SOFTWARE USER MANUAL

Version: 6.X
Date: March 2021
(Compact)

Leonton is a worldwide industrial networking communication manufacturer providing high-quality custom design product solutions. Located in Taiwan, Leonton has been a customer-centric company offering exceptional service and superb product quality inspections since its founding in 2012. We are recognized in the industry for our outstanding industrial networking product lines of industrial Ethernet switches and media converters. Leonton's superior product design capability allows for a quick and flawless time to market process. We are proud of our ability to manage and customize any project requiring a specific product to meet and exceed customer expectations.

+886-2-2218-3113
info@leonton.com
www.leonton.com

Disclaimer

Leonton Technologies, Co. Ltd. provides this manual without warranty of any kind, expressed or implied, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. Leonton Technologies, Co. Ltd. may make improvements and/or changes to the product and/or specifications of the product described in this manual, without prior notice. Leonton Technologies, Co. Ltd. will not be liable for any technical inaccuracies or typographical errors found in this guide. Changes are periodically made to the information contained herein and will be incorporated into later versions of the manual. The information contained is subject to change without prior notice.

Software Manual 6.x

Version 1.0 (March 2021)

This manual applies to firmware version 6.0 on the following products:

BT Compact Model Series
CBG5-0602-SFP(-T)
CEG5-0602-SFP(-T)

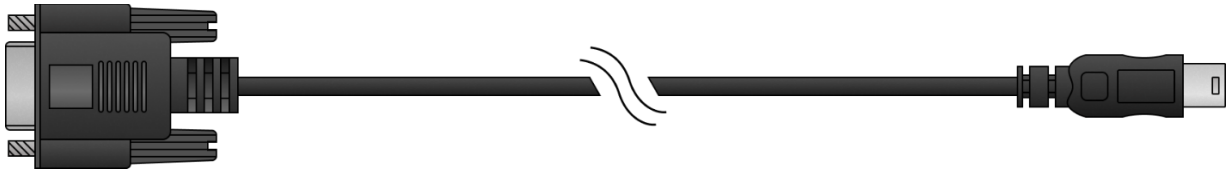
CONTENT

CLI Management

Configuration by serial console

LEONTON Ethernet switches supports CLI management. You can use console or telnet to manage the switch by CLI.

Before configuring RS-232 serial console, connect the RS-232 port of the switch to your PC Com port using a RJ45 to DB9-Female cable.



1. Connect your PC to the switches' Console port.
2. Launch the serial terminal program.
3. Configure the port settings of the serial terminal program to match the console port:
   - 115200 baud
   - 8 data bits
   - No parity
   - 1 stop bit
   - No flow control
4. The administrator username/ password are admin/admin by default. Enter the username and password to login the serial console.

```
Press ENTER to get started

Username: admin
Password:
# configure terminal
```

Configuration by Telnet console

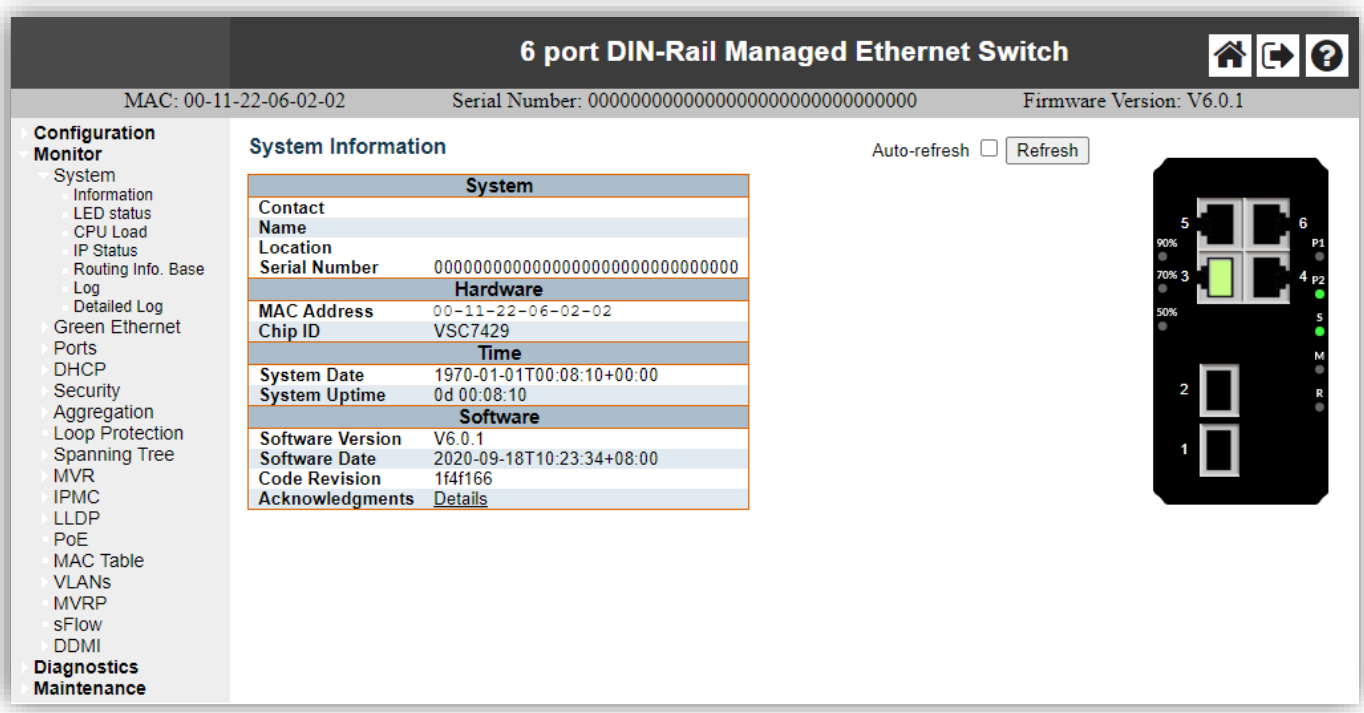
1. Connect your PC and the switches on the same logical subnetwork.
2. Launch the Telnet program.
3. Configure the switches default settings of the Telnet program:
   - **IP Address:** 192.168.1.254
   - **Subnet Mask:** 255.255.255.0
   - **Default Gateway:** none
4. The administrator username/ password are admin/admin by default. Enter the username and password to login the Telnet console.

```
Press ENTER to get started

Username: admin
Password:
# configure terminal
```

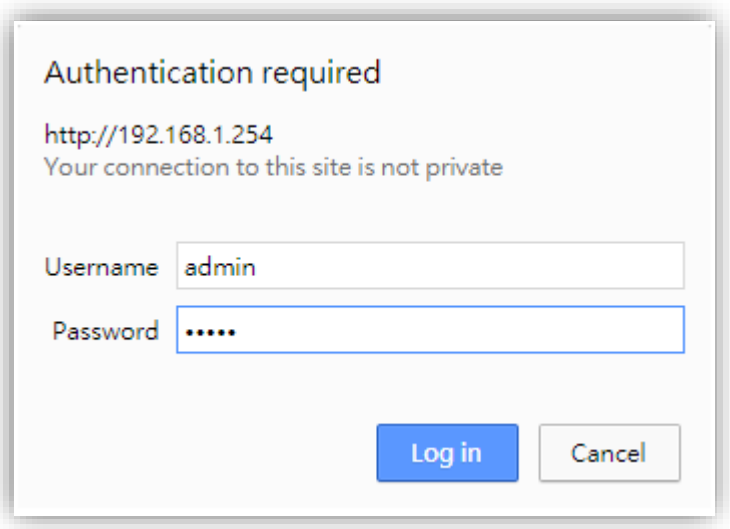
Web Management

Besides CLI-based management, LEONTON Ethernet switches also supports Web-based management. This section describes the Web console interface for a series Industrial Management Switch. This is a **user friendly** design with advanced management features that allow you to manage switches through Internet browser.



Connecting to the Web Console Interface

1. Initiate a connection from a browser to the default IP address: http://192.168.1.254 The Login page appears.
2. The administrator username/password is admin/admin by default. Enter the username and password and then click the Login button.



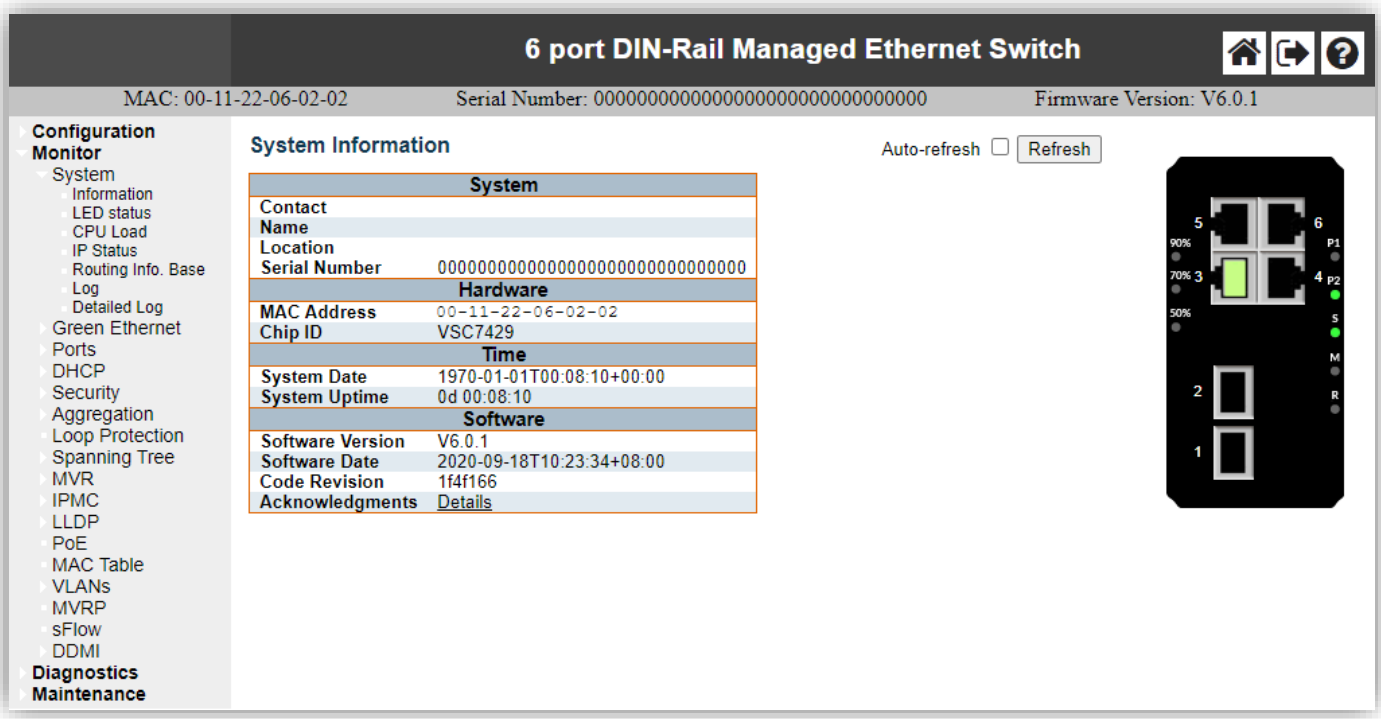
NOTE	Make sure that the PC and Switches are on the same logical subnetwork.

Monitor

Configuration > System > Information

- **Switch State Overview**

When logged into the Web GUI Interface, Switch State Overview page provides an overview of the current switch system and port states.



- **System Status**

LED	Color		Description
P1, P2	Green	On	Power input 1/2 is active
		Off	Power input 1/2 is inactive
STATUS	Green	On	Operating normal
		Off	Power off
		Flashing	Device initialization
	Red	On	Fault Alarm is set and the condition is inactive
MASTER	Green	On	ERPS Owner Mode (Ring Master) is ready
		Off	ERPS Owner Mode is not active
RING	Green	On	Ring Network is active and works well
		Off	Ring Network is inactive
		Flashing	Ring Network works abnormally or misconfigure
PoE Load	-	Off	PoE Load ≤ 50%
	Blue	On	PoE Load 51-70%
	Red	On	PoE Load 71-90%
	Red	Flashing	PoE Load 91-100%

- **Port Status**

Port	State		
RJ45	 Disabled	 Down	 Link
SFP	 Disabled	 Down	 Link

- **Check Box**

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

- **Buttons**

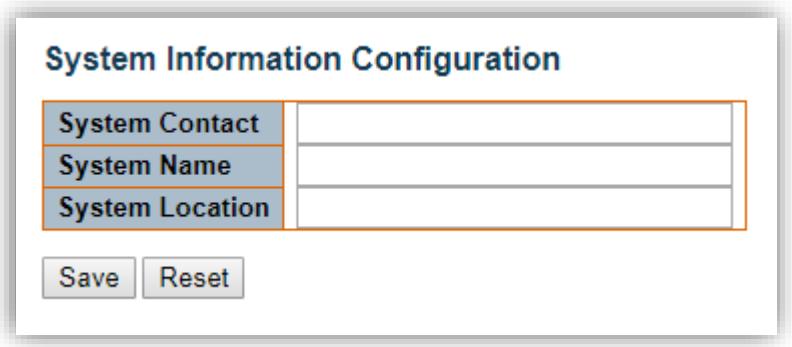
Button	Description
Refresh	Click to refresh the page.

Configuration

Configuration > System > Information

- **System Information Configuration**

The switch system information is provided here.



- **System Contact**

Setting	Description	Factory Default
Max. 255 Characters	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 255, and the allowed content is the ASCII characters from 32 to 126.	None

- **System Name**

Setting	Description	Factory Default
Max. 255 Characters	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-Z, a-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 255.	None

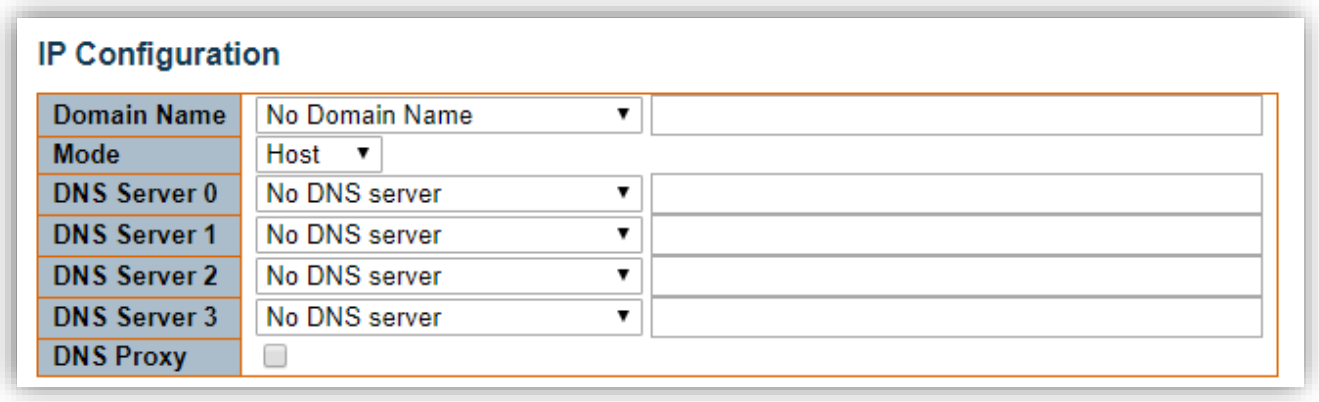
- **System Location**

Setting	Description	Factory Default
Max. 255 Characters	The physical location of this node(e.g., telephone closet, 3rd floor). The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.	None

Configuration > System > IP

- **IP Configuration**

Configure IP basic settings, control IP interfaces and IP routes.
The maximum number of interfaces supported is 8 and the maximum number of routes is 32.



Domain Name
The name string of local domain where the device belongs.
Most queries for names within this domain can use short names relative to the local domain. The system then appends the domain name as a suffix to unqualified names.
For example, if domain name is set as 'example.com' and you specify the PING destination by the unqualified name as 'test', then the system will qualify the name to be 'test.example.com'.

Setting	Description	Factory Default
No Domain Name	No domain name will be used.	No Domain Name
Configured Domain Name	Explicitly specify the name of local domain. Make sure the configured domain name meets your organization's given domain.	
From any DHCPv6 interfaces	The first domain name offered from a DHCPv6 lease to a DHCPv6-enabled interface will be used.	
From this DHCPv6 interface	Specify from which DHCPv6-enabled interface a provided domain name should be preferred.	

Mode
Configure whether the IP stack should act as a Hostor a Router.

Setting	Description	Factory Default
Host	IP traffic between interfaces will not be routed.	Host
Router	IP traffic is routed between all interfaces.	

DNS Server

This setting controls the DNS name resolution done by the switch. There are four servers available for configuration, and the index of the server presents the preference (less index has higher priority) in doing DNS name resolution. System selects the active DNS server from configuration in turn, if the preferred server does not respond in five attempts.

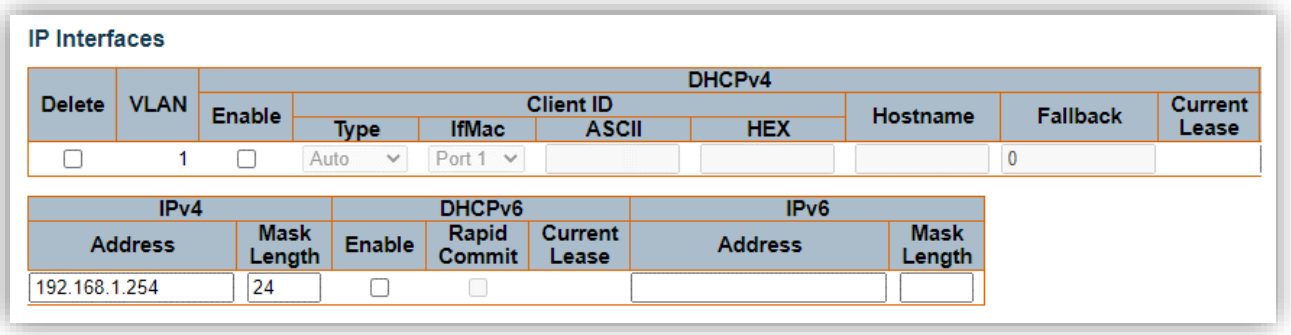
Setting	Description	Factory Default
From any DHCPv4 interfaces	The first DNS server offered from a DHCPv4 lease to a DHCPv4-enabled interface will be used.	No DNS server
No DNS server	No DNS server will be used.	
Configured IPv4	Explicitly provide the valid IPv4 unicast address of the DNS Server in dotted decimal notation. Make sure the configured DNS server could be reachable (e.g. via PING) for activating DNS service.	
From this DHCPv4 interface	Specify from which DHCPv4-enabled interface a provided DNS server should be preferred.	
Configured IPv6	Explicitly provide the valid IPv6 unicast (except linklocal) address of the DNS Server. Make sure the configured DNS server could be reachable (e.g. via PING6) for activating DNS service.	
From this DHCPv6 interface	Specify from which DHCPv6-enabled interface a provided DNS server should be preferred.	
From any DHCPv6 interfaces	The first DNS server offered from a DHCPv6 lease to a DHCPv6-enabled interface will be used.	

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. Only IPv4 DNS proxy is now supported.

- **IP Interfaces**

Click the **Add Interface** button to add a new IP interface. A maximum of 8 interfaces is supported.

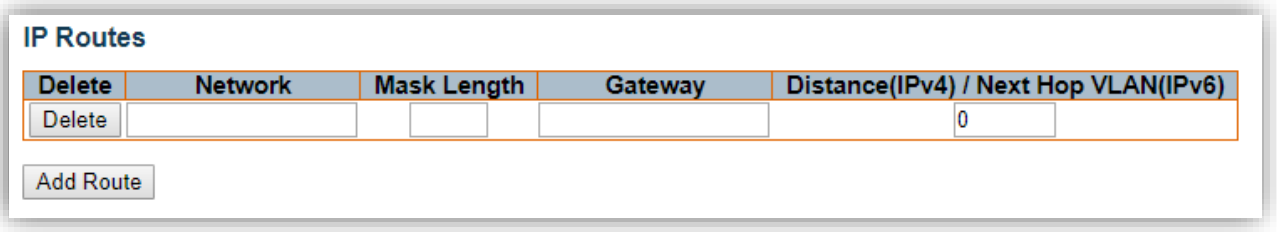


Setting	Description
Delete	Select this option to delete an existing IP interface.
VLAN	The VLAN associated with the IP interface. Only ports in this VLAN will be able to access the IP interface. This field is only available for input when creating a new interface.
IPv4 DHCP Enabled	Enable the DHCPv4 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. The DHCPv4 client will announce the configured System Name as hostname to provide DNS lookup.
IPv4 DHCP Client Identifier Type	The type of DHCP client identifier. User can choose Auto, ifmac, ASCII, and HEX.
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	For DHCPv6 interface with an active lease, this column shows the interface address provided by the DHCPv6 server.
IPv6 Address	The IPv6 address of the interface. A IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, fe80::215:c5ff:fe03:4dc7. The symbol :: is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. System accepts the valid IPv6 unicast address only, except IPv4-Compatible address and IPv4-Mapped address. The field may be left blank if IPv6 operation on the interface is not desired.
IPv6 Mask	The IPv6 network mask, in number of bits (prefix length). Valid values are between 1 and 128 bits for a IPv6 address. The field may be left blank if IPv6 operation on the interface is not desired.

- **IP Routes**

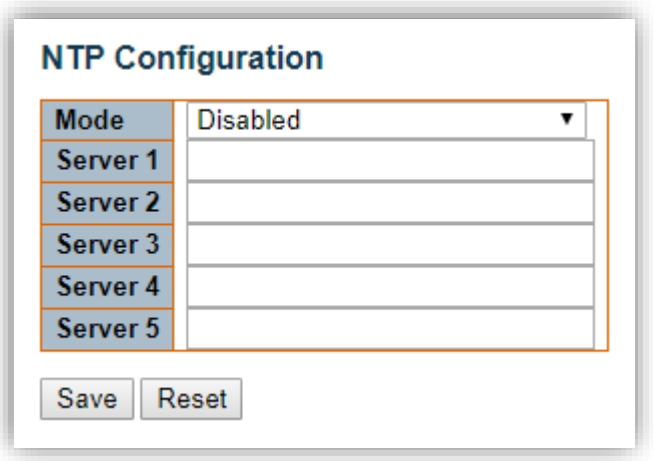
Click the **Add Route** button to add a new IP route. A maximum of 32 routes is supported.



Setting	Description
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 **0.0.0.0** or IPv6 **::** notation.
Mask Length	The destination IP network or host mask, in number of bits (prefix length). It defines how much of a network address that must match, in order to qualify for this route. Valid values are between 0 and 32 bits respectively 128 for IPv6 routes. Only a default route will have a mask length of **0** (as it will match anything).
Gateway	The IP address of the IP gateway. Valid format is dotted decimal notation or a valid IPv6 notation. Gateway and Network must be of the same type.
Distance (Only for IPv4)	The distance value of route entry is used to provide the priority information of the routing protocols to routers. When there are two or more different routing protocols are involved and have the same destination, the distance value can be used to select the best path.
Next Hop VLAN (Only for IPv6)	The VLAN ID (VID) of the specific IPv6 interface associated with the gateway. The given VID ranges from 1 to 4095 and will be effective only when the corresponding IPv6 interface is valid. If the IPv6 gateway address is link- local, it must specify the next hop VLAN for the gateway. If the IPv6 gateway address is not link-local, system ignores the next hop VLAN for the gateway.

Configuration > System > NTP

- **NTP Configuration**



Mode

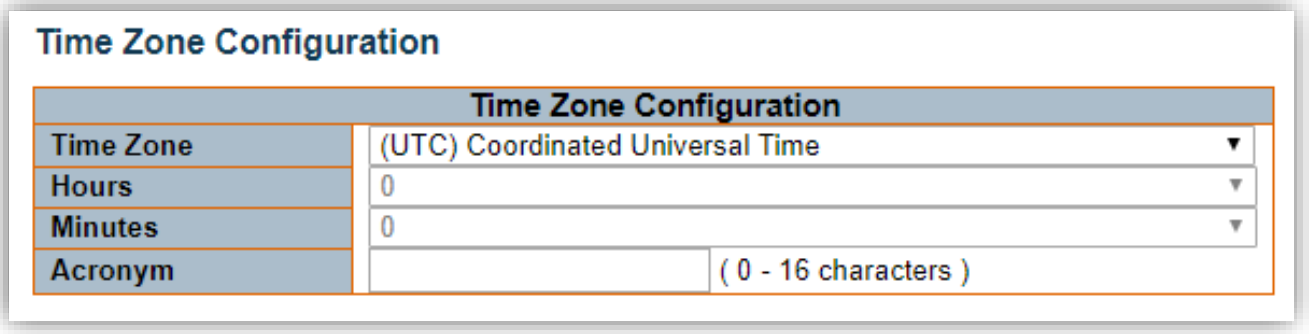
Setting	Description	Factory Default
Enabled	Enable NTP client mode operation.	Disabled
Disabled	Disable NTP client mode operation.	

Server

Setting	Description	Factory Default
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.	None

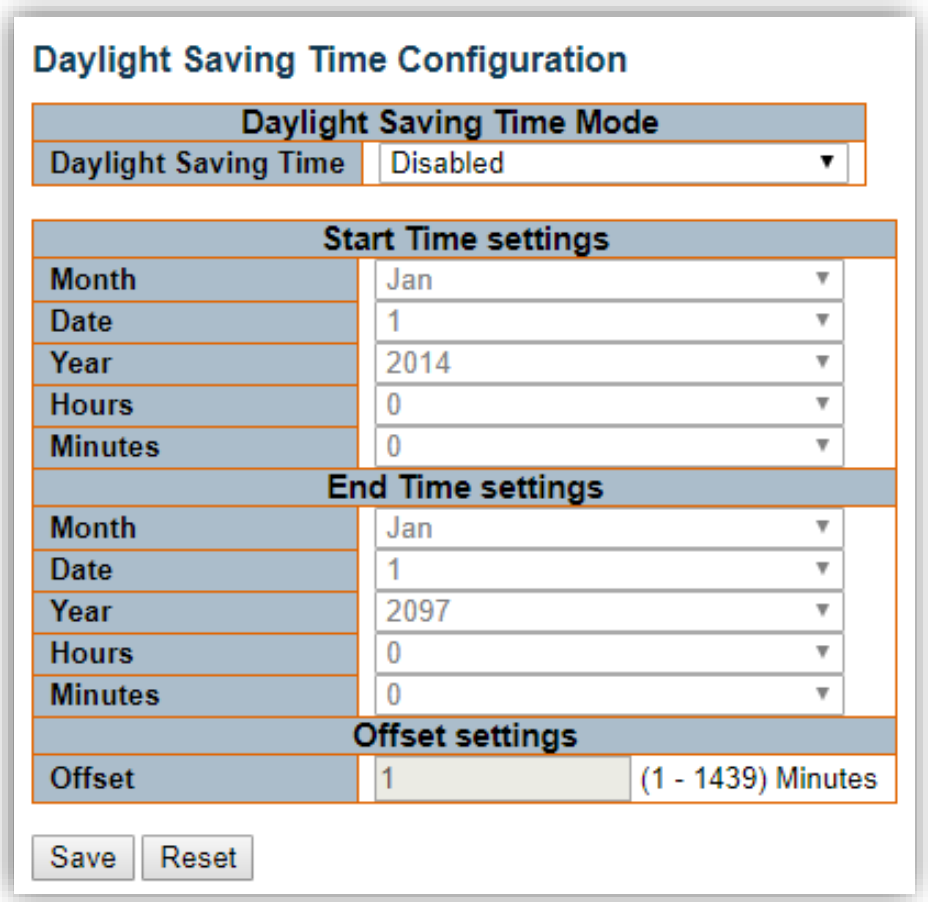
Configuration > System > Time

- **Time Zone Configuration**



Setting	Description	Factory Default
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.	UTC
Hours	Number of hours offset from UTC. The field only available when time zone manual setting.	0
Minutes	Number of minutes offset from UTC. The field only available when time zone manual setting.	0
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.	None

- **Daylight Saving Time Configuration**



Daylight Saving Time Mode

Setting	Description	Factory Default
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.	Disabled

Start time settings
Select the starting Month, Date, Year, Hours and Minutes.

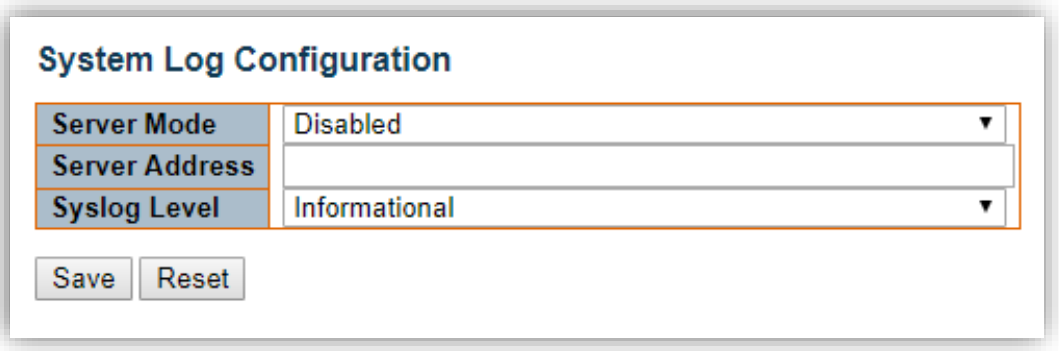
End time settings
Select the ending Month, Date, Year, Hours and Minutes.

Offset settings

Setting	Description	Factory Default
Offset	Enter the number of minutes to add during Daylight Saving Time. (Range: 1 to 1439)	1

Configuration > System > Log

- **System Log Configuration**



Server Mode
Indicates 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.

Setting	Description	Factory Default
Enabled	Enable server mode operation.	Disabled
Disabled	Disable server mode operation.	

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

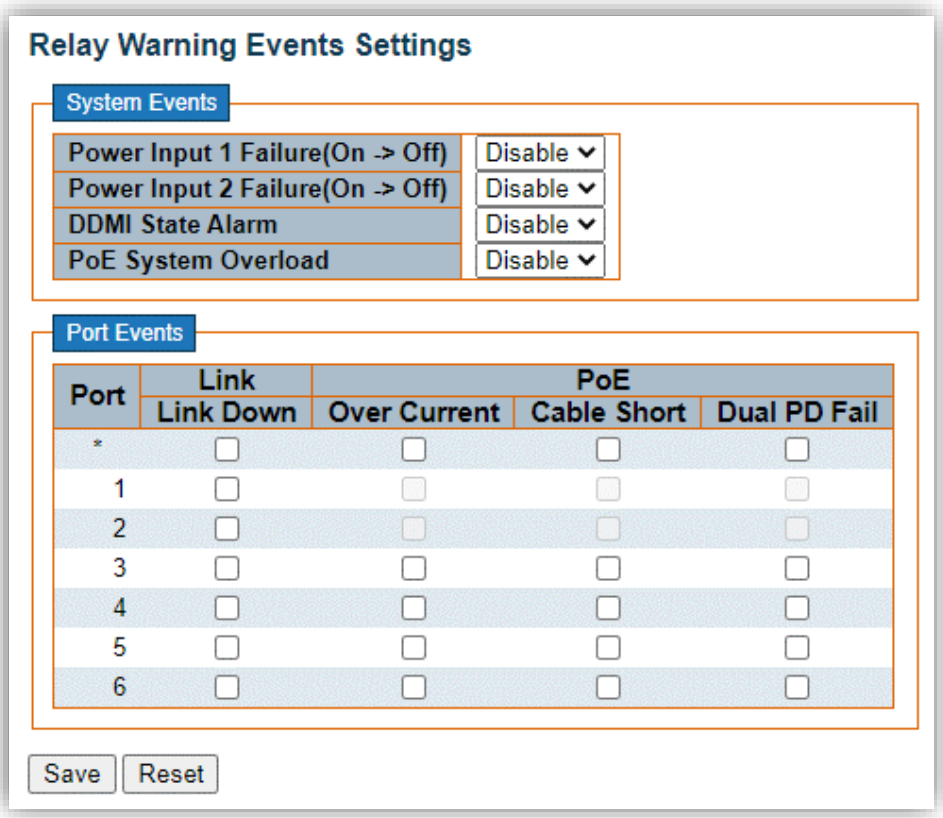
Syslog Level
Indicates what kind of message will send to syslog server.

Setting	Description	Factory Default
Error	Send the specific messages which severity code is less or equal than Error(3).	Informational
Warning	Send the specific messages which severity code is less or equal than Warning(4).	
Notice	Send the specific messages which severity code is less or equal than Notice(5).	
Informational	Send the specific messages which severity code is less or equal than Informational(6).	

Configuration > System > Event Warning > Relay

- **Relay Warning Events Settings**

The Relay Warning function uses relay output to alert the user when certain user-configured events take place.



System Events

Power Failure Events

Indicates power down mode operation. Warning Relay output is triggered when switch is powered down.

Setting	Description	Factory Default
Enabled	Enable power failure event mode operation.	Disabled
Disabled	Disable power failure event mode operation.	

DDMI State Alarm

Indicates the SFP DDMI information alarm operation. Warning Relay output is triggered when switch SFP DDMI current value exceeds the alarm threshold.

* DDMI function only supported by the SFP model.

Setting	Description	Factory Default
Enabled	Enable DDMI information alerts.	Disabled
Disabled	Disable DDMI information alerts.	

PoE System Overload

Indicates the total PoE power budget. Warning Relay output is triggered when the total PoE power budget is overload.

Setting	Description	Factory Default
Enabled	Enable the PoE system overload event.	Disabled
Disabled	Disable the PoE system overload event.	

Port Events

Port Link Status Events

Indicates the port link status operation. Warning Relay output is triggered when the port is linkdown.

Setting	Description
Link Down	Controls whether port link down event warning is enabled on this switch port.

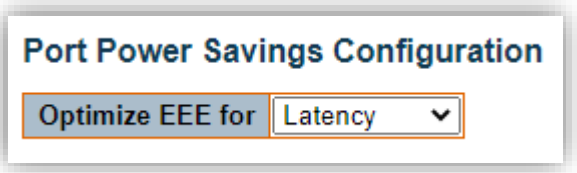
Port PoE Status Events

Indicates the port link status and PoE status operation. Warning Relay output is triggered when the port is linkdown or the configured PoE events occur.

Setting	Description
Over Current	Controls whether PoE over current event warning is enabled on this switch port.
Cable Short	Controls whether PoE cable short event warning is enabled on this switch port.
Dual PD Fail	Controls whether the dual PD fail event warning of the BT port is enabled (when the Dual PD check is disabled only).

Configuration > Green Ethernet > Port Power Savings

- **Port Power Saving Configuration**



What is EEE

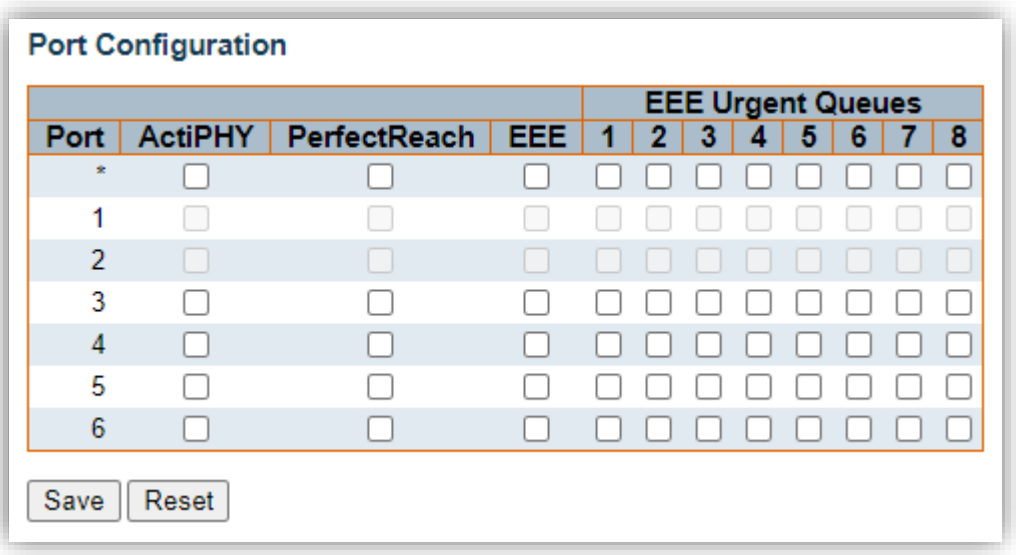
EEE is a power saving option that reduces the power usage when there is low or no traffic utilization.
EEE works by powering down circuits when there is no traffic. When a port gets data to be transmitted all circuits are powered up. The time it takes to power up the circuits is named wakeup time. The 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.

Optimize EEE for

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

Setting	Description	Factory Default
Power	Best power saving	Latency
Latency	Least traffic latency	

- **Port Configuration**

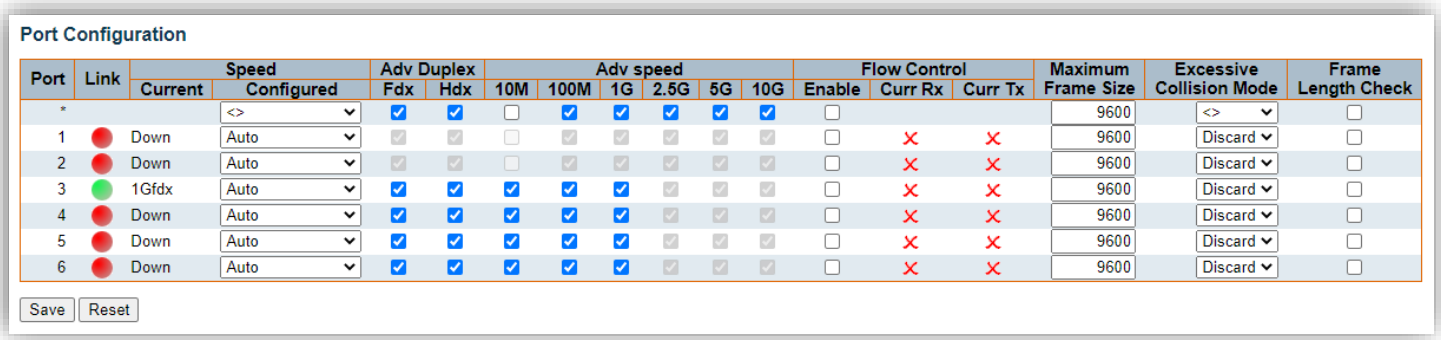


Setting	Description
Port	The switch port number of the logical port.
ActiPHY	Link down power savings enabled. ActiPHY works by lowering the power for a port when there is no link. The port is power up for short moment in order to determine if cable is inserted.
PerfectReach	Cable length power savings enabled. PerfectReach works by determining the cable length and lowering the power for ports with short cables.
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.

Configuration > Ports

● Port Configuration

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



Port

This is the logical port number for this row.

Link

The current link state is displayed graphically.

Color	Description
Green	Link is up.
Red	Link is down.

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.

Setting	Description	Factory Default
Disabled	Disables the switch port operation.	Auto
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.	
5Gbps FDX	Forces the Serdes port in 5Gbps full duplex mode.	
10Gbps FDX	Forces the Serdes port in 10Gbps full duplex mode.	
SFP_Auto	Automatically determines the speed of the SFP. **Note:** There is no standardized way to do SFP auto detect, so here it is done by reading the SFP rom. Due to the missing standardized way of doing SFP auto detect some SFPs might not be detectable.	
100-FX	SFP port in 100-FX speed.	
1000-X	SFP port in 1000-X speed.	

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.

NOTE	The 100FX standard doesn't support Auto Negotiation, so when in 100FX mode the flow control capabilities will always be shown as disabled.

Maximum Frame Size

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

Excessive Collision Mode
Configure port transmit collision behavior.

Setting	Description	Factory Default
Discard	Discard frame after 16 collisions.	Discard
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).

Setting	Description	Factory Default
Checked	Frames with payload size less than 1536 bytes are dropped, if the EtherType/Length field doesn't match the actually payload length.	Unchecked
Unchecked	Frames are not dropped due to frame length mismatch.	

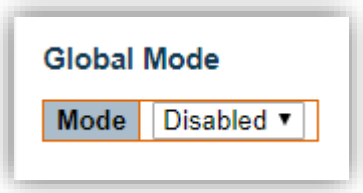
NOTE	No drop counters count frames dropped due to frame length mismatch.

Configuration > DHCP > Server > Mode

- **DHCP Server Mode Configuration**

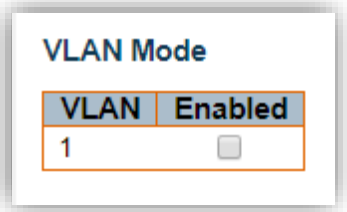
This page configures global mode and VLAN mode to enable/disable DHCP server per system and per VLAN.

Global Mode



Setting	Description	Factory Default
Enabled	Enable DHCP server per system.	Disabled
Disabled	Disable DHCP server per system.	

VLAN Mode



Mode

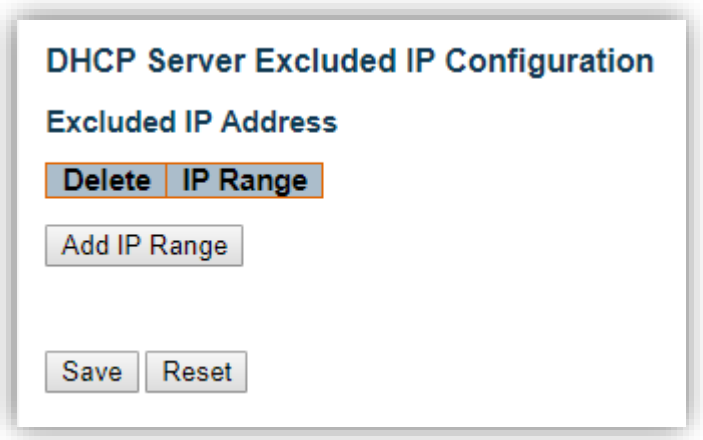
Setting	Description	Factory Default
Checked	Enable DHCP server per VLAN n.	Unchecked
Unchecked	Disable DHCP server per VLAN n.	

Configuration > DHCP > Server > Excluded IP

- **DHCP Server Excluded IP Configuration**

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

Excluded IP Address



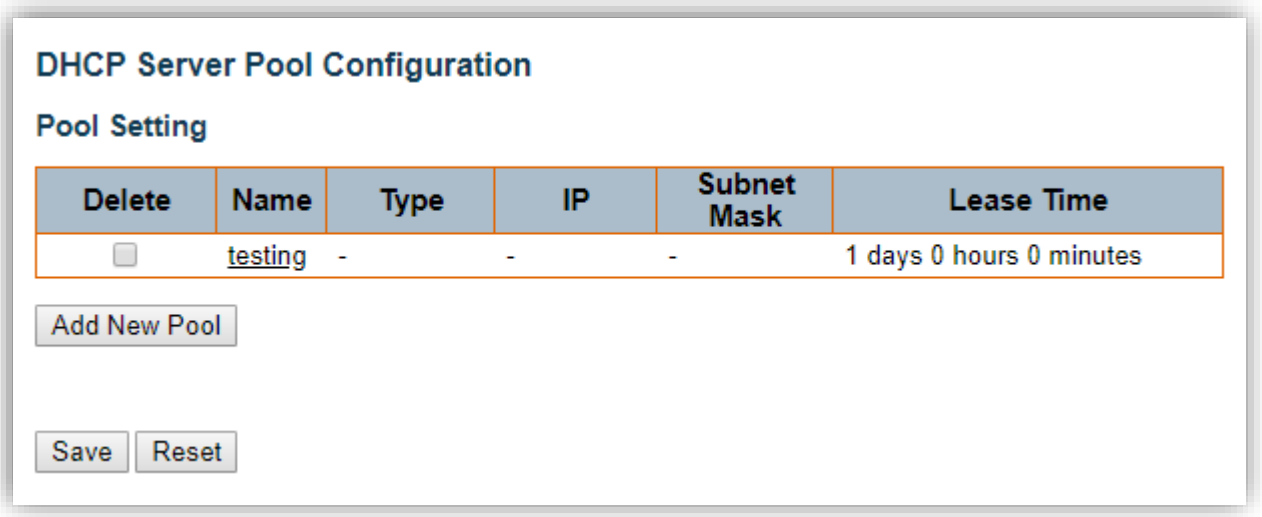
IP Range

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.

Configuration > DHCP > Server > Pool

- **DHCP Server Pool Configuration**

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



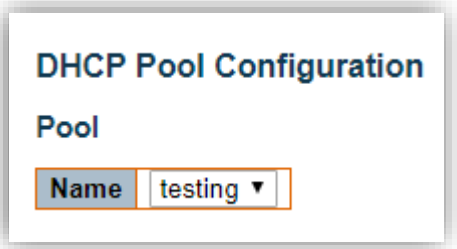
Pool Setting

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.

Setting	Description
Name	Configure the pool name that accepts all printable characters, except white space. If you want to configure the detail settings, you can click the pool name to go into the configuration page.
Type	Display which type of the pool is. **Network:** the pool defines a pool of IP addresses to service more than one DHCP client. **Host:** the pool services for a specific DHCP client identified by client identifier or hardware address. If - is displayed, it means not defined.
IP	Display network number of the DHCP address pool. If - is displayed, it means not defined.
Subnet Mask	Display subnet mask of the DHCP address pool. If - is displayed, it means not defined.
Lease Time	Display lease time of the pool.

