# Managed Industrial Ethernet Switch

# Web Configuration Tool Guide

**Version Number: 1.0**
**Issue: 1.0r02, Dec. 2023**

# [CONTENTS]

# 1. Introductions

## 1.1 System Description

The industrial Ethernet switch series delivers high quality, wide operating temperature range, extended power input range, IP-30 design, and advanced VLAN & QoS features. It's ideal for harsh environments and mission critical applications.
Managed QoS the switch provides enterprise-class networking features to fulfill the needs of large network infrastructure and extreme environments.
The switch eases the effort to build a network infrastructure which offers a reliable, well managed and good QoS networking for any business requiring continuous and well-protected services in management environments. With the features such as Fast Failover ring protection and QoS, customers can ensure their network is qualified to deliver any real-time and high quality applications.

## 1.2 Using the Web Interface

The object of this document "Web Configuration Tool Guide" is to address the web feature, design layout and descript how to use the web interface.

### 1.2.1 Web Browser Support

IE 7 (or newer version) with the following default settings is recommended:

| | |
|---|---|
| Language script | Latin based |
| Web page font | Times New Roman |
| Plain text font | Courier New |
| Encoding | Unicode (UTF-8) |
| Text size | Medium |

Firefox with the following default settings is recommended:

| | |
|---|---|
| Web page font | Times New Roman |
| Encoding | Unicode (UTF-8) |
| Text size | 16 |

Google Chrome with the following default settings is recommended:

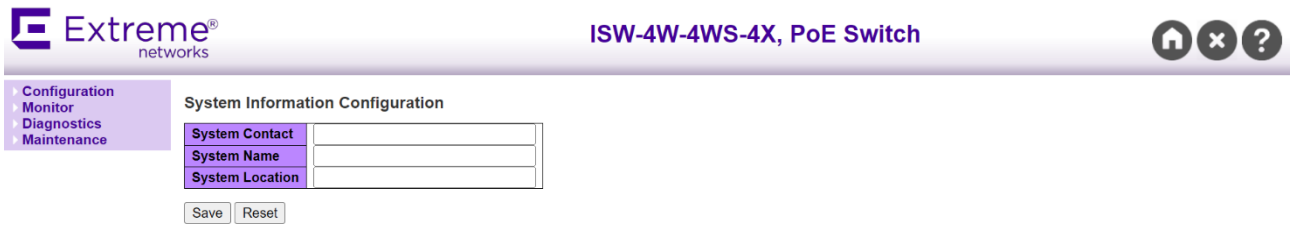
| | |
|---|---|
| Web page font | Times New Roman |
| Encoding | Unicode (UTF-8) |
| Text size | Medium |

## 1.2.2 Navigation

All main screens of the web interface can be reached by clicking on hyperlinks in the four menu boxes on the left side of the screen:

- **Configuration**
- **Monitor**
- **Diagnostics**
- **Maintenance**

## 1.2.3 Title Bar Icons




**Home Button**

User can go back to the main page using Home button. Click Home button and return to the initial page.

**Logout Button**

User can logout the system using Logout button. Click Logout button and a window appears to ask you if you want to log out the web site. Click “Yes” to leave the web site or “No” to stay in the web site.

**Help Button** 

For more information about any screen, click on the Help button on the screen.
Help information is displayed in the same window.

### 1.2.4 Ending a Session

To end a session, close your web browser. This prevents an unauthorized user from accessing the system using your user name and password.

## 1.3 Using the Online Help

Each screen has a Help button  that invokes a page of information relevant to the particular screen. The Help is displayed in a new window.
Each web page of Configuration/Status/System functions has a corresponding help page.

# 2. Using the Web

## 2.1 Login

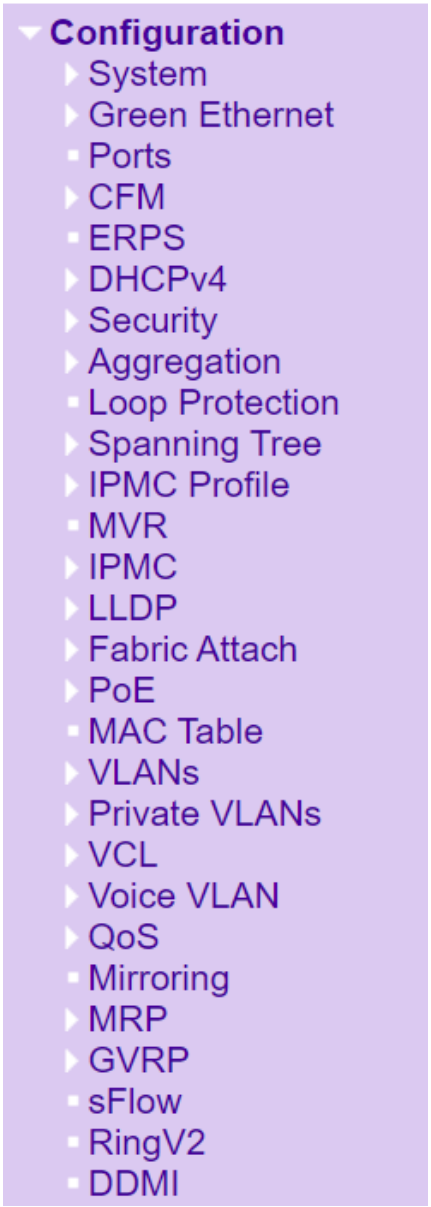
| | |
|---|---|
| **Operation** | 1. Fill out Username and Password<br>2. Click “Sign in” |
| **Field** | Description |
| **Username** | Login user name. The maximum length is 32.<br>Default: admin |
| **Password** | Login user password. The maximum length is 32.<br>Default: none |

## 2.2 Tree View

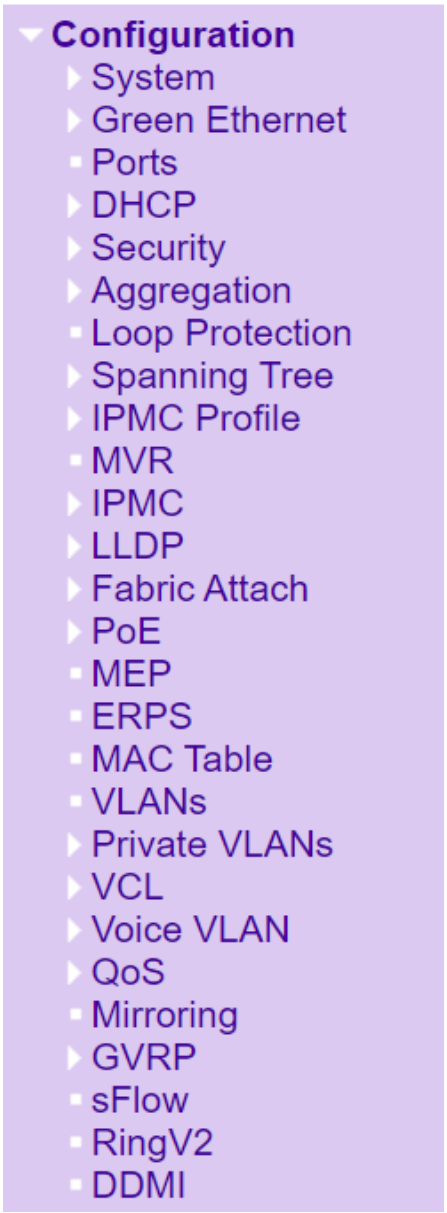
The tree view is a menu of the web. It offers user quickly to get the page for expected data or configuration.

### 2.2.1 Configuration Menu

90W PoE Model

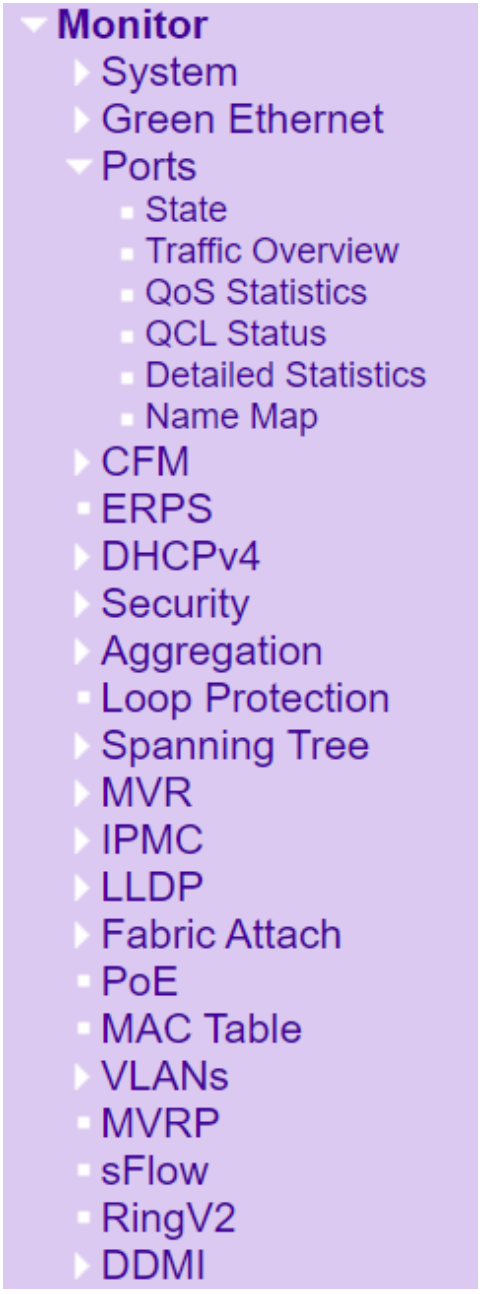



30W PoE Model



## 2.2.2 Monitor Menu

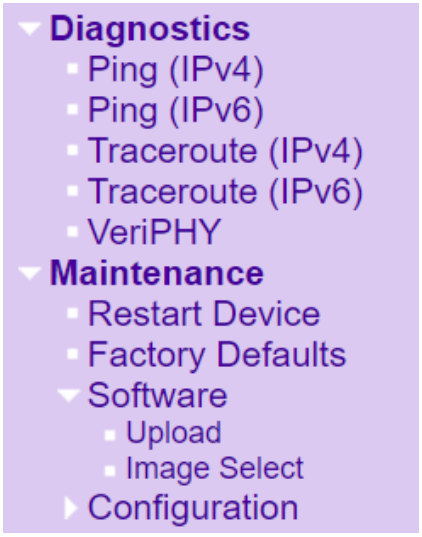
90W PoE Model



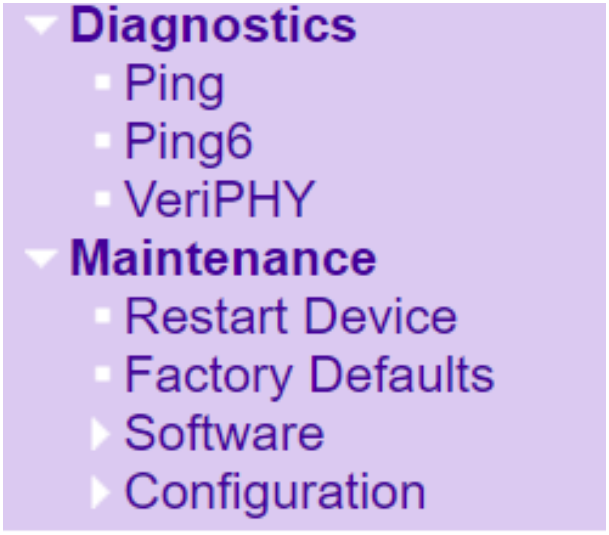

30W PoE Model

### 2.2.3 Diagnostics/Maintenance Menu

90W PoE Model




30W PoE Model

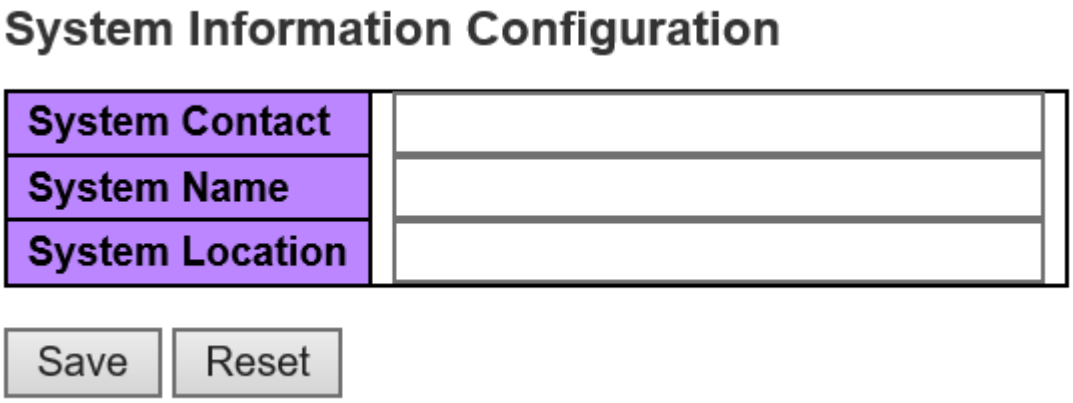


## 2.3 Configuration

### 2.3.1 System

### 2.3.2 System Information

The switch system information is provided here.




| Object | Description |
|---|---|
| **System Contact** | The textual identification of the contact person for this managed node, together with information on how to contact this person. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126. |
| **System Name** | An administratively assigned name for this managed node. By convention, this is the node's fully-qualified domain name. A domain name is a text string drawn from the alphabet (A-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. |
| **System Location** | 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. |

| Buttons | |
|---|---|
| Save | Click to save changes. |

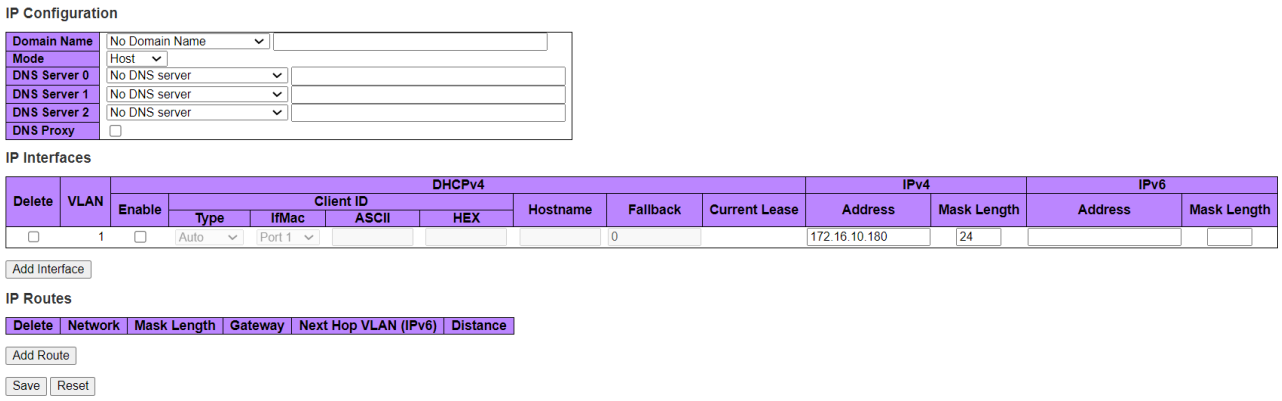
| | |
|---|---|
| Reset | Click to revert to previously saved values. |

## 2.3.3 System IP

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.

90W PoE Model




| Object | Description |
|---|---|
| **IP Configuration** | |
| **Domain Name** | The name string of local domain where the device belongs.<br>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.<br>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'.<br>The following modes are supported:<br>˙No Domain Name<br>No domain name will be used.<br><br>˙Configured Domain Name<br>Explicitly specify the name of local domain.<br>Make sure the configured domain name meets your organization's given domain. |
| **Mode** | Configure whether the IP stack should act as a Host or a Router. In Host mode, IP traffic between interfaces will not be routed. In Router mode traffic is routed |

| | |
|---|---|
| | between all interfaces. |
| **DNS Server** | This setting controls the DNS name resolution done by the switch.<br>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.<br>The following modes are supported:• No DNS server<br>No DNS server will be used<br>• Configured IPv4<br>Explicitly provide the valid IPv4 unicast address of the DNS Server in dotted decimal notation.<br>Make sure the configured DNS server could be reachable (e.g. via PING) for activating DNS service.<br>• Configured IPv6<br>Explicitly provide the valid IPv6 unicast (except linklocal) address of the DNS Server.<br>Make sure the configured DNS server could be reachable (e.g. via PING6) for activating DNS service.<br>• From any DHCPv4 interfaces<br>The first DNS server offered from a DHCPv4 lease to a DHCPv4-enabled interface will be used.<br>• From this DHCPv4 interface<br>Specify from which DHCPv4-enabled interface a provided DNS server should be preferred. |
| **DNS Proxy** | When DNS proxy is enabled, system will relay DNS requests to the currently configured DNS server, and reply as a DNS resolver to the client devices on the network.<br>Only IPv4 DNS proxy is now supported. |
| **IP Interfaces** | |
| **Delete** | Select this option to delete an existing IP interface. |
| **VLAN** | The VLAN associated with the IP interface. Only ports in this VLAN will be able to access the IP interface. This field is only available for input when creating a new interface. Valid VLAN ID range from 1 to 4095. |
| **IPv4 DHCP Enabled** | Enable the DHCPv4 client by checking this box. If this option is enabled, the system will configure the IPv4 address and mask of the interface using the DHCPv4 protocol. |
| **IPv4 DHCP Client Identifier Type** | This specified which of the three types below, i.e. IfMac, ASCII or HEX, shall be used for the Client Identifier. See RFC-2132 section 9.14. |
| **IPv4 DHCP Client Identifier** | The interface name of DHCP client identifier. When DHCPv4 client is enabled and |

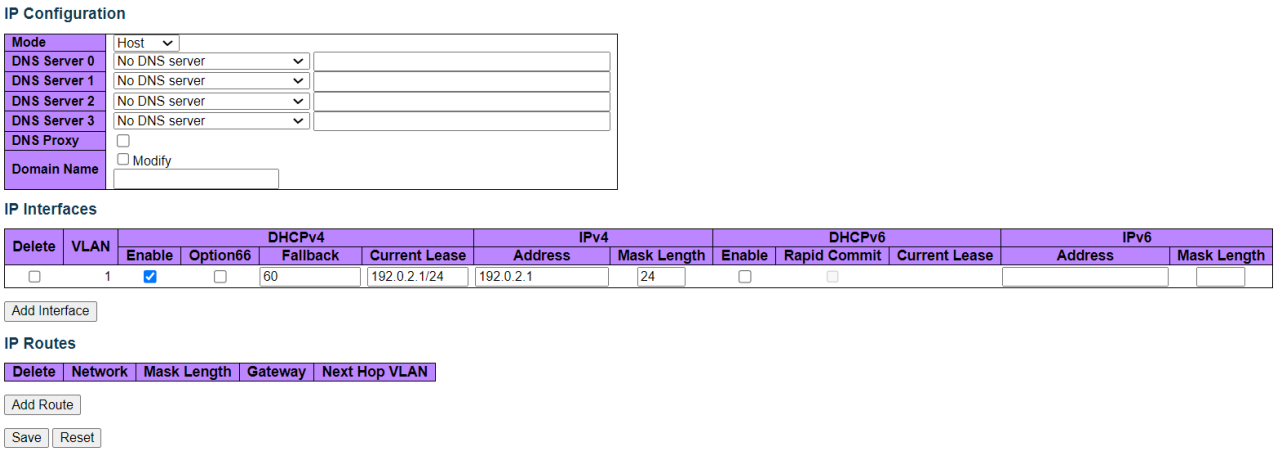
| | |
|---|---|
| **IfMac** | the client identifier type is 'ifmac', the configured interface's hardware MAC address will be used in the DHCP option 61 field. |
| **IPv4 DHCP Client Identifier ASCII** | The ASCII string of DHCP client identifier. When DHCPv4 client is enabled and the client identifier 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 shows the current interface address, as provided by the DHCP server. |
| **IPv4 Address** | The IPv4 address of the interface in dotted decimal notation.<br>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.<br>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. |
| **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.<br>System accepts the valid IPv6 unicast address only, except IPv4-Compatible address and IPv4-Mapped address.<br>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.<br>The field may be left blank if IPv6 operation on the interface is not desired. |

| | |
|---|---|
| **Resolving IPv6 DAD** | The link-local address is formed from an interface identifier based on the hardware address which is supposed to be uniquely assigned. Once the DAD (Duplicate Address Detection) detects the address duplication, the operation on the interface SHOULD be disabled.<br>At this moment, manual intervention is required to resolve the address duplication. For example, check whether the loop occurs in the VLAN or there is indeed other device occupying the same hardware address as the device in the VLAN.<br>After making sure the specific link-local address is unique on the IPv6 link in use, delete and then add the specific IPv6 interface to restart the IPv6 operations on this interface. |
| **IP Routes** | |
| **Delete** | Select this option to delete an existing IP route. |
| **Network** | The destination IP network or host address of this route. Valid format is dotted decimal notation or 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. |
| **Next Hop VLAN(Only for IPv6)** | The VLAN ID (VID) of the specific IPv6 interface associated with the gateway.<br>The given VID ranges from 1 to 4094 and will be effective only when the corresponding IPv6 interface is valid.<br>If the IPv6 gateway address is link-local, it must specify the next hop VLAN for the gateway.<br>If the IPv6 gateway address is not link-local, system ignores the next hop VLAN for the gateway. |
| **Distance** | The distance value of the route entry is used to provide the priority information of the routing protocols to routers. When two or more different routing protocols are involved and have the same destination, the distance value can be used to select the best path. |

| **Buttons** | |
|---|---|
| Add Interface | Click to add a new IP interface. A maximum of 128 interfaces is supported. |

| | |
|---|---|
| Add Route | Click to add a new IP route. A maximum of 128 routes is supported. |
| Save | Click to save changes. |
| Reset | Click to revert to previously saved values. |

## 30W PoE Model




| Object | Description |
|---|---|
| **IP Configuration** | |
| **Mode** | Configure whether the IP stack should act as a Host or a Router. In Host mode, IP traffic between interfaces will not be routed. In Router mode traffic is routed between all interfaces. |
| **DNS Server** | This setting controls the DNS name resolution done by the switch.<br>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.<br>System selects the active DNS server from configuration in turn, if the preferred server does not respond in five attempts.<br>The following modes are supported:<br>•From any DHCPv4 interfaces<br>The first DNS server offered from a DHCPv4 lease to a DHCPv4-enabled interface will be used.<br>•No DNS server<br>No DNS server will be used.<br>•Configured IPv4<br>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.<br>•From this DHCPv4 interface<br>Specify from which DHCPv4-enabled interface a provided DNS server should be preferred.<br>•Configured IPv6<br>Explicitly provide the valid IPv6 unicast (except linklocal) address of the DNS Server.<br>Make sure the configured DNS server could be reachable (e.g. via PING6) for activating DNS service.<br>•From this DHCPv6 interface<br>Specify from which DHCPv6-enabled interface a provided DNS server should be preferred.<br>•From any DHCPv6 interfaces<br>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.<br>Only IPv4 DNS proxy is now supported. |
| **Domain Name** | The name string of local domain where the device belongs.<br>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.<br>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'.<br>The following modes are supported:<br>˙No Domain Name<br>No domain name will be used.<br><br>˙Configured Domain Name<br>Explicitly specify the name of local domain.<br>Make sure the configured domain name meets your organization's given domain. |
| **IP Interfaces** | |
| **Option66** | The option is used to control whether automatically upgrade by DHCP options.<br>•Enabled<br>It means that system will get boot file from TFTP and upgrade firmware |

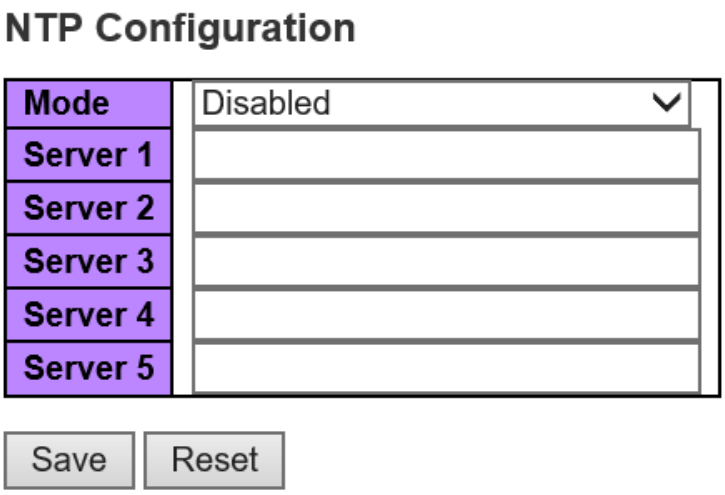
| | |
|---|---|
| | automatically. Note: If the device cannot get expected files that follow correct naming rule, system SHOULD NOT upgrade firmware. Also the running-config.<br>•Disabled<br>It means system SHOULD NOT upgrade firmware/running-config, in any case. |
| **Delete** | Select this option to 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. Valid VLAN ID range from 1 to 4095. |
| **IPv4 DHCP Enabled** | Enable the DHCPv4 client by checking this box. If this option is enabled, the system will configure the IPv4 address and mask of the interface using the DHCPv4 protocol. |
| **IPv4 DHCP 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 shows the current interface address, as provided by the DHCP server. |
| **IPv4 Address** | The IPv4 address of the interface in dotted decimal notation.<br>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.<br>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.<br>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.<br>System accepts the valid IPv6 unicast address only, except IPv4-Compatible address and IPv4-Mapped address.<br>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.<br>The field may be left blank if IPv6 operation on the interface is not desired. |
| **Resolving IPv6 DAD** | The link-local address is formed from an interface identifier based on the hardware address which is supposed to be uniquely assigned. Once the DAD (Duplicate Address Detection) detects the address duplication, the operation on the interface SHOULD be disabled.<br>At this moment, manual intervention is required to resolve the address duplication. For example, check whether the loop occurs in the VLAN or there is indeed other device occupying the same hardware address as the device in the VLAN.<br>After making sure the specific link-local address is unique on the IPv6 link in use, delete and then add the specific IPv6 interface to restart the IPv6 operations on this interface. |
| **IP Routes** | |
| **Delete** | Select this option to delete an existing IP route. |
| **Network** | The destination IP network or host address of this route. Valid format is dotted decimal notation or 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. |
| **Next Hop VLAN(Only for IPv6)** | The VLAN ID (VID) of the specific IPv6 interface associated with the gateway.<br>The given VID ranges from 1 to 4094 and will be effective only when the corresponding IPv6 interface is valid.<br>If the IPv6 gateway address is link-local, it must specify the next hop VLAN for the gateway.<br>If the IPv6 gateway address is not link-local, system ignores the next hop VLAN for the gateway. |

| Buttons | |
|---|---|
| Add Interface | Click to add a new IP interface. A maximum of 128 interfaces is supported. |
| Add Route | Click to add a new IP route. A maximum of 128 routes is supported. |
| Save | Click to save changes. |
| Reset | Click to revert to previously saved values. |

## 2.3.4 System NTP

Configure NTP on this page.




| Object | Description |
|---|---|
| **Mode** | Indicates the NTP mode operation. Possible modes are:<br>Enabled: Enable NTP client mode operation.<br>Disabled: Disable NTP client mode operation. |
| **Server #** | Provide the IPv4 or IPv6 address of a NTP server. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of |

| | |
|---|---|
| | contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'. In addition, it can also accept a domain name address. |

| Buttons | |
|---|---|
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

## 2.3.5 System Time

This page allows you to configure the Time Zone

### Time Zone Configuration

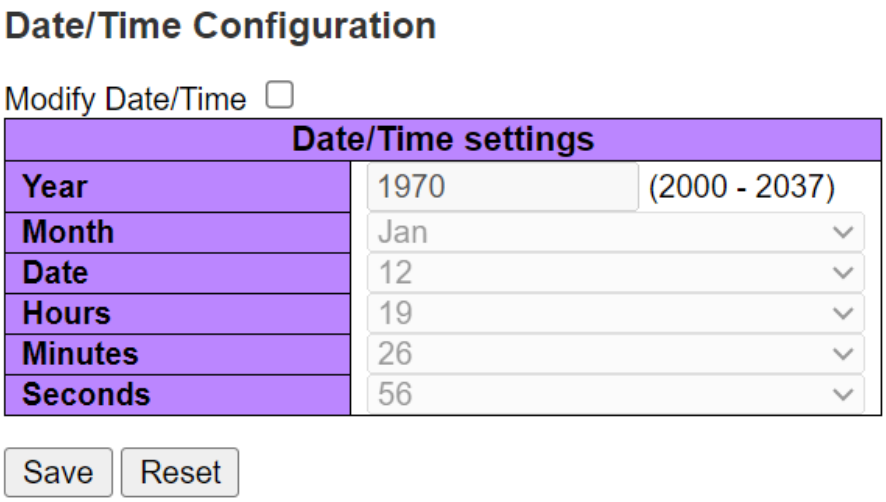
| Time Zone Configuration | | |
|---|---|---|
| Time Zone | (UTC) Coordinated Universal Time | |
| Hours | 0 | |
| Minutes | 0 | |
| Acronym | | ( 0 - 16 characters ) |

### Daylight Saving Time Configuration

| Daylight Saving Time Mode | |
|---|---|
| Daylight Saving Time | Disabled |

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

Save Reset




| Object | Description |
|---|---|
| **Time Zone Configuration** | |
| **Time Zone** | Lists various Time Zones worldwide. Select appropriate Time Zone from the drop down and click Save to set. The 'Manual Setting' options is used for the specific time zone which is excluded from the options list. |
| **Hours (For 90W Model)** | Number of hours offset from UTC. The field only available when time zone manual setting. |
| **Minutes (For 90W Model)** | Number of minutes offset from UTC. The field only available when time zone manual setting. |
| **Acronym** | User can set the acronym of the time zone. This is a User configurable acronym to identify the time zone. ( Range : Up to 16 characters ) Notice the string '' is a special syntax that is reserved for null input. |
| **Daylight Saving Time Configuration** | |
| **Daylight Saving Time** | This is used to set the clock forward or backward according to the configurations set below for a defined Daylight Saving Time duration. Select 'Disable' to disable the Daylight Saving Time configuration. Select 'Recurring' and configure the Daylight Saving Time duration to repeat the configuration every year. Select 'Non-Recurring' and configure the Daylight Saving Time duration for single time configuration. ( Default : Disabled ) |
| **Recurring Configurations** | |
| **Start time settings** | |
| **Week** | Select the starting week number. |
| **Day** | Select the starting day. |
| **Month** | Select the starting month. |

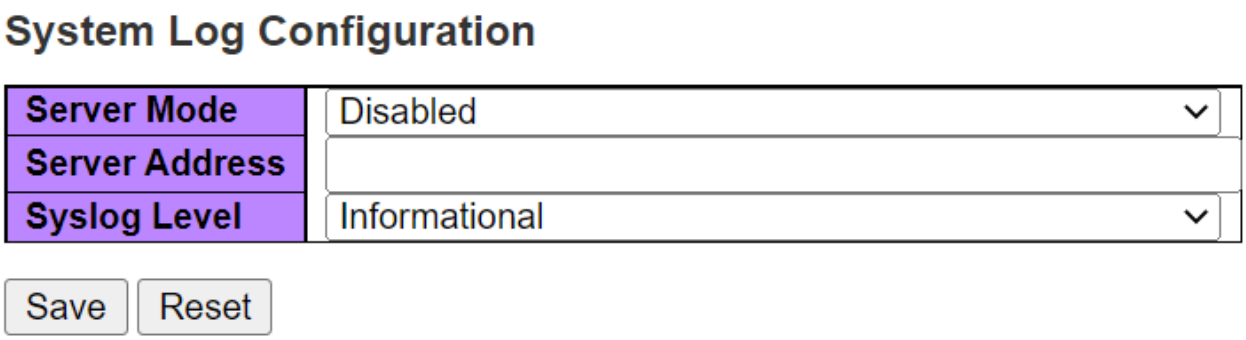
| | |
|---|---|
| **Hours** | Select the starting hour. |
| **Minutes** | Select the starting minute |
| **End time settings** | |
| **Week** | Select the ending week number. |
| **Day** | Select the ending day. |
| **Month** | Select the ending month. |
| **Hours** | Select the ending hour. |
| **Minutes** | Select the ending minute |
| **Offset settings** | |
| **Offset** | Enter the number of minutes to add during Daylight Saving Time. ( Range: 1 to 1440 ) |
| **Non Recurring Configurations** | |
| **Start time settings** | |
| **Month** | Select the starting month. |
| **Date** | Select the starting date. |
| **Year** | Select the starting year. |
| **Hours** | Select the starting hour. |
| **Minutes** | Select the starting minute |
| **End time settings** | |
| **Month** | Select the ending month. |
| **Date** | Select the ending date. |
| **Year** | Select the ending year. |
| **Hours** | Select the ending hour. |
| **Minutes** | Select the ending minute |
| **Offset settings** | |
| **Offset** | Enter the number of minutes to add during Daylight Saving Time. ( Range: 1 to 1440 ) |
| **Date/Time Configuration** | |
| **Year** | Year of current datetime. ( Range: 2000 to 2037 ) |
| **Month** | Month of current datetime. |
| **Date** | Date of current datetime. |
| **Hours** | Hour of current datetime. |
| **Minutes** | Minute of current datetime. |
| **Seconds** | Second of current datetime. |

| **Buttons** |
|---|

| | |
|---|---|
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

## 2.3.6 System Log

Configure System Log on this page.



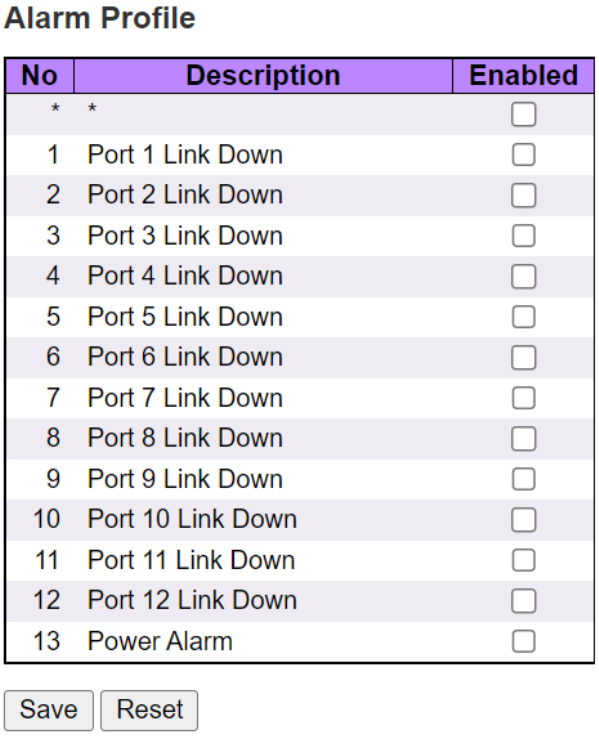

| Object | Description |
|---|---|
| **Server Mode** | Indicates the server mode operation. When the mode operation is enabled, the syslog message will send out to syslog server. The syslog protocol is based on UDP communication and received on UDP port 514 and the syslog server will not send acknowledgments 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. Possible modes are:<br>`Enabled`: Enable server mode operation.<br>`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 host name. |
| **Syslog Level** | Indicates what kind of message will send to syslog server. Possible modes are:<br>Error: Send the specific messages which severity code is less or equal than Error(3).<br>Warning: Send the specific messages which severity code is less or equal than Warning(4).<br>Notice: Send the specific messages which severity code is less or equal than Notice(5).<br>Informational: Send the specific messages which severity code is less or equal than Informational(6). |

| Buttons | |
|---|---|
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

## 2.3.7 System Alarm Profile

Alarm Profile is provided here to enable/disable alarm.

90W PoE Model




| Object | Description |
|---|---|
| **No** | The identification of the Alarm Profile entry. |
| **Description** | Alarm Type Description. |
| **Enabled** | If alarm entry is Enabled, then alarm will be shown in alarm history/current when it occurs.<br>Alarm LED will be on (lighted), Alarm Relay also be enabled.<br>SNMP trap will be sent if any SNMP trap entry exists and enabled. |
| **Disabled** | If alarm entry is Disabled, then alarm will not be captured/shown in alarm |

| | |
|---|---|
| | history/current when alarm occurs;<br>then it will not trigger the Alarm LED change, Alarm Relay and SNMP trap either. |
| Note: When any alarm exists, the Alarm LED will be on (lighted), Alarm Output Relay will also be enabled. | |

| Buttons | |
|---|---|
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

30W PoE Model

**System Temperature Threshold Config**

| | | |
|---|---|---|
| **High Temp. Threshold for Alarm Set** | 90 | ( 70-100°C ) |
| **High Temp. Threshold for Alarm Clear** | 80 | ( 55-85°C ) |
| **Low Temp. Threshold for Alarm Set** | 10 | ( 5-15°C ) |
| **Low Temp. Threshold for Alarm Clear** | 15 | ( 10-30°C ) |

**Alarm Profile**

| ID | Description | Enabled |
|---|---|---|
| * | * | ☐ |
| 1 | Port 1 Link Down | ☐ |
| 2 | Port 2 Link Down | ☐ |
| 3 | Port 3 Link Down | ☐ |
| 4 | Port 4 Link Down | ☐ |
| 5 | Port 5 Link Down | ☐ |
| 6 | Port 6 Link Down | ☐ |
| 7 | Port 7 Link Down | ☐ |
| 8 | Port 8 Link Down | ☐ |
| 9 | Power Alarm | ☐ |
| 10 | High Temperature Alarm | ☐ |
| 11 | Low Temperature Alarm | ☐ |

Save Reset

| Object | Description |
|---|---|
| **System Temperature Threshold Config** | |
| **High Temperature Threshold for Alarm Set** | High Temperature Alarm will be generated when system temperature exceeds this value. |
| **High Temperature Threshold for Alarm** | High Temperature Alarm will be eliminated when system temperature lower than this value. |

| | |
|---|---|
| **Clear** | |
| **Low Temperature Threshold for Alarm Set** | Low Temperature Alarm will be generated when system temperature less than this value. |
| **Low Temperature Threshold for Alarm Clear** | Low Temperature Alarm will be eliminated when system temperature exceeds this value. |
| **Alarm Profile** | |
| **ID** | The identification of the Alarm Profile entry. |
| **Description** | Alarm Type Description. |
| **Enabled** | If alarm entry is Enabled, then alarm will be shown in alarm history/current when it occurs.<br>Alarm LED will be on (lighted), Alarm Relay also be enabled.<br>SNMP trap will be sent if any SNMP trap entry exists and enabled. |
| **Disabled** | If alarm entry is Disabled, then alarm will not be captured/shown in alarm history/current when alarm occurs;<br>then it will not trigger the Alarm LED change, Alarm Relay and SNMP trap either. |
| Note: When any alarm exists, the Alarm LED will be on (lighted), Alarm Output Relay will also be enabled. | |

| **Buttons** | |
|---|---|
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

### 2.3.8 Green Ethernet

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.

## Port Power Savings Configuration

**Optimize EEE for** Latency

### Port Configuration

| | | | | EEE Urgent Queues | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **Port** | **ActiPHY** | **PerfectReach** | **EEE** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** |
| * | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 1 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 2 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 3 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 4 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 5 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 6 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 7 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 8 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 9 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 10 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 11 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 12 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |

Save Reset

| Object | Description |
|---|---|
| **Optimize EEE for** | The switch can be set to optimize EEE for either best power saving or least traffic latency. |
| **Port** | The switch port number of the logical port. |
| **ActiPHY** | Link down power savings enabled.<br>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.<br>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.<br>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.<br>If desired it is possible to minimize the latency for specific frames, by mapping the frames to a specific queue (done with QOS), and then mark the queue as an urgent queue. When an urgent queue gets data to be transmitted, the circuits will be |

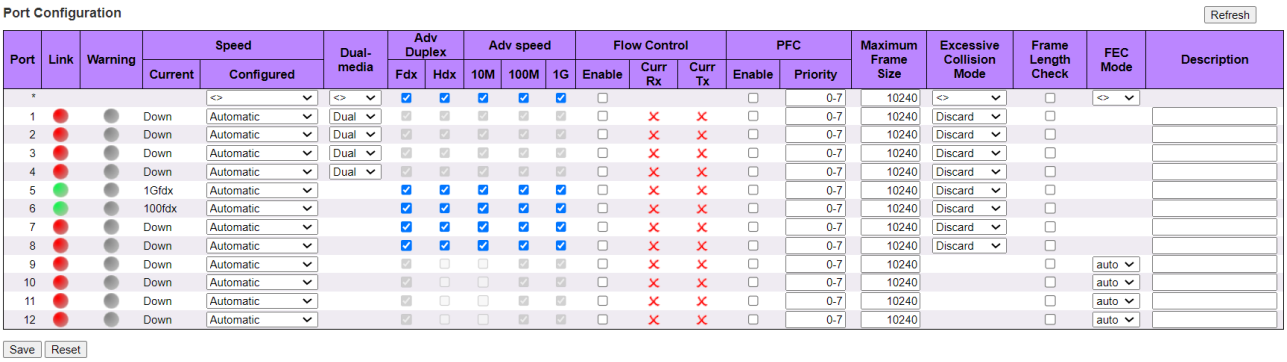
| | |
|---|---|
| | powered up at once and the latency will be reduced to the wakeup time. |
| **EEE Urgent Queues** | Queues set will activate transmission of frames as soon as data is available. Otherwise the queue will postpone transmission until a burst of frames can be transmitted. |

| **Buttons** | |
|---|---|
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

## 2.3.9 Port

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

### 90W PoE Model



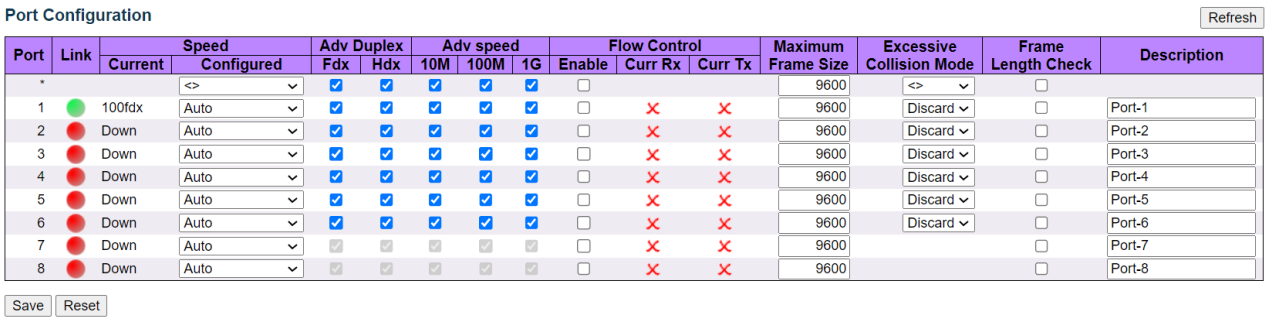

| Object | Description |
|---|---|
| **Port** | This is the logical port number for this row. |
| **Link** | The current link state is displayed graphically. Green indicates the link is up and red that it is down. |
| **Warning** | Operational warnings of the port.<br>': No warnings<br>: There are warnings, use tooltip to see. |
| **Current Link Speed** | Provides the current link speed of the port. |
| **Configured Link Speed** | Selects any available link speed for the given switch port. Only speeds supported by the specific port is shown. Possible speeds are:<br>Disabled - Disables the switch port operation.<br>Automatic - Port auto negotiating speed and duplex with the link partner and selects the highest speed that is compatible with the link partner.<br>10Mbps HDX - Forces the port in 10Mbps half duplex mode.<br>10Mbps FDX - Forces the port in 10Mbps full duplex mode.<br>100Mbps HDX - Forces the port in 100Mbps half duplex mode.<br>100Mbps FDX - Forces the port in 100Mbps full duplex mode.<br>1Gbps FDX - Forces the port in 1Gbps full duplex<br>2.5Gbps FDX - Forces the port in 2.5Gbps full duplex mode.<br>10Gbps FDX - Forces the port in 10Gbps full duplex mode. |
| **Dual-media** | If a port is Dual-media, this field selects which of the ports to use. If Auto is selected, |

| | |
|---|---|
| | both ports can be used, and if both ports has link, the SFP port will be preferred. |
| **Advertise Duplex** | When duplex is set as auto i.e auto negotiation, the port will only advertise the specified duplex as either Fdx or Hdx to the link partner. By default port will advertise all the supported duplexes if the Duplex is Auto. |
| **Advertise Speed** | When Speed is set as auto i.e auto negotiation, the port will only advertise the specified speeds (10M 100M 1G 2.5G 5G 10G) to the link partner. By default port will advertise all the supported speeds if speed is set as Auto. |
| **Flow Control** | When Auto Speed is selected on a port, this section indicates the flow control capability that is advertised to the link partner.<br>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.<br>Check the configured column to use flow control. This setting is related to the setting for Configured Link Speed.<br>NOTICE: The 100FX standard does not support Auto Negotiation, so when in 100FX mode the flow control capabilities will always be shown as "disabled". |
| **PFC** | When PFC (802.1Qbb Priority Flow Control) is enabled on a port then flow control on a priority level is enabled. Through the Priority field, range (one or more) of priorities can be configured, e.g. '0-3,7' which equals '0,1,2,3,7'. PFC is not supported through auto negotiation. PFC and Flowcontrol cannot both be enabled on the same port. |
| **Maximum Frame Size** | Enter the maximum frame size allowed for the switch port, including FCS. The range is 1518-10240 bytes. |
| **Excessive Collision Mode** | Configure port transmit collision behavior.<br>**Discard**: Discard frame after 16 collisions (default).<br>**Restart**: Restart backoff algorithm after 16 collisions. |
| **Frame Length Check** | Configures if frames with incorrect frame length in the EtherType/Length field shall be dropped. An Ethernet frame contains a field EtherType which can be used to indicate the frame payload size (in bytes) for values of 1535 and below. If the EtherType/Length field is above 1535, it indicates that the field is used as an EtherType (indicating which protocol is encapsulated in the payload of the frame). If "frame length check" is enabled, frames with payload size less than 1536 bytes are dropped, if the EtherType/Length field does not match the actually payload length. If "frame length check" is disabled, frames are not dropped due to frame length mismatch. Note: No drop counters count frames dropped due to frame length mismatch |
| **FEC** | FEC is short for Forward Error Correction. It is a technique for controlling errors over an unreliable link. The idea is that the sender adds some extra bits to the frame that |

| | |
|---|---|
| | allows a receiver to correct bit errors in the received frame.<br>R-FEC (IEEE802.3 clause 74 - sometimes called Firecode). This is meant for 10G. The parameter affects both what is requested during clause 73 aneg and what the port is configured to use if not running clause 73 aneg. If running clause 73 aneg on 10G ports we always tell the link partner that we support R-FEC. What the end user can control with the fec command is whether we request R-FEC. If either us or the link partner requests R-FEC, the port will end up using R-FEC.<br><br>auto: This is the default and means the following:<br>If a 10G port runs clause 73, R-FEC will be requested.<br>Otherwise, no FEC will be enabled.<br>r-fec: If a 10G port runs clause 73, only R-FEC will be requested. If a 10G port does not run clause 73, but is loaded with at least a 10G SFP and the speed is at least 5G, only R-FEC will be enabled. Otherwise, no FEC will be enabled.<br>none: If the port is running clause 73, R-FEC will not be requested (but remember that this does not mean that the clause 73 aneg will not result in the port running FEC). Otherwise, the port will not run any FEC. |

| Buttons | |
|---|---|
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |
| Refresh | Click to refresh the page. Any changes made locally will be undone. |

## 30W PoE Model




| Object | Description |
|---|---|
| **Port** | This is the logical port number for this row. |

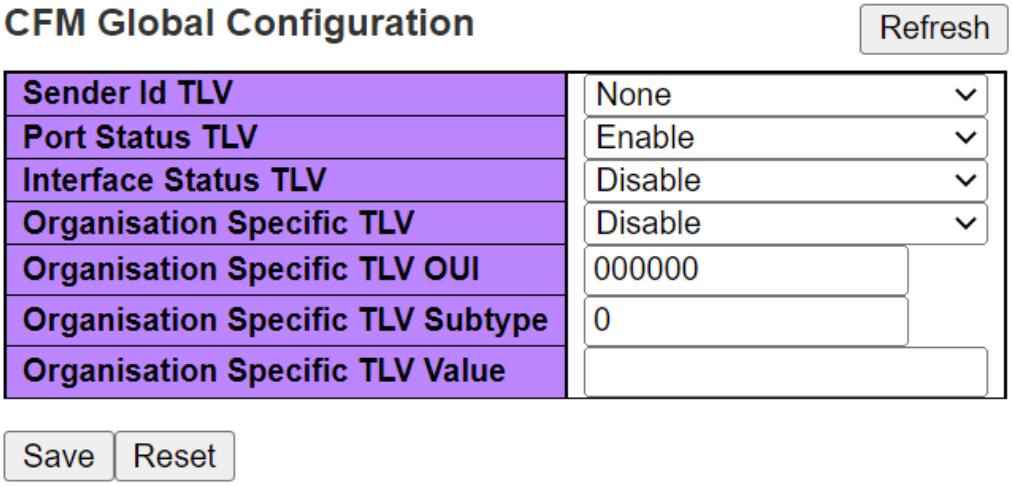
| | |
|---|---|
| **Link** | The current link state is displayed graphically. Green indicates the link is up and red that it is down. |
| **Current Link Speed** | Provides the current link speed of the port. |
| **Configured Link Speed** | Selects any available link speed for the given switch port. Only speeds supported by the specific port is shown. Possible speeds are:<br>Disabled - Disables the switch port operation.<br>Auto - Port auto negotiating speed with the link partner and selects the highest speed that is compatible with the link partner.<br>10Mbps HDX - Forces the cu port in 10Mbps half duplex mode.<br>10Mbps FDX - Forces the cu port in 10Mbps full duplex mode.<br>100Mbps HDX - Forces the cu port in 100Mbps half duplex mode.<br>100Mbps FDX - Forces the cu port in 100Mbps full duplex mode.<br>1Gbps FDX - Forces the port in 1Gbps full duplex<br><br>SFP_Auto_AMS - 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. The port is set in AMS mode. Cu port is set in Auto mode.<br>100-FX - SFP port in 100-FX speed. Cu port disabled.<br>1000-X - SFP port in 1000-X speed. Cu port disabled.<br>Ports in AMS mode with 1000-X speed has Cu port preferred.<br>Ports in AMS mode with 1000-X speed has fiber port preferred.<br>Ports in AMS mode with 100-FX speed has fiber port preferred. |
| **Advertise Duplex** | When duplex is set as auto i.e auto negotiation, the port will only advertise the specified duplex as either Fdx or Hdx to the link partner. By default port will advertise all the supported duplexes if the Duplex is Auto. |
| **Advertise Speed** | When Speed is set as auto i.e auto negotiation, the port will only advertise the specified speeds (10M 100M 1G 2.5G 5G 10G) to the link partner. By default port will advertise all the supported speeds if speed is set as Auto. |
| **Flow Control** | When Auto Speed is selected on a port, this section indicates the flow control capability that is advertised to the link partner.<br>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.<br>Check the configured column to use flow control. This setting is related to the setting for Configured Link Speed.<br>NOTICE: The 100FX standard does not support Auto Negotiation, so when in 100FX |

| | |
|---|---|
| | mode the flow control capabilities will always be shown as "disabled". |
| **PFC** | When PFC (802.1Qbb Priority Flow Control) is enabled on a port then flow control on a priority level is enabled. Through the Priority field, range (one or more) of priorities can be configured, e.g. '0-3,7' which equals '0,1,2,3,7'. PFC is not supported through auto negotiation. PFC and Flowcontrol cannot both be enabled on the same port. |
| **Maximum Frame Size** | Enter the maximum frame size allowed for the switch port, including FCS. The range is 1518-9600 bytes. |
| **Excessive Collision Mode** | Configure port transmit collision behavior.<br>**Discard**: Discard frame after 16 collisions (default).<br>**Restart**: Restart backoff algorithm after 16 collisions. |
| **Frame Length Check** | Configures if frames with incorrect frame length in the EtherType/Length field shall be dropped. An Ethernet frame contains a field EtherType which can be used to indicate the frame payload size (in bytes) for values of 1535 and below. If the EtherType/Length field is above 1535, it indicates that the field is used as an EtherType (indicating which protocol is encapsulated in the payload of the frame). If "frame length check" is enabled, frames with payload size less than 1536 bytes are dropped, if the EtherType/Length field does not match the actually payload length. If "frame length check" is disabled, frames are not dropped due to frame length mismatch. Note: No drop counters count frames dropped due to frame length mismatch |
| **Description** | Port Description, max length 255 characters. |

| **Buttons** | |
|---|---|
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |
| Refresh | Click to refresh the page. Any changes made locally will be undone. |

## 2.3.10 CFM – Global (For 90W PoE Model)

Configure CFM Global parameters on this page.



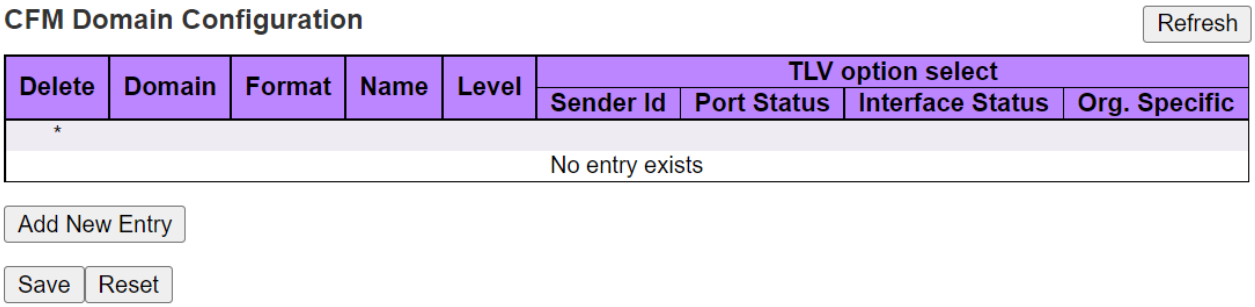

| Object | Description |
|---|---|
| **Sender Id TLV** | Choose whether and what to use as Sender ID TLVs in CCMs generated by this switch. Can be overridden by Domain and Service level configuration.<br>None<br>Chassis<br>Manage<br>ChassisManage |
| **Port Status TLV** | Choose whether to send Port Status TLVs in CCMs generated by this switch. Can be overridden by Domain and Service level configuration.<br>Enable Send Port Status TLVs in CCMs generated by this switch.<br>Disable Do not send Port Status TLVs in CCMs generated by this switch. |
| **Interface Status TLV** | Choose whether to send Interface Status TLVs in CCMs generated by this switch. Can be overridden by Domain and Service level configuration.<br>Enable Send Interface Status TLVs in CCMs generated by this switch.<br>Disable Do not Send Interface Status TLVs in CCMs generated by this switch. |
| **Organisation Specific TLV** | Choose whether to send Organisation Specific TLVs in CCMs generated by this switch. Can be overridden by Domain and Service level configuration.<br>Enable Send Organisation Specific TLVs in CCMs generated by this switch.<br>Disable Do not send Organisation Specific TLVs in CCMs generated by this switch. |
| **Organisation Specific TLV OUI** | This is the three-bytes OUI transmitted with the Organization-Specific TLVs. Enter as 6 characters 0-9, a-f. |
| **Organisation Specific TLV Subtype** | This is the subtype transmitted with the Organization-Specific TLV. Can be any value in range [0; 255] |

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

| Buttons | |
|---|---|
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

## 2.3.11 CFM – Domain (For 90W PoE Model)

Configure CFM Domain parameters on this page.




| Object | Description |
|---|---|
| **Delete** | Check to delete the entry. It will be deleted during the next save. |
| **Domain** | Name of Domain. Value is a single word which begins with an alphabetic letter A-Z or a-z with length 1-15. |
| **Format** | Select the MD name format. To mimic Y.1731 MEG IDs, use type None.<br>None<br>String |
| **Name** | The contents of this parameter depend on the value of the format member.<br>If format is None: Name is not used, but will be set to all-zeros behind the scenes. This format is typically used by Y.1731-kind-of-PDUs.<br>If format is String: Name must contain a string from 1 to 43 characters long. |
| **Level** | MD/MEG level of this domain. Valid values are restricted to 0 - 7.<br><br>About leak prevention<br>Leak prevention is about discarding OAM PDUs with MEG levels lower than the MEP they hit when the OAM PDUs are ingressing the port on which the MEP resides, and to discard OAM PDUs with MEG levels at or lower than the MEP's when the OAM |

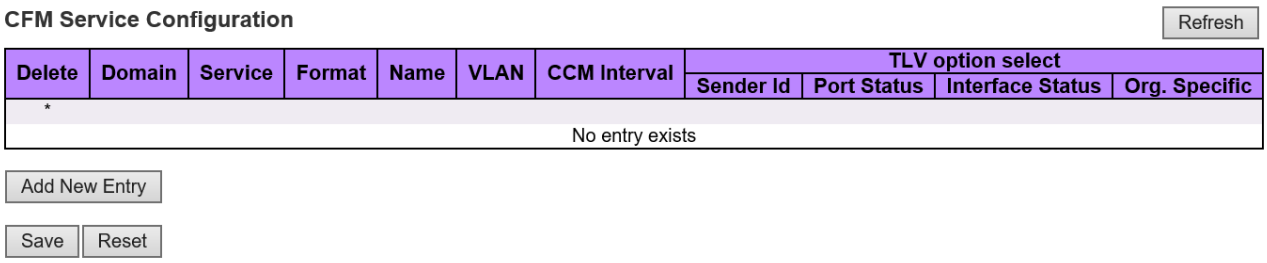
| | |
|---|---|
| | PDUs are ingressing other ports.<br>There are two categories of architectures, when it comes to leak-prevention: Those that use Shared MEG level and those that use Independent MEG level:<br><br>Shared MEG level<br>On Shared MEG level architectures, Port Down MEPs always perform level filtering no matter which VLAN ID (VID) OAM PDUs get classified to, unless the same port has a VLAN MEP on the VID in question. So if you have a Port MEP in VID X and a VLAN MEP in VID Y, an OAM frame arriving on the port and gets classified to VID X or VID Z will be handled/level-filtered by the Port MEP, whereas an OAM frame ingressing the port in VID Y will be handled by the VLAN MEP. Likewise, if the switch has a Port MEP on VID X on Port X and an OAM frame ingresses on VID Y on Port Y, it is subject to level filtering before egressing Port X, unless Port X also has a VLAN MEP on VID Y, in which case the VLAN MEP will take care of level-filtering the OAM PDU.<br>On Shared MEG level architectures, all Port MEPs must have the same MEG level and any VLAN MEP must have a MEG level higher than the Port MEPs' MEG level.<br><br>Independent MEG level<br>On Independent MEG level architectures, Port Down MEPs never perform level filtering on frames not classified to the MEP's VID. So if you have a Port MEP on VID X and a VLAN MEP on VID Y and an OAM frame ingresses any port on VID Z, it is not subject to handling/level-filtering by any of the two MEPs.<br><br>This switch exhibits Independent MEG level. |
| **TLV option select** | Sender Id: Default Sender ID TLV format to be used in CCMs generated by this Domain (may be overridden in service)<br>None Do not include Sender ID TLVs.<br>Chassis Enable Sender ID TLV and send Chassis ID (MAC Address).<br>Manage Enable Sender ID TLV and send Management address (IPv4 Address).<br>ChassisManage Enable Sender ID TLV and send both Chassis ID (MAC Address) and Management Address (IPv4 Address).<br>Defer Let the global configuration decide if Sender ID TLVs shall be included (may be overridden in service).<br><br>Port Status: Include or exclude Port Status TLV in CCMs generated by this Domain or let higher level determine (may be overridden in Service).<br>Disable Do not include Port Status TLVs. |

| | |
|---|---|
| | Enable Include Port Status TLVs.<br>Defer Let the global configuration decide if Port Status TLVs shall be included (may be overridden in Service).<br><br>Interface Status: Include or exclude Interface Status TLV in CCMs generated by this Domain or let higher level determine (may be overridden in Service).<br>Disable Do not include Interface Status TLVs.<br>Enable Include Interface Status TLVs.<br>Defer Let the global configuration decide if Interface Status TLVs shall be included (may be overridden in Service).<br><br>Org. Specific: Exclude Organization-Specific TLV in CCMs generated by this Domain or let higher level determine (may be overridden in Service).<br>Disable Do not include Organization-Specific TLVs.<br>Defer Let the global configuration decide if Organization-Specific TLVs shall be included (may be overridden in Service). |

| Buttons | |
|---|---|
| Add New Entry : | Click to add a new Domain entry. |
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

## 2.3.12 CFM – Service (For 90W PoE Model)

Configure CFM Service parameters on this page.




| Object | Description |
|---|---|
| **Delete** | Check to delete the entry. It will be deleted during the next save. |
| **Domain** | Name of Domain under which this Service resides. |

| | |
|---|---|
| **Service** | Name of Service. Value is a single word which begins with an alphabetic letter A-Z or a-z with length 1-15. |
| **Format** | Select the short Service name format. This decides how the value of the Name parameter will be interpreted. To mimic Y.1731 MEG IDs, create an MD instance with an empty name and use Y1731 ICC or Y1731 ICC CC.<br>Possible values are:<br>String<br>Two Octets<br>Y1731 ICC<br>Y1731 ICC CC<br>Look under Name for explanation. |
| **Name** | The contents of this parameter depends on the value of the format member. Besides the limitations explained for each of them, the following applies in general:<br>If the Domain Format is None, the size of this cannot exceed 45 bytes.<br>If the Domain Format is not None, the size of this cannot exceed 44 bytes.<br><br>If Format is String, the following applies:<br>length must be in range [1; 44]<br>Contents must be in range [32; 126]<br><br>If Format is Two Octets, the following applies: Name[0] and Name[1] will both be interpreted as unsigned 8-bit integers (allowing a range of [0; 255]). Name[0] will be placed in the PDU before Name[1].<br>The remaining available bytes in name will not be used.<br><br>If Format is Y1731 ICC, the following applies:<br>length must be 13.<br>Contents must be in range [a-z,A-Z,0-9]<br>Y.1731 specifies that it is a concatenation of ICC (ITU Carrier Code) and UMC (Unique MEG ID Code):<br>ICC: 1-6 bytes<br>UMC: 7-12 bytes<br>In principle UMC can be any value in range [1; 127], but this API does not allow for specifying length of ICC, so the underlying code doesn't know where ICC ends and UMC starts.<br>The Domain Format must be None.<br><br>If Format is Y1731 ICC CC, the following applies: |

| | |
|---|---|
| | length must be 15.<br>First 2 chars (CC): Must be amongst [A-Z]<br>Next 1-6 chars (ICC): Must be amongst [a-z,A-Z,0-9]<br>Next 7-12 chars (UMC): Must be amongst [a-z,A-Z,0-9]<br>There may be ONE (slash) present in name[3-7].<br>The Domain format must be None. |
| **VLAN** | The MA's primary VID. A primary VID of 0 means that all MEPs created within this MA will be created as port MEPs (interface MEPs). There can only be one port MEP per interface. A given port MEP may still be created with tags, if that MEP's VLAN is non-zero."<br>A non-zero primary VID means that all MEPs created within this MA will be created as VLAN MEPs. A given MEP may be configured with another VLAN than the MA's primary VID, but it is impossible to have untagged VLAN MEPs. |
| **CCM Interval** | The CCM rate of all MEPs bound to this Service. |
| **TLV option select** | Sender Id: Default Sender ID TLV format to be used in CCMs generated by this Service.<br>None Do not include Sender ID TLVs.<br>Chassis Enable Sender ID TLV and send Chassis ID (MAC Address).<br>Manage Enable Sender ID TLV and send Management address (IPv4 Address).<br>ChassisManage Enable Sender ID TLV and send both Chassis ID (MAC Address) and Management Address (IPv4 Address).<br>Defer Let the Domain configuration decide if Sender ID TLVs shall be included.<br>Port Status: Include or exclude Port Status TLV in CCMs generated by this Service or let higher level determine.<br>Disable Do not include Port Status TLVs.<br>Enable Include Port Status TLVs.<br>Defer Let the Domain configuration decide if Port Status TLVs shall be included.<br>Interface Status: Include or exclude Interface Status TLV in CCMs generated by this Service or let higher level determine.<br>Disable Do not include Interface Status TLVs.<br>Enable Include Interface Status TLVs.<br>Defer Let the Domain configuration decide if Interface Status TLVs shall be included.<br>Org. Specific: Exclude Organization-Specific TLV in CCMs generated by this Service or let higher level determine.<br>Disable Do not include Organization-Specific TLVs.<br>Defer Let the Domain configuration decide if Organization-Specific TLVs shall be included. |

| Buttons | |
|---|---|
| Add New Entry : | Click to add a new access management entry. |
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

## 2.3.13 CFM – MEP (For 90W PoE Model)

Configure CFM MEP parameters on this page.

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

Port Down-MEPs

In 802.1Q terminology, Port MEPs are located below the EISS entity, that is, closest to the physical port. Port MEPs are used by e.g. APS for protection purposes.

Port MEPs are created when the encompassing service has type "Port".

Port MEPs may send OAM PDUs tagged or untagged. An OAM PDU will be sent untagged only if the MEP's VLAN is set to "Inherit" (0). Any other value will cause it to be sent tagged with the port's TPID, whether or not the VLAN matches the port's PVID and that PVID is meant to be sent untagged.

VLAN Down-MEPs

In 802.1Q terminology, VLAN MEPs are located above the EISS entity.

This means that tagging of OAM PDUs will follow the port's VLAN configuration.

Thus, if a VLAN MEP is created on the Port's PVID and PVID is configured to be untagged, OAM PDUs will be transmitted untagged.

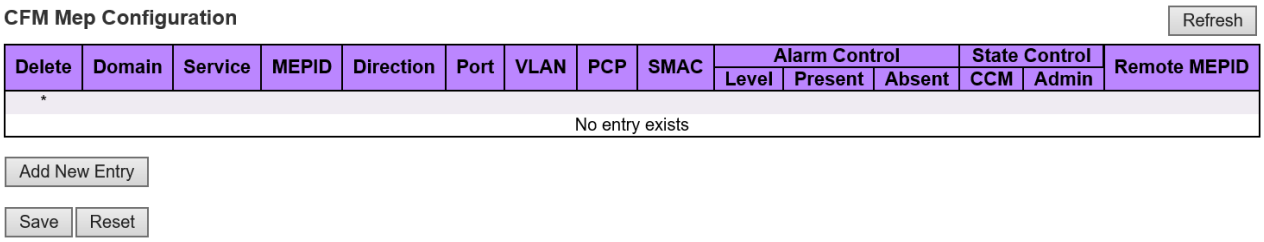
VLAN MEPs are created when the encompassing service has type "VLAN".

Down-MEP creation rules

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

1. There can only be one Port MEP on the same port.
2. There can only be one VLAN MEP on the same port and VLAN.
3. A VLAN MEP must have a higher MD/MEG level than a Port MEP on the same port and VLAN.

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




| Object | Description |
|---|---|
| **Delete** | Check to delete the entry. It will be deleted during the next save. |
| **Domain** | Name of Domain under which this MEP |
| **Service** | Name of Service under which this MEP resides. |
| **MEPID** | The identification of this MEP. Must be an integer [1..8091] |
| **Direction** | Set whether this MEP is an Up- or a Down-MEP. |
| **Port** | Port on which this MEP resides. |
| **VLAN** | VLAN ID. Use the value 0 to indicate untagged traffic (implies a port MEP). |
| **PCP** | Choose PCP value in PDUs' VLAN tag. Not used if untagged. |
| **SMAC** | Set a Source MAC address to be used in CCM PDUs originating at this MEP. Must be a unicast address. Format is XX:XX:XX:XX:XX:XX. If all-zeros, the switch port's MAC address will be used instead. |
| **Alarm Control** | Level: If a defect is detected with a priority higher than this level, a fault alarm notification will be generated.<br>Valid range is [1; 6] with 1 indicating that any defect will cause a fault alarm and 6 indicating that no defect can cause a fault alarm. See 802.1Q-2018, clause 20.9.5, LowestAlarmPri<br>The possible defects and their priorities are:<br>Short name Description Priority<br>DefRDICCM Remote Defect Indication 1<br>DefMACstatus MAC Status 2<br>DefRemoteCCM Remote CCM 3<br>DefErrorCCM Error CCM Received 4<br>DefXconCCM Cross Connect CCM Received 5<br><br>Present: The time in milliseconds that defects must be present before a fault alarm notification is issued. Default is 2500 ms.<br>Absent: The time in milliseconds that defects must be absent before a fault alarm notification is reset. Default is 10000 ms. |
| **State Control** | CCM: Enable or disable generation of continuity-check messages (CCMs)<br>Admin: Enable or disable this MEP. When this MEP is enabled, it will check |

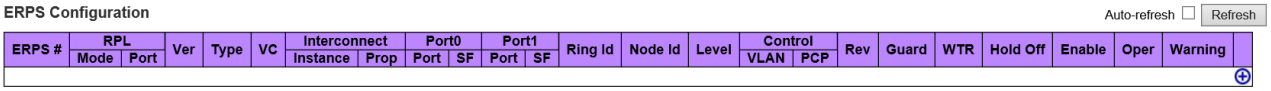
| | |
|---|---|
| | received/missing CCMs and can raise defects. |
| **Remote MEPID** | Specify the Remote MEP that this MEP is expected to receive CCM PDUs from. Must be an integer [0..8091] where 0 means undefined. The value of Remote MEPID must be different from the value of MEPID. |

| **Buttons** | |
|---|---|
| Add New Entry : | Click to add a new MEP entry. |
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

## 2.3.14 ERPS

The ERPS instances are configured here.

### 90W PoE Model

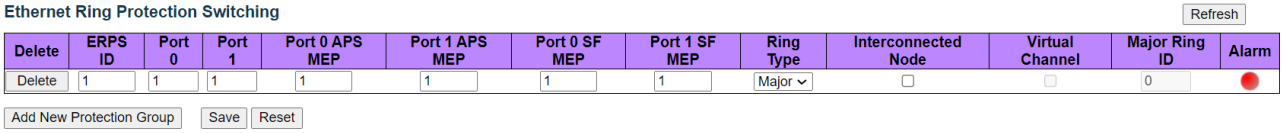



| Object | Description |
|---|---|
| **ERPS #** | The ID of ERPS. Valid range 1 - 64. |
| **RPL Role** | Ring Protection Link mode. Possible values:<br>None<br>Owner<br>Neighbor |
| **RPL Port** | Indicates whether it is port0 or port1 that is the Ring Protection Link. Not used if RPL Mode is None. |
| **Ver** | ERPS protocol version. v1 and v2 are supported. |
| **Type** | Type of ring. Possible values:<br>Major: ERPS major ring (G.8001-2016, clause 3.2.39)<br>Sub: ERPS sub-ring (G.8001-2016, clause 3.2.66)<br>InterSub: ERPS sub-ring on an interconnection node (G.8001-2016, clause 3.2.66) |
| **VC** | Controls whether to use a Virtual Channel with a sub-ring. |
| **Interconnect Instance** | For a sub-ring on an interconnection node, this must reference the instance ID of the ring to which this sub-ring is connected. |
| **Interconnect Prop** | Controls whether the ring referenced by Interconnect Instance shall propagate R-APS flush PDUs whenever this sub-ring's topology changes. |
| **Port0/Port1 Interface** | Interface index of ring protection Port0/Port1. |
| **Port0/Port1 SF** | Selects whether Signal Fail (SF) comes from the link state of a given interface, or from a Down-MEP. Possible values:<br>MEP: Down-MEP<br>Link: Link |
| **Ring ID** | The Ring ID is used - along with the control VLAN - to identify R-APS PDUs as belonging to a particular ring. |
| **Node ID** | The Node ID is used inside the R-APS specific PDU to uniquely identify this node (switch) on the ring. |
| **Level** | MD/MEG Level of R-APS PDUs we transmit. |

| | |
|---|---|
| **Control VLAN** | The VLAN on which R-APS PDUs are transmitted and received on the ring ports. |
| **Control PCP** | The PCP value used in the VLAN tag of the R-APS PDUs. |
| **Rev** | Revertive (true) or Non-revertive (false) mode. |
| **Guard** | Guard time in ms. Valid range is 10 - 2000 ms. |
| **WTR** | "Wait-to-Restore time in seconds. Valid range 1 - 720 sec. |
| **Hold Off** | Hold off time in ms. Value is rounded down to 100ms precision. Valid range is 0 - 10000 ms. |
| **Enable** | The administrative state of this APS ERPS. Check to make it function normally and uncheck to make it cease functioning. |
| **Oper** | The operational state of ERPS instance.<br>: Active<br>: Disabled or Internal error. |
| **Warning** | Operational warnings of ERPS instance.<br>: No warnings<br>: There are warnings, use tooltip to see. |
| **Configuration Buttons** | You can modify each ERPS in the table using the following buttons:<br>: Edits the ERPS row.<br>: Deletes the ERPS.<br>: Adds new ERPS. |

| Buttons | |
|---|---|
| Auto-refresh ☐ | Check this box to refresh the page automatically. |
| Refresh | Click to refresh the page immediately. |

## 30W PoE Model




| Object | 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 |

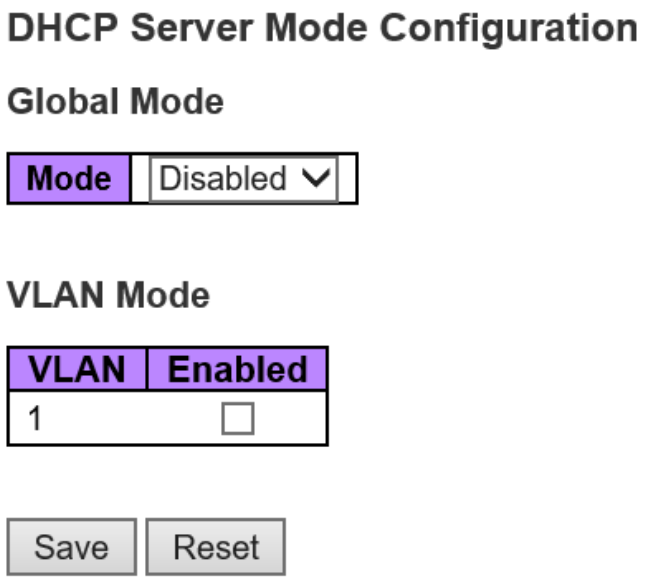
| | |
|---|---|
| | field indicates that no "Port 1" is associated with this instance |
| **Port 0 SF MEP** | The Port 0 Signal Fail reporting MEP. |
| **Port 1 SF MEP** | The Port 1 Signal Fail reporting MEP. As only one SF MEP is associated with interconnected sub-ring without virtual channel, it is 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. |

| **Buttons** | |
|---|---|
| Add New Protection Group: | Click to add a new Protection group entry. |
| Refresh | Click to refresh the page immediately. |
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

## 2.3.15 DHCP Server Mode

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

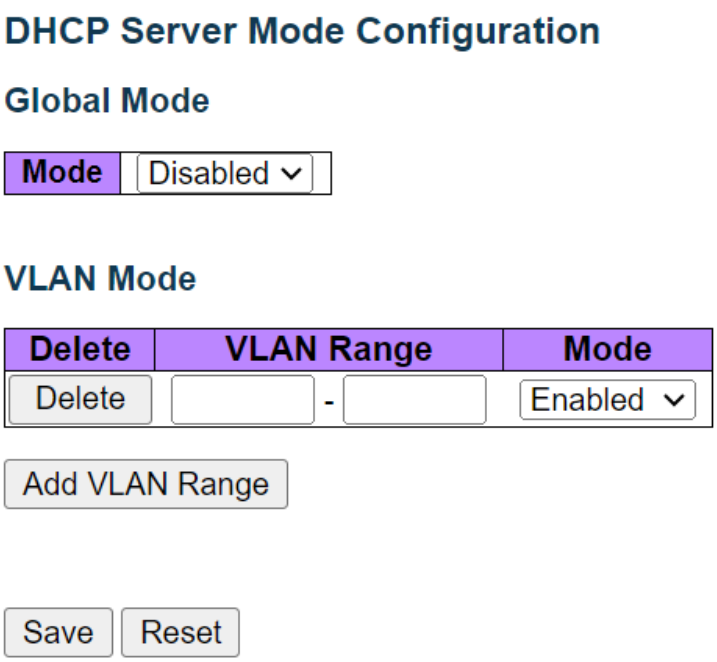
90W PoE Model




| Object | Description |
|---|---|
| **Global Mode** | |
| **Mode** | Configure the operation mode per system. Possible modes are:<br>`Enabled`: Enable DHCP server per system.<br>`Disabled`: Disable DHCP server pre system. |
| **VLAN Mode** | |
| **VLAN** | The VLAN ID of the entry. |
| **Mode** | Enable the DHCP server per VLAN by checking this box. |

| Buttons | |
|---|---|
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

30W PoE Model

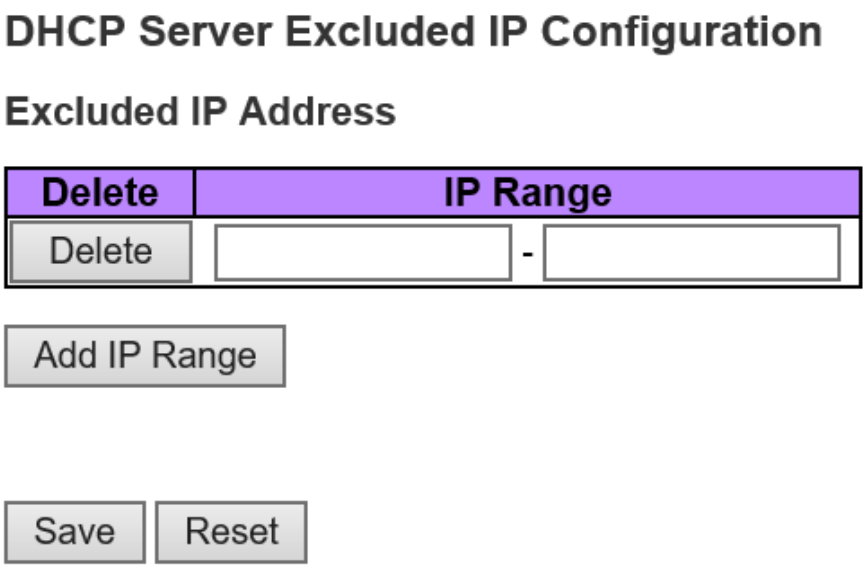



| Object | Description |
|---|---|
| **Global Mode** | |
| **Mode** | Configure the operation mode per system. Possible modes are:<br>`Enabled`: Enable DHCP server per system.<br>`Disabled`: Disable DHCP server pre system. |
| **VLAN Mode** | |
| **VLAN Rangr** | Indicate the VLAN range in which DHCP server is enabled or disabled. The first VLAN ID must be smaller than or equal to the second VLAN ID. BUT, if the VLAN range contains only 1 VLAN ID, then you can just input it into either one of the first and second VLAN ID or both.<br>On the other hand, if you want to disable existed VLAN range, then you can follow the steps.<br>1. press Add VLAN Range to add a new VLAN range.<br>2. input the VLAN range that you want to disable.<br>3. choose Mode to be Disabled.<br>4. press Save to apply the change.<br>Then, you will see the disabled VLAN range is removed from the DHCP Server mode configuration page. |
| **Mode** | Enable the DHCP server per VLAN by checking this box. |

| Buttons | |
|---|---|
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

## 2.3.16 DHCP Server Excluded IP

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



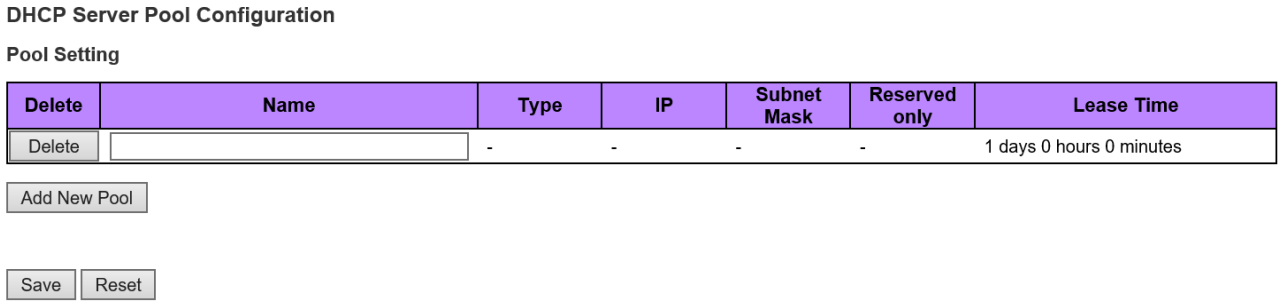

| Object | Description |
|---|---|
| **IP Range** | Define the IP range to be excluded IP addresses. The first excluded IP must be smaller than or equal to the second excluded IP. BUT, if the IP range contains only 1 excluded IP, then you can just input it to either one of the first and second excluded IP or both. |

| Buttons | |
|---|---|
| Delete | Click to delete the setting. |

| | |
|---|---|
| Add IP Range | Click to add a new excluded IP range. |
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

## 2.3.17 DHCP Server Pool

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



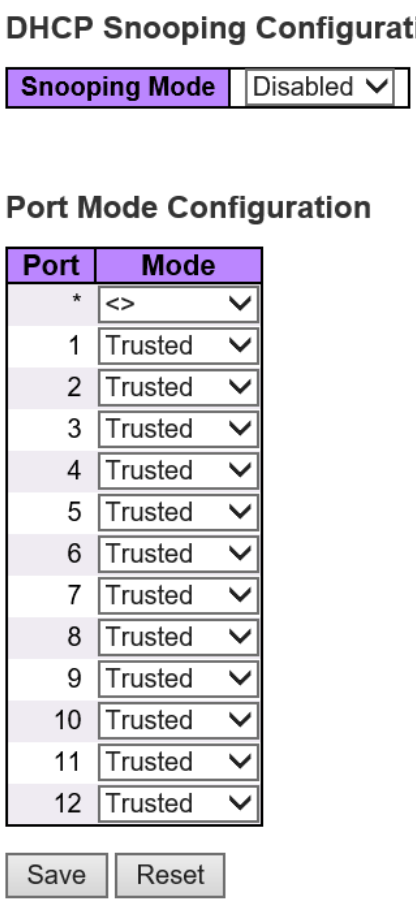

| Object | Description |
|---|---|
| **Name** | Configure the pool name that accepts all printable characters, except white space. If you want to configure the detail settings, you can click the pool name to go into the configuration page. |
| **Type** | Display which type of the pool is.<br>`Network`: the pool defines a pool of IP addresses to service more than one DHCP client.<br>`Host`: the pool services for a specific DHCP client identified by client identifier or hardware address.<br>If "-" is displayed, it means not defined. |
| **IP** | Display network number of the DHCP address pool.<br>If "-" is displayed, it means not defined. |
| **Subnet Mask** | Display subnet mask of the DHCP address pool.<br>If "-" is displayed, it means not defined. |
| **Reserved Only (For 90W PoE Model)** | If on, Ip addresses obtainable from the pool are limited to those entered into the reserved entries table. |

| | |
|---|---|
| **Lease Time** | Display lease time of the pool. |

| Buttons | |
|---|---|
| Delete | Click to delete the setting. |
| Add New Pool | Click to add a new DHCP pool. |
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

## 2.3.18 DHCP Snooping

Configure DHCP Snooping on this page.



