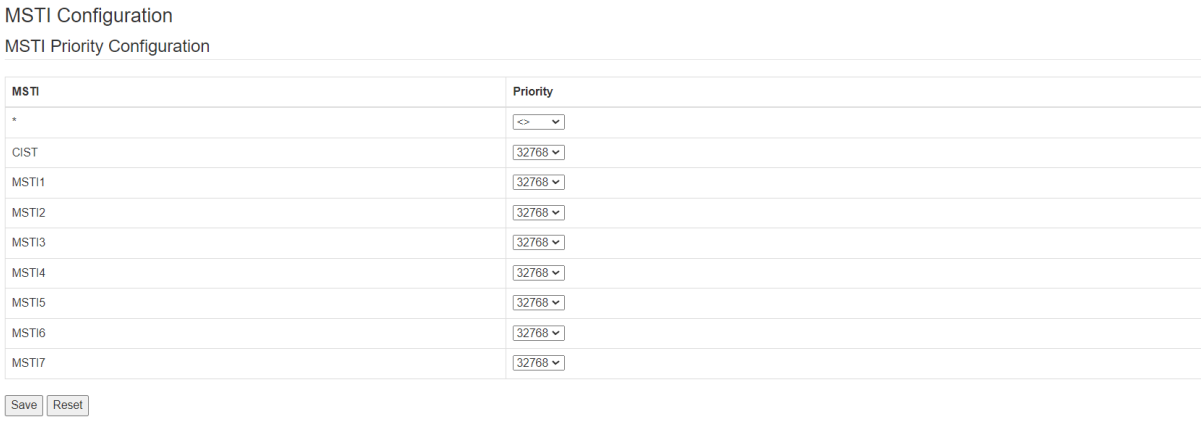


Figure 2-13.3: The MSTI Configuration

Parameter description:

- **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.

2-13.4 CIST Ports

When you implement a Spanning Tree protocol on the switch that the bridge instance. You need to configure the CIST Ports. The section describes it allows the user to inspect the current STP CIST port configurations, and possibly change them as well. This page contains settings for physical and aggregated ports.

Web Interface

To configure the Spanning Tree CIST Ports parameters in the web interface:

1. Click Configuration, Spanning Tree, CIST Ports.
2. Scroll and evoke to set all parameters of CIST Aggregated Port Configuration.
3. Evoke to enable or disable the STP, then scroll and evoke to set all parameters of the CIST normal Port configuration.
4. Click the save to save the setting.
5. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.

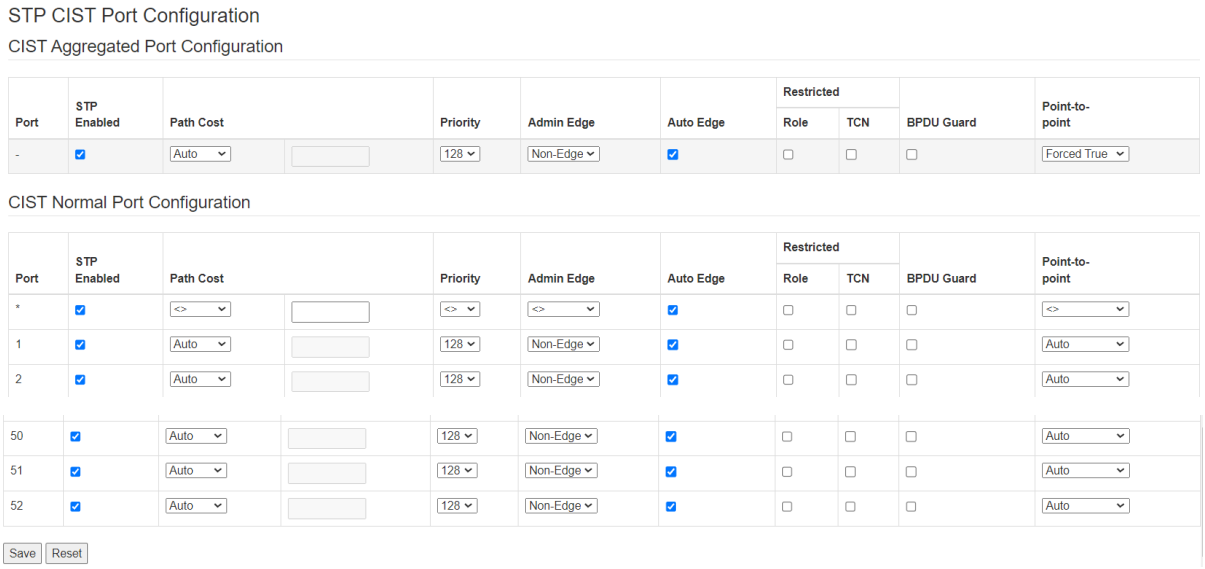


Figure 2-13.4: The STP CIST Port Configuration

Parameter description:

- **Port :**

  The switch port number of the logical STP port.

- **STP Enabled :**

  Controls whether STP is enabled on this switch port. This field will be read only if Voice VLAN feature is enabled. The Voice VLAN port mode will be read only if this field be Enabled.

- **Path Cost :**

  Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range 1 to 200000000.

- **Priority :**

Controls the port priority. This can be used to control priority of ports having identical port cost. (See above). Lower priority is better.

- **operEdge (state flag) :**

  Operational flag describing whether the port is connecting directly to edge devices. (No Bridges attached). Transition to the forwarding state is faster for edge ports (having operEdge true) than for other ports.The value of this flag is based on AdminEdge and AutoEdge fields. This flag is displayed as Edge in Monitor->Spanning Tree -> STP Detailed Bridge Status.

- **AdminEdge :**

  Controls whether the operEdge flag should start as set or cleared. (The initial operEdge 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.

- **Restricted 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.

- **Restricted 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 affect 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.

2-13.5 MSTI Ports

The section describes it 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. It contains MSTI port settings for physical and aggregated ports.

Web Interface

To configure the Spanning Tree MSTI Port Configuration parameters in the web interface:

1. Click Configuration, Spanning Tree, MSTI Ports
2. Scroll to select the MST1 or other MSTI Port
3. Click Get to set the detail parameters of the MSTI Ports.
4. Scroll to set all parameters of the MSTI Port configuration.
5. Click the save to save the setting
6. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values

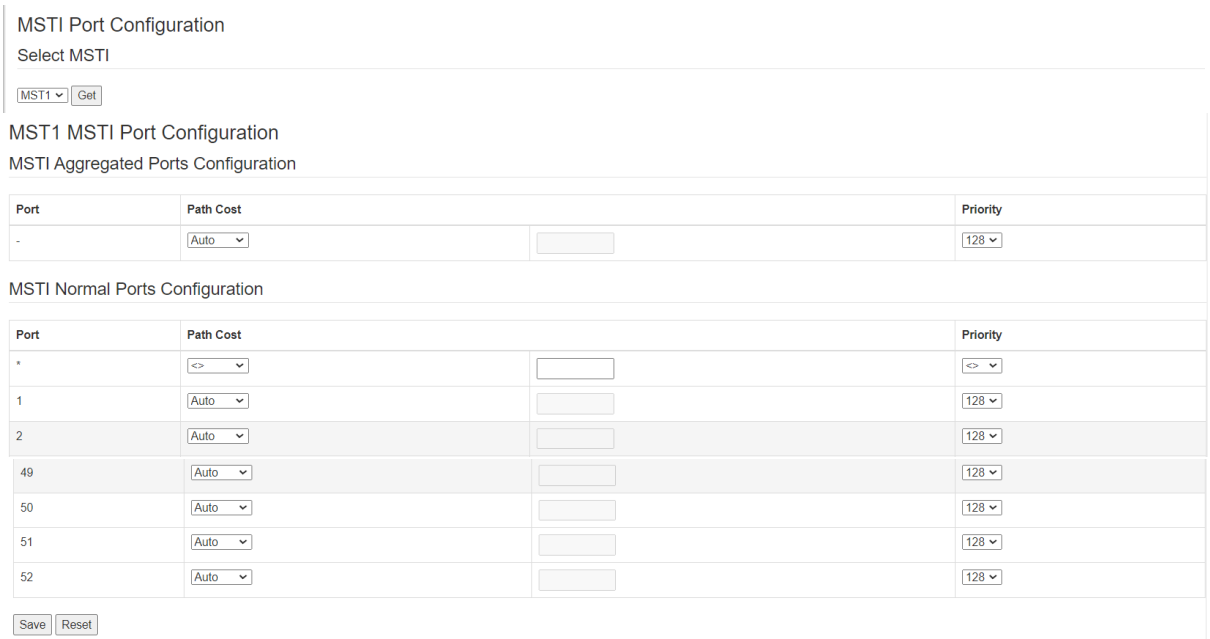


Figure 2-13.5: The MSTI Port Configuration

Parameter description:

- **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

favor of higher path cost ports. Valid values are in the range 1 to 200000000.

- **Priority :**

  Controls the port priority. This can be used to control priority of ports having identical port cost. (See above).

Buttons

- **Get :**

  Click to retrieve settings for a specific MSTI.

- **Save :**

  Click to save changes.

- **Reset :**

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

2-14 IPMC Profile

This page provides IPMC Profile related configurations.

2-14.1 Profile Table

The IPMC profile is used to deploy the access control on IP multicast streams. It is allowed to create at maximum 64 Profiles with at maximum 128 corresponding rules for each.

Web Interface

To configure the IPMC Profile Configuration in the web interface:

1. Click Configuration, IPMC Profile and Profile Table.
2. Select “Enabled” in the Mode of Global Profile Mode.
3. Click Add New IPMC Profile.
4. Specify the IPMC Profile Table Setting parameters in the field. Specify the Profile Name and Profile Description blank field.
5. Click Save.
6. Click the button  to specify IPMC Profile Rule Settings.
7. Click Add Last Rule and can manage the rules.

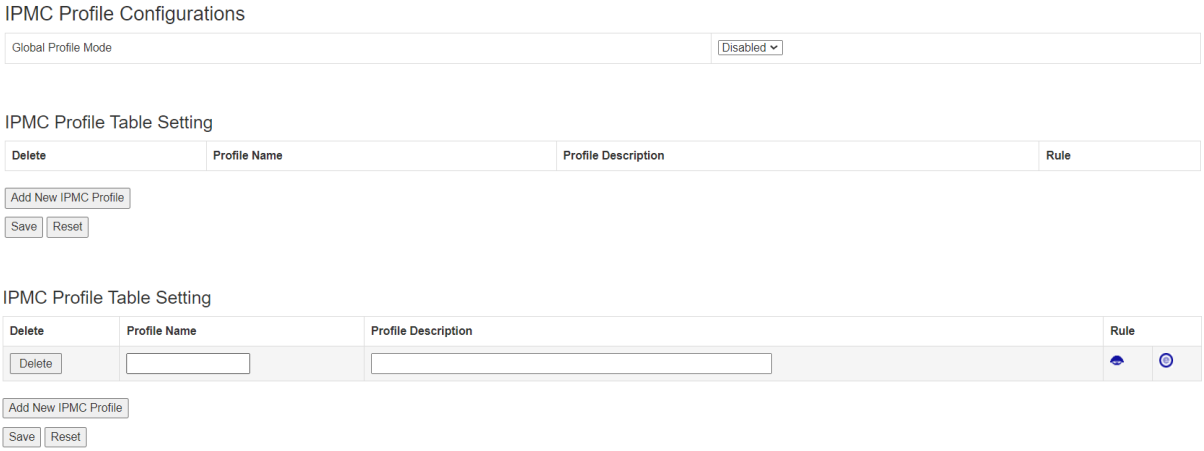


Figure 2-14.1: The IPMC Profile Configuration

Parameter description:

- **Global Profile Mode**

  Enable/Disable the Global IPMC Profile.
  System starts to do filtering based on profile settings only when the global profile mode is enabled.

- **Delete :**

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

- **Profile Name :**

  The name used for indexing the profile table.

Each entry has the unique name which is composed of at maximum 16 alphabetic and numeric characters. At least one alphabet must be present.

- **Profile Description :**

  Additional description, which is composed of at maximum 64 alphabetic and numeric characters, about the profile.

  No blank or space characters are permitted as part of description. Use "_" or "-" to separate the description sentence.

- **Rule :**

  When the profile is created, click the edit button to enter the rule setting page of the designated profile. Summary about the designated profile will be shown by clicking the view button. You can manage or inspect the rules of the designated profile by using the following buttons:

   : List the rules associated with the designated profile.

   : Adjust the rules associated with the designated profile

Buttons

- **Save :**

  Click to save changes.

- **Reset :**

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

- **Add New IPMC Profile :**

  Click to add new IPMC profile. Specify the name and configure the new entry. Click "Save".

2-14.2 Address Entry

This page provides address range settings used in IPMC profile.

The address entry is used to specify the address range that will be associated with IPMC Profile. It is allowed to create at maximum 128 address entries in the system.

Web Interface

To configure the IPMC Profile Address Configuration in the web interface:

1. Click Configuration, IPMC Profile and Address Entry.
2. Click Add New Address (Range) Entry.
3. Specify the IPMC Profile Address Configuration parameters in the field. Specify the Entry Name and Start Address and End Address blank field.
4. Click Save.

Figure 2-14.2: The IPMC Profile Address Configuration

Parameter description:

- **Entry Name :**

  The name used for indexing the address entry table.
  Each entry has the unique name which is composed of at maximun 16 alphabetic and numeric characters. At least one alphabet must be present.

- **Start Address :**

  The starting IPv4/IPv6 Multicast Group Address that will be used as an address range.

- **End Address :**

  The ending IPv4/IPv6 Multicast Group Address that will be used as an address range.

Buttons

- **Save :**

  Click to save changes.

- **Reset :**

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

- **Delete :**

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

- **Add New Address (Range) Entry :**

  Click to add new address range. Specify the name and configure the addresses. Click "Save"

- **Refresh :**

Refreshes the displayed table starting from the input fields.

-  **<< :**

  Updates the table starting from the first entry in the IPMC Profile Address Configuration.

-  **>> :**

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

2-15 MVR

The MVR feature enables multicast traffic forwarding on the Multicast VLANs.

In a multicast television application, a PC or a network television or a set-top box can receive the multicast stream. Multiple set-top boxes or PCs can be connected to one subscriber port, which is a switch port configured as an MVR receiver port. When a subscriber selects a channel, the set-top box or PC sends an IGMP/MLD report message to Switch A to join the appropriate multicast group address. Uplink ports that send and receive multicast data to and from the multicast VLAN are called MVR source ports.

It is allowed to create at maximum 4 MVR VLANs with corresponding channel profile for each Multicast VLAN.

The channel profile is defined by the IPMC Profile which provides the filtering conditions.

Web Interface

To configure the MVR Configuration in the web interface:

1. Click Configuration, MVR.
2. Scroll the MVR mode to enable or disable
3. Click "Add New MVR VLAN" to add a new entry
4. Specify the VLAN interface settings
5. Scroll to select the Immediate Leave disabled/enabled.
6. Click the save to save the setting.
7. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.

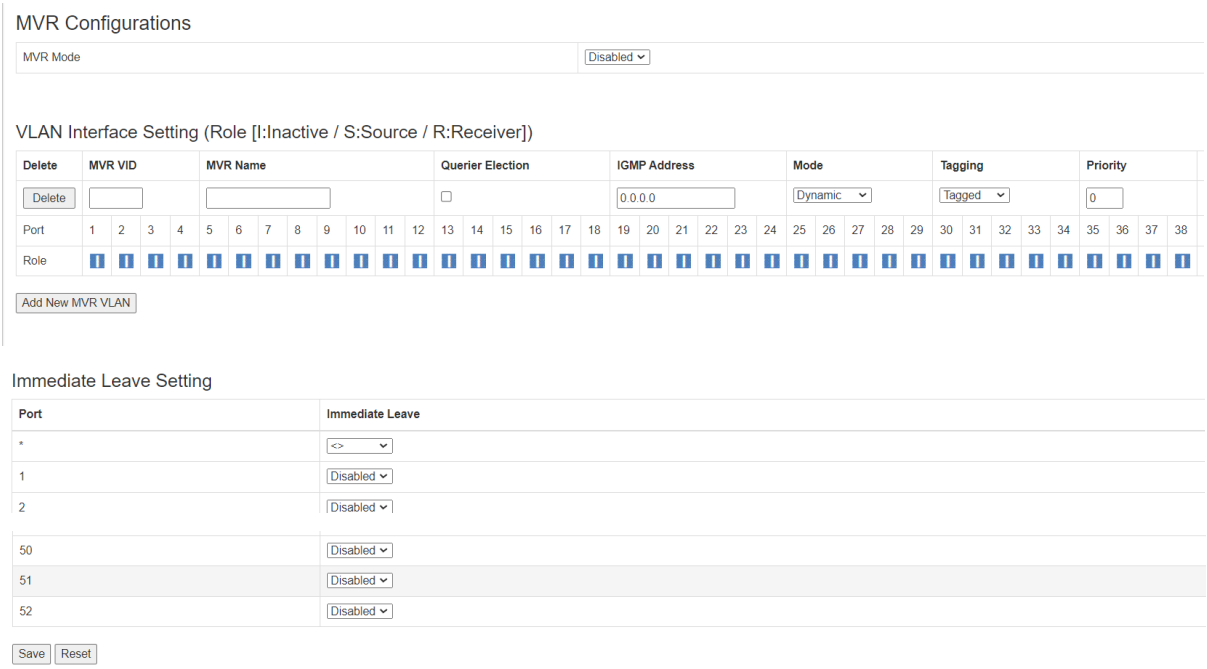


Figure 2-15: The MVR Configuration

Parameter description:

- **MVR Mode :**

  Enable/Disable the Global MVR.
  The Unregistered Flooding control depends on the current configuration in IGMP/MLD Snooping. It is suggested to enable Unregistered Flooding control when the MVR group table is full.

- **MVR VID :**

  Specify the Multicast VLAN ID.
  Be Caution: MVR source ports are not recommended to be overlapped with management VLAN ports.

- **MVR Name :**

  MVR Name is an optional attribute to indicate the name of the specific MVR VLAN. Maximum length of the MVR VLAN Name string is 32. MVR VLAN Name can only contain alphabets or numbers. When the optional MVR VLAN name is given, it should contain at least one alphabet. MVR VLAN name can be edited for the existing MVR VLAN entries or it can be added to the new entries.

- **Querier Election :**

  Enable to join IGMP Querier election in the VLAN. Disable to act as an IGMP Non-Querier.

- **IGMP Address :**

  Define the IPv4 address as source address used in IP header for IGMP control frames.

  The default IGMP address is not set (0.0.0.0).

  When the IGMP 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.

- **Mode :**

  Specify the MVR mode of operation. In Dynamic mode, MVR allows dynamic MVR membership reports on source ports. In Compatible mode, MVR membership reports are forbidden on source ports. The default is Dynamic mode.

- **Tagging :**

  Specify whether the traversed IGMP/MLD control frames will be sent as Untagged or Tagged with MVR VID. The default is tagged.

- **Priority :**

  Specify how the traversed IGMP/MLD control frames will be sent in prioritized manner. The default Priority is 0.

- **LLQI :**

  Define the maximum time to wait for IGMP/MLD report memberships on a receiver port before removing the port from multicast group membership. The value is in units of tenths of a seconds. The range is from 0 to 31744. The default LLQI is 5 tenths or one-half second.

- **Interface Channel Profile :**

  When the MVR VLAN is created, select the IPMC Profile as the channel filtering condition for the specific MVR VLAN. Summary about the Interface Channel Profiling (of the MVR VLAN) will be shown by clicking the view button. Profile selected for designated interface channel is not allowed to have overlapped permit group address.

- **Profile Management Button :**

  You can inspect the rules of the designated profile by using the following button:

   : List the rules associated with the designated profile.

- **Port :**

  The logical port for the settings.

- **Port Role :**

  Configure an MVR port of the designated MVR VLAN as one of the following roles.

  Inactive: The designated port does not participate MVR operations.

  Source: Configure uplink ports that receive and send multicast data as source ports. Subscribers cannot be directly connected to source ports.

  Receiver: Configure a port as a receiver port if it is a subscriber port and should only receive multicast data. It does not receive data unless it becomes a member of the multicast group by issuing IGMP/MLD messages.

  Be Caution: MVR source ports are not recommended to be overlapped with management VLAN ports. Select the port role by clicking the Role symbol to switch the setting. I indicates Inactive; S indicates Source; R indicates Receiver. The default Role is Inactive.

- **Immediate Leave :**

  Enable the fast leave on the port.

Buttons

- **Save :**

  Click to save changes.

- **Reset :**

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

- **Delete :**

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

- **Add New MVR VLAN :**

  Click to add new MVR VLAN. Specify the VID and configure the new entry. Click "Apply".

2-16 IPMC

2-16.1 IGMP Snooping

The function, is used to establish the multicast groups to forward the multicast packet to the member ports, and, in nature, avoids wasting the bandwidth while IP multicast packets are running over the network. This is because a switch that does not support IGMP or IGMP Snooping cannot tell the multicast packet from the broadcast packet, so it can only treat them all as the broadcast packet. Without IGMP Snooping, the multicast packet forwarding function is plain and nothing is different from broadcast packet.

A switch supported IGMP Snooping with the functions of query, report and leave, a type of packet exchanged between IP Multicast Router/Switch and IP Multicast Host, can update the information of the Multicast table when a member (port) joins or leaves an IP Multicast Destination Address. With this function, once a switch receives an IP multicast packet, it will forward the packet to the members who joined in a specified IP multicast group before.

The packets will be discarded by the IGMP Snooping if the user transmits multicast packets to the multicast group that had not been built up in advance. IGMP mode enables the switch to issue IGMP function that you enable IGMP proxy or snooping on the switch, which connects to a router closer to the root of the tree. This interface is the upstream interface. The router on the upstream interface should be running IGMP.

It can support up to 1024 multicast groups.

2-16.1.1 Basic Configuration

This page provides IGMP Snooping related configuration.

Web Interface

To configure the IGMP Snooping Configuration in the web interface:

1. Click Configuration, IPMC, IGMP Snooping, Basic Configuration.
2. Evoke to select enable or disable the parameter in the Global Configuration and Port Related Configuration Mode.
3. Click the Save to save the setting.
4. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.

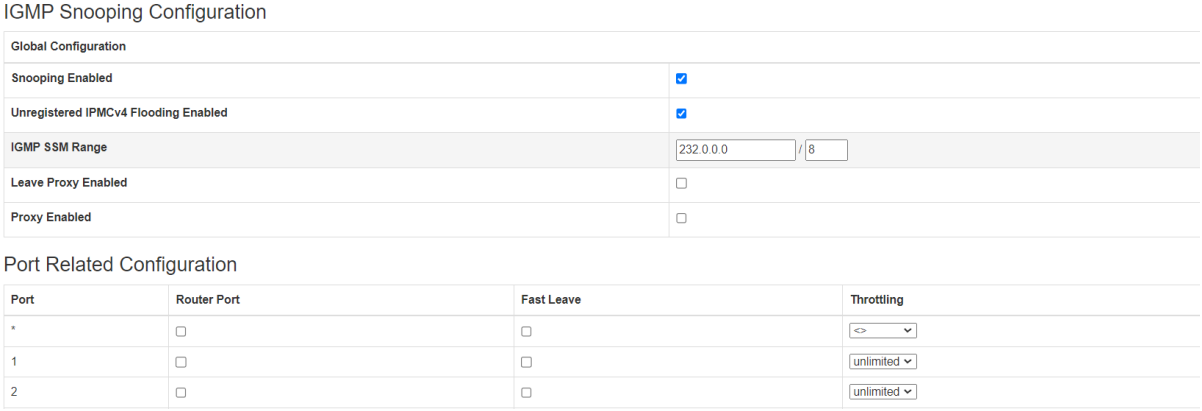


Figure 2-16.1.1: The IGMP Snooping Configuration.

Parameter description:

- **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.

- **IGMP SSM Range :**

  SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address range.

- **Leave Proxy Enabled :**

  Enable IGMP Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.

- **Proxy Enabled :**

  Enable IGMP Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.

- **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.

  System will remove group record and stop forwarding data upon receiving the IGMPv2 leave message without sending last member query messages.
  It is recommended to enable this feature only when a single IGMPv2 host is connected to the specific 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.

The section describes the VLAN configuration setting process integrated with IGMP Snooping function. For each setting 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 button will update the displayed table starting from that or the next closest VLAN Table match.

Web Interface

To configure the IGMP Snooping VLAN Configuration in the web interface:

1. Click Configuration, IPMC, IGMP Snooping and VLAN Configuration.
2. Evoke to select enable or disable Snooping, Querier Address. Specify the parameters in the blank field.
3. Click the refresh to update the data or click << or > to display previous entry or next entry.
4. Click the save to save the setting
5. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values

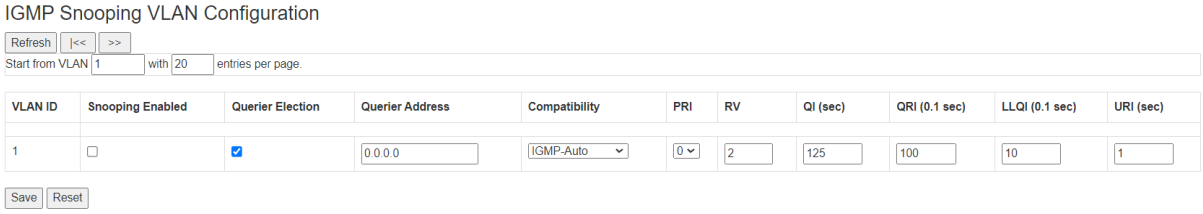


Figure 2-16.1.2: The IGMP Snooping VLAN Configuration.

Parameter description:

- **VLAN ID :**

  It displays the VLAN ID of the entry.

- **IGMP Snooping Enabled :**

  Enable the per-VLAN IGMP Snooping. Only up to128 VLANs can be selected. .

- **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.

- **Compatibility :**

  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.

- **PRI :**

  Priority of Interface.

  It indicates the IGMP control frame priority level generated by the system. These values can be used to prioritize different classes of traffic.

  The allowed range is 0 (best effort) to 7 (highest), default interface priority value is 0.

- **RV :**

  Robustness Variable. The Robustness Variable allows tuning for the expected packet loss on a network. The allowed range is 1 to 255; default robustness variable value is 2.

- **QI :**

  Query Interval. The Query Interval is the interval between General Queries sent by the Querier. The allowed range is 1 to 31744 seconds; default query interval is 125 seconds.

- **QRI :**

  Query Response Interval. The Max Response Time used to calculate the Max Resp Code inserted into the periodic General Queries. The allowed range is 0 to 31744 in tenths of seconds; default query response interval is 100 in tenths of seconds (10 seconds).

- **LLQI (LMQI for IGMP) :**

  Last Member Query Interval. The Last Member Query Time is the time value represented by the Last Member Query Interval, multiplied by the Last Member Query Count. The allowed range is 0 to 31744 in tenths of seconds; default last member query interval is 10 in tenths of seconds (1 second).

- **URI :**

  Unsolicited Report Interval. The Unsolicited Report Interval is the time between repetitions of a host's initial report of membership in a group. The allowed range is 0 to 31744 seconds, default unsolicited report interval is 1 second. .

Buttons

- **Save :**

  Click to save changes.

- **Reset :**

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

-  **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.

The section describes how to set the IGMP Port Group Filtering with the IGMP filtering feature, a user can exert this type of control. In some network Application environments, as like the metropolitan or multiple-dwelling unit (MDU) installations, a user might want to control the multicast groups to which a user on a switch port can belong. It allows the user to control the distribution of multicast services, such as IP/TV, based on some type of subscription or service plan.

With this feature, you can filter multicast joins on a per-port basis by configuring IP multicast profiles and associating them with individual switch ports. An IGMP profile can contain one or more multicast groups and specifies whether access to the group is permitted or denied. If an IGMP profile denying access to a multicast group is applied to a switch port, the IGMP join report requesting the stream of IP multicast traffic is dropped, and the port is not allowed to receive IP multicast traffic from that group. If the filtering action permits access to the multicast group, the IGMP report from the port is forwarded for normal processing.

IGMP filtering controls only IGMP membership join reports and has no relationship to the function that directs the forwarding of IP multicast traffic.

Web Interface

To configure the IGMP Snooping Port Filtering Profile Configuration in the web interface:

1. Click Configuration, IPMC, IGMP Snooping and Port Filtering Profile.
2. Scroll the Port to enable the Port Group Filtering.
3. Click the save to save the setting.
4. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.

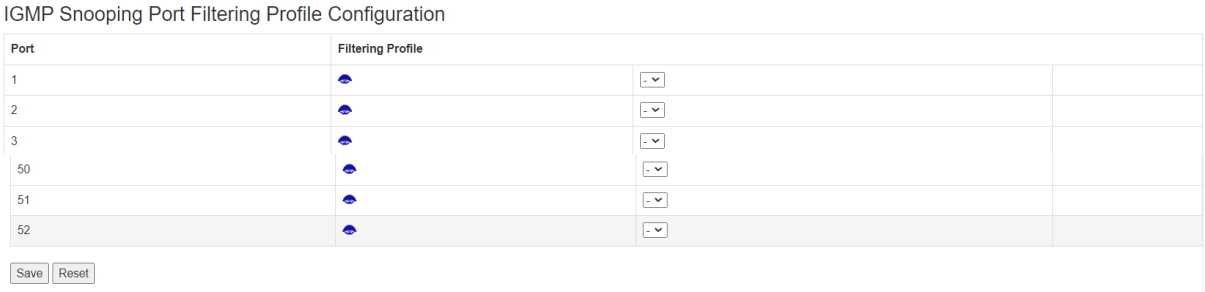


Figure 2-16.1.3: The IGMP Snooping Port Group Filtering Profile.

Parameter description:

- **Port :**

  The logical port for the settings.

- **Filtering Profile :**

  Select the IPMC Profile as the filtering condition for the specific port. Summary about the designated profile will be shown by clicking the view button.

- **Profile Management Button :**

  You can inspect the rules of the designated profile by using the following button:
  : List the rules associated with the designated profile.

Buttons

- **Save :**

  Click to save changes.

- **Reset :**

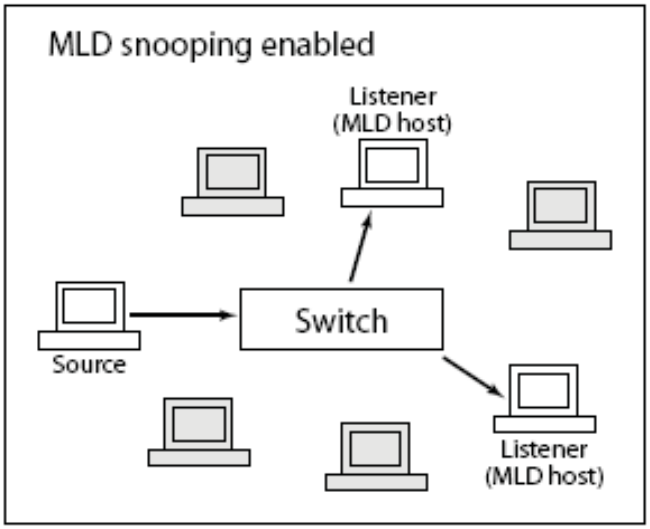
  Click to undo any changes made locally and revert to previously saved values.

2-16.2 MLD Snooping

Curiously enough, a network node that acts as a source of IPv6 multicast traffic is only an indirect participant in MLD snooping—it just provides multicast traffic, and MLD doesn't interact with it. (Note, however, that in an application like desktop conferencing a network node may act as both a source and an MLD host; but MLD interacts with that node only in its role as an MLD host.)

A source node creates multicast traffic by sending packets to a multicast address. In IPv6, addresses with the first eight bits set (that is, "FF" as the first two characters of the address) are multicast addresses, and any node that listens to such an address will receive the traffic sent to that address. Application software running on the source and destination systems cooperates to determine what multicast address to use. (Note that this is a function of the application software, not of MLD.)

When MLD snooping is enabled on a VLAN, the switch acts to minimize unnecessary multicast traffic. If the switch receives multicast traffic destined for a given multicast address, it forwards that traffic only to ports on the VLAN that have MLD hosts for that address. It drops that traffic for ports on the VLAN that have no MLD hosts



2-16.2.1 Basic Configuration

The section will let you understand how to configure the MLD Snooping basic configuration and the parameters.

Web Interface

To configure the MLD Snooping Configuration in the web interface:

1. Click Configuration, IPMC, MLD Snooping and Basic Configuration.
2. Evoke to enable or disable the Global configuration parameters. Evoke the port to join Router port and Fast Leave.
3. Scroll to select the Throttling mode with unlimited or 1 to 10.
4. Click save to save the setting.
5. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.

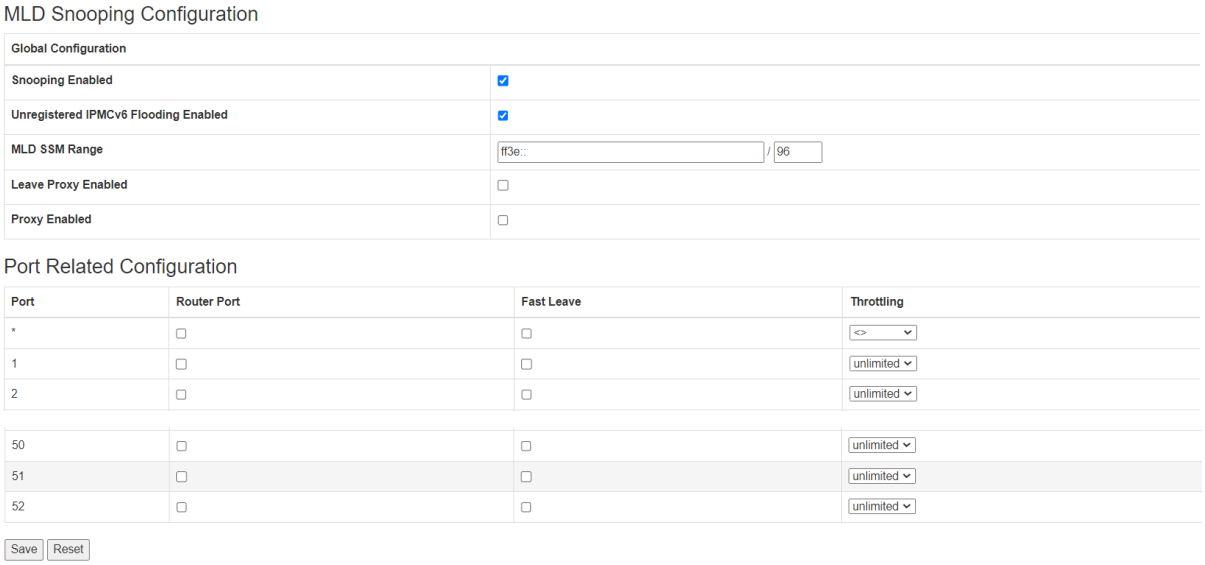


Figure 2-16.2.1: The MLD Snooping Configuration.

Parameter description:

- **Snooping Enabled :**

  Enable the Global MLD Snooping.

- **Unregistered IPMCv6 Flooding enabled :**

  Enable unregistered IPMCv6 traffic flooding.

  The flooding control takes effect only when MLD Snooping is enabled.

  When MLD Snooping is disabled, unregistered IPMCv6 traffic flooding is always active in spite of this setting.

- **MLD SSM Range :**

  SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address range.
  Assign valid IPv6 multicast address as prefix with a prefix length (from 8 to 128) for the range.

- **Leave Proxy Enabled :**

  Enable MLD Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.

- **Proxy Enabled :**

  Enable MLD Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.

- **Fast Leave :**

  Enable the fast leave on the port.
  System will remove group record and stop forwarding data upon receiving the MLDv1 leave message without sending last member query messages.
  It is recommended to enable this feature only when a single MLDv1 host is connected to the specific port.

- **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 MLD querier. If an aggregation member port is selected as a router port, the whole aggregation will act as a router 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.

When MLD snooping is enabled on a VLAN, the switch acts to minimize unnecessary multicast traffic. If the switch receives multicast traffic destined for a given multicast address, it forwards that traffic only to ports on the VLAN that have MLD hosts for that address. It drops that traffic for ports on the VLAN that have no MLD hosts

The 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.

Web Interface

To configure the MLD Snooping VLAN Configuration in the web interface:

1. Click Configuration, IPMC, MLD Snooping and VLAN Configuration.
2. Specify the VLAN ID with entries per page.
3. Click save to save changes
4. Click “Refresh” to refresh an entry of the MLD Snooping VLAN Configuration Information.
5. Click “<< or > “to move to previous or next entry.

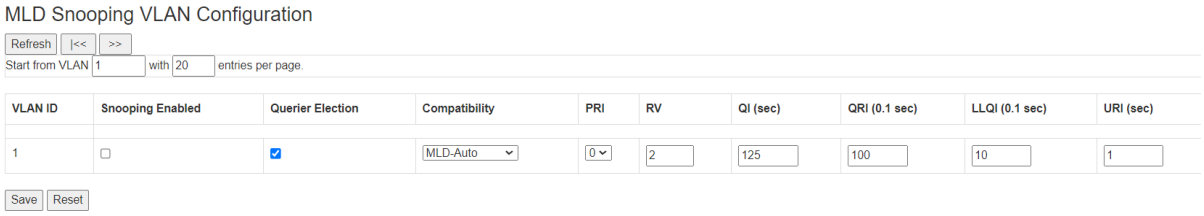


Figure 2-16.2.2: The MLD Snooping VLAN Configuration.

Parameter description:

- **VLAN ID :**

  It displays the VLAN ID of the entry.

- **MLD Snooping Enabled :**

  Enable the per-VLAN MLD Snooping. Up to 32 VLANs can be selected for MLD Snooping.

- **Querier Election :**

  Enable to join MLD Querier election in the VLAN. Disable to act as a MLD Non-Querier.

- **Compatibility :**

  Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of MLD operating on hosts and routers within a network.

  The allowed selection is MLD-Auto, Forced MLDv1, default compatibility value is MLD-Auto.

- **PRI :**

  Priority of Interface.

  It indicates the MLD control frame priority level generated by the system. These values can be used to prioritize different classes of traffic.

  The allowed range is 0 (best effort) to 7 (highest), default interface priority value is 0.

- **RV :**

  Robustness Variable.

The Robustness Variable allows tuning for the expected packet loss on a link.

The allowed range is 1 to 255, default robustness variable value is 2.

- **QI :**

  Query Interval.

  The Query Interval is the interval between General Queries sent by the Querier.

  The allowed range is 1 to 31744 seconds, default query interval is 125 seconds.

- **QRI :**

  Query Response Interval.

  The Maximum Response Delay used to calculate the Maximum Response Code inserted into the periodic General Queries.

  The allowed range is 0 to 31744 in tenths of seconds, default query response interval is 100 in tenths of seconds (10 seconds).

- **LLQI :**

  Last Listener Query Interval.

  The Last Listener Query Interval is the Maximum Response Delay used to calculate the Maximum Response Code inserted into Multicast Address Specific Queries sent in response to Version 1 Multicast Listener Done messages. It is also the Maximum Response Delay used to calculate the Maximum Response Code inserted into Multicast Address and Source Specific Query messages.

  The allowed range is 0 to 31744 in tenths of seconds, default last listener query interval is 10 in tenths of seconds (1 second).

- **URI :**

  Unsolicited Report Interval.

  The Unsolicited Report Interval is the time between repetitions of a node's initial report of interest in a multicast address.

  The allowed range is 0 to 31744 seconds, default unsolicited report interval is 1 second.

Buttons

- **Save :**

  Click to save changes.

- **Reset :**

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

-  **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.

The section describes that you could to set the Port Group Filtering in the MLD Snooping function. On the UI that you could add new filtering group and safety policy.

Web Interface

To configure the Port Filtering Profile in the web interface:

1. Click Configuration, IPMC, MLD Snooping and Port Filtering Profile.
2. Scroll the Port to enable the Port Group Filtering. Specify the Filtering Groups in the blank field.
3. Click the save to save the setting.
4. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.

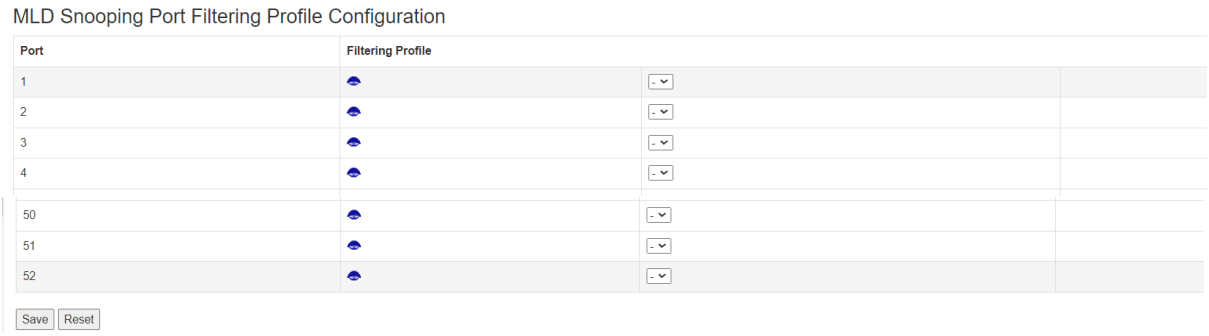


Figure 2-16.2.3: The MLD Snooping Port Group Filtering Configuration

Parameter description:

- **Port :**

  The logical port for the settings.

- **Filtering Profile :**

  Select the IPMC Profile as the filtering condition for the specific port. Summary about the designated profile will be shown by clicking the view button.

Buttons

- **Save :**

  Click to save changes.

- **Reset :**

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

- **Profile Management Button :**

  You can inspect the rules of the designated profile by using the following button:

  : List the rules associated with the designated profile.

2-17 LLDP

The switch supports the LLDP. For current information on your switch model, The Link Layer Discovery Protocol (LLDP) provides a standards-based method for enabling switches to advertise themselves to adjacent devices and to learn about adjacent LLDP devices. The Link Layer Discovery Protocol (LLDP) is a vendor-neutral Link Layer protocol in the Internet Protocol Suite used by network devices for advertising their identity, capabilities, and neighbors on a IEEE 802 local area network, principally wired Ethernet. The protocol is formally referred to by the IEEE as Station and Media Access Control Connectivity Discovery specified in standards document IEEE 802.1AB.

2-17.1 LLDP

You can per port to do the LLDP configuration and the detail parameters, the settings will take effect immediately. This page allows the user to inspect and configure the current LLDP port settings.

Web Interface

To configure the LLDP in the web interface:

1. Click Configuration, LLDP and LLDP.
2. Modify LLDP parameters
3. Set the required mode for transmitting or receiving LLDP messages
4. Specify the information to include in the TLV field of advertised messages
5. Click the Save to save the setting.
6. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.

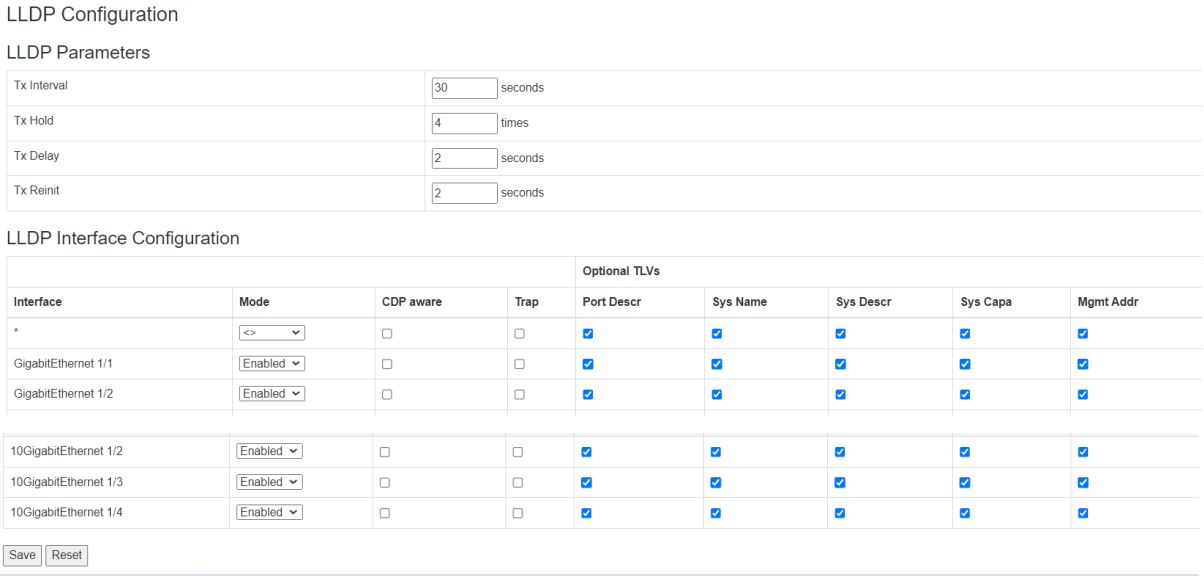


Figure 2-17.1: The LLDP Configuration

Parameter description:

LLDP Parameters

- **Tx Interval :**

  The switch periodically transmits LLDP frames to its neighbours 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 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 port is disabled, LLDP is disabled or the switch is rebooted, an 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 Port Configuration

- **Port :**

  The switch port number of the logical LLDP port.

- **Mode :**

  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.

  Enabled: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 port 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 ports have CDP awareness disabled the switch forwards CDP frames received from neighbor devices. If at least one port has CDP awareness enabled all CDP frames are terminated by the switch.

NOTE: When CDP awareness on a port is disabled the CDP information isn't removed immediately, but gets when the hold time is exceeded.

- **Port Descr :**

  Optional TLV: When checked the "port description" is included in LLDP information transmitted.

- **Sys Name :**

  Optional TLV: When checked the "system name" is included in LLDP information transmitted.

- **Sys Descr :**

  Optional TLV: When checked the "system description" is included in LLDP information transmitted.

- **Sys Capa :**

  Optional TLV: When checked the "system capability" is included in LLDP information transmitted.

- **Mgmt Addr :**

  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.

2-17.2 LLDP-MED

Media Endpoint Discovery is an enhancement of LLDP, known as LLDP-MED that provides the following facilities:

Auto-discovery of LAN policies (such as VLAN, Layer 2 Priority and Differentiated services (Diffserv) settings) enabling plug and play networking.

Device location discovery to allow creation of location databases and, in the case of Voice over Internet Protocol (VoIP), Enhanced 911 services.

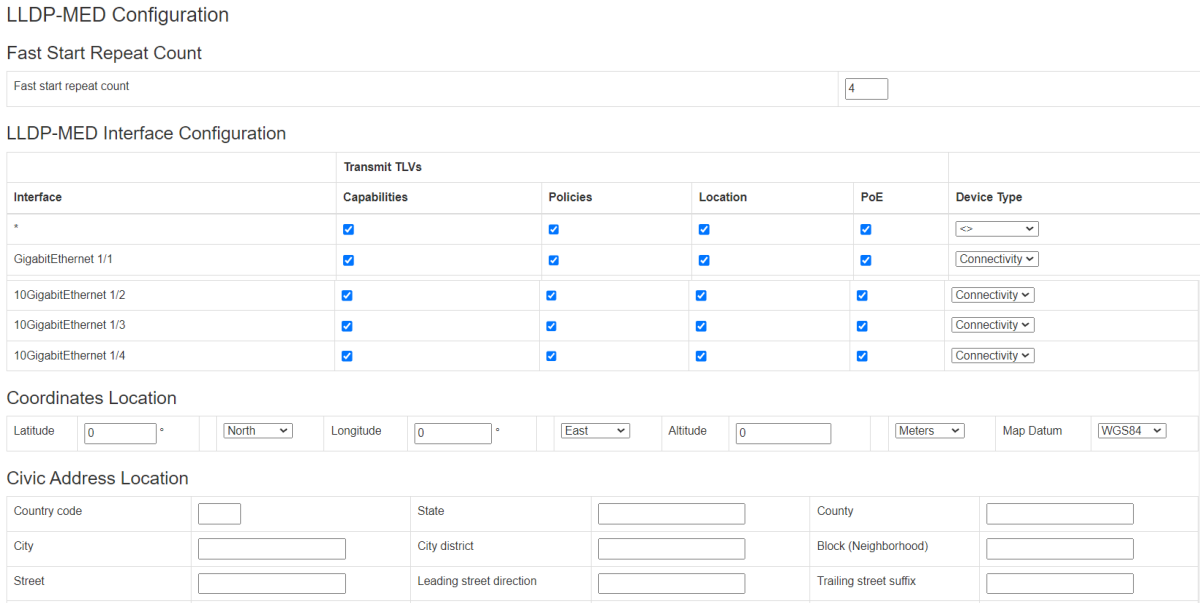
Inventory management, allowing network administrators to track their network devices, and determine their characteristics (manufacturer, software and hardware versions, and serial or asset number).