- **Pool Setting Configuration page**

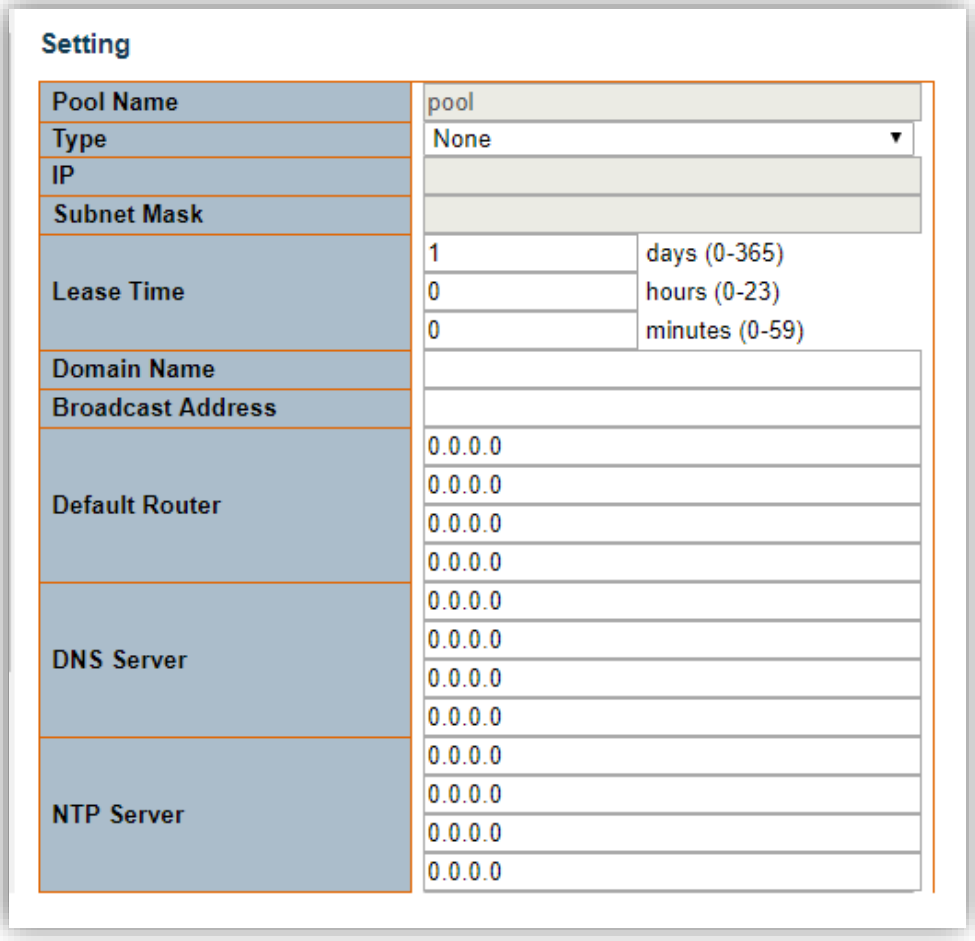
Pool

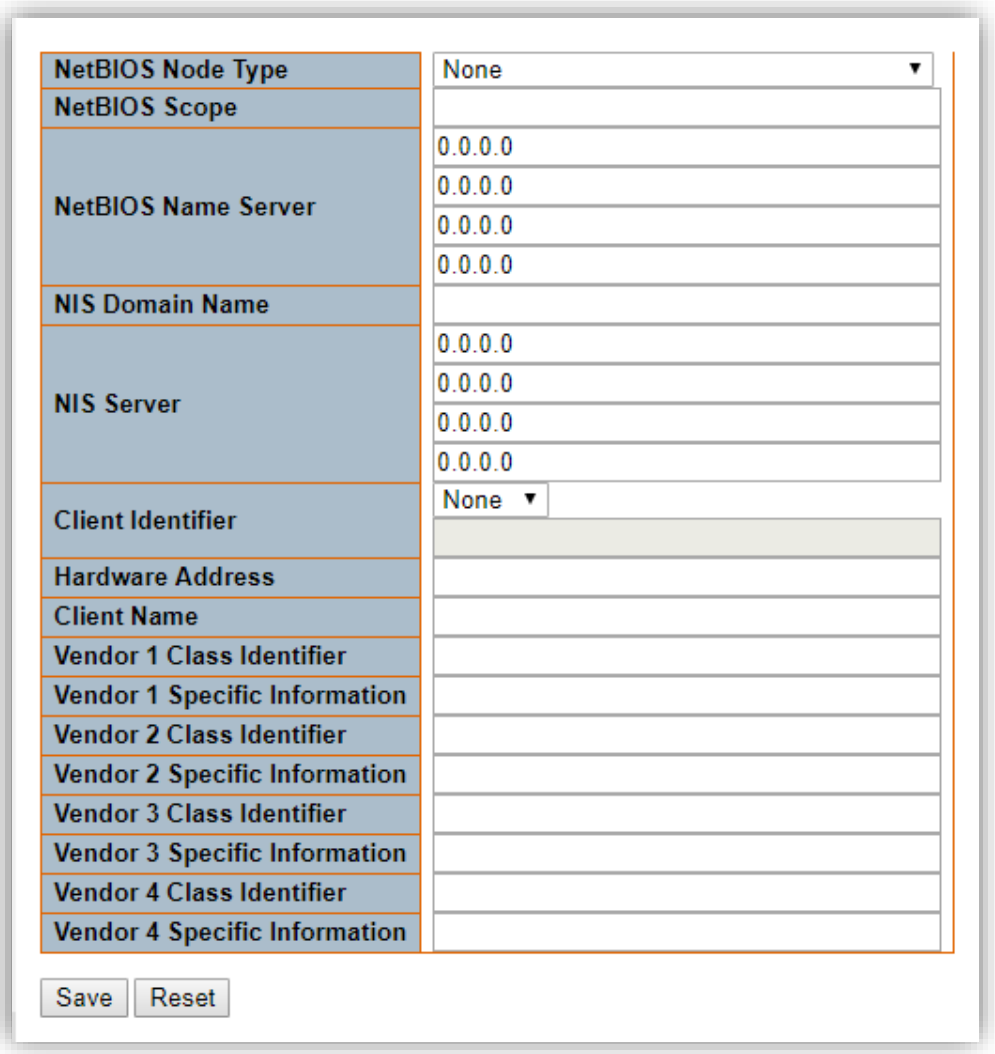


Pool

Setting	Description
Name	Select a pool by pool name.

Setting



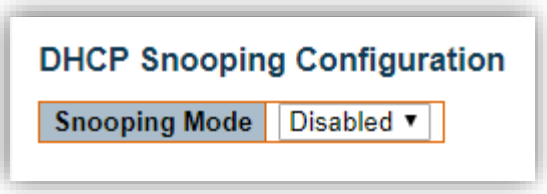


Setting	Description
Name	Display the selected pool name.
Type	Specify which type of the pool is. **Network:** the pool defines a pool of IP addresses to service more than one DHCP client. **Host:** the pool services for a specific DHCP client identified by client identifier or hardware address.
IP	Specify network number of the DHCP address pool.
Subnet Mask	Specify subnet mask of the DHCP address pool.
Lease Time	Specify lease time that allows the client to request a lease time for the IP address. If all are 0's, then it means the lease time is infinite.
Domain Name	Specify domain name that client should use when resolving hostname via DNS.
Broadcast Address	Specify the broadcast address in use on the client's subnet.
Default Router	Specify a list of IP addresses for routers on the client's subnet.
DNS Server	Specify a list of Domain Name System name servers available to the client.
NTP Server	Specify a list of IP addresses indicating NTP servers available to the client.
NetBIOS Node Type	Specify NetBIOS node type option to allow Netbios over TCP/IP clients which are configurable to be configured as described in RFC 1001/1002.
NetBIOS Scope	Specify the NetBIOS over TCP/IP scope parameter for the client as specified in RFC 1001/1002.

NetBIOS Name Server	Specify a list of NBNS name servers listed in order of preference.
NIS Domain Name	Specify the name of the client's NIS domain.
NIS Server	Specify a list of IP addresses indicating NIS servers available to the client.
Client Identifier	Specify client's unique identifier to be used when the pool is the type of host.
Hardware Address	Specify client's hardware (MAC) address to be used when the pool is the type of host.
Client Name	Specify the name of client to be used when the pool is the type of host.
Vendor # Class Identifier	Specify to be used by DHCP client to optionally identify the vendor type and configuration of a DHCP client. DHCP server will deliver the corresponding option 43 specific information to the client that sends option 60 vendor class identifier.
Vendor # Specific Information	Specify vendor specific information according to option 60 vendor class identifier.

Configuration > DHCP > Snooping

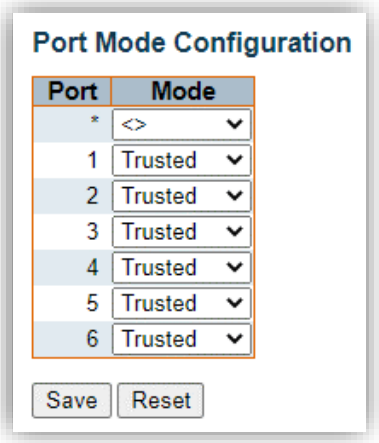
- **DHCP Snooping Configuration**



Snooping Mode

Setting	Description	Factory Default
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
Disabled	Disable DHCP snooping mode operation.	

- **Port Mode Configuration**

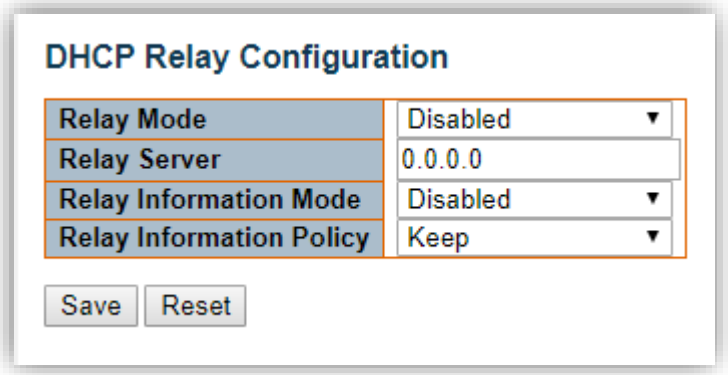


Setting	Description	Factory Default
Trusted	Configures the port as trusted source of the DHCP messages.	Trusted
Untrusted	Configures the port as untrusted source of the DHCP messages.	

Configuration > DHCP > Relay

- **DHCP Relay Configuration**

A DHCP relay agent is used to forward and to transfer DHCP messages between the clients and the server when they are not in the same subnet domain. It stores the incoming interface IP address in the GIADDR field of the DHCP packet. The DHCP server can use the value of GIADDR field to determine the assigned subnet. For such condition, please make sure the switch configuration of VLAN interface IP address and PVID(Port VLAN ID) correctly.



Relay Mode

Setting	Description	Factory Default
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
Disabled	Disable DHCP relay mode operation.	

Relay Server

Setting	Description
IP address.	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.

Setting	Description	Factory Default
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
Disabled	Disable DHCP relay information mode operation.	

Relay Information Policy

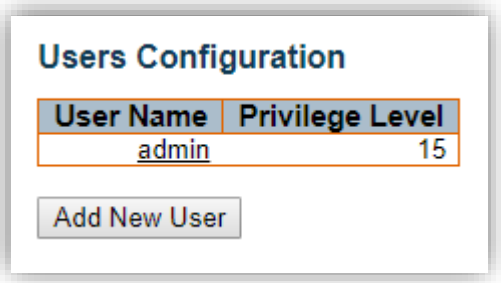
Indicates the DHCP relay information option policy. When DHCP relay information mode operation is enabled, if the agent receives a DHCP message that already contains relay agent information it will enforce the policy. The 'Replace' policy is invalid when relay information mode is disabled.

Setting	Description	Factory Default
Replace	Replace the original relay information when a DHCP message that already contains it is received.	Keep
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.	

Configuration > Security > Switch > 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.

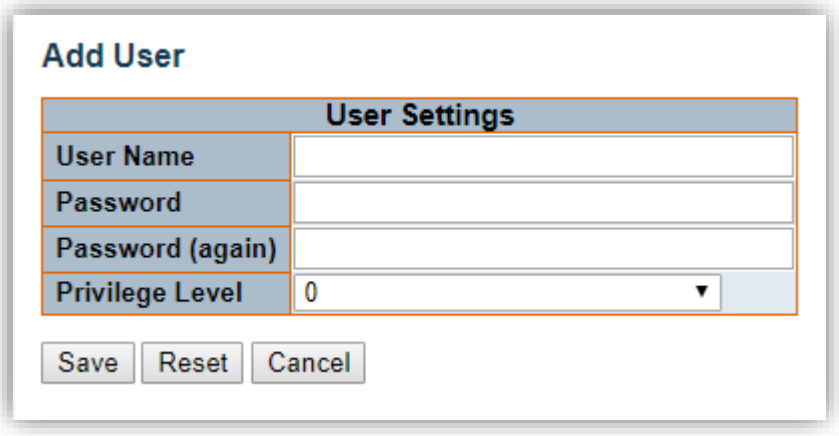
- **Users Configuration**



Setting	Description	Factory Default
User Name	The name identifying the user.	None
Privilege Level 0~15	The privilege level of the user. The allowed range is 0 to 15. If the privilege level value is 15, it can access all groups, i.e. that is granted the fully control of the device. But 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 group's privilege level 5 has the read-only access and privilege level 10 has the read-write access. And the system maintenance (software upload, factory defaults and etc.) need user privilege level 15. Generally, the privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account and privilege level 5 for a guest account.	0

- **Add/Edit User**

Click the **Add New User** button to add a new user. Also you can click User Name to edit a user.



User Name

Setting	Description	Factory Default
Max. 31 Characters	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.	None

Password

Setting	Description	Factory Default
Max. 31 Characters	The password of the user. The allowed string length is **0 to 31**. Any printable characters including space is accepted.	None

Privilege Level

Setting	Description	Factory Default
0~15	The privilege level of the user. The allowed range is **0 to 15**. If the privilege level value is 15, it can access all groups, i.e. that is granted the fully control of the device. But 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 group's privilege level 5 has the read-only access and privilege level 10 has the read-write access. And the system maintenance (software upload, factory defaults and etc.) need user privilege level 15. Generally, the privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account and privilege level 5 for a guest account.	0

Configuration > Security > Switch > Privilege Levels

- **Privilege Level Configuration**

Privilege Level Configuration

Group Name	Privilege Levels			
	Configuration Read-only	Configuration/Execute Read/write	Status/Statistics Read-only	Status/Statistics Read/write
Aggregation	5	10	5	10
Alarm	5	10	5	10
DDMI	5	10	5	10
DHCP	5	10	5	10
DHCPv6_Client	5	10	5	10
Diagnostics	5	10	5	10
Discovery	5	10	5	10
ERPS	5	10	5	10
EventWarning	5	10	5	10
Firmware	5	10	5	10
FRR	5	10	5	10
Green_Ethernet	5	10	5	10
IP	5	10	5	10
IPMC_LIB	5	10	5	10
IPMC_Snooping	5	10	5	10
LACP	5	10	5	10
LLDP	5	10	5	10
Loop_Protect	5	10	5	10
MAC_Table	5	10	5	10
MEP	5	10	5	10
Miscellaneous	15	15	15	15
Modbus	5	10	5	10
MRP	5	10	5	10
MVR	5	10	5	10
NTP	5	10	5	10
POE	5	10	5	10
Ports	5	10	1	10
Private_VLANs	5	10	5	10
QoS	5	10	5	10
RMirror	5	10	5	10
RMON	5	10	5	10
Security(access)	10	10	5	10
Security(network)	5	10	5	10
sFlow	5	10	5	10
SNMP	5	10	5	10
Spanning_Tree	5	10	5	10
System	5	10	1	10
Traceroute	5	10	5	10
uFDMA_AIL	5	10	5	10
uFDMA_CIL	5	10	5	10
VCL	5	10	5	10
VLANs	5	10	5	10
XXRP	5	10	5	10

Save Reset

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:

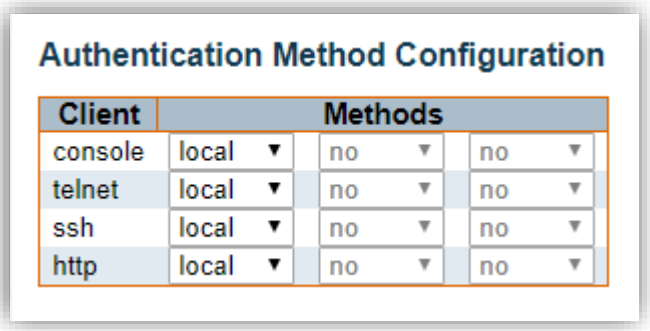
- **System:** Contact, Name, Location, Timezone, Daylight Saving Time, Log.
- **Security:** Authentication, System Access Management, Port (contains Dot1x port, MAC based and the MAC Address Limit), ACL, HTTPS, SSH, ARP Inspection, IP source guard.
- **IP:** Everything except ping.
- **Port:** Everything 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 **15** (where 0 is lowest level and 15 is highest level) Every group has an authorization Privilege level for the following sub groups: configuration read-only, configuration/execute read-write, status/statistics read-only, status/statistics read-write (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.

Configuration > Security > Switch > Auth Method

- **Authentication Method Configuration**

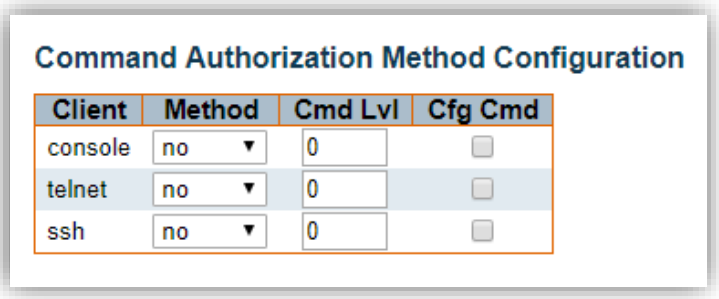
The authentication section allows you to configure how a user is authenticated when he logs into the switch via one of the management client interfaces.



Setting	Description
Client	The management client for which the configuration below applies.
Methods	Method can be set to one of the following values: • **no:** Authentication is disabled and login is not possible. • **local:** Use the local user database on the switch for authentication. • **radius:** Use remote RADIUS server(s) for authentication. • **tacacs:** Use remote TACACS+ server(s) 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

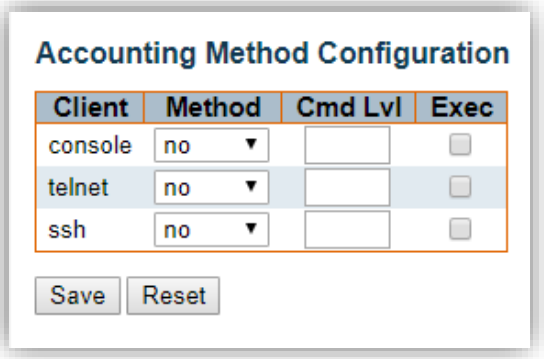
The command authorization section allows you to limit the CLI commands available to a user.



Setting	Description
Client	The management client for which the configuration below applies.
Methods	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 (0~15)	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

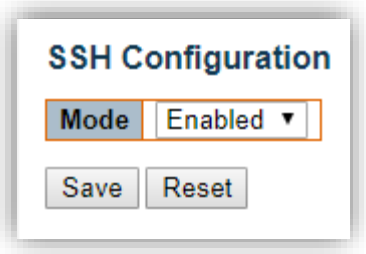
The accounting section allows you to configure command and exec (login) accounting.



Setting	Description
Client	The management client for which the configuration below applies.
Methods	Method can be set to one of the following values: • **no:** Accounting is disabled. • **tacacs:** Use remote TACACS+ server(s) for accounting.
Cmd Lvl (0~15)	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.

Configuration > Security > Switch > SSH

- **SSH Configuration**

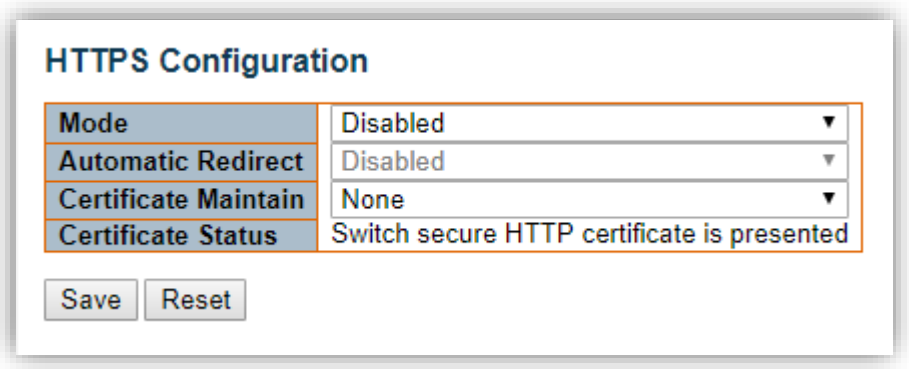


Setting	Description	Factory Default
Enabled	Enable SSH mode operation.	Enabled
Disabled	Disable SSH mode operation.	

Configuration > Security > Switch > HTTPS

- **HTTPS Configuration**

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



Mode

Setting	Description	Factory Default
Enabled	Enable HTTPS mode operation.	Disabled
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.

Setting	Description	Factory Default
Enabled	Enable HTTPS redirect mode operation.	Disabled
Disabled	Disable HTTPS redirect mode operation.	

Certificate Maintain

Setting	Description	Factory Default
None	No operation.	None
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

Setting	Description	Factory Default
Pass phrase	Enter the pass phrase in this field if your uploading certificate is protected by a specific passphrase.	None

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.

Setting	Description	Factory Default
Web Browser	Upload a certificate via Web browser.	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

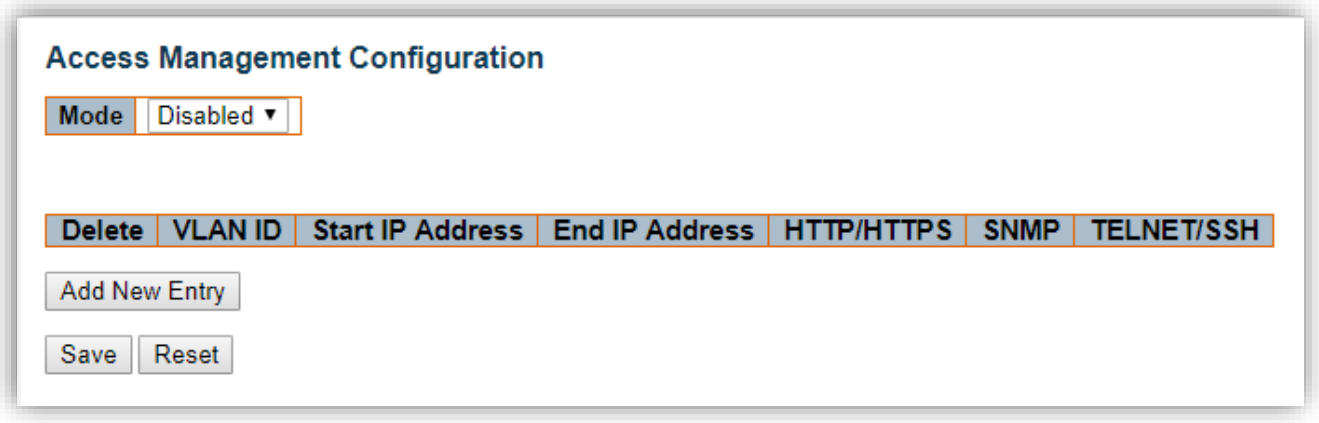
Display the current status of certificate on the switch.

- Switch secure HTTP certificate is presented.
- Switch secure HTTP certificate is not presented.
- Switch secure HTTP certificate is generating ...

Configuration > Security > Switch > Access Management

- **Access Management Configuration**

Configure access management table on this page. 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.



Mode

Indicates the access management mode operation.

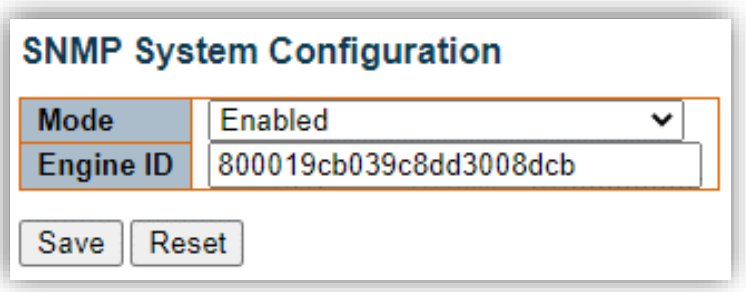
Setting	Description	Factory Default
Enabled	Enable access management mode operation.	Disabled
Disabled	Disable access management mode operation.	

Add New Entry

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

Configuration > Security > Switch > SNMP > System

- **SNMP System Configuration**



Mode

Setting	Description	Factory Default
Enabled	Enable SNMP mode operation.	Enabled
Disabled	Disable SNMP mode operation.	

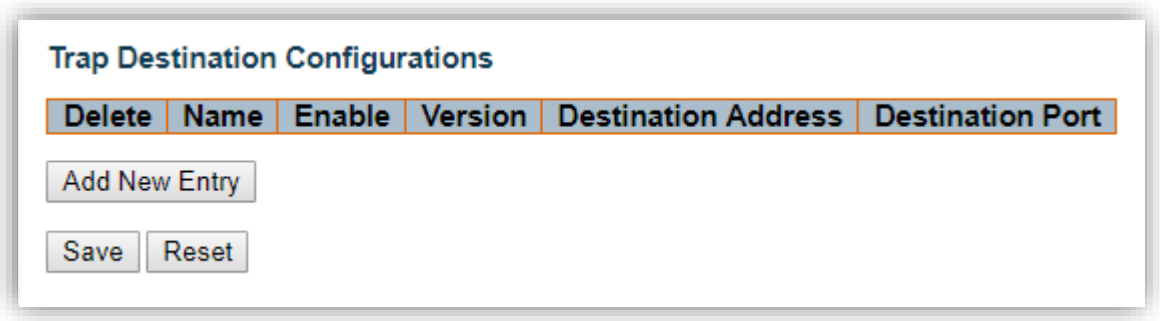
Engine ID

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. Only users on this Engine ID can access the device (local users), so changing the Engine ID will revoke access for all current local users.

Configuration > Security > Switch > SNMP > Trap

- **Trap Configuration**

Trap Destination Configurations



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

Enable
Indicates the trap destination mode operation.

Setting	Description	Factory Default
Enabled	Enable SNMP trap mode operation.	Disabled
Disabled	Disable SNMP trap mode operation.	

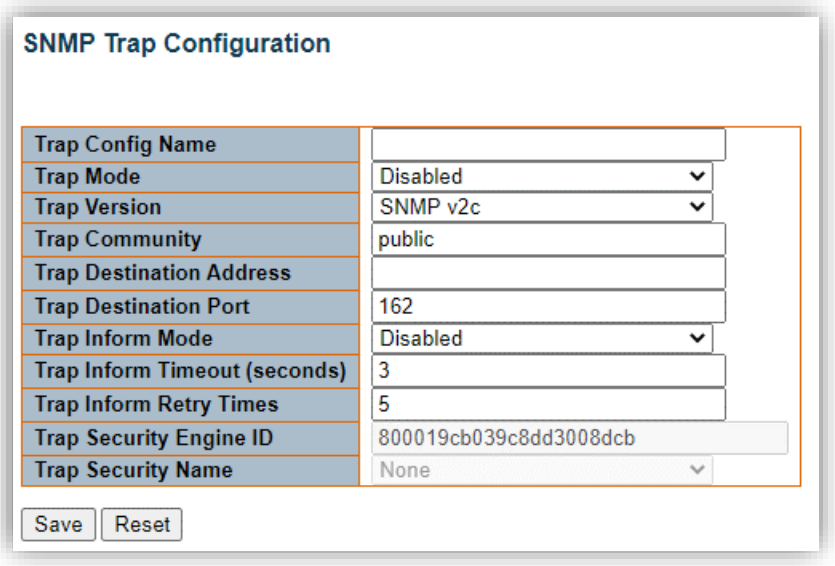
Version

Setting	Description	Factory Default
SNMP v1	Set SNMP supported version 1.	SNMP v2c
SNMP v2c	Set SNMP supported version 2c.	
SNMP v3	Set SNMP 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.

SNMP Trap Configuration



Trap Config Name

Setting	Description	Factory Default
1~32 characters	Indicates which trap Configuration's name for configuring. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.	None

Trap Mode

Setting	Description	Factory Default
Enabled	Enable SNMP trap mode operation.	Disabled
Disabled	Disable SNMP trap mode operation.	

Trap Version

Setting	Description	Factory Default
SNMP v1	Set SNMP supported version 1.	SNMP v2c
SNMP v2c	Set SNMP supported version 2c.	
SNMP v3	Set SNMP supported version 3.	

Trap Community

Setting	Description	Factory Default
0 ~ 63 characters	Indicates the community access string when sending SNMP trap packet. The allowed string length is 0 to 63, and the allowed content is ASCII characters from 33 to 126.	Public

Trap Destination Address

Setting	Description	Factory Default
IP 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**.	None

Trap Destination port

Setting	Description	Factory Default
1~65535	Indicates the SNMP trap destination port. SNMP Agent will send SNMP message via this port, the port range is 1~65535.	162

Trap Inform Mode

Setting	Description	Factory Default
Enabled	Enable SNMP trap inform mode operation.	Disabled
Disabled	Disable SNMP trap inform mode operation.	

Trap Inform Timeout (seconds)

Setting	Description	Factory Default
0~2147	Indicates the SNMP trap inform timeout. The allowed range is 0 to 2147.	3

Trap Inform Retry Times

Setting	Description	Factory Default
0~255	Indicates the SNMP trap inform retry times. The allowed range is 0 to 255.	5

Trap Security Engine ID

Indicates the SNMP trap security engine ID. SNMPv3 sends traps and informs using USM for authentication and privacy. A unique engine ID for these traps and informs is needed. When Trap Probe Security Engine ID is enabled, the ID will be probed automatically. Otherwise, the ID specified in this field is used. The string

must contain an even number(in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed.

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

SNMP Trap Source Configurations

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

Name
Indicates the name for the entry.

Type
The filter type for the entry.

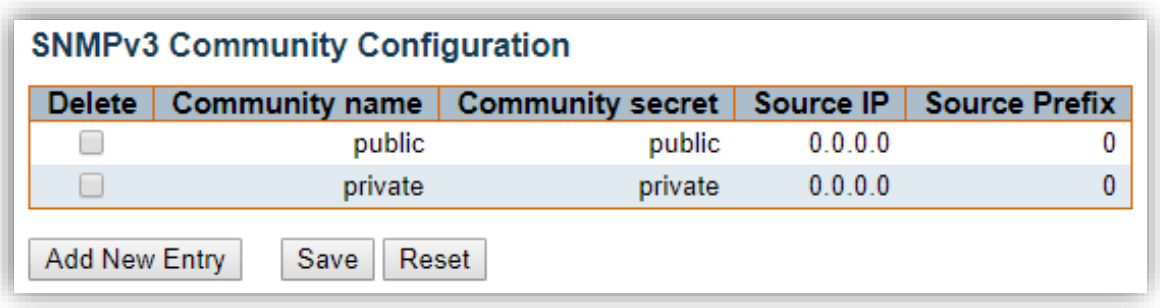
Setting	Description	Factory Default
included	An optional flag to indicate a trap is sent for the given trap source is matched.	included
excluded	An optional flag to indicate a trap is not sent for the given trap source is matched.	

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.

Configuration > Security > Switch > SNMP > Communities

- **SNMPv3 Community Configuration**

  Configure SNMPv3 community table on this page. The entry index key is **Community**.



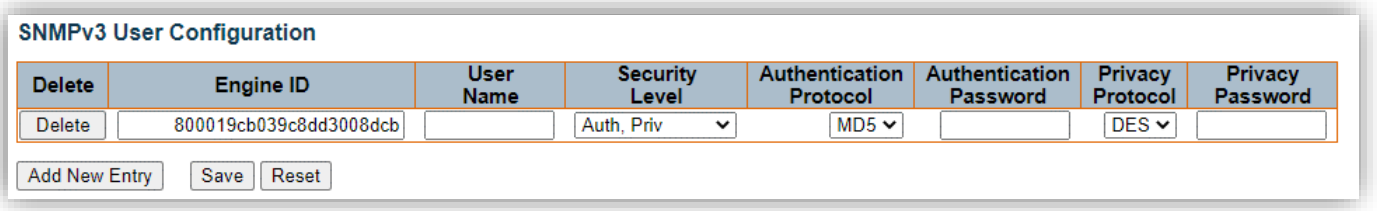
Add New Entry

Setting	Description
Delete	Check to delete the entry. It will be deleted during the next save.
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 prefix.
Source Prefix	Indicates the SNMP access source address prefix.

Configuration > Security > Switch > SNMP > Users

● SNMPv3 User Configuration

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



Add New Entry

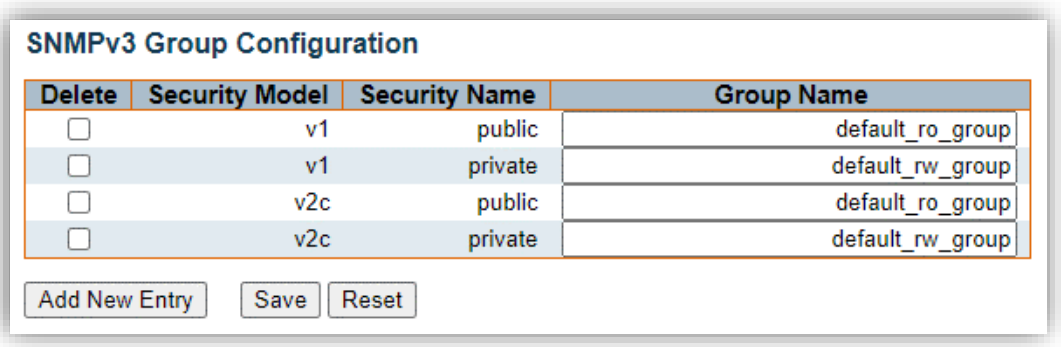
Setting	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Engine ID	An octet string identifying the engine ID that this entry should belong to. The string must contain an even number(in hexadecimal format) with number of digits between 10 and 64, but all-zeros and 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:** 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.

Configuration > Security > Switch > SNMP > Groups

● SNMPv3 Group Configuration

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



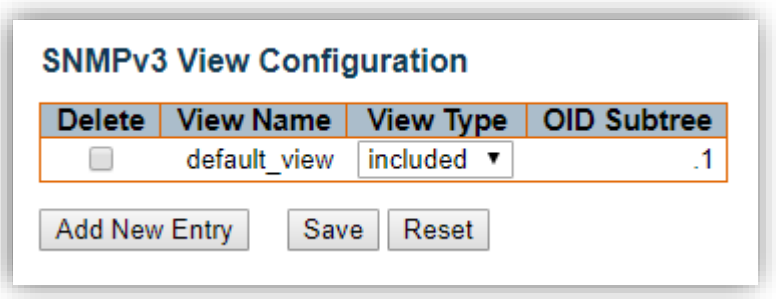
Add New Entry

Setting	Description
Delete	Check to delete the entry. It will be deleted during the next save.
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. **NOTE:** The value is pre-configured in the **Configuration > Security > Switch > SNMP > Communities** section.
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.

Configuration > Security > Switch > SNMP > Views

- **SNMPv3 View Configuration**

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



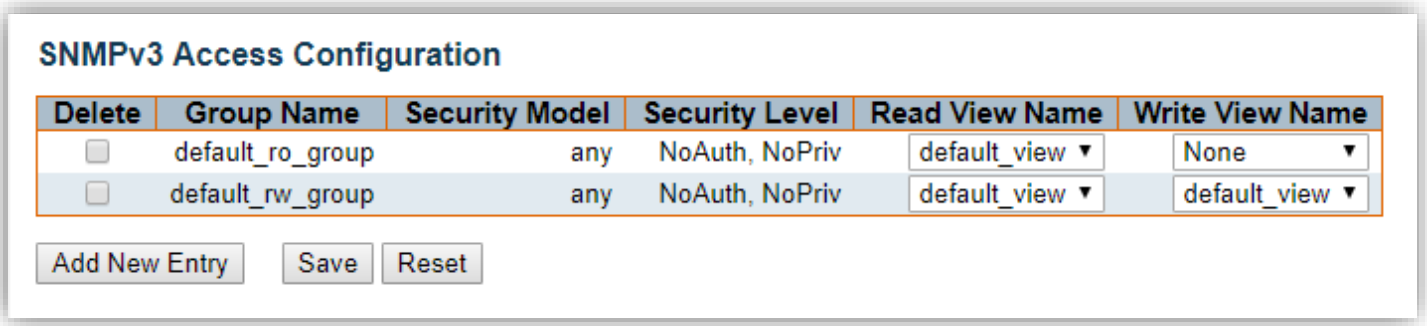
Add New Entry

Setting	Description
Delete	Check to delete the entry. It will be deleted during the next save.
View Name	A string identifying the view name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
View Type	Indicates the view type that this entry should belong to. Possible view types are: • **included:** An optional flag to indicate that this view subtree should be included. • **excluded:** An optional flag to indicate that this view subtree should be excluded. In general, if a view entry's view type is **excluded**, there should be another view entry existing with view type as 'included' and it's OID subtree should overstep the **excluded** view entry.
OID Subtree	The OID defining the root of the subtree to add to the named view. The allowed OID length is 1 to 128. The allowed string content is digital number or asterisk(*).

Configuration > Security > Switch > SNMP > Access

- **SNMPv3 Access Configuration**

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



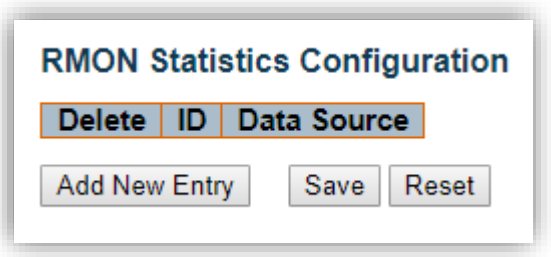
Add New Entry

Setting	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Group Name	A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
Security Model	Indicates the security model that this entry should belong to. Possible security models are: • **any:** Any security model accepted(v1|v2c|usm). • **v1:** Reserved for SNMPv1. • **v2c:** Reserved for SNMPv2c. • **usm:** User-based Security Model (USM).
Security Level	Indicates the security model that this entry should belong to. Possible security models are: • **NoAuth, NoPriv:** No authentication and no privacy. • **Auth, NoPriv:** Authentication and no privacy. • **Auth, Priv:** Authentication and privacy.
Read View Name	The name of the MIB view defining the MIB objects for which this request may request the current values. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
Write View Name	The name of the MIB view defining the MIB objects for which this request may potentially set new values. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Configuration > Security > Switch > RMON > Statistics

- **RMON statistics Configuration**

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



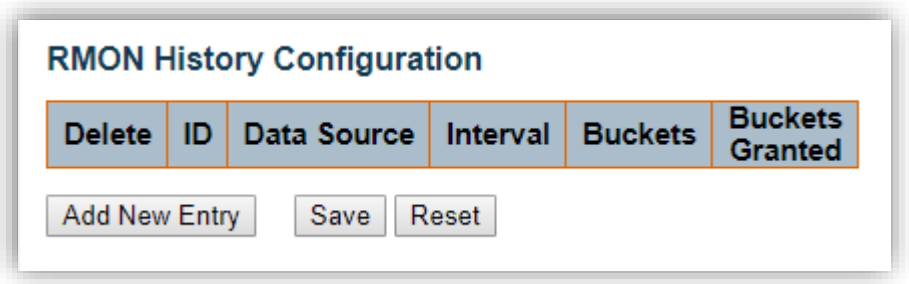
Add New Entry

Setting	Description
Delete	Check to delete the entry. It will be deleted during the next save.
ID	Indicates the index of the entry. The range is from 1 to 65535.
Data Source	Indicates the port ID which wants to be monitored. If in stacking switch, the value must add 1000000*(switch ID-1), for example, if the port is switch 3 port 5, the value is 2000005.

Configuration > Security > Switch > RMON > History

- **RMON History Configuration**

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



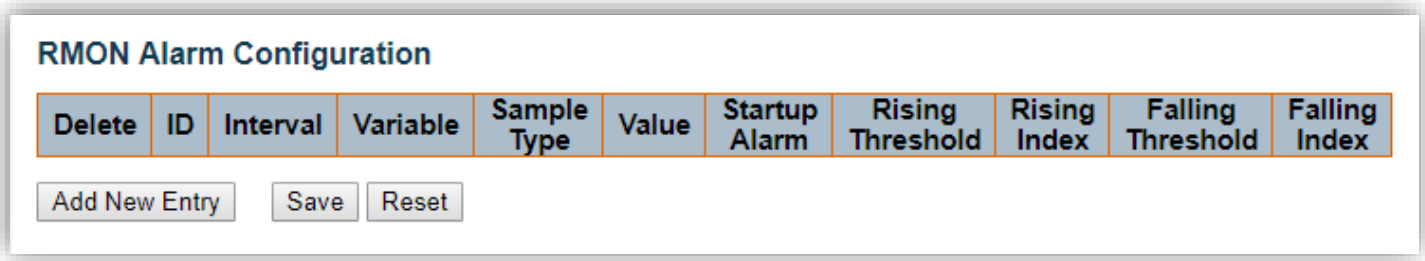
Add New Entry

Setting	Description
Delete	Check to delete the entry. It will be deleted during the next save.
ID	Indicates the index of the entry. The range is from 1 to 65535.
Data Source	Indicates the port ID which wants to be monitored. If in stacking switch, the value must add 1000000*(switch ID-1), for example, if the port is switch 3 port 5, the value is 2000005.
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.

Configuration > Security > Switch > RMON > Alarm

- **RMON Alarm Configuration**

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



Add New Entry

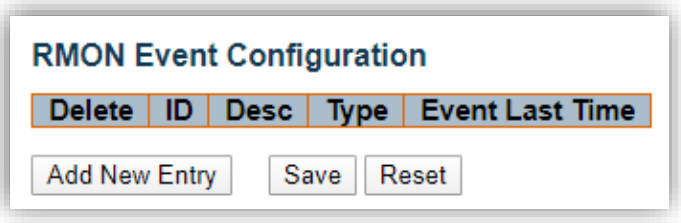
Setting	Description
Delete	Check to delete the entry. It will be deleted during the next save.
ID	Indicates the index of the entry. The range is from 1 to 65535.
Interval	Indicates the interval in seconds for sampling and comparing the rising and falling threshold. The range is from 1 to 2^31-1.
Variable	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: • **Rising:** Trigger alarm when the first value is larger than the rising threshold. • **Falling:** Trigger alarm when the first value is less than the falling threshold. • **RisingOrFalling:** Trigger alarm when the first value is larger than the rising threshold or less than the falling threshold (default).
Rising Threshold	Rising threshold value (-2147483648-2147483647).
Rising Index	Rising event index (1-65535).
Falling Threshold	Falling threshold value (-2147483648-2147483647).
Falling Index	Falling event index (1-65535).

Configuration > Security > Switch > RMON > Event

- **RMON Event Configuration**

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



Add New Entry

Setting	Description
Delete	Check to delete the entry. It will be deleted during the next save.
ID	Indicates the index of the entry. The range is from 1 to 65535.
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. **snmptrap:** Send SNMP trap when the event is triggered. **logandtrap:** Create SNMP log entry and sent SNMP trap when the event is triggered.
Event Last Time	Indicates the value of sysUpTime at the time this event entry last generated an event.

Configuration > Security > Network

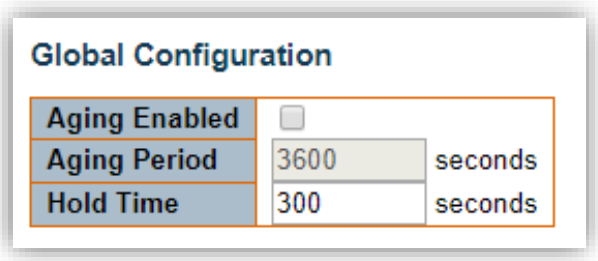
- **Port Security Configuration**

The Port Security Configuration allows you to configure the Port Security global and per-port settings.

Port Security allows for limiting the number of users on a given port. A user is identified by a MAC address and VLAN ID. If Port Security is enabled on a port, the limit specifies the maximum number of users on the port. If this number is exceeded, an action is taken depending on violation mode. The violation mode can be one of the three different described below.

The Port Security configuration consists of two sections, a global and a per-port.

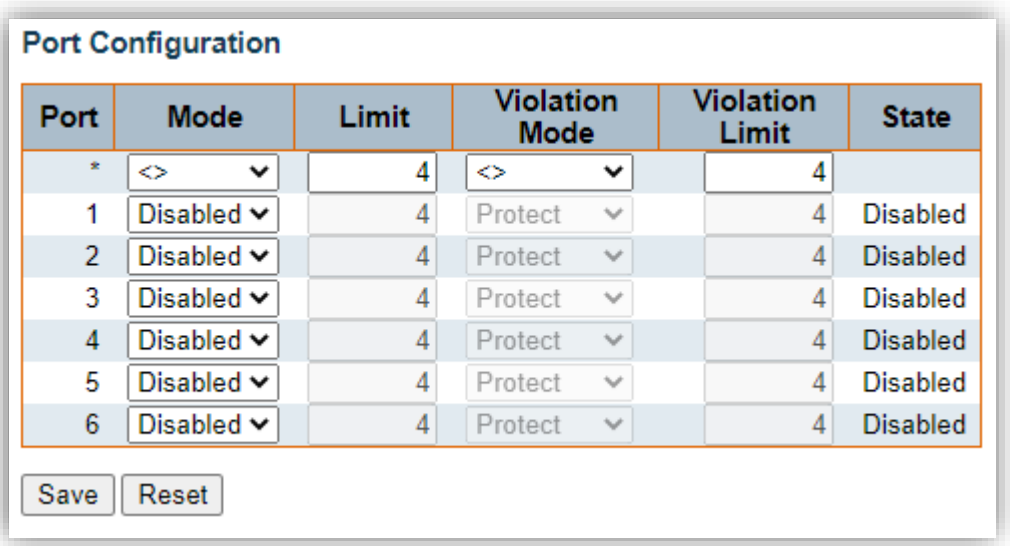
Global Configuration



Setting	Description
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 functionality for securing MAC addresses, they may have other requirements to the aging period. The underlying functionality will use the shorter requested aging period of all modules that have aging enabled. The Aging Period can be set to a number between 10 and 10000000 seconds with a default of 3600 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 Port Security 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.
Hold Time	The hold time - measured in seconds - is used to determine how long a MAC address is held in the MAC table if it has been found to violate the limit. Valid range is between 10 and 10000000 seconds with a default of 300 seconds. The reason for holding a violating MAC address in the MAC table is primarily to ensure that the same MAC address doesn't give rise to continuous notifications (if notifications on violation count is enabled).