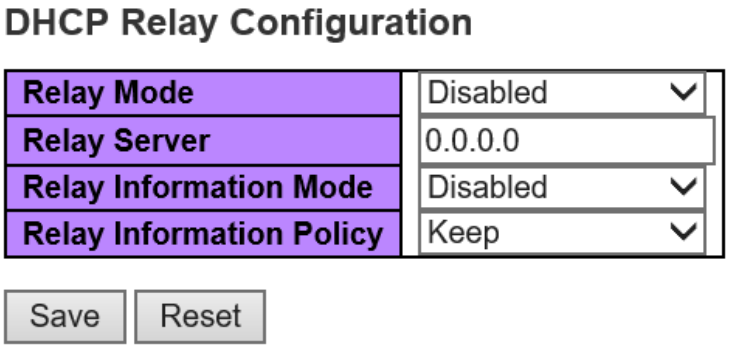

| Object | Description |
|---|---|

| | |
|---|---|
| **Snooping Mode** | Indicates the DHCP snooping mode operation. Possible modes are:<br>**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.<br>**Disabled**: Disable DHCP snooping mode operation. |
| **Port Mode Configuration** | Indicates the DHCP snooping port mode. Possible port modes are:<br>**Trusted**: Configures the port as trusted source of the DHCP messages.<br>**Untrusted**: Configures the port as untrusted source of the DHCP messages. |

| Buttons | |
|---|---|
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

## 2.3.19 DHCP Relay

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




| Object | Description |
|---|---|
| **Relay Mode** | Indicates the DHCP relay mode operation.<br>Possible modes are:<br>**Enabled**: Enable DHCP relay mode operation. When DHCP relay mode operation is |

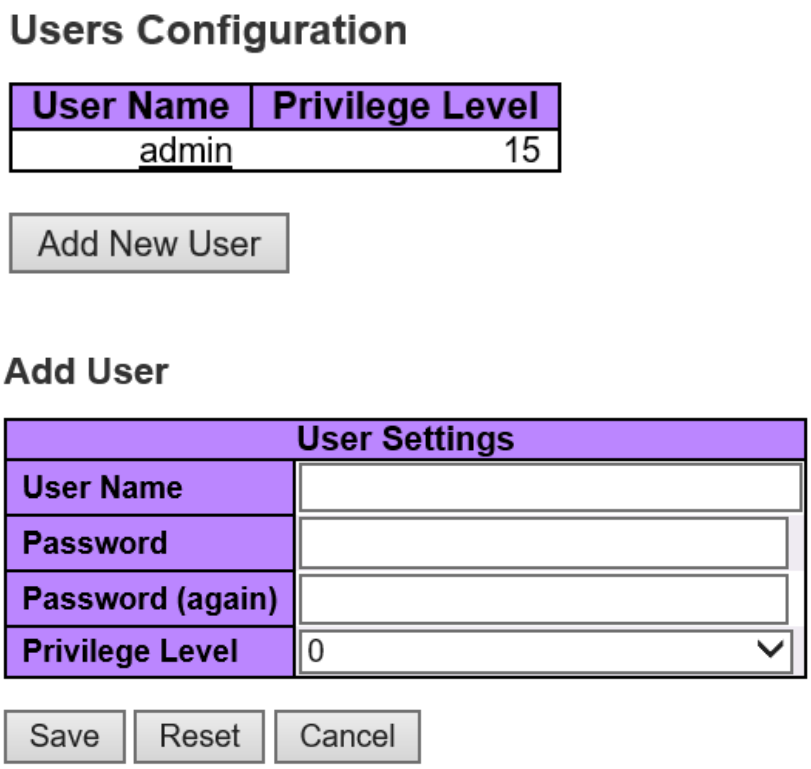
| | |
|---|---|
| | enabled, the agent forwards and transfers DHCP messages between the clients and the server when they are not in the same subnet domain. And the DHCP broadcast message won't be flooded for security considerations.<br>**Disabled**: Disable DHCP relay mode operation. |
| **Relay Server** | Indicates the DHCP relay server IP address. |
| **Relay Information Mode** | Indicates the DHCP relay information mode option operation. The option 82 circuit ID format as "[vlan_id][module_id][port_no]". The first four characters represent the VLAN ID, the fifth and sixth characters are the module ID(in standalone device it always equal 0, in stackable device it means switch ID), and the last two characters are the port number. For example, "00030108" means the DHCP message receive form VLAN ID 3, switch ID 1, port No 8. And the option 82 remote ID value is equal the switch MAC address.<br>Possible modes are:<br>**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.<br>**Disabled**: Disable DHCP relay information mode operation. |
| **Relay Information Policy** | Indicates the DHCP relay information option policy. When DHCP relay information mode operation is enabled, if the agent receives a DHCP message that already contains relay agent information it will enforce the policy. The 'Replace' policy is invalid when relay information mode is disabled. Possible policies are:<br>**Replace**: Replace the original relay information when a DHCP message that already contains it is received.<br>**Keep**: Keep the original relay information when a DHCP message that already contains it is received.<br>**Drop**: Drop the package when a DHCP message that already contains relay information is received. |

| Buttons | |
|---|---|
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

## 2.3.20 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.

90W PoE Model

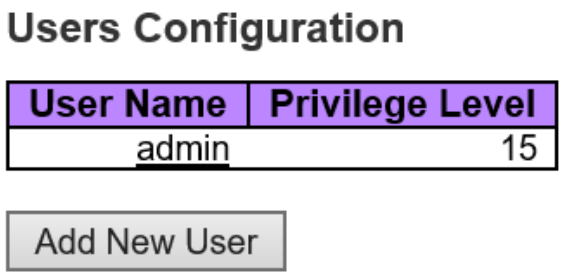


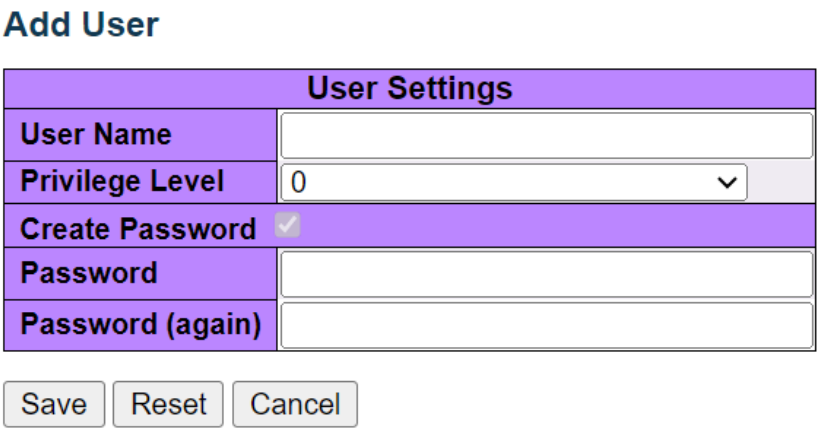

| Object | Description |
|---|---|
| **User Name** | A string identifying the user name that this entry should belong to. The allowed string length is 1 to 31. The valid user name allows letters, numbers and underscores. |
| **Password** | The password of the user. The allowed string length is 0 to 31. Any printable characters including space is accepted. |
| **Privilege Level** | The privilege level of the user. The allowed range is 0 to 15. If the privilege level value is 15, it can access all groups, i.e. that is granted the fully control of the device. But others value need to refer to each group privilege level. User's privilege should be same or greater than the group privilege level to have the access of that group. By default setting, most groups privilege level 5 has the read-only access and privilege level 10 has the read-write access. And the system maintenance (software upload, factory defaults and etc.) need user privilege level 15. Generally, the privilege level 15 can be used for an administrator account, privilege level 10 for a standard |

| | |
|---|---|
| | user account and privilege level 5 for a guest account. |

| Buttons | |
|---|---|
| Add New User | Click to add a new user. |
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |
| Cancel | Click to undo any changes made locally and return to the Users. |
| Delete User : | Delete the current user. This button is not available for new configurations (Add new user) |

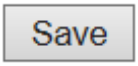
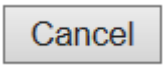
30W PoE Model




| Object | Description |
|---|---|
| **User Name** | A string identifying the user name that this entry should belong to. The allowed string length is 1 to 31. The valid user name allows letters, numbers and underscores. |
| **Privilege Level** | The privilege level of the user. The allowed range is 0 to 15. If the privilege level value is 15, it can access all groups, i.e. that is granted the fully control of the device. |

| | |
|---|---|
| | But others value need to refer to each group privilege level. User's privilege should be same or greater than the group privilege level to have the access of that group. By default setting, most groups privilege level 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. |
| **Modify Password** | Selected checkbox to create or modify password. |
| **Password** | The password of the user. The allowed string length is `0` to `31`. Any printable characters including space is accepted. |

| **Buttons** | |
|---|---|
|  | Click to add a new user. |
|  | Click to save changes. |
|  | Click to undo any changes made locally and revert to previously saved values. |
|  | Click to undo any changes made locally and return to the Users. |
|  | Delete the current user. This button is not available for new configurations (Add new user) |

## 2.3.21 Security Switch - Privilege Level

This page provides an overview of the privilege levels.

**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 |
| alm_profile | 5 | 10 | 5 | 10 |
| CFM | 5 | 10 | 5 | 10 |
| DDMI | 5 | 10 | 5 | 10 |
| Debug | 15 | 15 | 15 | 15 |
| DHCP | 5 | 10 | 5 | 10 |
| DHCPv6_Client | 5 | 10 | 5 | 10 |
| Diagnostics | 5 | 10 | 5 | 10 |
| ERPS | 5 | 10 | 5 | 10 |
| Firmware | 5 | 10 | 5 | 10 |
| IP | 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 |
| Miscellaneous | 15 | 15 | 15 | 15 |
| 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 |
| Security(access) | 10 | 10 | 5 | 10 |
| Security(network) | 5 | 10 | 5 | 10 |
| sFlow | 5 | 10 | 5 | 10 |
| Spanning_Tree | 5 | 10 | 5 | 10 |
| System | 5 | 10 | 1 | 10 |
| tyndbg | 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 |
| Voice_VLAN | 5 | 10 | 5 | 10 |
| XXRP | 5 | 10 | 5 | 10 |

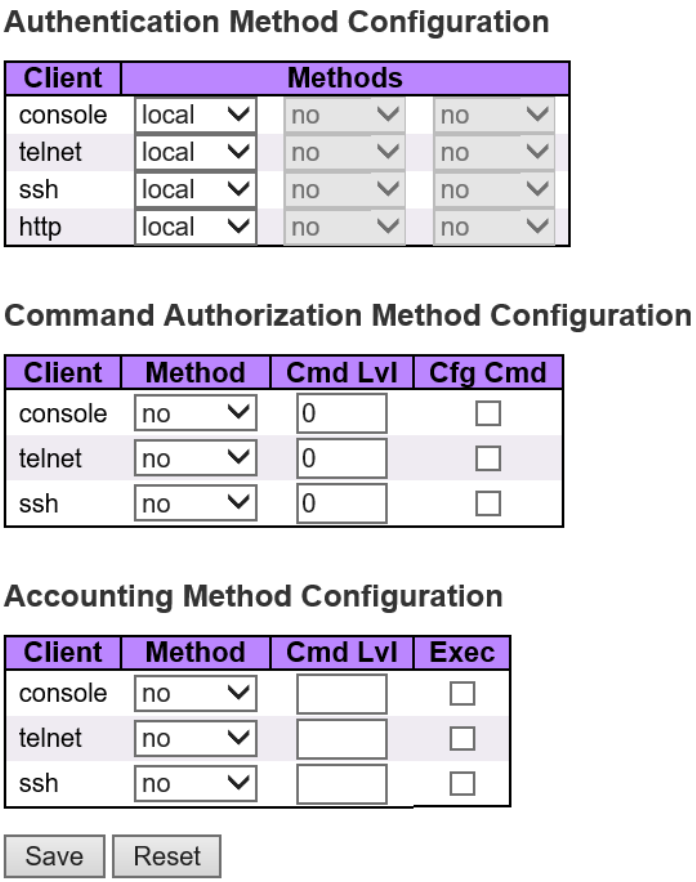
Save Reset

| Object | Description |
|---|---|
| **Group Name** | The name identifying the privilege group. In most cases, a privilege level group consists of a single module (e.g. LACP, RSTP or QoS), but a few of them contains more than one. The following description defines these privilege level groups in details:<br>System: Contact, Name, Location, Timezone, Daylight Saving Time, Log.<br>Security: Authentication, System Access Management, Port (contains Dot1x port, MAC based and the MAC Address Limit), ACL, HTTPS, SSH, ARP Inspection, IP source guard.<br>IP: Everything except 'ping'.<br>Port: Everything except 'VeriPHY'.<br>Diagnostics: 'ping' and 'VeriPHY'.<br>Maintenance: CLI- System Reboot, System Restore Default, System Password, Configuration Save, Configuration Load and Firmware Load. Web- Users, Privilege Levels and everything in Maintenance.<br>Debug: Only present in CLI. |
| **Privilege Levels** | 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. |

| Buttons | |
|---|---|
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

## 2.3.22 Security Switch - Auth Method

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



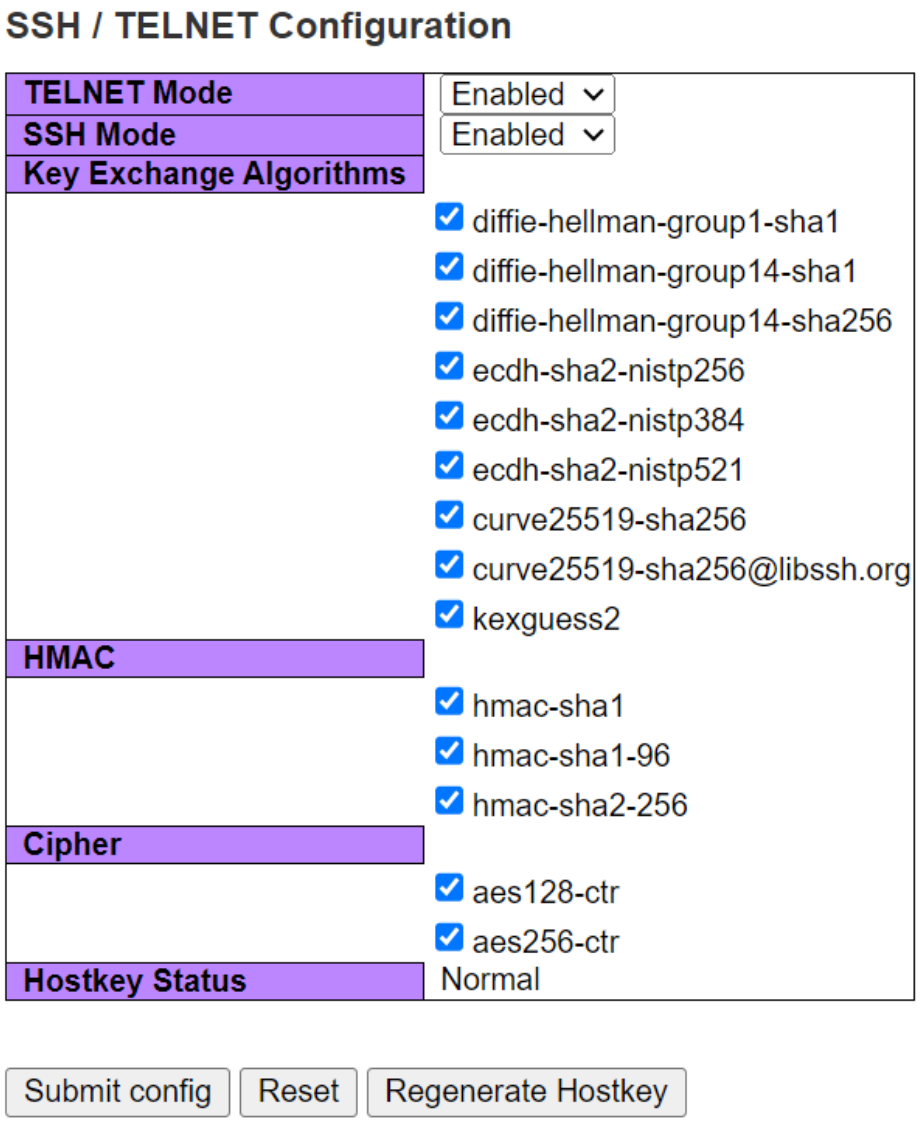

| Object | Description |
|---|---|
| **Authentication Method Configuration** | |
| **Client** | The management client for which the configuration below applies. |
| **Methods** | Method can be set to one of the following values:<br>• no: Authentication is disabled and login is not possible.<br>• local: Use the local user database on the switch for authentication.<br>• radius: Use remote RADIUS server(s) for authentication.<br>• tacacs+: Use remote TACACS+ server(s) for authentication.<br><br>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** | |
| **Client** | The management client for which the configuration below applies. |
| **Methods** | Method can be set to one of the following values:<br>• no: Command authorization is disabled. User is granted access to CLI commands according to his privilege level.<br>• tacacs: Use remote TACACS+ server(s) for command authorization. If all remote servers are offline, the user is granted access to CLI commands according to his privilege level. |
| **Cmd Lvl** | Authorize all commands with a privilege level higher than or equal to this level. Valid values are in the range 0 to 15. |
| **Cfg Cmd** | Also authorize configuration commands. |
| **Accounting Method Configuration** | |
| **Client** | The management client for which the configuration below applies. |
| **Methods** | Method can be set to one of the following values:<br>• no: Accounting is disabled.<br>• tacacs: Use remote TACACS+ server(s) for accounting. |
| **Cmd Lvl** | Enable accounting of all commands with a privilege level higher than or equal to this level.<br>Valid values are in the range 0 to 15. Leave the field empty to disable command accounting. |
| **Exec** | Enable exec (login) accounting. |

| **Buttons** | |
|---|---|
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

## 2.3.23 Security Switch – SSH/TELNET

Configure SSH / TELNET on this page.



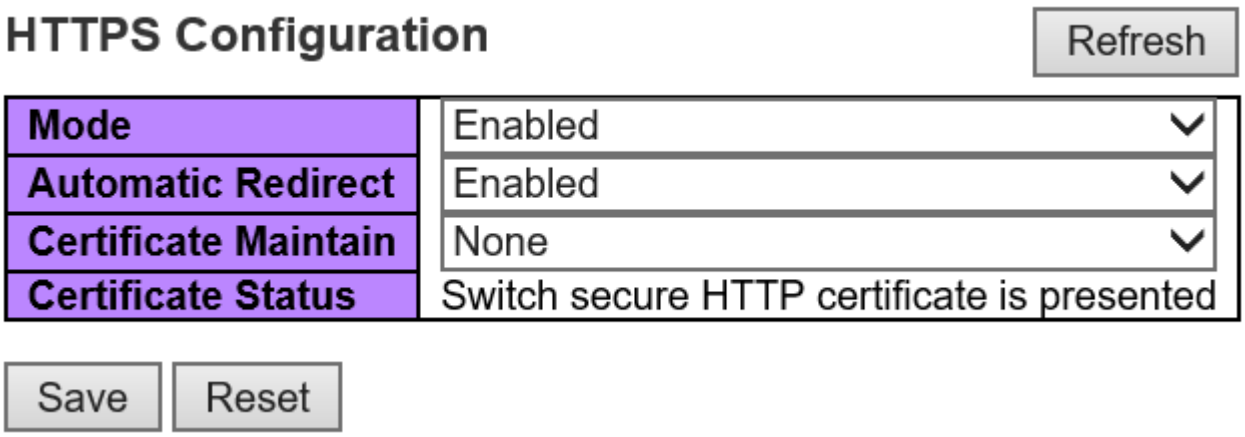

| Object | Description |
|---|---|
| **Mode** | Indicates the SSH mode operation. Possible modes are:<br>Enabled: Enable SSH / TELNET mode operation.<br>Disabled: Disable SSH / TELNET mode operation. (TELNET is Enabled by Default.) |
| **Key Exchange Algorithms** | Indicates the Key Exchange Algorithms enabled. Supported algorithms are:<br>`diffie-hellman-group1-sha1`: diffie-hellman-group1-sha1<br>`diffie-hellman-group14-sha1`: diffie-hellman-group14-sha1<br>`diffie-hellman-group14-sha256`: diffie-hellman-group14-sha256 |

| | |
|---|---|
| | **diffie-hellman-group16-sha512**: diffie-hellman-group16-sha512, disabled<br>**ecdh-sha2-nistp256**: ecdh-sha2-nistp256<br>**ecdh-sha2-nistp384**: ecdh-sha2-nistp384<br>**ecdh-sha2-nistp521**: ecdh-sha2-nistp521<br>**curve25519-sha256**: curve25519-sha256<br>**curve25519-sha256-libssh-org**: curve25519-sha256@libssh.org<br>**kexguess2**: kexguess2@matt.ucc.asn.au |
| **HMAC: Hashing Message Authentication Code** | Indicates the HMAC enabled. Supported algorithms are:<br>**hmac-sha1**: SHA1 HMAC<br>**hmac-sha1-96**: SHA1-96 HMAC<br>**hmac-sha2-256**: SHA2-256 HMAC<br>**hmac-sha2-512**: SHA2-512 HMAC, disabled<br>**hmac-md5**: MD5 HMAC, disabled |
| **Ciphers** | Specifies the SSH ciphers to use in SSH communication. Supported algorithms are:<br>**aes128-ctr**: AES128-CTR<br>**aes256-ctr**: AES256-CTR<br>**3des-ctr**: 3DES-CTR, disabled<br>**aes128-cbc**: AES128-CBC, disabled<br>**aes256-cbc**: AES256-CBC, disabled<br>**twofish256-cbc**: TwoFish256-CBC, disabled<br>**twofish-cbc**: TwoFish-CBC, disabled<br>**twofish128-cbc**: TwoFish128-CBC, disabled<br>**3des-cbc**: 3DES-CBC, disabled<br>**blowfish-cbc**: BlowFish-CBC, disabled |
| **Hostkey** | Specifies the SSH hostkey to use in SSH communication. Supported algorithms are:<br>**rsa**: RSA<br>**dss**: DSS, disabled<br>**ecdsa-256**: ECDSA-256, disabled<br>**ecdsa-384**: ECDSA-384, disabled<br>**ecdsa-521**: ECDSA-521, disabled |
| **Regenerate Hostkey status** | Re-generation hostkey on the switch of status.<br>Possible statuses are:<br>**Normal**<br>**Success**<br>**Fail**<br>**Generating...**<br>Note: The key re-generation would take 1~2 minutes. |

| Buttons | |
|---|---|
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |
| Regenerate Hostkey : | Click to regenerate hostkey. |

## 2.3.24 Security Switch - HTTPS

Configure HTTPS on this page.




| Object | Description |
|---|---|
| **Mode** | Indicates the HTTPS mode operation. When the current connection is HTTPS, to apply HTTPS disabled mode operation will automatically redirect web browser to an HTTP connection. Possible modes are:<br>`Enabled`: Enable HTTPS mode operation.<br>`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.<br>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.<br>Possible modes are: |

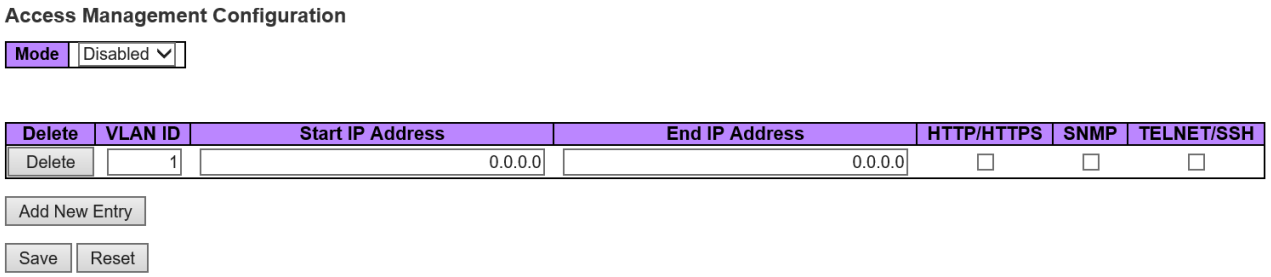
| | |
|---|---|
| | **Enabled**: Enable HTTPS redirect mode operation.<br>**Disabled**: Disable HTTPS redirect mode operation. |
| **Certificate Maintain** | The operation of certificate maintenance.<br>Possible operations are:<br>**None**: No operation.<br>**Delete**: Delete the current certificate.<br>**Upload**: Upload a certificate PEM file. Possible methods are: **Web Browser** or **URL**.<br>**Generate**: Generate a new self-signed RSA certificate. |
| **Certificate Pass Phrase** | Enter the pass phrase in this field if your uploading certificate is protected by a specific passphrase. |
| **Certificate Upload** | Upload a certificate PEM file into the switch. The file should contain the certificate and private key together. If you have two separated files for saving certificate and private key. Use the Linux cat command to combine them into a single PEM file. For example, cat my.cert my.key > my.pem<br>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.<br>Possible methods are:<br>Web Browser: Upload a certificate via Web browser.<br>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.<br>Possible statuses are:<br>**Switch secure HTTP certificate is presented**.<br>**Switch secure HTTP certificate is not presented**.<br>**Switch secure HTTP certificate is generating ...**. |

| **Buttons** | |
|---|---|
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

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

## 2.3.25 Security Switch - Access Management

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.




| Object | Description |
|---|---|
| **Mode** | Indicates the access management mode operation. Possible modes are:<br>`Enabled`: Enable access management mode operation.<br>`Disabled`: Disable access management mode operation. |
| **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. |

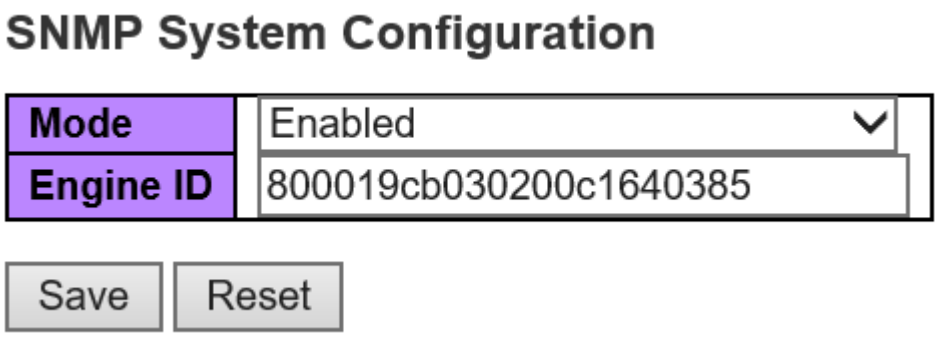
| Buttons | |
|---|---|
| Add New Entry | Click to add a new access management entry. |
| Save | Click to save changes. |

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

## 2.3.26 SNMP System Configuration

Configure SNMP on this page.

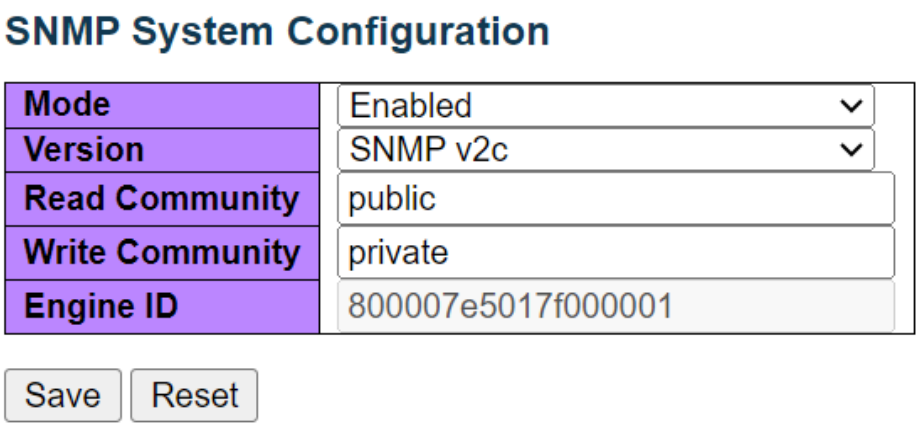
90W PoE Model




| Object | Description |
|---|---|
| **Mode** | Indicates the SNMP mode operation. Possible modes are:<br>`Enabled`: Enable SNMP mode operation.<br>`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. |

| Buttons | |
|---|---|
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

30W PoE Model



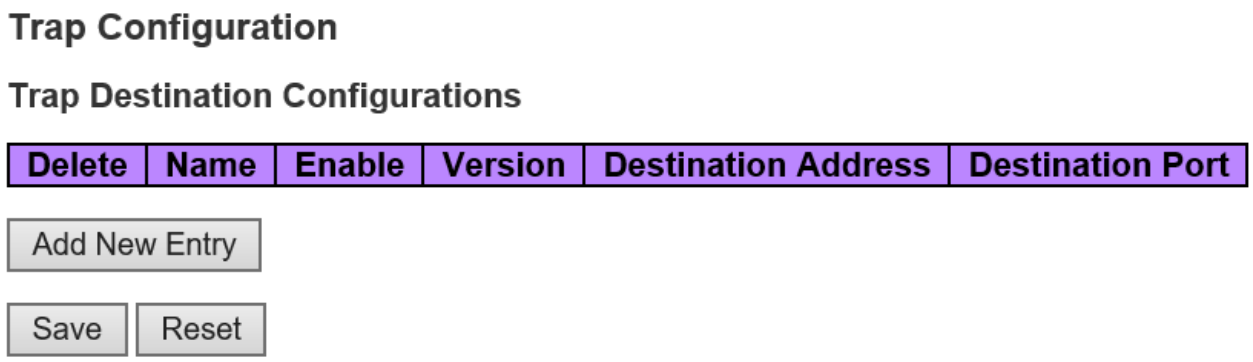

| Object | Description |
|---|---|
| **Mode** | Indicates the SNMP mode operation. Possible modes are:<br>`Enabled`: Enable SNMP mode operation.<br>`Disabled`: Disable SNMP mode operation. |
| **Version** | Indicates the SNMP supported version. Possible versions are:<br>SNMP v1: Set SNMP supported version 1.<br>SNMP v2c: Set SNMP supported version 2c.<br>SNMP v3: Set SNMP supported version 3. |
| **Read Community** | Indicates the community read access string to permit access to SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126.<br>The field is applicable only when SNMP version is SNMPv1 or SNMPv2c. If SNMP version is SNMPv3, the community string will be associated with SNMPv3 communities table. It provides more flexibility to configure security name than a SNMPv1 or SNMPv2c community string. In addition to community string, a particular range of source addresses can be used to restrict source subnet. |
| **Write Community** | Indicates the community write access string to permit access to SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126.<br>The field is applicable only when SNMP version is SNMPv1 or SNMPv2c. If SNMP version is SNMPv3, the community string will be associated with SNMPv3 communities table. It provides more flexibility to configure security name than a SNMPv1 or SNMPv2c community string. In addition to community string, a particular range of source addresses can be used to restrict source subnet. |
| **Engine ID** | Indicates the SNMPv3 engine ID. The string must contain an even number(in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all- |

| | |
|---|---|
| | 'F's are not allowed. 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. |

| Buttons | |
|---|---|
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

## 2.3.27 SNMP Trap Destination

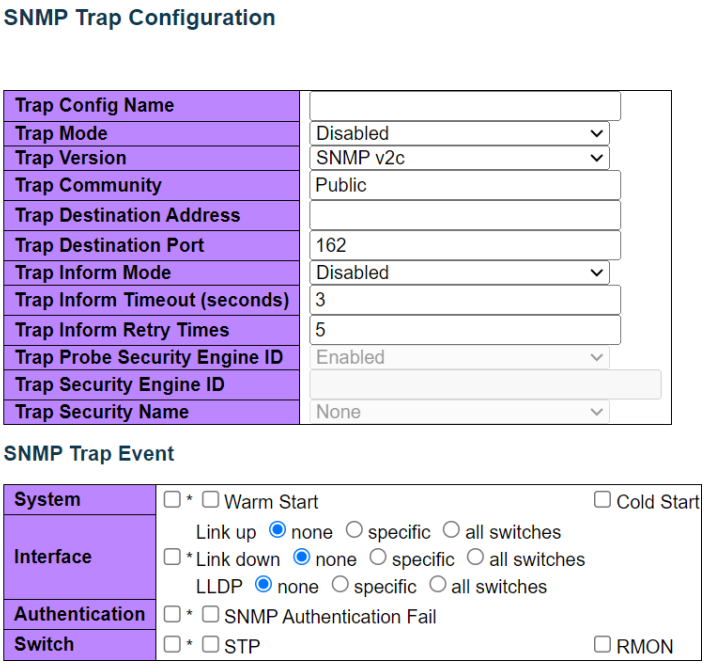
Configure trap destinations on this page.




| Object | Description |
|---|---|
| **Trap Destination Configurations** | |
| **Name** | Indicates the trap Configuration's name. Indicates the trap destination's name. |
| **Enable** | Indicates the trap destination mode operation. Possible modes are:<br>`Enabled`: Enable SNMP trap mode operation.<br>`Disabled`: Disable SNMP trap mode operation. |
| **Version** | Indicates the SNMP trap supported version. Possible versions are:<br>`SNMPv1`: Set SNMP trap supported version 1.<br>`SNMPv2c`: Set SNMP trap supported version 2c.<br>`SNMPv3`: Set SNMP trap supported version 3. |
| **Destination Address** | Indicates the SNMP trap destination address. It allow a valid IP address in dotted decimal notation ('x.y.z.w'). |

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

The SNMP Trap Configuration page includes the following fields:




| Object | Description |
|---|---|
| **SNMP Trap Configuration** | |
| **Trap Config Name** | Indicates which trap Configuration's name for configuring. The allowed string length is 0 to 255, and the allowed content is ASCII characters from 33 to 126. |
| **Trap Mode** | Indicates the SNMP trap mode operation. Possible modes are: |

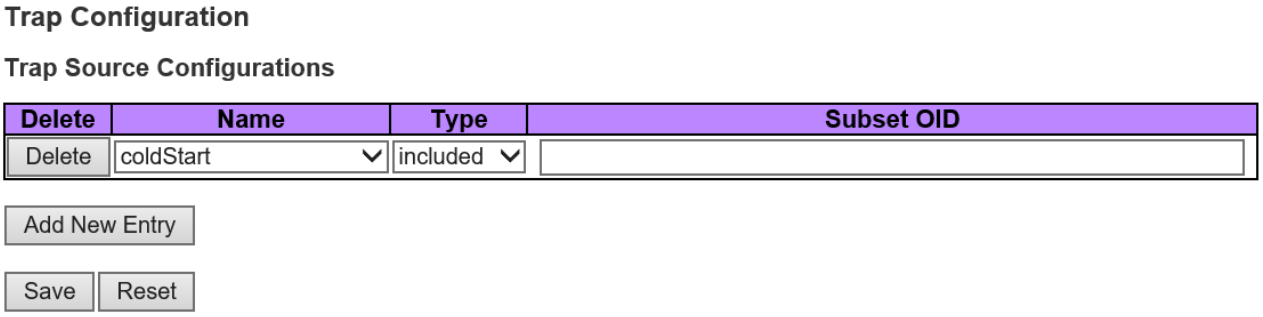
| | |
|---|---|
| | **Enabled**: Enable SNMP trap mode operation.<br>**Disabled**: Disable SNMP trap mode operation. |
| **Trap Version** | Indicates the SNMP trap supported version. Possible versions are:<br>**SNMP v1**: Set SNMP trap supported version 1.<br>**SNMP v2c**: Set SNMP trap supported version 2c.<br>**SNMP v3**: Set SNMP trap supported version 3. |
| **Trap Community** | Indicates the community access string when sending SNMP trap packet. The allowed string length is 0 to 255, and the allowed content is ASCII characters from 33 to 126. |
| **Trap Destination Address** | Indicates the SNMP trap destination address. It allow a valid IP address in dotted decimal notation ('x.y.z.w').<br>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 |
| **Trap Destination Port** | Indicates the SNMP trap destination port. SNMP Agent will send SNMP message via this port, the port range is 1~65535. |
| **Trap Inform Mode** | Indicates the SNMP trap inform mode operation. Possible modes are:<br>**Enabled**: Enable SNMP trap inform mode operation.<br>**Disabled**: Disable SNMP trap inform mode operation. |
| **Trap Inform Timeout (seconds)** | Indicates the SNMP trap inform timeout. The allowed range is **0** to **2147**. |
| **Trap Inform Retry Times** | Indicates the SNMP trap inform retry times. The allowed range is **0** to **255**. |
| **Trap Probe Security Engine ID** | Indicates the SNMP trap probe security engine ID mode of operation. Possible values are:<br>**Enabled**: Enable SNMP trap probe security engine ID mode of operation.<br>**Disabled**: Disable SNMP trap probe security engine ID mode of operation. |
| **Trap Security Engine ID** | Indicates the SNMP trap security engine ID. SNMPv3 sends traps and informs using USM for authentication and privacy. A unique engine ID for these traps and informs is needed. When "Trap Probe Security Engine ID" is enabled, the ID will be probed automatically. Otherwise, the ID specified in this field is used. The string must contain an even number(in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed. |
| **Trap Security Name** | Indicates the SNMP trap security name. SNMPv3 traps and informs using USM for authentication and privacy. A unique security name is needed when traps and informs are enabled. |
| **SNMP Trap Event** | |
| **System** | Enable/disable that the Interface group's traps. Possible traps are: |

| | |
|---|---|
| | **Warm Start**: Enable/disable Warm Start trap.<br>**Cold Start**: Enable/disable Cold Start trap. |
| **Interface** | Indicates that the Interface group's traps. Possible traps are: Indicates that the SNMP entity is permitted to generate authentication failure traps. Possible modes are:<br>**Link Up**: Enable/disable Link up trap.<br>**Link Down**: Enable/disable Link down trap.<br>**LLDP**: Enable/disable LLDP trap. |
| **Authentication** | Indicates that the authentication group's traps. Possible traps are:<br>**SNMP Authentication Fail** : Enable/disable SNMP trap authentication failure trap. |
| **Switch** | Indicates that the Switch group's traps. Possible traps are:<br>**STP**: Enable/disable STP trap.<br>**RMON**: Enable/disable RMON trap. |

| Buttons | |
|---|---|
| Add New Entry | Click to add a new user. |
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

## 2.3.28 SNMP Trap Source (For 90W PoE Model)

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




| Object | Description |
|---|---|
| **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. Possible types are:<br>included: An optional flag to indicate a trap is sent for the given trap source is matched.<br>excluded: An optional flag to indicate a trap is not sent for the given trap source is matched. |
| **Subset OID** | The subset OID for the entry. The value should depend on the what kind of trap name. For example, the ifIdex is the subset OID of linkUp and linkDown. A valid subset OID is one or more digital number(0-4294967295) or asterisk(*) which are separated by dots(.). The first character must not begin withasterisk(*) and the maximum of OID count must not exceed 128. |

| Buttons | |
|---|---|
| Add New Entry | Click to add a new entry. The maximum entry count is 32. |
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

## 2.3.29 SNMP Communities

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

90W PoE Model

**SNMPv3 Community Configuration**

| Delete | Community name | Community secret | Source IP | Source Prefix |
|---|---|---|---|---|
| ☐ | public | public | 0.0.0.0 | 0 |
| ☐ | private | private | 0.0.0.0 | 0 |

Add New Entry Save Reset

| Object | 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 mask. |
| **Source Mask** | Indicates the SNMP access source address mask. |

| Buttons | |
|---|---|
| Add New Entry | Click to add a new community entry. |
| Delete | Click to delete the entry. |
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

30W PoE Model

**SNMPv3 Community Configuration**

| Delete | Community | Source IP | Source Mask |
|---|---|---|---|
| ☐ | public | 0.0.0.0 | 0.0.0.0 |
| ☐ | private | 0.0.0.0 | 0.0.0.0 |
| Delete | | 0.0.0.0 | 0.0.0.0 |

Add New Entry Save Reset

| Object | 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 mask. |

| | |
|---|---|
| **Source Mask** | Indicates the SNMP access source address mask. |

| Buttons | |
|---|---|
| Add New Entry | Click to add a new community entry. |
| Delete | Click to delete the entry. |
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

## 2.3.30 SNMP Users

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

**SNMPv3 User Configuration**

| Delete | Engine ID | User Name | Modify Password | Security Level | Authentication Protocol | Authentication Password | Privacy Protocol | Privacy Password |
|---|---|---|---|---|---|---|---|---|
| ☐ | 800007e5017f000001 | default_user | ☐ | NoAuth, NoPriv | None | None | None | None |

Add New Entry Save Reset

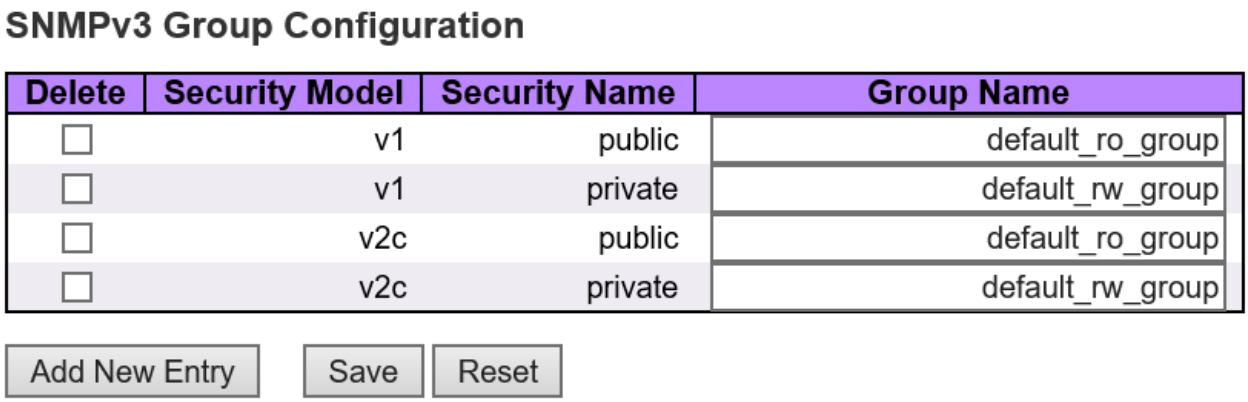
| Object | Description |
|---|---|
| **Delete** | Check to delete the entry. It will be deleted during the next save. |
| **Engine ID** | An octet string identifying the engine ID that this entry should belong to. The string must contain an even number(in hexadecimal format) with number of digits between 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. |
| **Modify Password (For** | Select this checkbox to create new entry with password. To modify password, this |

| | |
|---|---|
| **30W PoE Model)** | checkbox should be selected also, otherwise the password will not be modified. |
| **Security Level** | Indicates the security model that this entry should belong to. Possible security models are:<br>**`NoAuth, NoPriv`**: No authentication and no privacy.<br>**`Auth, NoPriv`**: Authentication and no privacy.<br>**`Auth, Priv`**: Authentication and privacy.<br>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:<br>**`None`**: No authentication protocol.<br>**`MD5`**: An optional flag to indicate that this user uses MD5 authentication protocol.<br>**`SHA`**: An optional flag to indicate that this user uses SHA authentication protocol.<br>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:<br>**`None`**: No privacy protocol.<br>**`DES`**: An optional flag to indicate that this user uses DES authentication protocol.<br>**`AES`**: An optional flag to indicate that this user uses AES authentication protocol. |
| **Privacy Password** | A string identifying the privacy password phrase. The allowed string length is 8 to 32, and the allowed content is ASCII characters from 33 to 126. |

| **Buttons** | |
|---|---|
| Add New Entry | Click to add a new user entry. |
| Delete | Click to delete the entry. |
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

## 2.3.31 SNMP Groups

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

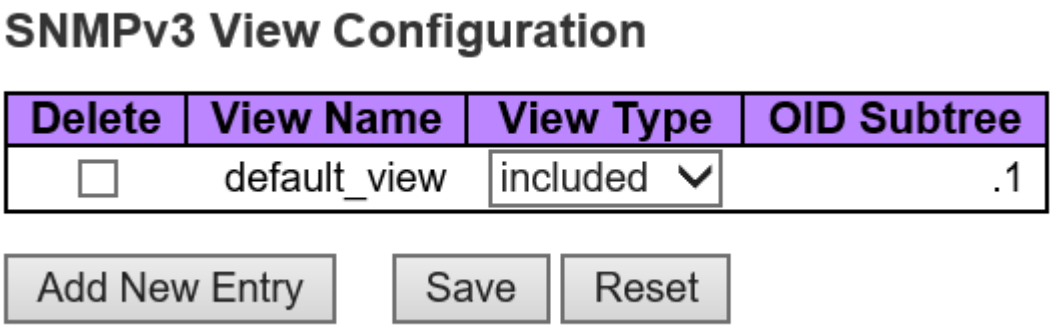



| Object | Description |
|---|---|
| **Delete** | Check to delete the entry. It will be deleted during the next save. |
| **Security Model** | Indicates the security model that this entry should belong to. Possible security models are:<br>`v1`: Reserved for SNMPv1.<br>`v2c`: Reserved for SNMPv2c.<br>`usm`: User-based Security Model (USM). |
| **Security Name** | A string identifying the security name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126. |
| **Group Name** | A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126. |

| Buttons | |
|---|---|
| Add New Entry | Click to add a new group entry |
| Delete | Click to delete the entry. |
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

## 2.3.32 SNMP Views

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




| Object | 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:<br>`included`: An optional flag to indicate that this view subtree should be included.<br>`excluded`: An optional flag to indicate that this view subtree should be excluded.<br>In general, if a view entry's view type is 'excluded', there should be another view entry existing with view type as 'included' and it's OID subtree should overstep the 'excluded' view entry. |
| **OID Subtree** | The OID defining the root of the subtree to add to the named view. The allowed OID length is 1 to 128. The allowed string content is digital number or asterisk(*). |

| Buttons | |
|---|---|
| Add New Entry | Click to add a new view entry. |
| Delete | Click to delete the entry. |
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

## 2.3.33 SNMP Access

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

**SNMPv3 Access Configuration**

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

Add New Entry | Save | Reset

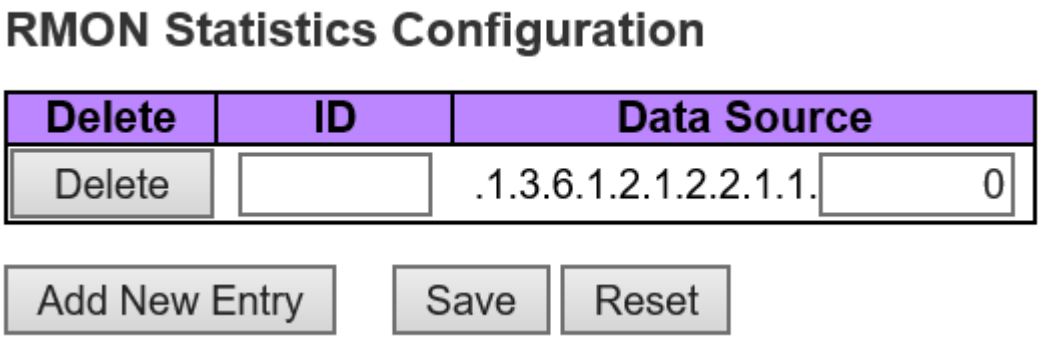
| Object | Description |
|---|---|
| **Delete** | Check to delete the entry. It will be deleted during the next save. |
| **Group Name** | A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to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

| Buttons | |
|---|---|
| Add New Entry | Click to add a new access entry. |

| | |
|---|---|
| Delete | Click to delete the entry. |
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

## 2.3.34 RMON Statistics

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

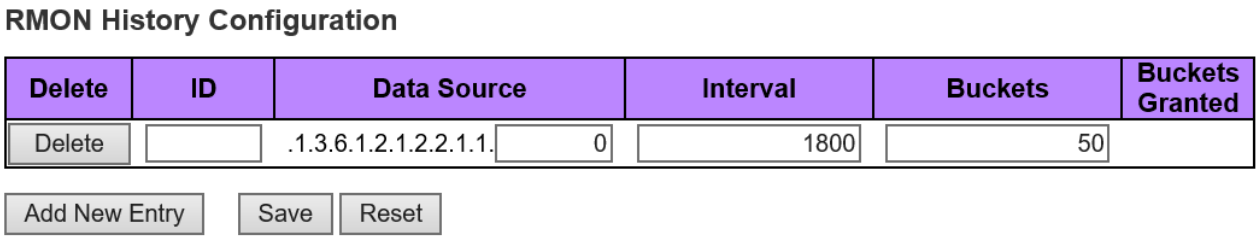



| Object | Description |
|---|---|
| **Delete** | Check to delete the entry. It will be deleted during the next save. |
| **ID** | Indicates the index of the entry. The range is from 1 to 65535. |
| **Data Source** | Indicates the port ID which wants to be monitored. If in stacking switch, the value must add 1000000*(switch ID), for example, if the port is switch 3 port 5, the value is 3000005. |

| Buttons | |
|---|---|
| Add New Entry | Click to add a new community entry. |
| Delete | Click to delete the entry. |
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

## 2.3.35 RMON History

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

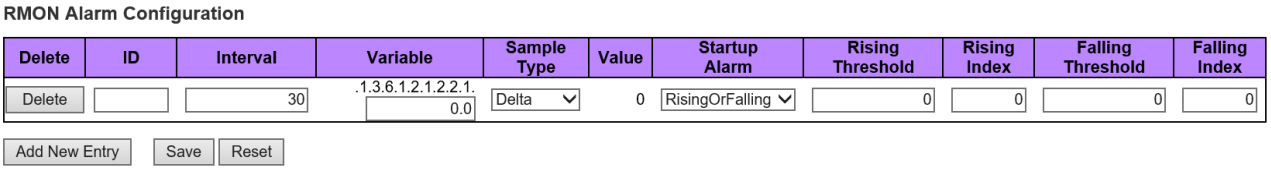



| Object | Description |
|---|---|
| **Delete** | Check to delete the entry. It will be deleted during the next save. |
| **ID** | Indicates the index of the entry. The range is from 1 to 65535. |
| **Data Source** | Indicates the port ID which wants to be monitored. If in stacking switch, the value must add 1000000*(switch ID), for example, if the port is switch 3 port 5, the value is 3000005. |
| **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 (For 90W PoE Model)** | Indicates the maximum data entries associated this History control entry stored in RMON. The range is from 1 to 65535, default value is 50. |
| **Buckets (For 30W PoE Model)** | Indicates the maximum data entries associated this History control entry stored in RMON. The range is from 1 to 3600, default value is 50. |
| **Buckets Granted** | The number of data shall be saved in the RMON. |

| Buttons | |
|---|---|
| Add New Entry | Click to add a new community entry. |
| Delete | Click to delete the entry. |
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

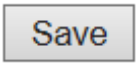
## 2.3.36 RMON Alarm

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



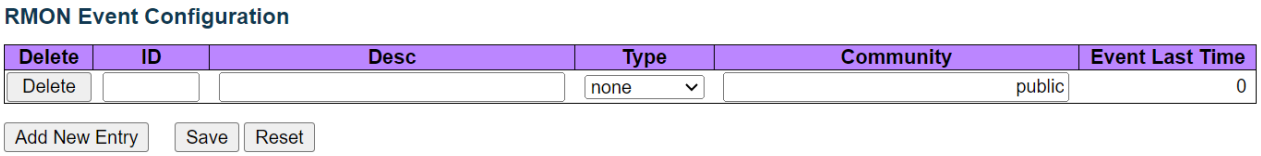

| Object | Description |
|---|---|
| **Delete** | Check to delete the entry. It will be deleted during the next save. |
| **ID** | Indicates the index of the entry. The range is from 1 to 65535 |
| **Interval** | Indicates the interval in seconds for sampling and comparing the rising and falling threshold. The range is from 1 to 2^31-1. |
| **Variable** | Indicates the particular variable to be sampled, the possible variables are:<br>`InOctets`: The total number of octets received on the interface, including framing characters.<br>`InUcastPkts:` The number of uni-cast packets delivered to a higher-layer protocol.<br>`InNUcastPkts`: The number of broad-cast and multi-cast packets delivered to a higher-layer protocol.<br>`InDiscards`: The number of inbound packets that are discarded even the packets are normal.<br>`InErrors`: The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.<br>`InUnknownProtos`: the number of the inbound packets that were discarded because of the unknown or un-support protocol.<br>`OutOctets`: The number of octets transmitted out of the interface , including framing characters.<br>`OutUcastPkts`: The number of uni-cast packets that request to transmit.<br>`OutNUcastPkts`: The number of broad-cast and multi-cast packets that request to transmit.<br>`OutDiscards`: The number of outbound packets that are discarded event the packets is normal.<br>`OutErrors`: The number of outbound packets that could not be transmitted because of errors.<br>`OutQLen`: The length of the output packet queue (in packets).<br>Example: xx.ifIndex, where the xx range 10~21 indicates the InOctets~OutQLen, |

| | |
|---|---|
| | ifIndex starts with 1000001~(1000000+portNum). |
| **Sample Type** | The method of sampling the selected variable and calculating the value to be compared against the thresholds, possible sample types are:<br>**`Absolute`**: Get the sample directly.<br>**`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:<br>**`Rising`**Trigger alarm when the first value is larger than the rising threshold.<br>**`Falling`**Trigger alarm when the first value is less than the falling threshold.<br>**`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 (For 90W PoE Model)** | Rising event index (0-65535). If this value is zero, no associated event will be generated, as zero is not a valid event index. |
| **Rising Index (For 30W PoE Model)** | Rising event index (1-65535). |
| **Falling Threshold** | Falling threshold value (-2147483648-2147483647) |
| **Falling Index (For 90W PoE Model)** | Falling event index (0-65535). If this value is zero, no associated event will be generated, as zero is not a valid event index. |
| **Falling Index (For 30W PoE Model)** | Falling event index (1-65535). |

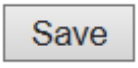
| **Buttons** | |
|---|---|
|  | Click to add a new community entry. |
|  | Click to delete the entry. |
|  | Click to save changes. |
|  | Click to undo any changes made locally and revert to previously saved values. |

## 2.3.37 RMON Event

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




| Object | 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:<br>`none`: No SNMP log is created, no SNMP trap is sent.<br>`log`: Create SNMP log entry when the event is triggered.<br>`snmptrap`: Send SNMP trap when the event is triggered.<br>`logandtrap`: Create SNMP log entry and sent SNMP trap when the event is triggered. |
| **Community (For 30W PoE Model)** | Specify the community when trap is sent, the string length is from 0 to 127, default is "public". |
| **Event Last Time** | Indicates the value of sysUpTime at the time this event entry last generated an event. |

| Buttons | |
|---|---|
|  | Click to add a new community entry. |
|  | Click to delete the entry. |
|  | Click to save changes. |
|  | Click to undo any changes made locally and revert to previously saved values. |

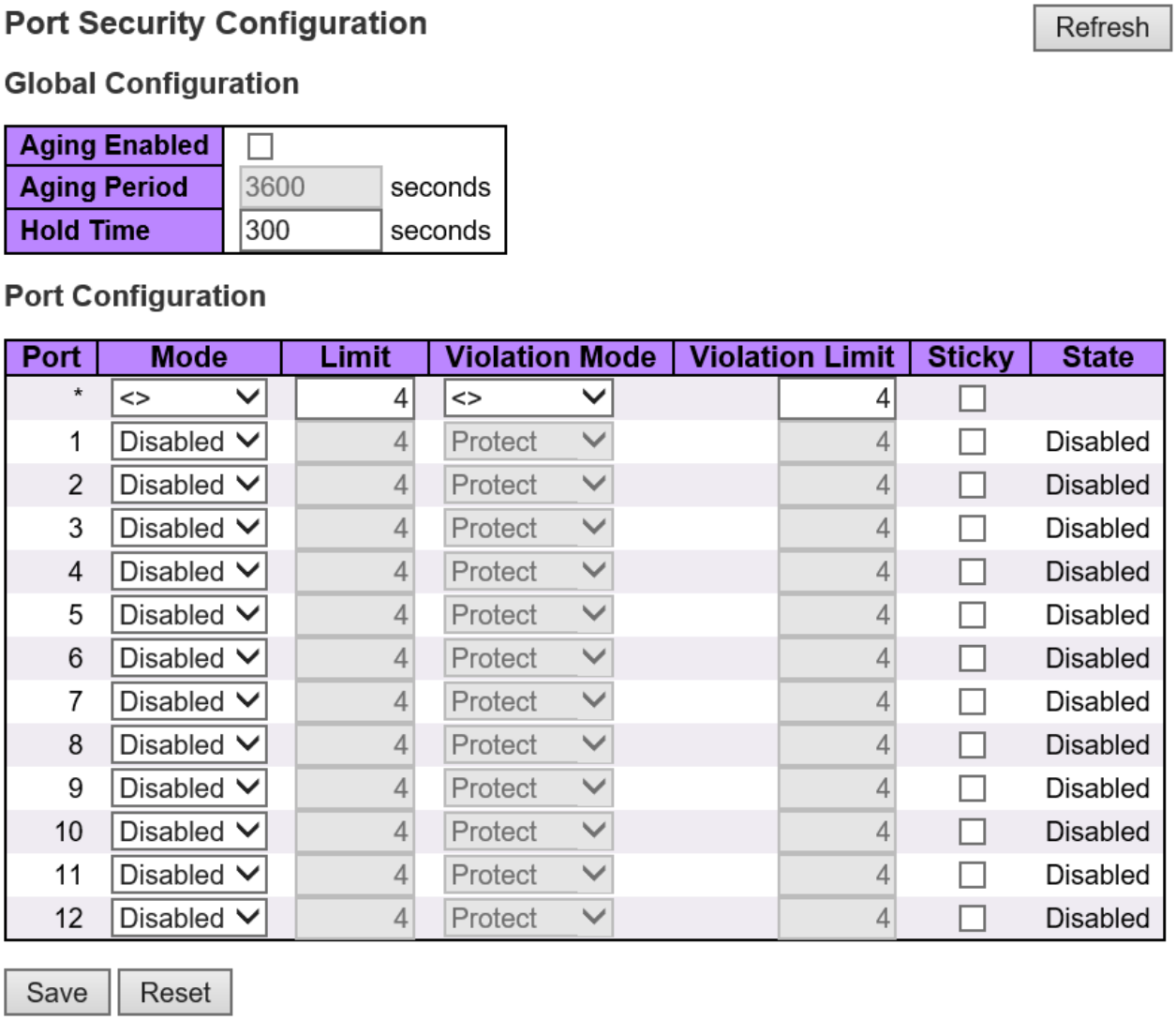
## 2.3.38 Port Security Configuration

This page 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 four different described below.

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

90W PoE Model




| Object | Description |
|---|---|
| Global Configuration | |
| **Aging Enabled** | If checked, secured MAC addresses are subject to aging as discussed under Aging |

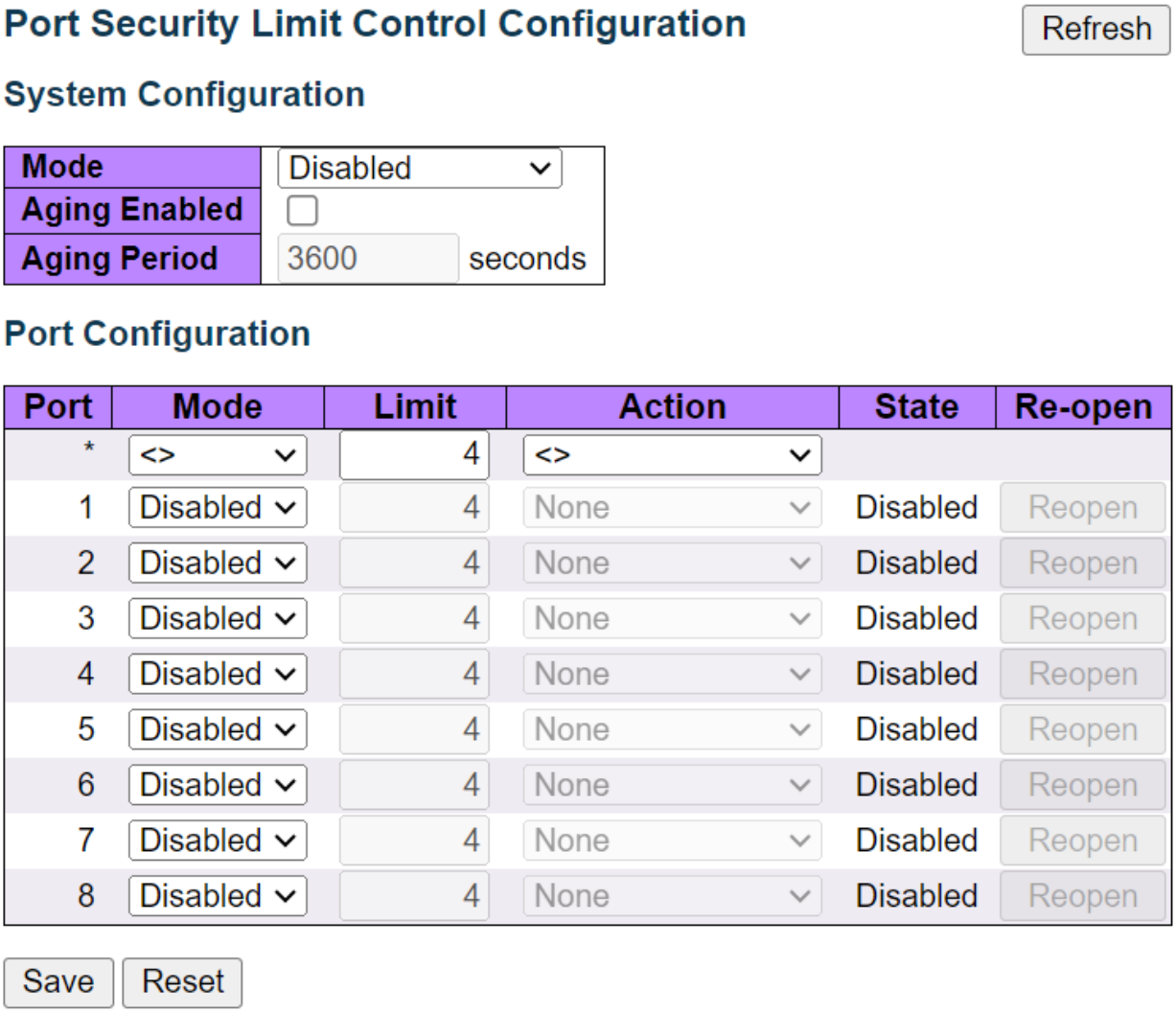
| | |
|---|---|
| | Period . |
| **Aging Period** | If Aging Enabled is checked, then the aging period is controlled with this input. If other modules are using the underlying port security for securing MAC addresses, they may have other requirements to the aging period. The underlying port security will use the shorter requested aging period of all modules that use the functionality.<br>The Aging Period can be set to a number between 10 and 10,000,000 seconds.<br>To understand why aging may be desired, consider the following scenario: Suppose an end-host is connected to a 3rd party switch or hub, which in turn is connected to a port on this switch on which Limit Control is enabled. The end-host will be allowed to forward if the limit is not exceeded. Now suppose that the end-host logs off or powers down. If it wasn't for aging, the end-host would still take up resources on this switch and will be allowed to forward. To overcome this situation, enable aging. With aging enabled, a timer is started once the end-host gets secured. When the timer expires, the switch starts looking for frames from the end-host, and if such frames are not seen within the next Aging Period, the end-host is assumed to be disconnected, and the corresponding resources are freed on the switch. |
| **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.<br>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** | |
| **Port** | The port number to which the configuration below applies. |
| **Mode** | Controls whether Limit Control is enabled on this port. Both this and the Global Mode must be set to Enabled for Limit Control to be in effect. Notice that other modules may still use the underlying port security features without enabling Limit Control on a given port. |
| **Limit** | The maximum number of MAC addresses that can be secured on this port. This number cannot exceed 1023. Default is 4. If the limit is exceeded, an action is taken corresponding to the violation mode.<br>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. |
| **Violation Mode** | If Limit is reached, the switch can take one of the following actions:<br>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 addresses 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.<br>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:<br>1) In the "Configuration→Ports" page's "Configured" column, first disable the port, then restore the original mode.<br>2) Make a Port Security configuration change on the port.<br>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. |
| **Sticky** | Enables sticky learning of MAC addresses on this port. When the port is in sticky mode, all MAC addresses that would otherwise have been learned as dynamic are learned as sticky.<br>Sticky MAC addresses are part of the running-config and can therefore be saved to startup-config. Sticky MAC addresses survive link changes (in contrast to Dynamic, which will have to be learned again). They also survive reboots if running-config is saved to startup-config.<br>A port can be Sticky-enabled whether or not Port Security is enabled on that interface. In that way, it is possible to add sticky MAC addresses managementwise before enabling Port Security. To do that, use the "Configuration→Security→Port Security→MAC Addresses" page. |
| **State** | This column shows the current Port Security state of the port. The state takes one of four values:<br>Disabled: Port Security is disabled on the port.<br>Ready: The limit is not yet reached. This can be shown for all violation modes.<br>Limit Reached: Indicates that the limit is reached on this port. This can be shown for all violation modes.<br>Shutdown: Indicates that the port is shut down by Port Security. This state can only be shown if violation mode is set to Shutdown. |

| **Buttons** | |
|---|---|
| Refresh | Click to refresh the page. Note that non-committed changes will be lost. |

| | |
|---|---|
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

30W PoE Model




| Object | Description |
|---|---|
| System Configuration | |
| **Mode** | Indicates if Limit Control is globally enabled or disabled on the switch. If globally disabled, other modules may still use the underlying functionality, but limit checks and corresponding actions are disabled. |
| **Aging Enabled** | If checked, secured MAC addresses are subject to aging as discussed under Aging Period . |
| **Aging Period** | If Aging Enabled is checked, then the aging period is controlled with this input. If other modules are using the underlying port security for securing MAC addresses, |

| | |
|---|---|
| | they may have other requirements to the aging period. The underlying port security will use the shorter requested aging period of all modules that use the functionality. The Aging Period can be set to a number between 10 and 10,000,000 seconds.<br>To understand why aging may be desired, consider the following scenario: Suppose an end-host is connected to a 3rd party switch or hub, which in turn is connected to a port on this switch on which Limit Control is enabled. The end-host will be allowed to forward if the limit is not exceeded. Now suppose that the end-host logs off or powers down. If it wasn't for aging, the end-host would still take up resources on this switch and will be allowed to forward. To overcome this situation, enable aging. With aging enabled, a timer is started once the end-host gets secured. When the timer expires, the switch starts looking for frames from the end-host, and if such frames are not seen within the next Aging Period, the end-host is assumed to be disconnected, and the corresponding resources are freed on the switch. |
| **Port Configuration** | |
| **Port** | The port number to which the configuration below applies. |
| **Mode** | Controls whether Limit Control is enabled on this port. Both this and the Global Mode must be set to Enabled for Limit Control to be in effect. Notice that other modules may still use the underlying port security features without enabling Limit Control on a given port. |
| **Limit** | The maximum number of MAC addresses that can be secured on this port. This number cannot exceed 1024. If the limit is exceeded, the corresponding action is taken.<br>The switch is "born" with a total number of MAC addresses from which all ports draw whenever a new MAC address is seen on a Port Security-enabled port. Since all ports draw from the same pool, it may happen that a configured maximum cannot be granted, if the remaining ports have already used all available MAC addresses. |
| **Action** | If Limit is reached, the switch can take one of the following actions:<br>None: Do not allow more than Limit MAC addresses on the port, but take no further action.<br>Trap: If Limit + 1 MAC addresses is seen on the port, send an SNMP trap. If Aging is disabled, only one SNMP trap will be sent, but with Aging enabled, new SNMP traps will be sent every time the limit gets exceeded.<br>Shutdown: If Limit + 1 MAC addresses is seen on the port, shut down the port. This implies that all secured MAC addresses will be removed from the port, and no new address will be learned. Even if the link is physically disconnected and reconnected on the port (by disconnecting the cable), the port will remain shut down. There are three ways to re-open the port:<br>1) Boot the switch, |

| | |
|---|---|
| | 2) Disable and re-enable Limit Control on the port or the switch,<br>3) Click the Reopen button.<br>Trap & Shutdown: If Limit + 1 MAC addresses is seen on the port, both the "Trap" |
| **State** | This column shows the current state of the port as seen from the Limit Control's point of view. The state takes one of four values:<br>Disabled: Limit Control is either globally disabled or disabled on the port.<br>Ready: The limit is not yet reached. This can be shown for all actions.<br>Limit Reached: Indicates that the limit is reached on this port. This state can only be shown if Action is set to None or Trap.<br>Shutdown: Indicates that the port is shut down by the Limit Control module. This state can only be shown if Action is set to Shutdown or Trap & Shutdown. |
| **Re-open Button** | If a port is shutdown by this module, you may reopen it by clicking this button, which will only be enabled if this is the case. For other methods, refer to Shutdown in the Action section.<br>Note that clicking the reopen button causes the page to be refreshed, so non-committed changes will be lost. |

| **Buttons** | |
|---|---|
| Refresh | Click to refresh the page. Note that non-committed changes will be lost. |
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

## 2.3.39 Port Security MAC Addresses (For 90W PoE Model)

On this page, you may add and delete static and sticky MAC addresses managed by Port Security.

Port security defines three types of MAC addresses, of which static and sticky can be added and removed on this page: • Dynamic: A MAC address learned through learn frames coming to the Port Security module while the interface in question is not in sticky mode. Dynamic entries disappear if it ages out or if the interface link goes down.

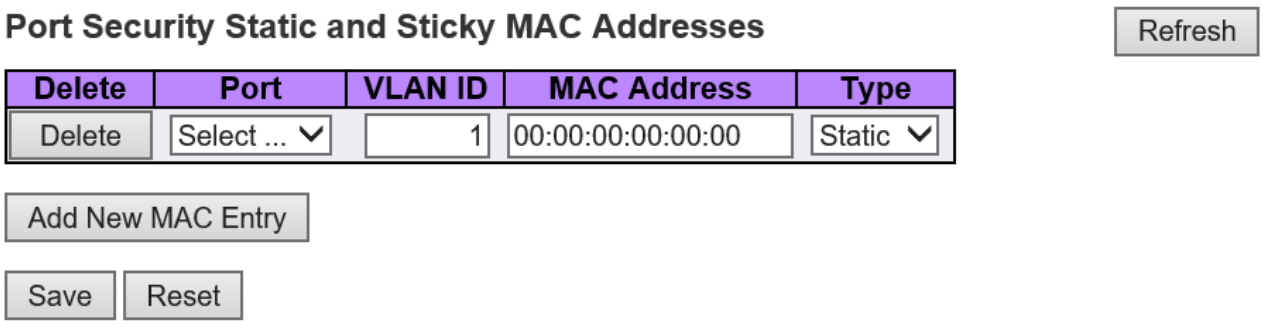
- Static: A MAC address added by end-user through management. Static MAC addresses are not subject to aging and will be added to the MAC address table once Port Security gets enabled on the interface.

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

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

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

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




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

| | |
|---|---|
| **Port** | The port number to which this MAC address is bound. |
| **VLAN ID & MAC Address** | The VLAN ID and MAC address in question. |
| **Type** | Indicates the type of entry and may be either Static or Sticky (see description above). |

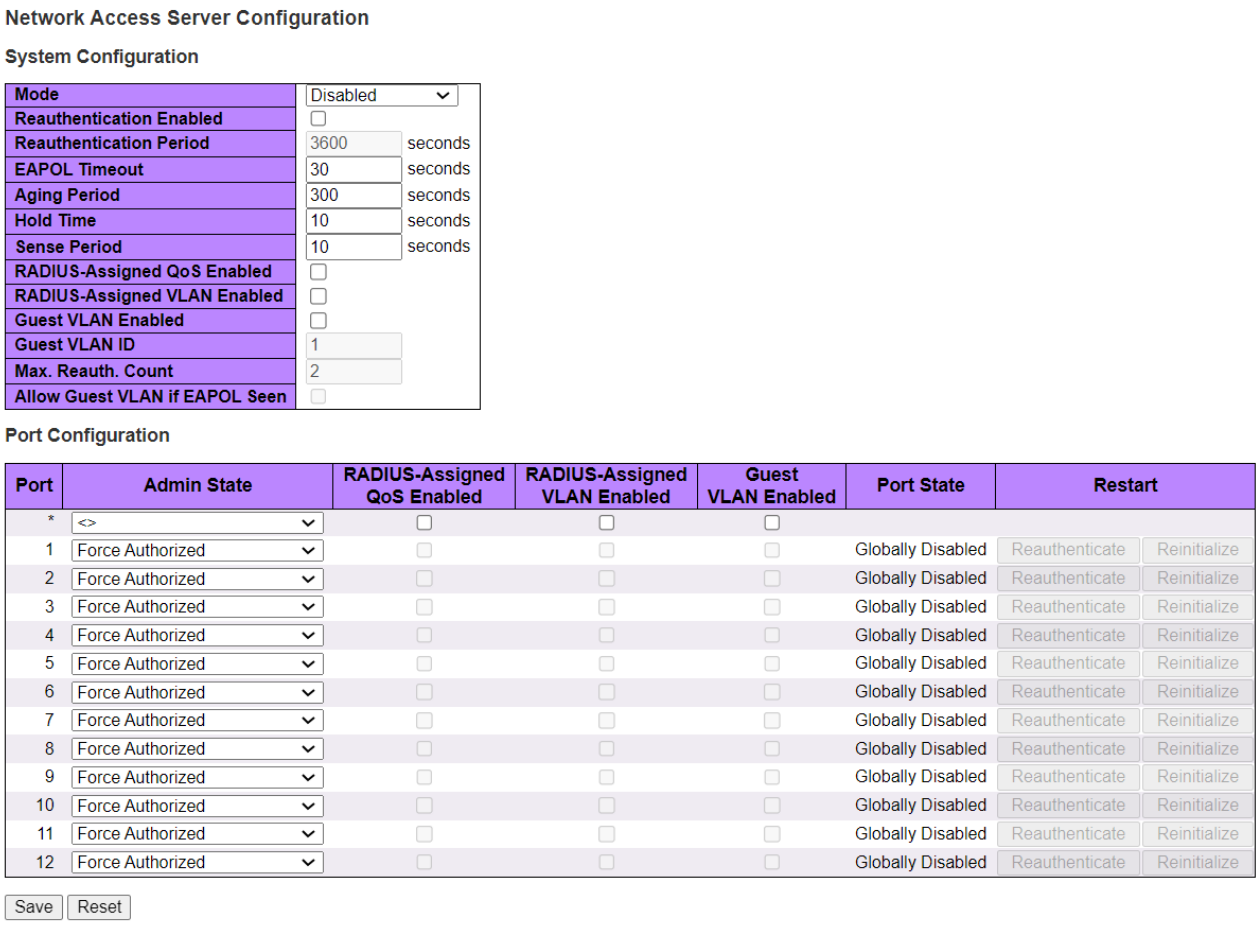
| **Buttons** | |
|---|---|
| Add New MAC Entry : | Clicking this button will add a new row to the table. This new row allows for adding a static or sticky MAC address to a particular interface. Once satisfied, click the Save-button to save the changes to running-config.<br>Notice that sticky entries are normally added automatically through learning on the interface. |
| Refresh | Click to refresh the page. Note that non-committed changes will be lost. |
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

## 2.3.40 NAS

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.




| Object | Description |
|---|---|
| **System Configuration** | |
| **Mode** | Indicates if NAS is globally enabled or disabled on the switch. If globally disabled, all ports are allowed forwarding of frames. |
| **Reauthentication Enabled** | If checked, successfully authenticated supplicants/clients are reauthenticated after the interval specified by the Reauthentication Period. Reauthentication for 802.1X-enabled ports can be used to detect if a new device is plugged into a switch port or if a supplicant is no longer attached.<br>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.<br>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:<br>• Single 802.1X<br>• Multi 802.1X<br>• MAC-Based Auth.<br>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.<br>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.<br>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:<br>• Single 802.1X<br>• Multi 802.1X<br>• MAC-Based Auth.<br>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.<br>In MAC-based Auth. mode, the switch will ignore new frames coming from the client during the hold time.<br>The Hold Time can be set to a number between 10 and 1000000 seconds. |
| **Sense Period** | This period time for a port in 802.1X or MAC-based Auth. sense mode to sense 802.1X EAPOL packet, if sensing any EAPOL packet passthrough the port then stays in Port-based 802.1X authentication, otherwise will go to MAC-based authentication, until the port Down will reset the port control mode back to Port-based 802.1X authentication then re-sense again.<br>The Sense Period can be set to a number between 10 and 255 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).<br>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).<br>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.<br>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.<br>Guest VLAN will enabled until global config "Max. Reauth. Count" * "EAPOL Timeout" timeout in seconds.<br>When in 802.1X or MAC-based Auth. sense, if the Guest VLAN timeout is more than Sense Period, the port control will change to MAC-based authentication before Guest VLAN enable timeout. |
| **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.<br>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.<br>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.<br>The value can only be changed if the Guest VLAN option is globally enabled. |
| **Port Configuration** | |
| **Port** | The port number for which the configuration below applies. |
| **Admin State** | If NAS is globally enabled, this selection controls the port's authentication mode. The following modes are available:<br><br>Force Authorized<br>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.<br><br>Force Unauthorized<br>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.<br><br>Port-based 802.1X<br>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 |

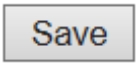
| | |
|---|---|
| | encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it.<br>When authentication is complete, the RADIUS server sends a special packet containing a success or failure indication. Besides forwarding this decision to the supplicant, the switch uses it to open up or block traffic on the switch port connected to the supplicant.<br>**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.<br><br>Single 802.1X<br>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.<br>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.<br><br>Multi 802.1X<br>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.<br>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.<br>The maximum number of supplicants that can be attached to a port can be limited using the Port Security Limit Control functionality.<br><br>MAC-based Auth<br>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.<br>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.<br>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. |

| | |
|---|---|
| | 802.1X or MAC-based Auth. sense<br>This mode is sense 802.1X BPDU packet in period time when port is link up, if timeout the port will go to MAC-based authentication. |
| **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).<br>This option is only available for single-client modes, i.e.<br>• Port-based 802.1X<br>• Single 802.1X<br><br>**RADIUS attributes used in identifying a QoS Class:**<br>The User-Priority-Table attribute defined in RFC4675 forms the basis for identifying the QoS Class in an Access-Accept packet.<br>Only the first occurrence of the attribute in the packet will be considered, and to be valid, it must follow this rule:<br>• 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.<br>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).<br>This option is only available for single-client modes, i.e.<br>• Port-based 802.1X |

| | |
|---|---|
| | • Single 802.1X<br>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.<br><br>**RADIUS attributes used in identifying a VLAN ID:**<br>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:<br>• The Tunnel-Medium-Type, Tunnel-Type, and Tunnel-Private-Group-ID attributes must all be present at least once in the Access-Accept packet.<br>• The switch looks for the first set of these attributes that have the same Tag value and fulfil the following requirements (if Tag == 0 is used, the Tunnel-Private-Group-ID does not need to include a Tag):<br>- Value of Tunnel-Medium-Type must be set to "IEEE-802" (ordinal 6).<br>- Value of Tunnel-Type must be set to "VLAN" (ordinal 13).<br>- 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.<br>This option is only available for EAPOL-based modes, i.e.:<br>• Port-based 802.1X<br>• Single 802.1X<br>• Multi 802.1X<br>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.<br><br>**Guest VLAN Operation:**<br>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.<br>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:<br>**Globally Disabled:** NAS is globally disabled.<br>**Link Down:** NAS is globally enabled, but there is no link on the port.<br>**Authorized:** The port is in Force Authorized or a single-supplicant mode and the supplicant is authorized.<br>**Unauthorized:** The port is in Force Unauthorized or a single-supplicant mode and the supplicant is not successfully authorized by the RADIUS server.<br>**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.<br>Clicking these buttons will not cause settings changed on the page to take effect.<br>**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.<br>The button only has effect for successfully authenticated clients on the port and will not cause the clients to get temporarily unauthorized.<br>**Reinitialize:** Forces a reinitialization of the clients on the port and thereby a reauthentication immediately. The clients will transfer to the unauthorized state while the reauthentication is in progress. |

| Buttons | |
|---|---|
|  | Click to refresh the page. Note that non-committed changes will be lost. |
|  | Click to save changes. |

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

## 2.3.41 ACL Port

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.


| Object | Description |
|---|---|
| **Port** | The logical port for the settings contained in the same row. |
| **Policy ID** | Select the policy to apply to this port. The allowed values are `0` through `255`. The default value is 0. |
| **Action** | Select whether forwarding is permitted ("Permit") or denied ("Deny"). The default value is "Permit". |
| **Rate Limiter ID** | Select which rate limiter to apply on this port. The allowed values are `Disabled` or the values `1` through `16`. The default value is "Disabled". |
| **Port Redirect** | Select which port frames are redirected on. The allowed values are `Disabled` or a |

| | |
|---|---|
| | specific port number and it can't be set when action is permitted. The default value is "Disabled". |
| **Mirror** | Specify the mirror operation of this port. The allowed values are:<br>**`Enabled`**: Frames received on the port are mirrored.<br>**`Disabled`**: Frames received on the port are not mirrored.<br>The default value is "Disabled". |
| **Loggig** | Specify the logging operation of this port. Notice that the logging message doesn't include the 4 bytes CRC. The allowed values are:<br>**`Enabled`**: Frames received on the port are stored in the System Log.<br>**`Disabled`**: Frames received on the port are not logged.<br>The default value is "Disabled". Note: The logging feature only works when the packet length is less than 1518(without VLAN tags) and the System Log memory size and logging rate is limited. |
| **Shutdown** | Specify the port shut down operation of this port. The allowed values are:<br>**`Enabled`**: If a frame is received on the port, the port will be disabled.<br>**`Disabled`**: Port shut down is disabled.<br>The default value is "Disabled".<br>Note: The shutdown feature only works when the packet length is less than 1518(without VLAN tags). |
| **State** | Specify the port state of this port. The allowed values are:<br>**`Enabled`**: To reopen ports by changing the volatile port configuration of the ACL user module.<br>**`Disabled`**: To close ports by changing the volatile port configuration of the ACL user module.<br>The default value is "Enabled". |
| **Counter** | Counts the number of frames that match this ACE. |

| **Buttons** | |
|---|---|
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |
| Refresh | Click to refresh the page; any changes made locally will be undone. |
| Clear | Click to clear the counters. |

## 2.3.42 ACL Rate Limiters

Configure the rate limiter for the ACL of the switch.

**ACL Rate Limiter Configuration**

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

Save Reset

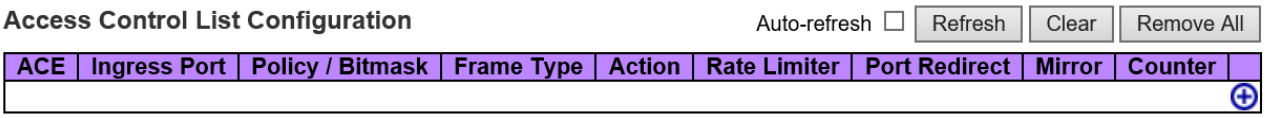
| Object | Description |
|---|---|
| **Rate Limiter ID** | The rate limiter ID for the settings contained in the same row. |
| **Rate (For 90W PoE Model)** | The valid rate is `0, 10, 20, 30, ..., 5000000` in pps<br>or `0, 25, 50, 75, ..., 10000000` in kbps. |
| **Rate (For 30W PoE Model)** | The valid rate is 0-3276700 in pps.<br>or 0, 100, 200, 300, ..., 1000000 in kbps. |
| **Unit** | Specify the rate unit. The allowed values are:<br>`pps`: packets per second.<br>`kbps`: Kbits per second. |

| Buttons |
|---|

| | |
|---|---|
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

## 2.3.43 Access Control List

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.