This page allows you to configure the LLDP-MED. This function applies to VoIP devices which support LLDP-MED.

Web Interface

To configure the LLDP-MED in the web interface:

1. Click Configuration, LLDP and LLDP-MED Configuration.
2. Modify Fast start repeat count parameter, default is 4
3. Modify Coordinates Location parameters
4. Fill Civic Address Location parameters
5. Add new policy
6. Click save, will show following Policy Port Configuration
7. Select Policy ID for each port
8. Click the save to save the setting.
9. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.



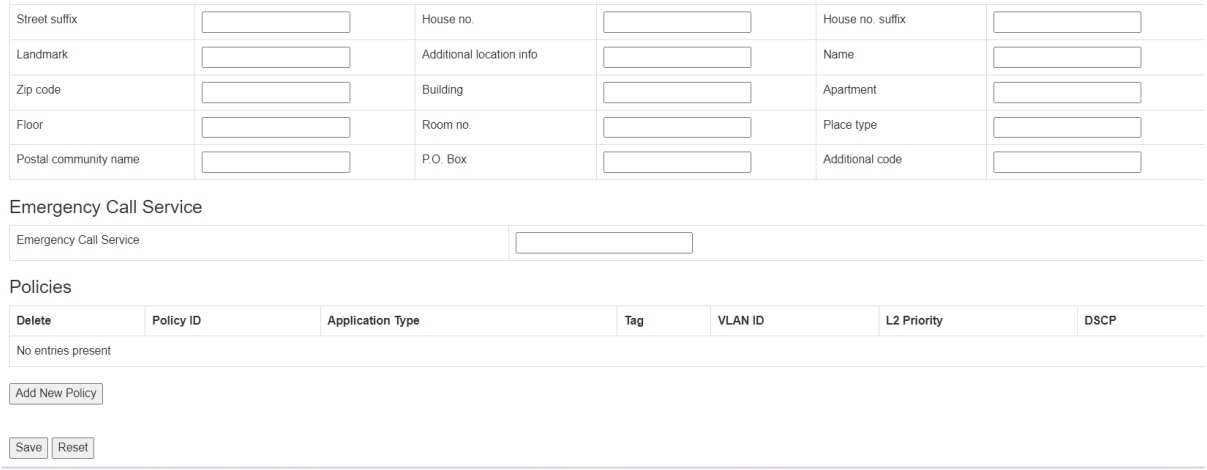


Figure 2-17.2: Te LLDP-MED Configuration

Parameter description:

Fast start repeat count

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 port. 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.

LLDP Interface Configuration

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.

- **Transmit TLVs - Capabilities:**

  When checked the switch's capabilities is included in LLDP-MED information transmitted.

- **Transmit TLVs - Policies:**

  When checked the configured policies for the interface is included in LLDP-MED information transmitted.

- **Transmit TLVs - Location:**

  When checked the configured location information for the switch is included in LLDP-MED information transmitted.

- **Transmit TLVs - PoE:**

  When checked the configured PoE (Power Over Ethernet) information for the interface is included in LLDP-MED information transmitted.

- **Device Type:**

  Any LLDP-MED Device is operating as a specific type of LLDP-MED Device, which may be either a Network Connectivity Device or a specific Class of Endpoint Device, as defined below.

  A Network Connectivity Device is a LLDP-MED Device that provides access to the IEEE 802 based LAN infrastructure for LLDP-MED Endpoint Devices

  An LLDP-MED Network Connectivity Device is a LAN access device based on any of the following technologies :

  1. LAN Switch/Router

  2. IEEE 802.1 Bridge

  3. IEEE 802.3 Repeater (included for historical reasons)

  4. IEEE 802.11 Wireless Access Point

  5. Any device that supports the IEEE 802.1AB and MED extensions that can relay IEEE 802 frames via any method.

  An Endpoint Device a LLDP-MED Device that sits at the network edge and provides some aspect of IP communications service, based on IEEE 802 LAN technology.

  The main difference between a Network Connectivity Device and an Endpoint Device is that only an Endpoint Device can start the LLDP-MED information exchange.

  Even though a switch always should be a Network Connectivity Device, it is possible to configure it to act as an Endpoint Device, and thereby start the LLDP-MED information exchange (In the case where two Network Connectivity Devices are connected together)

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, and Prime Meridian Name: Greenwich.

  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).A couple of notes to the limitation of 250 characters.

1) If more than one civic address location is used, each of the additional civic address locations will use 2 extra characters in addtion to the civic address location text.

2) The 2 letter country code is not part of the 250 characters limitation.

- **Country code :**

  The two-letter ISO 3166 country code in capital ASCII letters - Example: DK, DE or US.

- **State :**

  National subdivisions (state, canton, region, province, prefecture).

- **County :**

  County, parish, gun (Japan), district.

- **City :**

  City, township, shi (Japan) - Example: Copenhagen.

- **City district :**

  City division, borough, city district, ward, chou (Japan).

- **Block (Neighbourhood) :**

  Neighbourhood, block.

- **Street :**

  Street - Example: Poppelvej.

- **Leading street direction :**

  Leading street direction - Example: N.

- **Trailing street suffix :**

  Trailing street suffix - Example: SW.

- **Street suffix :**

  Street suffix - Example: Ave, Platz.

- **House no. :**

  House number - Example: 21.

- **House no. suffix :**

  House number suffix - Example: A, 1/2.

- **Landmark :**

  Landmark or vanity address - Example: Columbia University.

- **Additional location info :**

  Additional location info - Example: South Wing.

- **Name :**

  Name (residence and office occupant) - Example: Flemming Jahn.

- **Zip code :**

  Postal/zip code - Example: 2791.

- **Building :**

  Building (structure) - Example: Low Library.

- **Apartment :**

  Unit (Apartment, suite) - Example: Apt 42.

- **Floor :**

  Floor - Example: 4.

- **Room no. :**

  Room number - Example: 450F.

- **Place type :**

  Place type - Example: Office.

- **Postal community name :**

  Postal community name - Example: Leonia.

- **P.O. Box :**

  Post office box (P.O. BOX) - Example: 12345.

- **Additional code :**

  Additional code - Example: 1320300003.

  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.

Policies

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:

1. Layer 2 VLAN ID (IEEE 802.1Q-2003)

2. Layer 2 priority value (IEEE 802.1D-2004)

3. Layer 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:

1. Voice

2. Guest Voice

3. Softphone Voice

4. Video Conferencing

5. Streaming Video

6. Control / Signalling (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.

- **Policy ID :**

  ID for the policy. This is auto generated and shall be used when selecting the polices that shall be mapped to the specific ports.

- **Application Type :**

  Intended use of the application types:

  1. 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.

2. Voice Signalling (conditional) - for use in network topologies that require a different policy for the voice signalling 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.

3. 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.

4. Guest Voice Signalling (conditional) - for use in network topologies that require a different policy for the guest voice signalling 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.

5. 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.

6. Video Conferencing - for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services.

7. 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.

8. Video Signalling (conditional) - for use in network topologies that require a separate policy for the video signalling 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 port 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.

- **Adding 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".

Port Policies Configuration

Every port may advertise a unique set of network policies or different attributes for the same network policies, based on the authenticated user identity or port configuration.

- **Interface:**

  The port number to which the configuration applies.

- **Policy ID :**

  The set of policies that shall apply to a given port. The set of policies is selected by check marking the checkboxes that corresponds to the policies.

Buttons

- **Save :**

  Click to save changes.

- **Reset :**

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

- **Delete**

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

2-18 PoE

Power-over-Ethernet (PoE), means Ethernet network power supply via 100BASE-TX, 1000BASE-T. Its maximum power distance is 100 meters. By PoE power system, based on Ethernet wiring network of UTP Cat5 or higher Cable, it can give power to IP camera, VoIP phone, wireless AP, as well as transmit data. So there is no need to concern about the power wire building, reducing the cost of networking building.

PoE power supply system has unified standard, IEEE 802.3af and 802.3at. So devices from different manufacturers have no problem in general usage, as long as they are complied with these standards.

PD, it is defined as powered device in the PoE Power Supply System , primarily including IP camera, wireless AP, network VoIP phone, and other IP-based terminal equipment.

The whole process of PoE:

Detection: At beginning, PSE device output a very small voltage, to detect and judge if its linked PD is IEEE802.3af / IEEE802.3at compliant device. Only if detected that PD is a standard compliant device, then it will go to next step.

PD Classification: After detected PDs, PSE will classify them and recognize what is the power that PD required.

Power up: When above 2 steps finished, PSE start feeding required power for PD, with 44~57VDC output voltage.

Power supply: PSE provides stable 44~57V DC to PDs, and auto feeding power as requirement of PDs. Maximum power of single PoE port for IEEE 802.3af devices: 15.4W; Maximum power of single PoE port for IEEE 802.3at devices: 25.5W.

Disconnection: If PD is disconnected or user disable PoE from management software, PSE will quickly(300- 400ms) stop powering PD.

In any moment of PSE powering PD process, PSE will stop working and then restart from step1 if abnormal situation happens, such as PD Short circuit, power consumption is higher than feeding power, and so on.

2-18.1 PoE config

You can per port to do the PoE configuration and the detail parameters, the settings will take effect immediately.

Web Interface

To configure the PoE in the web interface:

1. Click Configuration, PoE and PoE Config.
2. Modify PoE parameters
3. Click the Save to save the setting.
4. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.

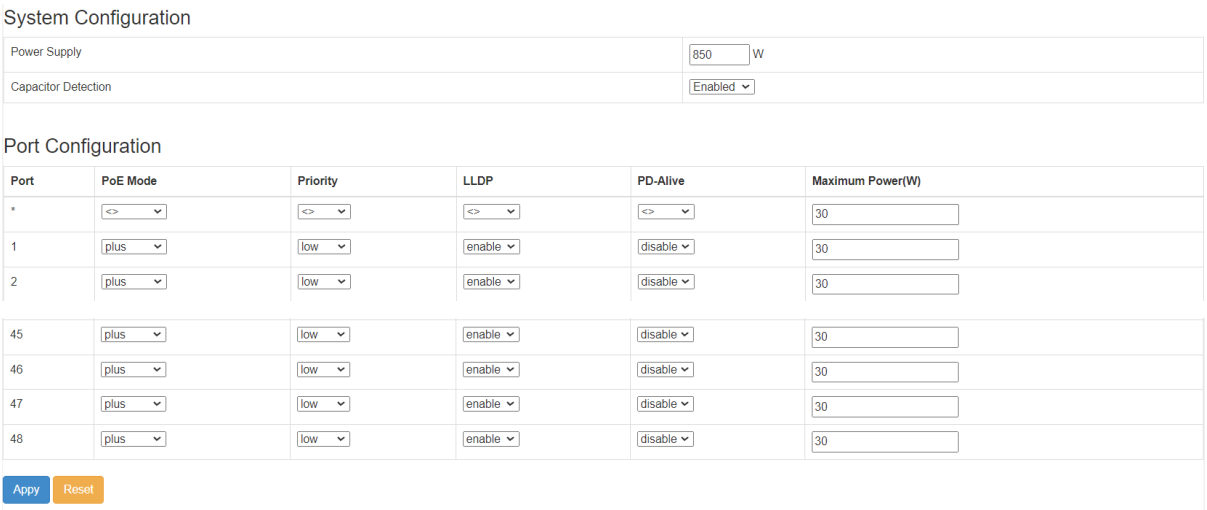


Figure 2-18.1: The PoE Config

Parameter description:

- **Power Supply :**

  The max PoE output for the swicth. It depends on the switch's power supply.

- **Capacitor Detection :**

  To detect the PD devices

- **PoE Mode :**

  To define the PoE mode, disable the PoE function or enable standard (AF) or plus(AT) modes.

- **Priority :**

  Define the priority of the PoE port. Priority from low to high is Low, High, Critical.

- **LLDP:**

  Enable or disable the LLDP function for the port

- **PD-Alive :**

  The port could monitor the RX traffic statistics and POE status, if it detects to have no traffic received about ~2minutes while POE status is on, the switch will reset the POE output.

- **Maximum Power(W) :**

  The max PoE output for the port. For AT mode max 30W, for BT mode max 90W

Buttons

- **Save:**

  Click to save changes.

- **Reset :**

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

2-18.2 PoE Schedule

In this page could configure the PoE schedule function.

Web Interface

Before configure the PoE schedule function, please set up the NTP server to get the correct day time.

To configure the PoE Schedule function in the web interface:

1. Click Configuration, PoE and PoE Schedule
2. Select the parameters
3. Click save

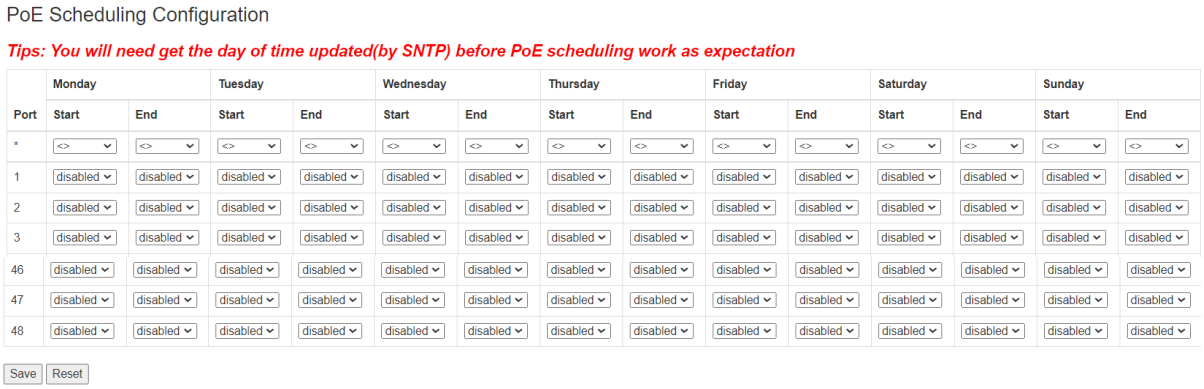


Figure 2-18.2: The PoE Schedule Configuration

Parameter description:

- **Start :**

  To select the time of turning on the PoE port.

- **End:**

  To select the time of turning off the PoE port

Buttons

- **Save :**

  Click to save changes.

- **Reset :**

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

2-19 MAC Table

Switching of frames is based upon the DMAC address contained in the frame. The switch builds up a table that maps MAC addresses to switch ports for knowing which ports the frames should go to (based upon the DMAC address in the frame). This table contains both static and dynamic entries. The static entries are configured by the network administrator if the administrator wants to do a fixed mapping between the DMAC address and switch ports.
The frames also contain a MAC address (SMAC address), which shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frame with the corresponding SMAC address have been seen after a configurable age time

Web Interface

To configure MAC Address Table in the web interface:

Aging Configuration

1. Click configuration and MAC Table.
2. Specify the Disable Automatic Aging and Aging Time.
3. Click the Save to save the setting.
4. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.

MAC Table Learning

1. Click configuration and MAC Table.
2. Specify the Port Members (Auto, Disable, Secure).
3. Click the Save to save the setting.
4. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.

Static MAC Table Configuration

1. Click configuration, MAC Table and Add new Static entry.
2. Specify the VLAN IP and Mac address, Port Members.
3. Click the Save to save the setting.
4. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.

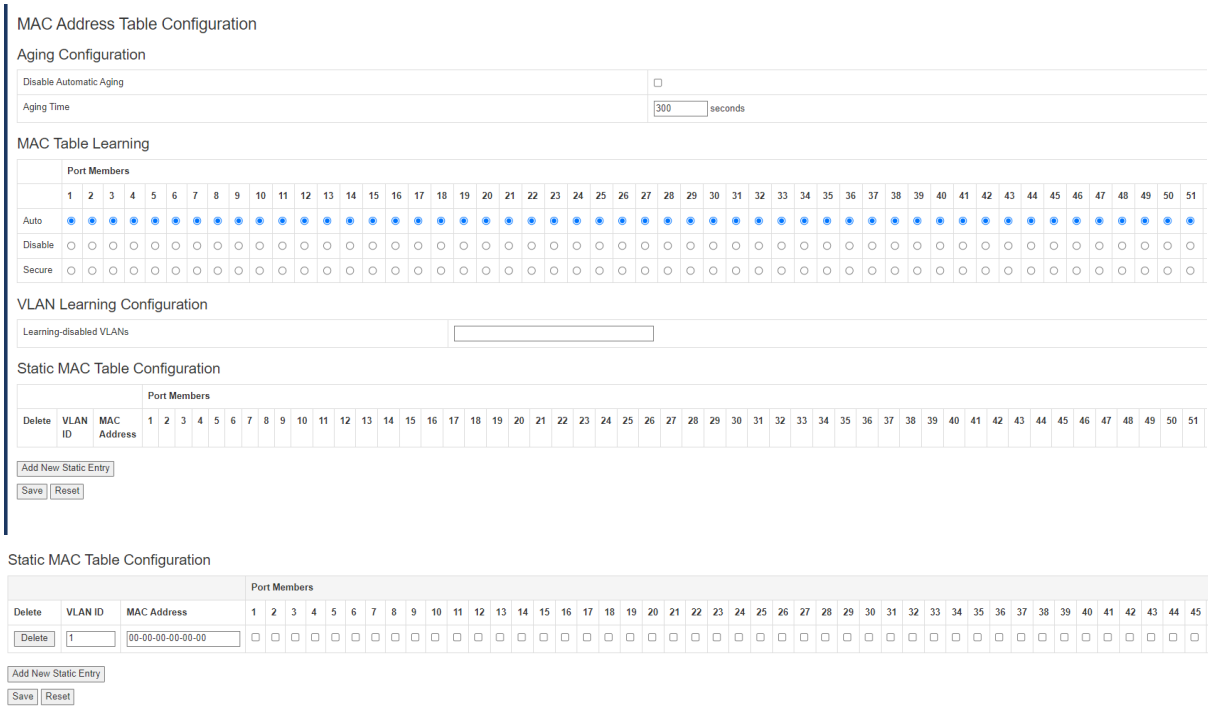


Figure 2-19: The MAC Address Table Configuration

Parameter description:

Aging Configuration

By default, dynamic entries are removed from the MAC table after 300 seconds. This removal is also called aging.

Configure aging time by entering a value here in seconds; for example, Age time  seconds.

The allowed range is 10 to 1000000 seconds.

Disable the automatic aging of dynamic entries by checking  Disable automatic 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. An example of such a module is the MAC-Based Authentication under 802.1X. Each port 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.

- **Secure :**

  Only static MAC entries are learned, all other frames are dropped.

NOTE: Make sure that the link used for managing the switch is added to the Static Mac Table before changing to secure learning mode, otherwise the management link is lost and can only be restored by using another non-secure port or by connecting to the switch via the serial interface.

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 maximum of 64 entries is for the whole stack, and not per switch.

The MAC table is sorted first by VLAN ID and then by MAC address.

- **VLAN ID :**

  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

- **Adding a New Static Entry :**

  Click Add New Static Entry to add a new entry to the static MAC table. Specify the VLAN ID, MAC address, and port members for the new entry. Click "Apply".

- **Save :**

  Click to save changes.

- **Reset :**

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

- **Delete :**

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

2-20 VLANs

To assign a specific VLAN for management purpose. The management VLAN is used to establish an IP connection to the switch from a workstation connected to a port in the VLAN. This connection supports a VSM, SNMP, and Telnet session. By default, the active management VLAN is VLAN 1, but you can designate any VLAN as the management VLAN using the Management VLAN window. Only one management VLAN can be active at a time.

When you specify a new management VLAN, your HTTP connection to the old management VLAN is lost. For this reason, you should have a connection between your management station and a port in the new management VLAN or connect to the new management VLAN through a multi-VLAN route

2-20.1 Configuration

This page allows for controlling VLAN configuration on the switch.
The page is divided into a global section and a per-port configuration section.

Web Interface

To configure VLAN membership configuration in the web interface:

1. Click Configuration, VLANS and Configuration.
2. Modify Global VLAN Configuration parameter.
3. Scroll the Mode, Port VLAN and Port Type to enable the Port VLAN Configuration parameter.
4. Click the Save to save the setting.
5. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.

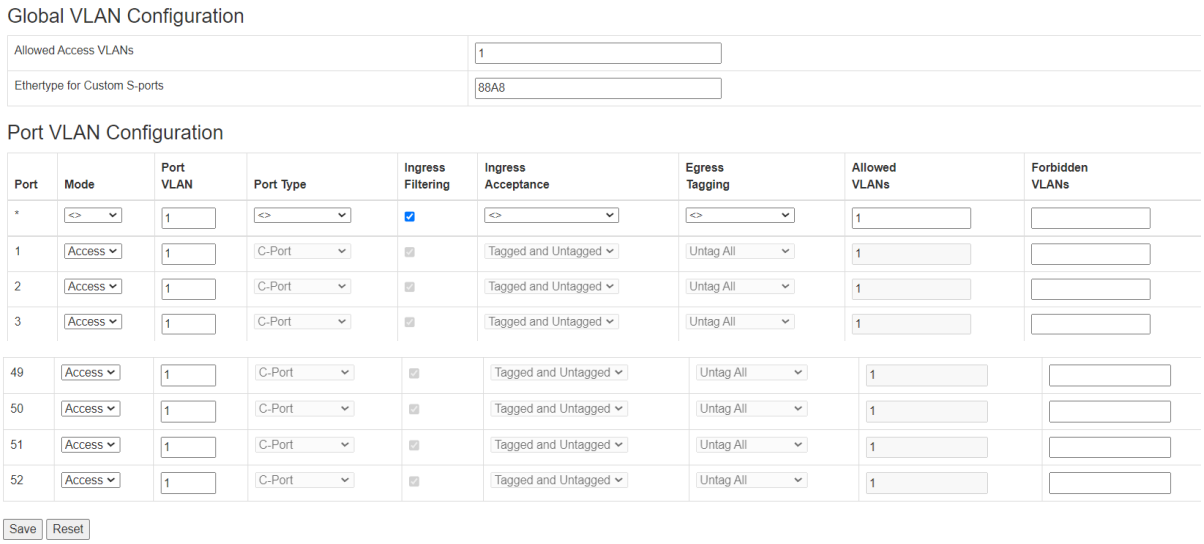


Figure 2-20.1: The VLAN Configuration

Parameter description:

Global VLAN Configuration

- **Allowed Access VLANs :**

  This field shows the allowed Access VLANs, i.e. it only affects ports configured as Access ports. Ports in other modes are members of all VLANs specified in the Allowed VLANs field. By default, only VLAN 1 is enabled. More VLANs may be created by using a list syntax where the individual elements are separated by commas. Ranges are specified with a dash separating the lower and upper bound.

  The following example will create VLANs 1, 10, 11, 12, 13, 200, and 300: 1,10-13,200,300. Spaces are allowed in between the delimiters.

- **Ethertype for Custom S-ports :**

  This field specifies the ethertype/TPID (specified in hexadecimal) used for Custom S-ports. The setting is in force for all ports whose Port Type is set to S-Custom-Port.

Port VLAN Configuration

- **Port :**

  This is the logical port number of this row.

- **Mode :**

  The port mode (default is Access) determines the fundamental behavior of the port in question. A port can be in one of three modes as described below.
  Whenever a particular mode is selected, the remaining fields in that row will be either grayed out or made changeable depending on the mode in question.
  Grayed out fields show the value that the port will get when the mode is applied.
  Access:
  Access ports are normally used to connect to end stations. Dynamic features like Voice VLAN may add the port to more VLANs behind the scenes. Access ports have the following characteristics:
  • Member of exactly one VLAN, the Port VLAN (a.k.a. Access VLAN), which by default is 1,
  • accepts untagged frames and C-tagged frames,
  • discards all frames that are not classified to the Access VLAN,
  • on egress all frames are transmitted untagged.
  Trunk:
  Trunk ports can carry traffic on multiple VLANs simultaneously, and are normally used to connect to other switches. Trunk ports have the following characteristics:
  • By default, a trunk port is member of all existing VLANs. This may be limited by the use of Allowed VLANs,
  • unless VLAN Trunking is enabled on the port, frames classified to a VLAN that the port is not a member of will be discarded,
  • by default, all frames but frames classified to the Port VLAN (a.k.a. Native VLAN) get tagged on egress. Frames classified to the Port VLAN do not get C-tagged on egress,
  • egress tagging can be changed to tag all frames, in which case only tagged frames are accepted on ingress,
  • VLAN trunking may be enabled.
  Hybrid:
  Hybrid ports resemble trunk ports in many ways, but adds additional port configuration features. In addition to the characteristics described for trunk ports, hybrid ports have these abilities:
  • Can be configured to be VLAN tag unaware, C-tag aware, S-tag aware, or S-custom-tag aware,
  • ingress filtering can be controlled,
  • ingress acceptance of frames and configuration of egress tagging can be configured independently.

- **Port VLAN :**

Determines the port's VLAN ID (a.k.a. PVID). Allowed VLANs are in the range 1 through 4095, default being 1.
On ingress, frames get classified to the Port VLAN if the port is configured as VLAN unaware, the frame is untagged, or VLAN awareness is enabled on the port, but the frame is priority tagged (VLAN ID = 0).
On egress, frames classified to the Port VLAN do not get tagged if Egress Tagging configuration is set to untag Port VLAN.
The Port VLAN is called an "Access VLAN" for ports in Access mode and Native VLAN for ports in Trunk or Hybrid mode.

- **Port Type :**

  Ports in hybrid mode allow for changing the port type, that is, whether a frame's VLAN tag is used to classify the frame on ingress to a particular VLAN, and if so, which TPID it reacts on. Likewise, on egress, the Port Type determines the TPID of the tag, if a tag is required.
  Unaware:
  On ingress, all frames, whether carrying a VLAN tag or not, get classified to the Port VLAN, and possible tags are not removed on egress.
  C-Port:
  On ingress, frames with a VLAN tag with TPID = 0x8100 get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with a C-tag.
  S-Port:
  On ingress, frames with a VLAN tag with TPID = 0x8100 or 0x88A8 get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with an S-tag.
  S-Custom-Port:
  On ingress, frames with a VLAN tag with a TPID = 0x8100 or equal to the Ethertype configured for Custom-S ports get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with the custom S-tag.

- **Ingress Filtering :**

  Hybrid ports allow for changing ingress filtering. Access and Trunk ports always have ingress filtering enabled.
  If ingress filtering is enabled (checkbox is checked), frames classified to a VLAN that the port is not a member of get discarded.
  If ingress filtering is disabled, frames classified to a VLAN that the port is not a member of are accepted and forwarded to the switch engine. However, the port will never transmit frames classified to VLANs that it is not a member of.

- **Ingress Acceptance :**

  Hybrid ports allow for changing the type of frames that are accepted on ingress.
  Tagged and untagged
  both tagged and untagged frames are accepted.
  Tagged Only
  Only tagged frames are accepted on ingress. Untagged frames are discarded.
  Untagged Only
  Only untagged frames are accepted on ingress. Tagged frames are discarded.

- **Egress Tagging :**

  Ports in Trunk and Hybrid mode may control the tagging of frames on egress.
  Untag Port VLAN
  Frames classified to the Port VLAN are transmitted untagged. Other frames are transmitted with the relevant tag.
  Tag All

All frames, whether classified to the Port VLAN or not, are transmitted with a tag.
Untag All
All frames, whether classified to the Port VLAN or not, are transmitted without a tag.
This option is only available for ports in Hybrid mode.

- **Allowed VLANs :**

  Ports in Trunk and Hybrid mode may control which VLANs they are allowed to become members of. Access ports can only be member of one VLAN, the Access VLAN.
  The field's syntax is identical to the syntax used in the Existing VLANs field. By default, a port may become member of all possible VLANs, and is therefore set to 1-4095.
  The field may be left empty, which means that the port will not be member of any of the existing VLANs, but if it is configured for VLAN Trunking it will still be able to carry all unknown VLANs.

- **Forbidden VLANs :**

  A port may be configured to never be member of one or more VLANs. This is particularly useful when dynamic VLAN protocols like MVRP and GVRP must be prevented from dynamically adding ports to VLANs.
  The trick is to mark such VLANs as forbidden on the port in question. The syntax is identical to the syntax used in the Existing VLANs field.
  By default, the field is left blank, which means that the port may become a member of all possible VLANs.

Buttons

- **Save :**

  Click to save changes.

- **Reset :**

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

2-20.2 SVL

This page allows for controlling SVL configuration on the switch.
In SVL, one or more VLANs map to a Filter ID (FID). By default, there is a one-to-one mapping from VLAN to FID, in which case the switch acts as an IVL bridge, but with SVL multiple VLANs may share the same MAC address table entries.

Web Interface

To configure VLAN membership configuration in the web interface:

1. Click Configuration, VLANS and SVL.
2. Click Add FID to add a new entry
3. Specify the SVL parameters
4. Click the Save to save the setting.
5. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.

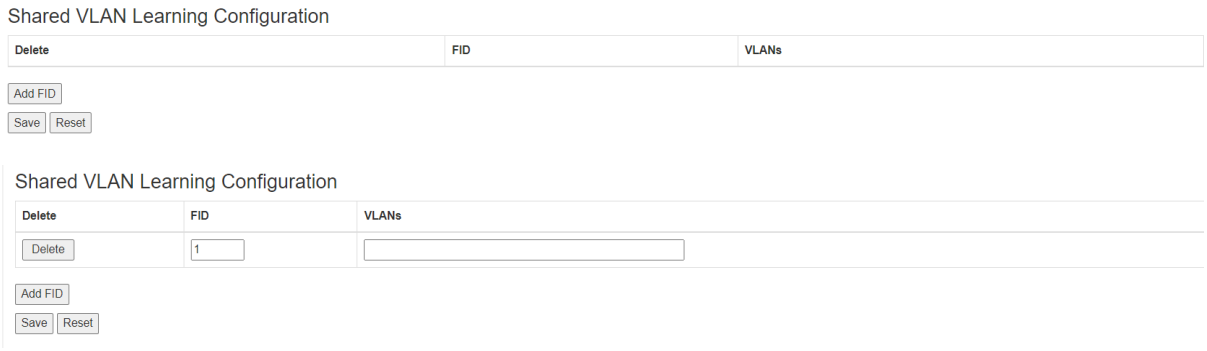


Figure 2-20.2: The SVL Configuration

Parameter description:

- **FID :**

  The Filter ID (FID) is the ID that VLANs get learned on in the MAC table when SVL is in effect. No two rows in the table can have the same FID and the FID must be a number between 1 and 4095.

- **VLANs :**

  List of VLANs mapped into FID.
  The syntax is as follows: Individual VLANs are separated by commas. Ranges are specified with a dash separating the lower and upper bound.
  The following example will map VLANs 1, 10, 11, 12, 13, 200, and 300: 1,10-13,200,300. Spaces are allowed in between the delimiters. The range of valid VLANs is 1 to 4095.
  The same VLAN can only be a member of one FID. A message will be displayed if one VLAN is grouped into two or more FIDs.
  All VLANs must map to a particular FID, and by default VLAN x maps to FID x. This implies that if FID x is defined, then VLAN x is implicitly a member of FID x unless it is specified for another FID. If FID x doesn't exist, a confirmation message will be displayed, asking whether to continue adding VLAN x implicitly to FID x.

Buttons

- **Delect :**

A previously allocated FID can be deleted by the use of this button.

- **Add FID :**

  Add a new row to the SVL table. The FID will be pre-filled with the first unused FID.

- **Save :**

  Click to save changes.

- **Reset :**

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

2-21 VLAN Translation

2-21.1 Port to Group Configuration

This page allows you to configure switch Ports to use a given VLAN Translation Mapping Group. This will enable all VLAN Translation mappings of that group (if any) on the selected switch port.

Web Interface

To configure port to group configuration in the web interface:

1. Click Configuration, VLAN Translation and Port to Group Configuration.
2. Evoke group configuration.
3. Click the Save to save the setting.
4. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.

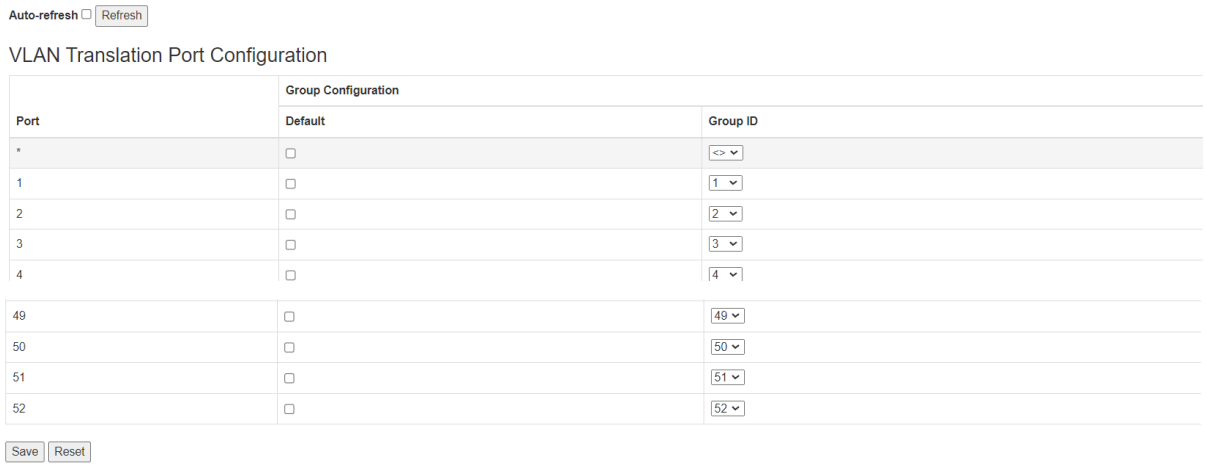


Figure 2-21.1: The Port to Group Configuration

Parameter description:

- **Port:**

  The Port column shows the list of ports for which you can configure the VLAN Translation Mapping Group.

- **Default :**

  To set the switch port to use the default VLAN Translation Group click the checkbox and press Save.

- **Group ID :**

  The VLAN Translation mappings are organized into Groups, identified by the Group ID. This way a port is configured to use a number of VLAN Translation mappings easily by simply configuring it to use a given group. Then number of possible groups in a switch is equal to the number of ports present in this switch. A port can be configured to use any of the groups, but only one at any given time. Multiple ports can be configured to use the same group. A valid Group ID is an integer value from 1 to 10.
  Note: By default, each port is set to use the group with Group ID equal to the port

number. For example, port #1 is by default set to use group with GID = 1.

Buttons

- **Auto-Refresh :**

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

- **Refresh:**

  Click to refresh the page immediately.

- **Save :**

  Click to save changes.

- **Reset :**

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

2-21.2 VLAN Translation Mappings

This page displays current VLAN Translation mapping configurations. The settings can also be configured here.

Web Interface

To configure VLAN translation mappings in the web interface:

1. Click Configuration, VLAN Translation and VLAN Translation Mappings.
2. Click ⊕ to add a mapping table
3. Specify the Group ID DIR, VID and TVID
4. Click the Save to save the setting.

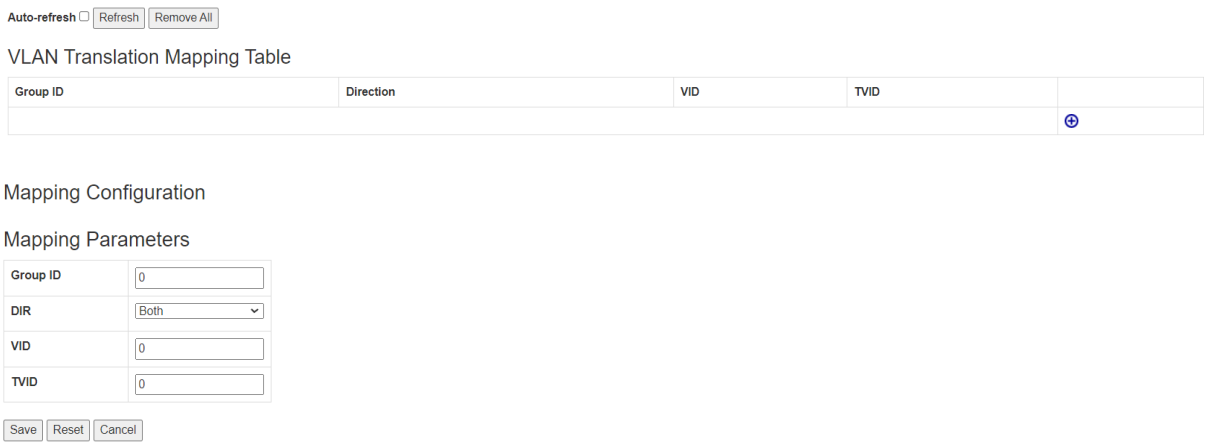


Figure 2-21.2: The VLAN Translation Mappings Configuration

Parameter description:

- **Group ID:**

  The VLAN Translation mappings are organized into Groups, identified by the Group ID. This way a port is configured to use a number of VLAN Translation mappings easily by simply configuring it to use a given group. Then number of possible groups in a switch is equal to the number of ports present in this switch. A port can be configured to use any of the groups, but only one at any given time. Multiple ports can be configured to use the same group. A valid Group ID is an integer value from 1 to 10.
  Note: By default, each port is set to use the group with Group ID equal to the port number. For example, port #1 is by default set to use group with GID = 1.

- **Direction :**

  Indicates the direction of the VLAN Translation and it refers to the switch. The direction can be 'Ingress', where the translation takes place on the VLAN ID of frames entering the switch port, 'Egress', where the translation takes place on the VLAN ID of frames exiting the switch port, or 'Both', where the translation takes place on both of the above directions.

- **VID :**

  Indicates the VLAN ID of the mapping (i.e. 'source' VLAN). A valid VLAN ID ranges

from 1 to 4095.

- **TVID :**

  Indicates the translated VLAN ID to which a VLAN ID of a frame will be translated to. A valid translated VLAN ID ranges from 1 to 4095.

Buttons

- **Cancel:**

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

- **Save :**

  Click to save changes.

- **Reset :**

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

2-22 Private VLANs

2-22.1 Membership

The Private VLAN membership configurations for the switch can be monitored and modified here. Private VLANs can be added or deleted here. Port members of each Private VLAN can be added or removed here.

Private VLANs are based on the source port mask, and there are no connections to VLANs. This means that VLAN IDs and Private VLAN IDs can be identical.

A port must be a member of both a VLAN and a Private VLAN to be able to forward packets. By default, all ports are VLAN unaware and members of VLAN 1 and Private VLAN 1.

A VLAN unaware port can only be a member of one VLAN, but it can be a member of multiple Private VLANs.

Web Interface

To configure Private VLAN Membership Configuration in the web interface:

1. Click Configuration, Private VLAN and Membership.
2. Evoke Private VLAN Membership Configuration.
3. Click the Save to save the setting.
4. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.

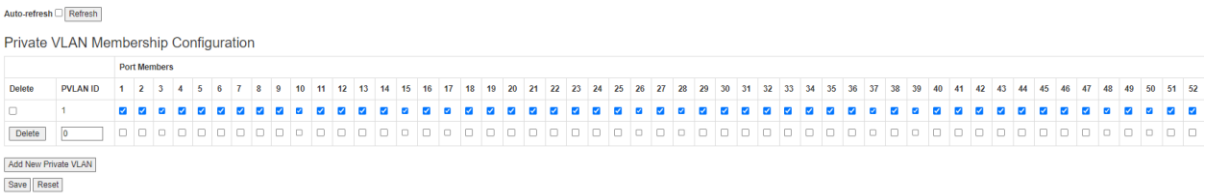


Figure 2-22.1: The Private VLAN Membership Configuration

Parameter description:

- **Private VLAN ID :**

  Indicates the ID of this particular private VLAN.

- **Port Members :**

  A row of check boxes for each port is displayed for each private VLAN ID. To include a port in a Private VLAN, check the box. To remove or exclude the port from the Private VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.

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 refresh the page automatically. Automatic refresh occurs every 3 seconds.

- **Refresh :**

  Click to refresh the page immediately.

- **Delete :**

  To delete a private VLAN entry, check this box. The entry will be deleted during the next save.

- **Adding a New Private VLAN :**

  Click Add New Private VLAN to add a new private VLAN ID. An empty row is added to the table, and the private VLAN can be configured as needed. The allowed range for a private VLAN ID is the same as the switch port number range. Any values outside this range are not accepted, and a warning message appears. Click "OK" to discard the incorrect entry, or click "Cancel" to return to the editing and make a correction.
  The Private VLAN is enabled when you click "Save".
  The Delete button can be used to undo the addition of new Private VLANs.

2-22.2 Port Isolation

The Private VLAN membership configurations for the switch can be monitored and modified here. Private VLANs can be added or deleted here. Port members of each Private VLAN can be added or removed here.

Private VLANs are based on the source port mask, and there are no connections to VLANs. This means that VLAN IDs and Private VLAN IDs can be identical.

A port must be a member of both a VLAN and a Private VLAN to be able to forward packets. By default, all ports are VLAN unaware and members of VLAN 1 and Private VLAN 1.

A VLAN unaware port can only be a member of one VLAN, but it can be a member of multiple Private VLANs.

Web Interface

To configure Port Isolation Configuration in the web interface:

1. Click Configuration, Private VLAN and Port Isolation.
2. Evoke Port Isolation Configuration.
3. Click the Save to save the setting.
4. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.

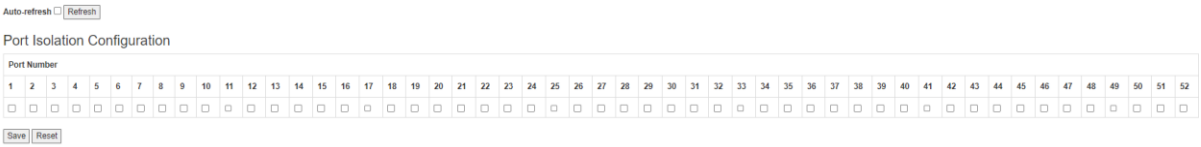


Figure 2-22.2: The Port Isolation Configuration

Parameter description:

- **Port Members :**

  A check box is provided for each port of a private VLAN. When checked, port isolation is enabled on that port. When unchecked, port isolation is disabled on that port. By default, port isolation is disabled on all ports.

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 refresh the page automatically. Automatic refresh occurs every 3 seconds.

- **Refresh :**

  Click to refresh the page immediately.

2-23 VCL

2-23.1 MAC-based VLAN

The MAC-based VLAN entries can be configured here. This page allows for adding and deleting MAC-based VLAN entries and assigning the entries to different ports. This page shows only static entries.

Web Interface

To configure MAC-based VLAN Membership Configuration in the web interface:

1. Click Configuration, VLC and MAC-based VLAN configuration.
2. Specify the MAC address and VLAN ID.
3. Click the Save to save the setting.
4. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.

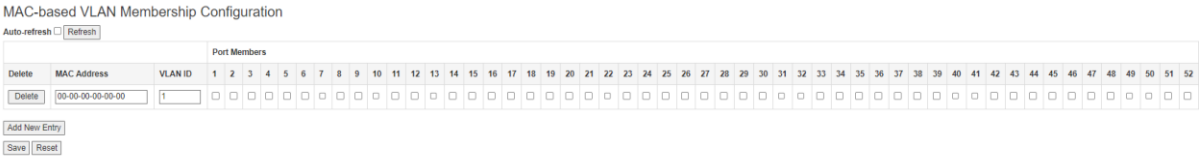


Figure 2-23.1: The MAC-based VLAN Membership Configuration

Parameter description:

- **MAC Address :**

  Indicates the MAC address of the mapping.

- **VLAN ID :**

  Indicates the VLAN ID the above MAC will be mapped to.

- **Port Members :**

  A row of check boxes for each port is displayed for each MAC-based VLAN entry. To include a port in a MAC-based VLAN, check the box. To remove or exclude the port from the MAC-based VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.

Buttons

- **Save :**

  Click to save changes.

- **Reset :**

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

- **Delete :**

  To delete a MAC-based VLAN entry, check this box and press save. The entry will be deleted on the selected switch in the stack.

- **Adding a New MAC-based VLAN :**

Click Add New Entry to add a new MAC-based VLAN entry. An empty row is added to the table, and the MAC-based VLAN entry can be configured as needed. Any unicast MAC address can be configured for the MAC-based VLAN entry. No broadcast or multicast MAC addresses are allowed. Legal values for a VLAN ID are 1 through 4095.

The MAC-based VLAN entry is enabled when you click on "Apply". A MAC-based VLAN without any port members will be deleted when you click "Apply".

The Delete button can be used to undo the addition of new MAC-based VLANs. The

- **Auto-refresh :**

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

- **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.

2-23.2 Protocol-based VLAN

This section describe Protocol -based VLAN, The Switch support Protocol include Ethernet LLC SNAP Protocol,

LLC

The Logical Link Control (LLC) data communication protocol layer is the upper sub-layer of the Data Link Layer (which is itself layer 2, just above the Physical Layer) in the seven-layer OSI reference model. It provides multiplexing mechanisms that make it possible for several network protocols (IP, IPX, Decent and Appletalk) to coexist within a multipoint network and to be transported over the same network media, and can also provide flow control and automatic repeat request (ARQ) error management mechanisms.

SNAP

The Subnetwork Access Protocol (SNAP) is a mechanism for multiplexing, on networks using IEEE 802.2 LLC, more protocols than can be distinguished by the 8-bit 802.2 Service Access Point (SAP) fields. SNAP supports identifying protocols by Ethernet type field values; it also supports vendor-private protocol identifier spaces. It is used with IEEE 802.3, IEEE 802.4, IEEE 802.5, IEEE 802.11 and other IEEE 802 physical network layers, as well as with non-IEEE 802 physical network layers such as FDDI that use 802.2 LLC.

2-23.2.1 Protocol to Group

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

Web Interface

To configure Protocol to Group Mapping Table configuration in the web interface:

1. Click Configuration, VLC, Protocol-based VLAN configuration and Protocol to Group.
2. Specify the Protocol to Group Mapping Table.
3. Click the Saveto save the setting.
4. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.

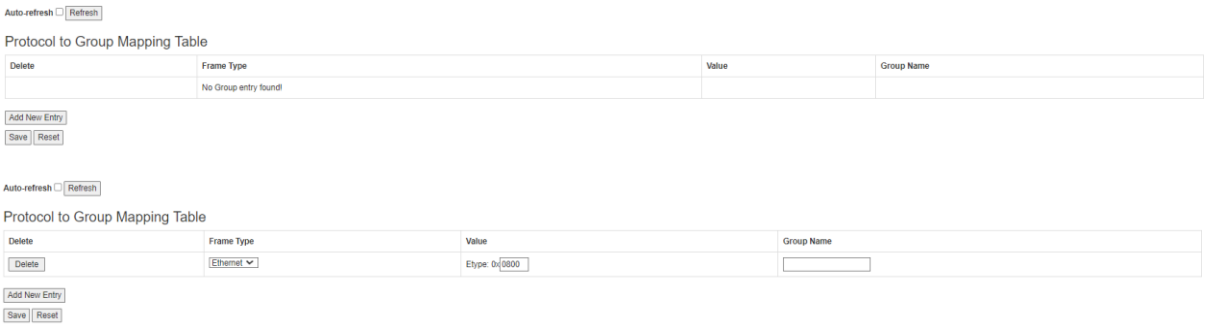


Figure 2-23.2.1: The Protocol to Group Mapping Table

Parameter description:

- **Frame Type :**

  Frame Type can have one of the following values:

  1. Ethernet

2. LLC
3. SNAP

NOTE: On changing the Frame type field, valid value of the following text field will vary depending on the new frame type you selected.

- **Value :**

  Valid value that can be entered in this text field depends on the option selected from the preceding Frame Type selection menu.
  Below are the criteria for the three different Frame Types:

  Ethernet: Value in the text field when Ethernet is selected as a Frame Type is called etype. Valid values for etype range between 0x0600 and 0xffff

  LLC: Valid value in this case is comprised of two different sub-values.
  a. DSAP: 1-byte long string (0x00-0xff)
  b. SSAP: 1-byte long string (0x00-0xff)

  SNAP: Valid value in this case is also comprised of two different sub-values.
  a. OUI: OUI (Organizationally Unique Identifier) is a parameter in the format of xx-xx-xx where each pair (xx) in the string is a hexadecimal value ranging between 0x00 and 0xff.
  b. PID: PID (Protocol ID). If OUI is hexadecimal 000000, then the protocol ID is the Ethernet type (EtherType) field value for the protocol running on top of SNAP; if OUI is an OUI for a particular organization, the protocol ID is a value assigned by that organization to the protocol running on top of SNAP.
  In other words, if the value of OUI field is 00-00-00 then the value of PID will be etype (0x0600-0xffff) and if the value of OUI is other than 00-00-00 then valid values of PID will be any value between 0x0000 and 0xffff.