Port Configuration

The table has one row for each port on the switch and a number of columns.



Setting	Description
Port	The port number to which the configuration below applies.
Mode	Controls whether Port security is enabled on this port. Notice that other modules may still use the underlying port security features without enabling Port security on a given port.
Limit	The maximum number of MAC addresses that can be secured on this port. This number cannot exceed 1023. If the limit is exceeded, an action is taken corresponding to the violation mode. The switch is born with a total number of MAC addresses from which all ports draw whenever a new MAC address is seen on a Port Security-enabled port. Since all ports draw from the same pool, it may happen that a configured maximum cannot be granted, if the remaining ports have already used all available MAC addresses. **Deafult**: 4
Violation Mode	If Limit is reached, the switch can take one of the following actions: **Protect**: Do not allow more than Limit MAC addresses on the port, but take no further action. **Restrict**: If Limit is reached, subsequent MAC addresses on the port will be counted and marked as violating. Such MAC addreses are removed from the MAC table when the hold time expires. At most Violation Limit MAC addresses can be marked as violating at any given time. **Shutdown**: If Limit is reached, one additional MAC address will cause the port to be shut down. This implies that all secured MAC addresses be removed from the port, and no new addresses be learned. There are three ways to re-open the port: 1. In the "Configuration→Ports" page's "Configured" column, first disable the port, then restore the original mode. 2. Make a Port Security configuration change on the port. 3. Boot the switch.
Violation Limit	The maximum number of MAC addresses that can be marked as violating on this port. This number cannot exceed 1023. Default is 4. It is only used when Violation Mode is **Restrict**.

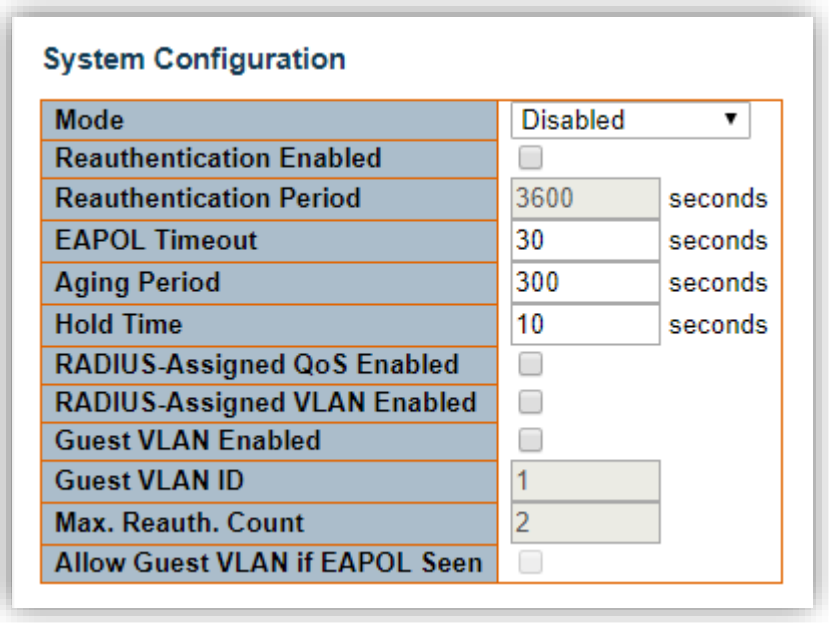
State	This column shows the current Port Security state of the port. The state takes one of four values: **Disabled**: Port Security is disabled on the port. **Ready**: The limit is not yet reached. This can be shown for all violation modes. **Limit Reached**: Indicates that the limit is reached on this port. This can be shown for all violation modes. **Shutdown**: Indicates that the port is shut down by Port Security. This state can only be shown if violation mode is set to **Shutdown**.

Configuration > Security > Network > NAS

- **Network Access Server Configuration**

This page allows you to configure the IEEE 802.1X and MAC-based authentication system and port settings. The IEEE 802.1X standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication. One or more central servers, the backend servers, determine whether the user is allowed access to the network. These backend (RADIUS) servers are configured on the 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.

System Configuration



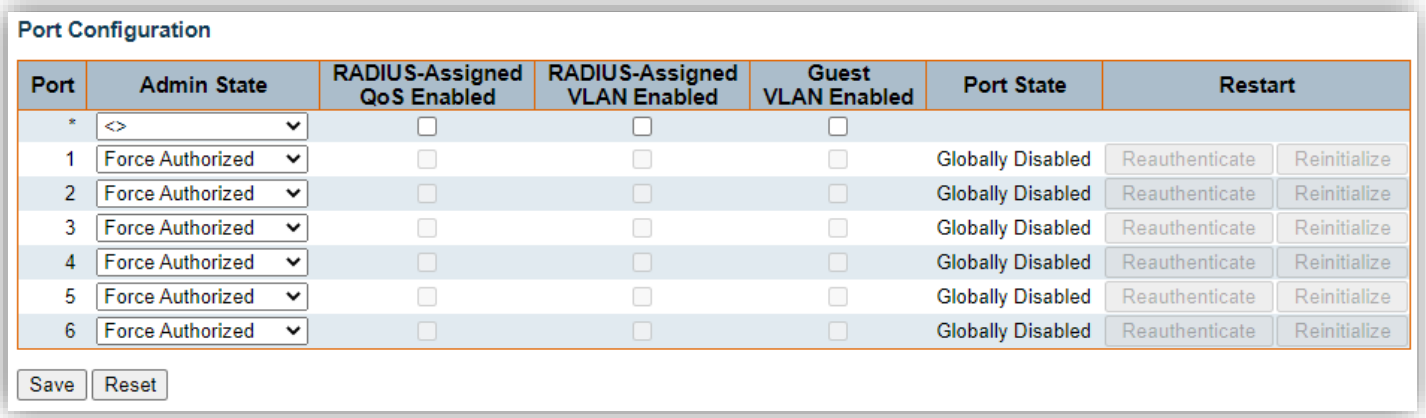
Setting	Description
Mode	Indicates if NAS is globally enabled or disabled on the switch. If globally disabled, all ports are allowed forwarding of frames.

Reauthentication Enabled	If checked, successfully authenticated supplicants/clients are reauthenticated after the interval specified by the Reauthentication Period. Reauthentication for 802.1X-enabled ports can be used to detect if a new device is plugged into a switch port or if a supplicant is no longer attached. For MAC-based ports, reauthentication is only useful if the RADIUS server configuration has changed. It does not involve communication between the switch and the client, and therefore doesn't imply that a client is still present on a port (see Aging Period below).
Reauthentication Period	Determines the period, in seconds, after which a connected client must be reauthenticated. This is only active if the Reauthentication Enabled checkbox is checked. Valid values are in the range 1 to 3600 seconds.
EAPOL Timeout	Determines the time for retransmission of Request Identity EAPOL frames. Valid values are in the range 1 to 65535 seconds. This has no effect for MAC-based ports.
Aging 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 reauthentication, which will fail. But if reauthentication is not enabled, the only way to free resources is by aging the entries. For ports in MAC-based Auth. mode, reauthentication doesn't cause direct communication between the switch and the client, so this will not detect whether the client is still attached or not, and the only way to free any resources is to age the entry.
Hold Time	This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses: • **Single 802.1X** • **Multi 802.1X** • **MAC-Based Auth.** If a client is denied access - either because the RADIUS server denies the client access or because the RADIUS server request times out (according to the timeout specified on the **Configuration > Security > AAA** page) - the client is put on hold in the Unauthorized state. The hold timer does not count during an on-going authentication. In MAC-based Auth. mode, the switch will ignore new frames coming from the client during the hold time. The Hold Time can be set to a number between 10 and 1000000 seconds
RADIUS-Assigned QoS Enabled	RADIUS-assigned QoS provides a means to centrally control the traffic class to which traffic coming from a successfully authenticated supplicant is assigned on the switch. The RADIUS server must be configured to transmit special RADIUS

	attributes to take advantage of this feature (see RADIUS-Assigned QoS Enabled below for a detailed description). The RADIUS-Assigned QoS Enabled checkbox provides a quick way to globally enable/disable RADIUS-server assigned QoS Class functionality. When checked, the individual ports' ditto setting determine whether RADIUS-assigned QoS Class is enabled on that port. When unchecked, RADIUS-server assigned QoS Class is disabled on all ports.
RADIUS-Assigned VLAN Enabled	RADIUS-assigned VLAN provides a means to centrally control the VLAN on which a successfully authenticated supplicant is placed on the switch. Incoming traffic will be classified to and switched on the RADIUS-assigned VLAN. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature (see **RADIUS-Assigned VLAN Enabled** below for a detailed description). The "RADIUS-Assigned VLAN Enabled" checkbox provides a quick way to globally enable/disable RADIUS-server assigned VLAN functionality. When checked, the individual ports' ditto setting determine whether RADIUS-assigned VLAN is enabled on that port. When unchecked, RADIUS-server assigned VLAN is disabled on all ports.
Guest VLAN Enabled	A Guest VLAN is a special VLAN - typically with limited network access - on which 802.1X-unaware clients are placed after a network administrator-defined timeout. The switch follows a set of rules for entering and leaving the Guest VLAN as listed below. The **Guest VLAN Enabled** checkbox provides a quick way to globally enable/ disable Guest VLAN functionality. When checked, the individual ports' ditto setting determines whether the port can be moved into Guest VLAN. When unchecked, the ability to move to the Guest VLAN is disabled on all ports.
Guest VLAN ID	This is the value that a port's Port VLAN ID is set to if a port is moved into the Guest VLAN. It is only changeable if the Guest VLAN option is globally enabled. Valid values are in the range [1; 4095].
Max. Reauth. Count	The number of times the switch transmits an EAPOL Request Identity frame without response before considering entering the Guest VLAN is adjusted with this setting. The value can only be changed if the Guest VLAN option is globally enabled. Valid values are in the range [1; 255].
Allow Guest VLAN if EAPOL Seen	The switch remembers if an EAPOL frame has been received on the port for the life-time of the port. Once the switch considers whether to enter the Guest VLAN, it will first check if this option is enabled or disabled. If disabled (unchecked; default), the switch will only enter the Guest VLAN if an EAPOL frame has not been received on the port for the life-time of the port. If enabled (checked), the switch will consider entering the Guest VLAN even if an EAPOL frame has been received on the port for the life-time of the port. The value can only be changed if the Guest VLAN option is globally enabled.

Port Configuration

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



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.

Setting	Description
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	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 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:
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' - '7', which translates into the desired QoS Class in the range [0; 7].

RADIUS-Assigned VLAN Enabled
When RADIUS-Assigned VLAN is both globally enabled and enabled (checked) for a given port, the switch reacts to VLAN ID information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, the port's Port VLAN ID will be changed to this VLAN ID, the port will be set to be a member of that VLAN ID, and the port will be forced into VLAN unaware mode. Once assigned, all traffic arriving on the port will be classified and switched on the RADIUS-assigned VLAN ID.
If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a VLAN ID or it's invalid, or the supplicant is otherwise no longer present on the port, the port's VLAN ID is immediately reverted to the original VLAN ID (which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned).
This option is only available for single-client modes, i.e.

- **Port-based 802.1X**
- **Single 802.1X**

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 fulfill the following requirements (if Tag == 0 is used, the **Tunnel-Private-Group-ID** does not need to include a Tag):
    - Value of **Tunnel-Medium-Type** must be set to IEEE-802.
    - Value of **Tunnel-Type** must be set to **VLAN**.
    - 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 transmission of EAPOL Request Identity frames is configured with EAPOL Timeout. If Allow Guest VLAN if EAPOL Seen is enabled, the port will now be placed in the Guest VLAN. If disabled, the switch will first check its history to see if an EAPOL frame has previously been received on the port (this history is cleared if the port link goes down or the port's Admin State is changed), and if not, the port will be placed in the Guest VLAN. Otherwise it will not move to the Guest VLAN, but continue transmitting EAPOL Request Identity frames at the rate given by EAPOL Timeout.
Once in the Guest VLAN, the port is considered authenticated, and all attached clients on the port are allowed access on this VLAN. The switch will not transmit an EAPOL Success frame when entering the Guest VLAN.
While in the Guest VLAN, the switch monitors the link for EAPOL frames, and if one such frame is received, the switch immediately takes the port out of the Guest VLAN and starts authenticating the supplicant according to the port mode. If an EAPOL frame is received, the port will never be able to go back into the Guest VLAN if the Allow Guest VLAN if **EAPOL Seen** is disabled.

Port State

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

- **Globally Disabled:** NAS is globally disabled.

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

Restart

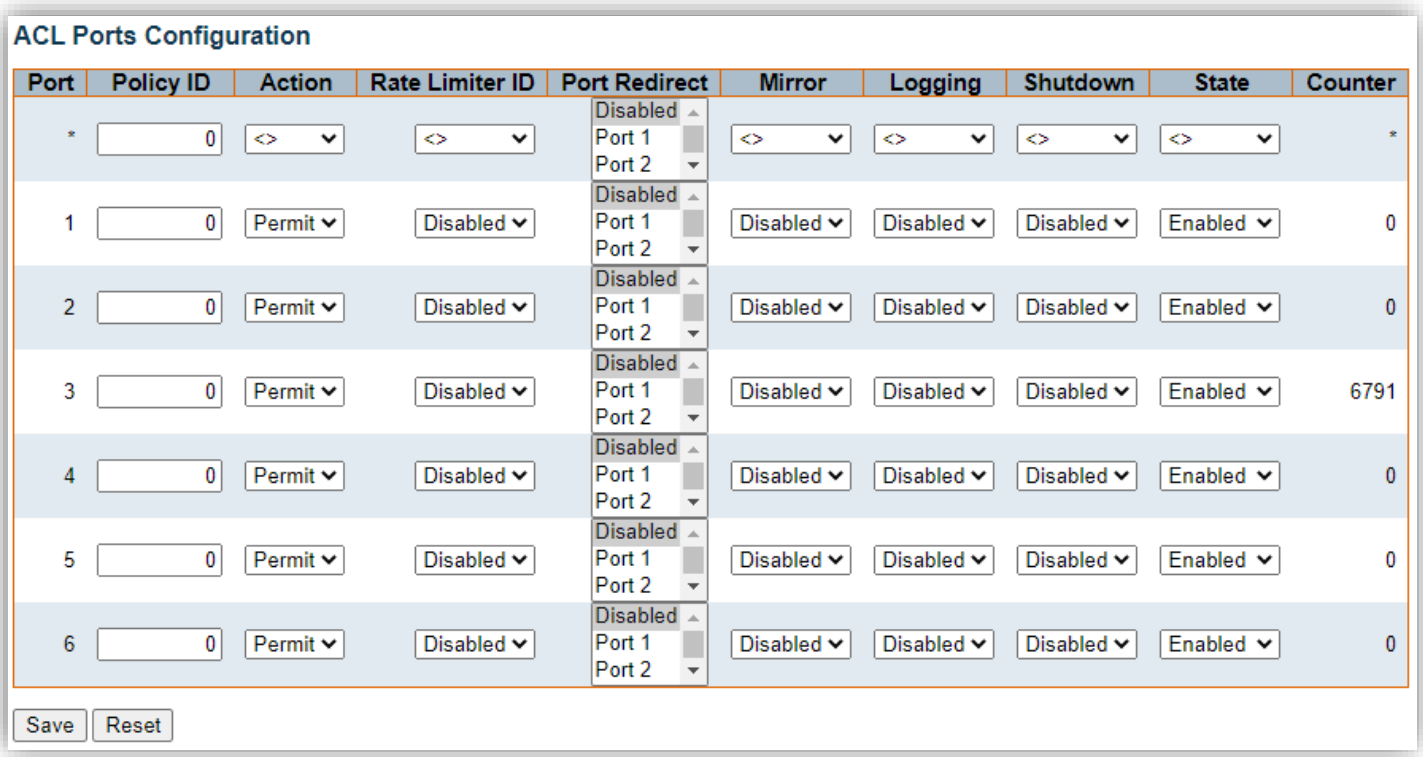
Two buttons are available for each row. The buttons are only enabled when authentication is globally enabled and the port's Admin State is in an EAPOL-based or MAC-based mode.
Clicking these buttons will not cause settings changed on the page to take effect.

- **Reauthenticate:** Schedules a reauthentication whenever the quiet-period of the port runs out (EAPOL-based authentication). For MAC-based authentication, reauthentication will be attempted immediately. The button only has effect for successfully authenticated clients on the port and will not cause the clients to get temporarily unauthorized.
- **Reinitialize:** Forces a reinitialization of the clients on the port and thereby a reauthentication immediately. The clients will transfer to the unauthorized state while the reauthentication is in progress.

Configuration > Security > Network > ACL > Ports

- **ACL Ports Configuration**

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



Port

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

Policy ID

Setting	Description	Factory Default
0~255	Select the policy to apply to this port. The allowed values are 0 through 255.	0

Action

Setting	Description	Factory Default
Permit	Forwarding is permitted.	Permit
Deny	Forwarding is denied.	

Rate Limiter ID

Setting	Description	Factory Default
Disabled	Rate Limiter is disabled.	Disabled
1~16	Select which rate limiter to apply on this port.	

Port Redirect

Setting	Description	Factory Default
Disabled	Port Redirect is disabled.	Disabled
Port X	Select which port frames are redirected on.	

Mirror

Setting	Description	Factory Default
Disabled	Frames received on the port are not mirrored.	Disabled
Enabled	Frames received on the port are mirrored.	

Logging

Specify the logging operation of this port. Notice that the logging message doesn't include the 4 bytes CRC.

Setting	Description	Factory Default
Disabled	Frames received on the port are not logged.	Disabled
Enabled	Frames received on the port are stored in the System Log.	
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.	

Shutdown

Setting	Description	Factory Default
Disabled	Port shut down is disabled.	Disabled
Enabled	If a frame is received on the port, the port will be disabled.	
NOTE	The shutdown feature only works when the packet length is less than 1518(without VLAN tags).	

State

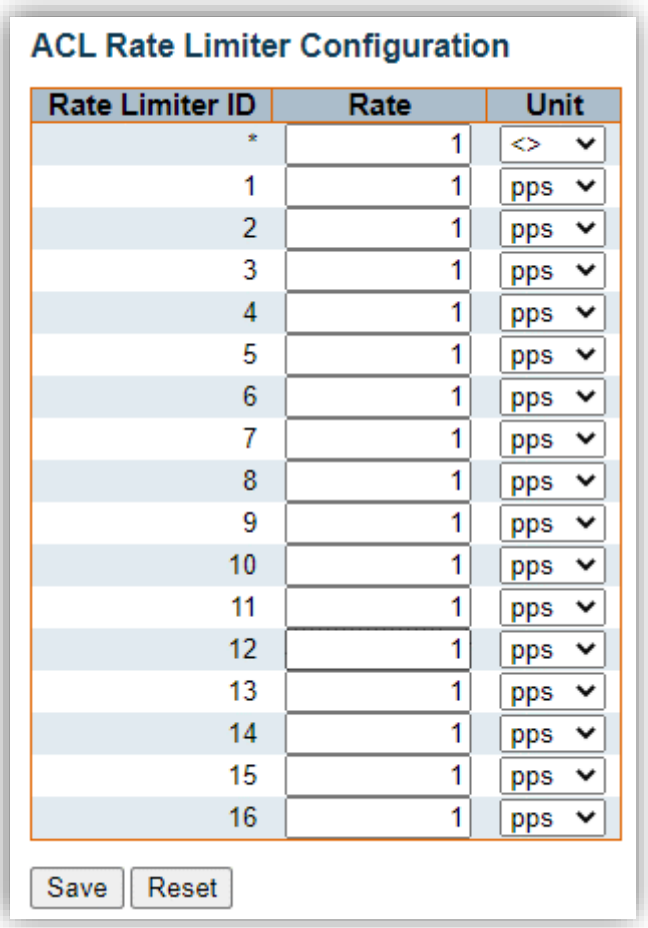
Setting	Description	Factory Default
Disabled	To close ports by changing the volatile port configuration of the ACL user module.	Enabled
Enabled	To reopen ports by changing the volatile port configuration of the ACL user module.	

Counter

Counts the number of frames that match this ACE.

Configuration > Security > Network > ACL > Rate Limiters

- **ACL Rate Limiter Configuration**



Rate Limiter ID

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

Rate

Setting	Description	Factory Default
0-3276700	The valid rate is 0-3276700 in pps. or 0, 100, 200, 300, ..., 1000000 in kbps	1

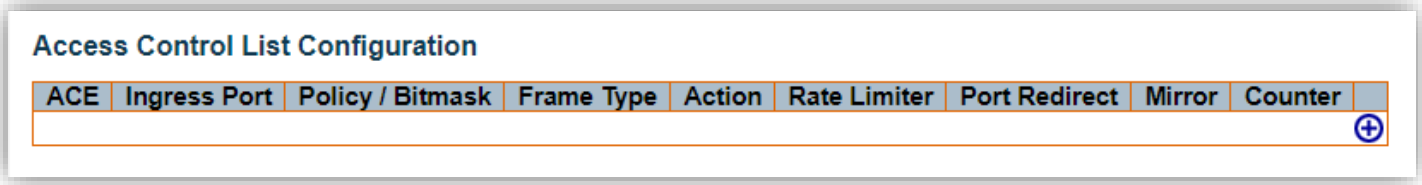
Unit

Setting	Description	Factory Default
pps	packets per second	pps
kbps	Kbits per second.	

Configuration > Security > Network > ACL > Access Control List

Access Control List Configuration

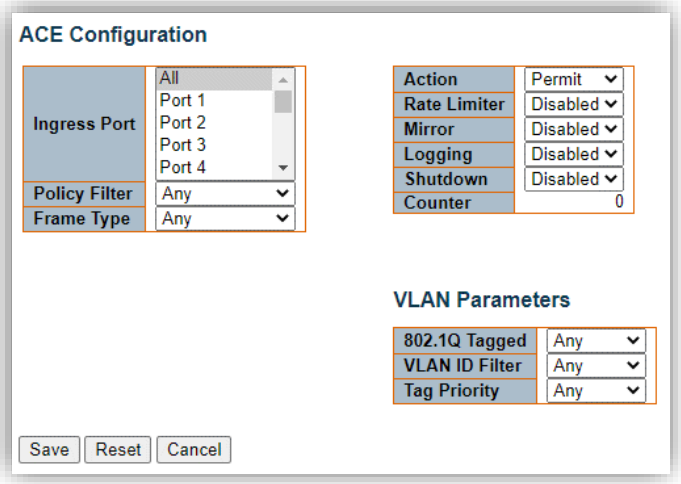
This page shows the Access Control List (ACL), which is made up of the ACEs defined on this switch. Each row describes the ACE that is defined. The maximum number of ACEs is 256 on each switch.



Click on the lowest plus sign to add a new ACE to the list. The reserved ACEs used for internal protocol, cannot be edited or deleted, the order sequence cannot be changed and the priority is highest.
You can modify each ACE (Access Control Entry) in the table using the following buttons:

- : Inserts a new ACE before the current row.
- : Edits the ACE row.
- : Moves the ACE up the list.
- : Moves the ACE down the list.
- : Deletes the ACE.
- : The lowest plus sign adds a new entry at the bottom of the ACE listings.

ACE Configuration



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

Ingress Port

Setting	Description	Factory Default
All	The ACE applies to all port.	All

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

Policy Filter

Setting	Description	Factory Default
Any	No policy filter is specified.	Any
Specific	If you want to filter a specific policy with this ACE, choose this value. Two field for entering an policy value and bitmask appears.	

Policy Value

Setting	Description	Factory Default
0~255	When **Specific** is selected for the policy filter, you can enter a specific policy value. The allowed range is 0 to 255.	0

Policy Bitmask

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

Frame Type

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

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

Action

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

Setting	Description	Factory Default
Permit	The frame that hits this ACE is granted permission for the ACE operation.	Permit
Deny	The frame that hits this ACE is dropped.	
Filter	Frames matching the ACE are filtered.	

Rate Limiter

Specify the rate limiter in number of base units.

Setting	Description	Factory Default
Disabled	Rate limiter operation is disabled.	Disabled
1~16	Specify the rate limiter in number of base units. The allowed range is 1 to 16.	

Port Redirect

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

Setting	Description	Factory Default
Disabled	Port redirect operation is disabled	Disabled
Enabled	Port redirect operation is enabled	

Mirror

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

Setting	Description	Factory Default
Enabled	Frames received on the port are mirrored.	Disabled
Disabled	Frames received on the port are not mirrored.	

Logging

Specify the logging operation of the ACE. Notice that the logging message doesn't include the 4 bytes CRC information.

Setting	Description	Factory Default
Enabled	Frames matching the ACE are stored in the System Log.	Disabled
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.	

Shutdown

Setting	Description	Factory Default
Enabled	If a frame matches the ACE, the ingress port will be disabled.	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).	

Counter

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

- **MAC Parameters**

SMAC Filter

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

Setting	Description	Factory Default
Any	No SMAC filter is specified.	Any
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

Setting	Description	Factory Default
MAC address	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.	00-00-00-00-00-01

DMAC Filter

Setting	Description	Factory Default
Any	No DMAC filter is specified.	Any
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

Setting	Description	Factory Default
MAC address	When **Specific** is selected for the DMAC 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 DMAC value.	00-00-00-00-00-02

- **VLAN Parameters**

802.1Q Tagged

Setting	Description	Factory Default
Any	Any value is allowed.	Any
Enabled	Tagged frame only.	
Disabled	Untagged frame only.	

VLAN ID Filter

Setting	Description	Factory Default
Any	No VLAN ID filter is specified.	Any
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

Setting	Description	Factory Default
1~4095	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.	1

Tag Priority

Setting	Description	Factory Default
Any	No tag priority is specified	Any
0~7, 0-1, 2-3, 4-5, 6-7, 0-3, 4-7	Specify the tag priority for this ACE. A frame that hits this ACE matches this tag priority.	

- **ARP Parameters**

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

ARP/RARP

Setting	Description	Factory Default
Any	No ARP/RARP OP flag is specified.	Any
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

Setting	Description	Factory Default
Any	No Request/Reply OP flag is specified	Any
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

Setting	Description	Factory Default
Any	No sender IP filter is specified.	Any
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

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

Sender IP Mask

Setting	Description	Factory Default
IP address	When **Network** is selected for the sender IP filter, you can enter a specific sender IP mask in dotted decimal notation.	255.255.255.0

Target IP Filter

Setting	Description	Factory Default
Any	No target IP filter is specified.	Any
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

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

Target IP Mask

Setting	Description	Factory Default
IP address	When **Network** is selected for the target IP filter, you can enter a specific target IP mask in dotted decimal notation.	255.255.255.0

ARP Sender MAC Match

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

Setting	Description	Factory Default
0	ARP frames where SHA is not equal to the SMAC address.	Any
1	ARP frames where SHA is equal to the SMAC address.	
Any	Any value is allowed.	

RARP Target MAC Match

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

Setting	Description	Factory Default
0	RARP frames where THA is not equal to the target MAC address.	Any
1	RARP frames where THA is equal to the target MAC address.	
Any	Any value is allowed.	

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.

Setting	Description	Factory Default
0	ARP/RARP frames where the HLN is not equal to Ethernet (0x06) or the (PLN) is not equal to IPv4 (0x04).	Any
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.	

IP

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

Setting	Description	Factory Default
0	ARP/RARP frames where the HLD is not equal to Ethernet (1).	Any
1	ARP/RARP frames where the HLD is equal to Ethernet (1).	
Any	Any value is allowed.	

Ethernet

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

Setting	Description	Factory Default
0	ARP/RARP frames where the PRO is not equal to IP (0x800).	Any
1	ARP/RARP frames where the PRO is equal to IP (0x800).	
Any	Any value is allowed.	

- **IP Parameters**

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

IP Protocol Filter

Setting	Description	Factory Default
Any	No IP protocol filter is specified	Any
Other	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

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

IP TTL

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

Setting	Description	Factory Default
zero	IPv4 frames with a Time-to-Live field greater than zero must not be able to match this entry.	Any
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.	

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.

Setting	Description	Factory Default
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.	Any
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.	

IP Option

Specify the options flag setting for this ACE.

Setting	Description	Factory Default
No	IPv4 frames where the options flag is set must not be able to match this entry.	Any
Yes	IPv4 frames where the options flag is set must be able to match this entry.	
Any	Any value is allowed.	

SIP Filter

Specify the source IP filter for this ACE.

Setting	Description	Factory Default
Any	No source IP filter is specified.	Any
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

Setting	Description	Factory Default
IP 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.	0.0.0.0

SIP Mask

Setting	Description	Factory Default
IP address	When **Network** is selected for the source IP filter, you can enter a specific SIP mask in dotted decimal notation.	255.255.255.0

DIP Filter

Specify the destination IP filter for this ACE.

Setting	Description	Factory Default
Any	No source IP filter is specified.	Any
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.	

DIP Address

Setting	Description	Factory Default
IP 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.	0.0.0.0

DIP Mask

Setting	Description	Factory Default
IP address	When **Network** is selected for the destination IP filter, you can enter a specific DIP mask in dotted decimal notation.	255.255.255.0

- **IPv6 Parameters**

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

Next Header Filter

Setting	Description	Factory Default
Any	No IPv6 next header filter is specified.	Any
Other	If you want to filter a specific IPv6 next header filter with this ACE, choose this value. A field for entering an IPv6 next header filter appears.	

ICMP	Select ICMP to filter IPv6 ICMP protocol frames. Extra fields for defining ICMP parameters will appear. These fields are explained later in this help file.	
UDP	Select UDP to filter IPv6 UDP protocol frames. Extra fields for defining UDP parameters will appear. These fields are explained later in this help file.	
TCP	Select TCP to filter IPv6 TCP protocol frames. Extra fields for defining TCP parameters will appear. These fields are explained later in this help f	

Next Header Value

Setting	Description	Factory Default
0~255	When **Other** 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.	255

SIP Filter

Specify the source IPv6 filter for this ACE.

Setting	Description	Factory Default
Any	No source IPv6 filter is specified.	Any
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

Setting	Description	Factory Default
IPv6 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

Setting	Description	Factory Default
IPv6 address	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.	0xFFFFFFFF

Hop Limit

Setting	Description	Factory Default
0	IPv6 frames with a hop limit field greater than zero must not be able to match this entry.	Any
1	IPv6 frames with a hop limit field greater than zero must be able to match this entry.	
Any	Any value is allowed.	

- **ICMP Parameters**

ICMP Type Filter

Setting	Description	Factory Default
Any	No ICMP filter is specified.	Any
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

Setting	Description	Factory Default
0~255	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.	255

ICMP Code Filter

Setting	Description	Factory Default
Any	No ICMP code filter is specified	Any
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

Setting	Description	Factory Default
0~255	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.	255

- **TCP/UDP Parameters**

TCP/UDP Source Filter

Setting	Description	Factory Default
Any	No TCP/UDP source filter is specified	Any
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.

Setting	Description	Factory Default
0 ~ 65535	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.	0

TCP/UDP Source Range

Setting	Description	Factory Default
0 ~ 65535	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.	0-65535

TCP/UDP Destination Port Filter

Setting	Description	Factory Default
Any	No TCP/UDP destination filter is specified	Any
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 Port Number

Setting	Description	Factory Default
0 ~ 65535	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.	0

TCP/UDP Destination Range

Setting	Description	Factory Default
0 ~ 65535	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.	0-65535

TCP FIN

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

Setting	Description	Factory Default
0	TCP frames where the FIN field is set must not be able to match this entry.	Any
1	TCP frames where the FIN field is set must be able to match this entry.	
Any	Any value is allowed.	

TCP SYN

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

Setting	Description	Factory Default

0	TCP frames where the SYN field is set must not be able to match this entry.	Any
1	TCP frames where the SYN field is set must be able to match this entry.	
Any	Any value is allowed.	

TCP RST

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

Setting	Description	Factory Default
0	TCP frames where the RST field is set must not be able to match this entry.	Any
1	TCP frames where the RST field is set must be able to match this entry.	
Any	Any value is allowed.	

TCP PSH

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

Setting	Description	Factory Default
0	TCP frames where the PSH field is set must not be able to match this entry.	Any
1	TCP frames where the PSH field is set must be able to match this entry.	
Any	Any value is allowed.	

TCP ACK

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

Setting	Description	Factory Default
0	TCP frames where the ACK field is set must not be able to match this entry.	Any
1	TCP frames where the ACK field is set must be able to match this entry.	
Any	Any value is allowed.	

TCP URG

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

Setting	Description	Factory Default
0	TCP frames where the URG field is set must not be able to match this entry.	Any
1	TCP frames where the URG field is set must be able to match this entry.	
Any	Any value is allowed.	

- **Ethernet Type Parameters**

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

EtherType Filter

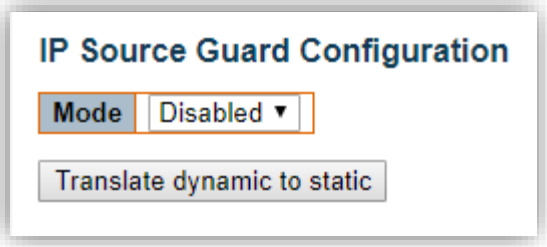
Setting	Description	Factory Default
Any	No EtherType filter is specified	Any
Specific	If you want to filter a specific EtherType filter with this ACE, you can enter a specific EtherType value. A field for entering a EtherType value appears.	

Ethernet Type Value

Setting	Description	Factory Default
0x600 ~ 0xFFFF excluding 0x800, 0x806, 0x86DD	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.	0xFFFF

Configuration > Security > Network > IP Source Guard > Configuration

- **IP Source Guard Configuration**

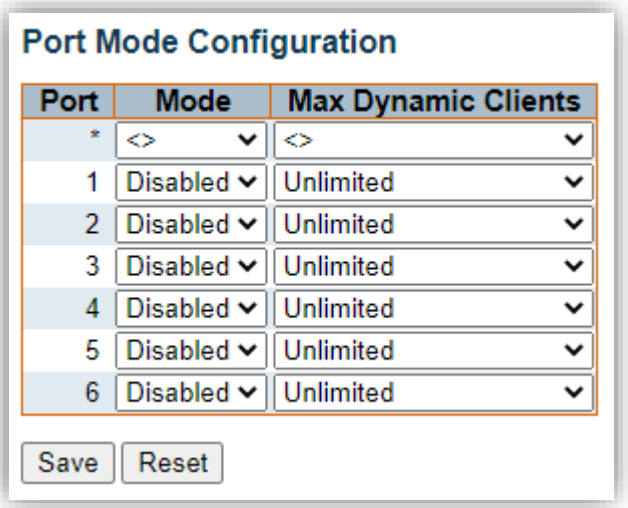


Mode

Setting	Description	Factory Default
Enabled	Enable the Global IP Source Guard. All configured ACEs will be lost when the mode is enabled.	Disabled
Disabled	Disable the Global IP Source Guard.	

Translate dynamic to static button
Click to translate all dynamic entries to static entries.

- **Port Mode Configuration**



Mode

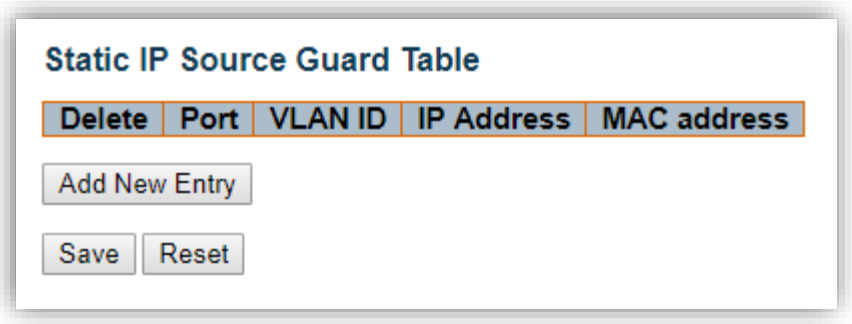
Setting	Description	Factory Default
Enabled	Port Mode is enabled	Disabled
Disabled	Port Mode is disabled	

Max Dynamic Clients

Setting	Description	Factory Default
0,1,2,Unlimited	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.	Unlimited

Configuration > Security > Network > IP Source Guard > Static Table

- **Static IP Source Guard Table**

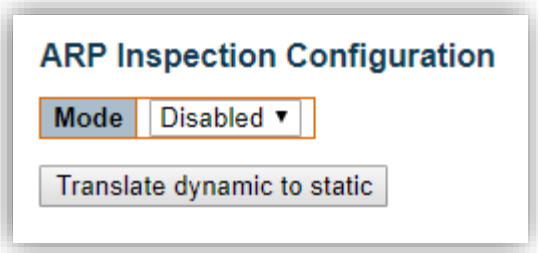


Add New Entry

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

Configuration > Security > Network > ARP Inspection > Port Configuration

- **ARP Inspection Configuration**



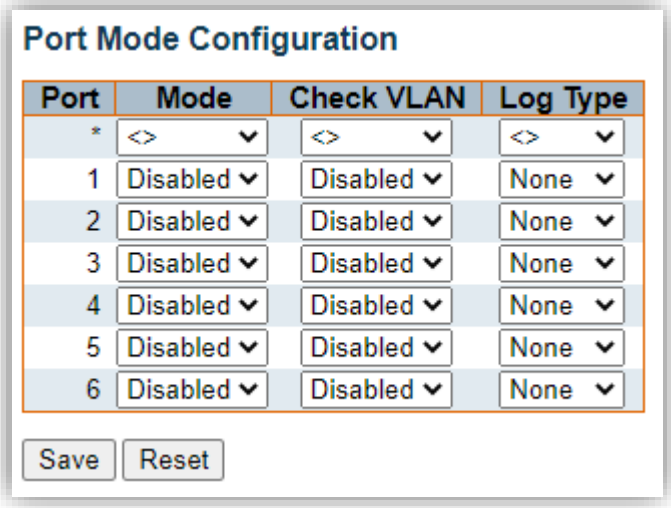
Mode

Setting	Description	Factory Default
Enabled	Enable the Global ARP Inspection	Disabled
Disabled	Disable the Global ARP Inspection	

Translate dynamic to static button
Click to translate all dynamic entries to static entries.

- **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.



Mode

Setting	Description	Factory Default
Enabled	Enable ARP Inspection operation.	Disabled
Disabled	Disable ARP Inspection operation.	

Check VLAN

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.

Setting	Description	Factory Default
Enabled	Enable check VLAN operation.	Disabled
Disabled	Disable check VLAN operation.	

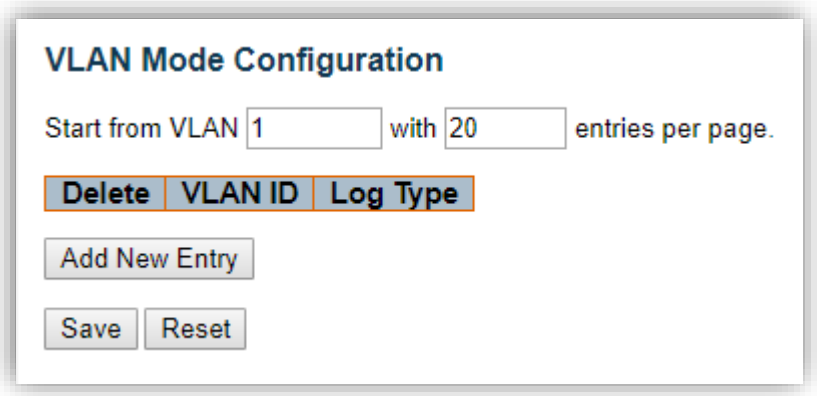
Log Type

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, the log type of ARP Inspection will refer to the port setting.

Setting	Description	Factory Default
None	Log nothing.	None
Deny	Log denied entries.	
Permit	Log permitted entries.	
ALL	Log all entries.	

Configuration > Security > Network > ARP Inspection > VLAN Configuration

- **VLAN Mode Configuration**



Navigating the VLAN Configuration
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.

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:

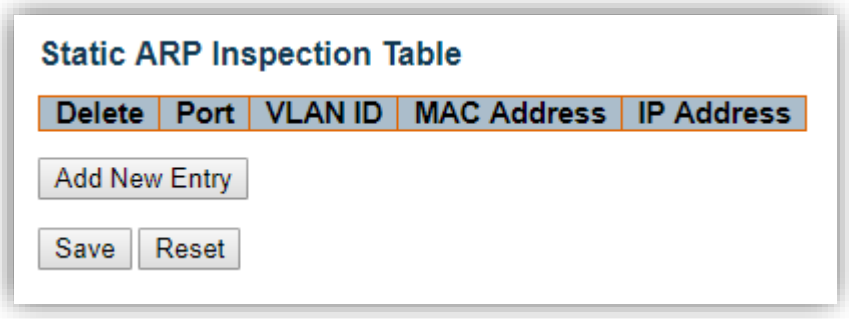
- **None:** Log nothing.
- **Deny:** Log denied entries.
- **Permit:** Log permitted entries.
- **ALL:** Log all entries.

Add New Entry Button
Click to add a new VLAN to the ARP Inspection VLAN table.

Configuration > Security > Network > ARP Inspection > Static Table

- **Static ARP Inspection Table**

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



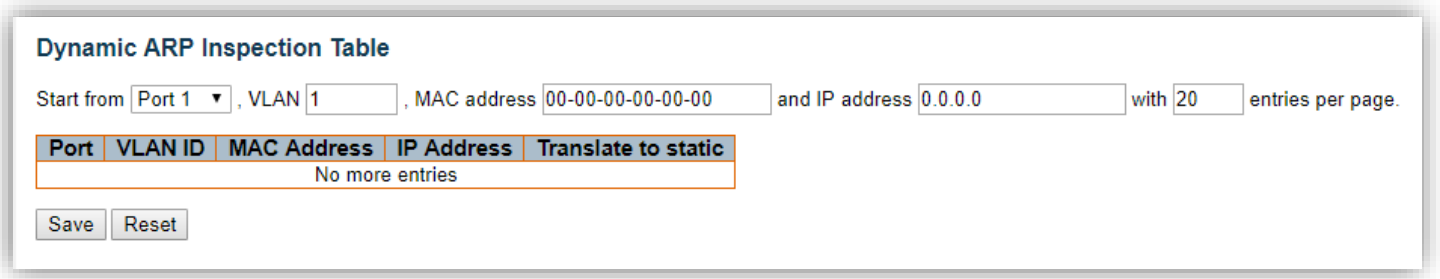
Add New Entry

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

Configuration > Security > Network > ARP Inspection > Dynamic Table

- **Dynamic ARP Inspection 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.



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.

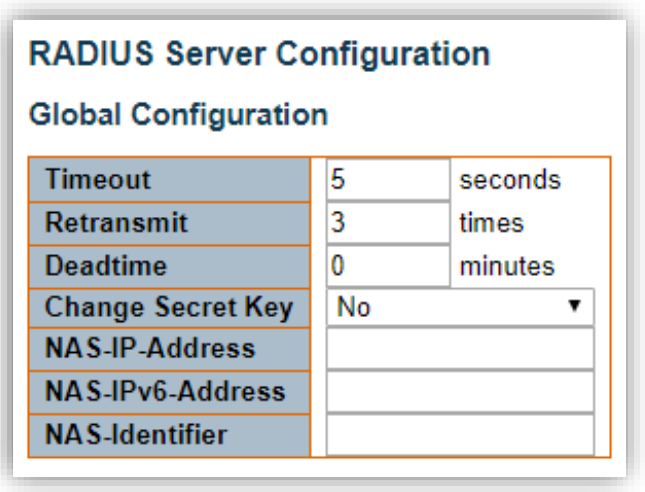
ARP Inspection Table Columns

Item	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.

Configuration > Security > AAA > RADIUS

- **RADIUS Server Configuration**

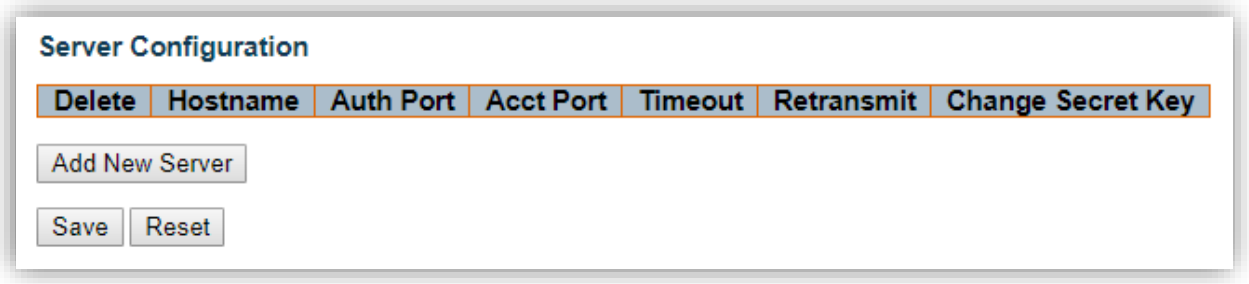
Global Configuration



Setting	Description	Factory Default
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.	5
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.	3
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.	0
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.	No
NAS-IP-Address	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.	None
NAS-IPv6-Address	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.	None
NAS-Identifier	The identifier - up to 253 characters long - to be used as attribute 32 in RADIUS Access-Request packets. If this field is left blank, the NAS-Identifier is not included in the packet.	None

Server Configuration

The table has one row for each RADIUS server and a number of columns.



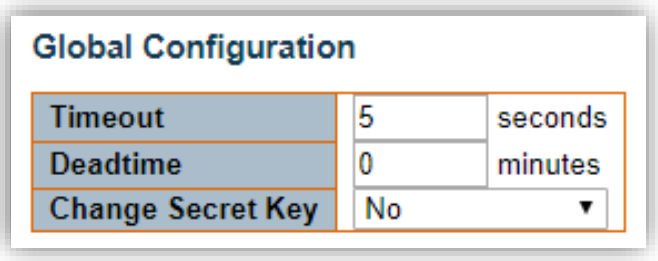
Setting	Description
Delete	To delete a RADIUS server entry, check this box. The entry will be deleted during the next Save.
Hostname	The IP address or hostname of the RADIUS server.
Auth Port	The UDP port to use on the RADIUS server for authentication. Set to 0 to disable authentication.
Acct Port	The 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	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.

“Add New Server” Button
Click “Add New Server” button 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 “Delete” button can be used to undo the addition of the new server.