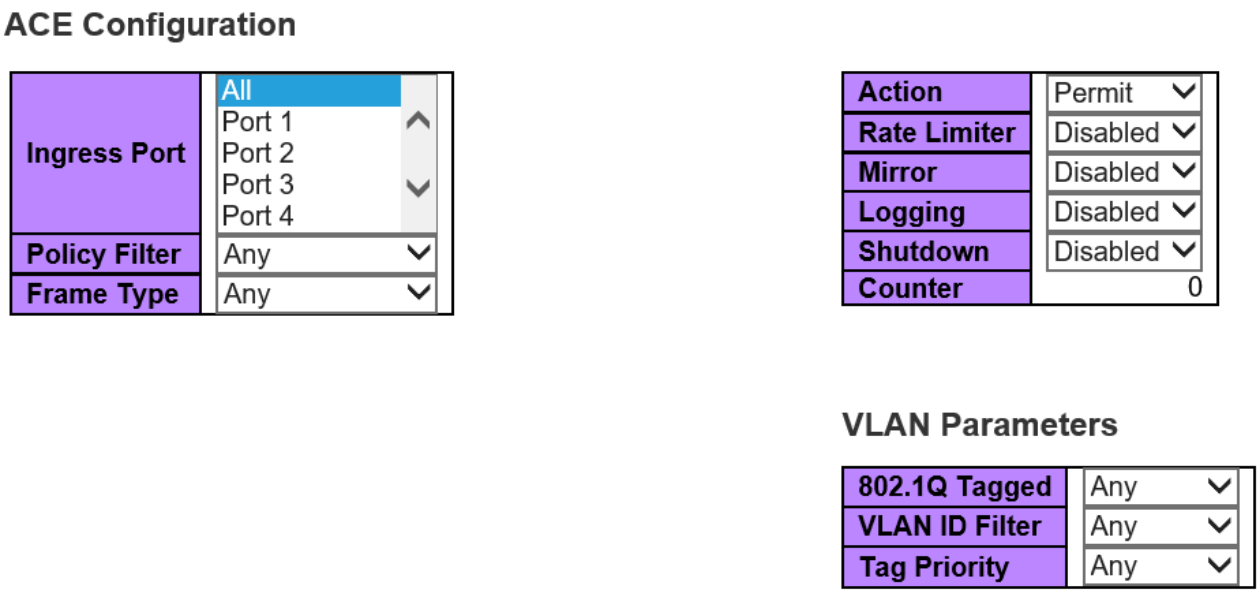



| Object | Description |
|---|---|
| **ACE** | Indicates the ACE ID. |
| **Ingress Port** | Indicates the ingress port of the ACE. Possible values are:<br>`All`: The ACE will match all ingress port.<br>`Port`: The ACE will match a specific ingress port. |
| **Policy / Bitmask** | Indicates the policy number and bitmask of the ACE. |
| **Frame Type** | Indicates the frame type of the ACE. Possible values are:<br>`Any`: The ACE will match any frame type.<br>`EType`: The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames.<br>`ARP`: The ACE will match ARP/RARP frames.<br>`IPv4`: The ACE will match all IPv4 frames.<br>`IPv4/ICMP`: The ACE will match IPv4 frames with ICMP protocol.<br>`IPv4/UDP`: The ACE will match IPv4 frames with UDP protocol.<br>`IPv4/TCP`: The ACE will match IPv4 frames with TCP protocol.<br>`IPv4/Other`: The ACE will match IPv4 frames, which are not ICMP/UDP/TCP.<br>`IPv6`: The ACE will match all IPv6 standard frames. |
| **Action** | Indicates the forwarding action of the ACE.<br>`Permit`: Frames matching the ACE may be forwarded and learned.<br>`Deny`: Frames matching the ACE are dropped.<br>`Filter`: Frames matching the ACE are filtered. |

| | |
|---|---|
| **Rate Limiter** | Indicates the rate limiter number of the ACE. The allowed range is `1` to `16`. When `Disabled` is displayed, the rate limiter operation is disabled. |
| **Port Redirect** | Indicates the port redirect operation of the ACE. Frames matching the ACE are redirected to the port number. The allowed values are `Disabled` or a specific port number. When `Disabled` is displayed, the port redirect operation is disabled. |
| **Mirror** | Specify the mirror operation of this port. Frames matching the ACE are mirrored to the destination mirror port. The allowed values are:<br>`Enabled`: Frames received on the port are mirrored.<br>`Disabled`: Frames received on the port are not mirrored.<br>The default value is "Disabled". |
| **Counter** | The counter indicates the number of times the ACE was hit by a frame. |
| **Modification Buttons** | You can modify each ACE (Access Control Entry) in the table using the following buttons:<br>: Inserts a new ACE before the current row.<br>: Edits the ACE row.<br>: Moves the ACE up the list.<br>: Moves the ACE down the list.<br>: Deletes the ACE.<br>: The lowest plus sign adds a new entry at the bottom of the ACE listings. |

| Buttons | |
|---|---|
| Auto-refresh ☐ | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |
| Refresh | Click to refresh the page; any changes made locally will be undone. |
| Clear | Click to clear the counters. |
| Remove All | Click to remove all ACEs. |

The ACE Configuration page includes the following fields:




| Object | Description |
|---|---|
| **Second Lookup** | Specify the second lookup operation of the ACE. |
| **Ingress Port** | Select the ingress port for which this ACE applies.<br>`All`: The ACE applies to all port.<br>`Port n`: The ACE applies to this port number, where *n* is the number of the switch port. |
| **Policy Filter** | Specify the policy number filter for this ACE.<br>`Any`: No policy filter is specified. (policy filter status is "don't-care".)<br>`Specific`: If you want to filter a specific policy with this ACE, choose this value. Two field for entering an policy value and bitmask appears. |
| **Policy Value** | When "Specific" is selected for the policy filter, you can enter a specific policy value. The allowed range is `0` to `255`. |
| **Policy Bitmask** | When "Specific" is selected for the policy filter, you can enter a specific policy bitmask. The allowed range is `0x0` to `0xff`. Notice the usage of bitmask, if the binary bit value is "0", it means this bit is "don't-care". The real matched pattern is [policy_value & policy_bitmask]. For example, if the policy value is 3 and the policy bitmask is 0000 0010 (bit 0 is "don't-care" bit), then policy 2 and 3 are applied to this rule. |
| **Frame Type** | Select the frame type for this ACE. These frame types are mutually exclusive.<br>`Any`: Any frame can match this ACE.<br>`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).<br>**ARP**: Only ARP frames can match this ACE. Notice the ARP frames won't match the ACE with ethernet type.<br>**IPv4**: Only IPv4 frames can match this ACE. Notice the IPv4 frames won't match the ACE with ethernet type.<br>**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.<br>**Permit**: The frame that hits this ACE is granted permission for the ACE operation.<br>**Deny**: The frame that hits this ACE is dropped.<br>**Filter**: Frames matching the ACE are filtered. |
| **Rate Limiter** | Specify the rate limiter in number of base units. The allowed range is **1** to **16**.<br>**Disabled** indicates that the rate limiter operation is disabled. |
| **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. |
| **Mirror** | Specify the mirror operation of this port. Frames matching the ACE are mirrored to the destination mirror port. The rate limiter will not affect frames on the mirror port. The allowed values are:<br>**Enabled**: Frames received on the port are mirrored.<br>**Disabled**: Frames received on the port are not mirrored.<br>The default value is "Disabled". |
| **Logging** | Specify the logging operation of the ACE. Notice that the logging message doesn't include the 4 bytes CRC information. The allowed values are:<br>**Enabled**: Frames matching the ACE are stored in the System Log.<br>**Disabled**: Frames matching the ACE are not logged.<br>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** | Specify the port shut down operation of the ACE. The allowed values are:<br>**Enabled**: If a frame matches the ACE, the ingress port will be disabled.<br>**Disabled**: Port shut down is disabled for the ACE.<br>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.)* |

| | |
|---|---|
| | Specify the source MAC filter for this ACE.<br>`Any`: No SMAC filter is specified. (SMAC filter status is "don't-care".)<br>`Specific`: If you want to filter a specific source MAC address with this ACE, choose this value. A field for entering an SMAC value appears. |
| **SMAC Value** | When "Specific" is selected for the SMAC filter, you can enter a specific source MAC address. The legal format is "xx-xx-xx-xx-xx-xx" or "xx.xx.xx.xx.xx.xx" or "xxxxxxxxxxxx" (x is a hexadecimal digit). A frame that hits this ACE matches this SMAC value. |
| **DMAC Filter** | Specify the destination MAC filter for this ACE.<br>`Any`: No DMAC filter is specified. (DMAC filter status is "don't-care".)<br>`MC`: Frame must be multicast.<br>`BC`: Frame must be broadcast.<br>`UC`: Frame must be unicast.<br>`Specific`: If you want to filter a specific destination MAC address with this ACE, choose this value. A field for entering a DMAC value appears. |
| **DMAC Value** | When "Specific" is selected for the DMAC filter, you can enter a specific destination MAC address. The legal format is "xx-xx-xx-xx-xx-xx" or "xx.xx.xx.xx.xx.xx" or "xxxxxxxxxxxx" (x is a hexadecimal digit). A frame that hits this ACE matches this DMAC value. |
| **VLAN Parameters** | |
| **802.1Q Tagged** | Specify whether frames can hit the action according to the 802.1Q tagged. The allowed values are:<br>`Any`: Any value is allowed ("don't-care").<br>`Enabled`: Tagged frame only.<br>`Disabled`: Untagged frame only.<br>The default value is "Any". |
| **VLAN ID Filter** | Specify the VLAN ID filter for this ACE.<br>`Any`: No VLAN ID filter is specified. (VLAN ID filter status is "don't-care".)<br>`Specific`: If you want to filter a specific VLAN ID with this ACE, choose this value. A field for entering a VLAN ID number appears. |
| **VLAN ID** | When "Specific" is selected for the VLAN ID filter, you can enter a specific VLAN ID number. The allowed range is `1` to `4095`. A frame that hits this ACE matches this VLAN ID value. |
| **Tag Priority** | Specify the tag priority for this ACE. A frame that hits this ACE matches this tag priority. The allowed number range is `0` to `7` or range `0-1`, `2-3`, `4-5`, `6-7`, `0-3` and `4-7`. The value `Any` means that no tag priority is specified (tag priority is "don't-care".) |
| **ARP Parameters** | |

| | |
|---|---|
| **ARP/RARP** | Specify the available ARP/RARP opcode (OP) flag for this ACE.<br>**Any**: No ARP/RARP OP flag is specified. (OP is "don't-care".)<br>**ARP**: Frame must have ARP opcode set to ARP.<br>**RARP**: Frame must have RARP opcode set to RARP.<br>**Other**: Frame has unknown ARP/RARP Opcode flag. |
| **Request/Reply** | Specify the available Request/Reply opcode (OP) flag for this ACE.<br>**Any**: No Request/Reply OP flag is specified. (OP is "don't-care".)<br>**Request**: Frame must have ARP Request or RARP Request OP flag set.<br>**Reply**: Frame must have ARP Reply or RARP Reply OP flag. |
| **Sender IP Filter** | Specify the sender IP filter for this ACE.<br>**Any**: No sender IP filter is specified. (Sender IP filter is "don't-care".)<br>**Host**: Sender IP filter is set to Host. Specify the sender IP address in the SIP Address field that appears.<br>**Network**: Sender IP filter is set to Network. Specify the sender IP address and sender IP mask in the SIP Address and SIP Mask fields that appear. |
| **Sender IP Address** | When "Host" or "Network" is selected for the sender IP filter, you can enter a specific sender IP address in dotted decimal notation. |
| **Sender IP Mask** | When "Network" is selected for the sender IP filter, you can enter a specific sender IP mask in dotted decimal notation. |
| **Target IP Filter** | Specify the target IP filter for this specific ACE.<br>**Any**: No target IP filter is specified. (Target IP filter is "don't-care".)<br>**Host**: Target IP filter is set to Host. Specify the target IP address in the Target IP Address field that appears.<br>**Network**: Target IP filter is set to Network. Specify the target IP address and target IP mask in the Target IP Address and Target IP Mask fields that appear. |
| **Target IP Address** | When "Host" or "Network" is selected for the target IP filter, you can enter a specific target IP address in dotted decimal notation. |
| **Target IP Mask** | When "Network" is selected for the target IP filter, you can enter a specific target IP mask in dotted decimal notation. |
| **ARP Sender MAC Match** | Specify whether frames can hit the action according to their sender hardware address field (SHA) settings.<br>**0**: ARP frames where SHA is not equal to the SMAC address.<br>**1**: ARP frames where SHA is equal to the SMAC address.<br>**Any**: Any value is allowed ("don't-care"). |
| **RARP Target MAC Match** | Specify whether frames can hit the action according to their target hardware address field (THA) settings.<br>**0**: RARP frames where THA is not equal to the target MAC address.<br>**1**: RARP frames where THA is equal to the target MAC address. |

| | |
|---|---|
| | **Any**: Any value is allowed ("don't-care"). |
| **IP/Ethernet Length** | Specify whether frames can hit the action according to their ARP/RARP hardware address length (HLN) and protocol address length (PLN) settings.<br>**0**: ARP/RARP frames where the HLN is not equal to Ethernet (0x06) or the (PLN) is not equal to IPv4 (0x04).<br>**1**: ARP/RARP frames where the HLN is equal to Ethernet (0x06) and the (PLN) is equal to IPv4 (0x04).<br>**Any**: Any value is allowed ("don't-care"). |
| **IP** | Specify whether frames can hit the action according to their ARP/RARP hardware address space (HRD) settings.<br>**0**: ARP/RARP frames where the HLD is not equal to Ethernet (1).<br>**1**: ARP/RARP frames where the HLD is equal to Ethernet (1).<br>**Any**: Any value is allowed ("don't-care"). |
| **Ethernet** | Specify whether frames can hit the action according to their ARP/RARP protocol address space (PRO) settings.<br>**0**: ARP/RARP frames where the PRO is not equal to IP (0x800).<br>**1**: ARP/RARP frames where the PRO is equal to IP (0x800).<br>**Any**: Any value is allowed ("don't-care"). |
| **IP Parameters** | |
| **IP Protocol Filter** | Specify the IP protocol filter for this ACE.<br>**Any**: No IP protocol filter is specified ("don't-care").<br>**Specific**: If you want to filter a specific IP protocol filter with this ACE, choose this value. A field for entering an IP protocol filter appears.<br>**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.<br>**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.<br>**TCP**: Select TCP to filter IPv4 TCP protocol frames. Extra fields for defining TCP parameters will appear. These fields are explained later in this help file. |
| **IP Protocol Value** | When "Specific" is selected for the IP protocol value, you can enter a specific value. The allowed range is **0** to **255**. A frame that hits this ACE matches this IP protocol value. |
| **IP TTL** | Specify the Time-to-Live settings for this ACE.<br>**zero**: IPv4 frames with a Time-to-Live field greater than zero must not be able to match this entry.<br>**non-zero**: IPv4 frames with a Time-to-Live field greater than zero must be able to match this entry.<br>**Any**: Any value is allowed ("don't-care"). |

| | |
|---|---|
| **IP Fragment** | Specify the fragment offset settings for this ACE. This involves the settings for the More Fragments (MF) bit and the Fragment Offset (FRAG OFFSET) field for an IPv4 frame.<br>**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.<br>**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.<br>**Any**: Any value is allowed ("don't-care"). |
| **IP Option** | Specify the options flag setting for this ACE.<br>**No**: IPv4 frames where the options flag is set must not be able to match this entry.<br>**Yes**: IPv4 frames where the options flag is set must be able to match this entry.<br>**Any**: Any value is allowed ("don't-care"). |
| **SIP Filter** | Specify the source IP filter for this ACE.<br>**Any**: No source IP filter is specified. (Source IP filter is "don't-care".)<br>**Host**: Source IP filter is set to Host. Specify the source IP address in the SIP Address field that appears.<br>**Network**: Source IP filter is set to Network. Specify the source IP address and source IP mask in the SIP Address and SIP Mask fields that appear. |
| **SIP Address** | When "Host" or "Network" is selected for the source IP filter, you can enter a specific SIP address in dotted decimal notation. |
| **SIP Mask** | When "Network" is selected for the source IP filter, you can enter a specific SIP mask in dotted decimal notation. |
| **DIP Filter** | Specify the destination IP filter for this ACE.<br>**Any**: No destination IP filter is specified. (Destination IP filter is "don't-care".)<br>**Host**: Destination IP filter is set to Host. Specify the destination IP address in the DIP Address field that appears.<br>**Network**: Destination IP filter is set to Network. Specify the destination IP address and destination IP mask in the DIP Address and DIP Mask fields that appear. |
| **DIP Address** | When "Host" or "Network" is selected for the destination IP filter, you can enter a specific DIP address in dotted decimal notation. |
| **DIP Mask** | When "Network" is selected for the destination IP filter, you can enter a specific DIP mask in dotted decimal notation. |
| **IPv6 Parameters** | |
| **Next Header Filter** | Specify the IPv6 next header filter for this ACE.<br>**Any**: No IPv6 next header filter is specified ("don't-care").<br>**Specific**: If you want to filter a specific IPv6 next header filter with this ACE, choose this value. A field for entering an IPv6 next header filter appears.<br>**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.<br>**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.<br>**TCP**: Select TCP to filter IPv6 TCP protocol frames. Extra fields for defining TCP parameters will appear. These fields are explained later in this help file. |
| **Next Header Value** | When "Specific" is selected for the IPv6 next header value, you can enter a specific value. The allowed range is **0** to **255**. A frame that hits this ACE matches this IPv6 protocol value. |
| **SIP Filter** | Specify the source IPv6 filter for this ACE.<br>**Any**: No source IPv6 filter is specified. (Source IPv6 filter is "don't-care".)<br>**Specific**: Source IPv6 filter is set to Network. Specify the source IPv6 address and source IPv6 mask in the SIP Address fields that appear. |
| **SIP address** | When "Specific" is selected for the source IPv6 filter, you can enter a specific SIPv6 address. The field only supported last 32 bits for IPv6 address. |
| **SIP BitMask** | When "Specific" is selected for the source IPv6 filter, you can enter a specific SIPv6 mask. The field only supported last 32 bits for IPv6 address. Notice the usage of bitmask, if the binary bit value is "0", it means this bit is "don't-care". The real matched pattern is [sipv6_address & sipv6_bitmask] (last 32 bits). For example, if the SIPv6 address is 2001::3 and the SIPv6 bitmask is 0xFFFFFFFE(bit 0 is "don't-care" bit), then SIPv6 address 2001::2 and 2001::3 are applied to this rule. |
| **Hop Limit** | Specify the hop limit settings for this ACE.<br>**zero**: IPv6 frames with a hop limit field greater than zero must not be able to match this entry.<br>**non-zero**: IPv6 frames with a hop limit field greater than zero must be able to match this entry.<br>**Any**: Any value is allowed ("don't-care"). |
| **ICMP Parameters** | |
| **ICMP Type Filter** | Specify the ICMP filter for this ACE.<br>**Any**: No ICMP filter is specified (ICMP filter status is "don't-care").<br>**Specific**: If you want to filter a specific ICMP filter with this ACE, you can enter a specific ICMP value. A field for entering an ICMP value appears. |
| **ICMP Type Value** | When "Specific" is selected for the ICMP filter, you can enter a specific ICMP value. The allowed range is **0** to **255**. A frame that hits this ACE matches this ICMP value. |
| **ICMP Code Filter** | Specify the ICMP code filter for this ACE.<br>**Any**: No ICMP code filter is specified (ICMP code filter status is "don't-care").<br>**Specific**: If you want to filter a specific ICMP code filter with this ACE, you can enter a specific ICMP code value. A field for entering an ICMP code value appears. |

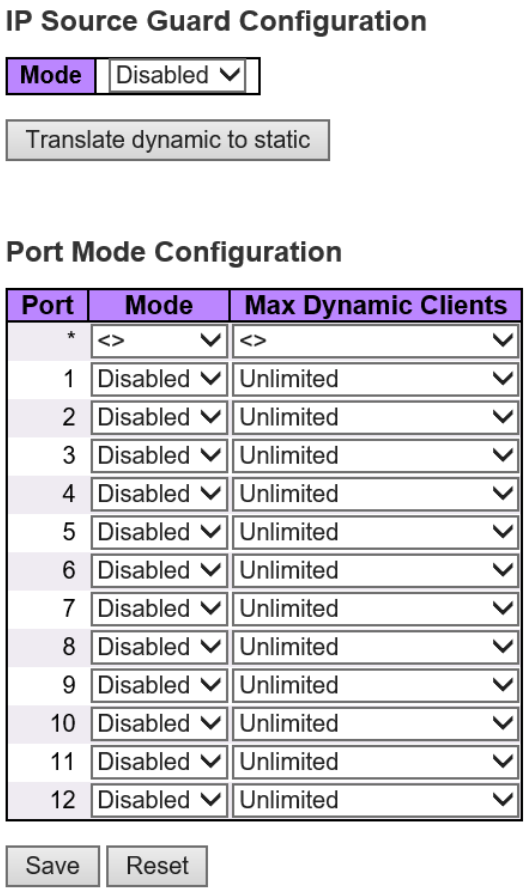
| | |
|---|---|
| **ICMP Code Value** | When "Specific" is selected for the ICMP code filter, you can enter a specific ICMP code value. The allowed range is `0` to `255`. A frame that hits this ACE matches this ICMP code value. |
| **TCP/UDP Parameters** | |
| **TCP/UDP Source Filter** | Specify the TCP/UDP source filter for this ACE.<br>`Any`: No TCP/UDP source filter is specified (TCP/UDP source filter status is "don't-care").<br>`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.<br>`Range`: If you want to filter a specific TCP/UDP source range filter with this ACE, you can enter a specific TCP/UDP source range value. A field for entering a TCP/UDP source value appears. |
| **TCP/UDP Source No.** | When "Specific" is selected for the TCP/UDP source filter, you can enter a specific TCP/UDP source value. The allowed range is `0` to `65535`. A frame that hits this ACE matches this TCP/UDP source value. |
| **TCP/UDP Source Range** | When "Range" is selected for the TCP/UDP source filter, you can enter a specific TCP/UDP source range value. The allowed range is `0` to `65535`. A frame that hits this ACE matches this TCP/UDP source value. |
| **TCP/UDP Destination Filter** | Specify the TCP/UDP destination filter for this ACE.<br>`Any`: No TCP/UDP destination filter is specified (TCP/UDP destination filter status is "don't-care").<br>`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.<br>`Range`: If you want to filter a specific range TCP/UDP destination filter with this ACE, you can enter a specific TCP/UDP destination range value. A field for entering a TCP/UDP destination value appears. |
| **TCP/UDP Destination Number** | When "Specific" is selected for the TCP/UDP destination filter, you can enter a specific TCP/UDP destination value. The allowed range is `0` to `65535`. A frame that hits this ACE matches this TCP/UDP destination value. |
| **TCP/UDP Destination Range** | When "Range" is selected for the TCP/UDP destination filter, you can enter a specific TCP/UDP destination range value. The allowed range is `0` to `65535`. A frame that hits this ACE matches this TCP/UDP destination value. |
| **TCP FIN** | Specify the TCP "No more data from sender" (FIN) value for this ACE.<br>`0`: TCP frames where the FIN field is set must not be able to match this entry.<br>`1`: TCP frames where the FIN field is set must be able to match this entry.<br>`Any`: Any value is allowed ("don't-care"). |

| | |
|---|---|
| **TCP SYN** | Specify the TCP "Synchronize sequence numbers" (SYN) value for this ACE.<br>`0`: TCP frames where the SYN field is set must not be able to match this entry.<br>`1`: TCP frames where the SYN field is set must be able to match this entry.<br>`Any`: Any value is allowed ("don't-care"). |
| **TCP RST** | Specify the TCP "Reset the connection" (RST) value for this ACE.<br>`0`: TCP frames where the RST field is set must not be able to match this entry.<br>`1`: TCP frames where the RST field is set must be able to match this entry.<br>`Any`: Any value is allowed ("don't-care"). |
| **TCP PSH** | Specify the TCP "Push Function" (PSH) value for this ACE.<br>`0`: TCP frames where the PSH field is set must not be able to match this entry.<br>`1`: TCP frames where the PSH field is set must be able to match this entry.<br>`Any`: Any value is allowed ("don't-care"). |
| **TCP ACK** | Specify the TCP "Acknowledgment field significant" (ACK) value for this ACE.<br>`0`: TCP frames where the ACK field is set must not be able to match this entry.<br>`1`: TCP frames where the ACK field is set must be able to match this entry.<br>`Any`: Any value is allowed ("don't-care"). |
| **TCP URG** | Specify the TCP "Urgent Pointer field significant" (URG) value for this ACE.<br>`0`: TCP frames where the URG field is set must not be able to match this entry.<br>`1`: TCP frames where the URG field is set must be able to match this entry.<br>`Any`: Any value is allowed ("don't-care"). |
| **Ethernet Type Parameters** | |
| **EtherType Filter** | Specify the Ethernet type filter for this ACE.<br>`Any`: No EtherType filter is specified (EtherType filter status is "don't-care").<br>`Specific`: If you want to filter a specific EtherType filter with this ACE, you can enter a specific EtherType value. A field for entering a EtherType value appears. |
| **Ethernet Type Value** | When "Specific" is selected for the EtherType filter, you can enter a specific EtherType value. The allowed range is `0x600` to `0xFFFF` but excluding 0x800(IPv4), 0x806(ARP) and 0x86DD(IPv6). A frame that hits this ACE matches this EtherType value. |

| **Buttons** | |
|---|---|
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |
| Cancel | Return to the previous page. |

## 2.3.44 IP Source Guard Configuration

This page provides IP Source Guard related configuration.

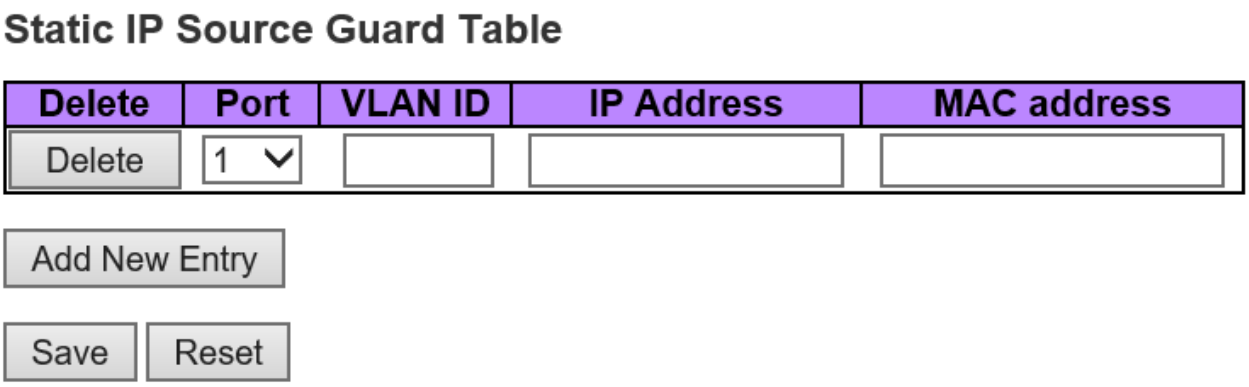



| Object | Description |
|---|---|
| **Mode of IP Source Guard Configuration** | Enable the Global IP Source Guard or disable the Global IP Source Guard. All configured ACEs will be lost when the mode is enabled. |
| **Port Mode Configuration** | Specify IP Source Guard is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, IP Source Guard is enabled on this given port. |
| **Max Dynamic Clients** | Specify the maximum number of dynamic clients that can be learned on given port. This value can be 0, 1, 2 or unlimited. If the port mode is enabled and the value of max dynamic client is equal to 0, it means only allow the IP packets forwarding that are matched in static entries on the specific port. |

| Buttons |
|---|

| | |
|---|---|
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |
| Translate dynamic to static | Click to translate all dynamic entries to static entries. |

## 2.3.45 IP Source Guard Static Table

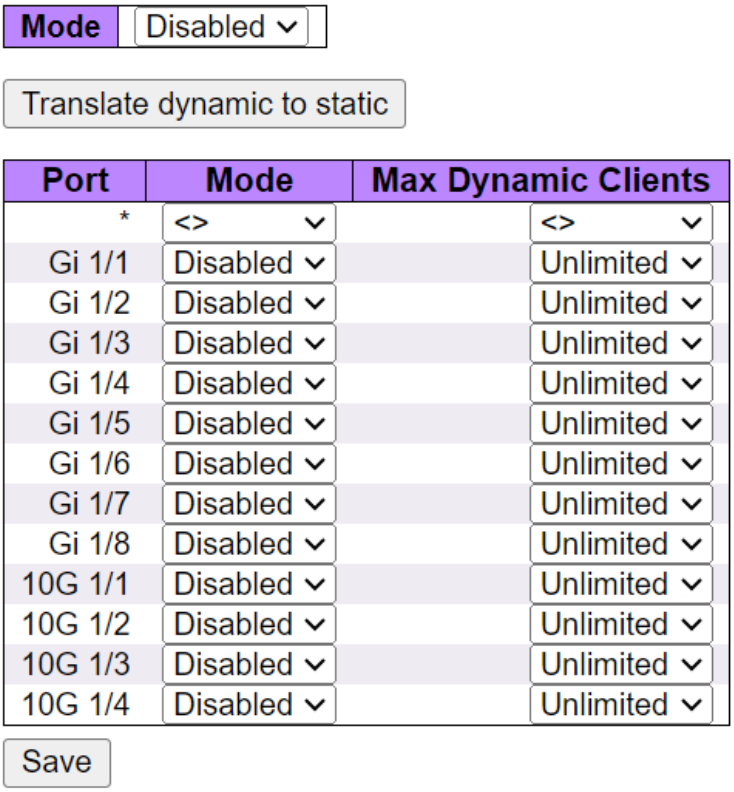



| Object | Description |
|---|---|
| **Delete** | Check to delete the entry. It will be deleted during the next save. |
| **Port** | The logical port for the settings. |
| **VLAN ID** | The vlan id for the settings. |
| **IP Address** | Allowed Source IP address. |
| **MAC address** | Allowed Source MAC address. |

| Buttons | |
|---|---|
| Add New Entry | Click to add a new entry to the Static IP Source Guard table. |
| Delete | Click to delete the entry. |
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

## 2.3.46 IPv6 Source Guard Configuration (For 90W PoE Model)

### IPv6 Source Guard Configuration

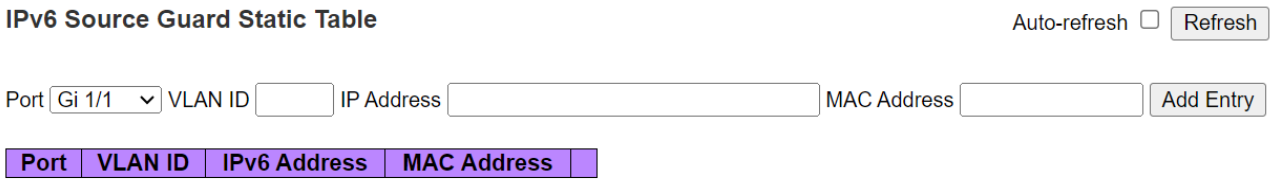



| Object | Description |
|---|---|
| **IPv6 Source Guard Mode Configuration** | Enable or disable the IPv6 Source Guard globally. |
| **Port Mode Configuration** | The table shows all ports on the device. There IPv6 Source Guard can be enabled/disabled on individual ports. Only when both Global Mode and Port Mode on a given port are enabled, IPv6 Source Guard is enabled on this given port. |
| **Max Dynamic Clients** | Specify the maximum number of dynamic clients that can be learned on given port. This value can be 0, 1, 2 or unlimited. If the port mode is enabled and the value of max dynamic client is equal to 0, only IPv6 packets that are matched in static entries on the specific port are forwarded. |

| Buttons | |
|---|---|
| Disabled | Toggle to change global mode. |

| | |
|---|---|
| Save | Click to save changes. |
| Translate dynamic to static | Click to translate all dynamic entries to static entries. |

## 2.3.47 IPv6 Source Guard Static Table (For 90W PoE Model)

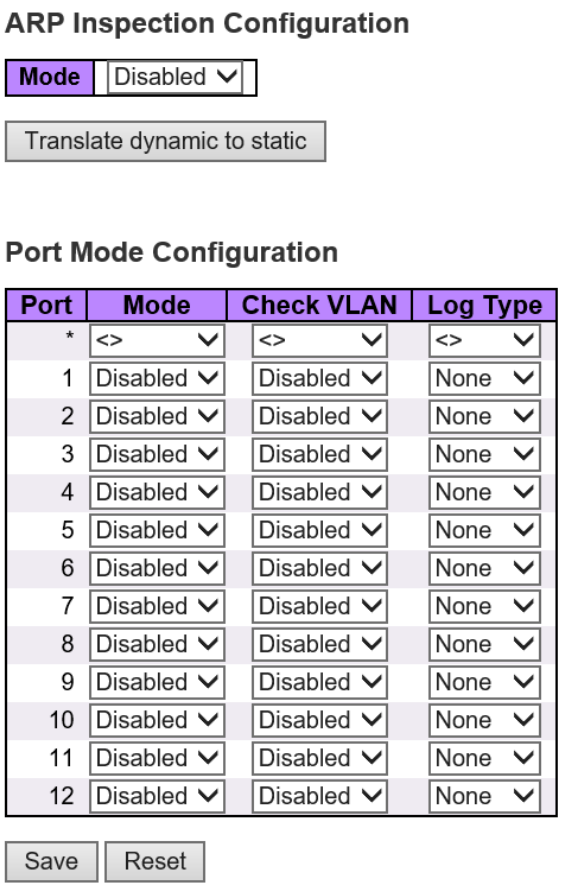



| Object | Description |
|---|---|
| **Delete** | Click entry Delete button to delete the entry. |
| **Port** | The logical port for the settings. |
| **VLAN ID** | The VLAN Id for the entry. If no VLAN Id is associated with the entry, this field shows 0. |
| **IPv6 Address** | Allowed Source IPv6 address. |
| **Prefix Size** | Prefix size of the IPv6 address. |
| **MAC address** | Allowed Source MAC address. |

| Buttons | |
|---|---|
| Gi 1/1 | Toggle to select entry port. |
| Add Entry: | Click to add a new entry to the Static IPv6 Source Guard table. |
| Auto-refresh : | Check this box to refresh the page automatically. |
| Refresh: | Refreshes the display table. |

## 2.3.48 ARP Inspection Port Configuration

This page provides ARP Inspection related configuration.




| Object | Description |
|---|---|
| **Mode of ARP Inspection Configuration** | Enable the Global ARP Inspection or disable the Global ARP Inspection. |
| **Port Mode Configuration** | Specify ARP Inspection is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port.<br>Possible modes are:<br>`Enabled`: Enable ARP Inspection operation.<br>`Disabled`: Disable ARP Inspection operation.<br>If you want to inspect the VLAN configuration, you have to enable the setting of "Check VLAN". The default setting of "Check VLAN" is disabled. When the setting of "Check VLAN" is disabled, the log type of ARP Inspection will refer to the port setting. And the setting of "Check VLAN" is enabled, the log type of ARP Inspection will refer |

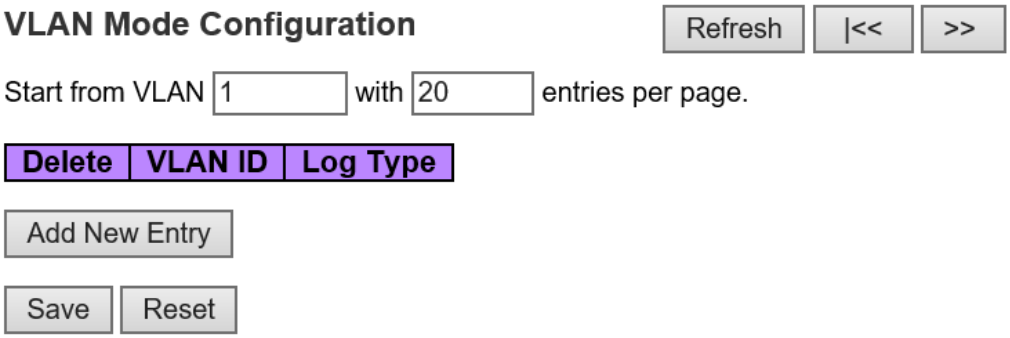
| | |
|---|---|
| | to the VLAN setting. Possible setting of "Check VLAN" are:<br>**Enabled**: Enable check VLAN operation.<br>**Disabled**: Disable check VLAN operation.<br>Only the Global Mode and Port Mode on a given port are enabled, and the setting of "Check VLAN" is disabled, the log type of ARP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

| Buttons | |
|---|---|
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |
| Translate dynamic to static | Click to translate all dynamic entries to static entries. |

## 2.3.49 ARP Inspection 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.

The "VLAN" input fields allow the user to select the starting point in the VLAN Table. Clicking the Refresh button will update the displayed table starting from that or the closest next VLAN Table match. The >> will use the next entry of the currently displayed VLAN entry as a basis for the next lookup. When the end is reached the warning message is shown in the displayed table. Use the |<< button to start over.




Specify ARP Inspection is enabled on which VLANs. First, you have to enable the port setting on Port mode configuration web page. Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port. Second, you can specify which VLAN will be inspected on VLAN mode configuration web page. The log type also can be configured on per VLAN setting.

Possible types are:

**None**: Log nothing.

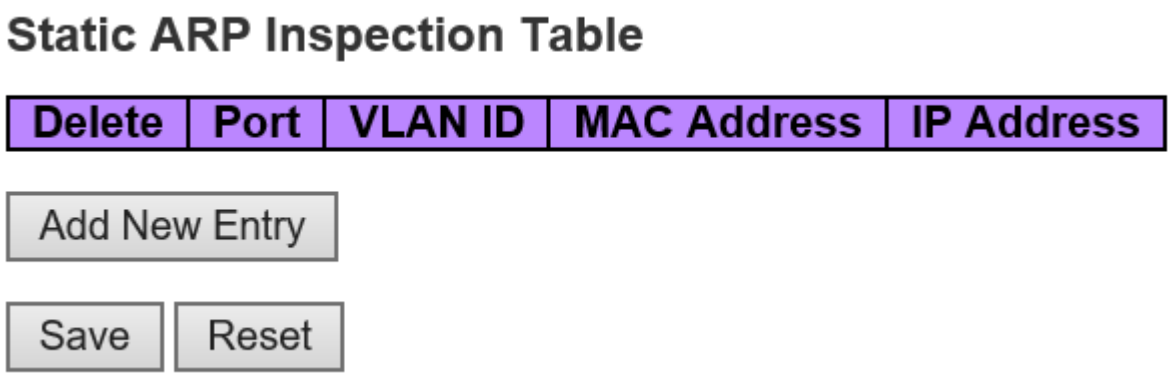
**Deny**: Log denied entries.

**Permit**: Log permitted entries.

**ALL**: Log all entries

| Buttons | |
|---|---|
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |
| Delete | Click to delete the entry. |
| Add New Entry | Click to add a new VLAN to the ARP Inspection VLAN table. |

## 2.3.50 ARP Inspection Static Table




| Object | 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 in ARP request packets. |
| **MAC Address** | Allowed Source MAC address in ARP request packets. |

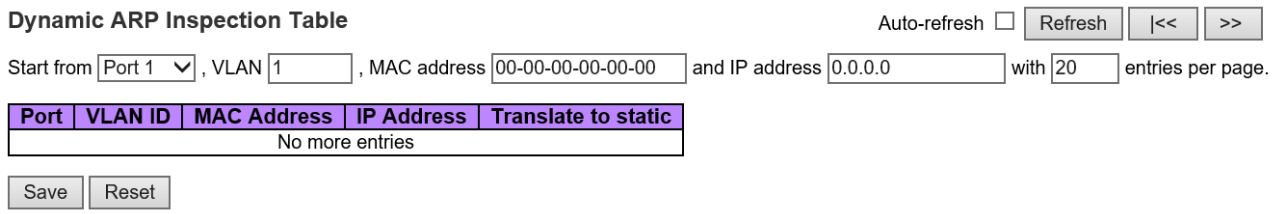
| Buttons | |
|---|---|
| Add New Entry | Click to add a new entry to the Static ARP Inspection table. |
| Delete | Click to delete the entry. |
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

## 2.3.51 ARP - Dynamic Table

Each page shows up to 99 entries from the Dynamic ARP Inspection table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Dynamic ARP Inspection Table.

The "Start from port address", "VLAN", "MAC address" and "IP address" input fields allow the user to select the starting point in the Dynamic ARP Inspection Table. Clicking the Refresh button will update the displayed table starting from that or the closest next Dynamic ARP Inspection Table match. In addition, the two input fields will - upon a Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

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




| Object | Description |
|---|---|
| **Port** | Switch Port Number for which the entries are displayed. |
| **VLAN ID** | VLAN-ID in which the ARP traffic is permitted. |
| **MAC Address** | User MAC address of the entry. |
| **IP Address** | User IP address of the entry. |
| **Translate to static** | Select the checkbox to translate the entry to static entry. |

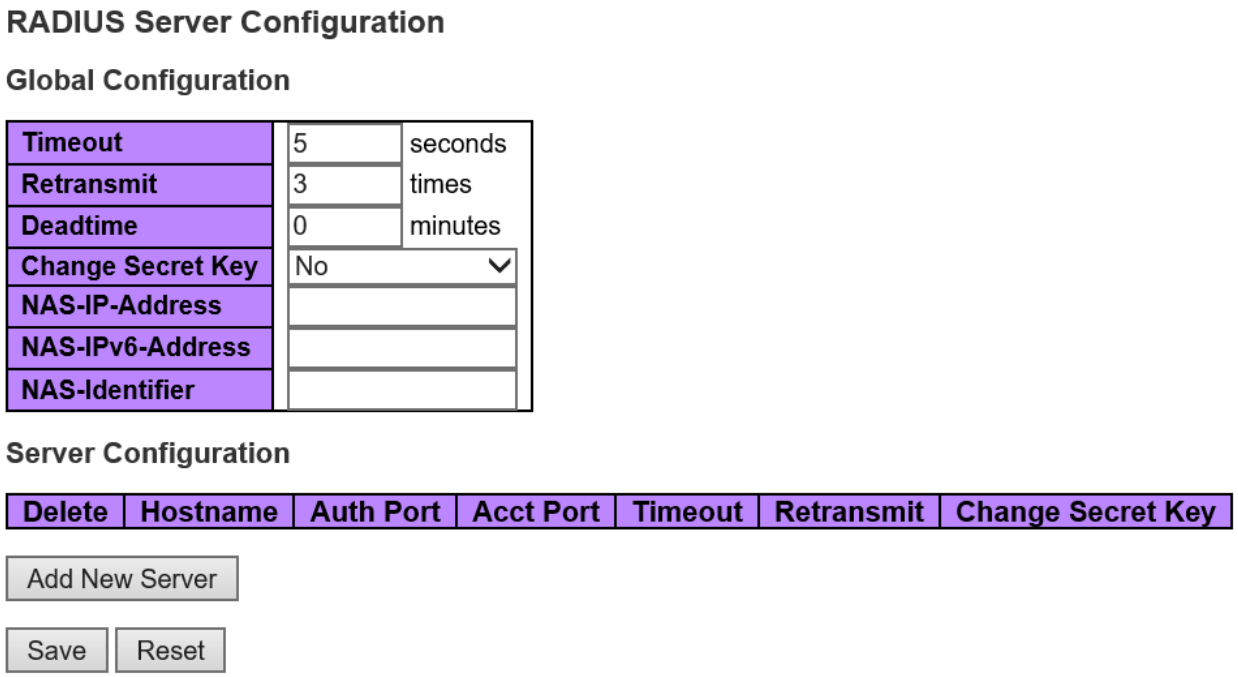
| Buttons | |
|---|---|
| Auto-refresh ☐ | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |
| Refresh | Refreshes the displayed table starting from the input fields. |

| | |
|---|---|
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |
| \|<< | Updates the table starting from the first entry in the Dynamic ARP Inspection Table. |
| >> | Updates the table, starting with the entry after the last entry currently displayed. |

## 2.3.52 RADIUS

This page allows you to configure the RADIUS servers.

90W PoE Model

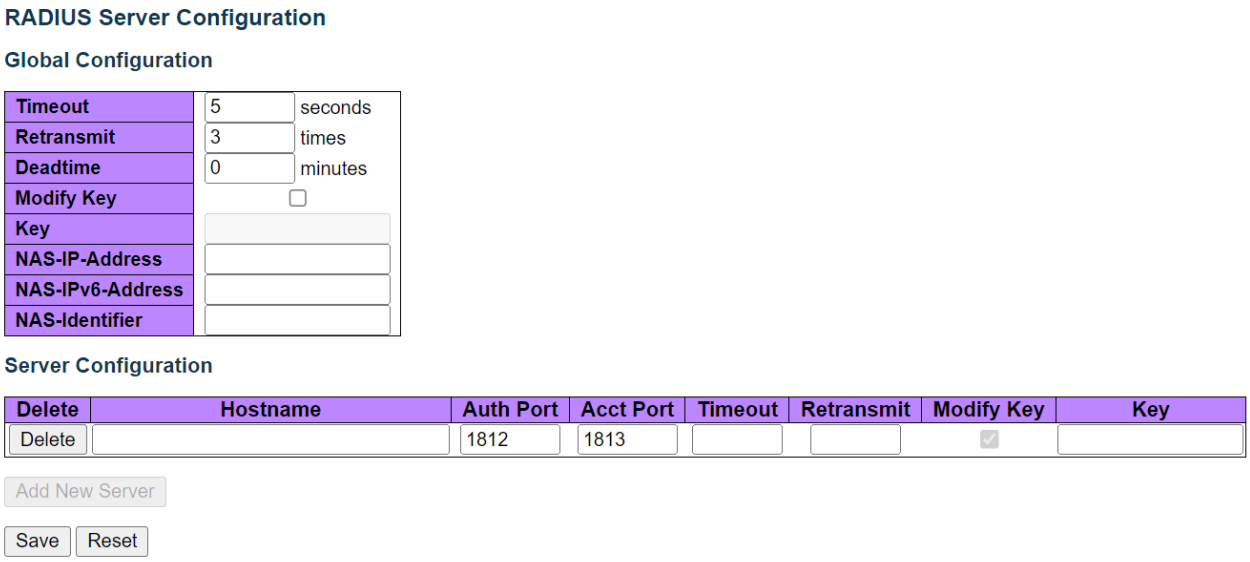



| Object | Description |
|---|---|
| **Global Configuration** | |
| **Timeout** | Timeout is the number of seconds, in the range 1 to 1000, to wait for a reply from a RADIUS server before retransmitting the request. |
| **Retransmit** | Retransmit is the number of times, in the range 1 to 1000, a RADIUS request is retransmitted to a server that is not responding. If the server has not responded after the last retransmit it is considered to be dead. |
| **Deadtime** | Deadtime, which can be set to a number between 0 to 1440 minutes, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead.<br>Setting the Deadtime to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured. |
| **Change Secret Key** | Specify to change the secret key or not. When "Yes" is selected for the option, you can change the secret key - up to 63 characters long - shared between the |

| | |
|---|---|
| | RADIUS server and the switch. |
| **NAS-IP-Address(Attribute 4)** | The IPv4 address to be used as attribute 4 in RADIUS Access-Request packets. If this field is left blank, the IP address of the outgoing interface is used. |
| **NAS-IPv6-Address(Attribute 95)** | The IPv6 address to be used as attribute 95 in RADIUS Access-Request packets. If this field is left blank, the IP address of the outgoing interface is used. |
| **NAS-Identifier (Attribute 32)** | The identifier - up to 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. |
| **Server Configuration** | |
| **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. |
| **Acct Port** | The UDP port to use on the RADIUS server for 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. |

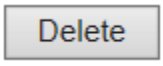
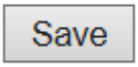
| **Buttons** | |
|---|---|
| Add New Server | Click to add a new RADIUS server, up to 5 servers are supported. |
| Delete | The button can be used to undo the addition of the new server. |
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

30W PoE Model




| Object | Description |
|---|---|
| **Global Configuration** | |
| **Timeout** | Timeout is the number of seconds, in the range 1 to 1000, to wait for a reply from a RADIUS server before retransmitting the request. |
| **Retransmit** | Retransmit is the number of times, in the range 1 to 1000, a RADIUS request is retransmitted to a server that is not responding. If the server has not responded after the last retransmit it is considered to be dead. |
| **Deadtime** | Deadtime, which can be set to a number between 0 to 1440 minutes, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead.<br>Setting the Deadtime to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured. |
| **Modify Key** | To modify secret key, this checkbox should be selected, otherwise the secret key won't be changed. |
| **Key** | The secret key - up to 63 characters long - shared between the RADIUS server and the switch. |
| **NAS-IP-Address(Attribute 4)** | The IPv4 address to be used as attribute 4 in RADIUS Access-Request packets. If this field is left blank, the IP address of the outgoing interface is used. |
| **NAS-IPv6-Address(Attribute 95)** | The IPv6 address to be used as attribute 95 in RADIUS Access-Request packets. If this field is left blank, the IP address of the outgoing interface is used. |
| **NAS-Identifier (Attribute 32)** | The identifier - up to 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 |

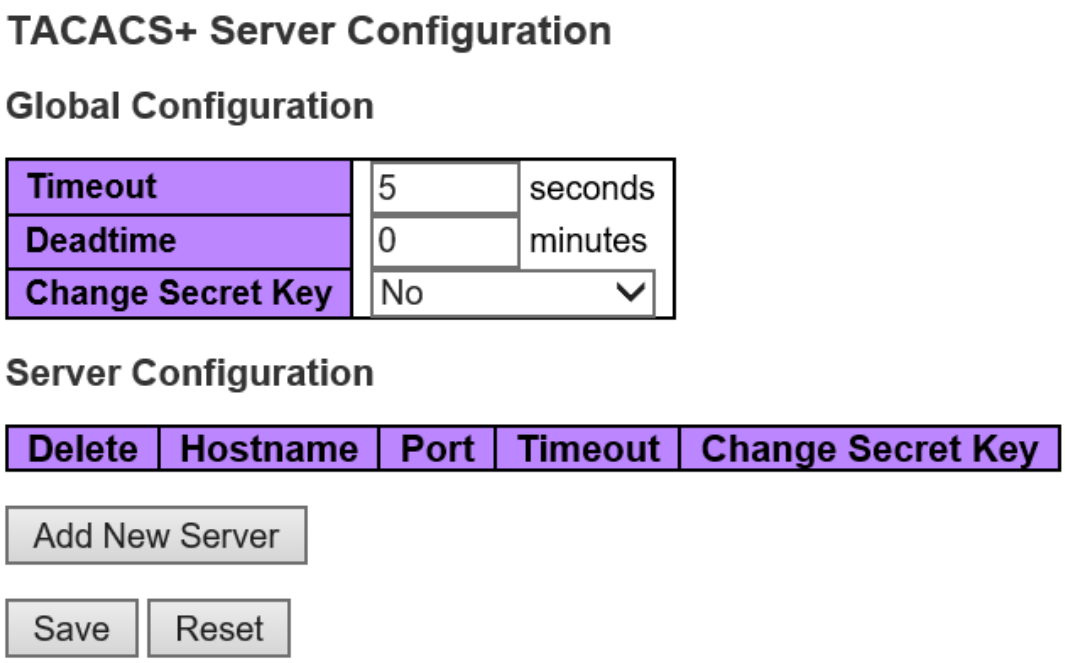
| | |
|---|---|
| | included in the packet. |
| **Server Configuration** | |
| **Delete** | To delete a RADIUS server entry, check this box. The entry will be deleted during the next Save. |
| **Hostname** | The IP address or hostname of the RADIUS server. |
| **Auth Port** | The UDP port to use on the RADIUS server for authentication. |
| **Acct Port** | The UDP port to use on the RADIUS server for 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. |
| **Modify Key** | Selected checkbox to create or modify server configuration Key. |
| **Key** | This optional setting overrides the global key. Leaving it blank will use the global key. |

| **Buttons** | |
|---|---|
|  | Click to add a new RADIUS server, up to 5 servers are supported. |
|  | The button can be used to undo the addition of the new server. |
|  | Click to save changes. |
|  | Click to undo any changes made locally and revert to previously saved values. |

## 2.3.53 TACACS+

This page allows you to configure the TACACS+ servers.

90W PoE Model

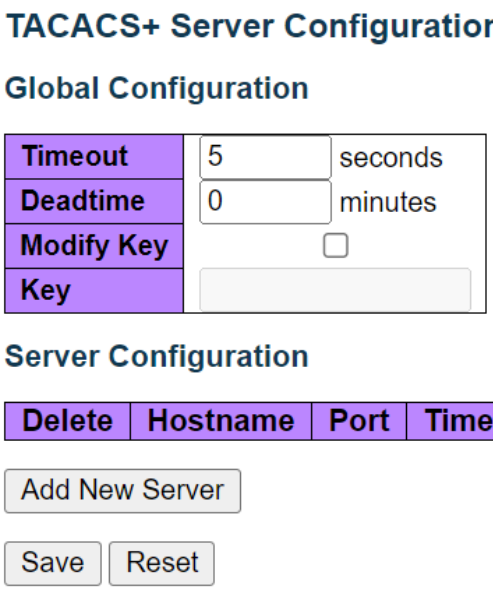



| Object | Description |
|---|---|
| **Global Configuration** | |
| **Timeout** | Timeout is the number of seconds, in the range 1 to 1000, to wait for a reply from a TACACS+ server before it is considered to be dead. |
| **Deadtime** | Deadtime, which can be set to a number between 0 to 1440 minutes, 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.<br>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** | |
| **Delete** | To delete a TACACS+ server entry, check this box. The entry will be deleted during the next Save. |

| | |
|---|---|
| **Hostname** | The IP address or hostname of the TACACS+ server. |
| **Port** | The TCP port to use on the TACACS+ server for authentication. |
| **Timeout** | This optional setting overrides the global timeout value. Leaving it blank will use the global timeout value. |
| **Change Secret Key** | Specify to change the secret key or not. When the checkbox is checked, you can change the setting overrides the global key. Leaving it blank will use the global key. |

| **Buttons** | |
|---|---|
| Add New Server | Click to add a new TACACS+ server, up to 5 servers are supported. |
| Delete | The button can be used to undo the addition of the new server. |
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

30W PoE Model



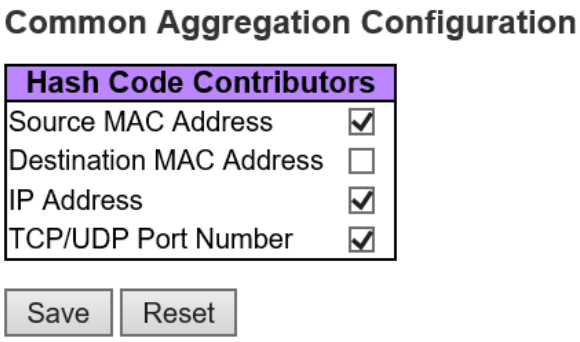

| Object | Description |
|---|---|
| **Global Configuration** | |
| **Timeout** | Timeout is the number of seconds, in the range 1 to 1000, to wait for a reply from a TACACS+ server before it is considered to be dead. |
| **Deadtime** | Deadtime, which can be set to a number between 0 to 1440 minutes, 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.<br>Setting the Deadtime to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured. |
| **Modify Key** | To modify secret key, this checkbox should be selected, otherwise the secret key won't be changed. |
| **Key** | The secret key - up to 63 characters long - shared between the TACACS+ server and the switch. |
| **Server Configuration** | |
| **Delete** | To delete a TACACS+ server entry, check this box. The entry will be deleted during the next Save. |
| **Hostname** | The IP address or hostname of the TACACS+ server. |
| **Port** | The TCP port to use on the TACACS+ server for authentication. |
| **Timeout** | This optional setting overrides the global timeout value. Leaving it blank will use the global timeout value. |
| **Change Secret Key** | Specify to change the secret key or not. When the checkbox is checked, you can change the setting overrides the global key. Leaving it blank will use the global key. |

| **Buttons** | |
|---|---|
| Add New Server | Click to add a new TACACS+ server, up to 5 servers are supported. |
| Delete | The button can be used to undo the addition of the new server. |
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

## 2.3.54 Aggregation – Common (For 90W PoE Model)

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

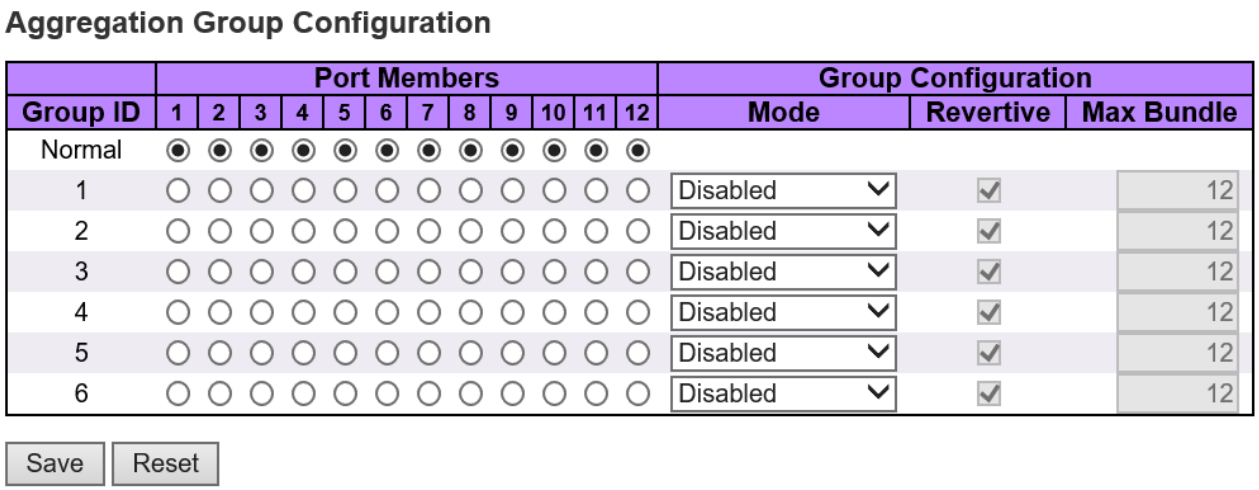



| Object | Description |
|---|---|
| **Source MAC Address** | The Source MAC address can be used to calculate the destination port for the frame. Check to enable the use of the Source MAC address, or uncheck to disable. By default, Source MAC Address is enabled. |
| **Destination MAC Address** | The Destination MAC Address can be used to calculate the destination port for the frame. Check to enable the use of the Destination MAC Address, or uncheck to disable. By default, Destination MAC Address is disabled. |
| **IP Address** | The IP address can be used to calculate the destination port for the frame. Check to enable the use of the IP Address, or uncheck to disable. By default, IP Address is enabled. |
| **TCP/UDP Port Number** | The TCP/UDP port number can be used to calculate the destination port for the frame. Check to enable the use of the TCP/UDP Port Number, or uncheck to disable. By default, TCP/UDP Port Number is enabled. |

| Buttons | |
|---|---|
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

## 2.3.55 Aggregation – Group (For 90W PoE Model)

This page is used to configure the aggregation groups.



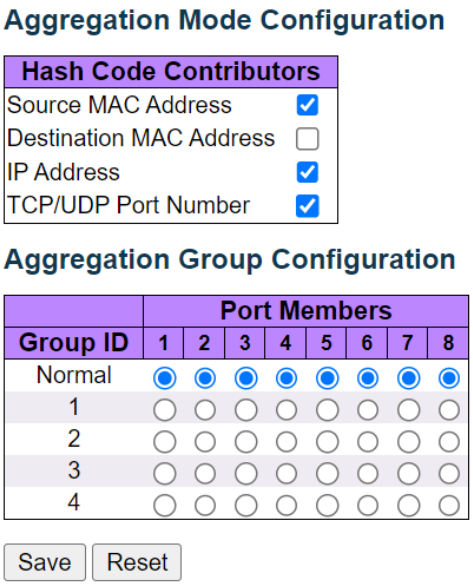

| Object | Description |
|---|---|
| **Group ID** | Indicates the aggregation group ID for the settings contained in the same row. Group ID "Normal" indicates there is no aggregation. Only one group ID is valid per port. |
| **Port Members** | Each switch port is listed for each group ID. Select a radio 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.<br>• Disabled: The group is disabled.<br>• Static: The group operates in static aggregation mode.<br>• LACP (Active): The group operates in LACP active aggregation mode. See IEEE 801.AX-2014, section 6.4.1 for details.<br>• LACP (Passive): The group operates in LACP passive aggregation mode. See IEEE 801.AX-2014, section 6.4.1 for details. |
| **Revertive** | This parameter only applies to LACP-enabled groups. It determines if the group will perform automatic link (re-)calculation when links with higher priority becomes available. |
| **Max Bundle** | This parameter only applies to LACP-enabled groups. It determines the maximum number of active bundled LACP ports allowed in an aggregation. |

| Buttons | |
|---|---|
| Save | Click to save changes. |

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

## 2.3.56 Aggregation – Static (For 30W PoE Model)

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




| Object | Description |
|---|---|
| **Aggregation Mode Configuration** | |
| **Source MAC Address** | The Source MAC address can be used to calculate the destination port for the frame. Check to enable the use of the Source MAC address, or uncheck to disable. By default, Source MAC Address is enabled. |
| **Destination MAC Address** | The Destination MAC Address can be used to calculate the destination port for the frame. Check to enable the use of the Destination MAC Address, or uncheck to disable. By default, Destination MAC Address is disabled. |
| **IP Address** | The IP address can be used to calculate the destination port for the frame. Check to enable the use of the IP Address, or uncheck to disable. By default, IP Address is enabled. |
| **TCP/UDP Port Number** | The TCP/UDP port number can be used to calculate the destination port for the frame. Check to enable the use of the TCP/UDP Port Number, or uncheck to disable. By default, TCP/UDP Port Number is enabled. |
| **Aggregation Group Configuration** | |
| **Group ID** | Indicates the aggregation group ID for the settings contained in the same row. Group ID "Normal" indicates there is no aggregation. Only one group ID is valid per port. |
| **Port Members** | Each switch port is listed for each group ID. Select a radio button to include a port in |

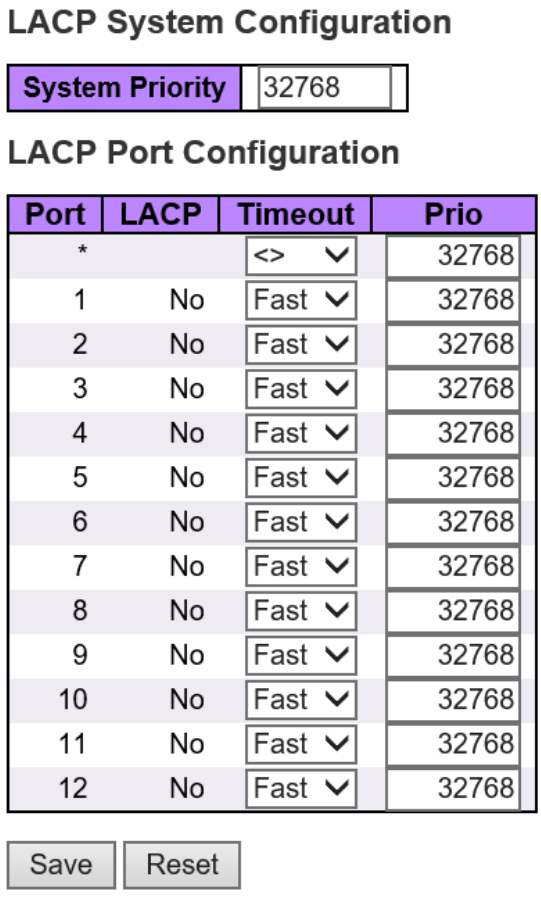
| | |
|---|---|
| | an aggregation, or clear the radio button to remove the port from the aggregation. By default, no ports belong to any aggregation group. Only full duplex ports can join an aggregation and ports must be in the same speed in each group. |

| Buttons | |
|---|---|
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

## 2.3.57 Aggregation - LACP

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

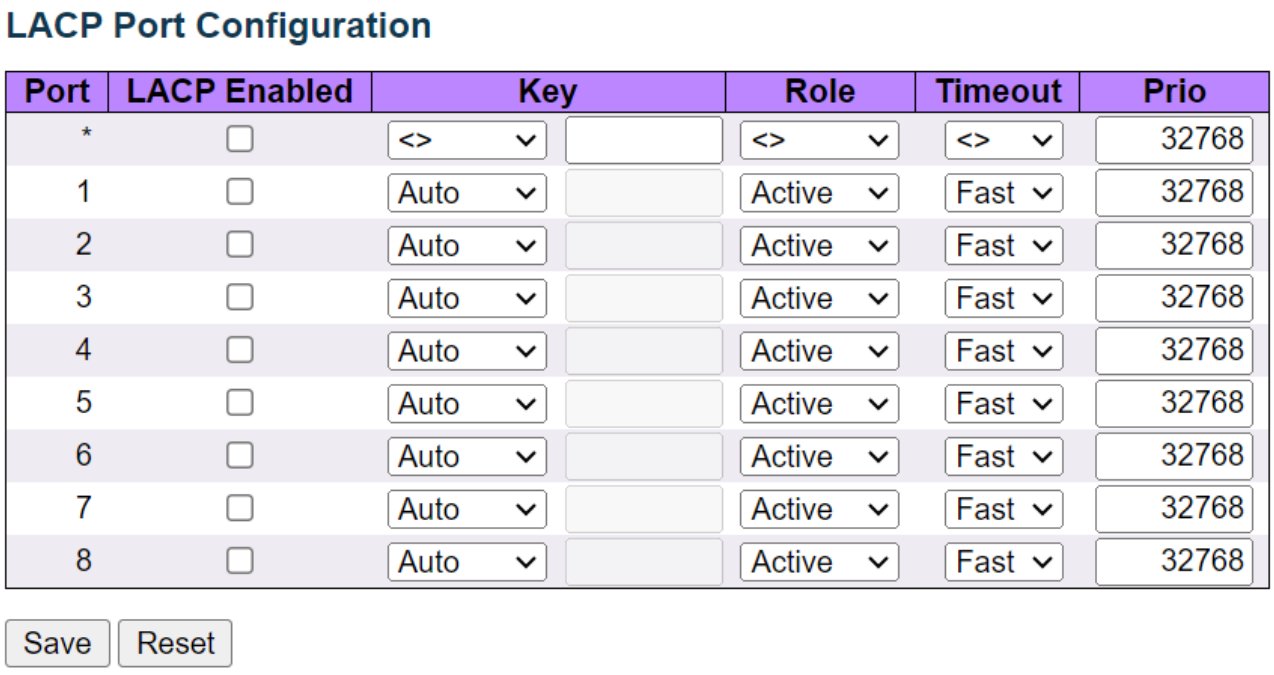
90W PoE Model



| Object | Description |
|---|---|
| **System Priority** | The "System Priority" controls the priority of the system, range 1-65535. |
| **Port** | The switch port number. |
| **LACP Enabled** | 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. |

| Buttons | |
|---|---|
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

30W PoE Model

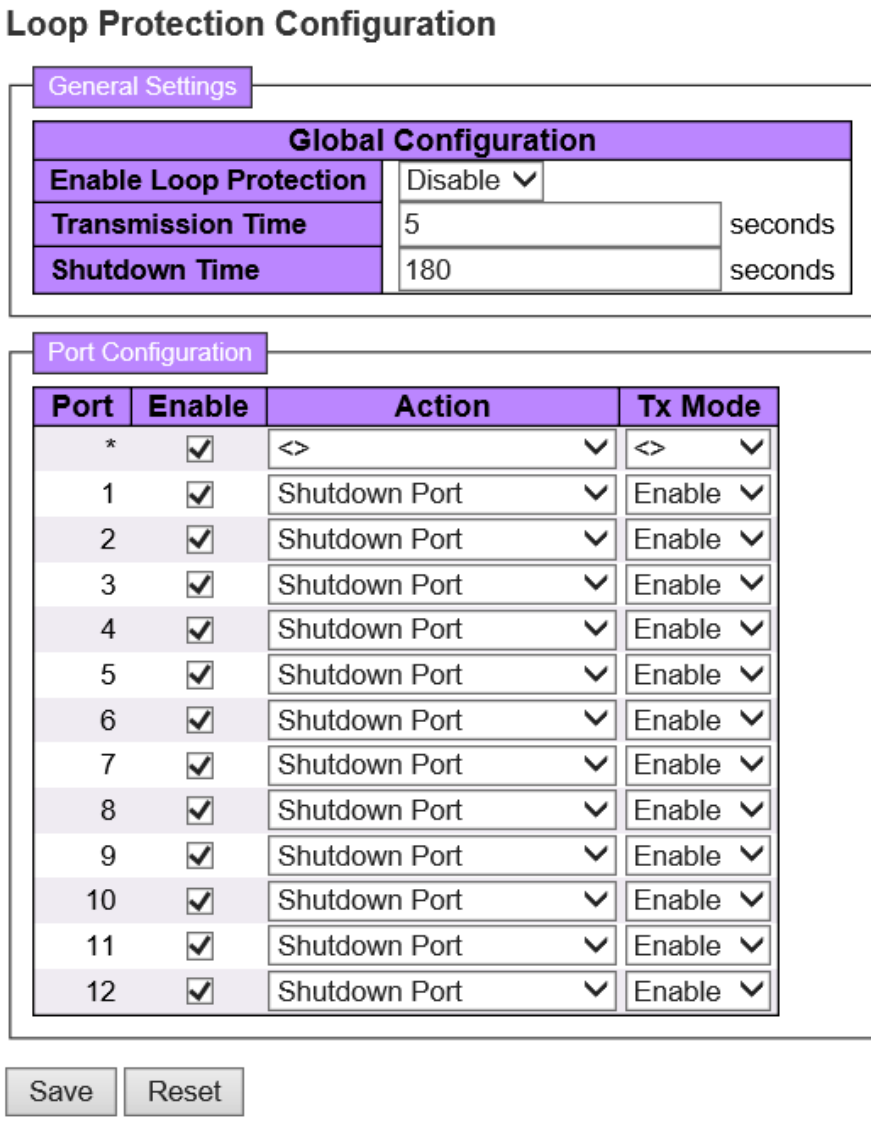


| Object | Description |
|---|---|
| **Port** | The switch port number. |
| **LACP Enabled** | Controls whether LACP is enabled on this switch port. LACP will form an aggregation when 2 or more ports are connected to the same partner. |
| **Key** | The Key value incurred by the port, range 1-65535 . The Auto setting will set the key as appropriate by the physical link speed, 10Mb = 1, 100Mb = 2, 1Gb = 3. Using the Specific setting, a user-defined value can be entered. Ports with the same Key value can participate in the same aggregation group, while ports with different keys cannot. |
| **Role** | The Role shows the LACP activity status. The Active will transmit LACP packets each second, while Passive will wait for a LACP packet from a partner (speak if spoken to). |
| **Timeout** | 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. |

| Buttons | |
|---|---|
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

## 2.3.58 Loop Protection

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



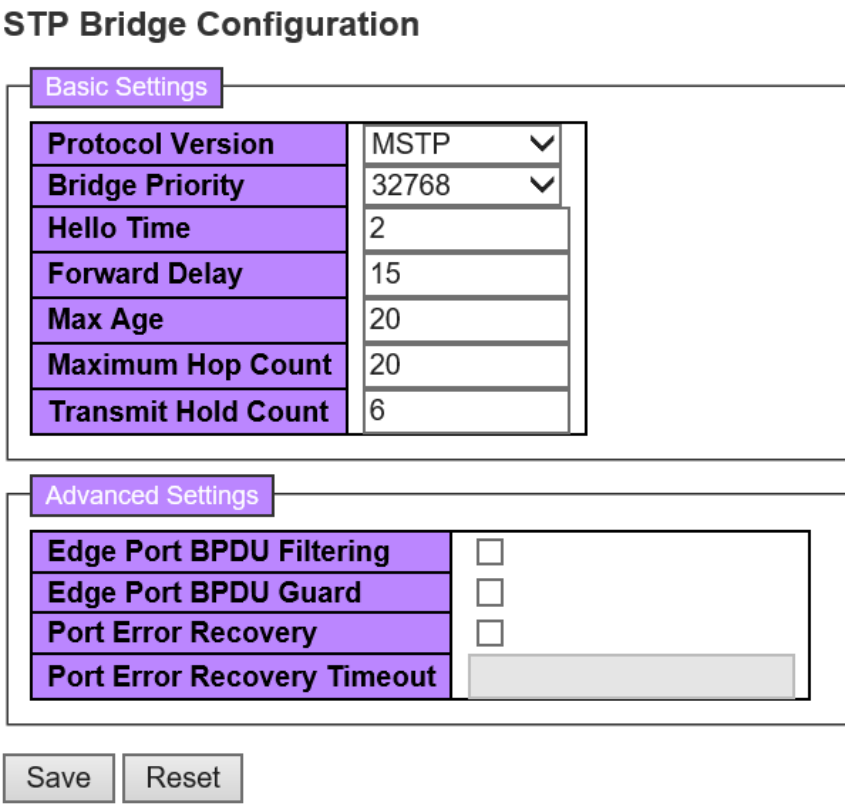

| Object | Description |
|---|---|
| **General Settings** | |
| **Enable Loop Protection** | Controls whether loop protections is enabled (as a whole). |
| **Transmission Time** | The interval between each loop protection PDU sent on each port. Valid values are 1 to 10 seconds. Default value is 5 seconds. |
| **Shutdown Time** | The period (in seconds) for which a port will be kept disabled in the event of a loop is detected (and the port action shuts down the port). Valid values are 0 to 604800 |

| | |
|---|---|
| | seconds (7 days). A value of zero will keep a port disabled (until next device restart). Default value is 180 seconds. |
| **Port Configuration** | |
| **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. |

| **Buttons** | |
|---|---|
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

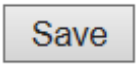
## 2.3.59 Spanning Tree - Bridge Settings

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



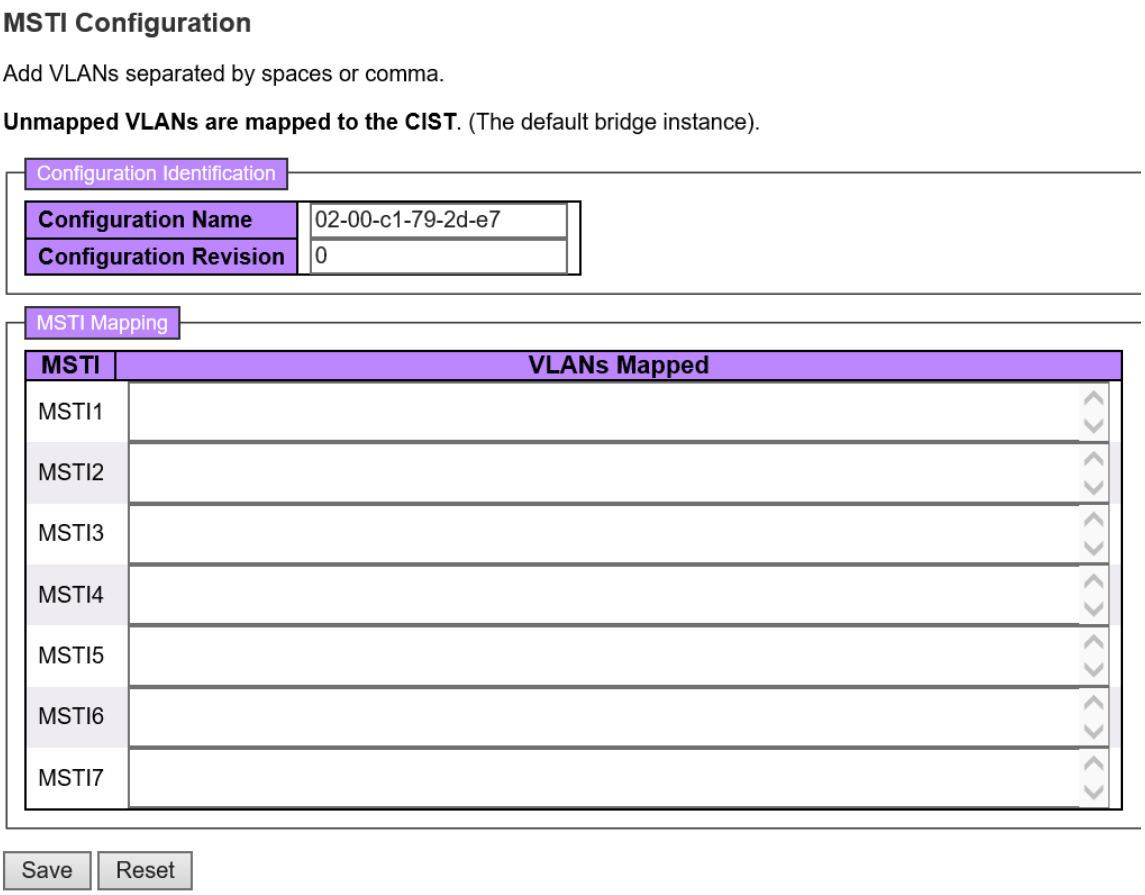

| Object | Description |
|---|---|
| **Basic Settings** | |
| **Protocol Version** | The MSTP / RSTP / STP protocol version setting. Valid values are `STP`, `RSTP` and `MSTP`. |
| **Bridge Priority** | Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a *Bridge Identifier*.<br>For `MSTP` operation, this is the priority of the CIST. Otherwise, this is the priority of the STP/RSTP bridge |
| **Hello Time** | The interval between sending STP BPDU's. Valid values are in the range 1 to 10 seconds, default is 2 seconds.<br>Note: Changing this parameter from the default value is not recommended, and may have adverse effects on your network. |

| | |
|---|---|
| **Forward Delay** | The delay used by STP Bridges to transit Root and Designated Ports to Forwarding (used in STP compatible mode). Valid values are in the range 4 to 30 seconds. |
| **Max Age** | The maximum age of the information transmitted by the Bridge when it is the Root Bridge. Valid values are in the range 6 to 40 seconds, and MaxAge must be <= (FwdDelay-1)*2. |
| **Maximum Hop Count** | This defines the initial value of remaining Hops for MSTI information generated at the boundary of an MSTI region. It defines how many bridges a root bridge can distribute its BPDU information to. Valid values are in the range 6 to 40 hops. |
| **Transmit Hold Count** | The number of BPDU's a bridge port can send per second. When exceeded, transmission of the next BPDU will be delayed. Valid values are in the range 1 to 10 BPDU's per second. |
| **Advanced Settings** | |
| **Edge Port BPDU Filtering** | Control whether a port *explicitly* configured as `Edge` will transmit and receive BPDUs. |
| **Edge Port BPDU Guard** | Control whether a port *explicitly* configured as `Edge` will disable itself upon reception of a BPDU. The port will enter the *error-disabled* state, and will be removed from the active topology. |
| **Port Error Recovery** | Control whether a port in the *error-disabled* state automatically will be enabled after a certain time. If recovery is not enabled, ports have to be disabled and re-enabled for normal STP operation. The condition is also cleared by a system reboot. |
| **Port Error Recovery Timeout** | The time to pass before a port in the *error-disabled* state can be enabled. Valid values are between 30 and 86400 seconds (24 hours). |

| **Buttons** | |
|---|---|
|  | Click to save changes. |
|  | Click to undo any changes made locally and revert to previously saved values. |

## 2.3.60 Spanning Tree - MSTI Mapping

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



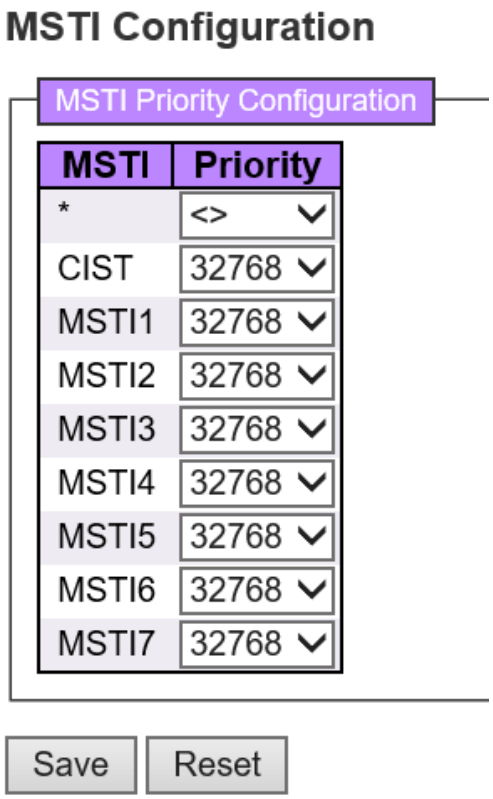

| Object | Description |
|---|---|
| **Configuration Identification** | |
| **Configuration Name** | The name identifying the VLAN to MSTI mapping. Bridges must share the name and revision (see below), as well as the VLAN-to-MSTI mapping configuration in order to share spanning trees for MSTI's (Intra-region). The name is at most 32 characters. |
| **Configuration Revision** | The revision of the MSTI configuration named above. This must be an integer between 0 and 65535. |
| **MSTI Mapping** | |
| **MSTI** | The bridge instance. The CIST is not available for explicit mapping, as it will receive the VLANs not explicitly mapped. |
| **VLANs Mapped** | The list of VLANs mapped to the MSTI. The VLANs can be given as a single (`xx`, xx being between 1 and 4094) VLAN, or a range (`xx-yy`), each of which must be |

| | |
|---|---|
| | separated with comma and/or space. A VLAN can only be mapped to *one* MSTI. An unused MSTI should just be left empty. (I.e. not having any VLANs mapped to it.) Example: `2,5,20-40`. |

| Buttons | |
|---|---|
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

## 2.3.61 Spanning Tree - MSTI Priorities

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




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

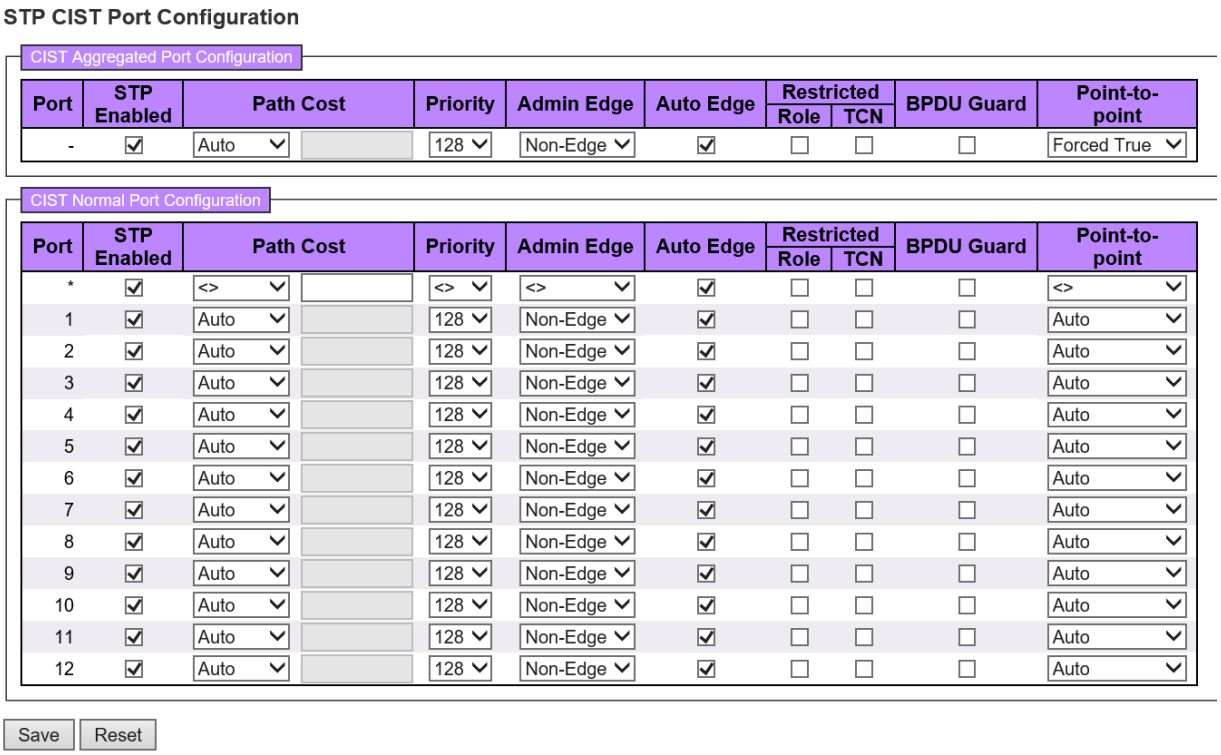
| Buttons | |
|---|---|
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

## 2.3.62 Spanning Tree - CIST Ports

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.