- **Group Name :**

  A valid Group Name is a unique 16-character long string for every entry which consists of a combination of alphabets (a-z or A-Z) and integers (0-9).

NOTE: Special character and underscore (_) are not allowed.

Buttons

- **Save :**

  Click to save changes.

- **Reset :**

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

- **Delete :**

  To delete a Protocol to Group Name map entry, check this box. The entry will be deleted on the switch during the next Save.

- **Adding a New Group to VLAN mapping entry :**

  Click to add a new entry in mapping table. An empty row is added to the table; Frame Type,

Value and the Group Name can be configured as needed.

The button can be used to undo the addition of new entry.

- **Auto-refresh :**

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

- **Refresh :**

  Refreshes the displayed table starting from the "VLAN" input fields.

2-23.2.2 Group to VLAN

This page allows you to map already configured Group Name to a VLAN for the switch.

Web Interface

To configure Group Name to VLAN mapping Table in the web interface:

1. Click Configuration, VLC, Protocol-based VLAN and Group to VLAN.
2. Specify the Group Name to VLAN Mapping Table.
3. Click the Apply to save the setting.
4. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.

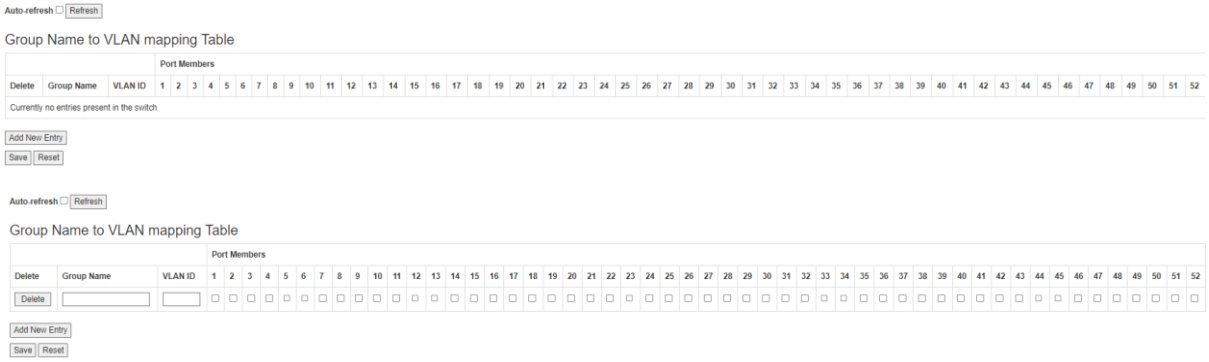


Figure 2-23.2.2: The Group Name to VLAN mapping Table

Parameter description:

- **Group Name :**

  A valid Group Name is a string, at the most 16 characters long, which consists of a combination of alphabets (a-z or A-Z) and integers(0-9) with no special characters allowed. You may either use a Group that already includes one or more protocols (see Protocol to Group mappings), or create a Group to VLAN ID mapping that will become active the moment you add one or more protocols inside that Group. Furthermore, the Group to VLAN ID mapping is not unique, as long as the port lists of these mappings are mutually exclusive (e.g. Group1 can be mapped to VID 1 on port#1 and to VID 2 on port#2).

- **VLAN ID :**

  Indicates the ID to which Group Name will be mapped. A valid VLAN ID ranges from 1-4095.

- **Port Members :**

  A row of check boxes for each port is displayed for each Group Name to VLAN ID mapping. To include a port in a mapping, check the box. To remove or exclude the port from the mapping, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.

Buttons

- **Save :**

  Click to save changes.

- **Reset :**

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

- **Delete :**

To delete a Group Name to VLAN map entry, check this box. The entry will be deleted on the switch during the next save

- **Adding a New Group to VLAN mapping entry :**

  Click Add New Entry to add a new entry in mapping table. An empty row is added to the table, the Group Name, VLAN ID and port members can be configured as needed. Legal values for a VLAN ID are 1 through 4095.

  The Delete button can be used to undo the addition of new entry. The maximum possible Group to VLAN mappings are limited to 64.

- **Auto-refresh :**

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

- **Refresh :**

  Refreshes the displayed table starting from the "VLAN" input fields.

2-23.3 IP Subnet-based VLAN

The IP subnet-based VLAN entries can be configured here. This page allows for adding, updating and deleting IP subnet-based VLAN entries and assigning the entries to different ports. This page shows only static entries.

Web Interface

To configure IP Subnet-based VLAN Membership Configuration in the web interface:

1. Click Configuration, VLC and IP Subnet-based VLAN.
2. Click Add New Entry.
3. Specify the IP Subnet-based VLAN Membership Configuration.
4. Click the Save to save the setting.
5. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.

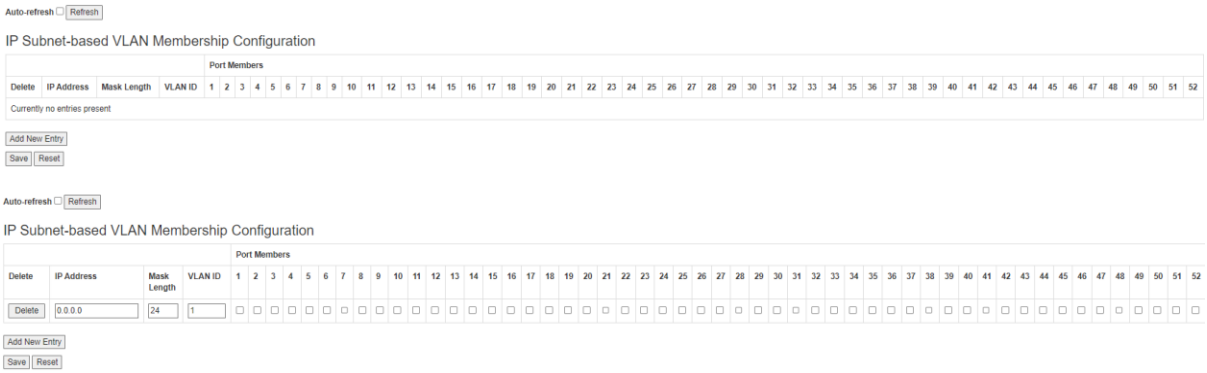


Figure 2-23.3: IP Subnet-based VLAN Membership Configuration

Parameter description:

- **IP Address :**

  Indicates the IP address.

- **Mask Length :**

  Indicates the network mask length.

- **VLAN ID :**

  Indicates the VLAN ID. VLAN ID can be changed for the existing entries.

- **Port Members :**

  A row of check boxes for each port is displayed for each IP subnet-based VLAN entry. To include a port in an IP subnet-based VLAN, check the box. To remove or exclude the port from the IP subnet-based VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.

Buttons

- **Save :**

  Click to save changes.

- **Reset :**

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

- **Delete :**

  To delete an IP subnet-based VLAN entry, check this box and press save. The entry will be deleted on the selected switch in the stack.

- **Adding a New IP subnet-based VLAN**

  Click “Add New Entry” to add a new IP subnet-based VLAN entry. An empty row is added to the table, and the IP subnet-based VLAN entry can be configured as needed. Any IP address/mask can be configured for the IP subnet-based VLAN entry. Legal values for a VLAN ID are 1 through 4095.

  The IP subnet-based VLAN entry is enabled on the selected stack switch unit when you click on "Save". The “Delete” button can be used to undo the addition of new IP subnet-based VLANs. The maximum possible IP subnet-based VLAN entries are limited to 128.

- **Auto-refresh :**

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

- **Refresh :**

  Refreshes the displayed table starting from the "VLAN" input fields.

2-24 VOICE VLAN

Voice VLAN is VLAN configured specially for voice traffic. By adding the ports with voice devices attached to voice VLAN, we can perform QoS-related configuration for voice data, ensuring the transmission priority of voice traffic and voice quality.

2-24.1 Configuration

The Voice VLAN feature enables voice traffic forwarding on the Voice VLAN, then the switch can classify and schedule network traffic. It is recommended that there be two VLANs on a port - one for voice, one for data. Before connecting the IP device to the switch, the IP phone should configure the voice VLAN ID correctly. It should be configured through its own GUI.

Web Interface

To configure Voice VLAN in the web interface:

1. Click Configuration, Voice VLAN and Configuration.
2. Select “Enabled” in the Voice VLAN Configuration.
3. Specify VLAN ID, Aging Time and Traffic Class.
4. Specify the Port Configuration.
5. Click the Save to save the setting.
6. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.

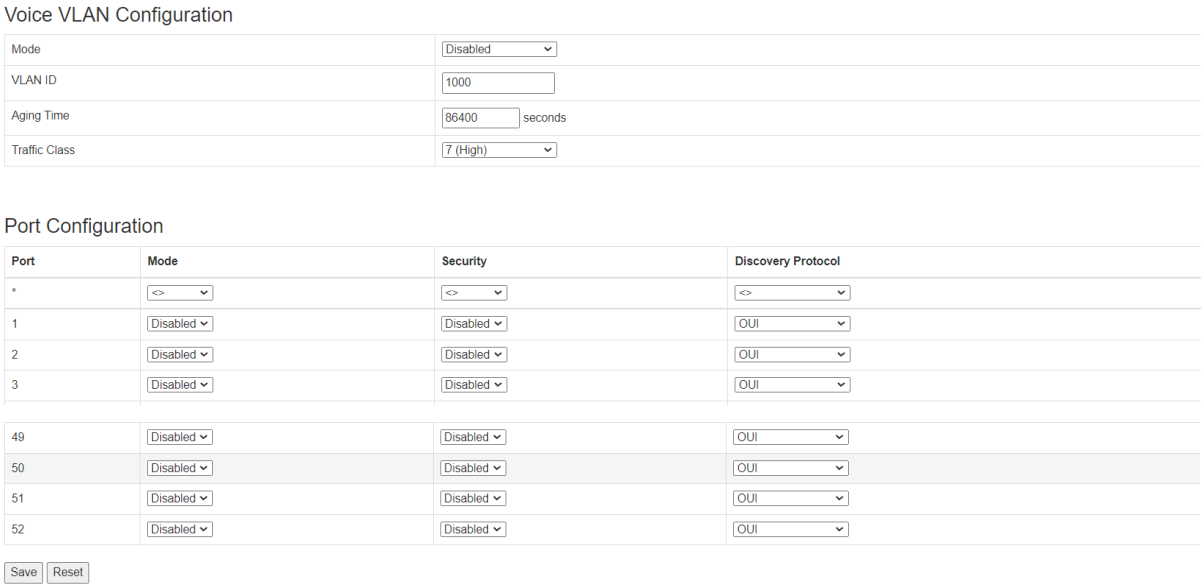


Figure 2-24.1: The Voice VLAN Configuration

Parameter description:

- **Mode :**

  Indicates the Voice VLAN mode operation. We must disable MSTP feature before we enable Voice VLAN. It can avoid the conflict of ingress filtering. Possible modes are:

  Enabled: Enable Voice VLAN mode operation.

  Disabled: Disable Voice VLAN mode operation.

- **VLAN ID :**

  Indicates the Voice VLAN ID. It should be a unique VLAN ID in the system and cannot equal each port PVID. It is a conflict in configuration if the value equals management VID, MVR VID, PVID etc. The allowed range is 1 to 4095.

- **Aging Time :**

  Indicates the Voice VLAN secure learning aging time. The allowed range is 10 to 10000000 seconds. It is used when security mode or auto detect mode is enabled. In other cases, it will be based on hardware aging time. The actual aging time will be situated between the [age_time; 2 * age_time] interval.

- **Traffic Class:**

  Indicates the Voice VLAN traffic class. All traffic on the Voice VLAN will apply this class.

- **Port Mode :**

  Indicates the Voice VLAN port mode. Possible port modes are:

  Disabled: Disjoin from Voice VLAN.

  Auto: Enable auto detect mode. It detects whether there is VoIP phone attached to the specific port and configures the Voice VLAN members automatically.

  Forced: Force join to Voice VLAN.

  This field will be read only if STP feature is enabled. And the STP port mode will be readonly if this field be set to the mode other than Disabled.

- **Port Security :**

  Indicates the Voice VLAN port security mode. When the function is enabled, all non-telephonic MAC addresses in the Voice VLAN will be blocked for 10 seconds. Possible port modes are:

  Enabled: Enable Voice VLAN security mode operation.

  Disabled: Disable Voice VLAN security mode operation.

- **Port Discovery Protocol**

  Indicates the Voice VLAN port discovery protocol. It will only work when auto detect mode is enabled. We should enable LLDP feature before configuring discovery protocol to "LLDP" or "Both". Changing the discovery protocol to "OUI" or "LLDP" will restart auto detect process. Possible discovery protocols are:

  OUI: Detect telephony device by OUI address.

  LLDP: Detect telephony device by LLDP.

  Both: Both OUI and LLDP.

Buttons

- **Save :**

  Click to save changes.

- **Reset :**

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

- **Delete :**

  To delete an IP subnet-based VLAN entry, check this box and press save. The entry will be deleted on the selected switch in the stack.

2-24.2 OUI

Configure VOICE VLAN OUI table on this page. The maximum number of entries is 16. Modifying the OUI table will restart auto detection of OUI process.

Web Interface

To configure Voice VLAN OUI Table in the web interface:

1. Click Configuration, Voice VLAN and OUI.
2. Click Add New Entry.
3. Specify the Voice VLAN OUI Table.
4. Click the Save to save the setting.
5. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.

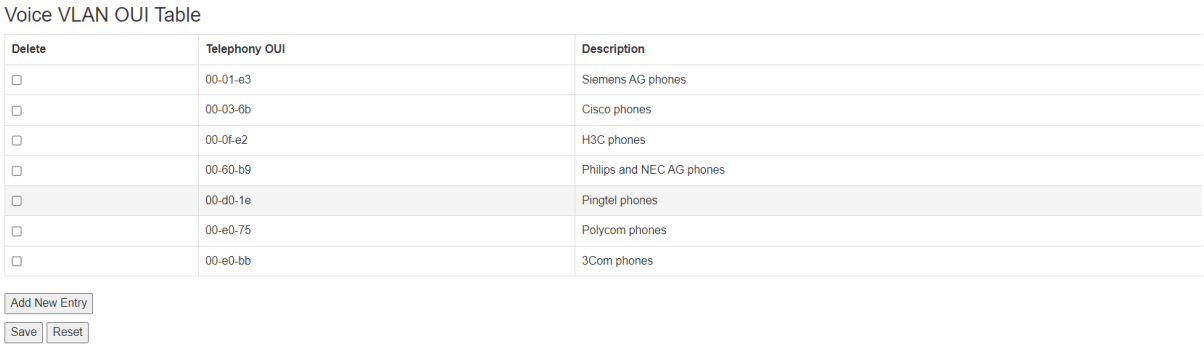


Figure 2-24.2: The Voice VLAN OUI Table

Parameter description:

- **Telephony OUI :**

  A telephony OUI address is a globally unique identifier assigned to a vendor by IEEE. It must be 6 characters long and the input format is "xx-xx-xx" (x is a hexadecimal digit).

- **Description :**

  The description of OUI address. Normally, it describes which vendor telephony device it belongs to. The allowed string length is 0 to 32.

Buttons

- **Save :**

  Click to save changes.

- **Reset :**

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

- **Delete :**

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

- **Add New entry :**

  Click to add a new access management entry.

2-25 QoS

The switch support four QoS queues per port with strict or weighted fair queuing scheduling. It supports QoS Control Lists (QCL) for advance programmable QoS classification, based on IEEE 802.1p, Ethertype, VID, IPv4/IPv6 DSCP and UDP/TCP ports and ranges.

High flexibility in the classification of incoming frames to a QoS class. The QoS classification looks for information up to Layer 4, including IPv4 and IPv6 DSCP, IPv4 TCP/UDP port numbers, and user priority of tagged frames. This QoS classification mechanism is implemented in a QoS control list (QCL). The QoS class assigned to a frame is used throughout the device for providing queuing, scheduling, and congestion control guarantees to the frame according to what was configured for that specific QoS class.

The switch support advanced memory control mechanisms providing excellent performance of all QoS classes under any traffic scenario, including jumbo frame. A super priority queue with dedicated memory and strict highest priority in the arbitration. The ingress super priority queue allows traffic recognized as CPU traffic to be received and queued for transmission to the CPU even when all the QoS class queues are congested.

2-19.1 Port Classification

The section allows you to configure the basic QoS Ingress Classification settings for all switch ports.

Web Interface

To configure the QoS Ingress Port Classification parameters in the web interface:

1. Click Configuration, QoS and Port Classification.
2. Scroll to select QoS Ingress Port parameters.
3. Click the Save to save the setting.
4. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.

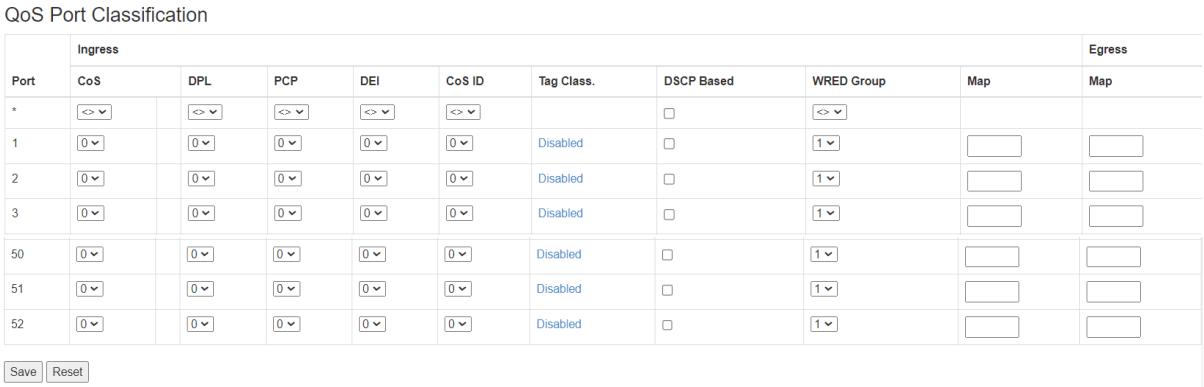


Figure 2-25.1: The QoS Ingress Port Classification

Parameter description:

- **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 and the frame is tagged, then the frame is classified to a CoS that is based on the PCP value in the tag as shown below. 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.

- **CoS ID:**

  Controls the default CoS ID value.

  Every incoming frame is classified to a CoS ID, which later can be used as basis for rewriting of different parts of the frame.

- **Tag Class :**

  Shows the classification mode for 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 is VLAN unaware. Tagged frames received on VLAN unaware ports are always classified to the default CoS and DPL.

- **DSCP Based :**

Click to Enable DSCP Based QoS Ingress Port Classification.

- **WRED Group :**

  Controls the WRED group membership.

- **Ingress Map :**

  Controls the Ingress Map selection through the Map ID. The Ingress Map ID ranges from 0 to 255. An empty field indicates no map selection.

- **Egress Map :**

  Controls the Egress Map selection through the Map ID. The Egress Map ID ranges from 0 to 511. An empty field indicates no map selection.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

2-25.2 Port Policing

This section provides an overview of f QoS Ingress Port Policers for all switch ports The Port Policing is useful in constraining traffic flows and marking frames above specific rates. Policing is primarily useful for data flows and voice or video flows because voice and video usually maintains a steady rate of traffic

Web Interface

To configure the QoS Ingress Port Policers in the web interface:

1. Click Configuration, QoS and Port Policing
2. Evoke which port need to enable the QoS Ingress Port Policers and type the Rate limit condition.
3. Scroll to select the column Rate and Unit.
4. Click the Save to save the setting.
5. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.

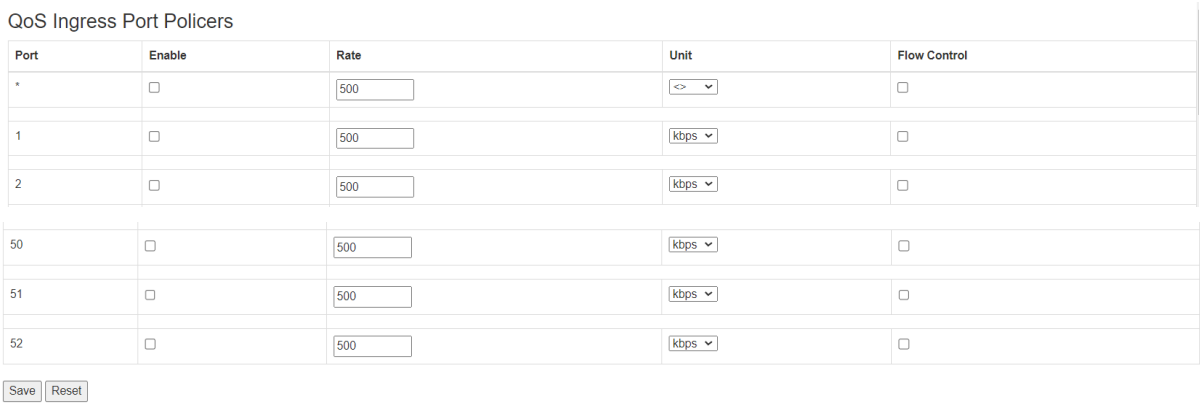


Figure 2-25.2: The QoS Ingress Port Policers

Parameter description:

- **Port :**

  The port number for which the configuration below applies.

- **Enabled :**

  Controls whether the policer is enabled on this switch port.

- **Rate :**

  Controls the rate for the port policer. This value is restricted to 100-13128072 when "Unit" is kbps, 1-13128 when "Unit" is mbps , 1-131071 when "Unit" is fps, and 1-131 when "Unit" is 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.

2-25.3 Queue Policing

This page allows you to configure the Queue Policer settings for all switch ports.

Web Interface

To configure the QoS Ingress Port Policers in the web interface:

1. Click Configuration, QoS and Queue Policing
2. Specify the Queue paremeters
3. Click the Save to save the setting.
4. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.

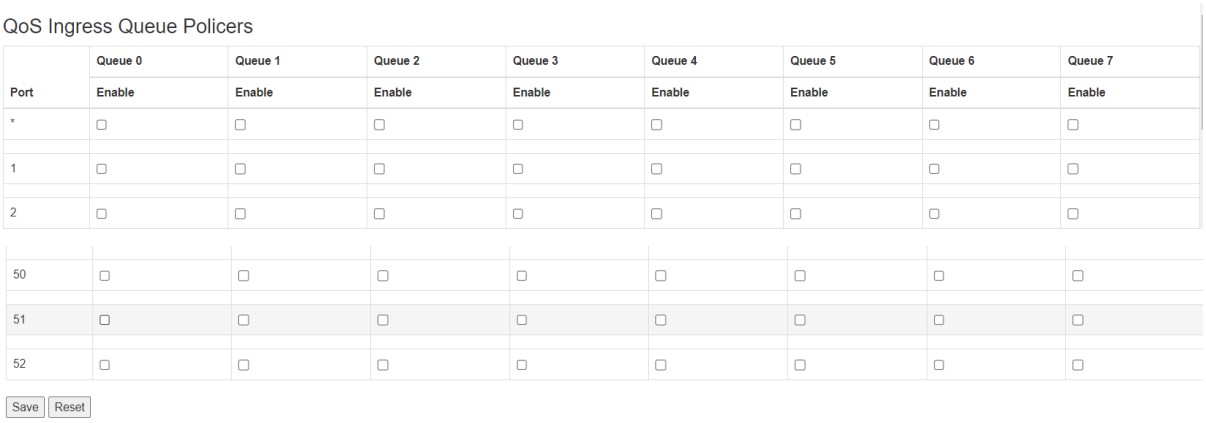


Figure 2-25.3: The QoS Ingress Port Policers

Parameter description:

- **Port :**

  The port number for which the configuration below applies.

- **Enable (E) :**

  Enable or disable the queue policer for this switch port.

- **Rate :**

  Controls the rate for the port policer. This value is restricted to 100-13128072 when "Unit" is kbps, 1-13128 when "Unit" is mbps , 1-131071 when "Unit" is fps, and 1-131 when "Unit" is kfps. The rate is internally rounded up to the nearest value supported by the port policer. This field is only shown if at least one of the queue policers are enabled.

- **Unit :**

  Controls the unit of measure for the port policer rate as kbps, Mbps, fps or kfps.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.

2-25.4 Port Schedulers

This page provides an overview of QoS Egress Port Schedulers for all switch ports.

Web Interface

To configure the QoS Ingress Port Policers in the web interface:

1. Click Configuration, QoS and Port Schedulers.
2. Click the Port and display the QoS Egress Port Schedulers
3. Scroll Port and Scheduler Mode, specify the Queue Shaper parameter.
4. Click the Save to save the setting.
5. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.

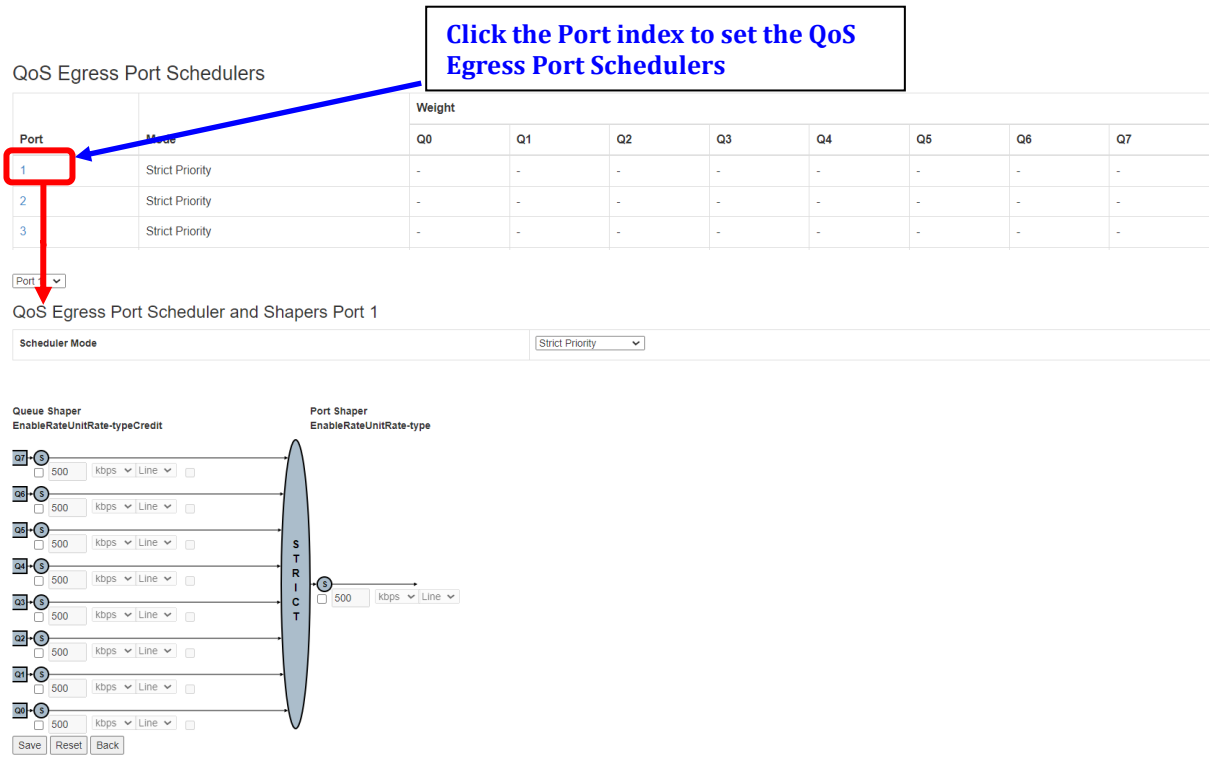


Figure 2-25.4: The QoS Egress Port Schedules

Parameter description:

- **Port :**

  The logical port for the settings contained in the same row. Click on the port number in order to configure the schedulers.

- **Scheduler Mode :**

  Controls whether the scheduler mode is "Strict Priority" or "Weighted" on this switch port.

- **Queue Shaper Enable :**

  Controls whether the queue shaper is enabled for this queue on this switch port.

- **Queue Shaper Rate :**

Controls the rate for the queue shaper. This value is restricted to 100-13107100 when "Unit" is kbps, and 1-13107 when "Unit" is Mbps. The rate is internally rounded up to the nearest value supported by the queue shaper.

- **Queue Shaper Unit :**

  Controls the unit of measure for the queue shaper rate as "kbps" or "Mbps". The default value is "kbps".

- **Queue Shaper Rate-Type :**

  The rate type of the queue shaper. The allowed values are:
  Line: Specify that this shaper operates on line rate.
  Data: Specify that this shaper operates on data rate.

- **Queue Shaper Credit :**

  Controls whether the queue has credit-based shaper enabled.

- **Queue Scheduler Preemption :**

  Controls whether the queue has frame preemption enabled.

- **Queue Scheduler Weight :**

  Controls the weight for this queue. The default value is "17". This value is restricted to 1-100. This parameter is only shown if "Scheduler Mode" is set to "Weighted".

- **Queue Scheduler Percent :**

  Shows the weight in percent for this queue. This parameter is only shown if "Scheduler Mode" is set to "Weighted"

- **Port Shaper Enable :**

  Controls whether the port shaper is enabled for this switch port.

- **Port Shaper Rate :**

  Controls the rate for the port shaper. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps", and it is restricted to 1-13200 when the "Unit" is "Mbps".

- **Port Shaper Unit :**

  Controls the unit of measure for the port shaper rate as "kbps" or "Mbps". The default value is "kbps".

- **Port Shaper Rate-Type:**

  The rate type of the port shaper. The allowed values are:
  Line: Specify that this shaper operates on line rate.
  Data: Specify that this shaper operates on data rate.

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 previous page.

2-25.5Port Shaping

This page provides an overview of QoS Egress Port Shapers for all switch ports.

Web Interface

To configure the QoS Egress Port Shapers in the web interface:

1. Click Configuration, QoS and Port Shaping.
2. Click the Port and display the Qos Egress Port Shapers.
3. Scroll the Port and Scheduler Mode and specify the Queue Shaper parameter.
4. Click the Apply to save the setting.
5. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.

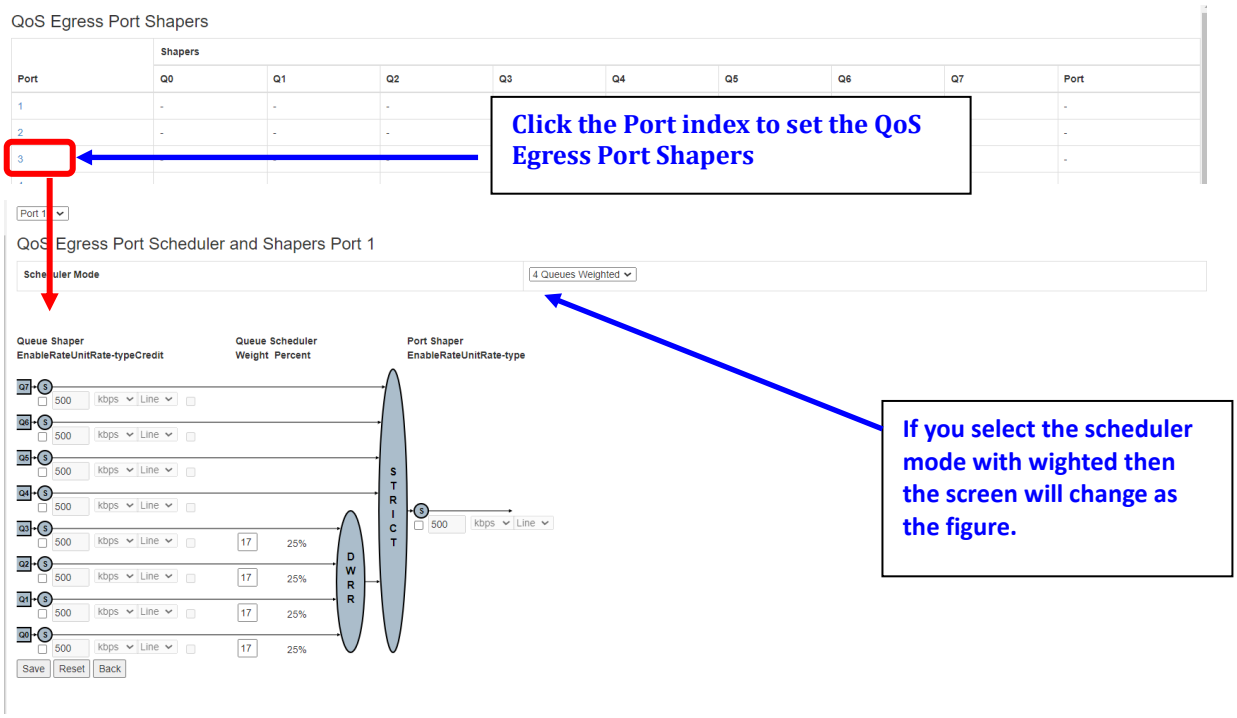


Figure 2-25.5: The QoS Egress Port Shapers

Parameter description:

- **Port :**

  The logical port for the settings contained in the same row. Click on the port number in order to configure the schedulers.

- **Scheduler Mode :**

  Controls whether the scheduler mode is "Strict Priority" or "Weighted" on this switch port.

- **Queue Shaper Enable :**

  Controls whether the queue shaper is enabled for this queue on this switch port.

- **Queue Shaper Rate :**

Controls the rate for the queue shaper. This value is restricted to 100-13107100 when "Unit" is kbps, and 1-13107 when "Unit" is Mbps. The rate is internally rounded up to the nearest value supported by the queue shaper

- **Queue Shaper Unit :**

  Controls the unit of measure for the queue shaper rate as "kbps" or "Mbps". The default value is "kbps".

- **Queue Shaper Rate-Type :**

  The rate type of the queue shaper. The allowed values are:
  Line: Specify that this shaper operates on line rate.
  Data: Specify that this shaper operates on data rate.

- **Queue Shaper Credit :**

  Controls whether the queue has credit-based shaper enabled.

- **Queue Scheduler Preemption :**

  Controls whether the queue has frame preemption enabled.

- **Queue Scheduler Weight :**

  Controls the weight for this queue. The default value is "17". This value is restricted to 1-100. This parameter is only shown if "Scheduler Mode" is set to "Weighted".

- **Queue Scheduler Percent :**

  Shows the weight in percent for this queue. This parameter is only shown if "Scheduler Mode" is set to "Weighted"

- **Port Shaper Enable :**

  Controls whether the port shaper is enabled for this switch port.

- **Port Shaper Rate :**

  Controls the rate for the port shaper. This value is restricted to 100-13107100 when "Unit" is kbps, and 1-13107 when "Unit" is Mbps. The rate is internally rounded up to the nearest value supported by the port shaper.

- **Port Shaper Unit :**

  Controls the unit of measure for the port shaper rate as "kbps" or "Mbps". The default value is "kbps".

- **Port Shaper Rate-Type :**

  The rate type of the port shaper. The allowed values are:
  Line: Specify that this shaper operates on line rate.
  Data: Specify that this shaper operates on data rate.

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 previous page.

2-25.6 Port Tag Remarking

The Section provides user to get an overview of QoS Egress Port Tag Remarking for all switch ports. Others the ports belong to the currently selected stack unit, as reflected by the page header. .

Web Interface

To configure the QoS Port Tag Remarking in the web interface:

1. Click Configuration, QoS and Port Tag Remarking.
2. Click the Port and display the Qos Port Tag Remarking.
3. Scroll the Port and Tag Remarking Mode and specify the Queue Shaper parameter.
4. Click the Save to save the setting.
5. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.

Figure 2-25.6: The Port Tag Remarking

Parameter description:

- **Port :**

The logical port for the settings contained in the same row.
Click on the port number in order to configure tag remarking.

- **Mode :**

  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.

- **Reset :**

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

- **Cancel :**

  Click to undo any changes made locally and return to the previous page.

2-25.7 Port DSCP

The section will teach user to set the QoS Port DSCP configuration that was allowed you to configure the basic QoS Port DSCP Configuration settings for all switch ports. Others the settings relate to the currently selected stack unit, as reflected by the page header.

Web Interface

To configure the QoS Port DSCP parameters in the web interface:

1. Click Configuration, QoS and Port DSCP.
2. Evoke to enable or disable the Ingress Translate and Scroll the Classify parameter.
3. Scroll to select Egress Rewrite parameters
4. Click the Save to save the setting
5. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved value

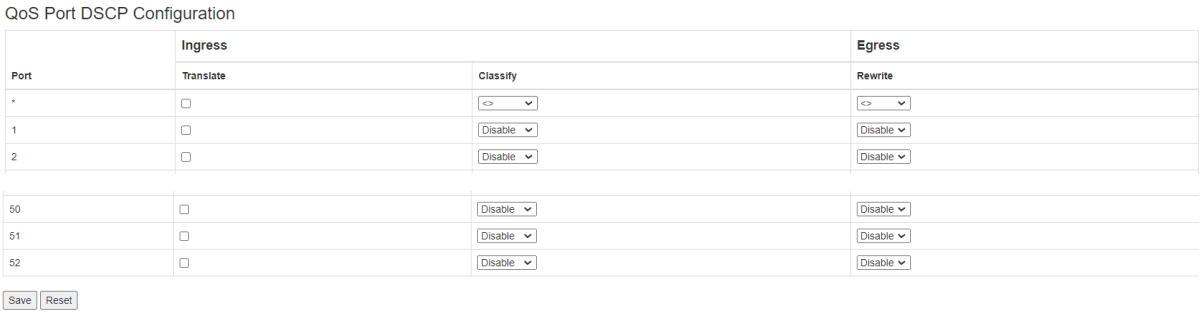


Figure 2-25.7: The QoS Port DSCP Configuration

Parameter description:

- **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:

  1. Translate: To Enable the Ingress Translation click the checkbox
  2. 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: Classify all DSCP.

- **Egress :**

  Port Egress Rewriting can be one of below parameters

- Disable: No Egress rewrite.
- Enable: Rewrite enable without remapped.
- Remap: DSCP from analyzer is remapped and frame is remarked with remapped DSCP value.

Buttons

- **Save:**

  Click to save changes.

- **Reset :**

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

2-25.8 DSCP-Based QoS

The section will teach user to configure the DSCP-Based QoS mode that This page allows you to configure the basic QoS DSCP based QoS Ingress Classification settings for all switches.

Web Interface

To configure the DSCP –Based QoS Ingress Classification parameters in the web interface:

1. Click Configuration, QoS and DSCP-Based QoS.
2. Evoke to enable or disable the DSCP for Trust
3. Scroll to select QoS Class and DPL parameters
4. Click the save to save the setting
5. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values

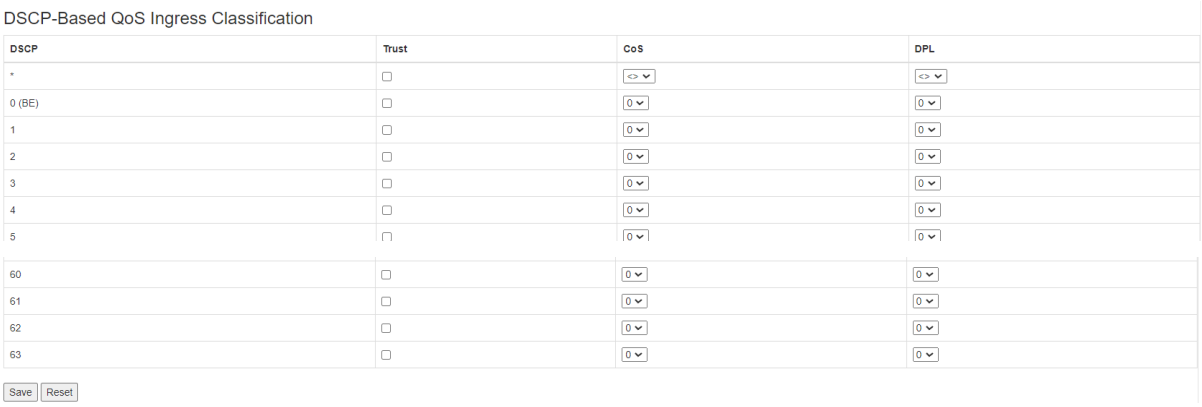


Figure 2-25.8: The DSCP-Based QoS Ingress Classification Configuration

Parameter description:

- **DSCP :**

  Maximum number of support ed DSCP values are 64.

- **Trust :**

  Controls whether a specific DSCP value is trusted. Only frames with trusted DSCP values are mapped to a specific CoS and DPL. Frames with untrusted DSCP values are treated as a non-IP frame.

- **Cos :**

  CoS value can be any of (0-7)

- **DPL :**

  Drop Precedence Level (0-3)

Buttons

- **Save :**

  Click to save changes.

- **Reset :**

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

2-25.9 DSCP Translation

The section describes the switch allows you to configure the basic QoS DSCP Translation settings for all switches. DSCP translation can be done in Ingress or Egress.

Web Interface

To configure the DSCP Translation parameters in the web interface:

1. Click Configuration, QoS and DSCP Translation
2. Scroll to set the Ingress Translate and Egress Remap DP0 and Remap DP1 Parameters
3. Evoke to enable or disable Classify
4. Click the apply to save the setting
5. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values

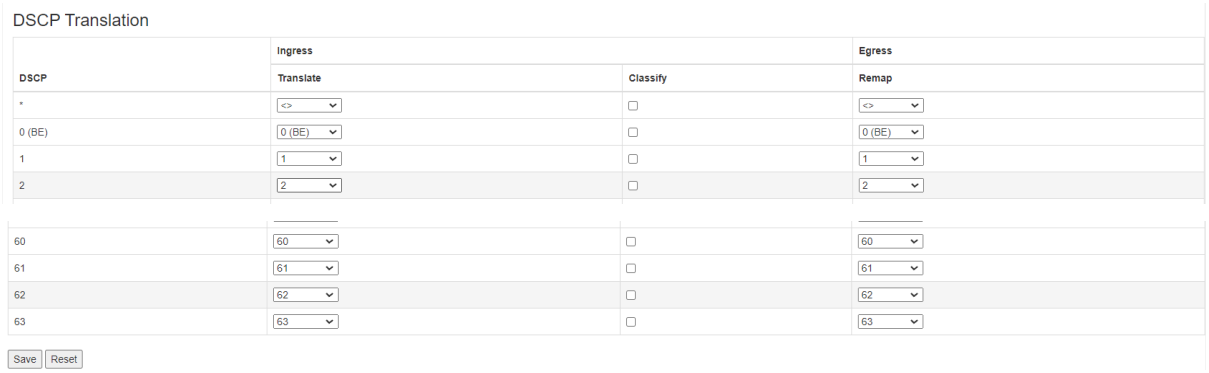


Figure 2-25.9: The DSCP Translation Configuration

Parameter description:

- **DSCP :**

  Maximum number of supported DSCP values are 64 and valid DSCP value ranges from 0 to 63.

- **Ingress :**

  Ingress side DSCP can be first translated to new DSCP before using the DSCP for QoS class and DPL map.

  There are two configuration parameters for DSCP Translation –

  1. Translate: DSCP at Ingress side can be translated to any of (0-63) DSCP values.
  2. Classify: Click to enable Classification at Ingress side.

- **Egress :**

  There are following configurable parameters for Egress side –

  1. Remap: 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.

2-25.10 DSCP Classification

The section describes to teach user to configure and allows you to map DSCP value to a QoS Class and DPL value. Others the settings relate to the currently selected stack unit, as reflected by the page header.

Web Interface

To configure the DSCP Classification parameters in the web interface:

1. Click Configuration, QoS and DSCP Translation
2. Scroll to set the DSCP Parameters
3. Click the Save to save the setting
4. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values

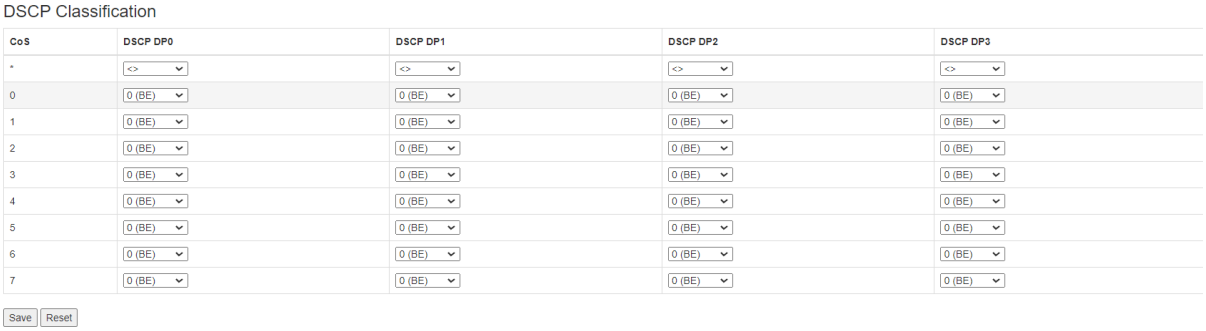


Figure 2-25.10: The DSCP Classification Configuration

Parameter description:

- **Cos :**

  Actual Class of Service

- **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

- **DSCP DP2 :**

  Select the classified DSCP value (0-63) for Drop Precedence Level2.

- **DSCP DP3 :**

  Select the classified DSCP value (0-63) for Drop Precedence Level3.

Buttons

- **Save:**

  Click to save changes.

- **Reset :**

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

2-25.11 Ingress Map

This page allows to edit or create a single QoS Ingress Map entry at a time. Each entry has a key and an action. The key indicates which fields of the frame will be mapped to the fields specified by and according to the action. Each Map can hold a number of map rules, or mappings between possible keys and actions. Which of those rules will be applied depends on the selection of (Key-Type, Action-Type). Here it is possible to configure these 'filters'.

Web Interface

To configure the Ingress Map parameters in the web interface:

1. Click Configuration, QoS and Ingress Map
2. Click the  to add a new entry
3. Specify the Ingress Map parameters
4. Click Save to save the setting
5. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values

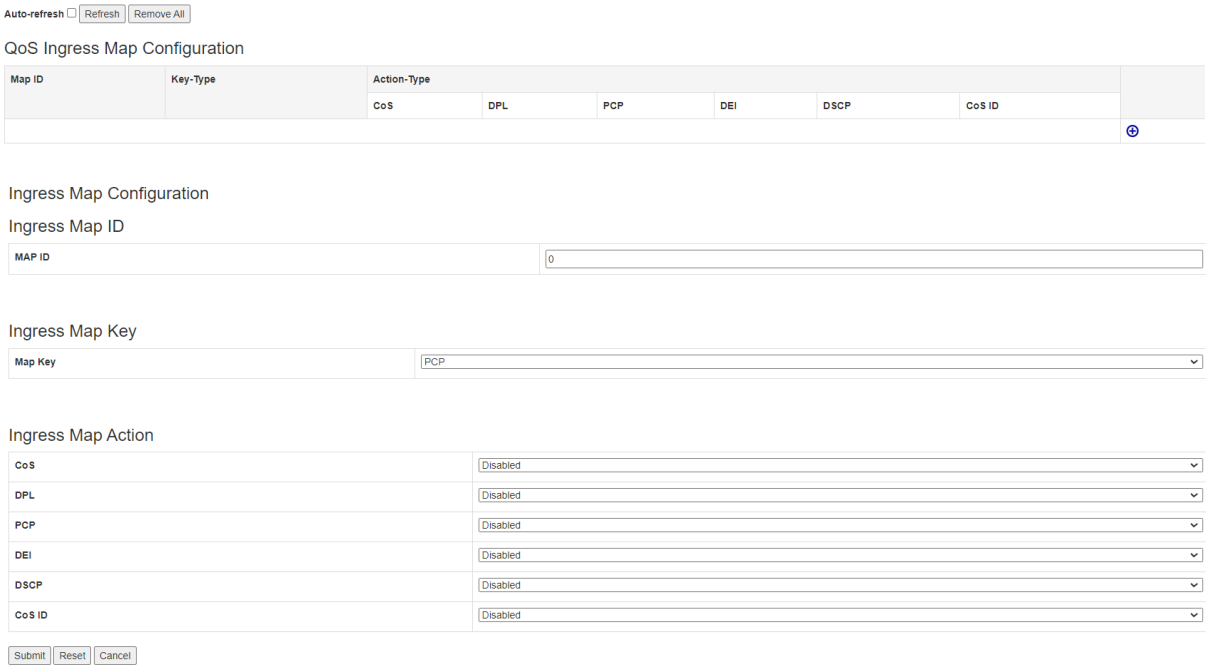


Figure 2-25.11: The Ingress Map Configuration

Parameter description:

- **Map ID :**

  Indicates the Map (unique) ID. Range is 0 to 255. When in edit mode, this is non-configurable. However, it is possible to overwrite an existing mapping through the create mode.