Configuration > Security > AAA > TACACS+

- **TACACS+ Server Configuration**

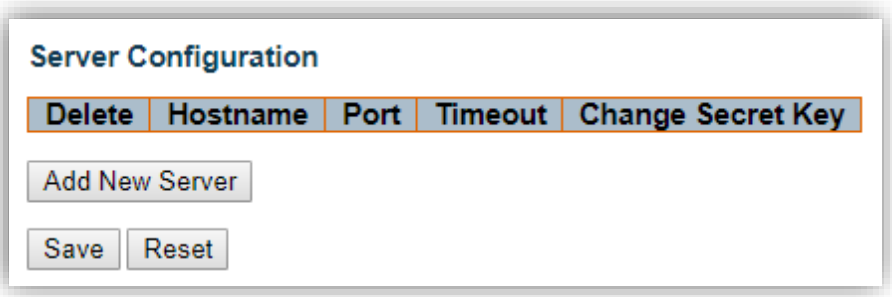
Global Configuration



Setting	Description
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.



Setting	Description
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.

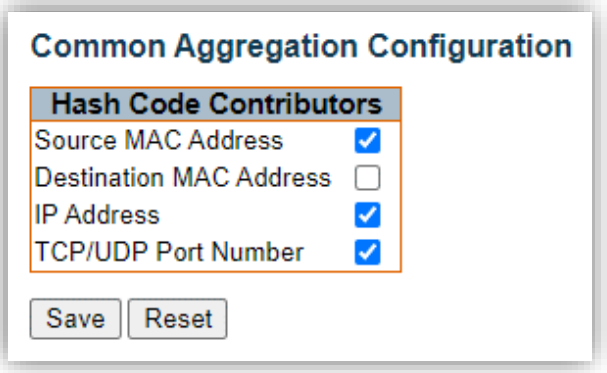
"Add New Server" Button

Click "Add New Server" button 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.

The "Delete" button can be used to undo the addition of the new server.

Configuration > Aggregation > Common

- **Common Aggregation Configuration**

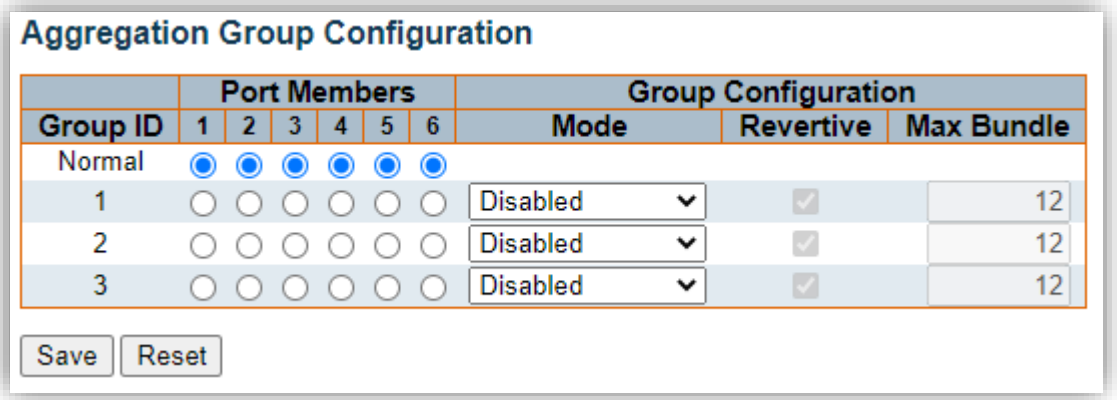


Hash Code Contributors

Setting	Description	Factory Default
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.	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.	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.	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.	Enabled

Configuration > Aggregation > Groups

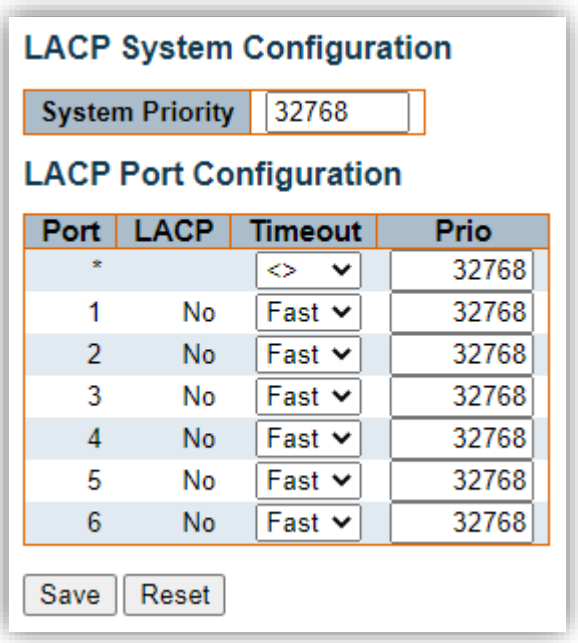
- **Aggregation Group Configuration**



Setting	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.

Configuration > Aggregation > LACP

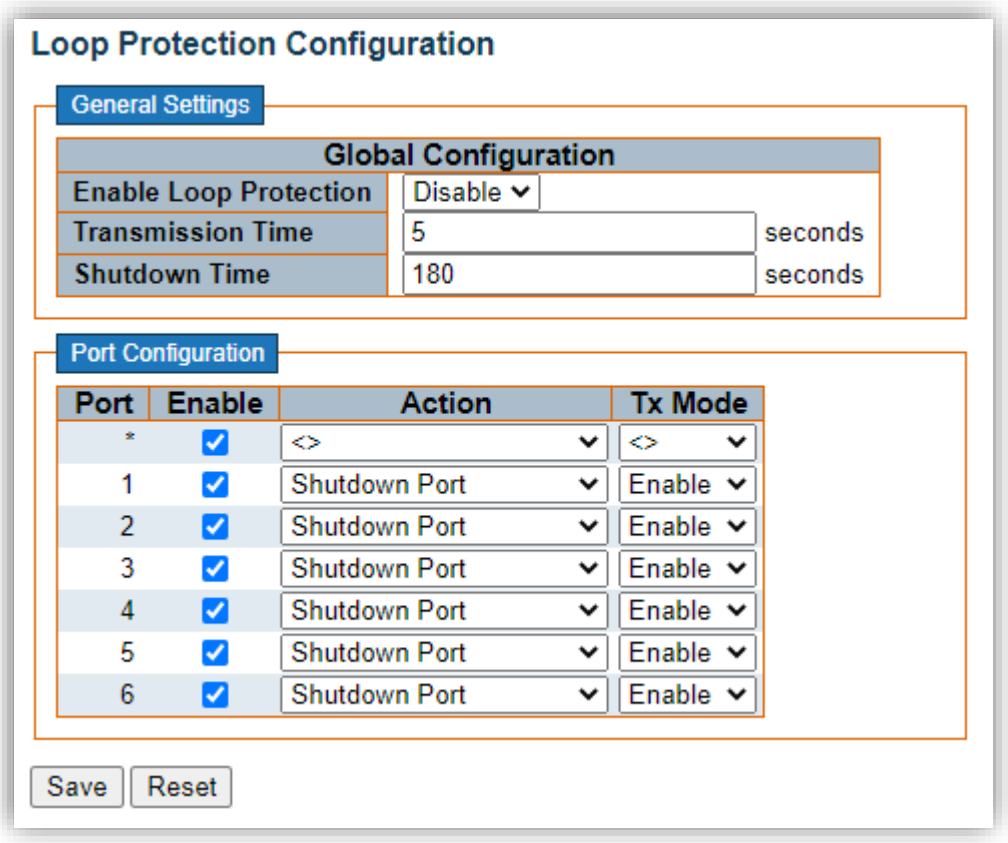
- **LACP Port Configuration**



Setting	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, range 1-65535. If the LACP partner wants to form a larger group than is supported by this device then this parameter will control which ports will be active and which ports will be in a backup role. Lower number means greater priority.

Configuration > Loop Protection

- **Loop Protection Configuration**



General Settings

Setting	Description	Factory Default
Enable Loop Protection	Controls whether loop protections is enabled (as a whole).	Disabled
Transmission Time	The interval between each loop protection PDU sent on each port.	5
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).	180

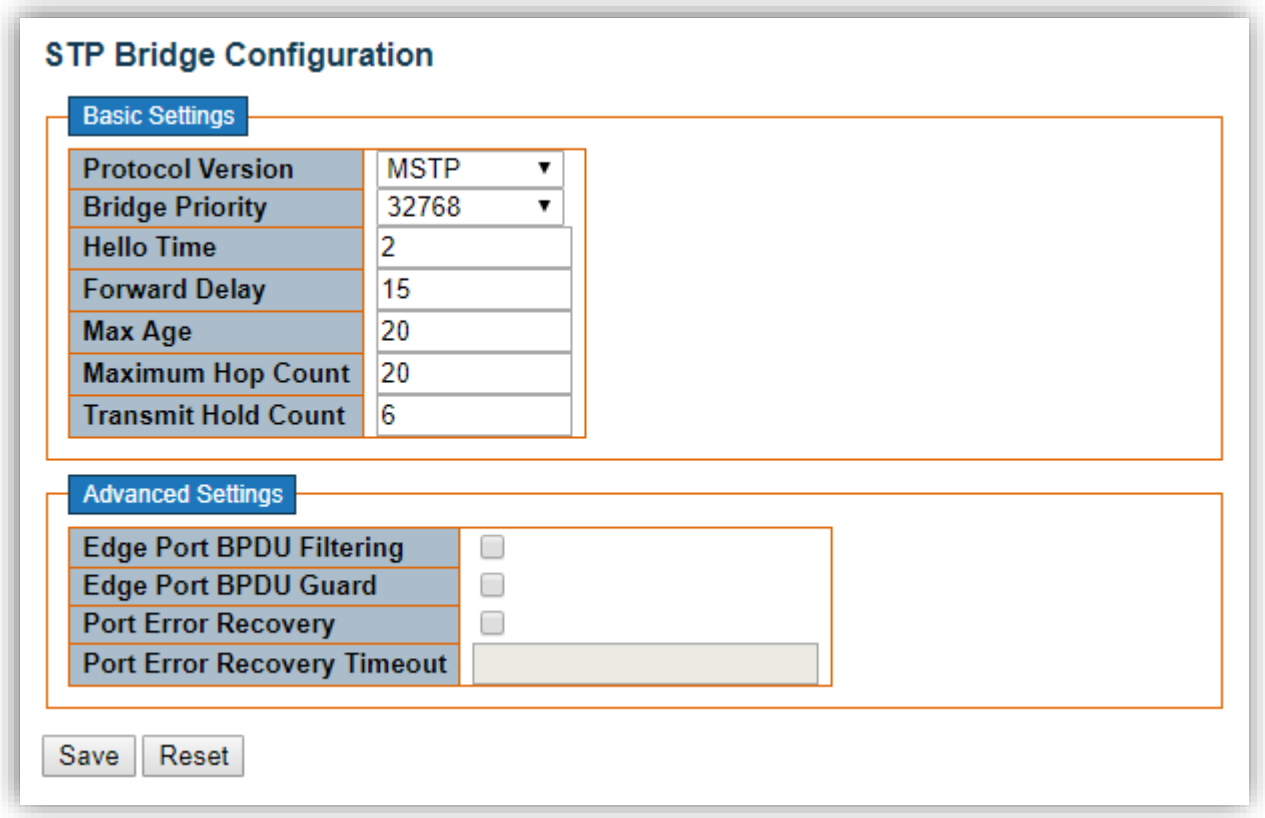
Port Configuration

Setting	Description
Port	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.

Configuration > Spanning Tree > Bridge Settings

- **STP Bridge Configuration**

This page allows you to configure STP system settings. The settings are used by all STP Bridge instances in the Switch.



Basic Settings

Setting	Description	Factory Default
Protocol Version	The MSTP / RSTP / STP protocol version setting. Valid values are **STP**, **RSTP** and **MSTP**.	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.	32768
Hello Time	The interval between sending STP BPDU's. Valid values are in the range 1 to 10 seconds. **NOTE:** Changing this parameter from the default value is not recommended, and may have adverse effects on your network.	2
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.	15

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.	20
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.	20
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.	6

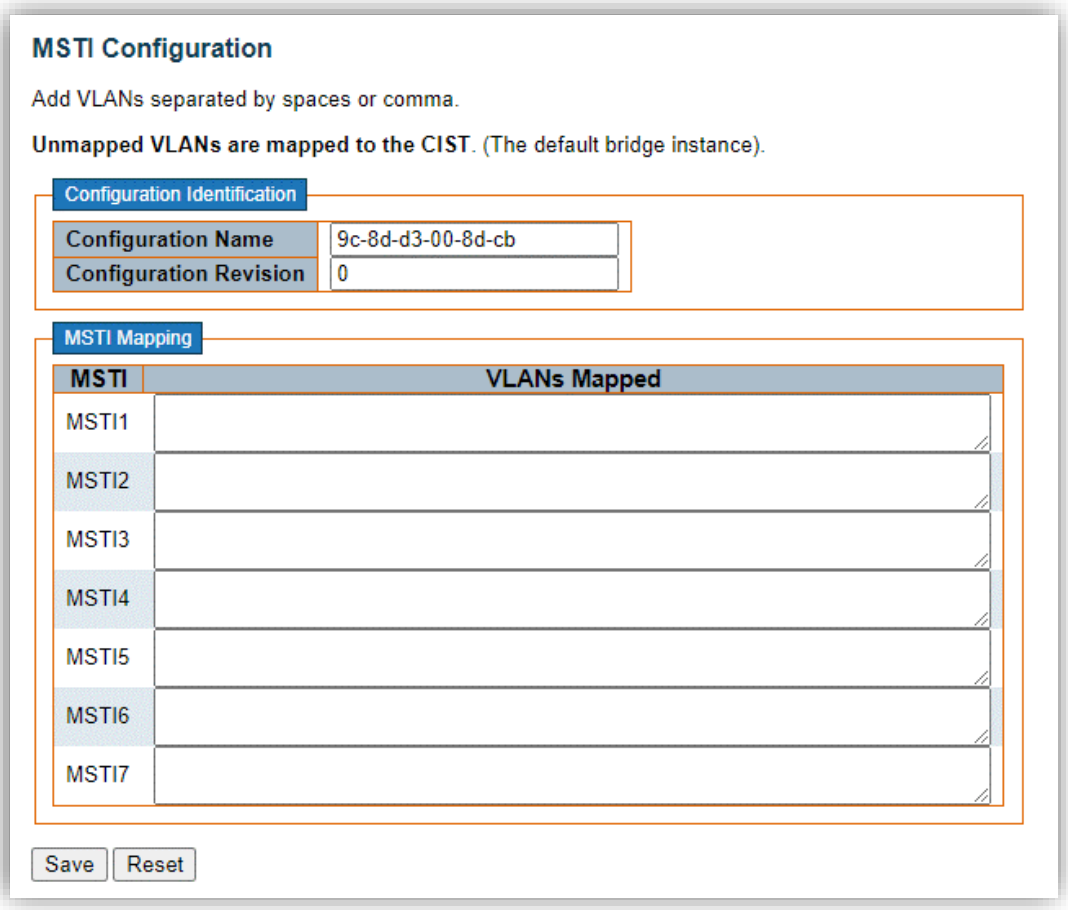
Advanced Settings

Setting	Description
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).

Configuration > Spanning Tree > MSTI Mapping

MSTI Configuration

This page allows the user to inspect the current STP MSTI bridge instance priority configurations.



Configuration Identification

Setting	Description
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.

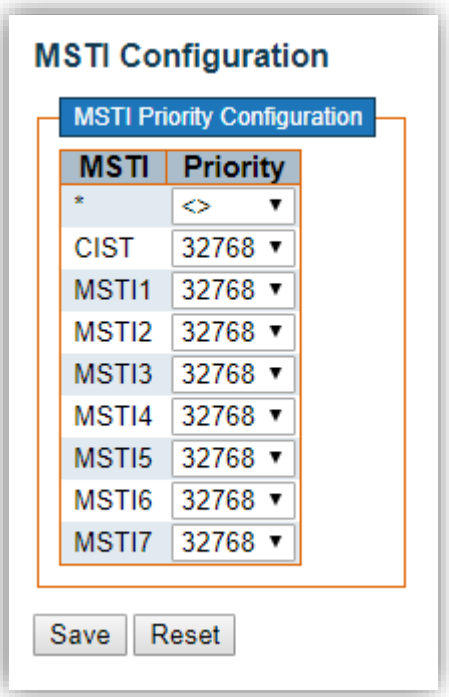
MSTI Mapping

Setting	Description
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**.

Configuration > Spanning Tree > MSTI Priorities

- **MSTI Configuration**

This page allows the user to inspect the current STP MSTI bridge instance priority configurations.



MSTI Priority Configuration

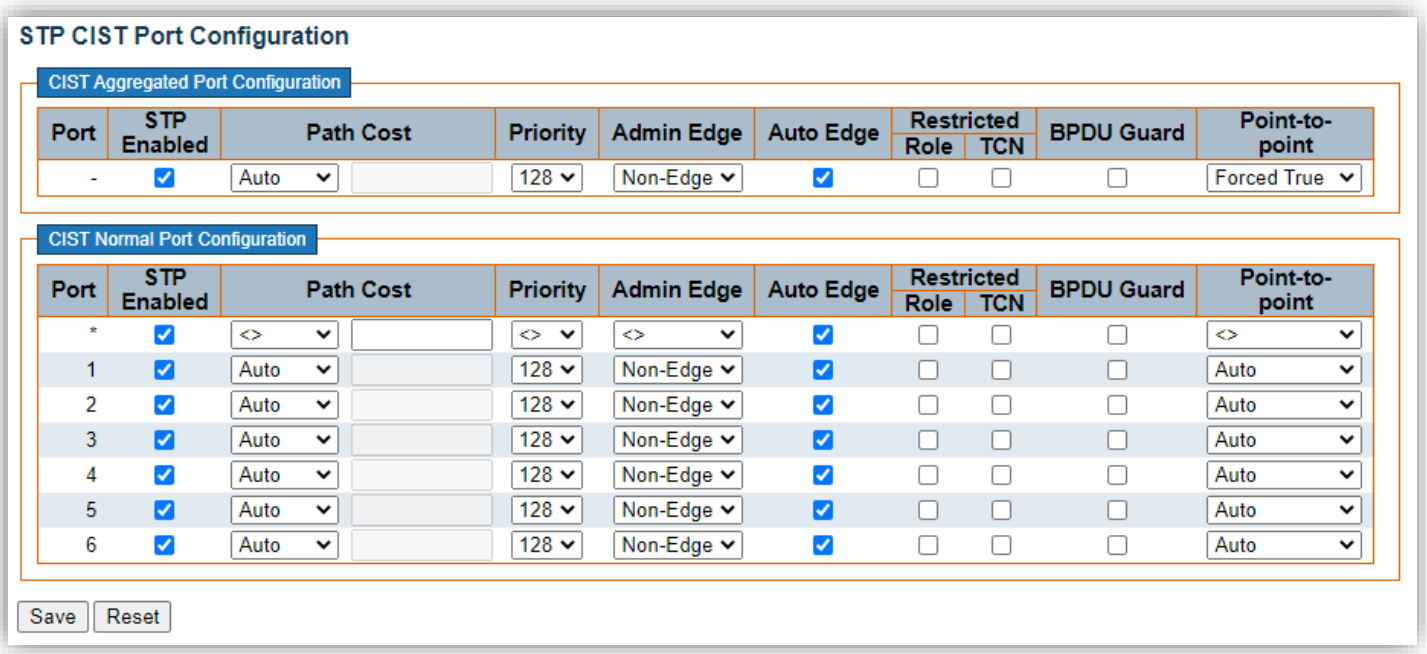
Setting	Description
MSTI	The bridge instance. The CIST is the default instance, which is always active.
Priority	Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier.

Configuration > Spanning Tree > CIST Ports

● STP CIST Port Configuration

This page 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.



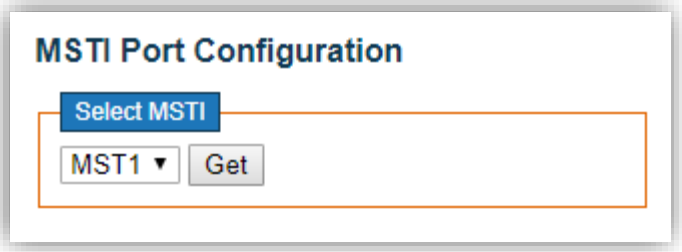
CIST Aggregated/ Normal Port Configuration

Setting	Description
Port	The switch port number of the logical STP port.
STP Enabled	Controls whether STP is enabled on this switch port.
Path Cost	Controls the path cost incurred by the port. The **Auto** setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the **Specific** setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favour of higher path cost ports. Valid values are in the range 1 to 200000000.
Priority	Controls the port priority. This can be used to control priority of ports having identical port cost.
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 effect this setting. A port entering error-disabled state due to this setting is subject to the bridge Port Error Recovery setting as well.
Point-to-Point	Controls whether the port connects to a point-to-point LAN rather than to a shared medium. This can be automatically determined, or forced either true or false. Transition to the forwarding state is faster for point-to-point LANs than for shared media.

Configuration > Spanning Tree > MSTI Ports

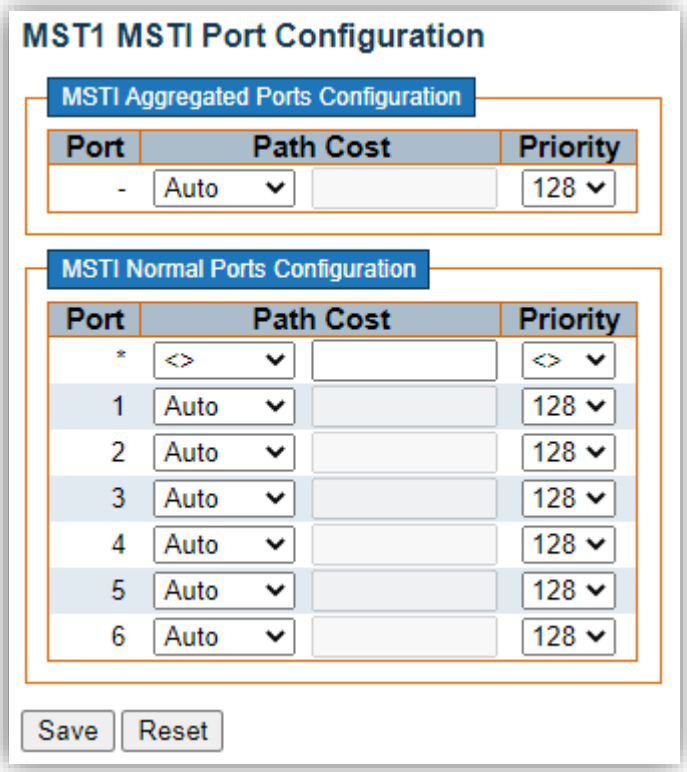
- **MSTI Port Configuration**



Select MSTI
Select **MSTI port number** and Click **"Get"** Button to configuration.

- **(MSTn) MSTI Port Configuration**

An MSTI port is a virtual port, which is instantiated separately for each active CIST (physical) port for each MSTI instance configured on and applicable to the port. The MSTI instance must be selected before displaying actual MSTI port configuration options.
This page contains MSTI port settings for physical and aggregated ports.



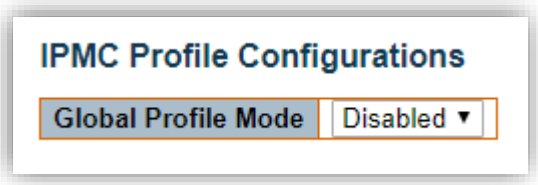
MSTI Aggregated/ Normal Ports Configuration

Setting	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 favour of higher path cost ports. Valid values are in the range 1 to 200000000.
Priority	Controls the port priority. This can be used to control priority of ports having identical port cost.

Configuration > IPMC Profile > Profile Table

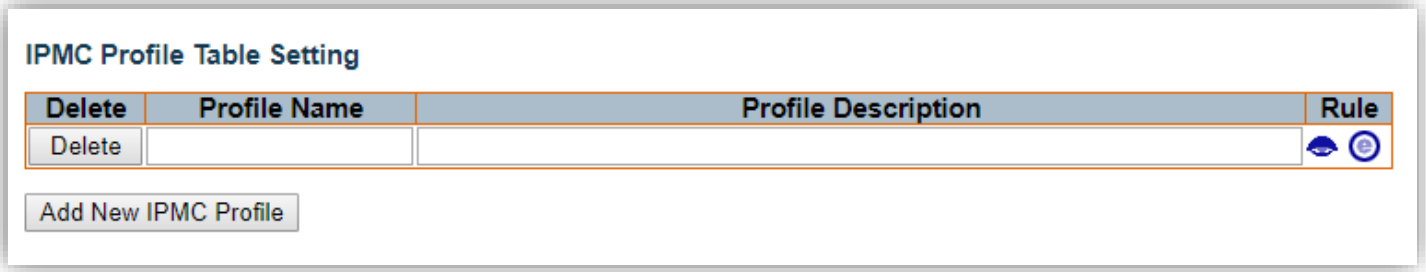
- **IPMC Profile Configurations**

This page provides IPMC Profile related configurations.
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.



Global Profile Mode
Enable/Disable the Global IPMC Profile.

- **IPMC Profile Table Setting**



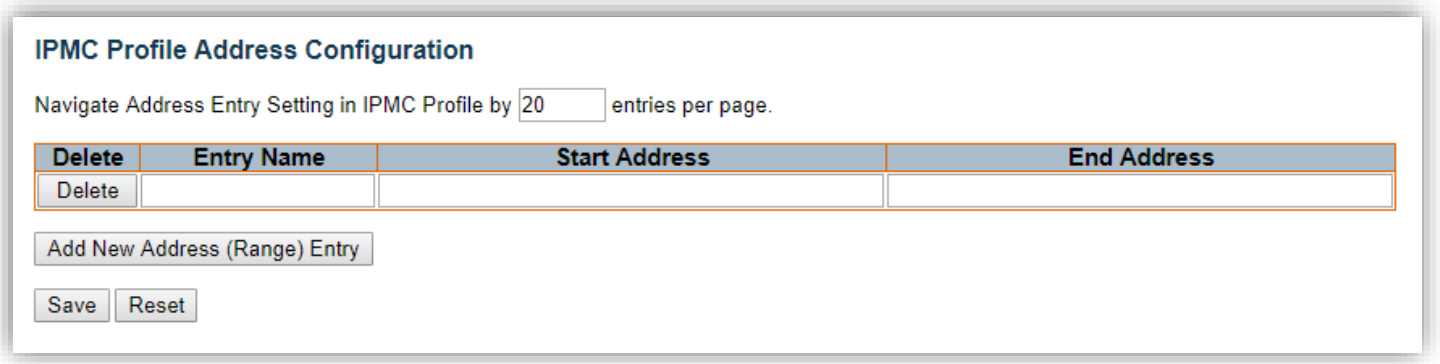
"Add New IPMC Profile" button
Click to add new IPMC profile. Specify the name and configure the new entry.

Setting	Description
Delete	Check to delete the entry. It 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.

Configuration > IPMC Profile > Address Entry

● IPMC Profile Address Configuration

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.



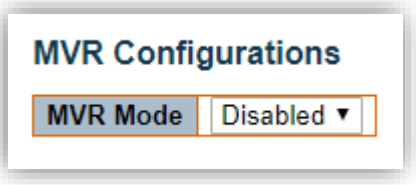
"Add New Address (Range) Entry" button

Setting	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Entry Name	The name used for indexing the address entry 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.
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.

Configuration > MVR

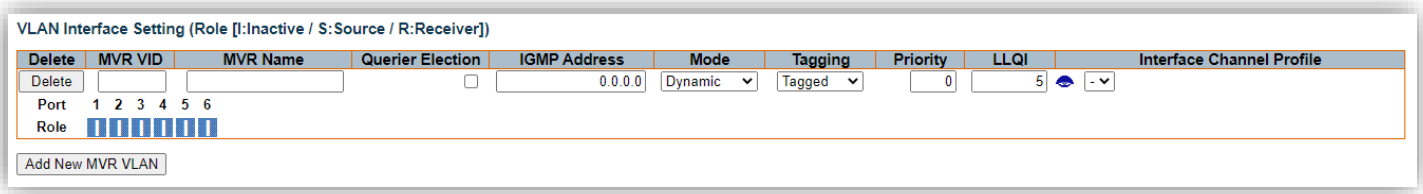
● MVR Configurations

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.
The Querier should to connect on the source port. By giving the static membership of MVR VLAN, device only forwards the IGMP reports from downstream(receiver ports) to upstream(source ports) and the Query packet which comes from the downstream will be ignored silently.
After the MVR VLAN members are properly configured, it is required to associate an IPMC profile with the specific MVR VLAN to be the expected channel. The channel profile is defined by the IPMC Profile which provides the filtering conditions. Notice that the profile only work when the global profile mode is enabled.
It is allowed to create at maximum 4 MVR VLANs with corresponding channel profile.



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.

● VLAN Interface Setting

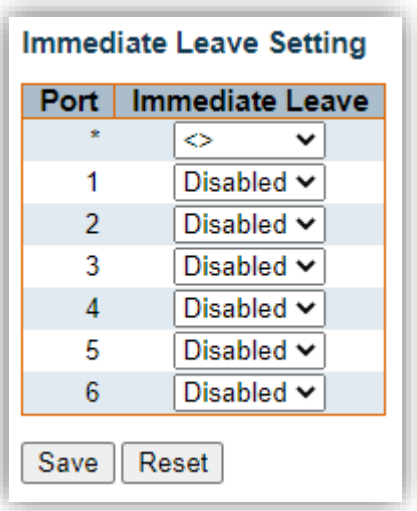


"Add New MVR VLAN" button

Setting	Description
Delete	Check to delete the entry. It will be deleted during the next save.
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 16. 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**	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.

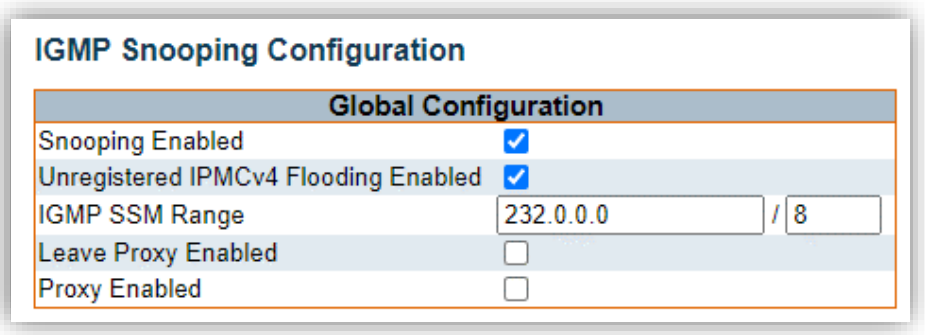
- **Immediate Leave Setting**



Setting	Description	Factory Default
Enabled	Enable the fast leave on the port. System will remove group record and stop forwarding data upon receiving the IGMPc2/MLDv1 leave message without sending last member query messages. It is recommend to enable this feature only when a single IGMPv2/MLDv1 host is connected to the specific port.	Disabled
Disabled	Disable the fast leave on the port.	

Configuration > IPMC > IGMP Snooping > Basic Configuration

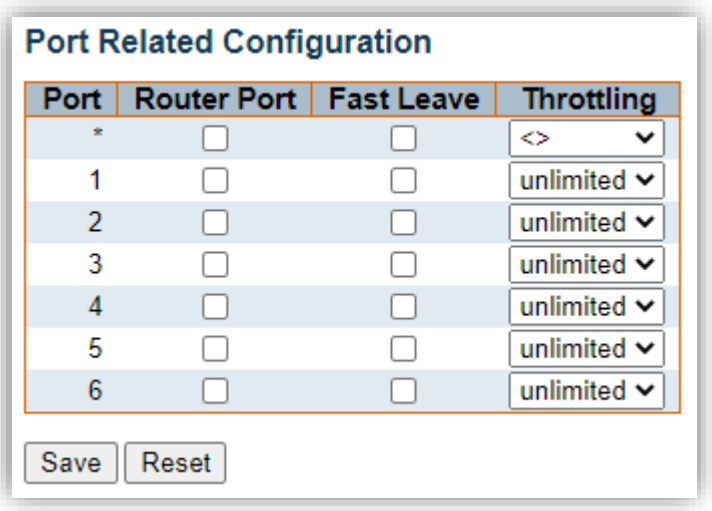
- **IGMP Snooping Configuration**



Global Configuration

Setting	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. Assign valid IPv4 multicast address as prefix with a prefix length (from 4 to 32) for the 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.

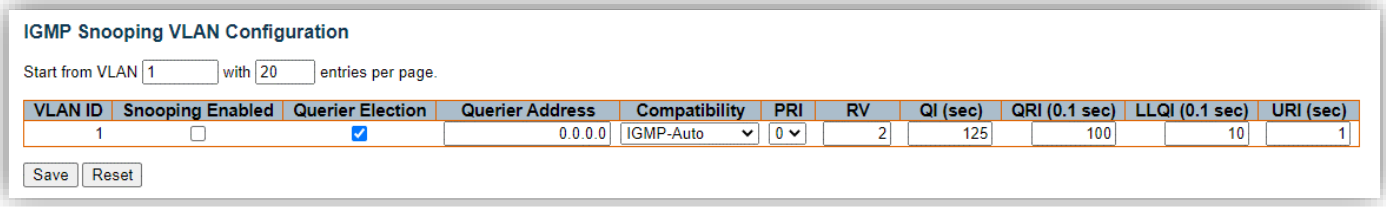
- **Port Related Configuration**



Setting	Description
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 recommend 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.

Configuration > IPMC > IGMP Snooping > VLAN Configuration

- **IGMP Snooping VLAN Configuration**



Navigating the IGMP Snooping VLAN Table

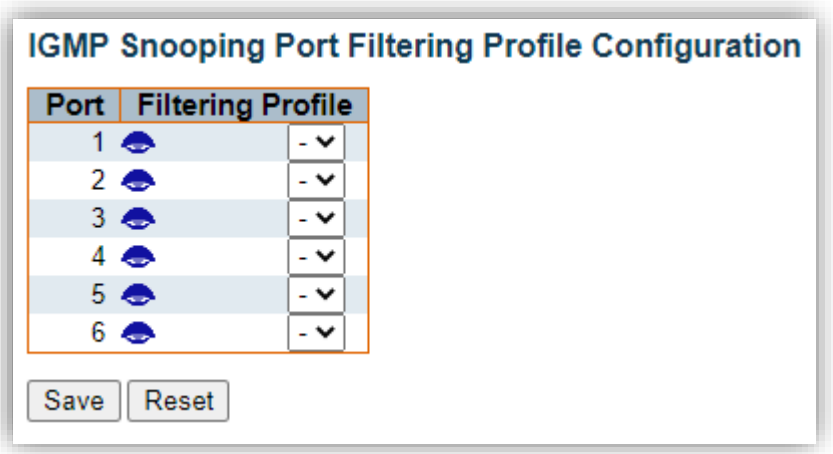
Each page shows up to 99 entries from the VLAN table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table.

Setting	Description
VLAN ID	The VLAN ID of the entry.
IGMP Snooping Enabled	Enable the per-VLAN IGMP Snooping. Up to **8** VLANs can be selected for IGMP Snooping.
Querier Election	Enable to join IGMP Querier election in the VLAN. Disable to act as an IGMP Non-Querier.
Querier Address	Define the IPv4 address as source address used in IP header for IGMP Querier election. When the Querier address is not set, system uses IPv4 management address of the IP interface associated with this VLAN. When the IPv4 management address is not set, system uses the first available IPv4 management address. Otherwise, system uses a pre-defined value. By default, this value will be 192.0.2.1.
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 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 (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.

Configuration > IPMC > IGMP Snooping > Port Filtering Profile

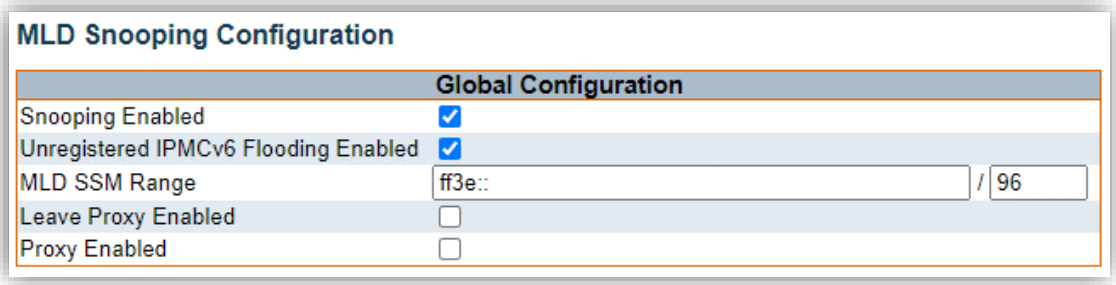
- **IGMP Snooping Port Filtering Profile Configuration**



Setting	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	List the rules associated with the designated profile.

Configuration > IPMC > MLD Snooping > Basic Configuration

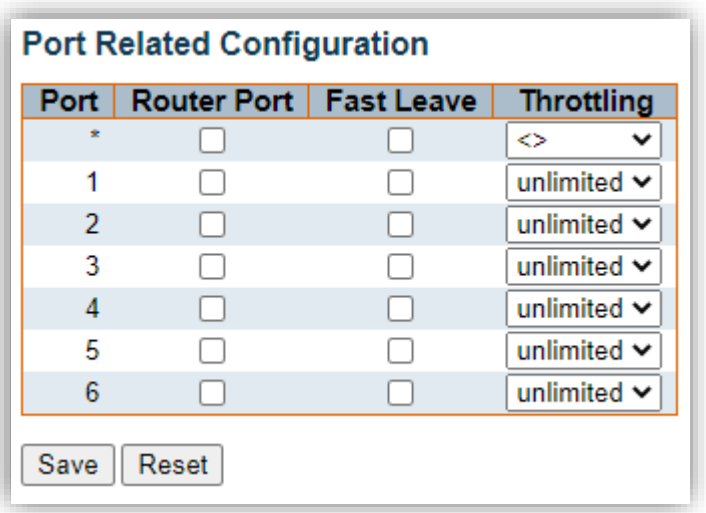
- **MLD Snooping Configuration**



Global Configuration

Setting	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.

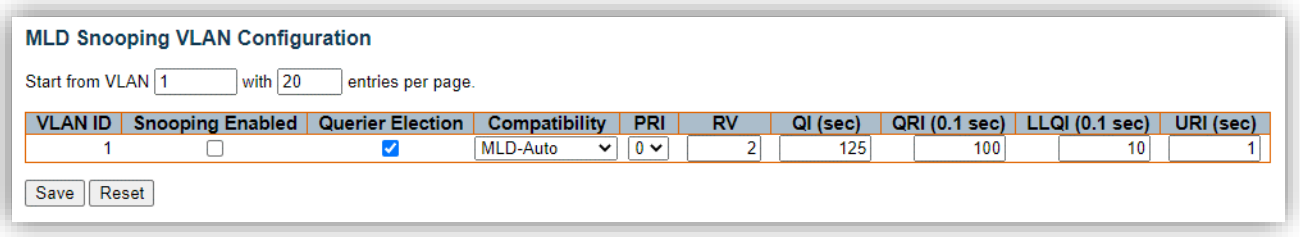
- **Port Releated Configuration**



Setting	Description
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.
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 recommend to enabled this feature only when a single MLDv1 host is connected to the specific port.
Throttling	Enable to limit the number of multicast groups to which a switch port can belong.

Configuration > IPMC > MLD Snooping > VLAN Configuration

- **MLD Snooping VLAN Configuration**



Navigating the MLD Snooping VLAN Table

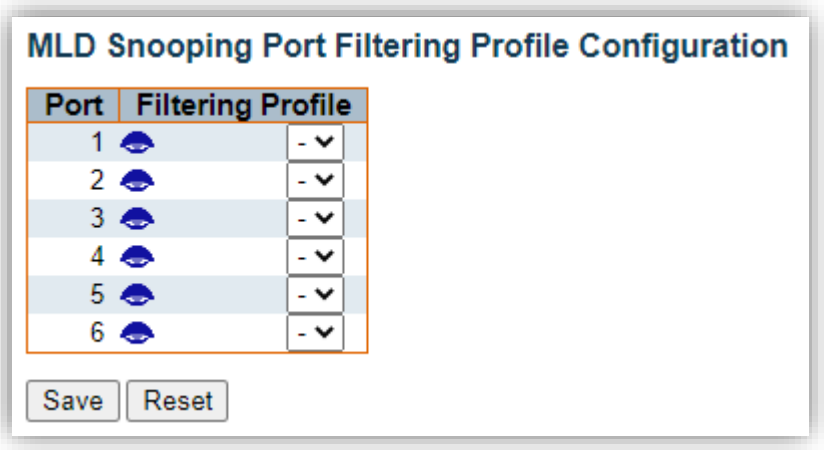
Each page shows up to 99 entries from the VLAN table, default being 20, selected through the entries per page input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table.

Setting	Description
VLAN ID	The VLAN ID of the entry.
Snooping Enabled	Enable the per-VLAN MLD Snooping. Up to **8** 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**, **Forced MLDv2**, 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.

Configuration > IPMC > MLD Snooping > Port Filtering Profile

- **MLD Snooping Port Filtering Profile Configuration**

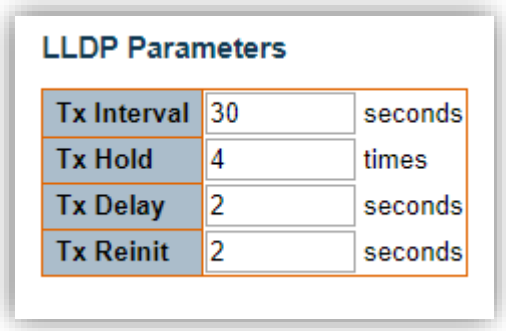


Setting	Description
Port	The logical port for the settings.
Filtering Profile	Select the IPMC Profile as the filtering condition for the specific port. Summary about the designated profile will be shown by clicking the view button.
 **Profile Management Button**	List the rules associated with the designated profile.

Configuration > LLDP > LLDP

- **LLDP Configuration**

LLDP Parameters



Tx Interval

Setting	Description	Factory Default
5 ~ 32768	The switch periodically transmits LLDP frames to its neighbors for having the network discovery information up-to-date. The interval between each LLDP frame is determined by the **Tx Interval** value. Valid values are restricted to 5 - 32768 seconds.	30

Tx Hold

Setting	Description	Factory Default
2 ~ 10	Each LLDP frame contains information about how long time the information in the LLDP frame shall be considered valid. The LLDP information valid period is set to **Tx Hold** multiplied by **Tx Interval** seconds. Valid values are restricted to 2 - 10 times.	4

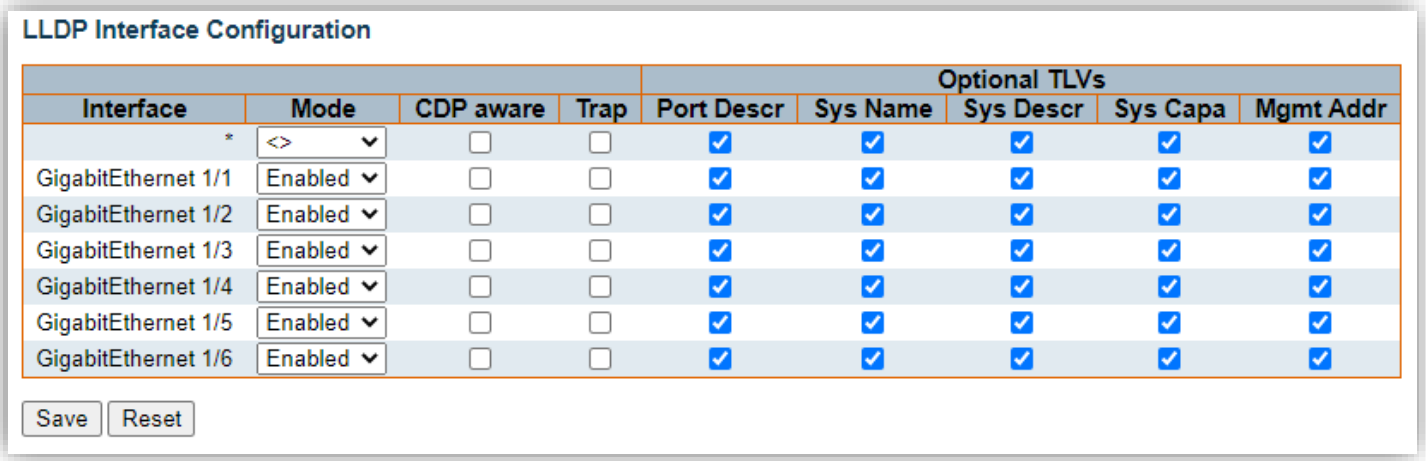
Tx Delay

Setting	Description	Factory Default
1 ~ 8192	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.	2

Tx Reinit

Setting	Description	Factory Default
1 ~ 10	When a interface is disabled, LLDP is disabled or the switch is rebooted, a LLDP shutdown frame is transmitted to the neighboring units, signaling that the LLDP information isn't valid anymore. **Tx Reinit** controls the amount of seconds between the shutdown frame and a new LLDP initialization. Valid values are restricted to 1 - 10 seconds.	2

LLDP Interface Configuration



Setting	Description
Interface	The switch interface name of the logical LLDP interface.
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 interface is enabled. Only CDP TLVs that can be mapped to a corresponding field in the LLDP neighbors' table are decoded. All other TLVs are discarded (Unrecognized CDP TLVs and discarded CDP frames are not shown in the LLDP statistics.). CDP TLVs are mapped onto LLDP neighbors' table as shown below. CDP TLV Device ID is mapped to the LLDP Chassis ID field. CDP TLV Address is mapped to the LLDP Management Address field. The CDP address TLV can contain multiple addresses, but only the first address is shown in the LLDP neighbors table. CDP TLV Port ID is mapped to the LLDP Port ID field. CDP TLV Version and Platform is mapped to the LLDP System Description field. Both the CDP and LLDP support system capabilities, but the CDP capabilities cover capabilities that are not part of the LLDP. These capabilities are shown as others in the LLDP neighbors' table. If all interfaces have CDP awareness disabled the switch forwards CDP frames received from neighbor devices. If at least one interface has CDP awareness enabled all CDP frames are terminated by the switch. **NOTE:** When CDP awareness on an interface is disabled the CDP information isn't removed immediately, but gets removed when the hold time is exceeded.
Port 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.