Note: RSTP & Ring cannot be enabled simutaneously.




| Object | 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. (See above).<br>Lower priority is better. |

| | |
|---|---|
| **operEdge (state flag)** | Operational flag describing whether the port is connecting directly to edge devices. (*No* Bridges attached). Transition to the forwarding state is faster for edge ports (having *operEdge true*) than for other ports. The value of this flag is based on AdminEdge and AutoEdge fields. This flag is displayed as Edge in Monitor->Spanning Tree -> STP Detailed Bridge Status. |
| **AdminEdge** | Controls whether the *operEdge* flag should start as set or cleared. (The initial *operEdge* state when a port is initialized). |
| **AutoEdge** | Controls whether the bridge should enable automatic edge detection on the bridge port. This allows *operEdge* to be derived from whether BPDU's are received on the port or not. |
| **Restricted Role** | If enabled, causes the port not to be selected as Root Port for the CIST or any MSTI, even if it has the best spanning tree priority vector. Such a port will be selected as an Alternate Port after the Root Port has been selected. If set, it can cause lack of spanning tree connectivity. It can be set by a network administrator to prevent bridges external to a core region of the network influence the spanning tree active topology, possibly because those bridges are not under the full control of the administrator. This feature is also known as **Root Guard**. |
| **Restricted TCN** | If enabled, causes the port not to propagate received topology change notifications and topology changes to other ports. If set it can cause temporary loss of connectivity after changes in a spanning tree's active topology as a result of persistently incorrect learned station location information. It is set by a network administrator to prevent bridges external to a core region of the network, causing address flushing in that region, possibly because those bridges are not under the full control of the administrator or the physical link state of the attached LANs transits frequently. |
| **BPDU Guard** | If enabled, causes the port to disable itself upon receiving valid BPDU's. Contrary to the similar bridge setting, the port **Edge** status does not effect this setting.<br>A port entering error-disabled state due to this setting is subject to the bridge Port Error Recovery setting as well. |
| **Point-to-Point** | Controls whether the port connects to a point-to-point LAN rather than to a shared medium. This can be automatically determined, or forced either true or false. Transition to the forwarding state is faster for point-to-point LANs than for shared media. |

| **Buttons** | |
|---|---|
| Save | Click to save changes. |

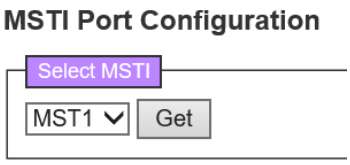
| | |
|---|---|
| Reset | Click to undo any changes made locally and revert to previously saved values. |

## 2.3.63 Spanning Tree - MSTI Ports

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

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

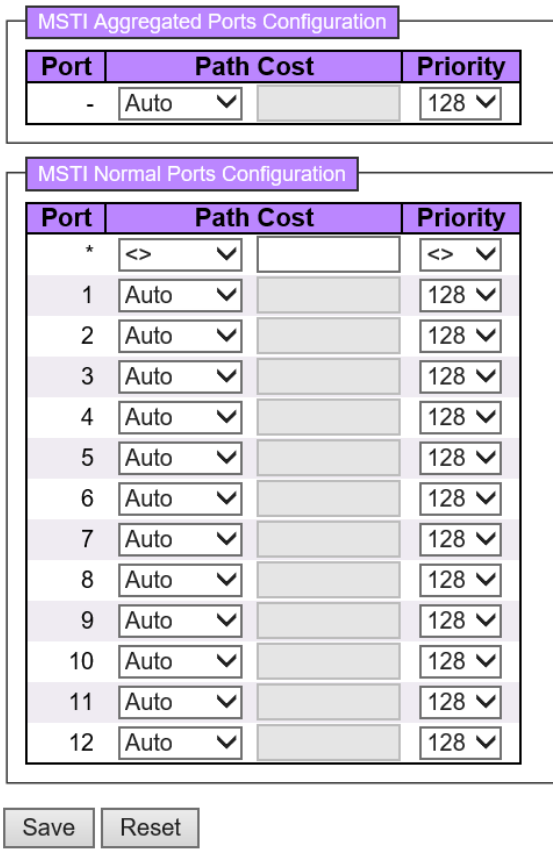
This page contains MSTI port settings for physical and aggregated ports.




Click 

to retrieve settings for a specific MSTI, the page displayed as follow.

### MST1 MSTI Port Configuration




| Object | 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. (See above). Lower priority is better. |

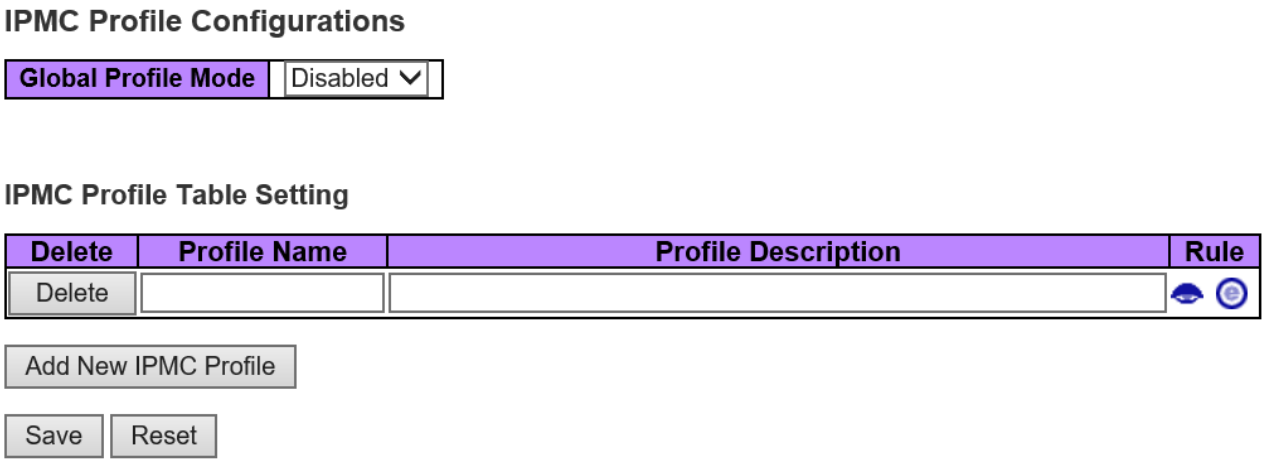
| Buttons | |
|---|---|
| Get | Click to retrieve settings for a specific MSTI. |
| Save | Click to save changes. |

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

## 2.3.64 IPMC Profile - Profile Table

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.



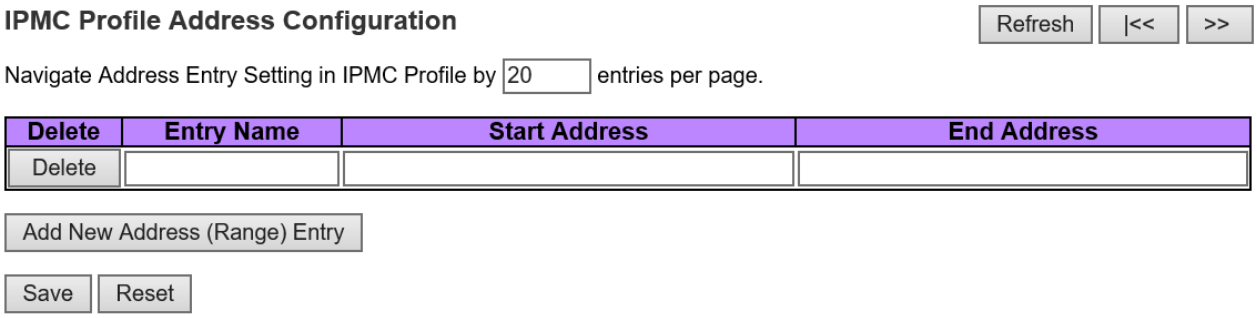

| Object | Description |
|---|---|
| **Global Profile Mode** | Enable/Disable the Global IPMC Profile.<br>System starts to do filtering based on profile settings only when the global profile mode is enabled. |
| **Delete** | Check to delete the entry.<br>The designated entry will be deleted during the next save. |
| **Profile Name** | The name used for indexing the profile table.<br>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.<br>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:<br>: List the rules associated with the designated profile.<br>: Adjust the rules associated with the designated profile. |

| Buttons | |
|---|---|
| Add New IPMC Profile | Click to add new IPMC profile. Specify the name and configure the new entry. Click "Save". |
| Delete | Click to delete the entry. |
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

## 2.3.65 IPMC Profile -Address Entry

This page provides address range settings used in IPMC profile.

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




| Object | Description |
|---|---|
| **Delete** | Check to delete the entry.<br>The designated entry will be deleted during the next save. |
| **Entry Name** | The name used for indexing the address entry table.<br>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. |

| Buttons | |
|---|---|
| Delete | Click to delete the entry. |
| Add New Address (Range) Entry | Click to add new address range. Specify the name and configure the addresses. Click "Save" |
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |
| Refresh | Refreshes the displayed table starting from the input fields. |
| \|<< | Updates the table starting from the first entry in the IPMC Profile Address Configuration. |
| >> | Updates the table, starting with the entry after the last entry currently displayed. |

## 2.3.66 MVR

This page provides MVR related configurations.

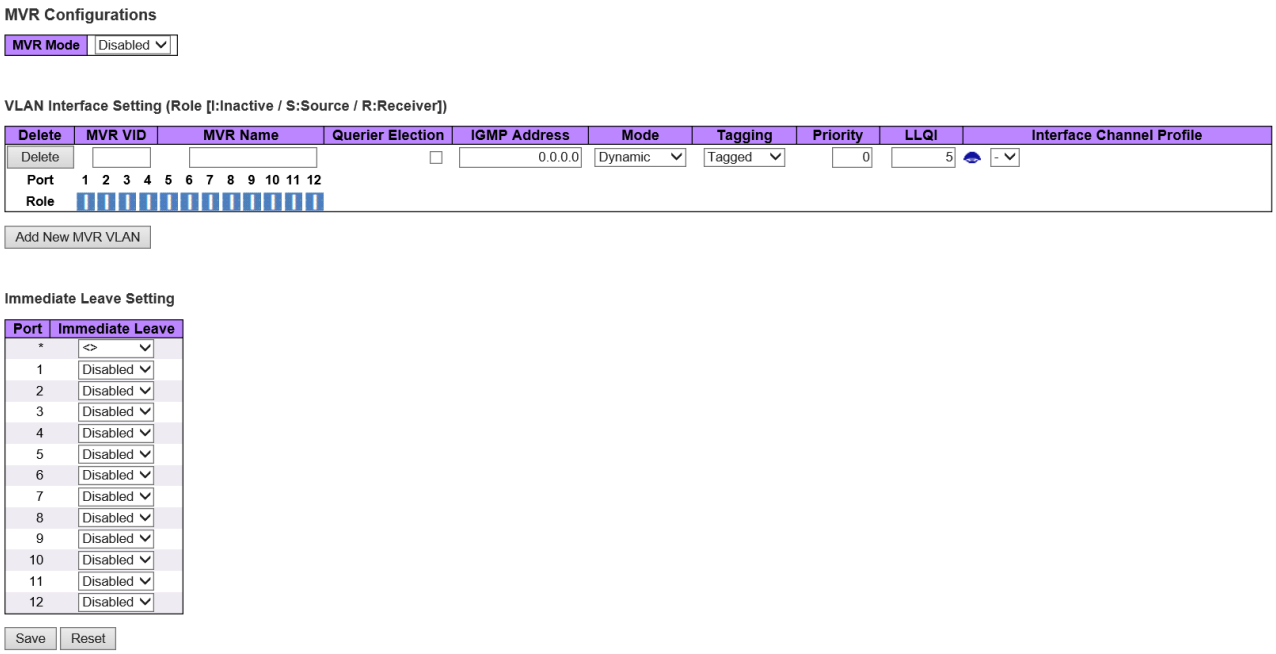
The MVR feature enables multicast traffic forwarding on the Multicast VLANs.

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.

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

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




| Object | Description |
|---|---|
| **MVR Configurations** | |
| **MVR Mode** | Enable/Disable the Global MVR.<br>The Unregistered Flooding control depends on the current configuration in IGMP/MLD Snooping.<br>It is suggested to enable Unregistered Flooding control when the MVR group table is full. |
| **VLAN Interface Setting** | |

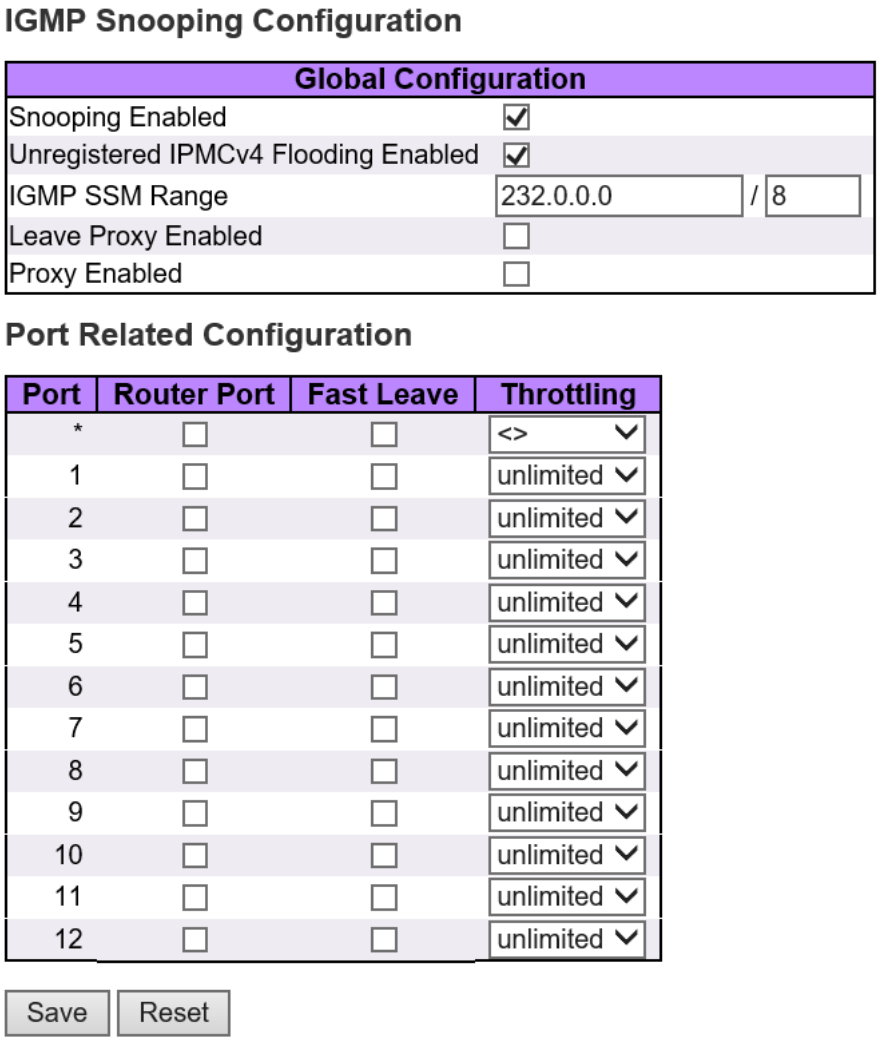
| | |
|---|---|
| **Delete** | Check to delete the entry. The designated entry will be deleted during the next save. |
| **MVR VID** | Specify the Multicast VLAN ID.<br>**Be Caution**: MVR source ports are not recommended to be overlapped with management VLAN ports. |
| **MVR Name** | MVR Name is an 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.<br>The default IGMP address is not set (0.0.0.0).<br>When the IGMP address is not set, system uses IPv4 management address of the IP interface associated with this VLAN.<br>When the IPv4 management address is not set, system uses the first available IPv4 management address.<br>Otherwise, system uses a pre-defined value. By default, this value will be 192.0.2.1. |
| **Mode** | Specify the MVR mode of operation. In Dynamic mode, MVR allows dynamic MVR membership reports on source ports. In Compatible mode, MVR membership reports are forbidden on source ports. The default is Dynamic mode. |
| **Tagging** | Specify whether the traversed IGMP/MLD control frames will be sent as Untagged or Tagged with MVR VID. The default is Tagged. |
| **Priority** | Specify how the traversed IGMP/MLD control frames will be sent in prioritized manner. The default Priority is 0. |
| **LLQI** | Define the maximum time to wait for IGMP/MLD report memberships on a receiver port before removing the port from multicast group membership. The value is in units of tenths of a seconds. The range is from 0 to 31744. The default LLQI is 5 tenths or one-half second. |
| **Interface Channel Profile** | When the MVR VLAN is created, select the IPMC Profile as the channel filtering condition for the specific MVR VLAN. Summary about the Interface Channel Profiling (of the MVR VLAN) will be shown by clicking the view button. Profile selected for designated interface channel is not allowed to have overlapped permit group address. |
| **Profile Management Button** | You can inspect the rules of the designated profile by using the following button:<br>  : List the rules associated with the designated profile. |

| Immediate Leave Setting | |
|---|---|
| **Port** | The logical port for the settings. |
| **Port Role** | Configure an MVR port of the designated MVR VLAN as one of the following roles.<br>**Inactive**: The designated port does not participate MVR operations.<br>**Source**: Configure uplink ports that receive and send multicast data as source ports. Subscribers cannot be directly connected to source ports.<br>**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.<br>**Be Caution**: MVR source ports are not recommended to be overlapped with management VLAN ports.<br>Select the port role by clicking the Role symbol to switch the setting.<br>I indicates Inactive; S indicates Source; R indicates Receiver<br>The default Role is Inactive. |
| **Immediate Leave** | Enable the fast leave on the port.<br>System will remove group record and stop forwarding data upon receiving the IGMPv2/MLDv1 leave message without sending last member query messages.<br>It is recommended to enable this feature only when a single IGMPv2/MLDv1 host is connected to the specific port. |

| Buttons | |
|---|---|
| Add New MVR VLAN | Click to add new MVR VLAN. Specify the VID and configure the new entry. Click "Save". |
| Delete | Click to delete the entry. |
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

## 2.3.67 IGMP Snooping - Basic Configuration

This page provides IGMP Snooping related configuration.




| Object | Description |
|---|---|
| **Snooping Enabled** | Enable the Global IGMP Snooping. |
| **Unregistered IPMCv4 Flooding Enabled** | Enable unregistered IPMCv4 traffic flooding.<br>The flooding control takes effect only when IGMP Snooping is enabled.<br>When IGMP Snooping is disabled, unregistered IPMCv4 traffic flooding is always active in spite of this setting. |
| **IGMP SSM Range** | SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address range. |
| **Leave Proxy Enabled** | Enable IGMP Leave Proxy. This feature can be used to avoid forwarding |

| | |
|---|---|
| | unnecessary leave messages to the router side. |
| **Proxy Enabled** | Enable IGMP Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side. |
| **Router Port** | Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier.<br>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.<br>System will remove group record and stop forwarding data upon receiving the IGMPv2 leave message without sending last member query messages.<br>It is recommended to enable this feature only when a single IGMPv2 host is connected to the specific port. |
| **Throttling** | Enable to limit the number of multicast groups to which a switch port can belong. |

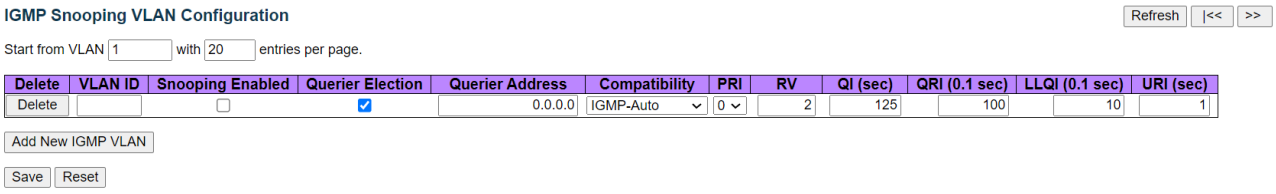
| **Buttons** | |
|---|---|
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

## 2.3.68 IGMP Snooping - VLAN Configuration

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

The "VLAN" input fields allow the user to select the starting point in the VLAN Table. Clicking the Refresh button will update the displayed table starting from that or the next closest VLAN Table match.

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



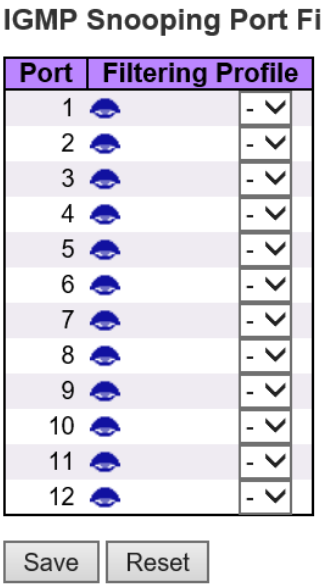

| Object | Description |
|---|---|
| **Delete (For 30W PoE Model)** | Check to delete the entry. The designated entry will be deleted during the next save. |
| **VLAN ID** | The VLAN ID of the entry. |
| **IGMP Snooping Enabled** | Enable the per-VLAN IGMP Snooping. Up to 64 VLANs can be selected for 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.<br>When the Querier address is not set, system uses IPv4 management address of the IP interface associated with this VLAN.<br>When the IPv4 management address is not set, system uses the first available IPv4 management address.<br>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.<br>It indicates the IGMP control frame priority level generated by the system. These values can be used to prioritize different classes of traffic.<br>The allowed range is `0` (best effort) to `7` (highest), default interface priority value is 0. |
| **RV** | Robustness Variable.<br>The Robustness Variable allows tuning for the expected packet loss on a network.<br>The allowed range is `1` to `255`, default robustness variable value is 2. |
| **QI** | Query Interval.<br>The Query Interval is the interval between General Queries sent by the Querier.<br>The allowed range is `1` to `31744` seconds, default query interval is 125 seconds. |
| **QRI** | Query Response Interval.<br>The Maximum Response Delay used to calculate the Maximum Response Code inserted into the periodic General Queries.<br>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.<br>The Last Member Query Time is the time value represented by the Last Member Query Interval, multiplied by the Last Member Query Count.<br>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.<br>The allowed range is `0` to `31744` seconds, default unsolicited report interval is 1 second. |

| **Buttons** | |
|---|---|
| Refresh | Refreshes the displayed table starting from the "VLAN" input fields. |
| \|<< | Updates the table starting from the first entry in the VLAN Table, i.e. the entry with the lowest VLAN ID. |
| >> | Updates the table, starting with the entry after the last entry currently displayed. |

| | |
|---|---|
| Delete | Click to delete the entry. |
| Add New IGMP VLAN | Click to add new IGMP VLAN. Specify the VID and configure the new entry. Click "Save". The specific IGMP VLAN starts working after the corresponding static VLAN is also created. |
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

## 2.3.69 IGMP Snooping - Port Filtering Profile

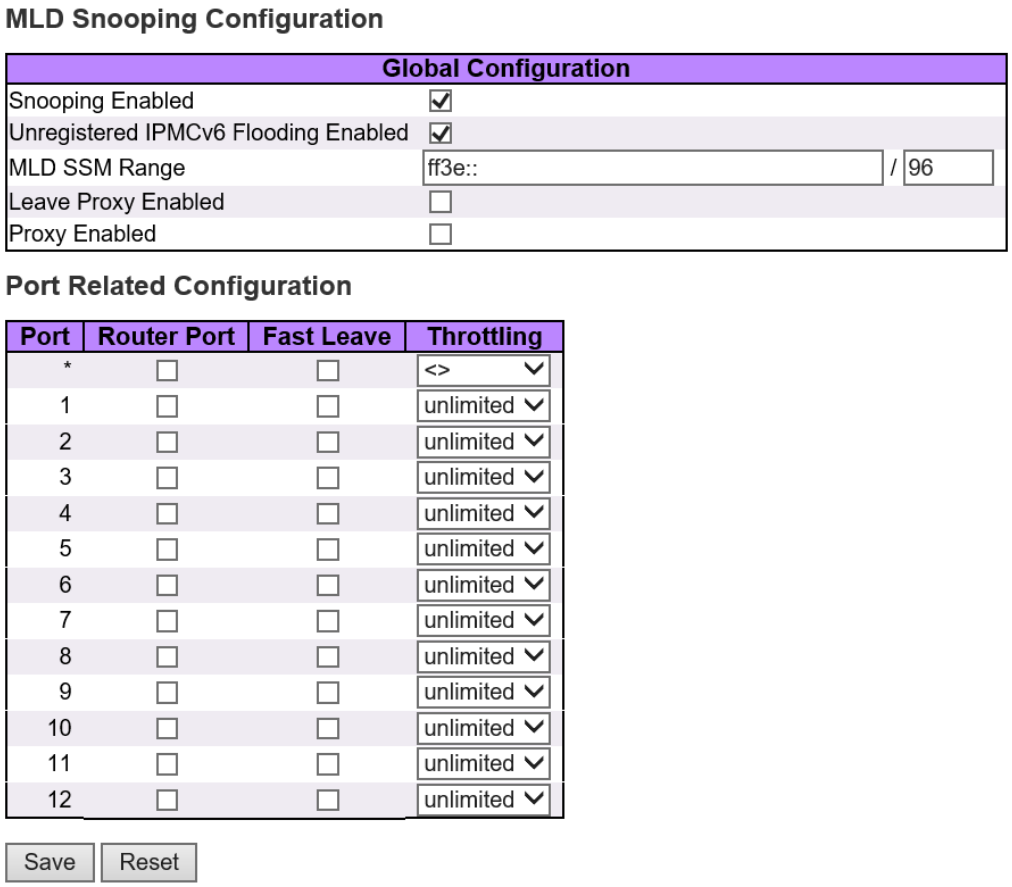



| Object | Description |
|---|---|
| **Port** | The logical port for the settings. |
| **Filtering Profile** | Select the IPMC Profile as the filtering condition for the specific port. Summary about the designated profile will be shown by clicking the view button. |
| **Profile Management Button** | You can inspect the rules of the designated profile by using the following button: : List the rules associated with the designated profile. |

| Buttons | |
|---|---|
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

## 2.3.70 MLD Snooping - Basic Configuration

This page provides MLD Snooping related configuration.




| Object | Description |
|---|---|
| **Snooping Enabled** | Enable the Global MLD Snooping. |
| **Unregistered IPMCv6 Flooding Enable** | Enable unregistered IPMCv6 traffic flooding.<br>The flooding control takes effect only when MLD Snooping is enabled.<br>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.<br>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. |
| **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.<br>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.<br>System will remove group record and stop forwarding data upon receiving the MLDv1 leave message without sending last member query messages.<br>It is recommended to enable 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. |

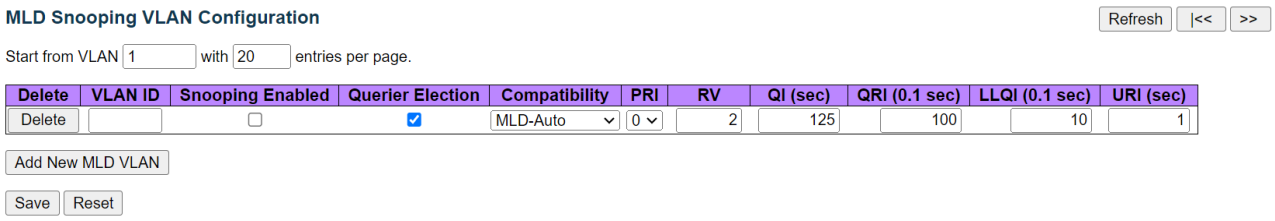
| **Buttons** | |
|---|---|
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

## 2.3.71 MLD Snooping - VLAN Configuration

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

The "VLAN" input fields allow the user to select the starting point in the VLAN Table. Clicking the Refresh button will update the displayed table starting from that or the next closest VLAN Table match.

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



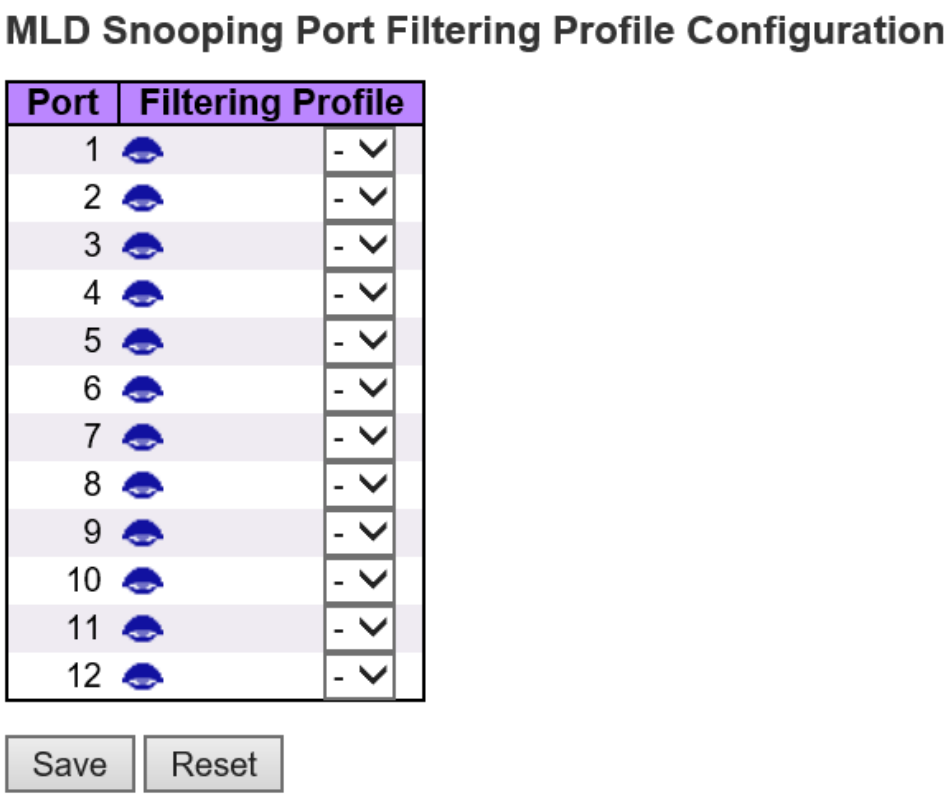

| Object | Description |
|---|---|
| **Delete (For 30W PoE Model)** | Check to delete the entry. The designated entry will be deleted during the next save. |
| **VLAN ID** | The VLAN ID of the entry. |
| **MLD Snooping Enabled (For 90W PoE Model)** | Enable the per-VLAN MLD Snooping. Up to 64 VLANs can be selected for MLD Snooping. |
| **MLD Snooping Enabled (For 30W PoE Model)** | Enable the per-VLAN MLD Snooping. Up to 32 VLANs can be selected for MLD Snooping. |
| **Querier Election** | Enable to join MLD Querier election in the VLAN. Disable to act as a MLD Non-Querier. |
| **Compatibility** | Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of MLD operating on hosts and routers within a network. The allowed selection is `MLD-Auto`, `Forced MLDv1`, `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.<br>The allowed range is `0` (best effort) to `7` (highest), default interface priority value is 0. |
| **RV** | Robustness Variable.<br>The Robustness Variable allows tuning for the expected packet loss on a link.<br>The allowed range is `1` to `255`, default robustness variable value is 2. |
| **QI** | Query Interval.<br>The Query Interval is the interval between General Queries sent by the Querier.<br>The allowed range is `1` to `31744` seconds, default query interval is 125 seconds. |
| **QRI** | Query Response Interval.<br>The Maximum Response Delay used to calculate the Maximum Response Code inserted into the periodic General Queries.<br>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.<br>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.<br>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.<br>The Unsolicited Report Interval is the time between repetitions of a node's initial report of interest in a multicast address.<br>The allowed range is `0` to `31744` seconds, default unsolicited report interval is 1 second. |

| **Buttons** | |
|---|---|
| Refresh | Refreshes the displayed table starting from the "VLAN" input fields. |
| \|<< | Updates the table starting from the first entry in the VLAN Table, i.e. the entry with the lowest VLAN ID. |
| >> | Updates the table, starting with the entry after the last entry currently displayed. |
| Add New MLD VLAN | Click to add new MLD VLAN. Specify the VID and configure the new entry. Click "Save". The specific MLD VLAN starts working |

| | |
|---|---|
| | after the corresponding static VLAN is also created. |
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

## 2.3.72 MLD Snooping - Port Filtering Profile



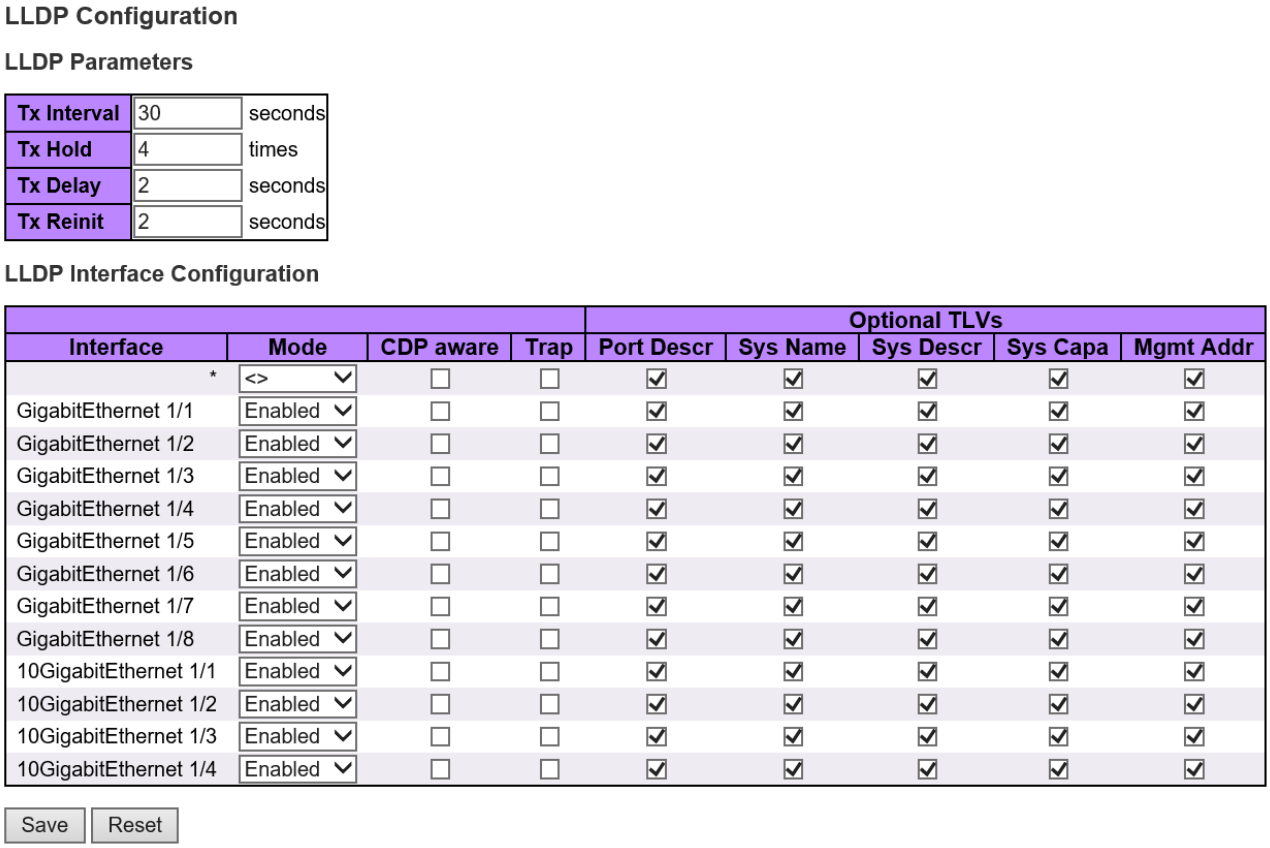

| Object | Description |
|---|---|
| **Port** | The logical port for the settings. |
| **Filtering Profile** | Select the IPMC Profile as the filtering condition for the specific port. Summary about the designated profile will be shown by clicking the view button. |
| **Profile Management Button** | You can inspect the rules of the designated profile by using the following button: : List the rules associated with the designated profile. |

| Buttons | |
|---|---|
| Save | Click to save changes. |

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

## 2.3.73 LLDP

This page allows the user to inspect and configure the current LLDP port settings.



**LLDP Configuration**

**LLDP Parameters**

| | | |
|---|---|---|
| **Tx Interval** | 30 | seconds |
| **Tx Hold** | 4 | times |
| **Tx Delay** | 2 | seconds |
| **Tx Reinit** | 2 | seconds |

**LLDP Interface Configuration**

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

Save Reset

| Object | Description |
|---|---|
| **LLDP Parameters** | |
| **Tx Interval** | The switch periodically transmits LLDP frames to its neighbors for having the network discovery information up-to-date. The interval between each LLDP frame is determined by the **Tx Interval** value. Valid values are restricted to 5 - 32768 seconds. |
| **Tx Hold** | Each LLDP frame contains information about how long the information in the LLDP frame shall be considered valid. The LLDP information valid period is set to **Tx Hold** multiplied by **Tx Interval** seconds. Valid values are restricted to 2 - 10 times. |
| **Tx Delay** | If some configuration is changed (e.g. the IP address) a new LLDP frame is transmitted, but the time between the LLDP frames will always be at least the value of **Tx Delay** seconds. **Tx Delay** cannot be larger than 1/4 of the **Tx Interval** value. Valid values are restricted to 1 - 8192 seconds. |

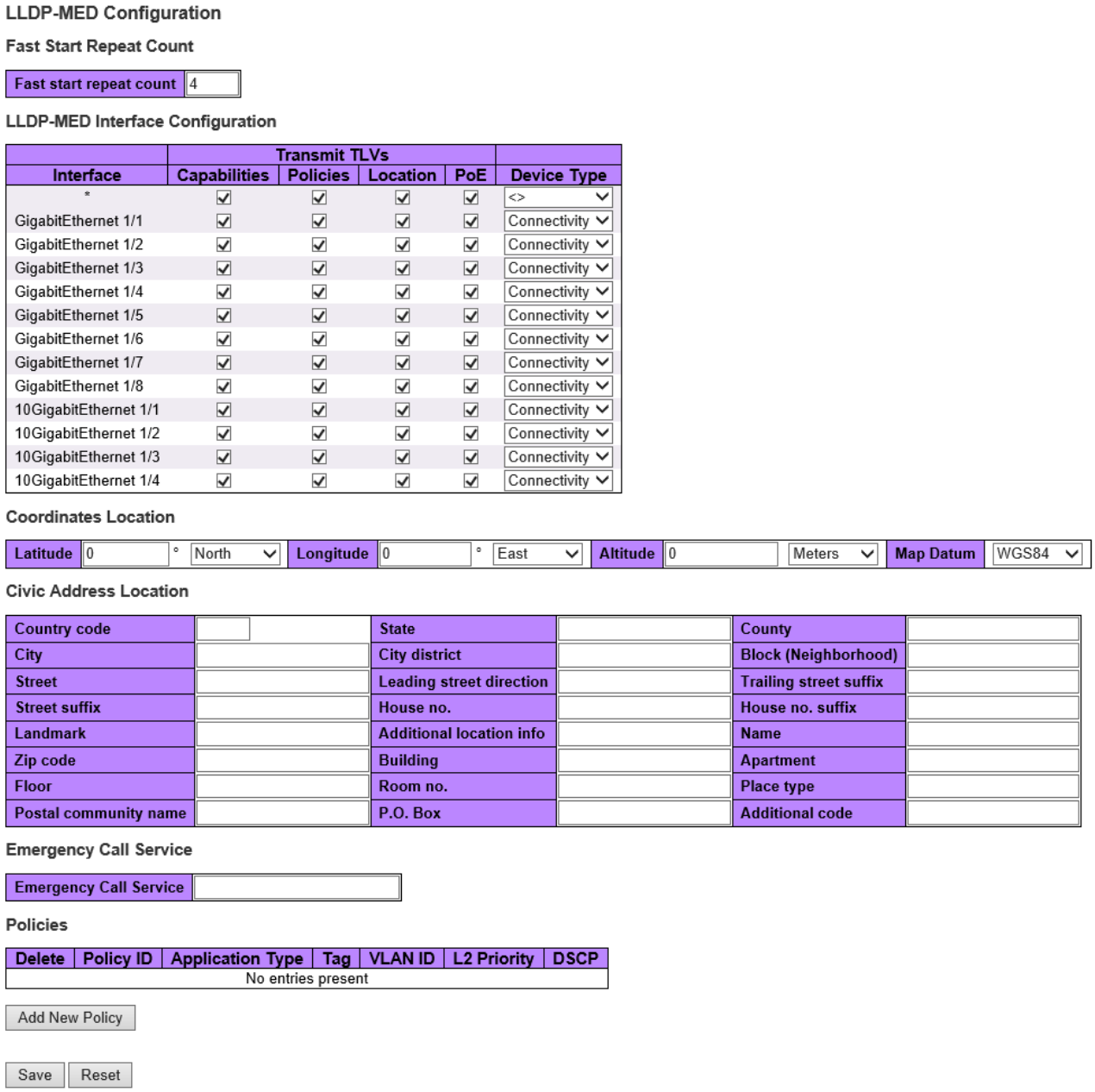
| | |
|---|---|
| **Tx Reinit** | When a port is disabled, LLDP is disabled or the switch is rebooted, an LLDP shutdown frame is transmitted to the neighboring units, signalling that the LLDP information isn't valid anymore. **Tx Reinit** controls the amount of seconds between the shutdown frame and a new LLDP initialization. Valid values are restricted to 1 - 10 seconds. |
| **LLDP Port Parameters** | |
| **Interface** | The switch port number of the logical LLDP port. |
| **Mode** | Select LLDP mode.<br>**`Rx only`** The switch will not send out LLDP information, but LLDP information from neighbor units is analyzed.<br>**`Tx only`** The switch will drop LLDP information received from neighbors, but will send out LLDP information.<br>**`Disabled`** The switch will not send out LLDP information, and will drop LLDP information received from neighbors.<br>**`Enabled`** The switch will send out LLDP information, and will analyze LLDP information received from neighbors. |
| **CDP Aware** | Select CDP awareness.<br>The CDP operation is restricted to decoding incoming CDP frames (The switch doesn't transmit CDP frames). CDP frames are only decoded if LLDP on the port is enabled.<br>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.<br>CDP TLV "Device ID" is mapped to the LLDP "Chassis ID" field.<br>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.<br>CDP TLV "Port ID" is mapped to the LLDP "Port ID" field.<br>CDP TLV "Version and Platform" is mapped to the LLDP "System Description" field.<br>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.<br>If all ports have CDP awareness disabled the switch forwards CDP frames received from neighbor devices. If at least one port has CDP awareness enabled all CDP frames are terminated by the switch.<br>Note: When CDP awareness on a port 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. |

| **Buttons** | |
|---|---|
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

## 2.3.74 LLDP-MED

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



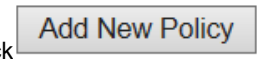

| Object | Description |
|---|---|
| **Fast start repeat count** | |
| **Fast start repeat count** | Rapid startup and Emergency Call Service Location Identification Discovery of endpoints is a critically important aspect of VoIP systems in general. In addition, it is best to advertise only those pieces of information which are specifically relevant to |

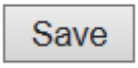
| | |
|---|---|
| | particular endpoint types (for example only advertise the voice network policy to permitted voice-capable devices), both in order to conserve the limited LLDPU space and to reduce security and system integrity issues that can come with inappropriate knowledge of the network policy.<br>With this in mind LLDP-MED defines an LLDP-MED Fast Start interaction between the protocol and the application layers on top of the protocol, in order to achieve these related properties. Initially, a Network Connectivity Device will only transmit LLDP TLVs in an LLDPDU. Only after an LLDP-MED Endpoint Device is detected, will an LLDP-MED capable Network Connectivity Device start to advertise LLDP-MED TLVs in outgoing LLDPDUs on the associated port. The LLDP-MED application will temporarily speed up the transmission of the LLDPDU to start within a second, when a new LLDP-MED neighbor has been detected in order share LLDP-MED information as fast as possible to new neighbors.<br>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.<br>It should be noted that LLDP-MED and the LLDP-MED Fast Start mechanism is only intended to run on links between LLDP-MED Network Connectivity Devices and Endpoint Devices, and as such does not apply to links between LAN infrastructure elements, including Network Connectivity Devices, or other types of links. |
| **LLDP Interface Configuration** | |
| **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 (For 90W PoE Model)** | 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<br>An LLDP-MED Network Connectivity Device is a LAN access device based on any of the following technologies.<br>1. LAN Switch/Router<br>2. IEEE 802.1 Bridge<br>3. IEEE 802.3 Repeater (included for historical reasons)<br>4. IEEE 802.11 Wireless Access Point<br>5. Any device that supports the IEEE 802.1AB and MED extensions that can relay IEEE 802 frames via any method.<br>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.<br>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.<br>Even though a switch always should be a Network Connectivity Device, it is possible to configure it to act as an Endpoint Device, and thereby start the LLDP-MED information exchange (In the case where two Network Connectivity Devices are connected together) |
| **Coordinates Location** | |
| **Latitude** | **Latitude** SHOULD be normalized to within 0-90 degrees with a maximum of 4 digits.<br>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.<br>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 -32767 to 32767 with a maximum of 4 digits.<br>It is possible to select between two altitude types (floors or meters).<br>**Meters**: Representing meters of Altitude defined by the vertical datum specified.<br>**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:<br>**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).<br>**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** | |
| **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** | Unit (Apartment, suite) - Example: Apt 42. |
| **Floor** | Floor - Example: 4. |
| **Room no.** | Room number - Example: 450F. |
| **Place type** | Place type - Example: Office. |
| **Postal community name** | Postal community name - Example: Leonia. |
| **P.O. Box** | Post office box (P.O. BOX) - Example: 12345. |
| **Additional code** | Additional code - Example: 1320300003. |
| **Emergency Call Service** | |
| **Emergency Call Service** | **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** | |
| **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 ports. |
| **Application Type** | Intended use of the application types:<br>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.<br>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.<br>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.<br>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.<br>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.<br>6. **Video Conferencing** - for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services.<br>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.<br>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.<br>**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.<br>**Tagged** indicates that the device is using the IEEE 802.1Q tagged frame format, and that both the VLAN ID and the Layer 2 priority values are being used, as well as the DSCP value. The tagged format includes an additional field, known as the tag header. The tagged frame format also includes priority tagged frames as defined by IEEE 802.1Q-2003. |
| **VLAN ID** | VLAN identifier (VID) for the port as defined in IEEE 802.1Q-2003. |
| **L2 Priority** | **L2 Priority** is the Layer 2 priority to be used for the specified application type. **L2 Priority** may specify one of eight priority levels (0 through 7), as defined by IEEE 802.1D-2004. A value of 0 represents use of the default priority as defined in IEEE 802.1D-2004. |
| **DSCP** | **DSCP** value to be used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474. **DSCP** may contain one of 64 code point values (0 through 63). A value of 0 represents use of the default DSCP value as defined in RFC 2475. |
| **Adding a new policy** | Click  to add a new policy. Specify the **Application type**, **Tag**, **VLAN ID**, **L2 Priority** and **DSCP** for the new policy. Click "Save".<br>The number of policies supported is 32 |
| **Port Policies Configuration** | |
| **Port** | The port number to which the configuration applies. |
| **Policy Id** | The set of policies that shall apply to a given port. The set of policies is selected by check marking the checkboxes that corresponds to the policies. |

| **Buttons** | |
|---|---|
|  | Click to save changes. |
|  | Click to undo any changes made locally and revert to previously saved values. |
|  | Click to delete the entry. |

## 2.3.75 Fabric Attach - FA Configuration

### FA Configuration

#### Global Configuration

| | |
|---|---|
| **FA Enable** | Enabled |
| **Extended Logging** | Disabled |
| **Display Level** | Error(major) |
| **Discovery Timeout(Sec)** | 240 |
| **Assignment Timeout(Sec)** | 240 |

#### Port Related Configuration

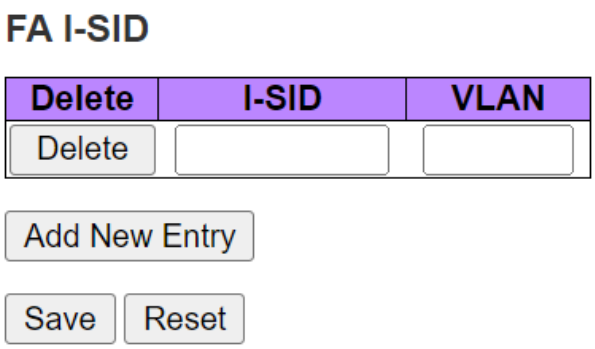
| Port | Enable | | Message Authentication Key | | Key Mode |
|---|---|---|---|---|---|
| 1 | ☑ | ☑ | | | Strict |
| 2 | ☑ | ☑ | | | Strict |
| 3 | ☑ | ☑ | | | Strict |
| 4 | ☑ | ☑ | | | Strict |
| 5 | ☑ | ☑ | | | Strict |
| 6 | ☑ | ☑ | | | Strict |
| 7 | ☑ | ☑ | | | Strict |
| 8 | ☑ | ☑ | | | Strict |
| 9 | ☑ | ☑ | | | Strict |
| 10 | ☑ | ☑ | | | Strict |
| 11 | ☑ | ☑ | | | Strict |
| 12 | ☑ | ☑ | | | Strict |

Save Reset

| Object | Description |
|---|---|
| Global Configuration | |
| **FA Enable** | Activate FA Client, FA function would standby right now. Valid values are Enabled/Disabled. Default value is "Enabled". |
| **Extended Logging** | To Control Extended Logging function. Valid values are Enabled/Disabled. Default value is "Disabled". |
| **Display Level** | This setting will control print message for console. Valid values are Error(major)/ Error(minor)/ Warning/Notice/Information. Default value is "Error(major)". |
| **Discovery Timeout(Sec)** | Discovery elements timeout. This value is the timeout for discovery elements TLV in LLDP package. Valid values are 45~480 seconds. Default value is "240" seconds. |
| **Assignment** | Assignment timeout. This value is the timeout for assignment TLV in LLDP package. |

| | |
|---|---|
| **Timeout(Sec)** | Valid values are 45~480 seconds. Default value is "240" seconds. |
| **Port Related Configuration** | |
| **Port** | Interface port number. |
| **Enable** | Select Enable check box Checked/Unchecked to control FA client function by port. Default is Unchecked(Copper Port), Checked(Fiber port). |
| **Message Authentication Key** | The check box is to control use authentication or not. Default value is unchecked. Fill Message Authentication Key twice and select check box when you want activate the Authentication. (not checked, no Fabric Attach Authentication) Text field is user define authentication key(range 0~32 characters). These two text fields should be the same. |
| **Key Mode** | Valid values are Strick/Standard. Default value is "Strick". Strick use only default authentication key. Standard use only user-defined authentication key. |

## 2.3.76 Fabric Attach - FA I-SID

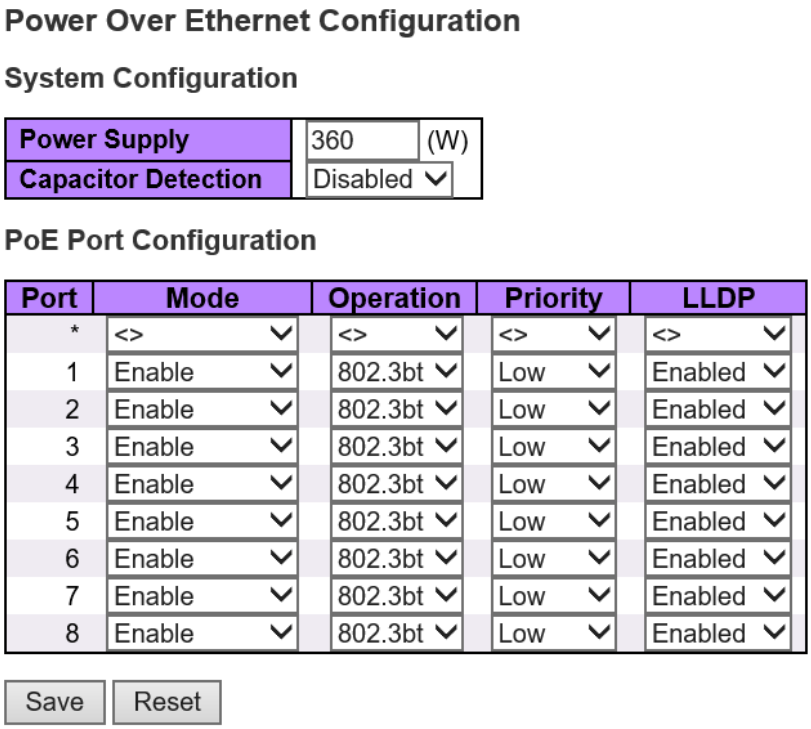



| Object | Description |
|---|---|
| **Delete** | Prepare delete data for enable check box. Click delete button to delete. |
| **I-SID** | Specifies the I-SID of the specific I-SID-to-VLAN assignment to remove. Valid values range from 1 to 16777214. |
| **VLAN** | Specifies the VLAN of the specific I-SID-to-VLAN assignment to remove. Valid values range from 1 to 4095. |

## 2.3.77 PoE

This page allows the user to inspect and configure the current PoE port settings.

90W PoE Model




| Object | Description |
|---|---|
| **System Configuration** | |
| **Power Supply** | For systems with external power supply, the available power supply must be specified. For systems with built-in power supply, the available power is shown. Values are in Watts. |
| **Port Configuration** | |
| **Port** | This is the logical port number for this row.<br>Ports that are not PoE-capable are not shown. |
| **PoE Mode** | The PoE Mode represents the PoE mode for the port.<br>Disable : PoE disabled for the port.<br>Enable : Enables PoE for the port.<br>Schedule : Enables PoE for the port by scheduling.<br>Auto-Restart : Enables PoE for the port by scheduling, and also provides the ICMP Ping Detection for Auto-Restart PD in additional. |

| | |
|---|---|
| **Operation Mode** | The Operation Mode represents the PoE operating mode for the port.<br>Disabled : PoE disabled for the port.<br>AT/AF : Enables PoE IEEE 802.3at/af compliant mode<br>uPoE : Enables PoE IEEE 802.3bt 60W<br>802.3bt : Enables PoE IEEE 802.3bt 90W<br>PoH : Enables PoE PoH |
| **Priority** | The Priority represents the ports priority. There are three levels of power priority named Low, High and Critical.<br>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. |
| **LLDP** | The LLDP configures the port behaviour with respect to LLDP.<br>Enable : PoE parameters received through LLDP are processed.<br>Disable : PoE parameters received through LLDP are ignored.<br>Please note that LLDP protocol is configured by its own configuration page and transmission of PoE information via LLDP can be configured with the LLDP-MED configuration page. |

| **Buttons** | |
|---|---|
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

30W PoE Model

### Power Over Ethernet Configuration

| | | | |
|---|---|---|---|
| **Reserved Power determined by** | ◉ Class | ○ Allocation | ○ LLDP-MED |
| **Power Management Mode** | ○ Actual Consumption | ◉ Reserved Power | |

### PoE Power Supply Configuration

| Primary Power Supply [W] |
|---|
| 120 |

### PoE Port Configuration

| Port | Mode | Operation | Priority | Maximum Power [W] |
|---|---|---|---|---|
| * | <> | <> | <> | 15.4 |
| 1 | Disable | 802.3af | Low | 15.4 |
| 2 | Disable | 802.3af | Low | 15.4 |
| 3 | Disable | 802.3af | Low | 15.4 |
| 4 | Disable | 802.3af | Low | 15.4 |

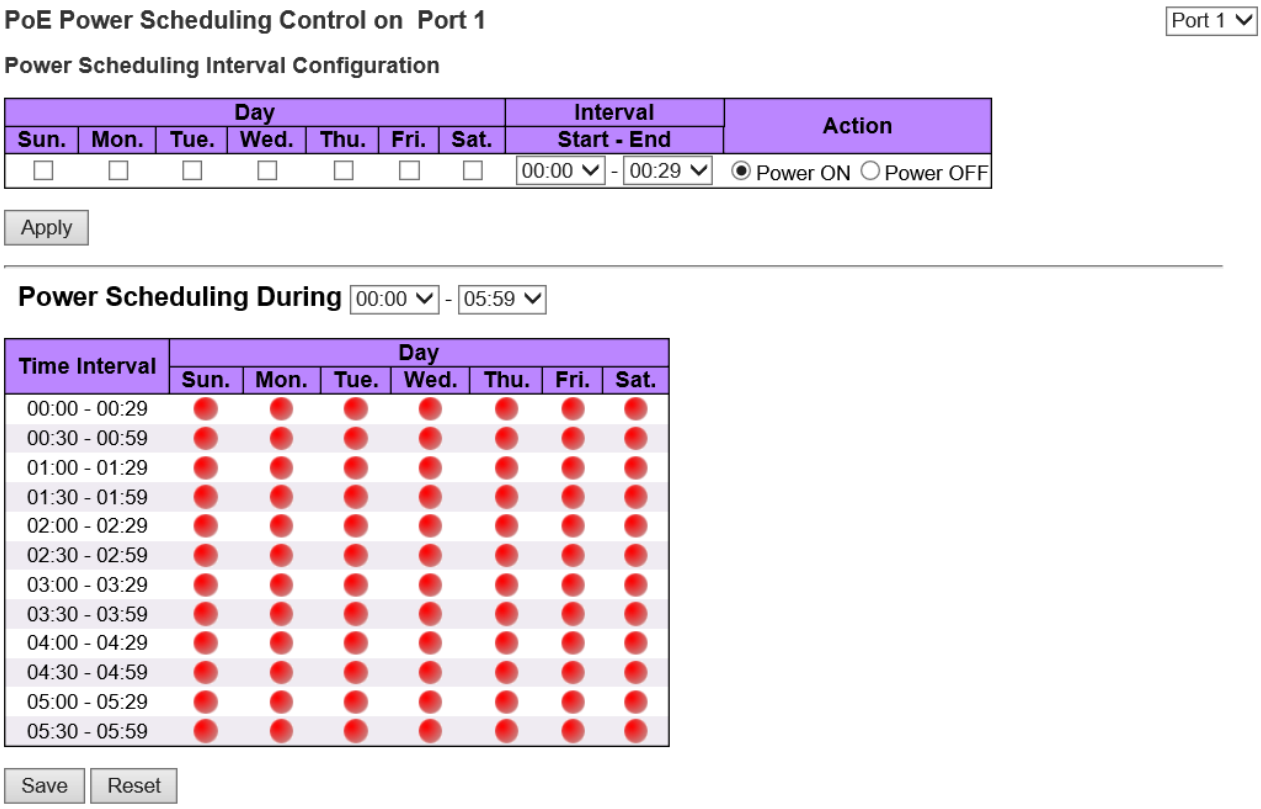
Save Reset

| Object | Description |
|---|---|
| **Power Over Ethernet Configuration** | |
| **Reserved Power determined by** | There are three modes for configuring how the ports/PDs may reserve power.<br>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.<br>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.<br>In this mode the Maximum Power fields have no effect.<br>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<br>In this mode the Maximum Power fields have no effect<br>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:<br>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.<br>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. |
| **Power Supply Configuration** | |
| **Power Source** | 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.<br>Valid values are in the range 0 to 120 Watts. |
| **Port Configuration** | |
| **Port** | This is the logical port number for this row.<br>Ports that are not PoE-capable are not shown. |
| **PoE Mode** | The PoE Mode represents the PoE operating mode for the port.<br>Disable : PoE disabled for the port.<br>Enable : Enables PoE for the port.<br>Schedule : Enables PoE for the port by scheduling. |
| **Operation Mode** | The Operation Mode represents the PoE power operating protocol for the port.<br>802.3af : Sets PoE protocol to IEEE 802.3af.<br>802.3at : Sets PoE protocol to IEEE 802.3at.<br>PoH : Sets PoE protocol to PoH. |
| **Priority** | The Priority represents the ports priority. There are three levels of power priority named Low, High and Critical.<br>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. |
| **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.<br>Valid values are in the range 0 to 30 Watts. |

| **Buttons** | |
|---|---|
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

## 2.3.78 Power Scheduler

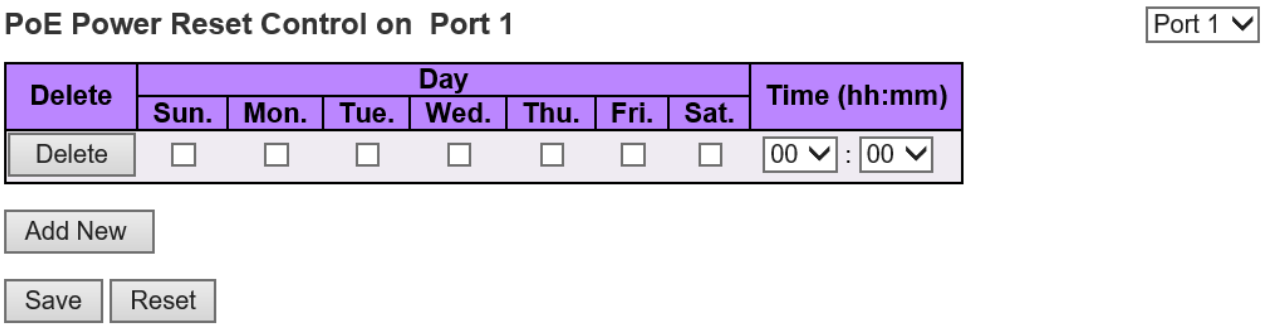



| Object | Description |
|---|---|
| **Power Scheduling Interval Configuration** | |
| **Day** | Checkmarks indicate which day are members of the set. |
| **Interval** | Start - Select the start hour and minute.<br>End - Select the end hour and minute. |
| **Action** | Power On - Select the radio button to apply power on during the interval.<br>Power Off - Select the radio button to apply power off during the interval. |
| **Power Scheduling During** | |
| **Time Interval** | There are 48 time interval one day. Each interval have 30 minutes. |
| **Day** | The current scheduling state is displayed graphically during the week.<br>Green indicates the power is on and red that it is off. Directly changes checkmarks to indicate which day are members of the time interval.<br>Check or uncheck as needed to modify the scheduling table. |

| Buttons |
|---|

| | |
|---|---|
| Apply | Click to apply the power scheduling interval. |
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

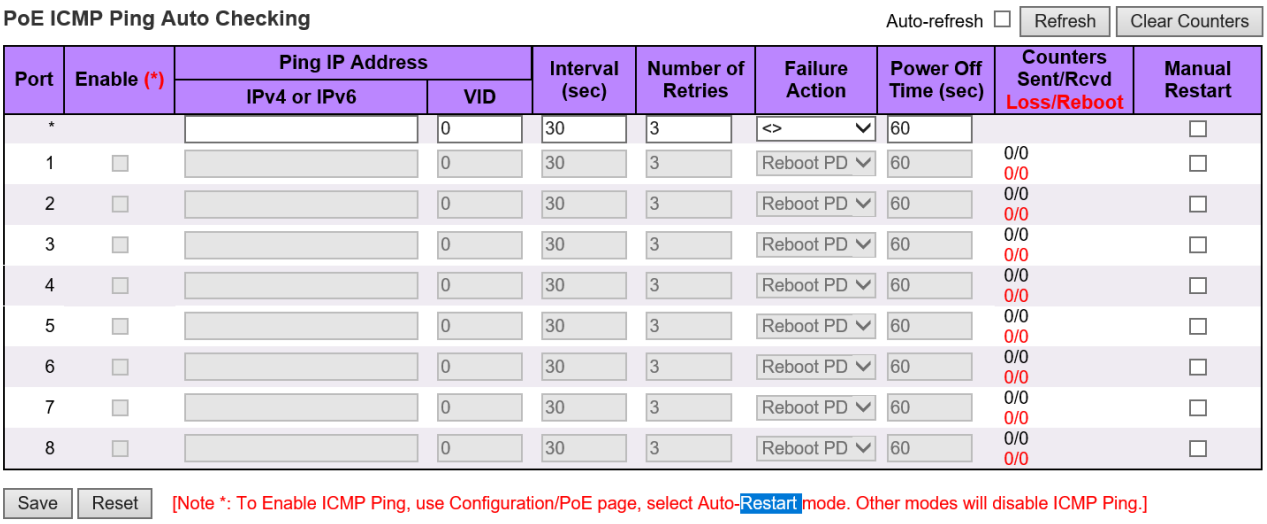
## 2.3.79 Power Reset




| Object | Description |
|---|---|
| **Delete** | Check to delete the entry.<br>The designated entry will be deleted during the next save. |
| **Day** | Checkmarks indicate which day are members of the entry. Check or uncheck as needed to modify the entry. |
| **Time (hh:mm)** | hh - Select the hour.<br>mm - Select the minute. |

| Buttons | |
|---|---|
| Add New : | Click to add new reset entry. |
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

## 2.3.80 Ping Auto Checking (For 90W PoE Model)

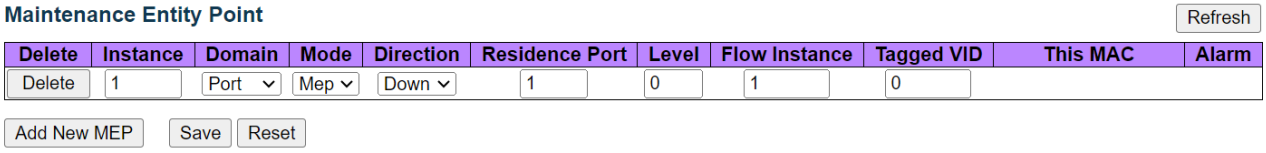



| Object | Description |
|---|---|
| **Port** | This is the logical port number for this row.<br>Ports not PoE-capable will not be available here. |
| **Enable** | ICMP Ping Checking function is Enabled/Disabled. In this page it is status for READ ONLY, to enable/disable it in PoE main configuration page. Select "Auto-Restart" option below the Schedule option. If Auto-Restart is selected, the Schedule still valid and works. So, if the Auto-Restart option is selected, PoE Schedule must be configured, otherwise, there could be no power output for PoE Ports.<br>Note:<br>There are 2 conditions that ping won't be started:<br>1. When IP is not valid, like 0.0.0.0.<br>2. When PoE port has no power output, it could be due to no PD connected, or power off per schedule configuration. |
| **Ping IP Address IPv4 or IPv6** | IPv4 or IPv6 address of PD for Ping detection per port. If IPv6 is used, must input the VID (VLAN ID). Default is ipv4 0.0.0.0. |
| **VID** | VLAN ID. If IPv6 address is input for Ping detection per port, VID should be set, range 1 ~ 4094. |
| **Interval (sec)** | Time interval in second per port, Ping starts when time waiting exceeds this interval since last round, but it would NOT be on time due to wait for other port. Range: 10 ~ 120 seconds. |
| **Number of Retries** | Number of ping retry, system will run the ping repeatly. If retry number is 5, then ping 5+1 times. Range: 1 ~ 5. |
| **Failure Action** | If ping, including ping retry, has no any packet received, it is a ping failure event. If |

| | |
|---|---|
| | failure event happens, system can do nothing or reboot PD per this option. Reboot PD means poe port will stop power output, wait for Power-Off Time and start power output again. |
| **Power Off Time (sec)** | Time of PD being power-off if ping failure event happens. If Failure Action is do nothing, this time parameter is not used. Range: 3 ~ 120sec. |
| **Counters Sent/Rcvd/Loss/Reboot** | Counters of ping packet sent/received/loss and reboot PD. Counters can be reset manually, if switch reboot, counters reset also. |
| **Manual Restart** | Restart the PD immediately. PoE of this port will disabled and enabled in 3~5 seconds. But the restart will NOT count in the reboot number. |

| **Buttons** | |
|---|---|
| Auto-refresh ☐ | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |
| Refresh | Click to refresh the page immediately. |
| Clear Counters : | Click to reset counters. |
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

## 2.3.81 MEP (For 30W PoE Model)



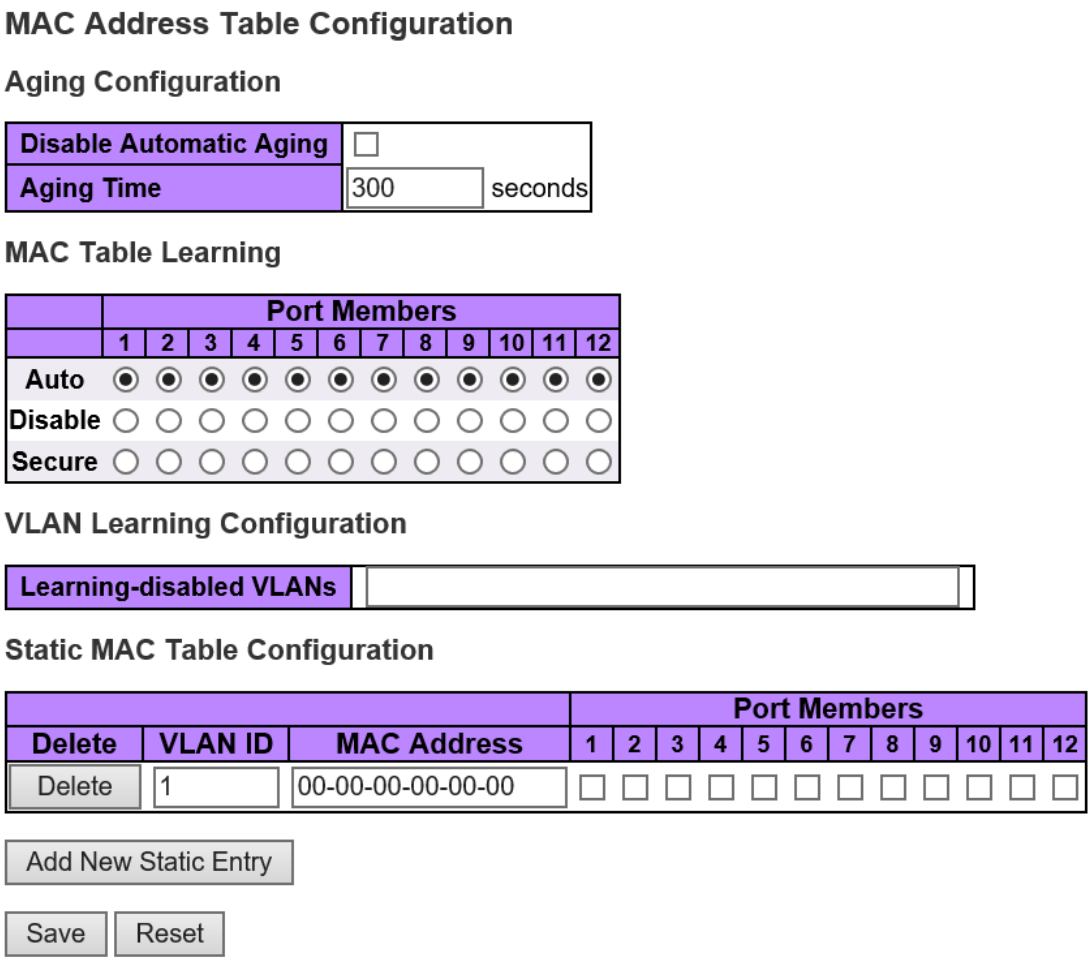

| Object | Description |
|---|---|
| **Delete** | This box is used to mark a MEP for deletion in next Save operation. |
| **Instance** | The ID of the MEP. Click on the ID of a MEP to enter the configuration page. The range is from 1 through 100. |
| **Domain** | Port: This is a MEP in the Port Domain. |
| **Mode** | MEP: This is a Maintenance Entity End Point.<br>MIP: This is a Maintenance Entity Intermediate Point. |
| **Direction** | Down: This is a Down MEP - monitoring ingress OAM and traffic on 'Residence Port'.<br>Up: This is a Up MEP - monitoring egress 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.<br>EVC MEP: This is not used.<br>VLAN MEP: This is not used.<br>EVC MIP: On Serval, this is the Subscriber VID that identify the subscriber flow in this EVC where the MIP is active.<br>This MAC |
| **This MAC** | The MAC of this MEP - can be used by other MEP when unicast is selected (Info only). |
| **Alarm** | There is an active alarm on the MEP. |

| Buttons | |
|---|---|
| Add New MEP: | Click to add a new MEP entry. |
| Refresh | Click to refresh the page immediately. |

| | |
|---|---|
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

## 2.3.82 MAC Table

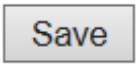
The MAC Address Table is configured on this page. Set timeouts for entries in the dynamic MAC Table and configure the static MAC table here.




| Object | Description |
|---|---|
| Aging Configuration | |
| **Disable Automatic Aging** | Disable the automatic aging of dynamic entries by ticking the item. |
| **Aging Time** | Enter a value in seconds.<br>The allowed range is `10` to `1000000` seconds. |

| VLAN Learning Configuration | |
|---|---|
| **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.<br>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. |
| **MAC Table Learning** | |
| **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.<br>**Note:** Make sure that the link used for managing the switch is added to the Static Mac Table before changing to secure learning mode, otherwise the management link is lost and can only be restored by using another non-secure port or by connecting to the switch via the serial interface. |
| **Static MAC Table Learning** | |
| **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. |
| **Adding a New Static Entry** | Click  to add a new entry to the static MAC table. Specify the VLAN ID, MAC address, and port members for the new entry. Click "Save". |

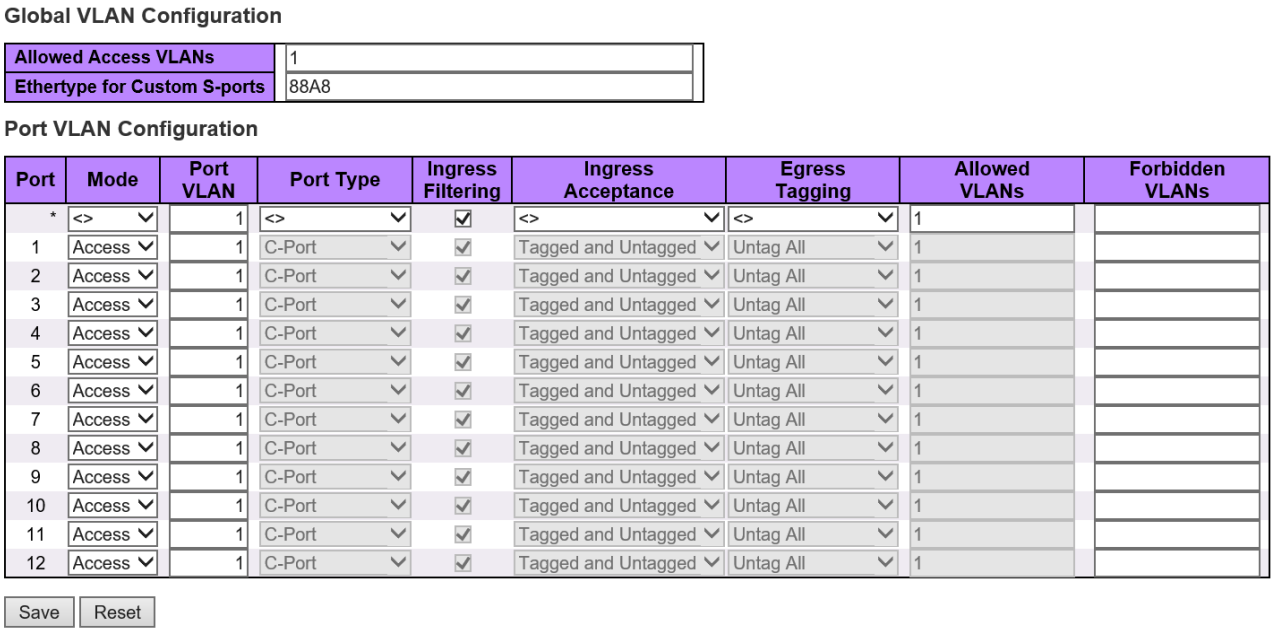


| Buttons | |
|---|---|
|  | Click to save changes. |
|  | Click to undo any changes made locally and revert to previously saved values. |
|  | Click to delete the entry. |

## 2.3.83 VLANs - Configuration

This page allows for controlling VLAN configuration on the switch.

The page is divided into a global section and a per-port configuration section.



Global VLAN Configuration

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

Port VLAN Configuration

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

Save Reset

| Object | Description |
|---|---|
| **Global VLAN Configuration** | |
| **Allowed Access VLANs** | This field shows the allowed Access VLANs, i.e. it only affects ports configured as Access ports. Ports in other modes are members of all VLANs specified in the Allowed VLANs field. By default, only VLAN 1 is enabled. More VLANs may be created by using a list syntax where the individual elements are separated by commas. Ranges are specified with a dash separating the lower and upper bound. The following example will create VLANs 1, 10, 11, 12, 13, 200, and 300: `1,10-13,200,300`. Spaces are allowed in between the delimiters. |
| **Ethertype for Custom S-ports** | This field specifies the ethertype/TPID (specified in hexadecimal) used for Custom S-ports. The setting is in force for all ports whose Port Type is set to S-Custom-Port. |
| **Port VLAN Configuration** | |
| **Port** | This is the logical port number of this row. |
| **Mode** | The port mode (default is Access) determines the fundamental behavior of the port in question. A port can be in one of three modes as described below.<br>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.<br>Grayed out fields show the value that the port will get when the mode is applied.<br><br>**Access:**<br>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:<br>• Member of exactly one VLAN, the Port VLAN (a.k.a. Access VLAN), which by default is 1<br>• Accepts untagged and C-tagged frames<br>• Discards all frames that are not classified to the Access VLAN<br>• On egress all frames classified to the Access VLAN are transmitted untagged. Other (dynamically added VLANs) are transmitted tagged<br>**Trunk:**<br>Trunk ports can carry traffic on multiple VLANs simultaneously, and are normally used to connect to other switches. Trunk ports have the following characteristics:<br>• By default, a trunk port is member of all VLANs (1-4095)<br>• The VLANs that a trunk port is member of may be limited by the use of Allowed VLANs<br>• Frames classified to a VLAN that the port is not a member of are discarded<br>• 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<br>• Egress tagging can be changed to tag all frames, in which case only tagged frames are accepted on ingress<br>**Hybrid:**<br>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:<br>• Can be configured to be VLAN tag unaware, C-tag aware, S-tag aware, or S-custom-tag aware<br>• Ingress filtering can be controlled<br>• Ingress acceptance of frames and configuration of egress tagging can be configured independently |
| **Port VLAN** | Determines the port's VLAN ID (a.k.a. PVID). Allowed VLANs are in the range 1 through 4095, default being 1.<br>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).<br>On egress, frames classified to the Port VLAN do not get tagged if Egress Tagging configuration is set to untag Port VLAN.<br>The Port VLAN is called an "Access VLAN" for ports in Access mode and Native VLAN for ports in Trunk or Hybrid mode. |
| **Port Type** | Ports in hybrid mode allow for changing the port type, that is, whether a frame's VLAN tag is used to classify the frame on ingress to a particular VLAN, and if so, which TPID it reacts on. Likewise, on egress, the Port Type determines the TPID of the tag, if a tag is required.<br>**Unaware:**<br>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.<br>**C-Port:**<br>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.<br>**S-Port:**<br>On ingress, frames with a VLAN tag with TPID = 0x8100 or 0x88A8 get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with an S-tag.<br>**S-Custom-Port:**<br>On ingress, frames with a VLAN tag with a TPID = 0x8100 or equal to the Ethertype configured for Custom-S ports get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with the custom S-tag. |
| **Ingress Filtering** | Hybrid ports allow for changing ingress filtering. Access and Trunk ports always have ingress filtering enabled.<br>If ingress filtering is enabled (checkbox is checked), frames classified to a VLAN that the port is not a member of get discarded.<br>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.<br>**Tagged and Untagged**<br>Both tagged and untagged frames are accepted.<br>**Tagged Only** |

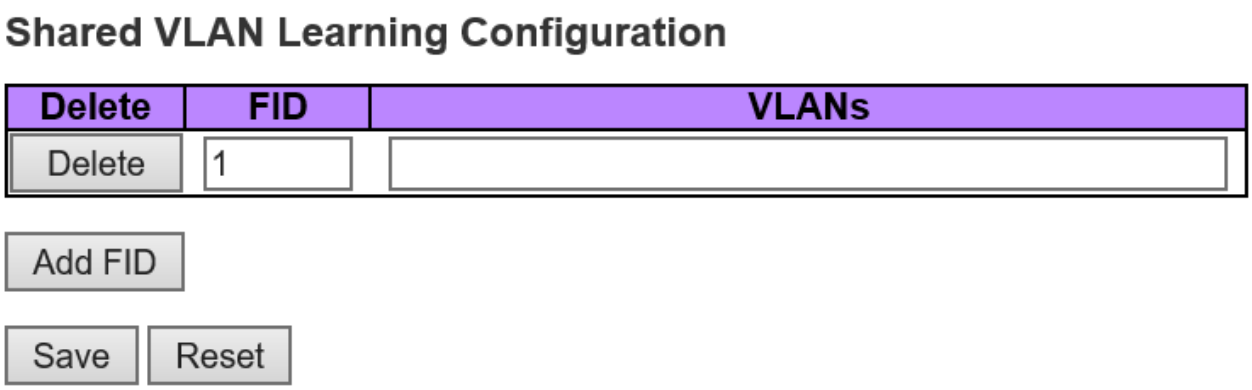
| | |
|---|---|
| | Only tagged frames are accepted on ingress. Untagged frames are discarded.<br>**Untagged Only**<br>Only untagged frames are accepted on ingress. Tagged frames are discarded. |
| **Egress Tagging** | Ports in Trunk and Hybrid mode may control the tagging of frames on egress.<br>**Untag Port VLAN**<br>Frames classified to the Port VLAN are transmitted untagged. Other frames are transmitted with the relevant tag.<br>**Tag All**<br>All frames, whether classified to the Port VLAN or not, are transmitted with a tag.<br>**Untag All**<br>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.<br>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`.<br>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 be member of one or more VLANs. This is particularly useful when dynamic VLAN protocols like MVRP and GVRP must be prevented from dynamically adding ports to VLANs.<br>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.<br>By default, the field is left blank, which means that the port may become a member of all possible VLANs. |

| **Buttons** | |
|---|---|
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

## 2.3.84 VLANs – SVL (For 90W PoE Model)

This page allows for controlling SVL configuration on the switch.

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




| Object | Description |
|---|---|
| **Delete** | A previously allocated FID can be deleted by the use of this button. |
| **FID** | The Filter ID (FID) is the ID that VLANs get learned on in the MAC table when SVL is in effect.<br>No two rows in the table can have the same FID and the FID must be a number between 1 and 4095. |
| **VLANs** | List of VLANs mapped into FID.<br>The syntax is as follows: Individual VLANs are separated by commas. Ranges are specified with a dash separating the lower and upper bound.<br>The following example will map VLANs 1, 10, 11, 12, 13, 200, and 300: 1,10-13,200,300. Spaces are allowed in between the delimiters. The range of valid VLANs is 1 to 4095.<br>The same VLAN can only be a member of one FID. A message will be displayed if one VLAN is grouped into two or more FIDs.<br>All VLANs must map to a particular FID, and by default VLAN x maps to FID x. This implies that if FID x is defined, then VLAN x is implicitly a member of FID x unless it is specified for another FID. If FID x doesn't exist, a confirmation message will be displayed, asking whether to continue adding VLAN x implicitly to FID x. |

| Buttons | |
|---|---|
| Save | Click to save changes. |

| | |
|---|---|
| Reset | Click to undo any changes made locally and revert to previously saved values. |
| Delete | Click to delete the entry. |
| Add FID : | Add a new row to the SVL table. The FID will be pre-filled with the first unused FID. |

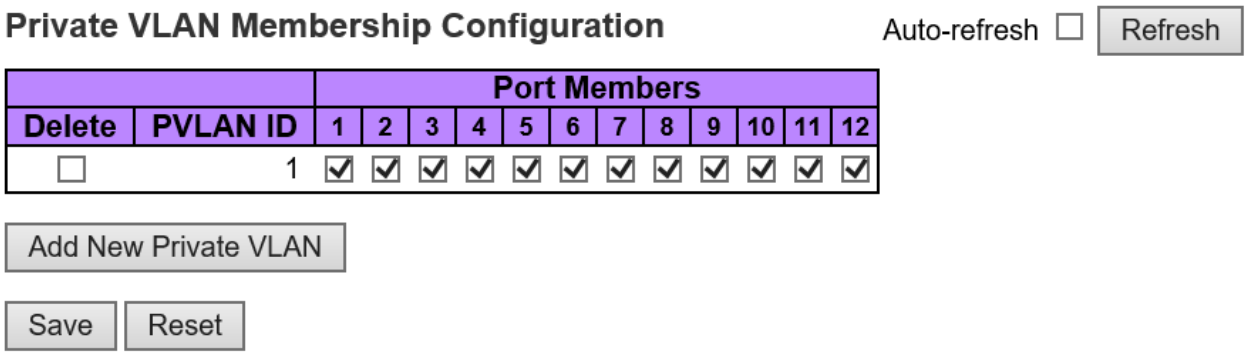
## 2.3.85 Private VLANs - Membership

The Private VLAN membership configurations for the switch can be monitored and modified here. Private VLANs can be added or deleted here. Port members of each Private VLAN can be added or removed here.