- **Map Key:**

  Indicates the Key type that will be used to filter the map rules when applying the map. As mentioned above, map rules can have various keys and this is to make a select set of them. Possible Key types are:
  PCP: Use PCP as key for tagged frames and none for the rest.

PCP - DEI: Use PCP/DEI as key for tagged frames and none for the rest.
DSCP: Use DSCP as key for IP frames and none for the rest.
DSCP - PCP - DEI: Use DSCP as key for IP frames, PCP/DEI for tagged frames and none for the rest.

- **Map Action:**

  Indicates the Action type that will be used to filter the map rules when applying the map. As mentioned above, map rules can have various actions available and this is to make a select set of them. Possible Action types are:
  CoS: Class of Service.
  DPL: Drop Precedence Level.
  PCP: Priority Code Point.
  DEI: Drop Eligible Indicator.
  DSCP: Differentiated Services Code Point.
  CoS ID: CoS ID.

Buttons

- **Save:**

  Click to save changes.

- **Cancel :**

  Return to the ingress map page without saving the configuration changes.

- **Submit:**

  Click to submit the map configuration and move to the main ingress map page.

2-25.12 Egress Map

This page allows to edit or create a single QoS Egress Map entry at a time. Each entry has a key and an action. The key indicates which fields of the frame will be mapped to the fields specified by and according to the action. Each Map can hold a number of map rules, or mappings between possible keys and actions. Which of those rules will be applied depends on the selection of (Key-Type, Action-Type). Here it is possible to configure these 'filters'.

Web Interface

To configure the QoS Egress MAp in the web interface:

1. Click Configuration, QoS and Egress Map
2. Click the  to add a new entry
3. Specify the Egress Map Parameters.
4. Click the save to save the setting
5. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values

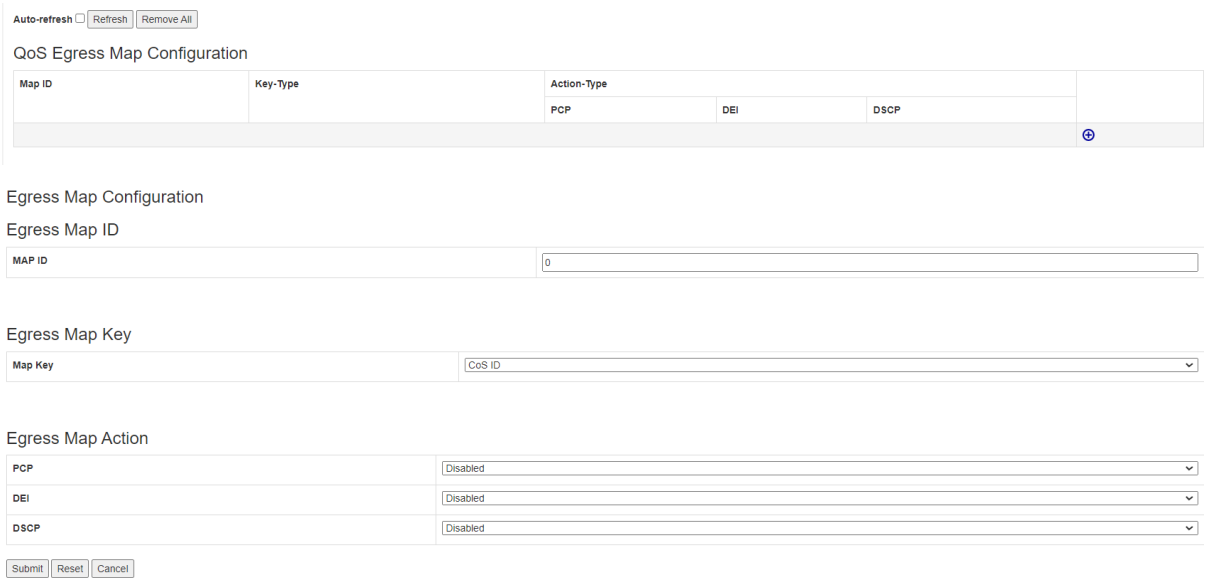


Figure 2-25.12: The Egress Map Configuration

Parameter description:

- **Map ID :**

  Indicates the Map (unique) ID. Range is 0 to 511. When in edit mode, this is non-configurable. However, it is possible to overwrite an existing mapping through the create mode.

- **Map Key:**

  Indicates the Key type that will be used to filter the map rules when applying the map. As mentioned above, map rules can have various keys and this is to make a select set of them. Possible Key types are:
  CoS ID: Use classified COS ID as key.
  CoS ID - DPL:Use classified COS ID and DPL as key.
  DSCP: Use classified DSCP as key.
  DSCP - DPL: Use classified DSCP and DPL as key.

- **Action Map :**

  Indicates the Action type that will be used to filter the map rules when applying the map. As mentioned above, map rules can have various actions available and this is to make a select set of them. Possible Action types are:
  PCP: Priority Code Point.
  DEI: Drop Eligible Indicator.
  DSCP: Differentiated Services Code Point.

Buttons

- **Save:**

  Click to save changes.

- **Reset :**

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

- **Cancel :**

  Return to the ingress map page without saving the configuration changes.

2-25.13 QoS Control List

The section 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.

Web Interface

To configure the QoS Control List parameters in the web interface:

1. Click Configuration, QoS and QoS Control List
2. Click the  to add a new QoS Control List
3. Scroll all parameters and evoke the Port Member to join the QCE rules
4. Click the save to save the setting
5. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values

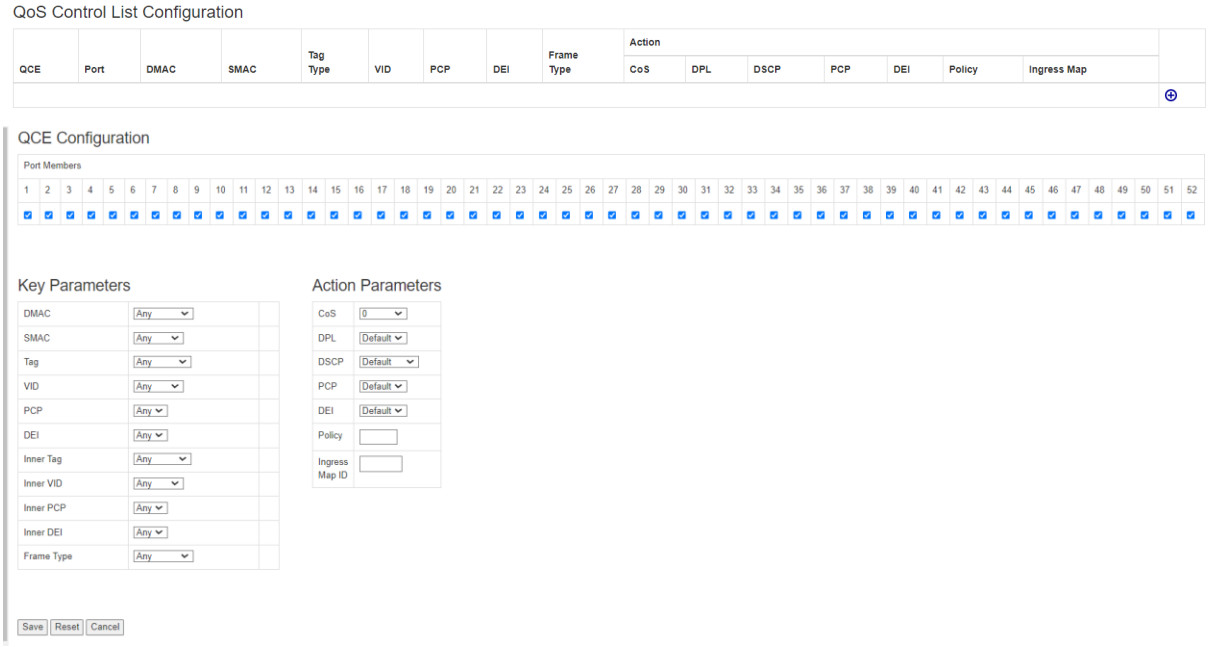


Figure 2-25.13: The QoS Control List Configuration

Parameter description:

- **QCE :**

  Indicates the index of QCE.

- **Port :**

  Indicates the list of ports configured with the QCE.

- **DMAC :**

  Indicates the destination MAC address. Possible values are:

  Any: Match any DMAC.

  Unicast: Match unicast DMAC.

  Multicast: Match multicast DMAC.

  Broadcast: Match broadcast DMAC.

<MAC>: Match specific DMAC.

The default value is 'Any'.

- **SMAC :**

  Match specific source MAC address or 'Any'.

  If a port is configured to match on DMAC/DIP, this field indicates the DMAC.

- **Tag Type :**

  Indicates tag type. Possible values are:
  Any: Match tagged and untagged frames.
  Untagged: Match untagged frames.
  Tagged: Match tagged frames.
  C-Tagged: Match C-tagged frames.
  S-Tagged: Match S-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 to look for incoming frames. Possible frame types are:

  Any: The QCE will match all frame type.

  Ethernet: Only Ethernet frames (with Ether Type 0x600-0xFFFF) are allowed.

  LLC: Only (LLC) frames are allowed.

  SNAP: Only (SNAP) frames are allowed

  IPv4: The QCE will match only IPV4 frames.

  IPv6: The QCE will match only IPV6 frames.

- **Action :**

  Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content.

  There are three action fields: Class, DPL and DSCP.

  Class: Classified QoS Class; if a frame matches the QCE it will be put in the queue.

  DPL: Drop Precedence Level; if a frame matches the QCE then DP level will set to value displayed under DPL column.

  DSCP: If a frame matches the QCE then DSCP will be classified with the value displayed under DSCP column.

- **Port Members :**

  Check the checkbox button in case you what to make any port member of the QCL entry. By default all ports will be checked

- **Key Parameters :**

Key configuration are described as below:

DMAC Destination MAC address: Possible values are 'Unicast', 'Multicast', 'Broadcast' or 'Any'.

SMAC Source MAC address: xx-xx-xx (24 MS bits OUI) or 'Any'.

Tag Value of Tag field can be 'Untagged', '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

1. Any
2. Ethernet
3. LLC
4. SNAP
5. IPv4
6. IPv6

NOTE: All frame types are explained below:
1. Any: Allow all types of frames.

2. Ethernet: Ethernet Type Valid Ethernet type can have value within 0x600-0xFFFF or 'Any', default value is 'Any'.

3. LLC: SSAP Address Valid SSAP(Source Service Access Point) can vary from 0x00 to 0xFF or 'Any', the default value is 'Any'
DSAP Address Valid DSAP(Destination Service Access Point) can vary from 0x00 to 0xFF or 'Any', the default value is 'Any'
Control Address Valid Control Address can vary from 0x00 to 0xFF or 'Any', the default value is 'Any'

4. SNAP : PID Valid PID(a.k.a Ethernet type) can have value within 0x00-0xFFFF or 'Any', default value is 'Any'

5. IPv4: Protocol IP protocol number: (0-255, TCP or UDP) or 'Any'
Source IP 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 DSCP Diffserv Code Point value (DSCP): It can be specific value, range of value or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43
IP Fragment IPv4 frame fragmented option: yes|no|any
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

6. IPv6 : Protocol IP protocol number: (0-255, TCP or UDP) or 'Any'
Source IP IPv6 source address: (a.b.c.d) or 'Any', 32 LS bits
DSCP Diffserv Code Point value (DSCP): It can be specific value, range of value 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 Configuration :**

  Cos: "class (0-7)", default- basic classification

  DP Valid DP Level can be (0-3)", default- basic classification

  DSCP Valid dscp value can be (0-63, BE, CS1-CS7, EF or AF11-AF43) or 'Default'.

  'Default' means that the default classified value is not modified by this QCE.

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 without saving the configuration change.

2-25.14 Storm Policing

There is a unicast storm rate control, multicast storm rate control, and a broadcast storm rate control. These only affect flooded frames, i.e. frames with a (VLAN ID, DMAC) pair not present on the MAC Address table.
The configuration indicates the permitted packet rate for unicast, multicast or broadcast traffic across the switch.

Web Interface

To configure the Storm Control Configuration parameters in the web interface:

1. Click Configuration, QoS and Storm Policing
2. Evoke to select the frame type to enable storm control
3. Scroll to set the Rate Parameters
4. Click the save to save the setting
5. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values

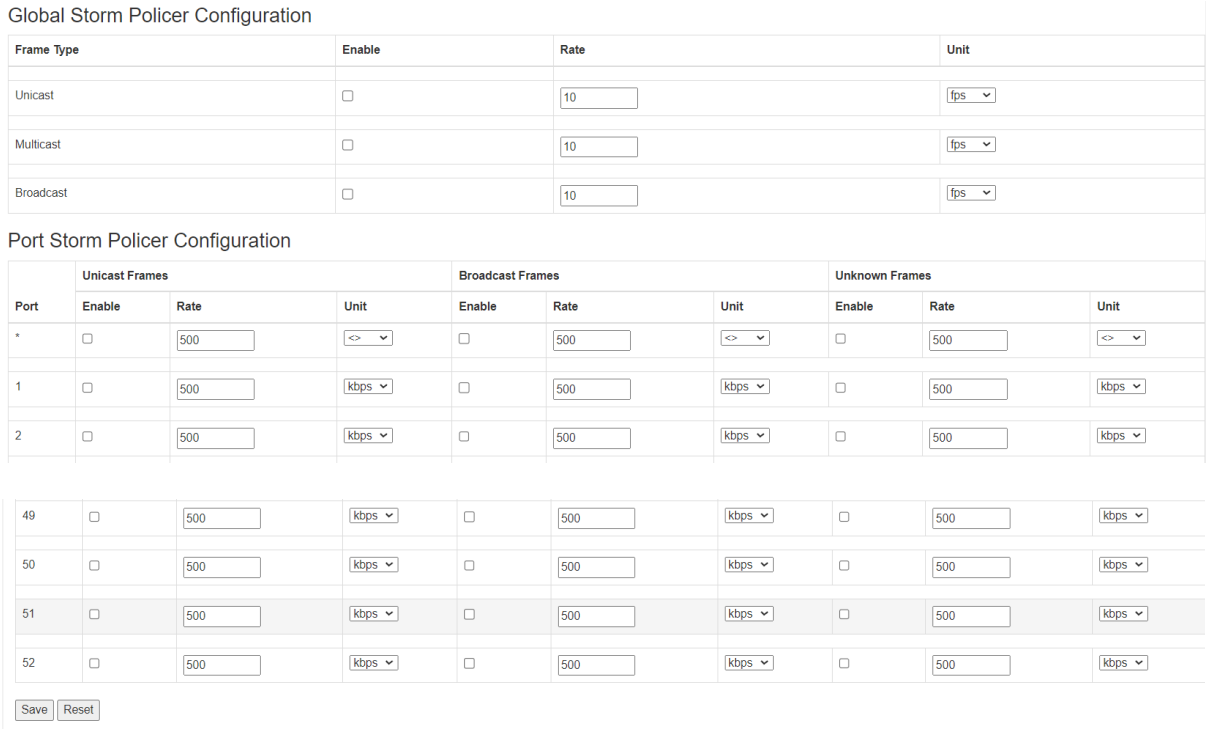


Figure 2-25.14: The Storm Control Configuration

Parameter description:

Global Storm Policer Configuration

- **Frame Type :**

  The frame type for which the configuration below applies.

- **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 10-13128147 when "Unit" is fps or kbps, and 1-13128 when "Unit" is kfps or Mbps. The rate is internally rounded up to the nearest value supported by the global storm policer. Supported rates

are divisible by 10 fps or 25 kbps.

- **Unit :**

  Controls the unit of measure for the global storm policer rate as fps, kfps, kbps or Mbps.

Port Storm Policer Configuration

- **Port :**

  The port number for which the configuration below applies.

- **Enable :**

  Enable or disable the storm policer for this switch port.

- **Rate :**

  Controls the rate for the port storm policer. This value is restricted to 10-13128147 when "Unit" is fps or kbps, and 1-13128 when "Unit" is kfps or Mbps. The rate is internally rounded up to the nearest value supported by the port storm policer. Supported rates are divisible by 10 fps or 25 kbps.

- **Unit :**

  Controls the unit of measure for the port storm policer rate as fps, kfps, kbps or Mbps.

Buttons

- **Save :**

  Click to save changes.

- **Reset :**

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

2-25.15 WRED

This page allows you to configure the Random Early Detection (RED) settings.
Through different RED configuration for the queues it is possible to obtain Weighted Random Early Detection (WRED) operation between queues.
The settings are global for all ports in the switch.

Web Interface

To configure the Storm Control Configuration parameters in the web interface:

1. Click Configuration, QoS and WRED
2. Specify the WRED parameters in the table
3. Click the save to save the setting
4. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values

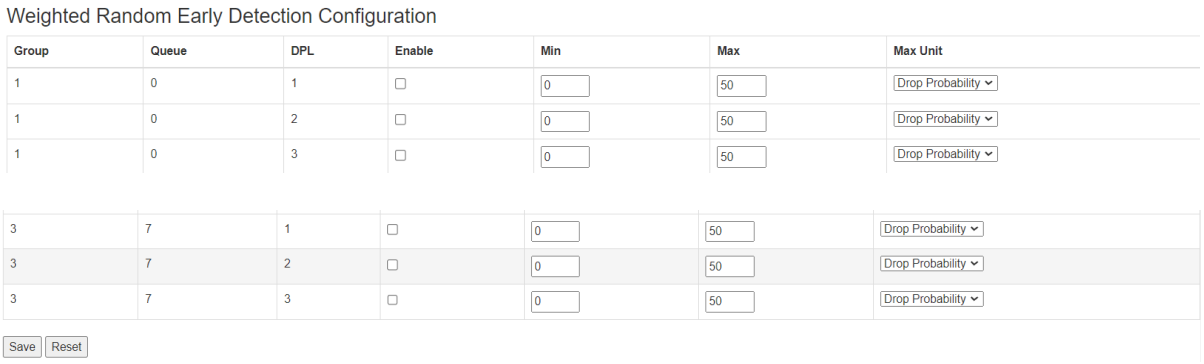


Figure 2-25.15: The WRED Configuration

Parameter description:

- **Group :**

  The WRED group number for which the configuration below applies.

- **Queue :**

  The queue number (CoS) for which the configuration below applies.

- **DPL :**

  The Drop Precedence Level for which the configuration below applies.

- **Enable:**

  Controls whether RED is enabled for this entry.

- **Min :**

  Controls the lower RED fill level threshold. If the queue filling level is below this threshold, the drop probability is zero. This value is restricted to 0-100%.

- **Max :**

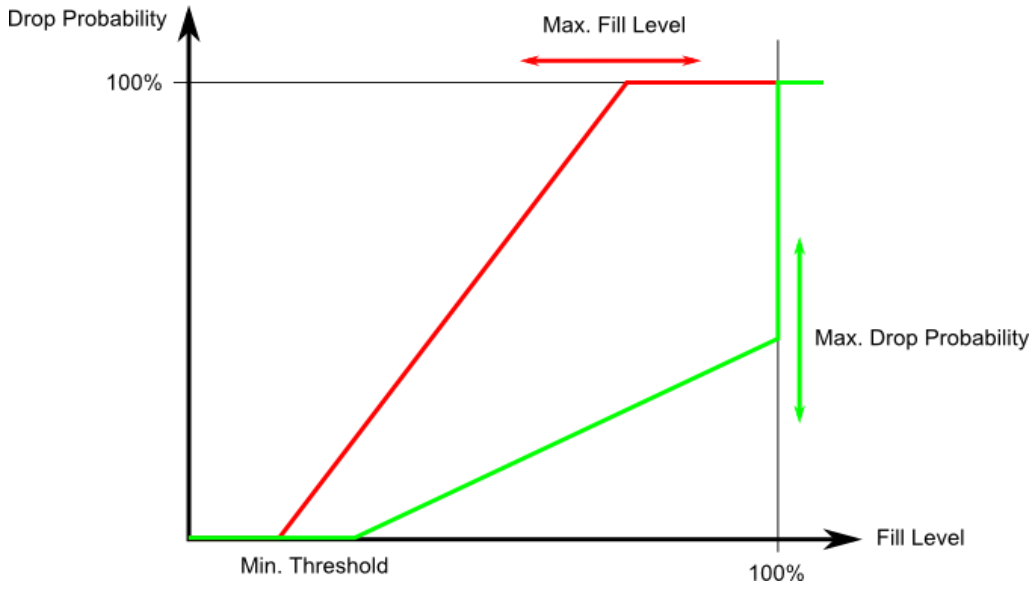
  Controls the upper RED drop probability or fill level threshold for frames marked with Drop Precedence Level > 0 (yellow frames). This value is restricted to 1-100%.

- **Max Unit :**

  Selects the unit for Max. Possible values are:
  Drop Probability: Max controls the drop probability just below 100% fill level.
  Fill Level: Max controls the fill level where drop probability reaches 100%.

RED Drop Probability Function

The following illustration shows the drop probability versus fill level function with associated parameters.



Min is the fill level where the queue randomly start dropping frames marked with Drop Precedence Level > 0 (yellow frames).
If Max Unit is 'Drop Probability' (the green line), Max controls the drop probability when the fill level is just below 100%.
If Max Unit is 'Fill Level' (the red line), Max controls the fill level where drop probability reaches 100%. This configuration makes it possible to reserve a portion of the queue exclusively for frames marked with Drop Precedence Level 0 (green frames). The reserved portion is calculated as (100 - Max) %.
Frames marked with Drop Precedence Level 0 (green frames) are never dropped.
The drop probability for frames increases linearly from zero (at Min average queue filling level) to Max Drop Probability or Fill Level.

Buttons

- **Save :**

  Click to save changes.

- **Reset :**

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

2-26 Mirroring

To debug network problems, selected traffic can be copied, or mirrored, on a mirror port where a frame analyzer can be attached to analyze the frame flow.
The traffic to be copied on the mirror port is selected as follows:
All frames received on a given port (also known as ingress or source mirroring).
All frames transmitted on a given port (also known as egress or destination mirroring).

Web Interface

To configure the Mirror in the web interface:

1. Click Configuration and Mirroring
2. Click the session ID into mirror global setting page
3. Scroll to select Port to mirror on which port
4. Scroll to disabled, enable, TX Only and RX only to set the Port mirror mode
5. Click the apply to save the setting
6. If you want to cancel the setting then you need to click the Reset button.

   It will revert to previously saved values

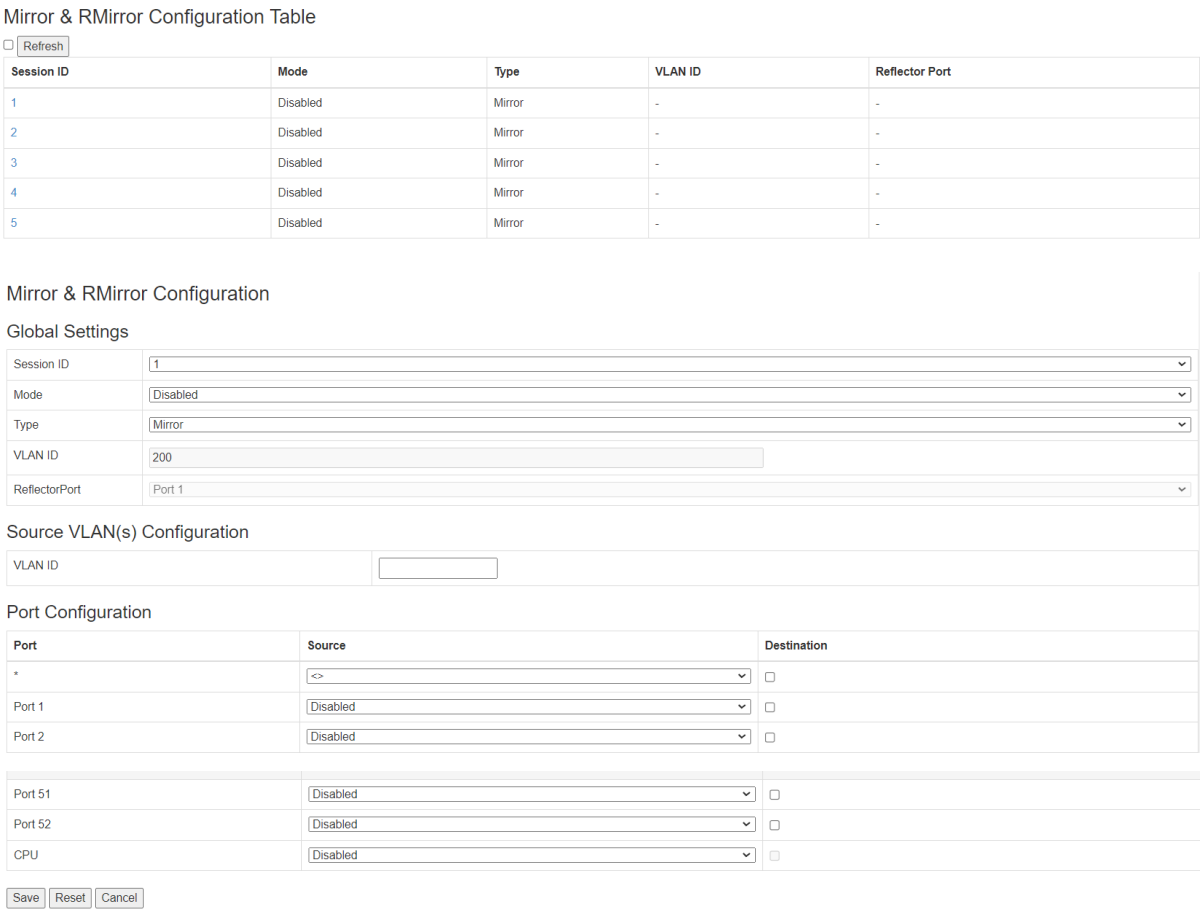


Figure 2-26: The Mirroring Configuration

Parameter description:

- **Session :**

  Select session id to configure.

- **Mode :**

  Select mirror mode.

  Rx only Frames received on this port are mirrored on the mirror port. Frames transmitted are not mirrored.

  Tx only Frames transmitted on this port are mirrored on the mirror port. Frames received are not mirrored.

  Disabled neither frames transmitted nor frames received are mirrored.

  Enabled Frames received and frames transmitted are mirrored on the mirror port.

NOTE: For a given port, a frame is only transmitted once. It is therefore not possible to mirror Tx frames on the mirror port. Because of this, mode for the selected mirror port is limited to Disabled or Rx only.

- **Type :**

  Select switch type.

  Mirror：

  The switch is running on mirror mode.
  The source port(s) and destination port are located on this switch.

  Source:

  The switch is a source node for monitor flow.
  The source port(s), reflector port are located on this switch.

  Rmirror Destination:

  The switch is an end node for monitor flow.
  The destination port(s) is located on this switch.

- **VLAN ID:**

  The VLAN ID points out where the monitor packet will copy to. The default VLAN ID is 200.

- **Reflector Port**

  The reflector port is a method to redirect the traffic to Remote Mirroring VLAN. Any device connected to a port set as a reflector port loses connectivity until the Remote Mirroring is disabled.
  In the stacking mode, you need to select switch ID to select the correct device.
  If you shut down a port, it cannot be a candidate for reflector port.
  If you shut down the port which is a reflector port, the remote mirror function cannot work.
  Note1: The reflector port needs to select only on Source switch type.
  Note2: The reflector port needs to disable MAC Table learning and STP.
  Note3: The reflector port only supports on pure copper ports.

Source VLAN(s) Configuration

The switch can supports VLAN-based Mirroring. If you want to monitor some VLANs on the switch, you can set the selected VLANs on this field.
Note1: The Mirroring session shall have either ports or VLANs as sources, but not both.

Remote Mirroring Port Configuration

- **Port:**

  The logical port for the settings contained in the same row.

- **Source :**

  Select mirror mode.
  Disabled Neither frames transmitted nor frames received are mirrored.
  Both Frames received and frames transmitted are mirrored on the Destination port.
  Rx only Frames received on this port are mirrored on the Destination port. Frames transmitted are not mirrored.
  Tx only Frames transmitted on this port are mirrored on the Destination port. Frames received are not mirrored.

- **Destination:**

  Select destination port.
  This checkbox is designed for mirror or Remote Mirroring.
  The destination port is a switched port that you receive a copy of traffic from the source port.
  Note1: On mirror mode, the device only supports one destination port.
  Note2: The destination port needs to disable MAC Table learning.

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 without saving the configuration change.

UPnP is an acronym for Universal Plug and Play. The goals of UPnP are to allow devices to connect seamlessly and to simplify the implementation of networks in the home (data sharing, communications, and entertainment) and in corporate environments for simplified installation of computer components

Web Interface

To configure the UPnP Configuration in the web interface:

1. Click Configuration and UPnP.
2. Scroll to select the mode to enable or disable.
3. Specify the parameters in each blank field.
4. Click save to save the setting.
5. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.

Figure 2-27: The UPnP Configuration

Parameter description:

- **Mode :**

  Indicates the UPnP operation mode. Possible modes are:

  Enabled: Enable UPnP mode operation.

  Disabled: Disable UPnP mode operation.

  When the mode is enabled, two ACEs are added automatically to trap UPNP related packets to CPU. The ACEs are automatically removed when the mode is disabled. .

- **TTL :**

  The TTL value is used by UPnP to send SSDP advertisement messages. Valid values are in the range 1 to 255.

- **Advertising Duration :**

  The duration, carried in SSDP packets, is used to inform a control point or control points how often it or they should receive an SSDP advertisement message from this switch. If a control point does not receive any message within the duration, it will think that the switch no longer exists. Due to the unreliable nature of UDP, in the standard it is recommended that such refreshing of advertisements to be done at less than one-half of the advertising duration. In the implementation, the switch sends SSDP messages periodically at the interval one-half of the advertising duration minus 30 seconds. Valid values are in the range 100 to 86400.

- **IP Addressing Mode :**

IP addressing mode provides two ways to determine IP address assignment:
Dynamic: Default selection for UPnP. UPnP module helps users choosing the IP address of the switch device. It finds the first available system IP address.
Static: User specifies the IP interface VLAN for choosing the IP address of the switch device.

- **Static VLAN Interface ID:**

  The index of the specific IP VLAN interface. It will only be applied when IP Addressing Mode is static. Valid configurable values ranges from 1 to 4095. Default value is 1.

Buttons

- **Save :**

  Click to save changes.

- **Reset :**

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

2-28 MRP

MRP, defined in International Electrotechnical Commission (IEC) standard 62439-2, provides fast convergence in a ring network topology for industrial networks.

A ring of Ethernet switches can use the Media Redundancy Protocol (MRP) to overcome a failure faster than with STP. An MRP network consists of a ring of switches with one master switch; the rest of the switches are clients. The switches in the ring must use physical ports to form the ring or a single port configured as a static trunk. The MRP ring ports are disabled in STP.

2.28.1 Ports

This page allows you to configure the MRP generic settings for all switch ports.

Web Interface

To configure the MRP Ports Configuration in the web interface:

1. Click Configuration MRP and Port
2. Specify the parameters in each blank field.
3. Click save to save the setting.
4. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.

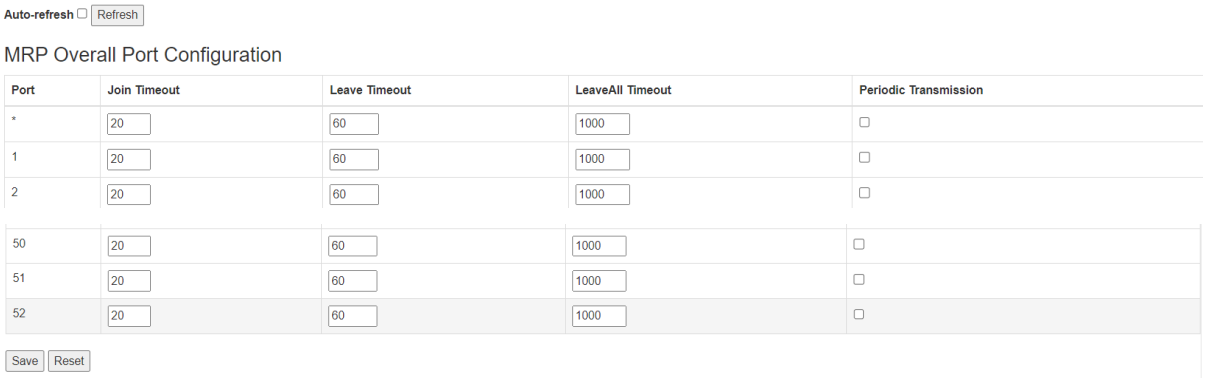


Figure 2-28.1: The MRP Ports Configuration

Parameter description:

- **Port :**

  The port number for which the following configuration applies.

- **Join Timeout:**

  Controls the timeout of the Join Timer for all MRP Applications on this switch port. This value is restricted to 1-20 centiseconds.

- **Leave Timeout:**

  Controls the timeout of the Leave Timer for all MRP Applications on this switch port. This value is restricted to 60- 300 centiseconds.

- **LeaveAll Timeout :**

  Controls the timeout of the LeaveAll Timer for all MRP Applications on this switch port. This value is restricted to 1000- 5000 centiseconds.

- **Periodic Transmission:**

Enable or disable the PeriodicTransmission feature for all MRP Applications on this switch port.

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.

- **Auto-refresh :**

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

2.28.2 MVRP

This section allows you to configure the MVRP global and per port settings altogether. The page

is divided into a global section and a per-port configuration section.

Web Interface

To configure the MRP Ports Configuration in the web interface:

1. Click Configuration MRP and MVRP
2. Specify the parameters in each blank field.
3. Click save to save the setting.
4. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.

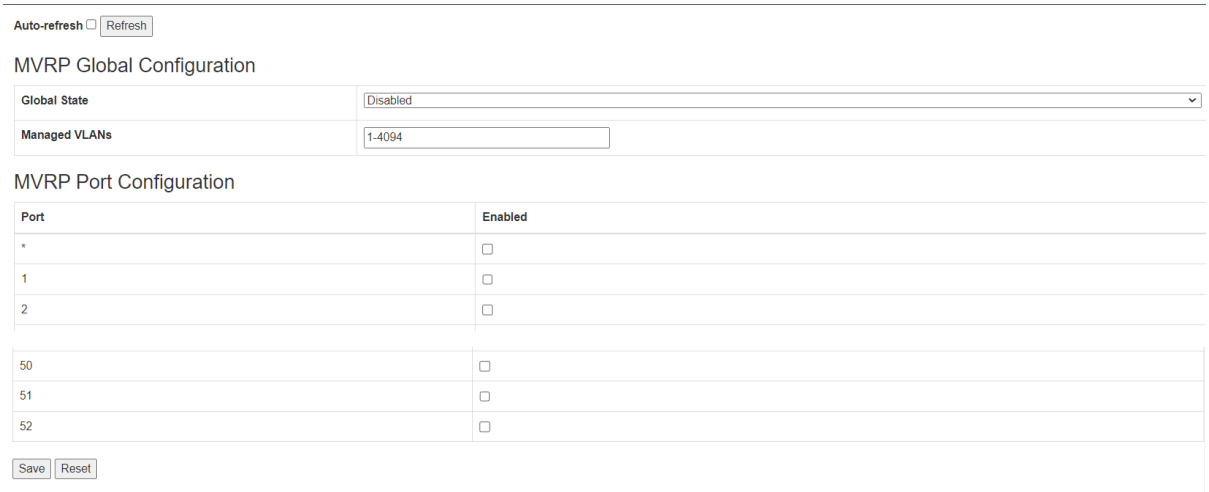


Figure 2-28.2: The MRP Ports Configuration

Parameter description:

- **Global State :**

  Enable or disable the MVRP protocol globally. This will enable or disable the protocol globally and at the same time on the switch ports that are MVRP enabled.

- **Managed VLANs:**

  This field shows the managed VLANs, i.e. the VLANs that MVRP will operate upon. By default, only VLANs 1- 4094 are managed, i.e. the entire range as defined in IEEE802.1Q-2014 for MVRP. However this range can be limited by using a list syntax where the individual elements are separated by commas. Ranges are specified with a dash separating the lower and upper bound.
  The following example will create VLANs 1, 10, 11, 12, 13, 200, and 300: 1,10-13,200,300. Spaces are allowed in between the delimiters.

- **Port:**

  The port number for which the following configuration applies.

- **Enabled :**

  Enable or disable the MVRP protocol on this switch port. This will enable or disable the protocol on the switch port given that MVRP is also globally enabled.

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.

- **Auto-refresh :**

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

2-29 GVRP

The Generic Attribute Registration Protocol (GARP) provides a generic framework whereby devices in a bridged LAN, e.g. end stations and switches, can register and de-register attribute values, such as VLAN Identifiers, with each other. In doing so, the attributes are propagated to devices in the bridged LAN, and these devices form a ¡°reachability¡± tree that is a subset of an active topology. GARP defines the architecture, rules of operation, state machines and variables for the registration and de-registration of attribute values.

A GARP participation in a switch or an end station consists of a GARP application component, and a GARP Information Declaration (GID) component associated with each port or the switch. The propagation of information between GARP participants for the same application in a bridge is carried out by the GARP Information Propagation (GIP) component. Protocol exchanges take place between GARP participants by means of LLC Type 1 services, using the group MAC address and PDU format defined for the GARP application concerned.

2-29.1 Global Config

This page allows you to configure the basic GVRP Configuration settings for all switch ports.

Web Interface

To configure the GVRP in the web interface:

1. Click Configuration, GVRP and Global Config
2. Evoke to enable or disable the GVRP.
3. Specify Join-time, Leave-time, Leave All-time, Max VLANs
4. Click Save to save the setting.
5. If you want to cancel the setting then you need to click the Reset button.

   It will revert to previously saved values.

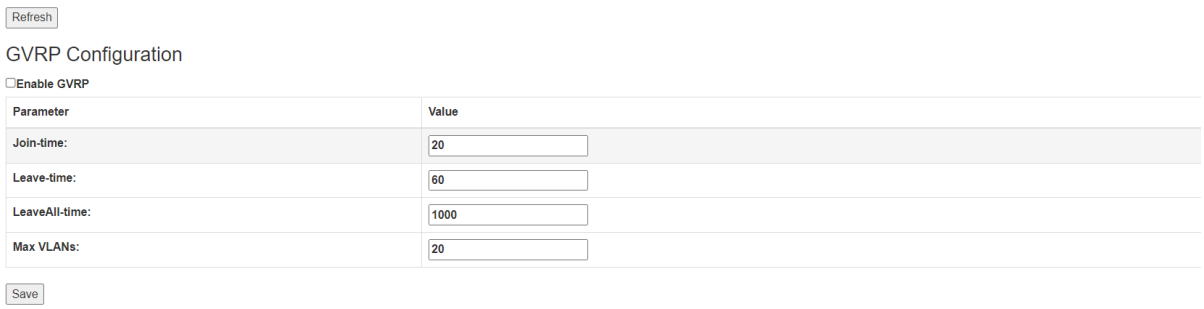


Figure 2-29.1: The GVRP Configuration

Parameter description:

Enable GVRP globally

The GVRP feature is enabled by setting the check mark in the checkbox named Enable GVRP.

GVRP protocol timers

Join-time is a value in the range 1-20cs in the units of centi seconds, i.e. in units of one hundredth of a second. The default is 20cs.

Leave-time is a value in the range 60-300cs in the units of centi seconds, i.e. in units of one hundredth of a second. The default is 60cs.

Leave All-time is a value in the range 1000-5000cs in the units of centi seconds, i.e. in units of one hundredth of a second. The default is 1000cs.

Max number of VLANs

When GVRP is enabled a maximum number of VLANs supported by GVRP is specified. By default this number is 20. This number can only be changed when GVRP is turned off.

Buttons

- **Save :**

  Click to save changes.

- **Reset :**

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

- **Refresh :**

  Refreshes the displayed table starting from the input fields.

2-29.2 Port Config

This page allows you to configure the basic GVRP Configuration settings for all switch ports. The settings relate to the currently selected unit, as reflected by the page header.

Web Interface

To configure the GVRP in the web interface:

1. Click Configuration, GVRP and Port Config
2. Evoke to enable or disable the Mode.
3. Click save to save the setting.
4. If you want to cancel the setting then you need to click the Reset button.

It will revert to previously saved values.

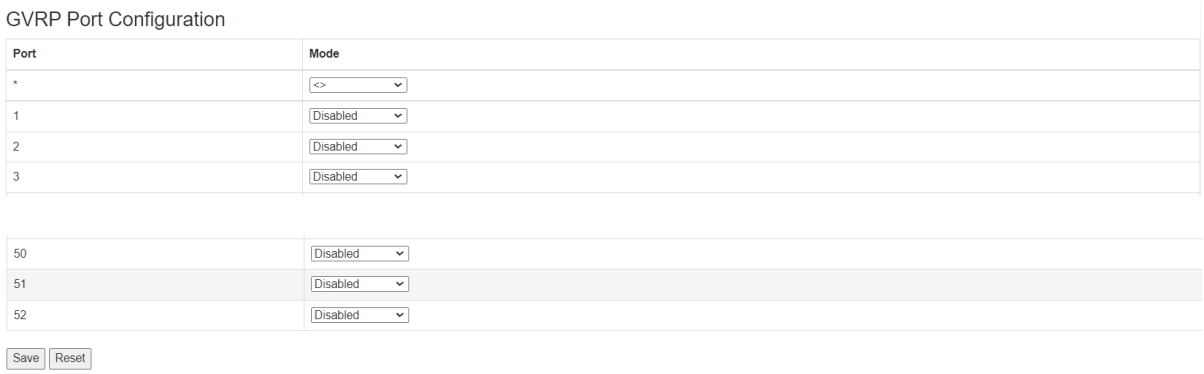


Figure 2-29.2: The GVRP Configuration

Parameter description:

- **Port :**

  The Port column shows the list of ports.

- **Mode :**

  This configuration is to enable/disable GVRP Mode on particular port locally.

  Disable: Select to Disable GVRP mode on this port.
  GVRP Enable: Select to Enable GVRP mode on this port.

Buttons

- **Save :**

  Click to save changes.

- **Reset :**

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

The sFlow Collector configuration for the switch can be monitored and modified here. The configuration is divided into two parts: Configuration of the sFlow receiver (a.k.a. sFlow collector) and configuration of per-port flow and counter samplers.

sFlow configuration is not persisted to non-volatile memory, which means that a reboot or master change will disable sFlow sampling.

Web Interface

To configure the sFlow in the web interface:

1. Click Configuration and sFlow.
2. Set the parameters.
3. Click save to save the setting.
4. If you want to cancel the setting then you need to click the Reset button.

   It will revert to previously saved values.

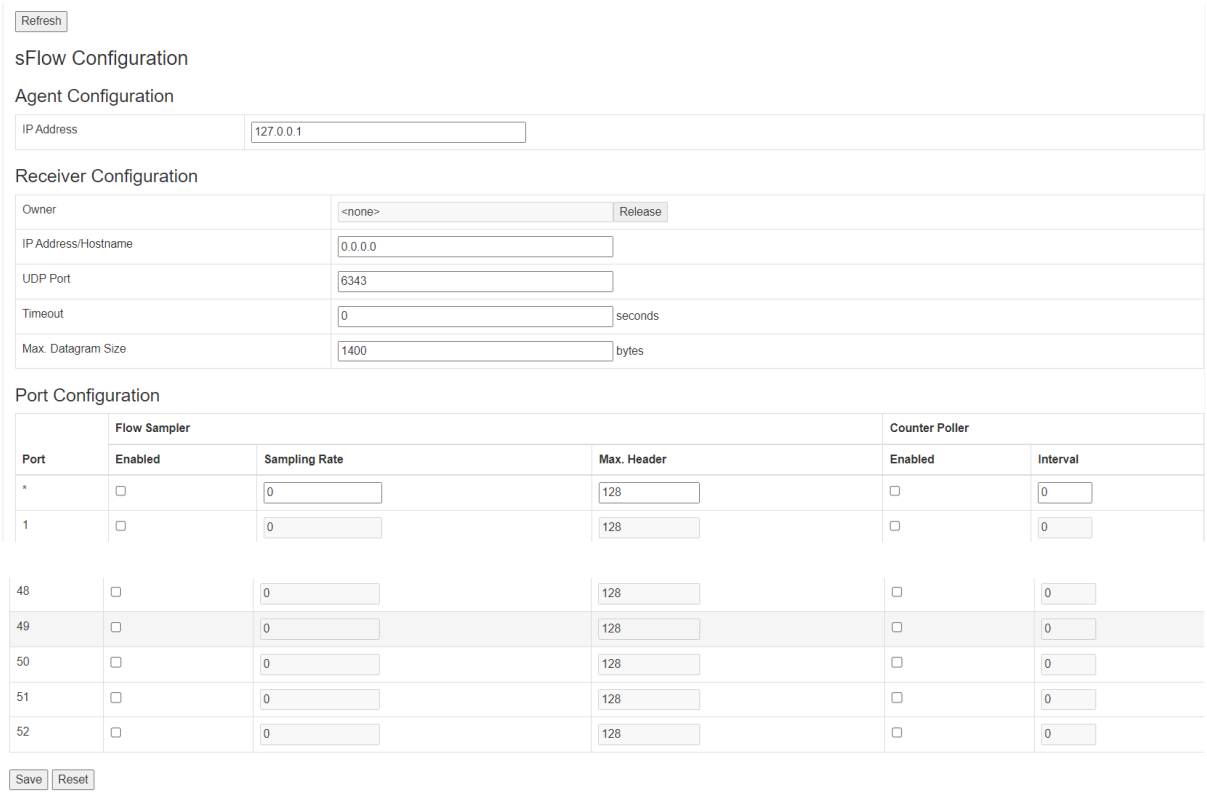


Figure 2-30: The sFlow Configuration

Parameter description:

Agent Configuration

- **IP Address :**

  The IP address used as Agent IP address in sFlow datagrams. It serves as a unique key that will identify this agent over extended periods of time.

  Both IPv4 and IPv6 addresses are supported.

Receiver Configuration

- **Owner :**

  Basically, sFlow can be configured in two ways: Through local management using the Web or CLI interface or through SNMP. This read-only field shows the owner of the current sFlow configuration and assumes values as follows:
  • If sFlow is currently unconfigured/unclaimed, Owner contains <none>.
  • If sFlow is currently configured through Web or CLI, Owner contains <Configured through local management>.
  • If sFlow is currently configured through SNMP, Owner contains a string identifying the sFlow receiver.
  If sFlow is configured through SNMP, all controls - except for the Release-button - are disabled to avoid inadvertent reconfiguration.

  The Release button allows for releasing the current owner and disable sFlow sampling. The button is disabled if sFlow is currently unclaimed. If configured through SNMP, the release must be confirmed (a confirmation request will appear).

- **IP Address/Hostname :**

  The IP address or hostname of the sFlow receiver. Both IPv4 and IPv6 addresses are supported.

- **UDP Port :**

  The UDP port on which the sFlow receiver listens to sFlow datagrams. If set to 0 (zero), the default port (6343) is used.

- **Timeout :**

  The number of seconds remaining before sampling stops and the current sFlow owner is released. While active, the current time left can be updated with a click on the Refresh-button. If locally managed, the timeout can be changed on the fly without affecting any other settings.

- **Max. Datagram Size :**

  The maximum number of data bytes that can be sent in a single sample datagram. This should be set to a value that avoids fragmentation of the sFlow datagrams. Valid range is 200 to 1468 bytes with default being 1400 bytes.

Port Configuration

- **Port :**

  The port number for which the configuration below applies.

- **Flow Sampler Enabled :**

  Enables/disables flow sampling on this port.

- **Flow Sampler Sampling Rate :**

  The statistical sampling rate for packet sampling. Set to N to sample on average 1/Nth of the packets transmitted/received on the port.
  Not all sampling rates are achievable. If an unsupported sampling rate is requested, the switch will automatically adjust it to the closest achievable. This will be reported back in this field.Valid range is 1 to 32767.

- **Flow Sampler Max. Header :**

  The maximum number of bytes that should be copied from a sampled packet to the sFlow datagram. Valid range is 14 to 200 bytes with default being 128 bytes.
  If the maximum datagram size does not take into account the maximum header size, samples may be dropped.

- **Counter Poller Enabled :**

  Enables/disables counter polling on this port.