Configuration > LLDP > LLDP-MED

- **LLDP-MED Configuration**

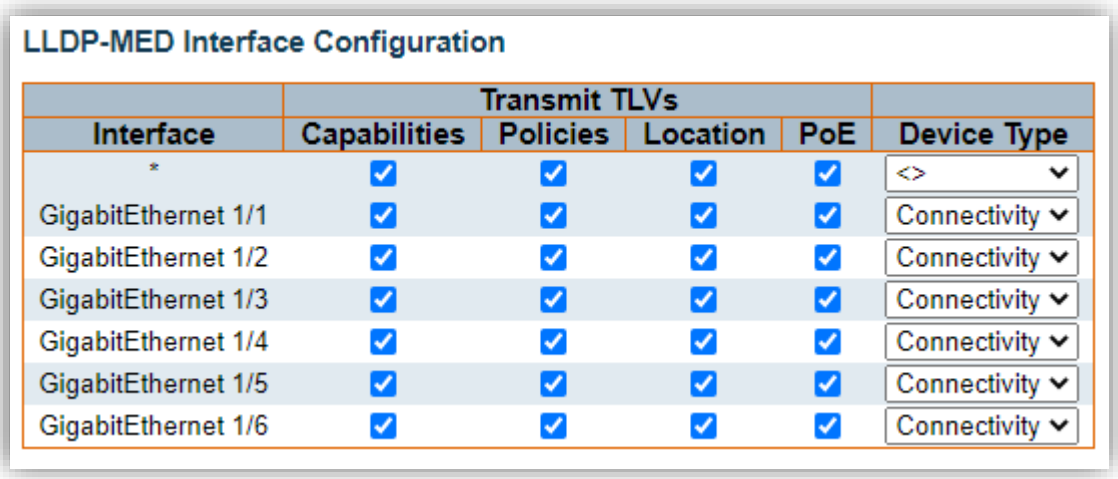
This page allows you to configure the LLDP-MED. This function applies to VoIP devices which support LLDP-MED.

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 interface. The LLDP-MED application will temporarily speed up the transmission of the LLDPDU to start within a second, when a new LLDP-MED neighbor has been detected in order share LLDP-MED information as fast as possible to new neighbors.
Because there is a risk of an LLDP frame being lost during transmission between neighbors, it is recommended to repeat the fast start transmission multiple times to increase the possibility of the neighbors receiving the LLDP frame. With **Fast start repeat count** it is possible to specify the number of times the fast start transmission would be repeated. The recommended value is 4 times, given that 4 LLDP frames with a 1 second interval will be transmitted, when an LLDP frame with new information is received.
It should be noted that LLDP-MED and the LLDP-MED Fast Start mechanism is only intended to run on links between LLDP-MED Network Connectivity Devices and Endpoint Devices, and as such does not apply to links between LAN infrastructure elements, including Network Connectivity Devices, or other types of links.

LLDP-MED Interface Configuration

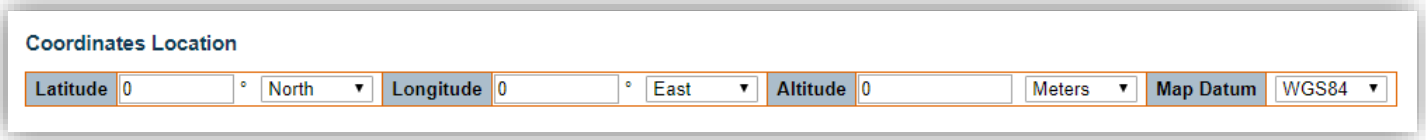
It is possible to select which LLDP-MED information that shall be transmitted to the neighbors. When the checkbox is checked the information is included in the frame transmitted to the neighbor.



Setting	Description
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

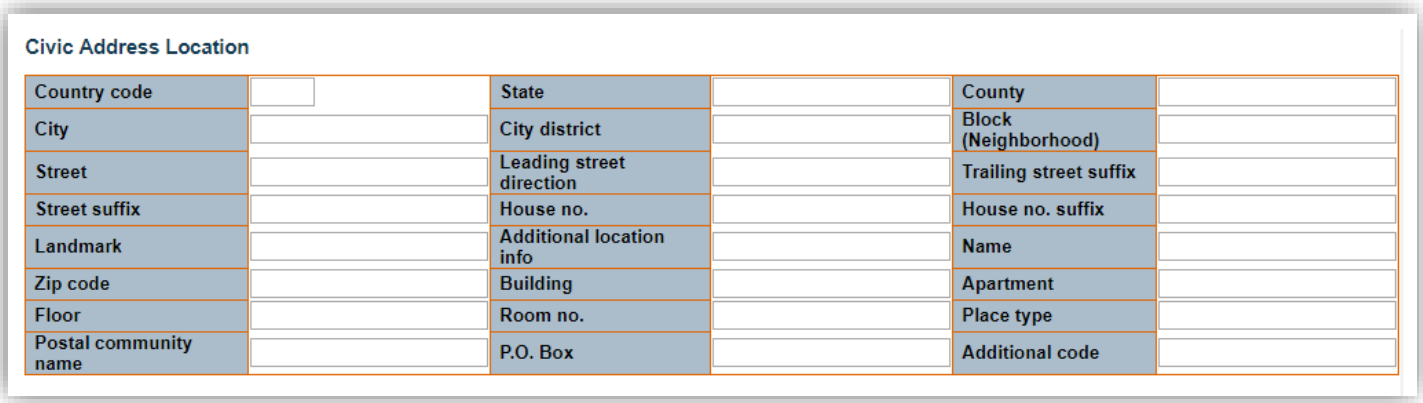


Setting	Description
Latitude	**Latitude** SHOULD be normalized to within 0-90 degrees with a maximum of 4 digits. It is possible to specify the direction to either **North** of the equator or **South** of the equator.
Longitude	**Longitude** SHOULD be normalized to within 0-180 degrees with a maximum of 4 digits. It is possible to specify the direction to either **East** of the prime meridian or **West** of the prime meridian.
Altitude	**Altitude** SHOULD be normalized to within -2097151.9 to 2097151.9 with a maximum of 1 digits. It is possible to select between two altitude types (floors or meters). • **Meters:** Representing meters of Altitude defined by the vertical datum specified. • **Floors:** Representing altitude in a form more relevant in buildings which have different floor-to-floor dimensions. An altitude = 0.0 is meaningful even outside a building, and represents ground level at the given latitude and longitude. Inside a building, 0.0 represents the floor level associated with ground level at the main entrance.
Map Datum	The **Map Datum** is used for the coordinates given in these options: • **WGS84:** (Geographical 3D) - World Geodesic System 1984, CRS Code 4327, Prime Meridian Name: 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). The total number of characters for the combined civic address information must not exceed 250 characters.
A couple of notes to the limitation of 250 characters.

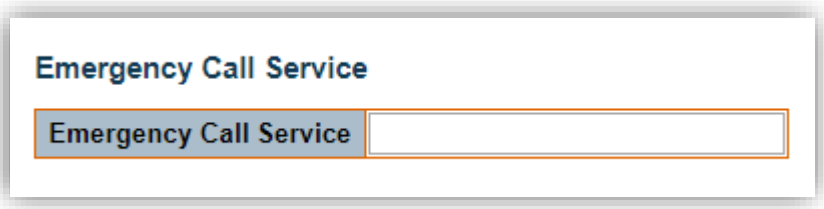
1. A non-empty civic address location will use 2 extra characters in addtion to the civic address location text.
2. The 2 letter country code is not part of the 250 characters limitation.



Setting	Description
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 (Neighborhood)	Neighborhood, 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	(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 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

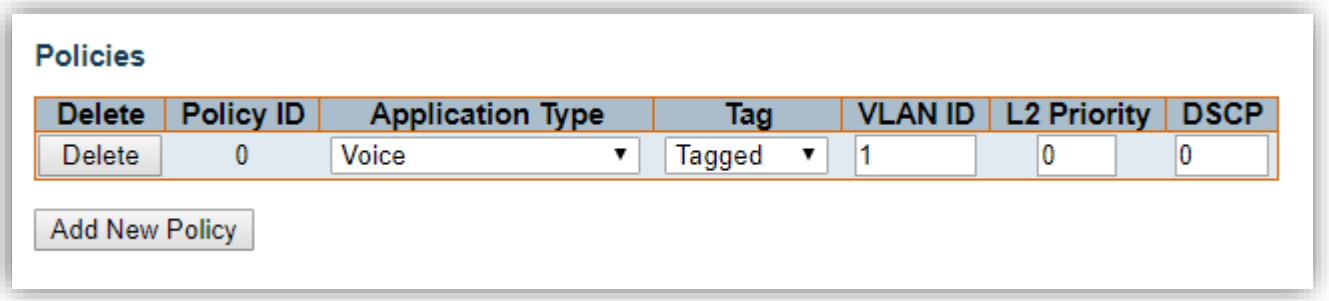
Network Policy Discovery enables the efficient discovery and diagnosis of mismatch issues with the VLAN configuration, along with the associated Layer 2 and Layer 3 attributes, which apply for a set of specific protocol applications on that port. Improper network policy configurations are a very significant 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.



Setting	Description
Delete	Check to delete the policy. It will be deleted during the next save.
Policy ID	ID for the policy. This is auto generated and shall be used when selecting the policies that shall be mapped to the specific interfaces.

Application Type	Intended use of the application types: 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 interface as defined in IEEE 802.1Q-2003.
L2 Priority	L2 Priority is the Layer 2 priority to be used for the specified application type. L2 Priority may specify one of eight priority levels (0 through 7), as defined by IEEE 802.1D-2004. A value of 0 represents use of the default priority as defined in IEEE 802.1D-2004.

DSCP	DSCP value to be used to provide Diffserv node behaviour for the specified application type as defined in IETF RFC 2474. DSCP may contain one of 64 code point values (0 through 63). A value of 0 represents use of the default DSCP value as defined in RFC 2475.
Adding a new policy	Click "**Add New Policy**" button to add a new policy. Specify the Application type, Tag, VLAN ID, L2 Priority and DSCP for the new policy. Click "Save". The number of policies supported is 32

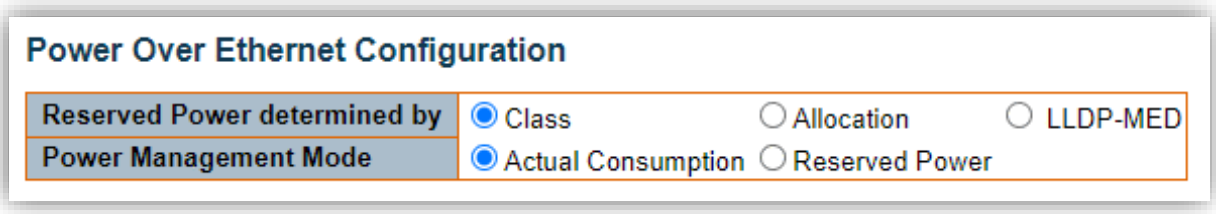
Policies Interface Configuration

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

Setting	Description
Interface	The interface name to which the configuration applies.
Policy Id	The set of policies that shall apply to a given interface. The set of policies is selected by check marking the checkboxes that corresponds to the policies.

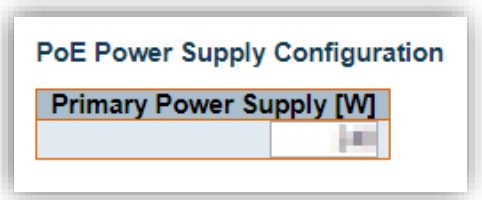
Configuration > PoE > Power Budget

- **Power Over Ethernet Configuration**



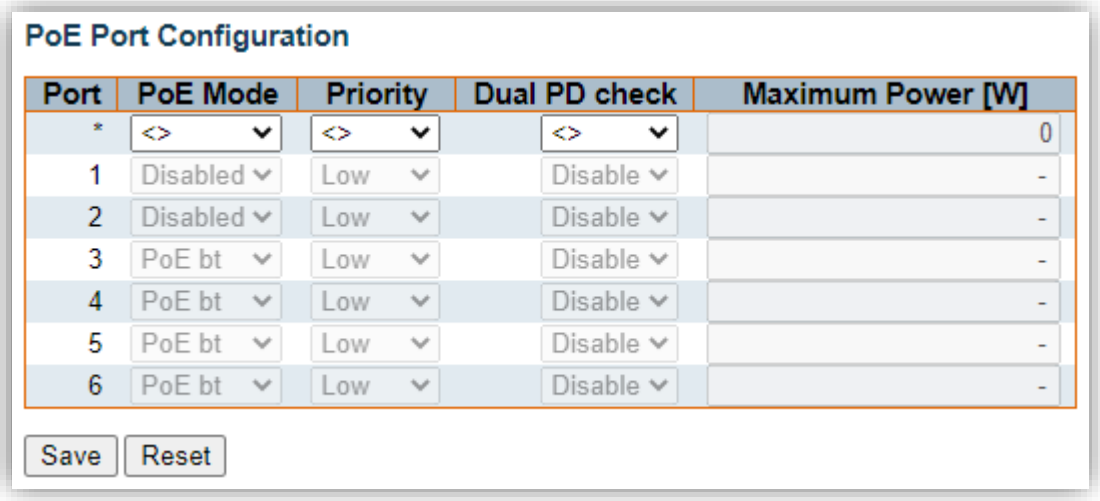
Setting	Description
Reserved Power determined by	There are three modes for configuring how the ports/PDsmay reserve power. 1. **Allocated mode:** In this mode the user allocates the amount of power that each port may reserve. The allocated/reserved power for each port/PD is specified in the Maximum Power fields. 2. **Class mode:** In this mode each port automatically determines how much power to reserve according to the class the connected PD belongs to, and reserves the power accordingly. Four different port classes exist and one for 4, 7, 15.4 or 30 Watts. In this mode the Maximum Power fields have no effect. 3. **LLDP-MED mode:** This mode is similar to the Class mode expect that each port determine the amount power it reserves by exchanging PoE information using the LLDP protocol and reserves power accordingly. If no LLDP information is available for a port, the port will reserve power using the class mode. In this mode the Maximum Power fields have no effect **For all modes:** If a port uses more power than the reserved power for the port, the port is shut down.
Power Management Mode	There are 2 modes for configuring when to shut down the ports: 1. **Actual Consumption:** In this mode the ports are shut down when the actual power consumption for all ports exceeds the amount of power that the power supply can deliver or if the actual power consumption for a given port exceeds the reserved power for that port. The ports are shut down according to the ports priority. If two ports have the same priority the port with the highest port number is shut down. 2. **Reserved Power:** In this mode the ports are shut down when total reserved powered exceeds the amount of power that the power supply can deliver. In this mode the port power is not turned on if the PD requests more power than available from the power supply.

- **PoE Power Supply Configuration**



Setting	Description
Primary Power Supply [W]	For being able to determine the amount of power the PD may use, it must be defined what amount of power a power source can deliver. Valid values are in the range 0 to 240 Watts.

- **PoE Port Configuration**

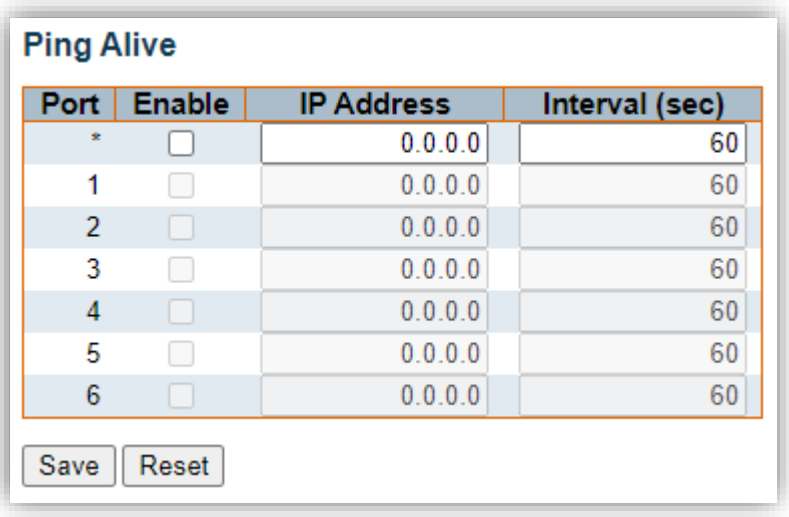


Setting	Description
PoE Mode	The PoE Mode represents the PoE operating mode for the port. • **Disabled:** PoE disabled for the port. • **PoE :** Enables PoE IEEE 802.3af (Class 4 PDs limited to 15.4W) • **PoE+ :** Enables PoE+ IEEE 802.3at (Class 4 PDs limited to 30W) • **PoE bt:** Enables PoE bt IEEE 802.3bt (Class 8 PDs limited to 90W)
Priority	The Priority represents the ports priority. There are three levels of power priority named **Low, High** and **Critical**. The priority is used in the case where the remote devices requires more power than the power supply can deliver. In this case the port with the lowest priority will be turn off starting from the port with the highest port number.
Dual PD check	When **Dual PD check** is set, if an invalid detection signature is discovered on either channel, port n will not perform classification or grant power on requests. When Dual PD check is clear, port n will detect, classify and service power on request for either channel regardless of the detection result on the other channel.
Maximum Power	The Maximum Power value contains a numerical value that indicates the maximum power in watts that can be delivered to a remote device. The maximum allowed value is 90 W.

Configuration > PoE > Ping Alive

- **Ping Alive**

This page allows to give the user control over the system's Powered Device failure check.



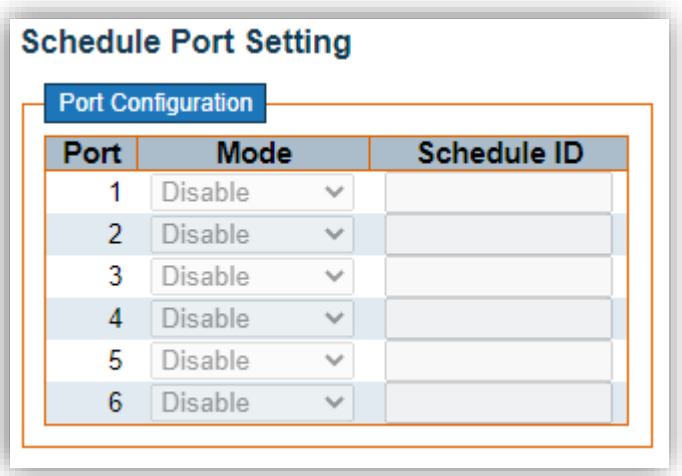
Port Configuration

Setting	Description
Port	The switch port number of the port.
Enable	Controls whether poe ping alive is enabled on this switch port.
IP Address	The IP for the Powered Device.
Interval	The time for IP checking period.

Configuration > PoE > Schedule

- **Schedule Port Setting**

This page divided into Port Configuration and Schedule Setting parts. Port Configuration allows to give the user set PoE schedule identifier and PoE schedule mode for each PoE port. Schedule Setting allows to give the user add new schedule timetabling.



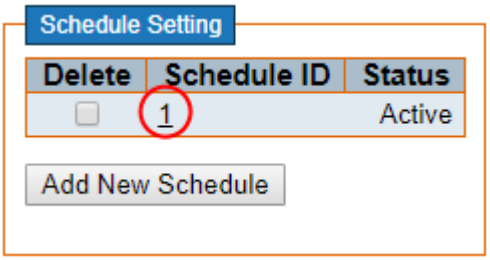
Port Configuration

Setting	Description
Port	The switch port number of the port.
Mode	**Disable:** Disable schedule operation. **Schedule On:** If current time is within the range of schedule limitation, PSE will be provide PD with power. **Schedule Off:** If current time is within the range of schedule limitation, PSE will not be provide PD with power.
Schedule ID	Controls whether schedule need to be executed. Schedule id is range from 1 to 32.

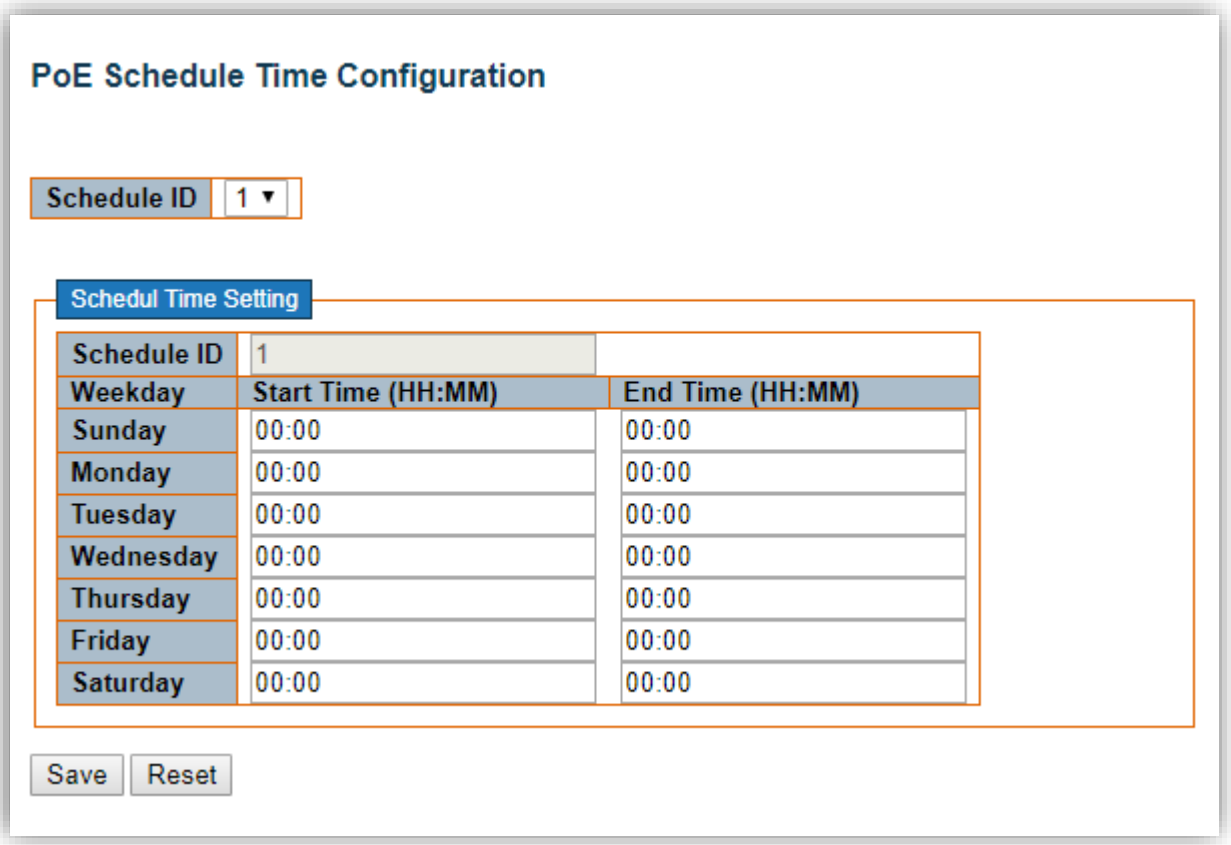
Schedule Setting

Setting	Description
Schedule ID	PoE schedule id. Schedule id is range from 1 to 32.
Status	PoE schedule status.

- **PoE Schedule Time Configuration**



Click **"Scheduled Setting"** schedule ID number to edit PoE schedule time configuration

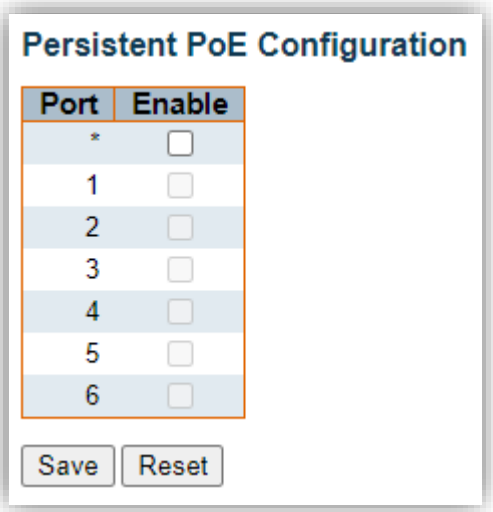


Setting	Description
Schedule ID	The schedule id number of the schedule.
Time	**Start Time:** Time tabling start time. Format: hh:mm; hh: 00 ~ 24, mm: 00 ~ 59. **End Time:** Time tabling end time. Format: hh:mm; hh: 00 ~ 24, mm: 00 ~ 59.

Configuration > PoE > Persistent PoE

- **Persistent PoE Configuration**

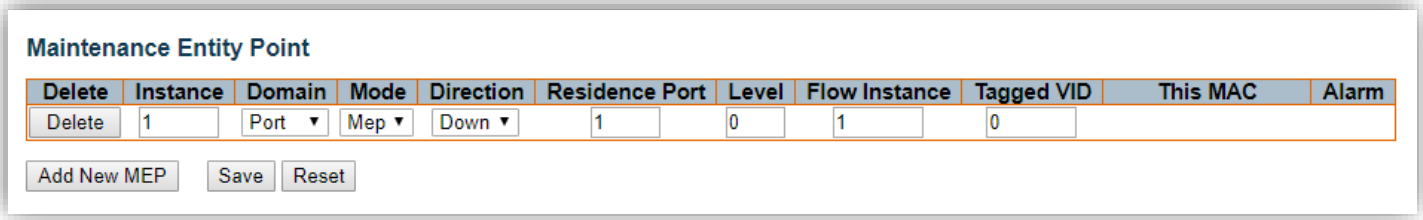
When the switch do the reset & FW upgrade, the PSE (PoE Switch) can continue provide the PoE power for PD.



Setting	Description	Factory Default
Enabled	Enable Persistent PoE operation.	Disabled
Disabled	Disable Persistent PoE operation.	

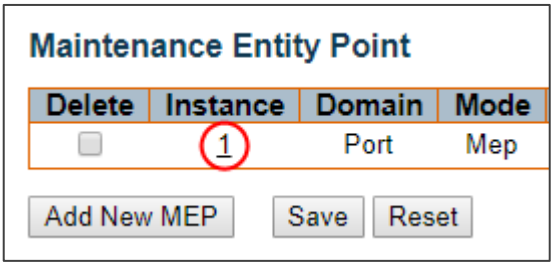
Configuration > MEP

- **Maintenance Entity Point**



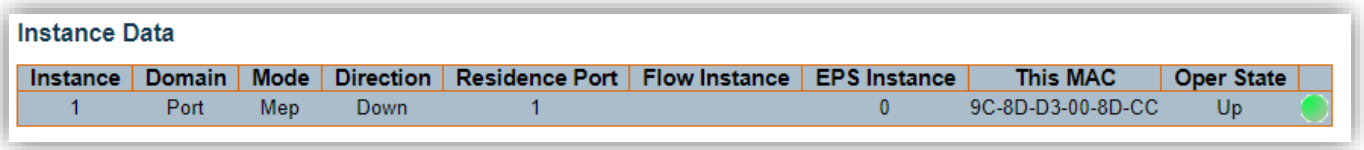
Setting	Description
Delete	This box is used to mark a MEP for deletion in next Save operation.
Instance	The ID of the MEP. Click on the ID of a MEP to enter the configuration page. The range is from **1** through **100**.
Domain	**Port:** This is a MEP in the Port Domain.
Mode	**MEP:** This is a Maintenance Entity End Point. **MIP:** This is a Maintenance Entity Intermediate Point.
Direction	**Down:** This is a Down MEP - monitoring ingress OAM and traffic on Residence Port. **Up:** This is a Up MEP – monitoring egree OAM and traffic on 'Residence Port'.
Residence Port	The port where MEP is monitoring - see 'Direction'. For a EVC MEP the port must be a port in the EVC. For a VLAN MEP the port must be a VLAN member.
Level	The MEG level of this MEP.
Flow Instance	The MEP is related to this flow - See 'Domain'. This is not relevant and not shown in case of Port MEP.
Tagged VID	**Port MEP:** An outer C/S-tag (depending on VLAN Port Type) is added with this VID. Entering '0' means no TAG added. **EVC MEP:** This is not used. **VLAN MEP:** This is not used. **EVC MIP:** On Serval, this is the Subscriber VID that identify the subscriber flow in this EVC where the MIP is active.
This MAC	The MAC of this MEP - can be used by other MEP when unicast is selected (Info only).
Alarm	There is an active alarm on the MEP.

- **MEP Configuration**



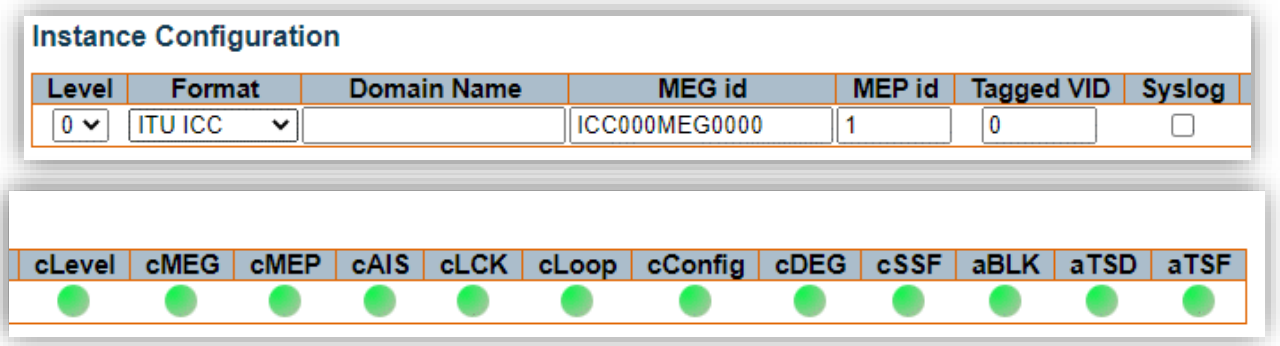
Click **"Maintenance Entity Point"** Instance number to edit MEP configuration

Instance Data



Setting	Description
Instance	The ID of the MEP.
Domain	**Port:** This is a MEP in the Port Domain.
Mode	**MEP:** This is a Maintenance Entity End Point. **MIP:** This is a Maintenance Entity Intermediate Point.
Direction	**Down:** This is a Down MEP - monitoring ingress OAM and traffic on Residence Port. **Up:** This is a Up MEP
Residence Port	The port where MEP is monitoring - see 'Direction'. For a EVC MEP the port must be a port in the EVC. For a VLAN MEP the port must be a VLAN member.
Flow Instance	The MEP is related to this flow - See 'Domain'. This is not relevant and not shown in case of Port MEP.
Tagged VID	**Port MEP:** An outer C/S-tag (depending on VLAN Port Type) is added with this VID. Entering '0' means no TAG added. **EVC MEP:** This is not used. **VLAN MEP:** This is not used. **EVC MIP:** On Serval, this is the Subscriber VID that identify the subscriber flow in this EVC where the MIP is active.
This MAC	The MAC of this MEP - can be used by other MEP when unicast is selected (Info only).
Oper State	Operational State that can have one of these values: **Up**: The instance is UP meaning it is physically configured and operational. **Down**: The instance is DOWN meaning it is NOT physically configured and operational. **Config**: The instance is DOWN due to invalid configuration. **HW**: The instance is DOWN due to failing OAM supporting HW resources. **MCE**: The instance is DOWN due to failing MCE resources.

Instance Configuration



Setting	Description
Level	The MEG level of this MEP.
Format	This is the configuration of the two possible Maintenance Association Identifier formats. • **ITU ICC:** This is defined by ITU (Y1731 Fig. A3). 'Domain Name' is not used. 'MEG id' must be max. 13 char. • **IEEE String:** This is defined by IEEE (802.1ag Section 21.6.5). 'Domain Name' can be max. 16 char. 'MEG id' (Short MA Name) can be max. 16 char. • **ITU CC ICC:** This is defined by ITU (Y1731 Fig. A5). 'Domain Name' is not used. 'MEG id' must be max. 15 char.
Domain Name	This is the IEEE Maintenance Domain Name and is only used in case of 'IEEE String' format. This string can be empty giving Maintenance Domain Name Format 1 - Not present. This can be max 16 char.
MEG Id	This is either ITU MEG ID or IEEE Short MA Name - depending on 'Format'. See 'Format'. In case of ITU ICC format this must be 13 char. In case of ITU CC ICC format this must be 15 char. In case of IEEE String format this can be max 16 char.
MEP Id	This value will become the transmitted two byte CCM MEP ID.
Tagged VID	This value will be the VID of a TAG added to the OAM PDU.
Syslog	If enabled, notifications are logged to Syslog.
cLevel	Fault Cause indicating that a CCM is received with a lower level than the configured for this MEP.
cMEG	Fault Cause indicating that a CCM is received with a MEG ID different from configured for this MEP.
cMEP	Fault Cause indicating that a CCM is received with a MEP ID different from all 'Peer MEP ID' configured for this MEP.
cAIS	Fault Cause indicating that AIS PDU is received.
cLCK	Fault Cause indicating that LCK PDU is received.
cLoop	Fault Cause indicating that a loop is detected, since CCM is received with own MEP ID and SMAC.
cConfig	Fault Cause indicating that a configuration error is detected, since CCM is received with own MEP ID.
cDEG	Fault Cause indicating that server layer is indicating Signal Degraded.
cSSF	Fault Cause indicating that server layer is indicating Signal Fail.
aBLK	The consequent action of blocking service frames in this flow is active.
aTSD	The consequent action of indicating Trail Signal Degrade is calculated.
aTSF	The consequent action of indicating Trail Signal Fail to-wards protection is active.

Peer MEP Configuration

Peer MEP Configuration

Delete	Peer MEP ID	Unicast Peer MAC		cLOC	cRDI	cPeriod	cPriority
	No Peer MEP Added						

Add New Peer MEP

Setting	Description
Delete	This box is used to mark a Peer MEP for deletion in next Save operation.
Peer MEP ID	This value will become an expected MEP ID in a received CCM - see 'cMEP'.
Unicast Peer MAC	This MAC will be used when unicast is selected with this peer MEP. Also this MAC is used to create HW checking of receiving CCM PDU (LOC detection) from this MEP.
cLOC	Fault Cause indicating that no CCM has been received (in 3,5 periods) - from this peer MEP.
cRDI	Fault Cause indicating that a CCM is received with Remote Defect Indication - from this peer MEP.
cPeriod	Fault Cause indicating that a CCM is received with a period different what is configured for this MEP - from this peer MEP.
cPriority	Fault Cause indicating that a CCM is received with a priority different what is configured for this MEP - from this peer MEP.

Functional Configuration

Functional Configuration

Continuity Check					APS Protocol				
Enable	Priority	Frame rate	TLV		Enable	Priority	Cast	Type	Last Octet
☐	0	1 f/sec	☐		☐	0	Multi	L-APS	1

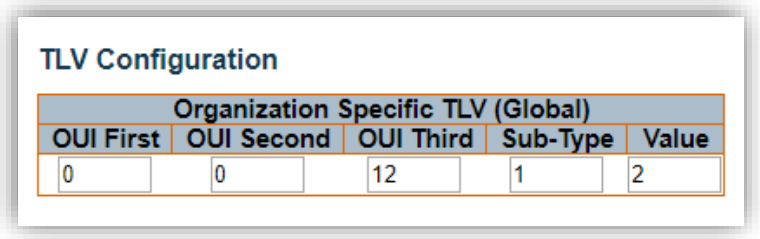
Fault Management Performance Monitoring

Setting	Description
Continuity Check	• **Enable:** Continuity Check based on transmitting/receiving CCM PDU can be enabled/disabled. The CCM PDU is always transmitted as Multi-cast Class 1. • **Priority:** The priority to be inserted as PCP bits in TAG (if any). In case of enable of Continuity Check and Loss Measurement both implemented on SW based CCM, 'Priority' has to be the same. • **Frame rate:** Selecting the frame rate of CCM PDU. This is the inverse of transmission period as described in Y.1731. This value has the following uses: a. The transmission rate of the CCM PDU. b. Fault Cause cLOC is declared if no CCM PDU has been received within 3.5 periods - see 'cLOC'. c. Fault Cause cPeriod is declared if a CCM PDU has been received with different period - see 'cPeriod'.

	Selecting 300f/sec or 100f/sec will configure HW based CCM (if possible). Selecting other frame rates will configure SW based CCM. In case of enable of Continuity Check and Loss Measurement both implemented on SW based CCM, 'Frame Rate' has to be the same. • **TLV:** Enable/disable of TLV insertion in the CCM PDU.
APS Protocol	• **Enable:** Automatic Protection Switching protocol information transportation based on transmitting/receiving R-APS/L-APS PDU can be enabled/disabled. Must be enabled to support ERPS/ELPS implementing APS. This is only valid with one Peer MEP configured. • **Priority:** The priority to be inserted as PCP bits in TAG (if any). • **Cast:** Selection of APS PDU transmitted unicast or multi-cast. The unicast MAC will be taken from the 'Unicast Peer MAC' configuration. Unicast is only valid for L-APS - see 'Type'. The R-APS PDU is always transmitted with multi-cast MAC described in G.8032. • **Type:** a. ***R-APS:*** APS PDU is transmitted as R-APS - this is for ERPS. b. ***L-APS:*** APS PDU is transmitted as L-APS - this is for ELPS. • **Last Octet:** This is the last octet of the transmitted and expected RAPS multi-cast MAC. In G.8031 (03/2010) a RAPS multi-cast MAC is defined as 01-19-A7-00-00-XX. In current standard the value for this last octet is '01' and the usage of other values is for further study.

TLV Configuration

Configuration of the OAM PDU TLV. Currently only TLV in the CCM is supported.



Setting	Description
Organization Specific - OUI First	The transmitted first value in the OS TLV OUI field.
Organization Specific - OUI Second	The transmitted second value in the OS TLV OUI field.
Organization Specific - OUI Third	The transmitted third value in the OS TLV OUI field.
Organization Specific - Sub-Type	The transmitted value in the OS TLV Sub-Type field.
Organization Specific - Value	The transmitted value in the OS TLV Value field.

TLV Status

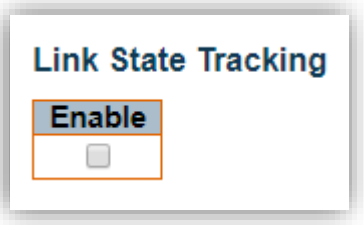
Display of the last received TLV. Currently only TLV in the CCM is supported.

TLV Status

Peer MEP ID	CC Organization Specific							CC Port Status			CC Interface Status	
	OUI First	OUI Second	OUI Third	Sub-Type	Value	Last RX		Value	Last RX		Value	Last RX

Setting	Description
CC Organization Specific - OUI First	The last received first value in the OUI field.
CC Organization Specific - OUI Second	The last received second value in the OS TLV OUI field.
CC Organization Specific - OUI Third	The last received third value in the OS TLV OUI field.
CC Organization Specific - Sub-Type	The last received value in the OS TLV Sub-Type field.
CC Organization Specific - Value	The last received value in the OS TLV Value field.
CC Organization Specific - Last RX	OS TLV was received in the last received CCM PDU.
CC Port Status - Value	The last received value in the PS TLV Value field.
CC Port Status - Last RX	PS TLV was received in the last received CCM PDU.
CC Interface Status - Value	The last received value in the IS TLV Value field.
CC Interface Status - Last RX	IS TLV was received in the last received CCM PDU.

Link State Tracking

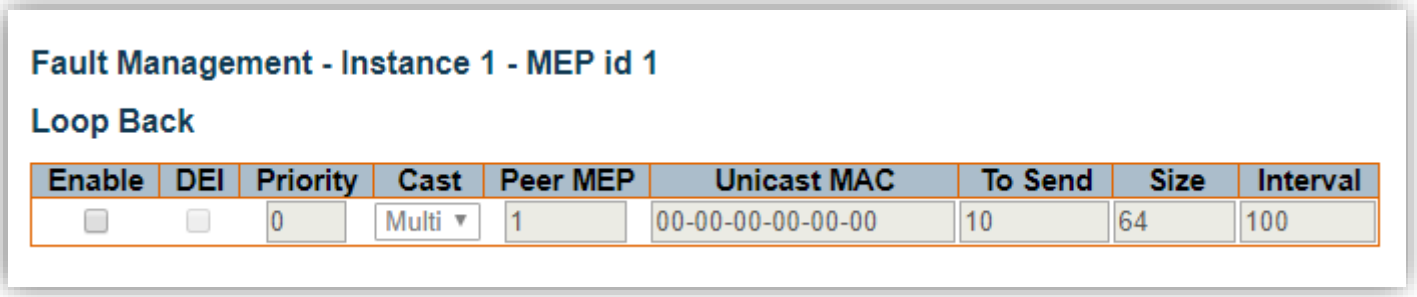


Setting	Description
Enable	When LST is enabled in an instance, Local SF or received 'isDown' in CCM Interface Status TLV, will bring down the residence port. Only valid in Up-MEP. The CCM rate must be 1 f/s or faster.

- **Fault Management**

This page allows the user to inspect and configure the Fault Management of the current MEP Instance.

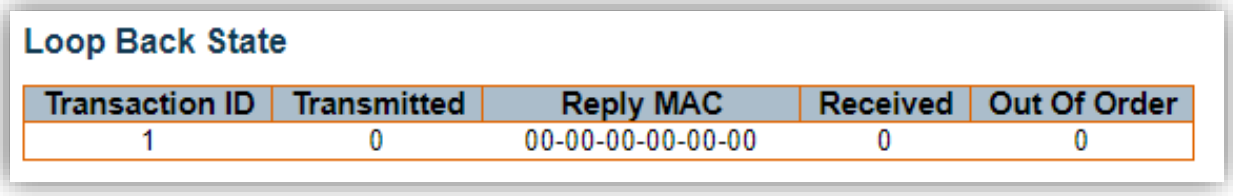
Loop Back



Setting	Description
Enable	Loop Back based on transmitting/receiving LBM/LBR PDU can be enabled/disabled. Loop Back is automatically disabled when all 'To Send' LBM PDU has been transmitted - waiting 5 sec. for all LBR from the end.
DEI	The DEI to be inserted as PCP bits in TAG (if any).
Priority	The priority to be inserted as PCP bits in TAG (if any).
Cast	Selection of LBM PDU transmitted unicast or multi-cast. The unicast MAC will be configured through 'Peer MEP' or 'Unicast Peer MAC'. To-wards MIP only unicast Loop Back is possible.
Peer MEP	This is only used if the 'Unicast MAC' is configured to all zero. The LBM unicast MAC will be taken from the 'Unicast Peer MAC' configuration of this peer.
Unicast MAC	This is only used if NOT configured to all zero. This will be used as the LBM PDU unicast MAC. This is the only way to configure Loop Back to-wards a MIP.
To Send	The number of LBM PDU to send in one loop test. The value 0 indicate infinite transmission (test behaviour). This is HW based LBM/LBR and Requires VOE.
Size	The LBM frame size. This is entered as the wanted size (in bytes) of a un-tagged frame containing LBM OAM PDU - including CRC (four bytes). Example when 'Size' = 64=> Un-tagged frame size = DMAC(6) + SMAC(6) + TYPE(2) + LBM PDU LENGTH(46) + CRC(4) = 64 bytes The transmitted frame will be four bytes longer for each tag added - 8 bytes in case of a tunnel EVC. There are two frame MAX sizes to consider.

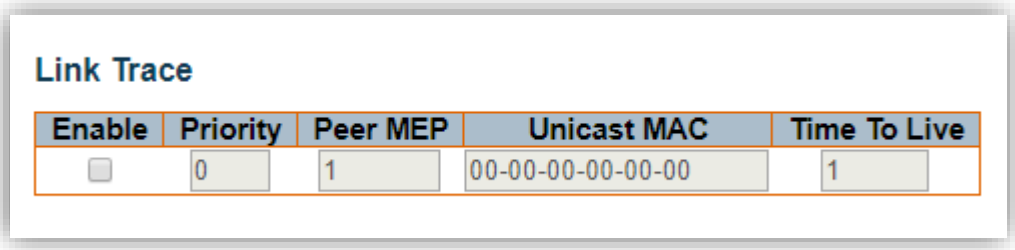
	• **Switch RX frame MAX size:** The MAX frame size (all inclusive) accepted on the switch port of 9600 Bytes • **CPU RX frame MAX size:** The MAX frame size (all inclusive) possible to copy to CPU of 9600 Bytes Consider that the Peer MEP must be able to handle the selected frame size. Consider that In case of SW based MEP, the received LBR PDU must be copied to CPU. Warning will be given if selected frame size exceeds the CPU RX frame MAX size Frame. MIN Size is 64 Bytes.
Interval	The interval between transmitting LBM PDU. In 10ms. in case 'To Send' != 0 (max 100 - '0' is as fast as possible) In 1us. in case 'To Send' == 0 (max 10.000)",

Loop Back State



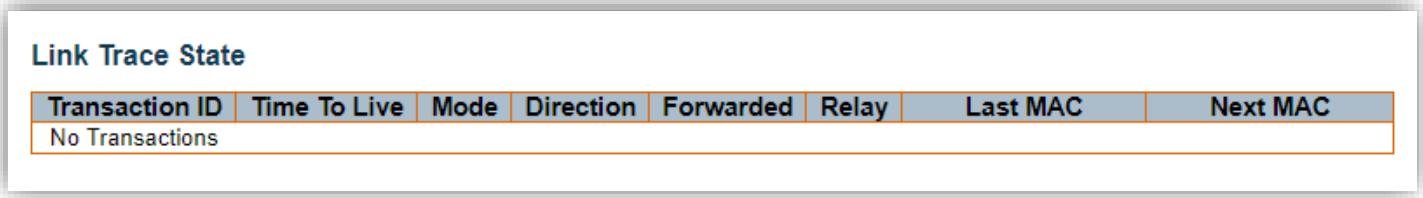
Setting	Description
Transaction ID	The transaction id of the first LBM transmitted. For each LBM transmitted the transaction id in the PDU is incremented.
Transmitted	The total number of LBM PDU transmitted.
Reply MAC	The MAC of the replying MEP/MIP. In case of multi-cast LBM, replies can be received from all peer MEP in the group. This MAC is not shown in case of 'To Send' == 0.
Received	The total number of LBR PDU received from this 'Reply MAC'.
Out Of Order	The number of LBR PDU received from this 'Reply MAC' with incorrect 'Transaction ID'.