Private VLANs are based on the source port mask, and there are no connections to VLANs. This means that VLAN IDs and Private VLAN IDs can be identical.

A port must be a member of both a VLAN and a Private VLAN to be able to forward packets. By default, all ports are VLAN unaware and members of VLAN 1 and Private VLAN 1.

A VLAN unaware port can only be a member of one VLAN, but it can be a member of multiple Private VLANs.




| Object | Description |
|---|---|
| **Delete** | To delete a private VLAN entry, check this box. The entry will be deleted during the next save. |
| **PVLAN 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. |

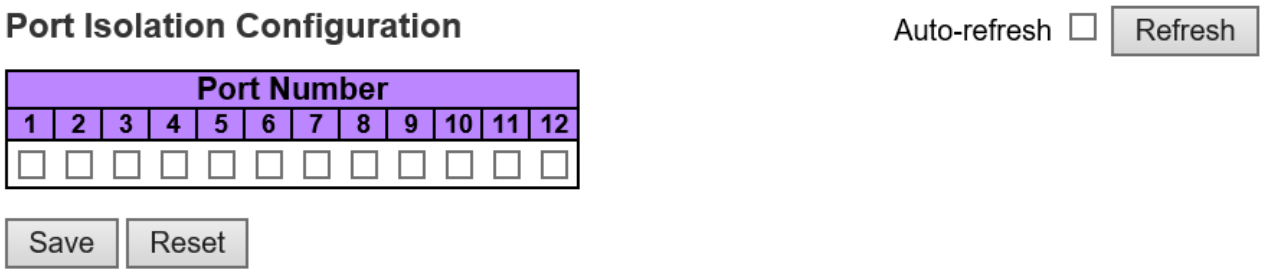
| | |
|---|---|
| **Adding a New Private VLAN** | Click Add New Private VLAN to add a new private VLAN ID. An empty row is added to the table, and the private VLAN can be configured as needed. The allowed range for a private VLAN ID is the same as the switch port number range. Any values outside this range are not accepted, and a warning message appears. Click "OK" to discard the incorrect entry, or click "Cancel" to return to the editing and make a correction.<br>The Private VLAN is enabled when you click "Save".<br>The Delete button can be used to undo the addition of new Private VLANs. |

| **Buttons** | |
|---|---|
| Auto-refresh ☐ | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |
| Refresh | Click to refresh the page immediately. |
| Add New Private VLAN | Click to add a new private VLAN ID |
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

## 2.3.86 Port Isolation

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.

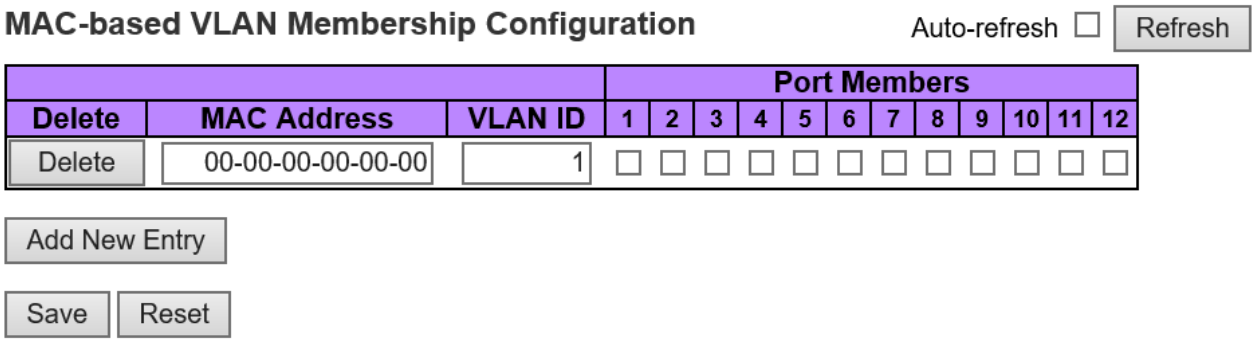



| Object | Description |
|---|---|
| **Port Members** | A check box is provided for each port of a private VLAN.<br>When checked, port isolation is enabled on that port.<br>When unchecked, port isolation is disabled on that port.<br>By default, port isolation is disabled on all ports. |

| Buttons | |
|---|---|
| Auto-refresh ☐ | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |
| Refresh | Click to refresh the page immediately. |
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

## 2.3.87 VCL - MAC-based VLAN

The MAC-based VLAN entries can be configured here. This page allows for adding and deleting MAC-based VLAN entries and assigning the entries to different ports. This page shows only static entries.

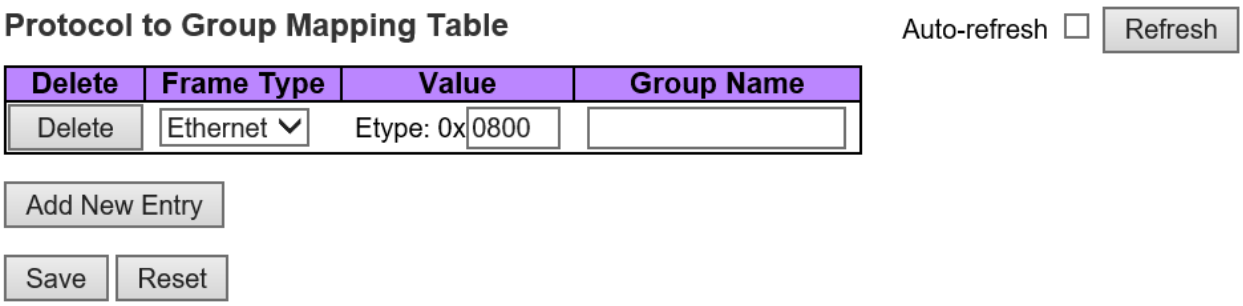



| Object | Description |
|---|---|
| **Delete** | To delete a MAC-based VLAN entry, check this box and press save. The entry will be deleted in the stack. |
| **MAC Address** | Indicates the MAC address of the mapping. |
| **VLAN ID** | Indicates the VLAN ID the above MAC will be mapped to. |
| **Port Members** | A row of check boxes for each port is displayed for each MAC-based VLAN entry. To include a port in a MAC-based VLAN, check the box. To remove or exclude the port from the MAC-based VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked. |
| **Adding a New MAC-based VLAN** | Click Add New Entry to add a new MAC-based VLAN entry. An empty row is added to the table, and the MAC-based VLAN entry can be configured as needed. Any unicast MAC address can be configured for the MAC-based VLAN entry. No broadcast or multicast MAC addresses are allowed. Legal values for a VLAN ID are `1` through `4095`.<br>The MAC-based VLAN entry is enabled when you click on "Save". A MAC-based VLAN without any port members will be deleted when you click "Save".<br>The Delete button can be used to undo the addition of new MAC-based VLANs.<br>The maximum possible MAC-based VLAN entries are limited to 256. |

| Buttons | |
|---|---|
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |
| Auto-refresh ☐ | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |
| Refresh | Refreshes the displayed table. |

## 2.3.88 Protocol-based VLAN - Protocol to Group

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



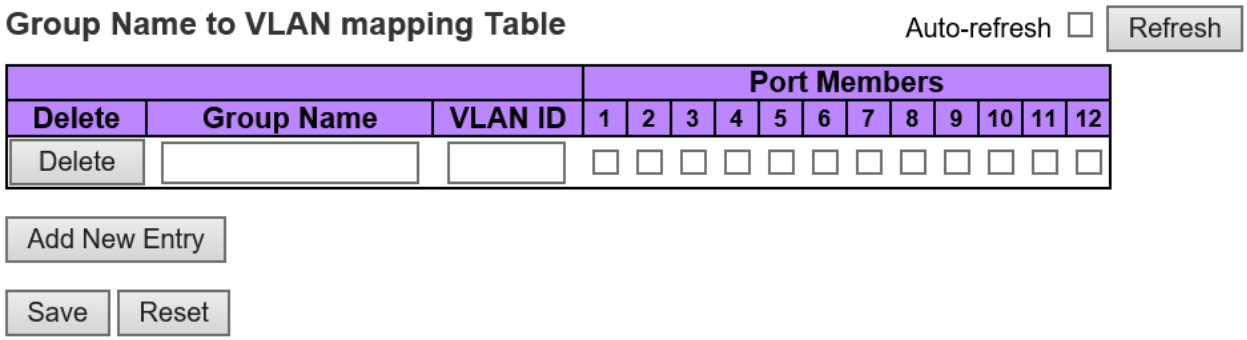

| Object | Description |
|---|---|
| **Delete** | To delete a Protocol to Group Name map entry, check this box. The entry will be deleted on the switch during the next Save. |
| **Frame Type** | Frame Type can have one of the following values:<br>**Ethernet**<br>**LLC**<br>**SNAP**<br>Note: On changing the Frame type field, valid value of the following text field will vary depending on the new frame type you selected. |
| **Value** | Valid value that can be entered in this text field depends on the option selected from the preceding Frame Type selection menu.<br>Below is the criteria for three different Frame Types:<br>**For Ethernet:** Values in the text field when Ethernet is selected as a Frame Type is called etype. Valid values for etype ranges from 0x0600-0xffff<br>**For LLC:** Valid value in this case is comprised of two different sub-values.<br>a. **DSAP:** 1-byte long string (0x00-0xff)<br>b. **SSAP:** 1-byte long string (0x00-0xff)<br>**For SNAP:** Valid value in this case also is comprised of two different sub-values.<br>a. **OUI:** OUI (Organizationally Unique Identifier) is value in format of xx-xx-xx where each pair (xx) in string is a hexadecimal value ranges from 0x00-0xff.<br>b. **PID:** If the OUI is hexadecimal 000000, the protocol ID is the Ethernet type (EtherType) field value for the protocol running on top of SNAP; if the 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.<br>In other words, if value of OUI field is 00-00-00 then value of PID will be etype (0x0600-0xffff) and if value of OUI is other than 00-00-00 then valid value of PID will be any value from 0x0000 to 0xffff. |
| **Group Name** | A valid Group Name is a unique 16-character long string for every entry which consists of a combination of alphabets (a-z or A-Z) and integers(0-9).<br>**Note:** special character and underscore(_) are not allowed. |
| **Adding a New Group to VLAN mapping entry** | Click Add New Entry to add a new entry in mapping table. An empty row is added to the table; Frame Type, Value and the Group Name can be configured as needed.<br>The Delete button can be used to undo the addition of new entry. The maximum possible Protocol to Group mappings are limited to 128. |

| Buttons | |
|---|---|
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |
| Delete | The button can be used to undo the addition of new entry. The maximum possible Protocol to Group mappings are limited to 128. |
| Add New Entry | Click to add a new entry in mapping table. |
| Auto-refresh ☐ | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |
| Refresh | Click to refresh the page immediately. |

## 2.3.89 Protocol-based VLAN - Group to VLAN

This page allows you to map an already configured Group Name to a VLAN for the switch.

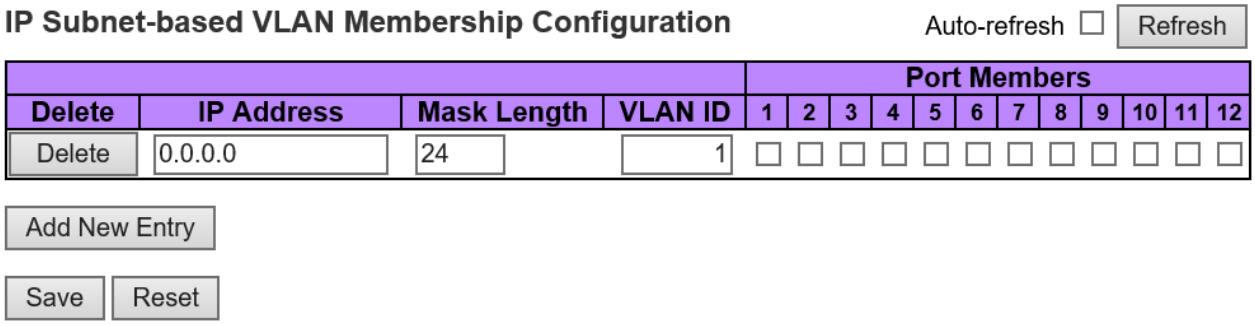



| Object | Description |
|---|---|
| **Delete** | To delete a Group Name to VLAN map entry, check this box. The entry will be deleted on the switch during the next Save. |
| **Group Name** | A valid Group Name is a string, at the most 16 characters long, which consists of a combination of alphabets (a-z or A-Z) and integers(0-9) with no special characters allowed. You may either use a Group that already includes one or more protocols (see Protocol to Group mappings), or create a Group to VLAN ID mapping that will become active the moment you add one or more protocols inside that Group. Furthermore, the Group to VLAN ID mapping is not unique, as long as the port lists of these mappings are mutually exclusive (e.g. Group1 can be mapped to VID 1 on port#1 and to VID 2 on port#2). |
| **VLAN ID** | Indicates the ID to which Group Name will be mapped. A valid VLAN ID ranges from 1-4095. |
| **Port Members** | A row of check boxes for each port is displayed for each Group Name to VLAN ID mapping. To include a port in a mapping, check the box. To remove or exclude the port from the mapping, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked. |
| **Adding a New Group to VLAN mapping entry** | Click Add New Entry to add a new entry in mapping table. An empty row is added to the table, the Group Name, VLAN ID and port members can be configured as needed. Legal values for a VLAN ID are `1` through `4095`.<br>The Delete button can be used to undo the addition of new entry. The maximum possible Group to VLAN mappings are limited to 64. |

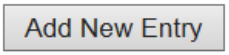
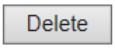
| Buttons | |
|---|---|
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |
| Add New Entry | Click to add a new entry in mapping table. Legal values for a VLAN ID are **1** through **4095**. |
| Delete | The button can be used to undo the addition of new entry. The maximum possible Group to VLAN mappings are limited to 64. |
| Auto-refresh ☐ | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |
| Refresh | Click to refresh the page immediately. |

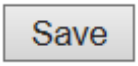
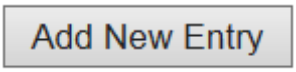
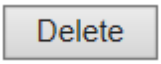
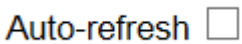
## 2.3.90 VCL - IP Subnet-based VLAN

The IP subnet-based VLAN entries can be configured here. This page allows for adding, updating and deleting IP subnet-based VLAN entries and assigning the entries to different ports. This page shows only static entries.



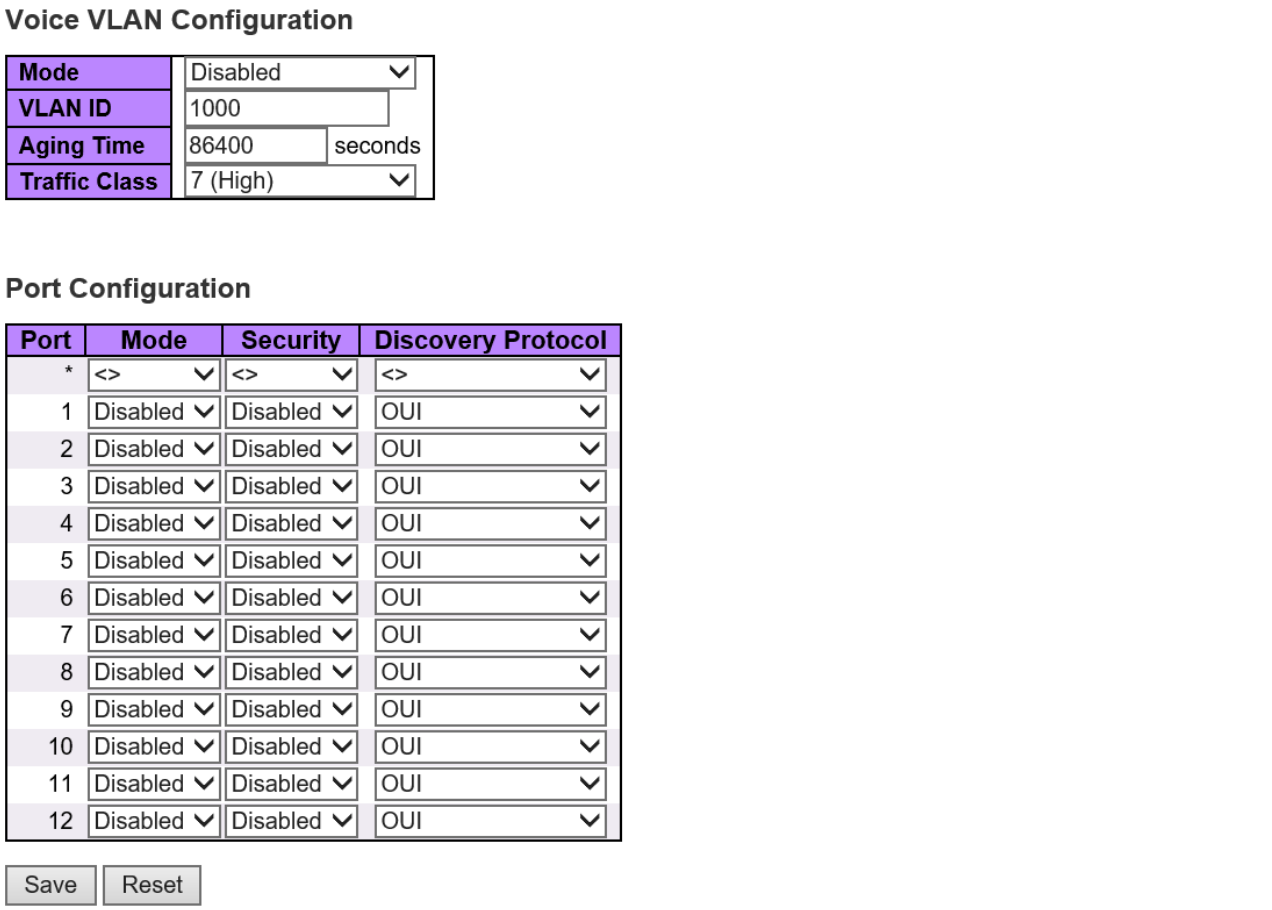

| Object | Description |
|---|---|
| **Delete** | To delete a IP subnet-based VLAN entry, check this box and press save. The entry will be deleted in the stack. |
| **IP Address** | Indicates the subnet's IP address (Any of the subnet's host addresses can be also provided here, the application will convert it automatically). |

| | |
|---|---|
| **Mask Length** | Indicates the network 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-based VLAN entry. To include a port in a IP subnet-based VLAN, check the box. To remove or exclude the port from the IP subnet-based VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked. |
| **Adding a New IP subnet-based VLAN** | Click  to add a new IP subnet-based VLAN entry. An empty row is added to the table, and the IP subnet-based VLAN entry can be configured as needed. Any IP address/mask can be configured for the IP subnet-based VLAN entry. Legal values for a VLAN ID are 1 through 4095.<br><br>The IP subnet-based VLAN entry is enabled when you click on "Save". The  button can be used to undo the addition of new IP subnet-based VLANs. The maximum possible IP subnet-based VLAN entries are limited to 128. |

| Buttons | |
|---|---|
|  | Click to save changes. |
|  | Click to undo any changes made locally and revert to previously saved values. |
|  | Click to add a new IP subnet-based VLAN entry. Legal values for a VLAN ID are `1` through `4095`. |
|  | The button can be used to undo the addition of new IP subnet-based VLANs. The maximum possible IP subnet-based VLAN entries are limited to 128. |
|  | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |
|  | Refreshes the displayed table. |

## 2.3.91 Voice VLAN - Configuration

The Voice VLAN feature enables voice traffic forwarding on the Voice VLAN, then the switch can classify and schedule network traffic. It is recommended that there be two VLANs on a port - one for voice, one for data. Before connecting the IP device to the switch, the IP phone should configure the voice VLAN ID correctly. It should be configured through its own GUI.




| Object | Description |
|---|---|
| Voice VLAN Configuration | |
| **Mode** | Indicates the Voice VLAN mode operation. We must disable MSTP feature before we enable Voice VLAN. It can avoid the conflict of ingress filtering. Possible modes are:<br>`Enabled`: Enable Voice VLAN mode operation.<br>`Disabled`: Disable Voice VLAN mode operation. |
| **VLAN ID** | Indicates the Voice VLAN ID. It should be a unique VLAN ID in the system and cannot equal each port PVID. It is a conflict in configuration if the value equals management VID, MVR VID, PVID etc. The allowed range is `1` to `4095`. |

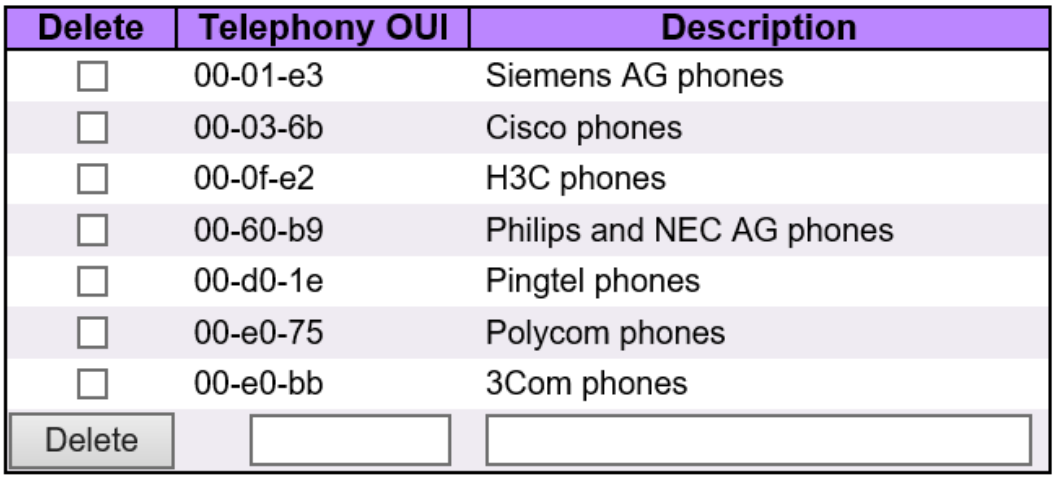
| | |
|---|---|
| **Aging Time** | Indicates the Voice VLAN secure learning aging time. The allowed range is `10` to `10000000` seconds. It is used when security mode or auto detect mode is enabled. In other cases, it will be based on hardware aging time. The actual aging time will be situated between the [age_time; 2 * age_time] interval. |
| **Traffic Class** | Indicates the Voice VLAN traffic class. All traffic on the Voice VLAN will apply this class. |
| **Port Configuration** | |
| **Port Mode** | Indicates the Voice VLAN port mode. Possible port modes are:<br>`Disabled`: Disjoin from Voice VLAN.<br>`Auto`: Enable auto detect mode. It detects whether there is VoIP phone attached to the specific port and configures the Voice VLAN members automatically.<br>`Forced`: Force join to Voice VLAN. |
| **Port Security** | Indicates the Voice VLAN port security mode. When the function is enabled, all non-telephonic MAC addresses in the Voice VLAN will be blocked for 10 seconds. Possible port modes are:<br>`Enabled`: Enable Voice VLAN security mode operation.<br>`Disabled`: Disable Voice VLAN security mode operation. |
| **Port Discovery Protocol** | Indicates the Voice VLAN port discovery protocol. It will only work when auto detect mode is enabled. We should enable LLDP feature before configuring discovery protocol to "LLDP" or "Both". Changing the discovery protocol to "OUI" or "LLDP" will restart auto detect process. Possible discovery protocols are:<br>`OUI`: Detect telephony device by OUI address.<br>`LLDP`: Detect telephony device by LLDP.<br>`Both`: Both OUI and LLDP. |

| **Buttons** | |
|---|---|
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

## 2.3.92 Voice VLAN OUI

Configure VOICE VLAN OUI table on this page. The maximum number of entries is `16`. Modifying the OUI table will restart auto detection of OUI process.

## Voice VLAN OUI Table




| Object | Description |
|---|---|
| **Delete** | Check to delete the entry. It will be deleted during the next save. |
| **Telephony OUI** | A telephony OUI address is a globally unique identifier assigned to a vendor by IEEE. It must be 6 characters long and the input format is "xx-xx-xx" (x is a hexadecimal digit). |
| **Description** | The description of OUI address. Normally, it describes which vendor telephony device it belongs to. The allowed string length is `0` to `32`. |

| Buttons | |
|---|---|
| Add New Entry | Click to add a new access management entry. |
| Delete | Click to delete the entry. |
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

## 2.3.93 QoS - Port Classification

This page allows you to configure the basic QoS Ingress Classification settings for all switch ports.

**QoS Port Classification**

| Port | Ingress | | | | | | | | Egress |
|---|---|---|---|---|---|---|---|---|---|
| | CoS | DPL | PCP | DEI | CoS ID | Tag Class. | DSCP Based | Map | Map |
| * | <> | <> | <> | <> | <> | | ☐ | | |
| 1 | 0 | 0 | 0 | 0 | 0 | Disabled | ☐ | | |
| 2 | 0 | 0 | 0 | 0 | 0 | Disabled | ☐ | | |
| 3 | 0 | 0 | 0 | 0 | 0 | Disabled | ☐ | | |
| 4 | 0 | 0 | 0 | 0 | 0 | Disabled | ☐ | | |
| 5 | 0 | 0 | 0 | 0 | 0 | Disabled | ☐ | | |
| 6 | 0 | 0 | 0 | 0 | 0 | Disabled | ☐ | | |
| 7 | 0 | 0 | 0 | 0 | 0 | Disabled | ☐ | | |
| 8 | 0 | 0 | 0 | 0 | 0 | Disabled | ☐ | | |
| 9 | 0 | 0 | 0 | 0 | 0 | Disabled | ☐ | | |
| 10 | 0 | 0 | 0 | 0 | 0 | Disabled | ☐ | | |
| 11 | 0 | 0 | 0 | 0 | 0 | Disabled | ☐ | | |
| 12 | 0 | 0 | 0 | 0 | 0 | Disabled | ☐ | | |

Save Reset

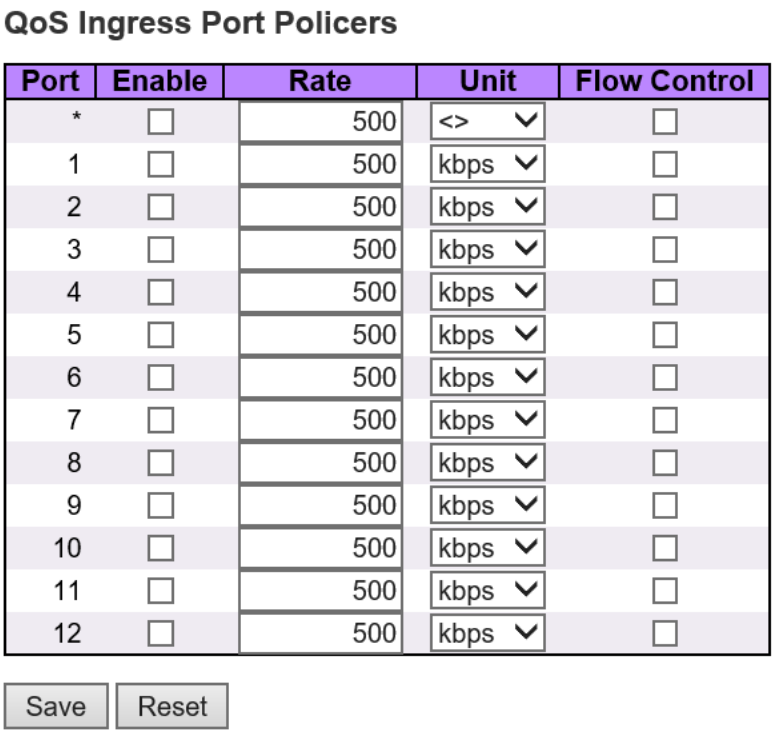
| Object | Description |
|---|---|
| **Port** | The port number for which the configuration below applies. |
| **CoS** | Controls the default CoS value.<br>All frames are classified to a CoS. There is a one to one mapping between CoS, queue and priority. A CoS of 0 (zero) has the lowest priority.<br>If 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.<br>The classified CoS can be overruled by a QCL entry.<br>Note: If the default CoS has been dynamically changed, then the actual default CoS is shown in parentheses after the configured default CoS. |
| **DPL** | Controls the default drop precedence level.<br>All frames are classified to a drop precedence level.<br>If the port is VLAN aware and the frame is tagged, then the frame is classified to a DPL that is equal to the DEI value in the tag. Otherwise the frame is classified to the default DPL. |

| | |
|---|---|
| | 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.<br>The classified DPL can be overruled by a QCL entry. |
| **PCP** | Controls the default PCP value.<br>All frames are classified to a PCP value.<br>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.<br>All frames are classified to a DEI value.<br>If the port is VLAN aware and the frame is tagged, then the frame is classified to the DEI value in the tag. Otherwise the frame is classified to the default DEI value. |
| **CoS ID** | Controls the default CoS ID value.<br>Every incoming frame is classified to a CoS ID, which later can be used as basis for rewriting of different parts of the frame. |
| **Tag Class.** | Shows the classification mode for tagged frames on this port.<br>`Disabled`: Use default CoS and DPL for tagged frames.<br>`Enabled`: Use mapped versions of PCP and DEI for tagged frames.<br>Click on the mode in order to configure the mode and/or mapping.<br>**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. |
| **Ingress Map (For 90W PoE Model)** | Controls the Ingress Map selection through the Map ID. The Ingress Map ID ranges from 0 to 255. An empty field indicates no map selection. |
| **Egress Map (For 90W PoE Model)** | Controls the Egress Map selection through the Map ID. The Egress Map ID ranges from 0 to 511. An empty field indicates no map selection. |

| **Buttons** | |
|---|---|
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

## 2.3.94 QoS - Port Policing

This page allows you to configure the Policer settings for all switch ports.




| Object | Description |
|---|---|
| **Port** | The port number for which the configuration below applies. |
| **Enabled** | Controls whether the policer is enabled on this switch port. |
| **Rate (For 90W PoE Model)** | Controls the rate for the port policer. This value is restricted to 10-13128147 when "Unit" is kbps or fps, and 1-13128 when "Unit" is Mbps or kfps. The rate is internally rounded up to the nearest value supported by the port policer. |
| **Rate (For 30W PoE Model)** | 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 policer rate as kbps, Mbps, fps or kfps . The default value is "kbps". |
| **Flow Control** | If flow control is enabled and the port is in flow control mode, then pause frames are sent instead of discarding frames. |

| Buttons |
|---|

| | |
|---|---|
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

## 2.3.95 QoS - Queue Policing

This page allows you to configure the Queue Policer settings for all switch ports.

**QoS Ingress Queue Policers**

| Port | Queue 0 | Queue 1 | Queue 2 | Queue 3 | Queue 4 | Queue 5 | Queue 6 | Queue 7 |
|---|---|---|---|---|---|---|---|---|
| | Enable | Enable | Enable | Enable | Enable | Enable | Enable | Enable |
| * | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 1 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 2 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 3 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 4 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 5 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 6 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 7 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 8 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 9 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 10 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 11 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 12 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |

Save Reset

| Object | Description |
|---|---|
| **Port** | The port number for which the configuration below applies. |
| **Enable (E)** | Enable or disable the queue policer for this switch port. |
| **Rate (For 90W PoE Model)** | Controls the rate for the queue policer. This value is restricted to 25-13128147 when "Unit" is kbps, and 1-13128 when "Unit" is Mbps. The rate is internally rounded up to the nearest value supported by the queue policer.<br>This field is only shown if at least one of the queue policers are enabled. |
| **Rate (For 30W PoE Model)** | 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.<br>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.<br>This field is only shown if at least one of the queue policers are enabled. |

| Buttons |
|---|

| | |
|---|---|
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

## 2.3.96 Port Scheduler

This page provides an overview of QoS Egress Port Schedulers for all switch ports.

### 90W PoE Model

**QoS Egress Port Schedulers**

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

**QoS Egress Port Scheduler and Shapers Port 1** Port 1

Scheduler Mode: Strict Priority

| Queue Shaper | | | | Queue Scheduler | Port Shaper | | | |
|---|---|---|---|---|---|---|---|---|
| Enable | Rate | Unit | Rate-type | Cut-through | Enable | Rate | Unit | Rate-type |
| Q7 | 500 | kbps | Line | | | | | |
| Q6 | 500 | kbps | Line | | | | | |
| Q5 | 500 | kbps | Line | | | | | |
| Q4 | 500 | kbps | Line | | | | | |
| Q3 | 500 | kbps | Line | | | | | |
| Q2 | 500 | kbps | Line | | | | | |
| Q1 | 500 | kbps | Line | | | | | |
| Q0 | 500 | kbps | Line | | | | | |
| | | | | | | 500 | kbps | Line |

STRICT

Save Reset Back

| Object | Description |
|---|---|
| **QoS Egress Port Schedulers** | |
| **Port** | The logical port for the settings contained in the same row.<br>Click on the port number in order to configure the schedulers. |
| **Mode** | Shows the scheduling mode for this port. |
| **Qn** | Shows the weight for this queue and port. |
| **QoS Egress Port Scheduler and Shapers Port No.** | |
| **Scheduler Mode** | Controls how many of the queues are scheduled as strict and how many are scheduled as weighted on this switch port. |
| **Queue Shaper Enable** | Controls whether the queue shaper is enabled for this queue on this switch port. |
| **Queue Shaper Rate** | Controls the rate for the queue shaper. This value is restricted to 100-13107100 when "Unit" is kbps, and 1-13107 when "Unit" is Mbps. The rate is internally rounded up to the nearest value supported by the queue shaper. |
| **Queue Shaper Unit** | Controls the unit of measure for the queue shaper rate as "kbps" or "Mbps". The default value is "kbps". |
| **Queue Shaper Rate-type** | The rate type of the queue shaper. The allowed values are:<br>Line: Specify that this shaper operates on line rate.<br>Data: Specify that this shaper operates on data rate. |
| **Queue Scheduler Cut-through** | Controls whether the queue has cut-through enabled. |
| **Queue Scheduler Preemption** | Controls whether the queue has frame preemption enabled. |
| **Queue Scheduler Weight** | Controls the weight for this queue. The default value is "17". This value is restricted to 1-100. This parameter is only shown if "Scheduler Mode" is set to "Weighted". |
| **Queue Scheduler Percent** | Shows the weight in percent for this queue. This parameter is only shown if "Scheduler Mode" is set to "Weighted". |
| **Port Shaper Enable** | Controls whether the port shaper is enabled for this switch port. |
| **Port Shaper Rate** | Controls the rate for the port shaper. This value is restricted to 100-13107100 when "Unit" is kbps, and 1-13107 when "Unit" is Mbps. The rate is internally rounded up to the nearest value supported by the port shaper. |
| **Port Shaper Unit** | Controls the unit of measure for the port shaper rate as kbps or Mbps. |
| **Port Shaper Rate-type** | The rate type of the port shaper. The allowed values are:<br>Line: Specify that this shaper operates on line rate.<br>Data: Specify that this shaper operates on data rate. |

| Buttons |
|---|

| | |
|---|---|
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |
| Back : | Click to undo any changes made locally and return to the previous page. |

## 30W PoE Model

**QoS Egress Port Schedulers**

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

**QoS Egress Port Scheduler and Shapers Port 1** Port 1

Scheduler Mode: Strict Priority

| Queue Shaper | | | | Queue Scheduler | Port Shaper | | | |
|---|---|---|---|---|---|---|---|---|
| Enable | Rate | Unit | Rate-type | Cut-through | Enable | Rate | Unit | Rate-type |
| Q7 | 500 | kbps | Line | | | | | |
| Q6 | 500 | kbps | Line | | | | | |
| Q5 | 500 | kbps | Line | | | | | |
| Q4 | 500 | kbps | Line | | | | | |
| Q3 | 500 | kbps | Line | | | | | |
| Q2 | 500 | kbps | Line | | | | | |
| Q1 | 500 | kbps | Line | | | | | |
| Q0 | 500 | kbps | Line | | | | | |
| | | | | STRICT | | 500 | kbps | Line |

Save Reset Back

| Object | Description |
|---|---|
| **QoS Egress Port Schedulers** | |
| **Port** | The logical port for the settings contained in the same row.<br>Click on the port number in order to configure the schedulers. |
| **Mode** | Shows the scheduling mode for this port. |
| **Qn** | Shows the weight for this queue and port. |
| **QoS Egress Port Scheduler and Shapers Port No.** | |
| **Scheduler Mode** | Controls how many of the queues are scheduled as strict and how many are scheduled as weighted on this switch port. |
| **Queue Shaper Enable** | Controls whether the queue shaper is enabled for this queue on this switch port. |
| **Queue Shaper Rate** | Controls the rate for the queue shaper. This value is restricted to 100-3281943 when "Unit" is kbps, and 1-3281 when "Unit" is Mbps. The rate is internally rounded up to the nearest value supported by the queue shaper. |
| **Queue Shaper Unit** | Controls the unit of measure for the queue shaper rate as kbps or Mbps. |
| **Queue Shaper Excess** | Controls whether the queue is allowed to use excess bandwidth. |
| **Queue Scheduler Weight** | Controls the weight for this queue. The default value is "17". This value is restricted to 1-100. This parameter is only shown if "Scheduler Mode" is set to "Weighted". |
| **Queue Scheduler Percent** | Shows the weight in percent for this queue. This parameter is only shown if "Scheduler Mode" is set to "Weighted". |
| **Port Shaper Enable** | Controls whether the port shaper is enabled for this switch port. |
| **Port Shaper Rate** | Controls the rate for the port shaper. This value is restricted to 100-3281943 when "Unit" is kbps, and 1-3281 when "Unit" is Mbps. The rate is internally rounded up to the nearest value supported by the port shaper. |
| **Port Shaper Unit** | Controls the unit of measure for the port shaper rate as kbps or Mbps. |
| **Port Shaper Rate-type** | The rate type of the port shaper. The allowed values are:<br>Line: Specify that this shaper operates on line rate.<br>Data: Specify that this shaper operates on data rate. |

| Buttons | |
|---|---|
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |
| Back : | Click to undo any changes made locally and return to the previous page. |

## 2.3.97 QoS - Port Shaping

This page provides an overview of QoS Egress Port Shapers for all switch ports.

**QoS Egress Port Shapers**

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

**QoS Egress Port Scheduler and Shapers Port 1** Port 1

Scheduler Mode: Strict Priority

| Queue Shaper | | | | Queue Scheduler | Port Shaper | | | |
|---|---|---|---|---|---|---|---|---|
| Enable | Rate | Unit | Rate-type | Cut-through | Enable | Rate | Unit | Rate-type |
| Q7 | 500 | kbps | Line | | | | | |
| Q6 | 500 | kbps | Line | | | | | |
| Q5 | 500 | kbps | Line | | | | | |
| Q4 | 500 | kbps | Line | | | | | |
| Q3 | 500 | kbps | Line | | | | | |
| Q2 | 500 | kbps | Line | | | | | |
| Q1 | 500 | kbps | Line | | | | | |
| Q0 | 500 | kbps | Line | | | | | |
| | | | | | | 500 | kbps | Line |

STRICT

Save Reset Back

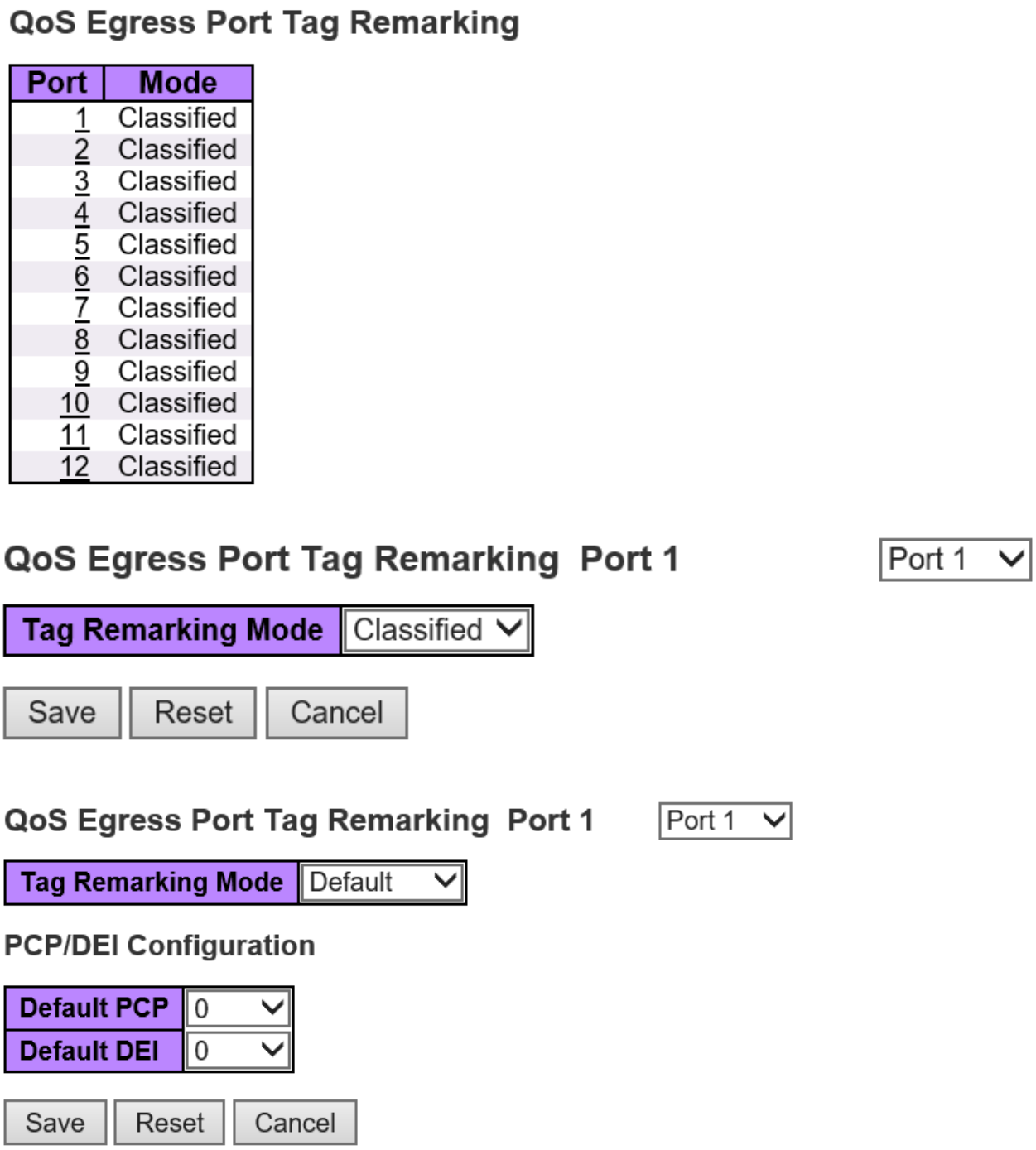
| Object | Description |
|---|---|
| **QoS Egress Port Shapers** | |
| **Port** | The logical port for the settings contained in the same row.<br>Click on the port number in order to configure the shapers. |
| **Qn** | Shows "disabled" or actual queue shaper rate - e.g. "800 Mbps". |
| **Port #** | Shows "disabled" or actual port shaper rate - e.g. "800 Mbps". |
| **QoS Egress Port Scheduler and Shapers Port No.** | |
| **Scheduler Mode** | Controls how many of the queues are scheduled as strict and how many are scheduled as weighted on this switch port. |
| **Queue Shaper Enable** | Controls whether the queue shaper is enabled for this queue on this switch port. |
| **Queue Shaper Rate** | Controls the rate for the queue shaper. This value is restricted to 100-13107100 when "Unit" is kbps, and 1-13107 when "Unit" is Mbps. The rate is internally rounded up to the nearest value supported by the queue shaper. |
| **Queue Shaper Unit** | Controls the unit of measure for the queue shaper rate as "kbps" or "Mbps". |
| **Queue Shaper Rate-type** | The rate type of the queue shaper. The allowed values are:<br>Line: Specify that this shaper operates on line rate.<br>Data: Specify that this shaper operates on data rate. |
| **Queue Scheduler Cut-through** | Controls whether the queue has cut-through enabled. |
| **Queue Scheduler Preemption** | Controls whether the queue has frame preemption enabled. |
| **Queue Scheduler Weight** | Controls the weight for this queue. The default value is "17". This value is restricted to 1-100. This parameter is only shown if "Scheduler Mode" is set to "Weighted". |
| **Queue Scheduler Percent** | Shows the weight in percent for this queue. This parameter is only shown if "Scheduler Mode" is set to "Weighted". |
| **Port Shaper Enable** | Controls whether the port shaper is enabled for this switch port. |
| **Port Shaper Rate** | Controls the rate for the port shaper. This value is restricted to 100-13107100 when "Unit" is kbps, and 1-13107 when "Unit" is Mbps. The rate is internally rounded up to the nearest value supported by the port shaper. |
| **Port Shaper Unit** | Controls the unit of measure for the port shaper rate as kbps or Mbps. |
| **Port Shaper Rate-type** | The rate type of the port shaper. The allowed values are:<br>Line: Specify that this shaper operates on line rate.<br>Data: Specify that this shaper operates on data rate. |

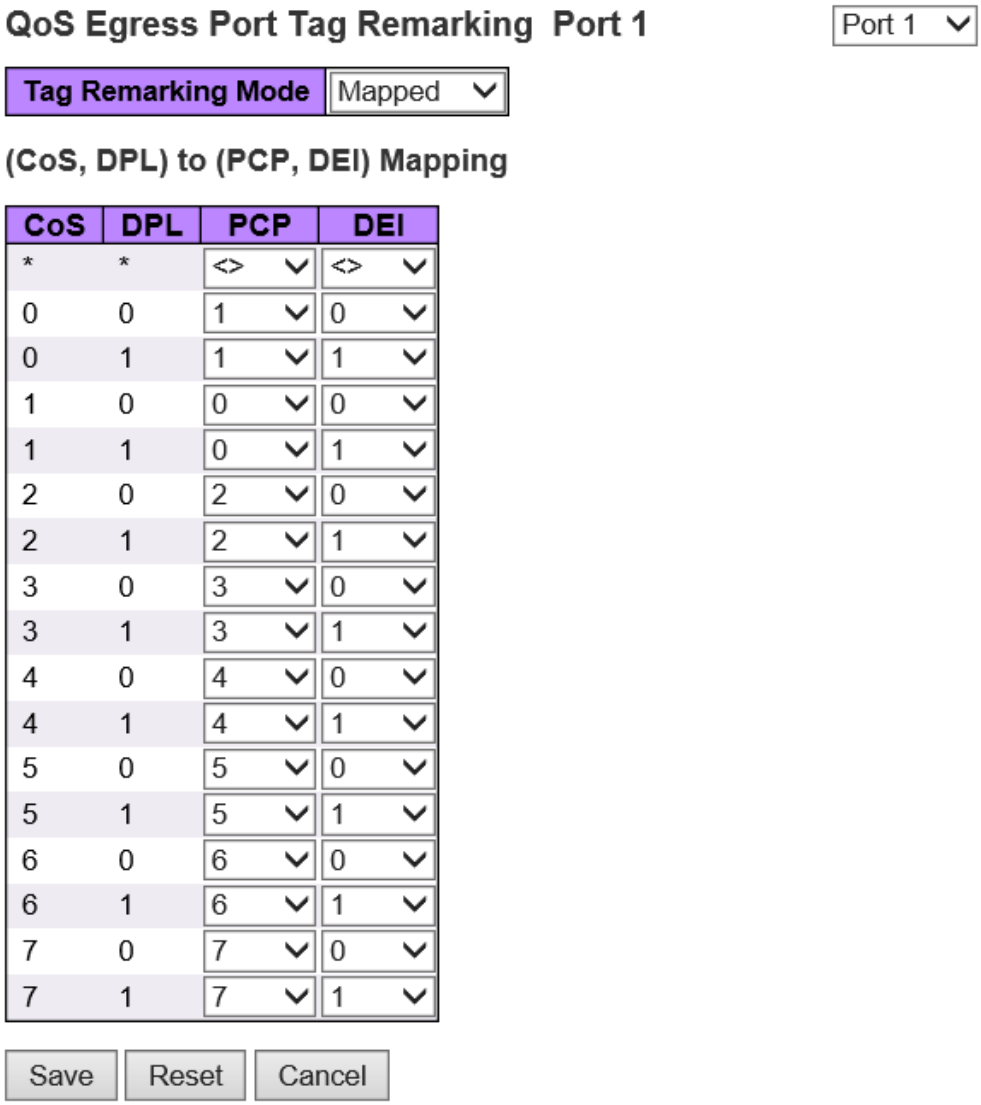
| Buttons |
|---|

| | |
|---|---|
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |
| Back : | Click to undo any changes made locally and return to the previous page. |

## 2.3.98 QoS - Port Tag Remarking

This page provides an overview of QoS Egress Port Tag Remarking for all switch ports.






| Object | Description |
|---|---|
| **QoS Egress Port Tag Remarking** | |
| **Port** | The logical port for the settings contained in the same row.<br>Click on the port number in order to configure tag remarking. |
| **Mode** | Shows the tag remarking mode for this port.<br>`Classified`: Use classified PCP/DEI values.<br>`Default`: Use default PCP/DEI values.<br>`Mapped`: Use mapped versions of QoS class and DP level. |
| **QoS Egress Port Tag Remarking Port No.** | |
| **Mode** | Controls the tag remarking mode for this port.<br>`Classified`: Use classified PCP/DEI values.<br>`Default`: Use default PCP/DEI values.<br>`Mapped`: Use mapped versions of QoS class and DP level. |

| (QoS class, DP level) to (PCP, DEI) Mapping | |
|---|---|
| **(QoS class, DP level) to (PCP, DEI) Mapping** | Controls the mapping of the classified (QoS class, DP level) to (PCP, DEI) values when the mode is set to Mapped. |
| **PCP/DEI Configuration** | |
| **PCP/DEI Configuration** | Controls the default PCP and DEI values used when the mode is set to Default. |

| Buttons | |
|---|---|
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |
| Cancel : | Click to undo any changes made locally and return to the previous page. |

## 2.3.99 QoS - Port DSCP

This page allows you to configure the basic QoS Port DSCP Configuration settings for all switch ports.

**QoS Port DSCP Configuration**

| Port | Ingress | | Egress |
|---|---|---|---|
| | Translate | Classify | Rewrite |
| * | ☐ | <> | <> |
| 1 | ☐ | Disable | Disable |
| 2 | ☐ | Disable | Disable |
| 3 | ☐ | Disable | Disable |
| 4 | ☐ | Disable | Disable |
| 5 | ☐ | Disable | Disable |
| 6 | ☐ | Disable | Disable |
| 7 | ☐ | Disable | Disable |
| 8 | ☐ | Disable | Disable |
| 9 | ☐ | Disable | Disable |
| 10 | ☐ | Disable | Disable |
| 11 | ☐ | Disable | Disable |
| 12 | ☐ | Disable | Disable |

Save Reset

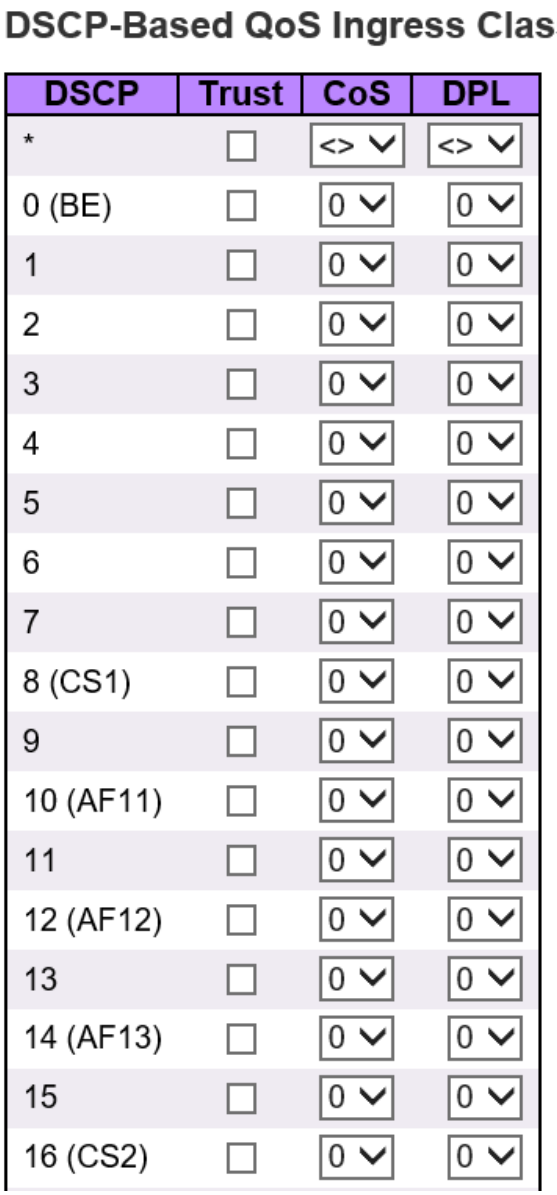
| Object | Description |
|---|---|
| **Port** | The Port column shows the list of ports for which you can configure dscp ingress and egress settings. |
| **Ingress** | In Ingress settings you can change ingress translation and classification settings for individual ports.<br>There are two configuration parameters available in Ingress:<br>`Translate`<br>`Classify` |
| **Translate** | To Enable the Ingress Translation click the checkbox. |
| **Classify** | Classification for a port have 4 different values.<br>`-Disable`: No Ingress DSCP Classification.<br>`-DSCP=0`: Classify if incoming (or translated if enabled) DSCP is 0.<br>`-Selected`: Classify only selected DSCP for which classification is enabled as specified in DSCP Translation window for the specific DSCP.<br>`-All`: Classify all DSCP. |
| **Egress** | Port Egress Rewriting can be one of - |

| | |
|---|---|
| | • Disable: No Egress rewrite.<br>• Enable: Rewrite enabled without remapping.<br>• Remap: DSCP from analyzer is remapped and frame is remarked with remapped DSCP value. |

| Buttons | |
|---|---|
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

## 2.3.100 QoS – DSCP Based QoS

This page allows you to configure the basic QoS DSCP based QoS Ingress Classification settings for all switches.




| Object | 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. |

| | |
|---|---|
| **CoS** | CoS value can be any of (0-7) |
| **DPL** | Drop Precedence Level (0-3) |

| **Buttons** | |
|---|---|
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

## 2.3.101 QoS - DSCP Translation

This page allows you to configure the basic QoS DSCP Translation settings for all switches. DSCP translation can be done in Ingress or Egress.

### DSCP Translation

| DSCP | Ingress | | Egress |
|---|---|---|---|
| | Translate | Classify | Remap |
| * | <> | ☐ | <> |
| 0 (BE) | 0 (BE) | ☐ | 0 (BE) |
| 1 | 1 | ☐ | 1 |
| 2 | 2 | ☐ | 2 |
| 3 | 3 | ☐ | 3 |
| 4 | 4 | ☐ | 4 |
| 5 | 5 | ☐ | 5 |
| 6 | 6 | ☐ | 6 |
| 7 | 7 | ☐ | 7 |
| 8 (CS1) | 8 (CS1) | ☐ | 8 (CS1) |
| 9 | 9 | ☐ | 9 |
| 10 (AF11) | 10 (AF11) | ☐ | 10 (AF11) |
| 11 | 11 | ☐ | 11 |
| 12 (AF12) | 12 (AF12) | ☐ | 12 (AF12) |
| 13 | 13 | ☐ | 13 |
| 14 (AF13) | 14 (AF13) | ☐ | 14 (AF13) |
| 15 | 15 | ☐ | 15 |
| 16 (CS2) | 16 (CS2) | ☐ | 16 (CS2) |
| 17 | 17 | ☐ | 17 |
| 18 (AF21) | 18 (AF21) | ☐ | 18 (AF21) |
| 19 | 19 | ☐ | 19 |

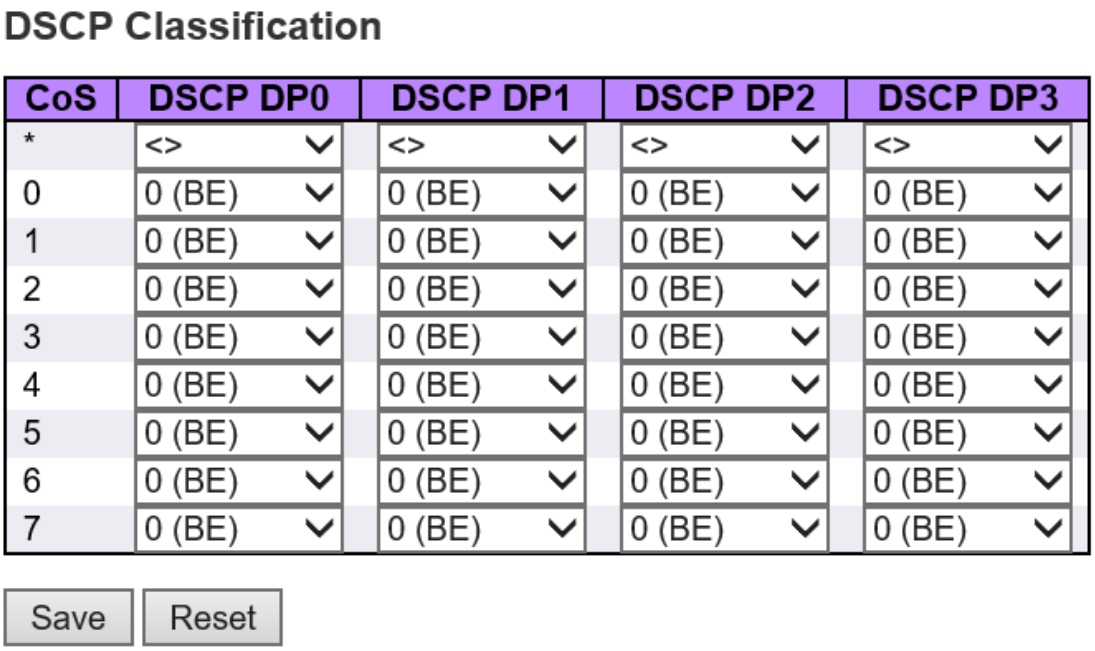
| Object | Description |
|---|---|
| **DSCP** | Maximum number of supported DSCP values are 64 and valid DSCP value ranges from 0 to 63. |
| **Ingress** | Ingress side DSCP can be first translated to new DSCP before using the DSCP for QoS class and DPL map. |

| | |
|---|---|
| | There are two configuration parameters for DSCP Translation -<br>`Translate`<br>`Classify` |
| **Translate** | DSCP at Ingress side can be translated to any of (0-63) DSCP values. |
| **Classify** | Click to enable Classification at Ingress side. |
| **Egress** | There is the following configurable parameter for Egress side -<br>Remap |
| **Remap** | Select the DSCP value from select menu to which you want to remap. DSCP value ranges from 0 to 63. |

| **Buttons** | |
|---|---|
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

## 2.3.102QoS - DSCP Classification

This page allows you to configure the mapping of QoS class and Drop Precedence Level to DSCP value.



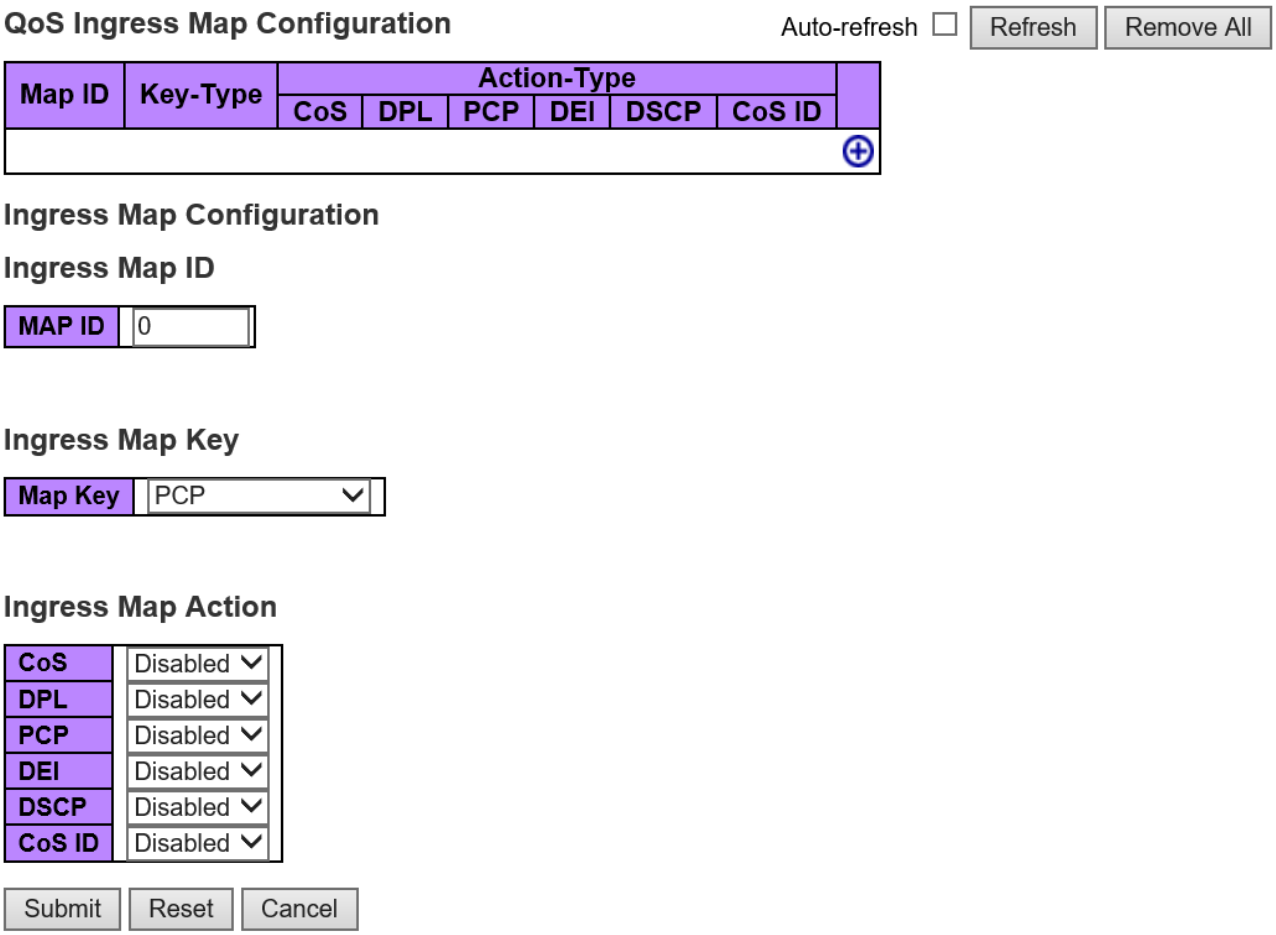

| Object | Description |
|---|---|
| **CoS** | Actual QoS class. |
| **DSCP DP0** | Select the classified DSCP value (0-63) for Drop Precedence Level 0. |
| **DSCP DP1** | Select the classified DSCP value (0-63) for Drop Precedence Level 1. |
| **DSCP DP2 (For 90W PoE Model)** | Select the classified DSCP value (0-63) for Drop Precedence Level 2. |
| **DSCP DP3 (For 90W PoE Model)** | Select the classified DSCP value (0-63) for Drop Precedence Level 3. |

| Buttons | |
|---|---|
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

## 2.3.103QoS - Ingress Map (For 90W PoE Model)

This page shows a table of QoS Ingress Maps which is made up of individual map entries. Each entry has a key and an action. The key indicates which fields of the frame will be mapped to the fields specified by and according to the action. Each Map can hold a number of map rules, or mappings between possible keys and actions. Which of those rules will be applied depends on the selection of (Key-Type, Action-Type). Each row describes a user-defined map. The maximum number of Ingress Maps is 256. Each Ingress Map uses a number of key-entries in a internal key mapping table which have 1004 key-entries available for configuration. The consumption of key-entries by Key Type are listed as table width in the Key-Type table below. A new Ingress Map can only be defined when there are sufficient free key-entries.

NOTE: This is just an overview of the configured maps. The user can add new ones or edit existing maps using the Add/Edit buttons. Click on the lowest plus sign (empty map entry) to add a new Ingress Map to the table.




| Object | Description |
|---|---|
| **QoS Ingress Map Configuration** | |
| **Map ID** | Indicates the Map (unique) ID. Range is 0 to 255. |

| | |
|---|---|
| **Key-Type** | Indicates the Key Type that will be used to filter the map rules when applying the map. As mentioned above, map rules can have various keys and this is to make a select set of them. Possible Key types are:<br>PCP: Use PCP as key for tagged frames and none for the rest. Table width: 1<br>PCP - DEI:Use PCP/DEI as key for tagged frames and none for the rest. Table width: 2<br>DSCP: Use DSCP as key for IP frames and none for the rest. Table width: 8<br>DSCP - PCP - DEI: Use DSCP as key for IP frames, PCP/DEI for tagged frames and none for the rest. Table width:10 |
| **Action-Type** | Indicates the Action Type that will be used to filter the map rules when applying the map. As mentioned above, map rules can have various actions available and this is to make a select set of them. Possible Action types are:<br>CoS: Class of Service.<br>DPL: Drop Precedence Level.<br>PCP: Priority Code Point.<br>DEI: Drop Eligible Indicator.<br>DSCP: Differentiated Services Code Point.<br>CoS ID: CoS ID. |
| **QoS Ingress Map Modification Buttons** | It is possible to modify each map (or add new maps) in the table using the following buttons:<br>  : Edits the map.<br>  : Deletes the map.<br>  : Adds a new map in the table. (can also be used to overwrite an existing map, so care on the map id). |
| **Ingress Map Configuration** | |
| **Map ID** | Indicates the Map (unique) ID. Range is 0 to 255. When in edit mode, this is non-configurable. However, it is possible to overwrite an existing mapping through the create mode. |
| **Map Key** | Indicates the Key type that will be used to filter the map rules when applying the map. As mentioned above, map rules can have various keys and this is to make a select set of them. Possible Key types are:<br>PCP: Use PCP as key for tagged frames and none for the rest.<br>PCP - DEI:Use PCP/DEI as key for tagged frames and none for the rest.<br>DSCP: Use DSCP as key for IP frames and none for the rest.<br>DSCP - PCP - DEI: Use DSCP as key for IP frames, PCP/DEI for tagged frames and none for the rest. |
| **Map Action** | Indicates the Action type that will be used to filter the map rules when applying the map. As mentioned above, map rules can have various actions available and this is |

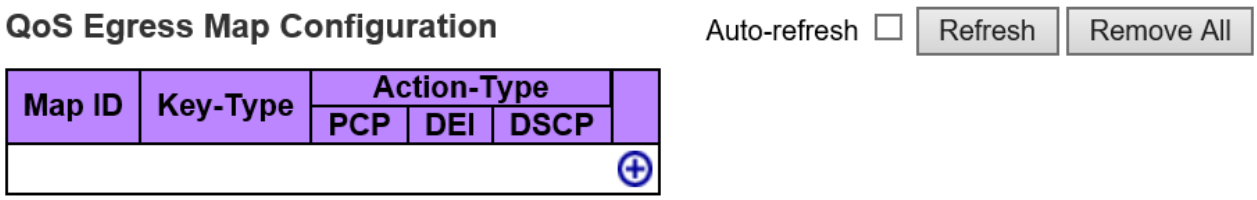
| | |
|---|---|
| | to make a select set of them. Possible Action types are:<br>CoS: Class of Service.<br>DPL: Drop Precedence Level.<br>PCP: Priority Code Point.<br>DEI: Drop Eligible Indicator.<br>DSCP: Differentiated Services Code Point.<br>CoS ID: CoS ID. |

| Buttons | |
|---|---|
| Auto-refresh ☐ | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |
| Refresh | Click to refresh the page. |
| Remove All | Click to remove all Ingress Maps (and their corresponding rules). |
| Submit | Click to submit the map configuration and move to the main ingress map page. |
| Reset : | Click to undo any changes made locally and revert to the previously saved values. |
| Cancel : | Return to the ingress map page without saving the configuration changes. |

## 2.3.104QoS - Egress Map (For 90W PoE Model)

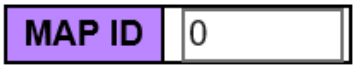
This page shows a table of QoS Egress Maps which is made up of individual map entries. Each entry has a key and an action. The key indicates which fields of the frame will be mapped to the fields specified by and according to the action. Each Map can hold a number of map rules, or mappings between possible keys and actions. Which of those rules will be applied depends on the selection of (Key-Type, Action-Type). Each row describes a user-defined map. The maximum number of Egress Maps is 512. Each Egress Map uses a number of key-entries in a internal key mapping table which have 960 key-entries available. The consumption of key-entries by Key Type are listed as table width in the Key-Type table below. A new Egress Map can only be defined when there are sufficient free key-entries.

NOTE: This is just an overview of the configured maps. The user can add new ones or edit existing maps using the Add/Edit buttons. Click on the lowest plus sign (empty map entry) to add a new Ingress Map to the table.



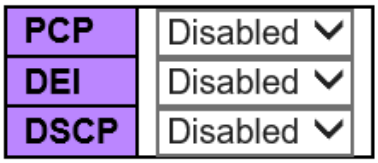
## Egress Map Configuration

### Egress Map ID




### Egress Map Key


### Egress Map Action





| Object | Description |
|---|---|
| QoS Ingress Map Configuration | |
| **Map ID** | Indicates the Map (unique) ID. Range is 0 to 511. |
| **Key-Type** | Indicates the Key Type that will be used to filter the map rules when applying the map. As mentioned above, map rules can have various keys and this is to make a select set of them. Possible Key types are:<br>CoS ID: Use classified COS ID as key. Table width: 1<br>CoS ID - DPL:Use classified COS ID and DPL as key. Table width: 4<br>DSCP: Use classified DSCP as key. Table width: 8<br>DSCP - DPL: Use classified DSCP and DPL as key. Table width: 32 |
| **Action-Type** | Indicates the Action Type that will be used to filter the map rules when applying the map. As mentioned above, map rules can have various actions available and this is to make a select set of them. Possible Action types are:<br>PCP: Priority Code Point.<br>DEI: Drop Eligible Indicator.<br>DSCP: Differentiated Services Code Point. |
| **QoS Ingress Map Modification Buttons** | It is possible to modify each map (or add new maps) in the table using the following buttons:<br>: Edits the map. |

| | |
|---|---|
| | : Deletes the map.<br>: Adds a new map in the table. (can also be used to overwrite an existing map, so care on the map id). |
| **Ingress Map Configuration** | |
| **Map ID** | Indicates the Map (unique) ID. Range is 0 to 511. When in edit mode, this is non-configurable. However, it is possible to overwrite an existing mapping through the create mode. |
| **Map Key** | Indicates the Key type that will be used to filter the map rules when applying the map. As mentioned above, map rules can have various keys and this is to make a select set of them. Possible Key types are:<br>CoS ID: Use classified COS ID as key.<br>CoS ID - DPL:Use classified COS ID and DPL as key.<br>DSCP: Use classified DSCP as key.<br>DSCP - DPL: Use classified DSCP and DPL as key. |
| **Map Action** | Indicates the Action type that will be used to filter the map rules when applying the map. As mentioned above, map rules can have various actions available and this is to make a select set of them. Possible Action types are:<br>PCP: Priority Code Point.<br>DEI: Drop Eligible Indicator.<br>DSCP: Differentiated Services Code Point. |

| **Buttons** | |
|---|---|
| Auto-refresh ☐ | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |
| Refresh | Click to refresh the page. |
| Remove All | Click to remove all Ingress Maps (and their corresponding rules). |
| Submit | Click to submit the map configuration and move to the main ingress map page. |
| Reset : | Click to undo any changes made locally and revert to the previously saved values. |
| Cancel : | Return to the ingress map page without saving the configuration changes. |

# 2.3.105QoS - Control List

This page shows the QoS Control List(QCL), which is made up of the QCEs. Each row describes a QCE that is defined. The maximum number of QCEs is `256` on each switch.

Click on the lowest plus sign to add a new QCE to the list.

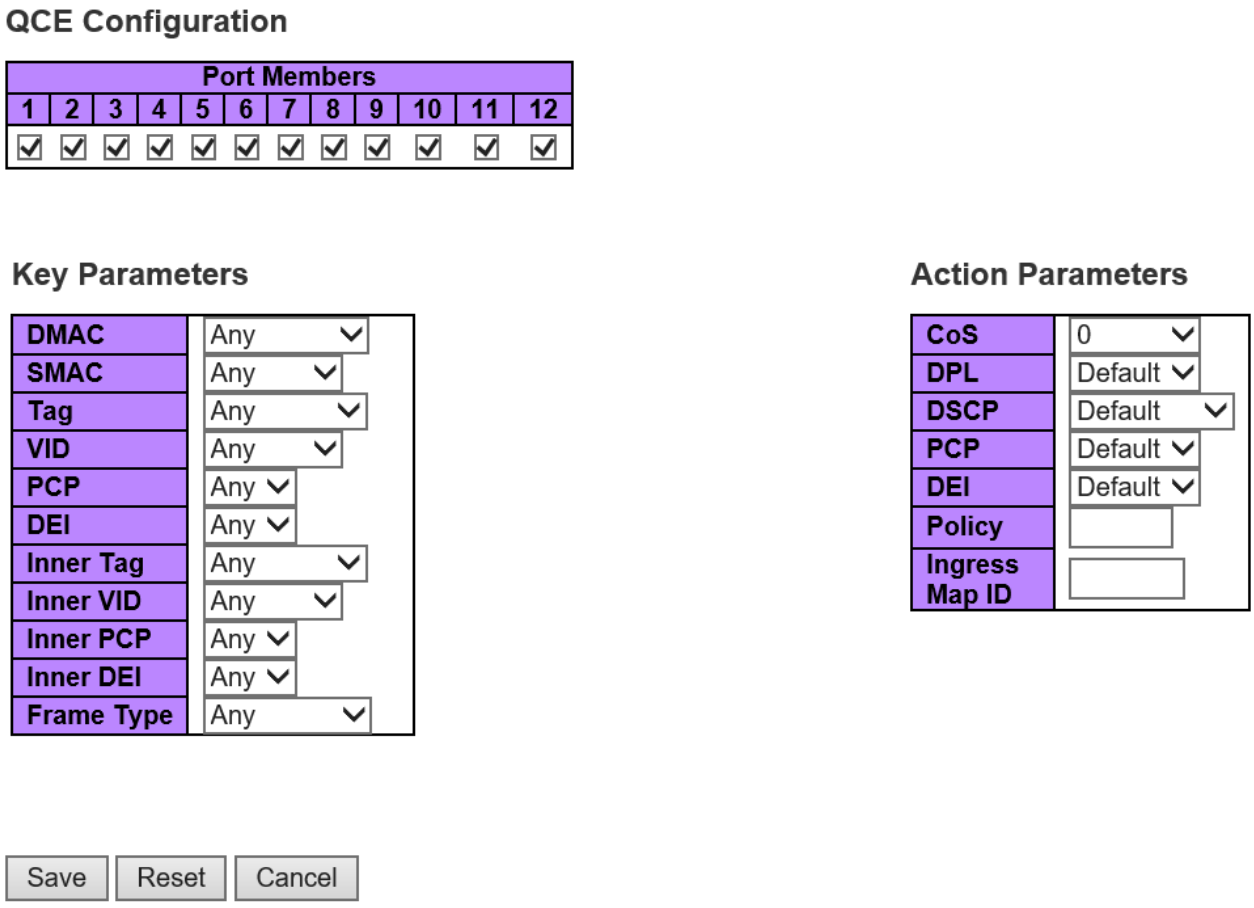
**QoS Control List Configuration**

| QCE | Port | DMAC | SMAC | Tag Type | VID | PCP | DEI | Frame Type | Action | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | CoS | DPL | DSCP | PCP | DEI | Policy | Ingress Map |
| | | | | | | | | | | | | | | | |

| Object | Description |
|---|---|
| **QCE** | Indicates the QCE id. |
| **Port** | Indicates the list of ports configured with the QCE. |
| **DMAC** | Indicates the destination MAC address. Possible values are:<br>`Any`: Match any DMAC.<br>`Unicast`: Match unicast DMAC.<br>`Multicast`: Match multicast DMAC.<br>`Broadcast`: Match broadcast DMAC.<br>The default value is 'Any'. |
| **SMAC** | Match specific source MAC address or 'Any'. |
| **Tag Type** | Indicates tag type. Possible values are:<br>`Any`: Match tagged and untagged frames.<br>`Untagged`: Match untagged frames.<br>`Tagged`: Match tagged frames.<br>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:<br>`Any`: Match any frame type.<br>`Ethernet`: Match EtherType frames.<br>`LLC`: Match (LLC) frames.<br>`SNAP`: Match (SNAP) frames. |

| | |
|---|---|
| | `IPv4`: Match IPv4 frames.<br>`IPv6`: Match IPv6 frames. |
| **Action** | Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content.<br>Possible actions are:<br>CoS: Classify Class of Service.<br>DPL: Classify Drop Precedence Level.<br>DSCP: Classify DSCP value.<br>PCP: Classify PCP value.<br>DEI: Classify DEI value.<br>Policy: Classify ACL Policy number.<br>Ingress Map: Classify Ingress Map ID. |
| **Modification Buttons** | You can modify each QCE (QoS Control Entry) in the table using the following buttons:<br>: Inserts a new QCE before the current row.<br>: Edits the QCE.<br>: Moves the QCE up the list.<br>: Moves the QCE down the list.<br>: Deletes the QCE.<br>: The lowest plus sign adds a new entry at the bottom of the QCE listings. |

The QCE page includes the following fields:




| Object | Description |
|---|---|
| **Port Members** | Check the checkbox button to include the port in the QCL entry. By default all ports are included. |
| **Key parameters** | Key configuration is described as below:<br><br>`DMAC` Destination MAC address: Possible values are 'Unicast', 'Multicast', 'Broadcast', 'Specific' (xx-xx-xx-xx-xx-xx) or 'Any'.<br>`SMAC` Source MAC address: xx-xx-xx-xx-xx-xx or 'Any'.<br>`Tag` Value of Tag field can be 'Untagged', 'Tagged', 'C-Tagged', 'S-Tagged' or 'Any'.<br>`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.<br>`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'.<br>`DEI` Valid value of DEI can be '0', '1' or 'Any'. |

| | |
|---|---|
| | **Inner Tag** Value of Inner Tag field can be 'Untagged', 'Tagged', 'C-Tagged', 'S-Tagged' or 'Any'.<br>**Inner VID** Valid value of Inner 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.<br>**Inner PCP** Valid value of Inner 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'.<br>**Inner DEI** Valid value of Inner DEI can be '0', '1' or 'Any'.<br>**Frame Type** Frame Type can have any of the following values:<br>1. **Any**<br>2. **EtherType**<br>3. **LLC**<br>4. **SNAP**<br>5. **IPv4**<br>6. **IPv6**<br>Note: 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'.<br>SSAP Address Valid SSAP(Source Service Access Point) can vary from 0x00 to 0xFF or 'Any'.<br>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'.<br>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.<br>Destination IP Specific Destination IP address in value/mask format or 'Any'.<br>IP Fragment IPv4 frame fragmented option: 'Yes', 'No' or 'Any'.<br>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.<br>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'.<br>Source IP 32 LS bits of IPv6 source address in value/mask format or 'Any'.<br>Destination IP Specific Destination IP address in value/mask format or 'Any'.<br>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.<br>Sport Source TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.<br>Dport Destination TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP. |
| **Action Parameters** | CoS Class of Service: (0-7) or 'Default'.<br>DP Drop Precedence Level: (0-3) or 'Default'.<br>DSCP: (0-63, BE, CS1-CS7, EF or AF11-AF43) or 'Default'.<br>PCP: (0-7) or 'Default'. Note: PCP and DEI cannot be set individually.<br>DEI: (0-1) or 'Default'.<br>Policy ACL Policy number: (0-255) or 'Default' (empty field).<br>Ingress Map ID Ingress Map ID: (0-255) or no Ingress Map (empty field).<br>'Default' means that the default classified value is not modified by this QCE. |

| **Buttons** | |
|---|---|
| Save | Click to save the configuration and move to main QCL page. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |
| Cancel | Return to the previous page without saving the configuration change. |

# 2.3.106QoS - Storm Policing

Storm control for the switch is configured on this page.

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

The configuration indicates the permitted packet rate for unicast, multicast or broadcast traffic across the switch.

**Global Storm Policer Configuration**

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

**Port Storm Policer Configuration**

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

Save Reset

| Object | Description |
|---|---|
| **Global Storm Policer Configuration** | |
| **Frame Type** | The frame type for which the configuration below applies. |
| **Enable** | Enable or disable the global storm policer for the given frame type. |
| **Rate (For 90W PoE Model)** | Controls the rate for the global storm policer. This value is restricted to 10-13128147 when "Unit" is fps or kbps, and 1-13128 when "Unit" is kfps or Mbps. The rate is internally rounded up to the nearest value supported by the global storm policer. |

| | |
|---|---|
| | Supported rates are divisible by 10 fps or 25 kbps. |
| **Rate (For 30W PoE Model)** | Controls the rate for the global storm policer. This value is restricted to 1-1024000 when "Unit" is fps, and 1-1024 when "Unit" is kfps. The rate is internally rounded up to the nearest value supported by the global storm policer. |
| **Unit** | Controls the unit of measure for the global storm policer rate as fps, kfps, kbps or Mbps. |
| **Port Storm Policer Configuration (For 90W PoE Model)** | |
| **Port** | The port number for which the configuration below applies. |
| **Enable** | Enable or disable the storm policer for this switch port. |
| **Rate** | Controls the rate for the port storm policer. This value is restricted to 10-13128147 when "Unit" is fps or kbps, and 1-13128 when "Unit" is kfps or Mbps. The rate is internally rounded up to the nearest value supported by the port storm policer. Supported rates are divisible by 10 fps or 25 kbps. |
| **Unit** | Controls the unit of measure for the port storm policer rate as fps, kfps, kbps or Mbps. |

| **Buttons** | |
|---|---|
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

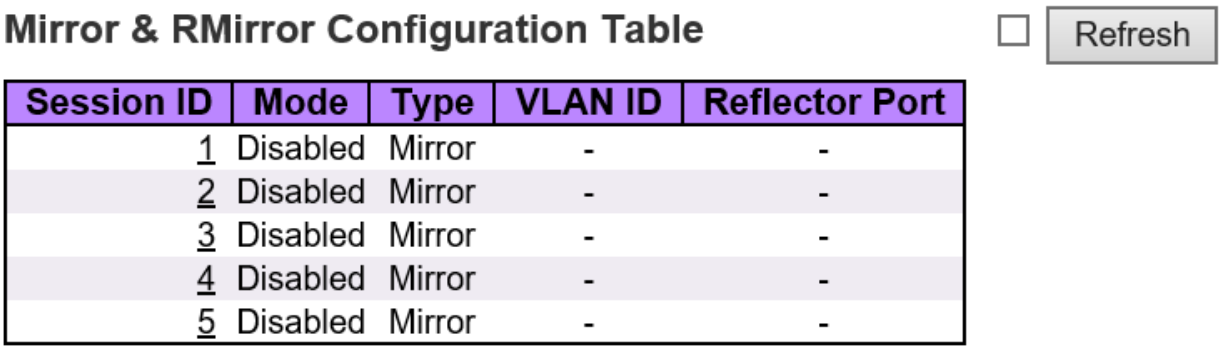
## 2.3.107 Mirror

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.