- **Counter Poller Interval :**

  With counter polling enabled, this specifies the interval - in seconds - between counter poller samples. Valid range is 1 to 3600 seconds.

Buttons

- **Save :**

  Click to save changes.

- **Reset :**

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

- **Release :**

  See description under Owner.

- **Refresh :**

  Click to refresh the page. Note that unsaved changes will be lost.

2-31 DDMI

DDMI or DDM, its full name is Digital Diagnostic Monitoring (Interface) is the technology used in optical modules so that users can monitor the real-time parameters of optical modules. These parameters include working temperature, working voltage, working current, transmitting and receiving optical power, etc., and can also display the factory information of the module and prompt alarms/warnings.

Web Interface

To configure the DDMI Configuration in the web interface:

1. Click Configuration, DDMI
2. Evoke to enable the DDMI Mode
3. Click the save to save the setting
4. If you want to cancel the setting then you need to click the Reset button.

   It will revert to previously saved values

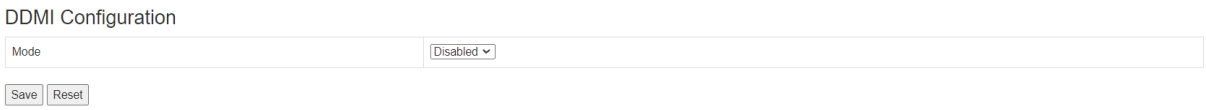


Figure 2-31: The DDMI Configuration

Parameter description:

- **Mode:**

  Indicates the DDMI mode operation. Possible modes are:
  Enabled: Enable DDMI mode operation.
  Disabled: Disable DDMI mode operation.

Buttons

- **Save :**

  Click to save changes.

- **Reset :**

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

Unidirectional Link Detection (UDLD) is a layer 2 protocol used to determine the physical status of a link. The purpose of UDLD is to detect and deter issues that arise from Unidirectional Links. UDLD helps to prevent forwarding loops and blackholing of traffic by identifying and acting on logical one-way links that would otherwise go undetected.

Web Interface

To configure the UDLD in the web interface:

5. Click Configuration, UDLD
6. Scroll to select the Severity Level
7. Specify the parameters in each blank field.
8. Click the apply to save the setting
9. If you want to cancel the setting then you need to click the Reset button.

It will revert to previously saved values

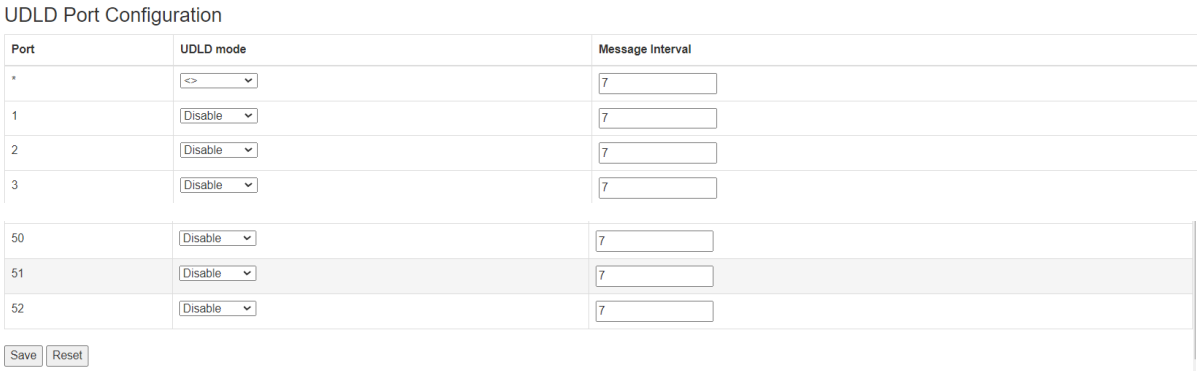


Figure 2-32: The UDLD Configuration

Parameter description:

- **Port :**

  Port number of the switch.

- **ULLD Mode :**

  Configures the UDLD mode on a port. Valid values are Disable, Normal and Aggressive. Default mode is Disable.

  Disable: In disabled mode, UDLD functionality doesn't exists on port.

  Normal: In normal mode, if the link state of the port was determined to be unidirectional, it will not affect the port state.

  Aggressive: In aggressive mode, unidirectional detected ports will get shutdown. To bring back the ports up, need to disable UDLD on that port.

- **Message Interval:**

  Configures the period of time between UDLD probe messages on ports that are in the advertisement phase and are determined to be bidirectional. The range is from 7 to 90 seconds(Default value is 7 seconds)(Currently default time interval is supported, due to lack of detailed information in RFC 5171).

Buttons

- **Save :**

  Click to save changes.

- **Reset :**

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

Chapter 3 Monitor

This chapter describes all of the basic network statistics which includes the Ports, Layer 2 network protocol (e.g. NAS, ACL, DHCP, AAA and RMON etc.) and any setting of the Switch.

3-1 System

After you login, the switch shows you the system information. This page is default and tells you the basic information of the system, including “Model Name”, “System Description”, “Contact”, “Location”, “System Up Time”, “Firmware Version”, “Host Mac Address”, “Device Port”. With this information, you will know the software version used, MAC address, serial number, how many ports good and so on. This is helpful while malfunctioning.

3-1.1 Information

The switch system information is provided here.

Web interface

To display System Information in the web interface:

1. Click Monitor, System and Information.
2. Check the contact information for the system administrator as well as the name and location of the switch. Also indicate the local time zone by configuring the appropriate offset.
3. Click the “Refresh”

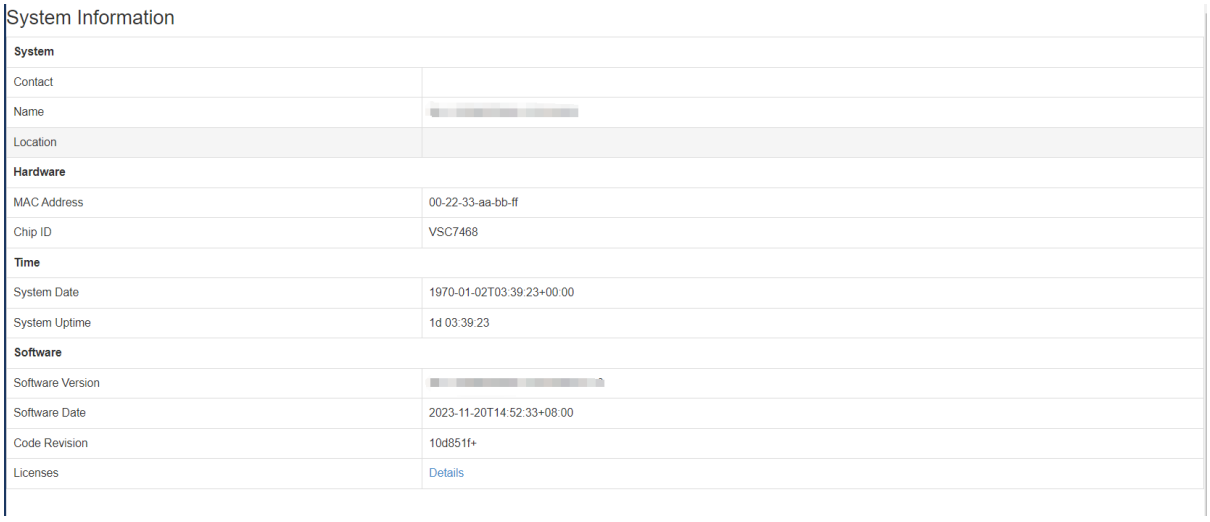


Figure 3-1.1: System Information

Parameter description:

- **Contact :**

  The system contact configured in Configuration | System | Information | System Contact.

- **Name :**

  Displays the user-defined system name that configured in System | System Information | Configuration | System Name.

- **Location:**

  The system location configured in Configuration | System | Information | System Location.

- **MAC Address :**

  The MAC Address of this switch.

- **Chip ID :**

  The Chip ID of this switch.

- **System Date :**

  The current (GMT) system time and date. The system time is obtained through the Timing server running on the switch, if any.

- **System Uptime :**

  The period of time the device has been operational.

- **Software Version :**

  Displays the current software version number.

- **Software Date :**

  The date when the switch software was produced.

- **Code Revision :**

  The version control identifier of the switch software.

3-1.2 LED

The switch system LED status is provided here.

Web interface

To display LED in the web interface:

1. Click Monitor, System and LED.

2. Check clear type

4. Click the "Refresh"

Figure 3-1.2: System Information

Parameter description:

- **Clear Type :**

  The types of system LED status clearing. Possible values are:
  All: Clear all error status of the system LED and back to normal indication.
  Fatal: Clear fatal error status of the system LED.
  Software: Clear generic software error status of the system LED.

- **Desription :**

  The description of system LED.

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 selected error status of system LED.

3-1.3 CPU Load

This page displays the CPU load, using an SVG graph.

The load is measured as averaged over the last 100ms, 1sec and 10 seconds intervals. The last 120 samples are graphed, and the last numbers are displayed as text as well.

In order to display the SVG graph, your browser must support the SVG format. Consult the SVG Wiki for more information on browser support. Specifically, at the time of writing, Microsoft Internet Explorer will need to have a plugin installed to support SVG.

Web interface

To display CPU Load in the web interface:

1. Click Monitor, System andCPU
2. Click the "Refresh"

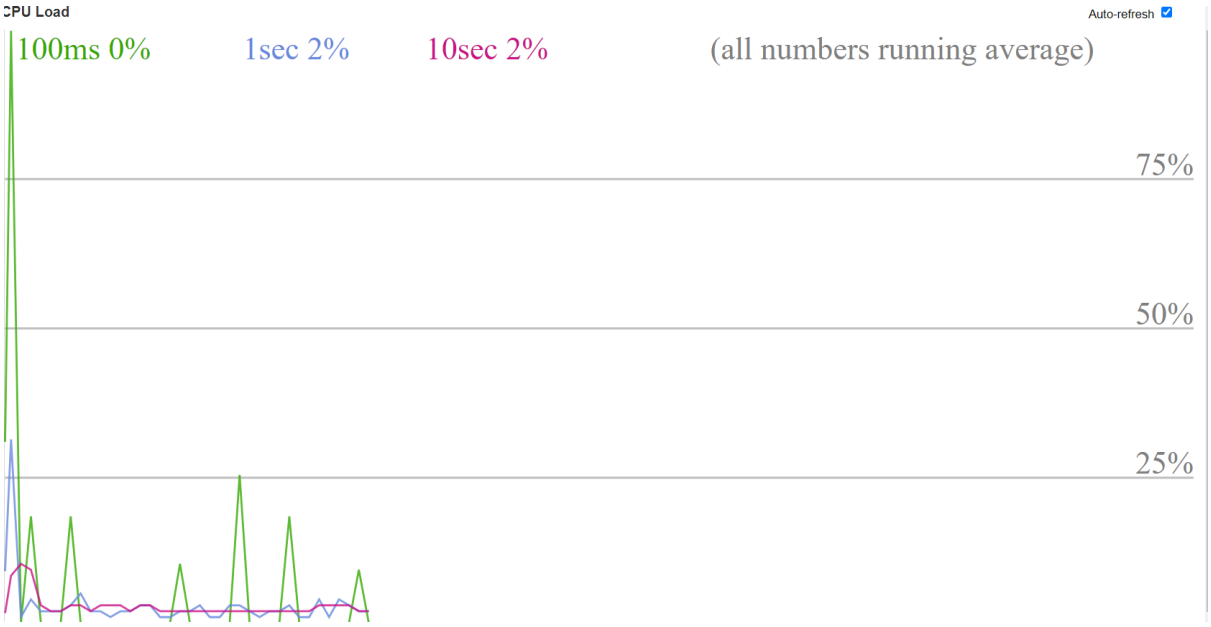


Figure 3-1.3: CPU Information

Buttons

- **Auto-refresh :**

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

3-1.4 IP Status

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.

Web Interface

To display the IP interfaces information in the web interface:

1. Click Monitor, System and IP Status.
2. Display the IP address information.

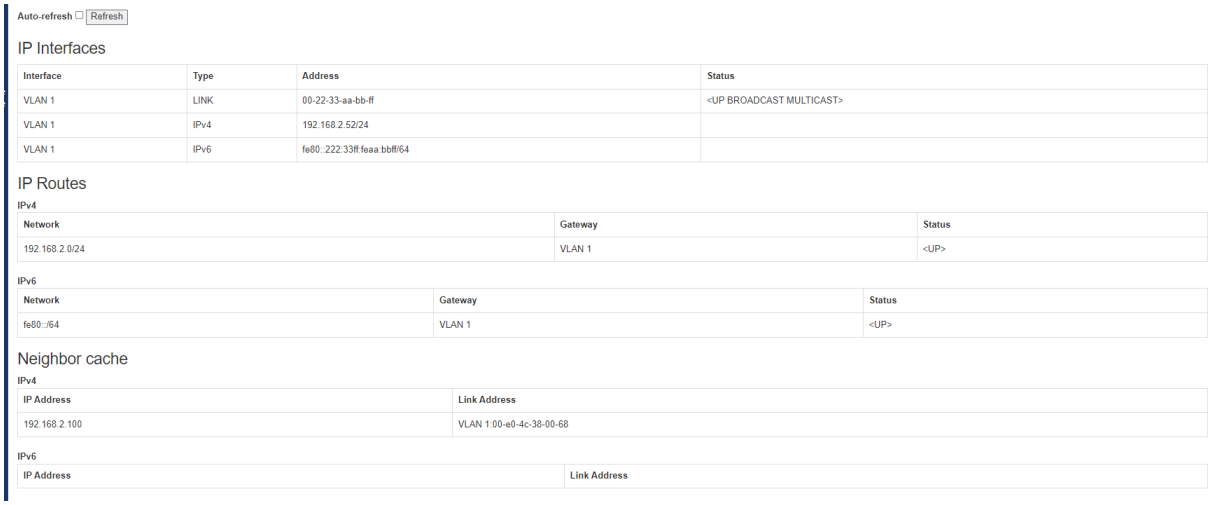


Figure 3-1.4:The IP Status

Parameter description:

IP Interfaces

- **Interface :**

  Show the name of the interface.

- **Type :**

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

- **Address :**

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

- **Status :**

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

IP Routes

- **Network :**

  Show the destination IPv4/IPv6 network or host address of this route.

- **Gateway :**

  Show the gateway address of this route.

- **Status :**

  Show the status flags of the route.

Neighbour cache

- **IP Address :**

  Show the IP address of the entry.

- **Link Address :**

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

Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page immediately.

3-1.5 IPv4 Routing Info. Base

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. This table provides IPv4 routing status.

Navigating the Routing Infomatoin Base Table

Each page shows up to 999 table entries, selected through the "entries per page" input field. When first visited, the web page will show the beginning entries of this table.

The "Start from ID" input field allow the user to change the starting point in this table. Clicking the button will update the displayed table starting from that or the closest next entry match.
In addition, these input fields will upon a button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start input field.

Web Interface

To display the IPv4 routing status in the web interface:

1. Click Monitor, System and IPv4 Routing Info. Base
2. Display the IP address information.

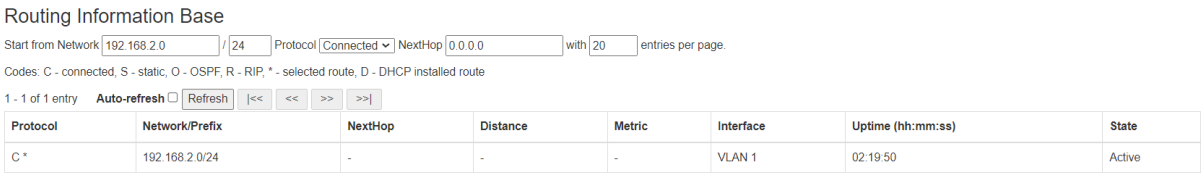


Figure 3-1.5:The IPv4 Routing Info Base

Parameter description:

- **Protocol :**

  The protocol that installed this route.
  DHCP: The route is created by DHCP.
  Connected: The destination network is connected directly.
  Static: The route is created by user.
  OSPF: The route is created by OSPF.

- **Network/Prefix :**

  Network and prefix (example 10.0.0.0/16) of the given route entry.

- **NextHop:**

  Next-hop IP address. All-zeroes indicates the link is directly connected.

- **Distance :**

  Distance of the route.

- **Metric :**

  Metric of the route.

- **Interface :**

  Next-hop interface.

- **Uptime(hh:mm:ss) :**

  Time (in seconds) since this route was created

- **State:**

  Destination is active.

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 entries, starting from the first available entry. If the first entry of the table is displayed, the button is disabled

- **<< :**

  Updates the table entries, ending at the entry prior to the first entry currently displayed. If the first entry of the table is displayed, the button is disabled

- **>>| :**

  Updates the table entries, starting from the entry next to the last entry currently displayed. If the last entry of the table is displayed, the button is disabled.

- **>> :**

  Updates the table entries, ending at the last available entry. If the last entry of the table is displayed, the button is disabled.

3-1.6 IPv6 Routing Info. Base

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. This table provides IPv6 routing status.

Navigating the Routing Infomatoin Base Table

Each page shows up to 999 table entries, selected through the "entries per page" input field. When first visited, the web page will show the beginning entries of this table.

The "Start from ID" input field allow the user to change the starting point in this table. Clicking the button will update the displayed table starting from that or the closest next entry match.
In addition, these input fields will upon a button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start input field.

Web Interface

To display the IPv6 routing status in the web interface.

1. Click Monitor, System and IPv6 Routing Info. Base
2. Display the IP address information.

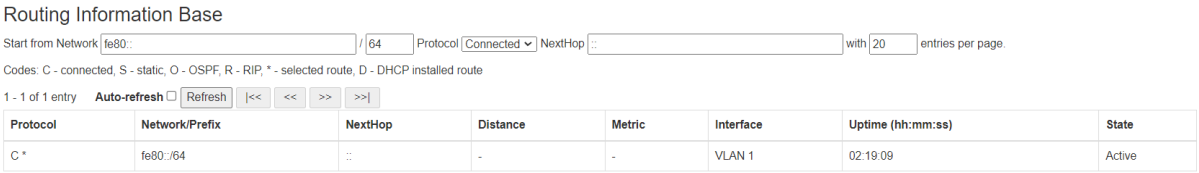


Figure 3-1.6:The IPv6 Routing Info Base

Parameter description:

- **Protocol :**

  The protocol that installed this route.
  DHCP: The route is created by DHCP.
  Connected: The destination network is connected directly.
  Static: The route is created by user.
  OSPF: The route is created by OSPF.

- **Network/Prefix :**

  Network and prefix (example 10.0.0.0/16) of the given route entry.

- **NextHop:**

  Next-hop IP address. All-zeroes indicates the link is directly connected.

- **Distance :**

  Distance of the route.

- **Metric :**

  Metric of the route.

- **Interface :**

  Next-hop interface.

- **Uptime(hh:mm:ss) :**

Time (in seconds) since this route was created

- **State:**

  Destination is active.

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 entries, starting from the first available entry. If the first entry of the table is displayed, the button is disabled

- **<< :**

  Updates the table entries, ending at the entry prior to the first entry currently displayed. If the first entry of the table is displayed, the button is disabled

- **>>| :**

  Updates the table entries, starting from the entry next to the last entry currently displayed. If the last entry of the table is displayed, the button is disabled.

- **>> :**

  Updates the table entries, ending at the last available entry. If the last entry of the table is displayed, the button is disabled.

3-1.7 Log

The switch system log information is provided here.

Web Interface

To display the log configuration in the web interface:

1. Click Monitor, System and Log.
2. Display the system log information

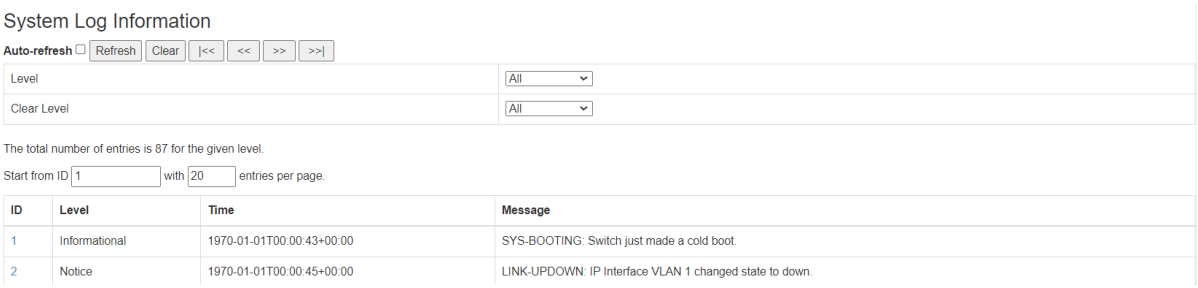


Figure 3-1.7: The System Log Information

Parameter description:

- **ID :**

  The identification of the system log entry.

- **Level :**

  The level of the system log entry.

  Info: The system log entry is belonged information level.
  Warning: The system log entry is belonged warning level.
  Error: The system log entry is belonged error level.

- **Time :**

  The occurred time of the system log entry.

- **Message :**

  The detail message of the system log entry.

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 entries, starting from the first available entry. If the first entry of the table is displayed, the button is disabled

- **<< :**

  Updates the table entries, ending at the entry prior to the first entry currently displayed. If the first entry of the table is displayed, the button is disabled

- **>>| :**

  Updates the table entries, starting from the entry next to the last entry currently displayed. If the last entry of the table is displayed, the button is disabled.

- **>> :**

  Updates the table entries, ending at the last available entry. If the last entry of the table is displayed, the button is disabled.

3-1.8 Detailed Log

The switch system detailed log information is provided here.

Web Interface

To display the detailed log configuration in the web interface:

1. Click Monitor, System and Detailed Log.
2. Display the log information.

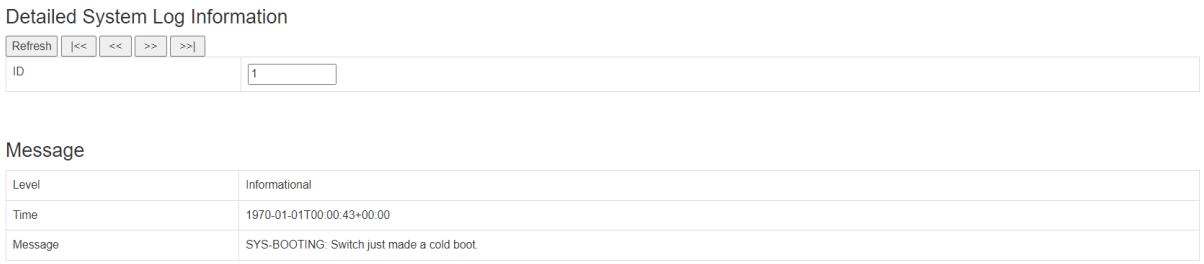


Figure 3-1.8: The Detailed System Log Information

Parameter description:

- **ID :**

  The ID (>= 1) of the system log entry.

- **Message :**

  The detailed message of the system log entry.

  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 entries, starting from the first available entry. If the first entry of the table is displayed, the button is disabled

- **<< :**

  Updates the table entries, ending at the entry prior to the first entry currently displayed. If the first entry of the table is displayed, the button is disabled

- **>>| :**

  Updates the table entries, starting from the entry next to the last entry currently displayed. If the last entry of the table is displayed, the button is disabled.

- **>> :**

  Updates the table entries, ending at the last available entry. If the last entry of the table is displayed, the button is disabled.

3-2 Green Ethernet

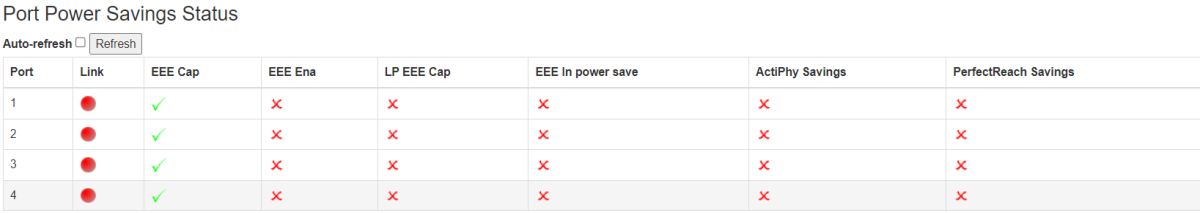
3-2.1 Port Power Savings

This page provides the current status for EEE.

Web Interface

To display the switch system overview in the web interface:

1. Click Monitor, Green Ethernet and Port Power Savings.
2. Display the Port Power Saving Status.


Port Power Savings Status

Auto-refresh ☐ Refresh

Port	Link	EEE Cap	EEE Ena	LP EEE Cap	EEE In power save	ActiPhy Savings	PerfectReach Savings
1		✓	×	×	×	×	×
2		✓	×	×	×	×	×
3		✓	×	×	×	×	×
4		✓	×	×	×	×	×

Figure 3-2.1: The Port Power Saving Status

Parameter description:

- **Local Port :**

  This is the logical port number for this row.

- **Link :**

  Shows if the link is up for the port (green = link up, red = link down).

- **EEE Cap:**

  Shows if the port is EEE capable.

- **EEE Ena:**

  Shows if EEE is enabled for the port (reflects the settings at the Port Power Savings configuration page).

- **LP EEE cap :**

  Shows if the link partner is EEE capable.

- **EEE In power save :**

  Shows if the system is currently saving power due to EEE. When EEE is enabled, the system will powered down if no frame has been received or transmitted in 5 uSec.

- **Actiphy Savings :**

  Shows if the system is currently saving power due to ActiPhy.

- **PerfectReach Savings :**

  Shows if the system is currently saving power due to PerfectReach.

Buttons

- **Auto-refresh :**

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

- **Refresh :** Click to refresh the page.

3-3 Ports

The section describes to configure the Port detail parameters of the switch. Others you could using the Port configure to enable or disable the Port of the switch. Monitor the ports content or status in the function.

3-3.1 Port State Overview

The port state overview is on the upper banner of the web interface.

Web Interface

This page is on the upper banner of the web interface. It is visible all the time for the users to understand the ports state quickly

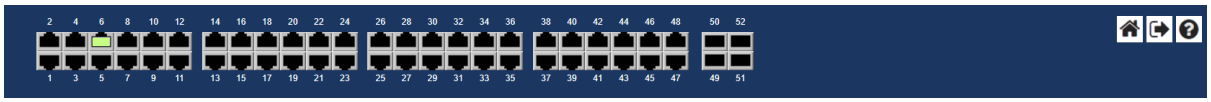
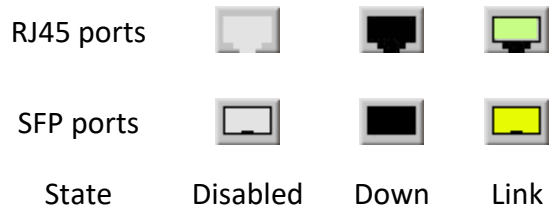


Figure 3-3.1: The Port State Overview

Parameter description:

- **The port states are illustrated as follows:**



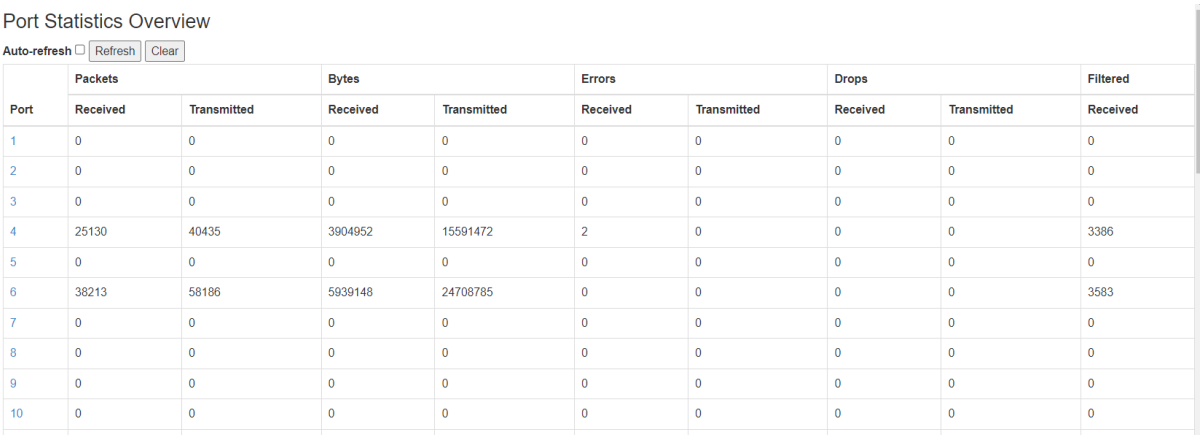
3-3.2 Traffic Overview

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

Web Interface

To Display the Port Statistics Overview in the web interface:

1. Click Monitor, Port and Traffic Overview.
2. If you want to auto-refresh then you need to evoke the “Auto-refresh”.
3. Click “ Refresh” to refresh the port statistics or clear all information when you click “ Clear”.



	Packets		Bytes		Errors		Drops		Filtered
Port	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	25130	40435	3904952	15591472	2	0	0	0	3386
5	0	0	0	0	0	0	0	0	0
6	38213	58186	5939148	24708785	0	0	0	0	3583
7	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0

Figure 3-3.2: The Port Statistics Overview

Parameter description:

- **Port :**

  The logical port for the settings contained in the same row.

- **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 discarded due to ingress or egress congestion.

- **Filtered :**

  The number of received frames filtered by the forwarding

Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page.

- **Clear :**

  Flushes the selected log entries.

3-3.3 Qos Statistics

This page provides statistics for the different queues for all switch ports.

Web Interface

To Display the Queuing Counters in the web interface:

1. Click Monitor, Ports and QoS Statistics
2. If you want to auto-refresh the information then you need to evoke the “Auto-refresh”.
3. Click “Refresh” to refresh the Queuing Counters or clear all information when you click “Clear”.

Queuing Counters

Auto-refresh ☐ Refresh Clear

	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q7	
Port	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	25128	28318	0	0	0	0	0	0	0	0	0	0	0	0	0	12117
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	40481	49673	0	0	0	0	0	0	0	0	0	0	0	0	0	12055
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Figure 3-3.3 The Queuing Counters Overview

Parameter description:

- **Port :**

  The logical port for the settings contained in the same row.

- **Qn :**

  Qn is the Queue number, There are 8 QoS queues per port. Q0 is the lowest priority queue.

- **Rx/Tx :**

  The number of received and transmitted 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.

- **Clear :**

  Flushes the selected log entries.

3-3.4 QCL Status

The section will let you know how to configure and 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.

Web Interface

To display the QoS Control List Status in the web interface:

1. Click Monitor, Ports and QCL Status
2. If you want to auto-refresh the information then you need to evoke the “Auto-refresh”.
3. Scroll to select the combined, static, Voice VLAN and conflict.
4. To click the “Refresh” to refresh an entry of the MVR Statistics Information.

Figure 3-3.4: The QoS Control List Status

Parameter description:

- **User :**

  Indicates the QCL user.

- **QCE :**

  Indicates the index of QCE.

- **Port :**

  Indicates the list of ports configured with the QCE.

- **Frame Type :**

  Indicates the type of frame to look for incoming frames. Possible frame types are:

  Any: The QCE will match all frame type.

  Ethernet: Only Ethernet frames (with Ether Type 0x600-0xFFFF) are allowed.

  LLC: Only (LLC) frames are allowed

  LLC: Only (SNAP) frames are allowed.

  IPv4: The QCE will match only IPV4 frames.

  IPv6: The QCE will match only 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.
Ingress Map: Classify Ingress Map ID.

- **Conflict :**

  Displays Conflict status of QCL entries. It may happen that resources required to add a QCE may not 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

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page.

- **Combined :**

  Select the QCL status from this drop down list.

- **Resolve Conflict :**

  Click to release the resources required to add QCL entry, in case the conflict status for any QCL entry is 'yes'.

3-3.5 Detailed Statistics

The section describes how to provide detailed traffic statistics for a specific switch port. Use the port select box to select which switch port details to display.

The displayed counters are the totals for receive and transmit, the size counters for receive and transmit, and the error counters for receive and transmit.

Web Interface

To Display per port detailed Statistics Overview in the web interface:

1. Click Monitor, Ports and Detailed Port Statistics
2. Scroll the Port Index to select which port you want to show the detailed
3. Port statistics overview.
4. If you want to auto-refresh the information then you need to evoke the “Auto-refresh”.
5. Click “Refresh” to refresh the port detailed statistics or clear all information when you click “Clear”.

Detailed Port Statistics

Port 1 **Auto-refresh** Refresh Clear

Receive Total		Transmit Total	
Rx Packets	0	Tx Packets	0
Rx Octets	0	Tx Octets	0
Rx Unicast	0	Tx Unicast	0
Rx Multicast	0	Tx Multicast	0
Rx Broadcast	0	Tx Broadcast	0
Rx Pause	0	Tx Pause	0
Receive Size Counters		**Transmit Size Counters**	
Rx 64 Bytes	0	Tx 64 Bytes	0
Rx 65-127 Bytes	0	Tx 65-127 Bytes	0
Rx 128-255 Bytes	0	Tx 128-255 Bytes	0
Rx 256-511 Bytes	0	Tx 256-511 Bytes	0
Rx 512-1023 Bytes	0	Tx 512-1023 Bytes	0
Rx 1024-1526 Bytes	0	Tx 1024-1526 Bytes	0
Rx 1527- Bytes	0	Tx 1527- Bytes	0

Receive Queue Counters		Transmit Queue Counters	
Rx Q0	0	Tx Q0	0
Rx Q1	0	Tx Q1	0
Rx Q2	0	Tx Q2	0
Rx Q3	0	Tx Q3	0
Rx Q4	0	Tx Q4	0
Rx Q5	0	Tx Q5	0
Rx Q6	0	Tx Q6	0
Rx Q7	0	Tx Q7	0
Receive Error Counters		**Transmit Error Counters**	
Rx Drops	0	Tx Drops	0
Rx CRC/Alignment	0	Tx Late/Exc. Coll.	0
Rx Undersize	0		
Rx Oversize	0		
Rx Fragments	0		
Rx Jabber	0		
Rx Filtered	0		

Figure 3-3.5: The Detailed Port Statistics

Parameter description:

Receive Total and Transmit Total

- **Rx and Tx Packets :**

  The number of received and transmitted (good and bad) packets.

- **Rx and Tx Octets :**

  The number of received and transmitted (good and bad) bytes. Includes FCS, but excludes framing bits.

- **Rx and Tx Unicast :**

  The number of received and transmitted (good and bad) unicast packets.

- **Rx and Tx Multicast :**

  The number of received and transmitted (good and bad) multicast packets.

- **Rx and Tx Broadcast :**

  The number of received and transmitted (good and bad) broadcast packets.

- **Rx and Tx Pause :**

  A count of the MAC Control frames received or transmitted on this port that have an opcode indicating a PAUSE operation.

Receive and Transmit Size Counters

The number of received and transmitted (good and bad) packets split into categories based on 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.

  Short frames are frames that are smaller than 64 bytes.

  Long frames are frames that are longer than the configured maximum frame length for this 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.

Receive MM Counters

- **Rx MM Fragments:**

  A count of received MAC frame fragments.

- **Rx MM Assembly Ok:**

  A count of MAC frames that were successfully reassembled and delivered to MAC.

- **Rx MM Assembly Errors :**

  A count of MAC frames with reassembly errors. The counter is incremented when the ASSEMBLY_ERROR state of the Receive Processing State Diagram is entered.

- **Rx MM SMD Errors:**

  A count of received MAC frames / MAC frame fragments rejected due to unknown SMD value or arriving with an SMD-C when no frame is in progress. The counter is incremented each time the BAD_FRAG state of the Receive Processing State Diagram is entered

Transmit MM Counters

- **Tx MM Fragments :**

  A count of transmitted MAC frame fragments.

- **Tx Hold :**

  A count of times MM_CTL.request(HOLD) primitive assertion caused preemption of a preemptable MAC frame.

Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page.

- **Clear :**

  Flushes the selected log entries.

Many Web pages use a port number to express an interface, whereas CLI uses interface names. The table on this page provides a means to convert from one to the other.

Web Interface

To Display interface name map on the web

1. Click Monitor, Ports and name map and show as following

Interface Name to Port Number Map

Interface Name	Port Number
Gi 1/1	1
Gi 1/2	2
Gi 1/3	3
Gi 1/4	4
Gi 1/5	5
Gi 1/6	6
Gi 1/7	7
Gi 1/8	8
Gi 1/9	9
Gi 1/10	10
Gi 1/47	47
Gi 1/48	48
10G 1/1	49
10G 1/2	50
10G 1/3	51
10G 1/4	52

Figure 3-3.6: The Detailed Port Statistics

This shows the current status of the ERPS instances.

Web Interface

To Display the ERPS status in the web interface:

1. Click Monitor and ERPS.
2. To display the ERPS status information

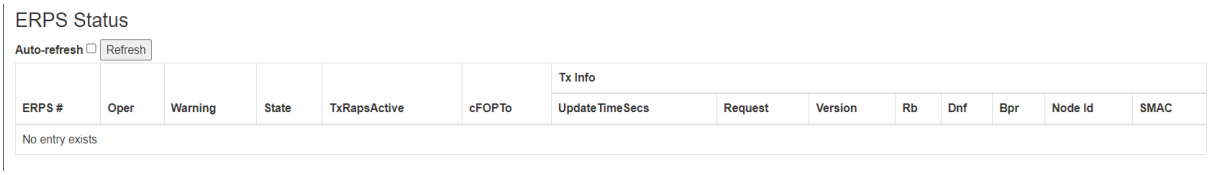


Figure 3-4: The ERPS Status Information

Parameter description:

- **ERPS# :**

  The ID of the ERPS. Click on link to get to ERPS detailed instance page, you can reset counters and issue commands.

- **Oper:**

  The operational state of ERPS instance.

  : Active.

  : Disabled or Internal error.

- **Warning :**

  Operational warnings of ERPS instance.

  : No warnings.

  : There are warnings, use tooltip to see.

- **State :**

  Specifies protection/node state of ERPS.

- **TxRapsActive :**

  Specifies whether we are currently supposed to be transmitting R-APS PDUs on our ring ports.

- **cFOPTo :**

  Failure of Protocol - R-APS Rx Time Out.

- **UpdateTimeSecs :**

  Time in seconds since boot that this structure was last updated.

- **Request :**

  Request/state according to G.8032, table 10-3.

- **Version:**

  Version of received/used R-APS Protocol. 0 means v1, 1 means v2, etc.

- **Rb:**

  RB (RPL blocked) bit of R-APS info. See Figure 10-3 of G.8032.

- **Dnf:**

  DNF (Do Not Flush) bit of R-APS info. See Figure 10-3 of G.8032."

- **Bpr:**

  BPR (Blocked Port Reference) of R-APS info. See Figure 10-3 of G.8032.

- **Node ID:**

  Node ID of this request.

- **SMAC:**

  The Source MAC address used in the request/state.

Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page.

Monitor MRP Status on this page.

Web Interface

To Display the MRP status in the web interface:

1. Click Monitor and MRP.
2. To display the MRP status information

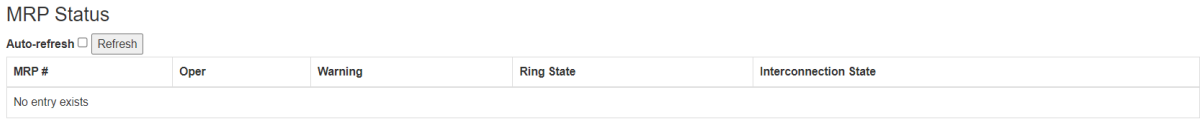


Figure 3-7 The MRP Status Information

Parameter description:

- **MRP# :**

  The ID of the ERPS. Click on link to get to ERPS detailed instance page, you can reset counters and issue commands.

Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page.

3-6 Link OAM

3-6.1 Statistics

This page provides detailed OAM traffic statistics for a specific switch port. Use the port select box to select which switch port details to display.
The displayed counters represent the total number of OAM frames received and transmitted for the selected port. Discontinuities of these counter can occur at re-initialization of the management system.

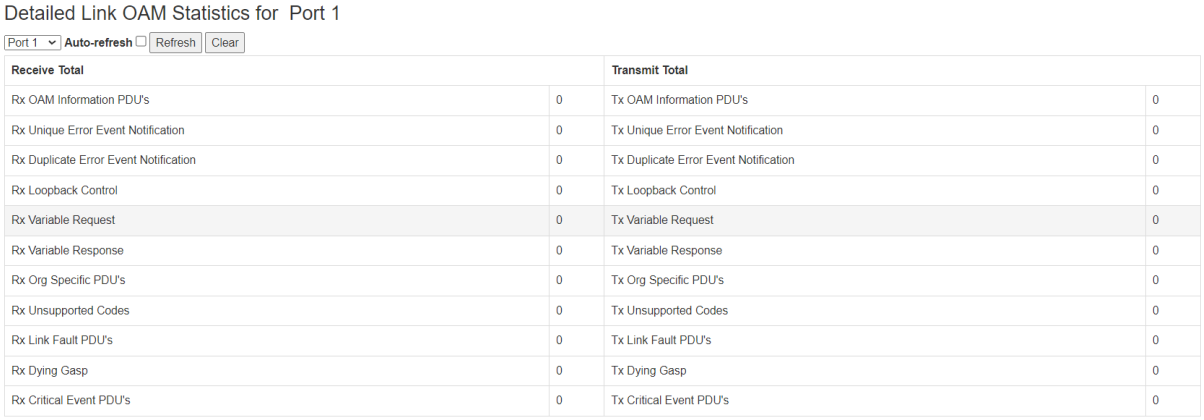
Web Interface

To Display the OAM Traffic Statistics in the web interface:

1. Click Monitor, OAM and Statistics

2. Select the port to show the details

3. To display the OAM statistics information


Detailed Link OAM Statistics for Port 1

Port 1 Auto-refresh Refresh Clear

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

Figure 3-6.1: The CFM Status Information

Parameter description:

- **Rx and Tx OAM Information PDU's:**

  The number of received and transmitted OAM Information PDU's. Discontinuities of this counter can occur at re-initialization of the management system.

- **Rx and Tx Unique Error Event Notification:**

  A count of the number of unique Event OAMPDUs received and transmitted on this interface. Event Notifications may be sent in duplicate to increase the probability of successfully being received, given the possibility that a frame may be lost in transit. Duplicate Event Notification transmissions are counted by Duplicate Event Notification counters for Tx and Rx respectively. A unique Event Notification OAMPDU is indicated as an Event Notification OAMPDU with a Sequence Number field that is distinct from the previously transmitted Event Notification OAMPDU Sequence Number.

- **Rx and Tx Duplicate Error Event Notification:**

  A count of the number of duplicate Event OAMPDUs received and transmitted on this interface. Event Notification OAMPDUs may be sent in duplicate to increase the probability of successfully being received, given the possibility that a frame may be lost in transit. A duplicate Event Notification OAMPDU is indicated as an Event Notification OAMPDU with a Sequence Number field that is identical to the previously transmitted Event Notification OAMPDU Sequence Number.

- **Rx and Tx Loopback Control :**

  A count of the number of Loopback Control OAMPDUs received and transmitted on this interface.

- **Rx and Tx Variable Request:**

  A count of the number of Variable Request OAMPDUs received and transmitted on this interface.

- **Rx and Tx Variable Response:**

  A count of the number of Variable Response OAMPDUs received and transmitted on this interface.

- **Rx and Tx Org Specific PDU's :**

  A count of the number of Organization Specific OAMPDUs transmitted on this interface.

- **Rx and Tx Unsupported Codes:**

  A count of the number of OAMPDUs transmitted on this interface with an unsupported op-code.

- **Rx and Tx Link fault PDU's :**

  A count of the number of Link fault PDU's received and transmitted on this interface.

- **Rx and Tx Dying Gasp :**

  A count of the number of Dying Gasp events received and transmitted on this interface.

- **Tx Rx and Tx Critical Event PDU's:**

  A count of the number of Critical event PDU's received and transmitted on this interface.

Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page.

This page provides Link OAM configuration operational status.
The displayed fields shows the active configuration status for the selected port.

Web Interface

To Display the OAM Traffic Statistics in the web interface:

1. Click Monitor, OAM and Statistics
2. Select the port to show the details
3. To display the OAM port status information

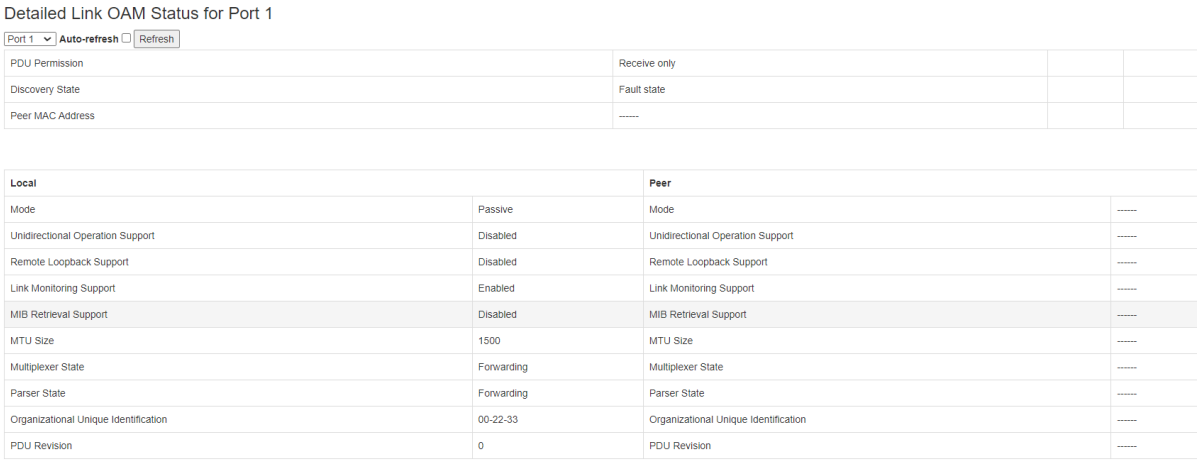


Figure 3-6.2: The OAM Port Status Information

Parameter description:

- **Mode:**

  The Mode in which the Link OAM is operating, Active or Passive.

- **Unidirectional Operation Support:**

  This feature is not available to be configured by the user. The status of this configuration is retrieved from the PHY.

- **Link Monitoring Support:**

  If status is enabled, DTE supports interpreting Link Events.

- **MIB Retrival Support:**

  If status is enabled, DTE supports interpreting Link Events.

- **MTU Size:**

  If status ie enabled DTE supports sending Variable Response OAMPDUs.

- **Multiplexer State:**

  It represents the largest OAMPDU, in octets, supported by the DTE. This value is compared to the remotes Maximum PDU Size and the smaller of the two is used.

- **Parser State:**

  When in forwarding state, the Device is forwarding non-OAMPDUs to the lower sublayer. Incase of discarding, the device discards all the non-OAMPDU's.

- **Organizational Unique Identification:**

24-bit Organizationally Unique Identifier of the vendor.

- **PDU Revision :**

  It indicates the current revision of the Information TLV. The value of this field shall start at zero and be incremented each time something in the Information TLV changes. Upon reception of an Information TLV from a peer, an OAM client may use this field to decide if it needs to be processed (an Information TLV that is identical to the previous Information TLV doesn't need to be parsed as nothing in it has changed).

- **PDU Permission :**

  This field is available only for the Local DTE. It displays the current permission rules set for the local DTE. Possible values are "Link fault","Receive only", "Information exchange only","ANY".

- **Discovery State:**

  Displays the current state of the discovery process. Possible states are Fault state, Active state, Passive state, SEND_LOCAL_REMOTE_STATE, SEND_LOCAL_REMOTE_OK_STATE, SEND_ANY_STATE.

Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page.

This page allows the user to inspect the current Link OAM Link Event configurations, and change them as well.

The left pane displays the Event status for the Local OAM unit while the right pane displays the status for the Peer for the respective port.