Link Trace



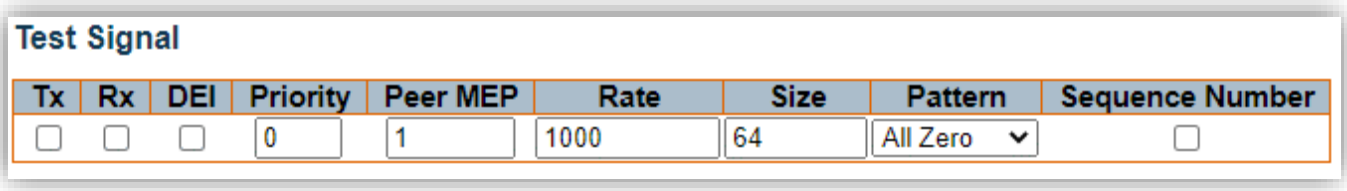
Setting	Description
Enable	Link Trace based on transmitting/receiving LTM/LTR PDU can be enabled/disabled. Link Trace is automatically disabled when all 5 transactions are done with 5 sec. interval - waiting 5 sec. for all LTR in the end. The LTM PDU is always transmitted as Multi-cast Class 2.
Priority	The priority to be inserted as PCP bits in TAG (if any).
Peer MEP	This is only used if the 'Unicast MAC' is configured to all zero. The Link Trace Target MAC will be taken from the 'Unicast Peer MAC' configuration of this peer.
Unicast MAC	This is only used if NOT configured to all zero. This will be used as the Link Trace Target MAC. This is the only way to configure a MIP as Target MAC.
Time To Live	This is the LTM PDU TTL value as described in Y.1731. This value is decremented each time forwarded by a MIP. Will not be forwarded reaching zero.

Link Trace State



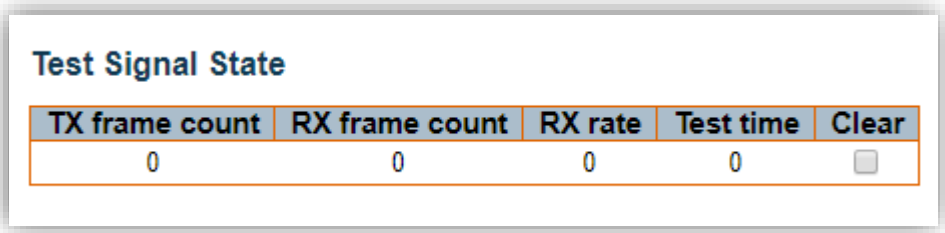
Setting	Description
Transaction ID	The transaction id is incremented for each LTM send. This value is inserted the transmitted LTM PDU and is expected to be received in the LTR PDU. Received LTR with wrong transaction id is ignored. There are five transactions in one Link Trace activated.
Time To Live	This is the TTL value taken from the LTM received by the MIP/MEP sending this LTR - decremented as if forwarded.
Mode	Indicating if is was a MEP/MIP sending this LTR.
Direction	Indicating if MEP/MIP sending this LTR is ingress/egress.
Forwarded	Indicating if MEP/MIP sending this LTR has forwarded the LTM.
Relay	The Relay action can be one of the following • **MAC:** The was a hit on the LT Target MAC • **FDB:** LTM is forwarded based on hit in the Filtering DB • **MFDB:** LTM is forwarded based on hit in the MIP CCM DB
Last MAC	The MAC identifying the last sender of the LBM causing this LTR - initiating MEP or previous MIP forwarding.
Next MAC	The MAC identifying the next sender of the LBM causing this LTR - MIP forwarding or terminating MEP.

Test Signal



Setting	Description
Enable	Test Signal based on transmitting TST PDU can be enabled/disabled.
DEI	The DEI to be inserted as PCP bits in TAG (if any).
Priority	The priority to be inserted as PCP bits in TAG (if any).
Peer MEP	The TST frame destination MAC will be taken from the 'Unicast Peer MAC' configuration of this peer.
Rate	The TST frame transmission bit rate - in Kilo bits pr. second. Limit in 10 Gbps. This is the bit rate of a standard frame without any encapsulation. If 1 Mbps rate is selected in a EVC MEP, the added tag will give a higher bitrate on the wire.
Size	The TST frame size. This is entered as the wanted size (in bytes) of a un-tagged frame containing TST OAM PDU - including CRC (four bytes). Example when 'Size' = 64=> Un-tagged frame size = DMAC(6) + SMAC(6) + TYPE(2) + TST PDU LENGTH(46) + CRC(4) = 64 bytes The transmitted frame will be four bytes longer for each tag added - 8 bytes in case of a tunnel EVC. There are two frame MAX sizes to consider. • **Switch RX frame MAX size:** The MAX frame size (all inclusive) accepted on the switch port of 10240 Bytes • **CPU RX frame MAX size:** The MAX frame size (all inclusive) possible to copy to CPU of 10240 Bytes Consider that the Peer MEP must be able to handle the selected frame size. Consider that in order to calculate the 'RX rate' a received TST PDU must be copied to CPU. Warning will be given if selected frame size exceeds the CPU RX frame MAX size. Frame MIN Size is 64 Bytes.
Pattern	The 'empty' TST PDU has the size of 12 bytes. In order to achieve the configured frame size a data TLV will be added with a pattern. Example when 'Size' = 64=> Un-tagged frame size = DMAC(6) + SMAC(6) + TYPE(2) + TST PDU LENGTH(46) + CRC(4) = 64 bytes The TST PDU needs to be 46 bytes so a pattern of 46-12=34 bytes will be added. **All Zero:** Pattern will be '00000000' **All One:** Pattern will be '11111111' **10101010:** Pattern will be '10101010'

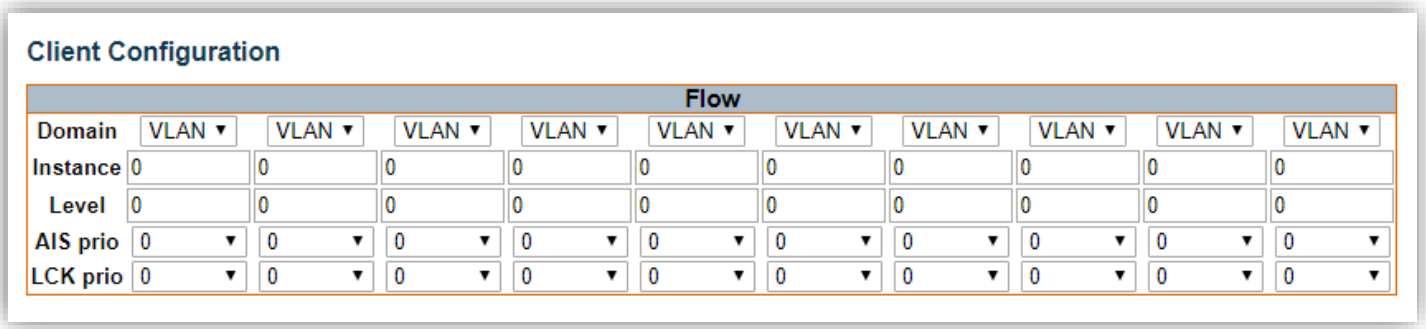
Test Signal State



Setting	Description
TX frame count	The number of transmitted TST frames since last 'Clear'.
RX frame count	The number of received TST frames since last 'Clear'.
RX rate	The current received TST frame bit rate in Kbps. This is calculated on a 1 s. basis, starting when first TST frame is received after 'Clear'. The frame size used for this calculation is the first received after 'Clear'
Test time	The number of seconds passed since first TST frame received after last 'Clear'.
Clear	This will clear all Test Signal State. Transmission of TST frame will be restarted. Calculation of 'Rx frame count', 'RX rate' and 'Test time' will be started when receiving first TST frame.

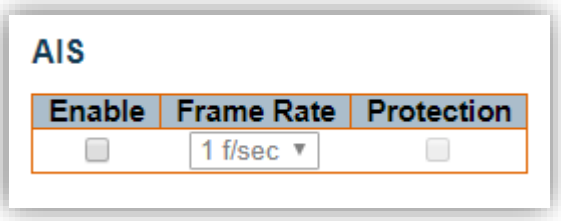
Client Configuration

Only a Port MEP is able to be a server MEP with flow configuration. The Priority in the client flow is always the highest priority configured in the EVC.



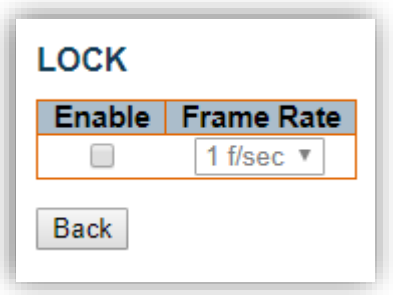
Setting	Description
Domain	The domain of the client layer flow.
Instance	Client layer flow instance numbers.
Level	Client layer level - AIS and LCK PDU transmitted in this client layer flow will be on this level.
AIS Prio	The priority to be used when transmitting AIS in each client flow. Priority resulting in highest possible PCP can be selected.
LCK Prio	The priority to be used when transmitting LCK in each client flow. Priority resulting in highest possible PCP can be selected.

AIS



Setting	Description
Enable	Insertion of AIS signal (AIS PDU transmission) in client layer flows, can be enable/disabled.
Frame Rate	Selecting the frame rate of AIS PDU. This is the inverse of transmission period as described in Y.1731.
Protection	Selecting this means that the first 3 AIS PDU is transmitted as fast as possible - in case of using this for protection in the end point.

Lock

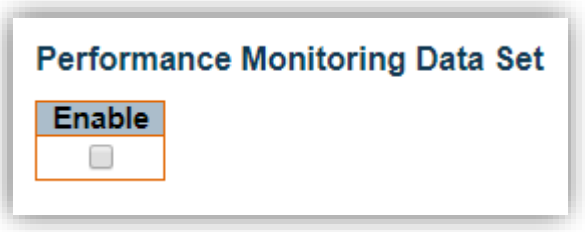


Setting	Description
Enable	Insertion of LOCK signal (LCK PDU transmission) in client layer flows, can be enable/disabled.
Frame Rate	Selecting the frame rate of LCK PDU. This is the inverse of transmission period as described in Y.1731.

- **Performance Monitoring**

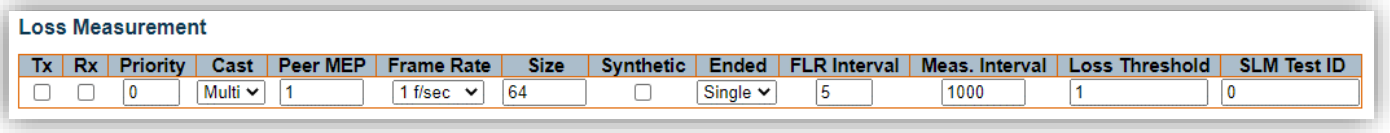
This page allows the user to inspect and configure the performance monitor of the current MEP Instance.

Performance Monitoring Data Set



Setting	Description
Enable	When enabled this MEP instance will contribute to the 'PM Data Set' gathered by the PM Session.

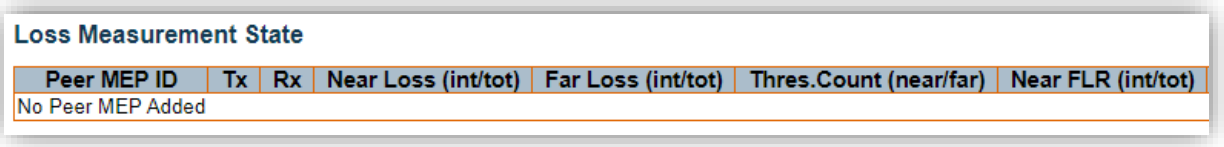
Loss Measurement

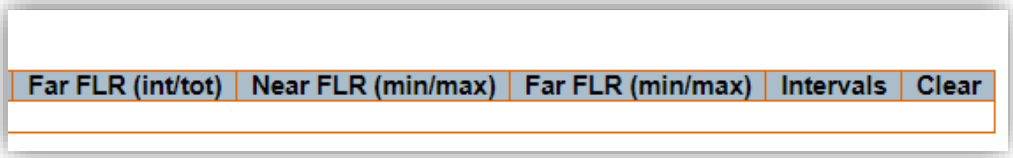


Setting	Description
Tx	transmitting/receiving CCM or LMM/LMR or SLM/SLR/1SL PDUs - see 'Synthetic' and 'Ended'. Service frame LM (not 'Synthetic') is only allowed with one Peer MEP configured. Synthetic frame LM is allowed with multiple Peer MEPs configured.
Rx	Enable loss calculation when receiving LM PDUs (LMM/SLM/1SL). This is ignored when LM initiator is enabled.
Priority	The priority to be inserted as PCP bits in TAG (if any). In case of enable of Continuity Check and Loss Measurement both implemented on SW based CCM, 'Priority' has to be the same.
Cast	Selection of LM PDU transmitted unicast or multicast. The unicast MAC will be taken from the 'Unicast Peer MAC' database. In case of enable of Continuity Check and dual ended Loss Measurement both implemented on SW based CCM, 'Cast' has to be the same.
Peer MEP	Peer MEP-ID for unicast LM. The MAC is taken from the 'Unicast Peer MAC' database. Only used in case of multiple peers ('Synthetic' LM).
Rate	Selecting the frame rate of LM PDU. This is the inverse of transmission period as described in Y.1731. Selecting 100f/sec is only valid in case of 'Synthetic' LM. Selecting 6f/min is not valid in case of dual ended 'Service frame' LM (CCM PDU based). In case of enable of Continuity Check and Loss Measurement both implemented on SW based CCM, 'Frame Rate' has to be the same.
Size	The 'Synthetic' SLM/1SL frame size. This is entered as the wanted size (in bytes) of a un-tagged frame containing LM OAM PDU - including CRC (four bytes). Example when 'Size' = 64=> Un-tagged frame size = DMAC(6) + SMAC(6) + TYPE(2) + LBM PDU LENGTH(46) + CRC(4) = 64 bytes

	The transmitted frame will be four bytes longer for each tag added - 8 bytes in case of a tunnel EVC. There are two frame MAX sizes to consider. • **Switch RX frame MAX size:** The MAX frame size (all inclusive) accepted on the switch port of Bytes • **CPU RX frame MAX size:** The MAX frame size (all inclusive) possible to copy to CPU of Bytes Consider that the Peer MEP must be able to handle the selected frame size. Consider that the received SLR PDU must be copied to CPU. Warning will be given if selected frame size exceeds the CPU RX frame MAX size. Frame MIN Size is 64 Bytes.
Synthetic	Synthetic frame LM is enable. This is SLM/SLR/1SL PDU based LM.
Ended	**Single:** Single ended Loss Measurement implemented on LMM/LMR or SLM/SLR. **Dual:** Dual ended Loss Measurement implemented on SW based CCM or 1SL.
FLR Interval	This is the interval in number of measurement intervals where the interval Frame Loss Ratio is calculated.
Meas. Interval	This is the 'synthetic' LM measurement interval in milliseconds. This must be a whole number of the LM PDU transmission interval (inverse 'Rate'). This is the interval in time where the loss and FLR is calculated based on the counted number of SL OAM PDUs. It is in this interval that the calculated FLR is checked against availability, high loss and degraded FLR threshold. example: 'Rate' = 100f/sec => 'Meas Interval' = N*10 milliseconds. example: 'Rate' = 10f/sec => 'Meas Interval' = N*100 milliseconds. In case of service frame based LM this attribute is not used and the measurement interval is always the LM PDU transmission interval.
Loss Threshold	Far end loss threshold count is incremented if a loss measurement is above this threshold.
SLM Test ID	The Test ID value to use in SLM PDUs (see G.8013, section 9.22.1). The default value is 0.

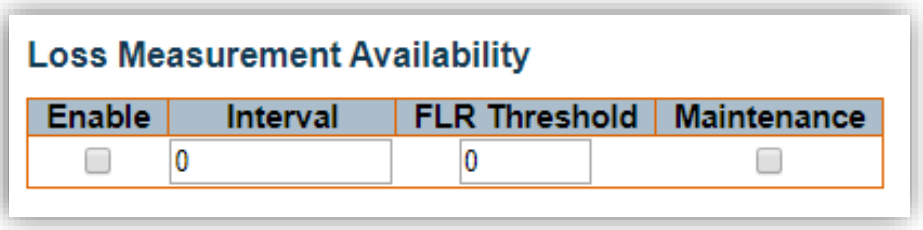
Loss Measurement State





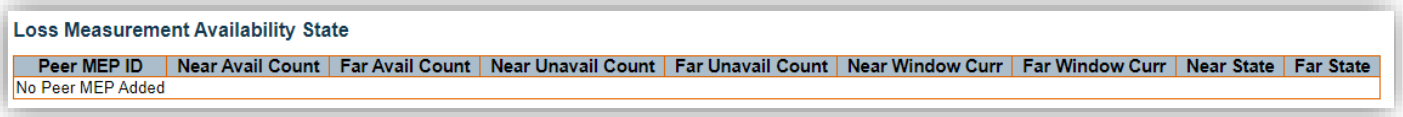
Setting	Description
Peer MEP	The Peer MEP ID that the following state relates to.
Tx	The accumulated transmitted LM PDUs - since last 'clear'.
Rx	The accumulated received LM PDUs - since last 'clear'.
Near Loss	This field contains both the number of measurement intervals that nas contributed to the near end frame loss and the total near end frame loss count – since last ‘clear’.
Far Loss	This field contains both the number of measurement intervals that nas contributed to the near end frame loss and the total far end frame loss count – since last ‘clear’.
Thres.Count(near/far)	The number of time the near end and far end frame loss thresholds has been crossed.
Near FLR (int/tot)	The interval and total near end frame loss ratio calculated based on the near end frame loss count and far end frame transmitted. The result is given in 100 percent.
Far FLR (int/tot)	The interval and total far end frame loss ratio calculated based on the far end frame loss count and near end frame transmitted. The result is given in 100 * percent.
Near FLR (min/max)	The minimum and maximum non-zero near end frame loss ratio calculated based on the near end frame loss count and far end frame transmitted. The result is given in 100 * percent. A value of zero means that no loss has been encountered since last clear.
Far FLR (min/max)	The minimum and maximum non-zero far end frame loss ratio calculated based on the far end frame loss count and near end frame transmitted. The result is given in 100 * percent. A value of zero means that no loss has been encountered since last clear.
Intervals	The number of FLR expired intervals.
Clear	Set of this check and save will clear the accumulated counters and restart ratio calculation.

Loss Measurement Availability



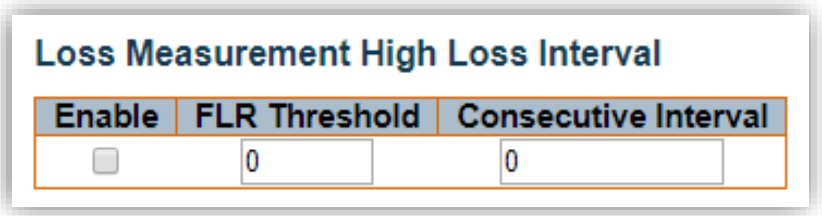
Setting	Description
Enable	Enable/disable of loss measurement availability.
Interval	Availability interval - number of measurements with same availability in order to change availability state. The valid range is 1 to 1000.
FLR Threshold	Availability frame loss ratio threshold in per mille.
Maintenance	Enable/disable of loss measurement availability maintenance.

Loss Measurement Availability Status



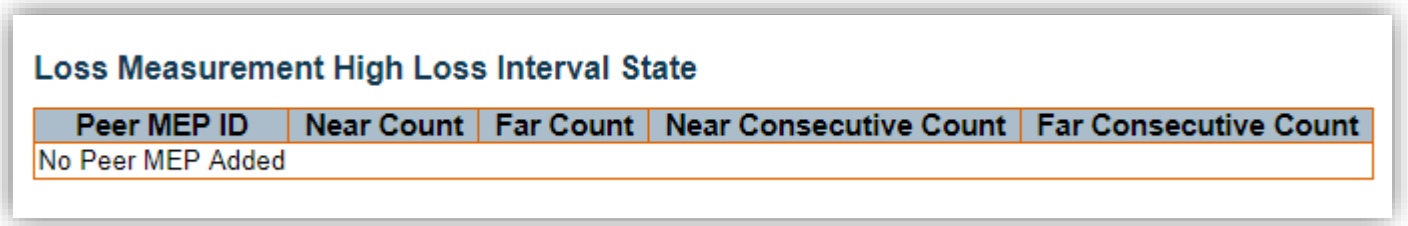
Setting	Description
Peer MEP	The Peer MEP ID that the following state relates to.
Near Avail Count	The number of measurements performed while the near end has been in the "Avail" state.
Far Avail Count	The number of measurements performed while the far end has been in the "Avail" state.
Near Unavail Count	The number of measurements performed while the near end has been in the "Unavail" state.
Far Unavail Count	The number of measurements performed while the far end has been in the "Unavail" state.
Near Window Curr	The current near-end availability window size. When **Near State** is "Avail" this value indicate the current number of consecutive measurements that are above the defined frame loss ratio threshold. When **Near State** is "Unavail" this value indicate the current number of consecutive measurements that are equal to or below the defined frame loss ratio threshold. Once this value reaches the defined "interval" value (aka. the "window size") the availability state will change.
Far Window Curr	The current far-end availability window size. See the description for **Near Window Curr** for more details.
Near State	The current near end availability state.
Far State	The current far end availability state.

Loss Measurement High Loss Interval



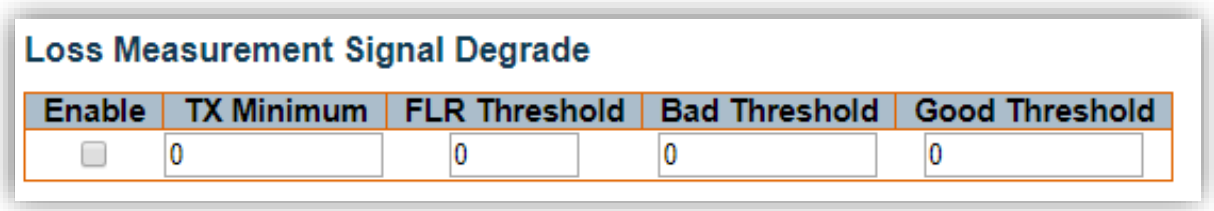
Setting	Description
Enable	Enable/disable of loss measurement high loss interval.
FLR Threshold	High Loss Interval frame loss ratio threshold in per mille.
Consecutive Interval	High Loss Interval consecutive interval (number of measurements).

Loss Measurement High Loss Interval Status



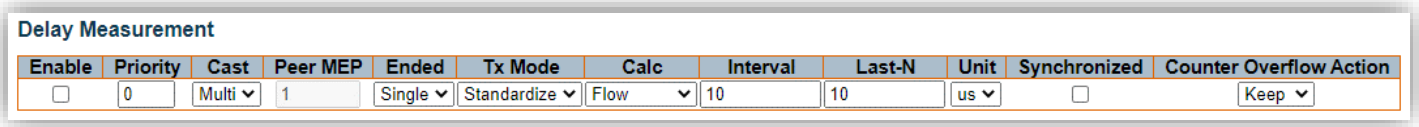
Setting	Description
Near Count	Near end high loss interval count (number of measurements where availability state is available and FLR is above high loss interval FLR threshold.
Far Count	Far end high loss interval count (number of measurements where availability state is available and FLR is above high loss interval FLR threshold.
Near Consecutive Count	Near end high loss interval consecutive count.
Far Consecutive Count	Far end high loss interval consecutive count.

Loss Measurement Signal Degrade



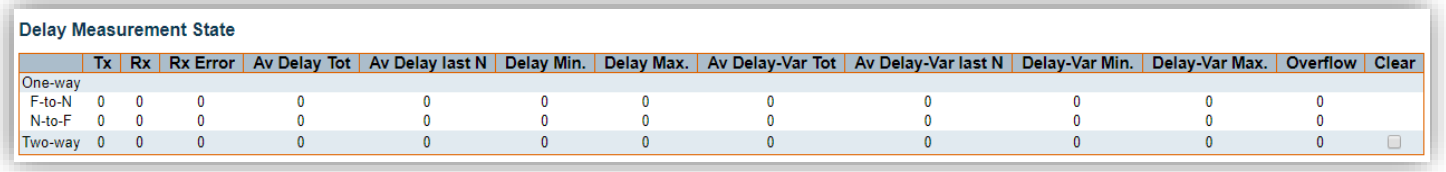
Setting	Description
Enable	Enable/disable of loss measurement signal degrade.
TX Minimum	Minimum number of frames that must be transmitted in a measurement before frame loss ratio is tested against loss ratio threshold.
FLR Threshold	Signal Degraded frame loss ratio threshold in per mile.
Bad Threshold	Number of consecutive bad interval measurements required to set degrade state.
Good Threshold	Number of consecutive good interval measurements required to clear degrade state.

Delay Measurement



Setting	Description
Enable	Delay Measurement based on transmitting 1DM/DMM PDU can be enabled/disabled. Delay Measurement based on receiving and handling 1DM/DMR PDU is always enabled.
Priority	The priority to be inserted as PCP bits in TAG (if any).
Cast	Selection of 1DM/DMM PDU transmitted unicast or multicast. The unicast MAC will be configured through 'Peer MEP'.
Peer MEP	This is only used if the 'Cast' is configured to Uni. The 1DM/DMR unicast MAC will be taken from the 'Unicast Peer MAC' configuration of this peer.
Ended	**Single:** Single ended Delay Measurement implemented on DMM/DMR. **Dual:** Dual ended Delay Measurement implemented on 1DM.
Tx Mode	**Standardize:** Y.1731 standardize way to transmit 1DM/DMR. **Proprietary:** Vitesse proprietary way with follow-up packets to transmit 1DM/DMR.
Calc	This is only used if the 'Ended' is configured to single ended. **Round trip:** The frame delay calculated by the transmitting and receiving timestamps of initiators. Frame Delay = RxTimeb-TxTimeStampf **Flow:** The frame delay calculated by the transmitting and receiving timestamps of initiators and remotes. Frame Delay = (RxTimeb-TxTimeStampf)-(TxTimeStampb-RxTimeStampf)
Interval	The Interval between transmitting 1DM/DMM PDU in 10ms. The range is 10 to 65535.
Last-N	The last N delays messurements used for average last N calulation. Min value is 10. Max value is 100.
Unit	The time resolution.
Synchronized	Enable to use DMM/DMR packet to calculate dual ended DM. If the option is enabled, the following action will be taken. When DMR is received, two-way delay (roundtrip or flow) and both near-end-to-far-end and far-end-to-near-end one-way delay are calculated. When DMM or 1DM is received, only far-end-to-near-end one-way delay is calculated.
Counter Overflow Action	The action to counter when overflow happens.

Delay Measurement State



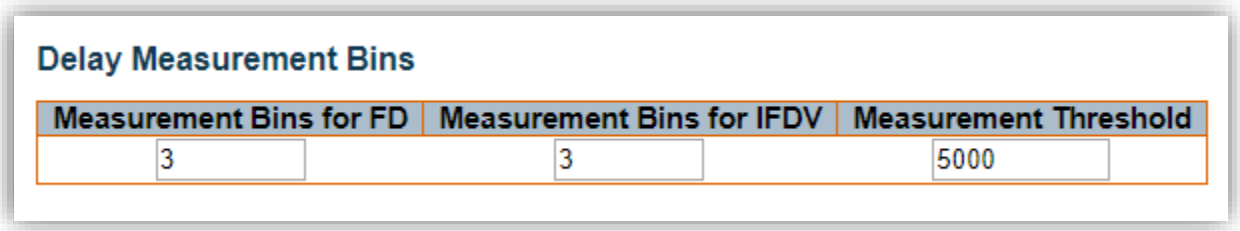
Delay Measurement State

	Tx	Rx	Rx Error	Av Delay Tot	Av Delay last N	Delay Min.	Delay Max.	Av Delay-Var Tot	Av Delay-Var last N	Delay-Var Min.	Delay-Var Max.	Overflow	Clear
One-way													
F-to-N	0	0	0	0	0	0	0	0	0	0	0	0	
N-to-F	0	0	0	0	0	0	0	0	0	0	0	0	
Two-way	0	0	0	0	0	0	0	0	0	0	0	0	☐

Setting	Description
Tx	The accumulated transmit count - since last 'clear'.
Rx	The accumulated receive count - since last 'clear'.
Rx Error	The accumulated receive error count - since last 'clear'. This is counting if the frame delay is larger than 1 second or if far end residence time is larger than the round trip time.
Av Delay Tot	The average total delay - since last 'clear'.
Av Delay last N	The average delay of the last n packets - since last 'clear'.
Delay Min.	The minimum delay - since last 'clear'.
Delay Max.	The maximum delay - since last 'clear'.
Av Delay-Var Tot	The average total delay variation - since last 'clear'.
Av Delay-Var last N	The average delay variation of the last n packets - since last 'clear'.
Delay-Var Min.	The minimum delay variation - since last 'clear'.
Delay-Var Max.	The maximum delay variation - since last 'clear'.
Overflow	The number of counter overflow - since last 'clear'.
Clear	Set of this check and save will clear the accumulated counters.
Far-end-to-near-end one-way delay	The one-way delay is from remote devices to the local devices. Here are the conditions to calculate this delay. 1. 1DM received. 2. DMM received with Synchronized enabled. 3. DMR received with Synchronized enabled.
Near-end-to-far-end one-way delay	The one-way delay is from the local devices to remote devices. The only case to calculate this delay is below. DMR received with Synchronized enabled.

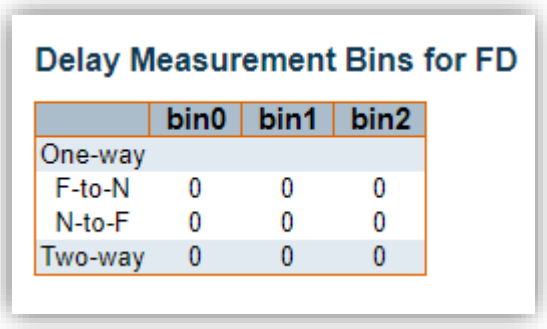
Delay Measurement Bins

A Measurement Bin is a counter that stores the number of delay measurements falling within a specified range, during a Measurement Interval.



Setting	Description	Factory Default
Measurement Bins for FD	Configurable number of Frame Delay Measurement Bins per Measurement Interval. The minimum number of FD Measurement Bins per Measurement Interval supported is 2. The maximum number of FD Measurement Bins per Measurement Interval supported is 10.	3
Measurement Bins for IFDV	Configurable number of Inter-Frame Delay Variation Measurement Bins per Measurement Interval. The minimum number of FD Measurement Bins per Measurement Interval supported is 2. The maximum number of FD Measurement Bins per Measurement Interval supported is 10.	3
Measurement Threshold	Configurable the Measurement Threshold for each Measurement Bin. The unit for a measurement threshold is in microseconds (us).	5000

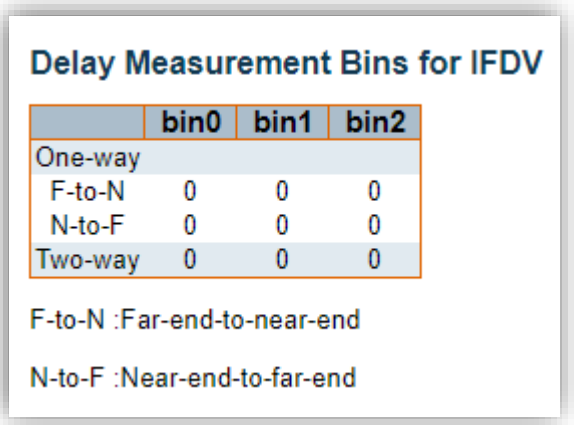
Delay Measurement Bins for FD



A Measurement Bin is a counter that stores the number of delay measurements falling within a specified range, during a Measurement Interval.
If the measurement threshold is 5000 us and the total number of Measurement Bins is four, we can give an example as follows.

Bin	Threshold	Range
bin0	0 us	0 us <= measurement < 5,000 us
bin1	5,000 us	5,000 us <= measurement < 10,000 us
bin2	10,000 us	10,000 us <= measurement < 15,000 us
bin3	15,000 us	15,000 us <= measurement < infinite us

Delay Measurement Bins for IFDV

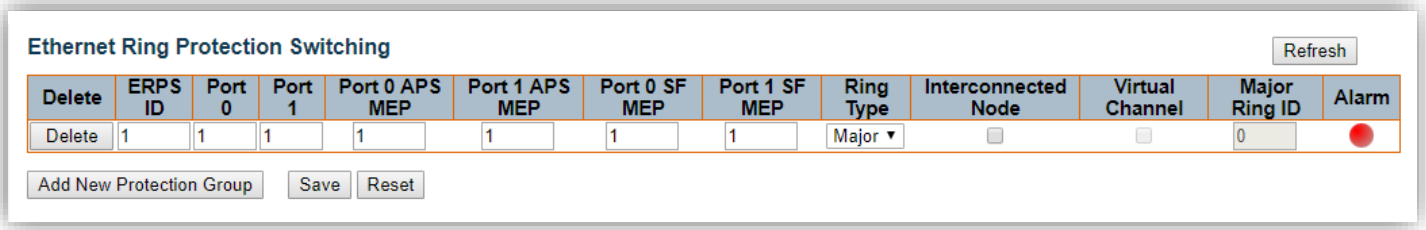


A Measurement Bin is a counter that stores the number of delay measurements falling within a specified range, during a Measurement Interval.
If the measurement threshold is 5000 us and the total number of Measurement Bins is four, we can give an example as follows.

Bin	Threshold	Range
bin0	0 us	0 us <= measurement < 5,000 us
bin1	5,000 us	5,000 us <= measurement < 10,000 us
bin2	10,000 us	10,000 us <= measurement < 15,000 us
bin3	15,000 us	15,000 us <= measurement < infinite us

Configuration > ERPS

- **Ethernet Ring Protection Switching**



Setting	Description
Delete	This box is used to mark an ERPS for deletion in next Save operation.
ERPS ID	The ID of the created Protection group, It must be an integer value between 1 and 64. The maximum number of ERPS Protection Groups that can be created are 64. Click on the ID of an Protection group to enter the configuration page.
Port 0	This will create a Port 0 of the switch in the ring.
Port 1	This will create Port 1 of the switch in the Ring. As interconnected sub-ring will have only one ring port, Port 1 is configured as 0 for interconnected sub-ring. 0 in this field indicates that no Port 1 is associated with this instance
Port 0 SF MEP	The Port 0 Signal Fail reporting MEP.
Port 1 SF MEP	The Port 1 Signal Fail reporting MEP. As only one SF MEP is associated with interconnected sub-ring without virtual channel, it is configured as 0 for such ring instances. 0 in this field indicates that no Port 1 SF MEP is associated with this instance.
Port 0 APS MEP	The Port 0 APS PDU handling MEP.
Port 1 APS MEP	The Port 1 APS PDU handling MEP. As only one APS MEP is associated with interconnected sub-ring without virtual channel, it is configured as 0 for such ring instances. 0 in this field indicates that no Port 1 APS MEP is associated with this instance.
Ring Type	Type of Protecting ring. It can be either major ring or sub-ring.
Interconnected Node	Interconnected Node indicates that the ring instance is interconnected. Click on the checkbox to configure this. Yes indicates it is an interconnected node for this instance. No indicates that the configured instance is not interconnected.
Virtual Channel	Sub-rings can either have virtual channel or not on the interconnected node. This is configured using Virtual Channel checkbox. Yes indicates it is a sub-ring with virtual channel. No indicates, sub-ring doesn't have virtual channel.
Major Ring ID	Major ring group ID for the interconnected sub-ring. It is used to send topology change updates on major ring. If ring is major, this value is same as the protection group ID of this ring.
Alarm	There is an active alarm on the ERPS.

- **ERPS Configuration n**

Instance Data

ERPS Configuration 1

Instance Data

ERPS ID	Port 0	Port 1	Port 0 SF MEP	Port 1 SF MEP	Port 0 APS MEP	Port 1 APS MEP	Ring Type
1	1	2	5	4	4	5	Major Ring

Setting	Description
ERPS ID	The ID of the Protection group.
Port 0	This is a Port 0 of the switch in the ring.
Port 1	This is a Port 1 of the switch in the ring.
Port 0 SF MEP	The Port 0 Signal Fail reporting MEP.
Port 1 SF MEP	The Port 1 Signal Fail reporting MEP.
Port 0 APS MEP	The Port 0 APS PDU handling MEP.
Port 1 APS MEP	The Port 1 APS PDU handling MEP.
Ring Type	Type of Protecting ring. It can be either major ring or sub-ring.

Instance Configuration

Ethernet Ring Protection Switching

Delete	ERPS ID	Port 0	Port 1	Port 0 APS MEP
☐	1	1	2	1

Add New Protection Group | Save | Reset

Click **"Ethernet Ring Protection Switching"** ERPS ID number to config instance

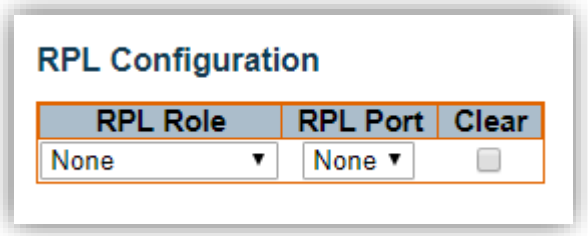
Instance Configuration

Configured	Guard Time	WTR Time	Hold Off Time	Version	Revertive	VLAN config
●	500	1min	0	v2	☑	VLAN Config

Setting	Description	Factory Default
Configured	• **Red:** This ERPS is only created and has not yet been configured - is not active. • **Green:** This ERPS is configured - is active.	None
Guard Time	Guard timeout value to be used to prevent ring nodes from receiving outdated R-APS messages. The period of the guard timer can be configured in 10 ms steps between 10 ms and 2 seconds.	500
WTR Time	The Wait To Restore timing value to be used in revertive switching. The period of the WTR time can be configured by the operator in 1 minute steps between 1 and 12 minutes.	1min
Hold Off Time	The timing value to be used to make persistent check on Signal Fail before switching.	0

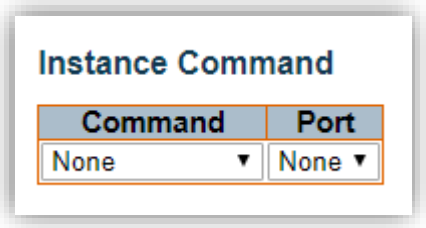
	The range of the hold off timer is 0 to 10 seconds in steps of 100 ms	
Version	ERPS Protocol Version - v1 or v2	v2
Revertive	In Revertive mode, after the conditions causing a protection switch has cleared, the traffic channel is restored to the working transport entity, i.e., blocked on the RPL. In Non-Revertive mode, the traffic channel continues to use the RPL, if it is not failed, after a protection switch condition has cleared.	Enabled
VLAN config	VLAN configuration of the Protection Group. Click on the "VLAN Config" link to configure VLANs for this protection group.	None

RPL Configuration



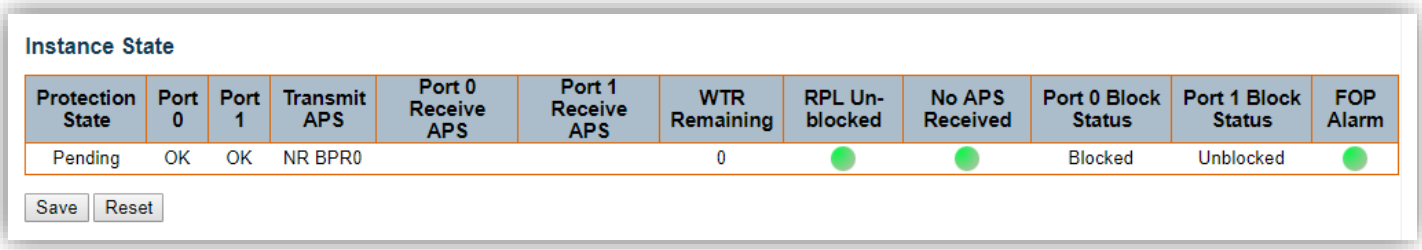
Setting	Description
RPL Role	It can be either RPL owner or RPL Neighbor.
RPL Port	This allows to select the east port or west port as the RPL block.
Clear	If the owner has to be changed, then the clear check box allows to clear the RPL owner for that ERPS ring.

Instance Command



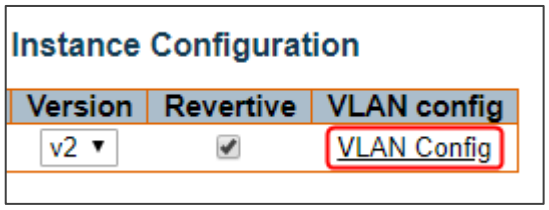
Setting	Description
Command	Administrative command. A port can be administratively configured to be in either manual switch or forced switch state.
Forced Switch	Forced Switch command forces a block on the ring port where the command is issued.
Manual Switch	In the absence of a failure or FS, Manual Switch command forces a block on the ring port where the command is issued.
Clear	The Clear command is used for clearing an active local administrative command (e.g., Forced Switch or Manual Switch).
Port	Port selection - Port0 or Port1 of the protection Group on which the command is applied.

Instance State

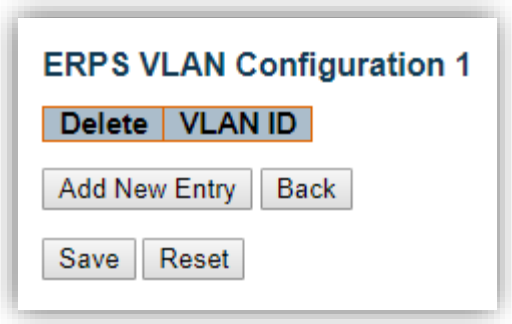


Setting	Description
Protection State	ERPS state according to State Transition Tables in G.8032.
Port 0	**OK:** State of East port is ok **SF:** State of East port is Signal Fail
Port 1	**OK:** State of West port is ok **SF:** State of West port is Signal Fail
Transmit APS	The transmitted APS according to State Transition Tables in G.8032.
Port 0 Receive APS	The received APS on Port 0 according to State Transition Tables in G.8032.
Port 1 Receive APS	The received APS on Port 1 according to State Transition Tables in G.8032.
WTR Remaining	Remaining WTR timeout in milliseconds.
RPL Un-blocked	APS is received on the working flow.
No APS Received	RAPS PDU is not received from the other end.
Port 0 Block Status	Block status for Port 0 (Both traffic and R-APS block status). R-APS channel is never blocked on sub-rings without virtual channel.
Port 1 Block Status	Block status for Port 1 (Both traffic and R-APS block status). R-APS channel is never blocked on sub-rings without virtual channel.
FOP Alarm	Failure of Protocol Defect(FOP) status. If FOP is detected, red LED glows; else green LED glows.

ERPS VLAN Configuration n



Click **"Instance Configuration"** VLAN config to setting ERPS VLAN ID number



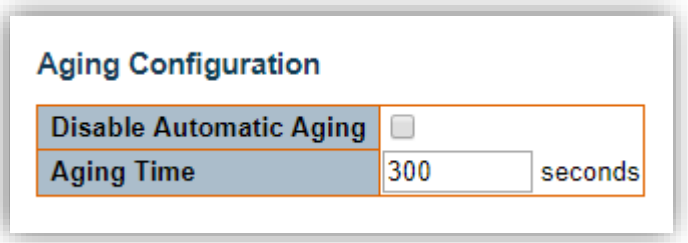
Setting	Description
Delete	To delete a VLAN entry, check this box. The entry will be deleted during the next Save.
VLAN ID	Indicates the ID of this particular VLAN.
Adding a New VLAN	Click "**Add New Entry**" button to add a new VLAN ID. Legal values for a VLAN ID are 1 through 4095. The VLAN is enabled when you click on "Save". A VLAN without any port members will be deleted when you click "Save". The "**Delete**" button can be used to undo the addition of new VLANs.

Configuration > MAC Table

- **MAC Address Table Configuration**

The MAC Address Table is configured on this page. Set timeouts for entries in the dynamic MAC Table and configure the static MAC table here.

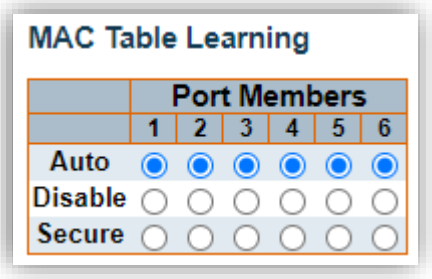
Aging Configuration



Setting	Description
Disable Automatic Aging	Disable the automatic aging of dynamic entries by checking Disable automatic aging.
Aging Time	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. The allowed range is 10 to 1000000 seconds.

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.



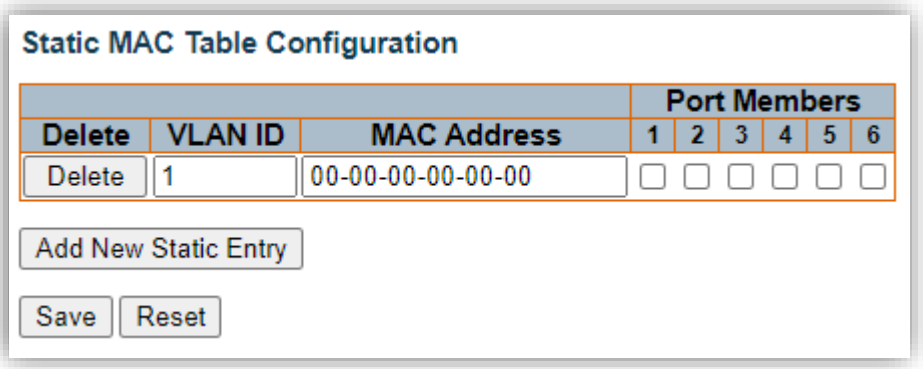
Setting	Description
Auto	Learning is done automatically as soon as a frame with unknown SMAC is received.
Disable	No learning is done.
Secure	Only static MAC entries are learned, all other frames are dropped. **NOTE:** Make sure that the link used for managing the switch is added to the Static Mac Table 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.