90W PoE Model



### Mirror & RMirror Configuration

#### Global Settings

| | |
|---|---|
| **Session ID** | 1 |
| **Mode** | Disabled |
| **Type** | Mirror |
| **VLAN ID** | 200 |
| **ReflectorPort** | Port 5 |

#### Source VLAN(s) Configuration

| | |
|---|---|
| **VLAN ID** | |

#### Port Configuration

| Port | Source | Destination |
|---|---|---|
| * | <> | |
| Port 1 | Disabled | |
| Port 2 | Disabled | |
| Port 3 | Disabled | |
| Port 4 | Disabled | |
| Port 5 | Disabled | |
| Port 6 | Disabled | |
| Port 7 | Disabled | |
| Port 8 | Disabled | |
| Port 9 | Disabled | |
| Port 10 | Disabled | |
| Port 11 | Disabled | |
| Port 12 | Disabled | |
| CPU | Disabled | |

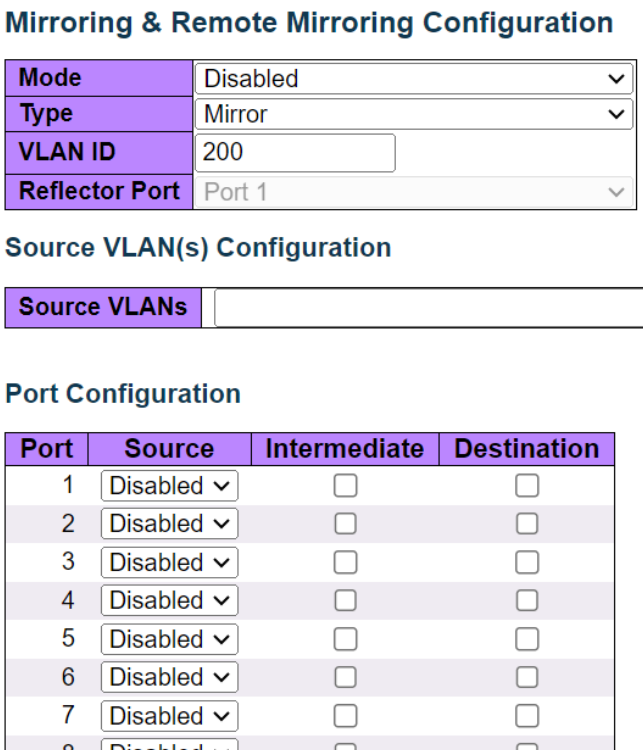
Save Reset Cancel

| Object | Description |
|---|---|
| **Mirror & RMirror Configuration Table/Global Settings** | |
| **Session ID** | Select session id to configure. |
| **Mode** | To Enabled/Disabled the mirror or Remote Mirroring function. |
| **Type** | Mirror: The switch is running on mirror mode. The source port(s) and destination port are located on this switch.<br>RMirror source: The switch is a source node for monitor flow. The source port(s), reflector port are located on this switch.<br>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.<br>In the stacking mode, you need to select switch ID to select the correct device.<br>If you shut down a port, it cannot be a candidate for reflector port.<br>If you shut down the port which is a reflector port, the remote mirror function cannot work.<br>Note1: The reflector port needs to select only on Source switch type.<br>Note2: The reflector port needs to disable MAC Table learning and STP.<br>Note3: The reflector port only supports on pure copper ports. |
| **Source VLAN(s) Configuration** | |
| **VLAN ID** | The switch can support VLAN-based Mirroring. If you want to monitor some VLANs on the switch, you can set the selected VLANs on this field. |
| **Port Configuration** | |
| **Port** | The logical port for the settings contained in the same row. |
| **Source** | Select mirror mode.<br>Disabled Neither frames transmitted nor frames received are mirrored.<br>Both Frames received and frames transmitted are mirrored on the Destination port.<br>Rx only Frames received on this port are mirrored on the Destination port. Frames transmitted are not mirrored.<br>Tx only Frames transmitted on this port are mirrored on the Destination port. Frames received are not mirrored. |
| **Destination** | Select destination port.<br>This checkbox is designed for mirror or Remote Mirroring.<br>The destination port is a switched port that you receive a copy of traffic from the source port.<br>Note1: On mirror mode, the device only supports one destination port.<br>Note2: The destination port needs to disable MAC Table learning. |

| **Buttons** | |
|---|---|
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

30W PoE Model



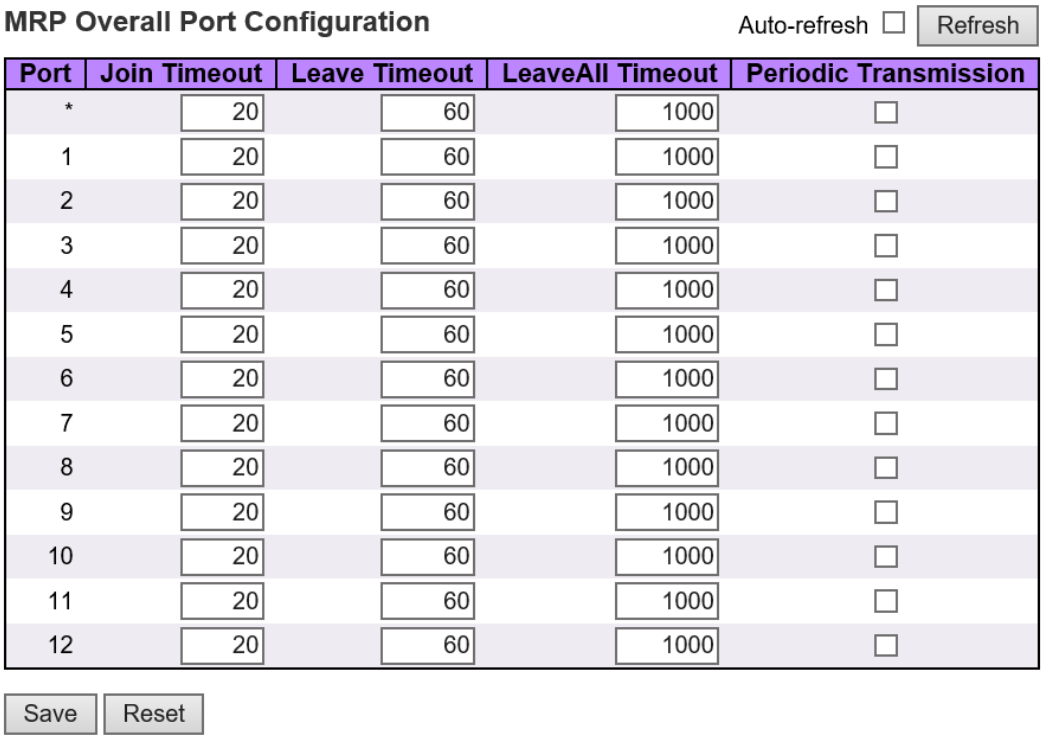

| Object | Description |
|---|---|
| **Mirror & RMirror Configuration Table/Global Settings** | |
| **Session ID** | Select session id to configure. |
| **Mode** | To Enabled/Disabled the mirror or Remote Mirroring function. |
| **Type** | Mirror: The switch is running on mirror mode. The source port(s) and destination port are located on this switch.<br>RMirror source: The switch is a source node for monitor flow. The source port(s), reflector port are located on this switch.<br>Intermediate: The switch is a forwarding node for monitor flow and the switch is an option node.<br>The object is to forward traffic from source switch to destination switch.<br>The intermediate ports are located on this switch.<br>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.<br>In the stacking mode, you need to select switch ID to select the correct device.<br>If you shut down a port, it cannot be a candidate for reflector port.<br>If you shut down the port which is a reflector port, the remote mirror function cannot work.<br>Note1: The reflector port needs to select only on Source switch type.<br>Note2: The reflector port needs to disable MAC Table learning and STP.<br>Note3: The reflector port only supports on pure copper ports. |
| **Source VLAN(s) Configuration** | |
| **Source VLANs** | The switch can support VLAN-based Mirroring. If you want to monitor some VLANs on the switch, you can set the selected VLANs on this field. |
| **Port Configuration** | |
| **Port** | The logical port for the settings contained in the same row. |
| **Source** | Select mirror mode.<br>Disabled Neither frames transmitted nor frames received are mirrored.<br>Both Frames received and frames transmitted are mirrored on the Destination port.<br>Rx only Frames received on this port are mirrored on the Destination port. Frames transmitted are not mirrored.<br>Tx only Frames transmitted on this port are mirrored on the Destination port. Frames received are not mirrored. |
| **Intermediate** | Select intermediate port.<br>This checkbox is designed for Remote Mirroring.<br>The intermediate port is a switched port to connect to other switch.<br>Note: The intermediate port needs to disable MAC Table learning. |
| **Destination** | Select destination port.<br>This checkbox is designed for mirror or Remote Mirroring.<br>The destination port is a switched port that you receive a copy of traffic from the source port.<br>Note1: On mirror mode, the device only supports one destination port.<br>Note2: The destination port needs to disable MAC Table learning. |

| **Buttons** | |
|---|---|
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

# 2.3.108MRP – Ports (For 90W PoE Model)

This page allows you to configure the MRP generic settings for all switch ports.



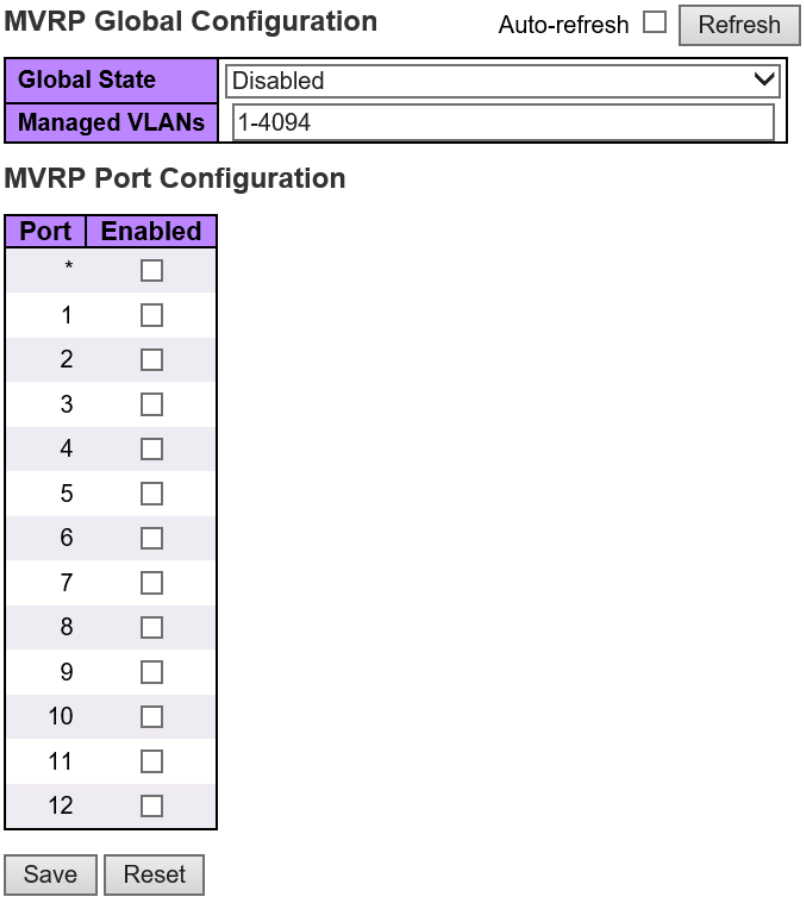

| Object | Description |
|---|---|
| **Port** | The port number for which the following configuration applies. |
| **Join Timeout** | Controls the timeout of the Join Timer for all MRP Applications on this switch port. This value is restricted to 1-20 centiseconds. |
| **Leave Timeout** | Controls the timeout of the Leave Timer for all MRP Applications on this switch port. This value is restricted to 60- 300 centiseconds. |
| **LeaveAll Timeout** | Controls the timeout of the LeaveAll Timer for all MRP Applications on this switch port. This value is restricted to 1000- 5000 centiseconds. |
| **Periodic Transmission** | Enable or disable the PeriodicTransmission feature for all MRP Applications on this switch port. |

| Buttons | |
|---|---|
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |
| Auto-refresh ☐ | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |

| | |
|---|---|
| Refresh | Click to refresh the page. |

## 2.3.109MRP – MVRP (For 90W PoE Model)

This page allows you to configure the MVRP global and per port settings altogether. The page is divided into a global section and a per-port configuration section.



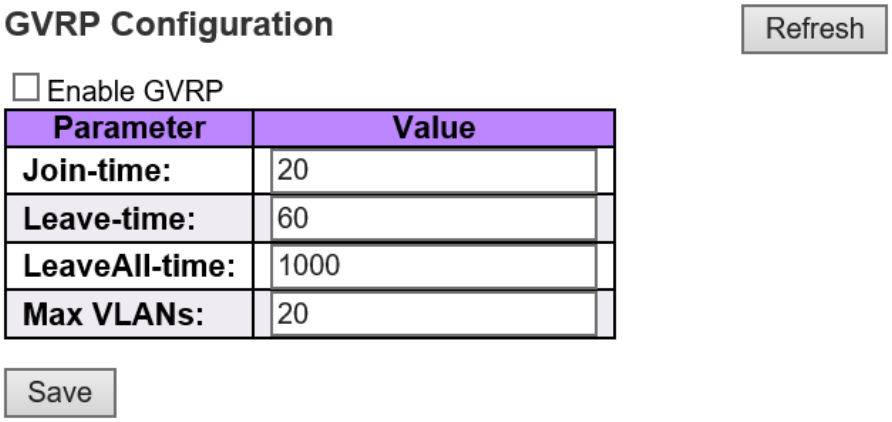

| Object | Description |
|---|---|
| **MVRP Global Configuration** | |
| **Global State** | Enable or disable the MVRP protocol globally. This will enable or disable the protocol globally and at the same time on the switch ports that are MVRP enabled. |
| **Managed VLANs** | This field shows the managed VLANs, i.e. the VLANs that MVRP will operate upon. By default, only VLANs 1- 4094 are managed, i.e. the entire range as defined in IEEE802.1Q-2014 for MVRP. However this range can be limited by using a list syntax where the individual elements are separated by commas. Ranges are specified with a dash separating the lower and upper bound.<br>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. |
| **MVRP Port Configuration** | |

| | |
|---|---|
| **Port** | The port number for which the following configuration applies. |
| **Enabled** | Enable or disable the MVRP protocol on this switch port. This will enable or disable the protocol on the switch port given that MVRP is also globally enabled. |

| **Buttons** | |
|---|---|
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |
| Auto-refresh ☐ | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |
| Refresh | Click to refresh the page. |

## 2.3.110GVRP - Global Config

This page allows you to configure the basic GVRP Configuration settings for all switch ports.

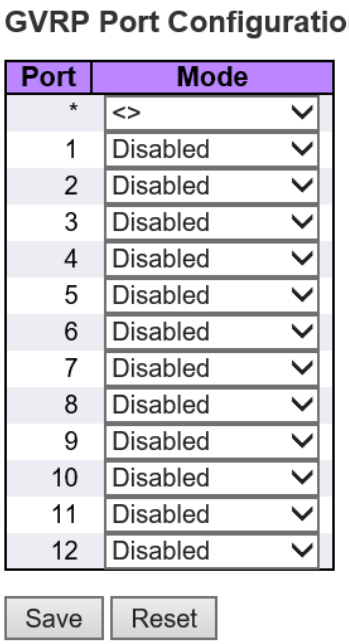



| Object | Description |
|---|---|
| **Enable GVRP** | The GVRP feature is enabled by setting the check mark in the checkbox named Enable GVRP. |
| **GVRP Protocol timers** | Join-time is a value in the range of 1-20cs, i.e. in units of one hundredth of a second. The default value is 20cs.<br>Leave-time is a value in the range of 60-300cs, i.e. in units of one hundredth of a second. The default is 60cs.<br>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. |
| **Max number of VLANs** | When GVRP is enabled a maximum number of VLANs supported by GVRP is specified. By default this number is 20. This number can only be changed when GVRP is turned off. |

| Buttons | |
|---|---|
| Save | Click to save changes. |
| Refresh | Click to refresh the page. Note that unsaved changes will be lost. |

## 2.3.111 GVRP - Port Config

This page allows you to enable a port for GVRP.



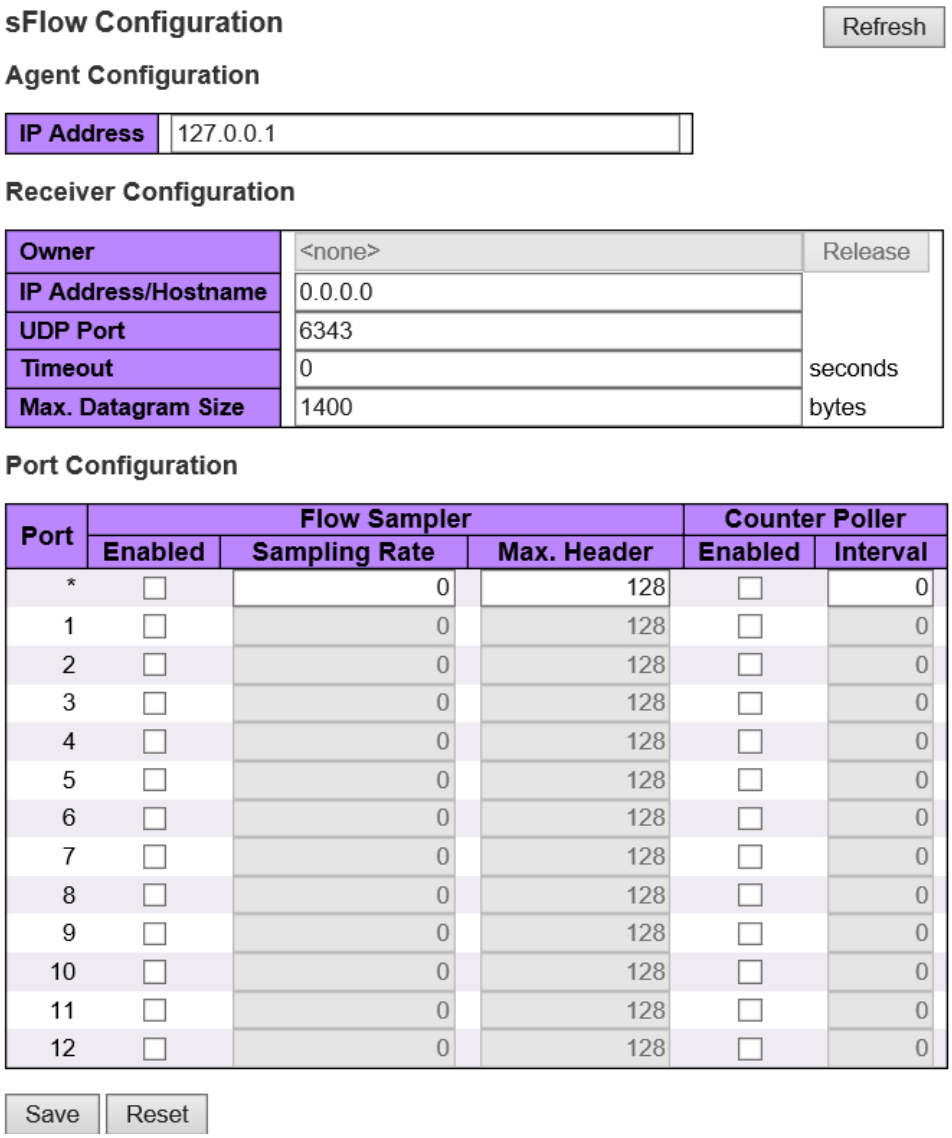

| Object | Description |
|---|---|
| **Port** | The logical port that is to be configured. |
| **Mode** | Mode can be either 'Disabled' or 'GVRP enabled'. These values turn the GVRP feature off or on respectively for the port in question. |

| Buttons | |
|---|---|
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

# 2.3.112sFlow

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.



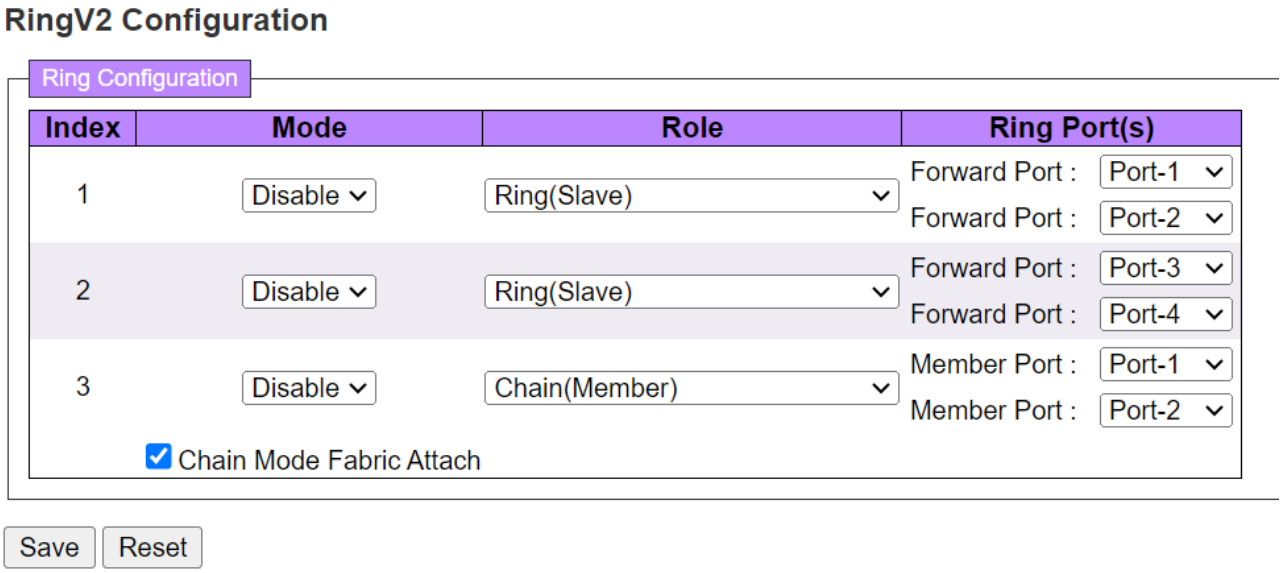

| Object | Description |
|---|---|
| **Agent Configuration** | |
| **IP Address** | The IP address used as Agent IP address in sFlow datagrams. It serves as a unique |

| | |
|---|---|
| | key that will identify this agent over extended periods of time.<br>Both IPv4 and IPv6 addresses are supported. |
| **Receiver Configuration** | |
| **Owner** | Basically, sFlow can be configured in two ways: Through local management using the Web or CLI interface or through SNMP. This read-only field shows the owner of the current sFlow configuration and assumes values as follows:<br>• If sFlow is currently unconfigured/unclaimed, Owner contains `<none>`.<br>• If sFlow is currently configured through Web or CLI, Owner contains `<Configured through local management>`.<br>• If sFlow is currently configured through SNMP, Owner contains a string identifying the sFlow receiver.<br>If sFlow is configured through SNMP, all controls - except for the Release-button - are disabled to avoid inadvertent reconfiguration.<br>The  button allows for releasing the current owner and disable sFlow sampling. The button is disabled if sFlow is currently unclaimed. If configured through SNMP, the release must be confirmed (a confirmation request will appear). |
| **IP Address/Hostname** | The IP address or hostname of the sFlow receiver. Both IPv4 and IPv6 addresses are supported. |
| **UDP Port** | The UDP port on which the sFlow receiver listens to sFlow datagrams. If set to 0 (zero), the default port (6343) is used. |
| **Timeout** | The number of seconds remaining before sampling stops and the current sFlow owner is released. While active, the current time left can be updated with a click on the Refresh-button. If locally managed, the timeout can be changed on the fly without affecting any other settings. Valid range is 0 to 2147483647 seconds. |
| **Max. Datagram Size** | The maximum number of data bytes that can be sent in a single sample datagram. This should be set to a value that avoids fragmentation of the sFlow datagrams. Valid range is 200 to 1468 bytes with default being 1400 bytes. |
| **Port Configuration** | |
| **Port** | The port number for which the configuration below applies. |
| **Flow Sampler Enabled** | Enables/disables flow sampling on this port. |
| **Flow Sampler Sampling Rate** | The statistical sampling rate for packet sampling. Set to N to sample on average 1/Nth of the packets transmitted/received on the port.<br>Not all sampling rates are achievable. If an unsupported sampling rate is requested, the switch will automatically adjust it to the closest achievable. This will be reported back in this field. Valid range is 1 to 32767. |
| **Flow Sampler Max.** | The maximum number of bytes that should be copied from a sampled packet to the |

| | |
|---|---|
| **Header** | sFlow datagram. Valid range is 14 to 200 bytes with default being 128 bytes.<br>To have room 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. |

| **Buttons** | |
|---|---|
| Release | See description under Owner. |
| Refresh | Click to refresh the page. Note that unsaved changes will be lost. |
| Save | Click to save changes. Note that sFlow configuration is not persisted to non-volatile memory. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

## 2.3.113RingV2



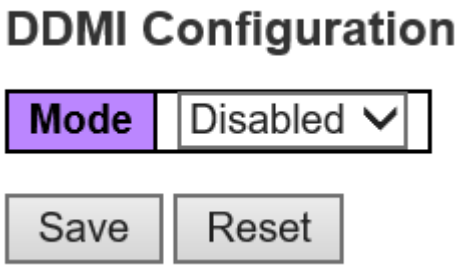

| Object | Description |
|---|---|
| **Index** | The group index. This parameter is used for easy identifying the ring when user configure it.<br>Group 1 (Index 1) - It supports configuration of ring.<br>Group 2 (Index 2) - It supports configuration of ring, coupling and dual-homing.<br>Group 3 (Index 3) - It supports configuration of chain and balancing-chain. |
| **Mode** | Enable Ring on the specific group.<br>When Group 1 or 2 is enabled, all configuration of Group 3 will be reset to default. Group 3 all configuration options will be locked.<br>To configure Group 3, both Group1 and 2 should be disabled first. When Group 3 is enabled, all configuration of Group1 and 2 will be reset to default. Group 1 and 2 all configuration options will be locked. |
| **Role** | Configure the Ring group on this switch as specific role.<br>Group 1 - support option of ring-master and ring-slave.<br># Ring - it could be master or slave.<br>Group 2 - support configuration of the ring, coupling and dual-homing.<br># Ring - it could be master or slave.<br># Coupling - it could be primary and backup.<br># Dual-Homing<br>Group 3 - support configuration of the chain and balancing-chain.<br># Chain - it could be head, tail or member.<br># Balancing Chain - it could be central-block, terminal-1/2 or member. |

| | |
|---|---|
| | Note 1 - Group 1 must be enabled before enable Group 2 to coupling.<br>Note 2 - When Group 1 or 2 is enabled, the configuration of Group 3 will be disabled.<br>Note 3 - When Group 3 is enabled, the configuration of Group 1 and 2 will be disabled. |
| **Ring Port(s)** | Selecting ring port(s).<br>Each ring port must be unique, CANNOT be configured in different groups; 2 ring ports between ring/chain CANNOT be the same.<br># When role is ring/master, one ring port is forward port and another is block port. The block port is redundant port; it is blocking port in normal state.<br># When role is ring/slave, both ring ports are forward port.<br># When role is coupling/primary, only need one ring port named primary port.<br># When role is coupling/backup, only need one ring port named backup port. This backup port is redundant port; it is blocking port in normal state.<br># When role is dual-homing, one ring port is primary port and another is backup port. This backup port is redundant port; it is blocking port in normal state.<br># When role is chain/head, one ring port is member port and another is head port. Both ring ports are forwarding port in normal state.<br># When role is chain/tail, one ring port is member port and another is tail port. The tail port is redundant port; it is blocking port in normal state.<br># When role is chain/member, both ring ports are member port. Both ring ports are forwarding port in normal state.<br># When role is balancing-chain/central-block, one ring port is member port and another is block port. The block port is redundant port; it is blocking port in normal state.<br># When role is balancing-chain/terminal-1/2, one ring port is member port and another is terminal port. Both ring ports are forwarding port in normal state.<br># When role is balancing-chain/member, both ring ports are member port. Both ring ports are forwarding port in normal state. |

| **Buttons** | |
|---|---|
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

## 2.3.114DDMI

Configure DDMI on this page.




| Object | Description |
|---|---|
| **Mode** | |
| **Enabled** | Enable DDMI mode operation. |
| **Disabled** | Disable DDMI mode operation. |

| Buttons | |
|---|---|
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

# 2.4 Monitor

## 2.4.1 System Information

The switch system information is provided here.

**System Information**

| System | |
|---|---|
| **Contact** | |
| **Name** | |
| **Location** | |
| **Hardware** | |
| **MAC Address** | 00-00-c1-0d-ae-fe |
| **Serial Number** | aaaaaaaaasssssss |
| **Chip ID** | VSC7546 |
| **Previous Restart** | Power on |
| **Time** | |
| **System Date** | 1970-01-02T01:32:18+00:00 |
| **System Uptime** | 1d 01:32:18 |
| **Software** | |
| **Software Version** | 00.00.01.0002 |
| **Software Date** | 2023-03-22T07:39:07+08:00 |
| **Code Revision** | ISTAX-APPL-2021.03 |
| **Licenses** | Details |

| Object | Description |
|---|---|
| **Contact** | The system contact configured in Configuration \| System \| Information \| System Contact. |
| **Name** | The system name configured in Configuration \| System \| Information \| System Name. |
| **Location** | The system location configured in Configuration \| System \| Information \| System Location. |
| **MAC Address** | The MAC Address of this switch. |
| **Serial No.** | The serial number of this switch. |
| **Chip ID** | The Chip ID of this switch. |
| **System Date** | The current (GMT) system time and date. The system time is obtained through the Timing server running on the switch, if any. |
| **System Uptime** | The period of time the device has been operational. |
| **Software Version** | The software version of this switch. |
| **Software Date** | The date when the switch software was produced. |
| **Code Revision (For 90W** | The version control identifier of the switch software. |

| | |
|---|---|
| **PoE Model)** | |

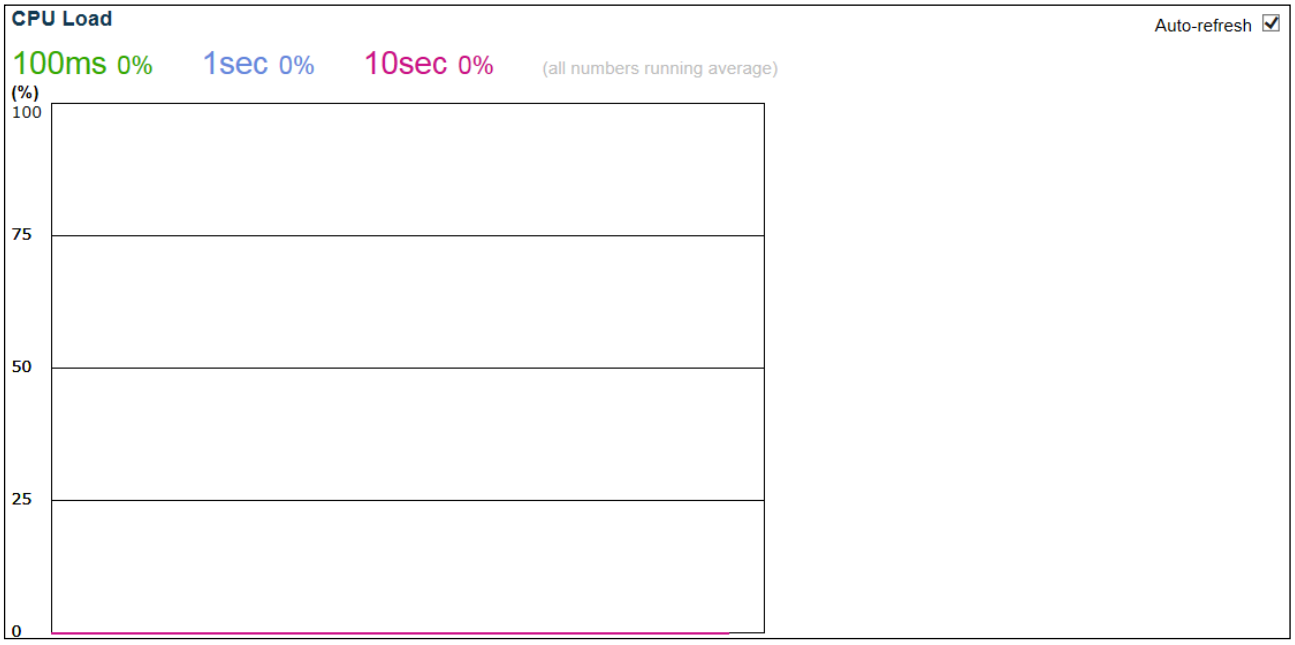
| **Buttons** | |
|---|---|
| Auto-refresh ☐ | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |
| Refresh | Click to refresh the page. |

## 2.4.2 CPU Load

This page displays the CPU load, using an SVG graph.

The load is measured as averaged over the last 100ms, 1sec and 10 seconds intervals. The last 120 samples are graphed, and the last numbers are displayed as text as well.

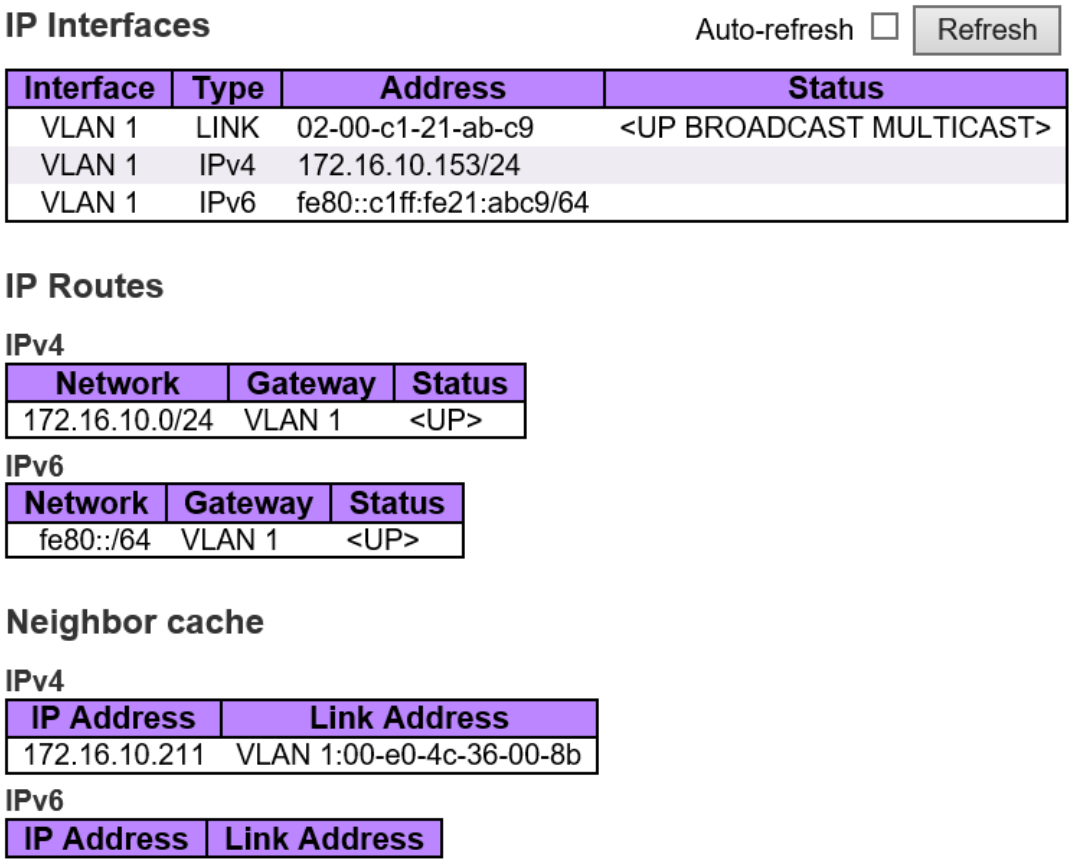
In order to display the SVG graph, your browser must support the SVG format. Consult the SVG Wiki for more information on browser support. Specifically, at the time of writing, Microsoft Internet Explorer will need to have a plugin installed to support SVG.




| **Buttons** | |
|---|---|
| Auto-refresh ☑ | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |

## 2.4.3 IP Status

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




| Object | Description |
|---|---|
| **IP Interfaces** | |
| **Interface** | The name of the interface. |
| **Type** | The address type of the entry. This may be LINK, IPv4 or IPv6. |
| **Address** | The current address of the interface (of the given type). |
| **Status** | The status flags of the interface (and/or address). |
| **IP Routes** | |
| **Network** | The destination IP network or host address of this route. |
| **Gateway** | The gateway address of this route. |
| **Status** | The status flags of the route. |

| Neighbor cache | |
|---|---|
| **IP Address** | The IP address of the entry. |
| **Link Address** | The Link (MAC) address for which a binding to the IP address given exist.. |

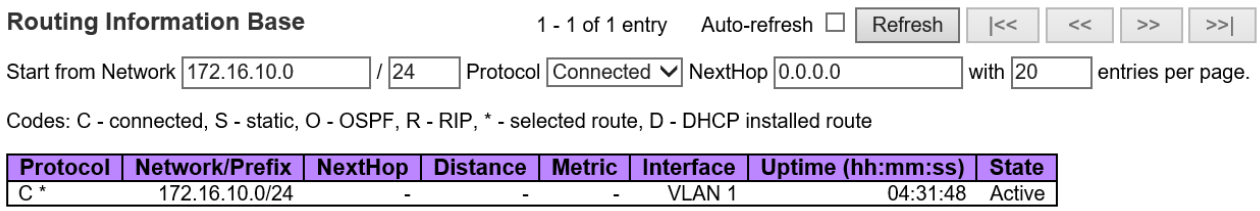
| Buttons | |
|---|---|
| Refresh | Click to refresh the page. |
| Auto-refresh ☑ | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |

## 2.4.4 IPv4 Routing Info. Base

Each page shows up to 999 table entries, selected through the "entries per page" input field. When first visited, the web page will show the beginning entries of this table.

The "Start from ID" input field allow the user to change the starting point in this table. Clicking the Refresh button will update the displayed table starting from that or the closest next entry match.

In addition, these input fields will upon a Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start input field.




| Object | Description |
|---|---|
| **Protocol** | The protocol that installed this route.<br>DHCP: The route is created by DHCP.<br>Connected: The destination network is connected directly.<br>Static: The route is created by user.<br>OSPF: The route is created by OSPF. |
| **Network/Prefix** | Network and prefix (example 10.0.0.0/16) of the given route entry. |
| **NextHop** | Next-hop IP address. All-zeroes indicates the link is directly connected. |
| **Interface** | Next-hop interface. |

| | |
|---|---|
| **Distance** | Distance of the route. |
| **Metric** | Metric of the route. |
| **Uptime (hh:ss:mm)** | Time (in seconds) since this route was created |
| **State** | Destination is active. |

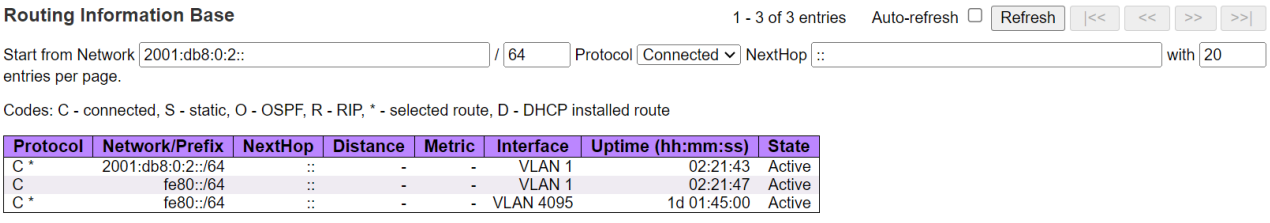
| Buttons | |
|---|---|
| Refresh | Click to refresh the page. |
| Auto-refresh ☑ | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |
| \|<< | Updates the table entries, starting from the first available entry. If the first entry of the table is displayed, the button is disabled |
| << | Updates the table entries, ending at the entry prior to the first entry currently displayed. If the first entry of the table is displayed, the button is disabled |
| >> | Updates the table entries, starting from the entry next to the last entry currently displayed. If the last entry of the table is displayed, the button is disabled. |
| >>\| | Updates the table entries, ending at the last available entry. If the last entry of the table is displayed, the button is disabled. |

## 2.4.5 IPv6 Routing Info. Base

Each page shows up to 999 table entries, selected through the "entries per page" input field. When first visited, the web page will show the beginning entries of this table.

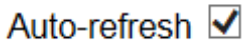
The "Start from ID" input field allow the user to change the starting point in this table. Clicking the Refresh button will update the displayed table starting from that or the closest next entry match.

In addition, these input fields will upon a Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start input field.




| Object | Description |
|---|---|
| **Protocol** | The protocol that installed this route. |

| | |
|---|---|
| | DHCP: The route is created by DHCP.<br>Connected: The destination network is connected directly.<br>Static: The route is created by user.<br>OSPF: The route is created by OSPF. |
| **Network/Prefix** | Network and prefix (example 10.0.0.0/16) of the given route entry. |
| **NextHop** | Next-hop IP address. All-zeroes indicates the link is directly connected. |
| **Interface** | If the next-hop address is a link-local address, then this is the VLAN interface of the link-local address. Otherwise this value is not used |
| **Distance** | Distance of the route. |
| **Metric** | Metric of the route. |
| **Uptime (hh:ss:mm)** | Time (in seconds) since this route was created |
| **State** | Destination is active. |

| **Buttons** | |
|---|---|
|  | Click to refresh the page. |
|  | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |
|  | Updates the table entries, starting from the first available entry. If the first entry of the table is displayed, the button is disabled |
|  | Updates the table entries, ending at the entry prior to the first entry currently displayed. If the first entry of the table is displayed, the button is disabled |
|  | Updates the table entries, starting from the entry next to the last entry currently displayed. If the last entry of the table is displayed, the button is disabled. |
|  | Updates the table entries, ending at the last available entry. If the last entry of the table is displayed, the button is disabled. |

## 2.4.6 System Log

Each page shows up to 999 table entries, selected through the "entries per page" input field. When first visited, the web page will show the beginning entries of this table.

The "Level" input field is used to filter the display system log entries.

The "Clear Level" input field is used to specify which system log entries will be cleared.

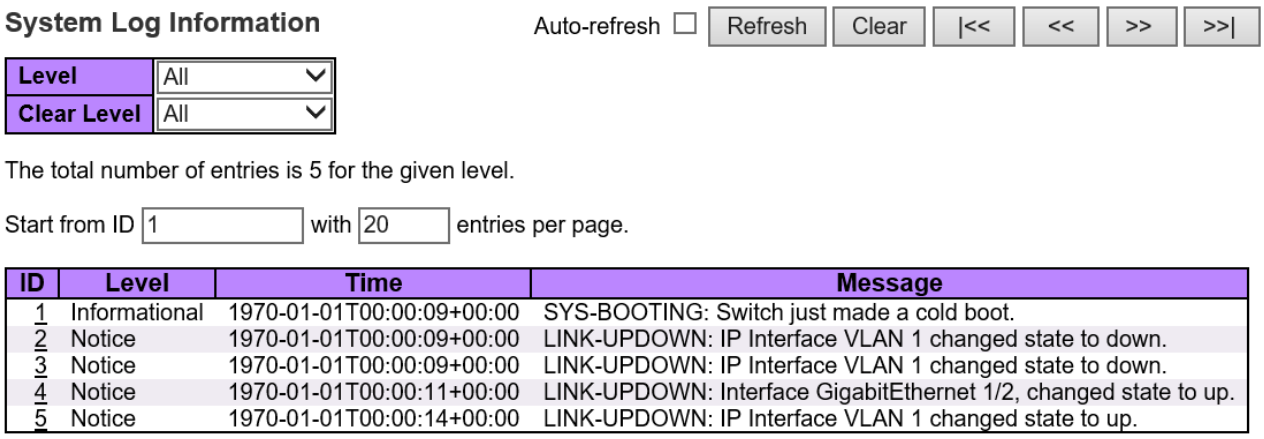
To clear specific system log entries, select the clear level first then click the Clear button.

The "Start from ID" input field allow the user to change the starting point in this table. Clicking the Refresh button will update the displayed table starting from that or the closest next entry match.

In addition, these input fields will upon a Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start input field.

The >> will use the last entry of the currently displayed table as a basis for the next lookup.

When the end is reached the text "No more entries" is shown in the displayed table. Use the |<< button to start over.



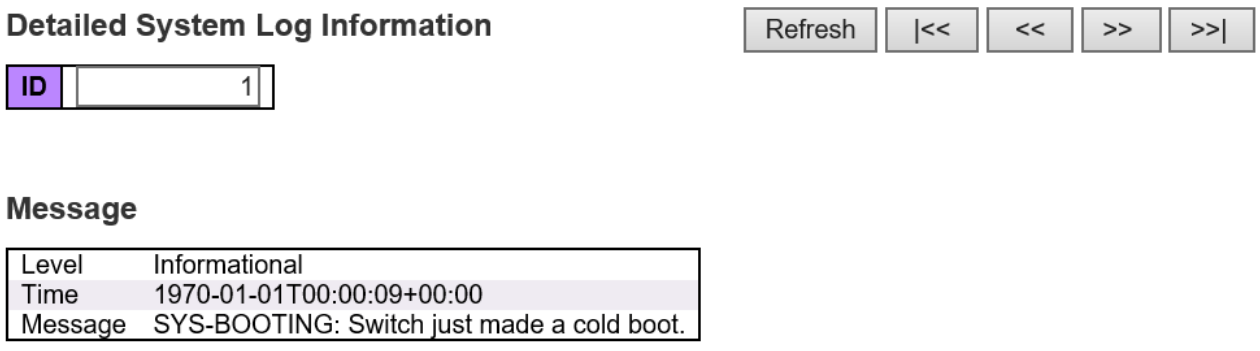

| Object | Description |
|---|---|
| **ID** | The identification of the system log entry. |
| **Level** | The level of the system log entry.<br>**Info**: The system log entry is belonged information level.<br>**Warning**: The system log entry is belonged warning level. |

| | |
|---|---|
| | **Error**: The system log entry is belonged error level. |
| **Time** | The occurred time of the system log entry. |
| **Message** | The detail message of the system log entry. |

| Buttons | |
|---|---|
| Auto-refresh ☑ | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |
| Refresh | Updates the table entries, starting from the current entry. |
| Clear | Flushes the selected entries. |
| \|<< | Updates the table entries, starting from the first available entry. |
| << | Updates the table entries, ending at the last entry currently displayed. |
| >> | Updates the table entries, starting from the last entry currently displayed. |
| >>\| | Updates the table entries, ending at the last available entry. |

## 2.4.7 System Detailed Log

The switch system detailed log information is provided here.



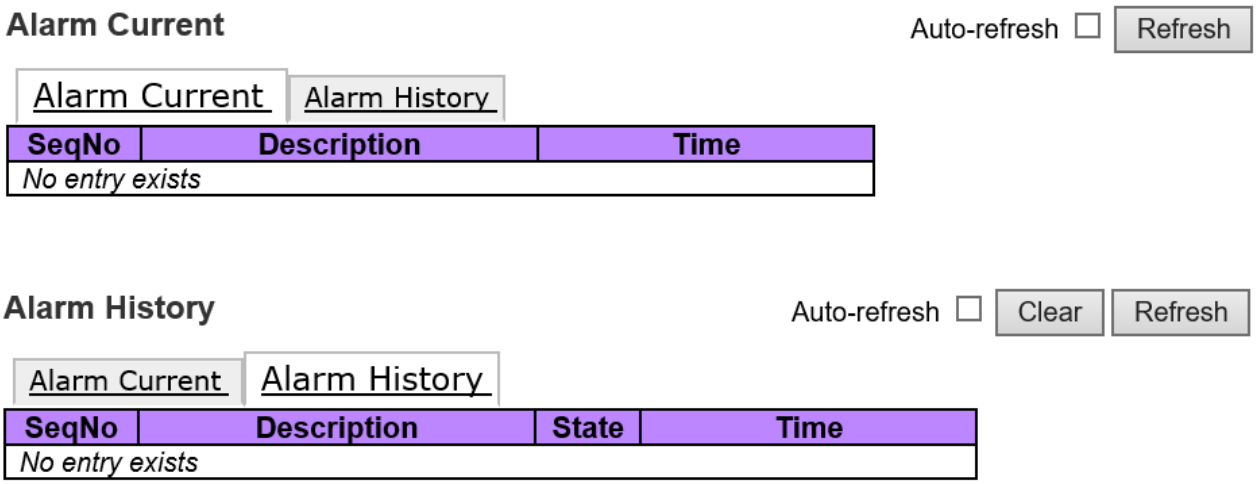

| Object | Description |
|---|---|
| **Level** | The severity level of the system log entry. |

| | |
|---|---|
| **ID** | The ID (>= 1) of the system log entry. |
| **Message** | The detailed message of the system log entry. |

| Buttons | |
|---|---|
| Refresh | Updates the system log entry to the current entry ID. |
| \|<< | Updates the system log entry to the first available entry ID. |
| << | Updates the system log entry to the previous available entry ID. |
| >> | Updates the system log entry to the next available entry ID. |
| >>\| | Updates the system log entry to the last available entry ID. |

## 2.4.8 System Alarm

Current Alarm is provided on this page.




| Object | Description |
|---|---|
| **SeqNo (For 90W PoE Model)** | Alarm Sequence Number. |

| | |
|---|---|
| **Description** | Alarm Type Description. |
| **State** | Alarm State. Set stands for alarm occurs; Cleared stands for alarm disappear. |
| **Time** | Alarm occurrence date time. |

| **Buttons** | |
|---|---|
| Auto-refresh ☐ | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |
| Refresh | Click to refresh data. |
| Clear : | Click to Clear data. |

## 2.4.9 Green Ethernet

**Port Power Savings Status**

Auto-refresh ☐ Refresh

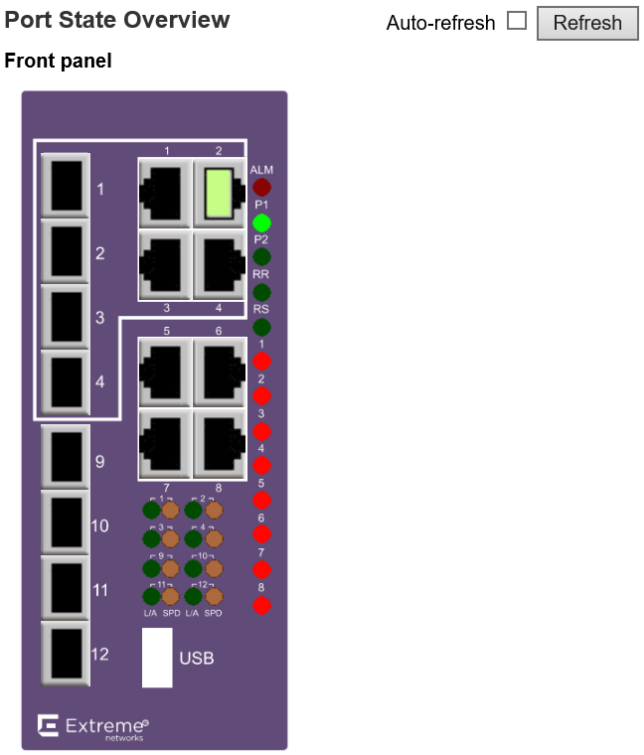
| Port | Link | EEE Cap | EEE Ena | LP EEE Cap | EEE In power save | ActiPhy Savings | PerfectReach Savings |
|---|---|---|---|---|---|---|---|
| 1 | ● | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ |
| 2 | ● | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ |
| 3 | ● | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ |
| 4 | ● | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ |
| 5 | ● | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ |
| 6 | ● | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ |
| 7 | ● | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ |
| 8 | ● | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ |
| 9 | ● | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| 10 | ● | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| 11 | ● | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| 12 | ● | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |

| Object | Description |
|---|---|
| **Local Port** | This is the logical port number for this row. |
| **Link** | Shows if the link is up for the port (green = link up, red = link down). |
| **EEE cap** | Shows if the port is EEE capable. |
| **EEE Ena** | Shows if EEE is enabled for the port (reflects the settings at the Port Power Savings configuration page). |
| **LP EEE cap** | Shows if the link partner is EEE capable. |
| **EEE In power save** | Shows if the system is currently saving power due to EEE. When EEE is enabled, the system will powered down if no frame has been received or transmitted in 5 uSec. |
| **Actiphy Savings** | Shows if the system is currently saving power due to ActiPhy. |
| **PerfectReach Savings** | Shows if the system is currently saving power due to PerfectReach. |

| Buttons | |
|---|---|
| Auto-refresh ☐ | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |
| Refresh | Click to refresh data. |

## 2.4.10 Ports State

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




The port states are illustrated as follows:

| **RJ45 ports** | | | |
|---|---|---|---|
| **State** | Disabled | Down | Link |

| Buttons | |
|---|---|
| Auto-refresh ☑ | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |
| Refresh | Click to refresh the page. |

## 2.4.11 Trafice Overview

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

**Port Statistics Overview**

Auto-refresh ☐ Refresh Clear

| Port | Packets | | Bytes | | Errors | | Drops | | Filtered |
|---|---|---|---|---|---|---|---|---|---|
| | Received | Transmitted | Received | Transmitted | Received | Transmitted | Received | Transmitted | Received |
| 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 2 | 25569 | 51168 | 2252917 | 55549827 | 6 | 0 | 0 | 0 | 1622 |
| 3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 6 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 7 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 9 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 10 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 11 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 12 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

| Object | Description |
|---|---|
| **Port** | The logical port for the settings contained in the same row. |
| **Packet** | The number of received and transmitted packets per port. |
| **Bytes** | The number of received and transmitted bytes per port. |
| **Errors** | The number of frames received in error and the number of incomplete transmissions per port. |
| **Drops** | The number of frames discarded due to ingress or egress congestion. |
| **Filtered** | The number of received frames filtered by the forwarding process. |

| Buttons | |
|---|---|
| Refresh | Click to refresh the page immediately. |
| Clear | Clears the counters for all ports. |
| Auto-refresh ☑ | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |

## 2.4.12 QoS Statistics

This page provides statistics for the different queues for all switch ports.

**Queuing Counters**

Auto-refresh ☐ Refresh Clear

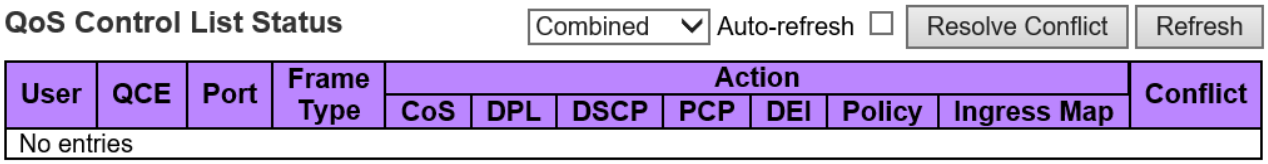
| Port | Q0 | | Q1 | | Q2 | | Q3 | | Q4 | | Q5 | | Q6 | | Q7 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Rx | Tx | Rx | Tx | Rx | Tx | Rx | Tx | Rx | Tx | Rx | Tx | Rx | Tx | Rx | Tx |
| 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 2 | 25602 | 40581 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 10650 |
| 3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 6 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 7 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 9 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 10 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 11 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 12 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

| Object | Description |
|---|---|
| **Port** | The logical port for the settings contained in the same row. |
| **Qn** | There are 8 QoS queues per port. Q0 is the lowest priority queue. |
| **Rx/Tx** | The number of received and transmitted packets per queue |

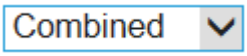
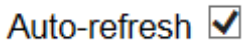
| Buttons | |
|---|---|
| Auto-refresh ☑ | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |
| Refresh | Click to refresh the page immediately. |
| Clear | Clears the counters for all ports. |

## 2.4.13 QCL Status

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



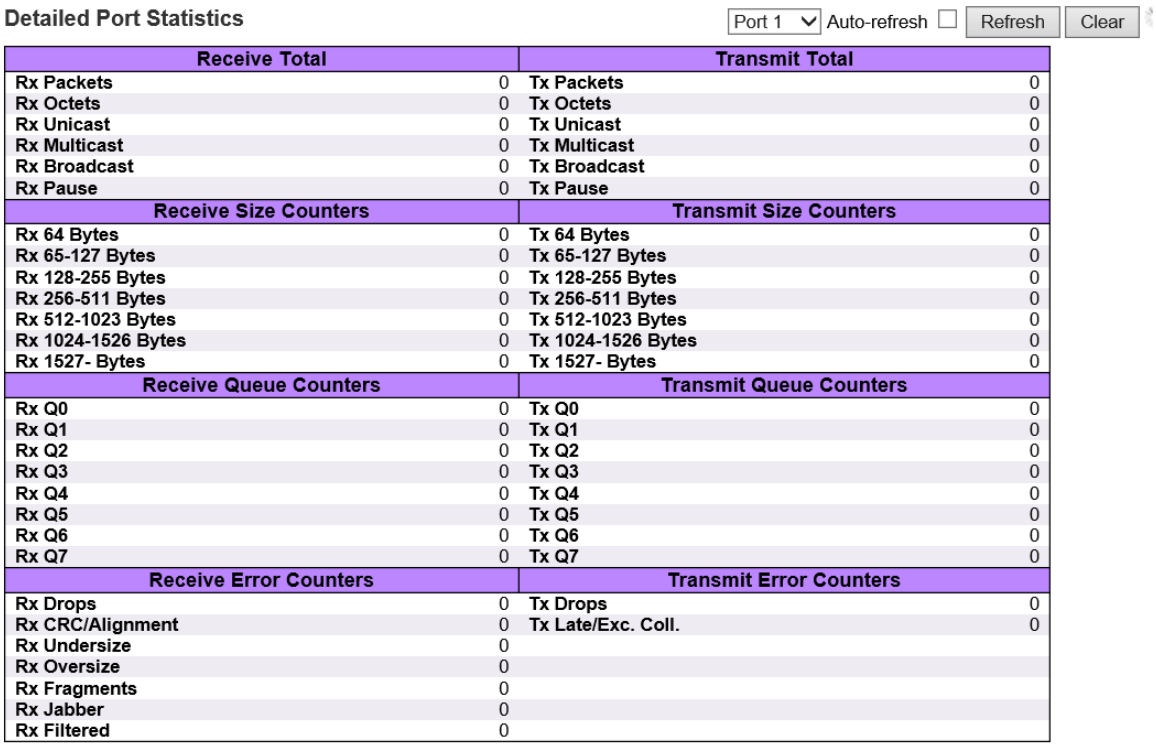

| Object | Description |
|---|---|
| **User** | Indicates the QCL user. |
| **QCE** | Indicates the QCE id. |
| **Port** | Indicates the list of ports configured with the QCE. |
| **Frame Type** | Indicates the type of frame. Possible values are:<br>**Any**: Match any frame type.<br>**Ethernet**: Match EtherType frames.<br>**LLC**: Match (LLC) frames.<br>**SNAP**: Match (SNAP) frames.<br>**IPv4**: Match IPv4 frames.<br>**IPv6**: Match IPv6 frames |
| **Action** | Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content.<br>Possible actions are:<br>CoS: Classify Class of Service.<br>DPL: Classify Drop Precedence Level.<br>DSCP: Classify DSCP value.<br>PCP: Classify PCP value.<br>DEI: Classify DEI value.<br>Policy: Classify ACL Policy number.<br>Ingress Map: Classify Ingress Map ID. (For 90W PoE Model) |
| **Conflict** | Displays Conflict status of QCL entries. As H/W resources are shared by multiple applications. It may happen that resources required to add a QCE may not be available, in that case it shows conflict status as 'Yes', otherwise it is always 'No'. Please note that conflict can be resolved by releasing the H/W resources required to add QCL entry on pressing 'Resolve Conflict' button. |

| Buttons | |
|---|---|
|  | Select the QCL status from this drop down list. |
|  | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |
|  | Click to release the resources required to add QCL entry, in case the conflict status for any QCL entry is 'yes'. |
|  | Click to refresh the page. |

## 2.4.14 Detailed Statistics

This page provides detailed traffic statistics for a specific switch port. Use the port select box to select which switch port details to display.

The displayed counters are the totals for receive and transmit, the size counters for receive and transmit, and the error counters for receive and transmit.




| Object | Description |
|---|---|
| **Receive Total and Transmit Total** | |
| **Rx and Tx Packets** | The number of received and transmitted (good and bad) packets. |
| **Rx and Tx Octets** | The number of received and transmitted (good and bad) bytes. Includes FCS, but excludes framing bits. |
| **Rx and Tx Unicast** | The number of received and transmitted (good and bad) unicast packets. |
| **Rx and Tx Multicast** | The number of received and transmitted (good and bad) multicast packets. |
| **Rx and Tx Broadcast** | The number of received and transmitted (good and bad) broadcast packets. |
| **Rx and Tx Pause** | A count of the MAC Control frames received or transmitted on this port that have an opcode indicating a PAUSE operation. |
| **Receive and Transmit Size Counters** | |
| The number of received and transmitted (good and bad) packets split into categories based on their respective frame sizes. | |

| Receive and Transmit Queue Counters | |
|---|---|
| The number of received and transmitted packets per input and output queue. | |
| **Receive Error Counters** | |
| **Rx Drops** | The number of frames dropped due to lack of receive buffers or egress congestion. |
| **Rx CRC/Alignment** | The number of frames received with CRC or alignment errors. |
| **Rx Undersize** | The number of short [1] frames received with valid CRC. |
| **Rx Oversize** | The number of long [2] frames received with valid CRC. |
| **Rx Fragments** | The number of short [1] frames received with invalid CRC. |
| **Rx Jabber** | The number of long [2] frames received with invalid CRC. |
| **Rx Filtered** | The number of received frames filtered by the forwarding process.<br>[1] Short frames are frames that are smaller than 64 bytes.<br>[2] Long frames are frames that are longer than the configured maximum frame length for this port. |
| **Transmit Error Counters** | |
| **Tx Drops** | The number of frames dropped due to output buffer congestion. |
| **Tx Late/Exc. Coll** | The number of frames dropped due to excessive or late collisions. |

| Buttons | |
|---|---|
| Refresh | Click to refresh the page immediately. |
| Clear | Click to refresh the page immediately. |
| Auto-refresh ☑ | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |

## 2.4.15 Name Map (For 90W PoE Model)

Many Web pages use a port number to express an interface, whereas CLI uses interface names. The table on this page provides a means to convert from one to the other.

### Interface Name to Port Number Map

| Interface Name | Port Number |
|---|---|
| Gi 1/1 | 1 |
| Gi 1/2 | 2 |
| Gi 1/3 | 3 |
| Gi 1/4 | 4 |
| Gi 1/5 | 5 |
| Gi 1/6 | 6 |
| Gi 1/7 | 7 |
| Gi 1/8 | 8 |
| 10G 1/1 | 9 |
| 10G 1/2 | 10 |
| 10G 1/3 | 11 |
| 10G 1/4 | 12 |

## 2.4.16 CFM (For 90W PoE Model)

Monitor CFM Status on this page.

**CFM MEP Status**

Auto-refresh ☐ Refresh

| Domain | Service | MEPID | Port | State | | SMAC | Defects | | CCM Rx | | | CCM Tx |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Active | Fng | | Highest | Defects | Valid | Invalid | Errors | |
| No entry exists | | | | | | | | | | | | |

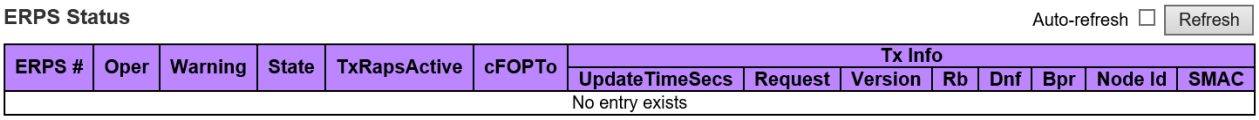
| Object | Description |
|---|---|
| **Domain** | Name of Domain under which this MEP resides. |
| **Service** | Name of Service under which this MEP resides. |
| **MEPID** | The identification of this MEP. |
| **Port** | Port on which this MEP resides. |
| **State** | Active Operational state of the MEP.<br>: OFF. This indicates that the MEP Admin State is disabled.<br>: DOWN. The MEP Admin State is enabled, but an error state exists.<br>: UP. The MEP Admin State is enabled, and no errors and defects exists.<br>Fng : Holds the current state of the Fault Notification Generator State Machine.<br>Values will be one of the following:<br>state Description<br>reset No defect has been present since reset timer expired or the State Machine was last reset.<br>defect A defect is present, but not for a long enough time to be reported.<br>reportDefect A transient state during which the defect is reported.<br>defectReported A defect is present, and some defect has been reported.<br>defectClearing No defect is present, but the ResetTime timer has not yet expired. |
| **SMAC** | This MEP's MAC address. |
| **Defects** | Highest priority defect that has been present since the MEP's fault notification generator state machine was last in the reset state.<br>Defects : A MEP can detect and report a number of defects, and multiple defects can be present at the same time. This is indicated the following letter code.<br>Code Defect Description<br>- Defect not present Defect not present<br>R someRDIdefect RDI received from at least one remote MEP<br>M someMACstatusDefect Received Port Status TLV != psUp or Interface Status TLV != isUp<br>C someRMEPCCMdefect Valid CCM is not received within 3.5 times CCM interval |

| | |
|---|---|
| | from at least one remote MEP<br>E errorCCMdefect Received CCM from an unknown remote MEP-ID or CCM interval mismatch<br>X xconCCMdefect Received CCM with an MD/MEG level smaller than configured or wrong MAID/MEGID (cross-connect) |
| **CCM Rx** | Valid: Total number of CCMs that hit this MEP and passed the validation test.<br>Invalid: Total number of CCMs that hit this MEP and didn't pass the validation test.<br>Errors: Total number of out-of-sequence errors seen from RMEPs. |
| **CCM Tx** | Total number of CCM PDUs transmitted by this MEP. |

| **Buttons** | |
|---|---|
| Refresh | Click to refresh the page immediately. |

## 2.4.17 ERPS (For 90W PoE Model)

This shows the current status of the ERPS instances.

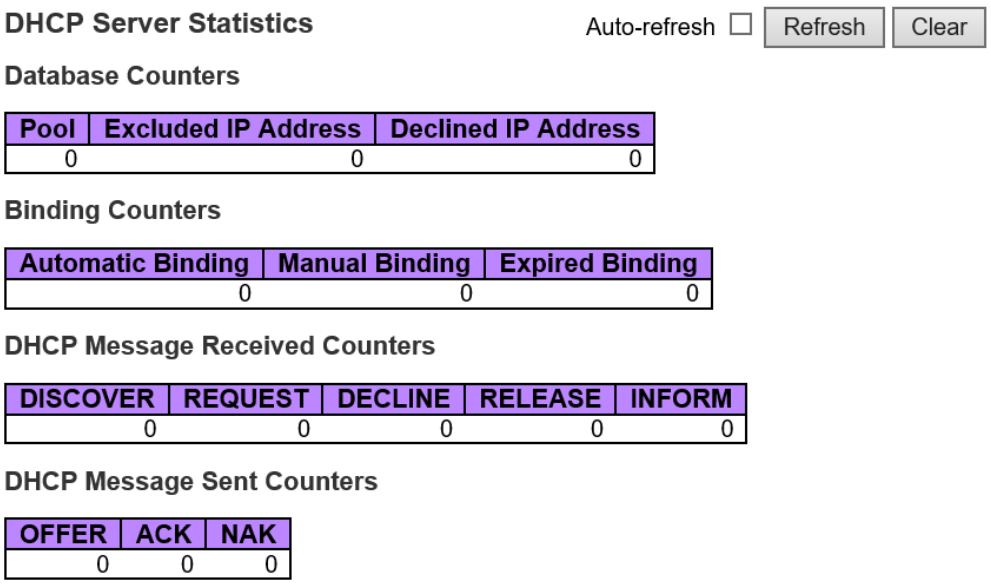



| Object | Description |
|---|---|
| **ERPS #** | The ID of the ERPS. Click on link to get to ERPS detailed instance page, you can reset counters and issue commands. |
| **Oper** | The operational state of ERPS instance.<br>: Active.<br>: Disabled or Internal error. |
| **Warning** | Operational warnings of ERPS instance.<br>: No warnings.<br>: There are warnings, use tooltip to see. |
| **State** | Specifies protection/node state of ERPS. |
| **TxRapsActive** | Specifies whether we are currently supposed to be transmitting R-APS PDUs on our ring ports. |
| **cFOPTo** | Failure of Protocol - R-APS Rx Time Out. |
| **UpdateTimeSecs** | Time in seconds since boot that this structure was last updated. |
| **Request** | Request/state according to G.8032, table 10-3. |
| **Version** | Version of received/used R-APS Protocol. 0 means v1, 1 means v2, etc. |
| **Rb** | RB (RPL blocked) bit of R-APS info. See Figure 10-3 of G.8032. |
| **Dnf** | DNF (Do Not Flush) bit of R-APS info. See Figure 10-3 of G.8032." |
| **Bpr** | BPR (Blocked Port Reference) of R-APS info. See Figure 10-3 of G.8032. |
| **Node ID** | Node ID of this request. |
| **SMAC** | The Source MAC address used in the request/state. |

| Buttons | |
|---|---|
| Auto-refresh ☑ | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |
| Refresh | Click to refresh the page immediately. |

## 2.4.18 DHCP Server - Statistics

This page displays the database counters and the number of DHCP messages sent and received by DHCP server.



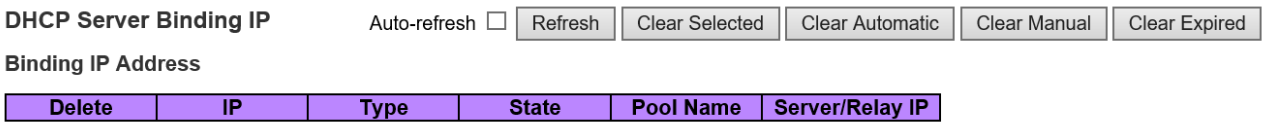

| Object | Description |
|---|---|
| **Database Counters** | |
| **Pool** | Number of pools. |
| **Excluded IP Address** | Number of excluded IP address ranges. |
| **Declined IP Address** | Number of declined IP addresses. |
| **Binding Counters** | |
| **Automatic Binding** | Number of bindings with network-type pools. |
| **Manual Binding** | Number of bindings that administrator assigns an IP address to a client. That is, the pool is of host type. |
| **Expired Binding** | Number of bindings that their lease time expired or they are cleared from Automatic/Manual type bindings. |
| **DHCP Message Received Counters** | |
| **DISCOVER** | Number of DHCP DISCOVER messages received. |
| **REQUEST** | Number of DHCP REQUEST messages received. |
| **DECLINE** | Number of DHCP DECLINE messages received. |
| **RELEASE** | Number of DHCP RELEASE messages received. |

| | |
|---|---|
| **INFORM** | Number of DHCP INFORM messages received. |
| **DHCP Message Sent Counters** | |
| **OFFER** | Number of DHCP OFFER messages sent. |
| **ACK** | Number of DHCP ACK messages sent. |
| **NAK** | Number of DHCP NAK messages sent. |

| **Buttons** | |
|---|---|
| Auto-refresh ☑ | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |
| Refresh | Click to refresh the page immediately. |
| Clear | Click to Clears DHCP Message Received Counters and DHCP Message Sent Counters. |

## 2.4.19 DHCP Server - Binding

This page displays bindings generated for DHCP clients.

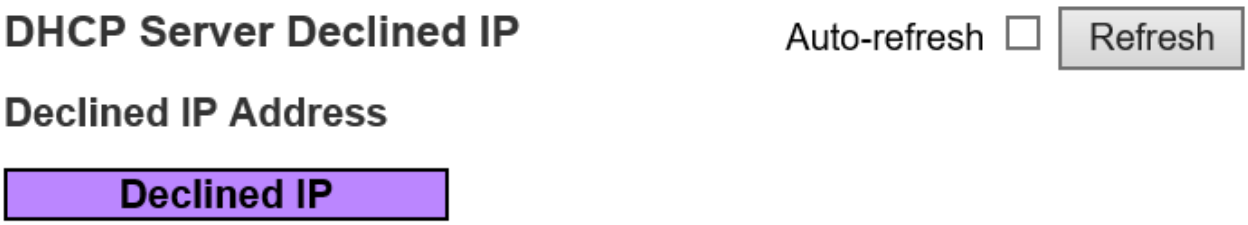



| Object | Description |
|---|---|
| **IP** | IP address allocated to DHCP client. |
| **Type** | Type of binding. Possible types are Automatic, Manual, Expired. |
| **State** | State of binding. Possible states are Committed, Allocated, Expired. |
| **Pool Name** | The pool that generates the binding. |
| **Server/Relay IP** | Either IP address of dhcp server or, in case of relayed binding, IP address of relay agent through which binding was negotiated. |

| Buttons | |
|---|---|
| Auto-refresh ☐ | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |
| Refresh | Click to refresh the page immediately. |
| Clear Selected | Click to clear selected bindings. If the selected binding is Automatic or Manual, then it is changed to be Expired. If the selected binding is Expired, then it is freed. |
| Clear Automatic | Click to clear all Automatic bindings and Change them to Expired bindings. |
| Clear Manual | Click to clear all Manual bindings and Change them to Expired bindings. |
| Clear Expired | Click to clear all Expired bindings and free them. |

## 2.4.20 DHCP Server - Declined IP

This page displays declined IP addresses.




| Object | Description |
|---|---|
| **Declined IP** | List of IP addresses declined. |

| Buttons | |
|---|---|
| Auto-refresh ☐ | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |
| Refresh | Click to refresh the page immediately. |

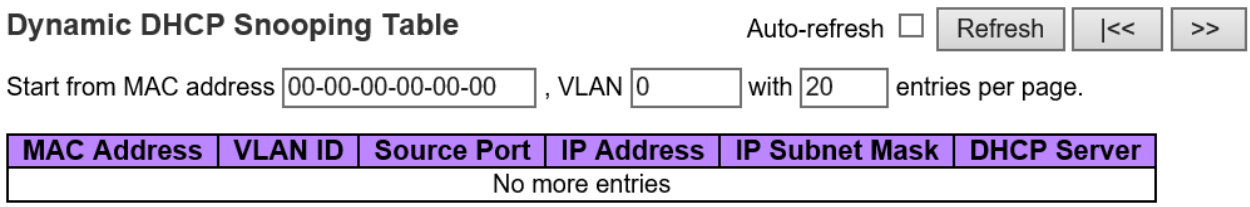
## 2.4.21 DHCP Snooping Table

Each page shows up to 99 entries from the Dynamic DHCP snooping 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 DHCP snooping Table.

The "MAC address" and "VLAN" input fields allows the user to select the starting point in the Dynamic DHCP snooping Table. Clicking the Refresh button will update the displayed table starting from that or the closest next Dynamic DHCP snooping Table match. In addition, the two input fields will - upon a Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The >> will use the last entry of the currently displayed table as a basis for the next lookup.

When the end is reached the text "No more entries" is shown in the displayed table. Use the |<< button to start over.



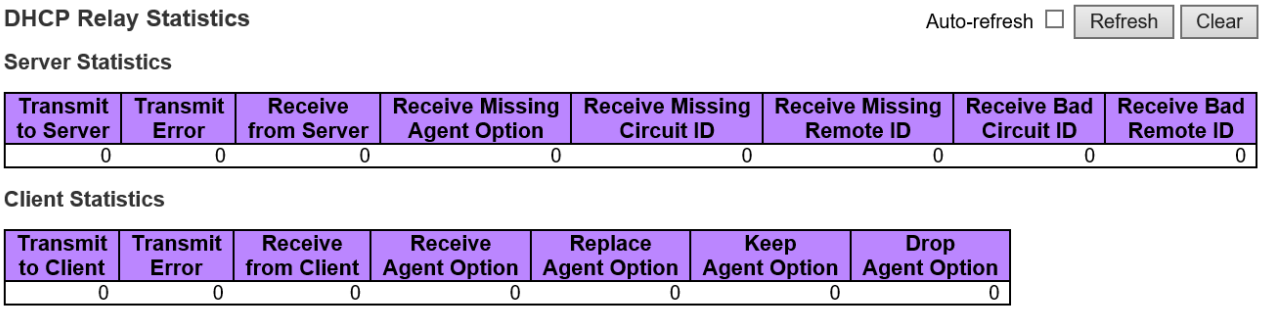

| Object | Description |
|---|---|
| **MAC Address** | User MAC address of the entry. |
| **VLAN ID** | VLAN-ID in which the DHCP traffic is permitted. |
| **Source Port** | Switch Port Number for which the entries are displayed. |
| **IP Address** | User IP address of the entry. |
| **IP Subnet Mask** | User IP subnet mask of the entry. |
| **DHCP Server Address** | DHCP Server address of the entry. |

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

| | |
|---|---|
| Refresh | Refreshes the displayed table starting from the input fields. |
| Clear | Flushes all dynamic entries. |
| \|<< | Updates the table starting from the first entry in the Dynamic DHCP snooping Table. |
| >> | Updates the table, starting with the entry after the last entry currently displayed. |

## 2.4.22 DHCP Relay Statistics

This page provides statistics for DHCP relay.



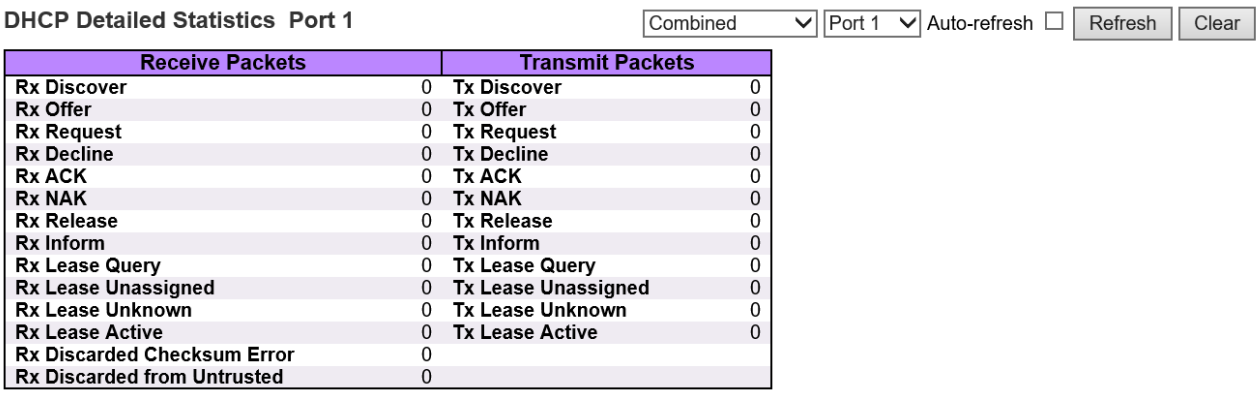

| Object | Description |
|---|---|
| Server Statistics | |
| **Transmit to Server** | The number of packets that are relayed from client to server. |
| **Transmit Error** | The number of packets that resulted in errors while being sent to clients. |
| **Receive from Server** | The number of packets received from server. |
| **Receive Missing Agent Option** | The number of packets received without agent information options. |
| **Receive Missing Circuit ID** | The number of packets received with the Circuit ID option missing. |
| **Receive Missing Remote ID** | The number of packets received with the Remote ID option missing. |
| **Receive Bad Circuit ID** | The number of packets whose Circuit ID option did not match known circuit ID. |
| **Receive Bad Remote ID** | The number of packets whose Remote ID option did not match known Remote ID. |

| Client Statistics | |
|---|---|
| **Transmit to Client** | The number of relayed packets from server to client. |
| **Transmit Error** | The number of packets that resulted in error while being sent to servers. |
| **Receive from Client** | The number of received packets from server. |
| **Receive Agent Option** | The number of received packets with relay agent information option. |
| **Replace Agent Option** | The number of packets which were replaced with relay agent information option. |
| **Keep Agent Option** | The number of packets whose relay agent information was retained. |
| **Drop Agent Option** | The number of packets that were dropped which were received with relay agent information. |

| Buttons | |
|---|---|
| Auto-refresh ☐ | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |
| Refresh | Click to refresh the page immediately. |
| Clear | Clear all statistics. |

## 2.4.23 DHCP Server - Detailed Statistics

This page provides statistics for DHCP snooping. Notice that the normal forward per-port TX statistics isn't increased if the incoming DHCP packet is done by L3 forwarding mechanism. And clear the statistics on specific port may not take effect on global statistics since it gathers the different layer overview.

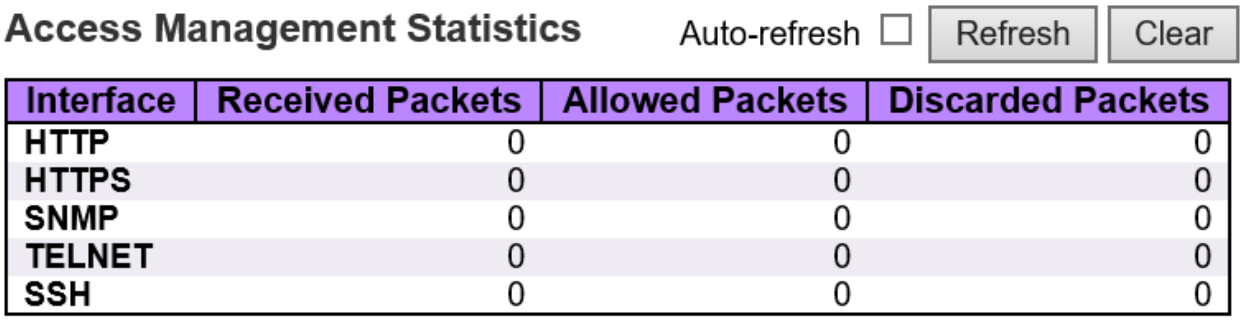


| Object | Description |
|---|---|
| **Rx and Tx Discover** | The number of discover (option 53 with value 1) packets received and transmitted. |
| **Rx and Tx Offer** | The number of offer (option 53 with value 2) packets received and transmitted. |
| **Rx and Tx Request** | The number of request (option 53 with value 3) packets received and transmitted. |
| **Rx and Tx Delcine** | The number of decline (option 53 with value 4) packets received and transmitted. |
| **Rx and Tx ACK** | The number of ACK (option 53 with value 5) packets received and transmitted. |
| **Rx and Tx NAK** | The number of NAK (option 53 with value 6) packets received and transmitted. |
| **Rx and Tx Release** | The number of release (option 53 with value 7) packets received and transmitted. |
| **Rx and Tx Inform** | The number of inform (option 53 with value 8) packets received and transmitted. |
| **Rx and Tx Lease Query** | The number of lease query (option 53 with value 10) packets received and transmitted. |
| **Rx and Tx Lease Unassigned** | The number of lease unassigned (option 53 with value 11) packets received and transmitted. |
| **Rx and Tx Unknown** | The number of lease unknown (option 53 with value 12) packets received and transmitted. |
| **Rx and Tx Active** | The number of lease active (option 53 with value 13) packets received and transmitted. |
| **Rx Discarded checksum error** | The number of discard packet that IP/UDP checksum is error. |
| **Rx Discarded from Untrusted** | The number of discarded packet that are coming from untrusted port. |

| Buttons | |
|---|---|
| Auto-refresh ☐ | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |
| Refresh | Refreshes the displayed table starting from the input fields. |
| Clear | Flushes all dynamic entries. |

## 2.4.24 Access Management Statistics

This page provides statistics for access management.