Web Interface

To Display the OAM event configurations in the web interface:

1. Click Monitor, OAM and Event Status
2. Select the port to show the details
3. To display the OAM event status information

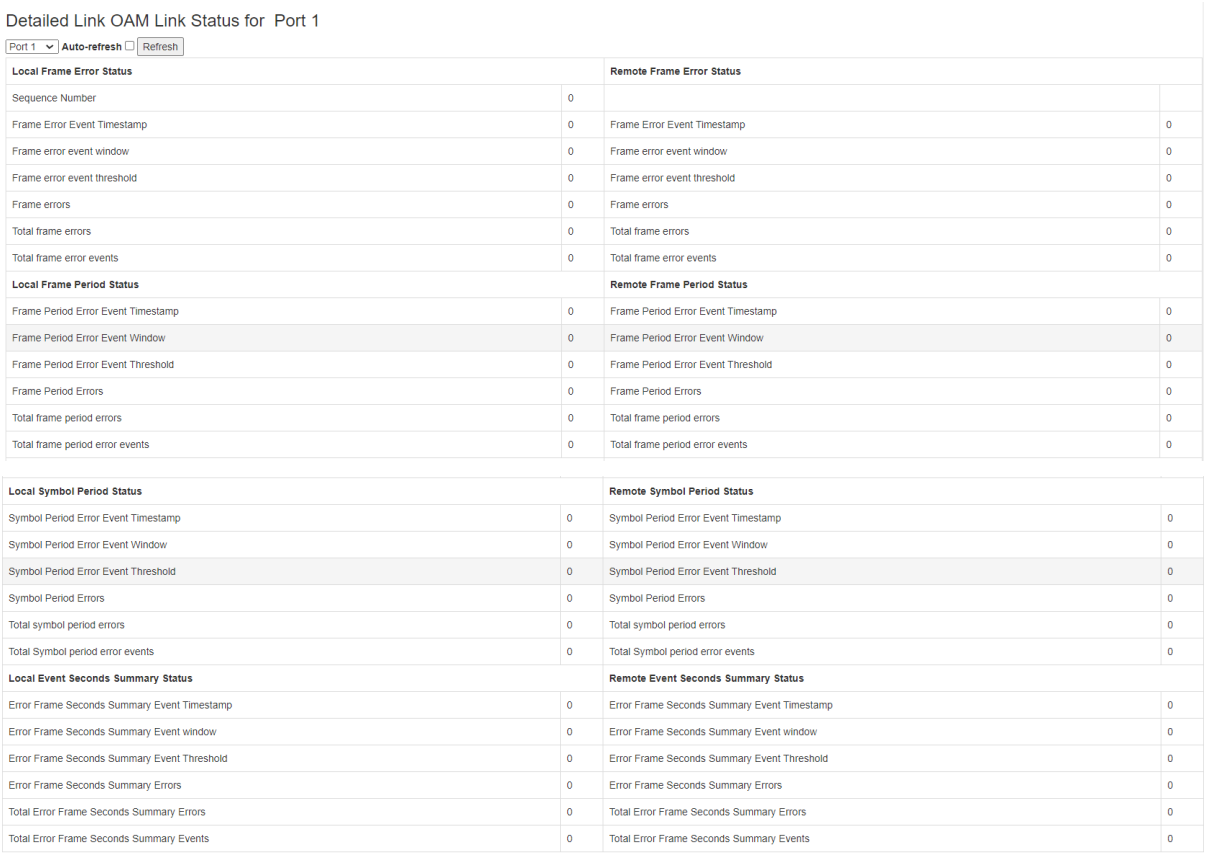


Figure 3-6.3: The OAM Event Status Information

Parameter description:

- **Port:**

  The switch port number

- **Sequence Number:**

  This two-octet field indicates the total number of events occurred at the remote end.

- **Notification Frame Error Event Timestamp:**

  This two-octet field indicates the time reference when the event was generated, in terms of 100 ms intervals.

- **Frame error event window:**

  This two-octet field indicates the duration of the period in terms of 100 ms intervals. 1) The default value is one second. 2) The lower bound is one second. 3) The upper bound is one

minute.

- **Frame error event threshold:**

  This four-octet field indicates the number of detected errored frames in the period is required to be equal to or greater than in order for the event to be generated. 1) The default value is one frame error. 2) The lower bound is zero frame errors. 3) The upper bound is unspecified.

- **Frame errors:**

  This four-octet field indicates the number of detected errored frames in the period.

- **Total frame errors:**

  This eight-octet field indicates the sum of errored frames that have been detected since the OAM sublayer was reset.

- **Total frame errors events:**

  This four-octet field indicates the number of Errored Frame Event TLVs that have been generated since the OAM sublayer was reset.

- **Frame Period Error Event Timestamp :**

  This two-octet field indicates the time reference when the event was generated, in terms of 100 ms intervals.

- **Frame Period Error Event Window :**

  This four-octet field indicates the duration of period in terms of frames.

- **Frame Period Error Event Threshold:**

  This four-octet field indicates the number of errored frames in the period is required to be equal to or greater than in order for the event to be generated.

- **Frame Period Errors:**

  This four-octet field indicates the number of frame errors in the period.

- **Total Frame Period Errors:**

  This eight-octet field indicates the sum of frame errors that have been detected since the OAM sublayer was reset.

- **Total Frame Period Error Events:**

  This four-octet field indicates the number of Errored Frame Period Event TLVs that have been generated since the OAM sublayer was reset.

- **Symbol Period Error Event Timestamp:**

  This two-octet field indicates the time reference when the event was generated, in terms of 100 ms intervals.

- **Symbol Period Error Event Window:**

  This eight-octet field indicates the number of symbols in the period.

- **Symbol Period Error Event Threshold:**

  This eight-octet field indicates the number of symbol errors in the period.

- **Symbol Period Errors:**

  This eight-octet field indicates the number of symbol errors in the period.

- **Total Symbol Period Errors:**

  This eight-octet field indicates the sum of symbol errors since the OAM sublayer was reset.

- **Total Symbol Period Errors Events:**

This four-octet field indicates the number of Errored Symbol Period Event TLVs that have been generated since the OAM sublayer was reset.

- **Error Frame Seconds Summary Event Timestamp:**

  This two-octet field indicates the time reference when the event was generated, in terms of 100 ms intervals, encoded as a 16-bit unsigned integer.

- **Error Frame Seconds Summary Event Window:**

  This two-octet field indicates the duration of the period in terms of 100 ms intervals, encoded as a 16-bit unsigned integer.

- **Error Frame Seconds Summary Event Threshold:**

  This two-octet field indicates the number of errored frame seconds in the period is required to be equal to or greater than in order for the event to be generated, encoded as a 16-bit unsigned integer.

- **Error Frame Seconds Summary Errors:**

  This two-octet field indicates the number of errored frame seconds in the period, encoded as a 16-bit unsigned integer.

- **Total Error Frame Seconds Summary Errors:**

  This four-octet field indicates the sum of errored frame seconds that have been detected since the OAM sublayer was reset.

- **Total Error Frame Seconds Summary Errors Events:**

  This four-octet field indicates the number of Errored Frame Seconds Summary Event TLVs that have been generated since the OAM sublayer was reset, encoded as a 32bit unsigned integer.

Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page.

- **Clear :**

  Click to clear the data.

3-7 DHCPv4

3-7.1 Server

DHCPv4 Server is used to allocate network addresses and deliver configuration parameters to dynamically configured hosts called DHCP client.

3-7.1.1 Statistics

This page displays the database counters and the number of DHCPv4 messages sent and received by DHCPv4 server.

Web Interface

To display the DHCPv4 server Statistics Overview in the web interface:

1. Click DHCPv4, Server and Statistics.
2. To display the DHCP Server Statistics.

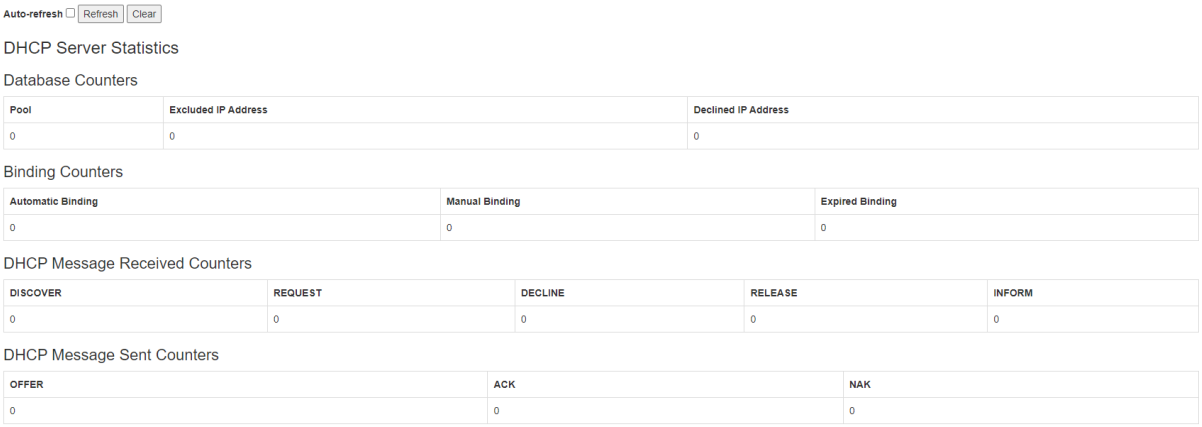


Figure 3-7.1.1: The DHCPv4 Server Statistics

Parameter description:

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 sec lined 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.

- **Clear :** Flushes the selected log entries.

3-7.1.2 Binding

This page displays bindings generated for DHCPv4 clients.

Web Interface

To Display DHCPv4 Server Binding IP in the web interface:

1. Click DHCPv4, Server and Binding.
2. To display the DHCP Server Binding IP.

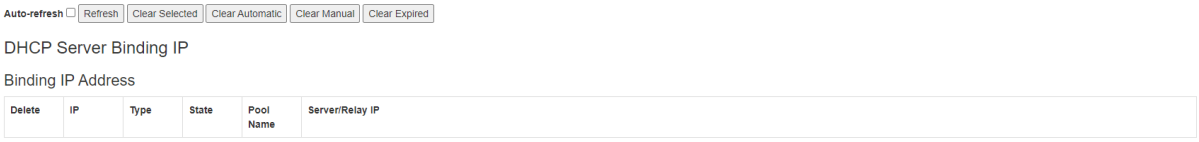


Figure 3-7.1.2: The DHCPv4 Server Binding IP

Parameter description:

Binding IP Address

Display all bindings.

- **IP :**

  IP address allocated to DHCP client.

- **Type :**

  Type of binding. Possible types are Automatic, Manual, and Expired.

- **State :**

  State of binding. Possible states are Committed, Allocated, and Expired.

- **Pool Name :**

  The pool that generates the binding.

- **Server/Relay ID :**

  Either IP address of dhcp server or, in case of relayed binding, IP address of relay agent through which binding was negotiated.

Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page.

- **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.

3-7.1.3 Declined IP

This page displays declined IP addresses.

Web Interface

To Display DHCPv4 Server Declined IP in the web interface:

1. Click DHCPv4, Server and Declined IP.
2. To display the DHCPv4 Declined IP.

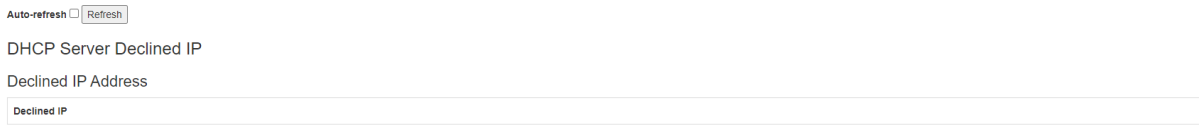


Figure 3-7.1.3: The Declined IP

Parameter description:

Declined IP Addresses

Display IP addresses declined by DHCP clients.

- **Declined 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.

3-7.2 Snooping Table

This page display the dynamic IP assigned information after DHCP Snooping mode is disabled. All DHCPv4 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.

Web Interface

To display the DHCPv4 in the web interface:

1. Click Monitor, DHCPv4 and Snooping table
2. To display Dynamic DHCPv4 Snooping Table.

Figure 3-7.2: The DHCPv4 snooping table

Parameter description:

- **MAC Address :**

  User MAC address of the entry.

- **VLAN ID :**

  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 Address :**

  DHCP Server address of the entry.

Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Refreshes the displayed table starting from the input fields.

- **Clear :**

  Flushes all dynamic entries.

- **|<<:**

  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.

3-7.3 Relay Statistics

This page provides statistics for DHCP relay.

Web Interface

To display monitor DHCPv4 Relay statistics in the web interface:

1. Click Monitor, DHCPv4 andrelay Statistics
2. To display DHCPv4 relay statistics.

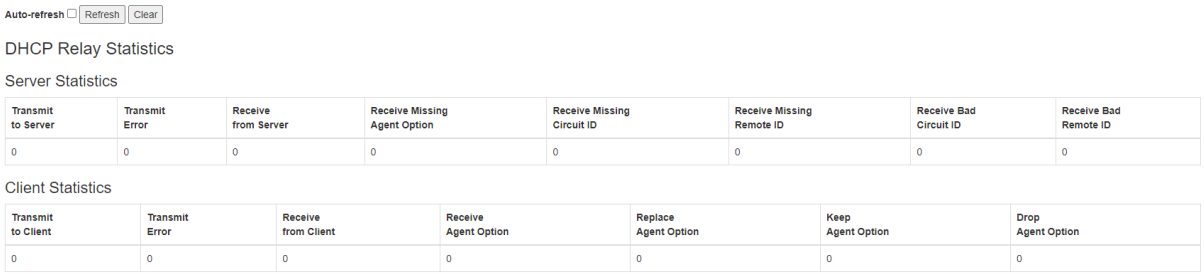


Figure 3-7.3: The DHCPv4 Detailed Statistics

Parameter description:

Server Statistics

- **Transmit to Server:**

  The number of packets that are relayed from client to server.

- **Transmit Error :**

  The number of packets received without agent information options.

- **Receive Missing Circuit ID:**

  The number of packets received with the Circuit ID option missing.

- **Receive Missing Remote ID:**

  The number of packets received with the Remote ID option missing.

- **Receive Bad Circuit ID:**

  The number of packets whose Circuit ID option did not match known circuit ID.

- **Receive Bad Remote ID:**

  The number of packets whose Remote ID option did not match known Remote ID.

Client Statistics

- **Transmit 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.

- **Keep Agent Option:**

  The number of packets whose relay agent information was retained.

- **Drop 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.

- **Clear :**

  Flushes the selected log entries.

3-7.4 Detailed Statistics

This page provides statistics for DHCPv4 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.

Web Interface

To display monitor DHCPv4 Relay statistics in the web interface:

3. Click Monitor, DHCPv4 and Detailed Statistics
4. To display DHCPv4 detailed statistics.

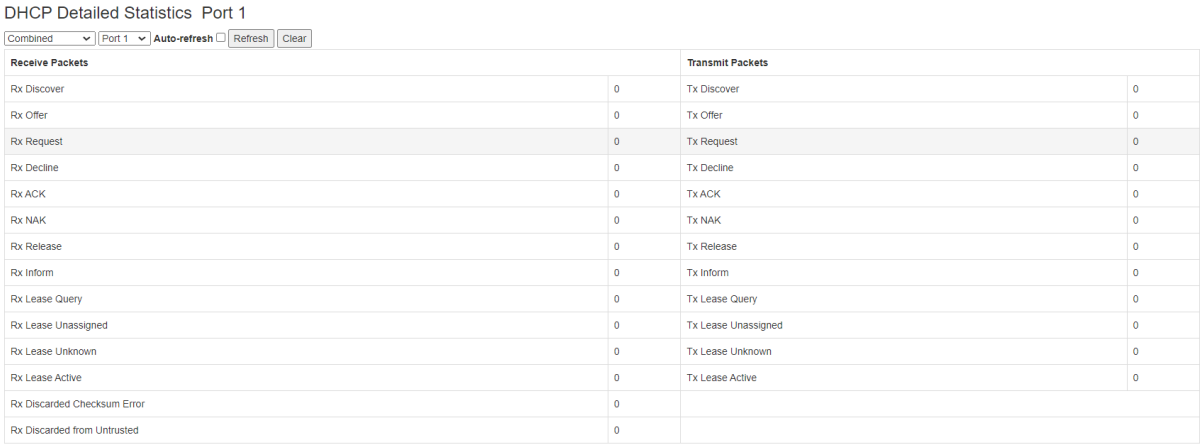


Figure 3-7.4: The DHCPv4 Detailed Statistics

Parameter description:

Server Statistics

- **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

- **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

The DHCP user select box determines which user is affected by clicking the buttons.

The port select box determines which port is affected by clicking the buttons.

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page.

- **Clear :**

  Flushes the selected log entries.

3-8 DHCPv6

3-8.1 Snooping Table

This page displays the content of the current DHCPv6 snooping table.

Web Interface

To display the DHCPv6 snooping table in the web interface:
1. Click Monitor, DHCPv6 and Snooping table
2. To display Dynamic DHCPv6 Snooping Table.

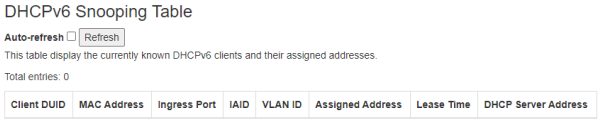


Figure 3-8.1: The DHCPv4 snooping table

Parameter description:

- **UDID:**

  The DHCP Unique Identifier (DUID) for the client. DHCPv6 uses this value to uniquely identify a client host instead of just using the MAC address of one of its interface ports (as DHCPv4 does).

- **MAC Address :**

  The MAC address for the client interface port that sent the DHCPv6 message.

- **IngressPort:**

  The local port on the snooping switch where client messages are received.

- **IAID:**

  Each client may contain multiple interfaces and may request addresses for each of these in the same DHCPv6 message. The Identity Association ID (IAID) value uniquely identifies the interface in the scope of the client.

- **VLAN ID :**

  The VLAN ID which is used by the client messages.

- **Assigned Address :**

  DHCP Server address of the entry. The address assigned to the interface identified by the IAID value.

- **Lease Time :**

  The lease time associated with the assigned address in seconds.

- **DHCP Server Address :**

  The IPv6 address of the DHCP server which assigned the address to the client.

Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Refreshes the displayed table starting from the input fields.

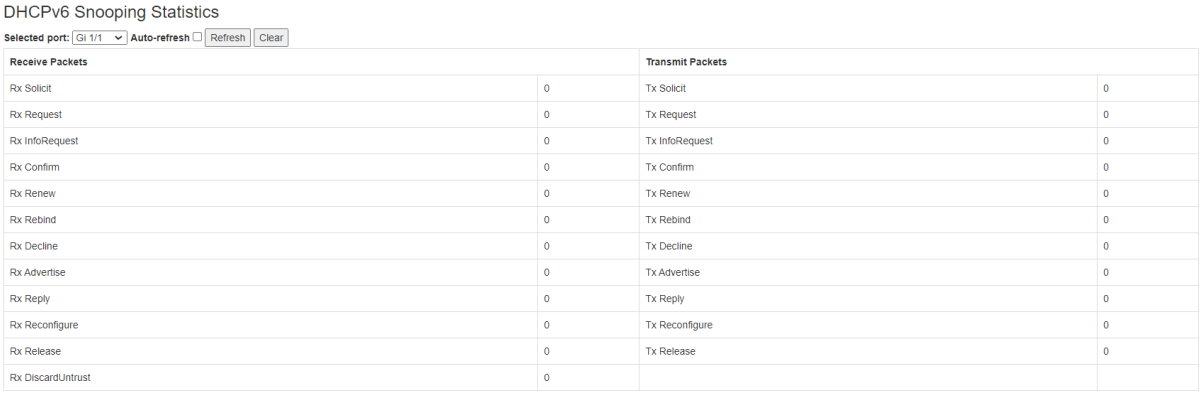
3-8.2 Snooping Statistics

This page provides statistics for DHCPv6 snooping.

Web Interface

To display the DHCPv6 snooping statistics in the web interface:

1. Click Monitor, DHCPv6 and Snooping Statistics
2. To display DHCPv6 Snooping Statistics.


DHCPv6 Snooping Statistics

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

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

Figure 3-8.2: The DHCPv4 Snooping Statistics

General Receive and Transmit Packets

The page contains both RX and TX counters for all known DHCPv6 message types. Please refer to RFC 3315 for details on the various DHCPv6 message types.

Untrusted Discards

The DiscardUntrust counter indicate the number of received DHCP server packets that has been discarded due to the port being untrusted.

Buttons

Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Refreshes the displayed table starting from the input fields.

- **Refresh :**

  Flushes all dynamic entries.

- **The port selection box selects the port for which you want to view and control statistics.**

Shows current, configured relay agents and their statistics.

Web Interface

To display the DHCPv6 relay status and statistics in the web interface:

1. Click Monitor, DHCPv6 and Relay
2. To display DHCPv6 Relay status and statistics

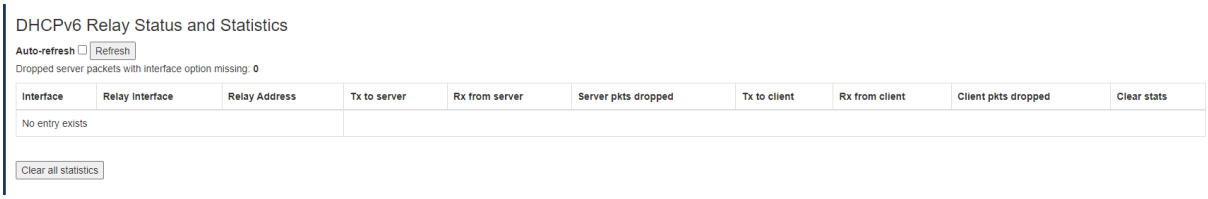


Figure 3-8.3: The DHCPv6 Relay Status and Statistics

Parameter description:

- **Interface :**

  Interface identification. The id of the interface that receives client requests.

- **Relay Interface:**

  Interface identification. The id of the interface used for relaying.

- **Relay Address:**

  An Ipv6 address represented as human readable test as specified in RFC5952. The IPv6 address that requests shall be relayed to. The default value 'ff05::1:3' means 'any DHCPv6 server'.

- **Tx to Server:**

  Integer number. Number of packets relayed to server.

- **Rx from Server:**

  Integer number. Number of packets received from server.

- **Server Pkts dropped:**

  Integer number. Number of packets from server that relay agent drops.

- **Tx to client:**

  Number of packets sent from client.

- **Rx from Client:**

  Number of packets received from client.

- **Client pkts dropped:**

  Number of packets from client that relay agent drops.

- **Clear stats:**

  Clear: Resets all statistics counters of relevant entry to zero.

Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Refreshes the displayed table starting from the input fields.

- **Clear all statistics :**

  Flushes all dynamic entries.

3-9 Security

3-9.1 Access Management Statistics

This section shows you a detailed statistics of the Access Management including HTTP, HTTPS, SSH. TELNET, and SSH.

Web Interface

To display the Assess Management Statistics in the web interface:

1. Click Security, Access Management Statistics.
2. Checked “Auto-refresh”.
3. Click “Refresh” to refresh the port detailed statistics or clear all information when you click “Clear”.

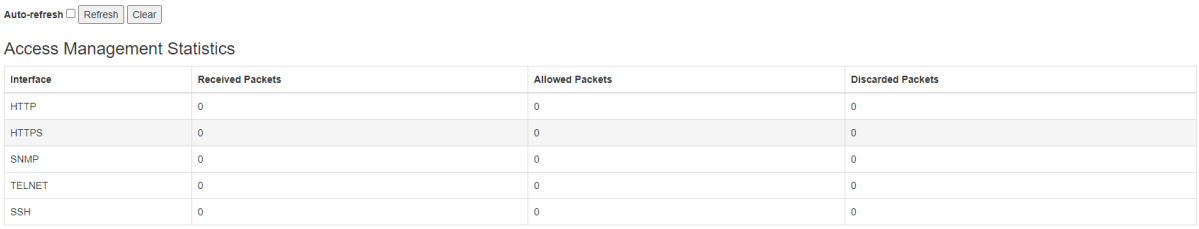


Figure 3-9.1: The Access Management Statistics

Parameter description:

- **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

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page.

- **Clear :**

  Clear all statistics

3-9.2 Network

3-9.2.1 Port Security

3-9.2.1.1 Overview

This section 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.

Web Interface

To display the Port Security Switch Status Configuration in the web interface:

1. Click Security, Network, Port Security and Switch
2. Checked "Auto-refresh".
3. Click "Refresh" to refresh the port detailed statistics.
4. Click the port number to check the port security port status

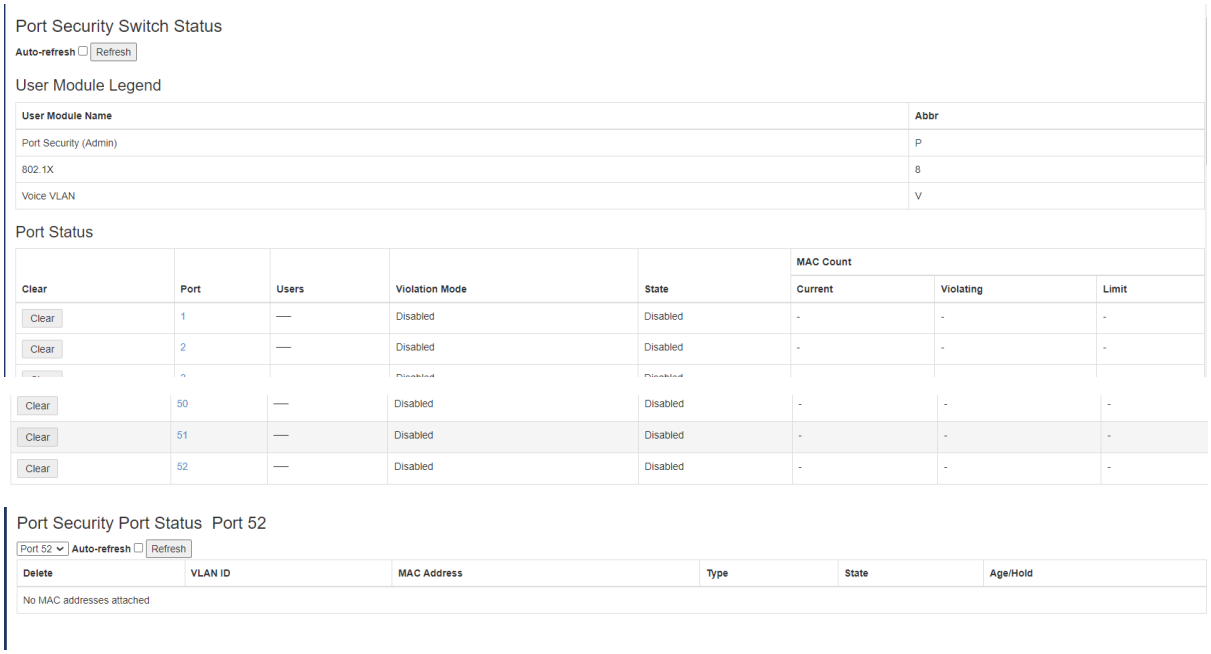


Figure 3-9.2.1.1: The Port Security Switch Status

Parameter description:

User Module Legend

The legend 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. This is used in the Users column in the port status table.

Port Status

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

- **Clear :**

  Click to remove all dynamic MAC addresses on all VLANs on this port. The button is only clickable if number of secured MAC addresses is non-zero.

- **Port :**

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

- **Users :**

  Each of the user modules has a column that shows whether that module has enabled Port Security or not. A '-' 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.

- **Violation Mode :**

  Shows the configured Violation Mode of the port. It can take one of four values:
  Disabled: Port Security is not administratively enabled on this port.
  Protect: Port Security is administratively enabled in Protect mode.
  Restrict: Port Security is administratively enabled in Restrict mode.
  Shutdown: Port Security is administratively enabled in Shutdown mode.

- **State :**

  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,Violating, Limit) :**

  The three columns indicate the number of currently learned MAC addresses (forwarding as well as blocked), the number of violating MAC address (only counting in Restrict mode) 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 Port Security is not administratively enabled on the port, the Violating and Limit columns will show a dash (-).

Port Security Port Status

This page shows the MAC addresses secured by the Port Security module. Port Security may be configured both administratively and indirectly through other software modules - the so-called 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.

Notice that if you have added static or sticky MAC addresses, they will show up on this page only if Port Security is enabled on the interface to which they pertain.

- **Delete :**

  Click to remove this particular MAC addresses from MAC address table. The button is only clickable if the entry type is Dynamic. Use the "Configuration→Security→Port Security→MAC Addresses" page to remove Static and Sticky entries

- **Port :**

  If all ports are shown (can be selected through the drop-down box on the top right), this one shows the port to which the MAC address is bound.

- **VLAN ID & MAC Address:**

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

- **Type :**

  Indicates the type of entry. Takes one of three values:

  Dynamic: The entry is learned through learn frames coming to the Port Security module while the port in question is not in sticky mode.

  Static: The entry is entered by the end-user through management. Entry is not subject to aging.

  Sticky: When the port is in sticky mode, all entries that would otherwise have been learned as dynamic are learned as sticky.

  Sticky entries are part of the running-config and can therefore be saved to startup-config. An important aspect of sticky MAC addresses is that they survive link changes (in contrast to Dynamic, which will have to be learned again). They also survive reboots if running-config is saved to startup-config.

- **State :**

  Indicates whether the corresponding MAC address is violating (administrative user has configured the interface in "Restrict" mode and the MAC address is blocked), blocked, or forwarding.

- **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 address 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 refresh the page automatically. Automatic refresh occurs every 3 seconds.

- **Refresh :**

  Click to refresh the page.

This section 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.

Web Interface

To display the Port Security Switch Status Configuration in the web interface:

1. Click Security, Network, Port Security and then Details.
2. Specify the Port which you want to monitor.
3. Checked “Auto-refresh”.
4. Click “Refresh” to refresh the port detailed statistics.

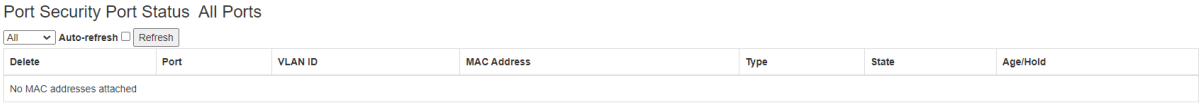


Figure 3-9.2.1.2: The Port Security Port Status

Parameter description:

- **Delete :**

  Click to remove this particular MAC addresses from MAC address table. The button is only clickable if the entry type is Dynamic. Use the "Configuration→Security→Port Security→MAC Addresses" page to remove Static and Sticky entries.

- **Port :**

  If all ports are shown (can be selected through the drop-down box on the top right), this one shows the port to which the MAC address is bound.

- **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.

- **State :**

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

- **Type :**

  Indicates the type of entry. Takes one of three values:

  Dynamic: The entry is learned through learn frames coming to the Port Security module while the port in question is not in sticky mode.

  Static: The entry is entered by the end-user through management. Entry is not subject to aging.

  Sticky: When the port is in sticky mode, all entries that would otherwise have been learned

as dynamic are learned as sticky.
Sticky entries are part of the running-config and can therefore be saved to startup-config. An important aspect of sticky MAC addresses is that they survive link changes (in contrast to Dynamic, which will have to be learned again). They also survive reboots if running-config is saved to startup-config.

- **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

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page.

3-9.2.2 NAS

3-9.2.2.1 Switch

The section describes to show the each port NAS status information of the switch. The status includes Admin State Port State, Last Source, Last ID, QoS Class, and Port VLAN ID.

Web Interface

To display the NAS Switch Status Configuration in the web interface:

1. Click Security, Network, NAS and then Port.
2. Checked “Auto-refresh”.
3. Click “Refresh” to refresh the port detailed statistics.
4. Click the Port number to view the port status details

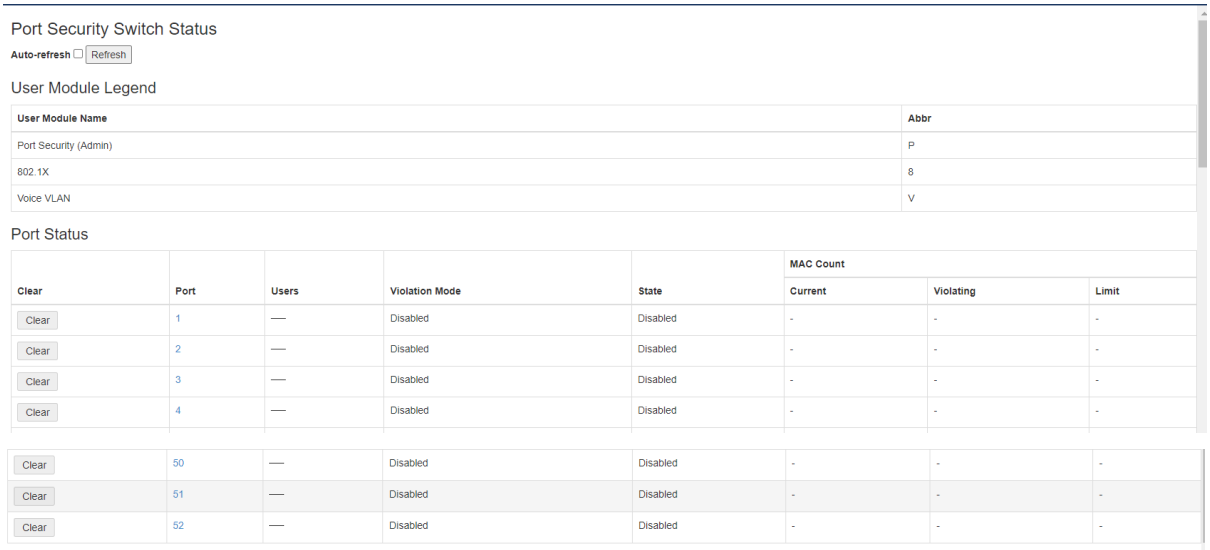


Figure 3-11.2.2.1: The Network Access Server Switch Status

Parameter description:

- **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 Port State for a description of the individual states.

- **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.

- **QoS Class :**

  QoS Class assigned to the port by the RADIUS server if enabled.

- **Port VLAN ID :**

  The VLAN ID that NAS has put the port in. The field is blank, if the Port VLAN ID is not overridden by NAS.

  If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID. Read more about RADIUS-assigned VLANs here.

  If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID. Read more about Guest VLANs here.

Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page.

The section describes to provide 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.

Web Interface

To display the NAS Port Status Configuration in the web interface:

1. Click Security, Network, NAS and then Port.
2. Checked “Auto-refresh”.
3. Click “Refresh” to refresh the port detailed statistics.

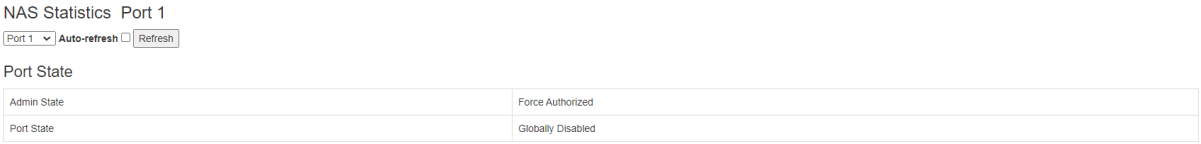


Figure 3-9.2.2.2: The NAS Statistics

Parameter description:

Port State

- **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 Port State for a description of the individual states.

- **QoS Class :**

  The QoS class assigned by the RADIUS server. The field is blank if no QoS class is assigned.

- **Port VLAN ID :**

  The VLAN ID that NAS has put the port in. The field is blank, if the Port VLAN ID is not overridden by NAS.

  If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID. Read more about RADIUS-assigned VLANs here.

  If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID. Read more about Guest VLANs here.

Port Counters

- **EAPOL Counters :**

  These supplicant frame counters are available for the following administrative states:

  • Force Authorized

  • Force Unauthorized

  • Port-based 802.1X

  • Single 802.1X

- Multi 802.1X

- **Backend Server Counters :**

  These backend (RADIUS) frame counters are available for the following administrative states:

  - Port-based 802.1X
  - Single 802.1X
  - Multi 802.1X
  - MAC-based Auth.

- **Last Supplicant/Client Info :**

  Information about the last supplicant/client that attempted to authenticate. This information is available for the following administrative states:

  - Port-based 802.1X
  - Single 802.1X
  - Multi 802.1X
  - MAC-based Auth.

Selected Counters

- **Selected Counters :**

  The Selected Counters table is visible when the port is in one of the following administrative states:

  - Multi 802.1X
  - MAC-based Auth.

  The table is identical to and is placed next to the Port Counters table, and will be empty if no MAC address is currently selected. To populate the table, select one of the attached MAC Addresses from the table below.

Attached MAC Addresses

- **Identity :**

  Shows the identity of the supplicant, as received in the Response Identity EAPOL frame. Clicking the link causes the supplicant's EAPOL and Backend Server counters to be shown in the Selected Counters table. If no supplicants are attached, it shows No supplicants attached.

  This column is not available for MAC-based Auth.

- **MAC Address :**

  For Multi 802.1X, this column holds the MAC address of the attached supplicant.For MAC-based Auth., this column holds the MAC address of the attached client.

  Clicking the link causes the client's Backend Server counters to be shown in the Selected Counters table. If no clients are attached, it shows No clients attached.

- **VLAN ID :**

  This column holds the VLAN ID that the corresponding client is currently secured through the Port Security module.

- **State :**

  The client can either be authenticated or unauthenticated. In the authenticated state, it is allowed to forward frames on the port, and in the unauthenticated state, it is blocked. As long as the backend server hasn't successfully authenticated the client, it is unauthenticated.

If an authentication fails for one or the other reason, the client will remain in the unauthenticated state for Hold Time seconds.

- **Last Authentication :**

  Shows the date and time of the last authentication of the client (successful as well as unsuccessful).

Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page.

- **Clear :**

  This button is available in the following modes:
  - Force Authorized
  - Force Unauthorized
  - Port-based 802.1X
  - Single 802.1X

  Click to clear the counters for the selected port.

- **Clear All:**

  This button is available in the following modes:
  - Multi 802.1X
  - MAC-based Auth.X

  Click to clear both the port counters and all of the attached client's counters. The "Last Client" will not be cleared, however.

- **Clear This :**

  This button is available in the following modes:
  - Multi 802.1X
  - MAC-based Auth.X

  Click to clear only the currently selected client's counters.

3-9.2.3 ACL Status

The section describes how to 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 512 on each switch.

Web Interface

To display the ACL status in the web interface:

1. Click Monitor, Network and ACL status
2. If you want to auto-refresh the information then you need to evoke the “Auto-refresh”.
3. Click “Refresh” to refresh the ACL Status

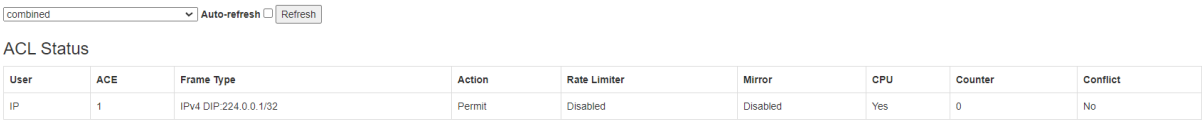


Figure 3-9.2.3: The ACL Status

Parameter description:

- **User :**

  Indicates the ACL user.

- **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 that an 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: 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.

- **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.

- **Conflict :**

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

Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page.

3-9.2.4 ARP Inspection

The section describes to configure the Dynamic ARP Inspection Table parameters of the switch. The Dynamic ARP Inspection Table contains up to 256 entries, and is sorted first by port, then by VLAN ID, then by MAC address, and then by IP address.

Web Interface

To display the Dynamic ARP Inspection Table Configuration in the web interface:

1. Click Security, Network, ARP Inspection.
2. Checked "Auto-refresh".
3. Click "Refresh" to refresh the port detailed statistics.
4. Specify the Start from port, VLAN ID, MAC Address, IP Address, and entries per page.

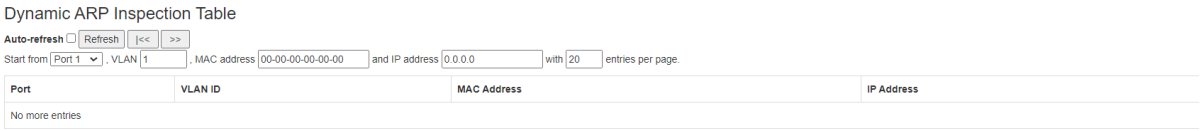


Figure 3-9.2.4: The Dynamic ARP Inspection Table

Parameter description:

ARP Inspection Table Columns

- **Port :**

  Switch Port Number for which the entries are displayed.

- **VLAN ID :**

  VLAN-ID in which the ARP traffic is permitted.

- **MAC Address :**

  User MAC address of the entry.

- **IP Address :**

  User IP address of the entry.

Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page.

- **|<< :**

  Updates the table starting from the first entry in the Dynamic ARP Inspection Table.

- **>> :**

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

3-9.2.5 IP Source Guard

Entries in the Dynamic IP Source Guard Table are shown on this page. The Dynamic IP Source Guard Table is sorted first by port, then by VLAN ID, then by IP address, and then by MAC address.
Each page shows up to 99 entries from the Dynamic IP Source Guard 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 Dynamic IP Source Guard Table.

Web Interface

To display the Dynamic IP Source Guard Table Configuration in the web interface:

1. Click Security, Network and IP Source Guard.
2. Checked “Auto-refresh”.
3. Click “Refresh” to refresh the port detailed statistics.
4. Specify the Start from port, VLAN ID, IP Address, and entries per page.

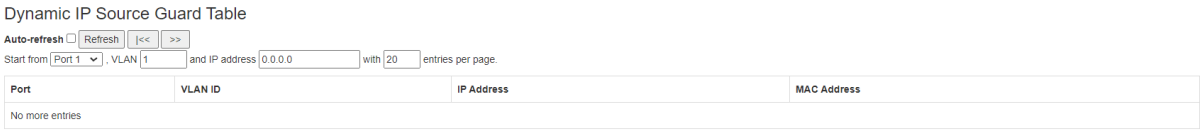


Figure 3-11.2.5: The Dynamic IP Source Table

Parameter description:

IP Source Guard Table Columns

- **Port :**

  Switch Port Number for which the entries are displayed.

- **VLAN ID :**

  VLAN-ID in which the IP traffic is permitted.

- **IP Address :**

  User IP address of the entry.

- **MAC Address :**

  Source MAC address.

Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page.

- **|<< :**

  Updates the table starting from the first entry in the Dynamic ARP Inspection Table.

- **>> :**

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

3-9.2.6 IPv6 Source Guard

Entries in the Dynamic IPv6 Source Guard Table are shown on this page.

Web Interface

To display the Dynamic IPv6 Source Guard Table Configuration in the web interface:

1. Click Security, Network and IPv6 Source Guard.
2. Checked “Auto-refresh”.
3. Click “Refresh” to refresh the port detailed statistics.
4. Specify the Start from port, VLAN ID, IP Address, and entries per page.

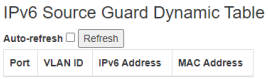


Figure 3-9.2.6: The Dynamic IPv6 Source Table

Parameter description:

IP Source Guard Table Columns

- **Port :**

  Switch Port Number for which the entries are bound.

- **VLAN ID :**

  VLAN-ID in which the IP traffic is permitted. If no VLAN-ID is associated with the entry, this field shows 0.

- **IP Address :**

  Source IPv6 address of the entry.

- **MAC Address :**

  Source MAC address.

Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page.

3-9.3 AAA

3-9.3.1 RADIUS Overview

This section shows you an overview of the RADIUS Authentication and Accounting servers' status to ensure the function is workable.

Web Interface

To display the RADIUS Overview Configuration in the web interface:

1. Click Security, AAA and RADIUS Overview.
2. Checked "Auto-refresh".
3. Click "Refresh" to refresh the port detailed statistics.
4. Click the number to check the details

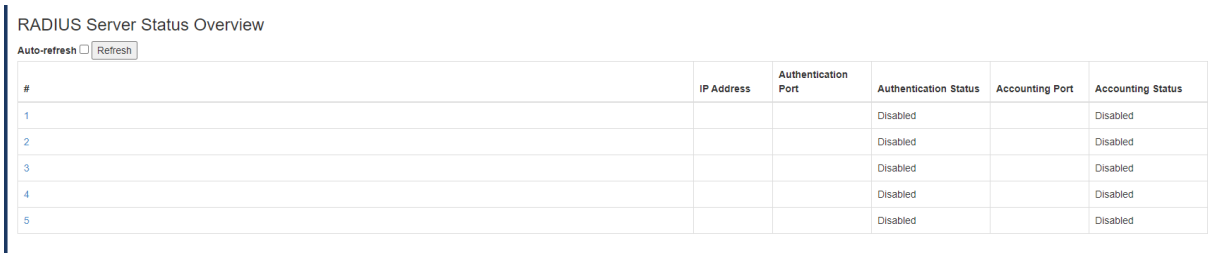


Figure 3-9.3.1: The RADIUS Server Status Overview

Parameter description:

RADIUS Authentication Servers

- **# :**

  The RADIUS server number. Click to navigate to detailed statistics for this server.

- **IP Address :**

  The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of this server.

- **Authentication Status:**

  The current state 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.

- **Authentication Port :**

  UDP port number for authentication.

- **Accounting Port:**

UDP port number for accounting.

- **Accounting Status :**

  The current state 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 accounting attempts.

  Dead (X seconds left): Accounting 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.

3-9.3.2 RADIUS Details

This section shows you a detailed statistics for a particular RADIUS server.

Web Interface

To display the RADIUS Details Configuration in the web interface:

1. Specify Port which want to check.
2. Click Security, AAA, RADIUS Overview.
3. Checked “Auto-refresh”.
4. Click “Refresh” to refresh the port detailed statistics or clear all information when you click “Clear” & ” Fresh”.

RADIUS Authentication Statistics for Server #1

Server #1 Auto-refresh Refresh Clear

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

RADIUS Accounting Statistics for Server #1

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

Figure 3-9.3.2: The RADIUS Authentication Statistics Server

Parameter description:

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.

- **Packet Counters :**

  RADIUS authentication server packet counter. There are seven receive and four transmit counters

- **Other Info :**

  This section contains information about the state of the server and the latest round-trip time.

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.

- **Packet Counters :**

  RADIUS accounting server packet counter. There are five receive and four transmit counters.

- **Other Info :**

  This section contains information about the state of the server and the latest round-trip time.

Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page.

- **Clear :**

  Clears the counters for the selected server. The "Pending Requests" counter will not be cleared by this operation.

3-9.4 Switch

3-9.4.1 RMON

3-9.4.1.1 Statistics

This section 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.

Web Interface

To display the RMON Statistics in the web interface:

1. Click Security, Switch, RMON and Statistics.
2. Specify Port which want to check.
3. Checked “Auto-refresh”.
4. Click “Refresh” to refresh the port detailed statistics.

Figure 3-9.4.1.1: The RMON Statistics Status Overview

Parameter description:

- **ID :**

  Indicates the index of Statistics entry.

- **Data Source(if Index) :**

  The port ID which wants to be monitored.

- **Drop :**

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

- **Octets :**

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

- **Pkts :**

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

- **Broad-cast :**

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

- **Multi-cast :**

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

- **CRC Errors :**

  The total number of packets received that had a length (excluding framing bits, but including

FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).

- **Under-size :**

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

- **Over-size :**

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

- **Frag. :**

  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.

- **Coll. :**

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

- **64 :**

  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 :**

  Refreshes the displayed table starting from the input fields.

- **|<<:**

  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.

This section 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.

Web Interface

To display the RMON history Configuration in the web interface:

1. Click Security, Switch, RMON and History.
2. Checked “Auto-refresh”.
3. Click “Refresh” to refresh the port detailed statistics or clear all information when you click “ Clear”.

Figure 3-9.4.1.2: RMON History Overview

Parameter description:

- **History Index :**

  Indicates the index of History control entry.

- **Sample Index :**

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

- **Sample Start :**

  The value of sysUpTime at the start of the interval over which this sample was measured.

- **Drop :**

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

- **Octets :**

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

- **Pkts :**

  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.

- **CRCErrors :**

  The total number of packets received that had a length (excluding framing bits, but including

FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (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.

- **Frag. :**

  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.

- **Coll. :**

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

- **Utilization :**

  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 :**

  Refreshes the displayed table starting from the input fields.

- **|<< :**

  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.

This page provides an overview of RMON Alarm 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 Alarm table. The first displayed will be the one with the lowest ID found in the Alarm table

Web Interface

To display the RMON Alarm Overview in the web interface:

1. Specify Port which wants to check.
2. Click Security, Switch, RMON and Alarm.
3. Checked “Auto-refresh”.
4. Click “Refresh” to refresh the port detailed statistics.

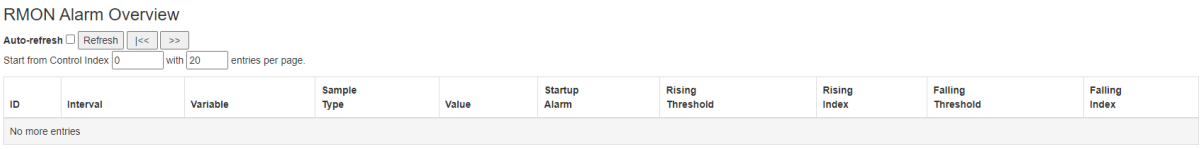


Figure 3-9.4.1.3: RMON Alarm Overview

Parameter description:

- **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 :**

  Refreshes the displayed table starting from the input fields.