VLAN Learing Configuration

Setting	Description
Learning-disabled VLANs	This field shows the Learning-disabled VLANs. When a NEW MAC arrives into a learning-disabled VLAN, the MAC won't be learnt. By the default, the field is empty. 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.

Static MAC Table Configuration

The static entries in the MAC table are shown in this table. The static MAC table can contain 64 entries. The MAC table is sorted first by VLAN ID and then by MAC address.

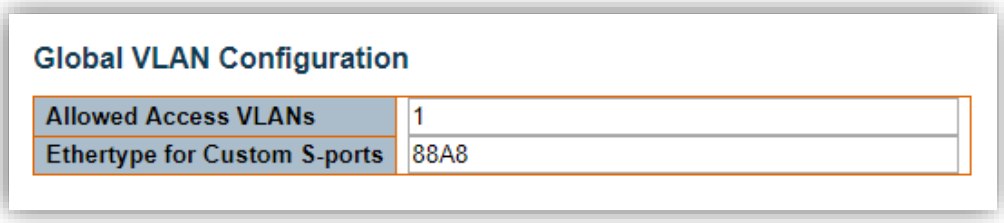


Setting	Description
Delete	Check to delete the entry. It will be deleted during the next save.
VLAN ID	The VLAN ID of the entry.
MAC Address	The MAC address of the entry.
Port Members	Checkmarks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry.

Configuration > VLANs

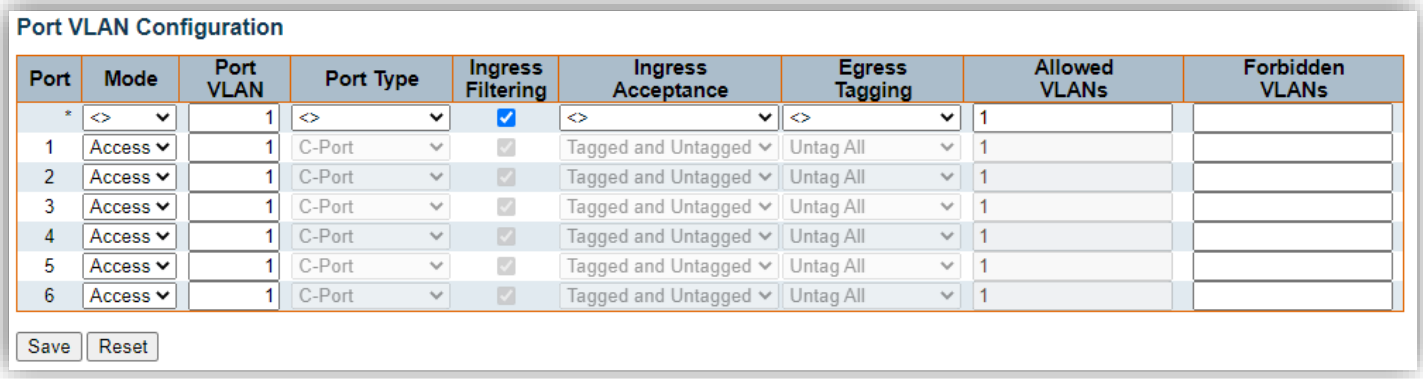
This page allows for controlling VLAN configuration on the switch.
The page is divided into a global section and a per-port configuration section.

- **Global VLAN Configuration**



Setting	Description
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 the 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**



Setting	Description
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 and C-tagged frames • Discards all frames 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 VLANs (1-4095) • The VLANs that a trunk port is member of may be limited by the use of Allowed VLANs • Frames classified to a VLAN that the port is not a member of are 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 **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 ports 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 frames 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 egress, if frames must be tagged, they will be tagged with an S-tag. On ingress, frames with a VLAN tag with TPID = 0x88A8 get classified to the VLAN ID embedded in the tag. Priority-tagged frames are classified to the Port VLAN. If the port is configured to accept Tagged Only frames (see Ingress Acceptance below), frames without this TPID are dropped. ***Notice:*** If the S-port is configured to accept Tagged and Untagged frames (see Ingress Acceptance below), frames with a C-tag are treated like frames with an S-tag. If the S-port is configured to accept Untagged Only frames, S-tagged frames will be discarded (except for priority S-tagged frames). C-tagged frames are initially considered untagged and will therefore not be discarded. Later on in the ingress classification process, they will get classified to the VLAN embedded in the tag instead of the port VLAN ID. **S-Custom-Port:** On egress, if frames must be tagged, they will be tagged with the custom S-tag. On ingress, frames with a VLAN tag with a TPID equal to the Ethertype configured for Custom-S ports get classified to the VLAN ID embedded in the tag. Priority-tagged frames are classified to the Port VLAN. If the port is configured to accept Tagged Only frames (see Ingress Acceptance below), frames without this TPID are dropped. ***Notice:*** If the custom S-port is configured to accept Tagged and Untagged frames (see Ingress Acceptance below), frames with a C-tag are treated like frames with a custom S-tag.

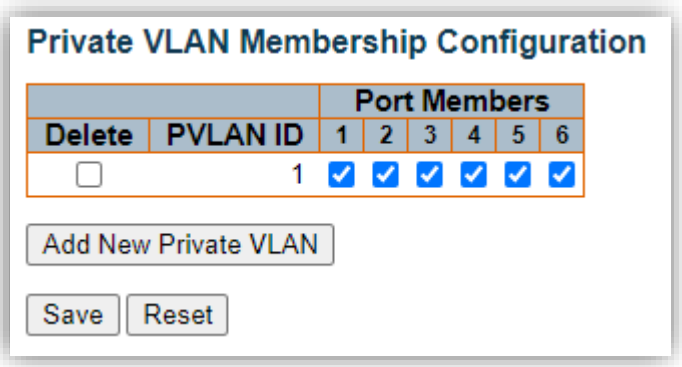
	If the Custom S-port is configured to accept Untagged Only frames, custom S-tagged frames will be discarded (except for priority custom S-tagged frames). C-tagged frames are initially considered untagged and will therefore not be discarded. Later on in the ingress classification process, they will get classified to the VLAN embedded in the tag instead of the port VLAN ID.
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. See Port Type for a description of when a frame is considered tagged. **Tagged Only:** Only frames tagged with the corresponding Port Type tag are accepted on ingress. **Untagged Only:** Only untagged frames are accepted on ingress. See Port Type for a description of when a frame is considered untagged.
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 Enabled VLANs field. By default, a Trunk or Hybrid port will become member of all VLANs, and is therefore set to **1-4095**. The field may be left empty, which means that the port will not become member of any VLANs.
Forbidden VLANs	A port may be configured to never become 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 Enabled VLANs field.

	By default, the field is left blank, which means that the port may become a member of all possible VLANs.

Configuration > Private VLANs > Membership

- **Private VLAN Membership Configuration**

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.

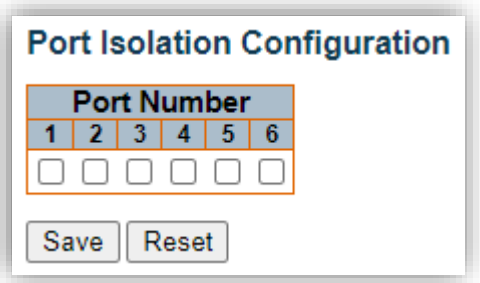


Setting	Description
Delete	To delete a private VLAN entry, check this box. The entry will be deleted during the next save.
Private VLAN ID	Indicates the ID of this particular private VLAN.
Port Members	A row of check boxes for each port is displayed for each private VLAN ID. To include a port in a Private 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.

Configuration > Private VLANs > Port Isolation

- **Port Isolation Configuration**

This page is used for enabling or disabling port isolation on ports in a Private VLAN.
A port member of a VLAN can be isolated to other isolated ports on the same VLAN and Private VLAN.



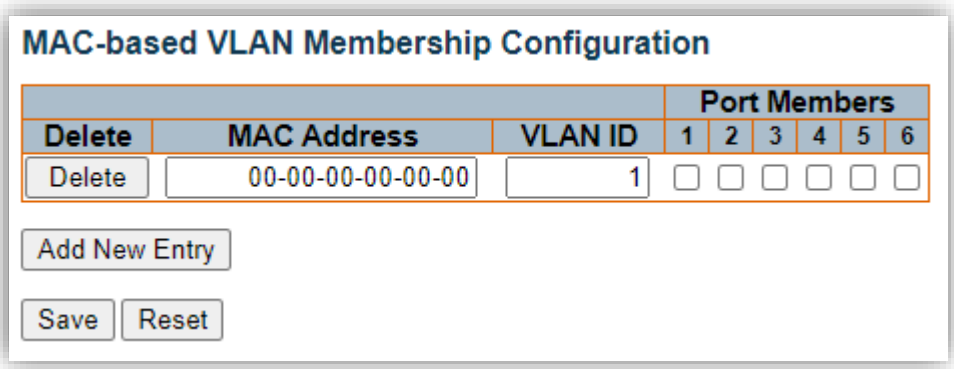
Port Number

Setting	Description	Factory Default
Checked	Port isolation is enabled on that port.	Unchecked
Unchecked	Port isolation is disabled on that port.	

Configuration > VCL > MAC-based VLAN

- **MAC-Based VLAN Membership Configuration**

The MAC address to VLAN ID mappings can be configured here. This page allows adding and deleting MAC-based VLAN Classification List entries and assigning the entries to different ports.



Setting	Description
Delete	To delete a MAC to VLAN ID mapping entry, check this box and press save. The entry will be deleted in the stack.
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 to VLAN ID mapping entry. To include a port in the 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.

"Add New Entry" button

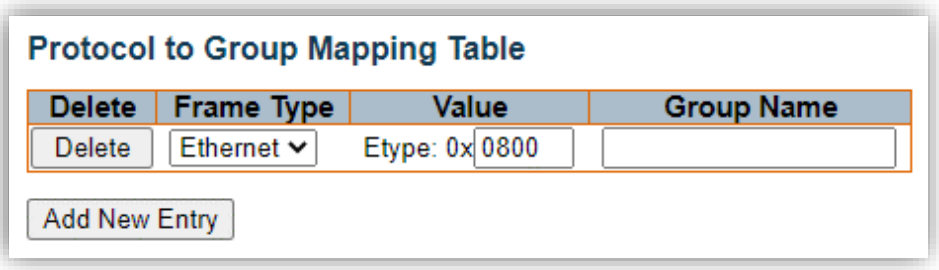
Click "Add New Entry" button to add a new MAC to VLAN ID mapping entry. An empty row is added to the table, and the mapping can be configured as needed. Any unicast MAC address can be used to configure the mapping. No broadcast or multicast MAC addresses are allowed. Legal values for a VLAN ID are **1** through **4095**.

The MAC to VLAN ID entry is enabled when you click on "Save". A mapping without any port members will not be added when you click "Save". The maximum possible MAC to VLAN ID mapping entries are limited to 256.

Configuration > VCL > Protocol-based VLAN > Protocol to Group

- **Protocol to Group Mapping Table**

This page allows you to add new Protocol to Group Name (each protocol can be part of only one Group) mapping entries as well as allow you to see and delete already mapped entries for the switch.



Setting	Description
Delete	To delete a Protocol to Group Name map entry, check this box. The entry will be deleted from the switch during the next Save.
Frame Type	Frame Type can have one of the following values: • **Ethernet** • **LLC** • **SNAP** **NOTE:** When changing the Frame type field, the 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 16-character long string, unique for every entry, which consists of a combination of alphabets (a-z or A-Z) and integers (0-9). **NOTE:** Special characters and underscores (_) are not allowed.

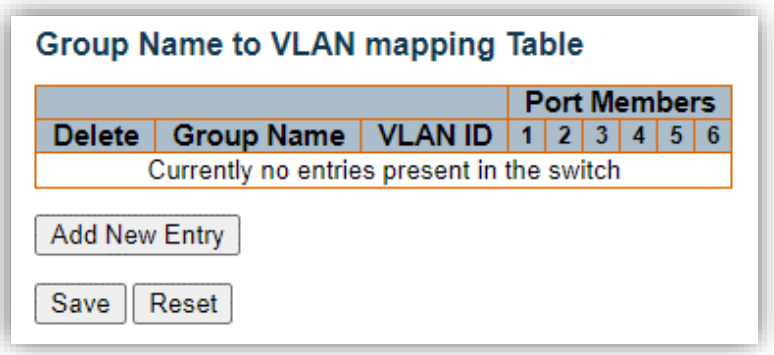
"Add New Entry" button

Click **“Add New Entry”** to add a new entry in the mapping table. An empty row is added to the table, where Frame Type, Value and the Group Name can be configured as needed. The maximum possible Protocol to Group mappings are limited to 128.

Configuration > VCL > Protocol-based VLAN > Group to VLAN

- **Group Name to VLAN mapping Table**

This page allows you to map a Group Name (already configured or to be configured in the future) to a VLAN for the switch.



Setting	Description
Delete	To delete a Group Name to VLAN mapping, check this box. The entry will be deleted from the switch during the next Save.
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 VLAN ID to which the Group Name will be mapped. A valid VLAN ID ranges from 1 to 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 the 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.

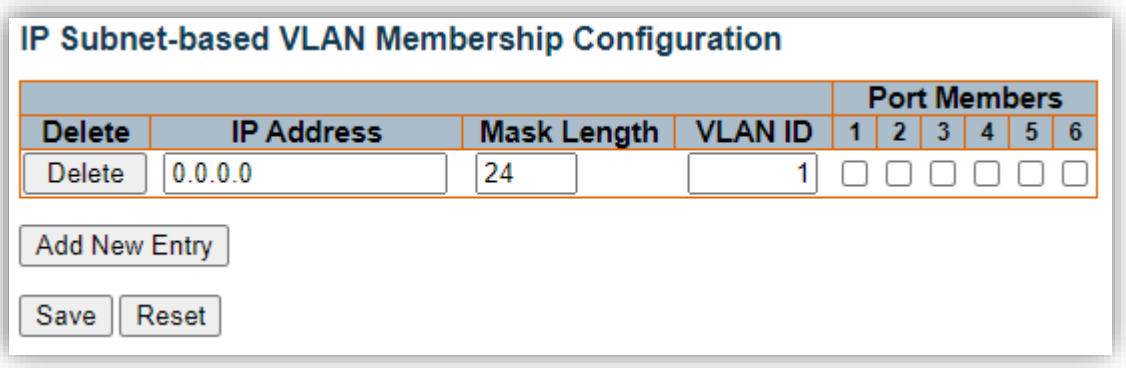
"Add New Entry" button

Click "Add New Entry" button to add a new entry in the mapping table. An empty row is added to the table and the Group Name, VLAN ID and port members can be configured as needed. Legal values for a VLAN ID are **1** through **4095**. The maximum possible Group to VLAN mappings are limited to 256.

Configuration > VCL > IP Subnet-based VLAN

- **IP Subnet-based VLAN Membership Configuration**

The IP subnet to VLAN ID mappings can be configured here. This page allows adding, updating and deleting IP subnet to VLAN ID mapping entries and assigning them to different ports.



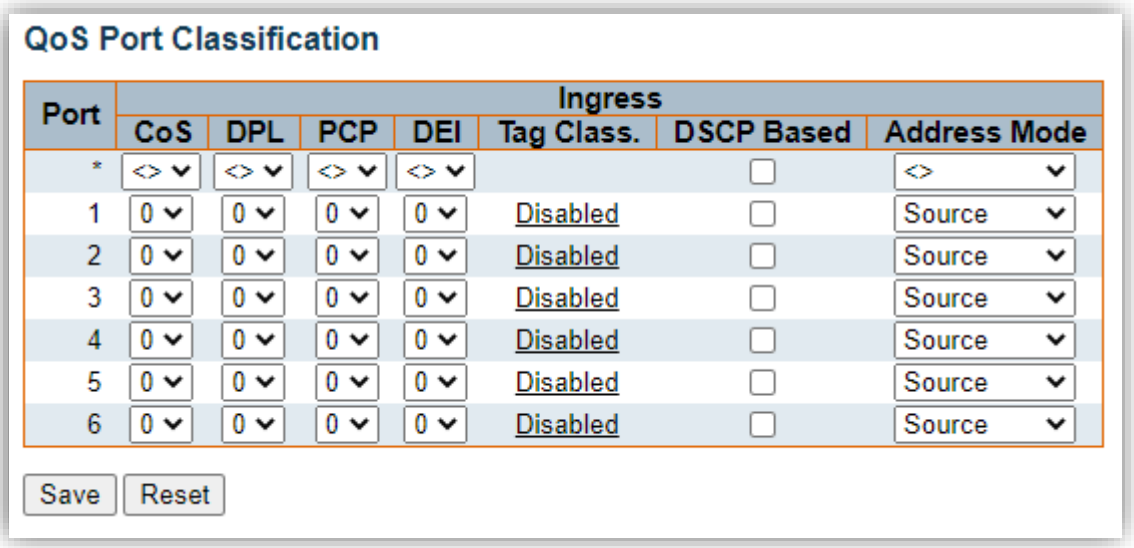
Setting	Description
Delete	To delete a mapping, check this box and press save. The entry will be deleted in the stack.
IP Address	Indicates the subnet's IP address (Any of the subnet's host addresses can be also provided here, the application will convert it automatically).
Mask Length	Indicates the subnet's mask length.
VLAN ID	Indicates the VLAN ID the subnet will be mapped to. IP Subnet to VLAN ID is a unique matching.
Port Members	A row of check boxes for each port is displayed for each IP subnet to VLAN ID mapping entry. To include a port in a mapping, simply 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.

"Add New Entry" button

Click "Add New Entry" button to add a new IP subnet to VLAN ID mapping entry. An empty row is added to the table, and the mapping can be configured as needed. Any IP address/mask can be configured for the mapping. Legal values for the VLAN ID are **1** to **4095**. The IP subnet to VLAN ID mapping entry is enabled when you click on "Save". The maximum possible IP subnet to VLAN ID mappings are limited to 128.

Configuration > QoS > Port Classification

- **QoS Ingress Port Classification**



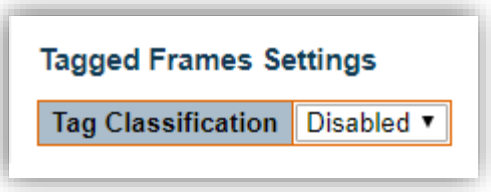
Setting	Description
Port	The port number for which the configuration below applies.
CoS	Controls the default CoS value. All frames are classified to a CoS. There is a one to one mapping between CoS, queue and priority. A CoS of 0 (zero) has the lowest priority. If the port is VLAN aware, the frame is tagged and Tag Class. is enabled, then the frame is classified to a CoS that is mapped from the PCP and DEI value in the tag. Otherwise the frame is classified to the default CoS. The classified CoS can be overruled by a QCL entry. **Note**: If the default CoS has been dynamically changed, then the actual default CoS is shown in parentheses after the configured default CoS.
DPL	Controls the default DPL value. All frames are classified to a Drop Precedence Level. If the port is VLAN aware, the frame is tagged and Tag Class. is enabled, then the frame is classified to a DPL that is mapped from the PCP and DEI value in the tag. Otherwise the frame is classified to the default DPL. The classified DPL can be overruled by a QCL entry.
PCP	Controls the default PCP value. All frames are classified to a PCP value. If the port is VLAN aware and the frame is tagged, then the frame is classified to the PCP value in the tag. Otherwise the frame is classified to the default PCP value.
DEI	Controls the default DEI value. All frames are classified to a DEI value. If the port is VLAN aware and the frame is tagged, then the frame is classified to the DEI value in the tag. Otherwise the frame is classified to the default DEI value.

Tag 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.
Address Mode	The IP/MAC address mode specifying whether the QCL classification must be based on source (SMAC/SIP) or destination (DMAC/DIP) addresses on this port. The allowed values are: • **Source:** Enable SMAC/SIP matching. • **Destination:** Enable DMAC/DIP matching.

- **QoS Ingress Port Tag Classification Port n**

The classification mode for tagged frames are configured on this page.

Tagged Frames Settings



Setting	Description	Factory Default
Enabled	Use mapped versions of PCP and DEI for tagged frames.	Disabled
Disabled	Use default QoS class and Drop Precedence Level for tagged frames.	

(PCP, DEI) to (QoS class, DP level) Mapping

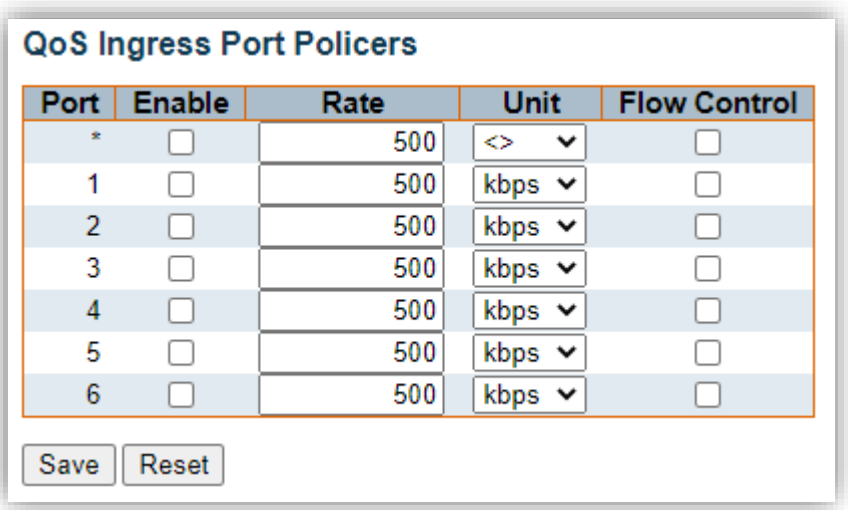
Controls the mapping of the classified (PCP, DEI) to (QoS class, DP level) values when Tag Classification is set to **Enabled**.

(PCP, DEI) to (CoS, DPL) Mapping

PCP	DEI	CoS	DPL
*	*	<>	<>
0	0	1	0
0	1	1	1
1	0	0	0
1	1	0	1
2	0	2	0
2	1	2	1
3	0	3	0
3	1	3	1
4	0	4	0
4	1	4	1
5	0	5	0
5	1	5	1
6	0	6	0
6	1	6	1
7	0	7	0
7	1	7	1

Configuration > QoS > Port Policing

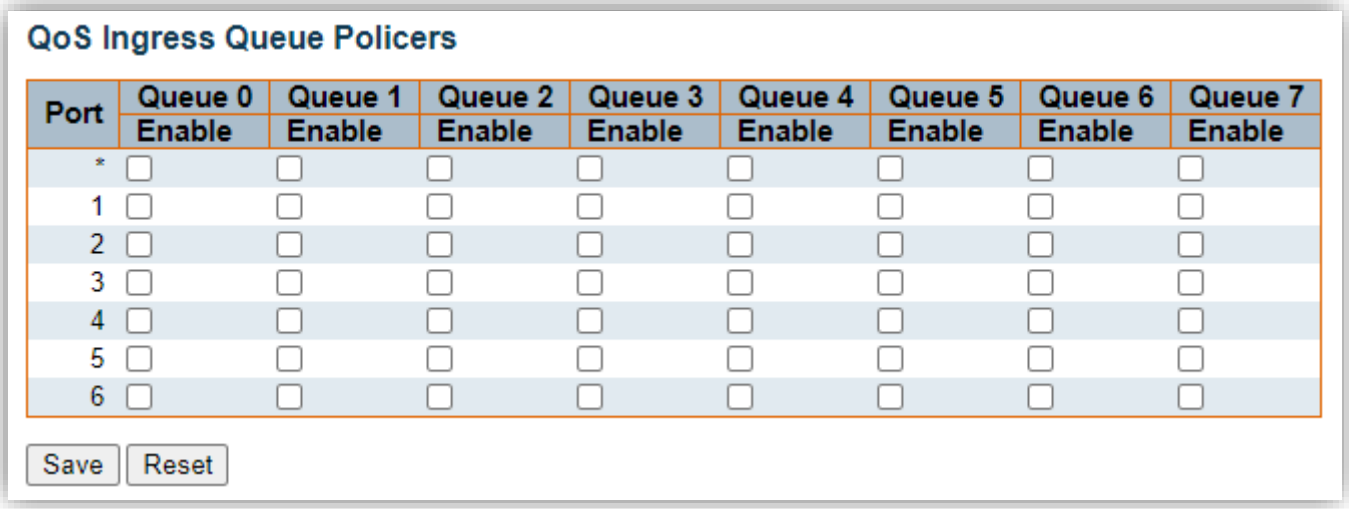
- **QoS Ingress Port Policers**



Setting	Description
Port	The port number for which the configuration below applies.
Enable	Enable or disable the port policer for this switch port.
Rate	Controls the rate for the port policer. This value is restricted to 100-3276700 when "Unit" is kbps or fps, and 1-3276 when "Unit" is Mbps or kfps. The rate is internally rounded up to the nearest value supported by the port policer.
Unit	Controls the unit of measure for the port policer rate as kbps, Mbps, fps or kfps.
Flow Control	If flow control is enabled and the port is in flow control mode, then pause frames are sent instead of discarding frames.

Configuration > QoS > Queue Policing

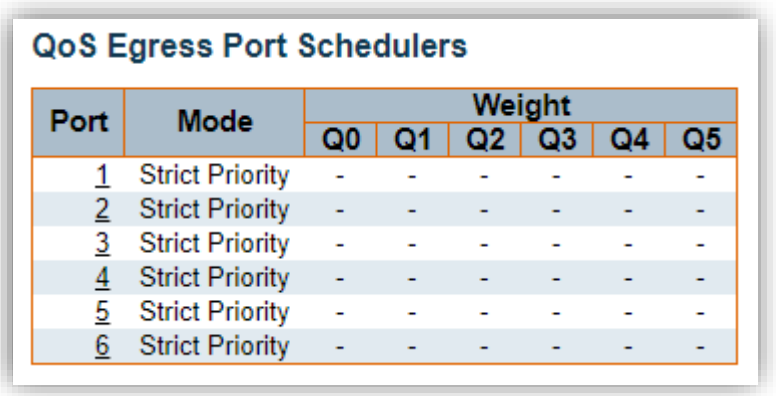
- **QoS Ingress Queue Policers**



Setting	Description
Port	The port number for which the configuration below applies.
Enable	Enable or disable the queue policer for this switch port.
Rate	Controls the rate for the port policer. This value is restricted to 100-3276700 when "Unit" is kbps or fps, and 1-3276 when "Unit" is Mbps or kfps. The rate is internally rounded up to the nearest value supported by the port policer. Controls the rate for the queue policer. This value is restricted to 100-3276700 when "Unit" is kbps, and 1-3276 when "Unit" is Mbps. The rate is internally rounded up to the nearest value supported by the queue policer. This field is only shown if at least one of the queue policers are enabled.
Unit	Controls the unit of measure for the queue policer rate as kbps or Mbps. This field is only shown if at least one of the queue policers are enabled.

Configuration > QoS > Port Scheduler

- **QoS Egress Port Schedulers**



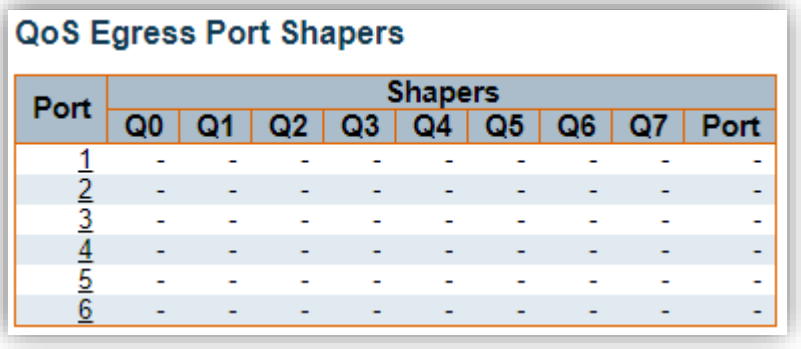
QoS Egress Port Schedulers

Port	Mode	Weight					
		Q0	Q1	Q2	Q3	Q4	Q5
1	Strict Priority	-	-	-	-	-	-
2	Strict Priority	-	-	-	-	-	-
3	Strict Priority	-	-	-	-	-	-
4	Strict Priority	-	-	-	-	-	-
5	Strict Priority	-	-	-	-	-	-
6	Strict Priority	-	-	-	-	-	-

Setting	Description
Port	The logical port for the settings contained in the same row. Click on the port number in order to configure the schedulers.
Mode	Shows the scheduling mode for this port.
Qn	Shows the weight for this queue and port.

Configuration > QoS > Port Shaping

- **QoS Egress Port Shapers**



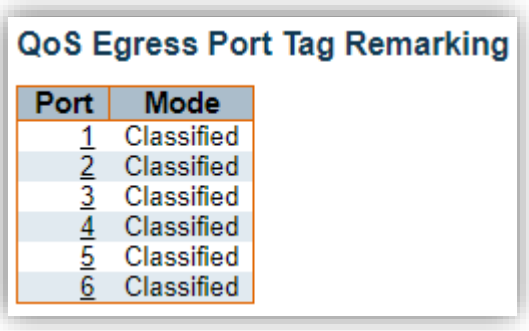
QoS Egress Port Shapers

Port	Shapers								
	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Port
1	-	-	-	-	-	-	-	-	-
2	-	-	-	-	-	-	-	-	-
3	-	-	-	-	-	-	-	-	-
4	-	-	-	-	-	-	-	-	-
5	-	-	-	-	-	-	-	-	-
6	-	-	-	-	-	-	-	-	-

Setting	Description
Port	The logical port for the settings contained in the same row. Click on the port number in order to configure the shapers.
Qn	Shows "-" for disabled or actual queue shaper rate - e.g. "800 Mbps".
Port	Shows "-" for disabled or actual port shaper rate - e.g. "800 Mbps".

Configuration > QoS > Port Tag Remarking

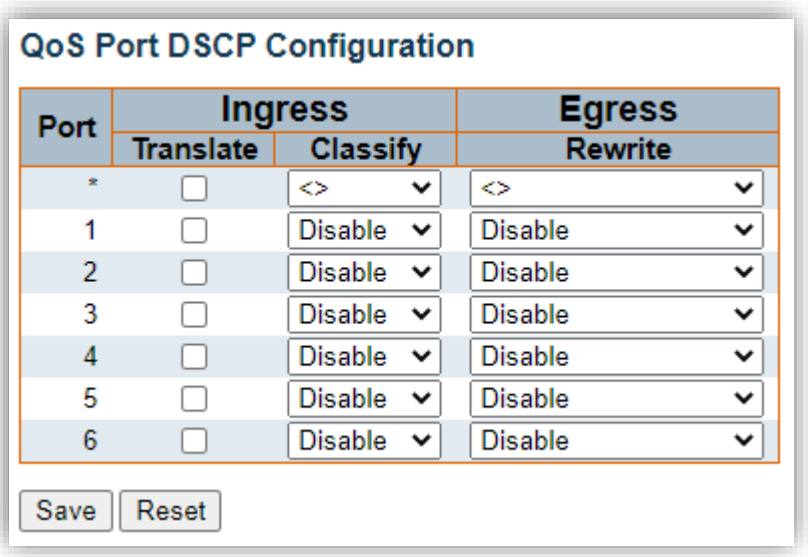
- **QoS Egress Port Tag Remarking**



Setting	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	Shows the tag remarking mode for this port. • **Classified:** Use classified PCP/DEI values. • **Default:** Use default PCP/DEI values. • **Mapped:** Use mapped versions of QoS class and DP level.

Configuration > QoS > Port DSCP

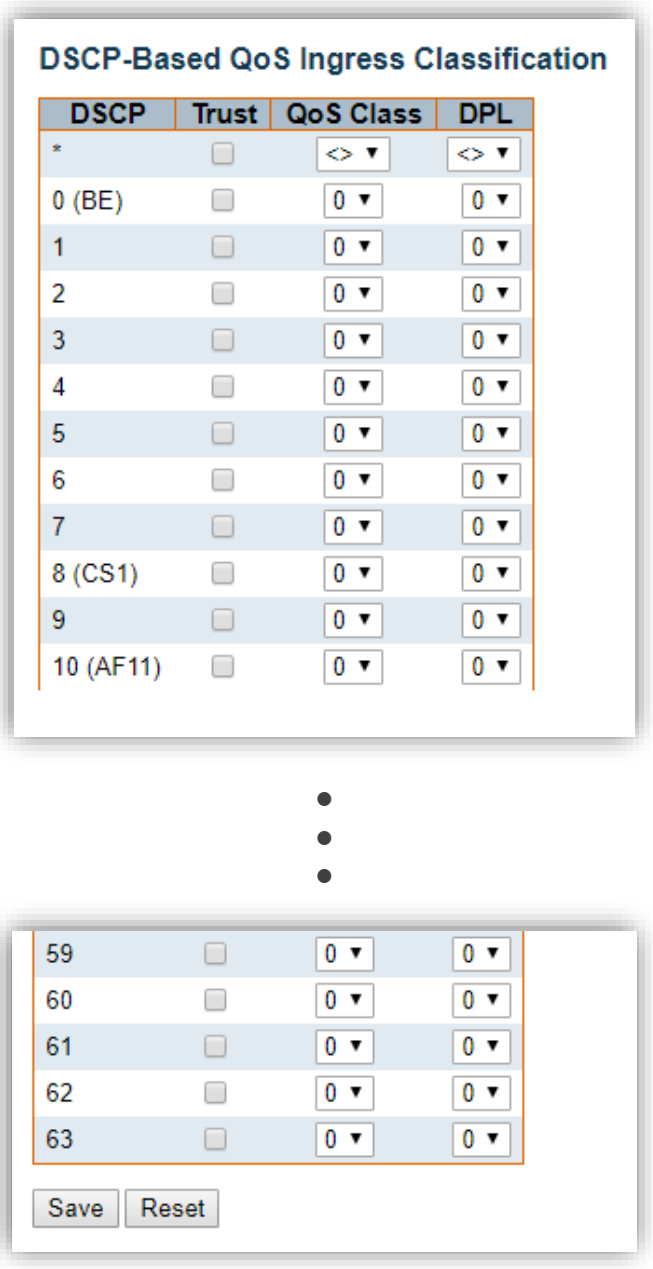
- **QoS Port DSCP Configuration**



Setting	Description
Port	The Port column shows the list of ports for which you can configure dscp ingress and egress settings.
Ingress	**Translate:** To Enable the Ingress Translation click the checkbox. **Classify:** Classification for a port have 4 different values. 1. **Disable:** No Ingress DSCP Classification. 2. **DSCP=0:** Classify if incoming (or translated if enabled) DSCP is 0. 3. **Selected:** Classify only selected DSCP for which classification is enabled as specified in DSCP Translation window for the specific DSCP. 4. **All:** Classify all DSCP.
Egress	**Disable:** No Egress rewrite. **Enable:** Rewrite enabled without remapping. **Remap DP Unaware:** DSCP from analyzer is remapped and frame is remarked with remapped DSCP value. The remapped DSCP value is always taken from the 'DSCP Translation->Egress Remap DP0' table. **Remap DP Aware:** DSCP from analyzer is remapped and frame is remarked with remapped DSCP value. Depending on the DP level of the frame, the remapped DSCP value is either taken from the 'DSCP Translation->Egress Remap DP0' table or from the 'DSCP Translation->Egress Remap DP1' table.

Configuration > QoS > DSCP-Based QoS

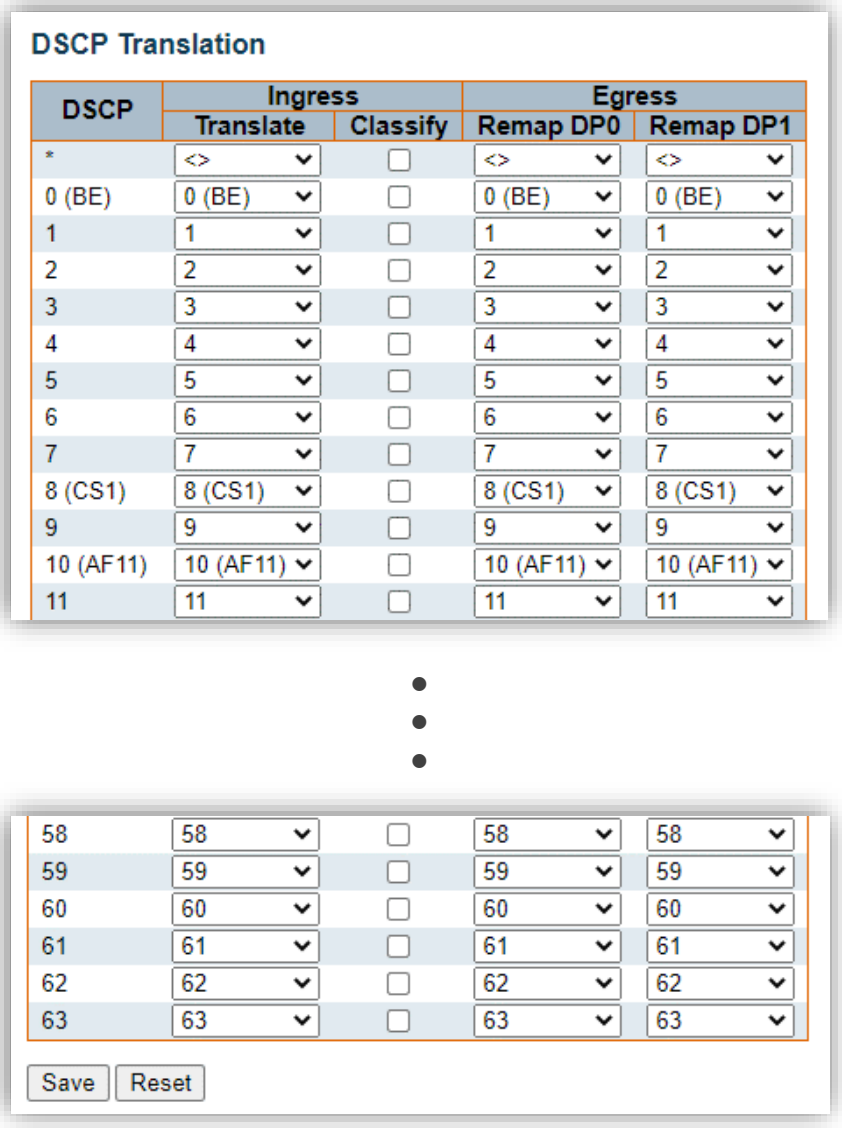
- **DSCP-based QoS Ingress Classification**



Setting	Description
DSCP	Maximum number of supported DSCP values are 64.
Trust	Controls whether a specific DSCP value is trusted. Only frames with trusted DSCP values are mapped to a specific QoS class and Drop Precedence Level. Frames with untrusted DSCP values are treated as a non-IP frame.
QoS Class	QoS class value can be any of (0-7)
DPL	Drop Precedence Level (0-3)

Configuration > QoS > DSCP Translation

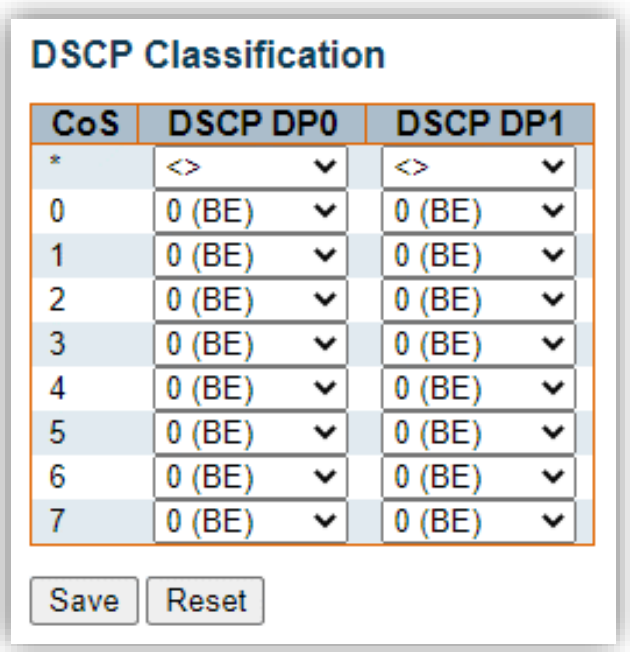
- **DSCP Translation**



Setting	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. • **Translate:** DSCP at Ingress side can be translated to any of (0-63) DSCP values. • **Classify:** Click to enable Classification at Ingress side.
Egress	• **Remap DP0:** Select the DSCP value from select menu to which you want to remap. DSCP value ranges from 0 to 63. • **Remap DP1:** Select the DSCP value from select menu to which you want to remap. DSCP value ranges form 0 to 63.

Configuration > QoS > DSCP Classification

- **DSCP Classification**

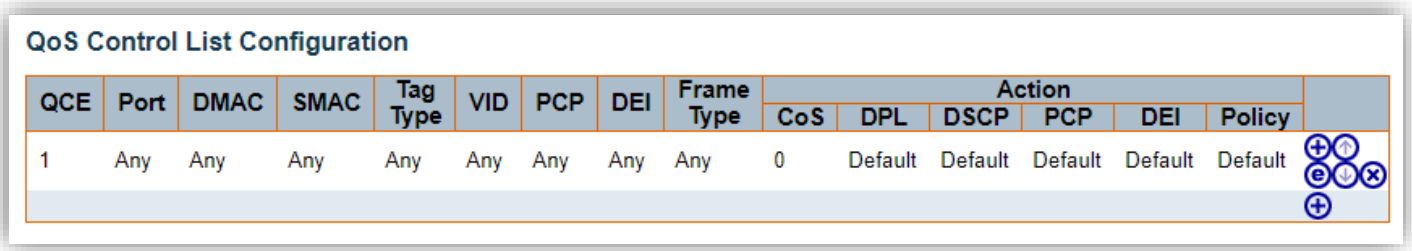


Setting	Description
QoS Class	Actual QoS class.
DSCP DP0	Select the classified DSCP value (0-63) for Drop Precedence Level 0.
DSCP DP1	Select the classified DSCP value (0-63) for Drop Precedence Level 1.

Configuration > QoS > QoS Control List

QoS Control List Configuration

This page shows the QoS Control List(QCL), which is made up of the QCEs. Each row describes a QCE that is defined. The maximum number of QCEs is **256** on each switch.
Click on the lowest plus sign to add a new QCE to the list.



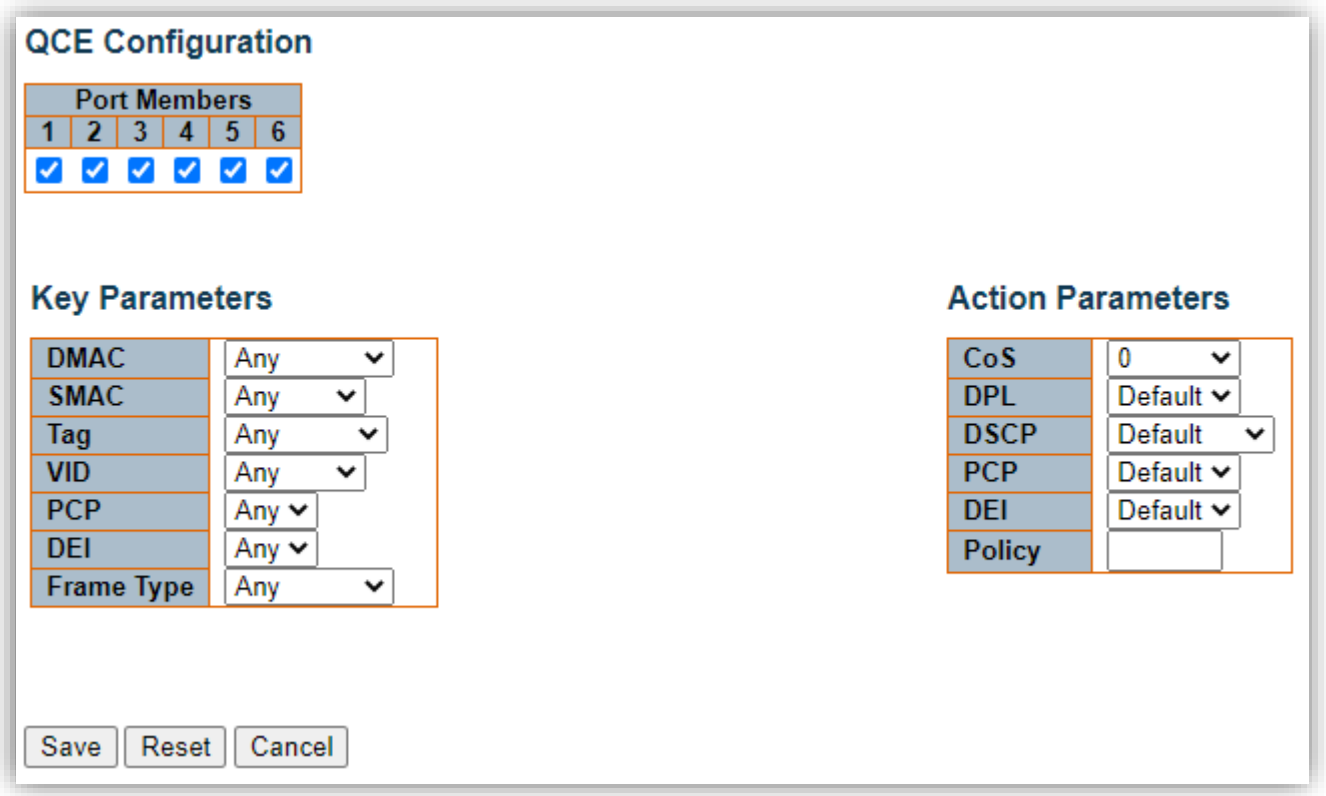
You can modify each QCE (QoS Control Entry) in the table using the following buttons: : Inserts a new QCE before the current row.
: Edits the QCE.
: Moves the QCE up the list.
: Moves the QCE down the list.
: Deletes the QCE.
: The lowest plus sign adds a new entry at the bottom of the QCE listings.