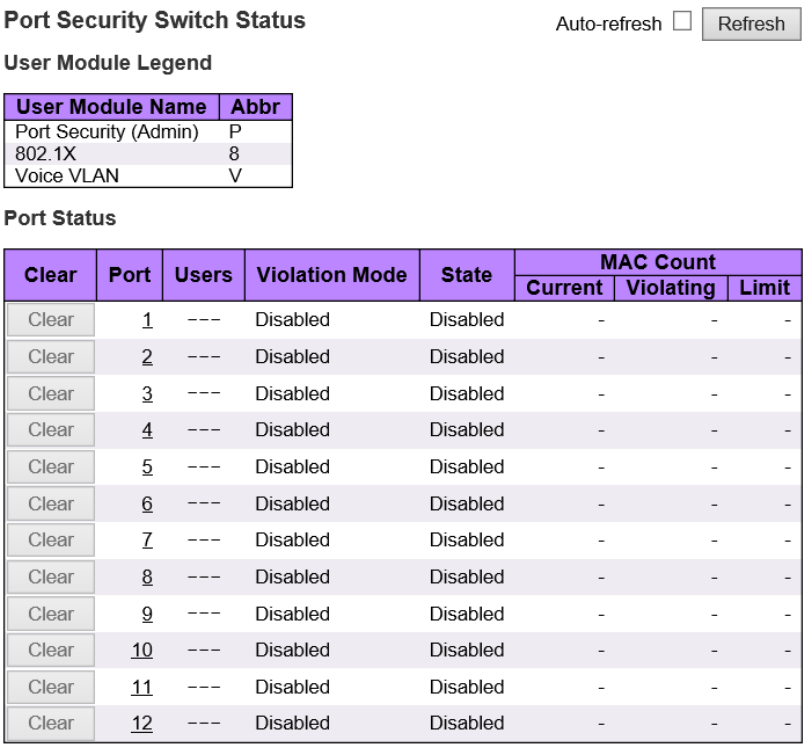

| Object | Description |
|---|---|
| **Interface** | The interface type through which the remote host can access the switch. |
| **Received Packets** | Number of received packets from the interface when access management mode is enabled. |
| **Allowed Packets** | Number of allowed packets from the interface when access management mode is enabled. |
| **Discarded Packets** | Number of discarded packets from the interface when access management mode is enabled. |

| Buttons | |
|---|---|
| Auto-refresh ☐ | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |
| Refresh | Click to refresh the page immediately. |
| Clear | Clear all statistics. |

## 2.4.25 Port Security - Switch Status

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

### 90W PoE Model




| Object | Description |
|---|---|
| **User Module Legend** | |
| **User Module Name** | The full name of a module that may request Port Security services. |
| **Abbr** | A one-letter abbreviation of the user module. This is used in the Users column in the port status table. |
| **Port Status** | |
| **Clear** | Click to remove all dynamic MAC addresses on all VLANs on this port. The button is only clickable if number of secured MAC addresses is non-zero. |

| | |
|---|---|
| **Port** | The port number for which the status applies. Click the port number to see the status for this particular port. |
| **Users** | Each of the user modules has a column that shows whether that module has enabled Port Security or not. A '-' means that the corresponding user module is not enabled, whereas a letter indicates that the user module abbreviated by that letter (see Abbr) has enabled port security. |
| **Violation Mode** | Shows the configured Violation Mode of the port. It can take one of four values:<br>Disabled: Port Security is not administratively enabled on this port.<br>Protect: Port Security is administratively enabled in Protect mode.<br>Restrict: Port Security is administratively enabled in Restrict mode.<br>Shutdown: Port Security is administratively enabled in Shutdown mode. |
| **State** | Shows the current state of the port. It can take one of four values:<br>`Disabled`: No user modules are currently using the Port Security service.<br>`Ready`: The Port Security service is in use by at least one user module, and is awaiting frames from unknown MAC addresses to arrive.<br>`Limit Reached`: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is reached and no more MAC addresses should be taken in.<br>`Shutdown`: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is exceeded. No MAC addresses can be learned on the port until it is administratively re-opened on the Limit Control configuration Web-page. |
| **MAC Count (Current, Limit)** | The two columns indicate the number of currently learned MAC addresses (forwarding as well as blocked) and the maximum number of MAC addresses that can be learned on the port, respectively.<br>If no user modules are enabled on the port, the Current column will show a dash (-).<br>If the Limit Control user module is not enabled on the port, the Limit column will show a dash (-). |

| **Buttons** | |
|---|---|
| Auto-refresh ☐ | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds |
| Refresh | Click to refresh the page immediately. |

30W PoE Model

**Port Security Switch Status** Auto-refresh ☐ Refresh

**User Module Legend**

| User Module Name | Abbr |
|---|---|
| Limit Control | L |
| 802.1X | 8 |
| Voice VLAN | V |

**Port Status**

| Port | Users | State | MAC Count | |
|---|---|---|---|---|
| | | | Current | Limit |
| 1 | --- | Disabled | - | - |
| 2 | --- | Disabled | - | - |
| 3 | --- | Disabled | - | - |
| 4 | --- | Disabled | - | - |
| 5 | --- | Disabled | - | - |
| 6 | --- | Disabled | - | - |
| 7 | --- | Disabled | - | - |
| 8 | --- | Disabled | - | - |

| Object | Description |
|---|---|
| **User Module Legend** | |
| **User Module Name** | The full name of a module that may request Port Security services. |
| **Abbr** | A one-letter abbreviation of the user module. This is used in the Users column in the port status table. |
| **Port Status** | |
| **Port** | The port number for which the status applies. Click the port number to see the status for this particular port. |
| **Users** | Each of the user modules has a column that shows whether that module has enabled Port Security or not. A '-' means that the corresponding user module is not enabled, whereas a letter indicates that the user module abbreviated by that letter (see Abbr) has enabled port security. |
| **State** | Shows the current state of the port. It can take one of four values:<br>`Disabled`: No user modules are currently using the Port Security service.<br>`Ready`: The Port Security service is in use by at least one user module, and is awaiting frames from unknown MAC addresses to arrive.<br>`Limit Reached`: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is reached and no more MAC addresses should be taken in.<br>`Shutdown`: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is exceeded. No MAC addresses can be learned on the port until it is administratively re-opened on the Limit Control configuration Web-page. |
| **MAC Count (Current,** | The two columns indicate the number of currently learned MAC addresses |

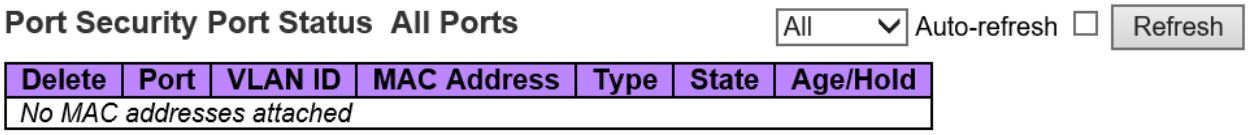
| | |
|---|---|
| **Limit)** | (forwarding as well as blocked) and the maximum number of MAC addresses that can be learned on the port, respectively.<br>If no user modules are enabled on the port, the Current column will show a dash (-).<br>If the Limit Control user module is not enabled on the port, the Limit column will show a dash (-). |

| **Buttons** | |
|---|---|
| Auto-refresh ☐ | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds |
| Refresh | Click to refresh the page immediately. |

## 2.4.26 Port Security – Port Status

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

90W PoE Model

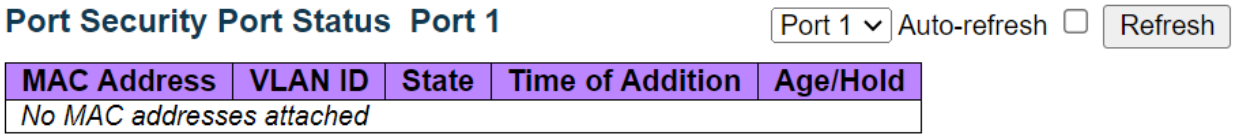



| Object | Description |
|---|---|
| **Delete** | Click to remove this particular MAC addresses from MAC address table. The button is only clickable if the entry type is Dynamic. Use the "Configuration→Security→Port Security→MAC Addresses" page to remove Static and Sticky entries. |
| **Port** | If all ports are shown (can be selected through the drop-down box on the top right), this one shows the port to which the MAC address is bound. |
| **VLAN ID & MAC Address** | The VLAN ID and MAC address that is seen on this port. If no MAC addresses are learned, a single row stating "No MAC addresses attached" is displayed. |
| **Type** | Indicates the type of entry. Takes one of three values:<br>• Dynamic: The entry is learned through learn frames coming to the Port Security module while the port in question is not in sticky mode.<br>• Static: The entry is entered by the end-user through management. Entry is not subject to aging.<br>• Sticky: When the port is in sticky mode, all entries that would otherwise have been learned as dynamic are learned as sticky.<br>Sticky entries are part of the running-config and can therefore be saved to startup-config. An important aspect of sticky MAC addresses is that they survive link changes (in contrast to Dynamic, which will have to be learned again). They also survive reboots if running-config is saved to startup-config. |
| **State** | Indicates whether the corresponding MAC address is violating (administrative user |

| | |
|---|---|
| | has configured the interface in "Restrict" mode and the MAC address is blocked), blocked, or forwarding. |
| **Age/Hold** | If at least one user module has decided to block this MAC address, it will stay in the blocked state until the hold time (measured in seconds) expires. If all user modules have decided to allow this MAC address to forward, and aging is enabled, the Port Security module will periodically check that this MAC address still forwards traffic. If the age period (measured in seconds) expires and no frames have been seen, the MAC address will be removed from the MAC address table. Otherwise a new age period will begin.<br>If aging is disabled or a user module has decided to hold the MAC address indefinitely, a dash (-) will be shown. |

| **Buttons** | |
|---|---|
| Auto-refresh ☐ | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |
| Refresh | Click to refresh the page immediately. |

30W PoE Model



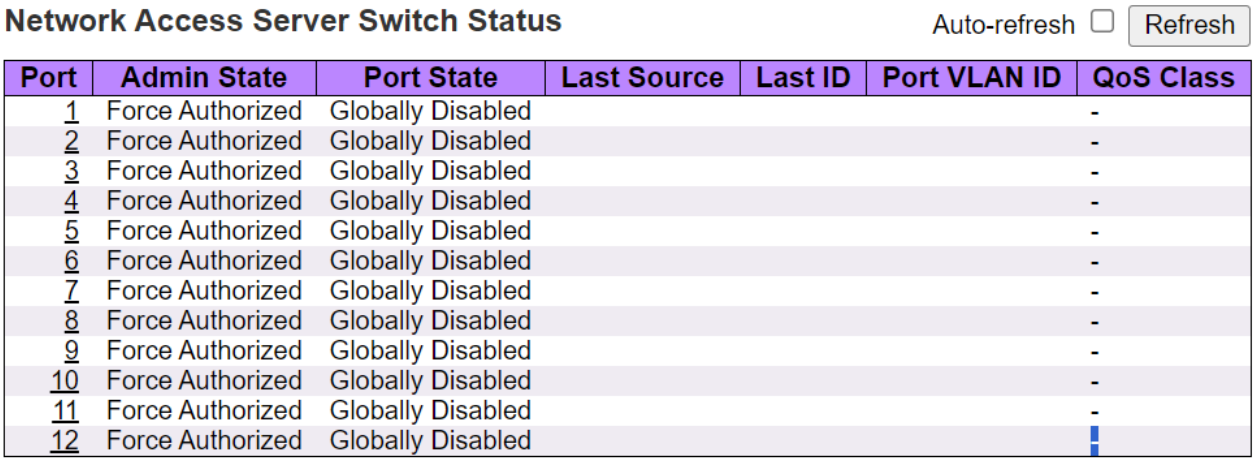

| Object | Description |
|---|---|
| **VLAN ID & MAC Address** | The VLAN ID and MAC address that is seen on this port. If no MAC addresses are learned, a single row stating "No MAC addresses attached" is displayed. |
| **State** | Indicates whether the corresponding MAC address is violating (administrative user has configured the interface in "Restrict" mode and the MAC address is blocked), blocked, or forwarding. |
| **Time of Addition** | Shows the date and time when this MAC address was first seen on the port. |
| **Age/Hold** | If at least one user module has decided to block this MAC address, it will stay in the blocked state until the hold time (measured in seconds) expires. If all user modules have decided to allow this MAC address to forward, and aging is enabled, the Port Security module will periodically check that this MAC address still forwards traffic. If the age period (measured in seconds) expires and no frames have been seen, the MAC address will be removed from the MAC address table. Otherwise a new age period will begin. |

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

| Buttons | |
|---|---|
| Auto-refresh ☐ | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |
| Refresh | Click to refresh the page immediately. |

## 2.4.27 NAS - Switch

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



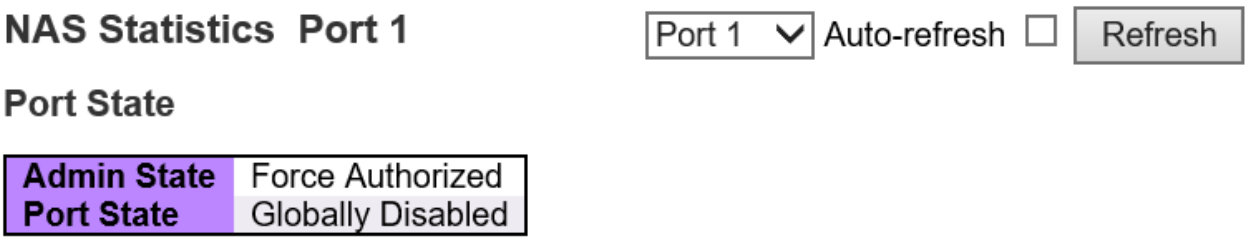

| Object | Description |
|---|---|
| **Port** | The switch port number. Click to navigate to detailed NAS statistics for this port. |
| **Admin State** | The port's current administrative state. Refer to NAS Admin State for a description of possible values. |
| **Port State** | The current state of the port. Refer to NAS Port State for a description of the individual states. |
| **Last Source** | The source MAC address carried in the most recently received EAPOL frame for EAPOL-based authentication, and the most recently received frame from a new client for MAC-based authentication. |
| **Last ID** | The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame for EAPOL-based authentication, and the source MAC address from the most recently received frame from a new client for MAC-based authentication. |
| **QoS Class** | QoS Class assigned to the port by the RADIUS server if enabled. |
| **Port VLAN ID** | The VLAN ID that NAS has put the port in. The field is blank, if the Port VLAN ID is not overridden by NAS.<br>If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID. Read more about RADIUS-assigned VLANs.<br>If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID. |

| Buttons | |
|---|---|
| Auto-refresh ☐ | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |
| Refresh | Click to refresh the page immediately. |

## 2.4.28 NAS - Port

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

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




| Object | Description |
|---|---|
| **Port State** | |
| **Admin State** | The port's current administrative state. Refer to NAS Admin State for a description of possible values. |
| **Port State** | The current state of the port. Refer to NAS Port State for a description of the individual states. |
| **QoS Class** | The QoS class assigned by the RADIUS server. The field is blank if no QoS class is assigned. |
| **Port VLAN ID** | The VLAN ID that NAS has put the port in. The field is blank, if the Port VLAN ID is not overridden by NAS.<br>If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID. Read more about RADIUS-assigned VLANs.<br>If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID. |

## Port Counters

**EAPOL Counters**

These supplicant frame counters are available for the following administrative states:

Force Authorized

Force Unauthorized

Port-based 802.1X

Single 802.1X

Multi 802.1X

| EAPOL Counters | | | |
|---|---|---|---|
| **Direction** | **Name** | **IEEE Name** | **Description** |
| Rx | **Total** | dot1xAuthEapolFramesRx | The number of valid EAPOL frames of any type that have been received by the switch. |
| Rx | **Response ID** | dot1xAuthEapolRespIdFramesRx | The number of valid EAPOL Response Identity frames that have been received by the switch. |
| Rx | **Responses** | dot1xAuthEapolRespFramesRx | The number of valid EAPOL response frames (other than Response Identity frames) that have been received by the switch. |
| Rx | **Start** | dot1xAuthEapolStartFramesRx | The number of EAPOL Start frames that have been received by the switch. |
| Rx | **Logoff** | dot1xAuthEapolLogoffFramesRx | The number of valid EAPOL Logoff frames that have been received by the switch. |
| Rx | **Invalid Type** | dot1xAuthInvalidEapolFramesRx | The number of EAPOL frames that have been received by the switch in which the frame type is not recognized. |
| Rx | **Invalid Length** | dot1xAuthEapLengthErrorFramesRx | The number of EAPOL frames that have been received by the switch in which the Packet Body Length field is invalid. |
| Tx | **Total** | dot1xAuthEapolFramesTx | The number of EAPOL frames of any type that have been transmitted by the switch. |
| Tx | **Request ID** | dot1xAuthEapolReqIdFramesTx | The number of EAPOL Request Identity frames that have been transmitted by the switch. |
| Tx | **Requests** | dot1xAuthEapolReqFramesTx | The number of valid EAPOL Request frames (other than Request Identity frames) that have been transmitted by the switch. |

**Backend Server Counters**

These backend (RADIUS) frame counters are available for the following administrative states:

Port-based 802.1X

Single 802.1X

Multi 802.1X

MAC-based Auth.

| Backend Server Counters | | | |
|---|---|---|---|
| **Direction** | **Name** | **IEEE Name** | **Description** |
| Rx | **Access Challenges** | dot1xAuthBackendAccessChallenges | **802.1X-based**:<br>Counts the number of times that the switch receives the first request from the backend server following the first response from the supplicant. Indicates that the backend server has communication with the switch.<br>**MAC-based**:<br>Counts all Access Challenges received from the backend server for this port (left-most table) or client (right-most table). |
| Rx | **Other Requests** | dot1xAuthBackendOtherRequestsToSupplicant | **802.1X-based**:<br>Counts the number of times that the switch sends an EAP Request packet following the first to the supplicant. Indicates that the backend server chose an EAP-method.<br>**MAC-based**:<br>Not applicable. |
| Rx | **Auth. Successes** | dot1xAuthBackendAuthSuccesses | **802.1X- and MAC-based**:<br>Counts the number of times that the switch receives a success indication. Indicates that the supplicant/client has successfully authenticated to the backend server. |
| Rx | **Auth. Failures** | dot1xAuthBackendAuthFails | **802.1X- and MAC-based**:<br>Counts the number of times that the switch receives a failure message. This indicates that the supplicant/client has not authenticated to the backend server. |
| Tx | **Responses** | dot1xAuthBackendResponses | **802.1X-based:**<br>Counts the number of times that the switch attempts to send a supplicant's first response packet to the backend server. Indicates the switch attempted communication with the backend server. Possible retransmissions are not counted.<br>**MAC-based:**<br>Counts all the backend server packets sent from the switch towards the backend server for a given port (left-most table) or client (right-most table). Possible retransmissions are not counted. |

**Last Supplicant/Client Info**

Information about the last supplicant/client that attempted to authenticate. This information is available for the following administrative states:

Port-based 802.1X

Single 802.1X

Multi 802.1X

MAC-based Auth.

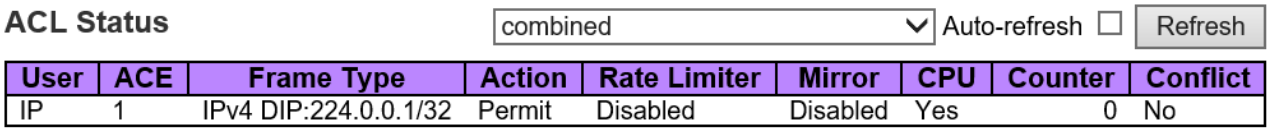
| Last Supplicant/Client Info | | |
|---|---|---|
| **Name** | **IEEE Name** | **Description** |
| **MAC Address** | dot1xAuthLastEapolFrameSource | The MAC address of the last supplicant/client. |
| **VLAN ID** | - | The VLAN ID on which the last frame from the last supplicant/client was received. |
| **Version** | dot1xAuthLastEapolFrameVersion | **802.1X-based**:<br>The protocol version number carried in the most recently received EAPOL frame.<br>**MAC-based**:<br>Not applicable. |
| **Identity** | - | **802.1X-based**:<br>The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame.<br>**MAC-based**:<br>Not applicable. |

| Selected Counters | |
|---|---|
| **Selected Counters** | The Selected Counters table is visible when the port is in one of the following administrative states:<br>• Multi 802.1X<br>• MAC-based Auth.<br>The table is identical to and is placed next to the Port Counters table, and will be empty if no MAC address is currently selected. To populate the table, select one of the attached MAC Addresses from the table below. |
| **Attached MAC Addresses** | |
| **Identity** | Shows the identity of the supplicant, as received in the Response Identity EAPOL frame.<br>Clicking the link causes the supplicant's EAPOL and Backend Server counters to be shown in the Selected Counters table. If no supplicants are attached, it shows *No supplicants attached*.<br>This column is not available for MAC-based Auth. |
| **MAC Address** | For Multi 802.1X, this column holds the MAC address of the attached supplicant.<br>For MAC-based Auth., this column holds the MAC address of the attached client.<br>Clicking the link causes the client's Backend Server counters to be shown in the Selected Counters table. If no clients are attached, it shows *No clients attached*. |
| **VLAN ID** | This column holds the VLAN ID that the corresponding client is currently secured through the Port Security module. |
| **State** | The client can either be authenticated or unauthenticated. In the authenticated state, it is allowed to forward frames on the port, and in the unauthenticated state, it is blocked. As long as the backend server hasn't successfully authenticated the client, it is unauthenticated. If an authentication fails for one or the other reason, the client will remain in the unauthenticated state for Hold Time seconds. |
| **Last Authentication** | Shows the date and time of the last authentication of the client (successful as well as unsuccessful). |

| Buttons | |
|---|---|
| Auto-refresh ☐ | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |
| Refresh | Click to refresh the page immediately |
| Clear | This button is available in the following modes:<br>• Force Authorized<br>• Force Unauthorized<br>• Port-based 802.1X<br>• Single 802.1X<br>Click to clear the counters for the selected port. |
| Clear All | This button is available in the following modes:<br>• Multi 802.1X<br>• MAC-based Auth.X<br>Click to clear both the port counters and all of the attached client's counters. The "Last Client" will not be cleared, however. |
| Clear This | This button is available in the following modes:<br>• Multi 802.1X<br>• MAC-based Auth.X<br>Click to clear only the currently selected client's counters. |

## 2.4.29 ACL Status

This page shows the ACL status by different ACL users. Each row describes the ACE that is defined. It is a conflict if a specific ACE is not applied to the hardware due to hardware limitations. The maximum number of ACEs is 512 on each switch.




| Object | Description |
|---|---|
| **User** | Indicates the ACL user. |
| **ACE** | Indicates the ACE ID on local switch. |
| **Frame Type** | Indicates the frame type of the ACE. Possible values are:<br>Any: The ACE will match any frame type.<br>EType: The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames.<br>ARP: The ACE will match ARP/RARP frames.<br>IPv4: The ACE will match all IPv4 frames.<br>IPv4/ICMP: The ACE will match IPv4 frames with ICMP protocol.<br>IPv4/UDP: The ACE will match IPv4 frames with UDP protocol.<br>IPv4/TCP: The ACE will match IPv4 frames with TCP protocol.<br>IPv4/Other: The ACE will match IPv4 frames, which are not ICMP/UDP/TCP.<br>IPv6: The ACE will match all IPv6 standard frames. |
| **Action** | Indicates the forwarding action of the ACE.<br>**Permit**: Frames matching the ACE may be forwarded and learned.<br>**Deny**: Frames matching the ACE are dropped.<br>**Filter**: Frames matching the ACE are filtered. |
| **Rate limiter** | Indicates the rate limiter number of the ACE. The allowed range is **1** to **16**. When **Disabled** is displayed, the rate limiter operation is disabled. |
| **CPU** | Forward packet that matched the specific ACE to CPU. |
| **Counter** | The counter indicates the number of times the ACE was hit by a frame. |
| **Conflict** | Indicates the hardware status of the specific ACE. The specific ACE is not applied to the hardware due to hardware limitations. |

| Buttons |
|---|

| | |
|---|---|
| Auto-refresh ☐ | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.. |
| Refresh | Click to refresh the page. |

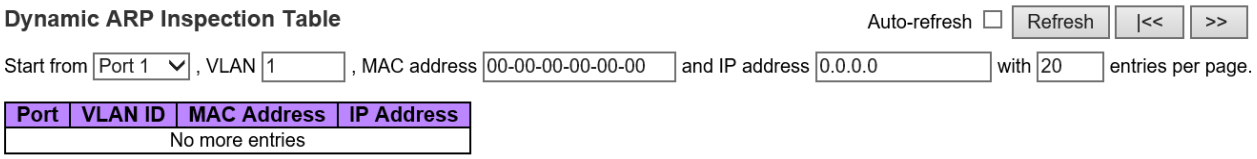
## 2.4.30 ARP Inspection

Each page shows up to 99 entries from the Dynamic ARP Inspection table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Dynamic ARP Inspection Table.

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

In addition, the two input fields will - upon a Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

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




| Object | 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. |

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

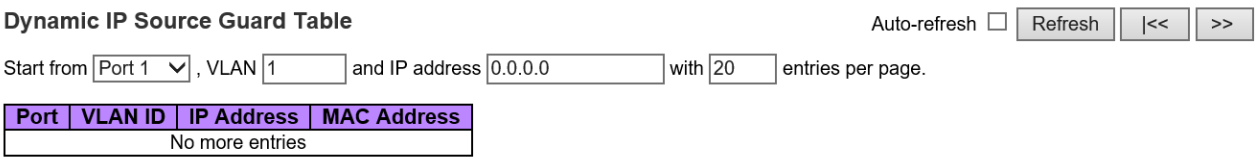
| | |
|---|---|
| Refresh | Refreshes the displayed table starting from the input fields. |
| Clear | Flushes all dynamic entries. |
| \|<< | Updates the table starting from the first entry in the Dynamic ARP Inspection Table. |
| >> | Updates the table, starting with the entry after the last entry currently displayed. |

## 2.4.31 IP Source Guard

Each page shows up to 99 entries from the Dynamic IP Source Guard table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Dynamic IP Source Guard Table.

The "Start from port address", "VLAN" and "IP address" input fields allow the user to select the starting point in the Dynamic IP Source Guard Table. Clicking the Refresh button will update the displayed table starting from that or the closest next Dynamic IP Source Guard Table match. In addition, the two input fields will - upon a Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

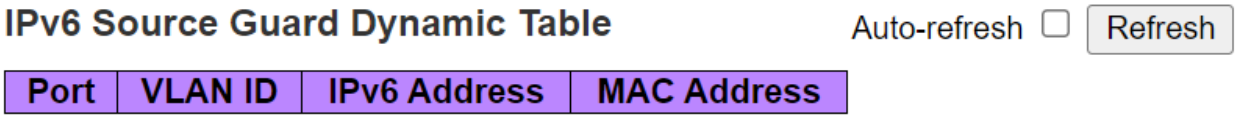
The >> will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the |<< button to start over.




| Object | Description |
|---|---|
| **Port** | Switch Port Number for which the entries are displayed. |
| **VLAN ID** | VLAN-ID in which the IP traffic is permitted. |
| **IP Address** | User IP address of the entry. |
| **MAC Address** | Source MAC address. |

| Buttons | |
|---|---|
| Auto-refresh ☐ | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |
| Refresh | Refresh the displayed table starting from the input fields. |
| Clear | Flush all dynamic entries. |
| \|<< | Update the table starting from the first entry in the Dynamic IP Source Guard Table. |
| >> | Updates the table, starting with the entry after the last entry currently displayed. |

## 2.4.32 IPv6 Source Guard (For 90W PoE Model)

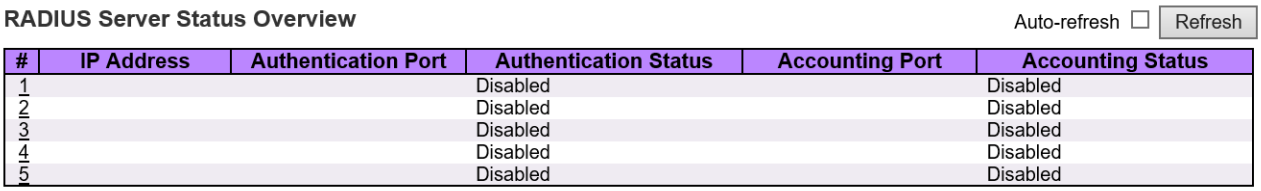



| Object | Description |
|---|---|
| **Port** | Switch Port Number to which the entries are bound. |
| **VLAN ID** | VLAN-ID in which the IP traffic is permitted. If no VLAN-ID is associated with the entry, this field shows 0. |
| **IP Address** | Source IPv6 address of the entry. |
| **MAC Address** | Source MAC address. |

| Buttons | |
|---|---|
| Auto-refresh ☐ | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |
| Refresh | Refreshes the display table. |

## 2.4.33 RADIUS Overview

This page provides an overview of the status of the RADIUS servers configurable on the Authentication configuration page.



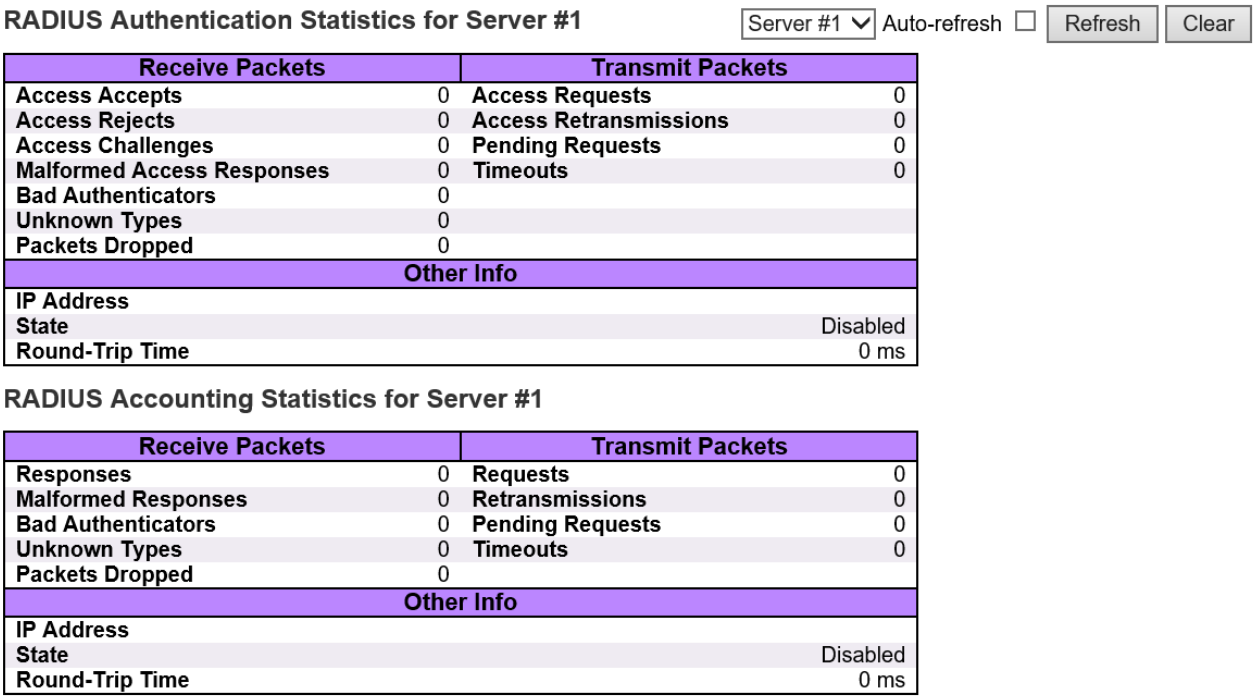

| Object | Description |
|---|---|
| **RADIUS Authentication Servers** | |
| **#** | The RADIUS server number. Click to navigate to detailed statistics for this server. |
| **IP Address** | The IP address of this server. |
| **Authentication Port** | UDP port number for authentication. |
| **Authentication Status** | The current status of the server. This field takes one of the following values:<br>**Disabled**: The server is disabled.<br>**Not Ready**: The server is enabled, but IP communication is not yet up and running.<br>**Ready**: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.<br>**Dead (X seconds left)**: Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled. |
| **Accounting Port** | UDP port number for accounting. |
| **Accounting Status** | The current status of the server. This field takes one of the following values:<br>**Disabled**: The server is disabled.<br>**Not Ready**: The server is enabled, but IP communication is not yet up and running.<br>**Ready**: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept accounting attempts.<br>**Dead (X seconds left)**: Accounting attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one |

| | |
|---|---|
| | server is enabled. |

| Buttons | |
|---|---|
| Auto-refresh ☐ | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |
| Refresh | Click to refresh the page immediately. |

## 2.4.34 RADIUS Details

This page provides detailed statistics for a particular RADIUS server.




| Object | Description |
|---|---|
| **RADIUS Authentication Statistics** | |
| **Packet Counters** | RADIUS authentication server packet counter. There are seven receive and four transmit counters. |

| Direction | Name | RFC4668 Name | Description |
|---|---|---|---|
| Rx | **Access Accepts** | radiusAuthClientExtAccessAccepts | The number of RADIUS Access-Accept packets (valid or invalid) received from the server. |
| Rx | **Access Rejects** | radiusAuthClientExtAccessRejects | The number of RADIUS Access-Reject packets (valid or invalid) received from the server. |
| Rx | **Access Challenges** | radiusAuthClientExtAccessChallenges | The number of RADIUS Access-Challenge packets (valid or invalid) received from the server. |
| Rx | **Malformed Access Responses** | radiusAuthClientExtMalformedAccessResponses | The number of malformed RADIUS Access-Response packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or Message Authenticator attributes or unknown types are not included as malformed access responses. |
| Rx | **Bad Authenticators** | radiusAuthClientExtBadAuthenticators | The number of RADIUS Access-Response packets containing invalid authenticators or Message Authenticator attributes received from the server. |
| Rx | **Unknown Types** | radiusAuthClientExtUnknownTypes | The number of RADIUS packets that were received with unknown types from the server on the authentication port and dropped. |
| Rx | **Packets Dropped** | radiusAuthClientExtPacketsDropped | The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason. |
| Tx | **Access Requests** | radiusAuthClientExtAccessRequests | The number of RADIUS Access-Request packets sent to the server. This does not include retransmissions. |
| Tx | **Access Retransmissions** | radiusAuthClientExtAccessRetransmissions | The number of RADIUS Access-Request packets retransmitted to the RADIUS authentication server. |
| Tx | **Pending Requests** | radiusAuthClientExtPendingRequests | The number of RADIUS Access-Request packets destined for the server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject, Access-Challenge, timeout, or retransmission. |
| Tx | **Timeouts** | radiusAuthClientExtTimeouts | The number of authentication timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout. |

| | |
|---|---|
| **Other Info** | This section contains information about the state of the server and the latest round-trip time. |

| Name | RFC4668 Name | Description |
|---|---|---|
| **IP Address** | - | IP address and UDP port for the authentication server in question. |
| **State** | - | Shows the state of the server. It takes one of the following values:<br>`Disabled` : The selected server is disabled.<br>`Not Ready` : The server is enabled, but IP communication is not yet up and running.<br>`Ready` : The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.<br>`Dead (X seconds left)` : Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled. |
| **Round-Trip Time** | radiusAuthClientExtRoundTripTime | The time interval (measured in milliseconds) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from the RADIUS authentication server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet. |

## RADIUS Accounting Statistics

| | |
|---|---|
| **Packet Counters** | RADIUS accounting server packet counter. There are five receive and four transmit counters. |

| Direction | Name | RFC4670 Name | Description |
|---|---|---|---|
| Rx | **Responses** | radiusAccClientExtResponses | The number of RADIUS packets (valid or invalid) received from the server. |
| Rx | **Malformed Responses** | radiusAccClientExtMalformedResponses | The number of malformed RADIUS packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or unknown types are not included as malformed access responses. |
| Rx | **Bad Authenticators** | radiusAcctClientExtBadAuthenticators | The number of RADIUS packets containing invalid authenticators received from the server. |
| Rx | **Unknown Types** | radiusAccClientExtUnknownTypes | The number of RADIUS packets of unknown types that were received from the server on the accounting port. |
| Rx | **Packets Dropped** | radiusAccClientExtPacketsDropped | The number of RADIUS packets that were received from the server on the accounting port and dropped for some other reason. |
| Tx | **Requests** | radiusAccClientExtRequests | The number of RADIUS packets sent to the server. This does not include retransmissions. |
| Tx | **Retransmissions** | radiusAccClientExtRetransmissions | The number of RADIUS packets retransmitted to the RADIUS accounting server. |
| Tx | **Pending Requests** | radiusAccClientExtPendingRequests | The number of RADIUS packets destined for the server that have not yet timed out or received a response. This variable is incremented when a Request is sent and decremented due to receipt of a Response, timeout, or retransmission. |
| Tx | **Timeouts** | radiusAccClientExtTimeouts | The number of accounting timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout. |

| | |
|---|---|
| **Other Info** | This section contains information about the state of the server and the latest round-trip time. |

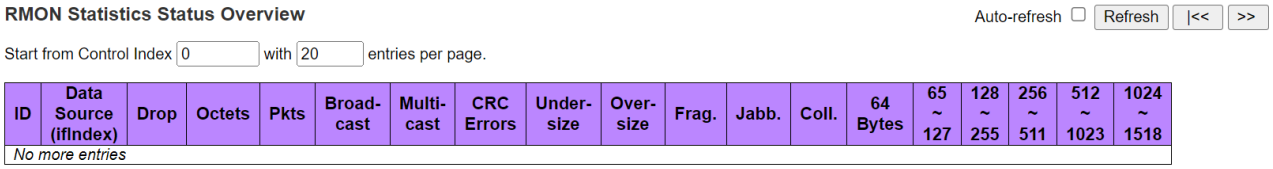
| Name | RFC4670 Name | Description |
|---|---|---|
| **IP Address** | - | IP address and UDP port for the accounting server in question. |
| **State** | - | Shows the state of the server. It takes one of the following values:<br>`Disabled` : The selected server is disabled.<br>`Not Ready` : The server is enabled, but IP communication is not yet up and running.<br>`Ready` : The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept accounting attempts.<br>`Dead (X seconds left)` : Accounting attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled. |
| **Round-Trip Time** | radiusAccClientExtRoundTripTime | The time interval (measured in milliseconds) between the most recent Response and the Request that matched it from the RADIUS accounting server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet. |

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

| | |
|---|---|
| Refresh | Click to refresh the page immediately. |
| Clear | Clears the counters for the selected server. The "Pending Requests" counter will not be cleared by this operation. |

## 2.4.35 RMON - Statistics

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



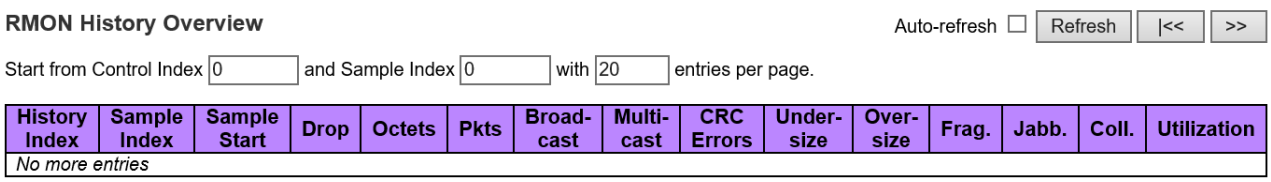

| Object | Description |
|---|---|
| **ID** | Indicates the index of Statistics entry. |
| **Data Source(ifIndex)** | The port ID which wants to be monitored. |
| **Drop** | The total number of events in which packets were dropped by the probe due to lack of resources. |
| **Octets** | The total number of octets of data (including those in bad packets) received on the network. |
| **Pkts** | The total number of packets (including bad packets, broadcast packets, and multicast packets) received. |
| **Broad-cast** | The total number of good packets received that were directed to the broadcast address. |
| **Multi-cast** | The total number of good packets received that were directed to a multicast address. |
| **CRC Errors** | The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). |
| **Under-Size** | The total number of packets received that were less than 64 octets. |
| **Over-size** | The total number of packets received that were longer than Max. Frame Size (default 10240). |
| **Frag.** | The number of frames which size is less than 64 octets received with invalid CRC. |
| **Jabb.** | The number of frames which size is longer than Max. Frame Size (default 10240) with invalid CRC.. |
| **Coll.** | The best estimate of the total number of collisions on this Ethernet segment. |
| **64** | The total number of packets (including bad packets) received that were 64 octets in |

| | |
|---|---|
| | length. |
| **65~127** | The total number of packets (including bad packets) received that were between 65 to 127 octets in length. |
| **128~255** | The total number of packets (including bad packets) received that were between 128 to 255 octets in length. |
| **256~511** | The total number of packets (including bad packets) received that were between 256 to 511 octets in length. |
| **512~1023** | The total number of packets (including bad packets) received that were between 512 to 1023 octets in length. |
| **1024~1518** | The total number of packets (including bad packets) received that were between 1024 to 1518 octets in length. |

| **Buttons** | |
|---|---|
| Auto-refresh ☐ | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |
| Refresh | Click to refresh the page immediately. |
| \|<< | Updates the table starting from the first entry in the Statistics table, i.e. the entry with the lowest ID. |
| >> | Updates the table, starting with the entry after the last entry currently displayed. |

## 2.4.36 RMON - History

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



| Object | Description |
|---|---|
| **History Index** | Indicates the index of History control entry. |
| **Sample Index** | Indicates the index of the data entry associated with the control entry. |
| **Sample Start** | The value of sysUpTime at the start of the interval over which this sample was measured. |
| **Drop** | The total number of events in which packets were dropped by the probe due to lack of resources. |
| **Octets** | The total number of octets of data (including those in bad packets) received on the network. |
| **Pkts** | The total number of packets (including bad packets, broadcast packets, and multicast packets) received. |
| **Broadcast** | The total number of good packets received that were directed to the broadcast address. |
| **Multicast** | The total number of good packets received that were directed to a multicast address. |
| **CRCErrors** | The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). |
| **Undersize** | The total number of packets received that were less than 64 octets. |
| **Oversize** | The total number of packets received that were longer than Max. Frame Size (default 10240). |
| **Frag.** | The number of frames which size is less than 64 octets received with invalid CRC. |
| **Jabb.** | The number of frames which longer than Max. Frame Size (default 10240) with invalid CRC. |
| **Coll.** | The best estimate of the total number of collisions on this Ethernet segment. |
| **Utilization** | The best estimate of the mean physical layer network utilization on this interface during this sampling interval, in hundredths of a percent. |

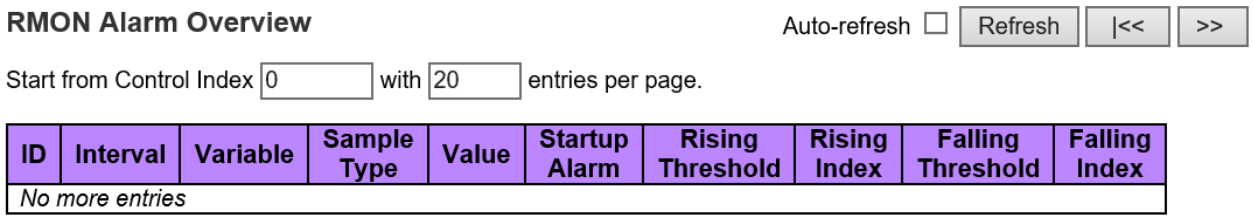
| Buttons | |
|---|---|
| Auto-refresh ☐ | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |
| Refresh | Click to refresh the page immediately. |
| \|<< | Updates the table starting from the first entry in the History table, i.e., the entry with the lowest History Index and Sample Index. |
| >> | Updates the table, starting with the entry after the last entry currently displayed. |

## 2.4.37 RMON - Alarm

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

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

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




| Object | Description |
|---|---|
| **ID** | Indicates the index of Alarm control entry. |
| **Interval** | Indicates the interval in seconds for sampling and comparing the rising and falling threshold. |
| **Variable** | Indicates the particular variable to be sampled. |
| **Sample Type** | The method of sampling the selected variable and calculating the value to be compared against the thresholds. |
| **Value** | The value of the statistic during the last sampling period. |
| **Startup Alarm** | The alarm that may be sent when this entry is first set to valid. |
| **Rising Threshold** | Rising threshold value. |
| **Rising Index** | Rising event index. |
| **Falling Threshold** | Falling threshold value. |
| **Falling Index** | Falling event index. |

| Buttons |
|---|

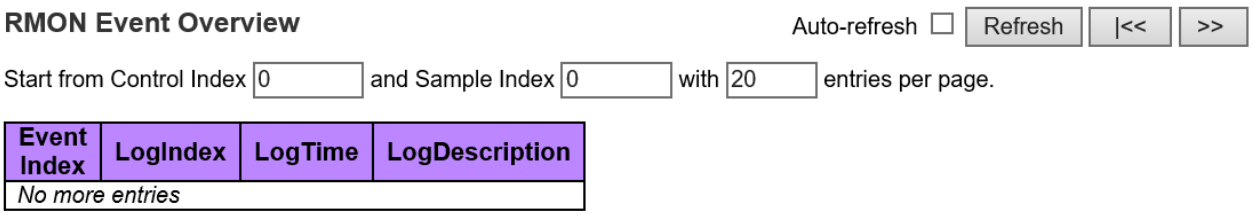
| | |
|---|---|
| Auto-refresh ☐ | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |
| Refresh | Click to refresh the page immediately. |
| \|<< | Updates the table starting from the first entry in the Alarm Table, i.e. the entry with the lowest ID. |
| >> | Updates the table, starting with the entry after the last entry currently displayed. |

## 2.4.38 RMON - Event

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

The "Start from Event Index and Log Index" allows the user to select the starting point in the Event table. Clicking the Refresh button will update the displayed table starting from that or the next closest Event table match.

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



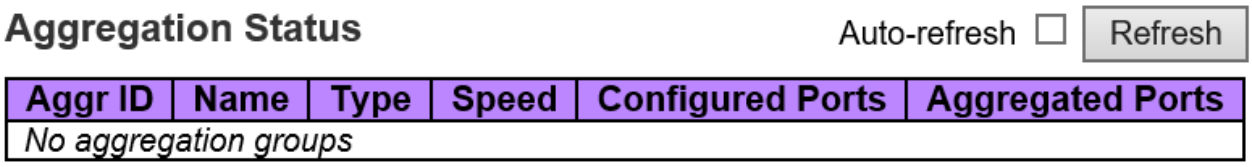

| Object | Description |
|---|---|
| **Event Index** | Indicates the index of the event entry. |
| **Log Index** | Indicates the index of the log entry. |
| **Log Time** | Indicates Event log time. |
| **LogDescription** | Indicates the Event description. |

| Buttons |
|---|

| | |
|---|---|
| Auto-refresh ☐ | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |
| Refresh | Click to refresh the page immediately. |
| \|<< | Updates the table starting from the first entry in the Event Table, i.e. the entry with the lowest Event Index and Log Index. |
| >> | Updates the table, starting with the entry after the last entry currently displayed. |

## 2.4.39 Aggregation Status

This page provides a status overview for all LACP instances.



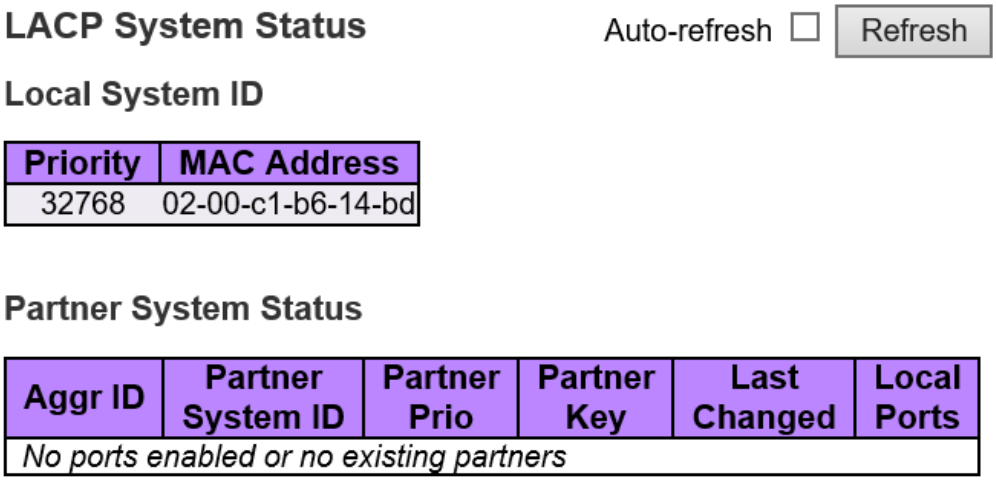

| Object | Description |
|---|---|
| **Aggr ID** | The Aggregation ID associated with this aggregation instance. |
| **Name** | Name of the Aggregation group ID. |
| **Type** | Type of the Aggregation group(Static or LACP). |
| **Speed** | Speed of the Aggregation group. |
| **Configured ports** | Configured member ports of the Aggregation group. |
| **Aggregated ports** | Aggregated member ports of the Aggregation group. |

| Buttons | |
|---|---|
| Refresh | Click to refresh the page immediately. |
| Auto-refresh ☐ | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |

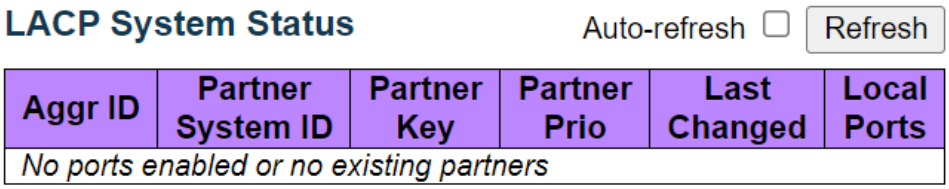
## 2.4.40 LACP - System Status

This page provides a status overview for the system-level LACP information.

90W PoE Model




30W PoE Model



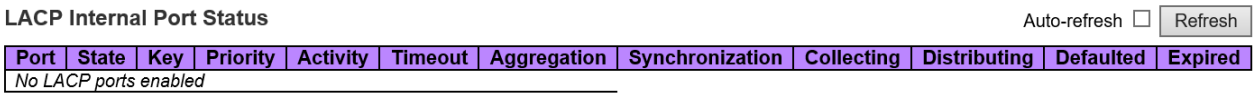

| Object | Description |
|---|---|
| **Aggr ID** | The Aggregation ID associated with this aggregation instance. |
| **Partner System ID** | The system ID (MAC address) of the aggregation partner. |
| **Partner Prio** | The priority that the partner has assigned to this aggregation ID. |
| **Partner Key** | The Key that the partner has assigned to this aggregation ID. |
| **Last Changed** | The time since this aggregation changed. |
| **Local Ports** | Shows which ports are a part of this aggregation for this switch |

| Buttons | |
|---|---|
| Refresh | Click to refresh the page immediately. |

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

## 2.4.41 LACP – Internal Port Status (For 90W PoE Model)

This page provides a status overview for the LACP internal (i.e. local system) status for all ports.




| Object | Description |
|---|---|
| **Port** | The switch port number. |
| **State** | The current port state:<br>• Down: The port is not active.<br>• Active: The port is in active state.<br>• Standby: The port is in standby state. |
| **Key** | The key assigned to this port. Only ports with the same key can aggregate together. |
| **Priority** | The priority assigned to this aggregation group. |
| **Activity** | The LACP mode of the group (Active or Passive). |
| **Timeout** | The timeout mode configured for the port (Fast or Slow). |
| **Aggregation** | Show whether the system considers this link to be "aggregateable"; i.e., a potential candidate for aggregation. |
| **Synchronization** | Show whether the system considers this link to be "IN_SYNC"; i.e., it has been allocated to the correct LAG, the group has been associated with a compatible Aggregator, and the identity of the LAG is consistent with the System ID and operational Key information transmitted. |
| **Collecting** | Show if collection of incoming frames on this link is enabled. |
| **Distributing** | Show if distribution of outgoing frames on this link is enabled. |
| **Defaulted** | Show if the Actor's Receive machine is using Defaulted operational Partner information. |
| **Expired** | Show if that the Actor's Receive machine is in the EXPIRED state. |

| Buttons | |
|---|---|
| Refresh | Click to refresh the page immediately. |

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

## 2.4.42 L ACP – Port Status (For 30W PoE Model)

This page provides a status overview for the LACP internal (i.e. local system) status for all ports.

**LACP Status** Auto-refresh ☐ Refresh

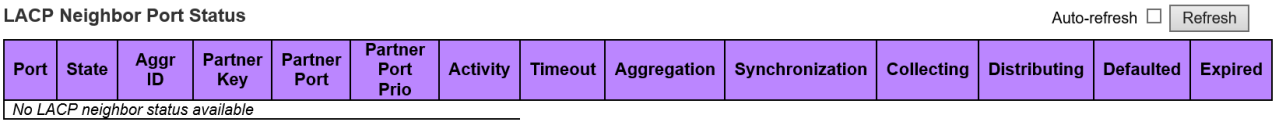
| Port | LACP | Key | Aggr ID | Partner System ID | Partner Port | Partner Prio |
|---|---|---|---|---|---|---|
| 1 | No | - | - | - | - | - |
| 2 | No | - | - | - | - | - |
| 3 | No | - | - | - | - | - |
| 4 | No | - | - | - | - | - |
| 5 | No | - | - | - | - | - |
| 6 | No | - | - | - | - | - |
| 7 | No | - | - | - | - | - |
| 8 | No | - | - | - | - | - |

| Object | Description |
|---|---|
| **Port** | The switch port number. |
| **LACP** | 'Yes' means that LACP is enabled and the port link is up. 'No' means that LACP is not enabled or that the port link is down. 'Backup' means that the port could not join the aggregation group but will join if other port leaves. Meanwhile it's LACP status is disabled. |
| **Key** | The key assigned to this port. Only ports with the same key can aggregate together. |
| **Aggr ID** | The Aggregation ID assigned to this aggregation group. |
| **Partner System ID** | The partner's System ID (MAC address). |
| **Partner Port** | The partner's port number connected to this port. |
| **Partner Prio** | The partner's port priority. |

| Buttons | |
|---|---|
| Refresh | Click to refresh the page immediately. |
| Auto-refresh ☐ | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |

## 2.4.43 LACP - Neighbor Status (For 90W PoE Model)

This page provides a status overview for the LACP neighbor status for all ports.

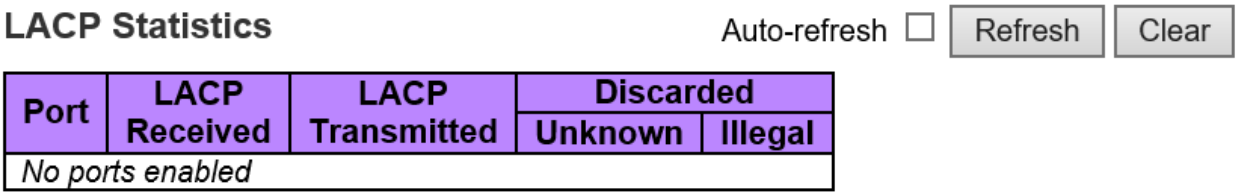



| Object | Description |
|---|---|
| **Port** | The switch port number. |
| **State** | The current port state:<br>• Down: The port is not active.<br>• Active: The port is in active state.<br>• Standby: The port is in standby state. |
| **Aggr ID** | The aggregation group ID which the port is assigned to. |
| **Partner Key** | The key assigned to this port by the partner. |
| **Partner Port** | The partner port number associated with this link. |
| **Partner Port Priority** | The priority assigned to this partner port . |
| **Activity** | The LACP mode of the group (Active or Passive). |
| **Timeout** | The timeout mode configured for the port (Fast or Slow). |
| **Aggregation** | Show whether the system considers this link to be "aggregateable"; i.e., a potential candidate for aggregation. |
| **Synchronization** | Show whether the system considers this link to be "IN_SYNC"; i.e., it has been allocated to the correct LAG, the group has been associated with a compatible Aggregator, and the identity of the LAG is consistent with the System ID and operational Key information transmitted. |
| **Collecting** | Show if collection of incoming frames on this link is enabled. |
| **Distributing** | Show if distribution of outgoing frames on this link is enabled. |
| **Defaulted** | Show if the Actor's Receive machine is using Defaulted operational Partner information. |
| **Expired** | Show if that the Actor's Receive machine is in the EXPIRED state. |

| Buttons | |
|---|---|
| Refresh | Click to refresh the page immediately. |
| Auto-refresh ☐ | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |

## 2.4.44 LACP- Port Statistics

This page provides an overview for LACP statistics for all ports.

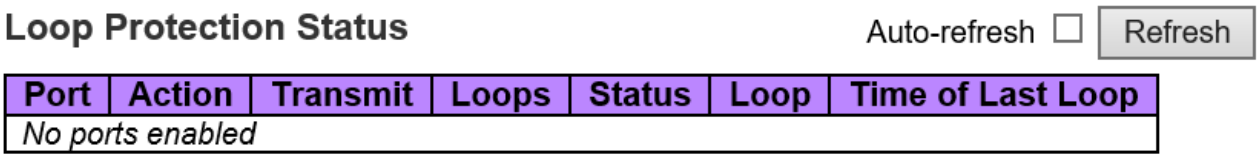



| Object | Description |
|---|---|
| **Port** | The switch port number. |
| **LACP Received** | Shows how many LACP frames have been received at each port. |
| **LACP Transmitted** | Shows how many LACP frames have been sent from each port. |
| **Discarded** | Shows how many unknown or illegal LACP frames have been discarded at each port. |

| Buttons | |
|---|---|
| Auto-refresh ☐ | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |
| Refresh | Click to refresh the page immediately. |
| Clear | Clears the counters for all ports. |

## 2.4.45 Loop Protection

This page displays the loop protection port status the ports of the switch.




| Object | Description |
|---|---|
| **Port** | The switch port number of the logical port. |
| **Action** | The currently configured port action. |
| **Transmit** | The currently configured port transmit mode. |
| **Loops** | The number of loops detected on this port. |
| **Status** | The current loop protection status of the port. |
| **Loop** | Whether a loop is currently detected on the port. |
| **Time of Last Loop** | The time of the last loop event detected. |

| Buttons | |
|---|---|
| Refresh | Click to refresh the page immediately. |
| Auto-refresh ☐ | Check this box to enable an automatic refresh of the page at regular intervals. |

## 2.4.46 Spanning Tree - Bridge Status

This page provides a status overview of all STP bridge instances.

**STP Bridges** Auto-refresh ☐ Refresh

| MSTI | Bridge ID | Root | | | Topology Flag | Topology Change Last |
|---|---|---|---|---|---|---|
| | | ID | Port | Cost | | |
| CIST | 32768.02-00-C1-B6-14-BD | 32768.02-00-C1-B6-14-BD | - | 0 | Steady | - |

**STP Detailed Bridge Status** Auto-refresh ☐ Refresh

| STP Bridge Status | |
|---|---|
| **Bridge Instance** | CIST |
| **Bridge ID** | 32768.02-00-C1-B6-14-BD |
| **Root ID** | 32768.02-00-C1-B6-14-BD |
| **Root Cost** | 0 |
| **Root Port** | - |
| **Regional Root** | 32768.02-00-C1-B6-14-BD |
| **Internal Root Cost** | 0 |
| **Topology Flag** | Steady |
| **Topology Change Count** | 0 |
| **Topology Change Last** | - |

**CIST Ports & Aggregations State**

| Port | Port ID | Role | State | Path Cost | Edge | Point-to-Point | Uptime |
|---|---|---|---|---|---|---|---|
| 2 | 128:002 | DesignatedPort | Forwarding | 200000 | Yes | Yes | 0d 00:20:52 |

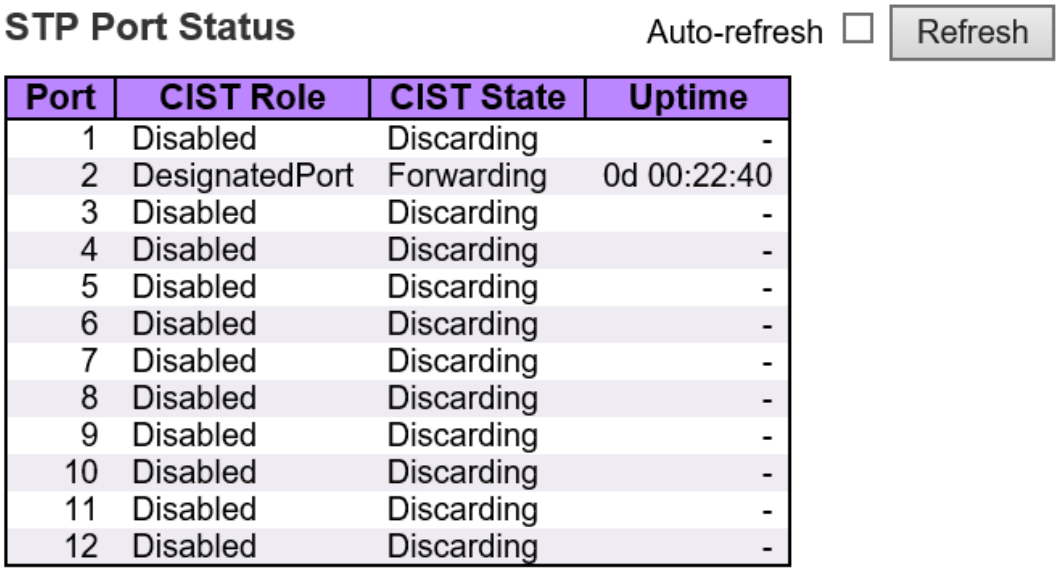
| Object | Description |
|---|---|
| **STP Bridges** | |
| **MSTI** | The Bridge Instance. |
| **Bridge ID** | The Bridge ID of this Bridge instance. |
| **Root ID** | The Bridge ID of the currently elected root bridge. |
| **Root Port** | The switch port currently assigned the *root* port role. |
| **Root Cost** | Root Path Cost. For the Root Bridge it is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge. |
| **Topology Flag** | The current state of the Topology Change Flag of this Bridge instance. |
| **Topology Change Last** | The time since last Topology Change occurred. |
| **STP Detailed Bridge Status** | |
| **Bridge Instance** | The Bridge instance - `CIST`, `MST1`, ... |
| **Bridge ID** | The Bridge ID of this Bridge instance. |
| **Root ID** | The Bridge ID of the currently elected root bridge. |

| | |
|---|---|
| **Root Port** | The switch port currently assigned the root port role. |
| **Root Cost** | Root Path Cost. For the Root Bridge this is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge. |
| **Regional Root** | The Bridge ID of the currently elected regional root bridge, inside the MSTP region of this bridge. (For the CIST instance only). |
| **Internal Root Cost** | The Regional Root Path Cost. For the Regional Root Bridge this is zero. For all other CIST instances in the same MSTP region, it is the sum of the Internal Port Path Costs on the least cost path to the Internal Root Bridge. (For the CIST instance only). |
| **Topology Flag** | The current state of the Topology Change Flag of this Bridge instance. |
| **Topology Change Count** | The number of times where the topology change flag has been set (during a one-second interval). |
| **Topology Change Last** | The time passed since the Topology Flag was last set. |
| **CIST Ports & Aggregations State** | |
| **Port** | The switch port number of the logical STP port. |
| **Port ID** | The port id as used by the STP protocol. This is the priority part and the logical port index of the bridge port. |
| **Role** | The current STP port role. The port role can be one of the following values: `AlternatePort` `BackupPort` `RootPort` `DesignatedPort`. |
| **State** | The current STP port state. The port state can be one of the following values: `Discarding` `Learning` `Forwarding`. |
| **Path Cost** | The current STP port path cost. This will either be a value computed from the Auto setting, or any explicitly configured value. |
| **Edge** | The current STP port (operational) Edge Flag. An Edge Port is a switch port to which no Bridges are attached. The flag may be automatically computed or explicitly configured. Each Edge Port transits directly to the Forwarding Port State, since there is no possibility of it participating in a loop. |
| **Point-to-Point** | The current STP port point-to-point flag. A point-to-point port connects to a non-shared LAN media. The flag may be automatically computed or explicitly configured. The point-to-point properties of a port affect how fast it can transit to STP state. |
| **Uptime** | The time since the bridge port was last initialized. |

| **Buttons** | |
|---|---|
| Refresh | Click to refresh the page immediately. |
| Auto-refresh ☐ | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |

## 2.4.47 Spanning Tree - Port Status

This page displays the STP CIST port status for physical ports of the switch.

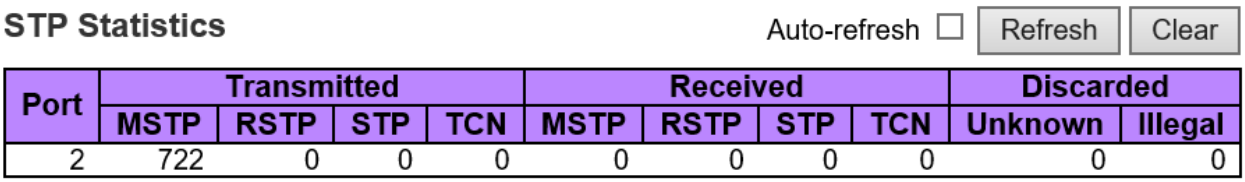



| Object | Description |
|---|---|
| **Port** | The switch port number of the logical STP port. |
| **CIST Role** | The current STP port role of the CIST port. The port role can be one of the following values: `AlternatePort` `BackupPort` `RootPort` `DesignatedPort` `Disabled`. |
| **CIST State** | The current STP port state of the CIST port. The port state can be one of the following values: `Discarding` `Learning` `Forwarding`. |
| **Uptime** | The time since the bridge port was last initialized. |

| Buttons | |
|---|---|
| Refresh | Click to refresh the page immediately. |
| Auto-refresh ☐ | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |

## 2.4.48 Spanning Tree - Port Statistics

This page displays the STP port statistics counters of bridge ports in the switch.

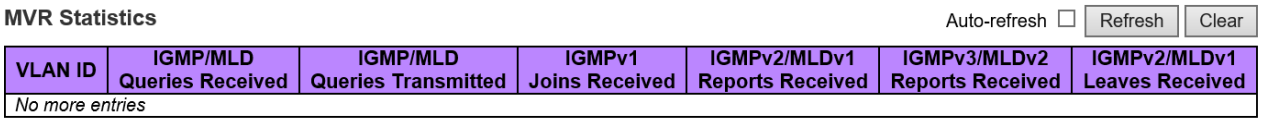



| Object | Description |
|---|---|
| **Port** | The switch port number of the logical STP port. |
| **MSTP** | The number of MSTP BPDU's received/transmitted on the port. |
| **RSTP** | The number of RSTP BPDU's received/transmitted on the port. |
| **STP** | The number of legacy STP Configuration BPDU's received/transmitted on the port. |
| **TCN** | The number of (legacy) Topology Change Notification BPDU's received/transmitted on the port. |
| **Discarded Unknown** | The number of unknown Spanning Tree BPDU's received (and discarded) on the port. |
| **Discarded Illegal** | The number of illegal Spanning Tree BPDU's received (and discarded) on the port. |

| Buttons | |
|---|---|
| Refresh | Click to refresh the page immediately. |
| Clear | Click to reset the counters. |
| Auto-refresh ☐ | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |

## 2.4.49 MVR - Statistics

This page provides MVR Statistics information.




| Object | Description |
|---|---|
| **VLAN ID** | The Multicast VLAN ID. |
| **IGMP/MLD Queries Received** | The number of Received Queries for IGMP and MLD, respectively. |
| **IGMP/MLD Queries Transmitted** | The number of Transmitted Queries for IGMP and MLD, respectively. |
| **IGMPv1 Joins Received** | The number of Received IGMPv1 Join's. |
| **IGMPv2/MLDv1 Report's Received** | The number of Received IGMPv2 Join's and MLDv1 Report's, respectively. |
| **IGMPv3/MLDv2 Report's Received** | The number of Received IGMPv1 Join's and MLDv2 Report's, respectively. |
| **IGMPv2/MLDv1 Leave's Received** | The number of Received IGMPv2 Leave's and MLDv1 Done's, respectively. |

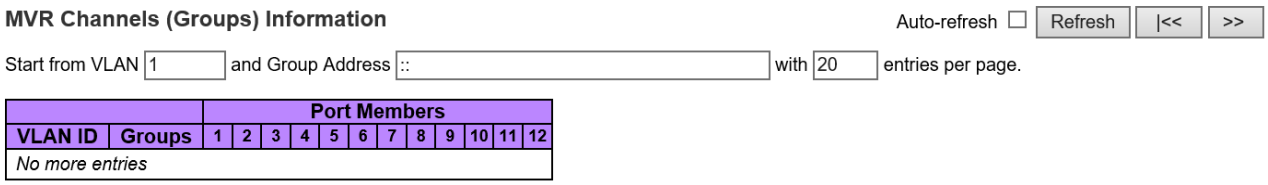
| Buttons | |
|---|---|
| Auto-refresh ☐ | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |
| Refresh | Click to refresh the page immediately. |
| Clear | Clears all Statistics counters. |

## 2.4.50 MVR Channel Groups

Each page shows up to 99 entries from the MVR Group table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MVR Channels (Groups) Information Table.

The "Start from VLAN", and "Group Address" input fields allow the user to select the starting point in the MVR Channels (Groups) Information Table. Clicking the Refresh button will update the displayed table starting from that or the closest next MVR Channels (Groups) Information Table match. In addition, the two input fields will - upon a Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

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




| Object | Description |
|---|---|
| **VLAN ID** | VLAN ID of the group. |
| **Groups** | Group ID of the group displayed. |
| **Port Members** | Ports under this group. |

| Buttons | |
|---|---|
| Auto-refresh ☐ | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |
| Refresh | Refreshes the displayed table starting from the input fields. |
| \|<< | Updates the table starting from the first entry in the MVR Channels (Groups) Information Table. |

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

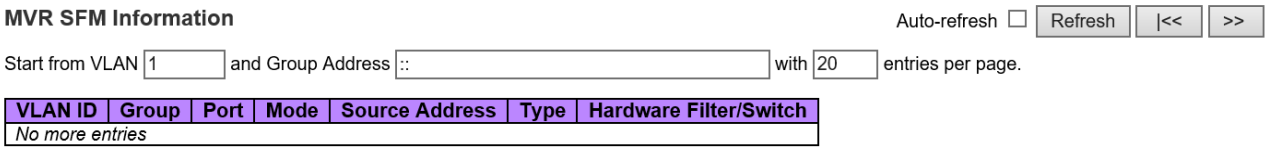
## 2.4.51 MVR SFM Information

Each page shows up to 99 entries from the MVR SFM Information Table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MVR SFM Information Table.

The "Start from VLAN", and "Group Address" input fields allow the user to select the starting point in the MVR SFM Information Table. Clicking the Refresh button will update the displayed table starting from that or the closest next MVR SFM Information Table match. In addition, the two input fields will - upon a Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The >> will use the last entry of the currently displayed table as a basis for the next lookup.

When the end is reached the text "No more entries" is shown in the displayed table. Use the |<< button to start over.



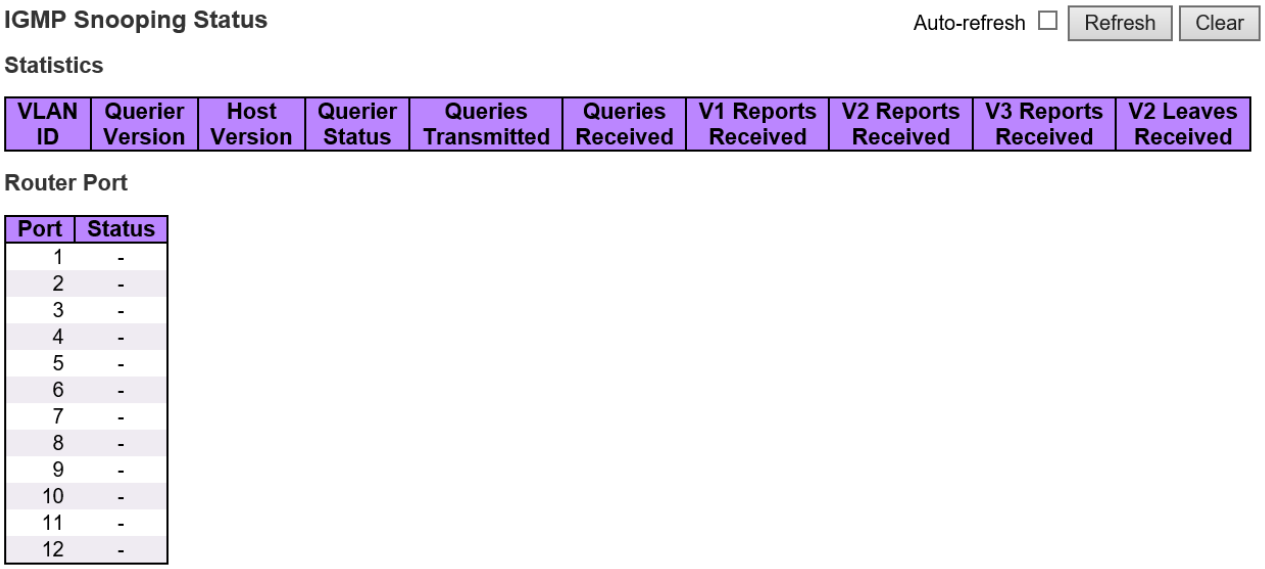

| Object | Description |
|---|---|
| **VLAN ID** | VLAN ID of the group. |
| **Group** | Group address of the group displayed. |
| **Port** | Switch port number. |
| **Mode** | Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude. |
| **Source Address** | IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128. When there is no any source filtering address, the text "None" is shown in the Source Address field. |

| | |
|---|---|
| **Type** | Indicates the Type. It can be either Allow or Deny. |
| **Hardware Filter/Switch** | Indicates whether data plane destined to the specific group address from the source IPv4/IPv6 address could be handled by chip or not. |

| **Buttons** | |
|---|---|
| Auto-refresh ☐ | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |
| Refresh | Refreshes the displayed table starting from the input fields. |
| \|<< | Updates the table starting from the first entry in the MVR SFM Information Table. |
| >> | Updates the table, starting with the entry after the last entry currently displayed. |

## 2.4.52 IGMP Snooping Status

This page provides IGMP Snooping status.




| Object | Description |
|---|---|
| **VLAN ID** | The VLAN ID of the entry. |
| **Querier Version** | Working Querier Version currently. |
| **Host Version** | Working Host Version currently. |
| **Querier Status** | Shows the Querier status is "ACTIVE" or "IDLE".<br>"DISABLE" denotes the specific interface is administratively disabled. |
| **Querier Transmitted** | The number of Transmitted Queries. |
| **Queries Received** | The number of Received Queries. |
| **V1 Report Received** | The number of Received V1 Reports. |
| **V2 Report Received** | The number of Received V2 Reports. |
| **V3 Report Received** | The number of Received V3 Reports. |
| **V2 Leaves Received** | The number of Received V2 Leaves. |
| **Router Port** | Display which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier.<br>Static denotes the specific port is configured to be a router port.<br>Dynamic denotes the specific port is learnt to be a router port.<br>Both denote the specific port is configured or learnt to be a router port. |
| **Port** | Switch port number. |

| | |
|---|---|
| **Status** | Indicate whether specific port is a router port or not. |

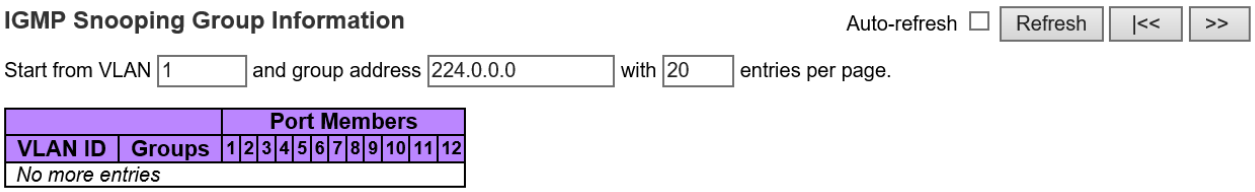
| Buttons | |
|---|---|
| Auto-refresh ☐ | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |
| Refresh | Click to refresh the page immediately. |
| Clear | Clears all Statistics counters. |

## 2.4.53 IGMP Snooping - Groups Information

Each page shows up to 99 entries from the IGMP Group table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the IGMP Group Table.

The "Start from VLAN", and "group" input fields allow the user to select the starting point in the IGMP Group Table. Clicking the Refresh button will update the displayed table starting from that or the closest next IGMP Group Table match. In addition, the two input fields will - upon a Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

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




| Object | Description |
|---|---|
| **VLAN ID** | VLAN ID of the group. |

| | |
|---|---|
| **Groups** | Group address of the group displayed. |
| **Port Members** | Ports under this group. |

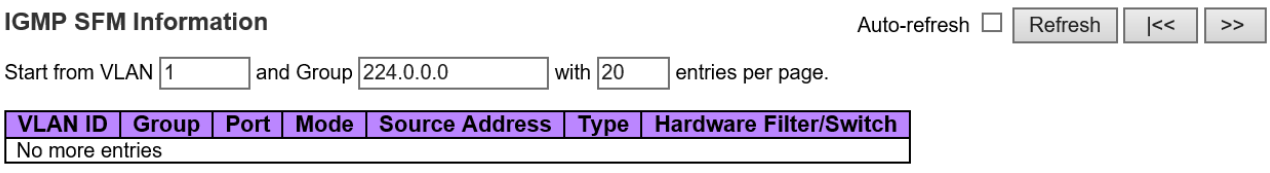
| Buttons | |
|---|---|
| Auto-refresh ☐ | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |
| Refresh | Refreshes the displayed table starting from the input fields. |
| \|<< | Updates the table, starting with the first entry in the IGMP Group Table. |
| >> | Updates the table, starting with the entry after the last entry currently displayed. |

## 2.4.54 IPv4 SFM Information

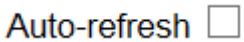
Each page shows up to 99 entries from the IGMP SFM Information table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the IGMP SFM Information Table.

The "Start from VLAN", and "group" input fields allow the user to select the starting point in the IGMP SFM Information Table. Clicking the Refresh button will update the displayed table starting from that or the closest next IGMP SFM Information Table match. In addition, the two input fields will - upon a Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

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

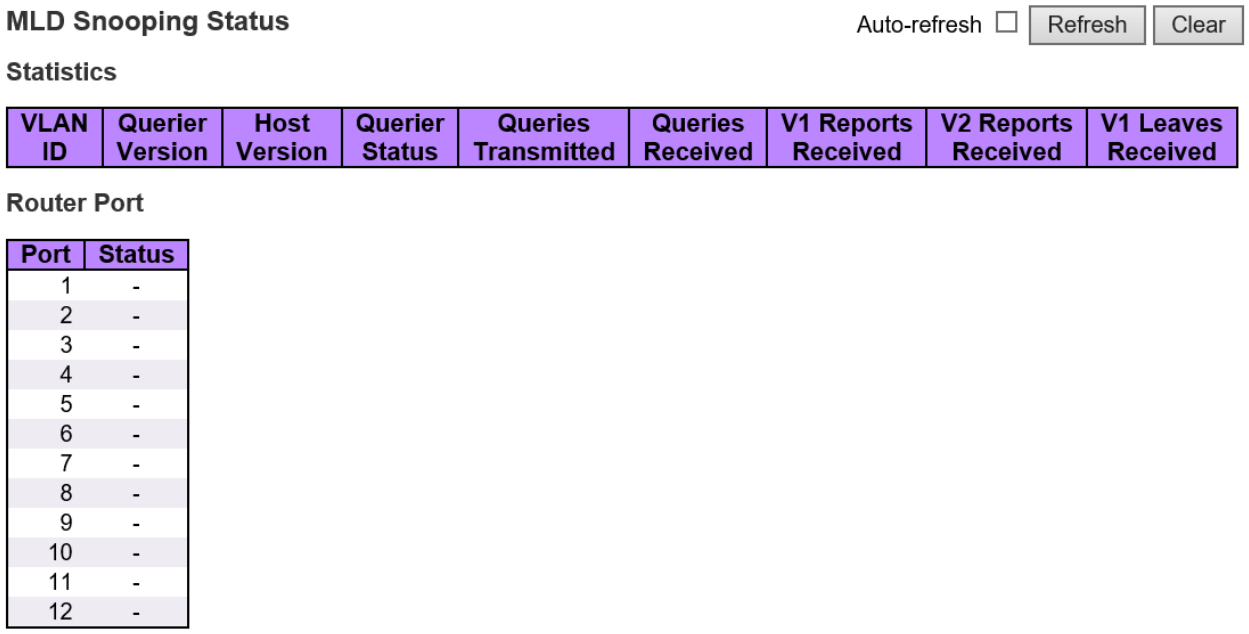


| Object | Description |
|---|---|
| **VLAN ID** | VLAN ID of the group. |
| **Group** | Group address of the group displayed. |
| **Port** | Switch port number. |
| **Mode** | Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude. |
| **Source Address** | IP Address of the source.<br>Currently, the maximum number of IPv4 source address for filtering (per group) is 8.<br>When there is no any source filtering address, the text "None" is shown in the Source Address field. |
| **Type** | Indicates the Type. It can be either Allow or Deny. |
| **Hardware Filter/Switch** | Indicates whether data plane destined to the specific group address from the source IPv4 address could be handled by chip or not. |

| Buttons | |
|---|---|
|  | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |
|  | Refreshes the displayed table starting from the input fields. |
|  | Updates the table starting from the first entry in the IGMP SFM Information Table. |
|  | Updates the table, starting with the entry after the last entry currently displayed. |

## 2.4.55 MLD Snooping Status

This page provides MLD Snooping status.




| Object | Description |
|---|---|
| **VLAN ID** | The VLAN ID of the entry. |
| **Querier Version** | Working Querier Version currently. |
| **Host Version** | Working Host Version currently. |
| **Quereier Status** | Shows the Querier status is "ACTIVE" or "IDLE".<br>"DISABLE" denotes the specific interface is administratively disabled. |
| **Queries Transmitted** | The number of Transmitted Queries. |
| **Queries Received** | The number of Received Queries. |
| **V1 Report Received** | The number of Received V1 Reports. |
| **V2 Report Received** | The number of Received V2 Reports. |
| **V1 Leaves Received** | The number of Received V1 Leaves. |
| **Router Port** | Display which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or MLD querier.<br>Static denotes the specific port is configured to be a router port.<br>Dynamic denotes the specific port is learnt to be a router port.<br>Both denote the specific port is configured or learnt to be a router port. |
| **Port** | Switch port number. |

| | |
|---|---|
| **status** | Indicate whether specific port is a router port or not. |

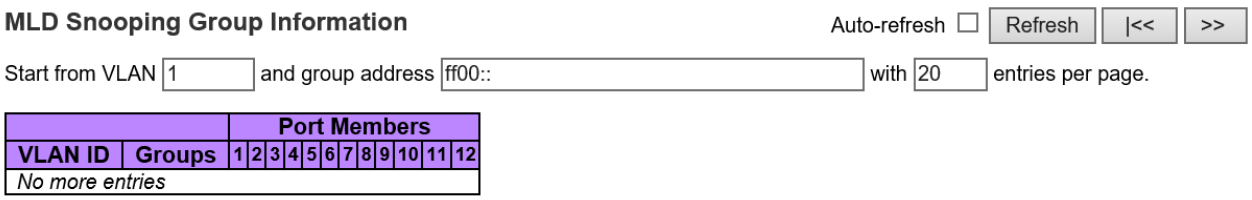
| Buttons | |
|---|---|
| Auto-refresh ☐ | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |
| Refresh | Click to refresh the page immediately. |
| Clear | Clears all Statistics counters. |

## 2.4.56 MLD Snooping - Groups Information

Each page shows up to 99 entries from the MLD Group table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MLD Group Table.