- **|<< :**

  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.

This page provides an overview of RMON Event table 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.

Web Interface

To display the RMON Event Overview in the web interface:

1. Click Security, Switch, RMON and Event.
2. Checked “Auto-refresh”.
3. Click “ Refresh“ to refresh the port detailed statistics
4. Specify Port which wants to check.

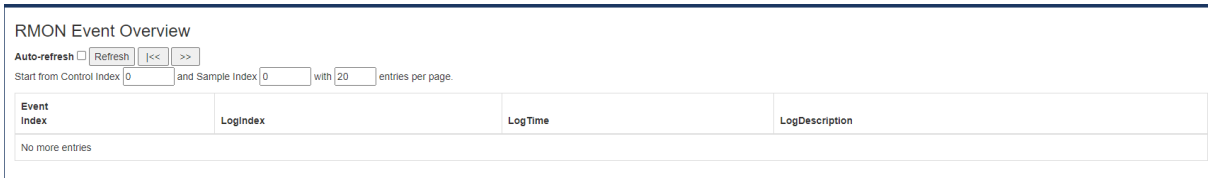


Figure 3-9.4.1.4: RMON Event Overview

Parameter description:

- **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 :**

  Refreshes the displayed table starting from the input fields.

- **|<<:**

  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.

3-10 Aggregation

3-10.1 Status

This page is used to see the staus of ports in Aggregation group.

Web Interface

To display aggregation status in the web interface:

1. Click Security, Aggregation and Status
2. Checked “Auto-refresh”.
3. Click “ Refresh” to refresh the port detailed statistics

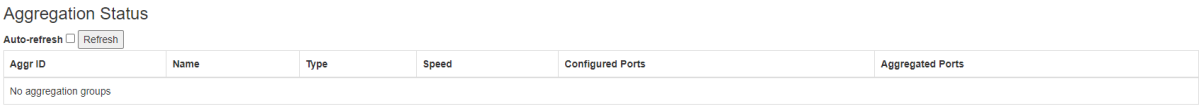


Figure 3-10.1: The Aggregation Status

Parameter description:

- **Aggr ID :**

  The Aggregation ID associated with this aggregation instance.

- **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

- **Auto-refresh :**

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

- **Refresh :**

  Refreshes the displayed table starting from the input fields.

3-10.2 LACP

3-10.2.1 System Status

This section describes that when you complete to set LACP function on the switch then it provides a status overview for all LACP instances

Web Interface

To display the LACP System status in the web interface:

1. Click Monitor, LACP and System Status
2. Checked “Auto-refresh”.
3. Click “Refresh” to refresh the port detailed statistics.

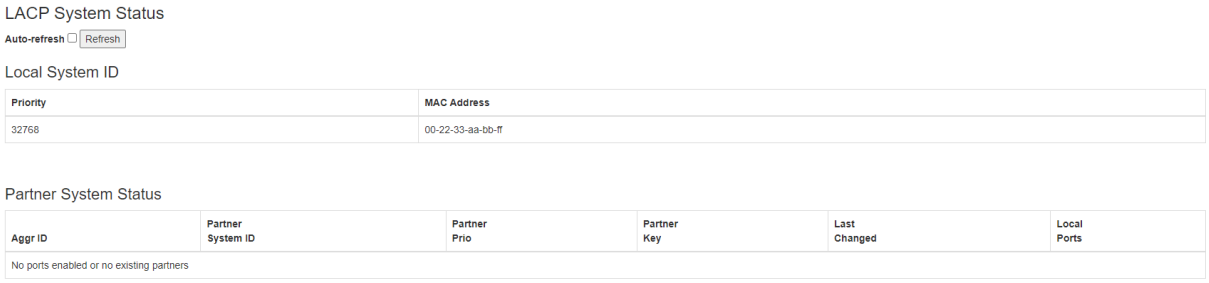


Figure 3-10.2.1 The LACP System Status

Parameter description:

- **Aggr ID :**

  The Aggregation ID associated with this aggregation instance. For LLAG the id is shown as 'isid: aggr-id' and for GLAGs as 'aggr-id'

- **Partner System ID :**

  The system ID (MAC address) of the aggregation partner.

- **Partner Prio :**

  The priority that the partner has assigned to this aggregation ID.

- **Partner Key :**

  The Key that the partner has assigned to this aggregation ID.

- **Last changed :**

  The time since this aggregation changed.

- **Local Ports :**

  Shows which ports are a part of this aggregation for this switch. The format is: "Switch ID:Port".

Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Refreshes the displayed table starting from the input fields.

3-10.2.2 Internal Status

This page provides a status overview for the LACP internal (i.e. local system) status for all ports.

Only ports that are part of an LACP group are shown.

For details on the shown parameters please refer to IEEE 801.AX-2014.

Web Interface

To display the LACP internal status in the web interface:

1. Click Monitor, Aggregation, LACP and Internal Status
2. If you want to auto-refresh the information then you need to evoke the “Auto-refresh”.
3. Click “Refresh” to refresh the LACP Internal Status.

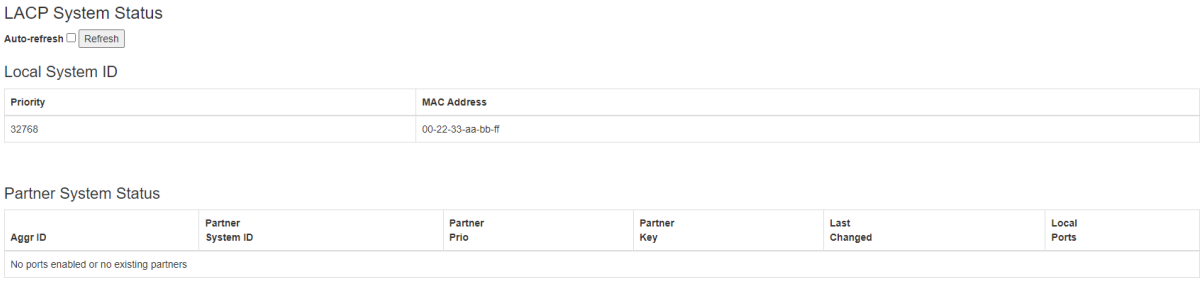


Figure 3-10.2.2: The LACP Internal Status

Parameter description:

- **Port :**

  The switch port number.

- **State:**

  The current port state:

  Down: The port is not active.

  Active: The port is in active state.

  Standby: The port is in standby state.

- **Key :**

  The key assigned to this port. Only ports with the same key can aggregate together.

- **Priority :**

  The priority assigned to this aggregation group.

- **Activity :**

  The LACP mode of the group (Active or Passive).

- **Timeout :**

  The timeout mode configured for the port (Fast or Slow).

- **Aggregation:**

  Show whether the system considers this link to be "aggregateable"; i.e., a potential candidate for aggregation.

- **Synchoronization :**

Show whether the system considers this link to be "IN_SYNC"; i.e., it has been allocated to the correct LAG, the group has been associated with a compatible Aggregator, and the identity of the LAG is consistent with the System ID and operational Key information transmitted.

- **Collecting:**

  Show if collection of incoming frames on this link is enabled.

- **Distributing :**

  Show if distribution of outgoing frames on this link is enabled.

- **Defaulted:**

  Show if the Actor's Receive machine is using Defaulted operational Partner information.

- **Expired:**

  Show if that the Actor's Receive machine is in the EXPIRED state.

Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Refreshes the displayed table starting from the input fields.

3-10.2.3 Neighbor Status

This page provides a status overview for the LACP neighbor status for all ports.

Only ports that are part of an LACP group are shown.

For details on the shown parameters please refer to IEEE 801.AX-2014.

Web Interface

To display the LACP neighbor status in the web interface:

1. Click Monitor, Aggregation, LACP and Neighbor Status

2. If you want to auto-refresh the information then you need to evoke the “Auto-refresh”.

3. Click “Refresh” to refresh the LACP Internal Status.

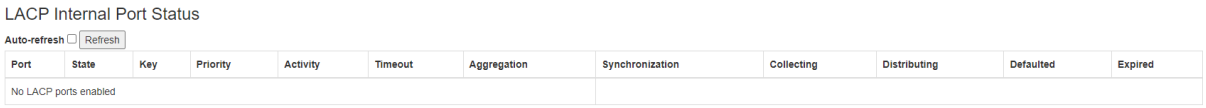


Figure 3-10.2.3: The LACP Neighbor Status

Parameter description:

- **Port :**

  The switch port number.

- **State:**

  The current port state:

  Down: The port is not active.

  Active: The port is in active state.

  Standby: The port is in standby state.

- **Aggr ID:**

  The aggregation group ID which the port is assigned to.

- **Partner Key :**

  The key assigned to this port by the partner.

- **Partner Port:**

  The partner port number associated with this link.

- **Partner Port Prio:**

  The priority assigned to this partner port .

- **Activity :**

  The LACP mode of the group (Active or Passive).

- **Timeout :**

  The timeout mode configured for the port (Fast or Slow).

- **Aggregation:**

  Show whether the system considers this link to be "aggregateable"; i.e., a potential candidate for aggregation.

- **Synchoronization :**

  Show whether the system considers this link to be "IN_SYNC"; i.e., it has been allocated to the correct LAG, the group has been associated with a compatible Aggregator, and the identity of the LAG is consistent with the System ID and operational Key information transmitted.

- **Collecting:**

  Show if collection of incoming frames on this link is enabled.

- **Distributing :**

  Show if distribution of outgoing frames on this link is enabled.

- **Defaulted:**

  Show if the Actor's Receive machine is using Defaulted operational Partner information.

- **Expired:**

  Show if that the Actor's Receive machine is in the EXPIRED state.

Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Refreshes the displayed table starting from the input fields.

3-10.2.4 Port Statistics

This section describes that when you complete to set LACP function on the switch then it provides a Port Statistics overview for all LACP instances

Web Interface

To display the LACP Port status in the web interface:

1. Click Monitor, LACP and Port Statistics
2. If you want to auto-refresh the information then you need to evoke the “Auto refresh”.
3. 3. Click “Refresh” to refresh the LACP Statistics.

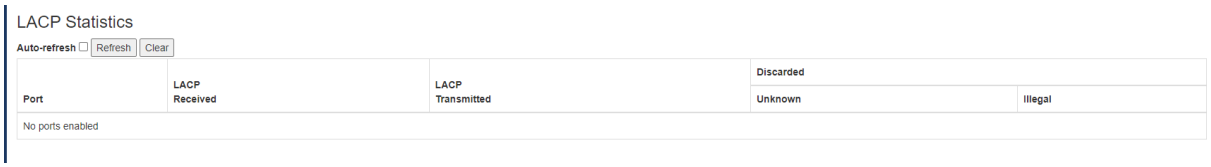


Figure 3-10.2.4: The LACP Statistics

Parameter description:

- **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 :**

  Shows how many unknown or illegal LACP frames have been discarded at each port.

Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page.

- **Clear :**

  Clears the counters for all ports.

3-11 Loop Protection

This section displays the loop protection port status the ports of the currently selected switch.

Web Interface

To display the Loop Protection status in the web interface:

1. Click Monitor and Loop Protection
2. If you want to auto-refresh the information then you need to evoke the “Auto refresh”.
3. Click “Refresh” to refresh the LACP Statistics.

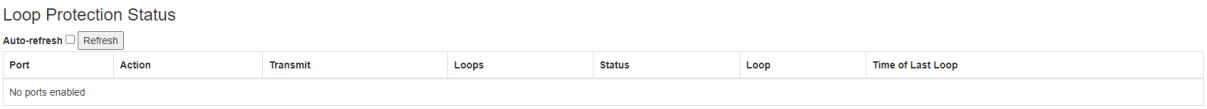


Figure 3-11: Loop Protection Status

Parameter description:

- **Port :**

  The switch port number of the logical port.

- **Action :**

  The currently configured port action.

- **Transmit :**

  The currently configured port transmit mode.

- **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

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page.

3-12 Spanning Tree

3-12.1 Bridge Status

After you complete the MSTI Port configuration then you could to ask the switch display the Bridge Status. The Section 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:

Web Interface

To display the STP Bridges status in the web interface:

1. Click Monitor, Spanning Tree and Bridge Status.
2. If you want to auto-refresh the information then you need to evoke the “Auto-refresh”.
3. Click “Refresh” to refresh the STP Bridges.
4. Click “CIST “to next page “STP Detailed Bridge Status”.

STP Bridges

Auto-refresh ☐ Refresh

MSTI	Bridge ID	Root ID	Root Port	Root Cost	Topology Flag	Topology Change Last
CIST	32768.00-22-33-AA-BB-FF	32768.00-22-33-AA-BB-FF	-	0	Steady	-

STP Detailed Bridge Status

Auto-refresh ☐ Refresh

STP Bridge Status	
Bridge Instance	CIST
Bridge ID	32768.00-22-33-AA-BB-FF
Root ID	32768.00-22-33-AA-BB-FF
Root Cost	0
Root Port	-
Regional Root	32768.00-22-33-AA-BB-FF
Internal Root Cost	0
Topology Flag	Steady
Topology Change Count	0
Topology Change Last	-

CIST Ports & Aggregations State

Port	Port ID	Role	State	Path Cost	Edge	Point-to-Point	Uptime
6	128.006	DesignatedPort	Forwarding	200000	Yes	Yes	0d 03:26:41

Figure 3-12.1: The STP Bridges status

Parameter description:

STP Bridge Status:

- **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 it 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.

CIST Ports & Aggregations State:

- **Port :**

  The switch port number of the logical STP port.

- **Port ID :**

  This is the priority part and the logical port index of the bridge port.

- **Role :**

  The port role can be one of the following values: Alternate Port Backup Port Root Port Designated Port.

- **State :**

  The switch port currently assigned the root port role. 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 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

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page.

3-12.2 Port Status

After you complete the STP configuration then you could to ask the switch display the STP Port Status. The Section provides you to ask switch to display the STP CIST port status for physical ports of the currently selected switch.

Web Interface

To display the STP Port status in the web interface:

1. Click Monitor, Spanning Tree and Port Status.
2. If you want to auto-refresh the information then you need to evoke the “Auto-refresh”.
3. Click “Refresh” to refresh the STP Bridges.

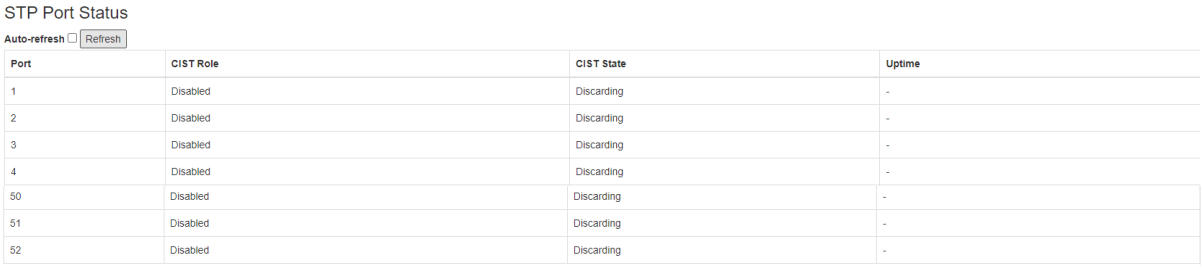


Figure 3-12.2: The STP Port status

Parameter description:

- **Port :**

  The switch port number of the logical STP port.

- **CIST Role :**

  The current STP port role of the CIST port. The port role can be one of the following values: AlternatePort, Backup Port, RootPort, DesignatedPort Disabled.

- **CIST State :**

  The current STP port state of the CIST port. The port state can be one of the following values: Blocking Learning Forwarding.

- **Uptime :**

  The time since the bridge port was last initialized.

Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page.

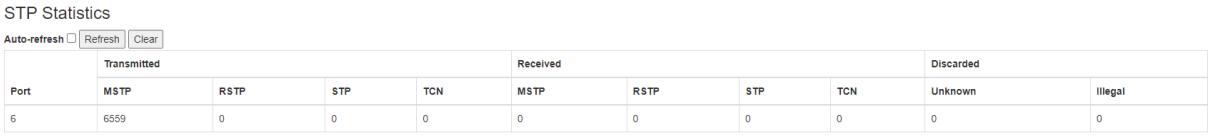
3-12.3 Port Statistics

After you complete the STP configuration then you could to let the switch display the STP Statistics. The Section provides you to ask switch to display the STP Statistics detail counters of bridge ports in the currently selected switch.

Web Interface

To display the STP Port status in the web interface:

1. Click Monitor, Spanning Tree and Port Statistics
2. If you want to auto-refresh the information then you need to evoke the “Auto-refresh”.
3. Click “Refresh” to refresh the STP Bridges.


STP Statistics

Auto-refresh ☐ Refresh Clear

	Transmitted				Received				Discarded	
Port	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
6	6559	0	0	0	0	0	0	0	0	0

Figure 3-12.3: The STP Statistics

Parameter description:

- **Port :**

  The switch port number of the logical STP port.

- **MSTP :**

  The number of MSTP Configuration BPDU's received/transmitted on the port.

- **RSTP :**

  The number of RSTP Configuration 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

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page.

- **Clear :**

  Click to reset the counters.

3-13 MVR

3-13.1 Statistics

The section describes the switch will display the MVR detail Statistics after you had configured MVR on the switch. It provides the detail MVR Statistics Information

Web Interface

To display the MVR Statistics Information in the web interface:

1. Click Monitor, MVR and Statistics
2. If you want to auto-refresh the information then you need to evoke the “Auto-refresh”.
3. To click the “Refresh” to refresh an entry of the MVR Statistics Information.

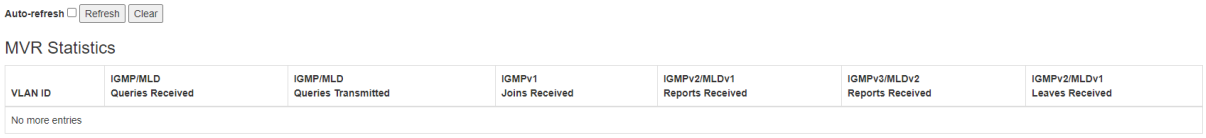


Figure 3-13.1: The MVR Statistics Information

Parameter description:

- **VLAN ID :**

  The Multicast VLAN ID.

- **IGMP/MLD Queries Received :**

  The number of Received Queries for IGMP and MLD, respectively.

- **IGMP/MLD Queries Transmitted :**

  The number of Transmitted Queries for IGMP and MLD, respectively.

- **IGMPv1 Joins Received :**

  The number of Received IGMPv1 Join's.

- **IGMPv2/MLDv1 Report's Received :**

  The number of Received IGMPv2 Join's and MLDv1 Report's, respectively.

- **IGMPv3/MLDv2 Report's Received :**

  The number of Received IGMPv1 Join's and MLDv2 Report's, respectively.

- **IGMPv2/MLDv1 Leave's Received :**

  The number of Received IGMPv2 Leave's and MLDv1 Done's, respectively.

Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page.

- **Clear :**

  Click to reset the counters

3-15.2 MVR Channels Groups

The section describes user could display the MVR Groups detail information on the switch. Entries in the MVR Group Table are shown on this page. The MVR Group Table is sorted first by VLAN ID, and then by group

Web Interface

To display the MVR Groups Information in the web interface:

1. Click Monitor, MVR and Groups Information
2. If you want to auto-refresh the information then you need to evoke the “Auto-refresh”.
3. To click the “Refresh” to refresh an entry of the MVR Groups Information.
4. Click “<< or >> “to move to previous or next entry.

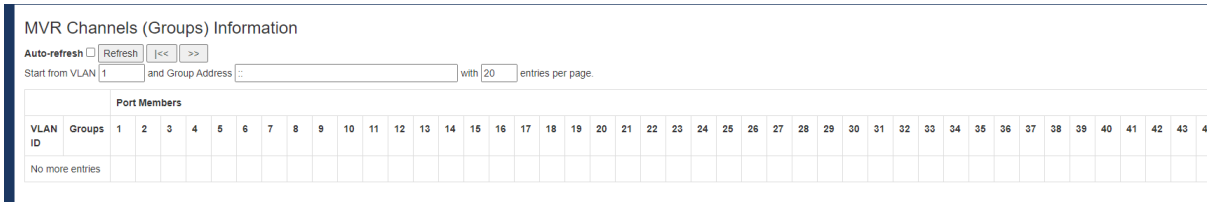


Figure 3-13.2: The MVR Groups Information

Parameter description:

MVR Channels (Groups) Information Table Columns

- **VLAN ID :**

  VLAN ID of the group.

- **Groups :**

  Group ID of the group displayed.

- **Port Members :**

  Ports under this group.

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 :**

  Flushes the selected log entries.

- **|<<:**

  Updates the table starting from the first entry in the MVR Channels (Groups) Information Table.

- **>>:**

  Updates the system log entries, ending at the last entry currently displayed.

3-12.3 MVR SFM Information

The MVR 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.

Web Interface

To display the MVR SFM Information in the web interface:

1. Click Monitor, MVR and MVR SFM Information
2. If you want to auto-refresh the information then you need to evoke the “Auto-refresh”.
3. To click the “Refresh” to refresh an entry of the MVR Groups Information.
4. Click “< < or > > ”to move to previous or next entry.

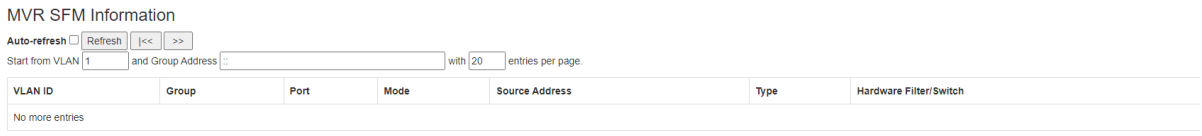


Figure 3-15.3: The MVR SFM Information

Parameter description:

MVR SFM Information Table Columns

- **VLAN ID :**

  VLAN ID of the group.

- **Group :**

  Group address of the group displayed.

- **Port :**

  Switch port number.

- **Mode :**

  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, system limits the total number of IP source addresses for filtering to be 128. 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/IPv6 address could be handled by chip or not.

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 MVR Channels (Groups) Information Table.

- **>>:**

  Updates the system log entries, ending at the last entry currently displayed.

3-14 IPMC

3-14.1 IGMP Snooping

3-14.1.1 Status

After you complete the IGMP Snooping configuration, then you could to let the switch display the IGMP Snooping Status. The Section provides you to let switch to display the IGMP Snooping detail status.

Web Interface

To display the IGMP Snooping status in the web interface:

1. Click Monitor, IGMP Snooping and Status
2. If you want to auto-refresh the information then you need to evoke the “Auto-refresh”.
3. Click “Refresh” to refresh the IGMP Snooping Status.
4. Click “Clear “to clear the IGMP Snooping Status.

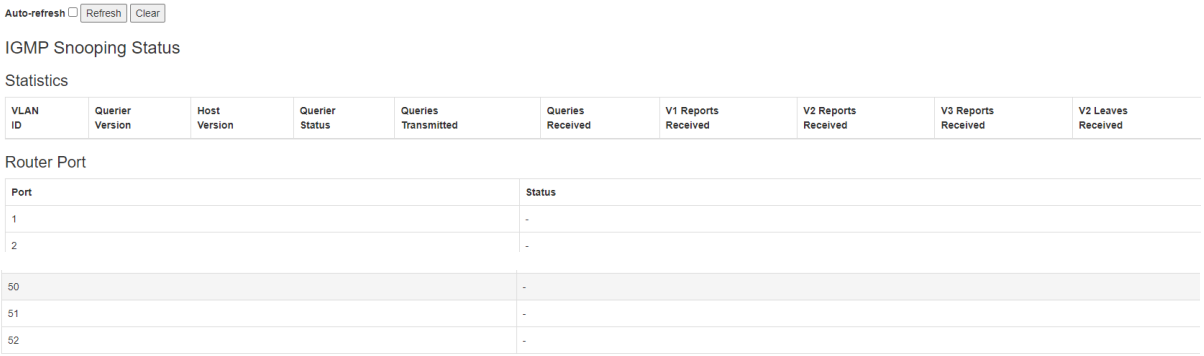


Figure 3-14.1.1: The IGMP Snooping Status.

Parameter description:

- **VLAN ID :**

  The VLAN ID of the entry.

- **Querier Version :**

  Working Querier Version currently.

- **Host Version :**

  Working Host Version currently.

- **Querier Status :**

  Shows the Querier status is "ACTIVE" or "IDLE".

  "DISABLE" denotes the specific interface is administratively disabled.

- **Queries Transmitted :**

  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 IGMP 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 :**

  Switch port number.

- **Status :**

  Indicate whether specific port is a router port or not.

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 all Statistics counters.

After you complete to set the IGMP Snooping function then you could let the switch to display the IGMP Snooping Group Information. 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. The 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.

Web Interface

To display the IGMP Snooping Group Information in the web interface:

1. Click Monitor, IGMP Snooping, Group Information
2. If you want to auto-refresh the information then you need to evoke the “Auto-refresh”.
3. Click “Refresh” to refresh an entry of the IGMP Snooping Groups Information.
4. Click “<< or >> “to move to previous or next entry.

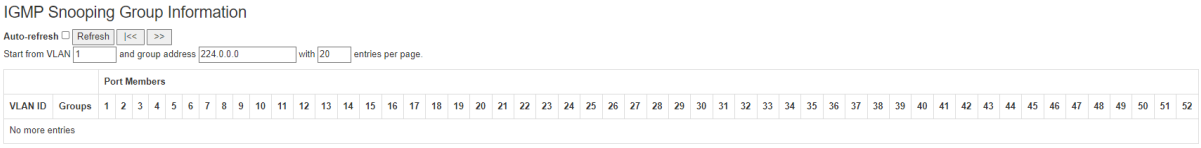


Figure 3-14.1.2: The IGMP Snooping Groups Information.

Parameter description:

IGMP Group Table Columns

- **VLAN ID :**

  VLAN ID of the group.

- **Groups :**

  Group address of the group displayed.

- **Port Members :**

  Ports under this group.

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 with the first entry in the IGMP Group Table.

- **>>:**

  Updates the system log entries, ending at the last entry currently displayed.

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.

Web Interface

To display the IPv4 SSM Information in the web interface:

1. Click Monitor, IGMP Snooping, IPv4 SSM Information
2. If you want to auto-refresh the information then you need to evoke the “Auto-refresh”.
3. Click “Refresh” to refresh an entry of the IPv4 SFM Information.
4. Click “<< or >> ”to move to previous or next entry.

Figure 3-14.1.3: The IPv4 SFM Information.

Parameter description:

IGMP SFM Information Table Columns

- **VLAN ID :**

  VLAN ID of the group.

- **Group :**

  Group address of the group displayed.

- **Port :**

  Switch port number.

- **Mode :**

  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, system limits the total number of IP source addresses for filtering to be 128. 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.

Ports under this group.

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 with the first entry in the IGMP Group Table.

- **>>:**

  Updates the system log entries, ending at the last entry currently displayed.

3-14.2 MLD Snooping

3-14.2.1 Status

The section describes when you complete the MLD Snooping and how to display the MLD Snooping Status and detail information. It will help you to find out the detail information of MLD Snooping status.

Web Interface

To display the MLD Snooping Status in the web interface:

1. Click Monitor, MLD Snooping and Status.
2. If you want to auto-refresh the information then you need to evoke the “Auto-refresh”.
3. Click “Refresh” to refresh an entry of the MLD Snooping Status Information.
4. Click “Clear “to clear the MLD Snooping Status.

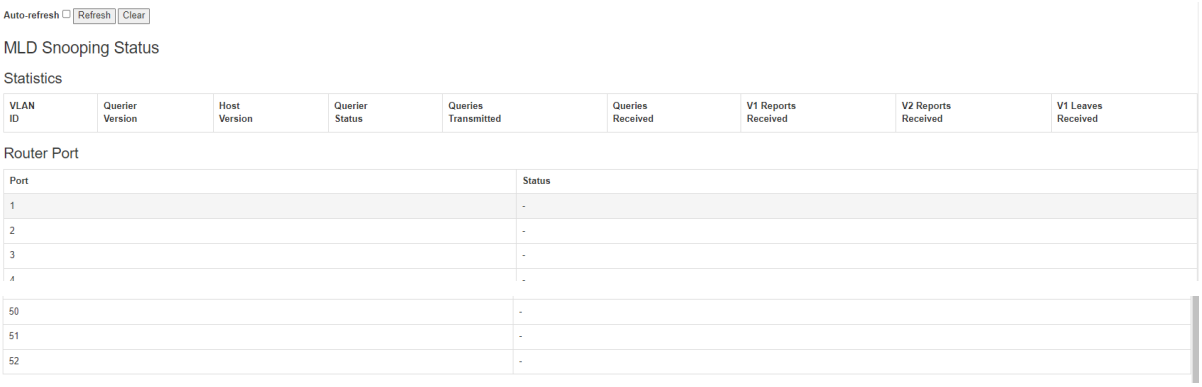


Figure 3-14.2.1: The MLD Snooping Status

Parameter description:

- **VLAN ID :**

  The VLAN ID of the entry.

- **Querier Version :**

  Working Querier Version currently.

- **Host Version :**

  Working Host Version currently.

- **Querier Status :**

  Show the Querier status is "ACTIVE" or "IDLE".

  "DISABLE" denotes the specific interface is administratively disabled.

- **Queries Transmitted :**

  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.

- **V1 Leaves Received :**

  The number of Received V1 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 :**

  Switch port number.

- **Status :**

  Indicate whether specific port is a router port or not.

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 all Statistics counters.

3-14.2.2 Group Information

The section describes user could set the MLD Snooping Groups Information. The "Start from VLAN", and "group" input fields allow the user to select the starting point in the MLD Group Table

Web Interface

To display the MLD Snooping Group information in the web interface:

1. Click Monitor, MLD Snooping and Group Information
2. If you want to auto-refresh the information then you need to evoke the “Auto-refresh”
3. Click “Refresh” to refresh an entry of the MLD Snooping Group Information.
4. Click “Clear “to clear the MLD Snooping Groups information..

Figure 3-14.2.2: The MLD Snooping Groups Information

Parameter description:

MLD Snooping Information Table Columns

- **VLAN ID :**

  VLAN ID of the group.

- **Groups :**

  Group address of the group displayed.

- **Port Members :**

  Ports under this group.

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 with the first entry in the IGMP Group Table.

- **>>:**

  Updates the system log entries, ending at the last entry currently displayed.

Entries in the MLD SFM Information Table are shown on this page. The MLD 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.

Web Interface

To display the MLDv2 IPv6 SSM Information in the web interface:

1. Click Monitor, MLD Snooping and IPv6 SFM Information.
2. If you want to auto-refresh the information then you need to evoke the “Auto-refresh”.
3. Click “Refresh” to refresh an entry of the MLDv2 IPv6 SSM Information.
4. Click “<< or >> ”to move to previous or next entry.

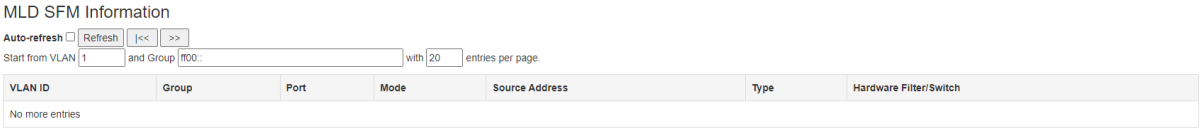


Figure 3-14.2.3: The IPv6 SFM Information

Parameter description:

MLD SFM Information Table Columns

- **VLAN ID :**

  VLAN ID of the group.

- **Group :**

  Group address of the group displayed.

- **Port :**

  Switch port number.

- **Mode :**

  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, system limits the total number of IP source addresses for filtering to be 128. 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 IPv6 address could be handled by chip or not.

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 with the first entry in the IGMP Group Table.

- **>>:**

  Updates the system log entries, ending at the last entry currently displayed.

3-17.1 Neighbour

This page provides a status overview for all LLDP neighbours. The displayed table contains a row for each port on which an LLDP neighbour is detected. The columns hold the following information

Web Interface

To display the LLDP neighbours:

1. Click Monitor, LLDP and Neighbours.
2. Click Refresh for manual update web screen
3. Click Auto-refresh for auto-update web screen

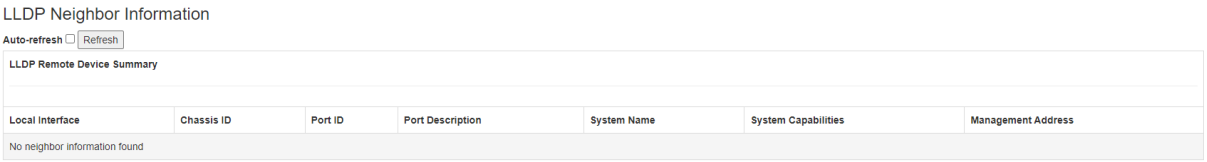


Figure 3-15.1: The LLDP Neighbours information

NOTE: If your network without any device supports LLDP then the table will show "No LLDP neighbour information found".

Parameter description:

- **Local Interface :**

  The port on which the LLDP frame was received.

- **Chassis ID :**

  The Chassis ID is the identification of the neighbour's LLDP frames.

- **Port ID :**

  The Remote Port ID is the identification of the neighbour port.

- **Port Description :**

  Port Description is the port description advertised by the neighbour unit.

- **System Name :**

  System Name is the name advertised by the neighbour unit.

- **System Capabilities :**

  System Capabilities describes the neighbour unit's capabilities. The possible capabilities are:

  1. Other
  2. Repeater
  3. Bridge
  4. WLAN Access Point

5. Router

6. Telephone

7. DOCSIS cable device

8. Station only

9. Reserved

When a capability is enabled, the capability is followed by (+). If the capability is disabled, the capability is followed by (-).

- **Management Address :**

  Management Address is the neighbour unit's address that is used for higher layer entities to assist discovery by the network management. This could for instance hold the neighbour'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 immediately.

This page provides a status overview of all LLDP-MED neighbours. The displayed table contains a row for each port on which an LLDP neighbour is detected. This function applies to VoIP devices which support LLDP-MED. The columns hold the following information:

Web Interface

To display the LLDP-MED neighbor:

1. Click Monitor, LLDP and LLDP-MED Neighbor.
2. Click Refresh for manual update web screen
3. Click Auto-refresh for auto-update web screen

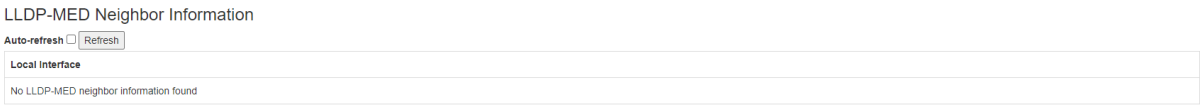


Figure 3-15.2: The LLDP-MED Neighbours information

NOTE: If your network without any device supports LLDP-MED then the table will show "No LLDP-MED neighbour information found".

Parameter description:

- **Interface:**

  The port on which the LLDP frame was received.

- **Device Type :**

  LLDP-MED Devices are comprised of two primary Device Types: Network Connectivity Devices and Endpoint Devices.

  LLDP-MED Network Connectivity Device Definition

  LLDP-MED Network Connectivity Devices, as defined in TIA-1057, provide access to the IEEE 802 based LAN infrastructure for LLDP-MED Endpoint Devices. An LLDP-MED Network Connectivity Device is a LAN access device based on any of the following technologies:

  1. LAN Switch/Router

  2. IEEE 802.1 Bridge

  3. IEEE 802.3 Repeater (included for historical reasons)

  4. IEEE 802.11 Wireless Access Point

  5. Any device that supports the IEEE 802.1AB and MED extensions defined by TIA-1057 and can relay IEEE 802 frames via any method.

  LLDP-MED Endpoint Device Definition :

  LLDP-MED Endpoint Devices, as defined in TIA-1057, are located at the IEEE 802 LAN network edge, and participate in IP communication service using the LLDP-MED framework.

  Within the LLDP-MED Endpoint Device category, the LLDP-MED scheme is broken into further Endpoint Device Classes, as defined in the following.

  Each LLDP-MED Endpoint Device Class is defined to build upon the capabilities defined for

the previous Endpoint Device Class. For-example will any LLDP-MED Endpoint Device claiming compliance as a Media Endpoint (Class II) also support all aspects of TIA-1057 applicable to Generic Endpoints (Class I), and any LLDP-MED Endpoint Device claiming compliance as a Communication Device (Class III) will also support all aspects of TIA-1057 applicable to both Media Endpoints (Class II) and Generic Endpoints (Class I).

LLDP-MED Generic Endpoint (Class I) :

The LLDP-MED Generic Endpoint (Class I) definition is applicable to all endpoint products that require the base LLDP discovery services defined in TIA-1057, however do not support IP media or act as an end-user communication appliance. Such devices may include (but are not limited to) IP Communication Controllers, other communication related servers, or any device requiring basic services as defined in TIA-1057.

Discovery services defined in this class include LAN configuration, device location, network policy, power management, and inventory management.

LLDP-MED Media Endpoint (Class II) :

The LLDP-MED Media Endpoint (Class II) definition is applicable to all endpoint products that have IP media capabilities however may or may not be associated with a particular end user. Capabilities include all of the capabilities defined for the previous Generic Endpoint Class (Class I), and are extended to include aspects related to media streaming. Example product categories expected to adhere to this class include (but are not limited to) Voice / Media Gateways, Conference Bridges, Media Servers, and similar.

Discovery services defined in this class include media-type-specific network layer policy discovery.

LLDP-MED Communication Endpoint (Class III) :

The LLDP-MED Communication Endpoint (Class III) definition is applicable to all endpoint products that act as end user communication appliances supporting IP media. Capabilities include all of the capabilities defined for the previous Generic Endpoint (Class I) and Media Endpoint (Class II) classes, and are extended to include aspects related to end user devices. Example product categories expected to adhere to this class include (but are not limited to) end user communication appliances, such as IP Phones, PC-based softphones, or other communication appliances that directly support the end user.

Discovery services defined in this class include provision of location identifier (including ECS / E911 information), embedded L2 switch support, inventory management.

- **LLDP-MED Capabilities :**

  LLDP-MED Capabilities describes the neighborhood unit's LLDP-MED capabilities. The possible capabilities are:

  1. LLDP-MED capabilities
  2. Network Policy
  3. Location Identification
  4. Extended Power via MDI - PSE
  5. Extended Power via MDI - PD
  6. Inventory
  7. Reserved

- **Application Type :**

  Application Type indicating the primary function of the application(s) defined for this network policy, advertised by an Endpoint or Network Connectivity Device. The possible application types are shown below.

1. 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.

2. Voice Signalling - for use in network topologies that require a different policy for the voice signalling than for the voice media.

3. Guest Voice - to 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.

4. Guest Voice Signalling - for use in network topologies that require a different policy for the guest voice signalling than for the guest voice media.

5. Softphone Voice - for use by softphone applications on typical data centric devices, such as PCs or laptops.

6. Video Conferencing - for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services.

7. 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.

8. Video Signalling - for use in network topologies that require a separate policy for the video signalling than for the video media.

- **Policy :**

  Policy indicates that an Endpoint Device wants to explicitly advertise that the policy is required by the device. Can be either Defined or Unknown

  Unknown: The network policy for the specified application type is currently unknown.

  Defined: The network policy is defined.

- **TAG :**

  TAG is indicative of whether the specified application type is using a tagged or an untagged VLAN. Can be Tagged or Untagged.

  Untagged: The device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003.

  Tagged: The device is using the IEEE 802.1Q tagged frame format.

- **VLAN ID :**

  VLAN ID is the VLAN identifier (VID) for the port as defined in IEEE 802.1Q-2003. A value of 1 through 4094 is used to define a valid VLAN ID. A value of 0 (Priority Tagged) is used if the device is using priority tagged frames as defined by IEEE 802.1Q-2003, meaning that only the IEEE 802.1D priority level is significant and the default PVID of the ingress port is used instead.

- **Priority :**

  Priority is the Layer 2 priority to be used for the specified application type.One of the eight priority levels (0 through 7).

- **DSCP :**

  DSCP is the DSCP value to be used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474. Contain one of 64 code point values (0 through 63).

- **Auto-negotiation :**

Auto-negotiation identifies if MAC/PHY auto-negotiation is supported by the link partner.

- **Auto-negotiation status :**

  Auto-negotiation status identifies if auto-negotiation is currently enabled at the link partner. If Auto-negotiation is supported and Auto-negotiation status is disabled, the 802.3 PMD operating mode will be determined the operational MAU type field value rather than by auto-negotiation.

- **Auto-negotiation Capabilities :**

  Auto-negotiation Capabilities shows the link partners MAC/PHY capabilities.

Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page immediately.

3-15.3 PoE

This page allows the user to inspect the current status for all PoE ports. The section show all port Power Over Ethernet Status.

Web Interface

To display the LLDP Neighbor Power Over Ethernet information:

1. Click Monitor ,LLDP, PoE
2. Display Power Over Ethernet Status Information
3. Click Auto-refresh for auto-update web screen

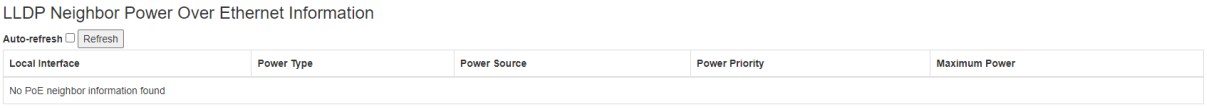


Figure 3-15.3: The LLDP Neighbors EEE information

Parameter description:

- **Local Interface :**

  The port 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".

- **Power 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 Priority represents the priority of the PD device, or the power priority associated with the PSE type device's port 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"

- **Maximum Power :**

  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 immediately.

By using EEE power savings can be achieved at the expense of traffic latency. This latency occurs due to that the circuits EEE turn off to save power, need time to boot up before sending traffic over the link. This time is called "wakeup time". To achieve minimal latency, devices can use LLDP to exchange information about their respective tx and rx "wakeup time ", as a way to agree upon the minimum wakeup time they need.

This page provides an overview of EEE information exchanged by LLDP.

Web Interface

To display the LLDP EEE neighbors:

1. Click Monitor, LLDP then click EEE to show discover EEE devices.
2. Click Refresh for manual update web screen.
3. Click Auto-refresh for auto-update web screen.

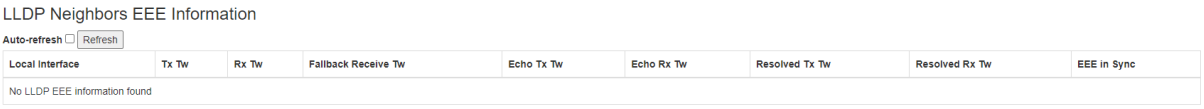


Figure 3-15.4: The LLDP Neighbors EEE information

NOTE: If your network without any devices which enables EEE function then the table will show “No LLDP EEE information found”.

Parameter description:

LLDP Neighbors EEE Information

The displayed table contains a row for each port. The columns hold the following information:

- **Local Interface :**

  The port on which LLDP frames are received or transmitted.

- **Tx Tw :**

  The link partner’s maximum time that transmit path can hold off sending data after reassertion of LPI.

- **Rx Tw :**

  The link partner’s time that receiver would like the transmitter to hold off to allow time for the receiver to wake from sleep.

- **Fallback Receive Tw :**

  The link partner’s fallback receive Tw.

  A receiving link partner may inform the transmitter of an alternate desired Tw_sys_tx. Since a receiving link partner is likely to have discrete levels for savings, this provides the transmitter with additional information that it may use for a more efficient allocation. Systems that do not implement this option default the value to be the same as that of the Receive Tw_sys_tx.

- **Echo Tx Tw :**

  The link partner's Echo Tx Tw value.

The respective echo values shall be defined as the local link partner's reflection (echo) of the remote link partners respective values. When a local link partner receives its echoed values from the remote link partner it can determine whether or not the remote link partner has received, registered and processed its most recent values. For example, if the local link partner receives echoed parameters that do not match the values in its local MIB, then the local link partner infers that the remote link partners request was based on stale information.

- **Echo Rx Tw :**

  The link partner's Echo Rx Tw value.

- **Resolved Tx Tw :**

  The resolved Tx Tw for this link. Note: NOT the link partner

  The resolved value that is the actual "tx wakeup time" used for this link (based on EEE information exchanged via LLDP).

- **Resolved Rx Tw :**

  The resolved Rx Tw for this link. Note: NOT the link partner

  The resolved value that is the actual "tx wakeup time" used for this link (based on EEE information exchanged via LLDP).

- **EEE in Sync :**

  Shows whether the switch and the link partner have agreed on wake times.

  Red - Switch and link partner have not agreed on wakeup times.

  Green - Switch and link partner have agreed on wakeup times.

Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page immediately.

Two types of counters are shown. Global counters are counters that refer to the whole switch, while local counters refer to per port counters for the currently selected switch

Web Interface

To display the LLDP Statistics:

1. Click Monitor ,LLDP, then click Port Statistics to show LLDP counters
2. Click Refresh for manual update web screen
3. Click Auto-refresh for auto-update web screen
4. Click Clear to clear all counters

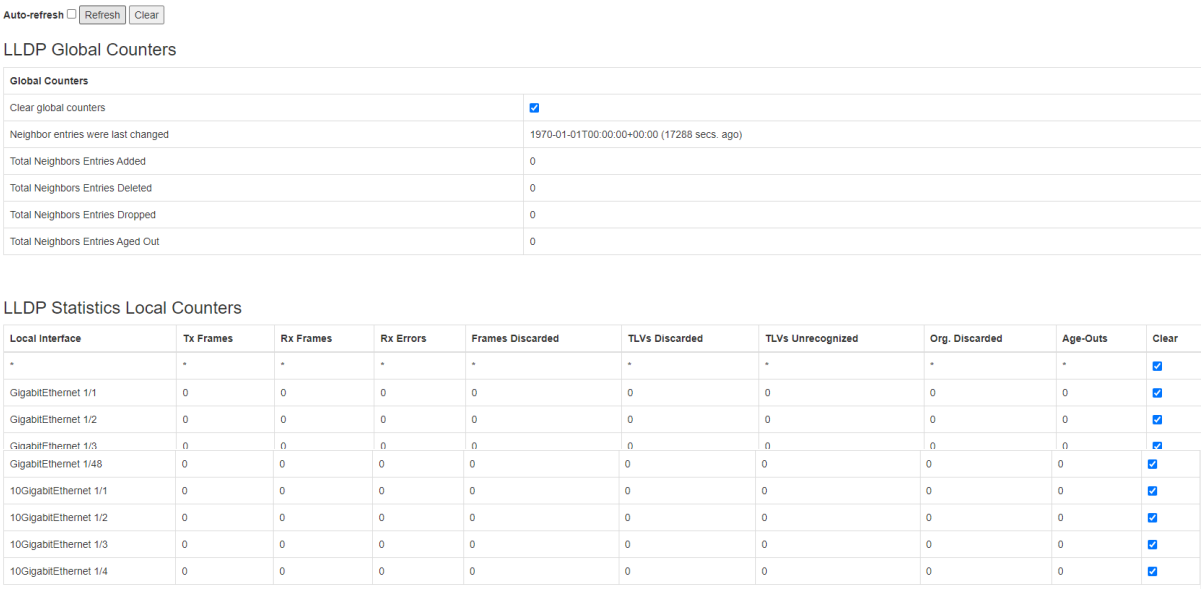


Figure 3-15.5: The LLDP Port Statistics information

Parameter description:

Global Counters

- **Clear Global Counters:**

  If checked the global counters are cleared when Clear is pressed.

- **Neighbour entries were last changed at :**

  It also 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 Neighbours Entries Added :**

  Shows the number of new entries added since switch reboot.

- **Total Neighbours Entries Deleted :**

  Shows the number of new entries deleted since switch reboot.

- **Total Neighbours Entries Dropped :**

  Shows the number of LLDP frames dropped due to the entry table being full.

- **Total Neighbours Entries Aged Out :**

  Shows the number of entries deleted due to Time-To-Live expiring.

Local Counters

The displayed table contains a row for each port. The columns hold the following information:

- **Local Interface :**

  The port on which LLDP frames are received or transmitted.

- **Tx Frames :**

  The number of LLDP frames transmitted on the port.

- **Rx Frames :**

  The number of LLDP frames received on the port.

- **Rx Errors :**

  The number of received LLDP frames containing some kind of error.