Setting	Description
QCE	Indicates the QCE id.
Port	Indicates the list of ports configured with the QCE or 'Any'.
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. The default value is 'Any'.
SMAC	Match specific source MAC address or 'Any'. If a port is configured to match on destination addresses, this field indicates the DMAC
Tag Type	Indicates tag type. Possible values are: • **Any:** Match tagged and untagged frames. • **Untagged:** Match untagged frames. • **Tagged:** Match tagged frames. The default value is 'Any'.
VID	Indicates (VLAN ID), either a specific VID or range of VIDs. VID can be in the range 1-4095 or 'Any'
PCP	Priority Code Point: Valid values of PCP are specific(0, 1, 2, 3, 4, 5, 6, 7) or range(0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'.
DEI	Drop Eligible Indicator: Valid value of DEI are 0, 1 or 'Any'.
Frame Type	Indicates the type of frame. Possible values are: 1. **Any:** Match any frame type.

	2. **Ethernet:** Match EtherType frames. 3. **LLC:** Match (LLC) frames. 4. **SNAP:** Match (SNAP) frames. 5. **IPv4:** Match IPv4 frames. 6. **IPv6:** Match IPv6 frames.
Action	Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content. Possible actions are: 1. **CoS:** Classify Class of Service. 2. **DPL:** Classify Drop Precedence Level. 3. **DSCP:** Classify DSCP value. 4. **PCP:** Classify PCP value. 5. **DEI:** Classify DEI value. 6. **Policy:** Classify ACL Policy number.

- **QCE Configuration**

This page allows to edit/ insert a single QoS Control Entry at a time. A QCE consists of several parameters. These parameters vary according to the frame type that you select.



Port Members
Check the checkbox button to include the port in the QCL entry. By default all ports are included.

- **Key Parameters**

Setting	Description
DMAC	Destination MAC address: Possible values are **Unicast**, **Multicast**, **Broadcast** or **Any**.
SMAC	Source MAC address: **xx-xx-xx-xx-xx-xx** or **Any**.
Tag	Value of Tag field can be **Untagged, Tagged, C-Tagged, S-Tagged** or **Any**.
VID	Valid value of VLAN ID can be any value in the range **1-4095** or **Any**; user can enter either a specific value or a range of VIDs.
PCP	Valid value PCP are specific (**0, 1, 2, 3, 4, 5, 6, 7**) or range (**0-1, 2-3, 4-5, 6-7, 0-3, 4-7**) or **Any**.
DEI	Valid value of DEI can be **0**, **1** or **Any**.
Frame Type	Frame Type can have any of the following. 1. **Any** 2. **EtherType** 3. **LLC** 4. **SNAP** 5. **IPv4** 6. **IPv6**

All frame types are explained below.

1. **Any:** Allow all types of frames.
2. **EtherType:** Ether Type Valid Ether Type can be 0x600-0xFFFF excluding 0x800(IPv4) and 0x86DD(IPv6) or 'Any'.
3. **LLC:**
   - ***DSAP Address:*** Valid DSAP(Destination Service Access Point) can vary from 0x00 to 0xFF or 'Any'.
   - ***SSAP Address:*** Valid SSAP(Source Service Access Point) can vary from 0x00 to 0xFF or 'Any'.
   - ***Control:*** Valid Control field can vary from 0x00 to 0xFF or 'Any'.
4. **SNAP:** PID Valid PID(a.k.a Ether Type) can be 0x0000-0xFFFF or '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. If a port is configured to match on DMAC/DIP, this field is the Destination IP address.
   - ***IP Fragment:*** IPv4 frame fragmented option: 'Yes', 'No' or 'Any'.
   - ***DSCP:*** Diffserv Code Point value (DSCP): It can be a specific value, range of values or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or 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.

6. **IPv6**
   - ***Protocol:*** IP protocol number: (0-255, 'TCP' or 'UDP') or 'Any'.
   - ***Source IP:*** 32 LS bits of IPv6 source address in value/mask format or 'Any'. If a port is configured to match on DMAC/DIP, this field is the Destination IP address.
   - ***DSCP:*** Diffserv Code Point value (DSCP): It can be a specific value, range of values or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43.
   - ***Sport:*** Source TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.
   - ***Dport:*** Destination TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.

- **Action Parameters**

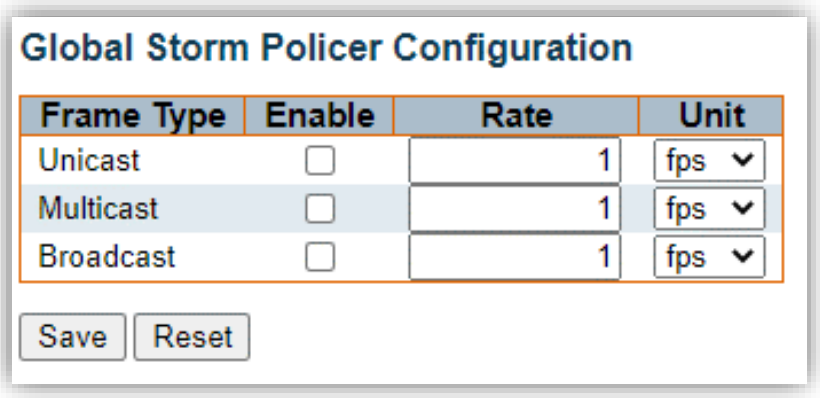
Setting	Description
CoS	Class of Service: (**0-7**) or **Default**.
DPL	Drop Precedence Level: (**0-1**) or **Default**.
DSCP	DS1CP: (**0-63, BE, CS1-CS7, EF** or **AF11-AF43**) or **Default**.
PCP	PCP: (**0-7**) or **Default**. Note: PCP and DEI cannot be set individually.
DEI	DEI: (**0-1**) or **Default**.
Policy	ACL Policy number: (**0-255**) or **Default** (empty field).

Note: "Default" means that the default classified value is not modified by this QCE.

Configuration > QoS > Storm Policing

- **Global Storm Policer Configuration**

There is a unicast storm policer, multicast storm policer, and a broadcast storm policer.
These only affect flooded frames, i.e. frames with a (VLAN ID, DMAC) pair not present in the MAC Address table.



Setting	Description
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 1-1024000 when "Unit" is fps, and 1-1024 when "Unit" is kfps. The rate is internally rounded up to the nearest value supported by the global storm policer. Supported rates are 1, 2, 4, 8, 16, 32, 64, 128, 256 and 512 fps for rates <= 512 fps and 1, 2, 4, 8, 16, 32, 64, 128, 256, 512 and 1024 kfps for rates > 512 fps.
Unit	Controls the unit of measure for the global storm policer rate fps, kfps, kbps or Mbps.

Configuration > Mirroring

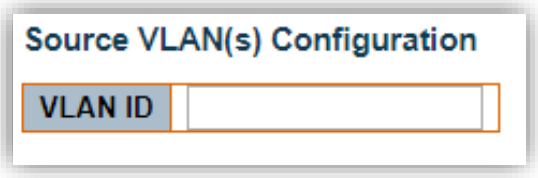
● Mirroring & Remote Mirroring Configuration

Mirroring is a feature for switched port analyzer. The administrator can use the Mirroring to debug network problems. The selected traffic can be mirrored or copied on a destination port where a network analyzer can be attached to analyze the network traffic.
Remote Mirroring is an extend function of Mirroring. It can extend the destination port in other switch. So the administrator can analyze the network traffic on the other switches.
If you want to get the tagged mirrored traffic, you have to set VLAN egress tagging as **Tag All** on the reflector port. On the other hand, if you want to get untagged mirrored traffic, you have to set VLAN egress tagging as **Untag ALL** on the reflector port.

Setting	Description
Session	Select session id to configure.
Mode	To Enabled/Disabled the mirror or Remote Mirroring function.
Type	Select switch type. • **Mirror:** The switch is running on mirror mode. The source port(s) and destination port are located on this switch. • **Rmirror 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.

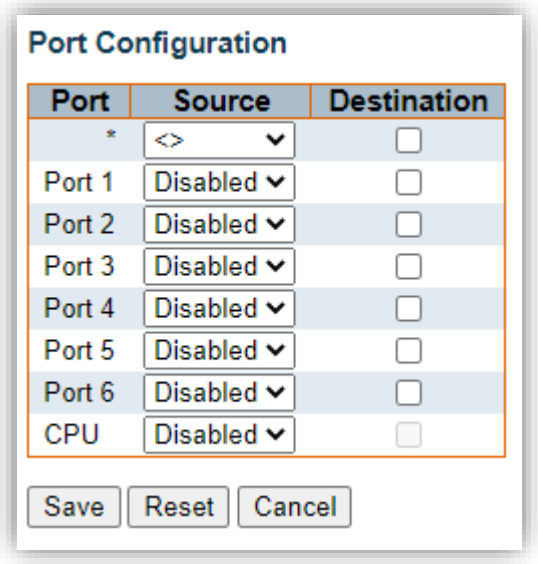
- **Source VLAN(s) Configuration**

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.



NOTE	The Mirroring session shall have either ports or VLANs as sources, but not both.

- **Port Configuration**



Setting	Description
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.

- **Configuration Guideline for All Features**

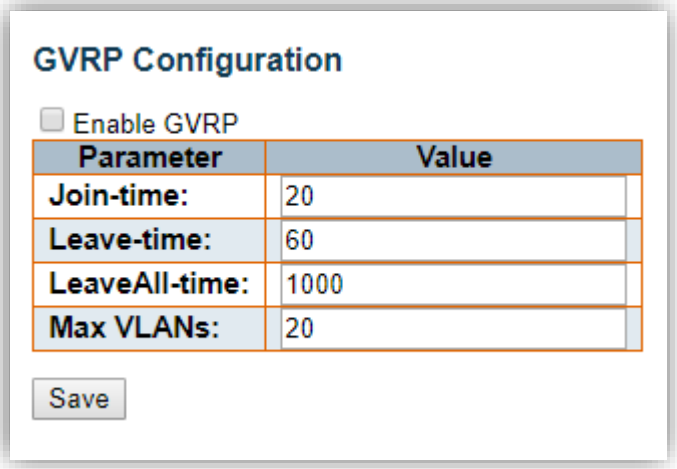
When the switch is running on Remote Mirroring mode, the administrator also needs to check whether or not other features are enabled or disabled.
For example, the administrator is not disabled the MSTP on reflector port. All monitor traffic will be blocked on reflector port.
All recommended settings are described as follows.

	Impact	Source Port	Reflector Port	Intermediate Port	Destination Port	Remote Mirroring VLAN
arp_inspection	High		* disabled	* disabled		
acl	Critical		* disabled	* disabled	* disabled	
dhcp_relay	High		* disabled	* disabled		
dhcp_snooping	High		* disabled	* disabled		
ip_source_guard	Critical		* disabled	* disabled	* disabled	
ipmc/igmpsnp	Critical					un-conflict
ipmc/mldsnp	Critical					un-conflict
lacp	Low				o disabled	
lldp	Low				o disabled	
mac learning	Critical		* disabled	* disabled	* disabled	
mstp	Critical		* disabled		o disabled	
mvr	Critical					un-conflict
nas	Critical		* authorized	* authorized	* authorized	
psec	Critical		* disabled	* disabled	* disabled	
qos	Critical		* unlimited	* unlimited	* unlimited	
upnp	Low				o disabled	
mac-based vlan	Critical		* disabled	* disabled		
protocol-based vlan	Critical		* disabled	* disabled		
vlan_translation	Critical		* disabled	* disabled	* disabled	
voice_vlan	Critical		* disabled	* disabled		
mrp	Low				o disabled	
mvrp	Low				o disabled	

Note:
* -- must
o -- optional
Impact: Critical/High/Low
Critical 5 packets -> 0 packet
High 5 packets -> 4 packets
Low 5 packets -> 6 packets

Configuration > GVRP > Global config

- **GVRP Configuration**



Enable GVRP
The GVRP feature is globally enabled by setting the check mark in the checkbox named Enable GVRP and pressing the Save button.

Join-time

Setting	Description	Factory Default
1 ~ 20	Join-time is a value in the range of 1-20cs, i.e. in units of one hundredth of a second.	20

Leave-time

Setting	Description	Factory Default
60 ~ 300	Leave-time is a value in the range of 60-300cs, i.e. in units of one hundredth of a second.	60

LeaveAll-time

Setting	Description	Factory Default
1000 ~ 5000	LeaveAll-time is a value in the range of 1000-5000cs, i.e. in units of one hundredth of a second. The default is 1000cs.	1000

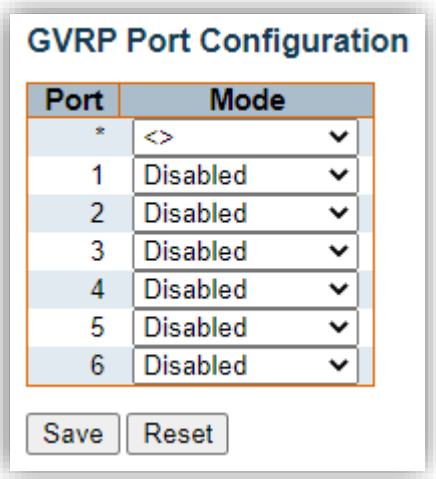
Max VLANs

Setting	Description	Factory Default
1 ~ 4094	When GVRP is enabled, a maximum number of VLANs supported by GVRP is specified. This number can only be changed when GVRP is turned off.	20

Configuration > GVRP > Port config

- **GVRP Port Configuration**

This configuration can be performed either before or after GVRP is configured globally - the protocol operation will be the same.

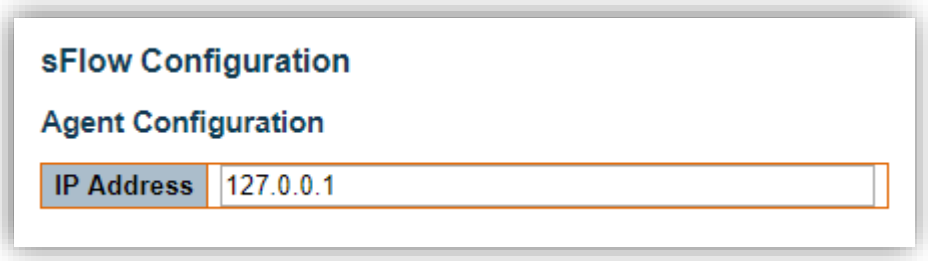


Setting	Description
Port	The logical port that is to be configured.
Mode	Mode can be either **Disabled** or **GVRP enabled**. These values turn the GVRP feature off or on respectively for the port in question.

Configuration > sFlow

This page allows for configuring sFlow. 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 will disable sFlow sampling.

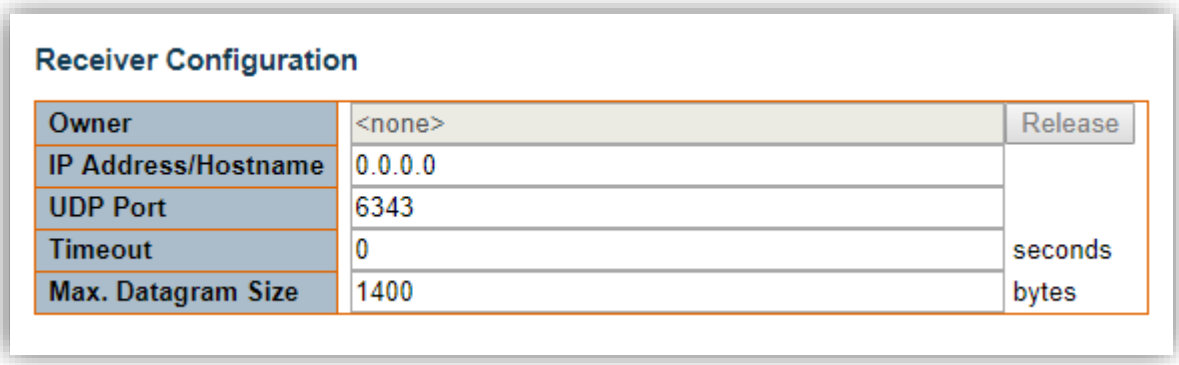
- **Agent Configuration**



IP Address

Setting	Description	Factory Default
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.	127.0.0.1

- **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

Setting	Description	Factory Default
IP Address	The IP address or hostname of the sFlow receiver. Both IPv4 and IPv6 addresses are supported.	0.0.0.0

UDP Port

Setting	Description	Factory Default
port number	The UDP port on which the sFlow receiver listens to sFlow datagrams. If set to 0, default port (6343) is used.	6343

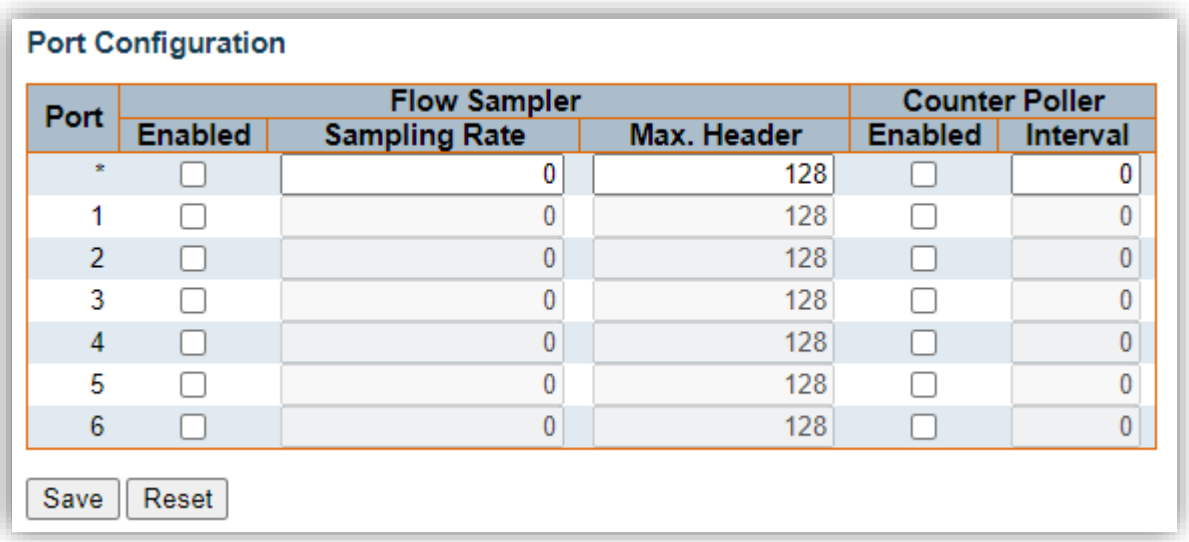
Timeout

Setting	Description	Factory Default
0 ~ 2147483647	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. Valid range is 0 to 2147483647 seconds.	0

Max. Datagram Size

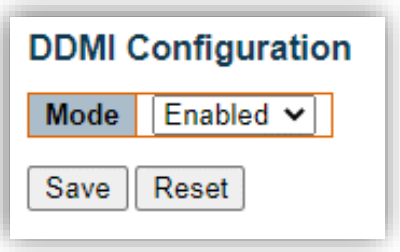
Setting	Description	Factory Default
200 ~ 1468	The maximum number of data bytes that can be sent in a single sample datagram. This should be set to a value that avoids fragmentation of the sFlow datagrams. Valid range is 200 to 1468 bytes.	1400

- **Port Configuration**



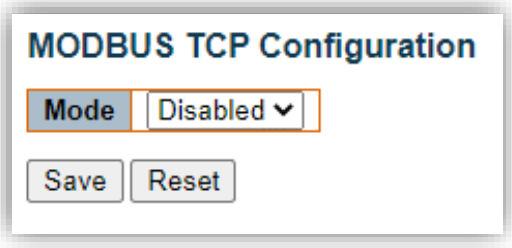
Setting	Description
Port	The port number for which the configuration below applies.
Flow Sampler Enabled	Enables/disables flow sampling on this port.
Flow Sampler Sampling Rate	The statistical sampling rate for packet sampling. Set to N to sample on average 1/Nth of the packets transmitted/received on 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 4294967295.
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. To have romm for any frame, the maximum datagram size should be roughly 100 bytes larger than the maximum header size. 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.

Configuration > DDMI



Setting	Description	Factory Default
Mode	Indicates the DDMI mode operation. Possible modes are: **Enabled**: Enable DDMI mode operation. **Disabled**: Disable DDMI mode operation.	Enabled

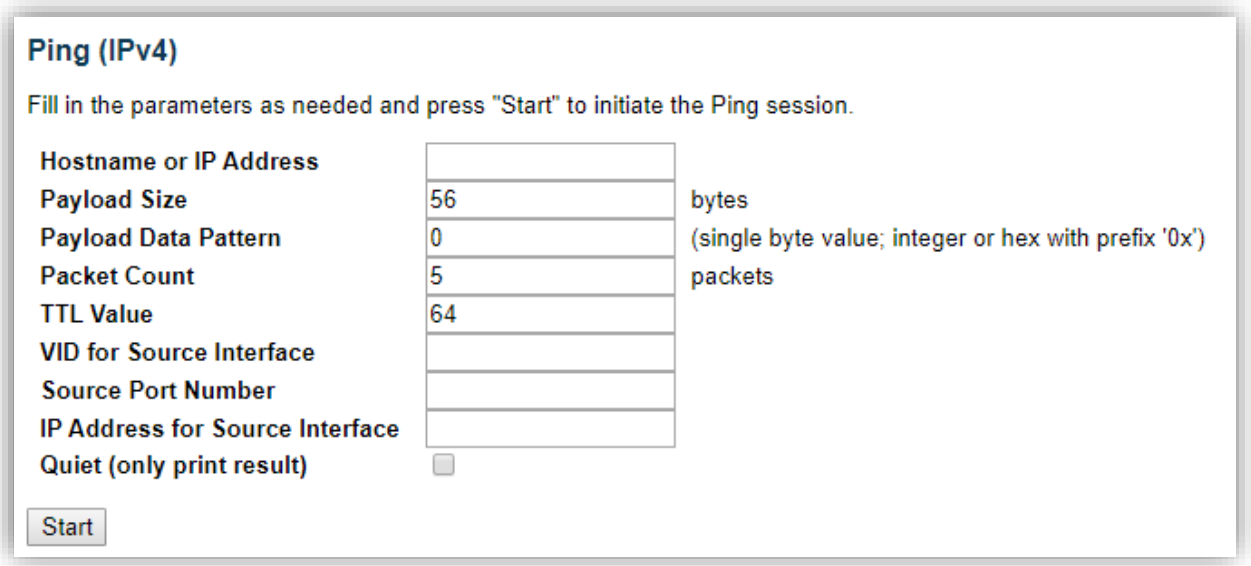
Configuration > MODBUS TCP



Setting	Description	Factory Default
Mode	Indicates the MODBUS TCP mode operation. Possible modes are: **Enabled**: Enable MODBUS TCP mode operation. **Disabled**: Disable MODBUS TCP mode operation.	Disabled

Diagnostics

Diagnostics > Ping(IPv4)



Setting	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.

After you press the **Start** button, ICMP packets are transmitted, and the sequence number and round trip time are displayed upon reception of a reply.

The amount of data received inside of an IP packet of type ICMP ECHO_REPLY will always be 8 bytes more than the requested payload data size (the difference is the ICMP header).

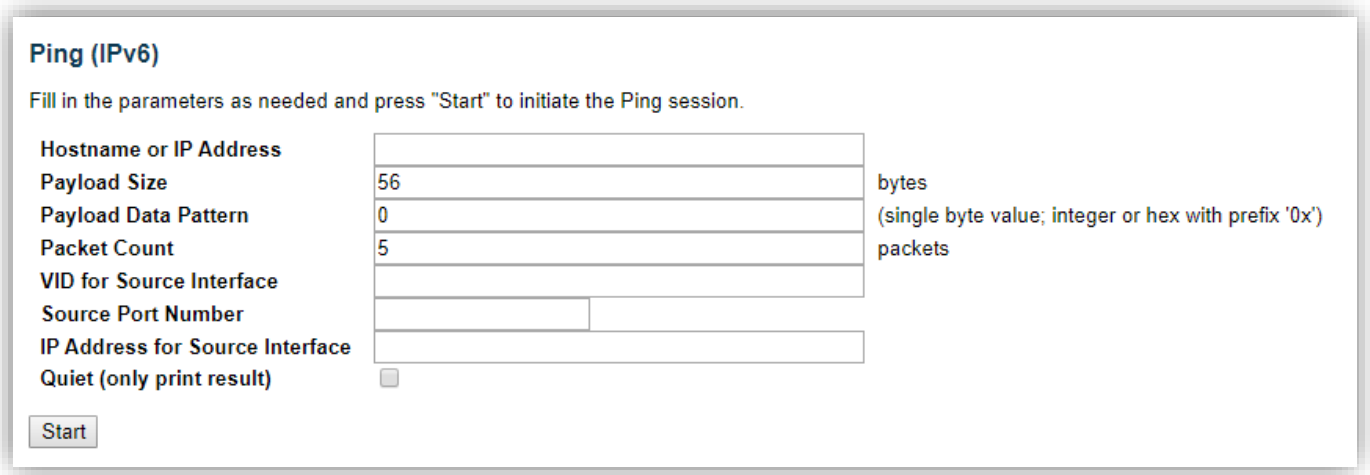
The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

The output from the command will look like the following:

PING 172.16.1.1 (172.16.1.1) from 172.16.1.10: 56 data bytes
64 bytes from 172.16.1.1: seq=0 ttl=64 time=2.034 ms
64 bytes from 172.16.1.1: seq=1 ttl=64 time=1.729 ms
64 bytes from 172.16.1.1: seq=2 ttl=64 time=1.954 ms
64 bytes from 172.16.1.1: seq=3 ttl=64 time=1.699 ms
64 bytes from 172.16.1.1: seq=4 ttl=64 time=1.916 ms

--- 172.16.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.699/1.866/2.034 ms

Diagnostics > Ping(IPv6)



Setting	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.

After you press the **Start** button, ICMP packets are transmitted, and the sequence number and round trip time are displayed upon reception of a reply.

The amount of data received inside of an IP packet of type ICMP ECHO_REPLY will always be 8 bytes more than the requested payload data size (the difference is the ICMP header).

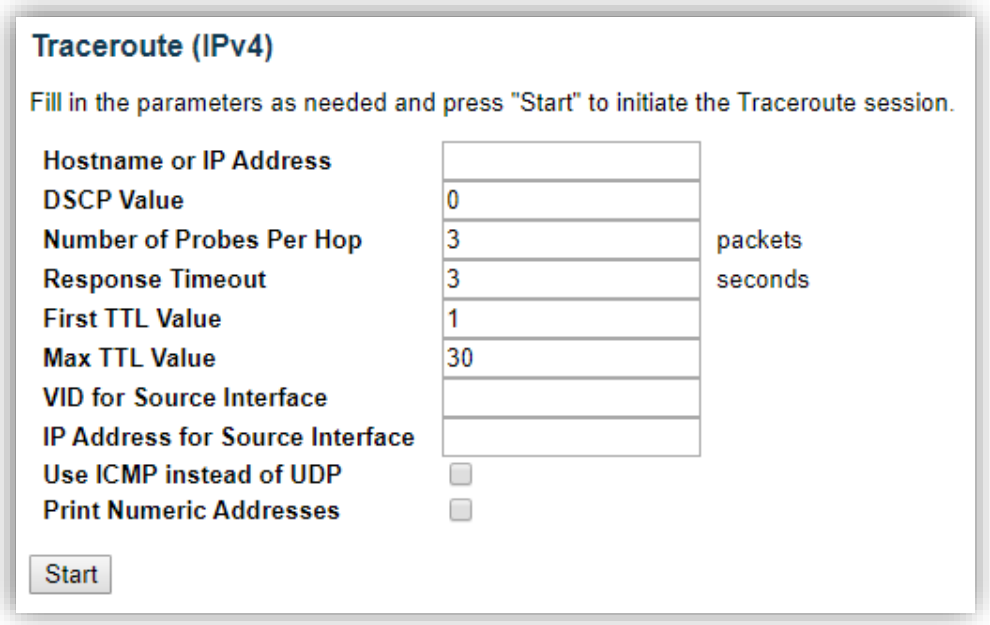
The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

The output from the command will look like the following:

PING 2001::01 (2001::1) from 2001::3: 56 data bytes
64 bytes from 2001::1: seq=0 ttl=64 time=2.118 ms
64 bytes from 2001::1: seq=1 ttl=64 time=2.009 ms
64 bytes from 2001::1: seq=2 ttl=64 time=1.852 ms
64 bytes from 2001::1: seq=3 ttl=64 time=2.869 ms
64 bytes from 2001::1: seq=4 ttl=64 time=1.845 ms

--- 2001::01 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.845/2.138/2.869 ms

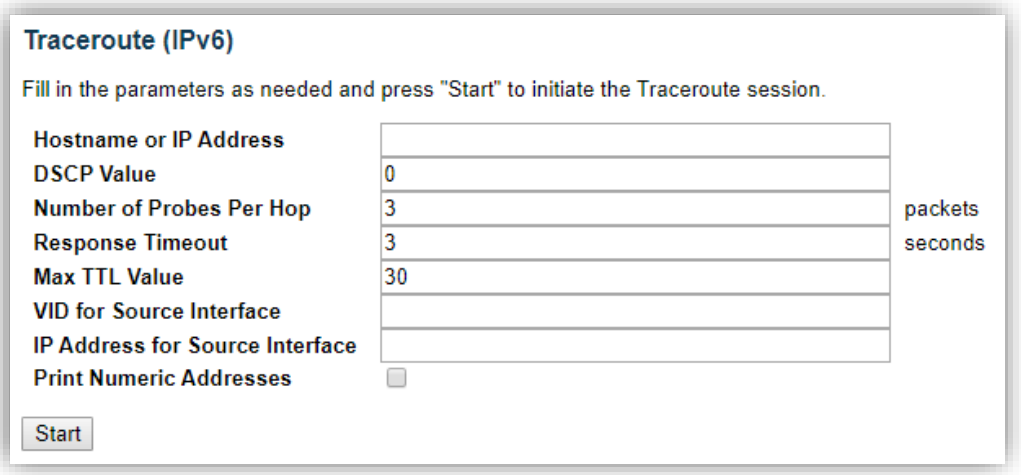
Diagnostics > Traceroute (IPv4)



Setting	Description
Hostname or IP Address	The destination IP Address.
DSCP Value	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.
Response Timeout	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.
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.

Diagnostics > Traceroute (IPv6)



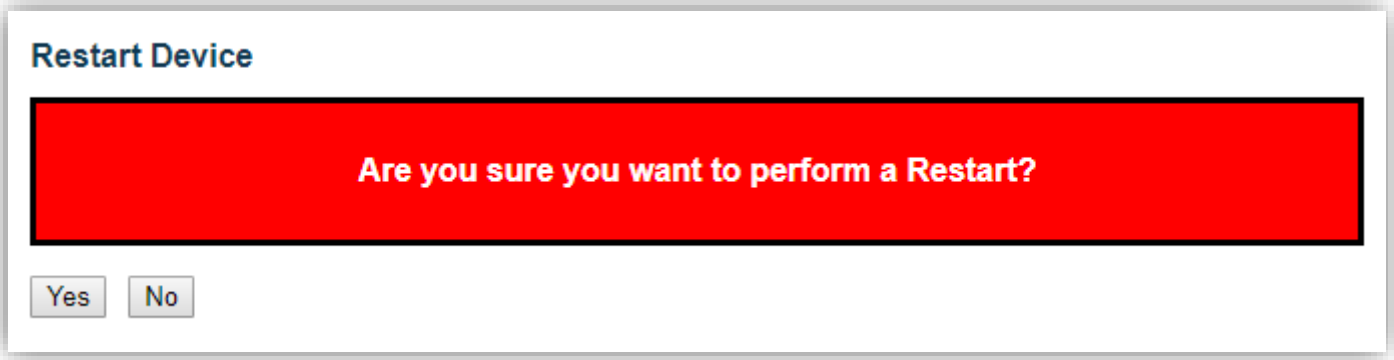
Setting	Description
Hostname or IP Address	The destination IP Address.
DSCP Value	This value is used for the DSCP value in the IPv4 header. The default value is 0. The valid range is 0-255.
Number of Probes Per Hop	Determines the number of probes (packets) sent for each hop. The default value is 3. The valid range is 1-60.
Response Timeout	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.

Maintenance

Maintenance > Restart Device

- **Restart Device**

You can restart the switch on this page. After restart, the switch will boot normally. Click **Yes** to restart device.
Click **No** to return to the Port State page without restarting.



Maintenance > Factory Defaults

- **Factory Defaults**

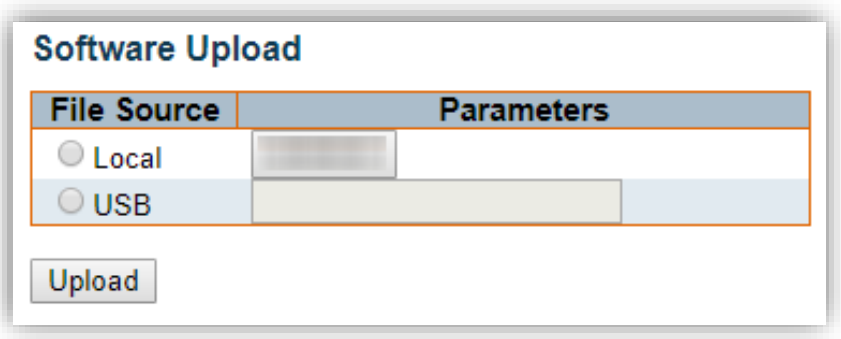
You can reset the configuration of the switch on this page. Only the IP configuration is retained. The new configuration is available immediately, which means that no restart is necessary.
Click **Yes** to reset the configuration to Factory Defaults.
Click **No** to return to the Port State page without resetting the configuration.

.

Maintenance > Software > Upload

- **Software Upload**

This page facilitates an update of the firmware controlling the switch. Chick **Choose File** to the location of a software image and click **Upload**.
After the software image is uploaded, a page announces that the firmware update is initiated. After about a minute, the firmware is updated and the switch restarts.



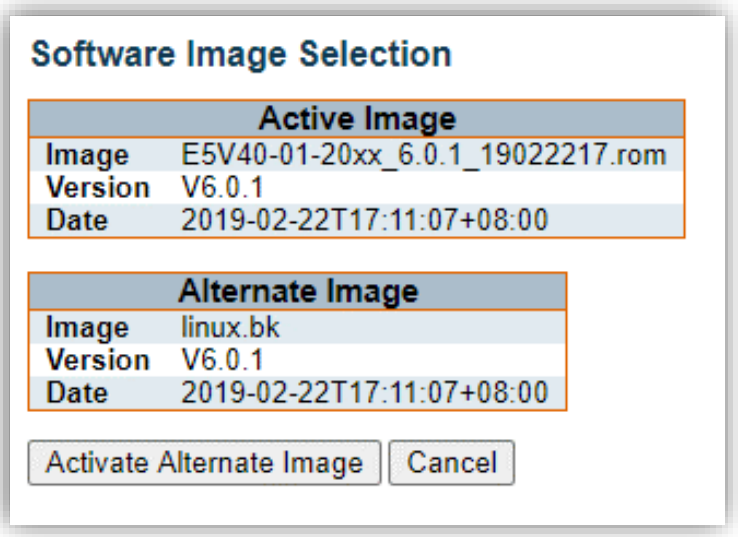
WARNING:

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.

Maintenance > Software > Image Select

- **Software Image Selection**

This page provides information about the active and alternate (backup) firmware images in the device, and allows you to revert to the alternate image.



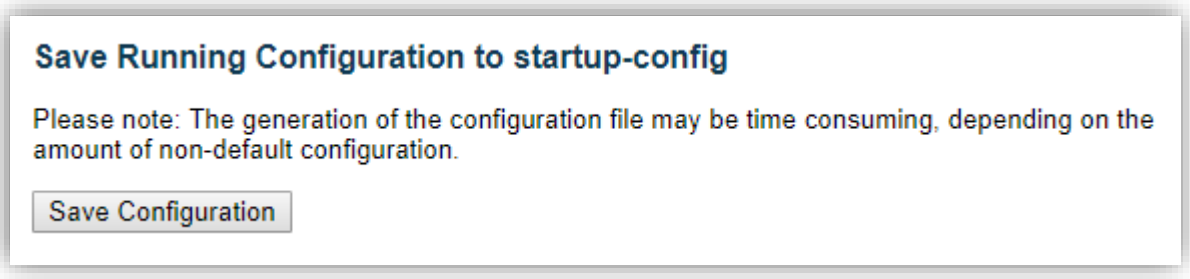
NOTE	In case the active firmware image is the alternate image, only the “Active Image” table is shown. In this case, the Activate Alternate Image button is also disabled. If the alternate image is active (due to a corruption of the primary image or by manual intervention), uploading a new firmware image 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.

Click **Activate Alternate Image** to use the alternate image. This button may be disabled depending on system state.
Click **Cancel** to activate the backup image. Navigates away from this page.

Maintenance > Configuration > Save startup-config

- **Save Running Configuration to startup-config**

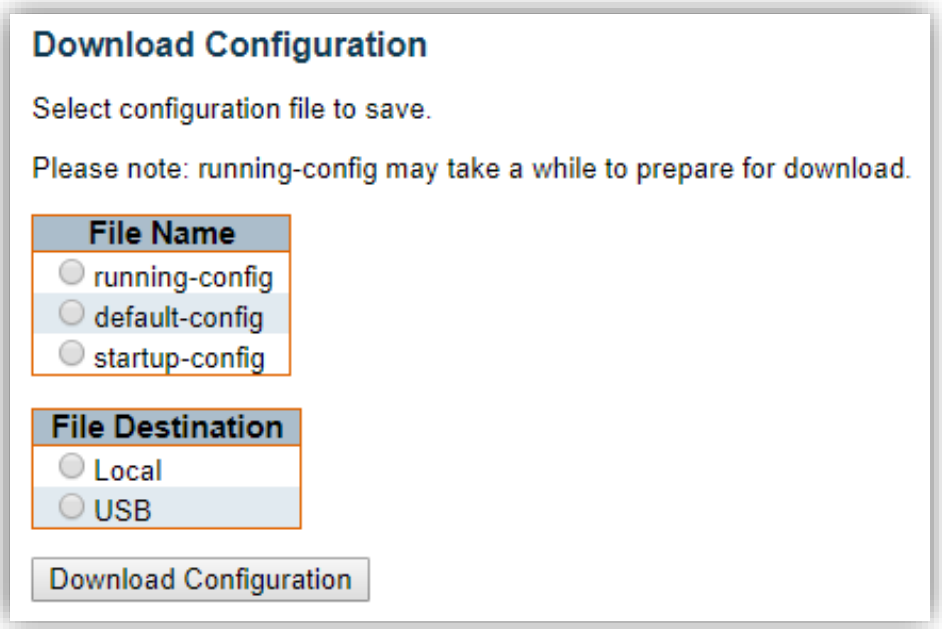
This copies running-config to startup-config, thereby ensuring that the currently active configuration will be used at the next reboot.



Maintenance > Configuration > Download

- **Download 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.

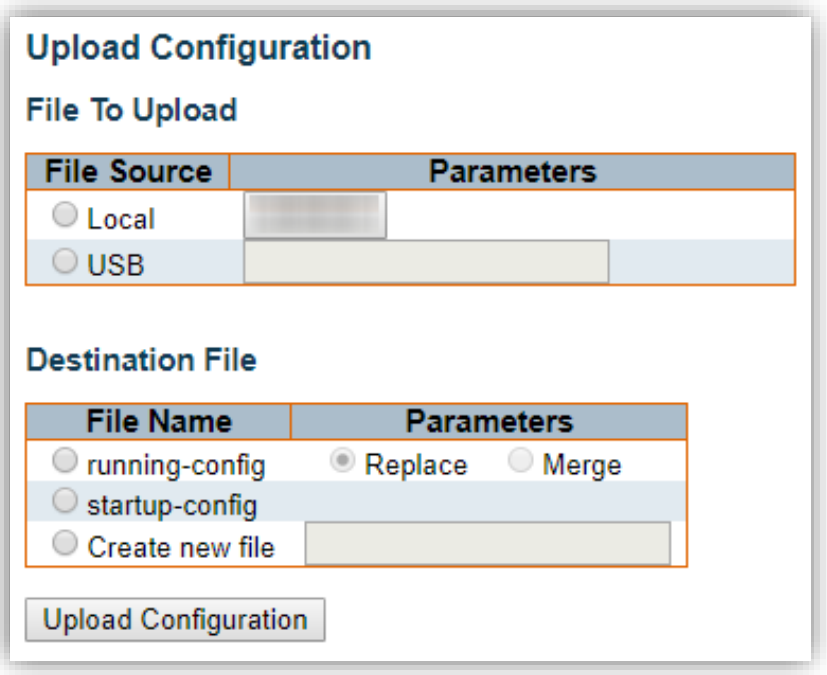


- **running-config:** A virtual file that represents the currently active configuration on the switch. This file is volatile.
- **default-config:** A read-only file with vendor-specific configuration. This file is read when the system is restored to default settings.
- **startup-config:** The startup configuration for the switch, read at boot time. If this file doesn't exist at boot time, the switch will start up in default configuration.
- Up to 31 other files, typically used for configuration backups or alternative configurations.

It is possible to download any of the files on the switch to the web browser. Select the file and click **Download Configuration**.
Download of running-config may take a little while to complete, as the file must be prepared for download.

Maintenance > Configuration > Upload

- **Upload Configuration**



It is possible to upload a file from the web browser to all the files on the switch, except default-config which is read-only.
Select the file to upload, select the destination file on the target, then click **Upload Configuration**.
If the destination is running-config, the file will be applied to the switch configuration. This can be done in two ways:

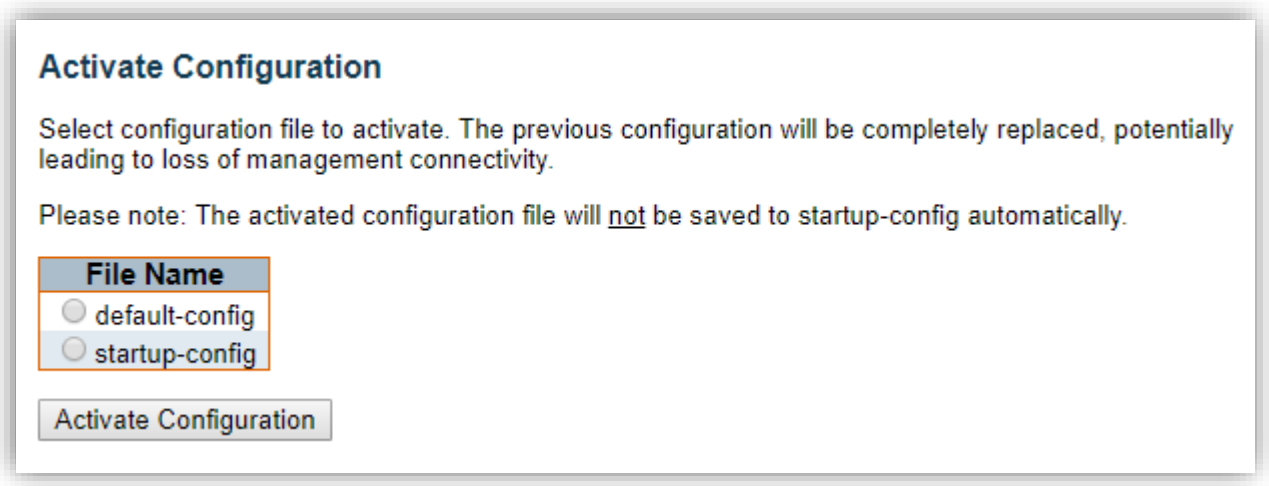
- **Replace mode:** The current configuration is fully replaced with the configuration in the uploaded file.
- **Merge mode:** The uploaded file is merged into running-config.

If the flash file system is full (i.e. contains default-config and 32 other files, usually including startup-config), it is not possible to create new files. Instead an existing file must be overwritten or another file must be deleted.

Maintenance > Configuration > Activate

- **Activate Configuration**

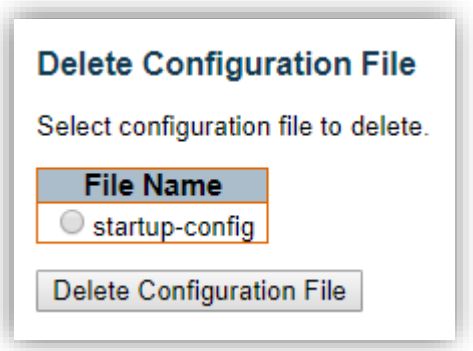
It is possible to activate any of the configuration files present on the switch, except for running-config which represents the currently active configuration.
Select the file to activate and click Activate Configuration. This will initiate the process of completely replacing the existing configuration with that of the selected file.



Maintenance > Configuration > Delete

- **Delete Configuration File**

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.



Appendix

Leonton product Industrial Ethernet Switches for critical user base on Linux. To ensure the security of the Linux open feature, Leonton set up the following general Hardening Guide to decrease attacked surface. Please note that different brands and models of Industrial Ethernet Switches may have different configuration options and security requirements, so it is advisable to consult your specific device's user manual and support documentation for detailed information.
Here are some common hardening recommendations:

- Change Default Passwords:

Ensure that you change all default usernames and passwords, including those for administrators and user accounts, to enhance access control for the devices.

- Enable Port Security:

Enable only the needed ports and disable unnecessary ports to reduce the attack surface.

- Enable 802.1X Authentication:

If your network supports it, use 802.1X authentication to control physical access to the devices.

- Enable Access Control Lists (ACLs):

Use ACLs to restrict access based on specific IP addresses or MAC addresses.

- Enable SSH or HTTPS for Remote Management:

Avoid using insecure protocols like Telnet or HTTP for device management; instead, use SSH or HTTPS to encrypt management traffic.

- Disable Unnecessary Services:

Disable unnecessary management and service features to further reduce the potential attack surface.

- Firmware Updates:

For bug fixing, it's recommended to arrange an update schedule immediately once we get a patch, to avoid cybersecurity risk.
For daily maintenance, tracing or subscription relevant thread information for Linux security issues will be suggested.

- Monitoring and Logging:

Enable logging and monitoring to detect and respond to security events promptly.

- Physical Security:

Place the switches in controlled physical environments to prevent unauthorized physical access.

- Regular Configuration Reviews:

Periodically review the configurations of the switches to ensure they align with best practices and make necessary improvements.

Please note that Industrial Ethernet Switches are typically used to control and monitor critical infrastructure, making security of utmost importance. Before making any changes or configurations, ensure you understand the specific requirements of your devices and proceed with caution to avoid disruptions to critical systems. If you need help with how to harden your switches or need more specific advice, consult the device manufacturer or security experts.