The "Start from VLAN", and "group" input fields allow the user to select the starting point in the MLD Group Table. Clicking the Refresh button will update the displayed table starting from that or the closest next MLD Group Table match. In addition, the two input fields will - upon a Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

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




| Object | Description |
|---|---|
| **VLAN ID** | VLAN ID of the group. |

| | |
|---|---|
| **Groups** | Group address of the group displayed. |
| **Port Members** | Ports under this group. |

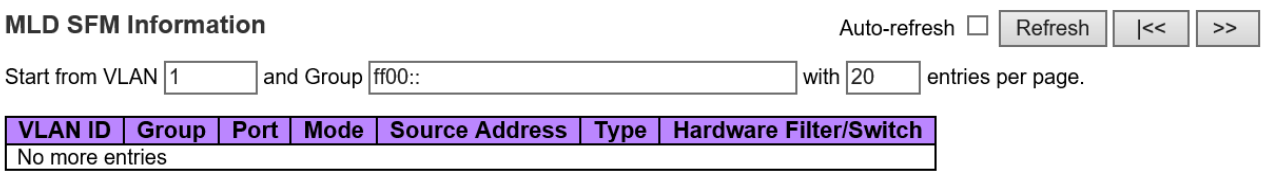
| Buttons | |
|---|---|
| Auto-refresh ☐ | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |
| Refresh | Refreshes the displayed table starting from the input fields. |
| \|<< | Updates the table, starting with the first entry in the MLD Group Table. |
| >> | Updates the table, starting with the entry after the last entry currently displayed. |

## 2.4.57 MLD Snooping - IPv6 SFM Information

Each page shows up to 99 entries from the MLD SFM Information table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MLD SFM Information Table.

The "Start from VLAN", and "group" input fields allow the user to select the starting point in the MLD SFM Information Table. Clicking the Refresh button will update the displayed table starting from that or the closest next MLD SFM Information Table match. In addition, the two input fields will - upon a Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

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

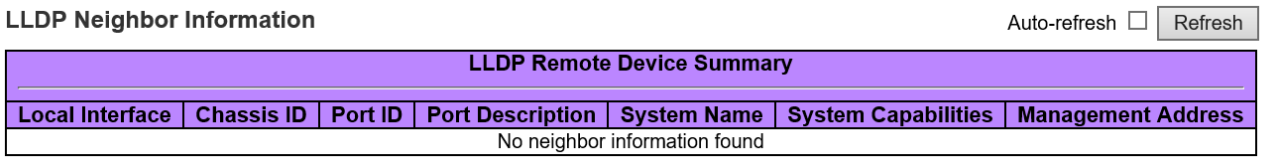


| Object | Description |
|---|---|
| **VLAN ID** | VLAN ID of the group. |
| **Group** | Group address of the group displayed. |
| **Port** | Switch port number. |
| **Mode** | Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude. |
| **Source Address** | IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128. |
| **Type** | Indicates the Type. It can be either Allow or Deny. |
| **Hardware Filter/Switch** | Indicates whether data plane destined to the specific group address from the source IPv6 address could be handled by chip or not. |

| Buttons | |
|---|---|
| Auto-refresh ☐ | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |
| Refresh | Refreshes the displayed table starting from the input fields.. |
| \|<< | Updates the table starting from the first entry in the MLD SFM Information Table. |
| >> | Updates the table, starting with the entry after the last entry currently displayed. |

## 2.4.58 LLDP - Neighbors

This page provides a status overview for all LLDP neighbors. The displayed table contains a row for each port on which an LLDP neighbor is detected.



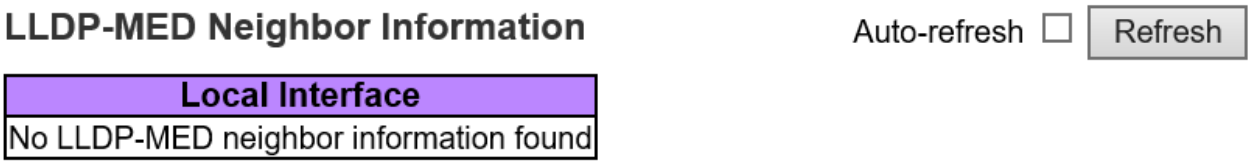

| Object | Description |
|---|---|
| **Local Port** | The port on which the LLDP frame was received. |
| **Chassis ID** | The **Chassis ID** is the identification of the neighbor's LLDP frames. |
| **Port ID** | The **Port ID** is the identification of the neighbor port. |
| **Port Description** | **Port Description** is the port description advertised by the neighbor unit. |
| **System Name** | **System Name** is the name advertised by the neighbor unit. |
| **System Capabilities** | **System Capabilities** describes the neighbor unit's capabilities. The possible capabilities are:<br>1. Other<br>2. Repeater<br>3. Bridge<br>4. WLAN Access Point<br>5. Router<br>6. Telephone<br>7. DOCSIS cable device<br>8. Station only<br>9. Reserved<br>When a capability is enabled, the capability is followed by (+). If the capability is disabled, the capability is followed by (-). |
| **Management Address** | **Management Address** is the neighbor unit's address that is used for higher layer entities to assist discovery by the network management. This could for instance hold the neighbor's IP address. |

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

| | |
|---|---|
| Refresh | Click to refresh the page. |

## 2.4.59 LLDP-MED Neighbors

This page provides a status overview of all LLDP-MED neighbors. The displayed table contains a row for each port on which an LLDP neighbor is detected. This function applies to VoIP devices which support LLDP-MED.




| Object | Description |
|---|---|
| **Port** | The port on which the LLDP frame was received. |
| **Device Type** | LLDP-MED Devices are comprised of two primary **Device Types**: Network Connectivity Devices and Endpoint Devices.<br>**LLDP-MED Network Connectivity Device Definition**<br>LLDP-MED Network Connectivity Devices, as defined in TIA-1057, provide access to the IEEE 802 based LAN infrastructure for LLDP-MED Endpoint Devices. An LLDP-MED Network Connectivity Device is a LAN access device based on any of the following technologies:<br>1. LAN Switch/Router<br>2. IEEE 802.1 Bridge<br>3. IEEE 802.3 Repeater (included for historical reasons)<br>4. IEEE 802.11 Wireless Access Point<br>5. Any device that supports the IEEE 802.1AB and MED extensions defined by TIA-1057 and can relay IEEE 802 frames via any method.<br>**LLDP-MED Endpoint Device Definition**<br>LLDP-MED Endpoint Devices, as defined in TIA-1057, are located at the IEEE 802 LAN network edge, and participate in IP communication service using the LLDP-MED framework.<br>Within the LLDP-MED Endpoint Device category, the LLDP-MED scheme is broken into further Endpoint Device Classes, as defined in the following. |

| | |
|---|---|
| | Each LLDP-MED Endpoint Device Class is defined to build upon the capabilities defined for the previous Endpoint Device Class. For-example will any LLDP-MED Endpoint Device claiming compliance as a Media Endpoint (Class II) also support all aspects of TIA-1057 applicable to Generic Endpoints (Class I), and any LLDP-MED Endpoint Device claiming compliance as a Communication Device (Class III) will also support all aspects of TIA-1057 applicable to both Media Endpoints (Class II) and Generic Endpoints (Class I).<br>**LLDP-MED Generic Endpoint (Class I)**<br>The LLDP-MED Generic Endpoint (Class I) definition is applicable to all endpoint products that require the base LLDP discovery services defined in TIA-1057, however do not support IP media or act as an end-user communication appliance. Such devices may include (but are not limited to) IP Communication Controllers, other communication related servers, or any device requiring basic services as defined in TIA-1057.<br>Discovery services defined in this class include LAN configuration, device location, network policy, power management, and inventory management.<br>**LLDP-MED Media Endpoint (Class II)**<br>The LLDP-MED Media Endpoint (Class II) definition is applicable to all endpoint products that have IP media capabilities however may or may not be associated with a particular end user. Capabilities include all of the capabilities defined for the previous Generic Endpoint Class (Class I), and are extended to include aspects related to media streaming. Example product categories expected to adhere to this class include (but are not limited to) Voice / Media Gateways, Conference Bridges, Media Servers, and similar.<br>Discovery services defined in this class include media-type-specific network layer policy discovery.<br>**LLDP-MED Communication Endpoint (Class III)**<br>The LLDP-MED Communication Endpoint (Class III) definition is applicable to all endpoint products that act as end user communication appliances supporting IP media. Capabilities include all of the capabilities defined for the previous Generic Endpoint (Class I) and Media Endpoint (Class II) classes, and are extended to include aspects related to end user devices. Example product categories expected to adhere to this class include (but are not limited to) end user communication appliances, such as IP Phones, PC-based softphones, or other communication appliances that directly support the end user.<br>Discovery services defined in this class include provision of location identifier (including ECS / E911 information), embedded L2 switch support, inventory management. |

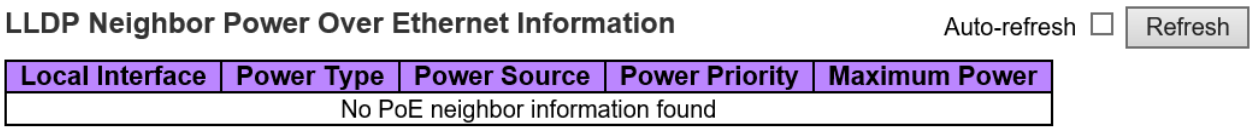
| | |
|---|---|
| **LLDP-MED Capabilities** | **LLDP-MED Capabilities** describes the neighbor unit's LLDP-MED capabilities. The possible capabilities are:<br>1. LLDP-MED capabilities<br>2. Network Policy<br>3. Location Identification<br>4. Extended Power via MDI - PSE<br>5. Extended Power via MDI - PD<br>6. Inventory<br>7. Reserved |
| **Application Type** | **Application Type** indicating the primary function of the application(s) defined for this network policy, advertised by an Endpoint or Network Connectivity Device. The possible application types are shown below.<br>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.<br>2. Voice Signalling - for use in network topologies that require a different policy for the voice signalling than for the voice media.<br>3. Guest Voice - to support a separate limited feature-set voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services.<br>4. Guest Voice Signalling - for use in network topologies that require a different policy for the guest voice signalling than for the guest voice media.<br>5. Softphone Voice - for use by softphone applications on typical data centric devices, such as PCs or laptops.<br>6. Video Conferencing - for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services.<br>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.<br>8. Video Signalling - for use in network topologies that require a separate policy for the video signalling than for the video media. |
| **Policy** | **Policy** indicates that an Endpoint Device wants to explicitly advertise that the policy is required by the device. Can be either Defined or Unknown<br>Unknown: The network policy for the specified application type is currently unknown.<br>Defined: The network policy is defined. |

| | |
|---|---|
| **TAG** | **TAG** is indicative of whether the specified application type is using a tagged or an untagged VLAN. Can be Tagged or Untagged.<br>Untagged: The device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003.<br>Tagged: The device is using the IEEE 802.1Q tagged frame format. |
| **VLAN ID** | **VLAN ID** is the VLAN identifier (VID) for the port as defined in IEEE 802.1Q-2003. A value of 1 through 4094 is used to define a valid VLAN ID. A value of 0 (Priority Tagged) is used if the device is using priority tagged frames as defined by IEEE 802.1Q-2003, meaning that only the IEEE 802.1D priority level is significant and the default PVID of the ingress port is used instead. |
| **Priority** | **Priority** is the Layer 2 priority to be used for the specified application type. One of the eight priority levels (0 through 7). |
| **DSCP** | **DSCP** is the DSCP value to be used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474. Contain one of 64 code point values (0 through 63). |
| **Auto-negotiation** | **Auto-negotiation** identifies if MAC/PHY auto-negotiation is supported by the link partner. |
| **Auto-negotiation status** | **Auto-negotiation status** identifies if auto-negotiation is currently enabled at the link partner. If **Auto-negotiation** is supported and **Auto-negotiation status** is disabled, the 802.3 PMD operating mode will be determined the operational MAU type field value rather than by auto-negotiation. |
| **Auto-negotiation Capabilities** | **Auto-negotiation Capabilities** shows the link partners MAC/PHY capabilities. |

| **Buttons** | |
|---|---|
| Auto-refresh ☐ | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |
| Refresh | Click to refresh the page. |

## 2.4.60 LLDP - PoE

This page provides a status overview for all LLDP PoE neighbors. The displayed table contains a row for each port on which an LLDP PoE neighbor is detected.




| Object | Description |
|---|---|
| **Local Port** | The port for this switch on which the LLDP frame was received. |
| **Power Type** | The **Power Type** represents whether the device is a Power Sourcing Entity (PSE) or Power Device (PD).<br>If the **Power Type** is unknown it is represented as "Reserved". |
| **Power Source** | The **Power Source** represents the power source being utilized by a PSE or PD device.<br>If the device is a PSE device it can either run on its Primary Power Source or its Backup Power Source. If it is unknown whether the PSE device is using its Primary Power Source or its Backup Power Source it is indicated as "Unknown"<br>If the device is a PD device it can either run on its local power supply or it can use the PSE as power source. It can also use both its local power supply and the PSE.<br>If it is unknown what power supply the PD device is using it is indicated as "Unknown". |
| **Power Priority** | Power Priority represents the priority of the PD device, or the power priority associated with the PSE type device's interface that is sourcing the power. There are three levels of power priority. The three levels are: Critical, High and Low.<br>If the power priority is unknown it is indicated as "Unknown" |
| **Maximum Power** | The Maximum Power Value contains a numerical value that indicates the maximum power in watts required by a PD device from a PSE device, or the minimum power a PSE device is capable of sourcing over a maximum length cable based on its current configuration.<br>The maximum allowed value is 102.3 W. If the device indicates value higher than 102.3 W, it is represented as "reserved" |

| Buttons |
|---|

| | |
|---|---|
| Auto-refresh ☐ | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |
| Refresh | Click to refresh the page. |

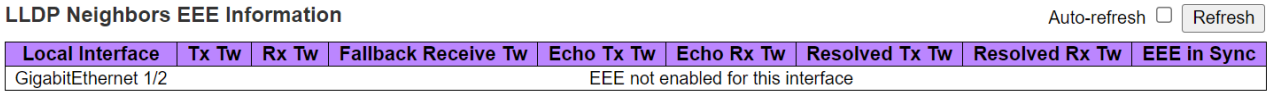
## 2.4.61 LLDP – EEE (For 90W PoE Model)

The displayed table contains a row for each interface.

If the interface does not supports EEE, then it displays as "EEE not supported for this interface".

If EEE is not enabled on particular interface, then it displays as "EEE not enabled for this interface".

If the link partner doesn't supports EEE, then it displays as "Link partner is not EEE capable.




| Object | Description |
|---|---|
| **Local Interface** | The interface at which LLDP frames are received or transmitted. |
| **Tx Tw** | The link partner's maximum time that transmit path can hold-off sending data after deassertion of LPI. |
| **Rx Tw** | The link partner's time that receiver would like the transmitter to hold-off to allow time for the receiver to wake from sleep. |
| **Fallback Receive Tw** | The link partner's fallback receive Tw.<br>A receiving link partner may inform the transmitter of an alternate desired Tw_sys_tx. Since a receiving link partner is likely to have discrete levels for savings, this provides the transmitter with additional information that it may use for a more efficient allocation. Systems that do not implement this option default the value to be the same as that of the Receive Tw_sys_tx. |
| **Echo Tx Tw** | The link partner's Echo Tx Tw value.<br>The respective echo values shall be defined as the local link partners reflection (echo) of the remote link partners respective values. When a local link partner receives its echoed values from the remote link partner it can determine whether or not the remote link partner has received, registered and processed its most recent values. For example, if the local link partner receives echoed parameters that do not match the values in its local MIB, then the local link partner infers that the remote link partners request was based on stale information. |
| **Echo Rx Tw** | The link partner's Echo Rx Tw value. |
| **Resolved Tx Tw** | The resolved Tx Tw for this link. Note : NOT the link partner |

| | |
|---|---|
| | The resolved value that is the actual "tx wakeup time " used for this link (based on EEE information exchanged via LLDP). |
| **Resolved Rx Tw** | The resolved Rx Tw for this link. Note : NOT the link partner<br>The resolved value that is the actual "tx wakeup time " used for this link (based on EEE information exchanged via LLDP). |
| **EEE in Sync** | Shows whether the switch and the link partner have agreed on wake times.<br>Red - Switch and link partner have not agreed on wakeup times.<br>Green - Switch and link partner have agreed on wakeup times. |
| | |

| **Buttons** | |
|---|---|
| Auto-refresh ☐ | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |
| Refresh | Click to refresh the page. |

## 2.4.62 LLDP - Port Statistics

This page provides an overview of all LLDP traffic.

Two types of counters are shown. **Global counters** are counters that refer to the whole switch, while **local counters** refer to per port counters for the currently selected switch.

**LLDP Global Counters**

Auto-refresh ☐ Refresh Clear

| Global Counters | |
|---|---|
| Clear global counters | ☑ |
| Neighbor entries were last changed | 1970-01-01T00:00:00+00:00 (2461 secs. ago) |
| Total Neighbors Entries Added | 0 |
| Total Neighbors Entries Deleted | 0 |
| Total Neighbors Entries Dropped | 0 |
| Total Neighbors Entries Aged Out | 0 |

**LLDP Statistics Local Counters**

| Local Interface | Tx Frames | Rx Frames | Rx Errors | Frames Discarded | TLVs Discarded | TLVs Unrecognized | Org. Discarded | Age-Outs | Clear |
|---|---|---|---|---|---|---|---|---|---|
| * | * | * | * | * | * | * | * | * | ☑ |
| GigabitEthernet 1/1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | ☑ |
| GigabitEthernet 1/2 | 80 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | ☑ |
| GigabitEthernet 1/3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | ☑ |
| GigabitEthernet 1/4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | ☑ |
| GigabitEthernet 1/5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | ☑ |
| GigabitEthernet 1/6 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | ☑ |
| GigabitEthernet 1/7 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | ☑ |
| GigabitEthernet 1/8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | ☑ |
| 10GigabitEthernet 1/1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | ☑ |
| 10GigabitEthernet 1/2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | ☑ |
| 10GigabitEthernet 1/3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | ☑ |
| 10GigabitEthernet 1/4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | ☑ |

| Object | Description |
|---|---|
| **Global Counters** | |
| **Clear global counters** | If checked the global counters are cleared when Clear is pressed. |
| **Neighbor entries were last change** | Shows the time when the last entry was last deleted or added. It also shows the time elapsed since the last change was detected. |
| **Total Neighbors Entries Added** | Shows the number of new entries added since switch reboot. |
| **Total Neighbors Entries Deleted** | Shows the number of new entries deleted since switch reboot. |
| **Total Neighbors Entries Dropped** | Shows the number of LLDP frames dropped due to the entry table being full. |
| **Total Neighbors Entries Aged Out** | Shows the number of entries deleted due to Time-To-Live expiring. |
| **Local Counters** | |
| **Local Port** | The port on which LLDP frames are received or transmitted. |
| **Tx Frames** | The number of LLDP frames transmitted on the port. |
| **Rx Frames** | The number of LLDP frames received on the port. |
| **Rx Errors** | The number of received LLDP frames containing some kind of error. |
| **Frames Discarded** | If a LLDP frame is received on a port, and the switch's internal table has run full, the LLDP frame is counted and discarded. This situation is known as "Too Many Neighbors" in the LLDP standard. LLDP frames require a new entry in the table when the Chassis ID or Remote Port ID is not already contained within the table. Entries are removed from the table when a given port's link is down, an LLDP shutdown frame is received, or when the entry ages out. |
| **TLVs Discarded** | Each LLDP frame can contain multiple pieces of information, known as TLVs (TLV is short for "Type Length Value"). If a TLV is malformed, it is counted and discarded. |
| **TLVs Unrecognized** | The number of well-formed TLVs, but with an unknown type value. |
| **Org. Discarded** | If LLDP frame is received with an organizationally TLV, but the TLV is not supported the TLV is discarded and counted. |
| **Age-Outs** | Each LLDP frame contains information about how long time the LLDP information is valid (age-out time). If no new LLDP frame is received within the age out time, the LLDP information is removed, and the **Age-Out** counter is incremented. |
| **Clear** | If checked the counters for the specific interface are cleared when Clear is pressed. |

| Buttons | |
|---|---|
| Auto-refresh ☐ | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |
| Refresh | Click to refresh the page. |
| Clear | Clears the **local counters**. All counters (including **global counters**) are cleared upon reboot. |

## 2.4.63 Fabric Attach - FA Agent

Fabric Attach is a software-based to using LLDP extensibility TLV feature. Create and implement a easy configuration function with I-SID/VLAN. Non fabric device also can be accept with FA equipment.

**FA Agent**

| Agent | Status |
|---|---|
| FA Service | Enabled |
| FA Element Type | Client |
| FA Assignment Timeout(sec) | 240 |
| FA Discovery Timeout(sec) | 240 |
| FA Extended Logging Status | Disabled |
| FA Upstream Switch System ID | 00:00:00:00:00:00:00:00:00:00 |
| FA Upstream Switch System Description | |

| Object | Description |
|---|---|
| **Agent Status** | These fields have agent and FA Server/Proxy information.<br>FA Service "Enabled" means system FA function is ready. "Disabled" is FA function down.<br>FA Element Type is "Client". This ISW switch role is FA client.<br>FA Zero Touch Status is show current status.<br>FA Assignment Timeout(sec) is FA Configuration "Assignment Timeout" setting value.<br>FA Discovery Timeout(sec) is FA Configuration "Discovery Timeout" setting value.<br>FA Extended Logging Status is FA Configuration "Extended Logging" setting value.<br>FA Primary Server ID is received FA Server/Proxy system ID.<br>FA Primary Serer Descr is received FA Server/Proxy description. |

## 2.4.64 Fabric Attach - FA Status

Fabric Attach is a software-based to using LLDP extensibility TLV feature. Create and implement a easy configuration function with I-SID/VLAN. Non fabric device also can be accept with FA equipment.

Supported Fabric Attach Element inter-connections Each FA element connection must be a single logical link. FA Servers must be a single entity and can support multiple FA Proxy or FA Client devices. An FA Proxy must communicate with one FA Server. An FA Client must communicate with one FA Server or one FA Proxy.

### FA Status

#### Discovery Elements

| Port | Type | VLAN | Status | System ID | ELEM AUTH | ASGN AUTH | ELEM OPER AUTH STATUS | ASGN OPER AUTH STATUS |
|---|---|---|---|---|---|---|---|---|

State Legend: (Tagging/AutoConfig)
T=Tagged, U=Untagged, D=Disabled, S=Spbm, V=Vlan, I=Invalid Auth

Auth Legend:
AP=Authentication Pass, AF=Authentication Fail, NA=Not Authenticated, N=None

#### Assignment

| Port | I-SID | VLAN | Status | Source |
|---|---|---|---|---|

| Object | Description |
|---|---|
| **Discovery Elements** | |
| **Port** | Interface port number. |
| **Type** | This interface received discovery elements type. Valid values are FA Serve/FA Proxy/FA Server (no authentication)/FA Proxy (no authentication)/FA Clients. FA Clients include WLAN AP Type1/WLAN AP Type2/Switch/IP Phone/IP Camera/ONA/Virt Switch/Server |
| **VLAN** | Specifies the VLAN of the specific I-SID-to-VLAN assignment to remove. Valid values range from 1 to 4095. |
| **Status** | T=Tagged, U=Untagged, D=Disabled, S=Spbm, V=Vlan, I=Invalid Auth. |
| **System ID** | FA device system ID. |
| **ELEM AUTH** | Element authentication status. |
| **ASGN AUTH** | Assignment authentication status. |
| **ELEM OPER AUTH STATUS** | Detail element authentication status. |
| **ASGN OPER AUTH STATUS** | Detail assignment authentication status. |
| **Assignment** | |
| **Port** | Interface port number. |
| **I-SID** | Specifies the I-SID of the specific I-SID-to-VLAN assignment to remove. Values range from 1 to 16777214. |
| **VLAN** | Specifies the VLAN of the specific I-SID-to-VLAN assignment to remove. Valid values range from 1 to 4095. |
| **Status** | Current status (Pending/Active/Rejection). |
| **Source** | Data source (Client/ Proxy/ Server/ Proxy,Client/ Server,Client). |

## 2.4.65 Fabric Attach - FA Statistics

Fabric Attach is a software-based to using LLDP extensibility TLV feature. Create and implement a easy configuration function with I-SID/VLAN. Non fabric device also can be accept with FA equipment.

Supported Fabric Attach Element inter-connections Each FA element connection must be a single logical link. FA Servers must be a single entity and can support multiple FA Proxy or FA Client devices. An FA Proxy must communicate with one FA Server. An FA Client must communicate with one FA Server or one FA Proxy.

**FA Statistics** Auto-refresh ☐ Refresh Clear

**Discovery Elements**

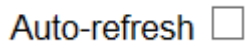
| Port | DiscElem Received | DiscElem Expired | DiscElem Deleted | DiscAuth Failed |
|---|---|---|---|---|
| 1 | 0 | 0 | 0 | 0 |
| 2 | 0 | 0 | 0 | 0 |
| 3 | 0 | 0 | 0 | 0 |
| 4 | 0 | 0 | 0 | 0 |
| 5 | 0 | 0 | 0 | 0 |
| 6 | 0 | 0 | 0 | 0 |
| 7 | 0 | 0 | 0 | 0 |
| 8 | 0 | 0 | 0 | 0 |
| 9 | 0 | 0 | 0 | 0 |
| 10 | 0 | 0 | 0 | 0 |
| 11 | 0 | 0 | 0 | 0 |
| 12 | 0 | 0 | 0 | 0 |
| summary | 0 | 0 | 0 | 0 |

**Assignment**

| Port | Asgn Received | Asgn Accepted | Asgn Rejected | Asgn Expired | Asgn Deleted | AsgnAuth Failed |
|---|---|---|---|---|---|---|
| 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| 2 | 0 | 0 | 0 | 0 | 0 | 0 |
| 3 | 0 | 0 | 0 | 0 | 0 | 0 |
| 4 | 0 | 0 | 0 | 0 | 0 | 0 |
| 5 | 0 | 0 | 0 | 0 | 0 | 0 |
| 6 | 0 | 0 | 0 | 0 | 0 | 0 |
| 7 | 0 | 0 | 0 | 0 | 0 | 0 |
| 8 | 0 | 0 | 0 | 0 | 0 | 0 |
| 9 | 0 | 0 | 0 | 0 | 0 | 0 |
| 10 | 0 | 0 | 0 | 0 | 0 | 0 |
| 11 | 0 | 0 | 0 | 0 | 0 | 0 |
| 12 | 0 | 0 | 0 | 0 | 0 | 0 |
| summary | 0 | 0 | 0 | 0 | 0 | 0 |

| Object | Description |
|---|---|
| **Discovery Elements** | |
| **Port** | Interface port number. |
| **DiscElem Received** | Discovery elements received package TLV number. |
| **DiscElem Expired** | Discovery elements expired number. |

| | |
|---|---|
| **DiscElem Deleted** | Discovery elements deleted number. |
| **DiscAuth Failed** | Discovery authentication failed number. |
| **Assignment** | |
| **Port** | Interface port number. |
| **Asgn Received** | Assignments received package TLV number. |
| **Asgn Accepted** | Assignments accepted package TLV number. |
| **Asgn Rejected** | Assignments rejected package TLV number. |
| **Asgn Expired** | Assignments expired number. |
| **Asgn Deleted** | Assignments deleted number. |
| **AsgnAuth Failed** | Assignments authentication failed package TLV number. |

| **Buttons** | |
|---|---|
|  | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |
|  | Click to refresh the page. |
|  | Clear statistics |

## 2.4.66 PoE

This page allows the user to inspect the current status for all PoE ports.

**Power Over Ethernet Status**

Auto-refresh ☐ Refresh

| Local Port | PD class | Power Requested | Power Allocated | Power Used | Current Used | Priority | Port Status |
|---|---|---|---|---|---|---|---|
| 1 | - | 0 [W] | 0 [W] | 0 [W] | 0 [mA] | Low | PoE turned OFF - PoE disabled |
| 2 | - | 0 [W] | 0 [W] | 0 [W] | 0 [mA] | Low | PoE turned OFF - PoE disabled |
| 3 | - | 0 [W] | 0 [W] | 0 [W] | 0 [mA] | Low | PoE turned OFF - PoE disabled |
| 4 | - | 0 [W] | 0 [W] | 0 [W] | 0 [mA] | Low | PoE turned OFF - PoE disabled |
| 5 | - | 0 [W] | 0 [W] | 0 [W] | 0 [mA] | Low | PoE turned OFF - PoE disabled |
| 6 | - | 0 [W] | 0 [W] | 0 [W] | 0 [mA] | Low | PoE turned OFF - PoE disabled |
| 7 | - | 0 [W] | 0 [W] | 0 [W] | 0 [mA] | Low | PoE turned OFF - PoE disabled |
| 8 | - | 0 [W] | 0 [W] | 0 [W] | 0 [mA] | Low | PoE turned OFF - PoE disabled |
| Total | | 0 [W] | 0 [W] | 0 [W] | 0 [mA] | | |

| Object | Description |
|---|---|
| **Local Port** | This is the logical port number for this row. |
| **PD Class** | Each PD is classified according to a class that defines the maximum power the PD will use. The PD Class shows the PDs class.<br>The following classes are defined:<br>Class 0: Max. power 15.4 W<br>Class 1: Max. power 4.0 W<br>Class 2: Max. power 7.0 W<br>Class 3: Max. power 15.4 W<br>Class 4: Max. power 30.0 W<br>Class 5: Max. power 45.0 W (For 90W PoE Model)<br>Class 6: Max. power 60.0 W (For 90W PoE Model)<br>Class 7: Max. power 70.0 W (For 90W PoE Model)<br>Class 8: Max. power 90.0 W (For 90W PoE Model) |
| **Power Requested** | The Power Requested shows the requested amount of power the PD wants to be reserved. |
| **Power Allocated** | The Power Allocated shows the amount of power the switch has allocated for the PD. |
| **Power Used** | The Power Used shows how much power the PD currently is using. |
| **Current Used** | The Power Used shows how much current the PD currently is using. |
| **Priority** | The Priority shows the port's priority configured by the user. |
| **Port Status (For 90W PoE Model)** | The Port Status shows the port's status. The status can be one of the following values:<br>On - A PD is detected for the port.<br>--- - No PD detected for the port.<br>Not Supported - PoE not supported for the port. |

| | |
|---|---|
| | Budget Exceeded - The total requested or used power by the PDs exceeds the maximum power the Power Supply can deliver, and port(s) with the lowest priority is/are powered down.<br>Off - PD is off.<br>Disabled - User has disabled PoE for the port.<br>Shutdown - The port is shut down.<br>Overload - The PD has requested or used more power than the port can deliver, and is powered down.<br>Unknown - PD detected, but is not working correctly. |
| **Port Status (For 30W PoE Model)** | The Port Status shows the port's status. The status can be one of the following values:<br>PoE not available - No PoE chip found - PoE not supported for the port.<br>PoE turned OFF - PoE disabled : PoE is disabled by user.<br>PoE turned OFF - Power budget exceeded - The total requested or used power by the PDs exceeds the maximum power the Power Supply can deliver, and port(s) with the lowest priority is/are powered down.<br>No PD detected - No PD detected for the port.<br>PoE turned OFF - PD overload - The PD has requested or used more power than the port can deliver, and is powered down.<br>PoE turned OFF - PD is off.<br>Invalid PD - PD detected, but is not working correctly. |

| **Buttons** | |
|---|---|
| Auto-refresh ☐ | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |
| Refresh | Click to refresh the page. |

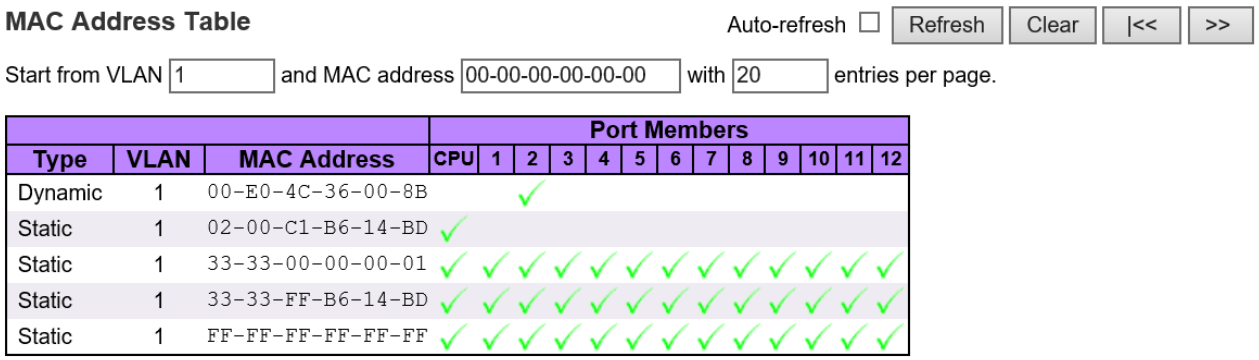
## 2.4.67 MAC Table

Each page shows up to 999 entries from the MAC table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MAC Table. The first displayed will be the one with the lowest VLAN ID and the lowest MAC address found in the MAC Table.

The "Start from MAC address" and "VLAN" input fields allow the user to select the starting point in the MAC Table. Clicking the Refresh button will update the displayed table starting from that or the closest next MAC Table match. In addition, the two input fields will - upon a Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The >> will use the last entry of the currently displayed VLAN/MAC address pairs as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table.

Use the |<< button to start over.




| Object | Description |
|---|---|
| **Type** | Indicates whether the entry is a static or a dynamic entry. |
| **MAC Address** | The MAC address of the entry. |
| **VLAN** | The VLAN ID of the entry. |
| **Port Members** | The ports that are members of the entry. |

| Buttons |
|---|

| | |
|---|---|
| Auto-refresh ☐ | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |
| Refresh | Refreshes the displayed table starting from the "Start from MAC address" and "VLAN" input fields. |
| Clear | Flushes all dynamic entries. |
| \|<< | Updates the table starting from the first entry in the MAC Table, i.e. the entry with the lowest VLAN ID and MAC address. |
| >> | Updates the table, starting with the entry after the last entry currently displayed. |

## 2.4.68 VLANs Membership

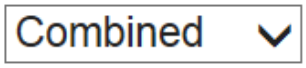
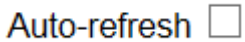
Each page shows up to 99 entries from the VLAN table (default being 20), selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the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

Clicking the Refresh button will update the displayed table starting from that or the closest next VLAN Table match.

The >> will use the last entry of the currently displayed VLAN entry as a basis for the next lookup. When the end is reached, the text "No data exists for the selected user" is shown in the table. Use the |<< button to start over.

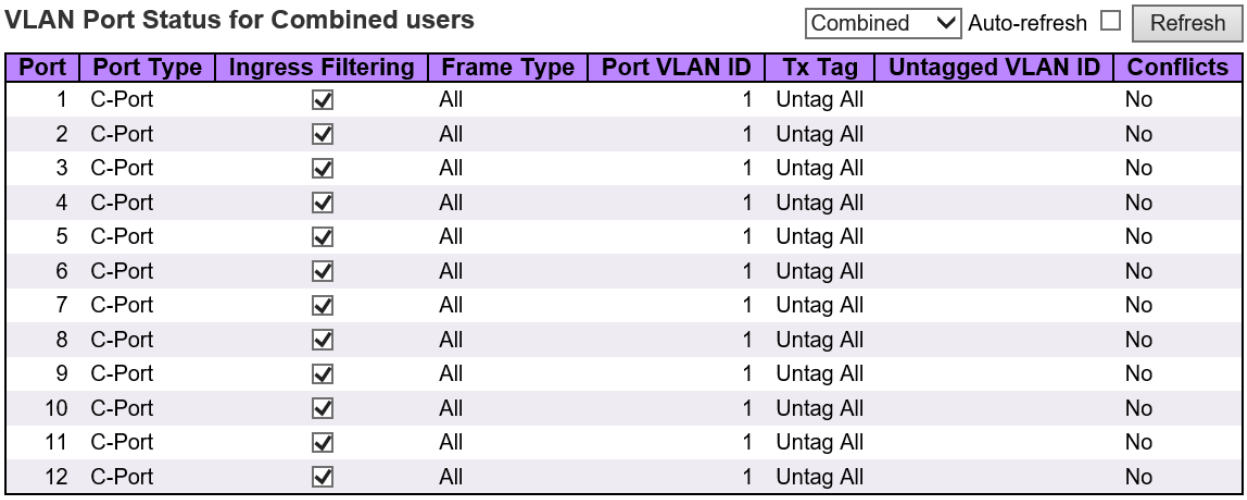

| Object | Description |
|---|---|
| **VLAN User** | Various internal software modules may use VLAN services to configure VLAN memberships on the fly.<br>The drop-down list on the right allows for selecting between showing VLAN memberships as configured by an administrator (Admin) or as configured by one of these internal software modules.<br>The "Combined" entry will show a combination of the administrator and internal software modules configuration, and basically reflects what is actually configured in hardware. |
| **VLAN ID** | VLAN ID for which the Port members are displayed. |
| **Port Members** | A row of check boxes for each port is displayed for each VLAN ID.<br>If a port is included in a VLAN, the following image will be displayed: ✓.<br>If a port is in the forbidden port list, the following image will be displayed: ✗.<br>If a port is in the forbidden port list and at the same time attempted included in the VLAN, the following image will be displayed: ✗. The port will not be a member of |

| | |
|---|---|
| | the VLAN in this case. |

| Buttons | |
|---|---|
|  | Select VLAN Users from this drop down list. |
|  | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |
|  | Click to refresh the page immediately. |

## 2.4.69 VLANs Ports

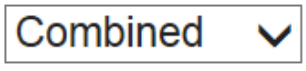
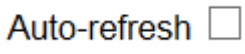
This page provides VLAN Port Status.




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

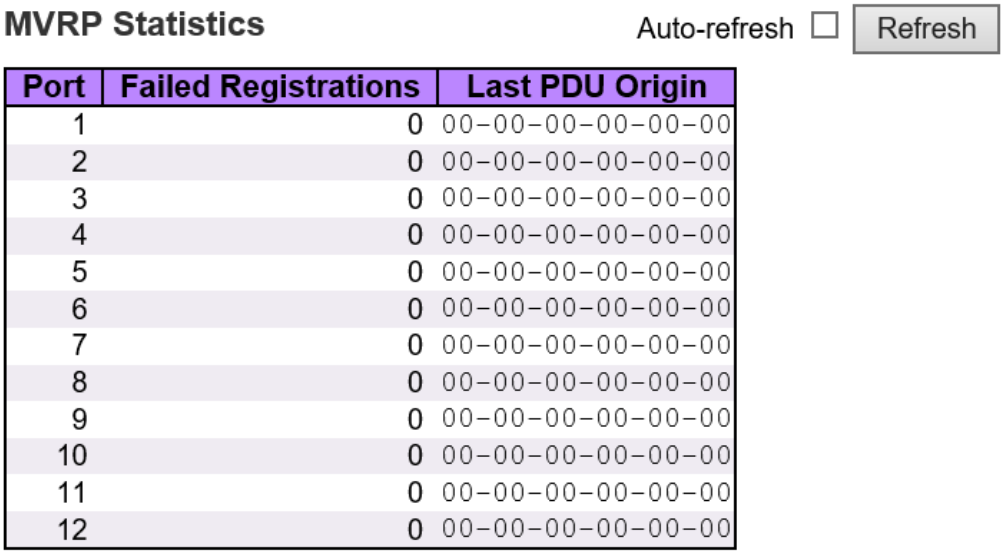
| Object | Description |
|---|---|
| **VLAN User** | Various internal software modules may use VLAN services to configure VLAN port configuration on the fly.<br>The drop-down list on the right allows for selecting between showing VLAN memberships as configured by an administrator (Admin) or as configured by one of these internal software modules.<br>The "Combined" entry will show a combination of the administrator and internal software modules configuration, and basically reflects what is actually configured in hardware.<br>If a given software modules hasn't overridden any of the port settings, the text "No data exists for the selected user" is shown in the table. |
| **Port** | The logical port for the settings contained in the same row. |

| | |
|---|---|
| **Port Type** | Shows the port type (Unaware, C-Port, S-Port, S-Custom-Port.) that a given user wants to configure on the port.<br>The field is empty if not overridden by the selected user. |
| **Ingress Filtering** | Shows whether a given user wants ingress filtering enabled or not.<br>The field is empty if not overridden by the selected user. |
| **Frame Type** | Shows the acceptable frame types (All, Taged, Untagged) that a given user wants to configure on the port.<br>The field is empty if not overridden by the selected user. |
| **Port VALN ID** | Shows the Port VLAN ID (PVID) that a given user wants the port to have.<br>The field is empty if not overridden by the selected user. |
| **Tx Tag** | Shows the Tx Tag requirements (Tag All, Tag PVID, Tag UVID, Untag All, Untag PVID, Untag UVID) that a given user has on a port.<br>The field is empty if not overridden by the selected user. |
| **Untagged VLAN ID** | If Tx Tag is overridden by the selected user and is set to Tag or Untag UVID, then this field will show the VLAN ID the user wants to tag or untag on egress.<br>The field is empty if not overridden by the selected user. |
| **Conflicts** | Two users may have conflicting requirements to a port's configuration. For instance, one user may require all frames to be tagged on egress while another requires all frames to be untagged on egress.<br>Since both users cannot win, this gives rise to a conflict, which is solved in a prioritized way. The Administrator has the least priority. Other software modules are prioritized according to their position in the drop-down list: The higher in the list, the higher priority.<br>If conflicts exist, it will be displayed as "Yes" for the "Combined" user and the offending software module.<br>The "Combined" user reflects what is actually configured in hardware. |

| **Buttons** | |
|---|---|
|  | Select VLAN Users from this drop down list. |
|  | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |
|  | Click to refresh the page immediately. |

## 2.4.70 MVRP (For 90W PoE Model)

This page provides statistics for the MVRP protocol for all switch ports.

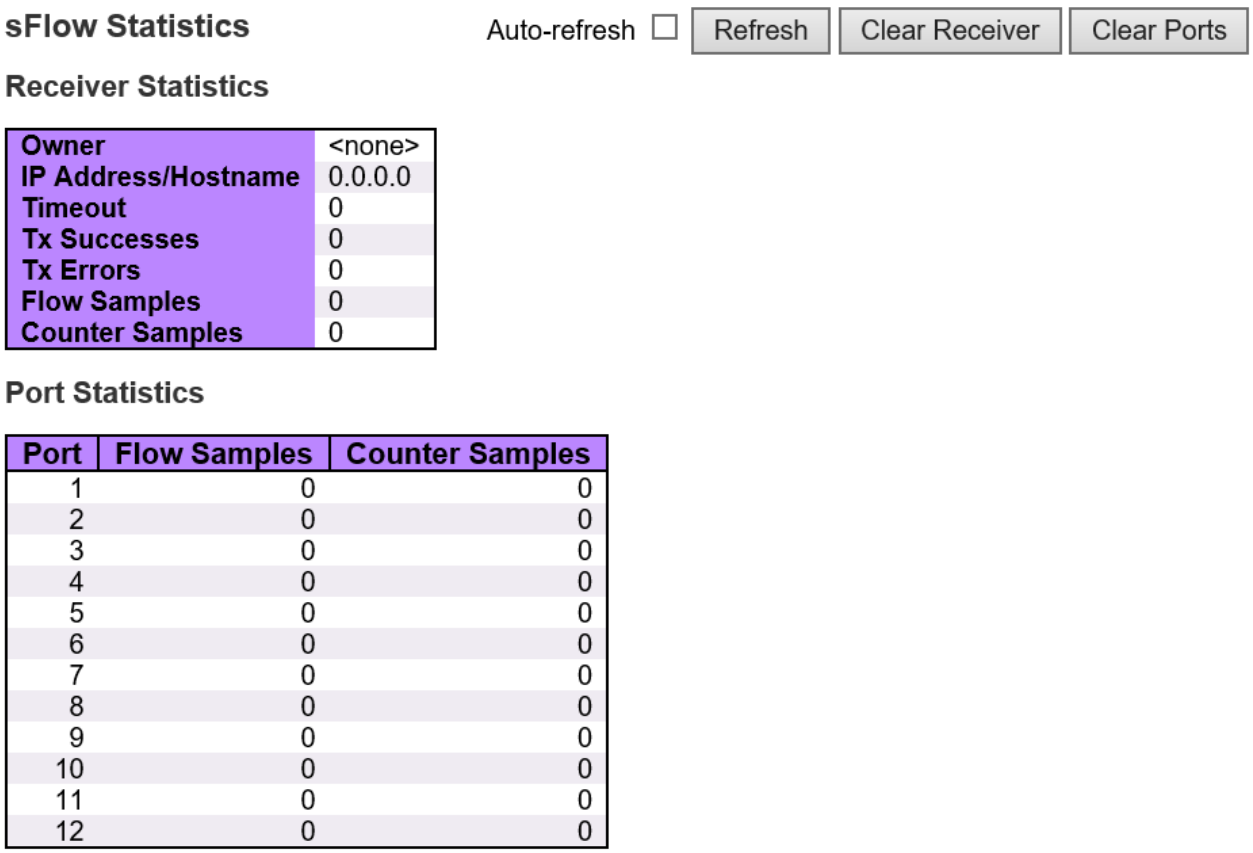



| Object | Description |
|---|---|
| **Port** | The logical port for the statistics contained in the same row. |
| **Failed Registrations** | The number of failed VLAN registrations on this switch port. Each port implementing the MVRP protocol maintains a count of the number of times it has received a VLAN registration request but has failed to register the VLAN due to lack of space in the Filtering Database. |
| **Last PDU Origin** | The MAC address of the most recent MVRP PDU received on this switch port. MAC is 00-00-00-00-00-00 if the protocol is not enabled on that switch port, or if the port has not received any MVRP PDUs yet. |

| Buttons | |
|---|---|
| Auto-refresh ☐ | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |
| Refresh | Refreshes the displayed table. |

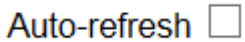
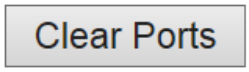
## 2.4.71 sFlow

This page shows receiver and per-port sFlow statistics.




| Object | Description |
|---|---|
| **Receiver Statistics** | |
| **Owner** | This field shows the current owner of the sFlow configuration. It assumes one of three values as follows:<br>• If sFlow is currently unconfigured/unclaimed, Owner contains `<none>`.<br>• If sFlow is currently configured through Web or CLI, Owner contains `<Configured through local management>`.<br>• If sFlow is currently configured through SNMP, Owner contains a string identifying the sFlow receiver. |
| **IP Address/Hostname** | The IP address or hostname of the sFlow receiver. |
| **Timeout** | The number of seconds remaining before sampling stops and the current sFlow owner is released. |
| **Tx Successes** | The number of UDP datagrams successfully sent to the sFlow receiver. |

| | |
|---|---|
| **Tx Errors** | The number of UDP datagrams that has failed transmission.<br>The most common source of errors is invalid sFlow receiver IP/hostname configuration. To diagnose, paste the receiver's IP address/hostname into the Ping Web page (Diagnostics → Ping/Ping6). |
| **Flow Samples** | The total number of flow samples sent to the sFlow receiver. |
| **Counter Samples** | The total number of counter samples sent to the sFlow receiver. |
| **Port Statistics** | |
| **Port** | The port number for which the following statistics applies. |
| **Flow Samples** | The number of flow samples sent to the sFlow receiver originating from this port. |
| **Counter Samples** | The total number of counter samples sent to the sFlow receiver originating from this port. |

| **Buttons** | |
|---|---|
|  | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |
|  | Click to refresh the page. |
|  | Clears the sFlow receiver counters. |
|  | Clears the per-port counters. |

## 2.4.72 RingV2

**RingV2 Group Status** Auto-refresh ☐ Refresh

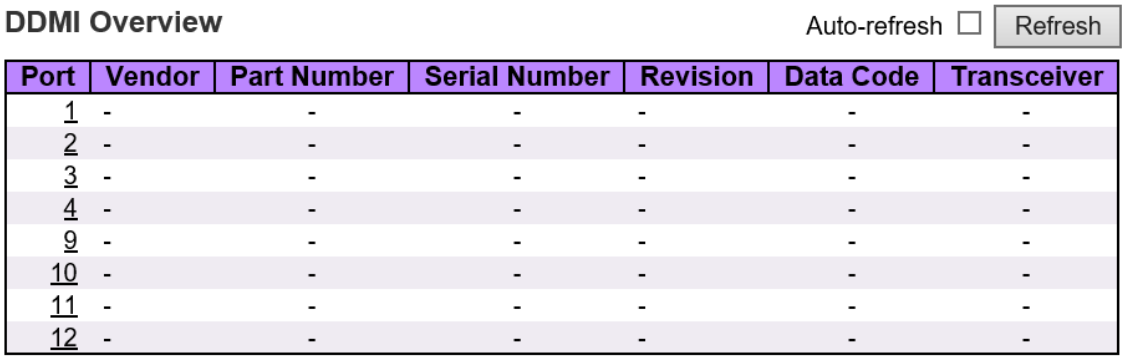
| Group index | Mode | State | Role | Ring Port(s) |
|---|---|---|---|---|
| 1 | Disable | -- | Ring(Slave) | -- |
| 2 | Disable | -- | Ring(Slave) | -- |
| 3 | Disable | -- | Chain(Member) | -- |

| Object | Description |
|---|---|
| **Group Index** | The group index. This parameter is used for easy identifying which ring group. |
| **Mode** | It indicates whether the group is enabled. |
| **Role** | It indicates group is configured as which role. |
| **State** | When ring is complete, it will show "Normal".<br>When ring is incomplete (at least one link is down), it will show "Fail". |
| **Ring Port(s)** | Describes current status of ring port(s). |

| Buttons | |
|---|---|
| Auto-refresh ☐ | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |
| Refresh | Click to refresh the page. |

## 2.4.73 DDMI Overview

Display DDMI overview information on this page.

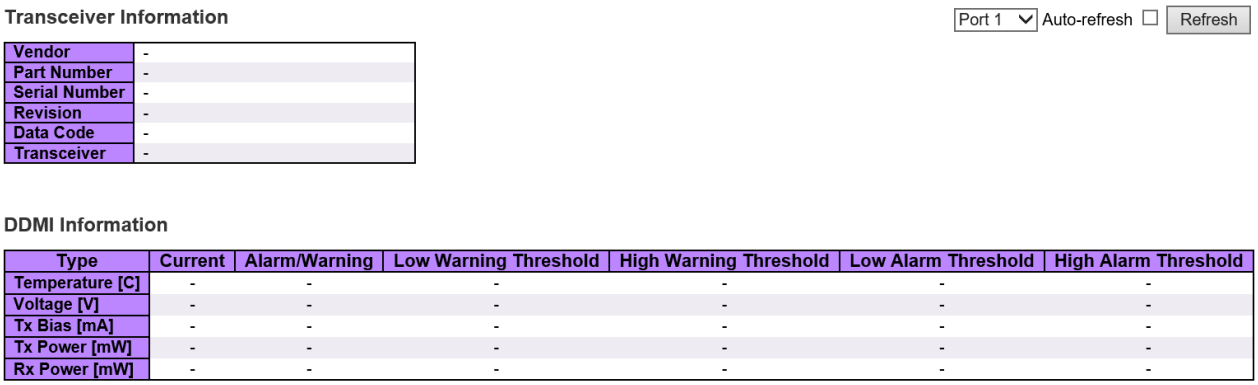



| Object | Description |
|---|---|
| **Port** | DDMI port. |
| **Vendor** | Indicates Vendor name SFP vendor name. |
| **Part Number** | Indicates Vendor PN Part number provided by SFP vendor. |
| **Serial Number** | Indicates Vendor SN Serial number provided by vendor. |
| **Revision** | Indicates Vendor rev Revision level for part number provided by vendor. |
| **Date Code** | Indicates Date code Vendor's manufacturing date code. |
| **Transceiver** | Indicates Transceiver compatibility. |

| Buttons | |
|---|---|
| Auto-refresh ☐ | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |
| Refresh | Click to refresh the page. |

## 2.4.74 DDMI Detailed

Display DDMI detailed information on this page.



Transceiver Information

Port 1 Auto-refresh Refresh

| | |
|---|---|
| Vendor | - |
| Part Number | - |
| Serial Number | - |
| Revision | - |
| Data Code | - |
| Transceiver | - |

DDMI Information

| Type | Current | Alarm/Warning | Low Warning Threshold | High Warning Threshold | Low Alarm Threshold | High Alarm Threshold |
|---|---|---|---|---|---|---|
| Temperature [C] | - | - | - | - | - | - |
| Voltage [V] | - | - | - | - | - | - |
| Tx Bias [mA] | - | - | - | - | - | - |
| Tx Power [mW] | - | - | - | - | - | - |
| Rx Power [mW] | - | - | - | - | - | - |

| Object | Description |
|---|---|
| **Transceiver Information** | |
| **Vendor** | Indicates Vendor name SFP vendor name. |
| **Part Number** | Indicates Vendor PN Part number provided by SFP vendor. |
| **Serial Number** | Indicates Vendor SN Serial number provided by vendor. |
| **Revision** | Indicates Vendor rev Revision level for part number provided by vendor. |
| **Date Code** | Indicates Date code Vendor's manufacturing date code. |
| **Transceiver** | Indicates Transceiver compatibility. |
| **DDMI Information** | |
| **Current** | The current value of temperature, voltage, TX bias, TX power, and RX power. |
| **Alarm/Warning (For 90W PoE Model)** | Indicates whether there is an alarm or warning. |
| **High Alarm Threshold** | The high alarm threshold value of temperature, voltage, TX bias, TX power, and RX power. |
| **High Warn Threshold** | The high warn threshold value of temperature, voltage, TX bias, TX power, and RX power. |
| **Low Warn Threshold** | The low warn threshold value of temperature, voltage, TX bias, TX power, and RX power. |
| **Low Alarm Threshold** | The low alarm threshold value of temperature, voltage, TX bias, TX power, and RX power. |

| Buttons |
|---|

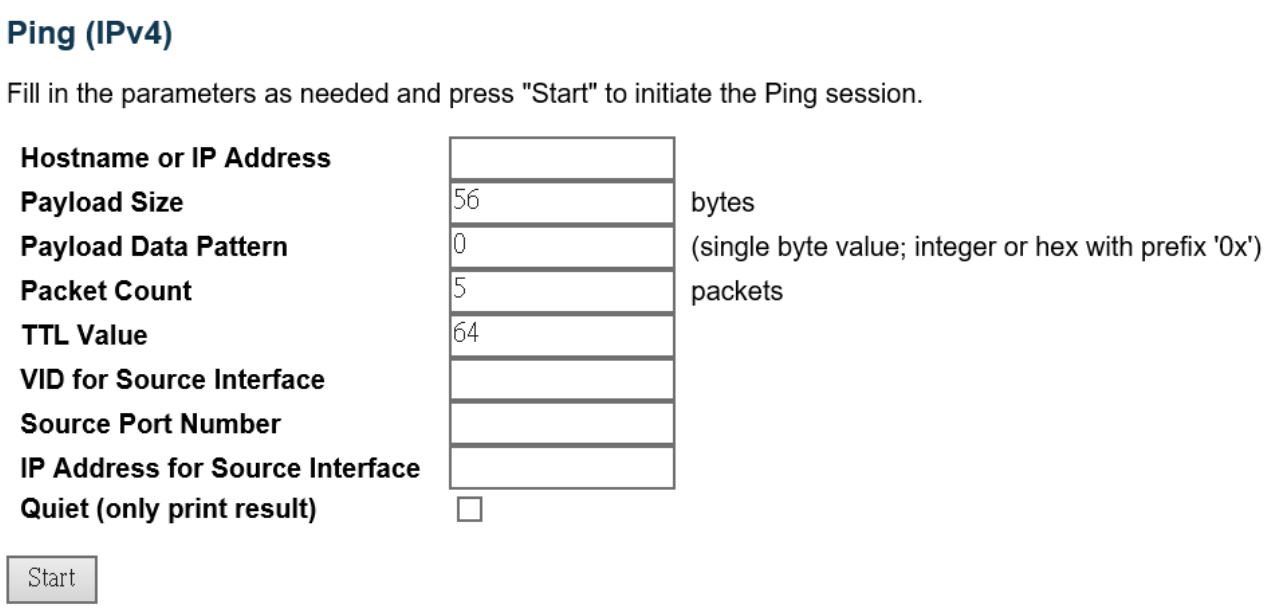
| | |
|---|---|
| Auto-refresh ☐ | Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |
| Refresh | Click to refresh the page. |

# 2.5 Diagnostics

## 2.5.1 Ping (IPv4)

This page allows you to issue ICMP PING packets to troubleshoot IP connectivity issues.

90W PoE Model




After you press 

, 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 ---

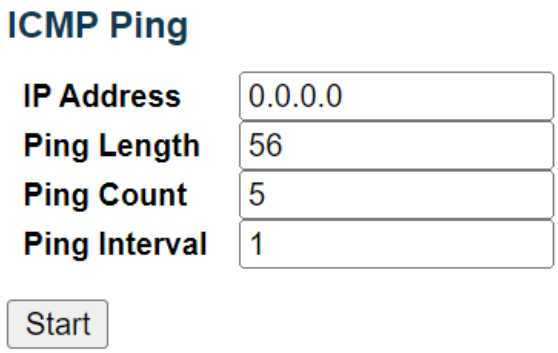
5 packets transmitted, 5 packets received, 0% packet loss

round-trip min/avg/max = 1.699/1.866/2.034 ms

| Object | 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.<br>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.<br>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.<br>Note: You may only specify either the VID or the IP Address for the source interface. |
| **Quiet (only print result)** | Checking this option will not print the result of each ping request but will only show the final result. |

| Buttons | |
|---|---|
| Start | Click to start transmitting ICMP packets. |
| New Ping | Click to re-start diagnostics with PING. |

30W PoE Model




After you press 

, 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 server 10.10.132.20, 56 bytes of data.

64 bytes from 10.10.132.20: icmp_seq=0, time=0ms

64 bytes from 10.10.132.20: icmp_seq=1, time=0ms

64 bytes from 10.10.132.20: icmp_seq=2, time=0ms

64 bytes from 10.10.132.20: icmp_seq=3, time=0ms

64 bytes from 10.10.132.20: icmp_seq=4, time=0ms

Sent 5 packets, received 5 OK, 0 bad

| Object | Description |
|---|---|
| **IP Address** | The destination IP Address. |
| **Ping Length** | The payload size of the ICMP packet. Values range from 2 bytes to 1452 bytes. |

| | |
|---|---|
| **Ping Count** | The count of the ICMP packet. Values range from 1 time to 60 times. |
| **Ping Interval** | The interval of the ICMP packet. Values range from 0 second to 30 seconds. |
| **Egress Interface (Only for IPv6)** | The VLAN ID (VID) of the specific egress IPv6 interface which ICMP packet goes.<br>The given VID ranges from 1 to 4094 and will be effective only when the corresponding IPv6 interface is valid.<br>When the egress interface is not given, PING6 finds the best match interface for destination.<br>Do not specify egress interface for loopback address.<br>Do specify egress interface for link-local or multicast address. |

| **Buttons** | |
|---|---|
| Start | Click to start transmitting ICMP packets. |
| New Ping | Click to re-start diagnostics with PING. |

## 2.5.2 Ping(IPv6)

This page allows you to issue ICMPv6 PING packets to troubleshoot IPv6 connectivity issues.

After you press Start, 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

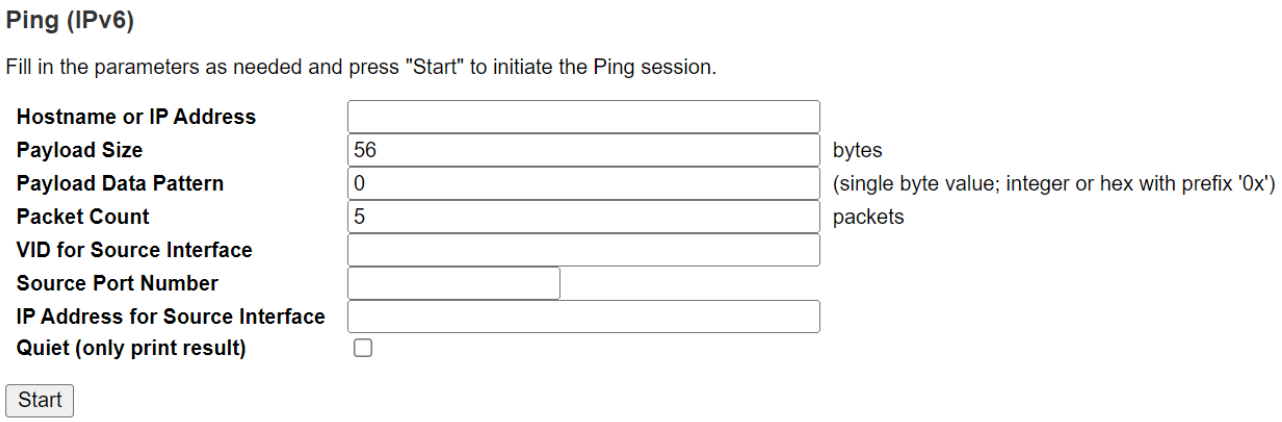
64 bytes from 2001::1: seq=4 ttl=64 time=1.845 ms

--- 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

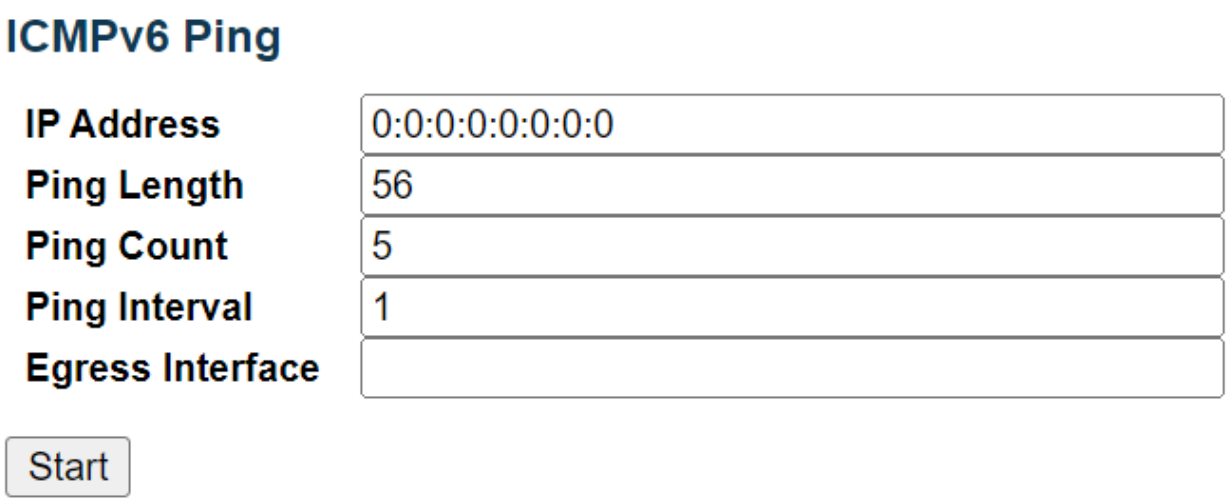
## 90W PoE Model




| Object | 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.<br>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.<br>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.<br>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. |

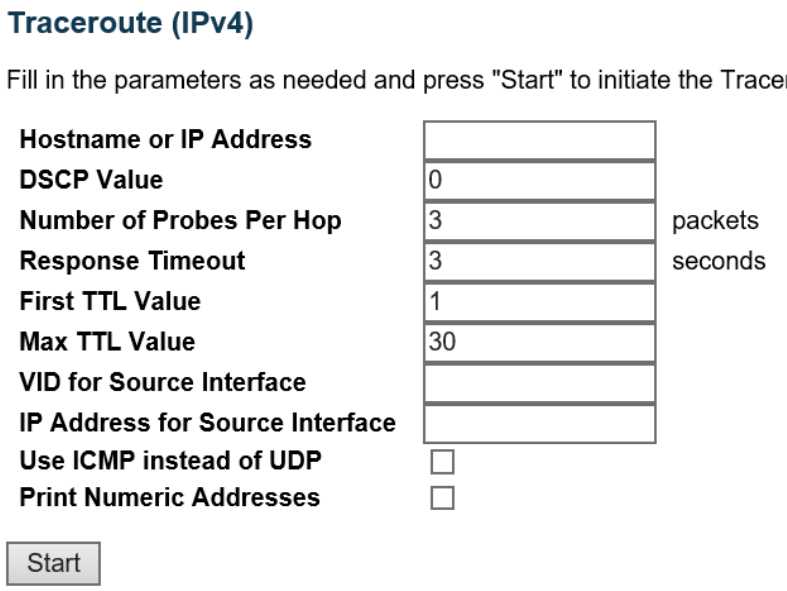
30W PoE Model




| Object | Description |
|---|---|
| **IP Address** | The destination IP Address. |
| **Ping Length** | The payload size of the ICMP packet. Values range from 2 bytes to 1452 bytes. |
| **Ping Count** | The count of the ICMP packet. Values range from 1 time to 60 times. |
| **Ping Interval** | The interval of the ICMP packet. Values range from 0 second to 30 seconds. |
| **Egress Interface (Only for IPv6)** | The VLAN ID (VID) of the specific egress IPv6 interface which ICMP packet goes. The given VID ranges from 1 to 4094 and will be effective only when the corresponding IPv6 interface is valid.<br>When the egress interface is not given, PING6 finds the best match interface for destination.<br>Do not specify egress interface for loopback address.<br>Do specify egress interface for link-local or multicast address. |

## 2.5.3 Traceroute (IPv4) (For 90W PoE Modle)

This page allows you to perform a traceroute test over IPv4 towards a remote host. traceroute is a diagnostic tool for displaying the route and measuring transit delays of packets across an IPv4 network.

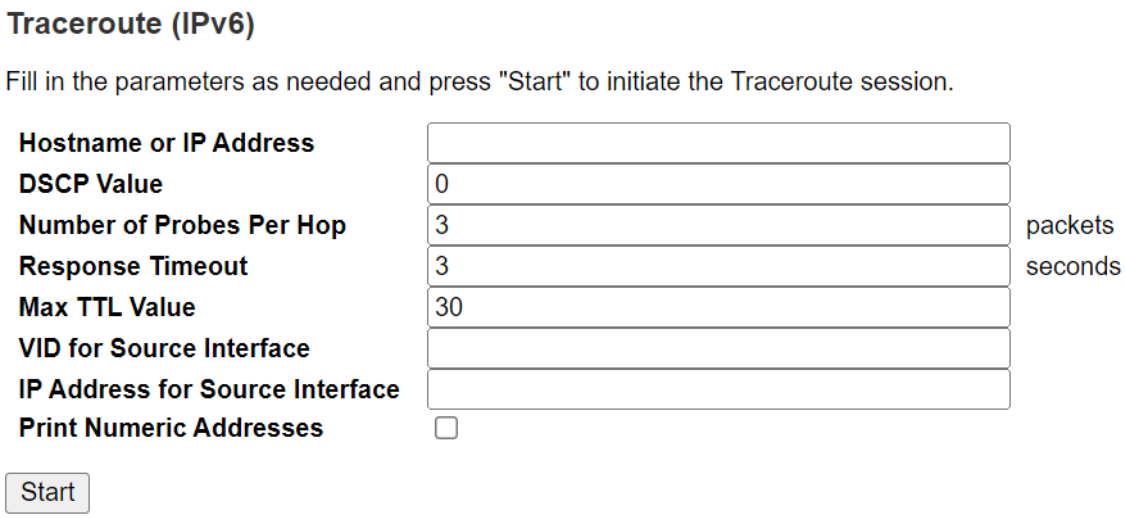



| Object | Description |
|---|---|
| **Hostname or IP Address** | The destination IP Address. |
| **DSCP Value** | This value is used for the DSCP value in the IPv4 header. The default value is 0. The valid range is 0-63. |
| **Number of Probes Per Hop** | Determines the number of probes (packets) sent 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.<br>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.<br>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. |

## 2.5.4 Traceroute (IPv6) (For 90W PoE Model)

This page allows you to perform a traceroute test over IPv6 towards a remote host. traceroute is a diagnostic tool for displaying the route and measuring transit delays of packets across an IPv6 network.




| Object | 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 255. 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.<br>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.<br>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. |

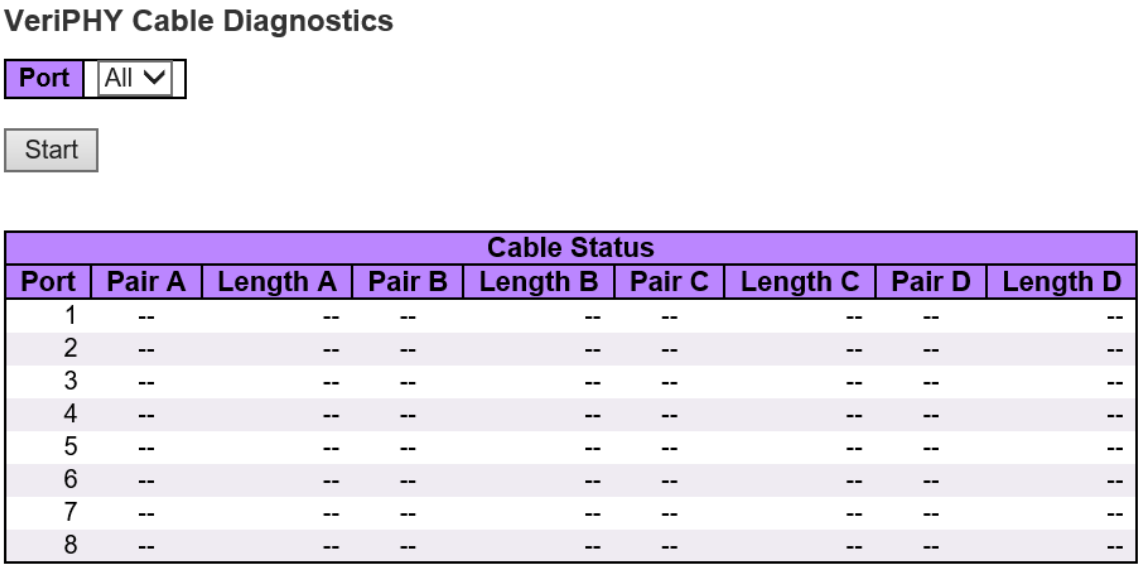
## 2.5.5 VeriPHY

This page is used for running the VeriPHY Cable Diagnostics for 10/100 and 1G copper ports.

Press 

to run the diagnostics. This will take approximately 5 seconds. If all ports are selected, this can take approximately 15 seconds. When completed, the page refreshes automatically, and you can view the cable diagnostics results in the cable status table. Note that VeriPHY is only accurate for cables of length 7 - 140 meters.

10 and 100 Mbps ports will be linked down while running VeriPHY. Therefore, running VeriPHY on a 10 or 100 Mbps management port will cause the switch to stop responding until VeriPHY is complete.




| Object | Description |
|---|---|
| **Port** | The port where you are requesting VeriPHY Cable Diagnostics. |
| **Cable Status** | **`Port`**:<br>Port number.<br>**`Pair`**:<br>The status of the cable pair.<br>OK - Correctly terminated pair<br>Open - Open pair<br>Short - Shorted pair<br>Short A - Cross-pair short to pair A |

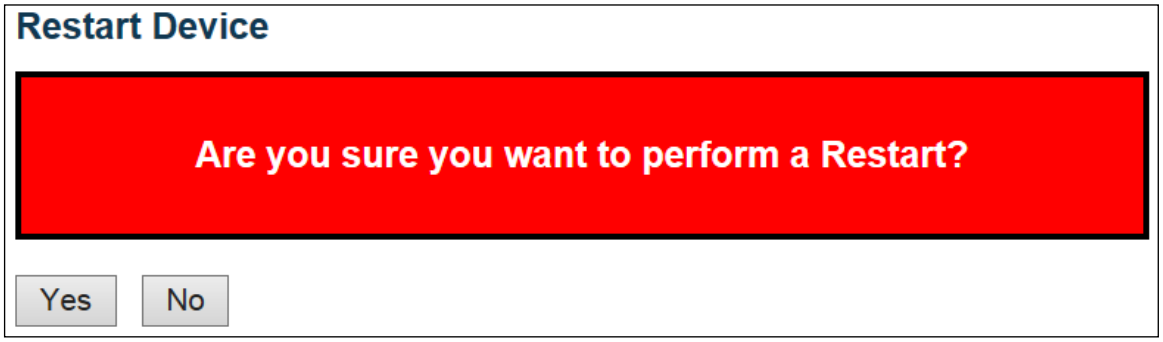
| | |
|---|---|
| | Short B - Cross-pair short to pair B<br>Short C - Cross-pair short to pair C<br>Short D - Cross-pair short to pair D<br>Cross A - Abnormal cross-pair coupling with pair A<br>Cross B - Abnormal cross-pair coupling with pair B<br>Cross C - Abnormal cross-pair coupling with pair C<br>Cross D - Abnormal cross-pair coupling with pair D<br>**Length**:<br>The length (in meters) of the cable pair. The resolution is 3 meters |

| Buttons | |
|---|---|
|  | Click to run the diagnostics. |

## 2.6 Maintenance

### 2.6.1 Restart Device

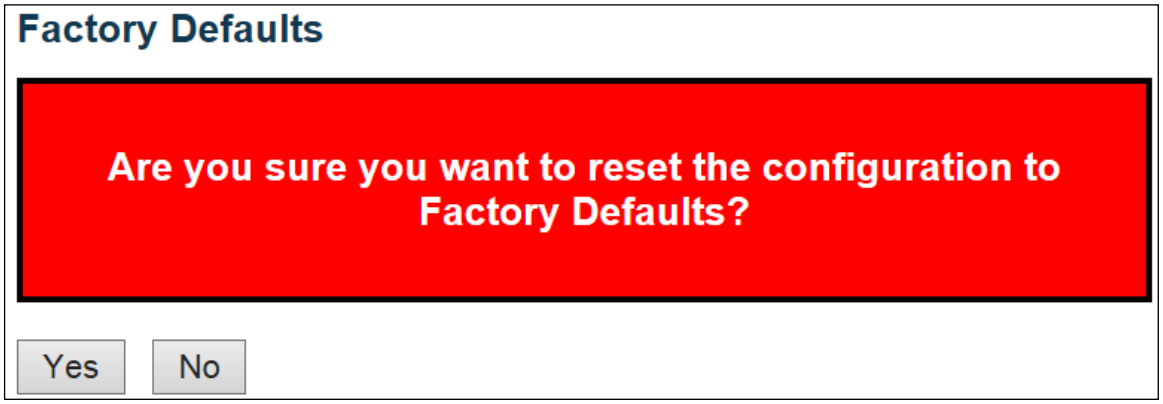
You can restart the switch on this page. After restart, the switch will boot normally.




| Buttons | |
|---|---|
| Yes | Click to restart device. |
| No | Click to return to the Port State page without restarting. |

## 2.6.2 Factory Default

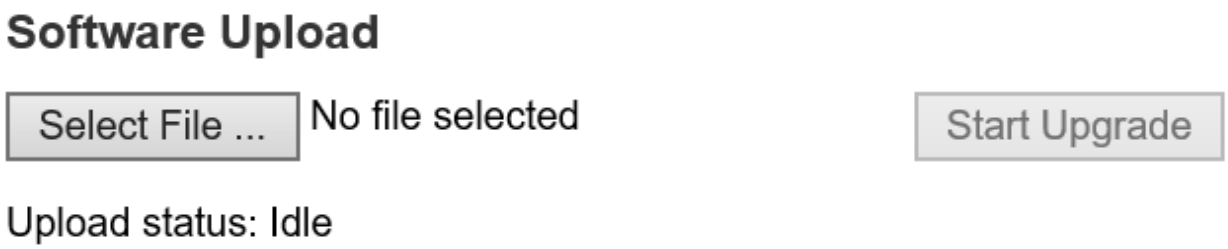
You can reset the configuration of the switch on this page. Only the IP configuration is retained. The new configuration is available immediately, which means that no restart is necessary.




| Buttons | |
|---|---|
| Yes | Click to reset the configuration to Factory Defaults. |
| No | Click to return to the Port State page without resetting the configuration. |

## 2.6.3 Software Upload

This page facilitates an update of the firmware controlling the switch.




| Buttons | |
|---|---|
| Select File ... | Go to find the software image and click Start Upgrade . |
| Start Upgrade | After finding the software image, click the button to update firmware. 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***:

***Do not restart or power off the device at this time*** *or the switch may fail to function afterwards*

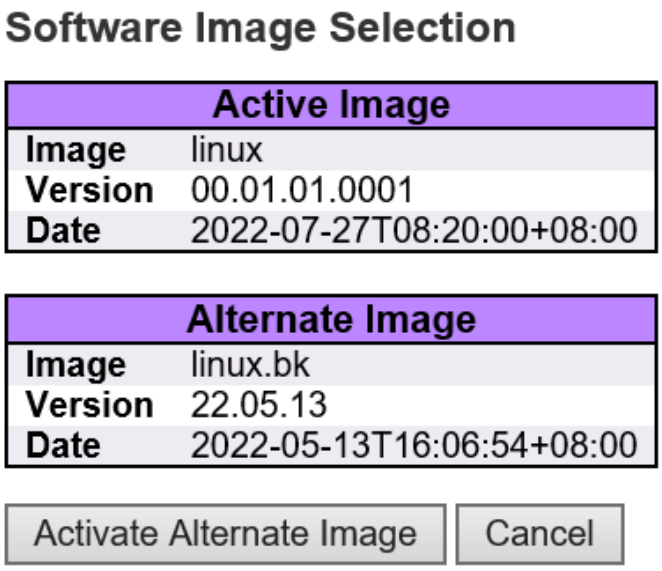
## 2.6.4 Software Upload

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

The web page displays two tables with information about the active and alternate firmware images.

Note:

1. 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.
2. 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.
3. The firmware version and date information may be empty for older firmware releases. This does not constitute an error.



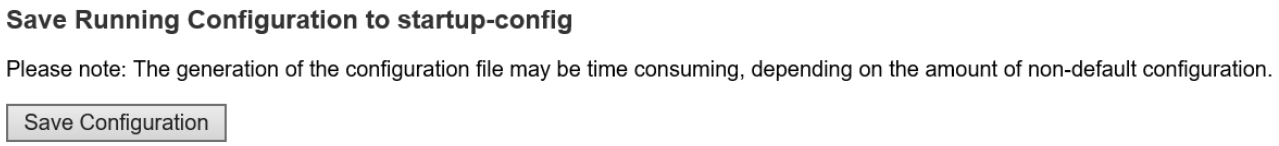

| Object | Description |
|---|---|
| **Image** | The flash index name of the firmware image. The name of primary (preferred) image is `image`, the alternate image is named `image.bk`. |
| **Version** | The version of the firmware image. |
| **Data** | The date where the firmware was produced. |

| Buttons |
|---|

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

## 2.6.5 Configuration - Save startup-config

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

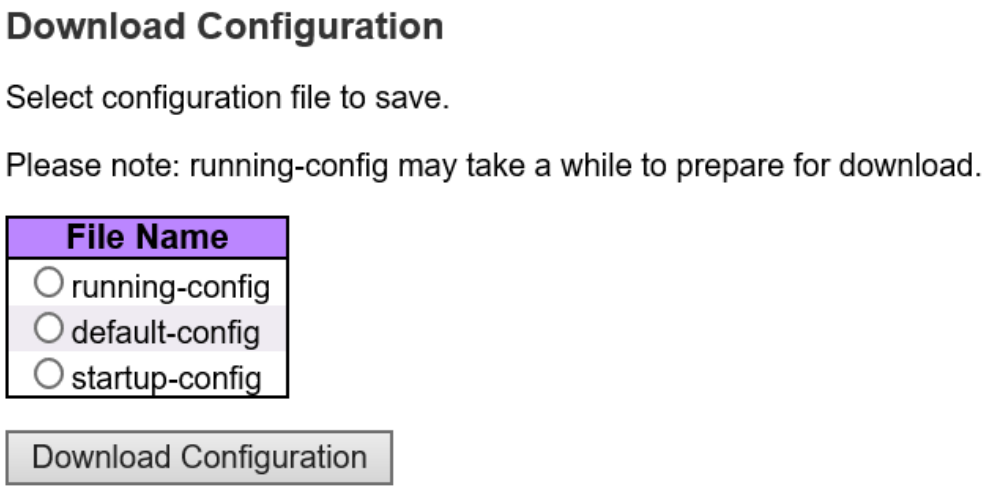



## 2.6.6 Configuration - Download

It is possible to download any of the files on the switch to the web browser. Select the file and click

Download Configuration .

Download *running-config* may take a little while to complete, as the file must be prepared for download.



## 2.6.7 Configuration - Upload

It is possible to upload a file from the web browser to all the files on the switch, except *default-config*, which is read-only.

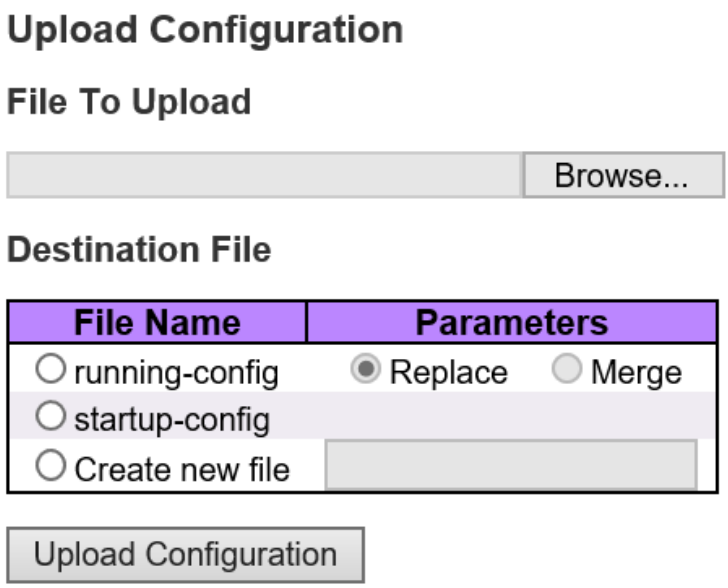
Select the file to upload, select the destination file on the target, then click Upload Configuration.

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 file system is full (i.e. contains the three system files mentioned above plus two other files), it is not possible to create new files, but an existing file must be overwritten or another deleted first.

90W PoE Model




30W PoE Model

## Upload Configuration

### File To Upload

Choose File No file chosen

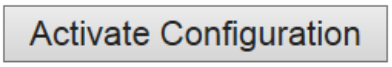
### Destination File

| File Name | Parameters |
| --- | --- |
| ○ running-config | ◉ Replace ○ Merge ☐ syntax_check |
| ○ startup-config | |
| ○ Create new file | |

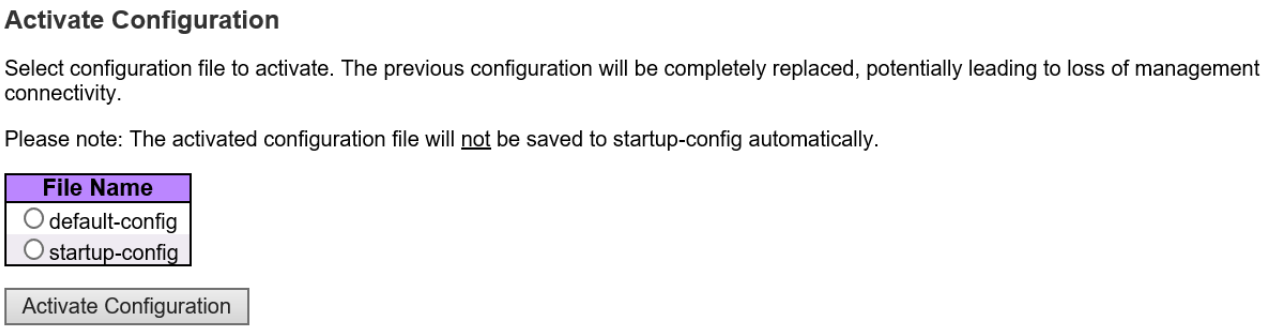
Upload Configuration

## 2.6.8 Configuration - Activate

It is possible to activate any of the configuration files present on the switch, except for *running-config* which represents the currently active configuration.

Select the file to activate and click 

. This will initiate the process of completely replacing the existing configuration with that of the selected file.




## 2.6.9 Configuration - Delete

It is possible to delete any of the writable files stored in flash, including *startup-config*. If this is done and the switch is rebooted without a prior Save operation, this effectively resets the switch to default configuration.