- **Frames Discarded :**

  If an LLDP frame is received on a port, and the switch's internal table has run full, the LLDP frame is counted and discarded. This situation is known as "Too Many Neighbours" 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 port'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 :**

  The number of organizationally received TLVs.

- **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 pressed

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 local counters. All counters (including global counters) are cleared upon reboot.

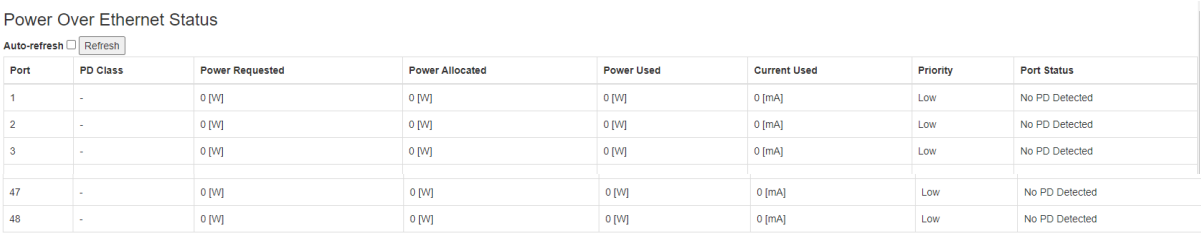
3-16 PoE

This page allows the user to inspect the current status for all PoE ports.

Web Interface

To Display PoE status in the web interface:

1. Click Monitor,PoE
2. Display PoE status.


Power Over Ethernet Status

Auto-refresh ☐ Refresh

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
47	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD Detected
48	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD Detected

Figure 3-16: The PoE Status

Parameter description:

- **Port:**

  This is the logical port number for this row.

- **PD Class :**

  The PD Class shows the PDs class.

  The following classes are defined:

  Class 0: Max. power 15.4 W

  Class 1: Max. power 4.0 W

  Class 2: Max. power 7.0 W

  Class 3: Max. power 15.4 W

  Class 4: Max. power 30.0 W

  Class 5: Max. power 45.0 W

  Class 6: Max. power 60.0 W

  Class 7: Max. power 70.0 W

  Class 8: Max. power 90.0 W

- **Power Requested :**

  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 current 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 ports that are members of the entry. The Port Status shows the port's status. The status can be one of the following values:

  On - A PD is detected for the port.

  Off - PD is off.

  Disabled - User has disabled PoE for the port.

  Overload - The PD has requested or used more power than the port can deliver, and is powered down.

Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Refreshes the displayed table starting from the "Start from MAC address" and "VLAN" input fields.

3-17 MAC Table

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.

Web Interface

To Display MAC Address Table in the web interface:

3. Click Monitor, Dynamic MAC Table.
4. Specify the VLAN and MAC Address.
5. Display MAC Address Table.

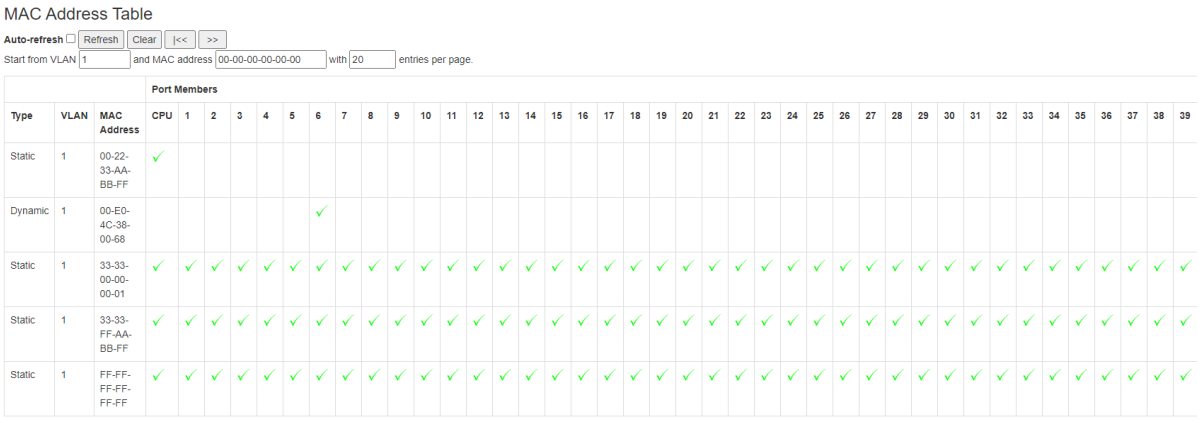


Figure 3-17: The MAC Address Table

Parameter description:

MAC Table Columns

- **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 :**

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

- **Refresh :**

  Refreshes the displayed table starting from the "Start from MAC address" and "VLAN" input fields.

- **Clear :**

  Flushes the selected log 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 system log entries, ending at the last entry currently displayed.

NOTE:
00-40-C7-73-01-29 : your switch MAC address (for IPv4)
33-33-00-00-00-01 : Destination MAC (for IPv6 Router Advertisement) (reference IPv6 RA.JPG)
33-33-00-00-00-02 : Destination MAC (for IPv6 Router Solicitation) (reference IPv6 RS.JPG)
33-33-FF-73-01-29 : Destination MAC (for IPv6 Neighbor Solicitation) (reference IPv6 DAD.JPG)
33-33-FF-A8-01-01: your switch MAC address (for IPv6 global IP)
FF-FF-FF-FF-FF-FF: for Broadcast.

3-18.1 Membership

This page provides an overview of membership status of VLAN users.

Web Interface

To display the VLAN membership configuration in the web interface:

1. Click Monitor, VLANs and VLAN membership.
2. Scroll the bar to choice which VLANs would like to show up.
3. Click Refresh to update the state.

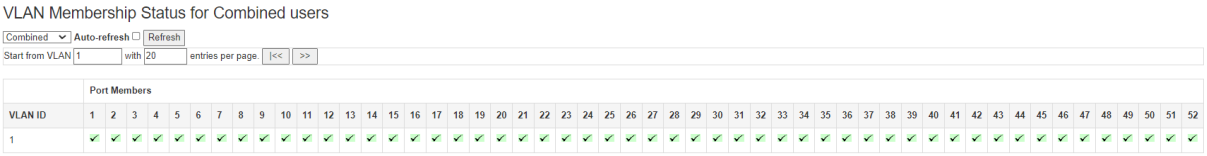


Figure 3-18.1: VLAN Membership Status for Combined users

Parameter description:

- **VLAN USER :**

  Various internal software modules may use VLAN services to configure VLAN memberships on the fly.

  The drop-down list on the right allows for selecting between showing VLAN memberships as configured by an administrator (Admin) or as configured by one of these internal software modules.

  The "Combined" entry will show a combination of the administrator and internal software modules configuration, and basically reflects what is actually configured in hardware.

- **VLAN ID :**

  VLAN ID for which the Port members are displayed.

- **Port Members :**

  A row of check boxes for each port is displayed for each VLAN ID.
  If a port is included in a VLAN, an image ✓ will be displayed.
  If a port is included in a Forbidden port list, an image ✗ will be displayed.
  If a port is included in a Forbidden port list and dynamic VLAN user register VLAN on same Forbidden port, then conflict port will be displayed as ✗c.

- **VLAN Membership**

  The VLAN Membership Status Page shall show the current VLAN port members for all VLANs configured by a selected VLAN User (selection shall be allowed by a Combo Box). When ALL VLAN Users are selected, it shall show this information for all the VLAN Users, and this is by default. VLAN membership allows the frames classified to the VLAN ID to be forwarded on the respective VLAN member ports.

Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Refreshes the displayed table starting from the "Start from MAC address" and "VLAN" input fields.

- **Combined :**

  Select VLAN Users from this drop down list.

3-18.2 Port

The function Port Status gathers the information of all VLAN status and reports it by the order of Static NAS MVRP MVP Voice VLAN MSTP GVRP Combined.

Web Interface

To Display VLAN Port Status in the web interface:

1. Click Monitor, VLAN and Port Status.
2. Specify the Static NAS MVRP MVP Voice VLAN MSTP GVRP Combined.
3. Display Port Status information.

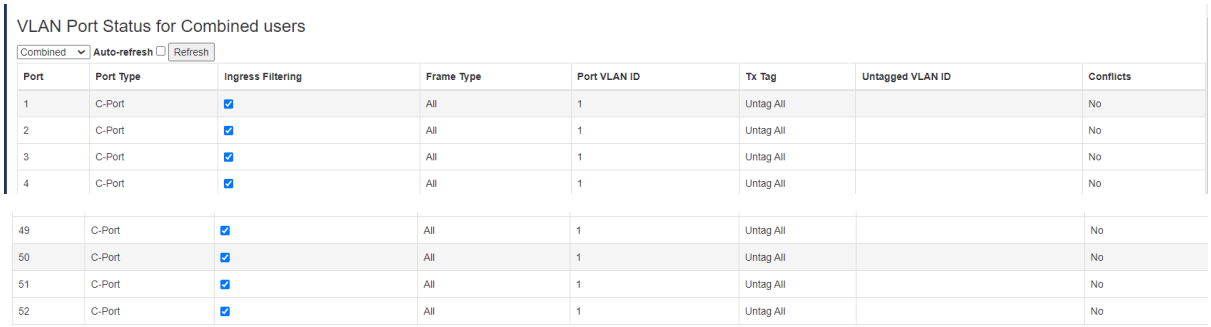


Figure 3-18.2: The VLAN Port Status for Static user

Parameter description:

- **VLAN USER :**

  VLAN User module uses services of the VLAN management functionality to configure VLAN memberships and VLAN port configuration such as PVID, UVID. Currently we support following VLAN User types:

  CLI/Web/SNMP : These are referred to as static.

  NAS : NAS provides port-based authentication, which involves communications between a Supplicant, Authenticator, and an Authentication Server.

  MVRP : Multiple VLAN Registration Protocol (MVRP) allows dynamic registration and deregistration of VLANs on ports on a VLAN bridged network.

  Voice VLAN : Voice VLAN is a VLAN configured specially for voice traffic typically originating from IP phones.

  MVR : MVR is used to eliminate the need to duplicate multicast traffic for subscribers in each VLAN. Multicast traffic for all channels is sent only on a single (multicast) VLAN.

  MSTP : The 802.1s Multiple Spanning Tree protocol (MSTP) uses VLANs to create multiple spanning trees in a network, which significantly improves network resource utilization while maintaining a loop-free environment.

- **Port :**

  The logical port for the settings contained in the same row.

- **Port Type :**

  Shows the Port Type. Port type can be any of Unaware, C-port, S-port, Custom S-port.

  If Port Type is Unaware, all frames are classified to the Port VLAN ID and tags are not removed. C-port is Customer Port. S-port is Service port. Custom S-port is S-port with Custom TPID.

- **Ingress Filtering :**

  Shows the ingress filtering on a port. This parameter affects VLAN ingress processing. If ingress filtering is enabled and the ingress port is not a member of the classified VLAN, the frame is discarded.

- **Frame Type :**

  Shows whether the port accepts all frames or only tagged frames. This parameter affects VLAN ingress processing. If the port only accepts tagged frames, untagged frames received on that port are discarded.

- **Port VLAN ID :**

  Shows the Port VLAN ID (PVID) that a given user wants the port to have.

  The field is empty if not overridden by the selected user.

- **Tx Tag :**

  Shows egress filtering frame status whether tagged or untagged.

- **Untagged VLAN ID:**

  Shows UVID (untagged VLAN ID). Port's UVID determines the packet's behavior at the egress side.

- **Conflicts :**

  Shows status of Conflicts whether exists or not. When a Volatile VLAN User requests to set VLAN membership or VLAN port configuration, the following conflicts can occur:

  Functional Conflicts between features.

  Conflicts due to hardware limitation.

  Direct conflict between user modules.

Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page immediately.

- **Combined :**

  Select VLAN Users from this drop down list.

This page provides statistics for the MVRP protocol for all switch ports.

Web Interface

To Display MVRP statistics in the web interface:

1. Click Monitor and MVRP
2. Display statistics for the MVRP protocol

Figure 3-19: The MVRP

Parameter description:

- **Port:**

  The logical port for the statistics contained in the same row.

- **Failed Registration:**

  The number of failed VLAN registrations on this switch port. Each port implementing the MVRP protocol maintains a count of the number of times it has received a VLAN registration request but has failed to register the VLAN due to lack of space in the Filtering Database.

- **Last PDU Origin :**

  The MAC address of the most recent MVRP PDU received on this switch port. MAC is 00-00-00-00-00-00 if the protocol is not enabled on that switch port, or if the port has not received any MVRP PDUs yet.

Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page immediately.

This session shows receiver and per-port sFlow statistics

Web Interface

To Display port sFlow statistics in the web interface:

1. Click Monitor and sFlow.
2. Display sFlow information.

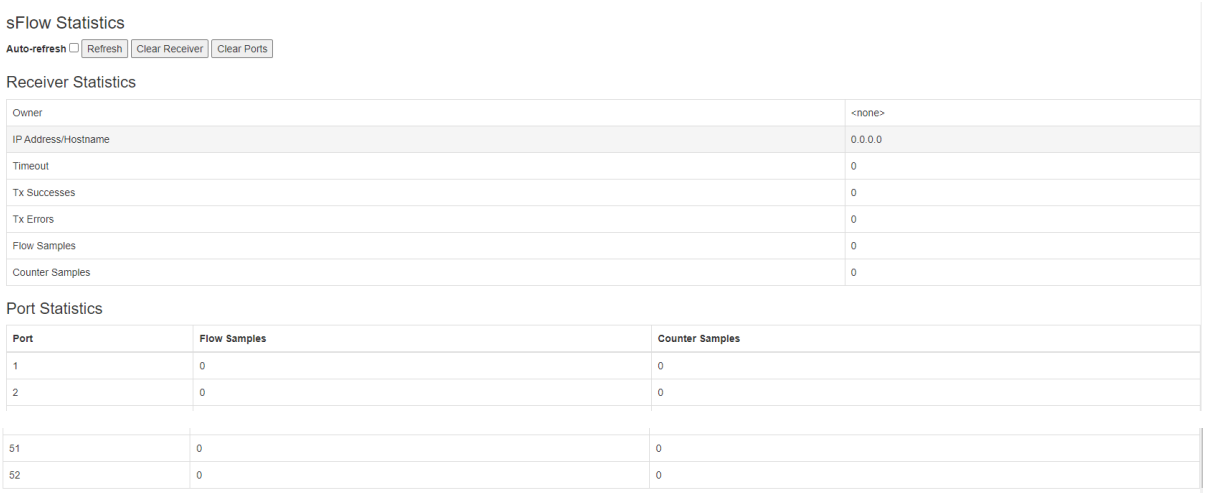


Figure 3-20: The sFlow Statistics

Parameter description:

Receiver Statistics

- **Owner :**

  This field shows the current owner of the sFlow configuration. It assumes one of three values as follows:

  • If sFlow is currently unconfigured/unclaimed, Owner contains <none>.

  • If sFlow is currently configured through Web or CLI, Owner contains <Configured through local management>.

  • If sFlow is currently configured through SNMP, Owner contains a string identifying the sFlow receiver.`

- **IP Address/Hostname :**

  The IP address or hostname of the sFlow receiver.

- **Timeout :**

  The number of seconds remaining before sampling stops and the current sFlow owner is released.

- **Tx Successes :**

  The number of UDP datagrams successfully sent to the sFlow receiver.

- **Tx Errors :**

The number of UDP datagrams that has failed transmission.
The most common source of errors is invalid sFlow receiver IP/hostname configuration. To diagnose, paste the receiver's IP address/hostname into the Ping Web page (Diagnostics → Ping/Ping6).

- **Flow Samples :**

  The total number of flow samples sent to the sFlow receiver.

- **Counter Samples :**

  The total number of counter samples sent to the sFlow receiver.

Port Statistics

- **Port :**

  The port number for which the following statistics applies.

- **Rx and Tx Flow Samples :**

  The number of flow samples sent to the sFlow receiver originating from this port. Here, flow samples are divided into Rx and Tx flow samples, where Rx flow samples contains the number of packets that were sampled upon reception (ingress) on the port and Tx flow samples contains the number of packets that were sampled upon transmission (egress) on the port.

- **Counter Samples :**

  The total number of counter samples sent to the sFlow receiver originating from this port.

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 Receiver :**

  Clears the sFlow receiver counters.

- **Clear Ports :**

  Clears the per-port counters.

3-21 DDMI

3.21.1 Overview

Display DDMI overview information on this page.

Web Interface

To Display DDMI overview information in the web interface:

1. Click Monitor, DDMI and overview.
2. Display DDMI overview information.

Figure 3-21.1 The DDMI Overview

Parameter description:

- **Port :**

  The DDMI port.

- **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.

Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page immediately.

3-21.2 Detailed

Display DDMI detailed information on this page.

Web Interface

To Display port sFlow statistics in the web interface:

1. Click Monitor, DDMI and Detailed.
2. Select the port to display the DDMI information
3. Display DDMI Detailed information.

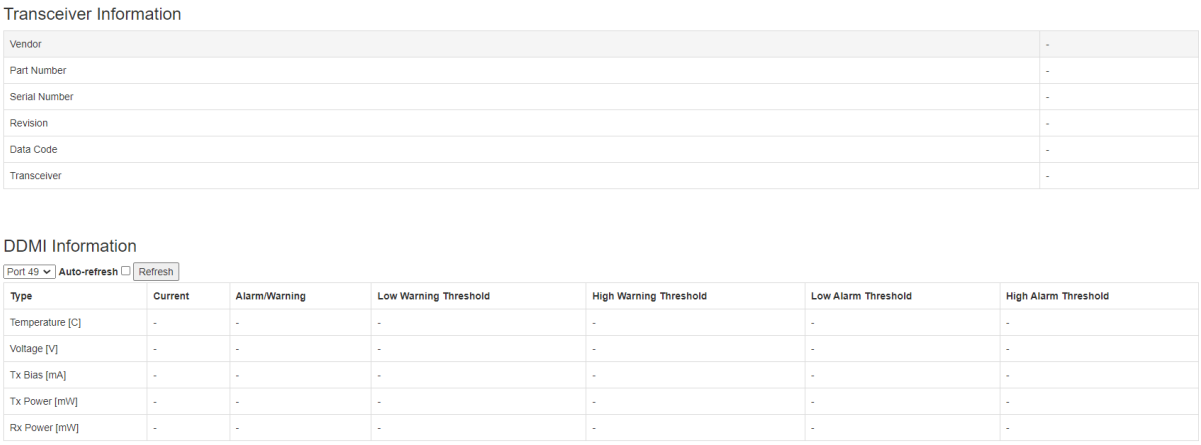


Figure 3-21.2: The DDMI Detailed Information

Parameter description:

Transceiver Information

- **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.

- **Alarm/Warning :**

  Indicates whether there is an alarm or warning.

- **Low Warning Threshold:**

  The low warning threshold value of temperature, voltage, Tx bias, Tx power, and Rx power.

- **High Warning Threshold :**

  The high warning 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.

- **High Alarm Threshold :**

  The high alarm threshold value of temperature, voltage, Tx bias, Tx power, and Rx power.

Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page immediately.

3-22 UDLD

This page displays the UDLD status of the ports

Web Interface

To Display the UDLD status of the ports in the web interface:

1. Click Monitor and UDLD.
2. Select the port to display
3. Display UDLD status information of the selected port.

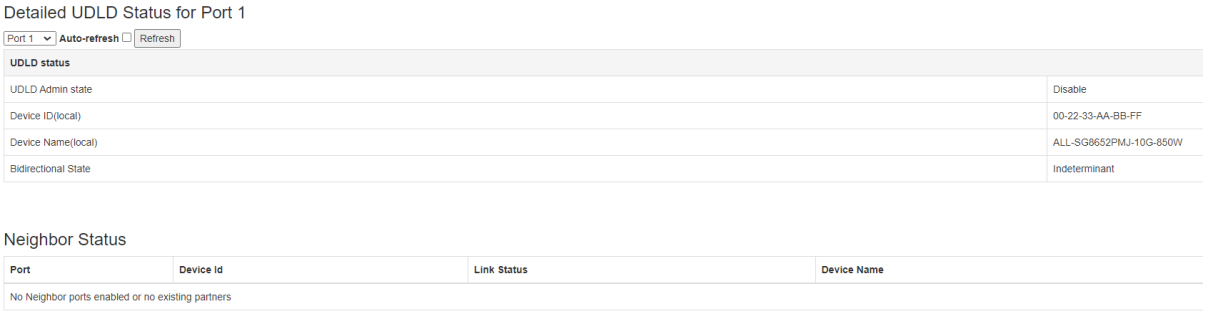


Figure 3-22: The UDLD Status

Parameter description:

UDLD Status

- **UDLD Admin State :**

  The current port state of the logical port, Enabled if any of state(Normal,Aggressive) is Enabled.

- **Device ID (Local) :**

  The ID of Device.

- **Device Name (Local) :**

  The name of Device

- **Biddirectional State:**

  The current state of the port.

Neighbor Status

- **Port :**

  The current port of neighbor device.

- **Device ID :**

  The current ID of neighbor device.

- **Link Status :**

  The current link status of neighbor device.

- **Device Name (Local) :**

The name of neighbor Device

Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page immediately.

Chapter 4 Diagnostics

This chapter provides a set of basic system diagnosis. It let users know that whether the system is health or needs to be fixed. The basic system check includes ICMP Ping, Link OAM, ICMPv6, and VeriPHY Cable Diagnostics.

4-1 Ping(IPv4)

This page allows you to issue ICMP (IPv4) PING packets to troubleshoot IP connectivity issues.

Web Interface

To configure an ICMP PING Configuration in the web interface:

1. Click Diagnotsics, Ping(IPv4)
2. Specify PING IP Address, payload size and other parameters.
3. Click Start.

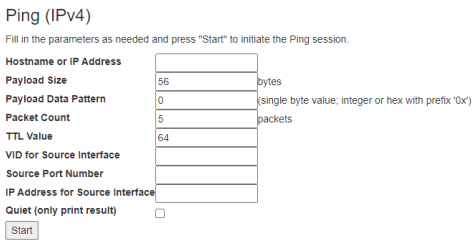


Figure 4-1: The Ping (IPv4)

Parameter description:

- **Hostname or IP Address:**

  The address of the destination host, either as a symbolic hostname or an IP Address.

- **Payload Size :**

  Determines the size of the ICMP data payload in bytes (excluding the size of Ethernet, IP and ICMP headers). The default value is 56 bytes. The valid range is 2-1452 bytes.

- **Payload Data Pattern :**

  Determines the pattern used in the ICMP data payload. The default value is 0. The valid range is 0-255.

- **Packet Count :**

  Determines the number of PING requests sent. The default value is 5. The valid range is 1-60.

- **TTL Value :**

Determines the Time-To-Live /TTL) field value in the IPv4 header. The default value is 64. The valid range is 1-255.

- **VID for Source Interface :**

  This field can be used to force the test to use a specific local VLAN interface as the source interface. Leave this field empty for automatic selection based on routing configuration.

  Note: You may only specify either the VID or the IP Address for the source interface.

- **Source Port Number:**

  This field can be used to force the test to use a specific local interface with the specified port number as the source interface. The specified port must be configured with a suitable IP address. Leave this field empty for automatic selection based on routing configuration.

  Note: You may only specify either the Source Port Number or the IP Address for the source interface.

- **Address for Source Interface :**

  This field can be used to force the test to use a specific local interface with the specified IP address as the source interface. The specified IP address must be configured on a local interface. Leave this field empty for automatic selection based on routing configuration.

  Note: You may only specify either the VID or the IP Address for the source interface.

- **Quiet(Only Print Result) :**

  Checking this option will not print the result of each ping request but will only show the final result.

Buttons

- **Start :**

  Click the "Start" button then the switch will start to ping the device using ICMP packet size what set on the switch.

  After you press , 5 ICMP packets are transmitted, and the sequence number and roundtrip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

  PING6 server ::10.10.132.20

  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

  Sent 5 packets, received 5 OK, 0 bad

4-2 Ping(IPv6)

This section allows you to issue ICMPv6 PING packets to troubleshoot IPv6 connectivity issues.

Web Interface

To configure an ICMPv6 PING Configuration in the web interface:

1. Click Diagnostics and Ping(IPv6)
2. Specify the detailed parameters in blank
3. Click Start.

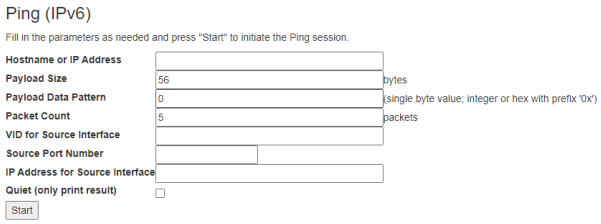


Figure 4-2: The ICMPv6 Ping

Parameter description:

- **Hostname or IP Address:**

  The address of the destination host, either as a symbolic hostname or an IP Address.

- **Payload Size :**

  Determines the size of the ICMP data payload in bytes (excluding the size of Ethernet, IP and ICMP headers). The default value is 56 bytes. The valid range is 2-1452 bytes.

- **Payload Data Pattern :**

  Determines the pattern used in the ICMP data payload. The default value is 0. The valid range is 0-255.

- **Packet Count :**

  Determines the number of PING requests sent. The default value is 5. The valid range is 1-60.

- **VID for Source Interface :**

  This field can be used to force the test to use a specific local VLAN interface as the source interface. Leave this field empty for automatic selection based on routing configuration.

  Note: You may only specify either the VID or the IP Address for the source interface.

- **Source Port Number:**

  This field can be used to force the test to use a specific local interface with the specified port number as the source interface. The specified port must be configured with a suitable IP address. Leave this field empty for automatic selection based on routing configuration.

  Note: You may only specify either the Source Port Number or the IP Address for the source interface.

- **Address for Source Interface :**

  This field can be used to force the test to use a specific local interface with the specified IP

address as the source interface. The specified IP address must be configured on a local interface. Leave this field empty for automatic selection based on routing configuration.

Note: You may only specify either the VID or the IP Address for the source interface.

- **Quiet(Only Print Result) :**

  Checking this option will not print the result of each ping request but will only show the final result.

Buttons

- **Start :**

  Click the "Start" button then the switch will start to ping the device using ICMPv6 packet size what set on the switch.

  After you press, 5 ICMPv6 packets are transmitted, and the sequence number and roundtrip time are displayed upon reception of a 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

  Sent 5 packets, received 10 OK, 0 bad

  You can configure the following properties of the issued ICMP packets:

4-3 Traceroute(IPv4)

This page allows you to perform a traceroute test over IPv4 towards a remote host. traceroute is a diagnostic tool for displaying the route and measuring transit delays of packets across an IPv4 network.

Web Interface

To configure an Traceroute IPv4 Configuration in the web interface:

1. Click Diagnotics and Traceroute(IPv4)
2. Specify traceroute IP Address, DSCP Value and other paramters.
3. Click Start.

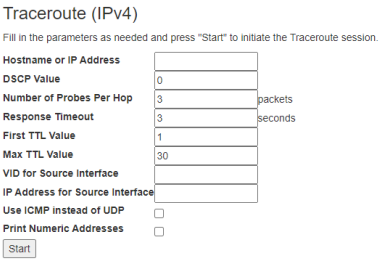


Figure 4-3: The Traceroute IPv4

Parameter description:

- **Hostname orIP Address:**

  The destination IP Address.

- **DSCP Value:**

  The destination IP Address. This value is used for the DSCP value in the IPv4 header. The default value is 0. The valid range is 0-63.

- **Number of Probes Per Hop :**

  Determines the number of probes (packets) sent for each hop. The default value is 3. The valid range is 1-60.

- **ResponseTimeout:**

  Determines the number of seconds to wait for a reply to a sent request. The default number is 3. The valid range is 1-86400.

- **First TTL Value:**

  Determines the value of the Time-To-Live (TTL) field in the IPv4 header in the first packet sent. The default number is 1. The valid range is 1-30.

- **Max TTL Value :**

  Determines the maximum value of the Time-To-Live (TTL) field in the IPv4 header. If this value is reached before the specified remote host is reached the test stops. The default number is 30. The valid range is 1-255.

- **VID for Source Interface :**

  This field can be used to force the test to use a specific local VLAN interface as the source interface. Leave this field empty for automatic selection based on routing configuration.

  Note: You may only specify either the VID or the IP Address for the source interface.

- **IP Address for Source Interface :**

  This field can be used to force the test to use a specific local interface with the specified IP address as the source interface. The specified IP address must be configured on a local interface. Leave this field empty for automatic selection based on routing configuration.

  Note: You may only specify either the VID or the IP Address for the source interface.

- **Use ICMP instead of UDP :**

  By default the traceroute command will use UDP datagrams. Selecting this option forces it to use ICMP ECHO packets instead.

- **Print Numeric Addresses :**

  By default the traceroute command will print out hop information using a reverse DNS lookup for the acquired host ip addresses. This may slow down the display if the DNS information is not available. Selecting this option will prevent the reverse DNS lookup and force the traceroute command to print numeric IP addresses instead.

Buttons

- **Start :**

  Click the "Start" button then the switch will start to ping the device using ICMPv6 packet size what set on the switch.

  After you press, Traceroute sends packets with gradually increasing TTL value, starting with TTL value of 1. The first router receives the packet, decrements the TTL value and drops the packet because it then has TTL value zero. The router sends an ICMP Time Exceeded message back to the source. The next set of packets are given a TTL value of 2, so the first router forwards the packets, but the second router drops them and replies with ICMP Time Exceeded. Proceeding in this way, traceroute uses the returned ICMP Time Exceeded messages to build a list of routers that packets traverse, until the destination is reached and returns an ICMP Echo Reply message.

  traceroute to 202.39.253.11 (202.39.253.11), 30 hops max, 40 byte packets
  1 192.168.10.254 ae-2-3508.edge4.Atlanta2.Level3.net. (192.168.10.254) 10 ms 10 ms 10 ms
  2 59-125-13-254.HINET-IP.hinet.net. (59.125.13.254) 20 ms 20 ms 20 ms
  3 h146.s228.ts.hinet.net. (168.95.228.146) 20 ms 10 ms 20 ms
  4 tchn-3011.hinet.net. (220.128.16.194) 20 ms TCHN-3112.hinet.net. (220.128.17.142) 20 ms tchn-3011.hinet.net. (220.128.16.202) 20 ms
  5 TPDT-3012.hinet.net. (220.128.17.6) 20 ms TPDT-3011.hinet.net. (220.128.16.10) 20 ms TPDT-3012.hinet.net. (220.128.17.6) 40 ms
  6 CHCH-3112.hinet.net. (220.128.2.13) 20 ms tchn-3011.hinet.net. (220.128.1.9) 10 ms CHCH-3112.hinet.net. (220.128.2.13) 30 ms
  7 211.22.41.237 CHCH-3112.hinet.net. (211.22.41.237) 20 ms 30 ms 30 ms
  8 202-39-253-11.HINET-IP.hinet.net. (202.39.253.11) 10 ms 10 ms

  You can configure the following properties:

4-4 Traceroute(IPv6)

This page allows you to perform a traceroute test over IPv6 towards a remote host. traceroute is a diagnostic tool for displaying the route and measuring transit delays of packets across an IPv6 network.

Web Interface

To configure an ICMPv6 PING Configuration in the web interface:

1. Click Diagnostic and Traceroute(IPv6)
2. Specify IP Addrss, DSCP Value and other parameters
3. Click Start.

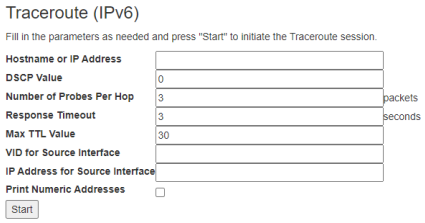


Figure 4-4: The Tracerout(IPv6)

Parameter description:

- **Hostname orIP Address:**

  The destination IP Address.

- **DSCP Value:**

  The destination IP Address. This value is used for the DSCP value in the IPv6 header. The default value is 0. The valid range is 0-63.

- **Number of Probes Per Hop :**

  Determines the number of probes (packets) sent for each hop. The default value is 3. The valid range is 1-60.

- **ResponseTimeout:**

  Determines the number of seconds to wait for a reply to a sent request. The default number is 3. The valid range is 1-86400.

- **Max TTL Value :**

  Determines the maximum value of the Time-To-Live (TTL) field in the IPv4 header. If this value is reached before the specified remote host is reached the test stops. The default number is 30. The valid range is 1-255.

- **VID for Source Interface :**

  This field can be used to force the test to use a specific local VLAN interface as the source interface. Leave this field empty for automatic selection based on routing configuration.

  Note: You may only specify either the VID or the IP Address for the source interface.

- **Address for Source Interface :**

This field can be used to force the test to use a specific local interface with the specified IP address as the source interface. The specified IP address must be configured on a local interface. Leave this field empty for automatic selection based on routing configuration.

Note: You may only specify either the VID or the IP Address for the source interface.

- **Print Numeric Addresses :**

  By default the traceroute command will print out hop information using a reverse DNS lookup for the acquired host ip addresses. This may slow down the display if the DNS information is not available. Selecting this option will prevent the reverse DNS lookup and force the traceroute command to print numeric IP addresses instead.

Buttons

- **Start :**

  Click the "Start" button then the switch will start to ping the device using ICMPv6 packet size what set on the switch.

  After you press, Traceroute sends packets with gradually increasing TTL value, starting with TTL value of 1. The first router receives the packet, decrements the TTL value and drops the packet because it then has TTL value zero. The router sends an ICMP Time Exceeded message back to the source. The next set of packets are given a TTL value of 2, so the first router forwards the packets, but the second router drops them and replies with ICMP Time Exceeded. Proceeding in this way, traceroute uses the returned ICMP Time Exceeded messages to build a list of routers that packets traverse, until the destination is reached and returns an ICMP Echo Reply message.

  traceroute to 202.39.253.11 (202.39.253.11), 30 hops max, 40 byte packets
  1 192.168.10.254 ae-2-3508.edge4.Atlanta2.Level3.net. (192.168.10.254) 10 ms 10 ms 10 ms
  2 59-125-13-254.HINET-IP.hinet.net. (59.125.13.254) 20 ms 20 ms 20 ms
  3 h146.s228.ts.hinet.net. (168.95.228.146) 20 ms 10 ms 20 ms
  4 tchn-3011.hinet.net. (220.128.16.194) 20 ms TCHN-3112.hinet.net. (220.128.17.142) 20 ms tchn-3011.hinet.net. (220.128.16.202) 20 ms
  5 TPDT-3012.hinet.net. (220.128.17.6) 20 ms TPDT-3011.hinet.net. (220.128.16.10) 20 ms TPDT-3012.hinet.net. (220.128.17.6) 40 ms
  6 CHCH-3112.hinet.net. (220.128.2.13) 20 ms tchn-3011.hinet.net. (220.128.1.9) 10 ms CHCH-3112.hinet.net. (220.128.2.13) 30 ms
  7 211.22.41.237 CHCH-3112.hinet.net. (211.22.41.237) 20 ms 30 ms 30 ms
  8 202-39-253-11.HINET-IP.hinet.net. (202.39.253.11) 10 ms 10 ms

  You can configure the following properties:

4-5 LINK OAM MIB Retrieval

4-5.1 MIB Retrieval

This page allows you to retrieve the local or remote OAM MIB variable data on a particular port. Select the appropriate radio button and enter the port number of the switch to retrieve the content of interest.

Web Interface

To configure an ICMPv6 PING Configuration in the web interface:

1. Click Diagnostics, LINK OAM and MIB Retrieval
2. Select local or peer
3. Select the port number
4. Click Start.

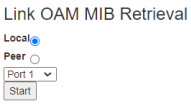


Figure 4-5.1: The Traceroute

Buttons

- **Start :**

  Click to retrieve the content

This page is used for running the VeriPHY Cable Diagnostics for copper ports.

Press Start to run the 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. Note that VeriPHY is only accurate for cables of length 7 - 140 meters.
10 and 100 Mbps ports will be linked down while running VeriPHY. Therefore, running VeriPHY on a 10 or 100 Mbps management port will cause the switch to stop responding until VeriPHY is complete.

Web Interface

To configure the VeriPHY Configuration in the web interface:

1. Click Diagnostics and VeriPHY
2. Select one port or all ports
3. Click start to run the process

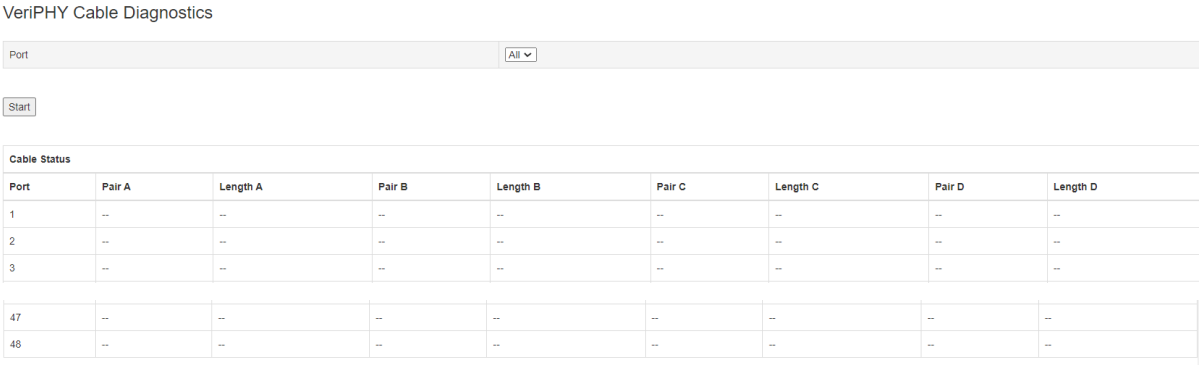


Figure 4-6: The VeriPHY

Parameter description:

- **Port :**

  The port where you are requesting VeriPHY Cable Diagnostics.

- **Cable Status :**

  Port:

  Port number.

  Pair:

  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:

The length (in meters) of the cable pair. The resolution is 3 meters

Buttons

- **Start :**

  Click the "Start" button then the switch will start to run VeriPHY cable diagnostics.

Chapter 5 Maintenance

This chapter describes the entire switch Maintenance configuration tasks to enhance the performance of local network including Restart Device, Firmware upgrade, Save/Restore, Import/Export.

5-1 Restart Device

This section describes how to restart switch for any maintenance needs. Any configuration files or scripts that you saved in the switch should still be available afterwards.

Web Interface

To configure a Restart Device Configuration in the web interface:

1. Click Maintenance and Restart Device.
2. Click Yes.

Figure 5-1: Restart Device

Parameter description:

Restart Device :

You can restart the switch on this page. After restart, the switch will boot normally.

Buttons

- **Yes :**

  Click to restart device

- **No :**

  Click to return to the Port State page without restarting.

5-2 Factory Defaults

You can reset the configuration of the switch on this page. Only the IP configuration is retained.
The new configuration is available immediately, which means that no restart is necessary.

Web Interface

To configure a Factory Defaults Configuration in the web interface:

1. Chick Maintenance and Factory Defaults.
2. Click Yes.

Figure 5-2: The Factory Defaults

Parameter description:

Buttons

- **Keep IP setup :**

  Check "Keep IP setup" if you want to keep current IP setting

- **Yes :**

  Click to reset the configuration to Factory Defaults.

- **No :**

  Click to return to the Port State page without restarting.

NOTE:
Restoring factory default can also be performed by making a physical loopback between port 1 and port 2 within the first minute from switch reboot. In the first minute after boot, 'loopback' packets will be transmitted at port 1. If a 'loopback' packet is received at port 2 the switch will do a restore to default

5-3 Firmware

This section describes how to upgrade Firmware. The Switch can be enhanced with more value-added functions by installing firmware upgrades.

5-3.1 Upload

This page facilitates an update of the firmware controlling the switch.

Web Interface

To configure a Firmware Upgrade Configuration in the web interface:

1. Click Maintenance, Firmware and Upload
2. Click Browser to select Maintenance/Software in you device.
3. Click upload

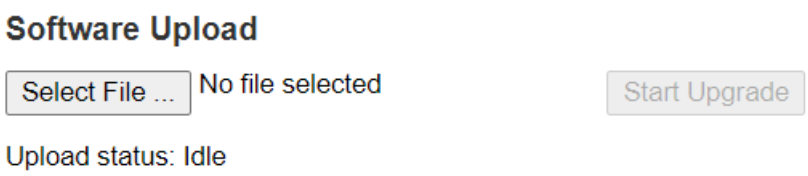


Figure 5-3.1: The firmware Download

Parameter description:

Buttons

- **Browse :**

  Click the "Browse..." button to search the Firmware URL and filename and click "Upload".

NOTE: This page facilitates an update of the firmware controlling the switch. Uploading software will update all managed switches to the location of a software image and click. After the software image is uploaded, a page announces that the firmware update is initiated. After about a minute, the firmware is updated and all managed switches restart. the switch restarts.

WARNING: While the firmware is being updated, Web access appears to be defunct. The front LED flashes Green/Off with a frequency of 10 Hz while the firmware update is in progress. Do not restart or power off the device at this time or the switch may fail to function afterwards.

- **Browse :**

  Click to start upgrade

5-3.2 Image Select

This page provides information about the active and alternate (backup) firmware images in the device, and allows you to revert to the alternate image.

The web page displays two tables with information about the active and alternate firmware images.

NOTE: In case the active firmware image is the alternate image, only the "Active Image" table is shown. In this case, the Activate Alternate Image button is also disabled.

If the alternate image is active (due to a corruption of the primary image or by manual intervention), uploading a new firmware image to the device will automatically use the primary image slot and activate this.

The firmware version and date information may be empty for older firmware releases. This does not constitute an error.

Web Interface

To configure a Firmware Upgrade Configuration in the web interface:

1. Click Maintenance, Firmware and Image Select
2. Click Activate Alternate Image to ative the alternative image
3. Click Cancel to cancel to operation

Figure 5-3.2: The Image Select

Parameter description:

Image Information

- **Image :**

  The flash index name of the firmware image. The name of primary (preferred) image is image, the alternate image is named image.bk.

- **Version :**

  The version of the firmware image.

- **Date :**

The date where the firmware was produced.

Buttons

- **Activate Alternate Image :**

  Click to use the "Activate Alternate Image". This button may be disabled depending on system state.

- **Cancel :**

  Cancel activating the backup image. Navigates away from this page.

5-4 Configuration

The switch stores its configuration in a number of text files in CLI format. The files are either virtual (RAM-based) or stored in flash on the switch.

There are three system files:

- running-config: A virtual file that represents the currently active configuration on the switch. This file is volatile.
- startup-config: The startup configuration for the switch, read at boot time.
- default-config: A read-only file with vendor-specific configuration. This file is read when the system is restored to default settings.

It is also possible to store up to two other files and apply them to running-config, thereby switching configuration.

5-4.1 Save startup-config

This copies running-config to startup-config, thereby ensuring that the currently active configuration will be used at the next reboot.

Web Interface

To save running configuration in the web interface:

1. Chick Browser to select Maintenance/Configuration in you device.
2. Click Apply Startup-Config Select.

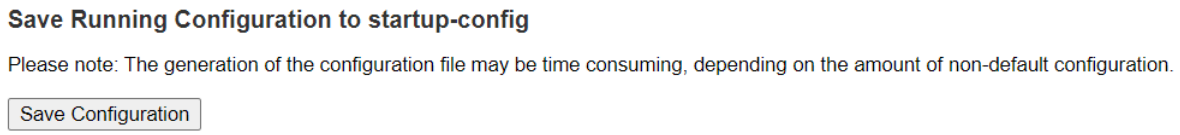


Figure 5-4.1: The Save Startup Configuration

Parameter description:

Buttons

- **Save Configuration:**

  Click to save configuration, the running configuration will be written to flash memory for system boot up to load this startup configuration file.

This section describes to export the Switch Configuration for maintenance needs. Any current configuration files will be exported as text format.

It is possible to download a file from the web browser to all the files on the switch, except default-config, which is read-only.

Select the file to download, select the destination file on the target, and click.

If the destination is running-config, the file will be applied to the switch configuration. This can be done in two ways:

- Replace mode: The current configuration is fully replaced with the configuration in the downloaded file.
- Merge mode: The downloaded file is merged into running-config.

If the file system is full (i.e. contains the three system files mentioned above plus two other files), it is not possible to create new files, but an existing file must be overwritten or another deleted first.

Web Interface

To download configuration in the web interface:

1. Chick Browser to select Maintenance/Configuration in you device.
2. Click Download Select.

Figure 5-4.2: Configuration Download

Parameter description:

Buttons

- **Download :**

  Click the “Download” button then the switch will start to download the configuration from configuration stored location PC or Server.

5-4.3 Upload

The configuration upload function will be backuped and saved configuration from the switch's configuration into the running web browser PC.

It is possible to upload any of the files on the switch to the web browser. Select the file and click Upload of running-config may take a little while to complete, as the file must be prepared for upload.

Web Interface

To upload configuration in the web interface:

1. Chick Browser to select Maintenance/Configuration in you device.
2. Click upload Select.

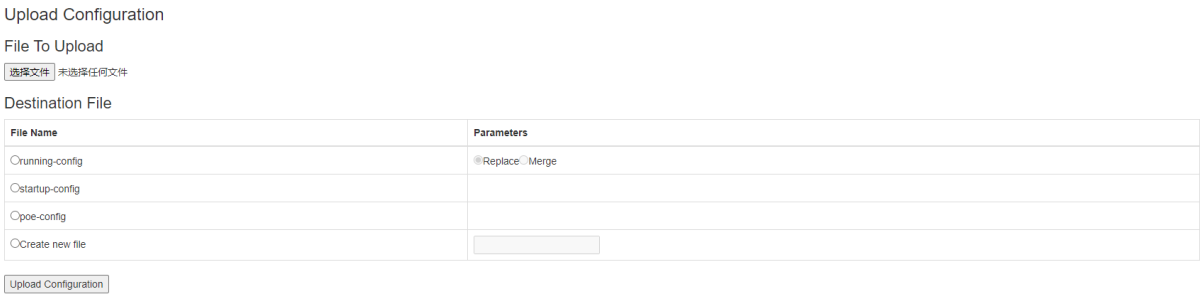


Figure 5-4.3: Configuration upload

Parameter description:

- **running-config :**

  the file will be applied to the switch configuration. This can be done in two ways:

  Replace mode: The current configuration is fully replaced with the configuration in the uploaded file.

  Merge mode: The uploaded file is merged into running-config.

- **startup-config :**

  The startup configuration for the switch, read at boot time.

- **default-config :**

  A read-only file with vendor-specific configuration. This file is read when the system is restored to default settings.

Buttons

- **Upload Configuration :**

  Click the "Upload" button then the running web management PC will start to upload the configuration from the managed switch configuration into the location PC, user can configure web browser's upload file path to keep configuration file.

5-4.4 Activate

It is possible to activate any of the configuration files present on the switch, except for running-config which represents the currently active configuration.

Select the file to activate and click. This will initiate the process of completely replacing the existing configuration with that of the selected file.

Web Interface

To activate configuration in the web interface:

1. Chick Browser to select Maintenance/Configuration in you device.
2. Click Activate Select.

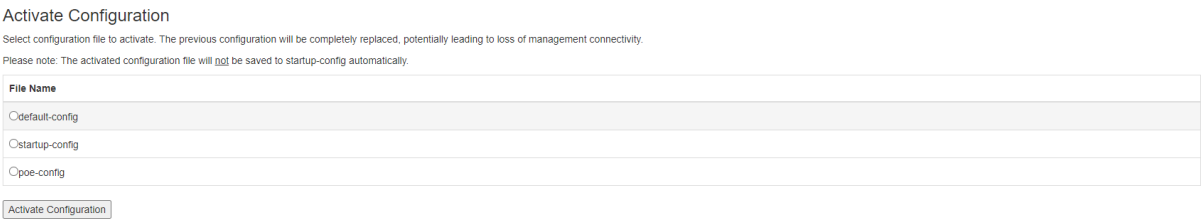


Figure 5-4.4: Configuration Activation

Parameter description:

- **default-config :**

  A read-only file with vendor-specific configuration. This file is read when the system is restored to default settings.

Buttons

- **Activate Configuration :**

  Click the “Activate” button then the default-config or startup-config file will be activated and to be this switch's running configuration.

5-4.5 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.

Web Interface

To delete configuration in the web interface:

1. Chick Browser to select Maintenance/Configuration in you device.
2. Click Delete Select.

Figure 5-4.5: Delete Configuration

Parameter description:

Buttons

- **Delete Configuration :**

  Click the "Delete" button then the startup-config file will be deleted, this effectively resets the switch to default configuration.